Automorphism Groups of Wada Dessins and Wilson Operations

Dissertation
zur Erlangung des Doktorgrades
der Naturwissenschaften

vorgelegt beim Fachbereich Informatik und Mathematik
der Johann Wolfgang Goethe-Universität
in Frankfurt am Main

von
Cristina Sarti
aus Ferrara (Italien)

Frankfurt 2010
(D30)

vom Fachbereich *Informatik und Mathematik* der
Johann Wolfgang Goethe–Universität als Dissertation angenommen.

Dekan: *Prof. Dr. -Ing. Detlef Krömker*

Gutachter: *Prof. Dr. Jürgen Wolfart, Prof. Dr. Gareth Jones*

Datum der Disputation:

Contents

Introduction **iii**

1 Difference Sets and Block Designs **1**

1.1 Difference Sets 1

1.1.1 Multipliers 3

1.2 Block Designs 5

1.2.1 Incidence Matrices 7

1.2.2 Multipliers and Block Designs 9

2 Finite Projective Spaces **11**

2.1 Finite Projective Spaces 11

2.2 Groups of Automorphisms 13

2.3 Finite Projective Spaces $\mathbb{P}^m(\mathbb{F}_n)$ as Block Designs 15

2.3.1 Constructing the associated Block Designs 16

2.3.2 Multipliers as Automorphisms of Projective Spaces 18

3 Difference Sets and the Frobenius Automorphism **21**

3.1 The Frobenius Automorphism 21

3.2 Frobenius Difference Sets 22

3.3 Frobenius Difference Sets and Point Numberings 31

4 Finite Projective Spaces and Dessins d'Enfants **37**

4.1 Introducing Dessins d'Enfants 37

4.2 Dessins d'Enfants associated with Projective Spaces 39

4.3 Wada Dessins 43

5 Automorphism Groups **47**

5.1 The Singer Group 47

5.2 The Frobenius Automorphism 49

5.3 The Full Automorphism Group 58

5.4 Generalizations 60

5.4.1 Special Cases 65

6 Wilson Operations **69**

6.1 Wilson Operations and 'mock' Wilson Operations 70

6.2 Wilson Operations on Wada Dessins 72

6.2.1 Constructing Uniform $< q, q, q >$-Dessins 79

6.3 'Mock' Wilson Operations on Wada Dessins 83

6.3.1 The Action of 'Mock' Wilson Operators $H_{k,k}$ 83

6.3.2 Constructing Regular Dessins 86

6.3.3 Defining Equations 96

6.3.4 Coverings 102

Outlook **109**

Zusammenfassung **117**

Bibliography **126**

Introduction

Dessins d'enfants (children's drawings) may be defined as hypermaps, i.e. as bipartite graphs embedded in Riemann surfaces (see [Wal75]). They are very important objects in order to describe the surface of the embedding as an algebraic curve. Knowing the combinatorial properties of the dessin may, in fact, help us determining defining equations or the field of definition of the surface. This task is easier if the automorphism group of the dessin is 'large'.
The theorem of Belyĭ (see [Bel80]) is fundamental in expressing the relation between dessins and surface of the embedding:

Theorem. *(**Belyĭ theorem** [LZ04]) A Riemann surface X admits a model over the field $\overline{\mathbb{Q}}$ of algebraic numbers if and only if there exists a covering $f : X \to \overline{\mathbb{C}}$ unramified outside $\{0, 1, \infty\}$. In such a case, the meromorphic function f can also be chosen in such a way that it will be defined over $\overline{\mathbb{Q}}$.*

The dessin is related to the covering in such a way that we may choose the vertices and the cell mid points of the underlying graph as preimages of the critical values $\{0, 1, \infty\}$. Thus the dessin is uniquely determined by the **Belyĭ pair** (X, f) and vice versa it uniquely determines it up to isomorphism. Nevertheless, if we do not consider a special function f on X, we should not expect X to be the surface of the embedding of a unique dessin. In fact, on a Riemann surface many different dessins may be embedded.
There are a lot of beautiful examples of dessins (see [LZ04], [Wol06]). In this thesis we consider a particular type of dessins called **Wada dessins**. Among them we, especially, consider those dessins with a 'large' automorphism group. The motivation for their study has come from an early work of Streit and Wolfart [SW01]: here these special dessins are defined and constructed starting from projective planes $\mathbb{P}^2(\mathbb{F}_n)$. Wada dessins illustrate the incidence structure of the points and of the lines belonging to the planes. In our work we show that the results of Streit and Wolfart may be extended to projective spaces $\mathbb{P}^m(\mathbb{F}_n)$. In particular, we show some important and new facts concerning the construction of Wada dessins with a 'large' automorphism

group. We show moreover that applying algebraic operations, so-called **Wilson operations**, on the constructed Wada dessins we may obtain new ones determining surfaces with special algebraic and topological properties.

The thesis is organised in the following way. In the first two chapters, Chapter 1 and 2 we explain some important and known facts about projective spaces and block designs. Projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ of dimension m over a finite field $\mathbb{F}_n$ may, in fact, be considered as block designs. Here the points of the associated space are the objects and the hyperplanes, i.e. the subspaces of dimension $m-1$, are the blocks. The objects (points) on a block (hyperplane) may be numbered using special kinds of sets, so-called **difference sets**. Special integers multiplying these sets describe the action of groups of automorphisms of the space on points and hyperplanes.

In Chapter 3 we consider the action of the cyclic group Φ_f generated by the **Frobenius automorphism**. This automorphism acts on a space $\mathbb{P}^m(\mathbb{F}_n)$ permuting the points lying on a hyperplane and vice versa it permutes the hyperplanes incident with a point. We show that the action of the group Φ_f may determine the choice of the difference set we use to number the points and the hyperplanes. For difference sets of special type fixed under the action of Φ_f the block design associated has Φ_f as a group of automorphisms. We call difference sets of this special type **Frobenius difference sets**.

In Chapter 4 we introduce the concept of **dessin d'enfant**. Extending some ideas of Streit and Wolfart [SW01] we construct dessins d'enfants associated with projective spaces $\mathbb{P}^m(\mathbb{F}_n)$. They are bipartite graphs embedded in Riemann surfaces. The incidence pattern of their white and black vertices illustrates the incidence structure of points and hyperplanes. In particular we explain how to construct **Wada dessins**.

In Chapter 5 we present new results regarding groups of automorphisms acting on Wada dessins. We show that a cyclic **Singer group** Σ_ℓ is always a group of automorphisms of these dessins. On the contrary, the cyclic group Φ_f and its subgroups are groups of automorphims only in special cases. We show that the choice of a Frobenius difference set is a necessary, but still not a sufficient condition. We analyse the very 'nice' case of projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ with $m+1$ prime and $n \not\equiv 0,1 \mod (m+1)$ and we show under which conditions dessins associated with them have Φ_f as a group of automorphisms (see [Sar10]). We show moreover that if this is the case the full automorphism group is the semidirect product $\Phi_f \ltimes \Sigma_\ell$. For the more general case of projective spaces with arbitrary parameters m and n we show that the full automorphism group may only be a subgroup of the semidirect product $\Phi_f \ltimes \Sigma_\ell$.

In Chapter 6 we present new results obtained applying to Wada dessins algebraic operations called **Wilson operations**. We show how we may construct new dessins starting from a given Wada dessin. In particular, we consider those dessins constructed with a special type of Wilson operations we call **'mock' Wilson operations**. We show how we may construct them, how we may determine algebraic models for the surface of the embedding and how this surface is topologically related to the surface of the embedding of the starting dessins.

Acknowledgments

At this point I really want to thank my supervisor Prof. Jürgen Wolfart for introducing me to the beautiful topic of dessins d'enfants. I am grateful to him for many productive discussions, for his support and for communicating to me his enthusiasm for mathematics. I want to thank Prof. Gareth Jones for accepting to be my second supervisor and for useful hints and discussions.
Many thanks also to Frank Feierabend, Benny Mühlbauer and to Manfred Streit for their readiness to talk about the one or the other mathematical topic. To Jörg Lehnert I am thankful for carefully reading this work. Last but not least, many thanks to my syster, Alessandra, to my husband and to my parents for their constant support during the work at this thesis.

Chapter 1

Difference Sets and Block Designs

Projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ can be regarded as arrangements of v points and v hyperplanes of dimension $m-1$, such that each point is incident with k hyperplanes and k points lie on every hyperplane. In terms of these parameters they can be described as **cyclic symmetric block designs** with associated **(v, k, λ)-difference set**.
In this chapter we introduce the notions of difference set and of block design. We explain some general facts related to them. In particular, we go deeper into the theory of multipliers of difference sets, since they play an important role as automorphisms of the associated block design.

1.1 Difference Sets

Difference sets can be defined as follows:

Definition 1.1.1 ([Bau71])**.** A (v, k, λ)-difference set $D = \{d_1, \ldots, d_k\}$ is a collection of k residues modulo v, such that for any residue $\alpha \not\equiv 0 \mod v$ the congruence

$$d_i - d_j \equiv \alpha \mod v \tag{1.1}$$

has exactly λ solution pairs (d_i, d_j) with d_i and d_j in D.

The parameters k, v and λ are related in the following way:

$$k(k-1) = \lambda(v-1). \tag{1.2}$$

In fact from the k elements we choose pairs (d_i, d_j), $i \neq j$ to build differences $d_i - d_j$. This is what is called in combinatorics a permutation without repetition and we can build:

$$\frac{k!}{(k-2)!} = k(k-1)$$

differences. Since we know that each residue $\alpha \mod v$ is represented by λ of these differences we obtain relation (1.1) as:

$$\frac{k(k-1)}{\lambda} = v - 1 \ .$$

Example 1. Difference sets are:

1. $D_1 = \{1, 2, 4\} \mod 7$, with parameters $v = 7$, $k = 3$, $\lambda = 1$;
2. $D_2 = \{0, 1, 3, 9\} \mod 13$, with parameters $v = 13$, $k = 4$, $\lambda = 1$;
3. $D_3 = \{1, 2, 3, 5, 6, 9, 14, 15, 18, 20, 25, 27, 35\} \mod 40$, with parameters $v = 40$, $k = 13$, $\lambda = 4$.

If 0 and 1 belong to D we speak of a **reduced difference set** ([Sin38]). In the example above D_2 is a reduced difference set.
Given integers $s \mod v$ and $t \mod v$ such that t and v are coprime, the following properties hold for a difference set D:

1. The set $D + s \equiv \{d_0 + s, \ldots, d_{k-1} + s\} \mod v$ is also a difference set. It is called a **shift** of D.
2. The set $tD \equiv \{td_0, \ldots, td_{k-1}\} \mod v$ is also a difference set.
3. If D_i and D_j are two difference sets with the same parameters v, k, λ and if $D_i \equiv tD_j + s \mod v$ for integers s and $t \mod v$, with $(t, v) = 1$, then D_i and D_j are said to be **equivalent difference sets**.

In particular for any set of parameters v, k, λ satisfying Equation (1.2) there may be no difference set, a single difference set or several inequivalent difference sets having these properties (see [Bau71]).
If we introduce an additional parameter $n = k - \lambda$ and for $\lambda = 1$ we choose $v = n^2 + n + 1$, we obtain difference sets of special type called **perfect difference sets**. Perfect difference sets with n a prime power p^e —for $n \neq p^e$ it is even not clear whether a difference set exists— are well studied examples of difference sets

associated with projective spaces (see [Bau71], [Sin38], [Goe05]), as we will see later on (see Chapter 3).
The sets D_1 and D_2 in Example 1 are perfect difference sets associated with the projective planes $\mathbb{P}^2(\mathbb{F}_2)$ (**Fano Plane**) and $\mathbb{P}^2(\mathbb{F}_3)$.

1.1.1 Multipliers

Among the properties of difference sets we saw that if D is a difference set, then tD is also a difference set for any integer $t \mod v$ with $(t, v) = 1$. In particular:

Definition 1.1.2. If t is prime to v and if tD is some shift $D + s$ of the original difference set D, then t is called a **multiplier** of D.

Clearly every $t \equiv 1 \mod v$ is a trivial multiplier of D, but all known (v, k, λ)-difference sets have non-trivial multipliers.
For a survey of the theory of multipliers related with difference sets see for instance [Bau71], [HP85].
Multipliers of special types are the ones which fix difference sets, i.e. multipliers t for which

$$tD \equiv D \mod v.$$

In particular

Proposition 1.1.3. *([Bau71]) Given a difference set D with multiplier t, there exist exactly $(t-1, v) = d$ shifts fixed by the multiplier. In fact if D' is a shift fixed by t, then t also fixes the d shifts $D' + j(\frac{v}{d})$, for $j = 0, 1, \ldots, d-1$.*

Proof. Since $(t-1, v) = d$ we can write t and v as:

$$v = k_1 d\,, \qquad t = k_2 d + 1$$

for some integers $k_1, k_2 \neq 0$.
Suppose $D' + s$ is another shift fixed by t. We obtain:

$$\begin{aligned}
t(D'+s) &\equiv D'+s \mod v \\
tD' + ts &\equiv D'+s \mod v \\
ts &\equiv s \mod v \\
(t-1)s &\equiv 0 \mod v \\
\Rightarrow \qquad k_2 \cdot s &\equiv 0 \mod \tfrac{v}{d}\,.
\end{aligned}$$

Since $gcd(k_2, v) = 1$ we obtain

$$s \equiv 0 \mod \frac{v}{d} .$$

Thus the multiplier t fixes the d shifts

$$D' + j\frac{v}{d} \mod v , \qquad j = 0, \ldots, d-1 .$$

□

Let us now consider multipliers t_1 and t_2 of the same difference set D. We have

Proposition 1.1.4. *([Bau71]) If t_1 and t_2 are multipliers of the same difference set then t_2 permutes the shifts fixed by t_1.*

Proof. Let t_1 and t_2 be multipliers of D and suppose that D is fixed by t_1. Then

$$t_1(t_2 D) = t_2(t_1 D) \equiv t_2 D \mod v.$$

Thus $t_2 D$ is also fixed by t_1. Since $t_2 D$ is by definition (see Definition 1.1.2) a shift $D + s$ of D, this means that t_2 only permutes the shifts fixed by t_1. □

Remark. From Proposition 1.1.4 follows directly that if t_1 fixes only one shift then that shift is fixed by all other multipliers. In fact from

$$t_1 D \equiv D \mod v$$

and

$$t_1(t_2 D) \equiv t_2 D \mod v$$

follows $t_2 D \equiv D \mod v$ for each other multiplier t_2.

If a multiplier fixes some shift D' of a difference set D, it acts on its elements fixing them or permuting them, so we can assume (see [Bau71]) that D' consists of sets $\{a, ta, \ldots, t^{m-1}a\}$ where $t^m a \equiv a \mod v$, $m \in \mathbb{N}\backslash\{0\}$. We call these sets **blocks** or **orbits** fixed by the multiplier t. The number m of distinct elements of each block is always a divisor of the order of t and it is equal to it, if $(a, v) = 1$. If v is prime, then all the blocks except $\{0\}$ contain the same number of distinct elements m.

Example 2. 1. Let us consider the difference set $D = \{1, 6, 7, 9, 19, 38, 42, 49\}$ ([Bau71]) with parameters $v = 57$, $k = 8$, $\lambda = 1$. It is easy to prove that 7 is a multiplier fixing D. The order of 7 is 3 since $7^3 \equiv 1 \mod 57$, so D can be divided in blocks of length 1 or 3 in the following way:

$$\{1, 7, 49\}, \{6, 9, 42\}, \{19\}, \{38\}.$$

The blocks of length 1 are a consequence of the fact that neither 19 nor 38 is prime to 57.

2. The difference set $D = \{1, 2, 3, 4, 6, 8, 12, 15, 16, 17, 23, 24, 27, 29, 30\}$ ([Bau71]) has parameters $v = 31$, $k = 15$, $\lambda = 7$. The residue class of 2 is a multiplier and its order is 5 since $2^5 \equiv 1 \mod 31$. D only consists of blocks of length 5 because $v = 31$ is prime and $0 \notin D$. In fact we obtain the following blocks:

$$\{1, 2, 4, 8, 16\}, \{3, 6, 12, 24, 17\}, \{15, 30, 29, 27, 23\}.$$

1.2 Block Designs

We define a (balanced incomplete) block design as follows:

Definition 1.2.1. ([Hal67]) A **balanced incomplete block design** is an arrangement of v distinct objects into b blocks such that each block contains exactly k distinct objects, each object occurs in exactly r different blocks and every pair of distinct objects occurs together in exactly λ blocks.

The design is said to be incomplete since we do not consider all the possible combinations of v objects taken k at a time but only a part of these, and it is balanced because of the constancy of the occurrences λ of each pair in the blocks (see [Hal67]). The parameters satisfy the relations:

$$bk = vr, \tag{1.3}$$

$$r(k-1) = \lambda(v-1)\ . \tag{1.4}$$

Relation (1.3) follows from counting the number of incidences block-object in two different ways. Since each of the b block contains k objects, we have the first part of relation (1.3). The second part follows from the fact that each object is contained

in r blocks.
Relation (1.4) follows from counting the occurrences of the object pairs using combinatorics: Each of the b blocks contains k elements and we can build $\binom{k}{2}$ pairs of objects. The total number of "pairs in blocks" is then:

$$b\binom{k}{2} = b\frac{k!}{2!(k-2)!} = b\frac{k(k-1)}{2} \ . \tag{1.5}$$

If we consider the v elements we can build $\binom{v}{2}$ pairs. From Definition (1.2.1) we know that each pair occurs in λ blocks so we obtain the following total number of "pairs in blocks":

$$\lambda\binom{v}{2} = \lambda\frac{v!}{2!(v-2)!} = \lambda\frac{v(v-1)}{2} \ . \tag{1.6}$$

Equating Eq. (1.5) and Eq. (1.6) and using Relation (1.3), we get Relation (1.4):

$$\begin{aligned} b\tfrac{k(k-1)}{2} &= \lambda\tfrac{v(v-1)}{2} \\ rv(k-1) &= \lambda v(v-1) \\ r(k-1) &= \lambda(v-1) \ . \end{aligned}$$

If $v = b$, i.e. the number of blocks and of objects is equal, we speak of a **symmetric** block design, for which we also have $r = k$ (see Relation 1.3).
In particular we say that a symmetric block design B is **cyclic** if there exists an automorphism α of B such that the objects and the blocks are permuted in a cycle of length v.
Every (v, k, λ)-difference set gives rise to a cyclic symmetric block design (see [Hal67], [Bau71]) and vice versa, every cyclic symmetric block design can be described using a $(v, k, \lambda)-$ difference set. The objects are $0, \ldots, v-1$, the blocks $B_0 = D, B_1 = D+1, \ldots, B_{v-1} = D+(v-1)$. The automorphism α permutes the objects and the blocks in the following way:

$$\begin{aligned} \alpha : i &\longmapsto i+1, \qquad i = 0, \ldots, v-1 \ , \\ B_i &\longmapsto B_{i+1}. \end{aligned}$$

Example 3. The $(7, 3, 1)$-difference set $D = \{1, 2, 4\}$ describes a block design with blocks:

$$\begin{aligned} B_0 &= D = \{1,2,4\}, \\ B_1 &= D+1 = \{2,3,5\}, \\ B_2 &= D+2 = \{3,4,6\}, \\ B_3 &= D+3 = \{4,5,0\}, \\ B_4 &= D+4 = \{5,6,1\}, \\ B_5 &= D+5 = \{6,0,2\}, \\ B_6 &= D+6 = \{0,1,3\}. \end{aligned}$$

1.2.1 Incidence Matrices

To a block design B is always associated a $v \times b$ matrix $A = (a_{ij})$, $i = 0, \ldots, v-1$, $j = 0, \ldots, b-1$. If we describe with $a_0, \ldots, a_{v-1}$ the objects and with $B_0, \ldots, B_{v-1}$ the blocks of B, we have

$$\begin{aligned} a_{ij} &= 1 \text{ if } a_i \in B_j, \\ a_{ij} &= 0 \text{ if } a_i \notin B_j. \end{aligned}$$

For the example above we have, for instance, the following incidence matrix A:

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix},$$

Of course, if we number the blocks and the objects in a different way, we will obtain a different incidence matrix. In particular, as we can easily see in the example above, if we number the blocks and the objects in the following way:

$$\begin{aligned}
B_0 &= D = \{0,1,3\},\\
B_1 &= D+1 = \{1,2,4\},\\
B_2 &= D+2 = \{2,3,5\},\\
B_3 &= D+3 = \{3,4,6\},\\
B_4 &= D+4 = \{4,5,0\},\\
B_5 &= D+5 = \{5,6,1\},\\
B_6 &= D+6 = \{6,0,2\}\ ,
\end{aligned}$$

the incidence matrices A' and A only differ by a cyclic shift of the columns. Each incidence matrix satisfies the following relations (see [Beu82], [Hal67]):

$$AA^t = \begin{pmatrix} r & \lambda & \dots & \lambda \\ \lambda & \ddots & & \vdots \\ \vdots & & \ddots & \lambda \\ \lambda & \dots & \lambda & r \end{pmatrix} = (r-\lambda)I + \lambda J \tag{1.7}$$

with $I = \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix}_{v\times v}$ and $J = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix}_{v\times v}$,

$$\det(AA^t) = (r-\lambda)^{v-1} rk\ . \tag{1.8}$$

Relation (1.7) follows directly from Definition 1.2.1. In fact, let $AA^t = M = (m_{ij})_{1\le i,j\le v}$. Each element m_{ij} is the product of the ith line of A with the jth column of A^t, i.e. it is the product of the ith and of the jth line of A.
If $i = j$, then $m_{ij} = m_{ii}$ is the number of the ones in a line of A, i.e. according to Definition 1.2.1 it is the number of the blocks incident with the ith object, which is r. If $i \neq j$ then m_{ij} is the number of blocks incident with the ith object, i.e. $m_{ij} = \lambda$ (see [Bau71]).
For the proof of the second relation we use the first one and we write:

$$\det(AA^t) = \det \begin{pmatrix} r & \lambda & \dots & \lambda \\ \lambda & \ddots & & \vdots \\ \vdots & & \ddots & \lambda \\ \lambda & \dots & \lambda & r \end{pmatrix} . \tag{1.9}$$

Now we subtract the first column from all the others and add all the other rows to the first. We obtain:

$$\det(AA^t) = \det \begin{pmatrix} r+(v-1)\lambda & 0 & \dots & 0 \\ \lambda & r-\lambda & 0 & \vdots \\ \vdots & \vdots & \ddots & 0 \\ \lambda & 0 & \dots & r-\lambda \end{pmatrix} . \tag{1.10}$$

The determinant of a lower triangular matrix is the product of the elements on the diagonal, so we obtain:

$$\det(AA^t) = [r + \lambda(v-1)](r-\lambda)^{v-1}. \tag{1.11}$$

Using Relation (1.4) we have:

$$\det(AA^t) = [r + r(k-1)](r-\lambda)^{v-1} = rk(r-\lambda)^{v-1}.$$

If the block design is symmetric then we have $r = k$ and (1.8) simplifies to

$$\det(AA^t) = k^2(k-\lambda)^{v-1}.$$

Thus for a nontrivial symmetric block design the matrix A is always non-singular since $k > \lambda$.

1.2.2 Multipliers and Block Designs

By definition (see Section 1.1.1), the action of a multiplier t on a difference set D corresponds to a shift:

$$tD \equiv D + s \mod v.$$

As difference sets describe cyclic symmetric block designs B the action of t on D corresponds to an automorphism τ of B, acting on the blocks and on the objects, such that:

$$\begin{aligned} \tau : i &\longmapsto ti\,, \qquad i = 0, \dots, v-1\,, \\ B_i &\longmapsto B_{ti}\,. \end{aligned} \tag{1.12}$$

In terms of the corresponding incidence matrix A, since

$$tD - s \equiv D \mod v$$

the integer t determines permutation matrices P and Q (see [Bau71]) such that:

$$PAQ = A,$$

with Q permuting the blocks and P permuting the objects of the design.
In particular since A (see Section 1.2.1) and Q are non-singular, we write:

$$A^{-1}PA = Q^{-1}$$

from which follows:

$$\mathrm{Tr}(P) = \mathrm{Tr}(A^{-1}PA) = \mathrm{Tr}(Q^{-1}) = \mathrm{Tr}(Q).$$

$\mathrm{Tr}(P)$ and $\mathrm{Tr}(Q)$ describe the number of blocks and of objects fixed by the multiplier t. This number corresponds to the number of solutions of the equation $tx \equiv x \mod v$ which is $(t-1, v) = d$. In fact, if $(t-1, v) = d$ then we can write t and v as:

$$t - 1 = k_1 d, \qquad v = k_2 d$$

for some integers $k_1, k_2 \neq 0$, and from $x(t-1) \equiv 0 \mod v$ we obtain:

$$x(k_1 d) \equiv 0 \mod k_2 d.$$

The equation is satisfied for $x = 0, k_2, 2k_2, \ldots, (d-1)k_2 \mod v$. Therefore it has $(t-1, v) = d$ solutions in $\mathbb{Z}/v\mathbb{Z}$. This result confirms the one obtained for difference sets (see Proposition 1.1.3).

Chapter 2

Finite Projective Spaces

In this chapter we introduce finite projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ and some basic concepts related to them. We see that points and hyperplanes belonging to a projective space may be regarded as the objects and the blocks of a block design. They may, therefore, be numbered using (v, k, λ)-difference sets.
In particular, we consider the groups of automorphisms acting on projective spaces $\mathbb{P}^m(\mathbb{F}_n)$. We see that their action on points and hyperplanes as elements of a block design is described by the action of mutlipliers t on the elements of the associated difference set.

2.1 Finite Projective Spaces

Let $\mathbb{F}_n$ be a finite field of order $n = p^e$, p prime, $e \in \mathbb{N}\backslash\{0\}$. We consider the vector space $\mathbb{F}_n^{m+1}$ of dimension $m+1$ over $\mathbb{F}_n$. In $\mathbb{F}_n^{m+1}\backslash\{0\}$ we introduce an equivalence relation (see [Hir05]):

$$x \sim y :\Leftrightarrow \exists k \in \mathbb{F}_n^* : x = ky \ .$$

The set of all equivalence classes of vectors different from zero in $\mathbb{F}_n^{m+1}$ is the projective space $\mathbb{P}^m(\mathbb{F}_n)$ of dimension m over $\mathbb{F}_n$, so we write:

$$\mathbb{P}^m(\mathbb{F}_n) := (\mathbb{F}_n^{m+1}\backslash\{0\})/\mathbb{F}_n^* \ . \tag{2.1}$$

The integer n is called the **order** of $\mathbb{P}^m(\mathbb{F}_n)$ (see [BR04], [Dem97]). Subspaces of $\mathbb{P}^m(\mathbb{F}_n)$ of dimension t correspond to subspaces of dimension $t+1$ of $\mathbb{F}_n^{m+1}$. A

subspace of $\mathbb{P}^m(\mathbb{F}_n)$ of dimension $t = 0$ is a **point**. For $t = 1$ and $t = 2$ we speak respectively of **lines** and of **planes**. A subspace of dimension $t = m - 1$ is a **hyperplane** (see [Hir05]).
From Equation (2.1) we compute the number of elements of $\mathbb{P}^m(\mathbb{F}_n)$ as:

$$\ell = |\mathbb{P}^m(\mathbb{F}_n)| = \frac{|\mathbb{F}_n^{m+1}\backslash\{0\}|}{|\mathbb{F}_n^*|} = \frac{n^{m+1} - 1}{n - 1} \,.$$

For each subspace $\mathbb{U}^t(\mathbb{F}_n) \subset \mathbb{P}^m(\mathbb{F}_n)$ of dimension t we obtain:

$$q = |\mathbb{U}^t(\mathbb{F}_n)| = \frac{|\mathbb{F}_n^{t+1}\backslash\{0\}|}{|\mathbb{F}_n^*|} = \frac{n^{t+1} - 1}{n - 1} \,.$$

We say that each of the $\frac{n^{t+1} - 1}{n - 1}$ points lying in $\mathbb{U}^t(\mathbb{F}_n)$ is **incident** with $\mathbb{U}^t(\mathbb{F}_n)$ or, equivalently, we say that $\mathbb{U}^t(\mathbb{F}_n)$ is **incident** with $\frac{n^{t+1} - 1}{n - 1}$ points.
We also say that points and hyperplanes of dimension $m - 1$ are **dual**, i.e. each statement formulated in terms of the points also holds in terms of the hyperplanes (see [Dem97], [Hir05], [BR04]). This means, for instance, that if every hyperplane h of dimension $m - 1$ is incident with $\frac{n^m - 1}{n - 1}$ points, so by duality each point is incident with $\frac{n^m - 1}{n - 1}$ hyperplanes h. For $m = 2$ we have duality between points and lines, for $m = 3$ between points and planes.

Example 4.

1. The smallest projective space over a finite field is the **Fano plane** $\mathbb{P}^2(\mathbb{F}_2)$ (see Figure 2.1) with $\ell = \frac{2^3 - 1}{2 - 1} = 7$ points (lines). Each line is incident with $q = \frac{2^2 - 1}{2 - 1} = 3$ points and by duality each point is incident with 3 lines.

2. The projective space of one dimension higher is the space $\mathbb{P}^3(\mathbb{F}_2)$. It has $\ell = \frac{2^4 - 1}{2 - 1} = 15$ points (planes) and each point (plane) is incident with $q = \frac{2^3 - 1}{2 - 1} = 7$ planes (points).

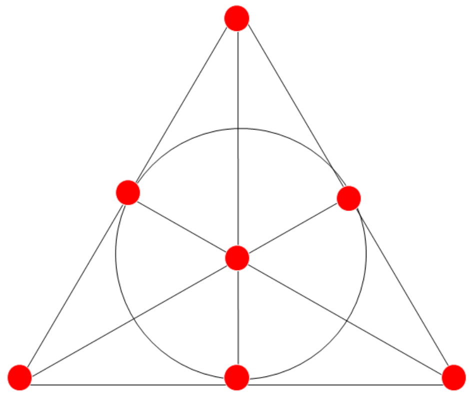


Figure 2.1: *The Fano plane.*

2.2 Groups of Automorphisms

Automorphisms μ of the projective space $\mathbb{P}^m(\mathbb{F}_n)$ are bijections preserving incidence, i.e. if a point P and a hyperplane h are incident, then $\mu(h)$ and $\mu(P)$ [1] are also incident.
Bijections which are induced by linear transformations are called **projectivities** of $\mathbb{P}^m(\mathbb{F}_n)$. Together they form the **projective linear group** $PGL(m+1,n)$ over the field $\mathbb{F}_n$ (see [Hir05]). If we only consider those transformations, for which the determinant of the corresponding matrix equals one, then we speak of the **projective special linear group** $PSL(m+1,n)$ (see [Hup79], [LZ04]). Both are normal subgroups in the full automorphism group of $\mathbb{P}^m(\mathbb{F}_n)$ ([Dem97] and see later in this section). This is the **collineation group** $P\Gamma L(m+1,n)$. A collineation is also a bijection preserving incidence, but it needs not be linear, in fact $P\Gamma L(m+1,n)$ is the group of all semilinear transformations of $\mathbb{P}^m(\mathbb{F}_n)$ ([LZ04]). A collineation μ'

[1] Here and in the following chapters we use the notation P and h for points and hyperplanes of $\mathbb{P}^m(\mathbb{F}_n)$. By this we mean the corresponding equivalence classes of vectors $p = (p_0,\ldots,p_m)$ and $h = (h_0,\ldots,h_m)$. For hyperplanes the coordinates are the coefficients of the equation $h_0p_0 + h_1p_1 + \ldots + h_mp_m = 0$ which is satisfied exactly by points P lying on h. Actions of automorphisms μ on P and on h are actions on the corresponding class of vectors.

acts on vectors $p, q \in \mathbb{F}_n^{m+1}$ in the following way:

$$\mu'(p+q) = \mu'(p) + \mu'(q),\ \mu'(\lambda p) = \sigma(\lambda)\mu'(p), \quad \lambda \in \mathbb{F}_n, \sigma \in Aut(\mathbb{F}_n)\ .$$

Each collineation μ' can be written as the product of a projectivity μ with an **automorphic collineation** σ (see [Hir05]) of $\mathbb{P}^m(\mathbb{F}_n)$. An automorphic collineation of $\mathbb{P}^m(\mathbb{F}_n)$ is an automorphism σ of $\mathbb{F}_n$ acting on the points X of $\mathbb{P}^m(\mathbb{F}_n)$, i.e. on the corresponding vectors p as:

$$\sigma(p) := (\sigma(p_0), \ldots, \sigma(p_m))\ ,$$

hence

$$\begin{aligned} &\sigma(p+q) = \sigma(p) + \sigma(q), \qquad p, q \in \mathbb{F}_n^{m+1}\ , \\ &\sigma(\lambda p) = \sigma(\lambda)\sigma(p), \qquad \lambda \in \mathbb{F}_n\ . \end{aligned}$$

Writing $\mu'(p) = \sigma(\mu(p))$ and letting μ' act on $(p+q)$ and on (λp), we obtain:

$$\begin{aligned} \mu'(p+q) &= \sigma(\mu(p+q)) = \sigma(\mu(p) + \mu(q)) \\ &= \sigma(\mu(p)) + \sigma(\mu(q)) = \mu'(p) + \mu'(q), \\ \mu'(\lambda p) &= \sigma(\mu(\lambda p)) = \sigma(\lambda\mu(p)) \\ &= \sigma(\lambda)\sigma(\mu(p)) = \sigma(\lambda)\mu'(p)\ , \end{aligned}$$

which is, in fact, the action of a semilinear transformation of $\mathbb{P}^m(\mathbb{F}_n)$. The full automorphism group of $\mathbb{F}_n$, with $n = p^e$, p prime, $e \in \mathbb{N}\backslash\{0\}$, is the group generated by the **Frobenius automorphism** σ (see [LZ04], [Wol96]):

$$\begin{aligned} \sigma :\ \mathbb{F}_n &\longrightarrow \mathbb{F}_n\ , \\ a &\longmapsto a^p\ . \end{aligned}$$

This group corresponds to the Galois group $Gal(\mathbb{F}_n/\mathbb{F}_p) \cong \Phi_e$, a cyclic group of order e.
Thus $P\Gamma L(m{+}1, n)$ is the group generated by the Galois group Φ_e and by $PGL(m+1, n)$. We write:

$$P\Gamma L(m+1, n) = \Phi_e \ltimes PGL(m+1, n)\ . \tag{2.2}$$

The fact that $PGL(m+1, n)$ is normal in $P\Gamma L(m+1, n)$ can be explained in the following way. Let $M = (m_{ij})_{0 \le i,j \le m}$ be the matrix of some linear transformation in $PGL(m+1,n)$ and let $p=(p_0,\dots,p_m)$ be a vector in $\mathbb{P}^m(\mathbb{F}_n)$. We consider the action $\sigma M\sigma^{-1}$ on p:

$$\begin{aligned}\sigma(M\sigma^{-1}(p)) &= \sigma((m_{00}\sigma^{-1}(p_0)+\ldots+m_{0m}\sigma^{-1}(p_m)),\ldots,(m_{m0}\sigma^{-1}(p_0)+\ldots+m_{mm}\sigma^{-1}(p_m)))\\ &= ((\sigma(m_{00})(p_0)+\ldots+\sigma(m_{0m})(p_m)),\ldots,(\sigma(m_{m0})(p_0)+\ldots+\sigma(m_{mm})(p_m)))\\ &= ((m^p_{00}(p_0)+\ldots+m^p_{0m}(p_m)),\ldots,(m^p_{m0}(p_0)+\ldots+m^p_{mm}(p_m)))\\ &= \sigma(M)(p) \qquad (2.3)\end{aligned}$$

where $\sigma(M)$ is again an element of $PGL(m+1,n)$, obtained from M by application of σ to the coefficients. It therefore follows that $PGL(m+1,n)\lhd P\Gamma L(m+1,n)$.

2.3 Finite Projective Spaces $\mathbb{P}^m(\mathbb{F}_n)$ as Block Designs

If we consider the points of $\mathbb{P}^m(\mathbb{F}_n)$ as objects and the dual hyperplanes as blocks, $\mathbb{P}^m(\mathbb{F}_n)$ forms a block design (see [Bau71]), which is symmetric and cyclic. The symmetry property relies on the fact that:

$$\#\text{ points } = \#\text{ hyperplanes (see 2.1)}\ .$$

It is cyclic as a consequence of the following proposition and definition:

Proposition (and Definition) 2.3.1. *Every $\mathbb{P}^m(\mathbb{F}_n)$ admits a cyclic transitive group of collineations. This group is known as a* ***Singer group****.*

This property was first proved by Singer ([Sin38]) for projective planes $\mathbb{P}^2(\mathbb{F}_n)$. Now it is widely known (see [Bau71], [Dem97], [Hir05]) that it also holds for spaces of higher dimension.
Here we will only briefly sketch a proof. For a more exhaustive proof see [Hup79, Section II.7].

Proof. We identify the vector space $\mathbb{F}_n^{m+1}$ with the additive group $\mathbb{F}_{n^{m+1}}$. Since

$$\mathbb{P}^m(\mathbb{F}_n)=(\mathbb{F}_n^{m+1}\backslash\{0\})/\mathbb{F}_n^*$$

we also have:

$$\mathbb{P}^m(\mathbb{F}_n)\cong\mathbb{F}_{n^{m+1}}^*/\mathbb{F}_n^*\ .$$

The quotient $\mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$ is a cyclic multiplicative group of order $l = \frac{n^{m+1}-1}{n-1}$ and we write all its elements as powers g^i of a generator $< g >$. Thus the action of $\Sigma_\ell \cong \mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$ on the elements of $\mathbb{P}^m(\mathbb{F}_n)$ is given by:

$$\gamma^k : g^i \longmapsto g^{i+k} .$$

This is a linear action on $\mathbb{F}_n^{m+1}$ cyclically permuting the elements g^i. It is easy to check that the equivalence relation induced by $\mathbb{F}^*_n$ is preserved. Let g^i and g^j be two equivalent elements in $\mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$. Thus we may write g^j as:

$$g^j = \lambda \cdot g^i , \qquad \lambda \in \mathbb{F}^*_n .$$

On the element $\lambda \cdot g^i$ the Singer group acts as:

$$\gamma^k : \ \lambda \cdot g^i \ \longmapsto \ \lambda \cdot g^{i+k} .$$

Since $\lambda \cdot g^{i+k}$ and g^{i+k} are equivalent in $\mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$, the equivalence relation is preserved. It follows that the Singer group Σ_ℓ is a cyclic transitive group of collineations of $\mathbb{P}^m(\mathbb{F}_n)$. □

Remark. Since we have $\mathbb{P}^m(\mathbb{F}_n) \cong \mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$, it is possible to number the points P_i and the hyperplanes $h_j$of $\mathbb{P}^m(\mathbb{F}_n)$ with integers $i, j \in \{0, \ldots, \ell\}$ corresponding to exponents of a generator $< g >$ of $\mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$.

$$g^i \leftrightarrow P_i , \qquad g^j \leftrightarrow h_j , \qquad i, j \in \mathbb{Z}/\ell\mathbb{Z}.$$

Consequently, the action of every $\gamma^k \in \Sigma_\ell$ on the elements P_i and h_j is expressed by:

$$\begin{aligned} \gamma^k : & P_i \longmapsto P_{i+k} , \\ & h_j \longmapsto h_{j+k} . \end{aligned}$$

2.3.1 Constructing the associated Block Designs

As we have seen, cyclic symmetric block designs can be described using (v, k, λ)-difference sets (see Section 1.2).
The existence of the Singer group allows us to relate points and dual hyperplanes of a projective space $\mathbb{P}^m(\mathbb{F}_n)$ to a difference set. For the sake of simplicity, we here discuss only the case $m = 2$ ([Sin38], [Hir05]). The construction can be extended with some generalizations to $m > 2$ ([Hir05]). First of all we construct an array M such that its elements are the points of $\mathbb{P}^2(\mathbb{F}_n)$ and its columns consist of the points

on the lines.
With the notation introduced in Section 2.1 we denote by $\ell = n^2 + n + 1$ the total number of points and of lines and with $q = n+1$ the number of points on a line and vice versa the number of lines through a point.
Let P_{d_0} and P_{d_1} be the points with indices $d_0 = 0$ and $d_1 = 1$. We indicate with l_0 the line through them and we suppose the points $P_{d_2}, \ldots, P_{d_{q-1}}$ being collinear with them. The points $P_{d_0}, \ldots, P_{d_{q-1}}$ describe the first column of M. Applying recursively $\gamma \in \Sigma_\ell$ and identifying each point with its index, we obtain the array M:

$$M = \begin{pmatrix} d_0 & d_0 + 1 & \ldots & d_0 + (\ell - 1) \\ d_1 & d_1 + 1 & & d_1 + (\ell - 1) \\ \vdots & \vdots & & \vdots \\ d_{q-1} & d_{q-1} + 1 & \ldots & d_{q-1} + (\ell - 1) \end{pmatrix} . \tag{2.4}$$

Since the first column represents the points of a line, then by construction each other column also represents the points on some line of $\mathbb{P}^2(\mathbb{F}_n)$.
Now we construct an array M' containing only those lines incident with P_{d_0}. This means that we only consider those lines containing a point P_{d_j+i} with:

$$\begin{aligned} & d_j + i \equiv 0 \mod \ell, \qquad j \in \mathbb{Z}/q\mathbb{Z},\, i \in \mathbb{Z}/\ell\mathbb{Z} \\ & \Rightarrow i \equiv -d_j \mod \ell. \end{aligned}$$

We obtain the following array:

$$M' = \begin{pmatrix} d_0 - d_0 & \ldots & d_0 - d_{q-1} \\ \vdots & & \vdots \\ d_{q-1} - d_0 & \ldots & d_{q-1} - d_{q-1} \end{pmatrix}$$

The array has q lines and q columns, since q points lie on a line of $\mathbb{P}^2(\mathbb{F}_n)$ and the point P_{d_0} we consider is incident with q lines. The elements on the diagonal of M' are all zero and as the q lines can only share one point, all the other differences $d_i - d_j$ must be different from each other. Each of them represents a point P_i, $i \in \{1, \ldots, \ell - 1\}$, in fact the number of differences different from zero is given by:

$$q \cdot q - q = n^2 + n \ ,$$

and

$$n^2 + n = \ell - 1 \ .$$

Therefore we have

Proposition 2.3.2. *([Hir05]) The integers $d_0, \dots d_{q-1}$ form a perfect difference set; that is the $(\ell - 1)$ integers $d_i - d_j$ with $i \neq j$ are all distinct modulo ℓ.*

This means that a perfect difference set with parameters

$$v = \ell = n^2 + n + 1, \quad k = q = n + 1, \quad \lambda = 1$$

is associated to every projective plane $\mathbb{P}^2(\mathbb{F}_n)$. In the general case of projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ we have

$$v = \ell = \frac{n^{m+1} - 1}{n - 1}, \quad k = q = \frac{n^m - 1}{n - 1}, \quad \lambda = \frac{n^{m-1} - 1}{n - 1}$$

and for $\lambda > 1$ the associated difference set is no longer perfect (see Section 1.1).

Remark. For block designs, λ gives the number of blocks in which two objects occur. If we consider projective spaces as block designs, λ is therefore the number of hyperplanes in which a pair of distinct points occurs and by duality it is the number of points shared by two hyperplanes.

Example 5. The block design of the Fano plane $\mathbb{P}^2(\mathbb{F}_2)$ (see Example 4) can be constructed using the difference set:

$$D = \{0, 1, 3\}$$

or any shift $\mod 7$ of it. The incidence pattern is described by the array M,

$$M = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \end{pmatrix}$$

where the points of the i-th column describes the points on the i-th line (see Figure 2.2).

For $\mathbb{P}^2(\mathbb{F}_2)$ we have $\lambda = 1$ which is geometrically motivated by the fact that two points lie on only one line and two lines only share one point.

2.3.2 Multipliers as Automorphisms of Projective Spaces

As we have seen (see Section 1.2.2) multipliers t of difference sets describe automorphisms of the associated block designs acting on the blocks and on the objects as given in Equation (1.12).

Since projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ can be considered as block designs, multipliers of the

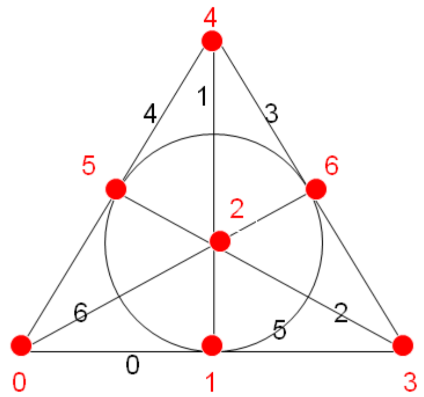


Figure 2.2: *The Fano plane as a block design.*

associated (v, k, λ)- difference set describe automorphisms α acting on the points and on the dual hyperplanes as:

$$\begin{aligned} \alpha : P_i &\longmapsto P_{ti} \ , \\ h_j &\longmapsto h_{tj} \ . \end{aligned}$$

Thus t is also said to be a **multiplier of the plane** $\mathbb{P}^m(\mathbb{F}_n)$ ([Bau71]).
We will come back to this in Chapter 3 describing the Galois group $Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$ generated by the Frobenius automorphism.

Chapter 3

Difference Sets and the Frobenius Automorphism

In this chapter we explain how the group Φ_f generated by the Frobenius automorphism, acting on the points and on the dual hyperplanes of a projective space $\mathbb{P}^m(\mathbb{F}_n)$, influences the construction of difference sets. We will see that only special difference sets give rise to block designs (see Chapter 1) for which Φ_f is a group of automorphisms.
Such difference sets are fixed under the action of Φ_f.
As usual $\ell = n^m + \ldots + 1$ is the number of points and of corresponding dual hyperplanes in $\mathbb{P}^m(\mathbb{F}_n)$. With $q = n^{m-1} + \ldots + 1$ we denote the number of points on each hyperplane and vice versa we denote the number of dual hyperplanes through a point.

3.1 The Frobenius Automorphism

As we have seen in Chapter 2, we may identify the projective space $\mathbb{P}^m(\mathbb{F}_n)$ over the finite field $\mathbb{F}_n$, $n = p^e$, p prime, $e \in \mathbb{N}\backslash\{0\}$, with the quotient $\mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$. Since $\mathbb{F}_{n^{m+1}}$ is a finite field, we know that there exists an automorphism σ, the **Frobenius automorphism**, acting on the elements $a \in \mathbb{F}_{n^{m+1}}$ in the following way:

$$\begin{array}{rccc} \sigma : & \mathbb{F}_{n^{m+1}} & \longrightarrow & \mathbb{F}_{n^{m+1}} \ , \\ & a & \longmapsto & a^p \ . \end{array}$$

The Frobenius automorphism σ generates the Galois group $Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p) = \Phi_f$ as a cyclic group of order $f = e \cdot (m+1)$.
Let g be a generator of the cyclic group $\mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$. As we have already seen in Section 2.3 the points P_i and the dual hyperplanes h_j of $\mathbb{P}^m(\mathbb{F}_n)$ correspond to powers of the generator g:

$$g^i \leftrightarrow P_i\,,\ g^j \leftrightarrow h_j \quad i,j \in \mathbb{Z}/\ell\mathbb{Z}\,, \quad \ell = \frac{n^{m+1}-1}{n-1}$$

Thus each $\sigma^k \in \Phi_f$ acts on P_i and h_j as:

$$\begin{array}{rrcl} \sigma^k : & P_i & \longmapsto & P_{ip^k}\,, \quad k \in (\mathbb{Z}/f\mathbb{Z}) \\ & h_j & \longmapsto & h_{jp^k}\,. \end{array}$$

The action of Φ_f divides the set of points $\mathcal{P}$ and the set of hyperplanes $\mathcal{H}$ into orbits with different lengths $\varphi \in \mathbb{N}$, $\varphi | f$. Observe that there always exist at least one point orbit and at least one hyperplane orbit of length 1, since

$$\begin{array}{rrcl} \sigma^k : & P_0 & \longmapsto & P_0\,, \quad \forall k \in (\mathbb{Z}/f\mathbb{Z})\,, \\ & h_0 & \longmapsto & h_0\,. \end{array}$$

3.2 Frobenius Difference Sets

In Chapter 2 we have seen that it is possible to construct difference sets associated with projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ relying on the action of the Singer group Σ_ℓ on points and hyperplanes.
Let D be such a difference set associated with a projective space $\mathbb{P}^m(\mathbb{F}_n)$. Then each shift $D + s$ and each multiplication tD by integers $t, s \in \mathbb{Z}/\ell\mathbb{Z}$, $(t, \ell) = 1$ or a combination of the two are still possible difference sets. Each of them determines different numberings of the points and of the hyperplanes of $\mathbb{P}^m(\mathbb{F}_n)$. Independently of the numbering, the Singer group Σ_ℓ is by construction always a group of automorphisms of the block design associated with $\mathbb{P}^m(\mathbb{F}_n)$ (see Section 2.3.1). Nevertheless, Φ_f is a group of automorphisms of the block design only for special numberings of the points and of the dual hyperplanes. This means that Φ_f acts as a group of automorphisms only by the choice of some of the difference sets. This fact can be made evident with an example:

Example 6. We consider the **Fano plane** (see Examples 4 and 5) and different numberings of its seven points P_i and lines h_i. The numberings are determined by the difference sets:

$$D = \{0, 1, 3\},$$
$$D' = \{1, 2, 4\},$$
$$D'' = \{3, 6, 5\}.$$

The difference set D' is a shift $(D+1) \mod 7$ of D, D'' is congruent to $3 \cdot D' \mod 7$. Suppose the integers of each difference set describe the indices of the points on the line h_0.
We recall the action of an element $\gamma \in \Sigma_\ell$ on the points and on the lines:

$$\gamma \;:\; \begin{array}{ccc} P_i & \longmapsto & P_{i+1}\,, \\ h_j & \longmapsto & h_{j+1}\,. \end{array} \qquad \forall i, j \in \mathbb{Z}/\ell\mathbb{Z}$$

Applying γ recursively to the points on h_0 and to h_0 itself we obtain a complete numbering of all points and dual lines. We get the block designs B, B', B'' given in Figures 3.1, 3.2 and 3.3.

It is easy to see that for each block design the Singer group Σ_7 is a group of

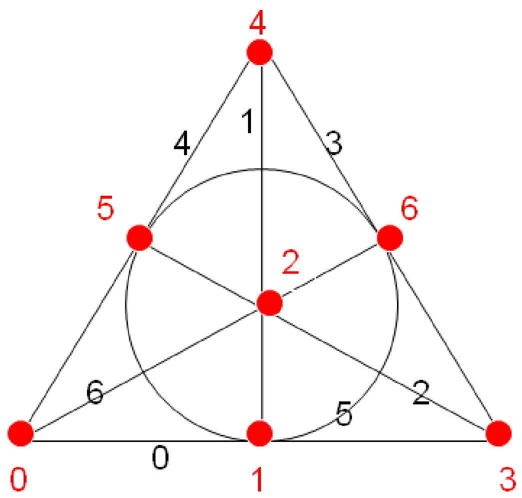


Figure 3.1: *Block design B of the Fano plane with difference set $D = \{0, 1, 3\}$.*

automorphisms preserving incidence between points and lines. On the contrary, the Galois group $Gal(\mathbb{F}_8/\mathbb{F}_2) \cong \Phi_3$ generated by the Frobenius automorphism

$$\sigma : \quad a \longmapsto a^2, \quad a \in \mathbb{F}_8\,,$$

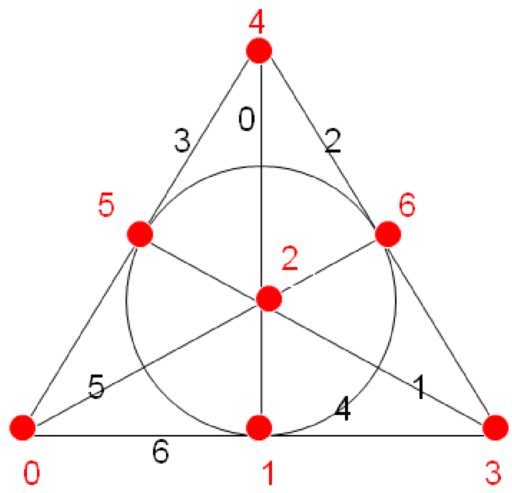


Figure 3.2: *Block design B' of the Fano plane with difference set $D' = \{1, 2, 4\}$.*

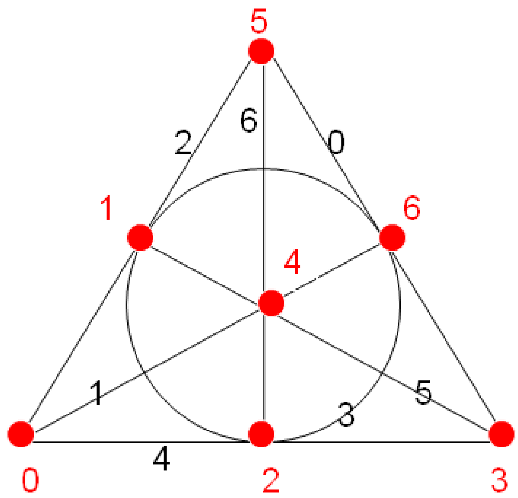


Figure 3.3: *Block design B'' of the Fano plane with difference set $D'' = \{3, 6, 5\}$.*

is an automorphism group of B' and of B'' but no longer of B. In fact, on B it does not preserve incidence, since

$$\sigma : \quad P_0, P_1, P_3 \longmapsto P_0, P_2, P_6$$

and $\{P_0, P_1, P_3\} \in h_0$, $\{P_0, P_2, P_6\} \in h_6$, but

$$\sigma : \quad h_0 \longmapsto h_0 \ .$$

We formulate the following

Proposition (and Definition) 3.2.1. *Let $\mathbb{P}^m(\mathbb{F}_n) \cong \mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$ be a projective space, $n = p^e$, $e \in \mathbb{N}\backslash\{0\}$ containing ℓ points and ℓ hyperplanes which can be numbered using difference sets.*
The Frobenius automorphism determines a difference set D_f, which is fixed under the action of $\Phi_f \cong Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$. Multiplying D_f with integers $t \in (\mathbb{Z}/\ell\mathbb{Z})^*$, we still obtain difference sets fixed under the action of Φ_f.
We call D_f and all difference sets $t \cdot D_f$ ***Frobenius difference sets****.*

Proof. As we have remarked in Section 3.1 Φ_f divides the set of points $\mathcal{P}$ and the set of hyperplanes $\mathcal{H}$ of $\mathbb{P}^m(\mathbb{F}_n)$ into orbits with different lengths. In particular there is always at least one orbit of length 1 in each set. In fact, there always are the fixed elements $P_0 \in \mathcal{P}$ and $h_0 \in \mathcal{H}$. Let us consider the hyperplane h_0. Every element $\sigma^k \in \Phi_f$ describes a collineation of $\mathbb{P}^m(\mathbb{F}_n)$ (see Section 2.2), so it preserves incidence. We now consider the set $\mathcal{P}_0 = \{P_{i_0}, P_{i_1}, \ldots, P_{i_{q-1}}\}$ of points on h_0. Since

$$\sigma^k : h_0 \longmapsto h_0, \quad \forall \sigma^k \in \Phi_f \ ,$$

by incidence preservation we also obtain

$$\sigma^k : \mathcal{P}_0 \longmapsto \mathcal{P}_0, \quad \forall \sigma^k \in \Phi_f \ .$$

In Section 2.3.1 we have seen that the indices of the points on a hyperplane describe a difference set associated with the projective space $\mathbb{P}^m(\mathbb{F}_n)$, so the set D_f of the indices of the points belonging to $\mathcal{P}_0$ is the Frobenius difference set we are looking for. It is easy to see that multiplying D_f with integers $t \in (\mathbb{Z}/\ell\mathbb{Z})^*$ again leads to Frobenius difference sets. In fact, Φ_f acts on the elements of D_f and of each tD_f by multiplication with powers p^k, $k \in \mathbb{Z}/f\mathbb{Z}$, so we have:

$$p^k \cdot t \cdot D_f = t \cdot p^k \cdot D_f \equiv t \cdot D_f \mod \ell \,, \quad \forall t \in (\mathbb{Z}/\ell\mathbb{Z})^* \ ,$$

i.e. each tD_f is fixed under the action of Φ_f. □

Since Φ_f acts on each tD_f by multiplication with powers p^k, $k \in \mathbb{Z}/f\mathbb{Z}$, from Proposition 3.2.1 follows

Corollary 3.2.2. *Every $p^k, k \in (\mathbb{Z}/f\mathbb{Z})$ is a multiplier of a Frobenius difference set D_f and*

$$p^k D_f \equiv D_f \mod \ell, \quad \forall k \in (\mathbb{Z}/f\mathbb{Z}) .$$

Moreover, Φ_f divides the points on h_0 into orbits with different lengths φ. As each D_f consists of the indices of these points, this means that Φ_f also divides the elements of D_f into orbits of different lengths φ. Thus we formulate the following:

Corollary 3.2.3. *Under the action of Φ_f, the elements of a Frobenius difference set D_f are subdivided into orbits of different lengths φ, $\varphi \in \mathbb{N}$, $\varphi \mid f$. The orbits correspond to orbits of points in $\mathbb{P}^m(\mathbb{F}_n)$.*

Remark. If a point P_i lies on a hyperplane h_j fixed under the action of Φ_f, then the entire Φ_f-orbit of P_i is incident with h_j. Incidence between points $P_i \in \mathbb{P}^m(\mathbb{F}_n)$ and hyperplanes $h_j \in \mathbb{P}^m(\mathbb{F}_n)$ may be expressed by a bilinear form on the underlying vector space:

$$B: \quad \mathbb{F}_n^{m+1}\backslash\{0\} \times \mathbb{F}_n^{m+1}\backslash\{0\} \longrightarrow \mathbb{F}_n$$

A point P_i and a hyperplane h_j are incident if:

$$B(P_i, h_j) = 0 .$$

As we have seen we may identify the points P_i and the hyperplanes h_j with powers g^i and g^j of a generator of $\mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$. Thus a point and a hyperplane are incident if

$$B(g^i, g^j) = 0 .$$

Due to our considerations above it is reasonable to choose as a bilinear form:

$$B(g^i, g^j) := tr(g^i \cdot g^j) = tr(g^{i+j}) = 0 , \tag{3.1}$$

where $tr(g^{i+j})$ is the **trace** of the element g^{i+j}. Since we consider here the action of the Galois group $\Phi_f \cong Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$, for $tr(g^{i+j})$ we choose the trace of the field extension $\mathbb{F}_{n^m}$ over the ground field $\mathbb{F}_p$:

$$\begin{array}{llll} tr: & \mathbb{F}_{n^{m+1}} & \longrightarrow & \mathbb{F}_p \\ & a & \longmapsto & tr(a) = \sum_{k=0}^m \sigma^k(a), \qquad \sigma^k \in Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p) . \end{array}$$

For hyperplanes $h_j \leftrightarrow g^j$ which are fixed under the action of each σ^k and for the points $P_i \leftrightarrow g^i$ on them we obtain:

$$\begin{aligned} tr(g^{i+j}) &= \sum_{k=0}^{m} g^j \sigma^k(g^i) \\ &= g^j \sum_{k=0}^{m} \sigma^k(g^i) . \end{aligned}$$

Due to condition (3.1) it follows:

$$\sum_{k=0}^{m} \sigma^k(g^i) = 0 \ .$$

Thus on a fixed hyperplane lie those points for which the trace defined by the action of Φ_f is equal to zero.

Example 7. Considering again Example 6, we see that the difference set D' is a Frobenius difference set since it consists of the indices of the points $P_1, P_2, P_4 \in h_0$, which belong to one single orbit under the action of Φ_3. Each 2^k is a multiplier of D' and $2^k D' \equiv D' \mod 7$, $\forall k \in (\mathbb{Z}/3\mathbb{Z})$. The same considerations hold for the difference set D'' but not for D, as it is easy to check.

Example 8. Let us consider the projective space $\mathbb{P}^3(\mathbb{F}_3) \cong \mathbb{F}^*_{3^4}/\mathbb{F}^*_3$ with 40 points and 40 hyperplanes of dimension 2. The Frobenius automorphism σ generates the Galois group $Gal(\mathbb{F}_{3^4}/\mathbb{F}_3) \cong \Phi_4$, which acts on the points P_i and on the hyperplanes h_i as

$$\sigma : \quad P_i \longmapsto P_{3i} \ ,$$
$$h_i \longmapsto h_{3i} \ .$$

We identify the points on the hyperplane h_0 fixed by C_4 with the elements of the following $(40, 13, 4)$-difference set ([Bau71]) [1]:

$$D_4 = \{21, 22, 23, 25, 26, 29, 34, 35, 38, 0, 5, 7, 15\} \mod 40 \ .$$

The set D_4 is a Frobenius difference set and it is easy to prove that multiplying it with 3 or with its powers 3^k, $k \in (\mathbb{Z}/4\mathbb{Z})$ we only have a permutation of its elements, i.e. we have

$$3^k D_4 \equiv D_4 \mod 40 \ , \quad \forall k \in (\mathbb{Z}/4\mathbb{Z}) \ .$$

The cyclic group Φ_4 divides the points (and the hyperplanes) of $\mathbb{P}^3(\mathbb{F}_3)$ into orbits of different lengths. The set D_4 consists of the indices of the points belonging to the following five orbits:

$$\{P_{21}, P_{23}, P_{29}, P_7\}, \{P_{22}, P_{26}, P_{34}, P_{38}\}, \{P_{25}, P_{35}\}, \{P_5, P_{15}\}, \{P_0\} \ .$$

[1] The choice of the following Frobenius difference set is not by accident. In the last section of this chapter we explain how it is possible to establish an unambiguous relation between Frobenius difference sets and point numberings.

Now the question arises whether there may also be shifts of a Frobenius difference set D_f which are again Frobenius difference sets. Indeed, depending on the number of fixed points and of fixed hyperplanes of Φ_f we can have more than one possible Frobenius difference set:

Proposition 3.2.4. *Let $\mathbb{P}^m(\mathbb{F}_n) \cong \mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$ be a projective space, $n = p^e$, $e \in \mathbb{N}\backslash\{0\}$. The projective space $\mathbb{P}^m(\mathbb{F}_n)$ contains ℓ points P_i and ℓ hyperplanes h_i: both of them can be numbered using a Frobenius difference set D_f. The set D_f is unique up to multiplication with integers $t \in (\mathbb{Z}/\ell\mathbb{Z})^*$ if and only if only h_0 and equivalently only P_0 are fixed by $\Phi_f \cong Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$. If there are more elements fixed, we will have shifts of D_f which are also Frobenius difference sets and:*

$$\#\textit{Frobenius difference sets } = \#\textit{ fixed points (fixed hyperplanes) of } \Phi_f$$

Proof. We consider the first part of the proposition and we show the two directions.

1. Let us assume that the Frobenius difference set is unique but there is another hyperplane h_i fixed by Φ_f. This would mean that h_0 and h_i share the same set $\mathcal{P}_0$ of points. Nevertheless sharing the same set of points means $h_0 = h_i$.

2. Now we assume that there is only one hyperplane fixed by Φ_f, but we can describe the points on it using two different Frobenius difference sets D_f and D'_f. Both D_f and D'_f are defined up to multiplication with integers $t \in (\mathbb{Z}/\ell\mathbb{Z})^*$. Let D_f be the difference set constructed as described in Section 2.3.1. By construction and due to the action of the Singer automorphism, the elements of D'_f correspond to a shift $D_f + i$, $i \in \mathbb{Z}/\ell\mathbb{Z}$ of the elements of D_f. Nevertheless, since the Singer automorphism also applies to h_0, if $D_f + i$ is fixed under the action of Φ_f, then the hyperplane h_i should also be fixed. This is a contradiction to the fact that h_0 is unique. It thus follows that D_f is unique up to multiplication with integers $t \in (\mathbb{Z}/\ell\mathbb{Z})^*$.

As we have already seen, the indices of the points on every hyperplane $h_i \neq h_0$ can be identified with the elements of a shift $D_f + i$. If Φ_f fixes some of the hyperplanes h_i, it directly follows that the indices of the points on h_i describe a new Frobenius difference set $D_f + i$ and we have:

$$\#\text{Frobenius difference sets } = \#\text{ fixed points (fixed hyperplanes) of } \Phi_f\,.$$

□

Remark. From the proof of Proposition 3.2.4 it follows that, once we know one Frobenius difference set D_f, it is easy to determine the other difference sets fixed by Φ_f. We only need to know which of the hyperplanes h_i is fixed by Φ_f. The corresponding difference sets are the shifts $D_f + i$. Recalling our considerations in Section 1.2.2 we formulate the following:

Corollary 3.2.5. *Let $k := gcd(p-1, \ell)$ and*

$$\begin{aligned} p - 1 &= s_1 \cdot k \\ \ell &= s_2 \cdot k \end{aligned}$$

with integers $s_1, s_2 \in \mathbb{N}\backslash\{0\}$.
The hyperplanes fixed under the action of Φ_f are those hyperplanes h_i with indices

$$i \in \{0, s_2, \dots, (k-1) \cdot s_2\} \ .$$

Proof. If $k := gcd(p-1, \ell) = 1$, then only one Frobenius difference set exists (see Proposition 1.1.3), i.e. only the hyperplane h_0 is fixed under the action of Φ_f.
Let $k \neq 1$. An hyperplane h_i with index i is fixed under the action of Φ_f if

$$\begin{aligned} p \cdot i &\equiv i \mod \ell \ , \\ \Rightarrow (p-1)i &\equiv 0 \mod \ell \ . \end{aligned}$$

Since $p - 1 = s_1 \cdot k$ and $\ell = s_2 \cdot k$ with $gcd(s_1, s_2) = 1$ we have:

$$\begin{aligned} s_1 \cdot k \cdot i &\equiv 0 \mod s_2 \cdot k \\ s_1 \cdot i &\equiv 0 \mod s_2 \\ \Rightarrow i &\equiv 0 \mod s_2 \ . \end{aligned}$$

It follows that the hyperplanes with indices

$$i \in \{0, s_2, \dots, (k-1)s_2\}$$

are exactly those, which are fixed by Φ_f. □

Example 9. For the Fano plane $\mathbb{P}^2(\mathbb{F}_2)$ we have $p = 2$ and $\ell = 7$. Thus we have $gcd(1, 7) = 1$ and there are only one hyperplane h_0 and one point P_0 which are fixed under the action of Φ_3. It follows that the Frobenius difference set $D_3 = \{1, 2, 4\}$ is unique up to multiplication with integers $t \in (\mathbb{Z}/7\mathbb{Z})^*$ as we have seen in Example 7.

Example 10. For the projective space $\mathbb{P}^3(\mathbb{F}_3)$ we have $\ell = 40$, $p = 3$ and $gcd(2, 40) = 2$. This means that there are two hyperplanes and, by duality, two points fixed by Φ_4. Since $\ell = 40 = 2 \cdot 20$ the fixed hyperplanes are h_0 and h_{20} and the fixed points are P_0 and P_{20}. As we have seen in Example 8, we may choose

$$D_4 = \{21, 22, 23, 25, 26, 29, 34, 35, 38, 0, 5, 7, 15\} \mod 40$$

as the Frobenius difference set corresponding to h_0. Therefore we have that

$$D_4' \equiv D_4 + 20 \mod 40 = \{1, 2, 3, 5, 6, 9, 14, 15, 18, 20, 25, 27, 35\} \mod 40$$

is the Frobenius difference set corresponding to h_{20} and it is easy to prove that $3^k(D_4 + 20) \equiv (D_4 + 20) \mod 40$, $\forall k \in \mathbb{Z}/4\mathbb{Z}$.

Example 11. We consider the projective space $\mathbb{P}^3(\mathbb{F}_5)$ with $p = 5$, $\ell = 156$. The Frobenius automorphism generates the cyclic group Φ_4.
Since $\ell = 4 \cdot 39$ we have $gcd(5 - 1, 156) = 4$ and there are four hyperplanes –and by duality four points– fixed under the action of Φ_4:

$$h_0, h_{39}, h_{78}, h_{117} \text{ and } P_0, P_{39}, P_{78}, P_{117} \,.$$

We consider the Frobenius difference set (see [Bau71])

$$D_4 = \{0, 1, 5, 11, 13, 25, 28, 39, 46, 55, 58, 65, 68, 74, 76, 86, \\ 87, 91, 111, 117, 118, 119, 122, 123, 125, 127, 134, 140, 142, 143, 147\} \mod 156\,.$$

and we let correspond its elements to the indices of the points on h_0.
The shifted difference sets:

$$D_4 + 39 \,, D_4 + 78 \,, D_4 + 117 \,.$$

are also Frobenius difference sets fixed by Φ_4. Their elements number the points on the other fixed hyperplanes.

Up to now we have considered difference sets which are fixed by Φ_f and therefore by all multipliers p^k, $k \in (\mathbb{Z}/f\mathbb{Z})$. Of course it can happen that a subgroup $\Phi_g \subset \Phi_f$ fixes a larger number of points (hyperplanes) of $\mathbb{P}^m(\mathbb{F}_n)$ and therefore of difference sets. The cyclic group Φ_g is generated by powers of the Frobenius automorphism σ^j such that $j \cdot g \equiv 0 \mod f$, and it acts on the elements of the difference sets it fixes by multiplication with powers p^j. We formulate the following:

Corollary 3.2.6. *The number of difference sets fixed by each subgroup* $\Phi_g \subset \Phi_f$ *is equal to the number of points (hyperplanes) of* $\mathbb{P}^m(\mathbb{F}_n)$ *it fixes. According to the action of* Φ_g*, all* p^j *with* $j \cdot g \equiv 0 \mod f$ *fix these difference sets by only permuting their elements.*

Remark. What we have remarked above for the different Frobenius difference sets also holds for the difference sets fixed by the subgroups $\Phi_g \subset \Phi_f$. If we know a Frobenius difference set D_f and we know that a subgroup Φ_g fixes a hyperplane h_i then we can determine the corresponding difference set fixed by Φ_g as a shift $D_f + i$.

Example 12. We consider again the projective space $\mathbb{P}^3(\mathbb{F}_3)$ with parameters $q = 13$ and $l = 40$.
We may easily extend the results of Corollary 3.2.5 to subgroups $\Phi_g \subset \Phi_f$. In fact, the subgroup $\Phi_2 \subset \Phi_4 \cong Gal(\mathbb{F}_{3^4}/\mathbb{F}_3)$ acts on the elements of the fixed difference set D_4 by multiplication with the power 3^2. We have $gcd(9-1, 40) = 8$, thus according to Corollary 3.2.5 the group Φ_2 fixes eight hyperplanes:

$$h_0, h_5, h_{10}, h_{15}, h_{20}, h_{25}, h_{30}, h_{35}.$$

So there are eight difference sets fixed by the multiplier 3^2. Let D_4 be the difference set corresponding to h_0. D_4 is as in Example 8. The other difference sets fixed by 3^2 are

$$D_4 + 5, D_4 + 10, D_4 + 15, D_4 + 20, D_4 + 25, D_4 + 30, D_4 + 35.$$

Each of them is subdivided by Φ_2 into orbits of length 1 or 2.

3.3 Frobenius Difference Sets and Point Numberings

At first sight, it seems to be arbitrary which Frobenius difference set we use to number the points on an hyperplane h_j fixed under the action of Φ_f. Nevertheless, due to combinatorial properties of Frobenius difference sets it is possible to determine an unambiguous relation between fixed hyperplanes and Frobenius difference sets.
At first, we formulate a useful lemma and proposition:

Lemma 3.3.1. *For a projective space* $\mathbb{P}^m(\mathbb{F}_n)$ *the integers* $q = \frac{n^m-1}{n-1}$ *and* $\ell = \frac{n^{m+1}-1}{n-1}$ *are coprime.*

Proof. We apply the Euclidean algorithm to the integers $n^{m+1}-1$ and n^m-1 and obtain:

$$\begin{aligned} n^{m+1}-1 &= n\cdot(n^m-1)+(n-1)\ , \\ n^m-1 &= (n-1)\cdot(n^{m-1}+n^{m-2}+\ldots+1)\ , \end{aligned}$$

i.e.:

$$gcd(n^{m+1}-1, n^m-1) = (n-1)\ .$$

Since we have $q=\frac{n^m-1}{n-1}$ and $\ell=\frac{n^{m+1}-1}{n-1}$, it directly follows:

$$gcd(q,\ell)=1\ .$$

□

Proposition 3.3.2. *Among the Frobenius difference sets associated with a projective space $\mathbb{P}^m(\mathbb{F}_n)$ there is always a difference set D_f^0 such that*

$$\sum_{i=1}^{q} d_i = 0\,,\quad d_i\in D_f^0\,,\quad q := \#\ \textit{Elements of } D_f^0\ .$$

D_f^0 is unique up to multiplication with integers $t\in(\mathbb{Z}/\ell\mathbb{Z})^*$.

Proof. Let D_f be a Frobenius difference set

$$D_f=\{d_1,\ldots,d_q\}\mod \ell$$

with

$$\sum_{i=1}^{q} d_i = N \mod \ell\ .$$

We write the points of $\mathbb{P}^m(\mathbb{F}_n)$ as powers $g^j, j\in\mathbb{Z}/\ell\mathbb{Z}$ of a generator of $\mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$ and we have

$$\prod_{i=1}^{q} g^{d_i} = g^{(\sum_{i=1}^{q} d_i \mod \ell)}\ .$$

We define $s:=(\sum_{i=1}^{q} d_i)\mod \ell$. So we get:

$$g^{\left((\sum_{i=1}^{q} d_i)-s\right)\mod \ell}=1\ . \tag{3.2}$$

Since q and ℓ are prime to each other (see Lemma 3.2.5), a number $\bar{q}\in(\mathbb{Z}/\ell\mathbb{Z})^*$ exists such that $q\bar{q}\equiv 1\mod l$. So we write Equation 3.2 as

$$g^{(\sum_{i=1}^{q}(d_i-\bar{q}s))\mod \ell}=1\ . \tag{3.3}$$

This means that the sum of the elements of the shift $(D_f - \bar{q}s) \mod l$ is congruent to $0 \mod \ell$. As it is easy to check $(D_f - \bar{q}s) \mod l$ is also fixed under the action of the Frobenius automorphism, i.e. $(D_f - \bar{q}s) \mod l$ is the difference set D_f^0 we are looking for.
The difference set D_f^0 is well defined and unique up to multiplication with integers $t \in (\mathbb{Z}/\ell\mathbb{Z})^*$. In fact, if we choose another Frobenius difference set $D'_f = \{d'_1, \dots, d'_q\}$ we can write it as $D'_f = (t \cdot D_f + r) \mod l$, $r, t \in \mathbb{Z}/\ell\mathbb{Z}$, $(t, \ell) = 1$ and we have

$$\sum_{i=1}^{q} d'_i = \sum_{i=1}^{q} (td_i + r) = q \cdot r + t \cdot \sum_{i=1}^{q} d_i \,.$$

We define $s' := \sum_{i=1}^{q} d'_i = (q \cdot r + t \cdot \sum_{i=1}^{q} d_i) = t \cdot s + q \cdot r$ and, as in the case of D_f, we obtain the Frobenius difference set $D'_f - \bar{q}s'$ for which the sum of the elements is equal to zero. It holds

$$\begin{aligned} D'_f - \bar{q}s' &= t \cdot D_f + r - \bar{q}(t \cdot s + q \cdot r) \\ &= t \cdot D_f + r - \bar{q} \cdot t \cdot s - r \\ &= t \cdot (D_f - \bar{q} \cdot s) \\ &= t \cdot D_f^0 \,. \end{aligned}$$

Thus D_f^0 is unique up to multiplication with integers $t \in (\mathbb{Z}/\ell\mathbb{Z})^*$. □

Example 13. We consider the projective plane $\mathbb{P}^2(\mathbb{F}_7)$ with $\ell = 57$, $q = 8$. The Frobenius automorphism generates the cyclic group Φ_3.
The difference set

$$D_3 = \{0, 4, 11, 20, 25, 26, 28, 38\} \mod 57$$

is fixed under the action of the multiplier $p = 7$ of the group Φ_3 thus a Frobenius difference set. For the elements $d_i \in D_3$ we have

$$\sum_{i=1}^{8} d_i = 152 \equiv 38 \mod 57 \,.$$

In $\mathbb{Z}/57\mathbb{Z}$ the integer $\bar{q} = 50$ is such that

$$50 \cdot 8 \equiv 1 \mod 57 \,.$$

Thus the Frobenius difference set

$$\begin{aligned} D_3^0 &= (D_3 - 50 \cdot 38) \mod 57 \\ &= \{1, 6, 7, 9, 19, 38, 42, 49\} \mod 57 \end{aligned}$$

is such that the sum of its elements is congruent $0 \mod 57$. Also the sum of the elements belonging to each other difference set $t \cdot D_3^0 \mod 57$, $t \in (\mathbb{Z}/57\mathbb{Z})^*$ is congruent to $0 \mod 57$, as it is easy to check.

For the other Frobenius difference sets we obtain:

Corollary 3.3.3. *Under the conditions of Proposition 3.3.2 and of Corollary 3.2.5 all Frobenius difference sets can be written as shifts*

$$D_f^j \equiv D_f^0 + j \cdot s_2 \mod \ell \ , \qquad \ell = s_2 \cdot k \, , \quad j \in \{0, 1, \ldots, (k-1)\} \tag{3.4}$$

and

$$\sum_{i=1}^{q} d_i = q \cdot j \cdot s_2 \mod \ell \ , \quad d_i \in D_f^j \tag{3.5}$$

Each shift D_f^j is unique up to multiplication with integers $t \in (\mathbb{Z}/\ell\mathbb{Z})^*$.

Proof. For each Frobenius difference set Equation (3.4) follows directly from Proposition 3.3.2 and from Corollary 3.2.5.
Equation (3.5) holds since:

$$\sum_{i=1}^{q} d_i = \sum_{i=1}^{q} (d_i' + j \cdot s_2) = q \cdot j \cdot s_2 \mod \ell \ , \quad d_i' \in D_f^0.$$

From Proposition 3.2.1 it follows that each D_f^j is unique up to multiplication with integers $t \in (\mathbb{Z}/\ell\mathbb{Z})^*$. □

Remark. Since D_f^0 is unique up to muliplication with integers $t \in (\mathbb{Z}/\ell\mathbb{Z})^*$ (see Proposition 3.3.2) each $t \cdot D_f^0$ is a Frobenius difference set which can be used to number the points on the fixed hyperplane h_0. Thus each shift $t \cdot D_f^0 + j \cdot s_2$ is a suitable Frobenius difference set to number the points on a fixed hyperplane $h_{j \cdot s_2}$.
Usually we have

$$(t \cdot D_f^0 + i \cdot s_2) \mod \ell \not\equiv (t' \cdot D_f^0 + i \cdot s_2) \mod \ell \quad \text{for } t \mod \ell \neq t' \mod \ell \, .$$

Equality holds if t and t' correspond to multipliers $p^k \mod l$, $k \in \mathbb{Z}/f\mathbb{Z}$ (see Corollary 3.2.2).

Example 14. For the projective plane $\mathbb{P}^2(\mathbb{F}_7)$ of Example 13 we have $l = 57 = 19 \cdot 3$. Since $gcd(p-1, \ell) = gcd(6, 57) = 3$ all fixed Frobenius difference sets can be written as:

$$t \cdot D_3^0 + k \cdot 19 \ , \quad t \in (\mathbb{Z}/57\mathbb{Z})^* \ , \quad k \in \{0, 1, 2\} \, .$$

According to our results it is natural to number the points on the fixed hyperplane h_0 with the Frobenius difference sets D_f^0. The points on each other fixed hyperplane $h_{j \cdot s_2}$, $j \in \{0, \ldots, (k-1)\}$ can be numbered using the shifts

$$D_f^j \equiv D_f^0 + j \cdot s_2 \ .$$

Chapter 4

Finite Projective Spaces and Dessins d'Enfants

Dessin d'enfants may be defined as bipartite graphs embedded in Riemann surfaces, each dessin defining in a unique way the surface of the embedding. In the first section of this chapter we shortly report some important facts about dessins d'enfants on Riemann surfaces. In the following sections, relying on and extending some results of Streit and Wolfart [SW01], we thus explain how we may construct bipartite graphs illustrating the incidence structure of points and hyperplanes belonging to projective spaces $\mathbb{P}^m(\mathbb{F}_n)$. The embeddings of such graphs in Riemann surfaces results in dessin d'enfants. Among them we especially concentrate on so-called **Wada dessins**.

4.1 Introducing Dessins d'Enfants

The term **dessins d'enfants** was first used by Grothendieck (1984) to refer to objects which are very simple but important to describe compact Riemann surfaces as smooth algebraic curves.

Dessins d'enfants $\mathcal{D}$ can be defined as hypermaps on compact orientable surfaces. A hypermap in its **Walsh representation** [Wal75] is a bipartite graph drawn without crossings on a surface X and cutting the surface into simply connected cells (faces). For a vertex of the graph we denote with **valency** the number of edges incident with it. For a cell the valency is the number of edges on its boundary. The edges have to be counted twice, if they border the cell at both sides (see [SW01] and [LZ04]). A characterising property of dessins is the signature $< p, q, r >$, where

1. p is the l.c.m. of all valencies of the white vertices,
2. q is the l.c.m. of all valencies of the black vertices,
3. $2r$ is the l.c.m. of all valencies of the cells.

A dessin is called **uniform** if all white vertices have the same valency p, all black vertices have the same valency q and all cells have the same valency $2r$. The existence of dessins on Riemann surfaces is an important property. In fact, a dessin with signature $< p, q, r >$ embedded in a surface X determines in a unique way the complex structure of the surface. According to uniformization theory (see, for instance, [Wol06] and [WJ06] for a survey) each Riemann surface can be expressed as a quotient of its universal covering space U by a group Γ. The covering space U corresponds either to the Riemann sphere $\widehat{\mathbb{C}} = \mathbb{P}^1(\mathbb{C})$, or to the Gauss plane $\mathbb{C}$ or to the hyperbolic plane $\mathbb{H}$. The group Γ is the covering group of the covering map:

$$f : U \longrightarrow \Gamma \backslash U \cong X \ .$$

In the special case of uniform dessins the group Γ is a torsion-free subgroup of a triangle group Δ acting discontinuously on U and having the presentation

$$\Delta =< \gamma_0, \gamma_1, \gamma_\infty | \gamma_0^p = \gamma_1^q = \gamma_\infty^r = \gamma_0\gamma_1\gamma_\infty = 1 > \ .$$

The integers p, q, r are related to the covering space U in the following way:

1. $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1 \implies U = \widehat{\mathbb{C}}$,
2. $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1 \implies U = \mathbb{C}$,
3. $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1 \implies U = \mathbb{H}$.

In the case of our dessins associated with projective spaces we will see (see Section 6.3.3) that we always have $U = \mathbb{H}$.
In this case, the dessin $\mathcal{D}$ on X can be identified with the Γ-quotient of the tessellation of the hyperbolic plane $\mathbb{H}$ given by the fundamental region of Δ and by its Δ-images on $\mathbb{H}$. With the covering map:

$$f : \mathbb{H} \longrightarrow \Gamma/\mathbb{H} \cong X$$

we, in fact, "project" the tesselllation of $\mathbb{H}$ onto $\mathcal{D}$. The vertices of $\mathcal{D}$ are points, the edges are curves on the surface X.
Furthermore, the existence of a uniform dessin $\mathcal{D}$ embedded in the surface X implies that there exists a meromorphic function

$$\beta : \ X \longrightarrow \widehat{\mathbb{C}}$$

ramified at most over three points of the Riemann sphere. It corresponds to the covering map:

$$\beta : \Gamma \backslash \mathbb{H} \longrightarrow \Delta \backslash \mathbb{H} \ ,$$

where we have the identification $\widehat{\mathbb{C}} \cong \Delta\backslash\mathbb{H}$ (see [Wol06]). Whithout loss of generality the three ramification points of the covering map may be identified with $\{0, 1, \infty\}$. The preimages of 0 and 1 are, respectively, the set of white and black vertices of the bipartite graph on X. The preimages of ∞ correspond to the cell midpoints.
According to Belyĭ's theorem a surface for which such a covering map β (Belyĭ function) exists may be defined over $\overline{\mathbb{Q}}$. Thus we have a dessin on a surface if and only if we may describe it with equations whose coefficients are in the field $\overline{\mathbb{Q}}$.
The automorphism group of the dessin $\mathcal{D}$ on $X = \Gamma\backslash\mathbb{H}$ is a subgroup of the automorphism group of the surface and is expressed by the quotient

$$Aut(\mathcal{D}) = N_\Delta(\Gamma)/\Gamma \ ,$$

where $N_\Delta(\Gamma)$ is the normalizer of Γ in Δ.
If we have not only a uniform but even a **regular** dessin, we have

$$Aut(\mathcal{D}) = \Delta/\Gamma$$

and Γ is a normal subgroup of Δ. In this case $Aut(\mathcal{D})$ acts transitively on the edges of the underlying dessin. Regular dessins are very useful since in this case it is much easier to relate the combinatorial properties of the embedded dessin to the algebraic properties of the surface of the embedding. It is, for instance, possible to describe more closely the defining equation, the moduli field and the definition field (see, for instance, the recent work of Jones, Streit and Wolfart [JSW10]) of the surface of the embedding.

4.2 Dessins d'Enfants associated with Projective Spaces

If we consider Singer's construction again (see Chapter 2.3.1) it turns out that for a projective plane $\mathbb{P}^2(\mathbb{F}_n)$ a line l_w (which we can identify with the wth column of the matrix given in (2.4)) is incident with a point P_b if $b - w \equiv d_i \mod \ell$, where d_i is an element of the corresponding difference set

$$D = \{d_1, \ldots, d_q\} \mod \ell\,.$$

Since Singer's construction is extendable to points P_b and dual hyperplanes h_w belonging to projective spaces $\mathbb{P}^m(\mathbb{F}_n)$, we also have P_b and h_w incident if $b - w \equiv d_i \mod \ell$. Knowing this relation, we can construct a bipartite graph $\mathcal{G}$ illustrating the incidence pattern of points and dual hyperplanes. The embedding of $\mathcal{G}$ in a Riemann surface is then a dessin d'enfant associated with $\mathbb{P}^m(\mathbb{F}_n)$.
First of all, since we can have more than one difference set with parameters ℓ and q and since for every difference set D shifts $\mod \ell$, multiplications with integers $t \mod \ell$, $(t, \ell) = 1$ and permutations of the elements are still suitable difference sets, we fix one difference set D and one ordering of its elements, unique up to cyclic permutations. For every other D with every possible ordering of its elements the construction of the graph will be the same, but in general we obtain a different embedding into an orientable surface and a different Belyĭ function.
We introduce the following conventions:

point	black vertex •
hyperplane	white vertex ◦
incidence	joining edge —

Table 4.1: *Conventions.*

Identifying each point and each hyperplane with its index b or w we then choose the local incidence pattern given in Figure 4.1 [1]. Here the black vertices are represented by the points and the white vertices are represented by the hyperplanes. The embedding of the bipartite graph into an orientable surface can now be constructed. Without loss of generality we start with the white vertex w_0 and we construct the cells around it beginning with the incident edge $\{w_0, w_0 + d_i\}$. Thus according to the local incidence pattern of the black and of the white vertices we have chosen (see Figure 4.1), the next incident edge going clockwise around a cell is

[1] We remark here that this is not the only possible incidence pattern we may choose. Here the white vertices incident with a black vertex are ordered anticlockwise and the black vertices incident with a white one are ordered clockwise. We have chosen these orderings since we are interested in special uniform dessins called **Wada dessins** wich we will introduce later on in this chapter and which are one of the main topic of study of this thesis.
The choice of different orderings is also possible and give rise to dessins of different type (see for instance the construction of uniform dessins sketched in Section 6.2).

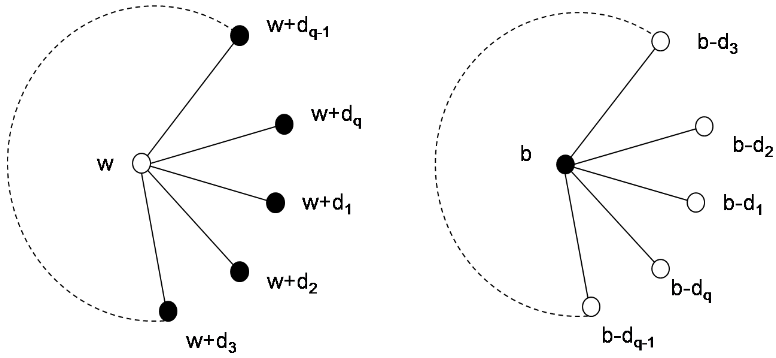


Figure 4.1: *Local incidence pattern.*

$\{w_0 + d_i, w_0 + d_i - d_{i+1}\}$ followed by $\{w_0 + d_i - d_{i+1}, w_0 + 2d_i - d_{i+1}\}$. Repeating the same construction, we obtain a cell with the following sequence of edges on it (see Figure 4.2):

$$\begin{aligned}
&\{w_0, w_0 + d_i\},\\
&\{w_0 + d_i, w_0 + d_i - d_{i+1}\},\\
&\{w_0 + d_i - d_{i+1}, w_0 + 2d_i - d_{i+1}\},\\
&\{w_0 + 2d_i - d_{i+1}, w_0 + 2(d_i - d_{i+1})\},\\
&\qquad\vdots\\
&\{\underbrace{w_0 + k_0 d_i - (k_0 - 1)d_{i+1}}_{w_0+d_{i+1}}, \underbrace{w_0 + k_0(d_i - d_{i+1})}_{w_0}\}\ .
\end{aligned} \tag{4.1}$$

Here we reach the starting edge after $2k_0$ steps for a minimal k_0 such that $k_0 \cdot (d_i - d_{i+1}) \equiv 0 \mod \ell$. This means that the cell we have constructed has valency $2k_0$ with k_0 black and k_0 white vertices on its boundary. The next cells are constructed in the same way starting with the edges

$$\{w_0, w_0 + d_{i+1}\}, \{w_0, w_0 + d_{i+2}\}, \dots, \{w_0, w_0 + d_{i+q-1}\}.$$

Depending on the values of differences $d_i - d_{i+1}$ of consecutive elements of D, we then obtain cells with valencies $2k_t$, $t = 0, \dots, N-1$, $N := \#$ cells. In general, some of the k_t's will be equal but not all of them, except for special cases (see next section).

We repeat the same construction for the next white vertices until each of them is

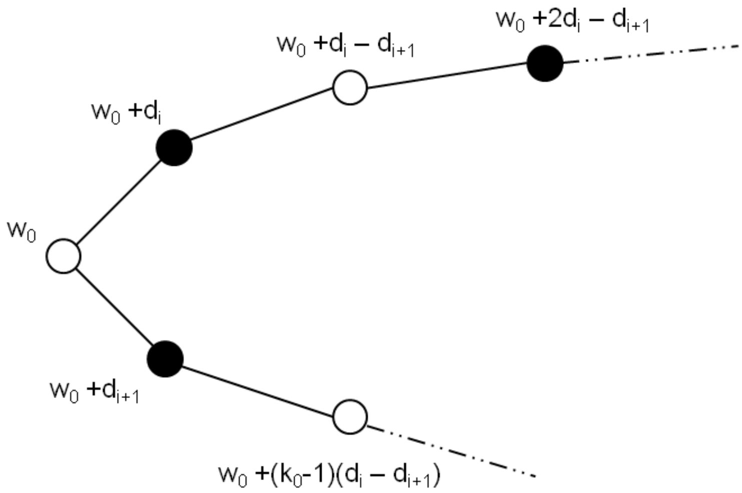


Figure 4.2: *Construction of a cell incident with* w_0.

surrounded by q black vertices [2] or until the sum of all the cell valencies divided by two is equal to $q \cdot \ell$. Since, in fact, q points lie on each hyperplane, we have a total of $q \cdot \ell$ incidence relations between the white and the black vertices. These relations are represented by the edges of the bipartite graph and since, for construction reasons, each relation is represented twice (by one edge of type ○—● and by one edge of type ●—○) we should divide the sum of all the cell valencies by two. At last, we obtain a dessin embedded in a Riemann surface 'gluing' together edges describing the same incidence relation. The dessin is a $< q, q, r >$-dessin with black and white vertices of the same valency q. The integer $2r$ is the l.c.m. of all valencies of the cells. The vertices and the edges of the bipartite graph are points and curves on the surface the graph is embedded in. According to the Euler formula the genus of the surface can be computed in the following way:

$$\begin{aligned} 2 - 2g &= \#vertices - \#edges + \#cells \\ &= 2\ell - q\ell + N \,. \end{aligned} \tag{4.2}$$

In general it is difficult to express the number of resulting cells in terms of the numbers q and ℓ, nevertheless this is possible in some special cases (see next section).

[2] For reasons of duality between hyperplanes (white vertices) and points (black vertices), we do not need to repeat the construction for the black vertices: if all white vertices are surrounded by q black vertices, then, by duality, all black vertices are surrounded by q white vertices.

Example 15. For the projective space $\mathbb{P}^3(\mathbb{F}_2)$ we may construct an associated dessin using the difference set:

$$D = \{8, 2, 10, 1, 5, 4, 0\} \mod 15 \ .$$

The dessin has signature $< 7, 7, 30 >$ with five cells of valency 30 and six cells of valency 10. The cells of smaller valency are a consequence of the fact that two differences of consecutive elements of D are not prime to 15, in fact, we have $(8-2) = 6$ and $(10-1) = 9$. According to the Euler formula, the genus of the surface the dessin is embedded in is 93.

4.3 Wada Dessins

We now consider a special case of the construction above.
Suppose that we can find at least one cyclic ordering of the elements of D such that all differences $d_i - d_{i+1}$ are prime to ℓ. In this case, it is easy to see that all cells of the dessin have the same valency 2ℓ. The dessin is therefore uniform with signature $< q, q, \ell >$ and with q cells. According to the Euler formula the genus of the Riemann surface the dessin is embedded in is thus given by

$$2 - 2g = 2\ell - q\ell + q \ . \tag{4.3}$$

Such dessins have the following nice property. On the boundary of each cell each white and each black vertex with a given index occurs precisely once. If two white vertices had the same index, then according to the incidence pattern in Figure 4.1 and to the construction described above we should have

$$w + \alpha \cdot (d_i - d_{i+1}) \equiv w + \beta \cdot (d_i - d_{i+1}) \ , \quad \alpha, \beta \in \mathbb{Z}/\ell\mathbb{Z} \ ,$$

but this is possible only for $\alpha \equiv \beta \mod \ell$ since differences $(d_i - d_{i+1})$ are prime to ℓ. The same can be proven for the black vertices. This property was first described by Streit and Wolfart [SW01] for bipartite graphs of projective planes $\mathbb{P}^2(\mathbb{F}_n)$ and is called **Wada property**. According to the authors we call **Wada dessins** those dessins resulting from embeddings of bipartite graphs with the Wada property. These dessins are by construction always uniform.
We give here the following definition of **Wada compatible** orderings of the elements of a difference set D associated with a projective space $\mathbb{P}^m(\mathbb{F}_n)$:

Definition 4.3.1. We call cyclic orderings of the q elements of a difference set D associated with a projective space $\mathbb{P}^m(\mathbb{F}_n)$ **Wada compatible** if differences $\mod \ell$ of consecutive elements d_i, d_{i+1} of D are prime to ℓ, i.e.:

$$((d_i - d_{i+1}), \ell) = 1 \ , \qquad \forall d_i, d_{i+1} \in D \qquad (\textbf{Wada condition}) \ . \tag{4.4}$$

Example 16. For the Fano plane $\mathbb{P}^2(\mathbb{F}_2)$ we can construct a $< 3, 3, 7 >$ $-$Wada dessin using the difference set

$$D = \{1, 2, 4\} \mod 7 \,.$$

Figure 4.3 and Figure 4.4 illustrate the dessin with corresponding edges marked by a cross. In the case of $\mathbb{P}^2(\mathbb{F}_2)$ since $\ell = 7$ is prime, each ordering of the elements of D gives rise to a uniform Wada dessin with signature $< 3, 3, 7 >$. These dessins are well studied examples of dessins embedded in Klein's quartic (see [Sin86]).

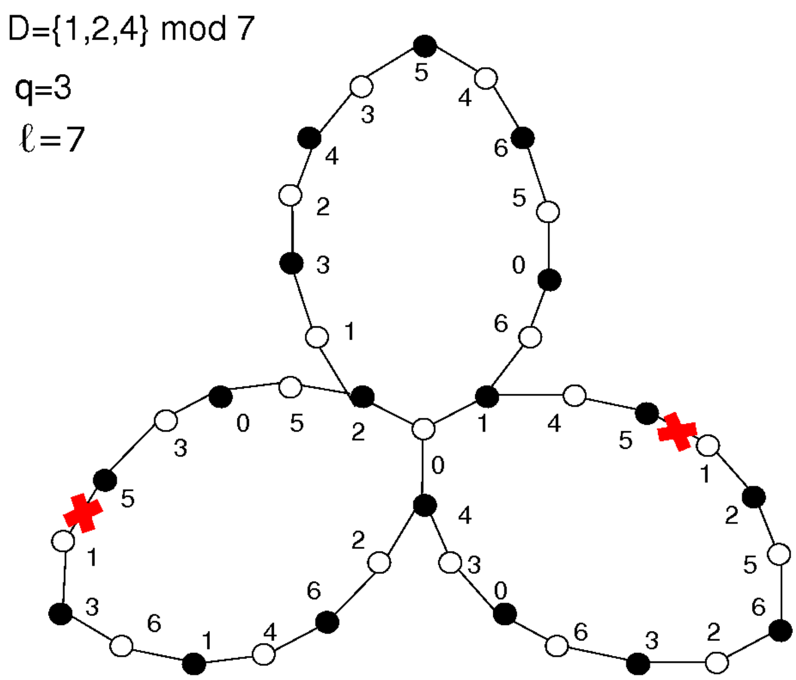


Figure 4.3: *Wada Dessin with signature* $< 3, 3, 7 >$ *associated with the Fano plane. The embedding of the underlying graph is obtained 'gluing' together correspondig edges. As an example, two corresponding edges are marked by a cross.*

Unfortunately, it is not always possible to permute the elements of a difference set D in such a way that we obtain a Wada dessin. For instance, it is a known fact (see [SW01]) that for the difference set associated with the projective plane $\mathbb{P}^2(\mathbb{F}_4)$

$$D = \{3, 6, 7, 12, 14\} \mod 21$$

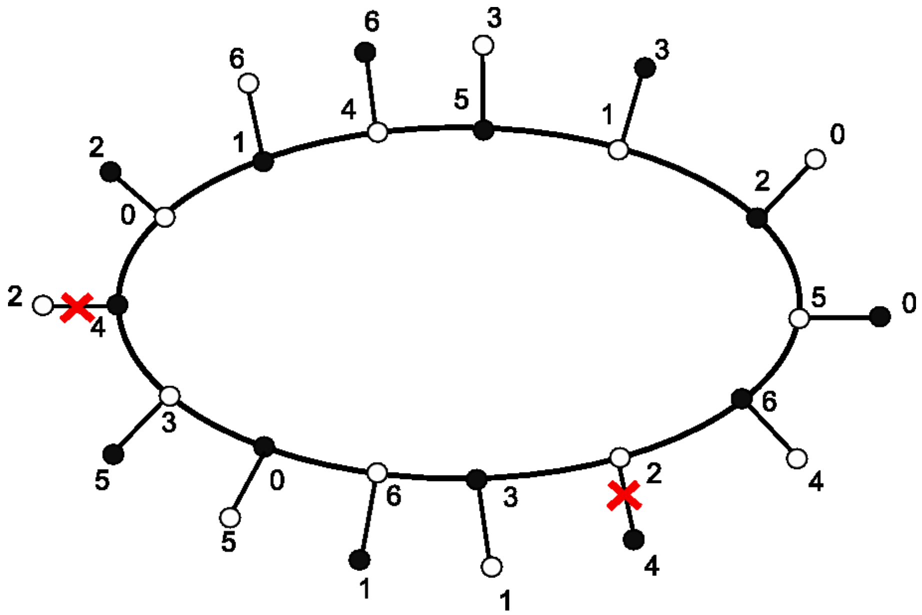


Figure 4.4: *Cell of the* $< 3, 3, 7 >$*-Wada dessin associated with the Fano plane. To obtain the other cells we 'glue' together corresponding edges not lying on the boundary of the cell sketched. As an example, two corresponding edges are marked by a cross.*

there is no suitable ordering of the elements such that we obtain a uniform Wada dessin.
Finally, our considerations about the construction of dessins show that not only different difference sets but also a single difference set can lead to the construction of very different dessins associated with a projective space $\mathbb{P}^m(\mathbb{F}_n)$. The resulting dessin depends on the ordering we choose for the elements of the difference set.

Chapter 5

Automorphism Groups

In this chapter we consider the groups of automorphisms acting on $< q, q, \ell >$-Wada dessins $\mathcal{D}$. They are associated with projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ with parameters $\ell = \frac{n^{m+1}-1}{n-1}$ and $q = \frac{n^m-1}{n-1}$ (see Section 2.1) and constructed as described in Section 4.2. The Singer group Σ_ℓ results to be always a group of automorphims acting by a cyclic permutation of the vertices on the cell boundaries. A second group $\Phi_f \cong Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$ generated by the Frobenius automorphism σ (see Section 3.1) turns out to be a group of automorphisms of the Wada dessins only for special choices of the underlying difference set D. As it is quite "cumbersome" to deal with the more general case of dessins associated with projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ with arbitrary parameters m and n, we first concentrate on the special and more interesting case of projective spaces for which n and $m+1$ are prime numbers. We discuss the general case later on in this chapter.

5.1 The Singer Group

As we have seen (see Section 2.3) every projective space $\mathbb{P}^m(\mathbb{F}_n)$ with parameters $q = \frac{n^m-1}{n-1}$ and $\ell = \frac{n^{m+1}-1}{n-1}$ admits a cyclic transitive group of collineations, the Singer group Σ_ℓ. We now consider dessins $\mathcal{D}$ associated with $\mathbb{P}^m(\mathbb{F}_n)$ and constructed as described in Section 4.2. We formulate the following proposition which generalizes results of Streit and Wolfart (see [SW01]):

Proposition 5.1.1. *Let $\mathcal{D}$ be the dessin associated with a projective space $\mathbb{P}^m(\mathbb{F}_n)$ and constructed as described in Section 4.2. The Singer group Σ_ℓ acts as an automorphism group of the dessin transitively permuting the set of the white vertices and the set of the black vertices on the boundary of every cell iff $\mathcal{D}$ is a $< q, q, \ell >$-Wada dessin. The edges belonging to each cell are subdivided into two orbits of length ℓ.*

Proof. We first prove the "if" direction of the proposition.
If $\mathcal{D}$ is a Wada dessin, then every white and black vertex lies on the boundary of every cell. The Singer group Σ_ℓ acts transitively on the points and hyperplanes of $\mathbb{P}^m(\mathbb{F}_n)$ (see Section 2.3). Recall that the black and the white vertices are numbered with integers $b, w \in \mathbb{Z}/\ell\mathbb{Z}$ given by the exponents of a generator $g \in \mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$ (see Section 2.3). The generator is related to the points and to the hyperplanes of $\mathbb{P}^m(\mathbb{F}_n)$ in the following way:

$$P_b \longleftrightarrow g^b \;, \quad h_w \longleftrightarrow g^w \;.$$

For each element $\gamma^i \in \Sigma_\ell$ we have:

$$\begin{aligned} \gamma^i : \quad & P_b \longmapsto P_{b+i} \\ & h_w \longmapsto h_{w+i} \;. \end{aligned}$$

This means that the action on the black and on the white vertices of $\mathcal{D}$ is a shift of the corresponding indices. Since every vertex of each colour lies on the boundary of every cell, Σ_ℓ transitively permutes the vertices on the boundary of the cells. The Singer group Σ_ℓ is a group of collineations of $\mathbb{P}^m(\mathbb{F}_n)$, so it preserves incidence. The property of incidence is described in the dessin via a joining edge between a black and a white vertex. It follows that the action on the vertices induces an action of Σ_ℓ on the edges of every cell.
Let $\{b, w\}$ and $\{w, b'\}$ be two contiguous edges on the boundary of a cell (see Figure 5.1). Due to their action on the vertices elements $\gamma^i \in \Sigma_\ell$ act on the edges in the following way:

$$\begin{aligned} \gamma^i : \quad \{b, w\} \quad &\longmapsto \quad \{b+i, w+i\} \;, \\ \{w, b'\} \quad &\longmapsto \quad \{w+i, b'+i\} \;. \end{aligned}$$

Since the cyclic group Σ_ℓ acts transitively on the vertices of each colour it follows that we are back to the starting edge $\{b, w\}$ or $\{w, b'\}$ after ℓ steps. In fact, the dessin $\mathcal{D}$ has the Wada property. To the orbit of $\{b, w\}$ only belong edges of type $\bullet\!\!-\!\!-\!\!\circ$, to the orbit of $\{w, b'\}$ only belong edges of type $\circ\!\!-\!\!-\!\!\bullet$. Thus it follows that the set of edges on the boundary of every cell is subdivided by Σ_ℓ into two orbits of length ℓ.
The other direction can be proved in a short way.

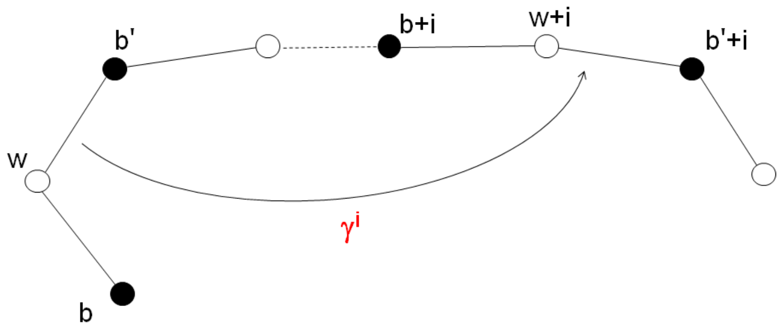


Figure 5.1: *Action of the Singer group on the edges of the cells.*

If Σ_ℓ acts transitively on the black and on the white vertices of every cell, this means that every white and every black vertex lies on the boundary of every cell. And this is exactly the Wada property. □

5.2 The Frobenius Automorphism

In Chapter 3 we have studied the cyclic group Φ_f generated by the Frobenius automorphism of a finite field $\mathbb{F}_{n^{m+1}}$. In particular, we have studied its relation to difference sets and block designs associated with projective spaces $\mathbb{P}^m(\mathbb{F}_n)$. We have seen that in contrast to the Singer group, Φ_f is not always a group of automorphisms of the block design associated with $\mathbb{P}^m(\mathbb{F}_n)$. Only for block designs contructed using difference sets of special type, that we have called Frobenius difference sets, Φ_f is a group of automorphisms. Now we consider dessins associated with projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ and constructed using Frobenius difference sets D_f (see Section 3.2). We are interested in the conditions on n under which we can construct dessins with Φ_f as a group of automorphisms. First of all we formulate two lemmas.

Lemma 5.2.1. *Let f be the order of the cyclic group $\Phi_f \cong Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$ generated by the Frobenius automorphism acting on a projective space $\mathbb{P}^m(\mathbb{F}_n)$ with $n = p^e, e \in \mathbb{N}\backslash\{0\}$. Let f be prime, thus we have:*

$$n = p\ , \quad f = m+1\ , \quad \Phi_f \cong Gal(\mathbb{F}_{p^{m+1}}/\mathbb{F}_p)\ . \tag{5.1}$$

If $p \not\equiv 0,\ 1 \mod (m+1)$, then f divides the valency q of the white and of the black vertices.

Proof. The proof follows from Fermat's little theorem.
For $n = p$ the integer q is given by:

$$q = \frac{p^m - 1}{p - 1} \ ,$$

so $f = m + 1$ divides q if

$$p^m \equiv 1 \mod (m+1) \ ,$$

and this is true due to Fermat's little theorem since we have chosen $p \not\equiv 0 \mod (m+1)$.
Now we need the denominator not to 'destroy' the divisibility property. In fact, we have to choose

$$p \not\equiv 1 \mod (m+1) \ ,$$

since for $p \equiv 1 \mod (m+1)$ we obtain:

$$q = p^{m-1} + \ldots + 1 \equiv m \mod (m+1)$$

and $\gcd(m, (m+1)) = 1$. □

Remark. For $m = 2$ we may even have $f = q$. In fact, since we have $p \equiv 2 \mod 3$, exactly for $p = 2$ we obtain $f = m + 1 = 3 = p + 1 = q$. The projective plane satisfying these conditions is the Fano plane $\mathbb{P}^2(\mathbb{F}_2)$.
For $m = 2$ we also have $f = q$ for the projective plane $\mathbb{P}^2(\mathbb{F}_8)$. Here we have $f = 3^2 = \frac{8^2-1}{8-1} = q$.
These two planes are well studied cases of projective spaces for which we are able to construct regular Wada dessins associated (see [Sin86], [Whi95]). Among all projective spaces they are the only two with this characteristic (see [SW01] and [Dem97, Section 1.4]).

Lemma 5.2.2. *We consider the Frobenius difference set D_f fixed by the cyclic group Φ_f. Under the conditions of Lemma 5.2.1 on f and n, no shifts of D_f are fixed by Φ_f and the following properties hold:*

1. $0 \notin D_f$ *and*
2. *all Φ_f-orbits of elements $d_i \in D_f$ have length f.*

Proof. As we have seen in Corollary 3.2.2 the cyclic group Φ_f acts on the elements of D_f by multiplication with powers of p and it divides the elements into orbits whose lengths are divisors of f. Since f is prime, we will only have orbits of length 1 or of length f. Suppose we have at least one orbit of length 1. Since f divides q (see Lemma 5.2.1 above), we necessarily have at least $f - 1$ other orbits of length

1. Let $0 \in D_f$ and let $\{0\}$ be an orbit of length 1.
Recalling some ideas of Baumert [Bau71] about projective planes, we first show that $(p-1, \ell) = 1$.
Dividing ℓ by $p-1$ we obtain:

$$\ell = (p-1)(p^{m-1} + \ldots + (m-1)p + m) + (m+1)\,.$$

We know

$$(p-1, m+1) = 1$$

due to $p \not\equiv 1 \mod (m+1)$ and to $m+1$ being prime. From the Euclidean algorithm it therefore follows that

$$(p-1, \ell) = 1\,.$$

The first consequence of this fact is that no shifts other than $D_f + 0$ are fixed by Φ_f (see Proposition 1.1.3). The difference set D_f is therefore unique up to multiplication with integers $k \in \mathbb{Z}/\ell\mathbb{Z}, (k, \ell) = 1$ (see Section 1.1). Now if at least $(f-1)$ elements $d_i \in D_f$ with $d_i \not\equiv 0 \mod \ell$ were fixed by p, then they should satisfy the congruence relation:

$$p \cdot d_i \equiv d_i \mod \ell \implies (p-1) \cdot d_i \equiv 0 \mod \ell\,.$$

Since $(p-1, \ell) = 1$, the congruence above cannot be satisfied for $d_i \not\equiv 0 \mod \ell$. This means that $\{0\}$ is the only possible orbit of length 1 under the action of p. Nevertheless we must exclude it, since in this case f would not divide q.
It thus follows that $0 \notin D_f$ and that D_f is decomposed only into Φ_f-orbits of length f. □

Remark. As remarked above, for the Fano plane $\mathbb{P}^2(\mathbb{F}_2)$ we have $f = 3 = q$. Let $D_3 = \{1, 2, 4\} \mod 7$ be the Frobenius difference set fixed by the cyclic group Φ_3. Under the action of Φ_3 the difference set D_3 consists of only one orbit and it is easy to see that Φ_3 acts transitively on its elements.

We now consider special orderings of the elements of a Frobenius difference set D_f with arbitrary f and we formulate the following

Definition 5.2.3. Consider the following cyclic orderings of the q elements of a Frobenius difference set D_f:

$$\begin{aligned} D_f =& \{d_1, \ldots, d_k,\ p^j d_1, \ldots, p^j d_k,\ \ldots\ldots\ldots, p^{(f-1)j} d_1, \ldots, p^{(f-1)j} d_k\}\,, \\ & \text{for some } j \in (\mathbb{Z}/f\mathbb{Z})^*,\ \frac{q}{f} = k\,. \end{aligned} \tag{5.2}$$

We call such orderings **Frobenius compatible** orderings.

Moreover since also Wada compatibility is needed for the construction of Wada dessins we formulate:

Proposition 5.2.4. *The elements of a Frobenius difference set D_f ordered in a Frobenius compatible way are also ordered in a Wada compatible way iff differences of consecutive elements belonging to the subset $\{d_1, \ldots, d_k\}$ are prime to ℓ, i.e.:*

$$(d_i - d_{i+1}, \ell) = 1 \ \forall i \in \{1, \ldots, k-1\} \tag{5.3}$$

and

$$\big(d_k - p^j d_1, \ell\big) = 1\,. \tag{5.4}$$

Proof. If the elements of D_f ordered in a Frobenius compatible way also satisfy the Wada condition, then conditions (5.3) and (5.4) necessarily hold.
If condition (5.3) holds then we also have

$$\big(p^j(d_i - d_{i+1}), l\big) = 1\ , \qquad \forall j \in (\mathbb{Z}/f\mathbb{Z})^* \tag{5.5}$$

since $\ell = \frac{n^{m+1}-1}{n-1} = n^m + n^{m-1} + \ldots + 1$ with $n = p^e$ not divisible by p. This means that all differences of consecutive elements belonging to a subset $\{p^j d_1, \ldots, p^j d_k\}$ are prime to ℓ, i.e. they satisfy the Wada condition. Conditon (5.4) is then necessary to make sure that when passing from one subset to the next the Wada condition also holds. If (5.4) holds then for the same reasons as in (5.5) we also have:

$$(p^{(h)j} d_k - p^{(h+1)j} d_1), \ell) = 1\ , \qquad \forall h \in \mathbb{Z}/f\mathbb{Z}\,.$$

□

With the elements of D_f ordered in a Frobenius compatible way, we obtain the local incidence pattern of each black and white vertex described by Figure (5.2).
For the projective spaces we have considered in the Lemmas 5.2.1 and 5.2.2 we get:

Corollary 5.2.5. *Under the conditions of Lemma 5.2.1, the elements of a Frobenius difference set D_f fixed by the cyclic group Φ_f may be ordered in a Frobenius compatible way. This ordering is fixed under the action of Φ_f up to cyclic permutations.*

Thus we may finally construct a set of Wada dessins with the property to have Φ_f as a group of automorphisms:

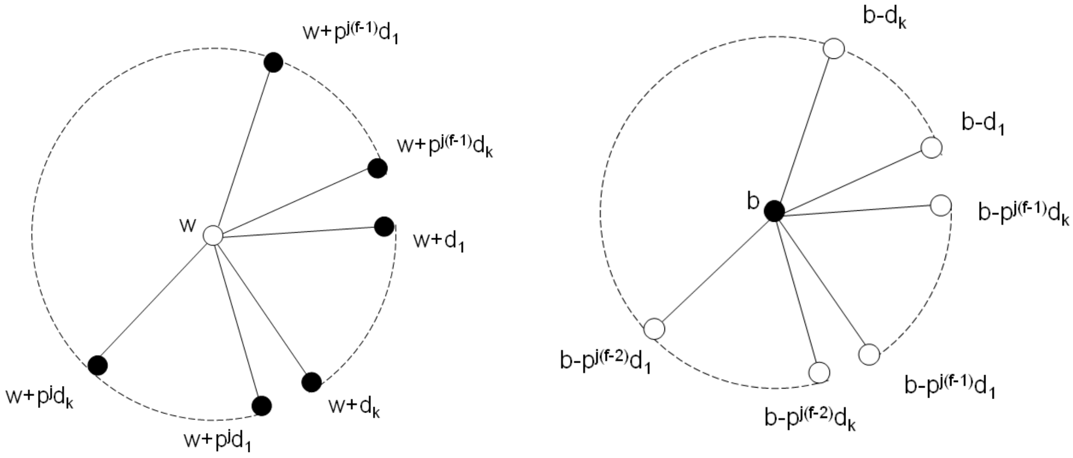


Figure 5.2: *Local incidence patterns with Frobenius compatible ordering of the elements of D_f.*

Proposition 5.2.6. *Let $\Phi_f \cong Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$ be the cyclic group generated by the Frobenius automorphism acting on a projective space $\mathbb{P}^m(\mathbb{F}_n)$. Let f be prime, $p \not\equiv 0, 1 \mod (m+1)$. Let D_f be a Frobenius difference set fixed by Φ_f whose elements are ordered in a Frobenius compatible way. If the elements of D_f are also ordered in a Wada compatible way so that we can construct a $< q, q, \ell >$-Wada dessin $\mathcal{D}$, then Φ_f is a group of automorphisms of $\mathcal{D}$ acting freely on the edges and rotating the set of cells around the vertices $b = w = 0$ fixed by Φ_f.*

Proof. We suppose that at least one Frobenius compatible ordering of the elements of D_f is also Wada compatible and we construct a $< q, q, \ell >$-Wada dessin $\mathcal{D}$. Since $f|q$ (see Lemma 5.2.1 above), Φ_f has a suitable size to be a group of automorphisms acting on the q cells of $\mathcal{D}$. The cyclic group $\sigma \in \Phi_f$ is generated by the Frobenius automorphism.

We consider the action of $\sigma \in \Phi_f$ on the points and on the hyperplanes of $\mathbb{P}^m(\mathbb{F}_n)$ and therefore on the vertices of $\mathcal{D}$. As we have seen in Section 2.3, we may write points P_b and dual hyperplanes h_w as powers of a generator g of $\mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$:

$$P_b \leftrightarrow g^b\,,\ \ h_w \leftrightarrow g^w \quad \text{with} \quad b, w \in \mathbb{Z}/\ell\mathbb{Z},\ \ell = \frac{n^{m+1}-1}{n-1}\,.$$

The Frobenius automorphism acts on $g^i \in \mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$ as:

$$\sigma :\ g^i \longmapsto g^{ip}\,,$$

therefore on the points and on the hyperplanes it acts as:

$$\begin{aligned} \sigma : \quad P_b &\longmapsto P_{pb} \\ h_w &\longmapsto h_{pw}. \end{aligned}$$

According to the notation introduced in Definition 5.2.3, we write the edges of $\mathcal{D}$ as $e^w_{\nu,i} = \{w, w{+}p^\nu d_i\}$ (○—●) and $e^b_{\nu,i} = \{b, b{-}p^\nu d_i\}$ (●—○) with $\nu \in \mathbb{Z}/f\mathbb{Z}$, $i \in \{0, \ldots, k-1\}$. The action of σ on the edges is given by:

$$\begin{aligned} \sigma : e^w_{\nu,i} = \{w, w + p^\nu d_i\} &\longmapsto p \cdot e^w_{\nu,i} = \{p \cdot w, p(w + p^\nu d_i)\} \ , \\ e^b_{\nu,i} = \{b, b - p^\nu d_i\} &\longmapsto p \cdot e^b_{\nu,i} = \{p \cdot b, p(b - p^\nu d_i)\} \ . \end{aligned}$$

If w and b are not fixed under the action of Φ_f, then none of the edges $e^w_{\nu,i}$ and $e^b_{\nu,i}$ is fixed by σ. If, on the contrary, w and b are fixed, then $\sigma(e^w_{\nu,i}) \neq e^w_{\nu,i}$ and $\sigma(e^b_{\nu,i}) \neq e^b_{\nu,i}$ only if d_i is not fixed by p. Indeed, this is true, otherwise we could not have chosen D_f with a Frobenius compatible ordering of its elements. Thus Φ_f does not fix any of the edges and its action is free.
We now consider the action of Φ_f on the set of cells around the vertices w and b of $\mathcal{D}$ which are fixed by Φ_f. Since Φ_f only fixes the difference set D_f (see Lemma 5.2.2), this means that it only fixes the vertices $b = w = 0$ of the dessin. In fact, according to Singer's construction (see Section 2.3), elements of difference sets D associated with projective spaces correspond to indices of points on hyperplanes (and by duality of hyperplanes through points). As D_f is the only difference set fixed by Φ_f, only h_0 and P_0 are fixed by Φ_f, from which it follows that $w = b = 0$ are the only vertices fixed by Φ_f.
Without loss of generality we consider the cells around $w = 0$ (see Figure 5.2 with $w = 0$). We have the following action of σ:

$$\begin{array}{ccccc} \{0, p^\nu d_i\}, & \{p^\nu d_i, p^\nu(d_i - d_{i+1})\}, & \{p^\nu(d_i - d_{i+1}), p^\nu(2d_i - d_{i+1})\}, & \ldots, & \{p^\nu d_{i+1}, 0\} \\ & & \downarrow \sigma & & \\ \{0, p^{1+\nu} d_i\}, & \{p^{1+\nu} d_i, p^{1+\nu}(d_i - d_{i+1})\}, & \{p^{1+\nu}(d_i - d_{i+1}), p^{1+\nu}(2d_i - d_{i+1})\}, & \ldots, & \{p^{1+\nu} d_{i+1}, 0\} \\ & & & & i = 1, \ldots, (k-1) \end{array} \tag{5.6}$$

and

$$\begin{array}{ccccc} \{0, p^\nu d_k\}, & \{p^\nu d_k, p^\nu(d_k - p^j d_1)\}, & \{p^\nu(d_k - p^j d_1), p^\nu(2d_k - p^j d_1)\}, & \ldots, & \{p^{j\nu} d_1, 0\} \\ & & \downarrow \sigma & & \\ \{0, p^{1+\nu} d_k\}, & \{p^{1+\nu} d_k, p^{1+\nu}(d_k - p^j d_1)\}, & \{p^{1+\nu}(d_k - p^j d_1), p^{1+\nu}(2d_k - p^j d_1)\}, & \ldots, & \{p^{1+j\nu} d_1, 0\} \end{array} \tag{5.7}$$

Thus, more in general, the action of σ on the cells $\mathcal{C}_c$, $c \in \mathbb{Z}/q\mathbb{Z}$ around $w = 0$ results in a mapping of every cell to a following cell (see Figure 5.3) such that:

$$\begin{aligned} &\sigma : \mathcal{C}_c \longmapsto \mathcal{C}_{c+mk \mod q}, \\ &m \in \mathbb{Z}/f\mathbb{Z} \ , k = \frac{q}{f} \ . \end{aligned}$$

We obtain the following relation between powers of p and the cells we run through:

p-powers	cells
p^0	$\mathcal{C}_c$
p^1	$\mathcal{C}_{c+mk \mod q}$
p^2	$\mathcal{C}_{c+2mk \mod q}$
p^3	$\mathcal{C}_{c+3mk \mod q}$
$\vdots$	$\vdots$
p^{f-1}	$\mathcal{C}_{c+(f-1)mk \mod q}$

Evidently, σ describes a rotation of the set of cells around 0. The order of the rotation is f. □

Remarks. 1. From the proof of Proposition 5.2.6 it is clear that we have to choose Frobenius compatible orderings of the elements of D_f. In fact, if we choose different orderings, the action of Φ_f on the cells of $\mathcal{D}$ is no longer a dessin

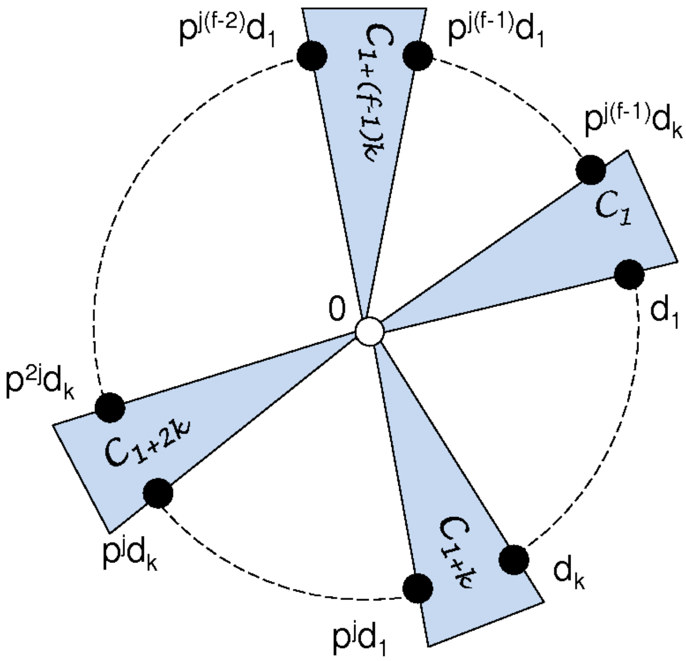


Figure 5.3: *Local ordering of the cells around $w = 0$ with a Frobenius difference set D_f. The elements of D_f are ordered in a Frobenius compatible way.*

automorphism.

2. A further consequence of the above proof is that Φ_f acts freely not only on the edges but also on the cells and it divides them into k orbits of length f. In the special case of the Fano plane $\mathbb{P}^2(\mathbb{F}_2)$, Φ_3 acts transitively on the edges and on the cells of the corresponding $< 3, 3, 7 >$-Wada dessin. All the cells belong to one orbit of length $f = q = 3$.

3. We consider the vertices fixed by Φ_f as fixed points x on the target surface X of the embedding. Then introducing local coordinates z we may suppose that $z(x) = 0$ and that Φ_f acts on a neighbourhood of $z = 0$ by multiplication with powers of a root of unity ζ_f:

$$z \longmapsto \zeta_f^a z \,, \quad a \in \mathbb{Z}/f\mathbb{Z} \,.$$

ζ_f is called the **multiplier** of the automorphism $\sigma \in \Phi_f$ on X (see [SW01]). We point out that the multipliers we consider here are not to be confused with the multipliers of the difference sets we have introduced in Section 1.1.1.

Example 17. For the projective space $\mathbb{P}^4(\mathbb{F}_2)$ we have $f = m + 1 = 5$. Thus f satisfies the conditions of Proposition 5.2.6. To $\mathbb{P}^4(\mathbb{F}_2)$ belong $\ell = 31$ points and, by duality, of $\ell = 31$ hyperplanes. Each point is contained in 15 hyperplanes, each hyperplane contains 15 points.
We may choose the following Frobenius difference set (see [Bau71])

$$D_5 = \{1, 3, 15, 2, 6, 30, 4, 12, 29, 8, 24, 27, 16, 17, 23\} \mod 31 \tag{5.8}$$

to describe the incidence pattern of points and hyperplanes. The set D_5 is unique up to multiplication with integers $k \in (\mathbb{Z}/31\mathbb{Z})^*$ (see Lemma 5.2.2).
The ordering of the elements of D_5 is Frobenius compatible as can easily be proved. Choosing the local incidence pattern for black and white vertices given in Figure 5.2, we construct the dessin associated with $\mathbb{P}^4(\mathbb{F}_2)$ as described in Chapter 4. The dessin has signature $< 15, 15, 31 >$ and is uniform with the Wada property. In particular, for $\mathbb{P}^4(\mathbb{F}_2)$ every Frobenius compatible ordering of the elements of D_5 is also Wada compatible since $\ell = 31$ is prime. For all Wada dessins constructed using these orderings Φ_5 is a group of automorphisms acting freely on the edges and on the cells. On the cells it acts with a rotation by the angle $\omega = \frac{2\pi}{5}$ around the fixed vertices $b = w = 0$. The cells are subdivided into three orbits of length 5. Other examples of projective spaces whose parameters satisfy the conditions of

	q	ℓ	f	Wada dessin	Φ_f
$\mathbb{P}^2(\mathbb{F}_5)$	6	31	3	$< 6, 6, 31 >$	$\Phi_3 \cong \mathrm{Gal}(\mathbb{F}_{5^3}/\mathbb{F}_5)$
$\mathbb{P}^4(\mathbb{F}_2)$	15	31	5	$< 15, 15, 31 >$	$\Phi_5 \cong \mathrm{Gal}(\mathbb{F}_{2^5}/\mathbb{F}_2)$
$\mathbb{P}^4(\mathbb{F}_3)$	40	$121 = 11^2$	5	$< 40, 40, 121 >$	$\Phi_5 \cong \mathrm{Gal}(\mathbb{F}_{3^5}/\mathbb{F}_3)$
$\mathbb{P}^4(\mathbb{F}_7)$	400	2801	5	$< 400, 400, 2801 >$	$\Phi_5 \cong \mathrm{Gal}(\mathbb{F}_{7^5}/\mathbb{F}_7)$
$\mathbb{P}^6(\mathbb{F}_2)$	63	127	7	$< 63, 63, 127 >$	$\Phi_7 \cong \mathrm{Gal}(\mathbb{F}_{2^7}/\mathbb{F}_2)$
$\mathbb{P}^6(\mathbb{F}_3)$	364	1093	7	$< 364, 364, 1093 >$	$\Phi_7 \cong \mathrm{Gal}(\mathbb{F}_{3^7}/\mathbb{F}_3)$
$\mathbb{P}^6(\mathbb{F}_5)$	3906	19531	7	$< 3906, 3906, 19531 >$	$\Phi_7 \cong \mathrm{Gal}(\mathbb{F}_{5^7}/\mathbb{F}_5)$
$\mathbb{P}^6(\mathbb{F}_{11})$	177156	$1948717 = 43 \cdot 45319$	7	$< 177156, 177156, 1948717 >$(?)	$\Phi_7 \cong \mathrm{Gal}(\mathbb{F}_{11^7}/\mathbb{F}_{11})$
$\mathbb{P}^{10}(\mathbb{F}_2)$	1023	$2047 = 23 \cdot 89$	11	$< 1023, 1023, 2047 >$(?)	$\Phi_{11} \cong \mathrm{Gal}(\mathbb{F}_{2^{11}}/\mathbb{F}_2)$
$\mathbb{P}^{10}(\mathbb{F}_3)$	29524	$88573 = 23 \cdot 3851$	11	$< 29524, 29524, 88573 >$(?)	$\Phi_{11} \cong \mathrm{Gal}(\mathbb{F}_{3^{11}}/\mathbb{F}_3)$

(?) = only if a Frobenius compatible ordering exists which is also Wada compatible.

Table 5.1: *Some projective spaces whose parameters satisfy the conditions of Proposition 5.2.6.*

the Proposition above are given in Table 5.1. For some of the listed spaces the total number ℓ of points (and of hyperplanes) is not prime. Thus we have to check whether Frobenius compatible orderings of the elements of the underlying difference set are also Wada compatible. According to Proposition 5.2.4, we only need to check differences of elements belonging to the first block and the one difference of elements at the 'transition' between the first and the second block. Other differences are multiplications with powers of the prime p for which we have $(\ell, p) = 1$.
For these spaces the prime factors of the integer ℓ are only few and quite big. For instance, for the spaces $\mathbb{P}^4(\mathbb{F}_3)$, $\mathbb{P}^{10}(\mathbb{F}_2)$ we have $\ell = 121 = 11 \cdot 11$ and $\ell = 2047 = 89 \cdot 23$, so it is very likely to find Frobenius and, at the same time, Wada compatible orderings. For $\mathbb{P}^4(\mathbb{F}_3)$ it is easy to check that the ordering of the elements of the following difference set (see [Bau71]) is Frobenius and Wada compatible.

$$D_5 = \{1, 4, 7, 11, 13, 34, 25, 67, 3, 12, 21, 33, 39, 102, 75, 80, 9, 36, 63, 99, 117, 64, 104, 119\\ 27, 108, 68, 55, 109, 71, 70, 115, 81, 82, 83, 44, 85, 92, 89, 103\} \mod 121\,.$$

In this case, the group generated by the Frobenius automorphism is cyclic of order five and it divides the elements of D_5 into eight orbits of length five.

The problem of determining under which conditions we can order the elements of a difference set in a Wada compatible way is still an open question. For planar difference sets associated with projective planes $\mathbb{P}^2(\mathbb{F}_n)$ it has been discussed in [SW01], [Goe05] and more recently in [Goe09].

5.3 The Full Automorphism Group

After considering the Singer group Σ_ℓ and the cyclic group Φ_f generated by the Frobenius automorphism, we are now interested in determining the full automorphism group of a Wada dessin $\mathcal{D}$ constructed under the conditions of Proposition 5.2.6. This means that the dessin is associated with a projective space $\mathbb{P}^m(\mathbb{F}_p)$ with $f = m+1$ prime, $p \not\equiv 0, 1 \mod m+1$ and it is constructed using a Frobenius difference set D_f with its elements ordered in a Frobenius and in a Wada compatible way.

At first, we look at the normaliser of Σ_ℓ in the collineation group $P\Gamma L(m+1,p)$ of the projective space $\mathbb{P}^m(\mathbb{F}_p)$. Since p is prime, from the considerations in Section 2.2 it follows that $P\Gamma L(m+1,p) = PGL(m+1,p)$ and from Huppert ([Hup79, Section II.7]) we know that the normaliser of Σ_ℓ in $PGL(m+1,p)$ is expressed by:

$$N_{PGL(m+1,p)}(\Sigma_\ell) = \Phi_f \ltimes \Sigma_\ell \ , \quad f = m+1 \ . \tag{5.9}$$

Now, as we have seen in Proposition 5.1.1 the action of the Singer group Σ_ℓ is geometrically a permutation of the edges on the boundary of each cell. The cyclic group Φ_f rotates the cells around the fixed points. We combine the actions of Σ_ℓ and Φ_f and we apply to a cell $\mathcal{C}$ a rotation $\alpha(\mathcal{C}) = \mathcal{C}'$, $\alpha \in \Phi_f$, followed by a permutation of the edges of $\mathcal{C}'$ by $\gamma \in \Sigma_\ell$. Thus applying again the same rotation in the opposite direction, i.e. $\alpha^{-1}(\gamma(\mathcal{C}'))$, we obtain a permutation of the edges of the original cell $\mathcal{C}$ by an element $\gamma' \in \Sigma_\ell$. If we consider the group generated by Σ_ℓ and Φ_f, which acts on $\mathcal{D}$ it therefore turns out that it is a semidirect product $\Phi_f \ltimes \Sigma_\ell$, which is indeed the normaliser of Σ_ℓ in $P\Gamma L(m+1,p) = PGL(m+1,p)$, as we have seen above. We show:

Proposition 5.3.1. *Under the conditions of Proposition 5.2.6 the full automorphism group of the* $< q, q, \ell >$*-Wada dessin* $\mathcal{D}$ *is the semidirect product* $\Phi_f \ltimes \Sigma_\ell$ *which acts freely (and even transitively for* $f = q$*) on the edges.*

Proof. The semidirect product $\Phi_f \ltimes \Sigma_\ell$ is a group of automorphisms of $\mathcal{D}$ due to Proposition 5.1.1 and 5.2.6 and to the geometrical considerations above. Since both

Φ_f and Σ_ℓ do not fix any of the edges of $\mathcal{D}$ and Φ_f acts freely on the cells and Σ_ℓ acts transitively on the edges of type •—○ and of type ○—• on the boundary of each cell, the action of $\Phi_f \ltimes \Sigma_\ell$ is also free. It is even transitive for $f = q$. In this case it is clear that $\Phi_f \ltimes \Sigma_\ell$ is not only a group of automorphisms but it is the full automorphism group of $\mathcal{D}$. The dessin $\mathcal{D}$ is then said to be regular (see Section 4.1). For the more general case with $f \neq q$, the group $\Phi_f \ltimes \Sigma_\ell$ is still the full automorphism group since it is the normaliser of Σ_ℓ in $P\Gamma L(m+1, p)$ as we have seen above. Let us suppose that another group $\Phi_{f'} \in P\Gamma L(m+1, p)$ exists with $\Phi_f \subset \Phi_{f'}$ which acts by rotating the cells of $\mathcal{D}$ around the fixed points. The group acts on the Singer group Σ_ℓ in the same way as Φ_f does due to the same geometrical reasons. So the group generated by $\Phi_{f'}$ and Σ_ℓ is a semidirect product $\Phi_{f'} \ltimes \Sigma_\ell$. It would therefore mean that $\Phi_{f'} \ltimes \Sigma_\ell$ with $\Phi_f \ltimes \Sigma_\ell \subset \Phi_{f'} \ltimes \Sigma_\ell$ is the normaliser of Σ_ℓ in $P\Gamma L(m+1, p)$, but this is a contradiction to the fact that the normaliser of Σ_ℓ in $P\Gamma L(m+1, p)$ cannot be larger than $\Phi_f \ltimes \Sigma_\ell$. □

Example 18. We consider again the $< 15, 15, 31 >$-Wada dessin $\mathcal{D}$ associated with $\mathbb{P}^4(\mathbb{F}_2)$ and constructed using the Frobenius difference set D_5 given in (5.8). As we have seen, the cyclic group Φ_5 acts freely on the cells of the dessin. It rotates them around the vertex $w = 0$ which is fixed under the action of Φ_5. The Singer group Σ_{31} permutes the edges on the boundary of every cell. So the semidirect product $\Phi_5 \ltimes \Sigma_{31}$ is the full automorphism group of $\mathcal{D}$ and is, in fact, the normaliser of Σ_{31} in $P\Gamma L(5, 2) = PGL(5, 2)$.

Corollary 5.3.2. *Under the conditions of Proposition 5.2.6, if the elements of D_f are chosen in a Wada but not in a Frobenius compatible order, then the full automorphism group of the $< q, q, \ell >$-Wada dessin $\mathcal{D}$ is the Singer group Σ_ℓ.*

Proof. As we have seen in the Remarks following Proposition 5.2.6, if the ordering of the elements of D_f is not Frobenius compatible then the cyclic group generated by the Frobenius automorphism Φ_f is no longer a group of automorphisms of $\mathcal{D}$. Recall that the order f of Φ_f is prime. Now, suppose that a group $\Phi_{f'} \subset P\Gamma L(m+1, p)$ exists with $f' \mid q$, $(f', f) = 1$ which is a group of automorphisms of $\mathcal{D}$ acting by rotating the cells around the vertices it fixes. The group generated by $\Phi_{f'}$ and Σ_ℓ is a group of automorphisms of $\mathcal{D}$ and is equal to $\Phi_{f'} \ltimes \Sigma_\ell$ for the same geometrical considerations as for Φ_f. Since $\Phi_{f'} \not\subset \Phi_f$ this would imply that the normaliser of Σ_ℓ in $P\Gamma L(m+1, p)$ is the semidirect product of the group generated by $\Phi_{f'}$ and Φ_f with Σ_ℓ. But this is a contradiction to the fact that $N_{P\Gamma L(m+1,p)}(\Sigma_\ell) = \Phi_f \ltimes \Sigma_\ell$. This means that, if Φ_f is not a group of automorphisms of $\mathcal{D}$, the full automorphism group is the Singer group Σ_ℓ. □

Example 19. For all possible orders of D_5 in (5.2) which are not Frobenius compatible we obtain dessins associated with $\mathbb{P}^4(\mathbb{F}_2)$ still having the Wada property. In fact, $\ell = 31$ which is prime. For all these dessins Σ_{31} is the full automorphism group.

5.4 Generalizations

We consider projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ with parameters m and $n = p^e$ which do not necessarily satisfy the conditions of Proposition 5.2.6, and, if it is possible, we construct the associated Wada dessins in the way described in Chapter 4. It is much more difficult to determine explicitly the full automorphism group of these dessins, but it is possible to make some statements about its structure and its size.
First of all, we consider the normaliser of the Singer group Σ_ℓ in the collineation group $P\Gamma L(m+1, n)$ of the projective space $\mathbb{P}^m(\mathbb{F}_n)$ and we formulate the following:

Proposition 5.4.1. *The normaliser of the Singer group Σ_ℓ in $P\Gamma L(m+1, n)$, $n = p^e$, is*

$$N_{P\Gamma L(m+1,n)}(\Sigma_\ell) = \Phi_{e(m+1)} \ltimes \Sigma_\ell \tag{5.10}$$

with $\Phi_{e(m+1)} \cong Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$.

Proof. According to [Hup79, Section II.7], we know that the normaliser of Σ_ℓ in $PGL(m+1, n)$ is

$$N_{PGL(m+1,n)}(\Sigma_\ell) = \Phi_{m+1} \ltimes \Sigma_\ell \ ,$$

with $\Phi_{m+1} \cong Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_n)$.
Since $(P\Gamma L(m+1, n) : PGL(m+1, n)) = e$ (see Chapter 3) we also have

$$\big(N_{P\Gamma L(m+1,n)}(\Sigma_\ell) : N_{PGL(m+1,n)}(\Sigma_\ell)\big) \leq e \ .$$

Equality holds if we can prove that $\Phi_{e(m+1)} \cong Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$ normalises Σ_ℓ i.e.

$$N_{P\Gamma L(m+1,n)}(\Sigma_\ell) = \Phi_{e(m+1)} \ltimes \Sigma_\ell \ .$$

Let Φ_e be the Galois group $Gal(\mathbb{F}_n/\mathbb{F}_p)$ generated by the Frobenius automorphism σ (see Chapter 3)

$$\begin{array}{rccc} \sigma : & \mathbb{F}_n & \longrightarrow & \mathbb{F}_n \ , \\ & a & \longmapsto & a^p \ . \end{array}$$

The action of Φ_e can be extended in a natural way to the elements of $\mathbb{F}_{n^{m+1}}$ and the group $\Phi_{e(m+1)}$ generated this way is then cyclic of order $f = e \cdot (m+1)$. It

corresponds to the Galois group $\Phi_{e(m+1)} \cong Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$.
The subgroup Φ_{m+1} of $\Phi_{e(m+1)}$ is the Galois group $Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_n)$ generated by σ^e (see [Wol96]).
That $\Phi_{e(m+1)}$ normalises Σ_ℓ can be seen as follows. For $c^j \in \Sigma_\ell$, $g^i \in \mathbb{F}^*_{n^{m+1}}$, $\sigma^k \in \Phi_{e(m+1)}$ we have:

$$\begin{aligned} \sigma^{-k} c^j \sigma^k (g^i) &= \sigma^{-k} c^j (g^{ip^k}) \\ &= \sigma^{-k}(g^{ip^k+j}) \\ &= g^{i+p^{-k}j} \\ &= c^{j'}(g^i)\,, \qquad \text{with}\, j' = p^{-k} j \mod \ell\,. \end{aligned} \tag{5.11}$$

Therefore we obtain $\sigma^{-k} c^j \sigma^k = c^{j'}, \forall j \in \mathbb{Z}/\ell\mathbb{Z}$.
Equality between j and j' cannot occur unless $k \equiv e{\cdot}(m{+}1)$. In fact, if $j' \equiv j \mod \ell$, then we should have:

$$p^{-k} j \equiv j \mod \ell\,.$$

Since $gcd(p, \ell) = 1$ due to $\ell = \frac{n^{m+1}-1}{n-1}$ the congruence above is satisfied only for

$$p^k \equiv 1 \mod \ell\,,$$

and, since we have $\Phi_{e(m+1)} \cong Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$, this is possible only for $k \equiv 0 \mod e \cdot (m+1)$. It follows that the cyclic group $\Phi_{e(m+1)}$ normalises Σ_ℓ in $P\Gamma L(m+1, n)$ and we have $N_{P\Gamma L(m+1,n)}(\Sigma_\ell) = \Phi_{e(m+1)} \ltimes \Sigma_\ell$. □

From now on let $\mathcal{D}$ be a Wada dessin associated with a projective space $\mathbb{P}^m(\mathbb{F}_n)$. Let Φ_f be the cyclic group generated by the Frobenius automorphism acting on the elements of $\mathbb{P}^m(\mathbb{F}_n)$ and let Σ_ℓ be the Singer group.
We formulate a definition and give some conditions on subgroups $\Phi_g \subseteq \Phi_f$ to be groups of automorphisms of $\mathcal{D}$. We extend Definition 5.2.3 in the following way:

Definition 5.4.2. Let D_g be a difference set associated with a projective space $\mathbb{P}^m(\mathbb{F}_n)$ and fixed under the action of a subgroup $\Phi_g \subseteq \Phi_f$, generated by a power σ^s of the Frobenius automorphism with $s \in \mathbb{Z}/f\mathbb{Z}$, $s \not\equiv 0 \mod f$, $s \cdot g \equiv 0 \mod f$. We consider the following cyclic orderings of elements of D_g:

$$\begin{aligned} D_g = &\{d_1, \ldots, d_k,\ t^j d_1, \ldots, t^j d_k,\ \ldots\ldots\ldots, t^{(g-1)j} d_1, \ldots, t^{(g-1)j} d_k\}\,, \\ &\text{for some } j \in (\mathbb{Z}/g\mathbb{Z})^*,\ t = p^s,\ \frac{q}{g} = k\,. \end{aligned}$$

We define them as compatible with the action of the group Φ_g.

Proposition 5.2.4 can easily be generalized to subgroups $\Phi_g \subseteq \Phi_f$:

Proposition 5.4.3. *Let D_g be a difference set defined as in Definition 5.4.2. The elements of D_g are also ordered in a Wada compatible way iff differences of consecutive elements belonging to the subset $\{d_1, \dots, d_k\}$ are prime to ℓ, i.e.:*

$$(d_i - d_{i+1}, \ell) = 1 , \qquad \forall i \in \{1, \dots, k-1\} \tag{5.12}$$

and

$$\big(d_k - t^j d_1, \ell\big) = 1 . \tag{5.13}$$

Proof. See the proof of Proposition 5.2.4 with p replaced by t and f replaced by g. □

Proposition 5.4.4. *Let $\mathcal{D}$ be a Wada dessin associated with a projective space $\mathbb{P}^m(\mathbb{F}_n)$ and let Φ_f, $f = e \cdot (m+1)$, be the cyclic group generated by the Frobenius automorphism σ. Let Φ_g be a subgroup of Φ_f with generator σ^s, $s \cdot g \equiv 0 \mod f$. The action of σ^s on the black and on the white vertices of the dessin $\mathcal{D}$ is described by a multiplication with a multiplier $p^s = t$. Thus Φ_g is a group of automorphisms rotating the set of cells around the fixed vertices of $\mathcal{D}$ if*

1. *g divides the valency q of the white and of the black vertices and $(t-1, \ell) = 1$,*
2. *the dessin $\mathcal{D}$ can be constructed using a difference set D_g fixed by Φ_g and with its elements ordered in a way compatible with the action of Φ_g.*

The difference set D_g fixed by Φ_g is unique up to mutliplication with integers $u \in (\mathbb{Z}/\ell\mathbb{Z})^*$.

Proof. If according to (1.) the order of Φ_g divides q, then Φ_g has a suitable size to be a group of automorphisms of $\mathcal{D}$ acting on the set of cells. If moreover we have $(t-1, \ell) = 1$, then exactly one difference set D_g exists which is fixed under the action of Φ_g (see Proposition 1.1.3 and Proposition 1.1.4) but not elementwise. Its elements are subdivided by Φ_g into orbits of length g. In fact, due to $(t-1, \ell) = 1$ for each element $d_i \in D_g$ the congruence

$$(t-1)d_i \equiv 0 \mod \ell ,$$

is satisfied only for $d_i \equiv 0 \mod \ell$. Nevertheless, we may not have $d_i \equiv 0 \mod \ell$ in D_g, otherwise D_g would consist of orbits of elements with length g and of one orbit of length 1. This would be a contradiction to the fact that g divides q.
Under these conditions it follows that none of the edges of $\mathcal{D}$ is fixed by a non-trivial

element of Φ_g, so Φ_g acts freely on them.
Since the elements of D_g are subdivided by Φ_g into $\frac{q}{g}$ orbits of length g, we can order its elements in a way compatible with the action of Φ_g. Moreover, if this ordering is also Wada compatible, we can construct a Wada dessin $\mathcal{D}$. We claim that Φ_g acts on the set of cells of $\mathcal{D}$ by rotating them around the fixed vertices. Without loss of generality we consider the cells incident with $w = 0$. For the proof we only need to replace in (5.6) and in (5.7) σ with σ^s and p with t and continue with the proof in the same way as we did for Proposition 5.2.6. Finally, we may conclude that Φ_g is a group of automorphisms of $\mathcal{D}$ acting by rotating the set of cells around the fixed vertices. □

Corollary 5.4.5. *Under the conditions of Proposition 5.4.4 if Φ_g is a group of automorphisms of $\mathcal{D}$ then the non-trivial elements of Φ_g and even of Φ_f fix only one hyperplane h_0 (one point P_0) of the projective space $\mathbb{P}^m(\mathbb{F}_n)$.*

Proof. As we have seen with Proposition 5.4.4, the difference set D_g is the only set fixed by Φ_g. Since $\Phi_g \subseteq \Phi_f$ the set of difference sets fixed by Φ_g is larger or equal to the set fixed by Φ_f. It directly follows that D_g is also the only difference set fixed by Φ_f.
As we have seen in Chapter 3, the elements d_i of D_g can be considered as the indices of the points on the hyperplane h_0 of $\mathbb{P}^m(\mathbb{F}_n)$ or by duality of the hyperplanes containing the point P_0. Since there is only one difference set fixed by Φ_g and by Φ_f, it follows that a consequence of Φ_g being a group of automorphisms of $\mathcal{D}$ is that the non-trivial elements of Φ_g and of Φ_f fix only one hyperplane h_0 and one point P_0 of $\mathbb{P}^m(\mathbb{F}_n)$. □

We conclude with a lemma and a proposition about the full automorphism group $Aut(\mathcal{D})$ of Wada dessins:

Lemma 5.4.6. *Let $\mathcal{D}$ be a $< q, q, \ell >$-Wada dessin associated with a projective space $\mathbb{P}^m(\mathbb{F}_n)$, $n = p^e$. Let Σ_ℓ be its Singer group and let Φ_f with $f = e \cdot (m + 1)$ be the cyclic group generated by the Frobenius automorphism. We consider the subgroup Φ_k of Φ_f, such that k is the g.c.d. of f and of the valency q of each white and of each black vertex of $\mathcal{D}$. Let $\Phi_g \subseteq \Phi_k$ be the largest subgroup satisfying the conditions of Proposition 5.4.4. Thus we have*

$$\Phi_g \ltimes \Sigma_\ell \subseteq Aut(\mathcal{D}) \ . \tag{5.14}$$

Proof. As we have seen in Proposition 5.1.1 the group Σ_ℓ is a group of automorphisms of $\mathcal{D}$.

Now let k be the g.c.d. of f and q and let Φ_k be the cyclic group of order k contained in Φ_f. Since $k|q$, each $\Phi_g \subseteq \Phi_k$ has a suitable size to be a group of automorphisms of $\mathcal{D}$.
We now consider that Φ_g with maximal order g, which satisfies the conditions of Proposition 5.4.4.
It is a group of automorphisms of $\mathcal{D}$ and it acts by rotating the set of cells around the fixed vertices $b = w = 0$, which are unique as a consequence of Corollary 5.4.5.
The group generated by Φ_g and by the Singer group Σ_ℓ is the semidirect product $\Phi_g \ltimes \Sigma_\ell$ for the same geometrical reasons we explained in Section 5.3. Since condition (1.) of Proposition 5.4.4 is only sufficient but not necessary, it is possible that a larger group $\Phi_{g'}$ with $\Phi_g \subset \Phi_{g'} \subseteq \Phi_k$ exists fixing the difference set $D_{g'}$ and subdividing its elements into orbits of the same length g'. The group $\Phi_{g'}$ also acts on the set of cells by rotating them around the fixed vertices $b = w = 0$.
Due to $N_{P\Gamma L(m+1,n)}(\Sigma_\ell) = \Phi_f \ltimes \Sigma_\ell$ (see Lemma 5.4.1) it thus follows

$$Aut(\mathcal{D}) \cong \Phi_{g'} \ltimes \Sigma_\ell$$

and for the group $\Phi_g \ltimes \Sigma_\ell$ we necessarily have

$$\Phi_g \ltimes \Sigma_\ell \subset Aut(\mathcal{D}) \ .$$

Equality holds in the special case of $\Phi_g = \Phi_{g'}$. □

Proposition 5.4.7. *Under the conditions of Lemma 5.4.6 the full automorphism group of a* $< q, q, \ell >$*-Wada dessin* $\mathcal{D}$ *is given by:*

$$Aut(\mathcal{D}) \cong \Phi_{g'} \ltimes \Sigma_\ell \tag{5.15}$$

where $\Phi_{g'} \subseteq \Phi_f$*, the order* g' *of* $\Phi_{g'}$ *being a divisor of the valency* q *of the vertices of* $\mathcal{D}$*.*

Proof. The fact that the order of $\Phi_{g'}$ must be a divisor of q has been already proved by Streit and Wolfart for projective planes $\mathbb{P}^2(\mathbb{F}_n)$ (see [SW01]). Here we extend their result to projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ with $m \geq 2$.
The proof follows directly from the proof of Lemma 5.4.6. □

Remark. Lemma 5.4.6 and Proposition 5.4.7 do not exclude the possibility that $g' = 1$. This may happen if

1. $(q, f) = 1$;

2. $(q, f) \neq 1$ but there are no subgroups $\Phi_{g'} \subseteq \Phi_f$ which subdivide the elements of the fixed difference sets $D_{g'}$ into orbits of the same length g';

3. $(q, f) \neq 1$ and there are subgroups $\Phi_{g'} \subseteq \Phi_f$ which subdivide the elements of the fixed difference sets $D_{g'}$ into orbits of the same length. Nevertheless, for the construction of the dessin $\mathcal{D}$ we choose element orderings which are Wada compatible, but they are not compatible with the action of any $\Phi_{g'}$ (see Definition 5.4.2).

In these cases the Singer group Σ_ℓ is the full automorphism group.

5.4.1 Special Cases

In this section we consider some projective spaces $\mathbb{P}^m(\mathbb{F}_n)$, $n = p^e$, with m, n and $\ell = \frac{n^{m+1}-1}{n-1}$ of special type, such that it is possible to describe the full automorphism group more precisely. As usual, we identify Φ_f, $f = e \cdot (m+1)$ with the cyclic group generated by the Frobenius automorphism acting on the elements of $\mathbb{F}_{n^{m+1}}$. The group Σ_ℓ is the Singer group transitively permuting the vertices of one colour on the boundary of the cells of a Wada dessin associated with the space $\mathbb{P}^m(\mathbb{F}_n)$. The valency of the vertices of each colour is q.

Projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ with $m + 1$ prime

Suppose that we have a projective space $\mathbb{P}^m(\mathbb{F}_n)$ with $m + 1$ prime, $n = p^e$ with $e \neq 1$. Let Φ_{m+1} be a cyclic subgroup of Φ_f. If $n \not\equiv 0, 1 \mod (m + 1)$ then we can easily prove that the Lemmas 5.2.1 and 5.2.2 hold. In each proof we only need to replace p with n and Φ_f with Φ_{m+1}. We therefore have that

1. $m + 1$ divides the valency q of each black and white vertex of the dessin associated with $\mathbb{P}^m(\mathbb{F}_n)$;

2. the elements of the difference set D_{m+1} fixed by Φ_{m+1} are subdivided by Φ_{m+1} only into orbits of length $m + 1$.

As a consequence of these facts, we can order the elements of D_{m+1} in a way compatible with the action of Φ_{m+1}. If this ordering is also Wada compatible, we can construct a $< q, q, \ell >$-Wada dessin $\mathcal{D}$, such that the conditions of Proposition 5.4.4 hold. The cyclic group Φ_{m+1} is then a group of automorphisms of the dessin and due to our considerations in Section 5.4 we have

$$\Phi_{m+1} \ltimes \Sigma_\ell \subseteq Aut(\mathcal{D}) \ .$$

Equality always holds if $e \nmid q$. Otherwise the automorphism group of $\mathcal{D}$ may be larger than $\Phi_{m+1} \ltimes \Sigma_\ell$ and we possibly have

$$Aut(\mathcal{D}) \cong \Phi_k \ltimes \Sigma_\ell \text{ with } k = g \cdot (m+1),\ g|e,\ \Phi_k \subseteq \Phi_f\,.$$

The existence of $\Phi_k \ltimes \Sigma_\ell$ as the full automorphism group of $\mathcal{D}$ depends on the difference set D_{m+1} which is fixed not only by Φ_{m+1} but also by Φ_k (see Corollary 5.4.5). If the elements of D_{m+1} are subdivided by Φ_k into orbits of the same length k, then we can choose an ordering of the elements of D_{m+1} which is compatible with the action of Φ_k. If this ordering is also Wada compatible, we can construct a Wada dessin $\mathcal{D}$ for which Φ_k is a group of automorphisms and $\Phi_k \ltimes \Sigma_\ell$ is the full automorphism group.
Resuming our results, we formulate the following proposition

Corollary 5.4.8. *Under the same conditions of Lemma 5.4.6 and additionally with* $m+1$ *prime,* $n \not\equiv 0,1 \mod (m+1)$*, the full automorphism group of a Wada dessin* $\mathcal{D}$ *associated with a projective space* $\mathbb{P}^m(\mathbb{F}_n)$ *is "bounded" by the groups* $\Phi_{m+1} \ltimes \Sigma_\ell$ *and* $\Phi_f \ltimes \Sigma_\ell$*, i.e.*

$$\begin{gathered} Aut(\mathcal{D}) \cong \Phi_k \ltimes \Sigma_\ell \\ s.t. \\ \Phi_{m+1} \ltimes \Sigma_\ell \subseteq \Phi_k \ltimes \Sigma_\ell \subseteq \Phi_f \ltimes \Sigma_\ell\,, \end{gathered} \tag{5.16}$$

with $\Phi_{m+1} \subseteq \Phi_k \subseteq \Phi_f$*.*

Example 20. For the projective space $\mathbb{P}^4(\mathbb{F}_4)$ we have $q = 85$ and $\ell = 341$. The group generated by the Frobenius automorphism is the cyclic group Φ_{10}. The order of Φ_{10} does not divide q, so it cannot be a group of automorphism of any of the dessins associated with $\mathbb{P}^4(\mathbb{F}_4)$. Nevertheless, the subgroup $\Phi_5 \subset \Phi_{10}$ with $5 = m+1$ can be. Since $4 \not\equiv 0 \mod 5$ and $4 \not\equiv 1 \mod 5$, the conditions of Corollary 5.4.8 are satisfied. This means that the difference set D_5 fixed by Φ_5 is subdivided into 17 Φ_5-orbits all of length 5. Its elements may therefore be ordered in a way compatible with the action of Φ_5. If this ordering is such that all differences of consecutive elements $(d_i - d_{i+1})$, $d_i, d_{i+1} \in D_5$ are prime to $\ell = 341 = 31 \cdot 11$, i.e. if it is Wada compatible, we may construct an $< 85, 85, 341 >$-Wada dessin with full automorphism group $\Phi_5 \ltimes \Sigma_{341}$. Similarly to Example 17, we remark here that since the prime factorization of $\ell = 341 = 31 \cdot 11$ consists of only two quite large primes, it is very likely to find an ordering of the elements of D_5 compatible with the action of Φ_5 and also Wada compatible.
The parameters of the projective spaces $\mathbb{P}^2(\mathbb{F}_{128})$ and $\mathbb{P}^6(\mathbb{F}_4)$ also satisfy the conditions of Proposition 5.4.8. For $\mathbb{P}^2(\mathbb{F}_{128})$ we have $q = 129$, $\ell = 16513$. The cyclic

group Φ_{21} generated by the Frobenius automorphism cannot be a group of automorphisms of the associated dessins, but $\Phi_3 \subset \Phi_{21}$ can be, since $gcd(21, 129) = 3$. Thus we may order the elements of the difference set D_3 fixed by Φ_3 in a way compatible with the action of this group. If the ordering is also Wada compatible, the full automorphism group of the $< 129, 129, 16513 >$-Wada dessin we construct is $\Phi_3 \ltimes \Sigma_{16513}$. Since the integers of the prime factorization of $\ell = 16513 = 7 \cdot 7 \cdot 337$ are only 7 and 337, and 337 is a large number, it is very likely to find a Wada compatible ordering of the elements of D_3 which is also compatible with the action of Φ_3.
For $\mathbb{P}^6(\mathbb{F}_4)$ we have $q = 1365$, $\ell = 5461$. The cyclic group Φ_{14} is the group generated by the Frobenius automorphism and we have $gcd(14, 1365) = 7$. This means that the subgroup $\Phi_7 \subset \Phi_{14}$ has a suitable size to be a group of automorphisms of possible Wada dessins associated with $\mathbb{P}^6(\mathbb{F}_4)$. Ordering the elements of the difference set D_7 fixed by Φ_7 in a way compatible with its action, we may construct a Wada dessin if this ordering is also Wada compatible. For the same resons mentioned above this is very likely to happen since $\ell = 5461 = 43 \cdot 127$. The full automorphism group of the dessin constructed is then the semidirect product $\Phi_7 \ltimes \Sigma_{5461}$.

Projective spaces with ℓ prime

Suppose that for a projective space $\mathbb{P}^m(\mathbb{F}_n)$ we have ℓ prime and $k := \gcd(f, q)$. Let t be the multipliers describing the action of $\Phi_k \subseteq \Phi_f$ on the elements of a fixed difference set D_k. Since ℓ is prime we have

$$(t - 1, \ell) = 1 \ .$$

As we have seen in the proof of Proposition 5.4.4 the condition above means that the difference set D_k does not contain elements fixed by Φ_k and its elements are subdivided by Φ_k into orbits of equal length k. The elements may therefore be arranged in ways compatible with the action of Φ_k. Since ℓ is prime these orderings are also Wada compatible, and we may therefore construct $< q, q, \ell >$-Wada dessins $\mathcal{D}$ for which Φ_k is a group of automorphisms rotating the set of cells around the fixed vertices $w = b = 0$ (see Proposition 5.4.4). From Lemma 5.4.6 and Proposition 5.4.7 it then follows that $\Phi_k \ltimes \Sigma_\ell$ is the full automorphism group of these dessins. We conclude with the following corollary:

Corollary 5.4.9. *Under the conditions of Proposition 5.4.6 and the additional assumption ℓ prime, for a projective space $\mathbb{P}^m(\mathbb{F}_n)$ we may construct Wada dessins $\mathcal{D}$ such that $\Phi_k \ltimes \Sigma_\ell$ with $k := gcd(f, q)$, $\Phi_k \subseteq \Phi_f$ is the full automorphism group.*

Example 21. A projective space with ℓ prime is $\mathbb{P}^2(\mathbb{F}_8)$ with $\ell = 73$ and $q = 9$. The automorphism group generated by the Frobenius automorphism is the cyclic group

Φ_9 and $\gcd(q, 9) = 9$. Since ℓ is prime the difference set fixed under the action of Φ_9 consists of only one Φ_9-orbit of length 9:

$$D_9 = \{1, 2, 4, 8, 16, 32, 64, 55, 37\} \mod 73\,. \tag{5.17}$$

The ordering of the elements of D_9 given in (5.17) is compatible with the action of Φ_9 and, since ℓ is prime, it is also Wada compatible. We may construct a $< 9, 9, 73 >$-Wada dessin such that $\Phi_9 \ltimes \Phi_{73}$ is the full automorphism group. In this special case the dessin in not only uniform but even regular.
Other examples of projective spaces with ℓ prime are $\mathbb{P}^2(\mathbb{F}_2)$ and $\mathbb{P}^4(\mathbb{F}_2)$. For the Fano plane $\mathbb{P}^2(\mathbb{F}_2)$ we have $\ell = 7$. We may construct a $< 3, 3, 7 >$-Wada dessin with automorphism group $\Phi_3 \ltimes \Phi_7$ for each Frobenius compatible ordering of the difference set D_3 fixed by Φ_3,

$$D_3 = \{1, 2, 4\} \mod 7\,.$$

Also in this case the dessin is regular (see also Example 16 and Section 5.2).
For $\mathbb{P}^4(\mathbb{F}_2)$ we have $\ell = 31$ and $q = 15$ (seealso Example 17). We may construct$<$ $15, 15, 31 >$-Wada dessins with automorphism group $\Phi_5 \ltimes \Sigma_{31}$. We use the difference set ([Bau71])

$$D_5 = \{1, 3, 15, 2, 6, 30, 4, 12, 29, 8, 24, 27, 16, 17, 23\} \mod 31$$

fixed under the action of Φ_5 and each other difference set, whose element ordering is a Frobenius compatible permutation of the elements of D_5.

Chapter 6

Wilson Operations

Wilson operations are algebraic operations acting on maps or hypermaps. They were first described by S.Wilson ([Wil79]) and their action on dessins d'enfants has been studied in a recent work of G.Jones, M.Streit and J.Wolfart ([JSW10]).

In this Chapter we see that if they are applied to $< q, q, \ell >$-Wada dessins associated wiht projective spaces $\mathbb{P}^m(\mathbb{F}_n)$, they are a powerful instrument to 'generate' new uniform dessins with the same vertex valency but with possibly different cell valencies.

In particular, we concentrate our attention on the action of special Wilson operations, so called 'mock' Wilson operations. They change the vertex valency of the dessin they are applied to. In general, they may lead to a completely new dessin, which is not even uniform. Nevertheless, in our case of Wada dessins we obtain very interesting results: we show that under some conditions the resulting dessins are regular with the same automorphism group of the dessins we started with. We describe these dessins in terms of automorphism group, defining equations and topological features of the surface of the embedding.

At this point I would like to thank Prof. Dr. Jürgen Wolfart and Prof. Dr. Gareth Jones for fruitful discussions contributing to the results in the Sections 6.3.3 and 6.3.4.

6.1 Wilson Operations and 'mock' Wilson Operations

We consider a **map** $\mathcal{M}$ of type (p, r). A map is a graph embedded in a surface, but other than a hypermap (see Section 4.1) the graph is not bipartite. The integer p corresponds to the l.c.m. of the valency of the vertices, the integer r corresponds to the l.c.m. of the valencies of the cell. A hole on a map is defined as follows:

Definition 6.1.1. [Wil79] A jth "hole" is a cyclic sequence of edges, each two consecutive sharing a vertex, so that at each vertex, the adjacent edges subtend j faces on one side, either the right or the left but consistently throughout.

Figure 6.2 represents a hole drawn on the graph of the icosahedron (see later in this section).
At first, we only consider those holes for which j is prime to p and draw on the graph $\mathcal{G}$ of $\mathcal{M}$ all possible holes of order j. The result is a new map $\mathcal{M}'$ with the same underlying graph as $\mathcal{M}$ and with the jth holes as new cells. The valencies of the vertices do not change due to $gcd(j, p) = 1$. Nevertheless, the valencies of the cells may change, since we construct the new cells of $\mathcal{M}'$ proceeding from one edge incident with a vertex of $\mathcal{G}$ to the jth incident one. What we get is thus a new map of type (p, r').

Definition 6.1.2. We call **Wilson operator** of **order j** that operator H_j drawing all possible holes of order j on the graph $\mathcal{G}$ of a map $\mathcal{M}$. If p is the l.c.m. of the valencies of the vertices of $\mathcal{M}$, we choose j such that $gcd(p, j) = 1$.

For the new map $\mathcal{M}'$ constructed above applying H_j to the edges of $\mathcal{M}$ we write $\mathcal{M}' := H_j\mathcal{M}$.

Example 22. (see [Wil79], [JSW10]) Consider the graph $\mathcal{G}$ of the icosahedron (see Figure 6.1). It describes a map $\mathcal{M}$ of type $(5, 3)$ on the Riemann sphere such that all vertices have the same valency 5 and all cells have the same valency 3. It has 20 faces, 30 edges and 12 vertices. We apply to $\mathcal{M}$ the Wilson operator H_2 (see Figure 6.2). We get a new map $H_2\mathcal{M}$ of type $(5, 5)$ with 12 faces, 30 edges and 12 vertices. All vertices and all cells have the same valency 5. It is embedded in a surface of genus 4 and is, in fact, the map corresponding to the great dodecahedron.

Wilson operations may also be applied to hypermaps $\mathcal{D}$ of type (p, q, r) (see the recent work of G.Jones, M.Streit and J.Wolfart [JSW10] for the action of Wilson operators on regular hypermaps). In this case we may apply an operator $H_{i,j}$ with

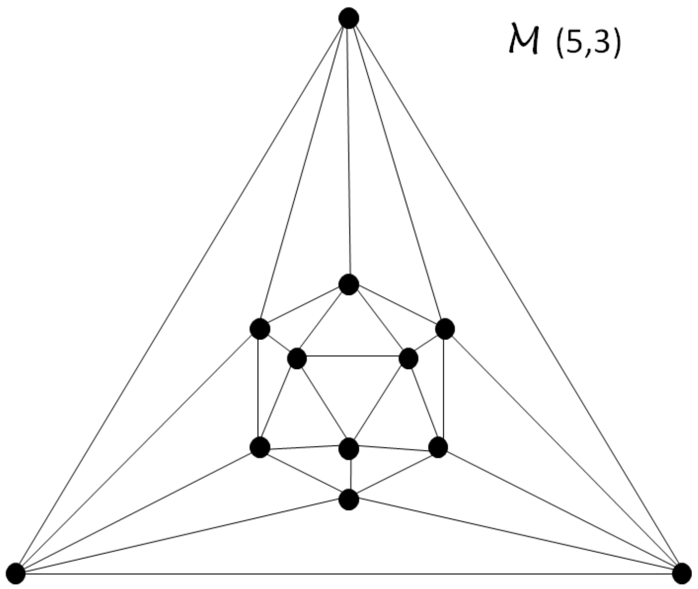


Figure 6.1: *The graph of the icosahedron. It describes a map of type* $(5,3)$ *embedded in the Riemann sphere.*

$gcd(p,i) = 1$ and $gcd(q,j) = 1$ acting locally as H_i on the white vertices and as H_j on the black ones. If $i = j$ we apply the same Wilson operator $H_i = H_j$. The result of the operations are new hypermaps $\mathcal{D}' := H_{i,j}\mathcal{D}$ or $\mathcal{D}' := H_{i,i}\mathcal{D}$ –for $i = j$– with the same underlying graph as $\mathcal{D}$. The valencies of the vertices are preserved, the valencies of the cells may change.
Special Wilson operators H_j or $H_{i,j}$ are those operators for which j or i are not prime to the valency of the vertices they are applied to. In this case, the underlying graph and the valencies of the vertices the operators act on are not preserved. We obtain completely new maps or hypermaps and in the worst case the result is even no longer a map or a hypermap (see [Wil79]).
Since in Section 6.3 we are, in particular, interested in the action of Wilson operators $H_{j,j}$ with $gcd(j,v) \neq 1$, we give the following definition:

Definition 6.1.3. We consider Wilson operators H_j or $H_{j,j}$ of order j acting on the edges incident with the vertices of a map or a hypermap. We call **'mock' Wilson operators** those operators for which j is not prime to the valencies of the vertices.

In particular, other than in the original work of Wilson, we will study the action of Wilson operators and of 'mock' Wilson operators not only on regular dessins, but also on uniform dessins associated with projective spaces $\mathbb{P}^m(\mathbb{F}_n)$.

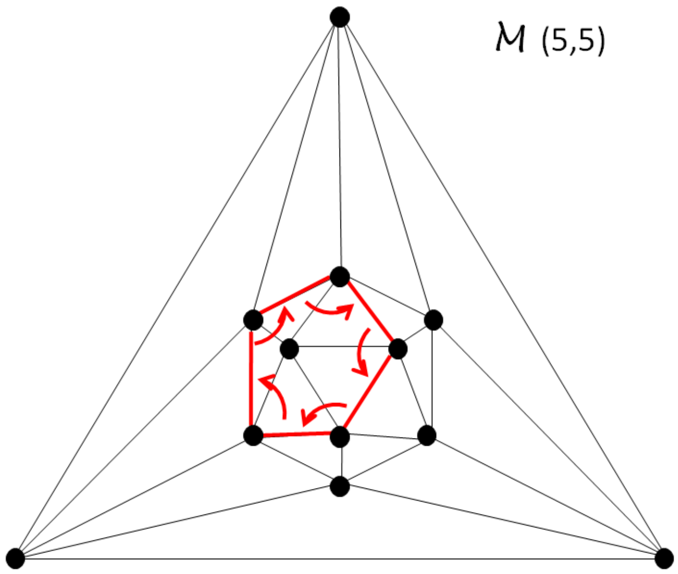


Figure 6.2: *Applying the Wilson operator H_2 to the edges of $\mathcal{M}$ we obtain a new map of type* $(5, 5)$. *It is the map corresponding to the great dodecahedron. The figure illustrates the construction of a cell of $H_2\mathcal{M}$.*

6.2 Wilson Operations on Wada Dessins

We consider Wada dessins $\mathcal{D}$ associated with projective spaces $\mathbb{P}^m(\mathbb{F}_n)$, which are constructed as described in Section 4.2.
To the edges incident with the vertices of the underlying graph we apply Wilson operators $H_{-j,k}$ with $k, j \in \mathbb{Z}/q\mathbb{Z}$. We choose k and j with opposite sign only for practical reasons, since in this way some steps of the following proofs are easier to describe. We remark that all our considerations for $H_{-j,k}$ also hold for $H_{q-j,k}$ since $H_{-j,k} = H_{q-j,k}$ by definition.
We consider the incidence pattern of the black vertices b_e and of the white vertices w_e, $e \in \mathbb{Z}/\ell\mathbb{Z}$ given in Figure 6.3. On the underlying graph $\mathcal{G}$ of $\mathcal{D}$ we draw a new dessin $\mathcal{D}' = H_{-j,k}\mathcal{D}$. The action of $H_{-j,k}$ is described by the action of the operator H_{-j} on the edges around a white vertex and by the action of the operator H_k on the edges around a black vertex. Starting with each edge $\{w_e, w_e + d_i\}$ and going clockwise around the cells as described in Section 4.2, we obtain the following

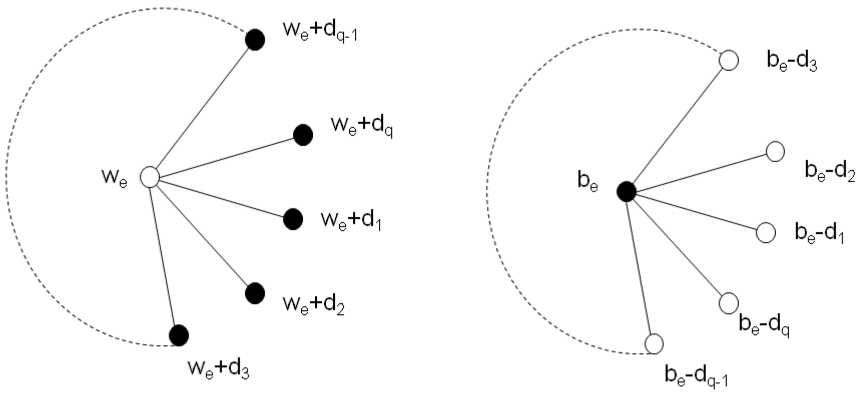


Figure 6.3: *Local incidence pattern of black and white vertices (see also Section 4.2).*

sequence of edges on the boundary of each new cell:

$$\begin{aligned}
&\{w_e, w_e + d_i\},\\
&\{w_e + d_i, w_e + d_i - d_{i+k}\},\\
&\{w_e + d_i - d_{i+k}, w_e + d_i - d_{i+k} + d_{i+k+j}\},\\
&\{w_e + d_i - d_{i+k} + d_{i+k+j}, w_e + d_i - d_{i+k} + d_{i+k+j} - d_{i+2k+j}\},\\
&\{w_e + d_i - d_{i+k} + d_{i+k+j} - d_{i+2k+j}, w_e + d_i - d_{i+k} + d_{i+k+j} - d_{i+2k+j} + d_{i+2k+2j}\},\\
&\qquad\vdots
\end{aligned} \tag{6.1}$$

We formulate the following:

Proposition 6.2.1. *We consider the local incidence pattern of the white and of the black vertices of a* $< q, q, \ell >$*-Wada dessin* $\mathcal{D}$ *associated with a projective space* $\mathbb{P}^m(\mathbb{F}_n)$ *(see Figure 6.3). Let* $D = \{d_1, \ldots, d_q\}$ *be the underlying difference set and let* $H_{-j,k}$ *be a Wilson operator with* $gcd(j, q) = gcd(k, q) = 1$, $j, k \in \mathbb{Z}/q\mathbb{Z}$*. We define:*

$$t := gcd(j + k, q)\ , \tag{6.2}$$

$$s_i := \sum_{\alpha=0}^{\frac{q}{t}-1} (d_{i+\alpha\cdot(k+j)} - d_{i+(\alpha+1)\cdot k+\alpha\cdot j}) \mod \ell\,, \quad i \in \mathbb{Z}/q\mathbb{Z}\ . \tag{6.3}$$

Applying H_{-j} to the vertices of one type and H_k to the vertices of the other we construct a new dessin with cell valencies

$$2 \cdot \frac{q}{t} \cdot \frac{\ell}{gcd(s_i, \ell)} \,. \tag{6.4}$$

Proof. We construct the cells in the way described above and we apply the operator $H_{-j,k}$ to the edges incident with the vertices of each type. We observe that alternatively an element of the difference set with sign (+) and an element with sign (−) are added. Elements $d_{i+\alpha\cdot(k+j)}$ and $d_{i+\beta\cdot(k+j)}$, $\alpha, \beta \in \mathbb{N}\backslash\{0\}$ are equal if:

$$\begin{aligned} &\alpha(k+j) \mod q \equiv \beta(k+j) \mod q \\ &\Rightarrow (\alpha-\beta)(k+j) \equiv 0 \mod q \,, \end{aligned}$$

i.e. if

$$(\alpha-\beta) \equiv 0 \mod \frac{q}{t} \,. \tag{6.5}$$

The same can be proven for elements $d_{i+(\alpha+1)\cdot k+\alpha\cdot j}$ and $d_{i+(\beta+1)\cdot k+\beta\cdot j}$.
Let $d_{i+\alpha\cdot(k+j)}$, $d_{i+\beta\cdot(k+j)}$ be such a pair of elements with $d_{i+\alpha\cdot(k+j)} = d_{i+\beta\cdot(k+j)}$, $(\alpha-\beta) \equiv 0 \mod \frac{q}{t}$. Without loss of generality we choose $\alpha \in \{0, \ldots, \frac{q}{t}-1\}$.
It follows that in Construction 6.1 above after $2 \cdot \frac{q}{t}$ steps the same series of elements of the difference set repeats.
We now consider the sum s_i of the first $2 \cdot \frac{q}{t}$ elements as defined in (6.3). If $gcd(s_i, \ell) = 1$ then we are back to the edge we started with exactly after $2 \cdot \frac{q}{t} \cdot \ell$ steps, but if $gcd(s_i, \ell) \neq 1$, then we are back to the starting edge in fewer steps, i.e. in $2 \cdot \frac{q}{t} \cdot \frac{\ell}{gcd(s_i,\ell)}$ steps.
Of course, it may happen that partial sums of s_i are congruent $0 \mod \ell$, but in these cases we would not reach the starting edge $\{w_e, w_e + d_i\}$ but another edge $\{w_e, w_e + d_{i+\alpha\cdot(k+j)}\}$. In fact, we have

$$d_i \equiv d_{i+\alpha\cdot(k+j)}$$

for

$$\alpha \equiv 0 \mod \frac{q}{t} \,.$$

As described in Section 4.2 we repeat the construction for all vertices w_e until every white and black vertex is surrounded by q neighbour vertices of the opposite color. In fact, due to the condition $gcd(j, q) = gcd(k, q) = 1$ the vertex valencies do not change. Finally, we obtain a dessin with cell valencies:

$$2 \cdot \frac{q}{t} \cdot \frac{\ell}{gcd(s_i, \ell)} \,.$$

□

Remark. Depending on the value of each s_i we obtain cells with different valencies if all or some of the sums s_i are different from each other, or we obtain cells with the same valency if all sums s_i have the same value s.

Example 23. We consider the projective space $\mathbb{P}^3(\mathbb{F}_4)$ with $\ell = 85$ points (or hyperplanes) and $q = 21$ hyperplanes through a point (or points on a hyperplane). Using the difference set (see [Bau71])

$$D = \{0, 1, 4, 51, 7, 8, 14, 16, 17, 23, 27, 28, 32, 34, 43, 46, 68, 54, 56, 64, 2\} \mod 85$$

we construct a $< 21, 21, 85 >$ - Wada dessin and we apply the Wilson operator $H_{-5,4}$ to its edges. Since $j + k = 9$ and $q = 21$ we have

$$t = gcd(9, 21) = 3\,.$$

This means that in Construction 6.1 after $2 \cdot \frac{q}{t} = 14$ steps, the elements of the difference set which we add or subtract repeat. Depending on the value of the sums s_i, we obtain cells with different valencies $2 \cdot 7 \cdot \frac{85}{gcd(s_i, 85)}$. In fact, for two of the cells we construct, we have $s_1 \equiv 19 \mod 85$ and $s_2 \equiv 61 \mod 85$, so they have full valency $2 \cdot 7 \cdot 85 = 1190$. But the sum of the first $2 \cdot \frac{q}{t}$ elements of the difference set for the last five cells is congruent $5 \mod 85$, so we obtain cells with valency $2 \cdot 7 \cdot 17 = 238$. Thus the resulting dessin has signature $< 21, 21, 595 >$ but it is no longer uniform with two cells with valency 1190 and five cells with valency 238.

Example 24. For the projective space $\mathbb{P}^4(\mathbb{F}_2)$ we have $\ell = 31$ and $q = 15$. With the difference set (see [Bau71])

$$D = \{1, 3, 15, 2, 6, 30, 4, 12, 29, 8, 24, 27, 16, 17, 23\} \mod 31$$

we construct the $< 15, 15, 31 >$ - Wada dessin associated with $\mathbb{P}^4(\mathbb{F}_2)$ and we apply the Wilson operator $H_{-2,7}$ to its edges. Since $j + k = 9$ and $q = 15$ we have

$$t = gcd(9, 15) = 3$$

and

$$\frac{q}{t} = 5\;.$$

This means that in the cell construction after $2 \cdot 5$ steps the elements of the difference set we add or subtract repeat. Nevertheless, since $\ell = 31$ is prime irrespective of the value of the sums s_i, we obtain a uniform dessin with signature $< 15, 15, 155 >$ and three cells.

Instead of considering the action of $H_{-j,k}$ on the edges incident with the vertices, we let H_{-j} and H_k act on the elements of the difference set D. We obtain the following new difference sets:

$$\begin{array}{rrcl} H_{-j}: & D & \longrightarrow & H_{-j}D \\ & \{d_i, d_{i+1}, d_{i+2}, \ldots d_{i+(q-1)}\} & \longmapsto & \{d_i, d_{i-j}, d_{i-2j}, \ldots d_{i-(q-1)j}\}\ , \\ H_k: & D & \longrightarrow & H_kD \\ & \{d_i, d_{i+1}, d_{i+2}, \ldots d_{i+(q-1)}\} & \longmapsto & \{d_i, d_{i+k}, d_{i+2k}, \ldots d_{i+(q-1)k}\}\ . \end{array} \tag{6.6}$$

We now describe the local incidence pattern of the black and of the white vertices using the new difference sets $H_{-j}D$ and H_kD respectively (see Figure 6.4). We show

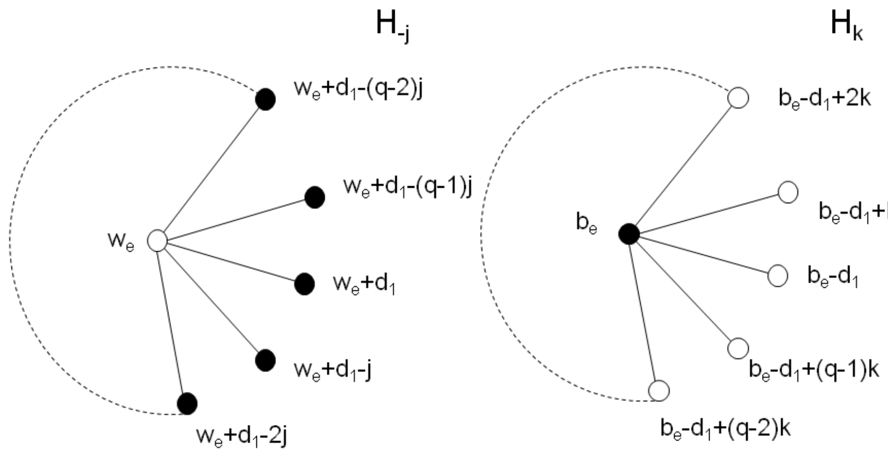


Figure 6.4: *Local incidence pattern with the difference sets $H_{-j}D$ and H_kD.*

that the dessin we construct is equivalent to the one we have constructed applying $H_{-j,k}$ to the edges incident with the white and with the black vertices:

Corollary 6.2.2. *Let*

$$H_{-j}D := \{d_i, d_{i-j}, d_{i-2j}, \ldots, d_{i-(q-1)j}\}$$

and

$$H_kD := \{d_i, d_{i+k}, d_{i+k}, \ldots, d_{i+(q-1)k}\}\ , i \in \mathbb{Z}/q\mathbb{Z}$$

be the difference sets resulting from the action of H_{-j} and H_k on D. We apply the Wilson operator $H_{-j,k}$ to the edges of the Wada dessin $\mathcal{D}$ associated with $\mathbb{P}^m(\mathbb{F}_n)$. The embedding of the new dessin $\mathcal{D}'$ we obtain corresponds to the embedding of the dessin we construct describing the local incidence pattern of the vertices of different type with the two difference sets $H_{-j}D$ and H_kD.

Proof. We consider the local incidence pattern of the white and of the black vertices given in Figure 6.4 and obtained using the difference sets $H_{-j}D$ and H_kD. Starting with a white vertex w_e, $e \in \mathbb{Z}/\ell\mathbb{Z}$ and applying the construction described in Section 4.2 we construct the edges on the cell boundaries in the following way:

$$\begin{aligned}
&\{w_e, w_e + d_i\},\\
&\{w_e + d_i, w_e + d_i - d_{i+k}\},\\
&\{w_e + d_i - d_{i+k}, w_e + d_i - d_{i+k} + d_{i+k+j}\},\\
&\{w_e + d_i - d_{i+k} + d_{i+k+j}, w_e + d_i - d_{i+k} + d_{i+k+j} - d_{i+2k+j}\},\\
&\{w_e + d_i - d_{i+k} + d_{i+k+j} - d_{i+2k+j}, w_e + d_i - d_{i+k} + d_{i+k+j} - d_{i+2k+j} + d_{i+2k+2j}\},\\
&\qquad\vdots
\end{aligned} \tag{6.7}$$

The cells we obtain correspond to the ones we obtain applying $H_{-j,k}$ directly to the edges incident with the white and with the black vertices (see Construction 6.1). Thus, the resulting dessin describes the same embedding in the same Riemann surface. □

Applying the Wilson operator $H_{k,k}$ to the edges of a Wada dessin we induce a permutation of the elements of the difference set D. With the new difference set H_kD we may construct a new Wada dessin if the Wada property is satisfied:

Corollary 6.2.3. *Let $k + j \equiv 0 \mod q$. In this case, the action of the Wilson operator $H_{k,k}$ corresponds to the action of H_k on the edges incident with the white as well as on the edges incident with the black vertices. The new dessin we obtain is still a Wada dessin if and only if all differences $d_i - d_{i+k}$ of elements $d_i, d_{i+k} \in D$ are prime to ℓ.*

Proof. If $k+j \equiv 0 \mod q$, then $k \equiv -j \mod q$, so we apply the operator $H_{k,k}$ to the edges of the dessin. Its action corresponds to the action of the same operator H_k on the edges incident with the white and with the black vertices. Since $gcd(k+j, q) = 0 \mod q$ thus for sums s_i in Equation (6.3) we obtain $s_i = d_i - d_{i+k} \mod \ell$, $\forall i \in \mathbb{Z}/q\mathbb{Z}$

and Construction 6.1 simplifies in

$$\begin{aligned}
&\{w_e, w_e + d_i\},\\
&\{w_e + d_i, w_e + d_i - d_{i+k}\},\\
&\{w_e + d_i - d_{i+k}, w_e + 2d_i - d_{i+k}\},\\
&\{w_e + 2d_i - d_{i+k}, w_e + 2(d_i - d_{i+k})\},\\
&\qquad\vdots
\end{aligned} \tag{6.8}$$

This construction corresponds to Construction 4.1 with 1 replaced by k. Thus, in a similar way, if all differences $d_i - d_{i+k}$ are prime to ℓ, we obtain a Wada dessin with q cells of valency 2ℓ, otherwise we obtain a dessin with cell valencies $2 \cdot \frac{\ell}{gcd(s_i,\ell)}$. □

Example 25. To the projective plane $\mathbb{P}^2(\mathbb{F}_7)$ belong $\ell = 57$ points (or lines) and $q = 8$ lines go through each point (or $q = 8$ points lie on each line). With the difference set (see [Bau71])

$$D = \{1, 42, 19, 6, 49, 9, 7, 38\} \mod 57$$

we construct an $< 8, 8, 57 >$-Wada dessin and we apply the Wilson operator $H_{-5,3}$ to the edges of the dessin. Since $5 + 3 \equiv 0 \mod 8$ we apply the same operation to the edges incident with the vertices of both type. As we have seen with Corollary 6.2.2 applying Wilson operators to the edges is equivalent to apply them to the difference set D. We consider

$$H_3D = \{1, 6, 7, 42, 49, 38, 19, 9\} \mod 57$$

and we construct a new dessin associated with $\mathbb{P}^2(\mathbb{F}_7)$. We obtain an $< 8, 8, 57 >$ dessin which is not uniform. In fact, for the elements 19 and 38 of D we have $19 - 38 \equiv 38 \mod 57$, $38 = 19 \cdot 2$. Since $\ell = 57 = 3 \cdot 19$ we obtain seven cells with valency 114 and 19 cells with valency 6.

Remark. From the example above is evident that Wilson operators applied to difference sets permute the ordering of the elements. On the one hand they may 'destroy' the Wada compatibility, on the other hand applying a suitable Wilson operator to a difference set for which the ordering of the elements is not Wada compatible we obtain Wada compatibility. In the example above, if we replace D by H_3D, applying H_3 to H_3D we obtain the original difference set D and we may construct an $< 8, 8, 57 >$-Wada dessin.

6.2.1 Constructing Uniform $< q, q, q >$-Dessins

In this section we discuss a nice property of Wilson operators acting on Wada dessins associated with projective spaces $\mathbb{P}^m(\mathbb{F}_n)$. Under some conditions on the parameters j and k of a Wilson operator $H_{-j,k}$ operating on the edges of a $< q, q, \ell >$-Wada dessin we may construct uniform $< q, q, q >$-dessins.

Proposition 6.2.4. *Under the conditions of Proposition 6.2.1 we choose k and j such that $gcd(k+j, q) = 1 \mod q$. Thus the number of elements q of the underlying difference set is odd. Applying the Wilson operator $H_{-j,k}$ to the edges incident with the vertices of a $< q, q, \ell >$-Wada dessin, we obtain a new uniform dessin with signature $< q, q, q >$.*

Proof. We suppose q is even. It follows that since $gcd(k, q) = gcd(j, q) = 1$, j and k must be odd. But then, the sum $(j + k)$ is even, this means $gcd(j + k, q) \neq 1$. This is a contradiction to the condition $gcd(j + k, q) = 1$, thus q is odd.
For Equation (6.3) we obtain

$$s_i := \sum_{\alpha=0}^{q-1} (d_{i+\alpha\cdot(k+j)} - d_{i+(\alpha+1)\cdot k+\alpha\cdot j}) \,, \tag{6.9}$$

i.e., according to the results of Proposition 6.2.1, s_i consists of the addition and, at the same time, of the subtraction of all elements of D. This means that we have $s_i \equiv 0 \mod \ell$ and according to (6.4) the valency of the cells is $2q$. The resulting dessin is uniform with signature $< q, q, q, >$. □

Example 26. We consider the regular Wada dessin $\mathcal{D}$ with signature $< 3, 3, 7 >$ associated with the Fano plane $\mathbb{P}^2(\mathbb{F}_2)$. We have $\ell = 7$ and $q = 3$ and we use the difference set $D = \{1, 2, 4, \} \mod 7$ for the construction. We apply to D the Wilson operators H_2 and H_{-2}, where H_{-2} just fixes the difference set:

$$\begin{aligned} H_2 D &= \{1, 4, 2\} \mod 7 \,, \\ H_{-2} D &= \{1, 2, 4\} \mod 7 \,. \end{aligned}$$

Since $j + k \equiv 2 + 2 = 4$ and $gcd(4, 7) = 1$ the conditions of Proposition 6.2.4 are satisfied. We describe the incidence pattern of the black vertices using $H_2 D$ and the one of the white vertices using $H_{-2} D$. The new dessin $H_{-2,2}\mathcal{D}$ we construct is still regular with signature $< 3, 3, 3 >$ and seven cells.
In a similar way, we may start from the regular Wada dessin $\mathcal{D}$ with signature

$< 9, 9, 73 >$ associated with the projective plane $\mathbb{P}^2(\mathbb{F}_8)$ (see also [SW01]). To the difference set ([Bau71])

$$D = \{1, 2, 4, 8, 16, 32, 37, 55, 64\} \mod 73 ,$$

we use to construct $\mathcal{D}$, we apply the Wilson operators H_5 and H_{-2}:

$$H_5 D = \{1, 32, 2, 37, 4, 55, 8, 64, 16\} \mod 73$$
$$H_{-2} D = \{1, 55, 32, 8, 2, 64, 37, 16, 4\} \mod 73 .$$

The conditions of Proposition 6.2.4 are satisfied since $j + k = 7$ and $gcd(7, 9) = 1$. According to the local incidence pattern of the vertices given in Figure 6.4 we construct a regular dessin $H_{-2,5}\mathcal{D}$ with signature $< 9, 9, 9 >$ and 73 cells.
Both dessins with signature $< 3, 3, 3 >$ and $< 9, 9, 9 >$ and the Riemann surfaces they are embedded in are discussed in detail in [SW01].

Example 27. We consider the projective space $\mathbb{P}^3(\mathbb{F}_2)$ with $q = 7$, $\ell = 15$. We construct a $< 7, 7, 15 >$ Wada dessin associated with $\mathbb{P}^3(\mathbb{F}_2)$ using the difference set ([Bau71])

$$D = \{0, 1, 5, 4, 8, 10, 2\} \mod 85 .$$

We apply to D the Wilson operators H_3 and H_{-2}:

$$H_3 D = \{0, 4, 2, 5, 10, 1, 8\} \mod 85 ,$$
$$H_{-2} D = \{0, 10, 4, 1, 2, 8, 5\} \mod 85$$

and since $j + k = 5$ we have $gcd(j + k, q) = gcd(5, 2) = 1$. The conditions of Proposition 6.2.4 are satisfied. We may thus construct a new uniform dessin with signature $< 7, 7, 7 >$ and with 15 cells.

Remark. It is possible to apply Wilson operators H_k and H_{-j} with $gcd(j + k, q) = 1$ also to difference sets D associated with projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ for which the ordering of the elements is not Wada compatible. This means that we may apply the operator $H_{-j,k}$ also to dessins which are not uniform. In this case too the result is a uniform $< q, q, q >$ dessin. In fact, the cell valencies do not depend on values of partial sums or differences of elements of D (see Equation 6.9). In the example above for $\mathbb{P}^3(\mathbb{F}_2)$, we could have chosen the difference set

$$D = \{1, 0, 2, 4, 5, 8, 10\} \mod 85 .$$

Using it we construct a $< 7, 7, 15 >$ dessin which is not uniform. In fact, the differences

$$8 - 5 \equiv 3 \mod 15 ,$$
$$1 - 10 \equiv 6 \mod 15$$

are not prime to 15, so we obtain six cells with valency ten and five cells with valency 30. Applying the Wilson operators H_3 and H_{-2} to D we obtain the difference sets

$$H_3D = \{1, 4, 10, 2, 8, 0, 5\} \mod 15\ ,$$
$$H_{-2}D = \{1, 8, 4, 0, 10, 5, 2\} \mod 15\ .$$

If we use H_3D and $H_{-2}D$ to describe the incidence pattern of the black and of the white vertices respectively, we may construct a uniform dessin with signature $< 7, 7, 7 >$ and 15 cells.

Corollary 6.2.5. *For q even we always have $t := gcd(j + k, q) \geq 2$. Applying the Wilson operator $H_{-j,k}$ to a $< q, q, \ell >$-Wada dessin we never obtain a uniform dessin of type $< q, q, q >$.*

This corollary is the counterpart of Proposition 6.2.4.

Proof. If q is even then k and j are odd due to $gcd(k, q) = gcd(j, q) = 1$. Thus the sum $j + k$ is even, so we have $t := gcd(j + k, q)$, $2|t$. This means that we never obtain cells with valency $2q$. In fact, if $gcd(s_i, \ell) = \ell$, we obtain cells with valency $2 \cdot \frac{q}{t}$. If $1 \leq gcd(s_i, \ell) < \ell$ due to $gcd(q, \ell) = 1$ (see Lemma 3.3.1) we have $t \nmid \ell$.
It follows that the cells have valencies $2 \cdot \frac{q}{t} \cdot \frac{\ell}{gcd(s_i,\ell)} \neq 2q$ with

$$2 \cdot \frac{q}{t} \leq 2 \cdot \frac{q}{t} \cdot \frac{\ell}{gcd(s_i, \ell)} \leq 2 \cdot \frac{q}{t} \cdot \ell\ .$$

□

Example 28. We consider again the projective plane $\mathbb{P}^2(\mathbb{F}_7)$ with $q = 8$ and $\ell = 57$. With the difference set ([Bau71])

$$D = \{19, 6, 49, 9, 7, 38, 1, 42\} \mod 57$$

we construct an $< 8, 8, 57 >$ - Wada dessin associated with $\mathbb{P}^2(\mathbb{F}_7)$ and we apply the Wilson operator $H_{-1,3}$ to its edges. This corresponds to the use of the difference sets

$$H_3D = \{19, 9, 1, 6, 7, 42, 49, 38\} \mod 57\ ,$$
$$H_{-1}D = \{19, 42, 1, 38, 7, 9, 49, 16\} \mod 57$$

to describe the incidence pattern of the edges incident with the black and with the white vertices. Since $q = 8$ is even, the conditions of Corollary 6.2.5 are satisfied.

In fact, we have $j + k = 4$ and $gcd(4, 8) = 4$. The new dessin we construct is uniform with signature $< 8, 8, 12 >$ and 38 cells. The cell valencies depend on $gcd(j + k, q) = gcd(4, 8) = 4$ and on the value of the sums s_i of the first four differences of elements of the difference set as given in (6.3). For all cells we have $gcd(s_i, \ell) = 19 \mod 57$. Thus they have valency $2r$ given by

$$2r = 2 \cdot \frac{8}{4} \cdot \frac{57}{19} = 24 \ .$$

Example 29. The projective space $\mathbb{P}^2(\mathbb{F}_9)$ consists of $\ell = 91$ points (or lines). Each point is incident with $q = 10$ lines and each line is incident with $q = 10$ points. We consider the difference set

$$D = \{0, 1, 3, 9, 49, 27, 56, 61, 77, 81\} \mod 91$$

associated with $\mathbb{P}^2(\mathbb{F}_9)$ and we construct a $< 10, 10, 91 >$ - Wada dessin $\mathcal{D}$. To the edges incident with the black and with the white vertices of $\mathcal{D}$ we apply the Wilson operator $H_{-1,3}$. Its action on the edges corresponds to an action on the elements of the difference set D, i.e.:

$$H_3 D = \{0, 9, 56, 81, 3, 27, 77, 1, 49, 61\} \mod 91 \ ,$$
$$H_{-1} D = \{0, 81, 77, 61, 56, 27, 49, 9, 3, 1\} \mod 91 \ .$$

Describing the incidence pattern of the black and of the white vertices using $H_3 D$ and $H_{-1} D$ we construct a new dessin $H_{-1,3}\mathcal{D}$ as described in Section 4.2. Since $q = 10$ is even the conditions of Corollary 6.2.5 are satisfied. We have $gcd(j+k, q) = gcd(4, 10) = 2$, so according to (6.4) we construct cells with valencies

$$2 \cdot \frac{q}{2} \cdot \frac{\ell}{gcd(s_i, \ell)} = 2 \cdot 5 \cdot \frac{\ell}{gcd(s_i, \ell)} \ .$$

Since for all the cells the values of the sums s_i are prime to ℓ, we obtain a new dessin with two cells with valency

$$2r = 2 \cdot 5 \cdot 91 = 910 \ .$$

The dessin is uniform with signature $< 10, 10, 455 >$.

Remark. Similarly to the remarks to Corollary 6.2.3 and to Proposition 6.2.4 we observe here that we may apply the Wilson operator $H_{-j,k}$ with $gcd(j + k, q) \geq 2$ and q even, also to dessins which are not uniform. If the elements of the difference sets $H_k D$ and $H_{-j} D$ are ordered in such a way that the sums s_i all have the same

value s, then we obtain uniform dessins.
In the example above we may construct a dessin $\mathcal{D}$ associated with $\mathbb{P}^2(\mathbb{F}_9)$ using the following difference set ([Bau71])

$$D = \{0, 1, 3, 9, 49, 56, 27, 61, 77, 81\} \mod 91\,.$$

Since $56 - 49 \equiv 7 \mod 91$ and $91 = 7 \cdot 13$, we obtain a dessin with signature $< 10, 10, 91 >$ which is not uniform. It consists of nine cells with valency 182 and of seven cells with valency 26. Nevertheless, applying the Wilson operators H_3 and H_{-1} to D and describing, as usual, with $H_3 D$ and with $H_{-1} D$ the incidence pattern of the black and of the white vertices respectively, we obtain a uniform $< 10, 10, 455 >$ dessin with two cells. The values of all the sums s_i are, in fact, prime to $\ell = 91$.

6.3 'Mock' Wilson Operations on Wada Dessins

In the sections above we have seen that applying Wilson operators $H_{-j,k}$ to the edges of Wada dessins we may construct completely new dessins. These dessins have the same vertex valency but the cell valency may be different. In some cases not even uniformity is preserved. We are now interested in constructing Wada dessins for which the cell valency is preserved, but the vertex valency changes. In particular, we want to construct regular Wada dessins starting from their uniform counterpart. To do this we apply 'mock' Wilson operators $H_{k,k}$ to the edges incident with the vertices of each type.

6.3.1 The Action of 'Mock' Wilson Operators $H_{k,k}$

As we have seen in Definition 6.1.3 the order of a 'mock' Wilson operator is not prime to the valency of the vertices belonging to the dessins. We apply the operator $H_{k,k}$ with $gcd(k, q) \neq 1$ to the edges incident with the vertices of a $< q, q, \ell >$-Wada dessin $\mathcal{D}$ associated with a projective space $\mathbb{P}^m(\mathbb{F}_n)$.

Proposition 6.3.1. *Let $\mathcal{D}$ be a $< q, q, \ell >$-Wada dessin associated with a projective space $\mathbb{P}^m(\mathbb{F}_n)$. Let D be the difference set used for the construction. We apply to the edges of $\mathcal{D}$ the 'mock' Wilson operator $H_{k,k}$ with $k|q$, $k \in \mathbb{Z}/q\mathbb{Z}$. The original dessin $\mathcal{D}$ 'splits' in k component dessins $(H_{k,k}\mathcal{D})_i$, $i = 1, \ldots, k$. Iff for a dessin $(H_{k,k}\mathcal{D})_i$ differences of elements $d_{i+h\cdot k}, d_{i+(h+1)\cdot k} \in D$, $h \in \mathbb{Z}/\frac{q}{k}\mathbb{Z}$ satisfy the Wada condition*

$$(d_{i+h\cdot k} - d_{i+(h+1)\cdot k}, \ell) = 1\ ,$$

then the new dessin $(H_{k,k}\mathcal{D})_i$ is a Wada dessin with signature $< \frac{q}{k}, \frac{q}{k}, \ell >$.

Proof. We consider the incidence pattern of the black and of the white vertices of $\mathcal{D}$ given in Figure 6.3. On the edges incident to the vertices of the underlying graph $\mathcal{G}$ of $\mathcal{D}$ we apply the Wilson operator $H_{k,k}$. We start with the edge $\{w_e, w_e + d_1\}$ and moving clockwise we construct the boundary of a new cell:

$$\{w_e, w_e + d_1\},$$
$$\{w_e + d_1, w_e + d_1 - d_{1+k}\},$$
$$\{w_e + d_1 - d_{1+k}, w_e + 2d_1 - d_{1+k}\},$$
$$\{w_e + 2d_1 - d_{1+k}, w_e + 2(d_1 - d_{1+k})\},$$
$$\vdots$$
$$\{w_e + sd_1 - (s-1)d_{1+k}, w_e\},$$
$$\{w_e, w_e + d_1\}\ ,$$

where the integer $s \in \mathbb{Z}/\ell\mathbb{Z}$ is such that $s \cdot (d_1 - d_{1+k}) \equiv 0 \mod \ell$. After $2s$ steps we are back to the first edge. In particular, if the value of the difference $(d_1 - d_{1+k})$ is prime to ℓ, we are back to the starting edge after 2ℓ steps. In this case none of the vertices of each type occurs more than once on the boundary. In fact, if two white vertices were equal, we should have

$$w_e + a \cdot (d_1 - d_{1+k}) \equiv w_e + b \cdot (d_1 - d_{1+k}) \quad a, b \in \mathbb{Z}/\ell\mathbb{Z}\,, \tag{6.10}$$

but this is possible only for $a \equiv b \mod \ell$ since $(d_i - d_{i+k})$ prime to ℓ.
In a similar way, we may prove the same for the black vertices.
We repeat the construction described above for the next incident edge, which due to the action of $H_{k,k}$ is $\{w_e, w_e + d_{1+k}\}$. We go on this way for all successive edges incident with w_e. If we have

$$(d_{1+h\cdot k} - d_{1+(h+1)\cdot k}, \ell) = 1\,,\ h \in \mathbb{Z}/\frac{q}{k}\mathbb{Z}$$

for all differences of elements $d_{1+h\cdot k}, d_{1+(h+1)\cdot k} \in D$, the Wada condition (see also Section 4.3) is satisfied. Since no vertex repeats on the boundary of any cell as it is easy to check for each of the remaining $\frac{q}{k} - 1$ cells (see Relation 6.10) we construct cells belonging to a possible Wada dessin $(H_{k,k}\mathcal{D})_1$.
Due to the action of $H_{k,k}$ with $(k, q) \neq 1$, only $\frac{q}{k}$ of the edges incident to the vertices of the original dessin $\mathcal{D}$ belong to the new Wada dessin. This means that only $\frac{q}{k} \cdot \ell$ incidence relations between points (black vertices) and hyperplanes (white vertices)

may be represented by the graph of $(H_{k,k}\mathcal{D})_1$. Due to the Wada property, after the construction of the $\frac{q}{k}$ cells around the white vertex w_e we have indeed $\frac{q}{k} \cdot \ell$ incidence relations represented. Thus, the dessin we have constructed is complete. It is a Wada dessin with signature $< \frac{q}{k}, \frac{q}{k}, \ell >$ and $\frac{q}{k}$ cells.
We repeat the construction of dessins sketched above starting with each other edge between $\{w_e, w_e + d_1\}$ and $\{w_e, w_e + d_k\}$. If the Wada condition is satisfied, we obtain new $< \frac{q}{k}, \frac{q}{k}, \ell >$-Wada dessins with different numberings of the vertices. □

Remarks. 1. We can imagine all the dessins $(H_{k,k}\mathcal{D})_i$ being the sheets of a new manifold $\mathcal{M}$. Each dessin is pinched to the others at the vertices on its cell boundaries (see also [Wil79]). Each 'sheet' is a Riemann surface whose genus g can be computed with the Euler formula:

$$2 - 2g = \#\text{ vertices } - \#\text{ edges } + \#\text{ cells}$$

$$2 - 2g = 2\ell - \tfrac{q}{k}\ell + \tfrac{q}{k} \tag{6.11}$$

$$\Rightarrow g = -\tfrac{1}{2}(2\ell - \tfrac{q}{k}\ell + \tfrac{q}{k} - 2)\ .$$

2. Each of the k possible new graphs $(H_{k,k}\mathcal{G})_i$, $i = 1, \ldots, k$, is no longer a bipartite graph of the projective space $\mathbb{P}^m(\mathbb{F}_n)$. In fact, the points and the hyperplanes are still completely represented but we do not have a complete representation of the flags, since each $(H_{k,k}\mathcal{G})_i$ lacks of some of the edges incident with the vertices of the original graph $\mathcal{G}$. We obtain a complete representation of the flags only if we consider all graphs $(H_{k,k}\mathcal{G})_i$ together i.e. the whole manifold $\mathcal{M}$ the component dessins belong to.

3. Similarly to the case of the Wilson operators described in Section 6.2 (see Corollary 6.2.2), we may apply the 'mock' operator $H_{k,k}$ directly to the elements of the difference set D. We obtain 'reduced' sets $(H_k D)_i$:

$$(H_k D)_i = \{d_i, d_{i+k}, d_{i+2k}, \ldots, d_{i+(\frac{q}{k}-1)k}\} \mod \ell\ , \quad i = 1, \ldots, k\ .$$

These sets are not difference sets since the integers $1, \ldots, (\ell - 1)$ are no longer completely represented by differences $(d_{i+t\cdot k} - d_{i+s\cdot k})$, $s, t \in \mathbb{Z}/\frac{q}{k}\mathbb{Z}$, $s \neq t$. We obtain k different 'reduced' sets, since we may start the construction of dessins $(H_{k,k}\mathcal{D})_i$ with every edge between $\{w_e, w_e + d_1\}$ and $\{w_e, w_e + d_k\}$. Each of the sets has one of the elements d_1, $d_2, d_3, \ldots, d_k$ at the starting position and the ordering of the elements is fixed up to cyclic permutations. The k sets describe the incidence pattern of the vertices belonging to the k dessins $(H_{k,k}\mathcal{D})_i$ (see Figure 6.5).

We only consider the edges between $\{w_e, w_e + d_1\}$ to $\{w_e, w_e + d_k\}$, since starting the construction with every other edge $\{w_e, w_e + d_i\}$ with $i \in \mathbb{Z}/q\mathbb{Z}$ but with $i \neq 1, \dots, k$ will only induce a cyclic permutation of the elements of one of the k underlying 'reduced' sets.

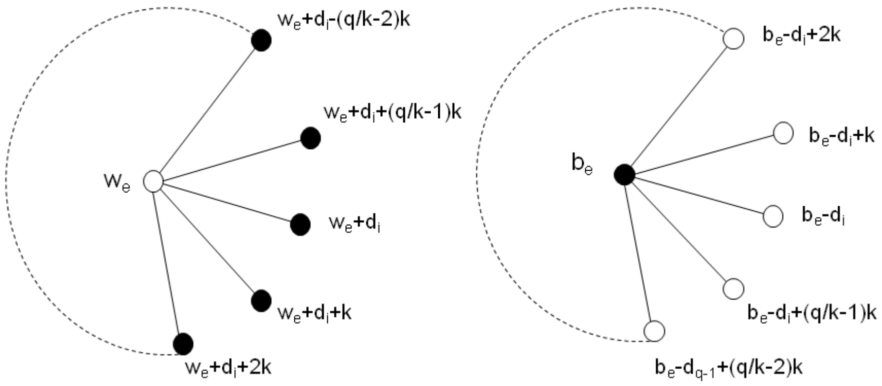


Figure 6.5: *Incidence pattern of the vertices of dessins $H_{k,k}\mathcal{D}$.*

6.3.2 Constructing Regular Dessins

For Wada dessins associated with projective spaces $\mathbb{P}^m(\mathbb{F}_n)$, $n = p^e$, the full automorphism group is usually the Singer group Σ_ℓ. Nevertheless, in Chapter 5 we have seen that in some cases it can be even larger, extended by the group $\Phi_f \cong \mathrm{Gal}(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$ generated by the Frobenius automorphism or by a subgroup $\Phi_g \subset \Phi_f$. We recall that groups $\Phi_g \subseteq \Phi_f$ are groups of automorphisms of Wada dessins if two conditions are satisfied:

1. The order g should divide the valency q of the vertices.

2. The elements of the difference set we use for the construction should be subdivided by Φ_g only into orbits of length g.

Thus, the full automorphism group is the semidirect product $\Phi_g \ltimes \Sigma_\ell$ (see Section 5.4). Since the action of the group Φ_g on the edges is free and only in some few cases transitive, we have uniform but not regular dessins. With the help of 'mock' Wilson operators we are able to construct regular dessins with $\Phi_g \ltimes \Sigma_\ell$ as the full automorphism group. To achieve this we start with a $< q, q, \ell >$-Wada dessin $\mathcal{D}$ associated with a projective space $\mathbb{P}^m(\mathbb{F}_n)$ and with automorphism group $\Phi_g \ltimes \Sigma_\ell$. The action of Σ_ℓ is always transitive on the edges of each type ∘—• or •—∘ on the boundary of the cells. Nevertheless, due to the fact that usually $g|q$ but $gcd(g, q) \neq q$ we only have a free but not a transitive action of Φ_g on the edges and on the cells. We need to 'modify' $\mathcal{D}$ so that we obtain a transitive action of Φ_g. We prove the following:

Proposition 6.3.2. *Let $\mathcal{D}$ be a $< q, q, \ell >$-Wada dessin associated with a projective space $\mathbb{P}^m(\mathbb{F}_n)$, $n = p^e$. Let $\Phi_g \ltimes \Sigma_\ell$ be its automorphism group acting freely on the edges, where $\Phi_g \subseteq \Phi_f$, $\Phi_f \cong Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$ and Σ_ℓ a Singer group. We apply to $\mathcal{D}$ the 'mock' Wilson operator $H_{k,k}$ with $k = \frac{q}{g}$. $\mathcal{D}$ 'splits' into k components $(H_{k,k}\mathcal{D})_i$, $i = 1, \ldots, k$. Each component $(H_{k,k}\mathcal{D})_i$ for which the Wada condition is satisfied is a regular $< g, g, \ell >$-Wada dessin with automorphism group $\Phi_g \ltimes \Sigma_\ell$.*

Proof. Let D_g be the difference set we have used for the construction of $\mathcal{D}$. The set D_g is fixed under the action of Φ_g and since $\Phi_g \ltimes \Sigma_\ell$ is the automorphism group of $\mathcal{D}$, its elements are ordered in a way compatible with the action of Φ_g (see Proposition 5.4.4). Let $t = p^s$, $s \in \mathbb{Z}/f\mathbb{Z}$, $sg \equiv 0 \mod f$, we have:

$$\begin{aligned} D_g =& \{d_1, \ldots, d_k,\ t^j d_1, \ldots, t^j d_k,\ \ldots\ldots\ldots, t^{(g-1)j} d_1, \ldots, t^{(g-1)j} d_k\}\ , \\ & j \in (\mathbb{Z}/g\mathbb{Z})^*,\ \frac{q}{g} = k\ . \end{aligned} \tag{6.12}$$

We apply H_k to the elements of D_g. Without loss of generality we start with d_1 and we obtain the 'reduced' set:

$$H_k D_g = \{d_1, t^j d_1, t^{2j} d_1, t^{3j} d_1, \ldots, t^{(g-1)j} d_1\}\ . \tag{6.13}$$

According to Remark 3 to Proposition 6.3.1 the set $H_k D_g$ describes the incidence pattern of one of k possible dessins (see Figure 6.6). Let us suppose that the ordering of the elements of $H_k D_g$ is also Wada compatible. Thus the dessin $H_{k,k}\mathcal{D}$ we construct is a Wada dessin with signature $< g, g, \ell >$. We now consider the sequence of edges on the boundary of a cell of $H_{k,k}\mathcal{D}$. Without loss of generality we consider

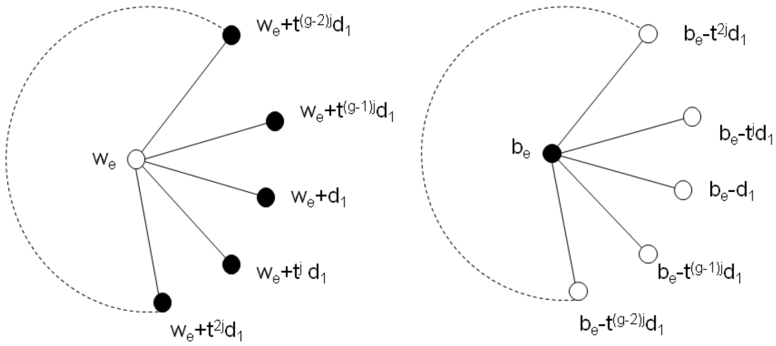


Figure 6.6: *Incidence pattern of the vertices of a dessin $H_{k,k}\mathcal{D}$ constructed using a reduce set H_kD_g. The ordering of the elements of the difference set D_g we started with is compatible with the action of the cyclic group Φ_g.*

the cell $\mathcal{C}_1$ with starting edge $w_e, w_e + d_1$:

$$\begin{aligned}
&\{w_e, w_e + d_1\},\\
&\{w_e + d_1, w_e + d_1 - t^j d_1\},\\
&\{w_e + d_1 - t^j d_1, w_e + 2d_1 - t^j d_1\},\\
&\{w_e + 2d_1 - t^j d_1, w_e + 2d_1 - 2t^j d_1\},\\
&\qquad\vdots\\
&\{w_e - (\ell - 1)t^j d_1, w_e\}\ .
\end{aligned} \tag{6.14}$$

We have seen (see Section 5.4) that Φ_g acts by rotating the cells around the fixed vertices. For the general case we do not have necessarily $gcd(t-1, \ell) = 1$, so there may be more fixed vertices other than the vertices $b_e = w_e = 0$. Nevertheless, without loss of generality we may choose $w_e = 0$. Recalling that Φ_g acts on the vertices by multiplication with the integer t, we obtain a mapping of the cell $\mathcal{C}_1$ onto a new cell $\mathcal{C}_1'$ with the following edges on its boundary:

$$\begin{aligned} &\{0, td_1\}, \\ &\{td_1, td_1 - t^{j+1}d_1\}, \\ &\{td_1 - t^{j+1}d_1, 2td_1 - t^{j+1}d_1\}, \\ &\qquad\vdots \\ &\{-(\ell-1)t^{j+1}d_1, 0\} \end{aligned} \tag{6.15}$$

According to the local incidence pattern (see Figure 6.6), $\mathcal{C}_1'$ corresponds to one of the cells $\mathcal{C}_1 + h$ with starting edge $\{0, t^{hj}d_1\}$. Due to the construction above we have:

$$hj \equiv 1 \mod g \ .$$

Since j and g are coprime, h is the multiplicative inverse of j in $(\mathbb{Z}/g\mathbb{Z})^*$. Moreover no one of the edges on the boundary of $\mathcal{C}_1$ is fixed under the action of Φ_g. Even if w_e or b_e are fixed, each of the incident vertices $w_e + t^{\nu j}d_i$ and $b_e - t^{\nu j}d_i$, $\nu \in \mathbb{Z}/g\mathbb{Z}$ cannot be. In fact, we have $t^{\nu j}d_1 \not\equiv d_1 \mod \ell$, $\forall \nu \in \mathbb{Z}/g\mathbb{Z}$, otherwise we could not have chosen an ordering of the elements of D_g compatible with the action of Φ_g. Thus, Φ_g rotates $\mathcal{C}_1$ around $w_e = 0$ by an angle $\frac{2\pi h}{g}$. Applying recursively Φ_g we are back to the first cell $\mathcal{C}_1$ after g steps, from which it follows that Φ_g acts transitively on the cells, i.e. on the edges belonging to their boundary. Finally, since the dessin $H_{k,k}\mathcal{D}$ is still a Wada dessin, Σ_ℓ still acts permuting transitively the edges of each type •——○ or ○——• on the boundary of each cell (see Proposition 5.1.1). Thus $\Phi_g \ltimes \Sigma_\ell$ is the full automorphism group acting transitively on the edges of $H_{k,k}\mathcal{D}$. It is easy to verify that our construction is independent from the choice of the starting element d_1. If the elements of a 'reduced' set $(H_k D_g)_i$, with $i \in \{1, \ldots, k\}$, satisfy the Wada condition, thus the component dessin associated $(H_{k,k}\mathcal{D})_i$ is regular with automorphism group $\Phi_g \ltimes \Sigma_\ell$. □

Remark. Each 'reduced' set $(H_k D_g)_i$, $i = 1, \ldots, k$ consists of the complete Φ_g-orbit of an element $d_i \in D_g$:

$$(H_k D_g)_i = \{d_i, t^j d_i, t^{2j} d_i, \ldots, t^{(g-1)} d_i\} \mod \ell$$

Thus, it is fixed under the action of Φ_g up to cyclic permutations.

Example 30. We consider the projective space $\mathbb{P}^4(\mathbb{F}_3)$ with $\ell = 121$ points and hyperplanes, and with $q = 40$ points on each hyperplane and, viceversa, $q = 40$

hyperplanes through a point. In order to construct a $< 40, 40, 121 >$-Wada dessin $\mathcal{D}$ associated with $\mathbb{P}^4(\mathbb{F}_3)$, we use the following difference set ([Bau71])

$$D_5 = \{1, 4, 7, 11, 13, 34, 25, 67, 3, 12, 21, 33, 39, 102, 75, 80, 9, 36, 63, 99, 117, 64, 104, 119 \\ 27, 108, 68, 55, 109, 71, 70, 115, 81, 82, 83, 44, 85, 92, 89, 103\} \mod 121\,.$$

The elements of D_5 are ordered in a Frobenius and in a Wada compatible way. The cyclic group $\Phi_5 \cong \mathrm{Gal}(\mathbb{F}_{3^5}/\mathbb{F}_3)$ is generated by the Frobenius automorphism. Since the conditions of Proposition 5.2.6 are satisfied, the full automorphism group acting freely on the edges of $\mathcal{D}$ is $\Phi_5 \ltimes \Sigma_{121}$ with Σ_{121} the Singer group. We apply the 'mock' Wilson operator H_8 to the difference set D_5 and starting with the element 1 we obtain the 'reduced' set:

$$H_8 D_5 = \{1, 3, 9, 27, 81\} \mod 121\,.$$

Since the ordering of the elements of $H_8 D_5$ is Wada compatible, we may construct a new Wada dessin $H_{8,8}\mathcal{D}$ with signature $< 5, 5, 121 >$. This dessin is regular with automorphism group $\Phi_5 \ltimes \Sigma_{121}$. The Riemann surface of the embedding has genus (see Equation 6.11)

$$g = -\frac{1}{2}(242 - 605 + 5 - 2)$$
$$\Rightarrow g = 185\,.$$

We may construct further regular Wada dessins also with the 'reduced' sets starting with the elements $4, 7, 13, 34, 25, 67$. On the contrary, for the set starting with 11 we may not construct a regular Wada dessin since the Wada condition is not satisfied.

In general the component dessins of manifolds $\mathcal{M}$ obtained by applying 'mock' Wilson operators $H_{k,k}$ to dessins $\mathcal{D}$ are not isomorphic to each other. Nevertheless, in the special case of the regular dessins constructed as described in Proposition 6.3.2 we have isomorphisms:

Corollary 6.3.3. *Under the conditions of Proposition 6.3.2 let D_g be the difference set we use for the construction of the dessin $\mathcal{D}$. All the component dessins $(H_{k,k}\mathcal{D})_i$ satisfying the Wada condition are isomorphic to each other.*

Proof. We consider the difference set D_g with its elements ordered in a way compatible with the action of the group Φ_g:

$$D_g = \{d_1, \ldots, d_k,\ t^j d_1, \ldots, t^j d_k,\ \ldots\ldots\ldots, t^{(g-1)j} d_1, \ldots, t^{(g-1)j} d_k\}\,, \\ j \in (\mathbb{Z}/g\mathbb{Z})^*,\ k := \frac{q}{g}\,. \tag{6.16}$$

Without loss of generality we consider the dessin $(H_{k,k}\mathcal{D})_1$ constructed with the 'reduced' set

$$(H_k D_g)_1 = \{d_1, t^j d_1, \ldots, t^{(g-1)j} d_1\}$$

and we suppose that it has the Wada property. This means $d_1 \in (\mathbb{Z}/\ell\mathbb{Z})^*$, i.e. an inverse element $d_1^* \in (\mathbb{Z}/\ell\mathbb{Z})^*$ exists such that $d_1 d_1^* \equiv 1 \mod \ell$. Multiplying $(H_k D_g)_1$ with integers $d_1^* d_i$, $i = 2, \ldots, k$ we obtain the 'reduced' sets of all other possible dessins $(H_{k,k}\mathcal{D}_g)_i$. Among them we only consider those for which the Wada condition is satisfied. I.e. we only consider those dessins for which the first element d_i of the 'reduced' set is also prime to ℓ. In fact, if $\gcd(d_i, \ell) \neq 1$, the Wada condition is never satisfied as it is easy to check. Since $d_1^* \in (\mathbb{Z}/\ell\mathbb{Z})^*$ and $d_i \in (\mathbb{Z}/\ell\mathbb{Z})^*$ for some $i \in \{2, \ldots, k\}$ the set $(H_k D_g)_1$ and the sets $d_1^* d_i\,(H_k D_g)_1$ are equivalent to each other (see 1.1). Thus the resulting dessins are isomorphic to each other, each of them resulting from a 'renumbering' of the vertices of the underlying graph. □

Example 31. In Example 30 the regular dessins constructed with the 'reduced' sets starting with the elements $1, 4, 7, 13, 34, 25, 67$ are isomorphic to each other.

For projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ with large parameters q and ℓ it is not easy to determine explicitely associated difference sets D_g. Nevertheless, if we know that D_g is fixed under the action of a group $\Phi_g \subseteq \Phi_f$, $\Phi_f \cong \mathrm{Gal}(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$ and its elements are subdivided into Φ_g-orbits with the same length g, under some conditions it is possible to determine explicitely at least one 'reduced' set $H_{k,k}D_g$ with $k = \frac{q}{g}$. Let $\mathcal{D}$ be the $< q, q, \ell >$-Wada dessin associated with $\mathbb{P}^m(\mathbb{F}_n)$, with automorphism group $\Phi_g \ltimes \Sigma_\ell$, Σ_ℓ the Singer group. The dessin $\mathcal{D}$ is constructed using a difference set D_g which is fixed under the action of Φ_g and whose elements are ordered in a way compatible with this action. The chosen difference set D_g is defined up to multiplication with integers $t \in (\mathbb{Z}/\ell\mathbb{Z})^*$. Thus, if D_g does not contain the orbit of 1, it is possible to 'normalize' it such that it contains this orbit. We suppose that at least one of the elements $d_i \in D_g$ is prime to ℓ and let d_i^* be the multiplicative inverse of d_i in $\mathbb{Z}/\ell\mathbb{Z}^*$. If we multiply D_g with d_i^* we obtain a mapping of the Φ_g-orbit of d_i to the Φ_g-orbit of 1. We apply to $D_g^* := d_i^* \cdot D_g$ the 'mock' Wilson operator H_k. As the ordering of the elements of D_g^* is still compatible with the action of Φ_g, applying H_k to D_g^* and starting with the element 1 we obtain the 'reduced' set:

$$H_k D_g^* = \{1, t^j, t^{2j}, \ldots, t^{(g-1)j}\}\ ,$$
$$j \in (\mathbb{Z}/g\mathbb{Z})^*\ , t = p^s\ , s \in (\mathbb{Z}/f\mathbb{Z})^*, s \cdot g \equiv 0 \mod f\ .$$

If the ordering of the elements of $H_k D_g^*$ is Wada compatible, we may construct a new Wada dessin $H_{k,k}\mathcal{D}$ which is regular with automorphism group $\Phi_g \ltimes \Sigma_\ell$.

Example 32. We consider the projective space $\mathbb{P}^6(\mathbb{F}_5)$ with parameters $q = 3906$ and $\ell = 19531$. The parameters of $\mathbb{P}^6(\mathbb{F}_5)$ satisfies the conditions of Proposition 5.2.6, so we may construct a $< 3906, 3906, 19531 >$-Wada dessin whose automorphism group is $\Phi_7 \ltimes \Sigma_{19531}$. Suppose we do not know explicitely the elements of the Frobenius difference set D_7 we use for the construction. Nevertheless, since Φ_7 is a group of automorphisms of $\mathcal{D}$, the elements of D_7 are ordered in a Frobenius compatible way. On D_7 the cyclic group Φ_7 acts with a multiplication of the elements by the multiplier 5. Suppose D_7 contains the orbit of 1. If this is not the case, we normalize D_7 in the way described above.
We apply to D_7 the 'mock' Wilson operator H_{558} and starting with the element 1 we obtain the 'reduced' set:

$$H_{558}D_7 = \{1, 5, 25, 125, 625, 3125, 15625\} \mod 19531 .$$

Since $\ell = 19531$ is prime, the elements of $H_{558}D_7$ necessarily satisfy the Wada condition, so we may construct the Wada dessin $H_{558,558}\mathcal{D}$. This turns out to be a regular dessin with automorphism group $\Phi_7 \ltimes \Sigma_{19531}$.

We may apply the construction described in the proof to Proposition 6.3.2 recursively. I.e. applying to regular $< g, g, \ell >$-Wada dessins $H_{k,k}\mathcal{D}$ further 'mock' Wilson operations we may again obtain regular dessins with a smaller automorphism group. We formulate the following

Corollary 6.3.4. *Let $\Phi_{g^*} \subset \Phi_g$ and let H_{k^*,k^*} be a 'mock' Wilson operator with $k^* = \frac{g}{g^*}$. Under the same conditions of Proposition 6.3.2, applying H_{k^*,k^*} to a regular $< g, g, \ell >$-Wada dessin $H_{k,k}\mathcal{D}$, $k = \frac{q}{g}$ we obtain new regular Wada dessins with automorphism group $\Phi_{g^*} \ltimes \Sigma_\ell$ iff the Wada condition is satisfied.*

Proof. The proof follows directly from the proof of Proposition 6.3.2. Let H_kD_g be the 'reduced' set we have used to construct the regular $< g, g, \ell >$-Wada dessin $H_{k,k}\mathcal{D}$.

$$H_kD_g = \{d_i, t^jd_i, t^{2j}d_i, \ldots, t^{(g-1)j}d_i\} \mod \ell\,,\ d_i \in D_g\ .$$

We apply H_{k^*} with $k^* = \frac{g}{g^*}$ to the difference set H_kD_g and obtain new sets

$$(H_{k^*} \circ H_kD_g)_i = \{d_i, t^{\nu j}d_i, t^{2\nu j}d_i, \ldots t^{(g^*-1)\nu j}d_i\}\,,$$

where $\nu \in \mathbb{Z}/g\mathbb{Z}$, $\nu g^* \equiv 0 \mod g$, $i \in \mathbb{Z}/k\mathbb{Z}$.
If the ordering of the elements of a $(H_{k^*} \circ H_kD_g)_i$ satisfies the Wada condition, then we may construct a $< g^*, g^*, \ell >$-Wada dessin $(H_{k^*,k^*} \circ H_{k,k}\mathcal{D})_i$.

The cyclic group Φ_g is generated by a power σ^s, $s \cdot g \equiv 0 \mod f$, $s \not\equiv 0 \mod f$ of the Frobenius automorphism. Thus, with the notation above we let $\Phi_{g^*} \subset \Phi_f$ be generated by a power $\sigma^{\nu s}$. The group Φ_{g^*} acts on the vertices of $(H_{k^*,k^*} \circ H_{k,k}\mathcal{D})_i$ by multiplication with the integer t^ν. Similarly to the proof of Proposition 6.3.2, we may prove that the action on the vertices induces a rotation of the cells around the fixed vertices. This action is transitive. Since the dessin $(H_{k^*,k^*} \circ H_{k,k}\mathcal{D})_i$ is a Wada dessin, the Singer group Σ_ℓ still acts permuting transitively the edges of each type on the boundary of the cells. Finally, due to the fact that Φ_g normalises Σ_ℓ in $P\Gamma L(m+1,n)$, Φ_{g^*} also normalises Σ_ℓ in $P\Gamma L(m+1,n)$. It follows that $\Phi_{g^*} \ltimes \Sigma_\ell$ is the full automorphism group acting transitively on the edges of the dessin $(H_{k^*,k^*} \circ H_{k,k}\mathcal{D})_i$. □

Example 33. We consider the projective plane $\mathbb{P}^2(\mathbb{F}_8)$ with parameters $q = 9$ and $\ell = 73$. Together with the Fano plane $\mathbb{P}^2(\mathbb{F}_2)$ (see [SW01]) it is one of only two projective spaces for which we may construct regular Wada dessins. We use the difference set

$$D_9 = \{1, 2, 4, 8, 16, 32, 64, 55, 37\} \mod 73$$

to construct such a dessin $\mathcal{D}$. The automorphism group of $\mathcal{D}$ is the semidirect product $\Phi_9 \ltimes \Sigma_{73}$ of the group $\Phi_9 \cong \mathrm{Gal}(\mathbb{F}_{2^9}/\mathbb{F}_2)$ generated by the Frobenius automorphism and of the Singer group Σ_{73}. Since $\mathcal{D}$ is already regular, applying a 'mock' Wilson operator $H_{3,3}$ on its edges means to generate new dessins $(H_{3,3}\mathcal{D})_i$, $i = 1, 2, 3$ with smaller automorphism group but still regular. We consider the 'reduced' set:

$$(H_3 D)_1 = \{1, 8, 64\} \mod 73 \,.$$

The dessin $(H_{3,3}\mathcal{D})_1$ we may construct is a Wada dessin with the Singer group Σ_{73} and the cyclic subgroup $\Phi_3 \subset \Phi_9$ as group of automophisms. The full automorphism group is the group $\Phi_3 \ltimes \Sigma_{73}$ and the surface of the embedding has genus $g = 36$. The same holds for the dessins constructed with the 'reduced' sets

$$(H_3 D)_2 = \{2, 16, 55\} \mod 73 \,,$$
$$(H_3 D)_3 = \{4, 32, 37\} \mod 73 \,.$$

From Proposition 6.3.2 and Corollary 6.3.4 we see that 'mock' Wilson operators applied to Wada dessins $\mathcal{D}$ are powerful tools to construct a possibly large number of regular Wada dessins. In the very special case of f prime, discussed in Section 5.2, under an additional condition we may predict when we have Wada compatibility, in fact

Corollary 6.3.5. *Let $\mathcal{D}$ be a $< q, q, \ell >$-Wada dessin of the same type as the ones constructed in Proposition 5.2.6. Thus the conditions of Proposition 5.2.6 hold. Let D_f be the Frobenius difference set used for the construction, i.e. its elements are ordered in a Frobenius compatible way*

$$D_f =\{d_1, \ldots, d_k,\ p^j d_1, \ldots, p^j d_k,\ \ldots\ldots\ldots, p^{(f-1)j} d_1, \ldots, p^{(f-1)j} d_k\}\ ,$$
$$j \in (\mathbb{Z}/f\mathbb{Z})^*\ ,\ k = \frac{q}{f}\ .$$

The ordering of the elements of a 'reduced' set

$$(H_k D_f)_i =\{d_i, p^j d_i, p^{2j} d_i, \ldots, p^{(f-1)j} d_i\}\ , \quad i \in \mathbb{Z}/k\mathbb{Z}.$$

is Wada compatibe iff $gcd(d_i, \ell) = 1$.

Proof. Under the conditions of Proposition 5.2.6 we consider $< q, q, \ell >$-Wada dessins associated with projective spaces $\mathbb{P}^m(\mathbb{F}_n)$, for which $n = p, p \not\equiv 0, 1 \mod (m+1)$, $m+1$ prime. The semidirect product $\Phi_f \ltimes \Sigma_\ell$ is the full automorphism group and since $m+1$ is prime, the order f of the cyclic group $\Phi_f \cong \mathrm{Gal}(\mathbb{F}_p^{m+1}/\mathbb{F}_p)$ is also prime.
We consider differences of elements belonging to 'reduced' sets $(H_{k,k} D_f)_i$. If we want the Wada condition to be satisfied, we need:

$$(p^{hj} d_i - p^{(h+1)j} d_i), \ell) = 1\ , \quad h \in \mathbb{Z}/f\mathbb{Z}\ .$$

We write each difference in the following way

$$(p^{hj} d_i - p^{(h+1)j} d_i) = -p^{hj} d_i (p^j - 1)\ .$$

Then

1. the integer p^{hj} does not divide ℓ since
$$\ell = p^m + p^{m-1} + \ldots + 1\,;$$
2. we claim that the difference $(p^j - 1)$ also does not divide ℓ.

At first, we factorize ℓ and $p^j - 1$ in the following way:

$$p^j - 1 = (p-1)(p^{j-1} + p^{j-2} + \ldots + 1)\ ,$$
$$\ell = (p-1)(p^{m-1} + 2p^{m-2} + \cdot + m) + (m+1)\ .$$

Due to the condition $p \not\equiv 1 \mod (m+1)$ (see Proposition 5.2.6) and since $(m+1)$ is prime we have:

$$(p-1, m+1) = 1 \ ,$$

From the Euclidean algorithm follows:

$$(p-1, \ell) = 1 \ .$$

We now need to show $(\ell, (p^{j-1} + p^{j-2} + \ldots + 1)) = 1$.
First, we write ℓ in the following way:

$$\ell = p^m + \ldots + p^{m-j-1} + p^{m-j} + \ldots + p^{m-2j-1} + p^{m-2j} + \ldots + p^{m-3j-1} + \ldots\ldots + 1 \ .$$

We divide it by $(p^{j-1} + p^{j-2} + \ldots + 1)$ and obtain:

$$\begin{aligned} \ell =& (p^{j-1} + p^{j-2} + \ldots + 1)(p^{m-j+1} + p^{m-2j+1} + p^{m-3j+1} + \ldots) \\ &+ (p^{s_0} + p^{s_0-1} + p^{s_0-2} + \ldots + 1) \ , \quad s_0 < j-1, \ s_0 \in \mathbb{N} \ . \end{aligned}$$

We proceed with the Euclidean algorithm and divide $(p^{j-1} + p^{j-2} + \ldots + 1)$ by $(p^{s_0} + p^{s_0-1} + p^{s_0-2} + \ldots + 1)$. So we get:

$$\begin{aligned} (p^{j-1} + p^{j-2} + \ldots + 1) =& (p^{s_0} + p^{s_0-1} + p^{s_0-2} + \ldots + 1)(p^{j-1-s_0} + p^{j-1-2s_0} + \ldots + 1) \\ &+ (p^{s_1} + p^{s_1-1} + p^{s_1-2} + \ldots + 1) \quad s_1 < s_0, \ s_1 \in \mathbb{N} \ . \end{aligned}$$

We go on with the Euclidean algorithm. Since the exponents s_i are decreasing, in the end we get a remainder which is equal one. It thus follows

$$(\ell, (p^{j-1} + p^{j-2} + \ldots + 1)) = 1 \ ,$$

which implies $((p^j - 1), \ell) = 1$.
Therefore, whether the Wada condition is satisfied or not, only depends on the value of d_i. □

Example 34. We consider again the projective space $\mathbb{P}^4(\mathbb{F}_3)$ discussed in Example 30. Here we may construct regular Wada dessins $H_{8,8}\mathcal{D}$ only if we use 'reduced' sets starting with elements not belonging to the orbit of the integer 11. In fact, since $\ell = 121 = 11^2$ the elements of the set containing the orbit of 11 do not satisfy the Wada condition.

6.3.3 Defining Equations

Wada dessins $\mathcal{D}$ associated with projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ determine uniquely the Riemann surface X of the embedding. For $\mathcal{D}$ with signature $< q, q, \ell >$ we have

$$\frac{1}{q} + \frac{1}{q} + \frac{1}{\ell} < 1 \ .$$

In fact:

$$\frac{1}{q} + \frac{1}{q} + \frac{1}{\ell} = \frac{2\ell + q}{q\ell} \ .$$

Due to $q < \ell$, $q \geq 3$, $\ell \geq 7$ it follows:

$$\frac{2\ell + q}{q\ell} < 1 \qquad \text{since} \qquad 2 + \frac{q}{\ell} < q \ .$$

Thus X is a quotient surface of the hyperbolic plane $\mathbb{H}$ with a torsion-free subgroup Γ_1 of the triangle group Δ_1 with signature $< q, q, \ell >$ and presentation:

$$\Delta_1 =< \gamma_0, \gamma_1, \gamma_\infty | \gamma_0^q = \gamma_1^q = \gamma_\infty^\ell = \gamma_0\gamma_1\gamma_\infty = 1 > \quad .$$

I.e. we have $X := \Gamma_1 \backslash \mathbb{H}$. Since $\mathcal{D}$ determines the complex structure of X, it helps determining explicitely algebraic models for X.

The following considerations rely on work of Streit and Wolfart (see [SW00], [SW01]) and of Wootton (see [Woo07]).

We consider a Wada dessin $\mathcal{D}$ with automorphism group $\Phi_g \ltimes \Sigma_\ell$, $\Phi_g \subseteq \Phi_f := Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$, Σ_ℓ a Singer group (see Section 5) and we first look at the dessin $\mathcal{D}/\Sigma_\ell$. It has signature $< q, q, 1 >$ and is embedded in the Riemann sphere $\mathbb{P}^1(\mathbb{C})$ as it is easy to check applying the Euler formula:

$$2 - 2g = q - q + 2 \quad \Longrightarrow \quad g = 0 \ .$$

According to the definition given by Streit and Wolfart, we call $\mathcal{D}$ a **globe covering dessin**. The dessin $\mathcal{D}/\Sigma_\ell$ corresponds to a normal subgroup of the triangle group Δ_1, to its commutator subgroup Γ_q of signature $< 0; \ell^{(q)} >$, such that the quotient space $\Gamma_q \backslash \mathbb{H}$ has genus 0 and the quotient map

$$\mathbb{H} \longrightarrow \Gamma_q \backslash \mathbb{H} \cong \mathbb{P}^1(\mathbb{C}) \tag{6.17}$$

branches over q points with ramification index ℓ.

The dessin $\mathcal{D}/\Sigma_\ell$ with q cells and two vertices, one black and one white, has automorphism group

$$\mathrm{Aut}(\mathcal{D}/\Sigma_\ell) \cong C_q \ , \tag{6.18}$$

thus Γ_q is the kernel of the epimorphism

$$\begin{array}{lcl} \Delta_1 & \stackrel{\theta}{\longrightarrow} & C_q \\ \triangledown & & \\ \Gamma_q & & \end{array} \tag{6.19}$$

mapping generators γ_0 and γ_1 onto generators of C_q. The generator γ_∞ belongs to the kernel of θ.
We now consider the torsion-free subgroup Γ_1 of Δ_1. Since $\mathcal{D}$ is not regular Γ_1 is a torsion-free subgroup of Δ_1 but it is not a normal subgroup. Let $N_{\Delta_1}(\Gamma_1)$ be the normaliser of Γ_1 in Δ_1. We know (see Section 4.1 and Chapter 5):

$$\mathrm{Aut}(\mathcal{D}) \cong N_{\Delta_1}(\Gamma_1)/\Gamma_1 \cong \Phi_g \ltimes \Sigma_\ell \ , \tag{6.20}$$

with the group Γ_1 being the kernel of an epimorphism κ:

$$\begin{array}{lcl} N_{\Delta_1}(\Gamma_1) & \stackrel{\kappa}{\longrightarrow} & \Phi_g \ltimes \Sigma_\ell \\ \triangledown & & \\ \Gamma_1 & & \end{array} \tag{6.21}$$

Let a and c be generators of Φ_g and Σ_ℓ respectively. Due to (6.20), the group $N_{\Delta_1}(\Gamma_1)/\Gamma_1$ is generated by elements of the same order as a and c. Let γ_0^k (or γ_1^k), $k = \frac{q}{g}$, and γ_∞ be two such generating elements. Since Γ_1 is torsion-free, dividing $N_{\Delta_1}(\Gamma_1)$ by Γ_1 does not affect such elements. Thus, we may assume that $N_{\Delta_1}(\Gamma_1)$ is generated by γ_0^k and γ_∞ together with other possible generators contained in Γ_1. Under the action of κ the elements γ_0^k and γ_∞ are mapped onto a and c. Since Γ_q has signature $< 0; \ell^{(q)} >$ and $\Gamma_q \triangleleft \Delta_1$ we also have $\Gamma_q \triangleleft N_{\Delta_1}(\Gamma_1) \subset \Delta_1$. Restricting the action of κ onto Γ_q we get an epimorphism κ^* mapping Γ_q onto the normal subgroup Σ_ℓ of $\Phi_g \ltimes \Sigma_\ell$. Under the action of κ^* the q generating elements of Γ_q are mapped onto powers of the element c generating Σ_ℓ:

$$\begin{array}{ccc} N_{\Delta_1}(\Gamma_1) & \stackrel{\kappa}{\longrightarrow} & \Phi_g \ltimes \Sigma_\ell \\ \triangledown & & \triangledown \\ \Gamma_q & \stackrel{\kappa^*}{\longrightarrow} & \Sigma_\ell \end{array} \tag{6.22}$$

The group Γ_q is the kernel of an epimorphism σ mapping $N_{\Delta_1}(\Gamma_1)$ onto the quotient group $\Phi_g \cong (\Phi_g \ltimes \Sigma_\ell)/\Sigma_\ell$:

$$\begin{array}{lcl} N_{\Delta_1}(\Gamma_1) & \stackrel{\sigma}{\longrightarrow} & \Phi_g \\ \triangledown & & \\ \Gamma_q & & \end{array} \tag{6.23}$$

Under the action of σ the generating element γ_0^k is mapped onto the generating element a of Φ_g, γ_∞ is mapped onto one and belongs to the kernel Γ_q of σ.
Due to (6.21) Γ_1 is a normal subgroup of Γ_q and since Γ_q is the preimage of Σ_ℓ under the action of κ, we have:

$$\begin{array}{lcl} \Gamma_q & \stackrel{\kappa^*}{\longrightarrow} & \Sigma_\ell \cong \Gamma_q/\Gamma_1 \\ \triangledown & & \\ \Gamma_1 & & \end{array} \tag{6.24}$$

According to results of Streit and Wolfart [SW00], [SW01], of Wootton [Woo07] and of González-Díez [GD91] we may thus determine algebraic models for the surface X:

Proposition 6.3.6. *Let Γ_q of signature $< 0; \ell^{(q)} >$ be the unique normal subgroup of the triangle group Δ_1 of signature $< q, q, \ell >$, $q > 2$, $l > 3$ with factor group C_q. Let Γ_1 of signature $< (\ell-1)(q-2)/2; 0 >$ be the torsion-free kernel of the epimorphism $\Gamma_q \longrightarrow \Sigma_\ell$ sending the canonical elliptic generators γ_i, $i = 0, \dots, q-1$ of Γ_q onto $b_i \in (\mathbb{Z}/\ell\mathbb{Z})^*$ with $\sum b_i \equiv 0 \mod \ell$. Let $(0, \zeta_q^i)$ be the ramification points of the mapping $\mathbb{H} \longrightarrow \Gamma_q \backslash \mathbb{H} \cong \mathbb{P}^1(\mathbb{C})$. Then as an algebraic curve, the quotient surface $X := \Gamma_1 \backslash \mathbb{H}$ has a (singular, affine) model given by the equation:*

$$y^\ell = \prod_{i=0}^{q-1} (x - \zeta_q^i)^{b_i} \,. \tag{6.25}$$

Proof. See mainly Section 1 of [GD91] and partially [SW01]. □

We remark here that our choice of the exponents $b_0, \dots, b_{q-1}$ is different from the one of Streit and Wolfart, which turns out to be incorrect in [SW01]. Our choice is justified in the following way.
Let c be a generator of the Singer group Σ_ℓ. It acts on the white vertices w and

on the black vertices b of each cell of the dessin $\mathcal{D}$ embedded in $X := \Gamma_1\backslash\mathbb{H}$ as (see Section 5.1)

$$\begin{aligned} c: \quad w &\longmapsto w+1 \\ b \quad &\longmapsto b+1 \ . \end{aligned}$$

According to the construction of Wada dessins described in Chapter 5 the action of each power c^{b_i} with exponent $b_i = (d_i - d_{i+1}) \mod \ell$ for some elements d_i, d_{i+1} of the underlying difference set D_g is thus given by:

$$\begin{aligned} c^{b_i}: \quad w &\longmapsto w+b_i \\ b &\longmapsto b+b_i \ . \end{aligned}$$

Thus on each of the q cells the corresponding power c^{b_i} fixes the cell mid points and rotates the black and the white vertices around it.
We introduce local coordinates (x, y). In these coordinates, the fixed points can be normalized to be $(\zeta_q^i, 0)$, $i \in \mathbb{Z}/q\mathbb{Z}$. The action of the powers c^{b_i} on the vertices on the cell bounaries is, locally, a rotation by the angle $\frac{2\pi}{\ell}$, i.e. it is expressed by the multiplier ζ_ℓ in such a way that:

$$c^{b_i}: \quad (x, y) \longmapsto (x, \zeta_\ell y) \ .$$

It follows that locally on each cell, the Singer automorphism c acts around the fixed points $(\zeta_q^i, 0)$ by multiplication with powers $\zeta_\ell^{\bar{b_i}}$. The integer $\bar{b_i}$ is the inverse of b_i in $(\mathbb{Z}/\ell\mathbb{Z})^*$ and we have

$$c^{b_i} : (x, y) \longmapsto (x, \zeta_\ell^{\bar{b_i} b_i} y) = (x, \zeta_\ell y) \ .$$

The action of the Singer automorphisms c^{b_i} on each cell justifies the choice of the exponents $b_1, \ldots, b_q$ for the factors of the product.
Moreover, we need the condition $\sum b_i \equiv 0 \mod \ell$ to make sure that the ramification points of the covering

$$\begin{aligned} f_1: \quad X \quad &\longrightarrow \quad \mathbb{P}^1(\mathbb{C}) \cong \Sigma_\ell\backslash X \\ (x, y) \quad &\longmapsto \quad x \end{aligned}$$

are only the cell mid points with coordinates $(\zeta_q^i, 0)$ such that the points with $x = \infty$

are not ramified. In fact, let $x \neq 0$. We may write Equation (6.25) as:

$$\begin{aligned} y^\ell &= \prod_{i=0}^{q-1}(x-\zeta_q^i)^{b_i} \\ &= \prod_{i=0}^{q-1} x^{b_i}(1-\frac{\zeta_q^i}{x})^{b_i} \\ &= x^{\sum_i^{q-1} b_i} \prod_{i=0}^{q-1}(1-\frac{\zeta_q^i}{x})^{b_i} \ . \end{aligned}$$

Due to the condition $\sum b_i \equiv 0 \mod \ell$ we can suppose without loss of generality $x^{(\sum b_i \mod \ell)} = 1$. Thus points with $x = \infty$ have coordinates:

$$(\infty, y_r = \zeta_\ell^r) \ , \quad r = 1, \ldots, \ell \ .$$

Under the action of f_1 each of them is mapped onto ∞, which on $\mathbb{P}^1(\mathbb{C})$ is thus not critical, having ℓ preimages.
Points with $x = 0$ are also unramified and have coordinates

$$(0, y_r = \zeta_\ell^r \cdot \zeta_q^{\tilde{b}}) \ , \quad \tilde{b} = \sum_{i=0}^{q-1} i \cdot b_i \ .$$

Under the action of f_1 each of them is mapped onto 0 which thus, similarly to ∞, is not ramified on $\mathbb{P}^1(\mathbb{C})$ having ℓ preimages.
Due to our considerations above, for $\mathcal{D}$ on X it is reasonable to make the following identification: the white vertices of $\mathcal{D}$ on X correspond to points with coordinates (∞, ζ_ℓ^r) and are mapped by f_1 onto the unique white vertex of $\mathcal{D}/\Sigma_\ell$ on $\mathbb{P}^1(\mathbb{C})$ corresponding to ∞. The black vertices of $\mathcal{D}$ correspond to points with coordinates $(0, \zeta_\ell^r \cdot \zeta_q^{\tilde{b}})$ and are mapped by f_1 onto the unique black vertex of $\mathcal{D}/\Sigma_\ell$ corresponding to 0.
As we have seen, the q cell mid points of $\mathcal{D}$ correspond to points with coordinates $(\zeta_q^i, 0)$ and are mapped by f_1 onto the q cell mid points ζ_q^i of $\mathcal{D}/\Sigma_\ell$.

Proposition 6.3.6 can be easily extended to dessins $H_{k,k}\mathcal{D}$ resulting from 'mock' Wilson operations applied to dessins $\mathcal{D}$. They are, in fact, still **globe covering** dessins as it is easy to check. In 6.3.6 we need to replace q with g and since $H_{k,k}\mathcal{D}$ is regular we need to replace Γ_1 with a torsion-free normal subgroup Γ_2 of a triangle group Δ_2. The group Δ_2 has signature $< g, g, \ell >$ and presentation:

$$\Delta_2 =< \delta_0, \delta_1, \delta_\infty | \delta_0^g = \delta_1^g = \delta_\infty^\ell = \delta_0\delta_1\delta_\infty = 1 > \ .$$

Due to the construction of dessins $H_{k,k}\mathcal{D}$ sketched in Section 6.3.2, the Singer group Σ_ℓ still acts on the white vertices w and on the black vertices b of the cell boundaries as

$$\begin{array}{rccl} c^{m_i}: & w & \longmapsto & w + m_i \ , \\ & b & \longmapsto & b + m_i \ , \end{array}$$

where $m_i = d_i - d_{i+1}$, $d_i, d_{i+1} \in H_k D_g$, $i \in \mathbb{Z}/g\mathbb{Z}$, D_g being the underlying difference set of the dessin $\mathcal{D}$. Since we only consider Wada dessins, each m_i is in $(\mathbb{Z}/\ell\mathbb{Z})^*$ and due to the definition of each m_i we have $\sum_{i=0}^{g-1} m_i \equiv 0 \mod \ell$. Thus a (singular, affine) model of the surface $Y := \Gamma_2 \backslash \mathbb{H}$ is given by

$$y^\ell = \prod_{i=0}^{g-1} (z - \zeta_g^i)^{m_i} \ .$$

The following proposition holds:

Proposition 6.3.7. *Let $\mathcal{D}$ be a $< q, q, \ell >$-Wada dessin associated with a projective space $\mathbb{P}^m(\mathbb{F}_n)$, $n = p^e$. Let the conditions of Proposition 6.3.6 hold. We replace q with g, Δ_1 with Δ_2 with signature $< g, g, \ell >$ and Γ_1 with a torsion-free normal subgroup $\Gamma_2 \triangleleft \Delta_2$. Thus, the Riemann surface $Y := \Gamma_2 \backslash \mathbb{H}$ defined by a dessin $H_{k,k}\mathcal{D}$, $k = \frac{q}{g}$ resulting from a 'mock' Wilson operation $H_{k,k}$ applied to $\mathcal{D}$ admits a (singular, affine) model given by*

$$w^\ell = \prod_{i=0}^{g-1} (z - \zeta_g^i)^{m_i} \ . \tag{6.26}$$

with $m_i = d_i - d_{i+1}$, $d_i, d_{i+1} \in H_k D_g$, D_g being the underlying difference set of $\mathcal{D}$.

Example 35. We consider the projective plane $\mathbb{P}^2(\mathbb{F}_5)$ with $\ell = 31$ points and hyperplanes. On each hyperplane lie $q = 6$ points and, viceversa, $q = 6$ hyperplanes are incident with a point. Using the difference set ([Bau71])

$$D_3 = \{1, 11, 5, 24, 25, 27\} \mod 31$$

we may construct a $< 6, 6, 31 >$-Wada dessin $\mathcal{D}$. The full automorphism group of $\mathcal{D}$ is $\Phi_3 \ltimes \Sigma_{31}$, $\Phi_3 \cong Gal(\mathbb{F}_{5^3}/\mathbb{F}_5)$. According to Proposition 6.3.6, for the surface X in which $\mathcal{D}$ is embedded we obtain following equation:

$$y^{31} = (x-1)^{21}(x-\zeta_6)^6(x-\zeta_6^2)^{12}(x-\zeta_6^3)^{30}(x-\zeta_6^4)^{29}(x-\zeta_6^5)^{26} \ . \tag{6.27}$$

Applying to D_3 the 'mock' operator H_2 we obatin the following 'reduced' set:

$$H_2 D_3 = \{1, 5, 25\} \mod 31 \ .$$

and we construct a regular $< 3, 3, 31 >$-Wada dessin $H_{2,2}\mathcal{D}$. The equation of the surface Y of the embedding is thus

$$w^{31} = (z-1)^{27}(z-\zeta_3)^{11}(z-\zeta_3^2)^{24} . \qquad (6.28)$$

Remark. We may consider the whole set of Wada dessins $(H_{k,k}\mathcal{D})_i$, $i = 1, \ldots, k'$, $k' \leqslant k$, which may be constructed with 'reduced' sets

$$(H_{k,k}D_g)_i = \{d_i, t^j d_i, t^{2j} d_i, \ldots, t^{(g-1)} d_i\} \ , d_i \in D_g \ .$$

As we have seen with Corollary 6.3.3 for each set $(H_k D_g)_i$ we have $d_i \in (\mathbb{Z}/\ell\mathbb{Z})^*$, otherwise the considered dessins would not have the Wada property. This means that we may normalize d_1 such that $d_1 \equiv 1 \mod \ell$ and all regular Wada dessins $(H_{k,k}\mathcal{D}_g)_i$ are isomorphic to each other, resulting from a multiplication of the set $(H_k D_g)_1$ with integers $d_1^* \cdot d_i$, $d_1^* \in (\mathbb{Z}/\ell\mathbb{Z})^*$, $d_1^* d_1 \equiv 1 \mod \ell$. The underlying surfaces X_i are also isomorphic to each other. In fact, let Equation (6.26) correspond to the surface X_1 of the embedding of the dessin $(H_{k,k}\mathcal{D})_1$. The equations defining the other surfaces X_i, $i = 2, \ldots, k'$ are thus given by

$$w^\ell = \prod_{j=0}^{g-1} (z-\zeta_g^j)^{m_j \cdot d_1^* \cdot d_i} . \qquad (6.29)$$

I.e. the exponents of the factors of the original equation are all multiplied with a common integer $d_1^* d_i$. According to results of González-Díez (Lemma 5.2, [GD91]) and Wootton ([Woo07]) surfaces which are coverings of $\mathbb{P}^1(\mathbb{C})$ and are defined in this way are isomorphic to each other.

6.3.4 Coverings

Wada dessins $\mathcal{D}$ with signature $< q, q, \ell >$ and their regular counterparts $H_{k,k}\mathcal{D}$ with signature $< g, g, \ell >$ are embedded in Riemann surfaces X and Y. As we have seen in Section 6.3.3 both surfaces are defined as quotients of the hyperbolic plane with torsion-free subgroups of triangle groups. For the surface $X := \Gamma_1 \backslash \mathbb{H}$ the group Γ_1 is a torsion-free subgroup of the triangle group Δ_1 with signature $< q, q, \ell >$. For $Y := \Gamma_2 \backslash \mathbb{H}$ the group Γ_2 is not only a torsion-free subgroup of the triangle group Δ_2 with signature $< g, g, \ell >$, but Γ_2 is even a normal subgroup. The dessins $H_{k,k}\mathcal{D}$ are in fact regular.
We show that a ramified covering of Y by X exists. We first prove the following proposition:

Proposition 6.3.8. *We consider a uniform* $< q, q, \ell >$*-Wada dessin* $\mathcal{D}$ *associated with a projective space* $\mathbb{P}^m(\mathbb{F}_n)$ *and a regular* $< g, g, \ell >$*-Wada dessin* $H_{k,k}\mathcal{D}$*,* $g = \frac{q}{k}$ *constructed as described in Proposition 6.3.2. Both dessins have the same automorphism group* $\Phi_g \ltimes \Sigma_\ell$ *and we suppose* $(k, g) = 1$*.*
Let $\Gamma_1\backslash\mathbb{H}$ *be the Riemann surface* X *the dessin* $\mathcal{D}$ *is embedded in, and let* $\Gamma_2\backslash\mathbb{H}$ *be the Riemann surface* Y *defined by* $H_{k,k}\mathcal{D}$*. Since* $\mathcal{D}$ *is uniform* Γ_1 *is a torsion free subgroup of the triangle group* Δ_1 *with signature* $< q, q, \ell >$*. Let* $N_{\Delta_1}(\Gamma_1)$ *be the normalizer of* Γ_1 *in* Δ_1*.*
Since $H_{k,k}\mathcal{D}$ *is regular* Γ_2 *is a torsion-free normal subgroup of the triangle group* Δ_2 *with signature* $< g, g, \ell >$*.*
Between Δ_1 *and* Δ_2 *we define an epimorphism* φ*. If we restrict the action of* φ *on the elements of the subgroup* $N_{\Delta_1}(\Gamma_1)$ *and define* $\varphi^* := \varphi|_{N_{\Delta_1}(\Gamma_1)}$ *then we have:*

$$\varphi^*(\Gamma_1) = \Gamma_2 \quad \textit{and} \quad \varphi^{*-1}(\Gamma_2) = \Gamma_1 \ . \tag{6.30}$$

Proof. We start with the triangle groups Δ_1 and Δ_2. They have the following presentations:

$$\Delta_1 =< \gamma_0, \gamma_1, \gamma_\infty | \gamma_0^q = \gamma_1^q = \gamma_\infty^\ell = \gamma_0\gamma_1\gamma_\infty = 1 > ,$$

$$\Delta_2 =< \delta_0, \delta_1, \delta_\infty | \delta_0^g = \delta_1^g = \delta_\infty^\ell = \delta_0\delta_1\delta_\infty = 1 > \ .$$

Between them we may define an epimorphism φ mapping generators of Δ_1 onto generators of Δ_2:

$$\varphi : \quad \Delta_1 \xrightarrow{\varphi} \Delta_2 \ ,$$

$$\gamma_i \mapsto \delta_i \qquad \text{for } i = 0, 1, \infty \ .$$

Elements $\gamma_0^{\frac{q}{k}}, \gamma_1^{\frac{q}{k}}$ belong to the kernel of φ.
We know

$$\mathrm{Aut}(\mathcal{D}) \cong N_{\Delta_1}(\Gamma_1)/\Gamma_1 \ ,$$

$$\mathrm{Aut}(H_{k,k}\mathcal{D}) \cong \Delta_2/\Gamma_2 \ . \tag{6.31}$$

Moreover we have (see Proposition 6.3.2)

$$\mathrm{Aut}(\mathcal{D}) \cong \Phi_g \ltimes \Sigma_\ell \cong \mathrm{Aut}(H_{k,k}\mathcal{D}) \ . \tag{6.32}$$

Let a and b be generators of Φ_g and of Σ_ℓ respectively. Due to (6.32) $N_{\Delta_1}(\Gamma_1)/\Gamma_1$ and Δ_2/Γ_2 are generated by elements of the same order of a and b. Let γ_0^k (or γ_1^k)

and γ_∞ be two such generating elements of $N_{\Delta_1}(\Gamma_1)/\Gamma_1$. For Δ_2/Γ_2 we just take the generators δ_0 (or δ_1) and δ_∞. We now restrict the action of the epimorphism φ to the elements of the subgroup $N_{\Delta_1}(\Gamma_1)$ and we define $\varphi^* := \varphi|_{N_{\Delta_1}(\Gamma_1)}$. We claim that φ^* describes an epimorphism between $N_{\Delta_1}(\Gamma_1)$ and Δ_2. Since Γ_1 is torsion free, dividing $N_{\Delta_1}(\Gamma_1)$ by Γ_1 does not affect the torsion elements γ_0^k and γ_∞. Thus, since they are generators of $N_{\Delta_1}(\Gamma_1)/\Gamma_1$, they also generate $N_{\Delta_1}(\Gamma_1)$ together with possible generators contained in Γ_1 . Since $(k, g) = 1$, k is in $(\mathbb{Z}/g\mathbb{Z})^*$. We consider the power $\gamma_0^{m\cdot k}$ of the generator γ_0^k where m is the inverse element of k in $(\mathbb{Z}/g\mathbb{Z})^*$. The element $\gamma_0^{m\cdot k}$ is also a generating element of $N_{\Delta_1}(\Gamma_1)$. So we can replace the generator γ_0^k with $\gamma_0^{m\cdot k}$.
Under the action of φ^* we map the elements $\gamma_0^{m\cdot k}$ and γ_∞ onto generators of Δ_2, in fact:

$$\gamma_0^{m\cdot k} \overset{\varphi^*}{\longmapsto} \delta_0^{m\cdot k} = \delta_0 \ ,$$
$$\gamma_\infty \overset{\varphi^*}{\longmapsto} \delta_\infty \ .$$

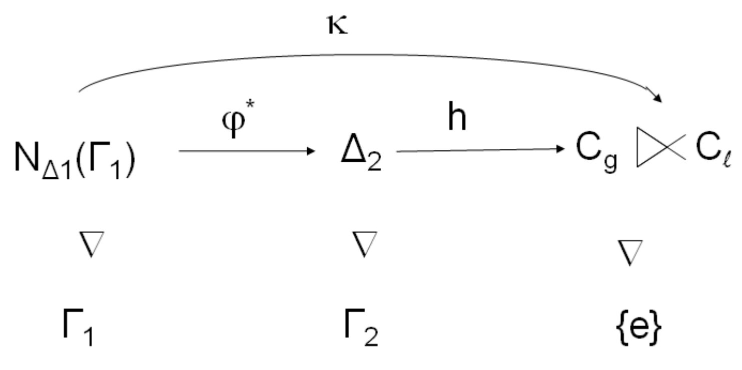
We obtain the third generator δ_1 applying φ^* to the element $(\gamma_0^{-m\cdot k}\gamma_\infty^{-1})$:

$$(\gamma_0^{-m\cdot k}\gamma_\infty^{-1}) \longmapsto (\delta_0^{-m\cdot k}\delta_\infty^{-1}) = \delta_0^{-1}\delta_\infty^{-1} = \delta_1 \ .$$

Thus φ^* describes an epimorphism between $N_{\Delta_1}(\Gamma_1)$ and Δ_2 since each generating element of Δ_2 has a preimage in $N_{\Delta_1}(\Gamma_1)$.
Due to the action of φ^* we may define:

$$\Gamma_2 := \varphi^*(\Gamma_1) \ .$$

We show that we also have $\varphi^{*-1}(\Gamma_2) = \Gamma_1$.
Besides the epimorphism φ^*, we consider the epimorphims h and k mapping Δ_2 onto $\Phi_g \ltimes \Sigma_\ell \cong \Delta_2/\Gamma_2$ and $N_{\Delta_1}(\Gamma_1)$ onto $\Phi_g \ltimes \Sigma_\ell \cong N_{\Delta_1}(\Gamma_1)/\Gamma_1$ respectively:



The subgroup Γ_2 is the kernel of h and the subgroup Γ_1 is the kernel of k. Thus the kernel of φ^* mapping Γ_1 onto Γ_2 is contained in Γ_1. From the second isomorphism theorem follows $\varphi^{*-1}(\Gamma_2) = \Gamma_1$. □

We now prove the following

Proposition 6.3.9. *Under the conditions of Proposition 6.3.8 there exists a ramified covering of the surface* $Y := \Gamma_2 \backslash \mathbb{H}$ *by the surface* $X := \Gamma_1 \backslash \mathbb{H}$.

Proof. On the hyperbolic plane $\mathbb{H}$ we consider the fundamental regions [1] F and F' of the triangle groups Δ_1 and Δ_2. According to the Riemann mapping theorem a biholomorphic function f exists mapping the inner part of F onto F' (see Figure 6.7). Over the smooth parts of the boundary of F, i.e. over the edges without the

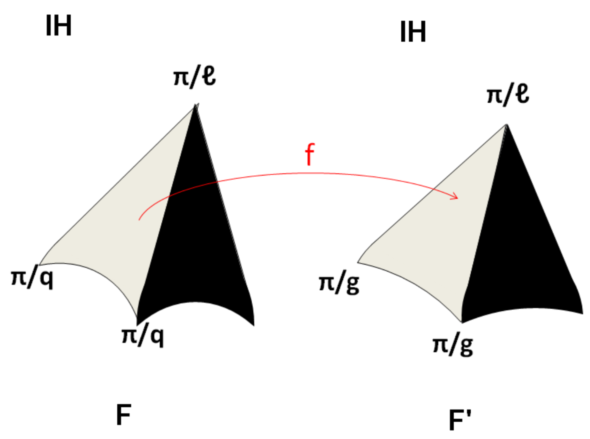


Figure 6.7: *Biholomorphic function f mapping the fundamental region F of the triangle group Δ_1 onto the fundamental region F' of the triangle group Δ_2. The hyperbolic plane $\mathbb{H}$ is here identified with the unit disk.*

vertices, the function f can be extended holomorphically. Even more, applying the Schwarz symmetry principle the function f can be extended holomorphically over the whole hyperbolic plane $\mathbb{H}$, except over the elliptic fixed points of each triangle group, i.e. over the vertices of the fundamental regions. Over them f can be

[1] According to [Leh66] a fundamental region of a triangle group Δ acting on $\mathbb{H}$ is a subset F of $\mathbb{H}$ containing exactly one point of each Δ-orbit of points. Every other point $z' \in \mathbb{H}$ is equivalent to a point of F. About triangle group operating on $\mathbb{H}$ see also [Kat92] and [Wol06].

extended holomorphically due to Riemann's removable singularity theorem. Thus, the function f is globally well defined over the whole hyperbolic plane $\mathbb{H}$. In fact, let us consider an elliptic fixed point of Δ_1 of order q and an orbit $\{\alpha z\}$, $\alpha \in \Delta_1$, $z \in \mathbb{H}$ of points around such a fixed point. Thus, the function f maps the orbit $\{\alpha z\}$ onto an orbit of points around a fixed point of Δ_2 of order g. Due to $(g, q) = k$, one 'loop' of points around a fixed point of order q corresponds, under the action of f, to k 'loops' of points around a fixed point of order g (see also [Kle81], Section 63). The action of f is compatible with the action of the epimorphism φ

$$\varphi : \quad \Delta_1 \longrightarrow \Delta_2$$

we have defined in Proposition 6.3.8. I.e. points $\alpha_1 z$, $\alpha_2 z$ belonging to the same orbit under the action of elements $\alpha_1, \alpha_2 \in \Delta_1$ are mapped by f onto points $\varphi(\alpha_1)f(z)$, $\varphi(\alpha_2)f(z)$ belonging to the same orbit under the action of elements $\varphi(\alpha_1), \varphi(\alpha_2) \in \Delta_2$.

The function f induces a covering of the surface $Y := \Gamma_2\backslash\mathbb{H}$ by the surface $X := \Gamma_1\backslash\mathbb{H}$. We show that the action of f on the points of the surfaces is well defined. Due to Proposition 6.3.8 we have that $\varphi^*(\Gamma_1) = \Gamma_2$ and $\varphi^{*-1}(\Gamma_2) = \Gamma_1$, where φ^* describes the action of φ restricted to the normalizer $N_{\Delta_1}(\Gamma_1)$ of Γ_1 in Δ_1. We consider points $\alpha_1\Gamma_1 z$ and $\alpha_2\Gamma_2 z$ on X which belong to the same orbit under the action of the automorphism group of the dessin $Aut(\mathcal{D}) \cong N_{\Delta_1}(\Gamma_1)/\Gamma_1$, $\alpha_1, \alpha_2 \in Aut(\mathcal{D})$. They are mapped by f onto points of Y which also belong to the same orbit, in fact:

$$f(\alpha_1\Gamma_1 z) = \varphi^*(\alpha_1)\varphi^*(\Gamma_1)f(z) = \alpha_1'\Gamma_2 f(z) \ ,$$

$$f(\alpha_2\Gamma_1 z) = \varphi^*(\alpha_2)\varphi^*(\Gamma_1)f(z) = \alpha_2'\Gamma_2 f(z) \ ,$$

α_1', α_2' being the images of α_1 and α_2 in Δ_2/Γ_2. Due to $\varphi^{*-1}(\Gamma_2) = \Gamma_1$ the vice versa is also true and points of Y belonging to the same orbit under the action of $Aut(\mathcal{D}) \cong \Delta_2/\Gamma_2$ have as preimages points belonging to the same orbit on X.

As we have seen above over the elliptic fixed points of Δ_1 and Δ_2 the function f can be extended holomorphically. Such points are the critical points of order k of the covering, which is ramified in them. □

Remark. The ramified covering f of Y by X is of degree k and satisfies the Riemann-Hurwitz relation:

$$g_1 = n(g_2 - 1) + 1 + \frac{B}{2} \ . \tag{6.33}$$

Here g_1 is the genus of X, g_2 is the genus of Y, n is the degree of the mapping f, B is the *total branching number* (see [FK92]) defined as the sum of the branch numbers b_f over all crtical points V. The critical points are in our case the white and the black vertices of $\mathcal{D}$ on X. Thus we have:

1. $2 - 2g_1 = 2\ell - q\ell + q$ (Euler Formula) ,
2. $2 - 2g_2 = 2\ell - \frac{q}{k}\ell + \frac{q}{k}$ (Euler Formula) ,
3. $B = \sum_{V \in X} b_f(V) = 2\ell(k-1)$,
4. $n = k$.

Writing the values of g_1, g_2, B, n in Equation (6.33), we obtain following equation:

$$-\frac{(2\ell - q\ell - q - 2)}{2} = k(\frac{-2\ell + \frac{q}{k}\ell - \frac{q}{k} + 2}{2} - 1) + 1 + \ell(k-1)$$

and it is easy to check that the Riemann-Hurwitz relation is in fact satisfied.

Example 36. We consider the projective space $\mathbb{P}^4(\mathbb{F}_2)$ with associated Wada dessin $\mathcal{D}$ with signature $< 15, 15, 31 >$ (see also Example 17 and Example 18). Applying the 'mock' Wilson operator $H_{3,3}$ to the edges of $\mathcal{D}$ we obtain a regular Wada dessin $H_{3,3}\mathcal{D}$ with signature $< 5, 5, 31 >$. The automorphism group of both dessins is $\Phi_5 \ltimes \Sigma_{31}$. The surface X the dessin $\mathcal{D}$ is embedded in is a ramified covering of the surface Y with dessin $H_{3,3}\mathcal{D}$.

Outlook

During the work on this thesis the topics concerning the groups of automorphisms and the 'mock' Wilson operations related to Wada dessins resulted to be far more interesting and productive than expected. Besides the results presented a lot of new questions arose. We list and explain here some of them, which can be a hint for further research:

1. In Chapter 3 we have seen that there exists a relation between difference sets and the group $\Phi_f \cong Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$, $n = p^e$, $f = e \cdot (m+1)$, generated by the Frobenius automorphism σ acting on points and hyperplanes of a projective space $\mathbb{P}^m(\mathbb{F}_n)$. We have seen that one or more difference sets exist which are fixed under the action of Φ_f. In Chapter 5 we have seen that under some conditions the group Φ_f or a subgroup Φ_g divides the elements of a difference set it fixes into orbits of the same length. For such a difference set we have seen that we may order its elements in a way compatible with the action of $\Phi_g \subseteq \Phi_f$ (see Definition 5.4.2):

$$\begin{aligned} D_g = &\{d_1, \dots, d_k,\ t^r d_1, \dots, t^r d_k,\ \dots\dots\dots, t^{(g-1)r} d_1, \dots, t^{(g-1)r} d_k\}\ , \\ &\text{for an } r \in (\mathbb{Z}/g\mathbb{Z})^*,\ t = p^r,\ \frac{q}{g} = k,\ r \not\equiv 0 \mod f,\ r \cdot g \equiv 0 \mod f\ . \end{aligned}$$

   It would be very interesting to develop a method to construct difference sets, if we know that they are difference sets fixed by the non-trivial elements of a group $\Phi_g \subseteq \Phi_f$. For these sets it is sufficient to have a method to determine the first k elements. The others are equal to the first elements multiplied by powers of the integer t.

2. In Chapter 5 we have seen that for the special case of $f = m+1$ prime, under some conditions, the group Φ_f is a group of automorphisms of Wada dessins associated with projective spaces $\mathbb{P}^m(\mathbb{F}_n)$. For the more general case we have seen that very often not the complete group Φ_f but subgroups $\Phi_g \subseteq \Phi_f$ are

groups of automorphisms of associated dessins. For the group order g we have seen that it has to divide q, the valency of the black and of the white vertices and, at the same time, the number of elements of the underlying difference set D_g. But on its structure we have made no precise statements. Relying on many examples we have studied, it seems to be reasonable that the order g has to be prime, nevertheless further examples and finally a concrete proof are necessary to confirm or to discard this assumption.
We remark that for the projective plane $\mathbb{P}^2(\mathbb{F}_8)$ the order f of the group Φ_f is $f = 9$. This group may be a group of automorphisms of Wada dessins associated with $\mathbb{P}^2(\mathbb{F}_8)$. Nevertheless, the fact that in this case f is not prime is a very special situation which might not influence the general assumption. The projective planes $\mathbb{P}^2(\mathbb{F}_2)$ and $\mathbb{P}^2(\mathbb{F}_8)$ are, in fact, 'exceptions' among projective spaces $\mathbb{P}^m(\mathbb{F}_n)$ since they are the only ones whose graphs can be embedded as regular dessins.

3. In Chapter 6 we have seen that 'mock' Wilson operations applied on Wada dessins may lead to the construction of new dessins which are regular. We have seen that the surface X defined by the original dessin is a covering for the surface Y defined by the dessin resulting from the Wilson operation (see Section 6.3.4). Unfortunately, we were not able to explicitely give the function f describing the covering, but we observed that we may derive the equation of the surface Y from the equation of the surface X mapping the coefficients of the first equation onto the coefficients of the second one.
We start considering a $< q, q, \ell >$-Wada dessin $\mathcal{D}$ associated with a projective space $\mathbb{P}^m(\mathbb{F}_n)$, $n = p^e$, and constructed with a Frobenius difference set D_g whose elements are ordered in a way compatible with the action of $\Phi_g \subseteq \Phi_f \cong Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$, $g = \frac{q}{k}$ [2]:

$$\begin{aligned} D_g =&\{d_0, \dots, d_{k-1},\ t^r d_0, \dots, t^r d_{k-1},\ \dots\dots\dots, t^{(g-1)r} d_0,\ \dots,\ t^{(g-1)r} d_{k-1}\}, \\ &\forall r \in (\mathbb{Z}/g\mathbb{Z})^*,\ t = p^r,\ \frac{q}{g} = k,\ r \not\equiv 0 \mod f,\ r \cdot g \equiv 0 \mod f\ . \end{aligned} \tag{6.34}$$

We suppose $(k, g) = 1$ and ℓ prime.
Furthermore we consider the $< g, g, \ell >$-Wada dessin $H_{k,k}\mathcal{D}$ resulting from the action of a 'mock' Wilson operator $H_{k,k}$ on $\mathcal{D}$ and having the underlying

[2] Other than in Definition 5.4.2 we here number the elements of D_g using the integers $0, \dots, k-1$. This has only practical reasons, since in this way some of the steps of the following construction simplify.

'reduced' set

$$H_{k,k}D_g = \{d_0, t^r d_0, t^{2r} d_0, \ldots, t^{(g-1)r} d_0\} \ . \tag{6.35}$$

The dessin $H_{k,k}\mathcal{D}$ is constructed as described in Proposition 6.3.2. We show now that we may derive the Equation defining Y (see Equation (6.26)) or defining a surface $Y' \cong Y$ from the equation of X (see Equation (6.25)).

We first consider the action of the automorphism group Φ_g on the set of cells of the dessin $\mathcal{D}$. With local coordinates (x, y) we describe the cell mid points as $(\zeta_q^i, 0)$, $i \in \mathbb{Z}/q\mathbb{Z}$. The action of Φ_g on the cells is expressed by the multiplier ζ_q^k:

$$(\zeta_q^i, 0) \longmapsto (\zeta_q^k \cdot \zeta_q^i, 0) \ .$$

On the cells of the dessin $H_{k,k}\mathcal{D}$ the automorphism group Φ_g acts by a multiplication with the multiplier ζ_g. Identifying the cell mid points of the dessin $H_{k,k}\mathcal{D}$ with the points $(\zeta_g^j, 0)$, $j \in \mathbb{Z}/g\mathbb{Z}$ we have:

$$(\zeta_g^j, 0) \longmapsto (\zeta_g \cdot \zeta_g^j, 0) \ .$$

Thus in order to obtain an admissible correspondence between the action of Φ_g on the cell mid points of $\mathcal{D}$ and the one on the cell mid points of $H_{k,k}\mathcal{D}$ we define the following mapping between the points $(\zeta_q^i, 0)$ of X and the points $(\zeta_g^j, 0)$ of Y:

$$\begin{aligned} \theta : \quad & (\zeta_q^i, 0) \longmapsto ((\zeta_q^i)^{s\cdot k} = \zeta_g^{i\cdot s}, 0), \\ & s \in (\mathbb{Z}/g\mathbb{Z})^* \ , s \cdot k \equiv 1 \mod g \ . \end{aligned}$$

The roots of unity ζ_q^i and ζ_g^j are the coefficients of the equations of X and of Y respectively.

Without loss of generality we consider the difference set for which $j = 1$, so we have:

$$D_g = \{d_0, \ldots, d_{k-1}, \ td_0, \ldots, td_{k-1}, \ \ldots\ldots\ldots, t^{(g-1)}d_0, \ \ldots, \ t^{(g-1)}d_{k-1}\} \ , \tag{6.36}$$

and the equation (Equation (6.25)) of the surface X can be written in the following way:

$$y^\ell = \prod_{j=0}^{g-1} (x - \zeta_q^{j\cdot k})^{t^j(d_0-d_1)} (x - \zeta_q^{j\cdot k+g})^{t^j(d_{0+g}-d_{1+g})} \ldots (x - \zeta_q^{j\cdot k+(k-1)g})^{t^j(d_{0+(k-1)g}-d_{1+(k-1)g})} \ . \tag{6.37}$$

Under the action of θ we have:

$$\theta: \quad (\zeta_q^0, 0), (\zeta_q^g, 0), (\zeta_q^{2g}, 0), \ldots, (\zeta_q^{(k-1)g}, 0) \longmapsto (\zeta_g^0, 0) \; , \tag{6.38}$$

and due to the condition $s \in (\mathbb{Z}/g\mathbb{Z})^*$ they are the only cell mid points mapped onto ζ_g^0. Thus, extendig the action of θ to the terms of Equation (6.37) the terms which contain one of the roots of unity in (6.38) are mapped onto a term $(x - \zeta_g^0)$ with exponent:

$$\sigma_0 = (d_0 - d_1) + (d_{0+g} - d_{1+g}) + (d_{0+2g} - d_{1+2g}) + \ldots + (d_{0+(k-1)g} - d_{1+(k-1)g}) \; . \tag{6.39}$$

In the sum above we consider the indices of the terms $\mod k$. Thus using (6.36) we may write:

$$\begin{aligned} \sigma_0 = (d_0 - d_1) + t^{r_g}(d_{0+g} - d_{1+g}) + t^{r_{2g}}(d_{0+2g} - d_{1+2g}) + \\ \ldots + t^{r_{(k-1)g}}(d_{0+(k-1)g} - d_{1+(k-1)g}) \; . \end{aligned} \tag{6.40}$$

The exponents r_{ig} of the prime powers t depends on the value of $(i \cdot g)$. For instance, according to the chosen ordering of the elements of D_g, for $i = 1$ if $k < g < 2k$ we have $r_g = 1$. Moreover in the sum σ_0, apart from the first term, we always have to substitute terms d_k with $t \cdot d_0$, due to the fact that among the first k terms of D_g the last difference is $(d_{k-1} - t \cdot d_0)$ and not $(d_{k-1} - d_0)$. Since we have supposed $(g, k) = 1$ we know that for $n \neq 0$, $n \in \mathbb{Z}/g\mathbb{Z}$ none of the exponents of the factors

$$(x - \zeta_q^{n \cdot k + mg}) \; , m \in \mathbb{Z}/k\mathbb{Z}$$

will be a term of the sum σ_0. More in general, under the action of θ we have

$$(\zeta_q^{n \cdot k}, 0), (\zeta_q^{n \cdot k + g}, 0), (\zeta_q^{n \cdot k + 2g}, 0), \ldots, (\zeta_q^{n \cdot k + (k-1)g}, 0) \longmapsto (\zeta_g^n, 0) \; .$$

We consider again the action of θ on the terms of Equation (6.37). The exponents of the factors $(x - \zeta_q^{n \cdot k + mg})$ for a given $n \in \mathbb{Z}/g\mathbb{Z}$ are summed to be the exponent σ_n of a term $(x - \zeta_g^n)$:

$$\sigma_n = t^n(d_0 - d_1) + t^n(d_{0+g} - d_{1+g}) + t^n(d_{0+2g} - d_{1+2g}) + \ldots + t^n(d_{0+(k-1)g} - d_{1+(k-1)g}) \; . \tag{6.41}$$

Again, using the definition of D_g in (6.36) and considering all indices $\mod k$ as described above we obtain

$$\begin{aligned} \sigma_n &= t^n(d_0 - d_1) + t^n \cdot t^{r_g}(d_{0+g} - d_{1+g}) + t^n \cdot t^{r_{2g}}(d_{0+2g} - d_{1+2g}) + \\ &\quad \ldots + t^n \cdot t^{r_{(k-1)g}}(d_{0+(k-1)g} - d_{1+(k-1)g}) \\ &= t^n \cdot \sigma_0 \; . \end{aligned} \tag{6.42}$$

Thus applying θ to the coefficients of the equation of X (Equations (6.25) and (6.37)) we obtain a new equation

$$y^\ell = \prod_{j=0}^{g-1} (x - \zeta_g^j)^{t^j \sigma_0} , \tag{6.43}$$

for which the exponents $t^j \sigma_0 \mod \ell$ are prime to ℓ, since ℓ prime.
We set $z = x$ and $w = y$. The new equation describes a surface $Y' \cong Y$ if each exponent $t^j \sigma_0$ is equal to the corresponding exponent m_i up to multiplication with integers $a \in (\mathbb{Z}/\ell\mathbb{Z})^*$ (see Lemma 5.2, [GD91] and [Woo07]). Due to the definition of $H_{k,k}D_g$ we write Equation (6.26) as

$$w^\ell = \prod_{j=0}^{g-1} (z - \zeta_g^j)^{t^j (1-t) d_0} . \tag{6.44}$$

I.e. we need to prove

$$a \cdot t^j \cdot (1-t) \cdot d_0 \equiv t^j \cdot \sigma_0 \mod \ell$$
$$a \cdot (1-t) \cdot d_0 \equiv \sigma_0 \mod \ell .$$

Since $d_0 \in (\mathbb{Z}/\ell\mathbb{Z})^*$ (see the proof to Corollary 6.3.3) we write

$$a \cdot (1-t) \equiv d_0^* \cdot \sigma_0 , \quad d_0^* \in (\mathbb{Z}/\ell\mathbb{Z})^* ,$$

such that $d_0 \cdot d_0^* \equiv 1 \mod \ell$.
We may compute a if σ_0 is divisible by $(1-t)$. In the sum σ_0 all terms $d_0, \ldots, d_{k-1}$ occur twice with different powers of t as a multiplying factor and with opposite sign. So we may write σ_0 as a sum of terms

$$d_i \cdot (t^{n_1} - t^{n_2}) , \quad i \in \mathbb{Z}/k\mathbb{Z} , \quad n_1, n_2 \in \mathbb{Z}/g\mathbb{Z}$$

and each of these terms is divisible by $(1-t)$.
Due to the fact that ℓ is prime the integer

$$a \equiv \frac{d_0^* \cdot \sigma_0}{(1-t)} \mod \ell \tag{6.45}$$

is prime to ℓ. It thus follows that Equation (6.26)and Equation (6.43) define isomorphic surfaces $Y' \cong Y$. For $a \equiv 1 \mod \ell$ they define the same surface Y.

Remark. Our construction holds also in case that ℓ is not prime. In this case we need the sum σ_0 being prime to ℓ. Thus the integer a is still in $(\mathbb{Z}/\ell\mathbb{Z})^*$.

Example 37. We consider again the projective plane $\mathbb{P}^2(\mathbb{F}_5)$ with $q = 6$ and $\ell = 31$ (see Example 35). We may derive the equation of a surface $Y' \cong Y$ from the equation of X given in (6.27).
We introduce local coordinates (x, y) and identify the cell mid points of $\mathcal{D}$ with the coordinates $(\zeta_6^i, 0)$, $i \in \mathbb{Z}/6\mathbb{Z}$. The automorphism group $\Phi_3 \cong Gal(\mathbb{F}_{5^3}/\mathbb{F}_5)$ acts locally on the cell mid points with the multiplier ζ_6^2:

$$(\zeta_6^i, 0) \longmapsto (\zeta_6^{i+2}, 0) \ .$$

We may describe the cell mid points of the dessin $H_{2,2}\mathcal{D}$ with the coordinates $(\zeta_3^j, 0)$, $j \in \mathbb{Z}/3\mathbb{Z}$. The automorphism group Φ_3 acts locally on them with the multiplier ζ_3:

$$(\zeta_3^j, 0) \longmapsto (\zeta_3^{j+1}, 0) \ .$$

In order to obtain a suitable correspondence between the actions of the multipliers ζ_6^2 and ζ_3, we define the mapping θ between the cell mid points in the following way:

$$\theta : \quad (\zeta_6^i, 0) \longmapsto (\zeta_6^{i \cdot 4} = \zeta_3^{2 \cdot i}, 0) \ , \quad 4 \equiv 1 \mod 3 \ .$$

I.e. we have:

$$\theta : \quad (\zeta_6^2, 0) \longmapsto (\zeta_3, 0) \ .$$

Applying θ to Equation (6.27) we obtain the equation of a new surface Y':

$$\begin{aligned} y^{31} &= (z-1)^{21}(z-\zeta_3^2)^6(z-\zeta_3)^{12}(z-\zeta_3^0)^{30}(z-\zeta_3^2)^{29}(z-\zeta_3)^{26} \\ &= (z-1)^{20}(z-\zeta_3)^7(z-\zeta_3^2)^4 \ . \end{aligned} \tag{6.46}$$

We consider the sum σ_0 defined in Equation (6.39) and here given by:

$$\sigma_0 = (d_0 - d_1) + (d_3 - d_4) \ .$$

With the difference set $D_3 = \{1, 11, 5, 24, 25, 27\} \mod 31$ we obtain:

$$\begin{aligned} \sigma_0 &= (1 - 11) + (24 - 25) \\ &= 20 \mod 31 \ . \end{aligned}$$

According to Equation (6.45) the integer a is given by:

$$a \equiv \frac{d_0^* \cdot \sigma_0}{(1-t)} \mod \ell \ ,$$

i.e. in our case

$$a \equiv \frac{20}{(1-5)} \mod 31$$
$$\equiv 26 \mod 31 .$$

Multiplying the exponents of the equation of Y (Equation (6.28)) with $a \equiv 26 \mod 31$ we obtain:

$$26 \cdot 27 \equiv 20 \mod 31 ,$$
$$26 \cdot 11 \equiv 7 \mod 31 ,$$
$$26 \cdot 24 \equiv 4 \mod 31 .$$

I.e. Equation (6.46) is a model for a surface $Y' \cong Y$.

The construction described above could be the starting point for determining the algebraic form of the function f. This function is of degree k and describes the covering of Y by X.

4. Another interesting point of research could be the analysis of the relation between Galois action and surfaces of the embedding of dessins resulting from 'mock' Wilson operations. To the regular dessins $H_{k,k}\mathcal{D}$ constructed as we have described in Chapter 6, we may in fact apply 'real' Wilson operations whose order is prime to the valency of the vertices. The resulting dessins are still regular with the same signature of the starting ones if the Wilson operation applied does not 'destroy' the Wada property. These dessins are embedded in Riemann surfaces. Relying on previous work of e.g. Streit and Wolfart [SW00] it would be of interest to find out more about Galois conjugacy of the surfaces of the embedding.

Zusammenfassung

Dessins d'enfants (Kinderzeichnungen) wurden zuerst von Grothendieck (1984) als Objekte eingeführt, die sehr einfach, aber sehr wichtig sind, um kompakte Riemannsche Flächen als glatte algebraische Kurven über einem Zahlenkörper zu beschreiben. Dessins d'enfants können durch ihre Walsh-Darstellung (s. [Wal75]) definiert werden und entsprechen bipartiten Graphen, die in Riemannsche Flächen eingebettet sind. Die Graphen werden auf der Fläche kreuzungsfrei 'gezeichnet': die schwarzen und die weißen Ecken entsprechen Punkten der Fläche, die verbindenden Kanten beschreiben Kurven auf der Fläche, die Zellen entsprechen einfach zusammenhängenden Teilmengen der Fläche, die der Einheitskreisscheibe isomorph sind. Die Anzahl der Kanten, die mit einer Ecke inzidieren, wird **Valenz** der Ecke genannt. Für die Zellen ist die Valenz die Anzahl der Kanten auf dem Rand.
Jedes entstehende Dessin ist durch seine Signatur $< p, q, r >$ eindeutig charakterisiert. Dabei bezeichnen p und q die größten gemeinsamen Vielfachen der Valenzen der weißen und der schwarzen Ecken, $2r$ ist das größte gemeinsame Vielfache der Valenz der Zellen. Wenn alle weißen Ecken die gleiche Valenz p, alle schwarzen Ecken die gleiche Valenz q und alle Zellen die gleiche Valenz $2r$ haben, dann spricht man von **uniformen Dessins**.
Die Dessins bestimmen die Fläche der Einbettung eindeutig. Ein grundlegendes Problem ist, wie man aus den kombinatorischen Eigenschaften des Dessins auf die algebraischen Eigenschaften der Fläche, wie z.B. auf definierende Gleichungen und auf den Definitionskörper, schließen kann. Die Aufgabe ist normalerweise sehr schwierig aber sie ist einfacher, wenn die Automorphismengruppe des Dessins besonders 'groß' ist.
Der Satz von Belyĭ ([Bel80]) drückt die Relation zwischen Dessin und Einbettungsfläche aus:

Satz. *(**Belyĭs Satz** (nach [LZ04])) Eine Riemannsche Fläche X kann durch eine Gleichung mit Koeffizienten in dem Körper $\overline{\mathbb{Q}}$ definiert werden genau dann, wenn eine meromorphe Funktion $f : X \to \overline{\mathbb{C}}$ existiert, die nur über den Punkten $\{0, 1, \infty\}$ verzweigt ist. In diesem Fall kann f so gewählt werden, daß ihre Koeffizienten im*

Körper $\overline{\mathbb{Q}}$ liegen.

Die Funktion f definiert das Dessin, das in der Fläche eingebettet ist. Die Urbilder der Verzweigungspunkte $\{0, 1\}$ können wir jeweils mit den weißen und mit den schwarzen Ecken des Dessins identifizieren. Dem Punkt ∞ können wir auf der Fläche X die Zellenmittelpunkte des Dessins entsprechen lassen. Das Dessin ist durch das **Belyĭ-Paar** (X, f) eindeutig festgelegt und umgekehrt legt das Belyĭ-Paar (X, f) das Dessin eindeutig fest. Allerdings bestimmt die Fläche ohne eine bestimmte meromorphe Funktion f das Dessin nicht, da in eine Riemannsche Fläche verschiedene Dessins eingebettet sein können.
In dem Spezialfall, daß sich in die Fläche ein uniformes Dessin einbetten läßt, läßt sich die Fläche als Quotient ausdrücken:

$$X := U/\Gamma \ .$$

Dabei ist U der universelle Überlagerungsraum, der entweder mit der Riemannschen Sphäre $\widehat{\mathbb{C}}$, mit der komplexen Ebene $\mathbb{C}$ oder mit der hyperbolischen Ebene $\mathbb{H}$ identifiziert werden kann. Die Gruppe Γ ist eine torsionsfreie Untergruppe einer Dreiecksgruppe Δ mit Präsentation:

$$\Delta = < \gamma_0, \gamma_1, \gamma_\infty | \gamma_0^p = \gamma_1^q = \gamma_\infty^r = \gamma_0\gamma_1\gamma_\infty = 1 > \ .$$

Insbesondere ist Γ eine normale Untergruppe von Δ falls das Dessin **regulär** ist, d.h. falls die Automorphismengruppe des Dessins transitiv auf den Kanten operiert.

In der vorliegenden Arbeit möchten wir uniforme Dessins mit einer möglichst 'großen' Automorphismengruppe konstruieren.
Wir starten mit der Inzidenzstruktur von endlichen projektiven Räumen und konstruieren bipartite Graphen, die die Inzidenzen zwischen Punkten und Hyperebenen darstellen. Projektve Räume $\mathbb{P}^m(\mathbb{F}_n)$ der Dimension m über endlichen Körpern $\mathbb{F}_n$, $n = p^e$, p prim, können wie folgt definiert werden:

$$\mathbb{P}^m(\mathbb{F}_n) := (\mathbb{F}_n^{m+1} \backslash \{0\})/\mathbb{F}_n^* \ .$$

Die Anzahl der **Punkte** des projektiven Raums ist somit gegeben durch

$$\ell = \frac{n^{m+1} - 1}{n - 1} \ .$$

Aus Dualitätsgründen ist diese auch die Anzahl der **Hyperebenen**, d.h. der Unterräume der Dimension $m - 1$. Die Anzahl der Punkte auf einer Hyperebene ist gegeben durch

$$q = \frac{n^m - 1}{n - 1} \ ,$$

und sie ist auch die Anzahl der Hyperebenen durch einen Punkt.
Projektive Räume können mit dem Quotienten der zyklischen Gruppen der endlichen Körper $\mathbb{F}_{n^{m+1}}$ und $\mathbb{F}_p$ wie folgt identifiziert werden

$$\mathbb{P}^m(\mathbb{F}_n) \cong \mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n \,.$$

Wir können die Elemente von $\mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$ als Potenzen eines erzeugenden Elements $< g >$ schreiben. Wenn wir die Punkte P_b und die Hyperebenen h_w mit Indizes $b, w \in \{1, \ldots, \ell\}$ versehen, dann können wir auf natürliche Art folgende Identifikation einführen

$$h_w \longleftrightarrow g^w \,, \quad P_b \longleftrightarrow g^b \,. \tag{6.47}$$

Die Inzidenzrelation zwischen Punkten und Hyperebenen kann nach Singer ([Sin38]) mithilfe von Differenzmengen ausgedrückt werden. Differenzmengen lassen sich wie folgt definieren ([Bau71]):

Definition. Eine (v, k, λ)-Differenzmenge $D = \{d_1, \ldots, d_k\}$ ist eine Menge von k Restklassen modulo v derart, daß für jedes $\alpha \not\equiv 0 \mod v$ die Kongruenz

$$d_i - d_j \equiv \alpha \mod v$$

genau λ Lösungspaare (d_i, d_j) mit d_i, $d_j \in D$ besitzt.

Für projektive Räume entsprechen v und k den Parametern ℓ und q.
Singer konnte zeigen, daß für projektive Ebenen ein Punkt P_b und eine Gerade h_w genau dann inzidieren, wenn

$$b - w \equiv d_i \mod \ell \,. \tag{6.48}$$

Die Relation läßt sich ohne weiteres auch auf die Punkte und auf die Hyperebenen von projektiven Räumen $\mathbb{P}^m(\mathbb{F}_n)$ mit Dimension $m > 2$ erweitern (siehe dazu [Hir05]).
Mithilfe von Relation (6.48) ist es möglich, einen bipartiten Graphen zu konstruieren, der die Inzidenzstruktur von Punkten und Hyperebenen darstellt. Dazu führen wir folgende Konventionen ein:

Punkt	schwarze Ecke •
Hyperebene	weiße Ecke ∘
Inzidenz	verbindende Kante —

Table 6.1: *Konventionen.*

Somit können wir die lokale Inzidenzstruktur in Abbildung 6.8 festlegen. Die Wahl

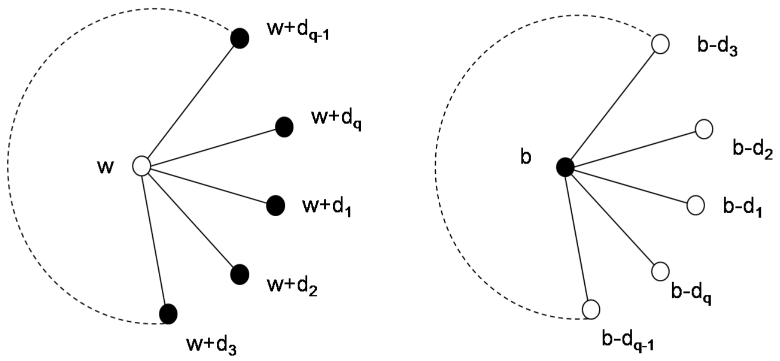


Figure 6.8: *Lokale Inzidenzstruktur.*

entgegengesetzter Anordnungen der Elemente der Differenzmenge ist dadurch motiviert, daß wir sogenannte **Wada-Dessins** konstruieren wollen. Diese Dessins sind zuerst von Streit und Wolfart([SW01]) eingeführt worden. Die ursprüngliche Konstruktion bezieht sich auf Dessins, für die der zugrundeliegende Graph die Inzidenzstruktur von projektiven Ebenen darstellt. In unserer Arbeit zeigen wir, daß die gleiche Konstruktion auch für projektive Räume höherer Dimension verwendet werden kann. Um die Ecken werden die Zellen als Folge von Kanten gemäß der Inzidenzstruktur konstruiert. Eine Zelle ist vollständig, wenn wir wieder die erste Kante erreichen und das Dessins ist vollständig, wenn alle $q \cdot \ell$ Inzidenzen von Punkten und von Hyperebenen dargestellt sind.
Wada-Dessins sind uniforme Dessins mit Signatur $< q, q, \ell >$ und mit der Eigenschaft, daß alle weißen Ecken und alle schwarzen Ecken mit Indizes von 1 bis ℓ auf dem Rand jeder Zelle liegen. Dafür muß die Anordnung der Elemente der Differenzmenge, die wir festgelegt haben, die **Wada-Bedingung** erfüllen:

$$((d_i - d_{i+1}), \ell) = 1 \ , \qquad \forall d_i, d_{i+1} \in D \ .$$

Für die konstruierten Dessins ist es möglich, die Automorphismengruppe zu bestimmen.

Die Ecken auf dem Rand der Zellen werden durch eine zyklische Gruppe Σ_ℓ permutiert. Dabei handelt es sich um eine **Singergruppe**, hier eine zyklische Gruppe der Ordnung ℓ, die wir wie folgt definieren können:

$$\Sigma_\ell \cong \mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n \ .$$

Wegen der Identifikation der Punkte und der Hyperebenen mit den Potenzen eines erzeugenden Elements $< g >$ von $\mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$ (siehe Relation (6.47)) ist die Operation von Automorphismen $\sigma^i \in \Sigma_\ell$ auf natürliche Art und Weise gegeben durch

$$\begin{aligned} \sigma^i : \quad P_b &\longmapsto P_{b+i} \ , \\ h_w &\longmapsto h_{w+i} \ . \end{aligned}$$

Die Operation ist transitiv auf den schwarzen bzw. auf den weißen Ecken auf dem Rand jeder Zelle wegen der Wada-Eigenschaft. Diese Operation induziert eine transitive Permutation der Kanten vom Typ •—◦ bzw. vom Typ ◦—•.
Für jedes Wada-Dessin ist die Singergruppe eine Gruppe von Automorphismen.
Wir betrachten eine zweite zyklische Gruppe. Es handelt sich dabei um die zyklische Gruppe $\Phi_f \cong Gal(\mathbb{F}_{n^{m+1}}/\mathbb{F}_p)$ mit Ordnung $f = e \cdot (m+1)$, die vom **Frobenius-Automorphismus** φ generiert wird. Wegen der Identifizierung der Punkte und der Hyperebenen mit den Potenzen eines erzeugenden Elements $< g >$ von $\mathbb{F}^*_{n^{m+1}}/\mathbb{F}^*_n$ ist die Operation des Frobenius-Automorphismus gegeben durch:

$$\begin{aligned} \varphi : \quad P_b &\longmapsto P_{b\cdot p} \ , \\ h_w &\longmapsto h_{w\cdot p} \ . \end{aligned}$$

Der Frobenius-Automorphismus ist ein Automorphismus von Wada-Dessins nur unter folgenden Bedingungen:

1. Für die Konstruktion wählen wir eine Differenzmenge, die unter der Operation des Frobenius-Automorphismus festgelassen wird, d.h. für die gilt:

   $$p \cdot D_f \equiv D_f \mod \ell \ .$$

   Aus geometrischen Gründen existiert so eine Differenzmenge für jeden projektiven Raum. Weitere Differenzmengen mit der obigen Eigenschaft existieren nur, wenn der Frobenius-Automorphismus mehrere Punkte bzw. Hyperebenen festläßt. Wir nennen die betrachteten Differenzmengen **Frobenius-Differenzmengen**.

2. Die zweite notwendige Bedingung ist die Existenz einer Anordnung der Elemente der Frobenius-Differenzmenge, die **kompatibel** mit der Operation von φ ist, d.h.:

$$D_f = \{d_1, \cdots, d_k,\ p^j d_1, \cdots, p^j d_k,\ \cdots\cdots, p^{j\cdot(f-1)} d_1, \cdots, p^{j\cdot(f-1)} d_k\}\ ,$$
$$\text{für ein } j \in (\mathbb{Z}/f\mathbb{Z})^*\ , \frac{q}{f} = k\ .$$

Die Wahl solcher Anordnungen ist nur möglich, wenn alle Φ_f-Bahnen von Elementen $d_i \in D_f$ die gleiche Länge k haben. Für projektive Räume $\mathbb{P}^m(\mathbb{F}_p)$ mit der Eigenschaft

$$p \not\equiv 0, 1 \mod (m+1)\ , \qquad m+1 \text{ prim}\ ,$$

ist es immer möglich, die Elemente auf eine Frobenius-kompatible Art anzuordnen. Für den allgemeineren Fall ist es schwieriger, Bedingungen für die Parameter m und n eines projektiven Raums $\mathbb{P}^m(\mathbb{F}_n)$ zu formulieren.

Wenn φ ein Automorphismus des betrachteten Wada-Dessins ist, dann ist die Operation von φ eine Rotation der Zellen um die Ecken mit Indizes w und b, die von φ festgelassen werden. Die zyklische Gruppe Φ_f, die von φ generiert wird, operiert dann auch auf den Zellen mit einer Rotation um die Ecken, die festgelassen werden. Die Operation ist frei und nur im Spezialfall der Wada-Dessins für die projektive Ebenen $\mathbb{P}^2(\mathbb{F}_2)$ und $\mathbb{P}^2(\mathbb{F}_8)$ ist sie transitiv.
Die vollständige Automorphismengruppe der betrachteten Wada-Dessins ist in diesem Fall von der Singergruppe Σ_ℓ und von der zyklischen Gruppe Φ_f erzeugt. Sie entspricht dem semidirekten Produkt

$$\Phi_f \ltimes \Sigma_\ell\ .$$

In dem allgemeineren Fall haben wir es nicht mit der ganzen Gruppe Φ_f zu tun, sondern meistens nur mit Untergruppen $\Phi_g \subset \Phi_f$. Demzufolge entspricht die Automorphismengruppe der betrachteten Wada-Dessins dem semidirekten Produkt

$$\Phi_g \ltimes \Sigma_\ell\ ,$$

wenn die Dessins mit Differenzmengen konstruiert werden können, für die die Anordnung der Elemente kompatibel mit der Operation von Φ_g ist. Solche Differenzmengen D_g sind eine Verallgemeinerung der Frobenius-Differenzmengen, die wir unter Punkt (2.) eingeführt haben.

Die konstruierten Wada-Dessins können wir modifizieren, wenn wir auf dem zugrundeliegenden bipartiten Graphen **Wilson-Operationen** (siehe dazu [Wil79]) anwenden. Wir betrachten zuerst Wilson-Operationen $H_{-j,k}$ mit Zahlen j und k, die zur Valenz der weißen und der schwarzen Ecken eines Wada-Dessins prim sind. Unter Anwendung dieser Operationen werden auf dem zugrundeliegenden Graphen 'neue' Zellen gezeichnet, so daß wir möglicherweise eine neue Einbettung des Graphen in eine Riemannsche Fläche erhalten können. Wenn z.B. $\mathrm{ggT}(k+j,q) \equiv 1 \mod q$ gilt, dann erhalten wir eine Einbettung des ursprünglichen $< q, q, \ell >$ Wada-Dessin als $< q, q, q >$ uniformes Dessin mit ℓ Zellen.
Als zweiten und wichtigeren Fall betrachten wir reguläre Dessins, die sich ausgehend von Wada-Dessins konstruieren lassen. Dafür, anders als in der urspünglichen Arbeit von Wilson, betrachten wir **'mock' Wilson-Operationen**. In diesem Fall sind die Indizes j und k von Operatoren $H_{-j,k}$ nicht prim zur Valenz der weißen bzw. der schwarzen Ecken. Insbesondere betrachten wir solche Wilson-Operatoren $H_{k,k}$, für die $-j \equiv k \mod \ell$.
Für ein uniformes Wada-Dessin $\mathcal{D}$ mit Automorphismengruppe $\Phi_f \ltimes \Sigma_\ell$ wählen wir k wie folgt:

$$k := \frac{q}{f} \; .$$

Unter Anwendung des Operators $H_{k,k}$ erhalten wir reguläre Wada-Dessins $H_{k,k}\mathcal{D}$ mit Signatur $< f, f, \ell >$, falls die Wada-Bedingung erfüllt ist. D.h. Differenzen der darauffolgenden Elemente der reduzierten Menge

$$\begin{aligned} H_k D_f = &\{d_i, p^j d_i, p^{2j} d_i, \ldots, p^{(f-1)j} d_i\} \mod \ell \\ &\text{für ein } i \in \mathbb{Z}/k\mathbb{Z} \text{ und ein } j \in (\mathbb{Z}/f\mathbb{Z})^* \end{aligned}$$

sind prim zu ℓ.
Jedes der konstruierten regulären Wada-Dessins $H_{k,k}\mathcal{D}$ ist in eine Riemannsche Fläche

$$Y := \Gamma_2 \backslash \mathbb{H} \; , \quad \Gamma_2 \lhd \Delta_2 \; .$$

eingebettet. Dabei ist Γ_2 eine torsionsfreie, normale Untergruppe einer Dreiecksgruppe Δ_2 mit Präsentation:

$$\Delta_2 =< \delta_0, \delta_1, \delta_\infty | \delta_0^f = \delta_1^f = \delta_\infty^\ell = \delta_0\delta_1\delta_\infty = 1 > \; .$$

Die Riemannsche Fläche X der Einbettung des uniformen Wada-Dessins $\mathcal{D}$ ist gegeben durch

$$X := \Gamma_1 \backslash \mathbb{H} \; , \quad \Gamma_1 \subset \Delta_1 \; .$$

Dabei ist Γ_1 eine torsionsfreie Untergruppe einer Dreiecksgruppe Δ_1 mit Präsentation

$$\Delta_1 =< \gamma_0, \gamma_1, \gamma_\infty | \gamma_0^q = \gamma_1^q = \gamma_\infty^\ell = \gamma_0\gamma_1\gamma_\infty = 1 > \ .$$

Für beide Flächen X und Y ist es möglich, definierende Gleichungen zu bestimmen, da beide eingebettete Dessins **globe covering Dessins** (s. [SW01]) sind. D.h. die Fläche der Einbettung des Quotientendessins $\mathcal{D}/\Sigma_\ell$ mit Signatur $< q, q, 1 >$ und des Quotientendessins $(H_{k,k}\mathcal{D})/\Sigma_\ell$ mit Signatur $< f, f, 1 >$ ist die Riemannsche Zahlenkugel.
Für X erhalten wird die Gleichung

$$y^\ell = \prod_{r=0}^{q-1} (x - \zeta_q^r)^{b_r} \ .$$

Die Exponenten b_r sind Differenzen von Elementen der Frobenius-Differenzmenge D_f. Die Koeffizienten ζ_q^r sind Einheitswurzeln $e^{\frac{2\pi i}{q} \cdot r}$.
Für die Fläche Y erhalten wir:

$$w^\ell = \prod_{s=0}^{f-1} (z - \zeta_f^s)^{m_s} \ .$$

In diesem Fall sind die Exponenten m_s Differenzen von Elementen der reduzierten Menge $H_k D_f$. Die Koeffizienten ζ_f^s entsprechen Einheitswurzeln $e^{\frac{2\pi i}{f} \cdot s}$.
Die beiden Einbettungsflächen hängen insofern zusammen, als die Fläche X die Fläche Y überlagert. Die Überlagerungsabbildung g ist vom Grad k. Kritische Punkte sind die weißen und die schwarzen Ecken des Dessins $H_{k,k}\mathcal{D}$. Die Existenz der Abbildung ist im wesentlichen durch den Riemannschen Abbildungssatz begründet (siehe Abbildung 6.9).

Die Dreiecksgruppen Δ_1 und Δ_2 definieren Parkettierungen der hyperbolischen Ebene $\mathbb{H}$. Wegen des Riemannschen Abbildungssatzes existiert eine holomorphe Funktion g, die Fundamentalgebiete von Δ_1 auf Fundamentalgebiete von Δ_2 abbildet. Die Funktion kann auf den Kanten und in den kritischen Punkten holomorph fortgesetzt werden. Wegen des Schwarz'schen Spiegelungsprinzips kann sie auf den ganzen hyperbolischen Raum fortgesetzt werden und induziert dadurch die

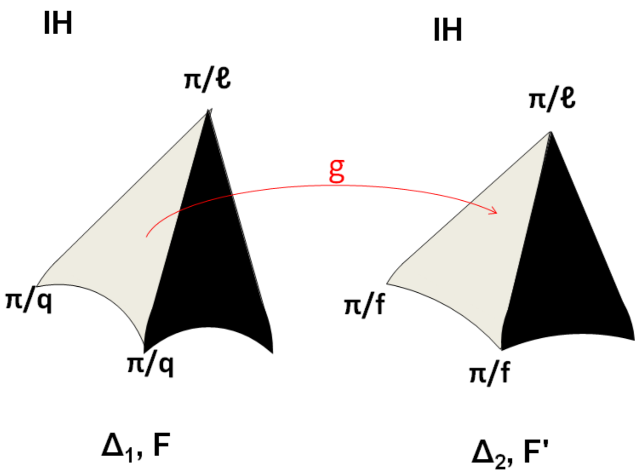


Figure 6.9: *Abbildung von Fundamentalgebieten (Riemanns Abbildungssatz).*

Überlagerung von Y durch X.
Die Konstruktion von regulären Dessins $H_{k,k}\mathcal{D}$ und die Eigenschaft der Einbettungsflächen können für Wada-Dessins mit Automorphismengruppe $\Phi_g \ltimes \Sigma_\ell$, $\Phi_g \subset \Phi_f$ verallgemeinert werden.

Bibliography

[Bau71] L. Baumert. *Cyclic Difference Sets.* Springer - Verlag, Berlin/Heidelberg/New York, 1971.

[Bel80] G.V. Belyĭ. On Galois extensions of a maximal cyclotomic field. *Math. USSR Isvestija*, 14:247–256, 1980.

[Beu82] A. Beutelspacher. *Einführung in die Endliche Geometrie.* Bibliographisches Institut, Mannheim/Wien/Zürich, 1982.

[BR04] A. Beutelspacher and U. Rosenbaum. *Projektive Geometrie.* Vieweg, Braunschweig/Wiesbaden, 2nd edition, 2004.

[Dem97] P. Dembowski. *Finite Geometries.* Springer - Verlag, Berlin/Heidelberg/New York, 2nd edition, 1997.

[FK92] H. M. Farkas and I. Kra. *Riemann Surfaces.* Springer - Verlag, Berlin/Heidelberg/New York, 1992.

[GD91] G. González-Díez. Loci of curves which are prime Galois coverings of $\mathbb{P}^1$. *Proceedings of the London Mathematical Society*, 62(3):469–489, 1991.

[Goe05] R. Goertz. *Über spezielle Anordnungen von perfekten Differenzmengen.* Diplomarbeit, Universität Hagen, Hagen, Germany, 2005.

[Goe09] R. Goertz. Coprime ordering of cyclic planar difference sets. *Discrete Mathematics*, 309(16):5248–5252, 2009.

[Hal67] Marshall Hall, Jr. *Combinatorial Theory.* Blaisdell, Waltham, Massachusetts, 1967.

[Hir05] J.W.P. Hirschfeld. *Projective Geometries over Finite Fields.* Clarendon Press, Oxford, 2nd edition, 2005.

[HP85] D. R. Hughes and F. C. Piper. *Design Theory.* Cambridge University Press, Cambridge, New York, etc., 1985.

[Hup79] B. Huppert. *Endliche Gruppen I.* Springer - Verlag, Berlin/Heidelberg/New York, 1979.

[JSW10] G. Jones, M. Streit, and J. Wolfart. Wilson's graph operations on regular dessins and cyclotomic filelds of definition. *Proceedings of the London Mathematical Society*, 100:510–532, 2010.

[Kat92] S. Katok. *Fuchsian Groups.* The University of Chicago Press, Chicago and London, 1992.

[Kle81] F. Klein. *Vorlesungen über die hypergeometrische Funktion.* Springer - Verlag, Berlin/Heidelberg/New York, Reprint, 1981.

[Leh66] J. Lehner. *A Short Course in Automorphic Functions.* Holt, Rinehart and Winston, New York/Chicago/San Francisco/Toronto/London, 1966.

[LZ04] S.K. Lando and A.K. Zvonkin. *Graphs on Surfaces and Their Applications.* Springer - Verlag, Berlin/Heidelberg/New York, 2004.

[Sar10] C. Sarti. Wada dessins associated with finite projective spaces and Frobenius compatibility. *Ars Mathematica Contemporanea*, 2010. (submitted to).

[Sin38] J. Singer. A theorem in finite projective geometry and some applications in number theory. *Transactions of the American Mathematical Society*, 43(3):377–385, 1938.

[Sin86] D. Singerman. Klein's Riemann surface of genus 3 and regular imbeddings of finite projective planes. *Bulletin of the London Mathematical Society*, 18:364–370, 1986.

[SW00] M. Streit and J. Wolfart. Galois actions on some infinite series of Riemann surfaces with many automorphisms. *Revista Matematica Complutense*, 13:49–81, 2000.

[SW01] M. Streit and J. Wolfart. Cyclic projective planes and Wada dessins. *Documenta Mathematica*, 6:39–68, 2001.

[Wal75] T. R. S. Walsh. Hypermaps versus bipartite maps. *J. Combinatorial Theory Ser. B*, 18:155–163, 1975.

[Whi95] A.T. White. Efficient imbeddings of finite projective planes. *Proceeding of the London Mathematical Society*, 70(3):33–55, 1995.

[Wil79] S.E. Wilson. Operators over regular maps. *Pacific Journal of Mathemtics*, 81(2):559–568, 1979.

[WJ06] J. Wolfart and G. Jones. Dessin d'Enfants: Function Theory and Algebra of Belyi Functions on Riemann Surfaces with Combinatorics and Group Theory of Belyi Functions on Riemann Surfaces. Technical report, University of Jyväskylä, 2006. Lecture notes taken by Tuomas Puurtinen at the 16^{th} Jyväskylä Summer School 24^{th} July - 4^{th} August 2006.

[Wol96] J. Wolfart. *Einführung in die Zahlentheorie und Algebra*. Vieweg, Braunschweig/Wiesbaden, 1996.

[Wol06] J. Wolfart. Abc for polynomials, dessins d'enfants, and uniformization - a survey. In J. Steuding W. Schwarz, editor, *Proceedings der ELAZ-Konferenz 2004*, pages 3131–345, Stuttgart, 2006. Steiner.

[Woo07] A. Wootton. Defining equations for cyclic prime covers of the Riemann sphere. *Israel Journal of Mathematics*, 157:103–122, 2007.