Cyclic Projective Planes and Wada Dessins

Manfred Streit and Jürgen Wolfart

Received: November 21, 2000
Revised: April 26, 2001

Communicated by Günter M. Ziegler

Abstract. Bipartite graphs occur in many parts of mathematics, and their embeddings into orientable compact surfaces are an old subject. A new interest comes from the fact that these embeddings give *dessins d'enfants* providing the surface with a unique structure as a Riemann surface and algebraic curve. In this paper, we study the (surprisingly many different) dessins coming from the graphs of finite cyclic projective planes. It turns out that all reasonable questions about these dessins — uniformity, regularity, automorphism groups, cartographic groups, defining equations of the algebraic curves, their fields of definition, Galois actions — depend on *cyclic orderings* of difference sets for the projective planes. We explain the interplay between number theoretic problems concerning these cyclic ordered difference sets and topological properties of the dessin like e.g. the *Wada property* that every vertex lies on the border of every cell.

2000 Mathematics Subject Classification: 51E15, 05C10, 14H25, 14H55, 20H10, 30F10
Keywords and Phrases: Projective planes, difference sets, dessins d'enfants, Riemann surfaces, Fuchsian groups, algebraic curves

1 Finite projective planes and dessins d'enfants

1.1 Projective planes, bipartite graphs, and maps

It is well known that the incidence pattern of finite projective planes can be made visible by connected bipartite graphs using the following dictionary.

$$\begin{array}{rcl} \text{line} & \longleftrightarrow & \text{white vertex} \\ \text{point} & \longleftrightarrow & \text{black vertex} \\ \text{incidence} & \longleftrightarrow & \text{existence of a joining edge} \\ \text{flag} & \longleftrightarrow & \text{edge} \end{array}$$

Following this dictionary, the axioms of projective geometry translate into graph–theoretic properties like
For any two different black vertices there exists a unique white vertex as a common neighbor.
The same is true for elementary properties like
Every black vertex has precisely $q = n + 1$ *white neighbors and every white vertex has precisely* $q = n + 1$ *black neighbors. The graph has* $l = n^2 + n + 1$ *black and white vertices, respectively, and* ql *edges.*
As usual, we will call n the *order* of the projective plane. (Recall that up to now only finite projective planes of prime power order are known.) On the other hand, it is well known that connected graphs can be embedded as maps into oriented compact surfaces [Li].

1.2 DESSINS D'ENFANTS

Now, bipartite graphs embedded into orientable compact surfaces cutting these surfaces into simply connected cells represent a way to describe Grothendieck's *dessins d'enfants.*
Definition. A (p, q, r)–DESSIN is a bipartite graph on an orientable compact surface X with the following properties.

1. The complement of the graph is the disjoint union of simply connected open cells.
2. p is the l.c.m. of all valencies of the graph at the black points.
3. q is the l.c.m. of all valencies of the graph at the white points.
4. $2r$ is the l.c.m. of all valencies of the cells (i.e. the numbers of bordering edges; they have to be counted twice if they border the cell at both sides).

Dessins arise in a natural way on compact Riemann surfaces (non–singular complex projective algebraic curves) X if there is a non–constant meromorphic (= rational) BELYI FUNCTION $\beta : X \to \overline{\mathbb{C}}$ ramified at most above $0, 1, \infty$. Then $\beta^{-1}\{0\}$, $\beta^{-1}\{1\}$ are the sets of white and black vertices respectively an the connected components of $\beta^{-1}]0, 1[$ are the edges of the dessin. According to a theorem of Belyi such a function exists if and only if — as an algebraic curve — X can be defined over a number field. Moreover, for every dessin $\mathcal{D}$ on a compact orientable surface X there is a unique conformal structure on X such that $\mathcal{D}$ results from a corresponding Belyi function β on X. Therefore the combinatorics of dessins should encode all properties of curves definable over $\overline{\mathbb{Q}}$. For a survey on this topic, see [JS]. In the present paper, we concentrate on two aspects namely *uniformization theory* and *Galois actions.*
As a Riemann surface with a (p, q, r)–dessin, X is the quotient space of a subgroup Γ of the triangle group Δ of signature $\langle p, q, r\rangle$, acting discontinuously on $\overline{\mathbb{C}}$, $\mathbb{C}$ or the hyperbolic plane $\mathcal{H}$ if

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1\,, \quad = 1 \quad \text{or} \quad < 1 \quad \text{respectively.}$$

The dessin is UNIFORM if all black points have equal valency p, all white points have equal valency q, and all cells have equal valency $2r$; equivalently, Γ has no torsion and is therefore the universal covering group of the Riemann surface. This is satisfied e.g. if the dessin is REGULAR, i.e. if its automorphism group G acts transitively on the edges; equivalently, Γ is a normal torsion–free subgroup of Δ (and then $\Delta/\Gamma \cong G$; for other reformulations of this condition see the first section of [StWo]). AUTOMORPHISM of the dessin means the restriction of an orientation–preserving topological — and automatically conformal — automorphism of X to the bipartite graph.

Recall that via the action of $\sigma \in \mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ on the coefficients of the defining equations of the algebraic curve X — or of an extension of σ to $\mathrm{Aut}\,\mathbb{C}/\mathbb{Q}$ on the coordinates of their points — one has a Galois action on the set of Riemann surfaces. We can even speak of Galois actions on dessins in the following sense: for a dessins $\mathcal{D}$ on X consider the corresponding Belyi function β. Clearly, for every $\sigma \in \mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ we have on the image curve X^σ a Belyi function β^σ defining a Galois conjugate dessin. (This Galois action is only the first step of Grothendieck's far reaching ideas for a better understanding of the structure of $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ via the so called Grothendieck–Teichmüller lego.)

1.3 The Fano plane. An easy observation

Concerning the embedding of the bipartite graph of a finite projective plane as a dessin on X, some immediate questions arise:

How does the structure of the Riemann surface depend on the choice of the embedding? Which additional structure of the projective plane (like e.g. $\mathrm{Aut}\,\mathbb{P}$*, the group of collineations) translates into a structure of the dessin and the Riemann surface?*

We are grateful to David Singerman who informed us about former work on these questions by himself [Si2], Fink and in particular Arthur White ([FiWh], [Wh]). In the following, we will take up their work under new topological and arithmetical aspects. Already the easiest example, i.e. the Fano plane $\mathbb{P}^2(\mathbb{F}_2)$, shows the existence of different embeddings leading to different dessins.

Fig. 6.5 of [JS] shows one of two embeddings of the graph of the Fano plane as a regular $(3,3,3)$–dessin, consisting of 7 hexagons on a torus. The underlying Riemann surface is the torus $\mathbb{C}/\Lambda$ for the sublattice Λ of the hexagonal lattice $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$ corresponding to one of the two prime ideals of norm 7 in that ring of integers. The automorphism group G of the dessin is isomorphic to $Z_7 \rtimes Z_3$, in fact a subgroup of $\mathrm{PGL}_3(\mathbb{F}_2)$ (Z_m denotes the cyclic group of order m). This full group of collineations of the Fano plane contains elements not giving automorphisms of the dessin because an automorphism of the dessin fixing an edge is automatically the identity. There is another embedding of the Fano plane graph as a dessin to be discussed now which is better for generalizations to other projective planes: Identify $\mathbb{F}_2^3 - \{0\}$ with the multiplicative group $\mathbb{F}_8^*$

of order 7 and generator g. The exponents m of g give a bijection

$$\mathbb{P}^2(\mathbb{F}_2) \quad \longleftrightarrow \quad \mathbb{Z}/7\mathbb{Z}$$

and an analogous bijection — with g^{-1} as generator — for the lines of the Fano plane. To make the incidence structure visible we use the trace t of the field extension $\mathbb{F}_8/\mathbb{F}_2$ as a nondegenerate bilinear form

$$b \; : \; \mathbb{F}_8 \times \mathbb{F}_8 \; \to \; \mathbb{F}_2 \; : \; (x,y) \; \mapsto \; t(xy) \; .$$

Then the point x and the line y are incident if and only if $t(xy) = 0$. We may choose the generator g such that $t(g) = 0$; then a point g^m and a line g^{-k} are incident if and only

$$t(g^{m-k}) \; = \; 0 \quad \iff \quad m - k \; \in \; \{1, 2, 4\}$$

what is easily seen using the Frobenius of $\mathbb{F}_8/\mathbb{F}_2$. Therefore, we may choose the local orientation of the Fano plane graph as given in Figure 1.

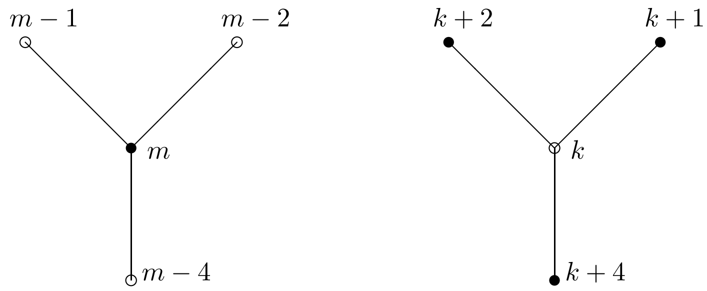

Figure 1: Local pattern of the Fano plane dessin

Then, the global dessin may be given as in Figure 2. To draw the picture on a Riemann surface, observe that every edge not incident with the white vertex 0 occurs twice. Identifying these edges, one obtains a $(3,3,7)$–dessin with 3 cells on a Riemann surface of genus 3. Here also, the automorphism group of the dessin is easily seen to be $Z_7 \rtimes Z_3$ which is a homomorphic image of the triangle group $\langle 3,3,7 \rangle$ as well. Moreover, one may prove that the kernel Γ of this homomorphism is torsion free and a normal subgroup even in the triangle group $\langle 2,3,7 \rangle$ with factor group $\mathrm{PSL}_2(\mathbb{F}_7) \cong \mathrm{PGL}_3(\mathbb{F}_2)$. The Riemann surface is known to be uniquely determined by this property: it is Klein's quartic. One may vary Figure 1 by taking the mirror image on both sides: the global result will be a regular dessin looking like Figure 2 but with completely different identifications of the edges. Its automorphism group is again $Z_7 \rtimes Z_3$ and its Riemann surface is again Klein's quartic, and both dessins are Galois conjugate in the sense explained above, see Theorem 1.

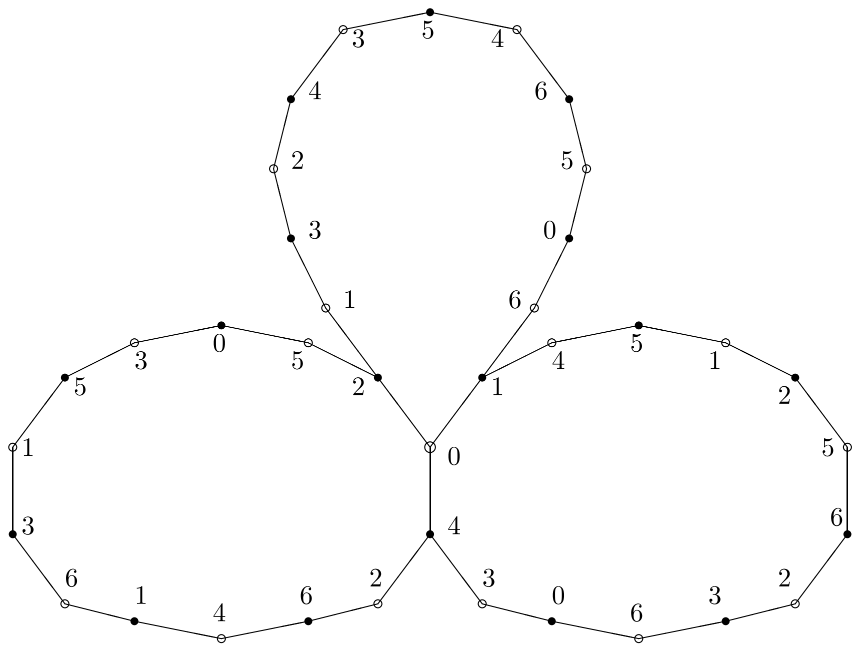

Figure 2: A $(3, 3, 7)$–dessin of the Fano plane

After all necessary identifications, we see that this Fano plane dessin has the remarkable property that every vertex lies on the border of every cell. Such phenomena occur even for subdivisions of the Euclidean plane into simply connected open domains, as was long time ago known to Kerékjártó and Brouwer ([Ke], p.120), and became popular more recently under the name *lakes of Wada* in the theory of dynamical systems [Ch]. Therefore, we propose the following

Definition. A Wada dessin is characterized by the property that every vertex lies on the border of every cell.

(This property may be reformulated passing to a dual dessin by exchanging e.g. the white vertices with the cells: then we obtain a complete bipartite graph embedded in such a way that every white vertex lies on the border of every cell.) Comparing the four realizations of the Fano plane graph as dessins one may remark that the global picture depends heavily on the choice of the local orientation of the edges around the vertices, see the proof of Proposition 2. How typical are the Fano plane dessins for the general situation? An evident observation is

PROPOSITION 1 *Let $\mathbb{P}$ be a finite projective plane of order n. Then any embedding of its graph as a dessin gives a (q,q,N)–dessin for some natural number N, where $q = n+1$ is the number of points on a line of $\mathbb{P}$. The automorphism group of the dessin corresponds to a subgroup of* $\mathrm{Aut}\,\mathbb{P}$ *acting fixed-point–free on the flags.*

To prove the last statement one has just to observe that only the identity automorphism of the dessin can fix an edge.

1.4 MAIN RESULTS

This first Proposition and the Fano plane example raise other questions:
is there a choice of the embedding such that $N = l$ is the number of points of $\mathbb{P}$? Is there a choice of the embedding such that the resulting dessin is a Wada dessin, uniform or even regular? Which subgroup of the collineation group of the projective plane becomes the automorphism group of the dessin? How does the absolute Galois group act on the corresponding set of algebraic curves? What is their field of definition?
It is not clear to us if these questions have a reasonable answer for very general embeddings of bipartite graphs coming from arbitrary finite projective planes. But it turns out that there is an interesting interplay between properties of $\mathbb{P}$ and the algebraic curve X if we concentrate on *cyclic* projective planes with an action of a *Singer group* Z_l and a *difference set* D — the definitions will be recalled in the beginning of the next section — and on embeddings compatible with the action of Z_l. First we (re)prove in Section 2

THEOREM 1 *For the known cyclic projective planes $\mathbb{P}^2(\mathbb{F}_n)$ the graph has embeddings into regular dessins if and only if $n = 2$ or 8. For $n = 2$ these are*

- 2 *non–isomorphic but Galois conjugate regular $(3,3,7)$–dessins on Klein's quartic (defined over $\mathbb{Q}$),*
- 2 *non–isomorphic but Galois conjugate regular $(3,3,3)$–dessins on the elliptic curve with affine model $y^2 = x^3 - 1$.*

For $n = 8$ there are embeddings into

- 6 *non–isomorphic, Galois conjugate regular $(9,9,73)$–dessins of genus* 252 *, defined over $\mathbb{Q}(\zeta_9)$, ζ_9 a 9–th primitive root of unity. Each pair of complex conjugate dessins lies on an algebraic curve defined over $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$.*
- 18 *non–isomorphic regular $(9,9,9)$–dessins of genus* 220 *defined over $\mathbb{Q}(\zeta_9)$ and forming* 3 *Galois orbits. They belong to* 18 *non–isomorphic algebraic curves definable over the same field and forming* 3 *Galois orbits as well.*

- 12 *non–isomorphic regular* $(9, 9, 3)$*–dessins of genus* 147 *lying on* 12 *non–isomorphic algebraic curves. The dessins and their curves form two Galois orbits and are defined over* $\mathbb{Q}(\zeta_9)$ *.*

The first sentence and the genera are known by [Si2], Sec. 5., 6., [FiWh], [Wh], Theorem 3.15, Theorem 5.3. Some results of [Wh], §3, Theorem 3.13, overlap also with

Theorem 2 *(and Definition). Let* $\mathbb{P}$ *be a cyclic projective plane with a fixed Singer group* Z_l *and a fixed difference set* D *. There is a bijection between*

- *pairs of cyclic orderings of* D *and*
- *embeddings of the graph of* $\mathbb{P}$ *as* (q, q, N)*–dessin* $\mathcal{D}$ *such that the automorphism group* $\mathrm{Aut}\,\mathcal{D}$ *contains* Z_l *.*

For special choices of these orderings, characterized by the fact that $\mathcal{D}/Z_l$ *is a genus* 0 *dessin,* $\mathcal{D}$ *becomes a* (q, q, l)*–dessin. We call these* $\mathcal{D}$ GLOBE COVERING *dessins; they depend on only one cyclic ordering of* D *.*

(For the terminology *globe covering* see the proof, and for existence of isomorphisms between the resulting dessins see the Remark following the proof in Section 2.)

Theorem 3 *If* l *is prime, all globe covering dessins of a cyclic projective plane are uniform Wada dessins.*

It will turn out that such (q, q, l)–dessins are typical Wada dessins, see Section 5, Proposition 7. Regular Wada dessins can be completely characterized by group theoretical properties (see Proposition 8 and 9) but are in general very different from dessins coming from projective planes (Proposition 11).
For all other cyclic projective planes with the (possible) exception $n = 4$ ($q = 5$, $l = 21$) there might exist embeddings onto uniform (q, q, l)–dessins as well. Some evidence for this conjecture — reformulated as a number theoretic question about cyclic orderings of difference sets — will follow from the proof of Theorem 3 (Section 3) and Proposition 4. Concerning the automorphism group of the dessin we will prove with similar methods as White [Wh], §3:

Theorem 4 *Let* $\mathbb{P}$ *be a cyclic projective plane of prime power order* $n = p^s \equiv 2 \bmod 3$ *, and suppose the number* $l = n^2 + n + 1$ *to be prime. Then the graph of* $\mathbb{P}$ *has embeddings as globe covering dessins with an automorphism group* $Z_l \rtimes Z_{3s}$ *.*

To explain how the subgroup Z_{3s} acts on the normal subgroup Z_l recall that p has the order $3s$ in the multiplicative group of prime residue classes $(\mathbb{Z}/l\mathbb{Z})^*$ [Wh], Lemma 3.3, hence acts by multiplication on $Z_l \cong \mathbb{Z}/l\mathbb{Z}$. As a special case, Theorem 4 contains the existence of regular dessins for the planes over

$\mathbb{F}_2, \mathbb{F}_8$. Section 6 gives a different proof of a more general result saying that for all l and all globe covering dessins, the automorphism group is of type $Z_l \rtimes Z_m$. Section 4 treats the explicit equations for the algebraic curves corresponding to the uniform globe covering dessins, in particular those of Theorem 3. We can give these equations in the relatively simple form

$$y^l \;=\; (x-\zeta^0)^{\overline{b_1}} \cdot \ldots \cdot (x-\zeta^{q-1})^{\overline{b_q}} \;,$$

where $\zeta = \zeta_q$ denotes a primitive q–th root of unity. The exponents $\overline{b_i}$ depend again on the ordering of the difference set of the projective plane, see Example 1 following Proposition 6. It will be shown that this equation can be replaced by another with coefficients in $\mathbb{Q}(\zeta+\zeta^{-1})$. Examples suggest that this field of definition is the smallest possible — Section 4 describes an effective procedure for the determination of the moduli field of the curve.
Even non–regular dessins have a description in terms of group theory, namely by their (hyper–) CARTOGRAPHIC GROUPS, i.e. the monodromy groups M of the Belyi function belonging to the dessin $\mathcal{D}$ (see the proof of Theorem 2 and Section 6). In the description given above using subgroups Γ of triangle groups Δ this monodromy group can be written as the quotient Δ/N by the maximal normal subgroup N of Δ contained in Γ . In other words, M is isomorphic to the automorphism group of the minimal regular cover R of $\mathcal{D}$. In particular, $M \cong \mathrm{Aut}\,\mathcal{D}$ for regular dessins. *How does M look like in the case of uniform dessins for cyclic projective planes?* In Section 6, we give the following partial answer:

THEOREM 5 *Under the conditions of Theorem 3, the cartographic group of the dessin $\mathcal{D}$ is isomorphic to a semidirect product*

$$Z_l^r \rtimes Z_q$$

with an exponent $r < q$.

Again, we will prove a slightly more general version than stated here. Again, the ordered difference sets determine the precise nature of the cartographic group, i.e. the exponent r and the action of Z_q on Z_l^r .
It is a great pleasure for us to thank Gareth Jones for the many fruitful discussions on these subjects during the last Southampton–Frankfurt workshops on dessins and group actions.

2 CYCLIC PROJECTIVE PLANES AND DIFFERENCE SETS

Recall that a finite projective plane $\mathbb{P}$ is called CYCLIC if there is a collineation a of order l generating a SINGER SUBGROUP of $\mathrm{Aut}\,\mathbb{P}$ acting sharply transitive on the points (and, by duality, on the lines) of $\mathbb{P}$. Fixing one point x and writing all points as $a^m(x)$ we may identify the points with the exponents $m \in \mathbb{Z}/l\mathbb{Z} \leftrightarrow Z_l$, hence read the cyclic automorphism group as the (additive) group Z_l acting by addition on Z_l. For the lines we adopt the same convention. In the case of the projective plane over the finite field $\mathbb{F}_n$ we may — as we did for the Fano plane — think of the exponents of some generator g of the multiplicative group $\mathbb{F}^*_{n^3}/\mathbb{F}^*_n$ and describe the incidence between points and lines using the trace t of $\mathbb{F}_{n^3}/\mathbb{F}_n$ as nondegenerate bilinear form. Locally, the embeddings in question will be chosen such that the incidence graph look as described in Figure 3,

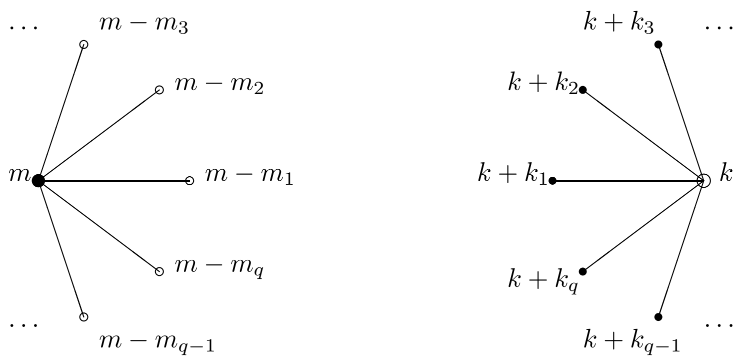

Figure 3: Local pattern of a dessin for a cyclic projective plane

for a fixed set $\{k_1, \dots, k_q\} = \{m_1, \dots, m_q\} \subset Z_l$ characterized by the property

$$t(g^{k_i}) = 0 \qquad \text{for all} \quad i = 1, \dots, q\,.$$

But we may use this figure for other cyclic projective planes as well (if there exist any) reading $\{k_1, \dots, k_q\} = \{m_1, \dots, m_q\} \subset Z_l$ as a DIFFERENCE SET D characterized by the property that for all $m \in Z_l$, $m \neq 0$, there are unique i and j with $m = k_i - k_j$. In any case, the cyclic collineation a of $\mathbb{P}$ can be identified with the shift

$$m \mapsto m + 1\,, \quad k \mapsto k + 1$$

proving graphically the *if* part of the following Proposition and the statement in Theorem 2 about the automorphism group as well.

PROPOSITION 2 *Let $\mathcal{D}$ be a dessin obtained by embedding the graph of a cyclic projective plane $\mathbb{P}$ with l points. Its Singer group Z_l becomes a subgroup of the automorphism group of $\mathcal{D}$ if and only if for all m and k the local orientation of the edges around the vertices are chosen as indicated in Figure 3. Such orientations correspond bijectively to the choice of a pair of orderings of a given difference set D for $\mathbb{P}$, both up to cyclic permutations.*

In fact, the translations $m \mapsto m + r$, $k \mapsto k + r$, $r \in Z_l$, preserve incidence and orientation and give the action of Z_l on the dessin. The *only if* part is true by the following reason: If a induces an automorphism of the dessin, the local orientations of the edges around the black vertices must show the same pattern as the left part of Figure 3, and an analogous statement is true for the white vertices.

Proof of Theorem 2. We know already by Proposition 2 that embeddings for the cyclic projective plane $\mathbb{P}$ as a dessin $\mathcal{D}$ with $Z_l \subseteq \operatorname{Aut}\mathcal{D}$ determine two orderings of the (fixed) difference set D. To prove the existence of such embeddings, choose a pair of orderings of D giving local orientations of the graph around all vertices as in Figure 3. These $2l$ drawings define in an obvious way local charts for an orientable surface into which the graph has to be embedded, and the numbering of the vertices gives the following unique prescription how to glue the local pieces together. Let Ω the set of all ql edges of $\mathcal{D}$ (flags of $\mathbb{P}$) and let M be the permutation group on Ω generated by b and w where b is the cyclic counterclockwise shift of all edges around the black vertices (i.e. sending the edge between m and $m - m_i$, for all $i \in Z_q$ and all $m \in Z_l$, to the edge between m and $m - m_{i+1}$ in the left part of Figure 3), and w is the corresponding counterclockwise shift of the edges around all white vertices. According to [JS], 5. Maps and Hypermaps, M and its generators b and w of order q define an *algebraic hypermap* on a unique compact Riemann surface X or — in the present terminology — a (q, q, N)–dessin on X where N is the order of wb in the *cartographic group* M. The surface X can be described explicitly as follows: there is an obvious homomorphism h of the triangle group $\Delta = \langle q, q, N\rangle$ onto M; let $H \subset M$ be the fixgroup of an arbitrary edge in Ω and let $\Gamma := h^{-1}(H)$, then we can define X as the quotient $\Gamma\backslash\mathcal{H}$.

For example, consider the case $n = 4$, $q = 5$, $l = 21$ with the cyclic ordering of a difference set

$$(m_i)_{i \bmod 5} = (-3, 0, 1, 6, 8) \quad , \qquad (k_i)_{i \bmod 5} = (8, 6, 1, 0, -3) \, .$$

Here one obtains a uniform $(5, 5, 5)$–dessin on a surface of genus 22 with 21 cells of valency 10 on which the Singer group Z_{21} acts fixed-point–free as cyclic permutation group of the set of cells. The quotient dessin $\mathcal{D}/Z_{21}$ has one cell, 5 edges, one black and one white vertex, hence genus 2.

For the last claim of the theorem suppose $\mathcal{D}$ to be globe covering. Since $\mathcal{D}/Z_l$ has genus 0 and q edges, one black and one white vertex (the poles), it has also q cells, and we can imagine the edges as meridians joining the poles and separating the cells. It is easy to see that this quotient dessin arises if and only if both orderings of D are the same, i.e. if in Figure 3 $m_i = k_i$ for all $i = 1, \ldots, q$. Clearly, the globe covering dessins depend on only one cyclic ordering of D. Their cells look as indicated in Figure 4.

Then, the numbers corresponding to the vertices on the border of the cell form arithmetic progressions in Z_l and therefore this cell has $2l/c_i$ edges where c_i is the gcd of l and $k_{i+1} - k_i$. The resulting dessin is therefore a (q, q, N)–dessin where $2N = 2l/c$ is the lcm of the valencies of the cells and c the gcd of all

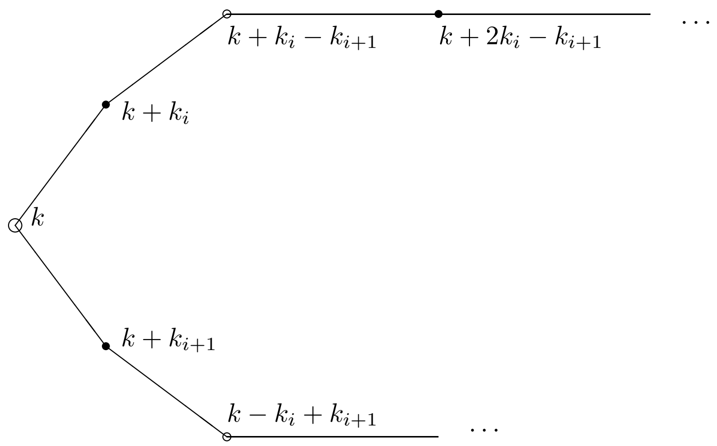

Figure 4: Cell of a globe covering dessin for a cyclic projective plane ($m_i = k_i$)

c_i . But $c > 1$ would imply that all differences $k_i - k_j$ were multiples of c in contradiction to the fundamental property of the difference set. Therefore, we have $N = l$ proving that globe covering dessins are (q, q, l)–dessins for $\mathbb{P}$.

Remark. Suppose $\mathcal{D}, \mathcal{D}'$ to be dessins resulting from two different pairs of orderings for D . Then there is no Z_l–equivariant isomorphism $i : \mathcal{D} \to \mathcal{D}'$, i.e. satisfying $i \circ a = a \circ i$, since in that case we could replace i by an isomorphism preserving the numbering of black and white vertices, hence also the local pattern of Figure 3. However, non–Z_l–equivariant isomorphisms may exist, related to multipliers of difference sets: for $n = 5, q = 6, l = 31$ take two different cyclic orderings of a fixed difference set D

$$(m_i) = (k_i) = (1,\ 5,\ 11,\ 25,\ 24,\ 27)\ , \quad (m'_i) = (k'_i) = (5,\ 25,\ 24,\ 1,\ 27,\ 11)$$

giving isomorphic dessins where the isomorphism is defined by $i : x \mapsto 5x$ mod l .

Exercise. Reverse the orientation in the right part of Figure 1 and show that this choice induces globally a $(3, 3, 3)$–Fano dessin. Reverse the orientation in the left part of Figure 1 to show that this choice induces globally another $(3, 3, 3)$–Fano dessin.

Proof of Theorem 1. That we can obtain regular dessins only for $n = 2$ and 8 follows directly from Proposition 1 and a theorem of Higman/McLaughlin [HML], Prop. 12, stating that for the planes $\mathbb{P}^2(\mathbb{F}_n)$ different from the Fano plane and $\mathbb{P}^2(\mathbb{F}_8)$, flag–transitive groups of collineations cannot act fixed-point–free on the flags. The converse direction is already verified for the Fano plane by giving two regular dessins in genus 1 and two in genus 3 . The genus 3 dessins belong to Klein's quartic which is known to be defined over $\mathbb{Q}$. As the two dessins on the elliptic curves they differ by their local orientation — see the exercise above (giving a *chiral pair of dessins*) — whence the dessins have to be complex conjugate. For the genus 1 dessins, the underlying elliptic curve is the same for both dessins since it has an automorphism of order 3, hence uniquely determined with model $y^2 = x^3 - 1$. On the other hand, the dessins are not isomorphic: their vertices are obtained (with suitable coloring) by the points of $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$ on the two tori

$$\mathbb{C}/(2 \pm \sqrt{-3})\mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})] \ .$$

These two tori are of course isomorphic but there is no isomorphism mapping the two dessins onto each other since multiplication by $(2+\sqrt{-3})/(2-\sqrt{-3})$ does not give an automorphism of the elliptic curve.
The two dessins for the Fano plane on Klein's quartic are non–isomorphic since they correspond to two different normal subgroups of the triangle group $\langle 3,3,7\rangle$ which are conjugate in the index 2 extension $\langle 2,3,14\rangle$, compare also Lemma 1 and 2 below.
For the plane $\mathbb{P}^2(\mathbb{F}_8)$ one may verify that

$$k_i \ = \ 2^i \bmod 73 \ , \quad i \ = \ 0 \, , \dots , 8 \ ,$$

form a difference set. A cyclic order is provided by the cyclic order of the exponents $i \bmod 9$. Therefore, it is easy to verify that

$$b \ : \ m \ \mapsto \ 2m \ : \ Z_{73} \ \to \ Z_{73}$$

together with a generates an edge–transitive automorphism group $G \cong Z_{73} \rtimes Z_9$ of the $(9,9,73)$–dessin described by Figure 4.
For the proof of the statements about the different possible images under these embeddings recall that cocompact triangle groups Δ with signature $\langle p,q,r\rangle$ are presented by generators and relations

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

The following is well known and turns out to be very useful for the classification of regular dessins.

Lemma 1 *Let* $\Delta = \langle p,q,r\rangle$ *be a Fuchsian triangle group. Then there is a bijection between*

- *isomorphism classes of regular* (p,q,r)*–dessins with automorphism group* G*,*
- *normal torsion free subgroups* Γ *of* Δ *with* $\Delta/\Gamma \cong G$*,*
- *equivalence classes of epimorphisms* $h : \Delta \to G$*, with torsion–free kernel, i.e. mapping the generators* γ_i *of* Δ *onto generators of* G *of the same order. Two epimorphisms are equivalent if they result from each other by combination with an automorphism of* G*.*

(The next lemma and the following remark will explain in more detail why non–isomorphic dessins may however lie on isomorphic Riemann surfaces.) For the special G under consideration, it is easy to see that such epimorphisms exist only for the triangle groups $\langle 9,9,m\rangle$ with $m = 73$, 9 or 3. Following closely the method described in [StWo] we can select homomorphisms h (with pairwise different kernels) onto $G \cong Z_{73} \rtimes Z_9$ with generators a, b as above in the following way. For $\langle 9,9,73\rangle$ we may take

$$h(\gamma_0) \;=\; b^s \;,\; h(\gamma_1) \;=\; b^{-s}a^k \;,\; h(\gamma_\infty) \;=\; a^{-k} \;, \quad s \in (\mathbb{Z}/9\mathbb{Z})^*$$

(another choice of $k \in (\mathbb{Z}/73\mathbb{Z})^*$ changes h only by composition with an element of $\operatorname{Aut} G$). For $\langle 9,9,9\rangle$ we may take

$$h(\gamma_0) \;=\; b^s \;,\; h(\gamma_1) \;=\; b^t a^k \;,\; h(\gamma_\infty) \;=\; a^{-k}b^u \;,$$

$$s\,,\,t\,,\,u \in (\mathbb{Z}/9\mathbb{Z})^* \quad \text{with} \quad s+t+u \;\equiv\; 0 \mod 9$$

(same remark for the choice of k), and for $\langle 9,9,3\rangle$ we may take

$$h(\gamma_0) \;=\; b^s \;,\; h(\gamma_1) \;=\; b^t a^k \;,\; h(\gamma_\infty) \;=\; a^{-k}b^{3u} \;,$$

$$s\,,\,t\,,\,u \in (\mathbb{Z}/9\mathbb{Z})^* \quad \text{with} \quad s+t+3u \;\equiv\; 0 \mod 9\;.$$

(same remark for the choice of k). The number of non–isomorphic dessins now follows from counting the possible parameter values s, t, u. The question if the underlying curves are isomorphic can be answered by another well known

Lemma 2 *Let Γ and N be two different torsion free normal subgroups of the Fuchsian triangle group Δ with isomorphic quotient $\Delta/\Gamma \cong G \cong \Delta/N$. The Riemann surfaces $\Gamma\backslash\mathcal{H}$ and $N\backslash\mathcal{H}$ are isomorphic if and only if the following equivalent conditions hold:*

- *Γ and N are $\mathrm{PSL}_2(\mathbb{R})$–conjugate.*
- *Γ and N are conjugate in some triangle group $\overline{\Delta} \supset \Delta$.*

(The two regular dessins corresponding to Γ and N are not isomorphic since the isomorphism of Riemann surfaces induced by the conjugation with $\overline{\Delta}$ permutes the different fix-point orbits of Δ, i.e. does not preserve at least the *color* of the vertices.) To apply this Lemma, one has to check if there are larger triangle groups and to control if the normal subgroups N remain normal in these larger triangle groups. Equivalently, one has to check if the homomorphisms found above are extendable to larger triangle groups than the original ones, see [StWo], Lemma 4. As an example, take the first case $m = 73$: here we obtain 6 different normal torsion–free subgroups N_s of Δ according to the 6 different choices of s. But Δ is contained with index 2 in the maximal triangle

group $\langle 2,9,146\rangle$ in which N_s and N_{-s} are conjugate. Therefore we obtain 6 non–isomorphic dessins but only 3 non–isomorphic Riemann surfaces.
The genera of the quotients of the upper half plane by these kernels can be computed by standard methods like Riemann–Hurwitz' theorem.
For the statements about fields of definition and Galois orbits recall first that curves X with many automorphisms can be defined over their field of moduli, i.e. the common fixed field of all σ with $X \cong X^\sigma$ [Wo1], Remark 4, [Wo2], Satz 3. For the determination of this field take again the example of the regular $(9,9,73)$–dessins. Let N_s be the kernel of the homomorphism h defined above by $h(\gamma_0) = b^s$, $h(\gamma_1) = b^{-s}a^k$ and let X_s be the quotient surface $N_s\backslash\mathcal{H}$. Recall that η is a MULTIPLIER of an automorphism α of X_s in some fixed point x if the action of α in a local coordinate z around x (corresponding to $z = 0$) can be described by $z \mapsto \eta z$ (not to be confused with multipliers in the theory of difference sets!). Then it is easy to prove

Lemma 3 *On X_s the automorphism b has two fixed points with multipliers $\zeta_9^{\overline{s}}$ and $\zeta_9^{-\overline{s}}$ where $\zeta_9 = e^{2\pi i/9}$ and $\overline{s}s \equiv 1 \bmod 9$.*

Using the representation of the automorphism group on the canonical model or Belyi's cyclotomic character one may prove moreover

Lemma 4 *Let σ be $\in \mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ and let b act as an automorphism of X with a multiplier η in the fixed point x. Then b acts in x^σ on X^σ with a multiplier $\sigma(\eta)$.*

Lemma 1, 2, 3 and the classification of the covering groups N_s show that the isomorphism class of X_s is uniquely determined among all surfaces with regular $(9,9,73)$–dessin and automorphism group G by the unordered pair of multipliers $\{\zeta_9^{\overline{s}}, \zeta_9^{-\overline{s}}\}$, and that the isomorphism class of dessins is uniquely determined by the ordered pair of multipliers. On the other hand, Lemma 4 shows that every σ fixing elementwise the cyclotomic field $\mathbb{Q}(\zeta_9)$ fixes the isomorphism class of dessin and curve. The Galois orbits are now easily determined by the action of $\mathrm{Gal}\,\mathbb{Q}(\zeta_9)/\mathbb{Q}$. The other cases can be treated in the same way.
It remains to prove that all the resulting bipartite graphs are isomorphic (as graphs, not as dessins) to the graph of $\mathbb{P}^2(\mathbb{F}_8)$. First, we observe that — by the freedom of choice of k — we may assume that all $h(\gamma_1)$ generate the same cyclic subgroup of G; the same observation holds trivially for all $h(\gamma_0)$. Then, from the first part of the proof we know that at least one resulting dessin has the desired property. Now, by the preceding classification of Riemann surfaces with a regular dessin and automorphism group G we obtain graph–isomorphic dessins what follows from a statement which might be of independent interest:

Proposition 3 *Let $\mathcal{D}_r, \mathcal{D}_l$ be regular (p,q,r)– and (m,n,l)–dessins with automorphism groups both isomorphic to G, induced by epimorphisms*

$$h_r \,:\, \langle p,q,r\rangle \,\to\, G\,, \quad h_l \,:\, \langle m,n,l\rangle \,\to\, G$$

with torsion–free kernels. The bipartite graphs of $\mathcal{D}_r$ and $\mathcal{D}_l$ are graph–isomorphic if

- $p = m$ *and* $q = n$ *,*
- *by combination with a group automorphism,* h_r *and* h_l *can be chosen such that*

  1. $h_r(\gamma_0)$ *and* $h_l(\gamma_0)$ *generate the same subgroup* B *of* G *,*
  2. $h_r(\gamma_1)$ *and* $h_l(\gamma_1)$ *generate the same subgroup* W *of* G *.*

Proof. A necessary condition for the existence of an isomorphism between both graphs is equality between the valencies in the vertices. Therefore we will suppose in the sequel that the first condition is satisfied. Since both dessins are regular with the same automorphism group, we can represent their edges by group elements $g \in G$ if we identify the edge 1 with the image of the hyperbolic line between the fixed points of γ_0 and γ_1 under the map of $\mathcal{H}$ onto its quotient by the kernels of h_r and h_l respectively. In order to describe the graph of $\mathcal{D}_r$ we have to describe incidence around black (white) vertices. Let B and W be the subgroups of G generated by $h_r(\gamma_0)$ and $h_r(\gamma_1)$ respectively. Then B and W consist of the edges incident with 1 in its black and white end–vertex, respectively. Using the G–action from the left, we see that the edge f is incident in its black end–vertex with all edges in fB and in its white end–vertex with all edges fW. Since this property does not depend on the choice of the generators of B and W, the conditions of Proposition 3 imply that the trivial and G–covariant application of edges $g \mapsto g$ induces an isomorphism of graphs.

Remarks. 1) The different non–isomorphic dessins for $P^2(\mathbb{F}_8)$ can be obtained as well by different pairs of orderings of the difference set. If one wants to obtain a regular dessin then only such permutations of D are admissible which are preserved by the multiplication with $2 \bmod 73$, and it is easy to see that there are precisely 6 such permutations. Applied independently to the incidence pattern around black and white vertices, this gives 36 different regular dessins as found in Theorem 1.
2) Which other cyclic projective planes besides the usual $P^2(\mathbb{F}_n)$ could exist, giving also a regular dessin? It is known that their order n has to be > 3600; furthermore, they should admit a sharply flag–transitive automorphism group, and by results of Kantor and Feit (see Theorem 8.18 of [Ju]) this could be possible only if a collection of exotic conditions holds: the order n of the plane must be a multiple of 8 but no power of 2, the number l of points is a prime, and the difference D set can be chosen as set of powers $n^k \bmod (\mathbb{Z}/l\mathbb{Z})^*$ (for this point one may also consult Proposition 11). Furthermore, D is its own group of multipliers and contains all divisors of n.
3) Galois conjugate dessins are in general not necessarily graph isomorphic. Some non–regular examples can be found in [JSt], but there are also such

examples for regular dessins: the three regular $(2,3,7)$–dessins with automorphism group $G = \mathrm{PSL}_2(\mathbb{F}_{13})$ on three Macbeath–Hurwitz curves treated in [St] give three non–isomorphic but Galois conjugate dessins whose graphs are not isomorphic.

3 THE WADA PROPERTY

We mention first that the *proof of Theorem 3* is an almost trivial consequence of the proof of Theorem 2: For prime l and globe covering dessins, i.e. with $m_i = k_i$ for all i in Figure 3, every cell in Figure 4 has valency $2l$. Therefore, the dessin is uniform, and every vertex lies on the border of every cell.
According to standard conjectures of number theory, there should exist an infinity of prime powers n such that $l = n^2 + n + 1$ is a prime ($n =$ 2, 3, 5, 8, 9, 17, ...). But even for composite l, each difference $k_i - k_{i+1}$ defines a module for an arithmetic progression in $\mathbb{Z}/l\mathbb{Z}$ giving the sequence of black points in clockwise order around the cell, and similarly for the white points. However, the length of these arithmetic progressions (determining the valency of the cell) is in general a proper divisor of l. For example in the case $n = 4$, $q = 5$, $l = 21$ the difference set

$$D \ := \ \{-3,\, 0,\, 1,\, 6,\, 8\}$$

has no arrangement such that all differences $k_i - k_{i+1}$ are coprime to l (the indices i have to be considered $\mod 5$, of course).
The question raised for composite l about the existence of uniform (q,q,l)–dessins for cyclic projective planes admitting Z_l as automorphism group may be reformulated now in the following way (note that for $n = 5$ we have $l = 31$ prime and that for $n = 6$ no difference set exists). *Let n be ≥ 7 and $l \geq 57$ be a composite number. Is it always possible to arrange a difference set*

$$D \ := \ \{\, k_i \mid i \bmod q\,\} \ \subset \ \mathbb{Z}/l\mathbb{Z}$$

in such a way that all successive differences $k_i - k_{i+1}$ are coprime to l ?
For small (prime powers) n the answer is positive thanks to the following Propositions.

PROPOSITION 4 *Let n be ≥ 7 and $l \geq 57$ be a composite number with prime divisor p. A difference set $D \subset \mathbb{Z}/l\mathbb{Z}$ can always be arranged in such a way that all successive differences of elements in D satisfy*

$$k_i \ - \ k_{i+1} \ \not\equiv \ 0 \mod p\,.$$

For the *proof* it is sufficient to show that no residue class $\mod p$ contains $\geq q/2$ elements among the elements of D. This will follow from

PROPOSITION 5 *Let n be ≥ 7 and $l \geq 57$ be a composite number with prime divisor p and a difference set $D \subset \mathbb{Z}/l\mathbb{Z}$. Let a_r be the number of elements $d \in$*

D with $d \equiv r \bmod p$, $r = 1, \dots, p$. Then the numbers a_r have the following properties.

$$\sum_r a_r \;=\; q \;=\; n+1\,, \tag{1}$$

$$\sum_r a_r^2 \;=\; \frac{l}{p} + n \;=\; \frac{1}{p}\,(n^2 + (p+1)n + 1)\,, \tag{2}$$

$$\sum_r a_r a_{r+s} \;=\; \frac{l}{p} \;=\; \frac{1}{p}\,(n^2+n+1) \quad \textit{for all} \quad s \not\equiv 0 \bmod p\,, \tag{3}$$

$$||\,(a_1,\dots,a_p) - \frac{1}{p}(n+1,\dots,n+1)\,||^2 \;=\; \frac{p-1}{p}\,n \tag{4}$$

$$Max\,|\,a_r - \frac{n+1}{p}\,| \;<\; \sqrt{n} \tag{5}$$

$$a_r \;<\; \sqrt{n} + \frac{n+1}{p} \quad \textit{for all} \quad r\,. \tag{6}$$

(In (4), we use the Euclidean norm in $\mathbb{R}^p$).

From the last inequality, $a_r < n/2$ follows for $n > 40$ and $p \geq 3$ or for $n > 8$ and $p \geq 7$ (note that the primes 2 and 5 never occur as divisors of l). Therefore, one has to check the truth of Proposition 4 by hand for some small n only. This can be done by giving the solutions of (1) to (3) for $p = 3$ and small n. These are, up to permutation of the coordinates

$$\begin{array}{rcrlrcl}
(a_1,a_2,a_3) & = & (4,3,1) & \text{for} & n & = & 7 \\
 & & (7,4,3) & \text{for} & n & = & 13 \\
 & & (9,7,4) & \text{for} & n & = & 19 \\
 & & (12,7,7) & \text{for} & n & = & 25 \\
 & & (13,12,7) & \text{for} & n & = & 31 \\
 & & (16,13,9) & \text{for} & n & = & 37\,.
\end{array}$$

Now we can explain the strategy how to construct uniform dessins for projective planes even in the case of composite l, e.g. for $n = 7$. Here we have two prime divisors $p = 3,\,19$ dividing $l = 57$ and we have to arrange D in such a way that just every second $k_i \in D$ is congruent to $1 \bmod 3$. Then, Proposition 5 is satisfied for $p = 3$, and we have $2 \cdot 4! \cdot 4!$ possibilities for such arrangements. Among these possibilities, one has to find an arrangement satisfying Proposition 5 also for $p = 19$. This is obviously possible since for $p = 19$, equations (1) and (2) are satisfied with one $a_r = 2$, for other six indices m one has $a_m = 1$, and all other a_t vanish.

Proof of Proposition 5. Equation (1) just counts the number of elements in D. Equation (2) follows from the fact that precisely $\frac{l}{p} - 1$ among the differences $k_i - k_j$, $i \neq j$, fall into the residue class $0 \bmod p$, and therefore

$$\sum_r a_r(a_r - 1) = \frac{l}{p} - 1 ,$$

Together with (1), this implies (2). Equation (3) follows by a similar consideration of the differences giving elements $\equiv d \not\equiv 0 \bmod p$. We may consider $(a_1, \ldots, a_p)$ as a point on the hyperplane given by equation (1). By Hesse's normal form, this hyperplane has square distance $\frac{1}{p}(n+1)^2$ from the origin, and the nearest point to the origin is of course $\frac{1}{p}(n+1, \ldots, n+1)$. Therefore, the square distance (2) and Pythagoras enable us to calculate the distance (4), and this implies (5).
Proof of Theorem 4. If $l = n^2 + n + 1$ is prime and $n = p^s$ a prime power, it is known [Wh], Lemma 3.3, that $p \bmod l$ has order $3s$ in the group $(\mathbb{Z}/l\mathbb{Z})^*$. Moreover, we may choose a difference set $D \subset Z_l = \mathbb{Z}/l\mathbb{Z}$ for the projective plane invariant under multiplication with $p \bmod l$. Therefore, as in the case of the plane $\mathbb{P}^2(\mathbb{F}_8)$ described in the proof of Theorem 1, we have at least a group of graph automorphisms isomorphic to $Z_l \rtimes Z_{3s}$. This group becomes an automorphism group of the globe covering dessin if and only if we can arrange D in such a way that the multiplication with p preserves this cyclic ordering of D.

LEMMA 5 *Under the hypotheses of Theorem 4, the action of Z_{3s} through multiplication by p^m on the p–invariant difference set D has orbits of length $3s$.*

Proof of the Lemma. Since l is prime and $p \bmod l$ has order $3s$, the orbits of the action on Z_l have length $3s$ or 1. Length 1 occurs for one orbit only, and this orbit cannot be contained in D since D has $q = n+1 \equiv 0 \bmod 3$ elements.
Proof of Theorem 4, continued. Now let $k_1, \ldots, k_r \in D$ represent the Z_{3s}–orbits of the Z_{3s}–invariant difference set D, $r = l/3s$. Arrange D as

$$k_1, \ldots, k_r, pk_1, \ldots, pk_r, p^2k_1, \ldots \ \ldots, p^{3s-1}k_r .$$

Then it is easy to check that the multiplication with $p \bmod l$ preserves the cyclic order of the edges incident with black and white vertices as described in Figure 3. Since l is prime, this arrangement does not bother the property that every cell has valency $2l$, see the proof of Theorem 3 in the beginning of this section.

4 EQUATIONS

The aim of this section is the determination of explicit algebraic models for the curves corresponding to the uniform (q, q, l)–dessins $\mathcal{D}$ coming from cyclic projective planes as described in Theorem 3 and the last Section. We begin with a more general remark about globe covering (q,q,l)–dessins. The genus 0 quotient $\mathcal{D}/Z_l$ with its q cells, q edges and two vertices, both of valency q, belongs to a unique Fuchsian subgroup of the triangle group Δ of signature $\langle q,q,l\rangle$, its commutator subgroup Ψ of signature $<0;l^{(q)}>$, i.e. of genus 0 and with q inequivalent elliptic fixed points of order l such that

$$\Gamma \lhd \Psi \quad \text{with} \quad \Psi/\Gamma \cong Z_l\,, \tag{7}$$

$$\Psi \lhd \Delta \quad \text{with} \quad \Delta/\Psi \cong Z_q\,, \tag{8}$$

if as before $\mathcal{D}$ corresponds to the Fuchsian group Γ. In the cases studied in Theorem 3 and the last Section, i.e. for uniform dessins, Γ is the universal (torsion–free) covering group of the curve whose equation we want to determine, but with the exception of the cases studied in Theorem 1 we cannot suppose that Γ is normal in Δ.

Lemma 6 *Suppose $q>2$ and $-2+q(1-\frac{1}{l})>0$, and let Ψ be a Fuchsian group of signature $<0;l^{(q)}>$. Then the number of torsion–free normal subgroups of Ψ with cyclic factor group $\cong Z_l$ is a multiplicative function $f_q(l)$ of l. For p prime and integer exponents $a\geq 1$ we have*

$$f_q(p^a) \;=\; [(p-1)^{q-1}+1]\,p^{aq-2a-q+1}$$

if q is even, and for q odd we have

$$f_q(p^a) \;=\; [(p-1)^{q-1}-1]\,p^{aq-2a-q+1}\,.$$

Proof. In order to obtain a torsion–free normal subgroup of Ψ we have to map the generators $\gamma_1,\dots,\gamma_q$ onto $b_1,\dots,b_q\in(\mathbb{Z}/l\mathbb{Z})^*$ such that $\sum b_i \equiv 0 \bmod l$. By an obvious extension of Lemma 1 to $\Gamma\lhd\Psi$, the number of these congruence solutions is $\varphi(l)f_q(l)$ because two such epimorphisms $\Psi\to Z_l$ have the same kernel if and only if they result from each other by combination with one of the $\varphi(l)$ automorphisms of Z_l where φ denotes the Euler function. The multiplicativity of f_q is therefore a consequence of the Chinese remainder theorem and the multiplicativity of φ.
First, let $l=p$ be prime. Then we count the congruence solutions

$$\begin{aligned}
(p-1)\,f_q(p) \;&=\; \#\{\,(b_1,\dots,b_q)\,|\,b_i\in(\mathbb{Z}/p\mathbb{Z})^*\,,\,\sum b_i\equiv 0 \bmod p\,\} \;= \\
&=\; \#\{\,(b_1,\dots,b_{q-2})\,|\,\sum^{q-2} b_i\equiv 0 \bmod p\,\}\,(p-1) \\
&\qquad +\#\{\,(b_1,\dots,b_{q-2})\,|\,\sum^{q-2} b_i\not\equiv 0 \bmod p\,\}\,(p-2) \;= \\
&=\; \#\{\,(b_1,\dots,b_{q-2})\,|\,b_i\in(\mathbb{Z}/p\mathbb{Z})^*\}\,(p-1)\;-\;(p-1)^{q-2} \\
&\qquad +\#\{\,(b_1,\dots,b_{q-2})\,|\,\sum^{q-2} b_i\equiv 0 \bmod p\,\} \;= \\
&=\; (p-1)^{q-1}\;-\;(p-1)^{q-2}\;+\;(p-1)\,f_{q-2}(p)
\end{aligned}$$

from which the formulae for $l = p$ follow easily by induction over q.
Now, let l be a prime power p^a, $a > 1$. Every solution of

$$\sum_{i=1}^{q} b_i \equiv 0 \bmod p^a , \quad b_i \in (\mathbb{Z}/p^a\mathbb{Z})^*$$

gives by reduction $\bmod\ p$ a solution of $\sum b_i \equiv 0 \bmod p$, and conversely every solution of $\sum b_i \equiv 0 \bmod p$ comes from $p^{(a-1)(q-1)}$ solutions $\bmod\ p^a$ since every $b_i \bmod p$ has p^{a-1} preimages in $(\mathbb{Z}/p^a\mathbb{Z})^*$, and we have a free choice for precisely $q-1$ of these preimages. Therefore Lemma 6 follows from

$$(p-1)\, p^{a-1}\, f_q(p^a) \;=\; p^{aq-a-q+1}\,(p-1)\, f_q(p)\,.$$

For another approach, in particular to the case of $l = p$ prime, see [J], p.500.

Proposition 6 *Let Ψ of signature $< 0; l^{(q)} >$ be the unique normal subgroup of the triangle group Δ of signature $\langle q, q, l\rangle$, $q > 2$, $l > 3$ with factor group Z_q. Let Γ of signature $< (l-1)(q-2)/2; 0 >$ be the torsion–free kernel of the epimorphism $\Psi \to Z_l$ sending the canonical elliptic generators γ_i, $i = 1, \dots, q$, of Ψ onto $b_i \in (\mathbb{Z}/l\mathbb{Z})^*$ with $\sum b_i \equiv 0 \bmod l$ (w.l.o.g. we may normalize these epimorphisms by taking $b_1 = 1$). Let $\overline{b_i}$ be defined by $\overline{b_i} b_i \equiv 1 \bmod l$, and let $\zeta = \exp(2\pi i/q)$ be the multiplier of all γ_i. Then, as an algebraic curve, the quotient surface $\Gamma\backslash\mathcal{H}$ has a (singular, affine) model given by the equation*

$$y^l \;=\; (x-\zeta^0)^{\overline{b_1}} \cdot \ldots \cdot (x-\zeta^{q-1})^{\overline{b_q}}\,.$$

Proof. This curve defines a function field built up by two consecutive cyclic extensions

$$\mathbb{C}(x,y) \;\supset\; \mathbb{C}(x) \;\supset\; \mathbb{C}(x^q)$$

of orders l and q. The function x^q on this curve is a Belyi function whose ramification points lie above $0, 1, \infty$ of orders q, l, q respectively. The condition $\sum b_i \equiv 0 \bmod l$ is necessary and sufficient to ensure that ∞ is unramified under the extension $\mathbb{C}(x,y)/\mathbb{C}(x)$. The choice of the exponents easily follows from a consideration of the local action of the automorphism group Z_l in its fixed points.

Example 1. For the globe covering dessins of Theorem 2, suppose that $k_1, \dots, k_q \in \mathbb{Z}/l\mathbb{Z}$ form the difference set D with $(k_i - k_{i+1}, l) = 1$ for all $i \in \mathbb{Z}/q\mathbb{Z}$. This is true for prime l (Theorem 3); the Propositions 4 and 5 give some evidence that there may exist orderings of D with that property as well for all other $q \neq 5$. Then the graph of the projective plane embeds into

$$y^l \;=\; (x-\zeta^0)^{\overline{k_2-k_1}} \cdot \ldots \cdot (x-\zeta^{q-1})^{\overline{k_1-k_q}}\,.$$

Remark. Cyclic permutations of the difference set in Example 1 give isomorphic dessins and should give therefore isomorphic curves. In Lemma 10 below, we will study these isomorphisms as coming from cyclic shifts of exponents.
Example 2. With $l = q$ and $b_1 = \ldots = b_q = 1$ the Fermat curves

$$y^q \ = \ (x - \zeta^0) \cdot \ \ldots \ \cdot (x - \zeta^{q-1}) \ = \ x^q \ - \ 1$$

fall under Proposition 6 as well.
Remark. Example 2 corresponds to a dessin for which — in the terminology of Proposition 6 — Γ is even normal in Δ. The dessin has therefore the larger automorphism group Z_q^2 inducing additional relations between the exponents (here: equality). Other examples of this type can be found in [StWo], Section 3.
The remaining part of this section is devoted to a determination of the moduli field for the curves treated in Proposition 6. To this aim, define

$$\mathbf{b} \ := \ (b_1, \ldots, b_q) \ = \ (1, b_2, \ldots, b_q)$$

and $X_{\mathbf{b}} := \Gamma \backslash \mathcal{H}$ to be the curve with the affine equation arising in Proposition 6, i.e. with $b_i \in (\mathbb{Z}/l\mathbb{Z})^*$ for all i and $1 + \sum_{i=2}^{q} b_i \equiv 0 \bmod l$. Clearly, the field of definition of $X_{\mathbf{b}}$ can be chosen as a subfield of the cyclotomic field $\mathbb{Q}(\zeta)$, hence also the field of moduli (recall that by the definition given in Section 2 between Lemma 2 and Lemma 3, the field of moduli is contained in any field of definition). We can give a slightly better result:

Lemma 7 *The curve $X_{\mathbf{b}}$ can be defined over $K = \mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(\cos 2\pi/q)$, and K contains the moduli field of $X_{\mathbf{b}}$.*

A direct *proof* is provided by a substitution $x = \mu(z)$ in the defining equation of $X_{\mathbf{b}}$ where μ denotes a fractional linear transformation defined over $\mathbb{Q}(\zeta)$ sending $\mathbb{R} \cup \{\infty\}$ onto the unit circle. Another way to prove the statement about the field of moduli relies on the fact that the complex conjugation on $X_{\mathbf{b}}$ corresponds on the one hand to the transformation

$$a \ : \ \mathbf{b} \ = \ (1, b_2, \ldots, b_q) \ \mapsto \ (1, b_q, \ldots, b_2) \ .$$

On the other hand, the same transformation of exponents corresponds to the isomorphism of curves given by

$$x \ \mapsto \ \frac{1}{x} \, , \quad y \ \mapsto \ \frac{y}{x} \ .$$

We know by Lemma 1 that there is a bijection between the normalized q–tuples $\mathbf{b}$ introduced above and the torsion–free normal subgroups N in this unique subgroup Ψ of $\Delta = \langle q, q, l \rangle$ with quotient $\Psi/N \cong Z_q$. The absolute Galois group does only permute the different curves $X_{\mathbf{b}}$. To determine their fields of moduli, one has therefore to determine the isomorphisms between these different $X_{\mathbf{b}}$, and by Lemma 2 we know that we have to determine all conjugacies between the different groups N in maximal triangle groups $\overline{\Delta}$.

Lemma 8 *Suppose* $q > 2$, $l > 3$, $q \neq l, 2l, 4l$ *and suppose that* $\langle q, q, l\rangle = \Delta$ *is a non–arithmetic triangle group. Then* $\overline{\Delta} = \langle 2, q, 2l\rangle$ *is the unique maximal triangle group containing* N, Ψ, Δ.

The uniqueness is a consequence of Margulis' characterization of non–arithmetic Fuchsian groups that the commensurator of N, Ψ, Δ is only a finite index supergroup of them. By work of Singerman [Si1], these supergroups are well known, and our hypotheses about q and l guarantee that $\langle 2, q, 2l\rangle$ is in fact *the* maximal triangle group to be considered here.
Remark. The Fermat curves give examples in which $\langle 2, q, 2q\rangle$ are not maximal — and for which the following determination of the moduli field needs an extra effort which is useless since we know that $K = \mathbb{Q}$. For the dessins arising from the embeddings of cyclic projective planes we have $l = q^2 - q + 1 > q$. The hypotheses of the Lemma are therefore violated only if Δ is an arithmetical triangle group. A look into Takeuchi's classification [Ta] shows that this is the case only for $\langle 3, 3, 7\rangle$. Since we already know that in this case $X_{\mathbf{b}}$ is isomorphic to Klein's quartic defined over $K = \mathbb{Q}$, we can concentrate on the cases satisfying the hypotheses of Lemma 8.
We continue with four rather obvious observations.

Lemma 9 *Under the hypotheses of Proposition 6,* Ψ *is a normal subgroup of* $\overline{\Delta} = \langle 2, q, 2l\rangle$*, and to the group inclusions* $\Psi \subset \Delta \subset \overline{\Delta}$ *correspond the normal function field extensions of their quotient spaces* $\mathbb{C}(x) \supset \mathbb{C}(x^q) \supset \mathbb{C}(x^q + x^{-q})$. *The quotient* $\overline{\Delta}/\Psi$ *is isomorphic to the dihedral group* $Z_q \rtimes Z_2$ *and acts as Galois group on the function field extension* $\mathbb{C}(x)/\mathbb{C}(x^q + x^{-q})$ *of degree* $2q$ *generated by*

$$a \,:\, x \mapsto \frac{1}{x} \quad , \quad b \,:\, x \mapsto \zeta x \,.$$

Lemma 10 *This group* $Z_q \rtimes Z_2$ *acts on the set of quotient curves* $X_{\mathbf{b}} \cong N\backslash\mathcal{H}$ *by*

$$a(\mathbf{b}) \;=\; a((1, b_2, \dots , b_q)) \;=\; (1, b_q, b_{q-1}, \dots , b_2)\,,$$

$$b(\mathbf{b}) \;=\; b((1, b_2, \dots , b_q)) \;=\; (1, b_3 b_2^{-1}, \dots , b_q b_2^{-1}, b_2^{-1})\,.$$

If the hypotheses of Lemma 8 are satisfied, the orbits under this group action form precisely the isomorphism classes among the curves $X_{\mathbf{b}}$.

Lemma 11 *For* $i \in \mathbb{Z}/q\mathbb{Z}$ *denote* $b^i(\mathbf{b}) =: (1, b'_2, \dots , b'_q)$. *There is a* $k \equiv 1 - i \bmod q$ *such that the cyclic sequences of quotients*

$$1\,,\, b_2\,,\, \dots\,,\, b_{q-1}\,,\, b_q \quad \textit{and} \quad 1\,,\, b'_{k+1}/b'_k\,,\, b'_{k+2}/b'_k\,,\, \dots\,,\, b'_{k-1}/b'_k$$

coincide. The action of a *reverses the order of these sequences, i.e. replaces* b'_{k+m} *by* b'_{k-m}.

Lemma 12 *The action of the absolute Galois group* $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ *on the set of curves* $X_{\mathbf{b}}$ *factorizes through* $G = \mathrm{Gal}\,\mathbb{Q}(\zeta)/\mathbb{Q}$ *. If we identify* G *in the usual way with the group of prime residue classes* $Z_q^* := (\mathbb{Z}/q\mathbb{Z})^*$ *, every* $r \in Z_q^*$ *acts on the set of* q*–tuples* $\mathbf{b}$ *by*

$$r \;:\; (1, b_2, \ldots, b_q) \;\mapsto\; (1, b_{r^{-1}+1}, b_{2r^{-1}+1}, \ldots, b_{(q-1)r^{-1}+1}) \,.$$

In particular, the action of $r = -1$ *coincides with the action of* a *.*

The last sentence again shows that the moduli field of every $X_{\mathbf{b}}$ is a real subfield of $\mathbb{Q}(\zeta)$. If $X_{\mathbf{b}}$ and $X_{\mathbf{b}'}$ are isomorphic curves, then their r–images are isomorphic, too, for all $r \in Z_q^*$. We obtain therefore

Lemma 13 *Under the hypotheses of Lemma 8 there is a well–defined action of the Galois group* $G = \mathrm{Gal}\,\mathbb{Q}(\zeta)/\mathbb{Q} = Z_q^*$ *on the* $Z_q \rtimes Z_2$*–orbits considered in Lemma 10. With this action of* G *, the moduli field of* $X_{\mathbf{b}}$ *is the fixed field of the stabilizer of* $(Z_q \rtimes Z_2)(\mathbf{b})$ *.*

Example. Let $n = 7$, $q = 8$, $l = 57$ and consider the uniform dessin for the plane $\mathbb{P}^2(\mathbb{F}_7)$ belonging to the cyclic ordered difference set

$$D \;=\; (0, 1, 3, 7, 21, -19, -24, -8)$$

satisfying in fact the condition $(k_i - k_{i+1}, l) = 1$, see the last section. Its algebraic curve $X_{\mathbf{b}}$ corresponds to the 8–tuple (of inverse exponents $\bmod 57$)

$$\mathbf{b} \;=\; (1, 2, 4, 14, 17, -5, 16, 8) \,.$$

For $r = 3$ and $r = 5 \in Z_8^* = G$ we obtain

$$3(\mathbf{b}) \;=\; (1, 14, 16, 2, 17, 8, 4, -5) \quad \text{and} \quad 5(\mathbf{b}) \;=\; (1, -5, 4, 8, 17, 2, 16, 14) \,.$$

Both do not belong to the $(Z_8 \rtimes Z_2)$–orbit of $\mathbf{b}$ what can easily be seen using Lemma 11: the cyclic sequence of the b_i contains the subsequent members $1, 2, 4$ which do not occur in any sequence of quotients 1 , $b'_{k\pm1}/b'_k$, $b'_{k\pm2}/b'_k$ for $3(\mathbf{b})$ and $5(\mathbf{b})$. Therefore, the field of moduli and the field of definition of $X_{\mathbf{b}}$ is in fact the fixed field $K = \cos 2\pi/8$ of the subgroup $\{1, -1\} \subset G$. Another interesting fact becomes visible in this example: Being the dessin of a projective plane is not a Galois invariant property because e.g. $5(\mathbf{b})$ does not consist of the successive differences of a difference set. By consequence, the existence or non–existence of quadrangle loops (see Prop. 10, next section) in a dessin is neither a Galois invariant.

5 Regular Wada dessins

We start with some more general remarks on the Wada property. Clearly, unicellular dessins are Wada dessins, and starting with unicellular dessins in

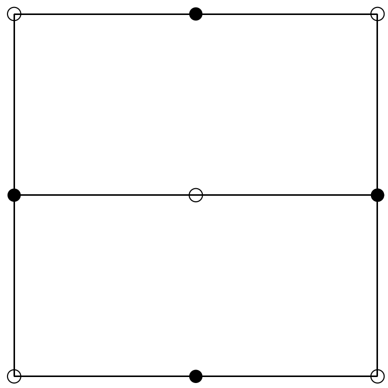

Figure 5: Non–uniform Wada dessin on a torus

positive genera, it is easy to construct Wada dessins by suitable subdivisions of the cell as in the following more general genus 1 example (Figure 5) in which the opposite borderlines have to be identified.

This $(4,4,3)$–dessin is not uniform since there are vertices of both colors with different valencies. The reason is the fact that on the border of each cell there are different vertices which have to be identified on the Riemann surface. In other words, one may draw a curve joining this vertex to itself in the cell but not null–homotopic in the (closed) cell. This turns out to be the only obstruction for Wada dessins with more than one cell to be uniform.

Definition. We call a dessin FLAT if the topological closure of all cells are simply connected.

PROPOSITION 7 *Let $\mathcal{D}$ be a flat Wada dessin with $q > 1$ cells. Then $\mathcal{D}$ is a uniform (q, q, l)–dessin where l denotes the number of black resp. white vertices.*

Proof. By definition, every vertex of $\mathcal{D}$ lies on the border of every cell, so the valencies of the vertices have to be at least q. On the other hand, no such valency can be $> q$: Otherwise there would exist a cell S having a vertex x twice on its border, more precisely one could join x with itself by a non–nullhomotopic curve in the cell, but — by hypothesis — null–homotopic in $\overline{S}$; therefore another vertex $y \neq x$ exists in the interior of this curve, lying on the border of (only) the cell S, hence $q = 1$, contradiction. By the same reason, every cell has precisely the valency $2l$.

Remark and Example. By Theorem 2, we know that the resulting dessin of the embedding of a cyclic projective plane's graph depends on the chosen orderings of the difference set. This is also true for the Wada property and for flatness: For $\mathbb{P}^2(\mathbb{F}_3)$ one has the difference set

$$D := \{0, 1, 3, 9\} \subset Z_{13} .$$

If we take the corresponding globe covering dessin, i.e. with $m_i = k_i$, we obtain a uniform flat $(4,4,13)$–dessin as in the proof of Theorem 3. If we change the cyclic orders of D into

$$(m_i)_{i=1,\dots,4} = (0,1,3,9) \quad \text{but} \quad (k_i)_{i=1,\dots,4} = (9,3,1,0)$$

we obtain a non–flat uniform $(4,4,26)$–Wada dessin with two cells. With the cyclic orders

$$(m_i)_{i=1,\dots,4} = (0,1,3,9) \quad \text{and} \quad (k_i)_{i=1,\dots,4} = (0,3,9,1)$$

we obtain a Wada dessin with two cells, one of valency $2 \cdot 13$ and the other of valency $2 \cdot 39$. In both examples the quotient by the Singer group Z_{13} is a dessin with one black vertex and one white vertex and $q = 4$ edges, but not with q cells in genus 0 (as for the globe covering dessins treated in Sections 3 and 4) but with two cells in genus 1.

In Section 2, we already met some special regular Wada dessins. Here we will characterize such dessins, give some more examples and explain why their underlying graphs do in general not come from finite projective planes even if the valencies q and l satisfy the necessary relation $l = n^2 + n + 1 = q^2 - q + 1$.

Proposition 8 *Let $\mathcal{D}$ be a regular (q,m,l)–dessin with automorphism group G, generated by elements b_0, b_1, b_∞ of respective orders q, m, l and generating cyclic subgroups B, W and C, respectively. Then $\mathcal{D}$ is a Wada dessin if and only if*

$$(G:B) = (C:C\cap B) \quad \textit{and} \quad (G:W) = (C:C\cap W)\,.$$

In that case, the number of cells of $\mathcal{D}$ is

$$(G:C) = (B:C\cap B) = (W:C\cap W)\,.$$

$\mathcal{D}$ is a flat Wada dessin if and only if moreover

$$C\cap B = C\cap W = \{1\}\,,$$

in other words if $\mathcal{D}$ has l black and l white vertices and $q = m$ cells.

Proof. There are a black vertex x fixed by B and a white vertex y fixed by W, both on the border of a cell fixed by C. Since $\mathcal{D}$ is a regular dessin, the automorphism group G acts transitively on all black (resp. white) vertices, and since B (resp. W) is the stabilizer subgroup of x (resp.y), the total number of black (resp. white) vertices is $(G:B)$ resp. $(G:W)$. Now, $\mathcal{D}$ is a Wada dessin if and only if all these black (resp. white) vertices form one orbit under the action of C. According to the class formula, this is the case if and only if

$$(G:B) = (C:C\cap B) \quad \text{and} \quad (G:W) = (C:C\cap W)\,.$$

The number of cells is deduced in a similar way by the action of G, B and W on the cells. Moreover, $\mathcal{D}$ is flat if and only if all the black (resp. white) vertices on the border of the cell fixed by C are pairwise different, i.e. if and only if l is the number of black (resp. white) vertices.
As a non–flat example, take the genus 3 curve with the affine model

$$y^2 \;=\; x^7 - x \,,$$

with $(4,4,6)$–dessin and an automorphism group G of order 12 (a semidirect product of a cyclic group of order 4 with a normal subgroup of order 3). Here we have two cells of valency 12 but only 3 different black (resp. white) vertices. It is not surprising that in the case of flat regular Wada dessins the structure of G can be determined rather precisely.

Proposition 9 *Let $\mathcal{D}$ be a regular (q,q,l)–Wada dessin with q cells and l black (resp. white) vertices. Then*

1. *$G = \mathrm{Aut}\,\mathcal{D}$ has order ql ,*
2. *$G = BC = WC$ for the cyclic stabilizer subgroups B, W of a black and a white neighbor vertex and the cyclic stabilizer subgroup C of a cell,*
3. *$G'' = \{1\}$, i.e. G is metabelian.*
4. *If q is prime and $l > 1$, one has even $l \geq q$.*
5. *In the case $l = q$ prime, the dessin belongs to a Fermat curve of exponent q and with $G \cong Z_q^2$.*
6. *If l is prime $> q$ (arbitrary), q divides $l-1$ and $G \cong Z_l \rtimes Z_q$.*

Proof. 1) Clearly, $\mathcal{D}$ has ql edges. Since G acts sharply transitive, the number of edges is the order of G . A similar argument proves assertion 2). As we learned from Gareth Jones, 3) follows from 2) by a theorem of Itô [I]. 4) Because G is generated by two cyclic subgroups B and W of order q , they coincide if and only if $l = 1$. If not and q is prime, they satisfy moreover $B \cap W = \{1\}$, $\mathrm{ord}\, G \geq q^2$ and hence $l \geq q$. 5),6) Since G contains a cyclic subgroup of order l , the statements about the structure of G are standard consequences of Sylow's theorems. It is well known that regular (q,q,q)–dessins with automorphism group Z_q^2 belong to Fermat curves, see e.g. [JS],7. Examples 3. On the other hand: that these dessins are flat Wada dessins can easily be verified using Proposition 8.

Remark. If q is not prime, the statement 4) in general fails as the following example shows. On the elliptic curve $y^2 = x^4 - 1$ there is a regular $(4,4,2)$–dessin with 8 edges, $q = 4$ cells, $l = 2$ black resp. white points, automorphism group $G \cong Z_4 \times Z_2$ and disjoint generating subgroups $B \cong W \cong Z_4$, $C \cong Z_2$ (complete the Figure 5 dessin by two edges forming a vertical middle axis).

For the structure of G in these more general cases one may consult a paper of Huppert [Hu]. Theorem 2 of [I] gives the existence of normal subgroups $N \lhd G$ containing B, W or C and other normal subgroups contained in these cyclic subgroups, so it is possible to represent $\mathcal{D}$ by successive cyclic coverings of very simple genus 0 dessins.
In [StWo] we studied a series of regular (q, q, l)–dessins with q, l prime, $q | l - 1$ and automorphism group $G \cong Z_l \rtimes Z_q$ giving examples for Proposition 9.6). For the purpose of the present paper, the hypothesis "q prime" is unnecessary, but we make the assumptions

$$q > 2 , \quad l = q^2 - q + 1 \quad \text{prime} , \quad G \cong Z_l \rtimes Z_q$$

where Z_l is generated by a and Z_q by b satisfying the relation

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

for some fixed prime residue class $u \in (\mathbb{Z}/l\mathbb{Z})^*$ of order q. Imitating the proof of Proposition 3, we generate the automorphism group of the dessin by a rotation b around a black vertex x and a rotation $b^{-1}a$ around a white vertex neighbor y. That all these dessins are flat Wada dessins follows again easily from Proposition 8.

Proposition 10 *Let $\mathcal{D}$ be a (q, q, m)–dessin with $l = q^2 - q + 1$ points, all vertices with valency $q > 2$. The underlying graph is the graph of a projective plane if and only if no quadrangle loop exists in $\mathcal{D}$, i.e. if there are no white vertices $y \neq y^*$, black vertices $x \neq x^*$ such that xyx^*y^*x are successive neighbors.*

Proof. If such a quadrangle loop exists, the uniqueness of the intersection points or joining lines is violated, whence we cannot have the graph of a projective plane. If no such quadrangle exists, counting neighbor vertices one easily shows that any two black vertices have a unique white neighbor in common, and that the respective statement is true for two white vertices. The existence of four points in general position follows easily from $q > 2$.
With Proposition 10 we can now see why e.g. the regular $(7, 7, 43)$–dessin with automorphism group $Z_{43} \rtimes Z_7$ has no underlying graph belonging to a projective plane:

Proposition 11 *Let $\mathcal{D}$ be a regular (q, q, l)–dessin with $l = q^2 - q + 1$ prime and automorphism group $G \cong Z_l \rtimes Z_q$ whose generators a, b of respective orders l, q satisfy*

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

$u \in (\mathbb{Z}/l\mathbb{Z})^*$ of order q. The underlying graph is a graph of a projective plane of order $n = q - 1$ if and only if the powers u^k, $k = 1, \ldots , q$, form a difference set in $\mathbb{Z}/l\mathbb{Z}$.

Proof. Because the dessin is regular, we can start with any black vertex x and a white neighbor y, hence we will take the fixed points of b and $b^{-1}a$. Suppose there is a quadrangle loop as forbidden by Proposition 9, then

$$x^* = (b^{-1}a)^k(x) , \quad y^* = b^m(y)$$

with $k, m \not\equiv 0 \bmod q$, and the subgroups fixing these two points are generated by

$$(b^{-1}a)^k \, b \, (b^{-1}a)^{-k} \quad \text{and} \quad b^m (b^{-1}a) b^{-m}$$

respectively. An edge joining x^* with y^* exists if and only if it is the G–image of the edge joining y and x by a group element which can be written in two ways:

$$(b^m (b^{-1}a) b^{-m})^s \, b^m = ((b^{-1}a)^k \, b \, (b^{-1}a)^{-k})^r \, (b^{-1}a)^k$$

with $r, s \not\equiv 0 \bmod q$. This equation is equivalent to

$$(b^{-1}a)^s = b^{-m} \, (b^{-1}a)^k \, b^r$$

or, using the relation between a and b,

$$a^{u+u^2+\ldots+u^s} \, b^{-s} = b^{-m} \, a^{u+u^2+\ldots+u^k} \, b^{-k+r} = a^{u^m(u+u^2+\ldots+u^k)} \, b^{-m-k+r} .$$

This relation holds if and only if

$$s + r \equiv m + k \bmod q \quad \text{and} \quad u + \ldots + u^s \equiv u^m(u + \ldots + u^k) \bmod l .$$

The second congruence is easily seen to be equivalent to

$$u^s - 1 \equiv u^{m+k} - u^m$$

meaning that the powers of u do not form a difference set in $\mathbb{Z}/l\mathbb{Z}$. On the other hand, if the powers of u form a difference set, the last congruence is unsolvable for $s, m, k \not\equiv 0 \bmod q$, whence a quadrangle loop cannot exist.

6 THE CARTOGRAPHIC GROUP

We prove the last theorem in the following more general form.

PROPOSITION 12 *Let $\mathcal{D}$ be a globe covering dessin obtained by embedding the graph of a cyclic projective plane $\mathbb{P}$ of order $n = q - 1$ with Singer group $Z_l \subseteq \mathrm{Aut}\,\mathcal{D}$. Then the cartographic group M of $\mathcal{D}$ is isomorphic to a semidirect product $A \rtimes Z_q$ for a quotient A of Z_l^n.*

As explained in the beginning of Section 4, the hypothesis *globe covering* says that $\mathcal{D}$ corresponds to a subgroup Γ of the triangle group $\Delta = \langle q, q, l \rangle$ with an intermediate normal subgroup $\Psi = \Delta'$ of signature $< 0; l^{(q)} >$ such that (7) and (8) hold. In contrast to Section 4, we can even admit the existence of torsion elements in Γ, in other words $\mathcal{D}$ is allowed to be a non–uniform dessin. The cartographic group of $\mathcal{D}$ can be introduced either as monodromy group of the corresponding Belyi function β or as a certain permutation group of the edges of $\mathcal{D}$ since these represent the sheets of the covering β. Here, the easiest way to determine M is the fact that M is isomorphic to the quotient Δ/N of Δ by its maximal normal subgroup N contained in Γ. Let Ψ' the commutator subgroup of Ψ. Since Ψ is normal in Δ, the same holds for Ψ'. The presentation of Ψ shows that

$$\Psi' \subseteq \Gamma \quad \text{with} \quad \Psi/\Psi' \cong Z_l^{q-1} .$$

Therefore, $\Psi' \subseteq N \subseteq \Gamma$, and if we denote the quotient Ψ/N by A, the result follows.

Remark. As in Section 4, the choice of the ordered difference set for $\mathbb{P}$ determines the homomorphism $\Psi \to Z_l$ with kernel Γ, and the action of Δ resp. Z_q on Z_l^{q-1} is also known. Using these data, it is in principle possible to determine A and the action of Z_q on A.

The same line of arguments as in the proof above gives a more general version of Theorem 4. Since the full automorphism group of $\mathcal{D}$ is isomorphic to $N_\Delta(\Gamma)/\Gamma$ where $N_\Delta(\Gamma)$ denotes the normalizer in Δ (containing Ψ, of course), we obtain

Proposition 13 *Under the hypotheses of Proposition 12 we have*

$$\operatorname{Aut}\mathcal{D} \cong Z_l \rtimes Z_m$$

for some divisor m of q.

References

[Ch] http://stripe.colorado.edu/˜sawyer/chaos.html

[FiWh] J. B. Fink, A. T. White: Regular imbeddings of finite projective planes, pp. 1233–1241 in Y. Alavi, A. Schwenk (eds.): Proceedings of the Seventh International Conference on Graph Theory, Combinatorics, Algorithms, and Applications, Wiley 1995

[HML] D. G. Higman, J. E. McLaughlin: Geometric ABA–groups, *Ill. J. Math.* 5 (1961), 382–397

[Hu] B. Huppert: Über das Produkt von paarweise vertauschbaren zyklischen Gruppen, *Math. Zeitschr.* 58 (1953), 243–264

[I] N. Itô: Über das Produkt von zwei abelschen Gruppen, *Math. Zeitschr.* 63 (1955), 400–401

[J] G. Jones: Enumeration of Homomorphisms and Surface Coverings, *Quart. J. Math. Oxford*, Ser. (2) 46 (1995), 485–507

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

[Ke] B. v. Kerékjártó: Vorlesungen über Topologie I. Flächentopologie. Springer 1923

[Li] J. H. Lindsay jr.: An elementary treatment of the imbedding of a graph in a surface, *Amer. Math. Monthly* 66 (1959), 117–118

[Si1] D. Singerman: Finitely Maximal Fuchsian Groups, *J. London Math. Soc.* (2) 6 (1972) 29–38.

[Si2] D. Singerman: Klein's Riemann Surface of Genus 3 and Regular Imbeddings of Finite Projective Planes, *Bull. London Math. Soc.* 18 (1986) 364–370

[St] M. Streit: Field of Definition and Galois Orbits for the Macbeath–Hurwitz Curves, Arch. Math. (2000) 342–349

[StWo] M. Streit, J. Wolfart: Characters and Galois invariants of regular dessins, *Revista Mat. Complutense* 13 (2000), 49–81

[Ta] K. Takeuchi: Arithmetic triangle groups, *J. Math. Soc. Japan* 29 (1977) 91–106.

[Wh] A. T. White: Efficient Imbeddings of Finite Projective Planes, *Proc. London Math. Soc.* (3) 70 (1995), 33–55

[Wo1] J. Wolfart: The 'Obvious' Part of Belyi'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: Kinderzeichnungen und Uniformisierungstheorie, http://www.math.uni–frankfurt.de/˜steuding/wolfart.shtml

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

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