Galois action on families of generalised Fermat curves

Gareth A. Jones a, Manfred Streit b, Jürgen Wolfart c,∗

a School of Mathematics, University of Southampton, Southampton SO17 1BJ, UK
b Oppenheimer Strasse 36, D-60594 Frankfurt am Main, Germany
c Mathematisches Seminar der Universität, Postfach 111932, D-60054 Frankfurt am Main, Germany

Received 27 October 2005
Available online 13 November 2006
Communicated by Gernot Stroth

Abstract

It is well known that the complete bipartite graphs \( K_{n,n} \) occur as dessins d’enfants on the Fermat curves of exponent \( n \). However, there are many more curves having \( K_{n,n} \) as the underlying graph of their dessins, even if we require the strongest regularity condition that the graphs define regular maps on the underlying Riemann surfaces. For odd prime powers \( n \) these maps have recently been classified [G.A. Jones, R. Nedela, M. Škoviera, Regular embeddings of \( K_{n,n} \) where \( n \) is an odd prime power, European J. Combin., in press]; they fall into certain families characterised by their automorphism groups. In the present paper we show that these families form Galois orbits. We determine the minimal field of definition of the corresponding curves, and in easier cases also their defining equations.

© 2006 Elsevier Inc. All rights reserved.

Keywords: Dessins d’enfants; Complete bipartite graphs; Graph embeddings; Regular maps; Hypermaps; Galois orbits; Fermat curves

1. Introduction

Belyi’s Theorem [Bel], as extended by Grothendieck and others [G,CIW,VS,JS,W1] tells us that for a smooth complex projective algebraic curve \( X \) (which we shall identify with its associated Riemann surface), the following conditions are equivalent:

* Corresponding author. Fax: +49 (0) 69 798 28444.
E-mail addresses: g.a.jones@maths.soton.ac.uk (G.A. Jones), manfred.streit@bahn.de (M. Streit), wolfart@math.uni-frankfurt.de (J. Wolfart).

0021-8693/$ – see front matter © 2006 Elsevier Inc. All rights reserved.
doi:10.1016/j.jalgebra.2006.10.009
of algebraic numbers acts naturally on Belyï pairs \( \beta \). In general this seems to be a very difficult problem, but it is a little easier when \( \mathcal{M} \) is a regular map (one possessing the greatest symmetry), or equivalently \( \Gamma \) is a normal subgroup of \( \Delta \); in this situation (where \( X \) is known as a quasiplatonic surface, or one with many automorphisms) the orientation-preserving automorphism group \( \text{Aut}^+ \mathcal{M} \cong \Delta / \Gamma \) of \( \mathcal{M} \), which is isomorphic to the monodromy group of the unbranched covering induced by \( \beta \), can sometimes be exploited to give information about the function field of \( X \) [JNS].

A further problem is that of determining Galois orbits: the Galois group \( \text{Gal} \mathcal{Q}/\mathbb{Q} \) of the field \( \mathcal{Q} \) of algebraic numbers acts naturally on Belyï pairs \((X, \beta)\), by acting on the coefficients of the equations defining them, and this induces an action of this group on the associated maps. Each map lies in a finite orbit, and it is interesting to determine all those maps equivalent under this action to a given map. Since \( \text{Aut}^+ \mathcal{M} \) is an invariant of the action, knowledge of this automorphism group is again useful in solving this problem.

A particularly well-known example of a regular map is the standard embedding of the complete bipartite graph \( K_{n,n} \), introduced by Biggs and White [BW, §5.6.7] as a Cayley map for the cyclic group \( C_{2n} \) of order \( 2n \). In this case \( X \) is the Fermat curve \( x^n + y^n + z^n = 0 \), with Belyï function \( \beta : [x, y, z] \mapsto (x/z)^n \); as a covering, this is branched over 0, 1 and \( \infty \), and the embedded graph \( K_{n,n} \) is the inverse image in \( X \) of the unit interval, with \( n \) black and \( n \) white vertices covering 0 and 1 respectively, and one edge joining each black and white pair. Since \( X \) and \( \beta \) are defined over \( \mathbb{Q} \), this map \( \mathcal{M} \) has no other Galois conjugates.

The regular embeddings of \( K_{n,n} \) have recently been classified in the cases where \( n \) is an odd prime power \( p^e \) [JNS]. Our aim here is to obtain information for these embeddings analogous to that given above for the standard embedding. It is shown in [JNS] that if \( p \) is odd there are \( p^{e-1} \) regular embeddings \( \mathcal{M} \), and in each case \( \text{Aut}^+ \mathcal{M} \) is a semidirect product of a colour-preserving normal subgroup

\[
\text{Aut}^+ \mathcal{M} \cong G_f := \left\{ g, h \mid g^n = h^n = 1, \ h^q = h^{1+p^f} \right\} \quad (f = 1, 2, \ldots, e),
\]

by a complement \( C_2 \) transposing the vertex-colours; for each \( f \) there are \( \phi(p^{e-f}) \) regular embeddings, where \( \phi \) denotes Euler’s function. The unique embedding for \( f = e \) is the standard embedding, with \( \text{Aut}^+ \mathcal{M} \cong G_e \cong C_n \times C_n \) obtained by multiplying \( x \) and \( y \) by \( n \)th roots of \( 1 \).

In this paper we show that for each odd \( n = p^e \) and each possible value of \( f \) the \( \phi(p^{e-f}) \) maps with \( \text{Aut}^+ \mathcal{M} \cong G_f \) are defined over the cyclotomic field of \( p^{e-f} \)th roots of unity, and that they form a single orbit under the Galois group of this field. By exploiting the Galois correspondence...
between groups and fields, we determine the field of functions of the corresponding algebraic
curve \( X \), which we call a \textit{generalised Fermat curve}. For technical reasons, we are able to obtain
explicit equations for \( X \) only when \( f \geq e/2 \), so that \( G_f \) is relatively close to being abelian
and hence more of its subgroups correspond to radical field extensions. In each case, instead
of obtaining a planar model of the curve, we give a pair of equations between three affine (or
equivalently four projective) coordinates.

2. Notation, conventions and other preliminaries

We take our notation from [JNS], in particular: \( n \) is an odd prime power \( p^f \), and \( q := p^f + 1 \)
for some \( f = 1, \ldots, e \). The bipartite graph \( K_{n,n} \) has \( p^{e-1} \) regular embeddings \( M_{f,u} \) in orientable
surfaces \( X_{f,u} \) depending on \( f \) and \( u = 1, \ldots, p^{e-f} \) coprime to \( p \). The automorphism group \( G_f \)
of \( X_{f,u} \) and the vertex colours is a semidirect product \( C_n \rtimes C_n \) defined in
the introduction, and the embedding is characterised by the pair \((g^u, g^u h)\) of generators of \( G_f \)
as \textit{hypermap} or \textit{monodromy} group for \( M_{f,u} \) on \( X_{f,u} \), see Theorem 1 of [JNS] and its proof.
These two generators \( g^u \) and \( g^u h \) cyclically permute successive edges around a black and a white
vertex, following the orientation of the surface. However, in order to compare the multipliers of
the group generators (see Lemma 7 and Remark 5 in Section 3), it is more convenient to use
another pair of generators, giving rise to an isomorphic map and surface:

Lemma 1. If \( u' \equiv u \mod p^{e-f} \) then the pair \((g^u, (gh)^u)\) belongs to the \text{Aut} \( G_f \)-orbit of
\((g^u, g^u h)\).

Proof. From [JNS, (4.7)], we have

\[
(gh)^u' = g^u' h q^{u'-1+u'-2+\cdots+q+1}.
\]

The exponent of \( h \) is \( \not\equiv 0 \mod p \), and there is an \( i \equiv 1 \mod p^{e-f} \) with \( u_i \equiv u' \mod p^{e-f} \), so the
claim follows from [JNS, Proposition 16].

For this part of the paper we need more information about the conformal and arithmetic
structure of the underlying surfaces. We therefore need to say more about their construction. First
we observe that—again by [JNS, (4.7)]—both generators and their product have order \( n \) and
therefore we obtain

Lemma 2. The triangle group

\[
\Delta = [n, n, n] := \langle \gamma_0, \gamma_1, \gamma_\infty \mid \gamma_0^n = \gamma_1^n = \gamma_\infty^n = 1 = \gamma_0 \gamma_1 \gamma_\infty \rangle
\]

admits a homomorphism \( \pi_{f,u} \) onto \( G_f \) with torsionfree kernel \( \Gamma = \Gamma_{f,u} \) defined by

\[
\gamma_0 \mapsto g^u, \quad \gamma_1 \mapsto (gh)^u.
\]

For \( n > 3 \) the groups \( \Delta \) and \( \Gamma \) are cocompact Fuchsian groups acting on the upper half
plane \( \mathbb{H} \), and we may consider \( X_{f,u} \) as the \text{quotient} Riemann surface \( \Gamma_{f,u} \backslash \mathbb{H} \) on which the action
of the automorphism group \( G_f = \Delta / \Gamma_{f,u} \) is induced by the action of \( \Delta \) on \( \mathbb{H} \).
Remark 1. In the case \( n = 3 \) we have \( f = e = 1, u = 1 \), the groups act on the complex plane \( \mathbb{C} \), and the quotient surface will be an elliptic curve, more precisely the Fermat curve with exponent 3. Our main result is trivially true for this case, so we will always assume that \( n > 3 \) in order to avoid special considerations for genus 1.

Remark 2. There is a classical equivalence of categories between compact Riemann surfaces and smooth complex projective algebraic curves, so we will often speak of the Riemann surfaces \( X_{f,u} \) as algebraic curves. Moreover, the canonical projection

\[
\beta : X_{f,u} = \Gamma_{f,u} \backslash \mathbb{H} \to \Delta \backslash \mathbb{H} = \mathbb{P}^1(\mathbb{C})
\]

onto the Riemann sphere is ramified above only three points. These critical values are the \( \Delta \)-orbits of the fixed points of \( \gamma_0, \gamma_1, \gamma_\infty \) respectively, and can be identified with the points 0, 1, \( \infty \). Such a function \( \beta \) is a Belyı\' function, and its existence implies that, as an algebraic curve, \( X_{f,u} \) and \( \beta \) can be defined over a number field. We have an obvious action of the absolute Galois group \( \text{Gal} \bar{\mathbb{Q}}/\mathbb{Q} \) on the isomorphism classes of these models, defined by

\[
X_{f,u} \mapsto X_{f,u}^\sigma, \quad \beta \mapsto \beta^\sigma
\]

applying the conjugation \( \sigma \in \text{Gal} \bar{\mathbb{Q}}/\mathbb{Q} \) to all coefficients of \( \beta \) and of the equations defining \( X_{f,u} \). For the framework of this theory of dessin d’enfants see e.g. [JS,StW1] or [W2], also for the systematic interplay between maps and hypermaps, Belyı\' functions and triangle groups.

Remark 3. We may replace the triangle group \( \Delta \) with the triangle group \( \Delta \supset \Gamma_{f,u} \) to be introduced in Lemma 3. We then obtain in the same way as in Remark 2 a Belyı\' function \( B \) on \( X_{f,u} \) related to \( \beta \) by \( B = 4\beta(1 - \beta) \), now with ramification orders \( n, 2n \) above 0, 1, \( \infty \).

Lemma 3.

(a) If \( p > 3 \) and \( f \leq e - 1 \), or if \( p = 3 \) and \( f \leq e - 2 \), then a fixed triangle group \( \Delta = [2, n, 2n] \) is the normaliser \( N(\Gamma_{f,u}) \) for all \( f \) and \( u \). The automorphism group \( \text{Aut} X_{f,u} = \tilde{G}_f \) is an extension of \( G_f \) by \( C_2 \).

(b) If \( f = e \), or if \( p = 3 \) and \( f = e - 1 \), then \( N(\Gamma_{f,u}) \) is a triangle group \( \Delta = [2, 3, 2n] \) and \( \text{Aut} X_{f,u} = \tilde{G}_f \), an extension of \( G_f \) by \( S_3 \).

Proof. In all cases, since \( X_{f,u} \) carries a regular map \( M \), it follows that \( \Gamma_{f,u} \) is a normal subgroup of a triangle group \( \Delta \) of type \([2, n, 2n]\), more precisely that triangle group (among three possible ones of the same signature) whose order 2 generator has its fixed point at the hyperbolic midpoint of the fixed points of \( \gamma_0 \) and \( \gamma_1 \) of \( \Delta \). The automorphism group \( \text{Aut} X_{f,u} \cong N(\Gamma_{f,u})/\Gamma_{f,u} \) of \( X_{f,u} \) contains the automorphism group \( \tilde{G}_f \cong \Delta/\Gamma_{f,u} \) of \( M \). The subgroup \( G_f = \text{Aut}_0^+ M \) of \( \text{Aut}^+ M \) lifts to the triangle group \( \Delta \) of type \([n, n, n]\) which has index 2 in \( \Delta \). Now \( N(\Gamma_{f,u}) \) is a Fuchsian group containing \( \Delta \), and by results of Singerman [Si] the only Fuchsian group properly containing \( \Delta \) is a triangle group \( \Delta \) of type \([2, 3, 2n]\), which contains \( \Delta \) as a non-normal subgroup of index 3, so \( N(\Gamma_{f,u}) \) must be either \( \Delta \) or \( \Delta \). In either case, \( \Delta \) is a normal subgroup of \( N(\Gamma_{f,u}) \), with quotient \( C_2 \) or \( S_3 \) respectively, so \( G_f \) is a normal subgroup of \( \text{Aut} X_{f,u} \) with the same quotient. These two possibilities correspond to the cases N8 and N7 of [BCC]. The latter case occurs if and only if \( G_f \) has an automorphism \( \theta \) inducing a 3-cycle on its corresponding...
generators $g^u$, $(gh)^u$ and $(g^u(gh)^u)^{-1}$. It is clear that if $f = e$, so that $G_f \cong C_n \times C_n$, then such an automorphism exists, induced by an order 3 element of $\Delta$ acting by conjugation on $\Delta$. So we may assume that $f < e$.

Since $f < e$, Proposition 16 of [JNS] implies that the automorphisms of $G_f$ are the mappings given by $g \mapsto g^ih^j$, $h \mapsto g^kh^l$ where $i, j, k, l \in \mathbb{Z}_n$ with $i \equiv 1 \mod (p^{e-f})$, $k \equiv 0 \mod (p^{e-f})$, and $l \not\equiv 0 \mod (p)$. In our case we require that $\theta$ sends $g$ to $gh$, and sends $gh$ to $(g^u(gh)^u)^{-u}$, where $uu' \equiv 1 \mod (n)$, so it sends $h$ to $(gh)^{-1}(g^u(gh)^u)^{-u}$; this is in $g^{3}(h)$, so $k \equiv -3 \mod (n)$. Since $k \equiv 0 \mod (p^{e-f})$ for each automorphism, we see that if $\theta$ exists then $p = 3$ and $f = e - 1$.

Conversely, let $p = 3$ and $f = e - 1$. If $\Phi$ denotes the Frattini subgroup of $G_f$ (generated by $p$th powers and commutators) then $(gh)^{-1}(g^u(gh)^u)^{-u} \in g^{-3}h^{-2}\Phi = h\Phi$, so $(gh)^{-1}(g^u(gh)^u)^{-u} = g^{-3}h^l$ for some $l \in \mathbb{Z}_n$ with $l \equiv 1 \mod (3)$. By taking this value of $l$, together with $i = j = 1$ and $k = -3$, we obtain the required automorphism $\theta$ of $G_f$. \qed

With respect to Remark 1, we will call the curves $X_{f,u}$ generalised Fermat curves. By abuse of notation we will also denote their isomorphism classes by $X_{f,u}$. For the following it is important to note that these $n/p = p^{e-1}$ curves are pairwise non-isomorphic.

**Lemma 4.** $X_{f,u} \cong X_{g,v}$ if and only if $f = g$ and $u \equiv v \mod (p^{e-f})$.

**Proof.** The *if* part follows from Lemma 1. For the *only if* part, $f = g$ is a necessary condition since otherwise the automorphism groups would not be isomorphic. If the curves are isomorphic, their surface groups $\Gamma_{f,u}$ and $\Gamma_{f,v}$ are conjugate by some $\alpha \in \text{PSL}_2 \mathbb{R}$, hence also their normalisers. By Lemma 3 the normalisers coincide and are their own normalisers, therefore $\alpha \in N(\Gamma_{f,u})$, hence $X_{f,u} = X_{f,v}$. One may also apply Theorem 5 and Table 1(iiib) of [GW] in case (a) of Lemma 3 and [GW, Corollary 11] in case (b). \qed

3. The main result

With these notations and preparations, we obtain

**Theorem 1.** For fixed $e$, $f$ and odd prime $p$ the generalised Fermat curves $X_{f,u}$, $u \in (\mathbb{Z}/p^{e-f}\mathbb{Z})^*$, form an orbit under the action of the absolute Galois group $\text{Gal} \overline{\mathbb{Q}}/\mathbb{Q}$.

**Proof.** Galois conjugation preserves the order of ramification of all Belyi functions and maps the automorphism group of the curve onto an isomorphic group. Therefore for all $\sigma \in \text{Gal} \overline{\mathbb{Q}}/\mathbb{Q}$ and all curves $X_{f,u}$ in question we have

$$X_{f,u}^\sigma \cong X_{f,v} \quad \text{for some } v \in (\mathbb{Z}/p^{e-f}\mathbb{Z})^*,$$

defining an action of $\text{Gal} \overline{\mathbb{Q}}/\mathbb{Q}$ on the set of prime residue classes $(\mathbb{Z}/p^{e-f}\mathbb{Z})^*$. We will show that this action is transitive, following the pattern of proof indicated in [St2] and [StW1], i.e. by the study of the Galois action on the multipliers.

To recall their definition, let $a$ be an automorphism of a Riemann surface $X$ with fixed point $P$. If $z$ is a local coordinate on $X$ in a neighbourhood of $P$ with $z(P) = 0$ then

$$z \circ a = \xi z + \text{higher order terms in } z,$$
and we call $\xi$ the multiplier of $a$ at $P$. Clearly, if $a$ is an automorphism of order $n$ then $\xi$ is an $n$th root of unity independent of the choice of $z$. By [StW2, Lemma 4] we have

**Lemma 5.** If $X$ has genus $g > 1$ and is defined over a number field, then $a$ is also defined over a number field, $P$ is a $\overline{Q}$-rational point of $X$, and for all $\sigma \in \text{Gal} \overline{Q}/Q$, Galois conjugation of the coefficients by $\sigma$ gives an automorphism $a^\sigma$ of $X^\sigma$ with multiplier $\sigma(\xi)$ at its fixed point $P^\sigma$.

The next step is the determination of the multipliers for the generators of $G_f$ on the curves $X_{f,u}$.

**Lemma 6.** The generator $g^u$ of $G_f$ has $pf$ fixed points on $X_{f,u}$.

For the proof of the lemma, recall that $G_f$ acts transitively on the set of black vertices of the embedded bipartite graph $K_{n,n}$, and that the subgroup $\langle g^u \rangle = \langle g \rangle$ can only have such black vertices as fixed points $P$. Then $\langle g \rangle$ is the subgroup stabilising $P$, and the number of its fixed points is its index $|N_{G_f}(\langle g \rangle) : \langle g \rangle|$ in its normaliser. By [JNS, (4.5)] this normaliser is $\langle g, h_{pf-e-f} \rangle \cong C_p \times C_{pf}$.

Theorem 1 of [JNS] shows that $g^u$ defines a rotation around a black vertex, sending each incident edge to the (counterclockwise) next one. This is in fact true for all fixed points of $g^u$ since the powers of $h_{pf-e-f}$ permuting these fixed points commute with $g^u$. As a consequence we have

**Lemma 7.** Let $u'$ be the inverse of $u$ in $\mathbb{(Z/nZ)}^*$ and $\xi := e^{2\pi i/n}$. Then the automorphism $g$ has multiplier $\xi^{u'}$ at each of its fixed points on $X_{f,u}$.

Together with Lemma 5, this completes the proof of Theorem 1: choose $\sigma \in \text{Gal} \overline{Q}/Q$ such that $\sigma(\xi) = \xi^{u'}$. Then we have $X_{\sigma f,1} \cong X_{f,u}$ giving the transitivity of the Galois action on the isomorphism classes of curves in question.

**Remark 4.** It is instructive to shed some light on the case $u' \not\equiv 1 \mod p^e$, but $\equiv 1 \mod p^{e-f}$. Then the kernels $\Gamma_{f,u}$ and $\Gamma_{f,1}$ of the two epimorphisms $\pi_{f,u}$ and $\pi_{f,1}$ onto $G_f$ are equal, differing by composition with an automorphism of $G_f$. The Galois conjugation given above does not change the curve $X_{f,1}$ but has a non-trivial effect on the multipliers because it changes the generators of $G_f$ and their fixed points. Of course the same kind of Galois conjugation of a curve $X_{f,u}$ into an isomorphic curve $X_{\sigma f,u} \cong X_{f,v}$ happens for $u \equiv v \mod p^{e-f}$.

**Remark 5.** We can play the same game as in the proof of Theorem 1 with the other generator $(gh)^u$ of $G_f$. This also has $pf$ fixed points with multiplier $\xi$. The $\pi_{f,u}$-image of $\gamma_{\infty}$ is

$$(g^u(gh)^u)^{-1} = g^{-2u}h^l$$

for some exponent $l \mod n$, and this element has also $pf$ fixed points, all with multiplier $\xi$.

**Theorem 2.** For fixed $e$, $f$ and odd prime $p$, let $\eta$ be the root of unity $\exp(2\pi i/p^{e-f})$. Then the generalised Fermat curves $X_{f,u}$, $u \in \mathbb{Z}/p^{e-f}\mathbb{Z}^*$, can be defined over the cyclotomic field $\mathbb{Q}(\eta)$. 
Proof. Suppose that $\sigma \in \text{Gal} \overline{Q}/Q(\eta)$, so $\sigma(\zeta) = \zeta^k$ for some $k \equiv 1 \mod p^{e-f}$. The action on the multipliers—see Lemma 7 and Remark 4—shows that $X_{f,u}^\sigma \cong X_{f,u}$ whence the moduli field of all these curves $X_{f,u}$ is contained in $Q(\eta)$. On the other hand, the moduli field cannot be strictly contained in $Q(\eta)$ since otherwise the Galois orbits would not contain $\phi(p^{e-f})$ non-isomorphic curves as predicted by Theorem 1. Finally the moduli field of the curves $X_{f,u}$ is a field of definition because this is true for all curves with a regular dessin (they are quasiplatonic, or in older terminology they have many automorphisms), see [W2, Theorem 5].

Remark 6. As Bernhard Köck has pointed out, the original proof of this result for quasiplatonic curves, given in [W1, Remark 4], is incomplete, and a full version can be found in [W2]. However the original proof is valid whenever the canonical covering of $\mathbb{P}^1$ has pairwise distinct ramification orders over 0, 1 and $\infty$, as happens here by Lemma 3.

Remark 7. The Galois conjugations $\sigma \in \text{Gal} \overline{Q}/Q$ induce the effect of Wilson’s operations $H_j$ on the embedded complete bipartite graphs $\mathcal{M}_{f,u}$, see [JNS, end of Section 7], [Wi].

4. Defining equations

With the moduli field known, it is now interesting to provide the defining equations of the corresponding curves. We do this for the cases $2f \geq e$. Certainly it is enough to give explicit equations for the curve $X_{f,u} = 1$ as a representative of the Galois orbit $X_{f,u}$ under the action of $\text{Gal} \overline{Q}/Q$. Although the construction is straightforward, we have to split it into several steps. For the moment we are not interested in different epimorphisms $\pi_{f,u}$ so we omit the parameter $u = 1$ and simply write $\pi_f$. All subgroups $U$ of $G_f$ correspond to some Fuchsian group $\Gamma_U := \pi_f^{-1}(U)$. If we have two subgroups $U \subset G$ of $G_f$ then all elements $g \in G$ act naturally on the cosets $U \setminus G$ by multiplication on the right. As permutations of cosets they will be denoted by $\tau_g$. We use them to describe the action of the generators of $\Gamma_G$ on the cosets of $\Gamma_U \setminus \Gamma_G$ and to determine generators of $\Gamma_U$ in terms of generators of $\Gamma_G$. Finally one can give the signature of $\Gamma_U$ and construct a fundamental domain for $\Gamma_U$ consisting of $[G : U]$ copies of a fundamental domain for $\Gamma_G$. In using these arguments we follow Singerman [Si]. We will again use $X_U$ as our notation for both the Riemann surface which is isomorphic to the quotient $\Gamma_U \setminus \mathcal{H}$ and the corresponding algebraic curve, as in Remark 2. Its genus will be denoted by $g(X_U)$ and $F(X_U)$ will be the function field of $X_U$. In this notation our aim is to describe the function field extension $\mathcal{F}(X_{(1)})/\mathcal{F}(X_{G_f})$. Again by Remark 2 it is clear that $\Gamma_{G_f} = \Delta$, $X_{G_f} = \mathbb{P}^1(\mathbb{C})$ and $\mathcal{F}(X_{G_f}) = \mathbb{C}(\beta)$.

Lemma 8. For the subgroup $H := \langle h \rangle \subset G_f$ the following statements are true:

(i) $\Gamma_H$ has signature $[g(X_H); 0]$ where $g(X_H) = (p^e - 1)/2 = (n - 1)/2$.
(ii) $\Gamma_H$ is a normal subgroup of $\Delta$ with a cyclic quotient $\mathbb{C}_n$.
(iii) $\mathcal{F}(X_H)/\mathbb{C}(\beta)$ is a radical extension of degree $n = p^e$.
(iv) $\mathcal{F}(X_H) = \mathbb{C}(v, \beta)$ with $v^n = \beta \cdot (\beta - 1)$.

Proof. The first point follows from the third paragraph of [JNS, §8]. However, since we will use it in the last point, we give a direct calculation of the signature of $\Gamma_H$. The elliptic periods of
Γ_H are obtained from the cycles of γ_0, γ_1 and γ_∞ on the cosets of Γ_H in Δ. Each cycle of γ_0 of length l less than the order n = p^e of γ_0 corresponds to an elliptic period n/l. Since Γ_H is a normal subgroup of Δ the cycles of γ_0 all have the same length l, and since γ_0 is mapped to a generator of the cyclic group Δ/Γ_H ≅ G_f/H of order n—giving statement (ii) of the lemma as a by—product—it has a single cycle of length l = n. Thus γ_0 induces no elliptic periods of Γ_H, and the same applies to γ_1 and γ_∞, which are mapped to Hg and Hg^{-2}, so Γ_H has no elliptic periods. The genus of the curve can be easily calculated from the index formula.

In terms of surfaces the triangle group corresponds to the Riemann sphere X_G, with function field C(β), and F(X_H) corresponds to a radical extension ramified only above 0, 1, ∞. This already shows that an equation of the form

\[ v_{β}^p = β^{r} \cdot (β - 1)^{s} \]

must hold. To see that we may choose r = s = 1 recall that by Remark 3 there is a Belyï function B = 4β(1 − β) corresponding to the triangle group Δ such that \( F(X_H) \) is a cyclic extension of \( C(β) \) of degree 2n. Since (2, n) = 1 we may write it as the composition of the quadratic extension \( C(β)/C(β) \) with a cyclic degree n extension of \( C(β) \). It is easy to see that this cyclic extension is ramified only above B = 0 and ∞, and is therefore defined by an equation \( v^{n} = -\frac{1}{4}B \). □

We will now establish the defining equation of the function field X_G where G := ⟨g⟩ ⊂ G_f. Note that Γ_G is not a normal subgroup of the triangle group Δ, but in the case of 2f ≥ e we can split the extension into two normal extensions. For the following we suppose that 2f ≥ e. In this case \( q' := 1 - p^{-f} \) is a representative of the multiplicative inverse of q mod p^e and we note that \( q' \equiv 1 \mod p^{e-f} \). Furthermore we have ghg^{-1} = h^{q'}. Let

**Lemma 9.**

(i) The subgroup U := ⟨g, h^{p^{-f}}⟩ ⊂ G_f is an abelian normal subgroup of G_f of index p^{e-f}.
(ii) The Fuchsian group Γ_U has signature \([0; p^e, \ldots, p^e, p^{f}, p^f]\) where the entry p^e is repeated \(p^{e-f}\) times.
(iii) The function field F(X_U) = C(w, β) is given by the equation

\[ w^{p^{e-f}} = 1 - β. \]

**Proof.** Clearly U is a normal subgroup of G_f with a quotient isomorphic to \( C_{p^{e-f}} \) as \( ⟨h^{p^{e-f}}⟩ \) has order \( p^f \) and lies in the centre of G_f, cf. [JNS]. To prove the second statement we again study the cycle structure of the action of the generators g, gh, h^{-1}g^{-2} on the left cosets of U. The permutation \( τ_g \) induced by g is the identity, while gh and h^{-1}g^{-2} induce mutually inverse cycles of length p^{e-f}, so the elliptic periods of Γ_U are as claimed. The genus can be easily calculated from the index formula for Fuchsian groups, and the function field extension is determined as in the previous lemma. □

For the second step we need to know the generators of Γ_U.

**Lemma 10.** A set of generators for the Fuchsian group Γ_U := π_f^{-1}(U) with signature \([0; p^e, \ldots, p^e, p^{f}, p^{f}]\) is given by \( γ_0, γ_1γ_0γ_1^{-1}, \ldots, γ_{p^{e-f}-1}γ_0γ_1^{-p^{e-f}+1}, γ_{p^{e-f}}, γ_{p^{e-f}} \).
Proof. The proof directly follows from [Si]. □

Remark 8. The quotient \( \Gamma U \backslash H \) is isomorphic to the Riemann sphere and can be identified with the function field \( \mathbb{C}(w) \), where \( w \) is as in the preceding lemma. The elliptic fixed points of the generating elements \( \gamma_0, \gamma_1 \gamma_0 \gamma_1^{-1}, \ldots, \gamma_1^{p^e-f-1} \gamma_0^{-1} \gamma_1^{p^e-f+1} \) will therefore be identified with

the preimages of \( \beta = v = 0 \) which are \( w = 1, \xi_{p^e-f}, \ldots, \xi_{p^e-f-1} \). The identification can be done in precisely this order: \( \gamma_1 \) acts on the branches of \( \beta \) by multiplication \( w \mapsto \xi_{p^e-f} w \), these branches correspond to the cosets of \( U \) and \( g \) fixes all cosets \( U h^i \). So we may replace the cosets \( U, U h, \ldots, U h^{p^e-f-1} \) by \( U, U (gh), \ldots, U (gh)^{p^e-f-1} \) to see that \( 1, \gamma_1, \ldots, \gamma_1^{p^e-f-1} \) form a set of Schreier coset representatives of \( \Delta \) modulo \( \Gamma U \) on which \( \gamma_1 \) acts by cyclic permutation in the same way as it acts on the fixed points of the elliptic generators given above.

Lemma 11. The group \( G := \langle g \rangle \) is a normal subgroup of index \( p^f \) in \( U \) with cyclic quotient. Let \( \eta \) be the root of unity \( \exp(2\pi i / p^e-f) \). The function field \( \mathcal{F}(X_G) \) is given as a relative function field extension \( \mathbb{C}(z, w)/\mathbb{C}(w) \) by the equation

\[
z^{p^f} = w^{-r} \prod_{k=0}^{p^e-1} (w - \eta^k)^{a_k},
\]

where \( a := p^{2f-e} \) and the exponent \( r := (q^{p^e-f} - 1)/p^e \) is an integer coprime to \( p \).

Proof. Again we need to study the action of the generators of \( \Gamma U \) on the left \( G \)-cosets in \( U \).

These cosets are given by \( G h^{-p^e-f}, G h^{-2p^e-f}, \ldots, G h^{-p^f} \) = \( G \). Clearly \( g \) again acts trivially on these cosets, as the coset representatives belong to the centre of \( G_f \). Therefore \( \tau_g \) is the identity. The equations \( \pi_f (\gamma_1 \gamma_0 \gamma_1^{-1}) = ghg^{-1} g^{-1} = gh^{-p^f} \) show that the operation of \( \gamma_1 \gamma_0 \gamma_1^{-1} \) on the cosets is given by the multiplication by \( h^{-p^f} \). By induction—recall that also \( h^{p^f} \) lies in the centre of \( G_f \)—we find that \( (gh)^k \cdot g \cdot (gh)^{-k} = h^{-kp^f} \cdot g = gh^{-kp^f} \).

Numbering the cosets in the order given above, we see that \( h^{-p^f} \) acts as the permutation \( (12 \ldots p^f) \), so \( h^{-p^f} = (h^{-p^e-f})^a \) acts as \( (12 \ldots p^f)^a \) and hence the permutations \( \tau_{(gh)^k g (gh)^{-k}} \) can be written as

\[
\tau_{(gh)^k g (gh)^{-k}} = (12 \ldots p^f)^{ak}.
\]

The remaining point is to show that \( (gh)^{p^e-f} \) acts as \( (12 \ldots p^f)^{-r} \) with \( r \) coprime to \( p \). By [JNS, (4.7)] we have

\[
(gh)^{p^e-f} = g^{p^e-f} \cdot h^s,
\]

where

\[
s = \frac{q^{p^e-f} - 1}{p^f}.
\]
By [JNS, Lemma 6] we find that \( p^e \| q^{p^{e-f}} - 1 \) and \( p^{e-f} \| s \), which is equivalent to the equation \( r \cdot p^{e-f} = s \) with \( r \) coprime to \( p \). Therefore \((gh)^{p^{e-f}}\) acts as multiplication by \( h^{rp^{e-f}} \) on the right cosets. Since \( \mathcal{F}(X_G)/\mathcal{F}(X_U) \) is a cyclic field extension of degree \( pf \), it is generated by some \( z \) such that \( z^{pf} \) is a rational function of \( w \). We know the possible linear factors of this rational function since ramification occurs precisely at 0, \( \infty \) and the points \( \eta^k \). To determine the exponents of the linear factors, identify the cosets with the branches of the covering

\[
X_G \to X_U : (z, w) \mapsto w
\]

and consider small loops around the critical values—corresponding to the generators found in Remark 8 and to \( \gamma_1^{p^{e-f}} \)—to compare the effect on the branches. □

**Theorem 3.** Suppose that \( p \) is an odd prime and \( 2f \geq e \). Then the equations in Lemma 8, Lemma 9 and Lemma 11 define an affine model of the generalised Fermat curve \( X_{f,1} \) in \( \mathbb{C}^3 \).

**Proof.** The statement follows from the fact that \( \langle g \rangle \) and \( \langle h \rangle \) intersect trivially in \( G_f \) but together generate the whole group. By Galois theory we find that the composite field \( \mathbb{C}(z, w, \beta) \cdot \mathbb{C}(v, \beta) \) is the function field of \( X_{f,1} \). Lemma 9 allows one to eliminate \( \beta \). □

5. Concluding remarks

5.1. Some common quotients

Even if we do not impose the assumption \( 2f \geq e \) made in Section 4, we can describe in a very explicit way—using the same notation—some interesting subfields of the function field \( \mathcal{F}(X_{f,u}) = \mathcal{F}_{(1)} \) or, in other words, quotients of the curves \( X_{f,u} \) by some particular subgroups of \( G_f \). These quotients turn out to be described by equations over \( \mathbb{Q} \), hence invariant under the Galois action, so they depend only on \( f \), not on \( u \in (\mathbb{Z}/p^{e-f} \mathbb{Z})^* \).

**Theorem 4.** Under the hypotheses of Section 2 and in the notation of Section 4 we have

1. \( X_{(g, hp^f)} \) is a cyclic cover of \( \mathbb{P}^1(\mathbb{C}) \) of degree \( pf \), with function field \( \mathbb{C}(y, \beta) \) such that
   \[
y^{pf} = 1 - \beta.
   \]
2. \( X_{(gh, hp^f)} \) is a cyclic cover of \( \mathbb{P}^1(\mathbb{C}) \) of degree \( pf \), with function field \( \mathbb{C}(x, \beta) \) such that
   \[
x^{pf} = \beta.
   \]
3. \( X_{(p^{pf}, hp^f)} \) is an abelian cover of \( \mathbb{P}^1(\mathbb{C}) \) with covering group \( C_{pf} \times C_{pf} \) and with function field \( \mathbb{C}(x, y) \) such that
   \[
x^{pf} + y^{pf} = 1.
   \]
4. $X_{(h^{p^f})}$ is an abelian cover of $\mathbb{P}^1(\mathbb{C})$ with covering group $C_n \times C_{pf}$ and with function field $\mathbb{C}(x, y, v)$ such that

$$x^{p^f} + y^{p^f} = 1 \quad \text{and} \quad xy = v^{p^{e-f}}.$$

5. The full function field $\mathcal{F}(X_{f,u}) = \mathcal{F}_{(1)}$ is an unramified cyclic extension of $\mathcal{F}_{(h^{p^f})}$ of degree $p^{e-f}$.

**Proof.** The first two claims can be proved precisely as in Lemma 9. In fact, both curves have genus 0. For the third claim we observe that the subgroups $\langle g, h^{p^f} \rangle$ and $\langle gh, h^{p^f} \rangle$ generate the group $G_f$ and intersect in the normal subgroup $\langle g^{p^f}, h^{p^f} \rangle$. The quotient is commutative since $\langle h^{p^f} \rangle$ (the subgroup in (4)) is the commutator subgroup of $G_f$. Therefore, the two first claims imply the third. For (4), we use Lemma 8 again, write its equation as

$$v^n = x^{p^f} y^{p^f},$$

and observe that $\langle h^{p^f} \rangle = \langle h \rangle \cap \langle g^{p^f}, h^{p^f} \rangle$, so the function field is generated by $\mathbb{C}(v, \beta)$ and $\mathbb{C}(x, y, \beta)$, and $\beta$ can be eliminated. The last point follows from Galois theory. The extension is unramified since by Lemma 8(i) the supergroup $\Gamma_H \supset \Gamma_{(h^{p^f})} \supset \Gamma_{f,n}$ has no torsion. □

5.2. Powers of 2

If $p = 2$, so that $n = 2^e$, $e > 1$, the groups $G_f$ defined in the introduction correspond to $2^{e-2}$ regular embeddings of $K_{n,n}$, namely $\phi(2^{e-f})$ for each $f = 2, \ldots, e$ (note that the value $f = 1$ does not arise in this case). With a few minor modifications, our methods show that all our theorems also apply to these dessins—with the only exception that the field extension discussed in Theorem 4.5 is ramified if $p = 2$. The main difference distinguishing the case $n = 2^e$ from the case of odd prime powers is the fact that these embeddings no longer form the complete list of all regular embeddings, as can be seen already in the case $n = 4$: here we have one non-standard embedding of $K_{4,4}$ on a torus giving a dessin d’enfant on the curve

$$y^2 = x^4 - 1 \quad \text{with Belyi function } \beta(x, y) = \frac{4x^4}{(x^4 - 1)^2}.$$

In the universal covering $\mathbb{C}$ the graph $K_{4,4}$ lifts to the lattice graph of the Gaussian integers $\mathbb{Z}[i]$ with an obvious bipartite colouring of the lattice points. The elliptic curve is obtained by taking the quotient by the lattice $2(1 + i)\mathbb{Z} + 2(1 - i)\mathbb{Z}$. For each $e \geq 3$ there are even four such exceptional embeddings for which the group $\text{Aut}^+_0 \mathcal{M}$ is not metacyclic. These all lead to curves whose full automorphism groups, described in [DJKNS2], are pairwise non-isomorphic. Since the automorphism group is an obvious Galois invariant, it is clear that the underlying curves can be defined over the rationals. It has recently been shown that the maps $\mathcal{M}$ discussed in this section are the only regular embeddings of $K_{n,n}$ when $n = 2^e$: see [DJKNS1] for the cases where the group $\text{Aut}^+_0 \mathcal{M}$ is metacyclic, and hence isomorphic to $G_f$ for some $f$, and [DJKNS2] for the exceptional cases where it is not.
Acknowledgments

The authors are grateful for a number of helpful suggestions by the referee, including a simplification of the proof of Lemma 4.

References

[JNS] G.A. Jones, R. Nedela, M. Škoviera, Regular embeddings of $K_{n,n}$ where $n$ is an odd prime power, European J. Combin., in press.