Galois actions on some series of Riemann surfaces with many automorphisms

Manfred Streit and **Jürgen Wolfart**

Mathematisches Seminar der J.W.Goethe–Universität,
Robert–Mayer–Str. 6–10, D–60054 Frankfurt a.M., Germany
Manfred.Streit@bahn.de wolfart@math.uni-frankfurt.de

1 Riemann surfaces with many automorphisms

The present paper is concerned with the classification of all Riemann surfaces with many automorphisms whose automorphism groups are semidirect products of two cyclic groups of prime order, with the action of the absolute Galois group on them, their Galois invariants, their field of definition and so on. We may restrict ourselves to compact Riemann surfaces X of genus $g > 1$. Recall that the property that X has *many automorphisms* may be defined in several equivalent ways [Wo1].

1. Every proper local deformation X_ϵ of X (corresponding to a point $P(X_\epsilon)$ in a small punctured neighbourhood of $P(X)$ in the moduli space $\mathcal{M}_g$) has an automorphism group which is strictly smaller than $\mathrm{Aut}\, X$.

2. The universal covering group $N \subset PSL_2(\mathbb{R})$ of X is a normal subgroup of a Fuchsian triangle group Δ (and $\mathrm{Aut}\, X \cong \Delta/N =: G$ if Δ is maximal with that property).

3. There exists a Belyi function $B : X \to \mathbb{P}^1$ (i.e. meromorphic with ramifications at most over $0, 1, \infty$) defining a normal covering, given by the canonical projection $N\backslash\mathcal{H} \to \Delta\backslash\mathcal{H} = G\backslash X$ where we denote the upper half plane by $\mathcal{H}$ and identify the target quotient space with $\mathbb{P}^1$ and the fixed point orbits of Δ with $0, 1, \infty$ respectively.

4. The conformal structure on X is characterized by a regular dessin given by the inverse image $B^{-1}[0, 1]$ of the real interval $[0, 1]$ under the canonical projection B (for the use of the word *canonical*, compare Remark 1 at the end of Section 4).

5. At least for genus $g > 3$ the corresponding point $P(X)$ of the moduli space is an isolated singularity of $\mathcal{M}_g$ in the sense of Zariski [Po] (not to be confused with the more restricted notion of topologically isolated points of the set of singular points in $\mathcal{M}_g$ as considered by Kulkarni [K]).

In the present paper, the most important characterizations are those given in 2. and 3.— As Felix Klein did, we may think of Riemann surfaces with many automorphisms as higher genus generalizations of the Platonic solids. In any case they are *Belyi surfaces*, i.e. equipped with a Belyi function or equivalently, with a *dessin d'enfant* in the sense of Grothendieck, or — by Belyi's theorem — as algebraic curves defined over number fields.

For reasons to be explained in the following section, we study in the present paper all Riemann surfaces with many automorphisms whose automorphism groups are semidirect products

$$G \cong Z_p \rtimes Z_q$$

of the multiplicative cyclic groups of prime order q and $p \equiv 1 \bmod q$. For simplicity we will suppose both primes to be > 3 and $q \neq 7$. We will further suppose that Z_q acts on Z_p by

$$b^{-1}ab = a^u$$

where a and b are generators of Z_p and Z_q respectively and u denotes a fixed prime residue class of order q in $(\mathbb{Z}/p\mathbb{Z})^*$.

Gareth Jones and David Singerman gave us some important hints. The second author thanks Chiba University and the Japan Society for the Promotion of Science for their hospitality in March 1998 when a first draft of this paper was written.

2 Introductory remarks about Galois actions

One of the main problems in the theory of Grothendieck's dessins d'enfants is to understand the action of the absolute Galois group $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ on them. This action is defined by the Galois action on the set of the corresponding Belyi surfaces, more precisely on the nonsingular projective algebraic curves via the action on the points and on the coefficients of their defining equations. For basic material on dessins, Belyi functions and Galois actions the reader may consult [JS] or [Wo] and the references quoted there. Every dessin has a *regular dessin* as a finite cover or equivalently, every Belyi surface Y is covered by a Riemann surface with many automorphisms X taking the normalization of the covering given by the original Belyi function $\beta : Y \to \mathbb{P}^1$. The resulting normal covering map $B : X \to \mathbb{P}^1$ is again a Belyi function whose dessin $B^{-1}[0,1]$ gives the regular covering of the original dessin $\beta^{-1}[0,1]$. Its automorphism group G, i.e. the covering group of B, is isomorphic to its hypermap group ($=$ monodromy group of B) and also to the hypermap group of the original dessin $\beta^{-1}[0,1]$, namely the monodromy group of β, and can also be identified with a subgroup of the automorphism group of the Belyi surface X. For more details about this regularization of dessins, see Theorem 2 of [Wo2]. Now Galois conjugations of Y (more precisely of the coefficients of the defining equations if we consider Y as an algebraic curve, and of the coefficients of the rational function β as well) induce Galois conjugations of X, therefore the problem of understanding these Galois actions can be divided into two parts.

- Describe the action of $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ on Belyi surfaces with many automorphisms X. In particular, determine the subgroup H of all Galois conjugations σ sending X to an isomorphic Belyi surface X^σ, and the fixed field $M(X)$ of H, the *moduli field* of X. By a result essentially due to Coombes and Harbater ([Wo1], [DE]) a Belyi surface with many automorphisms X has a model defined over its moduli field.

- Describe the action of H on the intermediate coverings of $B : X \to \mathbb{P}^1$, i.e. on all quotients of X by subgroups of G.

The second problem is connected to the theory of G–coverings and will not be the main point of interest here because in the examples treated below this action will be rather trivial.

For the first problem it is easy to see that if X has many automorphisms then so has X^σ for any Galois conjugation σ, that G is σ–conjugate to an automorphism group G^σ of X^σ, and the canonical Belyi function

$$B \,:\, X \;\to\; G\backslash X \;\cong\; \mathbb{P}^1 \quad \text{to} \quad B^\sigma \,:\, X^\sigma \;\to\; G^\sigma\backslash X^\sigma \;\cong\; \mathbb{P}^1$$

which is again a canonical Belyi function, with the same ramification orders as B (*canonical* means that B is uniquely determined by X and G which is $\mathrm{Aut}\,X$ in most cases — up to automorphisms of $\mathbb{P}^1$ possibly permuting $0, 1, \infty$). For an account of the actually known invariants of dessins under the action of $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ (monodromy and cartographic groups of Belyi functions) see [JSt]. Unfortunately these known invariants do not form a complete list of Galois invariants in general. They are sufficient to characterize Galois orbits in some important special cases such as elliptic curves with complex multiplication and uniform dessins (Singerman/Syddall [SSy]) or Hurwitz curves with automorphism groups $PSL_2\mathbb{F}_q$ over a finite field $\mathbb{F}_q$ (Streit [St2]). They are also trivially sufficient for curves X with many automorphisms in small genera g, $1 < g < 5$ since X is uniquely determined by its automorphism group $\mathrm{Aut}\,X$ in these cases. (Then, by the way, $M(X) = \mathbb{Q}$, so X may be defined over the rationals). As far as we know, historically the first examples where these invariants were known to be insufficient are 'Leila's flowers', see p.71 of [Sps]. The most reasonable way to gain more insight into such Galois actions seems to be the study of more nontrivial examples. For this reason, we consider in the following all Belyi surfaces with many automorphisms whose automorphism groups G are semidirect products $Z_p \rtimes Z_q$ as introduced at the end of Section 1. In the Theorems 1 and 3 we will see that the isomorphism classes of these Belyi surfaces form

1. one $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$–orbit of length $(q-1)/2$,
2. one $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$–orbit of length $(q-1)/3$ if $q \equiv 1 \bmod 3$,
3. $(q-1)/6$ $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$–orbits of length $q-1$ if $q \equiv 1 \bmod 3$,
4. $(q+1)/6$ $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$–orbits of length $q-1$ if $q \equiv -1 \bmod 3$.

We will moreover determine their fields of moduli (in these cases also their minimal fields of definition, as explained above). They are $\mathbb{Q}(e^{2\pi i/q})$ or their subfields of degree $(q-1)/2$ or $(q-1)/3$, respectively. As a byproduct we see that Hilbert's irreducibility argument fails to produce these groups as Galois groups over $\mathbb{Q}$ by specializing extensions of function fields ramified above three points only. On the way we will obtain a lot of further interesting information about the curves in question such as

- the decomposition of their Jacobians,
- the decomposition of the representation of G on the space of holomorphic differentials on X or
- properties of their canonical model.

3 Preliminaries concerning groups

As already introduced at the end of Section 1, let G denote the semidirect product of the cyclic normal subgroup Z_p of order p and with generator a and of the cyclic group Z_q of order q and with generator b. Let p and $q \neq 7$ be primes > 3, $p \equiv 1 \bmod q$ and let $u \in (\mathbb{Z}/p\mathbb{Z})^*$ be of order q. Then the action of Z_q on Z_p is well defined by

$$b^{-1}ab = a^u .$$

This is in fact the essential part of the presentation, as we can see in the first point of the following Lemma (1., 3. and 6. are taken from Section 25 of [JL], the others are obvious).

Lemma 1 *1. G is presented by the generators a and b and the relations*

$$a^p = b^q = 1 , \quad b^{-1}ab = a^u .$$

2. For all $n, m, j \in \mathbb{N}$

$$b^{-j}a^n b^m b^j = a^{nu^j} b^m .$$

3. Denote by S the subgroup generated by u in the group $(\mathbb{Z}/p\mathbb{Z})^*$ and denote by v_i, $i = 1, \ldots, r := (p-1)/q$ a system of representatives of $(\mathbb{Z}/p\mathbb{Z})^* \bmod S$. Then G splits into the $r+q$ conjugacy classes

$$\{1\} \quad , \quad \{a^{v_i S}\} := \{a^{v_i u^j} \mid j \in \mathbb{Z}/p\mathbb{Z}\} , \; i = 1, \ldots , r$$

and

$$\{a^m b^n \mid m \in \mathbb{Z}/p\mathbb{Z}\} , \; n \not\equiv 0 \bmod q .$$

4. *The only nontrivial subgroups of* G *are the commutator subgroup*

$$G' = Z_p = <a>$$

and the p *conjugate cyclic subgroups of order* q *generated respectively by* $a^m b$, $m \in \mathbb{Z}/p\mathbb{Z}$. *These subgroups form a partition of* G.

5. G *can be generated by any two elements taken from two different cyclic subgroups of order* p *or* q.

6. G *has* q *linear characters* χ_n, $n \in \mathbb{Z}/q\mathbb{Z}$, *defined by*

$$\chi_n(a^x b^y) = e^{2\pi i n y/q}$$

and r *irreducible characters* ϕ_j *of degree* q *defined by*

$$\phi_j(a^x b^y) = 0 \quad if \quad y \not\equiv 0 \bmod q$$

$$\phi_j(a^x) = \sum_{w \in S} e^{2\pi i v_j w x/p}.$$

For the next lemma recall that a triangle group Δ with signature $< p, q, r >$, $p, q, r \in \mathbb{N}$, is presented by generators and relations

$$\gamma_0, \gamma_1, \gamma_\infty; \quad \gamma_0^p = \gamma_1^q = \gamma_\infty^r = \gamma_0\gamma_1\gamma_\infty = 1$$

and that all elements of finite order in Δ are conjugate in Δ to powers of these generators. Therefore a homomorphism $h : \Delta \to G$ has a torsion free kernel if and only if the generators of Δ are mapped to elements of the same order in G. These homomorphisms are easy to classify since they are uniquely determined by the images of two generators.

Lemma 2 *Suppose* G *defined as above, and suppose that*

$$h : \Delta \to G$$

is a homomorphism with torsion free kernel. Then there are two possibilities for the signature of Δ.

1. $\Delta = < p, q, q >$. *In this case there are* $p(p-1)(q-1)$ *different homomorphisms with torsion free kernel according to the choice of*

$$h(\gamma_0) = a^m, \; h(\gamma_1) = a^n b^s, \; m \in (\mathbb{Z}/p\mathbb{Z})^*, \; n \in \mathbb{Z}/p\mathbb{Z}, \; s \in (\mathbb{Z}/q\mathbb{Z})^*.$$

2. $\Delta = < q, q, q >$. *In this case there are* $p(p-1)(q-1)(q-2)$ *different homomorphisms with torsion free kernel according to the choice of*

$$h(\gamma_0) = a^m b^n \ , \ h(\gamma_1) = a^s b^t \ , \ m, s \in \mathbb{Z}/p\mathbb{Z} \, , \ n, t \in (\mathbb{Z}/q\mathbb{Z})^* \, ,$$

and $a^m b^n$, $a^s b^t$ *neither lying in the same cyclic subgroup of* G *nor having a product in* $Z_p = < a >$ *(equivalent to* $n \not\equiv -t \bmod q$ *).*

The *proof* is obvious, only the last point deserves to be mentioned: $h(\gamma_0)$ can be chosen freely among the $p(q-1)$ elements of order q in G , and for the choice of $h(\gamma_1)$ one has to avoid the $q-1$ nontrivial powers of $h(\gamma_0)$ and the $p-1$ possibilities leading to an $h(\gamma_\infty) = (h(\gamma_0)h(\gamma_1))^{-1}$ of order p . For the reformulation with exponents, observe that $b^n a^s b^t = a^v b^n b^t$ for some $v \in \mathbb{Z}/p\mathbb{Z}$.

Lemma 3 *The automorphism group of* G *is isomorphic to the semidirect product* $AGL_1(p) \cong (\mathbb{Z}/p\mathbb{Z})^* \ltimes \mathbb{Z}/p\mathbb{Z}$. *The automorphisms are determined by*

$$a \ \mapsto \ a^k \ , \ k \in (\mathbb{Z}/p\mathbb{Z})^* \, , \quad b \ \mapsto \ a^m b \ , \ m \in \mathbb{Z}/p\mathbb{Z} \, .$$

Proof. Preserving the orders, every automorphism must satisfy

$$a \ \mapsto \ a^k \ , \ k \in (\mathbb{Z}/p\mathbb{Z})^* \, , \quad b \ \mapsto \ a^m b^n \ , \ m \in \mathbb{Z}/p\mathbb{Z} \, , \ n \in (\mathbb{Z}/q\mathbb{Z})^* \, .$$

Since the defining conjugation relation has to be preserved, we also have

$$a^{uk} = b^{-n} a^{-m} a^k a^m b^n = a^{u^n k} \, ,$$

see Lemma 1. But $uk \equiv u^n k \bmod p$ implies $u^{n-1} \equiv 1 \bmod p$, hence $n \equiv 1 \bmod q$.

Corollary 1 1. *There are* $q-1$ *different normal subgroups* N_s *of* $\Delta = < p, q, q >$, $s \in (\mathbb{Z}/q\mathbb{Z})^*$, *with quotient* $\Delta/N_s \cong G$.

2. *There are* $(q-1)(q-2)$ *different normal subgroups* $N_{n,t,v}$ *of* $\Delta = < q, q, q >$ *with quotient* $\Delta/N_{n,t,v} \cong G$ *where* $n, t, v \in (\mathbb{Z}/q\mathbb{Z})^*$ *satisfy the condition* $n + t + v \equiv 0 \bmod q$.

Proof and *comment.* It is easy to see that two homomorphisms $h_1, h_2 : \Delta \to G$ have the same kernel if and only if there is an automorphism α of G with $h_1 = \alpha \circ h_2$. Therefore the respective number of different normal subgroups with quotient G follows directly from the preceding lemmas. By combining the homomorphisms with suitable automorphisms, we can moreover normalize the homomorphisms in question in the following way.
For $\Delta = < p, q, q >$ we may assume $h =: h_s$ with

$$h(\gamma_0) = a \ , \ h(\gamma_1) = b^s$$

for some $s \in (\mathbb{Z}/q\mathbb{Z})^*$ uniquely determining the kernel.
For $\Delta = < q, q, q >$ we may assume $h =: h_{n,t,v}$ with

$$h(\gamma_0) = b^n , \quad h(\gamma_1) = ab^t , \quad h(\gamma_\infty) = a^{-u^t} b^v$$

with $n, t, v \in (\mathbb{Z}/q\mathbb{Z})^*$, $n + t + v \equiv 0 \bmod q$ following from $\gamma_0\gamma_1\gamma_\infty = 1$. We observe that the condition $n \not\equiv -t \bmod q$ is automatically satisfied and that the normal subgroups of Δ with quotient G are uniquely characterized by the triples (n, t, v) as the kernels of these normalized homomorphisms.

Lemma 4 *For these normal subgroups $N_s \lhd < p, q, q >$ and $N_{n,t,v} \lhd < q, q, q >$ we have:*

1. *$\Delta = < p, q, q >$ is the normalizer of N_s in $PSL_2(\mathbb{R})$.*
2. *$\Delta = < q, q, q >$ is the normalizer of $N_{n,t,v}$ in $PSL_2(\mathbb{R})$ if $n, t, v \in (\mathbb{Z}/q\mathbb{Z})^*$ are pairwise distinct. If not, only two of the indices can coincide, and then the normalizer is a triangle group $\overline{\Delta} = < 2q, q, 2 >$ containing Δ with index 2.*

Proof. In any case, the normalizer is a Fuchsian group containing Δ. It is known that triangle groups have only triangle groups as possible supergroups, and using Singerman's list of inclusions [Si], one may see that the only possibilities in our situation are

$$< p, q, q > \ \lhd \ < 2p, q, 2 >$$

$$< q, q, q > \ \lhd \ < 2q, q, 2 > , \ < q, 3, 3 > \subset < 2q, 3, 2 > \ .$$

(We excluded the case $q = 7$ since $< 7, 7, 7 >$ is exceptionally a non–normal subgroup of $< 2, 3, 7 >$.)
1. Suppose that N_s is a normal subgroup not only of $< p, q, q >$ but also of $< 2p, q, 2 >$. We may present the larger triangle group $\overline{\Delta}$ by generators and relations

$$\alpha , \gamma_1 , \delta ; \quad \alpha^{2p} = \gamma_1^q = \delta^2 = \alpha\gamma_1\delta = 1$$

and relate it to the generators of $\Delta = < p, q, q >$ by

$$\alpha^2 = \gamma_0 , \quad \delta^{-1}\gamma_1\delta = \gamma_\infty .$$

So, if we had a quotient $\overline{G} \cong \overline{\Delta}/N_s$ extending G with index 2, there would be an automorphism of G sending

$$h(\gamma_1) = b^s \quad \text{to} \quad h(\gamma_\infty) = (h(\gamma_0)h(\gamma_1))^{-1} = b^{-s}a^{-1} = a^{-u^s} b^{-s} ,$$

see Lemma 1. According to Lemma 3 this would imply $s \equiv -s \bmod q$ what is clearly impossible.
2. In the case $N_{n,t,v} \lhd \Delta = < q, q, q >$ we first note that $n \equiv t \equiv v \bmod q$ is impossible by our assumptions $n, t, v \in (\mathbb{Z}/q\mathbb{Z})^*$, $n + t + v \equiv 0 \bmod q$. Consequently, there is no automorphism

of G giving a cyclic permutation of the generators $h(\gamma_i)$ (see Lemma 3) whence $N_{n,t,v}$ is never a normal subgroup of $< q,3,3 >$ or $< 2q,3,2 >$ by arguments quite similar to the first case. The same arguments show that $N_{n,t,v}$ is not a normal subgroup of $\overline{\Delta} = < 2q,q,2 >$ if n,t,v are pairwise distinct. However, the groups $N_{n,t,t}$ (say) are in fact normal subgroups of $\overline{\Delta}$ what we may see as follows. Since the order of u in $(\mathbb{Z}/p\mathbb{Z})^*$ is odd ($= q$), it is a quadratic residue mod p. Therefore a $w \in (\mathbb{Z}/q\mathbb{Z})^*$ exists satisfying

$$w^2 \equiv u \quad \text{and hence} \quad w^q \equiv -1 \bmod q\,.$$

There is a supergroup $\overline{G}$ of G of index 2 presented by

$$\overline{G} = < a\,,c\,;\, a^p = c^{2q} = 1\,,\, c^{-1}ac = a^w >$$

containing G by $c^2 = b$. As above, let $\overline{\Delta}$ be generated by α, γ_1, δ of the respective orders $2q, q, 2$ and with $\alpha^2 = \gamma_0$, $\delta^{-1}\gamma_1\delta = \gamma_\infty$. Then one can check by a straightforward but lengthy calculation — playing with the relations and with $n + 2t \equiv 0 \bmod q$ — that

$$\alpha \mapsto c^n\,,\ \gamma_1 \mapsto ab^t\,,\ \delta \mapsto a^{-u^{-t}}c^q$$

defines a homomorphism $\overline{\Delta} \to \overline{G}$ which restricts on Δ to the original homomorphism h with kernel $N_{n,t,t}$.

Different normal subgroups N_s or $N_{n,t,v}$ can be conjugate in $PSL_2(\mathbb{R})$ only by elements of a group containing Δ with finite index, i.e. by elements of the respective maximal triangle group. Looking at the effect on the generators we can therefore deduce the

Corollary 2 *1. Among the normal subgroups N_s of $\Delta = < p,q,q >$ there are $(q-1)/2$ $PSL_2(\mathbb{R})$–conjugacy classes. For all $s \in (\mathbb{Z}/q\mathbb{Z})^*$, N_s is conjugated to N_{-s}.*

2. The normal subgroups $N_{n,t,v}$ and $N_{m,s,w}$ of $\Delta = < q,q,q >$ are $PSL_2(\mathbb{R})$–conjugated if and only if (n,t,v) is a permutation of (m,s,w). There are $q-1$ conjugacy classes of groups $N_{n,t,t}$ and $(q-1)(q-5)/6$ conjugacy classes of groups $N_{n,t,v}$ with pairwise different indices.

4 The Riemann surfaces with p–ramification

In the last point of the following theorem a *Belyi pair* means a pair (U,β) of a Belyi surface U with a Belyi function β on it. Two Belyi pairs (U,β) and (V,ϕ) are called *isomorphic*, if there are isomorphisms

$$f : U \to V\,,\ \mu : \mathbb{P}^1 \to \mathbb{P}^1 \quad \text{with} \quad \phi \circ f = \mu \circ \beta$$

(*weakly isomorphic* in the terminology of [CG]). As in the definition of moduli fields of Belyi surfaces, let H be the subgroup of $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ consisting of all σ which conjugate the Belyi pair

(U, β) into an isomorphic Belyi pair (U^σ, β^σ). Then call the fixed field $M(U, \beta)$ of H the *moduli field* of (U, β). It is automatically contained in every common field of definition of U and β.

Theorem 1 *Let $\Delta = < p, q, q >$, G and N_s , $s \in (\mathbb{Z}/q\mathbb{Z})^*$, be defined as in the first case of the last section, i.e. let N_s be the kernel of the homomorphism*

$$h_s \,:\, \Delta \to G \quad \textit{given by} \quad \gamma_0 \mapsto a \,,\, \gamma_1 \mapsto b^s \,.$$

Then

1. *the quotient spaces $N_s\backslash\mathcal{H}$, $s \in (\mathbb{Z}/q\mathbb{Z})^*$, form $(q-1)/2$ non–isomorphic compact Belyi surfaces X_s with $X_s \cong X_{-s}$ for all s .*
2. *The genus of all X_s is*
$$g(X_s) \;=\; \frac{1}{2}\,(p-1)\,(q-2)\,.$$
3. *Their automorphism group is $\mathrm{Aut}\, X_s \cong G$.*
4. *Let ζ denote a fixed q–th root of unity $\neq 1$ and choose an integer u representing its residue class $\bmod\ p$. Then, as an algebraic curve, X_s has the (affine, singular) model (with $\overline{s}s \equiv 1 \bmod q$)*
$$y^p \;=\; \prod_{k=1}^{q} \,(\, x \,-\, \zeta^{\overline{s}k}\,)^{u^k} \,.$$
5. *The curves X_s , $s \in (\mathbb{Z}/q\mathbb{Z})^*$ (or: their regular dessins) form an orbit for the action of $\mathrm{Gal}\,\mathbb{Q}(\zeta)/\mathbb{Q}$.*
6. *Their moduli field (or: minimal field of definition) is $\mathbb{Q}(\zeta + \zeta^{-1})$.*
7. *The triangle group Δ has a normal subgroup Γ of index q containing all subgroups N_s as normal subgroups of index p . With the homomorphisms h_s , it can be described as the preimage*
$$\Gamma \;:=\; h_s^{-1}(Z_p) \;=\; h_s^{-1}(< a >)$$
or as the kernel of the homomorphism
$$h \,:\, \Delta \to Z_q \quad \textit{given by} \quad \gamma_0 \mapsto 1 \,,\, \gamma_1 \mapsto b \,,\, \gamma_\infty \mapsto b^{-1} \,.$$
Its quotient surface $Y = \Gamma\backslash\mathcal{H}$ is of genus 0 and the covering $Y \to \Delta\backslash\mathcal{H}$ is normal and cyclic of order q . It is ramified at and above two points.

8. *Between* Δ *and every* N_s *lie* p *intermediate Fuchsian groups* $\Phi_{s,m}$, $m \in \mathbb{Z}/p\mathbb{Z}$ *with indices*

$$(\Delta : \Phi_{s,m}) \;=\; p\;, \quad (\Phi_{s,m} : N_s) \;=\; q$$

whose quotient surfaces $U_{s,m} := \Phi_{s,m}\backslash\mathcal{H}$ *are all of genus* $(p-1)(q-2)/2q$. *The projections*

$$\beta_{s,m} \;:\; U_{s,m} \;\to\; \mathbb{P}^1 \;:\; \Phi_{s,m}z \;\mapsto\; \Delta z$$

are Belyi functions. The Belyi pairs $(U_{s,m},\beta_{s,m})$ *and* $(U_{t,n},\beta_{t,n})$ *are isomorphic if and only if* $s \equiv \pm t \bmod q$. *The different isomorphism classes form an Galois orbit under the action of* $\mathrm{Gal}\,\mathbb{Q}(\zeta)/\mathbb{Q}$, *and their moduli field is again* $\mathbb{Q}(\zeta+\zeta^{-1})$.

Proof. 1. follows by Corollary 1.1 and Corollary 2.1.
2. follows by the index $(\Delta : N_s) = pq$ (and the usual comparison of the volumes of the involved fundamental domains) as

$$g \;=\; 1 + \frac{pq}{2}\,(1-\frac{1}{p}-\frac{2}{q})\;.$$

3. follows by Lemma 4.1 and $\Delta/N_s \cong G$.
7. The existence of Γ and its properties follow from isomorphism theorems of group theory. Note that all possible homomorphisms

$$h_s \;=\; h \;:\; \Delta \;\to\; Z_q \quad \text{given by} \quad \gamma_0 \;\mapsto\; 1\;,\; \gamma_1 \;\mapsto\; b^s\;,\; \gamma_\infty \;\mapsto\; b^{-s}$$

have the same kernel, so Γ is independent of s . The genus of Y may be computed in different ways. Since it is clear that the covering $Y \to \Delta\backslash\mathcal{H} \cong \mathbb{P}^1$ is cyclic of order q and ramified of order q precisely above 1 and ∞ — recall the identification of $0,1,\infty$ with the fixed point orbits of Δ given in Section 1 — we have also $Y \cong \mathbb{P}^1$. If we denote the respective function fields of Y and $\Delta\backslash\mathcal{H}$ by $\mathbb{C}(x)$ and $\mathbb{C}(t)$, the covering map (of course a Belyi function) can be explicitly given by

$$x \;\mapsto\; x^q \;=\; 1-t\;.$$

4. The function field of X_s is a Galois extension of $\mathbb{C}(t)$ with Galois group anti–isomorphic to G , and $\mathbb{C}(x)$ is the normal intermediate field fixed by the normal subgroup Z_p generated by a . As a cyclic extension of $\mathbb{C}(x)$ of order p , we may therefore write the function field of X_s in the form $\mathbb{C}(x,y)$ where y^p is a rational function of x , uniquely determined up to taking powers with exponents prime to p and up to multiplication with p–th powers in $\mathbb{C}(x)$. Moreover we may assume that the Belyi function $X_s \to \mathbb{P}^1$ is given by $(x,y) \mapsto x^q = 1-t$ ramifying precisely above $t=0$ with order p , i.e. in the points with $x = \zeta^k$, $k \in \mathbb{Z}/q\mathbb{Z}$. Therefore we can assume that

$$y^p \;=\; \prod_{k=1}^{q}\,(x-\zeta^k)^{c_k}$$

with some integers c_k not divisible by p . In fact, the cyclic extension only depends on the residue classes $c_k \bmod p$ and is invariant under multiplication with a common factor $c \in (\mathbb{Z}/p\mathbb{Z})^*$, so it corresponds to some point

$$(c_1,\ldots,c_q) \;\in\; \mathbb{P}^{q-1}(\mathbb{F}_p)$$

in a projective space over the finite field with p elements. According to Kummer theory (see e.g. [L]), this point is uniquely determined by the extension. Which point?
To decide this question we fix the q–th root of unity ζ and an (also primitive) p–th root of unity η such that the action of $G \cong \mathrm{Aut}\, X_s$ on the functions satisfies

$$a(y) := y \circ a^{-1} = \eta y \,, \quad a(x) := x \circ a^{-1} = x \,, \quad b(x) := x \circ b^{-1} = \zeta x \,.$$

Now the action of b on the equation for y^p induces a cyclic shift on the place of the exponents (to simplify the argument, we can assume that all $c_k \equiv 1 \bmod q$, hence $\sum c_k$ divisible by q)

$$\prod_{k=1}^{q} (\zeta x - \zeta^k)^{c_k} = \prod_{k \bmod q} (x - \zeta^{k-1})^{c_k} = \prod_{k \bmod q} (x - \zeta^k)^{c_{k+1}} \,.$$

Since $b(y)$ is also a p–th root generating the field extension $\mathbb{C}(x,y)/\mathbb{C}(x)$, the shift of exponents gives the same point in $\mathbb{P}^{q-1}(\mathbb{F}_p)$, hence

$$(c_1, \ldots, c_q) = (1, c, c^2, \ldots, c^{q-1})$$

for some $c \in \mathbb{F}_p^*$ of order q . We can moreover conclude that for a suitable integer representing the exponent, $b(y) = y^c g(x)$ with a rational function g . Using $ab = ba^u$ we get even $c = u$ (again a choice of an integer representing $u \bmod p$, w.l.o.g. $u \equiv 1 \bmod q$), and following the defining equation for y^p we may determine $g(x)$ explicitly by

$$g(x)^p = \frac{x-1}{(x-1)^{u^q}} = (x-1)^{1-u^q}$$

(recall that $1 - u^q$ is divisible by p). Note also that $\sum u^k$ is divisible by p whence the covering map $X_s \to Y$ is unramified over $x = \infty$.
Finally one can replace ζ by any other primitive q–th root of unity $\zeta^{\overline{s}}$ corresponding to other choices of the generator of Z_q or to other choices of the homomorphism h_s .
5. follows from the equation given in 4.
6. may be seen using $X_s \cong X_{-s}$ or also by a more direct argument involving the equations given in 4.: recall that $\sum u^k = pN$ for an integer N and that we can assume $u \equiv 1 \bmod q$ and therefore $\sum \overline{s} k u^k \equiv 0 \bmod q$. Now write the equation for X_{-s} as

$$y^p = \prod (x - \zeta^{-\overline{s}k})^{u^k} = x^{pN} \prod (\zeta^{\overline{s}k} - \frac{1}{x})^{u^k}$$

and write again x for $1/x$ and y for $\pm y/x^N$ to deduce the equation for X_s .
8. Define $\Phi_{s,m}$ as the inverse image of the cyclic subgroup $< a^m b >$ under the homomorphism $h_s : \Delta \to G \cong \Delta/N_s$. Computing the indices is an exercise in group theory. Every automorphism of X_s of order q has two fixed points of order q , so the genus of the surfaces $U_{s,m}$ can be computed using the Riemann–Hurwitz formula and the genus of X_s .
For s fixed, the different $\Phi_{s,m}$ are conjugated in Δ and $\Phi_{s,m}$, $\Phi_{-s,n}$ are conjugated in $\overline{\Delta}$.

Let $K_{s,m}$ be the function field of the Belyi surface $U_{s,m}$. Then the function field extension $\mathbb{C}(x,y)/\mathbb{C}(t)$ belonging to the covering $X_s/\mathbb{P}^1$ is the normalization of $K_{s,m}/\mathbb{C}(t)$ whence they give non–isomorphic extensions for different $s \in (\mathbb{Z}/q\mathbb{Z})^*/\pm 1$. This implies the assertions about the possible isomorphisms among the different $(U_{s,m}, \beta_{s,m})$, and the assertions on the Galois action easily follow from the action on the X_s taking the respective quotients.

Warning. $M(U_{s,m}, \beta_{s,m}) = \mathbb{Q}(\zeta + \zeta^{-1})$ does not mean that $U_{s,m}$ and $\beta_{s,m}$ can be defined over that field. Also it is possible that much more isomorphisms exist between the different $U_{s,m}$ but then not compatible with the respective Belyi functions.

Remarks. 1. We take the opportunity to point out a possible misunderstanding in Remark 4 of [Wo1]. For a Riemann surface with many automorphisms $N \backslash \mathcal{H} = X$, N a normal subgroup of a triangle group Δ, and its Belyi function $B : X \to \mathbb{P}^1 = \Delta \backslash \mathcal{H}$ it is true that the moduli fields $M(X)$ and $M(X, B)$ coincide if they are defined as at the beginning of this section, and that X can be defined over $M(X)$. But this is possibly not true for B because B is unique (canonical) only up to automorphisms of $\mathbb{P}^1$ exchanging $0, 1, \infty$. In cases where Δ is not maximal, i.e. if the same order occurs at non–equivalent fixed points it may happen that a Galois conjugation in $\mathrm{Gal}\, \overline{\mathbb{Q}}/M(X)$ exchanges the fixed points of Δ, hence $B \neq B^\sigma$ (in the terminology of [CG], the Belyi pairs are not *strongly isomorphic*). In that case, B can only be defined over a field containing $M(X)$ with index 2, 3 or 6. This phenomenon occurs precisely for our Belyi surfaces X_s where the isomorphism to X_{-s} corresponds to an exchange of 1 and ∞.
2. For Theorem 1 the primes $q = 3$ and 7 are admitted, but for $q = 3$ we obtain curves which will be treated in the next section under the name Y_{1,t,t^2} (the other prime here called p will be there called q).

5 A well–known normal subcovering

Now we will concentrate on those cases where G is a quotient of $\Delta = < q, q, q >$. In this section we consider the normal subcovering of $X_{n,t,v}/\mathbb{P}^1$ coming from the Fuchsian group $\Gamma_{n,t,v} := h_{n,t,v}^{-1}(Z_p)$ where $h_{n,t,v}$ denotes the normalized homomorphism $\Delta \to G$ introduced in the proof of Corollary 1.2. As always, $n, t, v \in (\mathbb{Z}/q\mathbb{Z})^*$ with $n + t + v \equiv 0 \bmod q$. We already know that the isomorphism classes of $X_{n,t,v}$ depend on n, t, v up to permutation only.

Lemma 5 *As n, t, v let $m, s, w \in (\mathbb{Z}/q\mathbb{Z})^*$ with $m + s + w \equiv 0 \bmod q$ and call*

$$(n, t, v) \ \sim \ (m, s, w)$$

if and only if these triples coincide up to permutation and multiplication by a common factor $c \in (\mathbb{Z}/q\mathbb{Z})^*$. This is an equivalence relation. We denote the equivalence classes by $[n, t, v]$.

1. *The only homomorphisms of* $\Delta = < q, q, q >$ *onto* $Z_q = < b >$ *with torsion–free kernel are given by*
$$f_{n,t,v} \; : \; \gamma_0 \; \mapsto \; b^n \; , \; \gamma_1 \; \mapsto \; b^t \; , \; \gamma_\infty \; \mapsto \; b^v$$
with $n, t, v \in (\mathbb{Z}/q\mathbb{Z})^*$, $n + t + v \equiv 0 \bmod q$.

2. *The kernel of* $f_{n,t,v}$ *is* $\Gamma_{n,t,v}$.

3. *There is a bijection between the* $PSL_2(\mathbb{R})$*–conjugacy classes of* $\Gamma_{n,t,v}$ *and the equivalence classes* $[n, t, v]$.

4. *The normalizer of* $\Gamma_{n,t,t}$ *is* $PSL_2(\mathbb{R})$ *is* $\overline{\Delta} = < 2q, q, 2 >$. *If there is a* $t \in (\mathbb{Z}/q\mathbb{Z})^*$ *of order* 3 *and with* $1+t+t^2 \equiv 0 \bmod q$ *(what happens if and only if* $q \equiv 1 \bmod 3$*) then the normalizer of* Γ_{1,t,t^2} *is* $\overline{\Delta} = < q, 3, 3 >$ *containing* Δ *as normal subgroup of index* 3. *In all other cases* Δ *is the normalizer of* $\Gamma_{n,t,v}$.

Proof. 1. follows from the relation between the generators of Δ.
2. The homomorphism $f_{n,t,v}$ is a combination of $h_{n,t,v}$ with the canonical projection of G onto the factor group $G/Z_p \cong Z_q \cong < b >$.
3. If $c \in (\mathbb{Z}/q\mathbb{Z})^*$, $f_{cn,ct,cv}$ is $f_{n,t,v}$, followed by the automorphism $Z_q \to Z_q$ given by $b \mapsto b^c$, whence the kernels are invariant under multiplication of the indices with common factors. The invariance of the $PSL_2(\mathbb{R})$–conjugacy class under permutations of the indices follows as in Corollary 2.2 by the fact that the generators of Δ can be permuted under the action of $\overline{\Delta} = < 2q, 3, 2 >$. The assumptions on p and q guarantee that no other conjugations between the $\Gamma_{n,t,v}$ are possible.
4. If $t = v$ the homomorphism $f_{n,t,v}$ clearly extends to a homomorphism of $< 2q, q, 2 >$ onto a group Z_{2q} containing $Z_q = < b >$ (exercise).
In the second case mentioned, there is an index 3 extension H of Z_q containing Z_q as normal subgroup and a non–normal subgroup $< d >$ of order 3 acting on Z_q via
$$d^{-1}\, b\, d \; = \; b^t \; .$$
Then f_{1,t,t^2} is extendable to a homomorphism of $< q, 3, 3 >$ onto this semidirect product $Z_q \rtimes Z_3$. Observe that the conjugation by one of the generators of $\overline{\Delta}$ permutes the generators of Δ.
It is easy to check that not both cases can occur at the same time, therefore Δ is the normalizer in all other cases.

Theorem 2 *Let* n, t, v *be as above and define* $Y_{n,t,v} := \Gamma_{n,t,v} \backslash \mathcal{H}$. *Then we have*

1. $Y_{n,t,v}$ *is a Belyi surface of genus* $(q-1)/2$ *and with many automorphisms. Its Belyi function*
$$Y_{n,t,v} \; \to \; \Delta\backslash\mathcal{H} \; \cong \; \mathbb{P}^1$$
is a normal cyclic covering of degree q *and with ramifications above* $0, 1, \infty$ *of order* q.

2. *The automorphism group is*

$$\mathrm{Aut}\, Y_{n,t,v} \;\cong\; Z_q \quad \textit{if} \quad n\,,\, t\,,\, v \quad \textit{are pairwise distinct and not}$$

equivalent to $(1, t, t^2)$ *with* $t^3 \equiv 1\ ,\ 1 + t + t^2 \equiv 0 \bmod q$, *and in these cases we have*

$$\mathrm{Aut}\, Y_{1,t,t^2} \;\cong\; Z_q \rtimes Z_3\ ,$$

$$\mathrm{Aut}\, Y_{n,t,t} \;\cong\; Z_2 \times Z_q\ .$$

The surfaces $Y_{n,t,t}$ *are hyperelliptic.*

3. $Y_{n,t,v} \cong Y_{m,s,w}$ *if and only if* $(n, t, v) \sim (m, s, w)$.

4. $Y_{n,t,v}$ *has the (affine, singular) model over* $\mathbb{Q}$

$$y^q \;=\; x^n\,(x-1)^t\ .$$

Proof. 1., 2. and 3. follow almost directly from Lemma 5. The genus can be again computed by Riemann–Hurwitz, and in the $t = v$ case one can see that in fact $Y_{n,t,t}/Z_2 \cong \mathbb{P}^1$ or transform the equation of part 4. into an equation $u^2 = \ldots$. The shape of the equation can be guessed as follows. The function field $\mathbb{C}(y, x)$ of $Y_{n,t,v}$ is a cyclic extension of the function field $\mathbb{C}(x)$ of $\mathbb{P}^1$, and the ramification shows that we can assume $y^q = x^\mu (x-1)^\nu$. To find the correct exponents, choose y such that $b(y) = \zeta y$, ζ the primitive q–th root of unity for which γ_0 acts in its fixed points on local branches of $\sqrt[q]{x}$ like multiplication by ζ , and so on for γ_1, γ_∞ .

Remarks. 3. The preceding proof follows a suggestion of Gareth Jones. Another possibility to distinguish the different non–isomorphic surfaces $Y_{n,t,v}$ is the fact that their Jacobians have complex multiplication by the cyclotomic field $\mathbb{Q}(\zeta)$ but that their isogeny class can be distinguished by the CM type. Moreover, the different CM types correspond bijectively to the equivalence classes $[n, t, v]$, see [KR], so we can apply Torelli's theorem to distinguish the curves.
4. In particular, this gives the following additional information. Non–isomorphic surfaces $Y_{n,t,v}$ are not Galois–conjugate, but the automorphism groups (or: hypermap groups for their canonical regular dessin) coincide — at least in general for $q \geq 17$, see below — so they are incomplete as Galois invariants. However, here the curves may be distinguished by representation theory: if we consider the usual representation

$$\rho\ :\ \alpha\ \mapsto\ (\omega\ \mapsto\ \omega \circ \alpha^{-1})\ ,\ \alpha \in Z_q\ ,$$

on the vector space of holomorphic differentials on $Y_{n,t,v}$, then the non–isomorphic surfaces can be distinguished by the trace of $\rho(b)$. We will come back to this question in Section 7.
5. For $q = 5$, there is only one equivalence class of triples corresponding to the well–known hyperelliptic curve $y^5 = x(x-1)$ or $u^2 = v^5 - 1$. For $q = 11$, there is one hyperelliptic and one ordinary triple. For $q = 13$, there are three inequivalent triples of all types, namely

$$[1, 6, 6]\ ,\ [1, 2, 10]\ ,\ [1, 3, 9] \qquad (g\ =\ 6)$$

The Jacobian of $Y_{1,3,9}$ is a product of three isogenous abelian varieties of dimension 2 , and the curve is a cover of another curve of genus 2 , obtained by taking the quotient by the factor Z_3 of the automorphism group. First for $q = 17$ we have two ordinary triples (and one hyperelliptic, of course), namely

$$[1,8,8]\,,\ [1,2,14]\,,\ [1,3,13] \qquad (g\ =\ 8)\ .$$

6. Let us shed some light on the excluded case $q = 7$. Here we are in genus 3 and have a hyperelliptic curve $Y_{1,3,3}$ and a non–hyperelliptic curve $Y_{1,2,4}$. By the techniques going back to Shimura and Taniyama and extensively used by Koblitz and Rohrlich [KR], the Jacobian of the latter curve is isogenous to a cube of an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-7})$. But here Z_7 or $Z_7 \rtimes Z_3$ are far from being the true automorphism group. As a consequence of the exceptional situation $< 7,7,7 > \subset < 2,3,7 >$, the full automorphism group is $PSL_2(\mathbb{F}_7)$ and the curve is isomorphic to Klein's quartic.

6 The Riemann surfaces without p–ramification

Theorem 3 *Let* $\Delta = < q,q,q >$, G *and* $N_{n,t,v}$ *be defined as in the second case of Section 3 , i.e. with* $n,t,v \in (\mathbb{Z}/q\mathbb{Z})^*$, $n+t+v \equiv 0 \bmod q$, $N_{n,t,v}$ *the kernel of the homomorphism*

$$h_{n,t,v}\ =\ h \quad \textit{defined by} \quad h(\gamma_0)\ =\ b^n\ ,\ h(\gamma_1)\ =\ ab^t\ ,\ h(\gamma_\infty)\ =\ a^{-u^t}b^v\ .$$

Then

1. *the quotient spaces* $N_{n,t,v}\backslash\mathcal{H}$ *are compact Belyi surfaces* $X_{n,t,v}$ *of genus*

$$g\ =\ 1 + \frac{1}{2}\,p\,(q-3)\ .$$

   $X_{n,t,v}$ *is isomorphic to* $X_{m,s,w}$ *if and only if* (n,t,v) *is a permutation of* (m,s,w) .

2. *Their automorphism group is*

$$G \qquad \textit{if the indices are pairwise distinct}$$

$$\overline{G}\ =\ Z_p \rtimes Z_{2q} \qquad \textit{for} \quad X_{n,t,t}$$

   (for the definition of $\overline{G}$ *see the proof of Lemma 4).*

3. *For* (n,t,v) *fixed, the surfaces* $X_{sn,st,sv}$, $s \in (\mathbb{Z}/q\mathbb{Z})^*$ *, form the orbit under the action of* $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ *. More precisely, for* $\zeta := e^{2\pi i/q}$ *and* $\sigma(\zeta) = \zeta^{\bar{s}}$, $\bar{s}s \equiv 1 \bmod q$ *, we have*

$$X^\sigma_{n,t,v}\ \cong\ X_{sn,st,sv}\ .$$

4. *Under the Galois action, the isomorphism classes form*

- *one orbit consisting of all* $q-1$ *surfaces* $X_{n,t,t}$, *all with moduli field (= minimal field of definition)* $\mathbb{Q}(\zeta)$,
- *one orbit consisting of all* $(q-1)/3$ *non–isomorphic surfaces* X_{s,st,st^3} *if* $q \equiv 1 \bmod 3$ *and* $t^3 \equiv 1 \bmod q$, $1+t+t^2 \equiv 0 \bmod q$. *In this case, their moduli field is the fixed field* $\mathbb{K}$ *of* $\tau : \zeta \mapsto \zeta^t$ *in the cyclotomic field* $\mathbb{Q}(\zeta)$.
- *All other orbits are of length* $q-1$ *and consist of surfaces* $X_{sn,st,sv}$, $s \in (\mathbb{Z}/q\mathbb{Z})^*$. *Here the moduli field is again* $\mathbb{Q}(\zeta)$.

5. *Between* Δ *and* $N_{n,t,v}$ *lie the unique torsion–free subgroup* $\Gamma_{n,t,v}$ *treated in Section 5 and* p Δ*–conjugate subgroups* $\Phi^m_{n,t,v}$, $m \in \mathbb{Z}/p\mathbb{Z}$ *with*

$$(\Delta : \Phi^m_{n,t,v}) \;=\; p\,, \quad (\Phi^m_{n,t,v} : N_{n,t,v}) \;=\; q$$

giving p isomorphic Belyi pairs $(U^m_{n,t,v}, \beta^m_{n,t,v})$ *where*

$$U^m_{n,t,v} \;:= \Phi^m_{n,t,v}\backslash\mathcal{H} \quad \textit{and} \quad \beta^m_{n,t,v} \;:\; U^m_{n,t,v} \;\to\; \Delta\backslash\mathcal{H} \;\cong \mathbb{P}^1$$

is the canonical projection. The genus is

$$g(U^m_{n,t,v}) \;=\; \frac{1}{2q}\,(p-1)\,(q-3)\;.$$

The Belyi pairs $(U^m_{n,t,v}, \beta^m_{n,t,v})$ *and* $(U^j_{k,s,w}, \beta^j_{k,s,w})$ *are isomorphic if and only if* (k,s,w) *is a permutation of* (n,t,v) . *Their moduli field is* $M(X_{n,t,v})$ *as above.*

6. *The cartographic group of the dessin on* $X_{n,t,v}$ *induced by the Belyi function* $B : X_{n,t,v} \to \Delta\backslash\mathcal{H}$ *is the monodromy group of*

$$\beta \;:=\; 4\,B\,(B-1) \;:\; X_{n,t,v} \;\to\; \overline{\Delta}\backslash\mathcal{H} \quad \textit{where} \quad \overline{\Delta} \;=<2q,q,2> \;\;.$$

This cartographic group is

- $\overline{G}$ *for* $X_{n,t,t}$
- *the wreath product* $(G\times G)\rtimes S_2$ *if* n,t,v *are pairwise distinct.*

Proof. 1. is clear by the definition of the normal torsion–free subgroups $N_{n,t,v}$ and a genus computation analogous to that of Theorem 1:

$$g \;=\; 1+\frac{pq}{2}\,(\,1-\frac{3}{q}\,)\;.$$

The isomorphisms between the different Belyi surfaces of this type are determined by Corollary 2.2.
2. follows from Lemma 4.2 and its proof.
3. If $X_{n,t,v}$ and $X_{m,s,w}$ belong to the same Galois orbit, then clearly also their respective

quotients $Y_{n,t,v}$ and $Y_{m,s,w}$ by the unique normal subgroup $Z_p \lhd G$. Theorem 2 shows that these are Galois conjugate if and only if they are isomorphic if and only if their index triples are equivalent. So $X_{n,t,v}$ and $X_{m,s,w}$ belong to the same Galois orbit at most if $(n,t,v) \sim (m,s,w)$. To see that this condition is also sufficient, we follow the ideas of [St2] and need some preparation. Recall that for $\alpha \in G$ with fixed point $P \in X_{n,t,v}$ there is a local variable z with $z(P) = 0$ such that the action of α locally is described by $z \mapsto \xi z$ for some root of unity ξ. We will call this ξ (uniquely determined by P and α) the *multiplier of* α *in* P.

Lemma 6 *1. For the action of G on $X_{n,t,v}$ there are $3p$ fixed points of order q.*

2. Every element $a^m b^n$ of order q, $m \in \mathbb{Z}/p\mathbb{Z}$, $n \in (\mathbb{Z}/q\mathbb{Z})^*$, has three fixed points.

3. In its three fixed points, b acts with multipliers $\zeta^{\bar{n}}$, $\zeta^{\bar{t}}$, $\zeta^{\bar{v}}$ where $\bar{n}, \bar{t}, \bar{v}$ denote the inverses of $n, t, v \in (\mathbb{Z}/q\mathbb{Z})^*$ respectively, i.e. with $\bar{n}n \equiv \bar{t}t \equiv \bar{v}v \equiv 1 \bmod q$.

Proof of Lemma 6. 1. follows by a simple counting argument: The surface is triangulated by $3pq$ images of Δ–fundamental domains. To each of these fundamental domains belong three fixed points of order q, but every such fixed point belongs to q Δ–fundamental domains. (David Singerman indicated to us another possible argument using results of Macbeath [Mc].)
2. In G, there are precisely p conjugate subgroups of order q, see Lemma 1.4. Two different such subgroups can be generated by $a^m b$, $a^k b$ with $m \not\equiv k \bmod p$. If P were a common fixed point for both it would also be a fixed point for a by consequence of

$$b^{-1}\, a^{-k+m}\, b\,(P) \;=\; P$$

and the defining relations in G. But a acts fixed–point free on the surface, whence every subgroup of order q has a fixed point triple, and these triples in fact form an orbit under the action of Z_p.
3. On the universal covering $\mathcal{H}$ of $X_{n,t,v}$ the generators $\gamma_0, \gamma_1, \gamma_\infty$ of Δ act in their respective fixed points with multiplier ζ. Since $h(\gamma_0) = b^n$, the fixed point of γ_0 has to be applied by the universal covering map $\mathcal{H} \to X_{n,t,v}$ on one of the fixed points of b, and there b must have the multiplier $\zeta^{\bar{n}}$. The same argument applies in the fixed points of γ_1 and γ_∞ if we observe that e.g. ab^t is conjugate to b^t (see Lemma 1.3) and has therefore the same multipliers in its fixed points.

Proof of Theorem 3, continued. Now we observe that no automorphism group of our surfaces in question contains Z_2 as normal subgroup whence they are not hyperelliptic. Therefore the *canonical model* exists, constructed as the image of the following embedding. Let $\omega_1, \dots, \omega_g$ be a basis of the vector space of holomorphic differentials on $X_{n,t,v}$. Then the map

$$X_{n,t,v} \;\to\; \mathbb{P}^{g-1} \;:\; P \;\mapsto\; (\omega_1(P), \dots, \omega_g(P))$$

is a well–defined holomorphic embedding, so we may now identify $X_{n,t,v}$ with its image (automatically a projective algebraic curve by Chow's theorem). By [St1] it has the following remarkable property. The representation — analogous to ρ in Remark 4 —

$$\psi \;:\; G \;\to\; GL(H^0(X_{n,t,v}, \Omega))$$

on the vector space of holomorphic differentials defined by

$$\psi(\alpha)\ :\ \omega\ \mapsto\ \omega\circ\alpha^{-1}$$

induces an action of $\psi(G)/\{\pm 1\}$ as subgroup of $PGL_g(\mathbb{C})$ on the canonical model. Now let P be a fixed point for $\alpha\in G$ on this canonical model with multiplier ξ. As in [St2], $P\in\mathbb{P}^{g-1}$ can be represented as an eigenvector for $\psi(\alpha)$ with eigenvalue ξ^{-1}. In our particular case, $\psi(b^{-1})$ has three eigenvectors giving fixed points of $X_{n,t,v}$ and belonging to eigenvalues $\zeta^{\bar n},\zeta^{\bar t},\zeta^{\bar v}$, see Lemma 6, and these eigenvalues uniquely determine the isomorphism class of $X_{n,t,v}$. ($\psi(b^{-1})$ may have more eigenvectors, in particular for other eigenvalues, but these do not give points of the canonical model.)
Let $\sigma\in\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ be any Galois conjugation, tacitly assumed to be extended to a field automorphism of $\mathbb{C}$. As explained in Section 2, σ maps $X_{n,t,v}$ to a Galois conjugated curve $X^\sigma_{n,t,v}$ which is again a canonical model because the basis $\omega_1,\dots,\omega_g$ is transformed into a basis $\omega_1^\sigma,\dots,\omega_g^\sigma$ of holomorphic differentials on $X^\sigma_{n,t,v}$. The representation matrices $\psi(\alpha)$ are transformed by coefficient–wise conjugation into representation matrices $\psi(\alpha)^\sigma$. In particular, the fixed points P of b^{-1} on $X_{n,t,v}$ become fixed points P^σ of b^{-1} on $X^\sigma_{n,t,v}$, now corresponding to eigenvectors of $\psi(b)^\sigma$ for eigenvalues $\sigma(\zeta^{\bar n}),\sigma(\zeta^{\bar t}),\sigma(\zeta^{\bar v})$. There is a unique $s\in(\mathbb{Z}/q\mathbb{Z})^*$ satisfying $\sigma(\zeta)=\zeta^{\bar s}$ for $\bar s\in(\mathbb{Z}/q\mathbb{Z})^*$, $\bar s s\equiv 1 \bmod q$. Since $X^\sigma_{n,t,v}$ is uniquely determined up to isomorphism by the eigenvalues $\zeta^{\bar s\bar n},\zeta^{\bar s\bar t},\zeta^{\bar s\bar v}$, the only choice of the Galois conjugated surface is $X_{sn,st,sv}$.
4. Observe that $\sigma\in\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ with $\sigma(\zeta)=\zeta^{\overline{s}}$, $s\in(\mathbb{Z}/q\mathbb{Z})^*$ transforms $X_{n,t,v}$ into an isomorphic surface if and only if (sn,st,sv) is a permutation of (n,t,v).
5. The proof of this point is similar to the proof of Theorem 1.8 with the difference that the automorphisms of order q on $X_{n,t,v}$ now have three fixed points. The details are left to the reader.
6. For the definition of the cartographic group and its meaning as a Galois invariant, see [JSt]. The reduction to the monodromy group of $X_{n,t,v}\to\overline{\Delta}\backslash\mathcal{H}$ follows directly from the definitions. In the case $t=v$ this is a normal covering, hence the cartographic group is isomorphic to the covering group $\overline{G}$. In the other cases, the proof goes along the lines of the constructions explained in [JSt].

Remarks. 7. The warning after Theorem 1 applies to the Belyi pairs $(U^m_{n,t,v},\beta^m_{n,t,v})$ as well. Also, Remark 1 applies vice versa to the surfaces X_{s,st,st^2} and their canonical Belyi functions B if $t^3\equiv 1$, $1+t+t^2\equiv 0 \bmod q$. Here B is definable over the cubic extension $\mathbb{Q}(\zeta)$ of its moduli field only.
8. The Belyi surfaces $X_{n,t,t}$ can further be divided by the cyclic subgroups Z_{2q} of $\overline{G}$ giving quotients $V^m_{n,t}$ of $U^m_{n,t,t}$. The covering $X_{n,t,t}\to V^m_{n,t}$ is ramified in one point with order $2q$, in two points with order q and in q points with order 2. So their genus is

$$g(V^m_{n,t})\ =\ \frac{(p-1)(q-3)}{4q}\,.$$

For example: in the case $q=5$, $p=11$ the $V^m_{n,t}$ are elliptic curves. It would be very interesting to know how they depend on (n,t).

9. We sketch another possibility for the proof of Theorem 3 suggested by the two preceding sections. Since $X_{n,t,v}$ is an unramified cyclic covering of $Y_{n,t,v}$, we can construct the function field of the covering by adjoining a function z to the function field $\mathbb{C}(x,y)$ of $Y_{n,t,v}$ where x,y,z satisfy (for the first equation see Theorem 2.4)

$$y^q \;=\; x^n\,(x-1)^t \quad , \quad z^p \;=\; f(x,y)$$

with a rational function f on the base curve. To avoid ramifications, this rational function must have a divisor (f) which is the p–th power of a non–principal divisor D. Since $D^p = (f)$ is principal, we can use Jacobi's theorem and look for the p–division points of the Jacobian $\mathrm{Jac}\,Y_{n,t,v}$. The dimension of the Jacobian is the genus of the curve whence the p–division points form — in obvious additive notation — a $(q-1)$–dimensional vector space over the field $\mathbb{F}_p$ with p elements. Kummer theory [L] implies that the different possible cyclic unramified extensions depend on these divisors D modulo principal divisors and modulo taking powers only (in vector space notation: modulo $\mathbb{F}_p^*$–multiples). So we can associate to every possible unramified cyclic covering of degree p a unique point in the projective space $\mathbb{P}^{q-2}(\mathbb{F}_p)$. Now we have a further restriction on the covering coming from the specific automorphism group acting on our covering spaces. The subgroup $Z_q = < b >$ acts on the base space, hence also as an automorphism group on the Jacobian and even $\mathbb{F}_p$–linear on the vector space of p–division points. In analogy to the proof of Theorem 1, part 4, we are looking for divisor classes $\overline{D}$ with $b(\overline{D}) = \overline{D}^c$, i.e. for eigenvectors of b in the vector space notation. Now one has to prove that $q-1$ eigenvalues occur and are admissible for our construction according to the different choices of the primitive q–th root of unity. The case (s, st, st^2) with $t^3 \equiv 1$, $1+t+t^2 \equiv 0 \bmod q$ is again very special because there the Jacobian is isogenous to a third power of a Jacobian of complex dimension $(q-1)/6$, see [KR].

10. Finally, the use of canonical models and multipliers in the proof can be replaced by the use of Belyĭ's cyclotomic character: here one has to study the coefficient–wise action of $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ on the Puiseux expansions of the inverse Belyi function B in the ramification points.

7 Representations

As in the proof of Theorem 3, let ψ be the representation of G on the vector space $H^0(X,\Omega)$ of holomorphic differentials on our Belyi surface X defined by

$$\psi \;:\; \alpha \;\mapsto\; (\,\omega \;\mapsto\; \omega\circ\alpha^{-1}\,)\;,\; \alpha\in G\;.$$

and $tr\psi$ its trace. By different reasons — explicit computation of the canonical models [St1], decomposition of the Jacobian, Galois invariants — its decomposition in irreducible representations is of some interest. The trace can be calculated as follows.

Lemma 7 *Let G, a, b, ζ, η, X_s, $X_{n,t,v}$ be defined as in Theorems 1 and 3 and their proofs, $\bar n$, $\bar t$, $\bar v$ as in Lemma 6, and as in Lemma 1 let S denote the subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ generated by u. For all $m\in\mathbb{Z}/p\mathbb{Z}$, $x\in(\mathbb{Z}/p\mathbb{Z})^*$, $y\in(\mathbb{Z}/q\mathbb{Z})^*$, we have*

1. *on* X_s

$$tr\psi(1) \;=\; \frac{1}{2}\,(p-1)\,(q-2) \quad , \quad tr\psi(a^m b^{-y}) \;=\; 0 \quad , \quad tr\psi(a^{-x}) \;=\; 1 + \sum_{w\in S} \frac{\eta^{xw}}{1-\eta^{xw}}\,,$$

2. *on* $X_{n,t,v}$

$$tr\psi(1) \;=\; 1 + \frac{1}{2}p(q-3)\,, \quad tr\psi(a^m b^{-y}) \;=\; 1 + \frac{\zeta^{\bar{n}y}}{1-\zeta^{\bar{n}y}} + \frac{\zeta^{\bar{t}y}}{1-\zeta^{\bar{t}y}} + \frac{\zeta^{\bar{v}y}}{1-\zeta^{\bar{v}y}}\,,$$

$$tr\psi(a^{-x}) \;=\; 1\,.$$

The *proof* is an application of Eichler's trace formula (see [FK]) counting fixed points and multipliers. For the surfaces $X_{n,t,v}$, this program is essentially carried out in Lemma 6: recall that by Lemma 1.3, $a^m b^{-y}$ is conjugate to b^{-y} and therefore has the same multipliers in its three fixed points, and recall that a acts without fixed points. For the first part of the Lemma consider first the quotient $Y = Z_p\backslash X_s = < a > \backslash X_s$ of genus 0 treated in Theorem 1.7. There, b has two fixed points with multipliers ζ and ζ^{-1}. Each of them lifts to p fixed points on X_s with the same multiplier (the covering $X_s \to Y$ is ramified in other points). Clearly, the generators $a^m b\,,\, m \in \mathbb{Z}/p\mathbb{Z}$ of the p subgroups of order q have two fixed points with multipliers ζ and ζ^{-1}, respectively. Taking $(-y)$–th powers, Eichler's trace formula gives for all $m \in \mathbb{Z}/p\mathbb{Z}\,,\, y \in (\mathbb{Z}/q\mathbb{Z})^*$

$$tr\psi(a^m b^{-y}) \;=\; 1 + \frac{\zeta^{y}}{1-\zeta^{y}} + \frac{\zeta^{-y}}{1-\zeta^{-y}} \;=\; 0\,.$$

By the construction of X_s, the element a has q fixed points given by the coordinates $x = \zeta^k\,,\, y = 0$ on the model of Theorem 1.4. Which multipliers? Let $z_0 \in \mathcal{H}$ be the fixed point of the generator γ_0 of Δ. Under the covering map, it goes to the fixed point $P := N_s z_0 \in X_s$ of a, of course with multiplier η. This point gives all fixed points of a in the form $b^k(P)\,,\, k \in \mathbb{Z}/q\mathbb{Z}$. We may describe fixed points by q–tuples in G^q as follows. P corresponds to $[1, a, a^2, \ldots, a^{q-1}]$ thinking of the $< a >$–orbit $a^m F$ of the image F of a canonical Δ–fundamental domain under the universal covering map, arranged in counterclockwise order around their common point P. There, the action of a is described by

$$[1, a, a^2, \ldots, a^{q-1}] \;\mapsto\; [a, a^2, \ldots, a^{q-1}, 1]\,.$$

The point $b^k(P)$ corresponds to

$$[b^k, b^k a, b^k a^2, \ldots, b^k a^{q-1}] \;=\; [b^k, a^{u^{-k}} b^k, a^{2u^{-k}} b^k, \ldots, a^{(q-1)u^{-k}} b^k]\,,$$

and at this fixed point it is now immediate that $a^{u^{-k}}$ acts with multiplier η, hence a with multiplier η^{u^k}. Each such multiplier occurs precisely once, therefore Eichler's trace formula proves the claim.

The behaviour of $tr\psi$ under Galois actions and the decomposition of ψ in irreducible components by means of Eichler's trace formula is not obvious. It becomes easier if we state it in a different but equivalent way, more in the spirit of Chevalley's and Weil's paper [CW]. For a real number r let $\langle r\rangle = r - [r]$ denote the *fractional part* and as always $\eta = e^{2\pi i/p}$.

Lemma 8 *Let* $m_1, \ldots, m_k$ *and* $\bar m_1, \ldots, \bar m_k \in (\mathbb{Z}/p\mathbb{Z})^*$ *satisfy* $m_j \bar m_j \equiv 1 \bmod p$ *for all* j *and* $m_1 + \ldots + m_k \equiv 0 \bmod p$. *Then*

$$1 + \sum_{j=1}^{k} \frac{\eta^{\bar m_j}}{1-\eta^{\bar m_j}} = \sum_{z=1}^{p-1} \left(-1 + \sum_{j=1}^{k} \langle -\frac{m_j z}{p}\rangle \right) \eta^z .$$

Proof. For every j,

$$\sum_{z=0}^{p-1} \langle \frac{m_j z}{p}\rangle \, \eta^z = \sum_z \langle \frac{z}{p}\rangle \, \eta^{\bar m_j z} ,$$

hence

$$(1-\eta^{\bar m_j}) \sum_z \langle \frac{m_j z}{p}\rangle \, \eta^z = \sum_z \langle \frac{z}{p} (\eta^{\bar m_j z} - \eta^{\bar m_j (z+1)}) =$$

$$= \sum_{z=0}^{p-1} \left(\langle \frac{z}{p}\rangle - \langle \frac{z-1}{p}\rangle \right) \eta^{\bar m_j z} = -1 + \frac{1}{p} + \sum_{z=1}^{p-1} \frac{1}{p} \eta^{\bar m_j z} = -1 .$$

Therefore

$$\frac{\eta^{\bar m_j}}{1-\eta^{\bar m_j}} = -1 + \frac{1}{1-\eta^{\bar m_j}} = -1 - \sum_z \langle \frac{m_j z}{p}\rangle \, \eta^z =$$

$$= \sum_{z=1}^{p-1} (1 - \langle \frac{m_j z}{p}\rangle) \, \eta^z = \sum_z \langle -\frac{m_j z}{p}\rangle \, \eta^z$$

and

$$1 + \sum_{j=1}^{k} \frac{\eta^{\bar m_j}}{1-\eta^{\bar m_j}} = 1 + \sum_z \left(\sum_{j=1}^{k} \langle -\frac{m_j z}{p}\rangle \right) \eta^z = \sum_{z=1}^{p-1} \left(-1 + \sum_j \langle \frac{-m_j z}{p}\rangle \right) \eta^z .$$

The relation to the Chevalley–Weil result becomes more explicit if we observe that $tr\psi(a^{-1})$ is the sum of the eigenvalues of a^{-1}, choosing a^{-1}–eigendifferentials as basis of $H(X,\Omega)$. Since the roots of unity η^z, $z \not\equiv 0 \bmod p$, are linearly independent over $\mathbb{Q}$ and since $1 + \sum_{z \not\equiv 0 \bmod p} \eta^z = 0$, we can draw the following conclusion (valid in more general cases, of course).

Corollary 3 *Let a be an automorphism of prime order p of the compact Riemann surface X, acting in its fixed points with multipliers $\eta^{-\bar{m}_j}$. Then, up to an additive term c independent of $z \neq 0$, the coefficient of η^z, $z \neq 0$, given by Lemma 8 is the dimension*

$$c \,+\, (\,-1 \,+\, \sum_j \langle \frac{-m_j z}{p} \rangle\,)$$

of the eigenspace for the eigenvalue η^z if we decompose $H^0(X,\Omega)$ in eigenspaces for the action of a^{-1}. The number c gives the dimension of the subspace of a–invariant differentials (i.e. those lifted from $Z_p\backslash X$, $Z_p = <a>$), hence the genus of $Z_p\backslash X$.

Remark 11. If we replace p by q and η by ζ we can apply Lemma 8 also to $tr\psi(a^m b^{-y})$ on $X_{n,t,v}$ given by Lemma 7. For $y \not\equiv 0 \bmod q$ the result is the same as for the representation ρ of $Z_q = <b>$ on the intermediate covering $Y_{n,t,v}$ (see Remark 4) and gives the well–known eigenspace decomposition for this curve whose Jacobian has complex multiplication by $\mathbb{Q}(\zeta)$, see [KR].

If we denote the representation ψ belonging to the surface $X_{n,t,v}$ more precisely by $\psi_{n,t,v}$ we obtain the following

Theorem 4 *The Belyi surfaces $X_{n,t,v}$ and $X_{m,s,w}$ belong to the same Galois orbit if and only if there is a $\sigma \in \mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ with the property*

$$\sigma(tr\psi_{n,t,v}(g)) \,=\, tr\psi_{m,s,w}(\tau g) \quad \textit{for all} \quad g \in G \quad \textit{and a fixed} \quad \tau \in \mathrm{Aut}\, G\,.$$

Proof. The comparison with Lemma 7 shows that any Galois conjugation σ with $\sigma(\zeta) = \zeta^{\bar{k}}$, $\bar{k}k \equiv 1 \bmod q$, maps $tr\psi_{n,t,v}$ to $tr\psi_{kn,kt,kv}$, so Galois conjugate surfaces (see Theorem 3) lead to Galois conjugate traces. On the other hand, if we have Galois conjugate traces for the triples (n,t,v) and (m,s,w), Lemma 8 implies the existence of some $k \in (\mathbb{Z}/q\mathbb{Z})^*$ with

$$-1 \,+\, \langle\frac{knz}{p}\rangle + \langle\frac{ktz}{p}\rangle + \langle\frac{kvz}{p}\rangle \;=\; -1 \,+\, \langle\frac{mz}{p}\rangle + \langle\frac{sz}{p}\rangle + \langle\frac{wz}{p}\rangle$$

for all $z \in (\mathbb{Z}/q\mathbb{Z})^*$, and by [KR] this is possible only for equivalent triples. Then Theorem 3 says that the surfaces are Galois conjugate.

Remarks. 12. The "only if" part of Theorem 4 can be proved using no special property of the surfaces $X_{n,t,v}$, just applying σ to the curve, its differentials, its automorphisms etc. It is therefore a general observation that the Galois orbit of the traces $tr\psi$ forms a new Galois invariant at least for Belyi surfaces with many automorphisms. The same is true for the Galois orbit of the totality of multipliers of the Elements of G in their fixed points. As part 6 of Theorem 3 shows, they give a sharper distinction between Galois orbits than monodromy groups and cartographic groups. It has to be worked out further how these invariants can be used for ordinary hypermap groups of Belyi pairs not having many automorphisms, and in which other

cases they could give not only necessary but also sufficient conditions for Galois conjugacy. Another open problem can be formulated as follows: is it possible to get better Galois invariants taking monodromy groups of $p(B)$ for other Shabat polynomials p combined with the original Belyi function B ?
13. The idea given in Remark 11 and also Eichler's trace formula work as well for differentials of higher degree.

Theorem 5 *The decomposition of the representation ψ into irreducible components is given by the decomposition of its trace into the irreducible characters of G (see Lemma 1.6) as follows.*

1. *On X_s we have*
$$tr\psi \;=\; \sum_{j=1}^{r} \left(-1 + \sum_{w\in S} \langle -\frac{wv_j}{p} \rangle \right) \phi_j \;.$$
2. *We consider the representation ρ introduced in Remark 4 as a component of ψ defined on the $(q-1)/2$–dimensional $\psi(G)$–invariant subspace of $H^0(X_{n,t,v},\Omega)$ of differentials lifted from $Y_{n,t,v}$. Then we have on $X_{n,t,v}$*
$$tr\psi \;=\; tr\rho \;+\; \frac{q-3}{2}\sum_{j=1}^{r}\phi_j \;,$$
$$tr\rho \;=\; \sum_{k=1}^{q-1}\left(-1 + \langle\frac{nk}{q}\rangle + \langle\frac{tk}{q}\rangle + \langle\frac{vk}{q}\rangle \right) \chi_k \;.$$

The *proof* can be given by the standard computation of multiplicities as inner products of traces or by counting eigenvalues or directly as follows. If we always denote the inverse mod p (or q, respectively) by the bar, we know by Lemma 7 and Lemma 8 that on X_s for $x \in (\mathbb{Z}/p\mathbb{Z})^*$
$$tr\psi(a^{-x}) \;=\; 1 + \sum_{w\in S}\frac{\eta^{xw}}{1-\eta^{xw}} \;=\; \sum_{z=1}^{p-1}\left(-1 + \sum_{w\in S}\langle -\frac{\bar{x}\bar{w}z}{p}\rangle \right) \eta^{z} \;.$$
We can replace z by $-v_j ux$ where u runs over S and v_j, $j = 1,\dots,r$, over a system of representatives of $(\mathbb{Z}/p\mathbb{Z})^*/S$ as in Lemma 1.6. With $s := \bar{w}u \in S$ we get
$$tr\psi(a^{-x}) \;=\; \sum_{j=1}^{r}\sum_{u\in S}\left(-1 + \sum_{w\in S}\langle\frac{\bar{w}uv_j}{p}\rangle \right) \eta^{-v_j ux} \;=\; \sum_{j}\left(\left(-1 + \sum_{s\in S}\langle\frac{sv_j}{p}\rangle \right) \sum_{u\in S}\eta^{-v_j ux} \right) \;.$$
Replacing again s by w, the right side becomes
$$\sum_{j}\left(-1 + \sum_{w\in S}\langle\frac{wv_j}{p}\rangle \right) \phi_j(a^{-x}) \;.$$

For $a^m b^{-y}$ instead of a^{-x} this identity holds trivially since both sides vanish, and the check that

$$tr\psi(1) \;=\; \frac{1}{2}\,(p-1)\,(q-2) \;=\; \sum_j \left(-1 + \sum_{w\in S} \langle \frac{wv_j}{p} \rangle \right) \phi_j(1)$$

easily follows from $qr = p - 1$ and

$$\sum_j \sum_{w\in S} \langle \frac{wv_j}{p} \rangle \;=\; \sum_{x=1}^{p-1} \langle \frac{x}{p} \rangle \;=\; \frac{p-1}{2} \,.$$

For part 2, we first observe that on $X_{n,t,v}$ the extension of ρ to G satisfies

$$tr\rho(a^x b^{-y}) \;=\; tr\psi(a^x b^{-y}) \quad , \quad tr\rho(a^{-x}) \;=\; \frac{q-1}{2}$$

for all $x \in \mathbb{Z}/p\mathbb{Z}\,, y \in (\mathbb{Z}/q\mathbb{Z})^*$. Now, reformulate $tr\rho(a^x b^{-y})$ as $tr\psi(a^m b^{-y})$ in the X_s–case above, replacing η by ζ and $\sum_S$ by a sum with three terms. Finally use

$$\sum_{j=1}^{r} \phi_j(a^{-x}) \;=\; -1 \qquad \text{for all} \quad x \not\equiv 0 \bmod p$$

to get the decomposition given in the theorem.

Corollary 4 *1. The Jacobian* $\mathrm{Jac}\, X_s$ *is isogenous to* A^q *where* A *denotes the Jacobian of the Belyi surface* $U_{s,m}$ *, see Theorem 1.8. The endomorphism algebra* $\mathrm{End}_0\, A := \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}\, A$ *contains the fixed field* $\mathbb{K} \subset \mathbb{Q}(\eta)$ *of the group* $S \subset (\mathbb{Z}/p\mathbb{Z})^* \cong \mathrm{Gal}\, \mathbb{Q}(\eta)/\mathbb{Q}$*. We have* $\dim A = r(q-2)/2$ *and* $[\mathbb{K} : \mathbb{Q}] = r$ *.*

2. The Jacobian $\mathrm{Jac}\, X_{n,t,v}$ *splits up to isogeny into*

$$\mathrm{Jac}\, Y_{n,t,v} \,\oplus\, A^q \quad \textit{with} \quad A \;:=\; \mathrm{Jac}\, U^m_{n,t,v}$$

and $\dim A = r(q-3)/2$ *for the surfaces* $U^m_{n,t,v}$ *considered in Theorem 3.5.*

Proof. Every $\psi(G)$–irreducible subspace of $H^0(X_s, \Omega)$ contains a b–invariant differential (more precisely: $\psi(b)$–invariant), i.e. lifted from the quotient surface $Z_q \backslash X_s \cong U_{s,m}$. Moreover, there is no a–invariant differential $\neq 0$ in $H^0(X_s, \Omega)$, whence we have an embedding $\mathbb{Q}(\eta) \subseteq \mathrm{End}_0(\mathrm{Jac}\, X_s)$. Let V_z a subspace of a–eigendifferentials for the eigenvalue η^z. Then, $Z_q =< b >$ permutes the a–eigenspaces V_{wz}, $w \in S$. This indicates, taking the quotient of $\mathrm{Jac}\, X_s$ by the induced action of Z_q, that the Jacobian is isogenous to a pure power of an abelian variety with $\mathbb{K}$–action.

The situation for $X_{n,t,v}$ differs from that for X_s in three points. First, there are Z_p–invariant differentials, i.e. those lifted from $Y_{n,t,v}$ whose Jacobian is a factor of the big Jacobian, whence we have to decompose the cofactor only. Second, in the special case $t = v$ we can decompose A even further in A_1^2 where $A_1 := \mathrm{Jac}\, V_{n,t}^m$ — see Remark 8 — is of dimension $r(q-3)/4$ and contains a subfield $\mathbb{K}_1 \subset \mathbb{Q}(\eta)$ of degree $r/2$ in its endomorphism algebra: take the quotient of $X_{n,t,v}$ by the subgroup Z_{2q} of $\overline{G}$ and the fixed field of the corresponding subgroup of $\mathrm{Gal}\,\mathbb{Q}(\eta)/\mathbb{Q}$. The third point is that there is still an embedding

$$\mathbb{K} \subseteq \mathrm{End}_0 \mathrm{Jac}\, A \qquad \text{or} \qquad \mathbb{K}_1 \subseteq \mathrm{End}_0 \mathrm{Jac}\, A_1$$

but it may have a different meaning than in the X_s–case: it is possible that e.g. $A \cong A_2^r$ and A_2 has the trivial endomorphism algebra $\mathbb{Q}$. For example, in the case $q = 5$, $p = 11$ mentioned in Remark 8, $\mathbb{K}_1 = \mathbb{Q}$. In general, this trivial situation does in not occur for X_s because $tr\psi$ is not rational, whence a splitting of the Jacobian into simple components with trivial endomorphism algebra is excluded: $\mathrm{End}_0 \mathrm{Jac}\, X_s$ cannot be isomorphic to a direct sum of matrix algebras $M_r(\mathbb{Q})$.

References

[CW] Cl.Chevalley, A.Weil: Über das Verhalten der Integrale 1. Gattung bei Automorphismen des Funktionenkörpers, Abh. math. Sem. Hamburg **10** (1934), 358–361.

[CG] J–M.Couveignes, L.Granboulan: Dessins from a geometric point of view, pp. 79–113 in L.Schneps (ed.): The Grothendieck Theory of Dessins d'Enfants. London Math. Soc. Lecture Note Series **200**, Cambridge UP 1994.

[DE] P.Dèbes, M.Emsalem: On Fields of Moduli of Curves, J. of Algebra **211** (1999), 42–56.

[FK] H.M.Farkas, I.Kra: Riemann Surfaces. Springer GTM **71**, 1980.

[JL] G.James, M.Liebeck: Representations and Characters of Groups. Cambridge UP 1993.

[JS] G.A.Jones, D.Singerman: Belyĭ Functions, Hypermaps and Galois Groups, Bull. London Math. Soc. **28** (1996), 561–590.

[JSt] G.A.Jones, M.Streit: Galois Groups, Monodromy Groups and Cartographic Groups, pp. 25–65 in L.Schneps, P.Lochak (ed.): Geometric Galois Actions 2. London Math. Soc. Lecture Note Series **243**, Cambridge UP 1997.

[KR] N.Koblitz, D.Rohrlich: Simple factors in the Jacobian of a Fermat curve. Can. J. Math. **30** (1978), 1183–1205.

[K] R.S.Kulkarni: Isolated points in the branch locus of the moduli space of compact Riemann surfaces, Ann. Acad. Sc. Fenn., Ser. A, I. Mathematica **16** (1991), 71–81.

[L] S.Lang: Algebra. Addison–Wesley 1965.

[Mc] A.M.Macbeath: Action of automorphisms of a compact Riemann surface on the first homology group, Bull. London Math. Soc. **5** (1973), 103–108.

[Po] H.Popp: On a conjecture of H. Rauch on theta constants and Riemann surfaces with many automorphisms, J. Reine Angew. Math. **253** (1972), 66–77.

[Sps] L.Schneps: Dessins d'enfants on the Riemann sphere, pp. 47–77 in L.Schneps (ed.): The Grothendieck Theory of Dessins d'Enfants. London Math. Soc. Lecture Note Series **200**, Cambridge UP 1994.

[Si] D.Singerman: Finitely Maximal Fuchsian Groups, J. London Math. Soc. (2) **6** (1972), 29–38.

[SSy] D.Singerman, R.I.Syddall: Belyĭ Uniformization of Elliptic Curves, Bull. London Math. Soc. **139** (1977), 443–451.

[St1] M.Streit: Homology, Belyĭ Functions and Canonical Curves, manuscripta math. **90** (1996), 489–509.

[St2] M.Streit: Field of Definition and Galois Orbits for Macbeath–Hurwitz curves, Arch. Math. **74** (2000), 342–349.

[Wo1] J.Wolfart: The 'Obvious' Part of Belyĭ's Theorem and Riemann Surfaces with Many Automorphisms, pp. 97–112 in L.Schneps, P.Lochak (ed.): Geometric Galois Actions 1. London Math. Soc. Lecture Note Series **242**, Cambridge UP 1997.

[Wo2] J.Wolfart: Triangle groups and Jacobians of CM type, homepage.