dc_821_13

Representations of loops in groups and projective planes

DSc dissertation

Gábor Péter Nagy
University of Szeged
Bolyai Institute

2014

dc_821_13

Contents

dc_821_13

Preface

The present work is a dissertation to obtain the title *Doctor of Sciences* (DSc) of the Hungarian Academy of Sciences. The dissertation consists of four parts. Part I is introductory, the other three resume eight papers, which appeared in well established international mathematical journals. For five of these articles I was the sole author, the other three had one or two coauthors. Roughly speaking, the eight chapters of Parts II-IV correspond to these eight papers; in fact, the texts needed a slight restructuring in order to avoid unnecessary repetitions.

The topics of the dissertation include different mathematical areas, the main guideline is that each of them is related to finite loops. Although the theory of loops and quasigroups is interesting on its own, in this presentation they are deeply involved in the theory of groups. In Part II, we present the theory of simple Bol loops using decompositions of abstract groups. Part III deals with finite multiply transitive sets; the results rely on the combinatorial and algebraic fundamentals of the theory of finite permutation groups. Finally in Part IV, we investigate the projective embedding of finite 3-nets. There, beside combinatorial counting arguments and the elementary geometry of conics and cubics, deep results are applied from the theory of projective linear groups.

The regulation of the Academy requires the candidate to present his or her results in *theses*. I aimed to formulate my theses such that they are accessible to a wider audience, even if this implied some mathematical inaccuracy. Moreover, my theses are written in first person form, despite that most of them were achieved in collaboration with my coauthors.

Thesis 1: Based on exact factorizations of groups, I give a construction of proper Bol loops. This method is powerful enough to produce simple proper Bol loops in different categories: finite, finite of odd order, differentiable and algebraic.

Thesis 2: Using the geometry of indecomposable $\mathbb{F}_2 S_5$-modules, I construct an infinite class of finite simple Bol loops of exponent 2. The Bol loops of this class have an automorphism with a fixed point free action on the set of nontrivial elements of the loop.

Thesis 3: Using an extremely simple combinatorial lemma, I am able to show the non-existence of sharply 2-transitive sets in the alternating group of degree $n \equiv 2, 3 \pmod 4$, and in two other 2-transitive finite simple groups: The Mathieu group of degree 23 and the Conway simple group

of degree 276. As a corollary, I show that the group of projectivities of a finite non-Desarguesian projective plane is either the alternating or the symmetric group.

Thesis 4: By combining the combinatorial lemma with computer methods and geometric arguments, I classify the right multiplication groups of finite quasifields. As a corollary, I obtain a classification of finite transitive linear groups which may contain a sharply transitive set, or equivalently, a classification of finite 2-transitive groups of affine type which may contain a sharply 2-transitive set.

Thesis 5: I prove that the multiplication group of a finite semifield lies between the projective special linear group and the projective general linear group. Moreover, any loop whose multiplication group is contained in the projective linear group is the multiplicative structure of a semifield. This answers an open question of A. Drápal.

Thesis 6: I give a complete classification of finite groups whose 3-net can be realized in the projective plane over a field of characteristic 0. These groups are the cyclic groups, the direct products of two cyclic groups, the dihedral groups and the quaternion group of order 8. Moreover, I describe the geometry of the realizations of these 3-nets.

As already mentioned, Part I is introductory. We listed all important definitions in Chapter 1 and gave the references to the general literature in Chapter 2.

Part II is on Bol loop constructions. In Chapter 3, we present a construction of Bol loops which is based on exact factorizations of groups. Using this method, we are able to construct many classes of finite and infinite simple non-Moufang non-Bruck Bol loops, and hence solve the problem of the existence of finite simple non-Moufang Bol loops. The Bol loop construction of Theorem 3.2, the simplicity conditions of Theorems 3.5 and 3.8, and the Examples support **Thesis 1** of the dissertation. In Chapter 4, we apply Aschbacher's recipe to construct a class of finite simple Bol loops of exponent 2. In Chapter 5, I answer three questions on simple Bol loops which were asked after my talk at the LOOPS'07 conference in Prague. The chapter ends with a few open problems which are related to simple Bol loops. Theorems 4.7, 4.14 and 5.7 support **Thesis 2.** In Chapter 6, we examine the class of *algebraic right Bol loops* and explain the relations between the classes of algebraic, strongly algebraic and local algebraic Bol loops by proving some structure theorems and giving many examples.

The main topic of Part III is the existence and non-existence problem of sharply transitive sets in finite permutation groups. For finite linear groups, this problem is also related to the (non-)existence of certain quasifields and semifields. In Chapter 7, we present simple combinatorial methods which are useful for non-existence proofs. Lemma 7.1, Theorems 7.4, 7.8, 7.10 and Corollary 7.7 support **Thesis 3.** In Chapter 8, we investigate finite transitive linear group can occur as right multiplication

group of a finite quasifield. A combination of theoretical arguments and computer proofs result in an explicit classification of all quasifields whose right multiplication group is an exceptional finite linear group. Theorem 8.17 supports the first part of **Thesis 4;** the second part follows from the equivalence of sharply transitive sets in the general linear group and sharply 2-transitive sets in the affine linear group. In the main result of Chapter 9, I answer Drápal's question on finite loops whose multiplication group contains the projective special linear group. Theorem 9.4 supports **Thesis 5.**

In Chapter 10 of Part IV, we give a complete classification of 3-nets realizing a finite group in a projective plane defined over an algebraically closed field of characteristic 0. We also prove that the only infinite families are previous constructions of Yuzvinsky and Pereira, and, the only sporadic example is the one by Urzúa realizing the quaternion group of order 8. If the characteristic is larger than the order of the group, the above classification holds true apart from three possible exceptions. Theorem 10.1 supports **Thesis 6.**

At the end of this preface, I would like to thank the persons whose constant encouragement motivated me a lot in the preparation of this dissertation: my father Péter T. Nagy and my friends Tamás Szőnyi and Gábor Korchmáros. Similarly, I would like to thank my wife Krisztina and our children for love and faith.

dc_821_13

Part I.

Fundamental ideas

dc_821_13

1. Preliminaries

1.1. Historical overview

For almost 2000 years, by exact mathematics one meant axiomatic geometry, whose rigorous order was set up by EUCLID and his students in the 3rd century BC. In this mathematics, the concept of a number and the computation with numbers played a relatively peripheral role. For the ancient Greeks, the concept of a number did not really exceeded the class of positive rational numbers. This situation started to change in the 12th century AD, when the Hindu-Arabic numeral system finally arrived at Europe with Arabic mediation. In the Christian Europe, the Hindu-Arabic numerals needed almost 300 more years to reach the same level of acceptance than Roman numerals. However, from the 15th century AD on, the development of the *calculative mathematics* was explosion-like.

In the 16th century, DESCARTES and FERMAT invented the concept of a coordinate system, which linked the world of geometry and computation. The "invention" of the decimal representation of positive real numbers and the negative numbers followed soon. The success story continued with the development of complex numbers, linear algebra and calculus, and we extended our calculation knowledge to new domains. In the beginning of the 19th century, ABEL and GALOIS created the abstract theories of fields and groups. This allowed them to solve many problems which were open for two millenniums. At the end of the 19th century, FELIX KLEIN's *Erlangen Program* formulated the object to characterize geometric structures by the abstract properties of the group of their invariant transformations. Since then, the theory of groups plays a central role in algebra and in the *algebraization* of almost all mathematical disciplines.

In the algebraization of geometric structures, the two main tools are the *transformation group* and the *coordinate structure.* From an abstract point of view, the latter is more exotic. On the one hand, in most cases the "invertibility" of the operations is trivial by a geometric argument. On the other hand, the associativity and distributivity of the operations correspond to special regularity properties of the geometry. For example, any desarguesian projective plane can be coordinatized with a skew field, and the commutativity of the coordinatizing skew field is equivalent with the Pappus property of the plane. This example shows another typical phenomenon: both the Pappus and the Desargues properties correspond to a specific *inner symmetry* of the projective plane.

The main topic of this dissertation is the theory of *quasigroups.* These are algebraic structures which can be seen as the nonassociative generalizations of groups.

The name is due to RUTH MOUFANG, who was motivated by the study of nondesarguesian projective planes. Approximatively in the same time, in the 1930's, starting from differential geometric investigations, BLASCHKE and BOL got in touch with abstract (local and global) quasigroups. In the 1940's, ALBERT and BRUCK worked out the foundations of the abstract theory; and the geometric and group theoretic relations are usually attributed to REINHOLD BAER.

1.2. Notation for groups and permutations

In mathematics, the abstract way of defining a *map* $f : X \to Y$ is to say that f is an appropriate subset of the direct product $X \times Y$. The image of $x \in X$ under f is denoted by $f(x)$, fx, xf, or x^f. Although in this dissertation, all notations will be used, I hope that the reader will not be confused. As a general rule, *groups act on the right.*

If not stated otherwise, groups are multiplicative. The unit element of a group is usually denoted by 1 or id. Let G be a group, X a set and $\varphi : X \times G \to X$ a map such that

$$(x, 1)^\varphi = x, \qquad ((x, g)^\varphi, h^\varphi) = (x, gh)^\varphi.$$

Then φ is called a *group action* of G on X. If φ is clear from the context, then $(x, g)^\varphi$ is denoted by xg or x^g; in this case we say that G acts on X. Any group G has a natural action on itself by conjugation. For $g, h \in G$, we say that $g^h = h^{-1}gh$ is the *conjugate* of g with h.

Let Ω be a set. *Permutations* of Ω are invertible maps $\Omega \to \Omega$. The set of permutations of Ω forms the *symmetric group* $\mathrm{Sym}(\Omega)$. Subgroups of $\mathrm{Sym}(\Omega)$ are called *permutations groups* acting on Ω. The set of even permutations forms the *alternating group* $\mathrm{Alt}(\Omega)$. If $|\Omega| = n$ then we use the notations Sym_n, S_n, Alt_n, A_n as well.

For $x \in \Omega$, $g \in \mathrm{Sym}(\Omega)$, x^g denotes the image of x under g. For a positive integer k, define

$$\Omega^{(k)} = \{(x_1, \ldots, x_k) \mid x_i \neq x_j \text{ for all } 1 \leq i \neq j \leq k\}.$$

Then, any element $g \in \mathrm{Sym}(\Omega)$ has a natural action

$$(x_1, \ldots, x_k)^g = (x_1^g, \ldots, x_k^g)$$

on $\Omega^{(k)}$.

1.3. Loops and multiplications

We call the abstract algebraic structure $(Q, \{\cdot, /, \backslash\})$ a *quasigroup,* if the three binary operations satisfy the identities

$$(x \cdot y)/y = (x/y) \cdot y = x, \quad x\backslash(x \cdot y) = x \cdot (x \cdot y) = y. \tag{1.1}$$

One sometimes says that the equation $x \cdot y = z$ has a unique solution whenever two of the three variables are fixed. The multiplication is usually denoted by juxtaposition $x \cdot y = xy$. The *left* and *right multiplication maps* of the quasigroup Q are defined by

$$L_x : y \mapsto xy, \qquad R_x : y \mapsto yx.$$

The requirement of the maps R_x, L_x to be bijective is equivalent with (1.1). If the quasigroup Q has an element e such that $ex = xe = x$ holds for all $x \in Q$, that is, if Q has a *unit element,* then Q is called a *loop.* Since in an associative quasigroup, x/x is a unit element for any x, the associative quasigroups are precisely the groups. In most cases, we denote the unit element of a loop by 1 and hope not to confuse the reader when 1 also stands for the unit of a group.

Analogously to groups, one can speak of *subloops, loop homomorphisms* and *factor loops.* The subloop K of Q is *normal* in Q if

$$xK = Kx, \quad x(yK) = (xy)K, \quad x(Ky) = (xK)y, \quad (Kx)y = K(xy)$$

hold for all $x, y \in K$. Normal subloops are precisely the kernels of loop homomorphisms. The loop is *simple,* if it has no proper normal subloops. A *normal series* of Q is a finite sequence of subloops

$$1 = H_0 \lneqq H_1 \lneqq \cdots \lneqq H_n = Q,$$

such that H_i is normal in H_{i+1}. The loop Q is *solvable,* if it has a normal series such that all factors H_{i+1}/H_i are cyclic groups. The Jordan-Hölder theorem holds for loops, too.

The *commutator-associator subloop* Q' is the smallest normal subloop of Q such that Q/Q' is an Abelian group. Define the sequence $Q_0 = Q$, $Q_{i+1} = Q_i'$ for $i = 1, 2, \ldots$. Then, Q is solvable if and only if $Q_k = 1$ for some k; the smallest such k is called the *solvability degree* of Q.

The *left, middle* and *right nucleus* and the *center* of a quasigroup are

$$\begin{aligned} N_\lambda(Q) &= \{n \in Q \mid n(xy) = (nx)y \ \forall x, y \in Q\}, \\ N_\mu(Q) &= \{n \in Q \mid (xn)y = x(ny) \ \forall x, y \in Q\}, \\ N_\rho(Q) &= \{n \in Q \mid (xy)n = x(yn) \ \forall x, y \in Q\}, \\ Z(Q) &= \{n \in N_\lambda \cap N_\mu \cap N_\rho \mid nx = xn \ \forall x \in Q\}. \end{aligned}$$

Quasigroups and loops can be classified up to isomorphism or up to isotopism. When Q_1, Q_2 are quasigroups, then the triple (α, β, γ) of bijections from Q_1 onto Q_2 is an *isotopism* of Q_1 onto Q_2 if $\alpha(x) \cdot \beta(y) = \gamma(x \cdot y)$ holds for every $x, y \in Q_1$. An isotopism with $Q_1 = Q_2$ is called an *autotopism.* Every isomorphism α gives rise to an isotopism (α, α, α). The notion of isotopism is superfluous in group theory, as any two groups that are isotopic are already isomorphic.

In terms of multiplication tables, Q_1 and Q_2 are isotopic if the multiplication table of Q_2 can be obtained from the multiplication table of Q_1 by permuting the

rows (by α), the columns (by β), and by renaming the elements (by γ). Isotopisms are therefore appropriate morphisms for the study of quasigroups and loops. On the other hand, every quasigroup is isotopic to a loop, which shows that the algebraic properties of isotopic quasigroups can differ substantially. A loop Q is a *G-loop* if every loop isotopic to Q is isomorphic to Q.

Let Q be a quasigroup. The group generated by the right multiplication maps

$$\mathrm{RMlt}(Q) = \langle R_x \mid x \in Q \rangle$$

is the *right multiplication group of* Q. Clearly, this is a permutation group acting transitively on Q. If Q is a loop, then the stabilizer subgroup $\mathrm{RInn}(Q)$ of the unit element is called the *right inner mapping group* of Q; the elements of $\mathrm{RInn}(Q)$ are the *right inner mappings* of Q.

The class of loops we are the most interested in is the class of *Bol loops.* This class is defined by the (right) Bol identity

$$((xy)z)y = x((yz)y). \tag{1.2}$$

Using right multiplication maps, the identity can be written as $R_y R_z R_y = R_{(yz)y}$. In fact, is suffices to require that $R_y R_z R_y = R_w$ holds for some $w \in Q$, since by applying both sides to the unit element, we have $(yz)y = w$.

Bol loops satisfy the *right inverse property,* that is, for an arbitrary element x of a Bol loop Q there is an *inverse element* x^{-1} such that

$$(yx)x^{-1} = y = (yx^{-1})x$$

holds for all $y \in Q$. In other words, $R_x^{-1} = R_{x^{-1}}$. More generally, for any integer k, the right translations of a Bol loop satisfy $R_x^k = R_{x^k}$. Finally, we mention that by switching the factors in (1.2), we obtain the *left Bol identity.*

1.4. Special classes of Bol loops: Bruck and Moufang

In this section, we define two important subclasses of Bol loops. A Bol loop satisfying the so called *automorph inverse identity*

$$(xy)^{-1} = x^{-1}y^{-1}. \tag{1.3}$$

is called a *Bruck loop.* Bruck loops are A_r*-loops,* that is, all right inner maps of a Bruck loop Q are automorphisms: $\mathrm{RInn}(Q) \leq \mathrm{Aut}(Q)$. Bruck loops are also called K-loops or B-loops. They play a central role in the theory of loops. On the one hand, this is due to the *hyperbolic plane loop,* which is the classical example for an infinite simple Bruck loop. On the other hand, the study of B-loops were initiated by G. Glauberman in [Gla64], leading to a celebrated result of finite group theory:

the Z^*-theorem. Roughly speaking, it shows that finite Bruck loops of odd order are solvable. Notice that (1.3) is automatically satisfied in Bol loops of exponent 2.

The underlying set of the hyperbolic plane loop is the unit disc $\{z \in \mathbb{C} \mid |z| < 1\}$ and the operation is given by

$$x \cdot y = \frac{x+y}{1+x\bar{y}}. \tag{1.4}$$

One can show that the right multiplication maps preserve the Poincaré model of the hyperbolic plane; in fact, they generate $PSL_2(\mathbb{R})$.

In contrast to the odd order case, we mention the class of *Bol loop of exponent 2*. These clearly satisfy (1.3), hence they are Bruck loops.

Loops satisfying both left and right Bol identities are called *Moufang loops.* The most important example of a Moufang loop is the multiplicative structure of *octonions.* Octonions can be constructed by linear algebra over an arbitrary field. More relevant for us is the construction of the *split octonions* $\mathbb{O}(F)$ over the field F. Following Zorn, one uses the *vector matrices*

$$x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}, \tag{1.5}$$

where $a, b \in F$ and α, β are vectors in F^3. The norm N is given as the "determinant" $\det x = ab - \alpha \cdot \beta$, where $\alpha \cdot \beta$ is the usual dot product. The conjugate of x is

$$\overline{x} = \begin{pmatrix} b & -\alpha \\ -\beta & a \end{pmatrix}, \tag{1.6}$$

and two vector matrices are multiplied according to

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha \cdot \delta & a\gamma + d\alpha - \beta \times \delta \\ c\beta + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{pmatrix}, \tag{1.7}$$

where $\beta \times \delta$ is the usual vector product.

The invertible elements of $\mathbb{O}(F)$ form a Moufang loop. The Moufang loop $M(F)$ consisting of elements of norm 1 modulo $\{\pm 1\}$ is a simple nonassociative Moufang loop. If $F = \mathbb{F}_q$ is a finite field, we obtained the complete class of nonassociative finite simple Moufang loops.

For many decades, the existence of non-Moufang non-Bruck simple Bol loops was an open question, in both the finite and infinite case.

A useful result on the right multiplication groups of simple Moufang loops is the following:

Proposition 1.1 ([Nag08a, Lemma 3]). *Let Q be a simple Moufang loop. Then* $\mathrm{RMlt}(Q)$ *is a simple group.*

Proof. If Q is a simple group, then $\mathrm{RMlt}(Q) \cong Q$ is simple. The left and right Bol identities can be written in the form

$$R_x^{-1} R_{xz} = L_x R_z L_x^{-1}, \quad L_y^{-1} L_{xy} = R_y L_x R_y^{-1}.$$

This means that for Moufang loops, the left and right multiplication groups are normal in the full multiplication group. Theorem 4.3 of [NV04] says that for an arbitrary nonassociative simple Moufang loop Q, the multiplication group is simple. Hence, $\mathrm{RMlt}(Q) = \mathrm{RMlt}(Q) = \mathrm{Mlt}(Q)$ is a simple group. □

1.5. The Baer correspondence

Let Q be a loop, $G = \mathrm{RMlt}(Q)$ its right multiplication group, $H = \mathrm{RInn}(Q)$ its right inner mapping group and let K denote the set of the right multiplication maps of Q. Then $1 \in K$, and the triple (G, H, K) has the following properties

(*) K is a system of right coset representatives for all conjugates of H in G.

We rephrase this as a decomposition:

(**) For any $x, y \in G$ there are unique elements $h \in H^y, k \in K$ such that $x = hk$.

Although these properties hold almost trivially, this type of argument is important therefore we explain it. Remember that e denotes the unit element of the loop Q. For the existence of the decomposition, we define the elements $u = e^y, v = u^x$ and $w = u \backslash v$ in Q. Put $k = R_w \in K$ and $h = xk^{-1}$. We have to show that $h \in H^y$, which is equivalent with $yxk^{-1}y^{-1} \in H$. First, $u^k = uw = v$ implies $v^{k^{-1}} = u$. Second,

$$e^{yxk^{-1}y^{-1}} = u^{xk^{-1}y^{-1}} = v^{k^{-1}y^{-1}} = u^{y^{-1}} = e.$$

The uniqueness follows from the fact that $h \in H^y$ implies $u^h = u$, and $u^x = u^k$ which determines $k \in K$ uniquely.

Definition 1.2. *Let G be a group, H a subgroup and $1 \in K \subseteq G$ a subset of G.*

(i) If (*) holds then the triple (G, H, K) is called a loop folder.

(ii) The loop folder (G, H, K) is faithful, if no proper normal subgroup of G is contained in H.

(iii) The loop folder (G_0, H_0, K_0) is a loop subfolder of (G, H, K) if $G_0 \leq G$, $H_0 \leq H$ and $K_0 \subseteq K$.

(iv) The map $\pi : (G, H, K) \to (G_1, H_1, K_1)$ between loop folders is a loop folder homomorphism, provided $\pi : G \to G_1$ is a group homomorphism and $H_1 \leq G^\pi$, $K_1 \subseteq K^\pi$ hold.

Any loop folder (G, H, K) determines a loop operation on K in the following way. Let $x, y \in K$ and take the unique decomposition $xy = hk$ with the elements $h \in H$ and $k \in K$. Define the operation $x * y = k$. Then $(K, *)$ is a loop with unit element 1. In order to see this, let us first assume that $y, k \in K$ are given. Let us decompose ky^{-1} as $h_1 x$ with $h_1 \in H$, $x \in K$. Then $xy = h_1^{-1}k$ and $x * y = k$. We have slightly more delicate situation when $x, k \in K$ are given. Then, we decompose $x^{-1}k$ as $h_2 y$ with $h_2 \in H^x$, $y \in K$. Since $h_2 = x^{-1}h_3 x$ for some $h_3 \in H$, we have

$$x^{-1}k = h_2 y = x^{-1}h_3 xy \quad \Longrightarrow \quad xy = h_3^{-1}k \quad \Longrightarrow \quad x * y = k.$$

Let Loop and Folder be the categories of loops and loop folders, respectively. We define the functors $\lambda : \mathsf{Folder} \to \mathsf{Loop}$ and $\mu : \mathsf{Loop} \to \mathsf{Folder}$. The functor λ maps the loop folder (G, H, K) to the loop $(K, *)$. The functor μ maps the loop $(Q, *)$ to the loop folder (G, H, K), where $G = \mathrm{RMlt}(Q)$, $H = \mathrm{RInn}(Q)$ and K is the set of the right multiplication maps of Q.

This functorial equivalence of the categories of loops and loop folders is called the *Baer correspondence.* It allows us to describe loops by group theoretical tools. The problem is that while $\lambda(\mu(Q)) \cong Q$ for all loops Q, the loop folders $\sigma = (G, H, K)$ and $\mu(\lambda(\sigma))$ may have very different structure. In particular, one can obtain a loop from many different loop folders. This causes special difficulties when one has to identify the subfolder corresponding to a subloop.

We have already seen that the Bol identity (1.2) can be expressed by right multiplication maps, as well. In terms of the loop folder (G, H, K), this means that $k\ell^{-1}k \in K$ holds for all $k, \ell \in K$. *Bol loop folders* have another useful property, namely, it suffices to require the factorization property (**) for the subgroup H only:

(***) For any $x \in G$ there are unique elements $h \in H, k \in K$ such that $x = hk$.

In order to see that (***) implies (**), we mention first that for any $\ell \in K$, $\ell^{-1} = 1\ell^{-1}1 \in K$. Now, fix elements $x, y \in G$ with decomposition $yxy = hk$, $h \in H$, $k \in K$. Define $\ell = y^{-1}ky^{-1} \in K$. Then,

$$x = y^{-1}hky^{-1} = y^{-1}hy\ell = h^y\ell$$

is a decomposition as required in (**) since $h^y \in H^y$ and $\ell \in K$.

Remember that two loops $(Q, \cdot)$ and $(K, \circ)$ are *isotopes* if bijections $\alpha, \beta, \gamma : Q \to K$ exist such that $\alpha(x) \circ \beta(y) = \gamma(x \cdot y)$ for all $x, y \in Q$.

Proposition 1.3 ([Nag08a, Proposition 1])**.** *(i) Let (G, H, S) be a loop folder with associated loop $Q = (S, \circ)$. For any $a, b \in S$, the triple $(G, H^a, b^{-1}S)$ is a loop folder and the associated loop is isotopic to Q. Moreover, all isotopes of Q can be represented in this way.*

(ii) Let (G, H, S) be a Bol loop folder with associated Bol loop Q. Then up to isomorphism, each isotope of Q corresponds to a folder $(G, H, c^{-1}S)$ for some $c \in S$.

(iii) Let (G, H, S) be a Bol loop folder. The associated Bol loop Q is a G-loop if and only if for all $s \in S$ there is an element $h \in H$ with $b^{-1}S = hSh^{-1}$.

Proof. (i) It is clear that $(G, H^a, b^{-1}S)$ is a loop folder. By [Pfl90, III.2.1 Theorem], it is sufficient to show that the respective associated loops of $(G, H, b^{-1}S)$ and (G, H^a, S) are isomorphic to the loops $(S, \bullet)$ and $(S, *)$, respectively, where

$$x \bullet y = x \circ b \backslash y, \qquad x * y = x/a \circ y.$$

Here, the operations $/, \backslash$ denote the right and left divisions of $(S, \circ)$, respectively. In the remaining of the proof, juxtaposition xy and inverting x^{-1} refer to *group operations* in G, all other infix operations refer to loop operations.

On the one hand, the loop $(b^{-1}S, \oplus)$ corresponding to the folder $(G, H, b^{-1}S)$ is defined by $[(b^{-1}x) \oplus (b^{-1}y)]H = b^{-1}xb^{-1}yH$.

$$b^{-1}xb^{-1}yH = b^{-1}(x \circ b \backslash y)H = b^{-1}(x \bullet y)H$$

shows that the map $x \mapsto b^{-1}x$ is a loop isomorphism between $(S, \bullet)$ and $(b^{-1}S, \oplus)$.

On the other hand, we have

$$xH = (x/a \circ a)H = (x/a)aH \Rightarrow (x/a)(aHa^{-1}) = xHa^{-1}.$$

Using this and the definition of the loop $(S, \circledast)$ corresponding to (G, aHa^{-1}, S), we obtain

$$\begin{aligned}
[(x/a) \circledast (y/a)](aHa^{-1}) &= (x/a)(y/a)(aHa^{-1}) \\
&= (x/a)((y/a) \circ a)Ha^{-1} \\
&= (x/a)yHa^{-1} \\
&= ((x/a) \circ y)Ha^{-1} \\
&= [((x * y)/a) \circ a]Ha^{-1} \\
&= ((x * y)/a)(aHa^{-1}).
\end{aligned}$$

This implies $(x/a) \circledast (y/a) = (x * y)/a$, showing that the map $x \mapsto x/a$ is an isomorphism between the loops $(S, *)$ and $(S, \circledast)$.

(ii) As the folders $(G, aHa^{-1}, b^{-1}S)$ and $(G, H, a^{-1}b^{-1}Sa)$ are isomorphic, the statement follows from $a^{-1}b^{-1}Sa = (aba)^{-1}S$.

(iii) If $b^{-1}S = hSh^{-1}$ then the loop folders $(G, H, b^{-1}S)$ and

$$(G, H, S) = (h^{-1}Gh, h^{-1}Hh, S)$$

are isomorphic. □

The loop folder (G, H, K) determines a Bol loop of exponent 2 if and only if $K = \{1\} \cup \bigcup_{i \in I} C_i$, where the C_i's are conjugacy classes of involutions in G.

1.6. Nets

Let $k > 2$ be an integer, $\mathcal{P}$ a set, and $\mathcal{L}_1, \ldots, \mathcal{L}_k$ disjoint sets of subsets of $\mathcal{P}$. Put $\mathcal{L} = \bigcup \mathcal{L}_i$. We call the elements of $\mathcal{P}$ and $\mathcal{L}$ *points* and *lines*, respectively, and use the common geometric terminology, such as "all lines through the point P", etc. For $\ell \in \mathcal{L}_i$, we also speak of a *line of type* i or an *i-line*. Lines of the same type are called *parallel*.

The pair $(\mathcal{P}, \mathcal{L})$ is a *k-net* if the following axioms hold:

1) Distinct lines of the same type are disjoint.

2) Two lines of different types have precisely one point in common.

3) Through any point, there is precisely one line of each type.

Upon interchanging the roles of points and lines, we obtain *dual k-nets*. In that case, the points can be partitioned into k classes so that:

1') Distinct points of the same type are not connected by a line.

2') Two points of different types are connected by a unique line.

3') Every line consists of k points of pairwise different types.

There is a natural relation between loops and 3-nets. Let us first start from a loop L and put $\mathcal{P} = L \times L$. Define the line classes

$$\begin{aligned} \mathcal{L}_1 &= \{\{(x, c) \mid x \in L\} \mid c \in L\}, \\ \mathcal{L}_2 &= \{\{(c, y) \mid y \in L\} \mid c \in L\}, \\ \mathcal{L}_3 &= \{\{(x, y) \mid x, y \in L,\, xy = c\} \mid c \in L\}. \end{aligned}$$

Then, $(\mathcal{P}, \mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3)$ is a 3-net. The lines of these classes are also called *horizontal, vertical* and *transversal lines,* respectively. The point $O = (e, e)$ is the *origin* of the net.

Let us now consider a 3-net $(\mathcal{P}, \mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3)$. Let $O \in \mathcal{P}$ be an arbitrary point, and let ℓ, k be the unique horizontal and vertical lines through O, respectively. Then the construction of Figure 1.1 defines a loop operation on ℓ with neutral element O. Since the parallel projections are bijection between lines of different type, we can index the points of k by points of ℓ, thus obtaining a bijection between $\mathcal{P}$ and $\ell \times \ell$. The three line classes are determined by the equations $X = c$, $Y = c$, $XY = c$, respectively, where c is a constant. We say that (ℓ, O) is a *coordinate loop* of the 3-net $(\mathcal{P}, \mathcal{L})$.

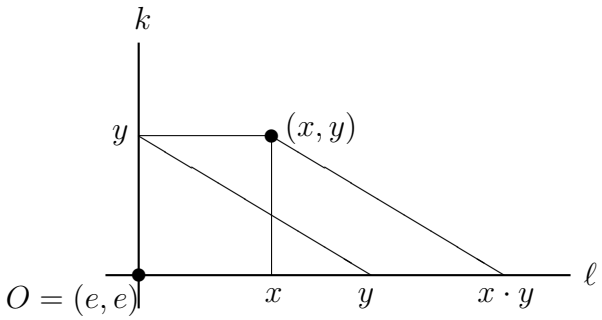


Figure 1.1.: The geometric definition of the coordinate loop.

1.7. Sharply transitive sets, projective and affine planes

Let $G \leq \mathrm{Sym}(\Omega)$ be a subgroup and k be a positive integer. We say that G acts *k-transitively* if for any $(x_1, \ldots, x_k), (y_1, \ldots, y_k) \in \Omega^{(k)}$ there is a element $g \in G$ such that

$$x_1^g = y_1, \cdots, x_k^g = y_k.$$

If the element g is unique then the action is said to be *sharply k-transitive.*

In a similar way, we can introduce the concept of *sharply k-transitive sets.* We say that the set $S \subseteq \mathrm{Sym}(\Omega)$ is a sharply k-transitive set of permutations, if for any $(x_1, \ldots, x_k), (y_1, \ldots, y_k) \in \Omega^{(k)}$ there is a unique element $s \in S$ with $x_1^s = y_1, \cdots, x_k^s = y_k$. When $k = 1$, then we simply speak of a *sharply transitive set.* The class of sharply transitive sets is essentially equivalent with the class of quasigroups, since the binary system $(Q, \cdot)$ is a quasigroup if and only if the set of right multiplication maps is a sharply transitive set on Q.

The finite sharply 2-transitive sets correspond to the class of finite *affine planes* in the following manner. Let S be a sharply 2-transitive set in $\mathrm{Sym}(n)$. Let $\mathcal{P} = \{1, \ldots, n\}^2$ and

$$\mathcal{L} = \{\xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_n\} \cup \{\ell_s \mid s \in S\} \subseteq 2^{\mathcal{P}},$$

where

$$\begin{aligned} \xi_k &= \{(k, t) \mid t = 1, \ldots, n\}, \\ \eta_k &= \{(t, k) \mid t = 1, \ldots, n\}, \\ \ell_s &= \{(t, t^s) \mid t = 1, \ldots, n\}. \end{aligned}$$

Then, the pair $(\mathcal{P}, \mathcal{L})$ forms an affine plane of order n. By omitting the details, we only mention that for the converse, we have to fix a coordinate frame on the affine plane which is similar to the cartesian coordinate system. It is important to notice that sharply transitive and sharply 2-transitive sets behave bad from the point of

view of isomorphy. For example, it is very hard to decide if two sharply 2-transitive sets correspond to isomorphic affine planes.

Let Π be a finite projective plane. The line ℓ of Π is a *translation line* if the *translation group* with respect to ℓ acts transitively (hence regularly) on the set of points $\Pi \setminus \ell$. Assume ℓ to be a translation line and let Π^ℓ be the affine plane obtained from Π with ℓ as the line at infinity. Then Π^ℓ is a *translation plane.*

1.8. Quasifields

A *translation plane* is often represented by an algebraic structure called a *quasifield.* The set Q endowed with two binary operations $+$, $\cdot$ is called a quasifield, if

(Q1) $(Q, +)$ is an abelian group with neutral element $0 \in Q$,

(Q2) $(Q \setminus \{0\}, \cdot)$ is a quasigroup,

(Q3) the right distributive law $(x + y)z = xz + yz$ holds, and,

(Q4) for each $a, b, c \in Q$ with $a \neq b$, there is a unique $x \in Q$ satisfying $xa = xb + c$.

For all $x \in Q$ we have $0 \cdot x = x \cdot 0 = 0$. Conversely, if Q is finite and $x \cdot 0 = 0$ then (Q1), (Q2), (Q3) imply (Q4). Moreover, if Q is finite then $(Q, +)$ is an elementary abelian group.

Many properties of the translation plane can be most easily understood by looking at the appropriate quasifield. However, isomorphic translation planes can be represented by nonisomorphic quasifields. Furthermore, the collineations do not always have a nice representation in terms of operations in the quasifields.

Let p be a prime number and $(Q, +, \cdot)$ be a quasifield of finite order p^n. We identify $(Q, +)$ with the vector group $(\mathbb{F}_p^n, +)$. With respect to the multiplication, the set Q^* of nonzero elements of Q form a *loop.* The *right multiplication maps* of Q are the maps $R_a : Q \to Q$, $xR_a = x \cdot a$, where $a, x \in Q$. By the right distributive law, R_a is a linear map of $Q = \mathbb{F}_p^n$. Clearly, R_0 is the zero map. If $a \neq 0$ then $R_a \in GL(n, p)$. In geometric context, the set of right translations are also called the *slope set* or the *spread set* of the quasifield Q. As the converse is also true, the following concepts are essentially equivalent:

(1) Finite quasifields of order p^n;

(2) Sharply transitive sets of the general linear group $GL(n, p)$, acting on $\mathbb{F}_p^n \setminus \{0\}$;

(3) Sharply 2-transitive sets of the affine linear group $AGL(n, p)$, acting on $\mathbb{F}_p^n$.

The *right multiplication group* $\mathrm{RMlt}(Q)$ of the quasifield Q is the linear group generated by the nonzero right multiplication maps. It is immediate to see that $\mathrm{RMlt}(Q)$ is a transitive linear group, that is, it acts transitively on the set of nonzero vectors of $Q = \mathbb{F}_p^n$. The complete classification of finite transitive linear groups is

known, the proof relies on the classification theorem of finite simple groups. Roughly speaking, there are four infinite classes and 27 exceptional constructions of finite transitive linear groups.

1.9. Semifields

A special case of quasifields is the class of (pre-)semifields, where both distributive laws hold. More precisely, a pre-semifield is a set $\mathbb{S}$ endowed with two binary operations $x + y$ and $x \circ y$ such that the addition is an elementary Abelian group with neutral element 0, $\mathbb{S}^* = \mathbb{S} \setminus \{0\}$ is a multiplicative quasifield and the two operations satisfy both distributive laws. A semifield is a pre-semifield with multiplicative unit element, that is, where $(\mathbb{S}^*, \circ)$ is a loop. Semifields are sometimes called non-associative division rings, as well.

The most known proper semifield is the division ring of the real octonions $\mathbb{O}$ and its complex counterpart $\mathbb{O}(\mathbb{C})$. Both are alternating algebras of dimension 8 over the ground field. On the one hand, a disadvantage of the complex octonions is that they contain zero divisors. On the other hand, it can be constructed over an arbitrary field F, and, the set of invertible elements form a loop in all cases. It is well known that these structures play an important role in the understanding of the orthogonal group $O^+(8, F)$ and its triality automorphism. In fact, $O^+(8, F)$ is the multiplication group of the loop of the invertible elements of $\mathbb{O}(F)$. Moreover, the automorphism group of $\mathbb{O}(F)$ is the exceptional Lie group $G_2(F)$. This fact explains the natural 7-dimensional orthogonal representation of $G_2(F)$.

Any finite semifield $\mathbb{S}$ defines a loop whose multiplication group is contained in $GL(n, q)$ where $\mathbb{F}_q$ is the center of $\mathbb{S}$. The center $Z(\mathbb{S}^*)$ of $\mathbb{S}^*$ is isomorphic to $\mathbb{F}_q^*$, hence for the multiplication group of the factor loop $Q = \mathbb{S}^*/Z(\mathbb{S}^*)$, we have $\mathrm{Mlt}(Q) \leq PGL(n, q)$. Conversely, let $(Q, \cdot)$ be a loop and assume that for some n, q, its multiplication group is contained in the group $\Gamma L(n, q)$, where the latter is considered as a permutation group acting on the nonzero vectors of $V = \mathbb{F}_q^n$. Then, we can identify Q with $V^* = V \setminus \{0\}$ and consider $V = (V, +, \cdot)$ as endowed with two binary operations, where $0 \cdot x = x \cdot 0 = 0$. The fact that the left and right multiplication maps are additive is equivalent with V being a semifield.

2. References

The basic references in the theory of quasigroups are the early papers [Mou35; Alb43; Alb44; Bae39] and the monographs [Bru58; Bel67; Pfl90; CPS90], or more recently [NS02]. Concerning octonions, we refer the reader to [CS03]. The main results on finite simple Moufang loops are due to PAIGE [Pai56], DORO [Dor78] and LIEBECK [Lie87b]. The representation of the hyperbolic plane loop is from [KK95]; further references on Bruck loops are [Gla64; Gla68] and [AKP06]. The problems on the existence of proper simple Bol loops were given in the papers [Rob76; Asc05] and [FKP06]. On the Wikipedia page [Wik14], the reader may follow the progress on problems in the theory of loops and quasigroups.

The idea of handling loops by group theoretical data based on their right multiplication groups goes back to BAER [Bae39]. In the last decades, the main proponent of this approach was Baer's student KARL STRAMBACH. Baer's school preferred terminology of *sections in groups.* Together with his coauthors FIGULA, PÉTER NAGY and others, Strambach was able to tackle many problems from the theory of analytic loops; see the monograph [NS02] and the references therein. The concept of a loop folder and the Baer correspondence was introduced by MICHAEL ASCHBACHER in his paper [Asc05]. Although the idea doubtlessly goes back to Baer, the small differences make this tool more effective for dealing with finite loops.

The relation between sharply 2-transitive sets and finite affine planes is *folklore,* the reader is referred to DEMBOWSKI's book [Dem68]. There are many excellent surveys and monographs on translation planes and quasifields, see [HP73; JJB07; Lü80] and the references therein. Our computational methods have similarities with those in [CD98; Dem94]. The computations on loop folders, sharply transitive sets and net embeddings were done usinge the computer algebra systems MAGMA [BCP97], GAP4 [Gap] and MAPLE 13 [Map].

dc_821_13

Part II.

Bol loops and decompositions in groups

dc_821_13

3. Finite simple Bol loops

In this chapter, we present a construction of Bol loops which is based on exact factorizations of groups. Group factorizations are intensively studied in many fields of mathematics. Using this method, we are able to construct many classes of finite and infinite simple non-Moufang non-Bruck Bol loops, and hence solve the problem of the existence of finite simple non-Moufang Bol loops.

Most part of this chapter has been published in [Nag08a]; the exceptions are Lemma 3.4 and Theorem 3.5 which are new, and Proposition 3.12 which is a generalization of [GN11, Proposition 3.2]. These new results enables us to prove simplicity of Bol loops. Example 3.14 is from [GN11]. The Bol loop construction of Theorem 3.2, the simplicity conditions of Theorems 3.5 and 3.8, and the Examples support **Thesis 1** of the dissertation.

The following papers make a substantial reference to the results of this chapter.

1) In [FS09], Figula and Strambach completed the structural description of topological loops in the case when the group G topologically generated by the right multiplication maps is a proper direct product of simple Lie groups G_1, G_2 and the stabilizer of $1 \in Q$ in G is a direct product $H = H_1 \times H_2$ with $1 \neq H_i \leq G_i$, $i = 1, 2$, and the transversal M is not the direct product of $M_1 = M \cap G_1$ and $M_2 = M \cap G_2$. The motivation for this completion was Example 3.11. Moreover, the authors used the construction of Theorem 3.2 for simple permutation groups G acting on a set Ω and having a sharply transitive subgroup C.

2) Foguel and Kinyon points out in the Introduction of [FK10] that the simple Bol loop of odd order given in Example 3.15 motivates some questions concerning nilpotence and solvability properties of finite Bol loops of odd order. These problems are investigated in [FK10].

3) The intention of the paper [JS10a] by Johnson and Smith is to provide a conceptual understanding of the Bol loop construction of Theorem 3.2, employing direct quasigroup-theoretical methods and the matched-pair approach to group factorizations.

3.1. Exact factorizations of groups

Definition 3.1. *The triple (G, A, B) is called an exact factorization triple if G is a group, A, B are subgroups of G satisfying $A \cap B = 1$ and $AB = G$. The*

exact factorization triple (G, A, B) *is faithful if* A, B *do not contain proper normal subgroups of* G.

If B does not contain any proper normal subgroup of G, then the fact that (G, A, B) is an exact factorization is equivalent with the fact that A is a regular subgroup in the permutation represetation of G on the cosets of B. In the mathematical literature, the group G is also called the *Zappa-Szép product* of the subgroups A, B.

Most importantly for us, if (G, A, B) is an exact factorization triple, then any element $x \in G$ has a unique decomposition $x = ab$ with elements $a \in A$, $b \in B$. The next proposition describes the construction of the Bol loop folder from the exact factorization triple.

Theorem 3.2. *Let* $\tau = (G, A, B)$ *be a faithful exact factorization triple. Let us define the triple* $(\mathcal{G}, \mathcal{H}, K)$ *by*

$$\mathcal{G} = G \times G, \quad \mathcal{H} = A \times B \leq \mathcal{G}, \quad K = \{(x, x^{-1}) \mid x \in G\}.$$

Then $(\mathcal{G}, \mathcal{H}, K)$ *is a Bol loop folder. The associated Bol loop* $(S, \circ)$ *is a G-loop.*

Proof. Clearly, $1 \in K$ and for any $x, y \in G$,

$$(x, x^{-1})(y, y^{-1})(x, x^{-1}) = (xyx, (xyx)^{-1}) \in K.$$

Hence, it suffices to show the decomposition property (***). Let $x_1, x_2 \in G$ be arbitrary elements and define $a_1, a_2 \in A$, $b_1, b_2 \in B$ by the decompositions $x_1 = a_1 b_1$ and $x_2^{-1} = a_2 b_2$. Straightforward calculation shows that with elements

$$c = a_1 a_2^{-1} \in A, \quad d = b_2^{-1} b_1 \in B, \quad x_3 = a_2 b_1 \in G,$$

we have $(x_1, x_2) = (c, d)(x_3, x_3^{-1})$, which shows the existence of the decomposition (***). In order to prove the uniqueness, we take arbitrary elements $c, c_0 \in A$, $d, d_0 \in B$, $x_3 = a_3 b_3, x_0 \in G$ and deduce

$$\begin{aligned}
(cx_3, dx_3^{-1}) = (c_0 x_0, d_0 x_0^{-1}) &\Longrightarrow x_0 = c_0^{-1} c x_3,\ x_0^{-1} = d_0^{-1} d x_3^{-1} \\
&\Longrightarrow 1 = c_0^{-1} c x_3 \cdot d_0^{-1} d x_3^{-1} = c_0^{-1} c a_3 b_3 \cdot d_0^{-1} d b_3^{-1} a_3^{-1} \\
&\Longrightarrow a_3^{-1} c^{-1} c_0 a_3 = b_3 d_0^{-1} d b_3^{-1} \in A \cap B = 1 \\
&\Longrightarrow c^{-1} c_0 = d_0^{-1} d = 1 \\
&\Longrightarrow c = c_0,\ d = d_0,\ x_3 = x_0.
\end{aligned}$$

This proves that $(\mathcal{G}, \mathcal{H}, K)$ is a Bol loop folder. Take arbitrary elements $x, y \in G$, and write $y = ab^{-1}$ with $a \in A, b \in B$. Then

$$(a, b)(x, x^{-1})(a, b)^{-1} = (y, y^{-1})(bxa^{-1}, ax^{-1}b^{-1}) \in (y, y^{-1})K.$$

Since $(a, b) \in \mathcal{H}$, Proposition 1.3(iii) implies that the associated Bol loop is a G-loop. □

Definition 3.3. *Let* $\tau = (G, A, B)$ *be a faithful exact factorization triple and let us define* $\mathcal{G}, \mathcal{H}, K$ *as in Theorem 3.2. The Bol loop corresponding to the Bol loop folder* $(\mathcal{G}, \mathcal{H}, K)$ *will be denoted by* $\beta(\tau)$.

3.2. Simplicity conditions for Bol loop folders

We need some technical information on the structure of the direct product $G \times G$.

Lemma 3.4. *Let G be a group, $K = \{(x, x^{-1}) \mid x \in G\} \subseteq G \times G$ and define the maps $\pi : G \times G \to G$ and $\alpha : G \times G \to G/G'$ by*

$$\pi(x, y) \mapsto y, \quad \text{and} \quad \alpha(x, y) = xyG'.$$

Then the following hold:

(i) $\pi(\langle K \rangle) = G$ *and* $\langle K \rangle \cap \ker \pi = G' \times 1$.

(ii) $\langle K \rangle = \ker \alpha$.

(iii) $AG' \cap B \leq \pi((A \times B) \cap \ker \alpha)$ *for any* $A, B \in G$.

Proof. $\pi(\langle K \rangle) = G$ and $\langle K \rangle \cap \ker \pi \leq G' \times 1$ are trivial. Since for arbitrary $x, y \in G$,

$$((xy)x^{-1}y^{-1}, (xy)^{-1}xy) = (xyx^{-1}y^{-1}, 1) \in \langle K \rangle \cap \ker \pi,$$

we have (i). For (ii), $\langle K \rangle \leq \ker \alpha$ is obvious. Let us assume $(x, y) \in \ker \alpha$, that is, $xy \in G'$. Then $(xy, 1) \in G' \times 1 \leq \langle K \rangle$ by (i), and

$$(xy, 1) = (x, y)(y, y^{-1}) \in (x, y)\langle K \rangle,$$

whence $(x, y) \in \langle K \rangle$. This shows (ii). Let $b \in B$ be an arbitrary element:

$$\begin{aligned} b \in AG' \cap B &\Longrightarrow \exists a \in A : \ b \in aG' \\ &\Longrightarrow \exists a \in A : \ (a^{-1}, b) \in \ker \alpha \\ &\Longrightarrow b \in \pi((A \times B) \cap \ker \alpha). \end{aligned}$$

This proves (iii). □

Theorem 3.5. *Let (G, A, B) be an exact factorization triple such that the following hold:*

(1) $\mathrm{core}_G(A) = \mathrm{core}_G(B) = C_G(G') = 1$.

(2) A is maximal in G and A' is maximal in G'.

(3) The normal closure of $AG' \cap B$ in G is G.

Then, $\beta(G, A, B)$ is a simple non-Moufang Bol loop.

Proof. We write $\mathcal{G} = \langle K \rangle$ and $\mathcal{H} = (A \cap B) \cap \mathcal{G}$. The faithful Bol envelop of Q is $(\mathcal{G}, \mathcal{H}, K)$. Let $\varphi_0 : Q \to \bar{Q}$ be a surjective loop homomorphism. Let us denote the corresponding folder homomorphism by $\varphi : (\mathcal{G}, \mathcal{H}, K) \to (\bar{\mathcal{G}}, \bar{\mathcal{H}}, \bar{K})$, where $(\bar{\mathcal{G}}, \bar{\mathcal{H}}, \bar{K})$ is the faithful Bol envelop of $\bar{Q}$. Put $\ker\varphi = (\mathcal{G}_0, \mathcal{H}_0, K_0)$; then by [Asc05, (2.7)], $\mathcal{G}_0 \lhd \mathcal{G}$, and

$$\bar{\mathcal{G}} \cong \mathcal{G}/\mathcal{G}_0, \quad \bar{\mathcal{H}} \cong \mathcal{G}_0\mathcal{H}/\mathcal{G}_0, \quad \bar{K} \cong \mathcal{G}_0 K/\mathcal{G}_0.$$

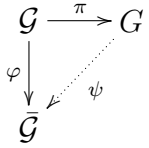
As $(\bar{\mathcal{G}}, \bar{\mathcal{H}}, \bar{K})$ is faithful, we have

$$\mathcal{G}_0 = \mathrm{core}_{\mathcal{G}}(\mathcal{G}_0\mathcal{H}). \tag{3.1}$$

By Lemma 3.4(i), $A' \times 1 \leq \mathcal{H}$. Moreover, $[\mathcal{G}_0, G' \times 1] = U \times 1$ is a normal subgroup of $\mathcal{G}_0$ for some $U \lhd G$. Hence, $UA' \times 1 \leq \mathcal{G}_0\mathcal{H}$. Since A' is maximal in G' by assumption, either $U \leq A'$, or $UA' = G'$.

Assume $U \leq A'$. By $\mathrm{core}_G(A) = 1$, $U = 1$. Then $C_G(G') = 1$ implies $\mathcal{G}_0 \leq 1 \times G$, thus, $\mathcal{G}_0 = 1 \times V$ for some $V \lhd G$. Furthermore, $K_0 = \mathcal{G}_0 \cap K = 1$, and, $\mathcal{G}_0 = \mathcal{H}_0 K_0 = \mathcal{H}_0 \leq \mathcal{H}$. As $\mathcal{H}$ is core-free, we have $\mathcal{G}_0 = 1$ and φ is injective.

Assume $UA' = G'$. Then the normal subgroup $G' \times 1$ is contained in $\mathcal{G}_0\mathcal{H}$; $G' \times 1 \leq \mathcal{G}_0$ holds by (3.1). As $\ker\pi \leq \mathcal{G}_0$ by Lemma 3.4(i), there is a surjective homomorphism $\psi : G \to \bar{\mathcal{G}}$ such that $\varphi = \psi\pi$.



By

$$\bar{K} = \varphi(K) = \psi(\pi(K)) = \psi(G) = \bar{\mathcal{G}},$$

we have $\bar{\mathcal{H}} = \varphi(\mathcal{H}) = 1$. This implies

$$\pi(\mathcal{H}) \leq \ker\psi. \tag{3.2}$$

By Lemma 3.4(iii),

$$\pi(\mathcal{H}) = \pi((A \times B) \cap \ker\alpha) \geq AG' \cap B,$$

whose normal closure in G is G. Therefore $G = \ker\psi$, hence ψ and φ are trivial. We have seen that φ is either injective or trivial, the simplicity of Q follows. Moreover, Q is non-Moufang by Proposition 1.1. □

Lemma 3.6. *Let k be a field and $A \leq GL_n(k)$ an irreducible linear group and let $G = A \ltimes k^n$. Then A is maximal in G and every normal subgroup of G contains k^n.* □

Lemma 3.7. *Let (G, H, K) be a faithful Bol envelop with corresponding Bol loop Q. Let σ be an automorphism of G such that $x^\sigma = x^{-1}$ for all $x \in K$. Assume that for any σ-invariant normal subgroup N of G, $NH = G$ holds. Then Q is simple.*

Proof. Let $\varphi_0 : Q \to \bar{Q}$ be a surjective loop homomorphism. Let us denote the corresponding folder homomorphism by $\varphi : (G, H, K) \to (\bar{G}, \bar{H}, \bar{K})$, where $(\bar{G}, \bar{H}, \bar{K})$ is the faithful Bol envelop of $\bar{Q}$. Put $\ker \varphi = (G_0, H_0, K_0)$ and assume that $G_0 \neq 1$. As $G_0 \triangleleft G$ and H is core-free in G, $1 \neq K_0 = G_0 \cap K$. By [Asc05, 6.1(1)],

$$K_0^\sigma = \{x^{-1} \mid x \in K_0\} = K_0.$$

This implies $K_0 \subseteq G_0^\sigma$, and $N = G_0 \cap G_0^\sigma$ is a nontrivial σ-invariant normal subgroup of G. By assumption, $NH = G$. Therefore, $G_0H = G$ and $G_0H/G_0 = G/G_0$, and $\bar{G} = \bar{H}$ follows from [Asc05, (2.7)]. Since $(\bar{G}, \bar{H}, \bar{K})$ is faithful, we obtained $\bar{G} = 1$ and $G = G_0$. The simplicity of Q follows. □

We call the group G *almost simple* if $T \leq G \leq \mathrm{Aut}(T)$ for some nonabelian simple group T. The group T is the *socle* of G.

Theorem 3.8. *Let G be an almost simple group with socle T. Let $\tau = (G, A, B)$ be a faithful exact factorization triple and assume $G = TA = TB$. Then $\beta(\tau)$ is a simple non-Moufang Bol loop.*

Proof. Let σ be the automorphism of $G \times G$ mapping $(x, y) \mapsto (y, x)$. Since $K^\sigma = K$, $\mathcal{G}^\sigma = \mathcal{G}$ has an automorphism which inverts the elements of K. Clearly, $T \times T \leq G' \times G' \leq \mathcal{G}$ and every σ-invariant normal subgroup of $\mathcal{G}$ contains $T \times T$. However, $(T \times T)(A \times B) = G \times G$ by assumption, which implies $\mathcal{G} = (T \times T)(\mathcal{G} \cap (A \times B)) = (T \times T)\mathcal{H}$. Thus, $\beta(\tau)$ is simple by Lemma 3.7. Moreover, Q is non-Moufang by Proposition 1.1. □

3.3. Some classes of simple proper Bol loops

In this section we present some finite and infinite simple proper Bol loops by applying the construction of Theorem 3.2.

Example 3.9. Put $G = PSL(n, 2)$, let A be a Singer cycle and B be the stabilizer of a projective point. Then $\beta(G, A, B)$ is a finite simple proper Bol loop by Theorem 3.8.

We notice that many other finite simple groups have exact factorizations. The factorizations of finite groups are intensively studied, cf. [LPS00], [Giu06] and the references therein.

Example 3.10. Let n be an even integer and put $G = S_n$, $A = \langle (1, 2, \ldots, n) \rangle$ and $B = S_{n-1}$ with $n \geq 4$. Define the loop $Q_n = \beta(G, A, B)$. If $n \geq 6$ then Q_n is simple by Theorem 3.8.

In the case $n = 4$, Q_4 is a Bol loop of order 24. This loop can be constructed as in Example 3.14, too. It turns out that this loop is simple, as well.

Example 3.11. Put $G = PSL_2(\mathbb{R})$ and define the subgroups

$$A = \left\{ \pm \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix} \mid t \in \mathbb{R} \right\}, \quad B = \left\{ \pm \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{R} \setminus \{0\}, b \in \mathbb{R} \right\}$$

of G. By Theorem 3.8, $\beta(G, A, B)$ is a simple non-Moufang Bol loop.

The right multiplication group of $\beta(G, A, B)$ is isomorphic to $PSL_2(\mathbb{R}) \times PSL_2(\mathbb{R})$. Moreover, the loop is isomorphic to all its isotopes; in particular, it is not isotopic to a Bruck loop. Recall that by definition, *Bruck loops* are Bol loops satisfying the *automorphic inverse property* $(xy)^{-1} = x^{-1}y^{-1}$. By [Rob76, Corollary 3.2.2], Bruck G-loops are Abelian groups. Until this construction, all known simple non-Moufang Bol loops were isotopes of Bruck loops, cf. [KK04].

In [Fig06], the author classified all differentiable Bol loops having a semi-simple right multiplications group of dimension at most 9. In fact, Example 3.11 showed that one has to pay special attention to the case when the group G topologically generated by the right multiplication maps is a proper direct product of simple Lie groups G_1, G_2 and the stabilizer of $1 \in Q$ in G is a direct product $H = H_1 \times H_2$ with $1 \neq H_i \leq G_i$, $i = 1, 2$, and the transversal M is not the direct product of $M_1 = M \cap G_1$ and $M_2 = M \cap G_2$. In [FS09], Figula and Strambach completed the classification and settled this problem in more generality.

Let k be an arbitrary field. With a vector $v \in k^n$, we mean a *row vector*. If a is an $n \times n$ matrix then the product of a and v is written as va. The commutator $[a, v]$ is the vector $va - v$. Let $A \leq GL_n(k)$ be a linear group. The *semi-direct product* $A \ltimes k^n$ consists of the pairs (a, v), $a \in A$, $v \in k^n$, with product

$$(a, v)(b, w) = (ab, vb + w).$$

Proposition 3.12. *Let k be a field and $A \leq GL_n(k)$ be a linear group. Let $\gamma : k^n \to A$ be a homomorphism such that $[T, k^n] \leq \ker\gamma$, where $T = \mathrm{Im}(\gamma)$. Put $G = A \ltimes k^n$ and define the subset*

$$B = \{(\gamma(-v), v) \mid v \in k^n\}$$

of G.

(i) $B \leq G$ and the triple $\tau = (G, A, B)$ is an exact factorization.

(ii) If A is irreducible and γ is nontrivial then τ is faithful.

(iii) If A, A' are irreducible and the normal closure of $\mathrm{Im}(\gamma)$ in A is A then $\beta(\tau)$ is a simple non-Moufang Bol loop.

Proof. (i) For any matrix $t \in T$ and vector $v \in k^n$, $\gamma(vt) = \gamma(v + [t, v]) = \gamma(v)$ by $[T, k^n] \leq \ker\gamma$. This implies

$$(\gamma(-v_1), v_1)(\gamma(-v_2), v_2) = (\gamma(-v_1 - v_2), v_1 + v_2).$$

In particular, $B \leq G$. $A \cap B = 1$ is obvious. The element $(a, v) \in G$ can be decomposed as

$$(a, v) = (a\gamma(v), 0)(\gamma(v)^{-1}, v)$$

with $(a\gamma(v), 0) \in A$ and $(\gamma(v)^{-1}, v) \in B$.

(ii) Let us assume that A is irreducible. Then k^n is a minimal normal subgroup in G, hence, A, B are core-free since none of them contains k^n.

(iii) Let us assume that A, A' are irreducible and the normal closure of $\mathrm{Im}(\gamma)$ in A is A. Since k^n is a minimal normal subgroup, $G' = A' \ltimes k^n$ and $Z(G') = 1$. This implies $Z(G) = C_G(G') = 1$. Moreover, A' is maximal in G' by the irreducibility of A'. Let N be the normal closure of $AG' \cap B = B$ in G and write N as $N_0 \ltimes k^n$ with $N_0 \lhd A$. Then $\mathrm{Im}(\gamma) \leq N_0$ and $N_0 = A$ by assumption. Thus, $N = G$. This shows that G, A, B satisfy the conditions of Theorem 3.5, and $\beta(\tau)$ is a simple non-Moufang Bol loop. □

Let A and γ be as in Proposition 3.12. The corresponding simple Bol loop will be denoted by $\beta^*(A, \gamma)$.

Corollary 3.13. *The right multiplication group of $\beta^*(A, \gamma)$ is solvable if and only if A is solvable. If the underlying field $k = \mathbb{F}_q$ is finite then $\beta^*(A, \gamma)$ has order $|A|q^n$.*

Proof. Since $\beta^*(A, \gamma)$ is constructed from an exact factorization, its right multiplication group is a subgroup between $G \times G$ and $G' \times G'$, where $G = A \ltimes k^n$. The solvability of the groups G, G', A and A' is equivalent. □

Example 3.14. Let k be a field, $A = SL_2(k)$ and $\gamma : k^2 \to A$ given by

$$\gamma(x_1, x_2) = \begin{pmatrix} 1 & x_1 \\ 0 & 1 \end{pmatrix}.$$

Then γ is a homomorphism and

$$[\gamma(x_1, x_2), (y_1, y_2)] = (0, x_1 y_1) \in \ker \gamma.$$

Moreover, the normal closure of the group $\mathrm{Im}(\gamma)$ of unipotent matrices is $SL_2(k)$. If $|k| \leq 3$ then this can be verified by hand. If $|k| > 3$ then $SL_2(k)$ is simple modulo its center, which implies our claim since the elements $\gamma(x_1, x_2)$ are not central. Therefore, the pair A, γ satisfies the conditions of Proposition 3.12, hence, it yields a simple non-Moufang Bol loop.

If $k = \mathbb{F}_2$ then the loop Q of Example 3.14 has order 24 and $\mathrm{RMlt}(Q)$ is a solvable group, see Corollary 3.13. In fact, Q is the same loop than constructed by Example 3.10 with $n = 4$. The computer result [Moo07] of G. E. Moorhouse shows that all Bol loops of order less than 24 are solvable, hence Q is a simple Bol loop of least possible order.

The last example gives a simple Bol loop of order $3^4 \cdot 13 = 1053$. This construction shows that the Odd Order Theorem does not hold for finite Bol loops, cf. [FKP06].

Example 3.15. Let $k = \mathbb{F}_3$ and identify k^3 with $\mathbb{F}_{27}$. Let g be a primitive element in $\mathbb{F}_{27}$ and define the linear map $\sigma : x \mapsto g^2 x$ of order 13. Let Φ be the Frobenius automorphism $x \mapsto x^3$ of $\mathbb{F}_{27}$. Then $\sigma\Phi = \Phi\sigma^3$ and $A = \langle \Phi, \sigma \rangle$ is a non-abelian linear group such that $A' = \langle \sigma \rangle$. For $x \in \mathbb{F}_{27}$, write $\mathrm{Tr}(x) = x^9 + x^3 + x$. Notice that for all $y \in \mathbb{F}_{27}$,

$$\mathrm{Tr}([\Phi^i, y]) = \mathrm{Tr}(y^{\Phi^i} - y) = 0. \tag{3.3}$$

Define the map $\gamma : \mathbb{F}_{27} \to A$ by $\gamma(x) = \Phi^{\mathrm{Tr}(x)}$. By (3.3), $[\gamma(x), y] \in \ker \gamma$ for all $x, y \in \mathbb{F}_{27}$. This means that A, γ satisfy the conditions of Proposition 3.12, and, $\beta^*(A, \gamma)$ is a simple Bol loop of order $3^4 \cdot 13$.

4. Finite simple Bol loops of exponent 2

Bol loops of exponent 2 which are not elementary Abelian groups have long been known to exist, the first construction is due to R. P. Burn [Bur78]. Later, many infinite classes of such loops were given, see [Kie02; KN02; KK95; Nag06]. All of these examples were solvable loops; equivalently the group G was a 2-group. The existence of nonsolvable finite Bol loops of exponent 2 was considered as one of the main open problem in the theory of loops and quasigroups. As the smallest such loop must be simple, this question was related to the existence of finite simple proper right Bol loops. Here by proper we mean right Bol loops which are not Moufang, that is, which do not satisfy the identity $x(yx) = (xy)x$.

By [Nag98], the solvability of a Bol loop of 2-power exponent is equivalent to having 2-power order. Later, S. Heiss [Hei96] showed that the solvability of the loop corresponding to the triple (G, H, K) is equivalent with the solvability of the group G. The next major step was the paper [Asc05] by M. Aschbacher. His main result gives a detailed description on the structure of the right multiplication group of minimal nonsolvable Bol loops of exponent 2. This result was achieved by using the classification of finite simple groups.

In this chapter we apply Aschbacher's recipe to construct a class of finite simple Bol loops of exponent 2. In this way, we give a negative answer to questions 2 and 3 of [Asc05] and [AKP06]. The smallest member of our class has order 96. We emphasize that this example is so small and the structural description of the smallest example in [Asc05] and [AKP06] is so precise that it was only a matter of time that somebody finds it by some short computer calculation. This explains the fact that this loop was indepently discovered by the author and by B. Baumeister and A. Stein [BS11] in 2007, with a time delay of 10 days.

The content of this chapter is almost identical with the paper [Nag09]. Theorems 4.7 and 4.14 support **Thesis 2.** These results had the following impacts:

1) Baumeister, Stein and Stroth continued the intensive investigations of finite Bol loops of 2-power exponent in a series of papers [BS10; BSS11; BS11; Bau12]. In fact, they gave a partial answer to Problem 4.16 by showing that whenever T is an almost simple groups for which an exponent 2 Bol loop folder (G, H, K) exists such that $T \cong G/O_2(G)$, T is isomorphic to $PSL(2, q)$ for $q = 9$ or a Fermat prime $q \geq 5$, cf [BS11, Theorem 1].

2) The paper [JS10b] by Johnson and Smith intends to give a more explicit combinatorial specification of the smallest simple, unipotent Bol loop of Theorem 4.7, making use of concepts from projective geometry and quasigroup theory along with the group-theoretical background.

4.1. The construction of the "smallest counterexample"

As usual, S_5 and $PGL(2,5)$ are the permutation groups acting on 5 and 6 points, respectively. It is well known that $S_5 \cong PGL(2,5) \cong \mathrm{Aut}(L_2(4)) \cong O_4^-(2)$, where $\mathrm{Aut}(L_2(4))$ is the extension of $L_2(4) = PSL(2,4) \cong A_5$ by a field automorphism of order 2, and $O_4^-(2)$ is the orthogonal group on a 4-dimensional orthogonal space over $\mathbb{F}_2$ of Witt index 1. We denote by F_{20} the affine linear group acting on $\mathbb{F}_5$, $F_{20} \cong C_5 \rtimes C_4$. On the one hand, F_{20} is the Borel subgroup of $PGL(2,5)$, that is, the stabilizer of a projective point. On the other hand, $F_{20} \leq S_5$ is a sharply 2-transitive permutation group on 5 points.

In the sequel, we define a group G which is a nonsplit extension of the elementary Abelian group of order 32 by S_5 such that the transpositions of S_5 lift to involutions in G and the even involutions of S_5 lift to elements of order 4. Despite the relatively small order of G, we found no simple description for this group; therefore our definion will be rather *ad hoc,* as well. We start with two technical lemmas.

Lemma 4.1. *We have the following presentations of groups with generators and relations.*

$$\begin{aligned} A_5 &= \langle a,b \mid a^2 = b^3 = (ab)^5 = 1\rangle, \\ S_5 &= \langle c,d \mid c^2 = d^4 = (cd)^5 = [c,d]^3 = 1\rangle, \\ 2.S_5 &= \langle C,D \mid C^2 = D^8 = (CD)^5 = [C,D]^3 = [C,D^4] = 1\rangle, \end{aligned}$$

where $2.S_5$ denotes the nonsplit central extension of S_5 in which the transpositions lift to involutions. In other words, $2.S_5$ is the semidirect product of $SL(2,5) = 2.A_5$ with a group of order 2.

Proof. The presentation for A_5 is well known. Assume $G = \langle c,d\rangle$ is the group presented by the second set of relations above. We observe first that S_5 satisfies these relations, hence no relation can collapse. Put $a = d^2$ and $b = [d,c] = [c,d]^{-1}$. Then $a^2 = b^3 = 1$ and $ab = (dc)^2 = ((cd)^2)^c$. This latter implies $(ab)^5 = 1$, hence $G_0 = \langle a,b\rangle \cong A_5$. Moreover, since $dc = (dc)^6 = (ab)^3 \in G_0$, we have $cd = dc[c,d] = dcb^{-1} \in G_0$ and

$$dbd^{-1} = cdcd^{-1} = (cd)^2 d^{-2} \in G_0.$$

This means that d and cd normalize G_0, so $G_0 \lhd G$. So $|G : G_0| = 2$ and $d \notin G_0$ since A_5 contains no element of order 4. This proves $G \cong S_5$. Finally, D^4 is a central

involution in $H = \langle C, D\rangle$ and $H/\langle D^4\rangle$ maps surjectively to S_5. The order of D is 8, thus, the extension is nonsplit and the involution C covers a transposition in S_5. □

Lemma 4.2. *The permutations*

$$\begin{aligned} c &= (1,4)(2,9)(3,10)(6,11)(7,12)(13,21)(14,22)(15,24)(16,23)(17,30)\\ &\quad (18,29)(19,31)(20,32)(33,35)(38,40),\\ d &= (1,2,4,6,8,7,5,3)(9,13,25,18,10,14,26,17)(11,15,27,20,12,16,\\ &\quad 28,19)(21,30,38,34,23,31,40,35)(22,32,39,36,24,29,37,33) \end{aligned}$$

acting on 40 *points satisfy the relations*

$$c^2 = d^8 = (cd)^5 = [c,d]^3 = [d^4,c]^2 = [d^4, cdcd^{-2}c] = 1. \tag{4.1}$$

Moreover, with $u_1 = d^4$, $u_2 = u_1^c$, $u_3 = u_1^{cd}$, $u_4 = u_1^{cdc}$, $u_5 = u_1^{cdcd}$, $u_6 = u_1^{cdcdc}$ *the identity* $u_1u_2u_3u_4u_5u_6 = 1$ *holds.*

Proof. We leave the straightforward calculations to the reader. □

Lemma 4.3. *The group* $G = \langle c, d\rangle$ *given in Lemma 4.2 satisfies*

(#) *G has an elementary Abelian normal subgroup J of order* 32 *such that* $G/J \cong PGL(2,5)$ *and J is the $\mathbb{F}_2$-permutation module modulo its center. Moreover,*

$$[G,G]/[G,J] \cong SL(2,5)$$

and G splits over $[G,G]J$.

Proof. We claim that the conjugacy class of $u_1 = d^4$ in G is $X = \{u_1, \ldots, u_6\}$. It is immediate that c induces the permutation $(u_1u_2)(u_3u_4)(u_5u_6)$ on X. Moreover, d centralizes u_1 and maps $u_2 \mapsto u_3$, $u_4 \mapsto u_5$. From the last relation in (4.1) follows $u_1^{cdc} = u_1^{cd^2}$, hence $u_3^d = u_3^c = u_4$. By $[d^4,c]^2 = 1$ we have

$$u_1^{cd^4c} = cd^4cd^4cd^4c = d^4[d^4,c]^2 = d^4 = u_1,$$

thus $u_2 = u_1^c = u_1^{cd^4} = u_4^{d^2} = u_5^d$. To see that d acts on X, we need to show that d centralizes u_6:

$$u_6^d = u_1^{cdcdcd} = u_1^{(cd)^{-2}} = u_1^{d^{-1}cd^{-1}c} = u_1^{cd^{-1}c} = u_2^{d^{-1}c} = u_5^c = u_6.$$

The action of d on X is therefore $(u_2u_3u_4u_5)$. This not only shows that X is a conjugacy class in G, but we also have the action of G on X. Indeed, one shows by straightforward calculation that $\tilde{c} = (12)(34)(56)$ and $\tilde{d} = (2345)$ satisfy the relations of S_5 from Lemma 4.1. Since the action of S_5 on 6 points is unique, we have $G/C_G(X) \cong PGL(2,5)$.

As $[u_1,u_2] = [d^4, cd^4c] = [d^4,c]^2 = 1$ and $PGL(2,5)$ acts 2-transitively, $[u_i,u_j] = 1$ holds for all i,j. This means that $J = \langle X\rangle$ is an elementary Abelian 2-group

and $|J| = 32$ by $u_1 \cdots u_6 = 1$. Using the presentation of $2.S_5$ from Lemma 4.1, $G/J_0 \cong 2.S_5$. This implies

$$[G,G]/[G,J] \cong [G/J_0, G/J_0] \cong 2.A_5 \cong SL(2,5).$$

Finally, G splits over $[G,G]J$ as $c \notin [G,G]J$. □

In the sequel, G will denote a group satisfying (#). We would like to make clear that it can be shown using the computer algebra system GAP [Gap] that the group given in Lemma 4.2 is the unique group with this property. However, we hope that this more general approach will help in future generalization of the constructions of this chapter.

Among other properties, we show in the next lemma that for our group G, $G' = [G,G]$ is a perfect group. Actually, we found G' by using the library of perfect groups in the computer algebra system GAP [Gap] and constructed G as a split extension of G' by an outer automorphism of order 2.

Lemma 4.4. *Let G be a group satisfying (#) and define $J_0 = [G,J]$.*

(i) We have $G'' = G' = [G,G] = [G,G]J$ and $|G : G'| = 2$.

(ii) $G \setminus J$ contains a unique class c^G of involutions, and $|c^G| = 80$. In particular, all involutions of $G' = [G,G] = [G,G]J$ lie in J.

(iii) Let P be a Sylow 5-subgroup. Then $N_{J_0}(P) = \{1\}$ and $N_G(P) \cong C_8 \ltimes C_5$. Moreover, if the subgroup $U \leq G$ maps onto F_{20} modulo J then $U = N_G(P)$ or $U = N_G(P)J_0$.

Proof. (i) Let V be the permutation $\mathbb{F}_2$-module of $PGL(2,5)$ with basis $\{u_1, \ldots, u_6\}$. Due to the 2-transitivity, the orbit of the element $u_1 + u_2$ consists of the elements $u_i + u_j$, $i \neq j$ which are different modulo the center $\langle u_1 + \ldots + u_6 \rangle$ of V. Hence both $PGL(2,5)$ and $PSL(2,5)$ act transitively on the nonidentity elements of $J_0 = [G,J]$, which implies that J_0 is a minimal normal subgroup in G and $[G,G]J$. It follows that $J_0 = [G', J_0]$ and $G''/J_0 = (G'/J_0)' = G'/J_0$ by $SL(2,5)' = SL(2,5)$. This means $G'' = G'$. Finally, $J \leq G'$ follows from $J/J_0 = Z(G/J_0) \leq (G/J_0)' = G'/J_0$.

(ii) Since G splits over $G' = G'J$ we can take an involution c from $G \setminus G'$; the image of c in $G/J \cong S_5$ is a transposition. As J is the permutation module modulo its center, $\dim_{\mathbb{F}_2}(C_{J_0}(c)) = 2$ and $\dim_{\mathbb{F}_2}(C_J(c)) = 3$. It is easy to check that $2.S_5 \cong G/J_0$ contains 20 non-central involutions and they are all conjugate.

Let c' be another involution in $G \setminus J$; we want show that c, c' are conjugate. For some $g \in G$, $(cJ_0)^{gJ_0} = c'J_0$, that is, $c^g \in c'J_0$. Hence we can assume $c \in c'J_0$, $c' = cj$ with $j \in J_0$. The element cj has order 2 if and only if $j \in C_{J_0}(c)$. On the one hand, $c^{J_0} \subseteq cC_{J_0}(c)$. On the other hand,

$$|c^{J_0}| = |J_0 : C_{J_0}(c)| = 4 = |C_{J_0}(c)| = |cC_{J_0}(c)|.$$

This implies $c^{J_0} = cC_{J_0}(c)$ and $c' \in c^{J_0}$. No involution of G' can be conjugate to c, hence all involutions of G' must lie in J. Finally, we show $|c^G| = 80$. As $c^g \in cJ_0$

if and only if $c^g = c^j$ for some $j \in J_0$, we have $N_G(cJ_0) = C_G(c)J_0$. Moreover, $C_{G/J_0}(cJ_0) = N_G(cJ_0)/J_0$. Thus,

$$\begin{aligned} |G : C_G(c)| &= |G : N_G(cJ_0)||C_G(c)J_0 : C_G(c)| \\ &= |G/J_0 : C_{G/J_0}(cJ_0)||J_0 : C_{J_0}(c)| \\ &= |(cJ_0)^{G/J_0}||c^{J_0}| = 20 \cdot 4 = 80. \end{aligned}$$

(iii) P acts fixed point free on the involutions of J_0, thus, $N_{J_0}(P) = 1$. Moreover, $5 \nmid |J| - 1$, hence P centralizes a unique element $a \in J$. Let U be a preimage of F_{20} modulo J and put $\bar{U} = U/\langle a \rangle$, $\bar{J} = J/\langle a \rangle$. Then $\bar{J}$ is a minimal normal subgroup of $\bar{U}$. Since $F_{20} = \bar{U}/\bar{J}$ acts faithfully on $\bar{J}$, we have $C_{\bar{U}}(\bar{J}) = \bar{J}$. By [Hup67, II.3.3. Satz], $\bar{J}$ has a complement $\bar{H}$ in $\bar{U}$, $\bar{H} \cong F_{20}$. Let H be the preimage of $\bar{H}$, then H has a unique (hence normal) 5-Sylow and $H \cong C_8 \ltimes C_5$. This shows $N_G(P) \cong C_8 \ltimes C_5$. For the last statement, record that $U \cap J_0$ is either 1 or J_0. □

The following proposition will apply in all of our examples of Bol loop folders of exponent 2. We hope that it will also apply in future constructions not considered here. Recall that $O_2(G)$ is the largest normal 2-subgroup of G.

Proposition 4.5. *Assume G is a finite group, $J = O_2(G)$ and $G^+ = G/J \cong S_5$. We denote by g^+ the element of S_5 corresponding to gJ. Set $L = G'J$, K_1 the involutions in $G \setminus L$, K_0 a G-invariant subset of J containing 1 such that $K_0 \setminus \{1\}$ consists of involutions, and $H \leq G$. Set $K = K_0 \cup K_1$, $n_0 = |K_0|$, and $n_1 = |K_1 \cap aJ|$ for $a \in K_1$. Assume*

(a) $(J, H \cap J, K_0)$ is a Bol loop folder of exponent 2.

(b) $n_0 = 2n_1$.

(c) $|G^+ : H^+| = 6$.

(d) For each $a \in K_1$, $C_{H \cap J}(a) = 1$.

(e) Every involution of L is contained in J.

Then (G, H, K) is a Bol loop folder of exponent 2, and $|K| = 6n_0 = 12n_1$.

Proof. First K_1^+ is the set of transpositions of S_5, so $|K_1^+| = 10$. This implies that n_1 is well defined. Indeed, for $a, b \in K_1$, aJ, bJ are conjugate, hence $K_1 \cap aJ, K_1 \cap bJ$ are conjugate in G. Moreover, $|K_1| = 10n_1$ and by (b),

$$|K| = |K_0| + |K_1| = 2n_1 + 10n_1 = 12n_1 = 6n_0.$$

Next by (a) and (c),

$$|G : H| = |G : HJ||HJ : H| = |G^+ : H^+||J : J \cap H| = 6|K_0| = 6n_0,$$

so $|G : H| = |K|$.

We claim $xy \notin H$ for distinct $x, y \in K$. If so, as $|G : H| = |K|$, K is a set of coset representatives for H in G. Then as K is G-invariant and $K \setminus \{1\}$ consists of involutions, (G, H, K) is a Bol loop folder of exponent 2.

If $x, y \in J$ then $x, y \in K_0$, so $xy \notin H$ by (a). Next $K_1^+ \cap H^+ = \emptyset$, so if $x \in J$ and $y \in K_1$ then $(xy)^+ = y^+ \notin H^+$, so $xy \notin H$. Thus we may take $x, y \in K_1$ and $xy \in H$. Now as K_1^+ is a set of transpositions in S_5, the order of $(xy)^+$ is $1, 2$ or 3. Since $H^+ \cong F_{20}$ has no element of order 3, we get $(xy)^2 \in J$. In particular, $D = \langle x, y \rangle$ is a 2-group. Let z be the unique involution in $\langle xy \rangle$. By $xy \in L$ and (e), $z \in H \cap J$. Moreover, x, y commute with z, which contradicts to (d). □

Remark 4.6. The fact that (e) is necessary can be seen from the counterexample $G = S_5 \ltimes J$.

Theorem 4.7. *Assume G is a group satisfying condition (#) of Lemma 4.3. Let J_0 be the minimal normal subgroup of G and put $K = J_0 \cup c^G$. Define $H = N_G(P)$ where P is a 5-Sylow subgroup of G. Then (G, H, K) is a Bol loop folder determining a simple Bol loop of exponent 2 of order 96. Conversely, if (G, H^*, K^*) is an exponent 2 Bol loop folder then H^* is a conjugate of H and $K^* = K$.*

Proof. With the notation of Proposition 4.5, $K_0 = J_0$ and $K_1 = c^G$. Then $n_0 = 16$, $n_1 = |c^G \cap cJ| = 80/10 = 8$ and $|G^+ : H^+| = 6$, so (b) and (c) hold. (e) follows from Lemma 4.4(ii). Since J is elementary Abelian, $H \cap J$ consists of 1 and the unique involution of H. This involution cannot be centralized by c, otherwise it would be central in $G = \langle c, P, J \rangle$; hence (d). Finally, $H \cap J$ is not contained in J_0, therefore J_0 is a complement to $H \cap J$ in J; showing (a). By Proposition 4.5, (G, H, K) is a Bol loop folder of exponent 2.

For the converse, we observe that (G, H^*, K^*) determines a Bol loop of exponent 2 with all proper subloops solvable. Thus, by the Main Theorem of [Asc05], H^* maps surjectively to F_{20}. By Lemma 4.4(iii), $H^* = H$ or $H^* = HJ_0$ up to conjugaction. In the latter case, the loop has order 6 which is impossible. Again by Aschbacher's result, $c^G \subset K^*$. Finally, if $J_0 \not\subseteq K^*$, then K^* will contain a conjugate of the involution of H, which is not possible. This proves the theorem. □

As the group given in Lemma 4.2 satisfies (#), we have:

Corollary 4.8. *There exists a simple Bol loop of exponent 2 and order 96.* □

Remark 4.9. The Bol loop folder (G, H, K) of Theorem 4.7 was discovered independently by B. Baumeister and A. Stein [BS11] (Free University of Berlin), as well.

4.2. S_5-modules over $\mathbb{F}_2$

In this section we collect some useful facts about kS_5-modules, where k is a field of characteristic 2.

Lemma 4.10. *The group S_5 has three absolutely irreducible representations over $\mathbb{F}_2$: the trivial representation and two representations M, N of dimension 4. The two 4-dimensional modules can be distinguished by the fact that $C_M(x) = 0$ and $\dim_{\mathbb{F}_2}(C_N(x)) = 2$ for an element $x \in S_5$ of order 3. Moreover, the following hold.*

(i) M is the 4-dimensional irreducible component in the 6-dimensional permutation module for $S_5 \cong PGL(2,5)$. Also, let V be the natural 2-dimensional module of $A_5 \cong SL(2,4)$ over the field $\mathbb{F}_4$ and σ be semilinear map of V induced by the Frobenius automorphism of $\mathbb{F}_4$. Then $S_5 \cong SL(2,4) \rtimes \langle\sigma\rangle$ and V is a 4-dimensional S_5-module over $\mathbb{F}_2$. The S_5-modules M and V are isomorphic.

(ii) N is is the 4-dimensional irreducible component in the 5-dimensional permutation module of S_5. Also if N is a 4-dimensional orthogonal space of Witt index 1 over $\mathbb{F}_2$, then $O(N) = O_4^-(2) \cong S_5$. Note that N has 5 singular and 10 nonsingular vectors and these are the S_5-orbits on N.

(iii) N is absolutely irreducible as A_5-module. M is irreducible but not absolutely as an A_5-module, the splitting field being $\mathbb{F}_4$. In particular, the modules are nonisomorphic as A_5-modules.

(iv) N and M are isomorphic absolutely irreducible projective F_{20}-modules.

Proof. Let us first define N, M as irreducible components of the permutation modules. By [Mor80, Table 1], they are absolutely irreducible. As S_5 has 3 classes of elements of odd order, by [Alp86; Alp86, Theorem 3.2] S_5 has no other absolutely irreducible modules over F_2. The properties of N, M can be verified by straightforward calculations, the irreducibility as A_5 and F_{20}-modules follows again from [Mor80, Table 1]. We show $N_{F_{20}} \cong M_{F_{20}}$. As F_{20} has two classes of elements of odd order, F_{20} has two absolutely irreducible modules: the trivial one and $N_{F_{20}}$ coming from the 2-transitive permutation representation. So if $M_{F_{20}}$ were not isomorphic to $N_{F_{20}}$ then it could be brought to upper triangular form over $\bar{\mathbb{F}}_2$, which is clearly impossible.

It remains to show that $N_{F_{20}}$ is projective. Since N_{C_4} is isomorphic to the group algebra $\mathbb{F}_2 C_4$, it is a projective C_4-module by [Alp86, Theorem 4.2]. Using [Alp86, Corollary 9.3], we obtain that N is projective as F_{20}-module. □

We observe that these S_5-modules can immediately be constructed using the Steinberg Tensor Product Theorem [Ste68, Theorem 13.1], as well.

We will now construct an S_5-module U which will play a central role in the generalization of our first construction of a Bol loop of exponent 2.

Let $U = U_1 \oplus U_2$ be the direct sum of two copies of N as an $\mathbb{F}_2 A_5$-module. As U_i is an orthogonal space, we can regard U as an orthogonal space which is the orthogonal direct sum of the two nondegenerate subspaces U_1 and U_2. The stabilizer B of $\{U_1, U_2\}$ in $O(U)$ is $(G_1 \times G_2)\langle\tau\rangle$ where

$$G_i = C_{O(U)}(U_{3-i}) \cong O(U_i) \cong S_5$$

and τ is an involution interchanging U_1, U_2. Thus B is the wreath product of S_5 with C_2. In particular, the elements τ and $(g_1, g_2) \in G_1G_2$ map $u_1 \oplus u_2 \in U$ to

$$(u_1 \oplus u_2)\tau = u_2 \oplus u_1, \text{ and } (u_1 \oplus u_2)(g_1, g_2) = u_1g_1 \oplus u_2g_2,$$

respectively. Set

$$G_0 = C_{G_1G_2}(\tau) = \{(g, g) \mid g \in S_2\} \cong S_5,$$

and let $L = [G_0, G_0] \cong A_5$, t_0 an involution (transposition) in $G_0 \setminus L$, $t = t_0\tau$, and $D = L\langle t\rangle$. Then $t\tau = \tau t$ and the action of t on U is

$$(u_1 \oplus u_2)t = u_2c \oplus u_1c,$$

where $c \in S_5$ is the transposition corresponding to t_0. It is immediate that $D \cong S_5$.

Set $W = C_U(\tau)$. Then W is an $\mathbb{F}_2D$-submodule of U, and also

$$W = [U, \tau] = \{u + u\tau \mid u \in U_1\} = \{u \oplus u \mid u \in N\},$$

with the map $u \mapsto [u, \tau] = u + u\tau$ an $\mathbb{F}_2L$-isomorphism of U_1 with W. If Q is the quadratic form on U then as $Q(u_1 \oplus u_2) = Q(u_1) + Q(u_2)$ and $Q(u) = Q(u\tau)$, $[u, \tau]$ is singular, so W is totally singular.

Lemma 4.11. *With the notation above, we have:*

(i) *U has 3 irreducible L-submodules, namely U_1, U_2 and W.*

(ii) *W is the unique proper D-submodule of U.*

(iii) *Let P be a Sylow 5-subgroup of D, $D_1 = N_D(P)$. Then $D_1 \cong F_{20}$ and U has precisely 3 D_1-submodules W, T_1, T_2.*

(iv) *The orbits of D_1 on T_i have length $1, 5, 10$. In particular, each member of T_i is fixed by some involution of D_1.*

Proof. By Lemma 4.10, N is projective as F_{20}-module. Since U/W is a 4-dimensional irreducible for D_1, U_{D_1} splits over $W_{D_1} \cong N_{D_1}$ and hence $U = W \oplus T_1$ with D_1-submodule T_1. Again by Lemma 4.10, N_L and N_{D_1} are completely irreducible, Schur's lemma then implies $\mathrm{End}_{\mathbb{F}_2L}(N) = \mathrm{End}_{\mathbb{F}_2D_1}(N) = \mathbb{F}_2$. We can now apply [Asc86, (27.14)] to obtain (i) and (iii). (ii) follows from (i). Finally, (iv) holds since T_i and W are D_1-isomorphic and W is the permutation module modulo the center. □

In the next lemma, we keep using the above notation.

Lemma 4.12. *(i)* $\dim C_U(t) = 4$, *$C_U(t) + T_1 = U$ and $C_U(t) \cap T_1 = 0$.*

(ii) *Under the action of A_5 on the submodules W, U_1, U_2 of U, the lengths of the orbits are $1, 5, 10$. Let S_0, S_1, S_2 be the orbits of length 5 in W, U_1, U_2, respectively. Then $S = \{0\} \cup S_0 \cup S_1 \cup S_2$ is a (nonlinear) S_5-invariant complement to T_1 in U, that is, $S + T_1 = U$.*

Proof. (i) We have $D = L\langle t\rangle \cong S_5$. Let us denote the element of S_5 corresponding to $a \in D$ by a^+, w.l.o.g. we can assume $t^+ = (12)$ and $P^+ = \langle(12345)\rangle$. Then $D_1^+ = \langle(12345), (1325)\rangle$. Let $b \in D$ such that $b^+ = (12)(35)$. Then $b \in D_1$ and b commutes with t and τ. Record that the action of b, t, τ on U is

$$\begin{aligned} b &: u_1 \oplus u_2 \mapsto u_1 b^+ \oplus u_2 b^+, \\ \tau &: u_1 \oplus u_2 \mapsto u_2 \oplus u_1, \\ t &: u_1 \oplus u_2 \mapsto u_2 t^+ \oplus u_1 t^+. \end{aligned}$$

Define the element $\tilde{c} \in B$ by

$$\tilde{c} : u_1 \oplus u_2 \mapsto u_1 t^+ \oplus u_2.$$

Then $\tilde{c}$ commutes with b and $\tau^{\tilde{c}} = t$. Put $E_1 = \langle t, b\rangle$, clearly $E_1^{\tilde{c}} = \langle \tau, b\rangle$. On the one hand, we have

$$\begin{aligned} \dim_{\mathbb{F}_2}(C_U(E_1)) &= \dim(C_U(\tau, b)) \\ &= \dim C_{C_U(b)}(\tau) \\ &= \dim C_{C_{U_1}(b)\oplus C_{U_2}(b)}(\tau) \\ &= \dim C_{U_1}(b) \\ &= \dim C_N(b^+) = 2. \end{aligned}$$

We show on the other hand that $\dim_{\mathbb{F}_2}(C_W(E_1)) \geq 2$. Indeed, the S_5-modules W and N are isomorphic and $\dim(C_W(t)) = \dim(C_N(t^+)) = 3$. Then $C_W(E_1) = C_{C_W(t)}(b)$ is of rank at least $\dim(C_W(t))/2 = 3/2$.

Now, from $\dim(C_W(E_1)) \geq 2$ follows $C_U(E_1) \leq W$. However if $C_{T_1}(t) \neq 0$ then $C_{T_1}(E_1) \neq 0$, contradicting $T_1 \cap W = 0$ and $C_U(E_1) \leq W$.

(ii) We have seen that S_i is the set of singular points in U_i for $i = 1, 2$. The action of $D_1 \cong F_{20}$ on S_i is its natural 2-transitive action on 5 points. $D_1 \cap L$ contains precisely 5 involutions and each member of S_i is fixed by exactly one involution of $D_1 \cap L$. Moreover, each member of T_1 is fixed by some involution of D_1.

We have to show that for distinct $x, y \in S$, $x + y \notin T_1$; then S is a complement to T_1 by an order argument. Assume $x + y \in T_1$ and denote by a an involution of D_1 fixing $x + y$. Then x, y are the projections of $x + y$ on S_i, S_j, so a fixes the projections x and y. As $T_1 \cap U_i = 0$ for $0 \leq i \leq 2$, $x \in S_i$ and $y \in S_j$ for some $i \neq j$. If $x \in S_1$ and $y \in S_2$, then x and y are the unique fixed points of a in S_1, S_2. By $a\tau = \tau a$, $x\tau = y$ holds, and hence $x + y = [x, \tau] \in W$, contradicting $T_1 \cap W = 0$.

Thus we may take $x \in S_0$ and $y \in S_1$. Then $x = x_1 + x_2$ with $x_i = S_i$, and as $x \in S_0$, $x_2 = x_1\tau$ with $x_i \in S_i$. Now, x_i is the unique fixed point of a in S_i and y the unique fixed point of a in S_1, so $y = x_1$ and $x + y = x_1 + x_2 + y = x_2 \in T_1 \cap U_2 = 0$, a contradiction. □

4.3. An infinite family of simple Bol loops of exponent 2

In this section, G denotes a group satisfying condition (#) of Lemma 4.3, H is the normalizer of a 5-Sylow P of G, c an involution from $G \setminus [G,G]J$. The S_5-modules N and U are defined as in Section 4.2. Also $U = U_1 \oplus U_2 = T_1 \oplus T_2$ where U_1, U_2 are A_5-submodules, and T_1, T_2 are F_{20}-submodules. Moreover, U_1, U_2, T_1, T_2 are different from the unique S_5-submodule W of U. All these subspaces are irreducible $\mathbb{F}_2P$-modules, which implies $U_i \cap T_j = 0$.

Let us fix a positive integer k and put

$$\mathscr{U} = U^k,\ \mathscr{U}_i = U_i^k,\ \mathscr{T}_i = T_i^k,\ \mathscr{W} = W^k.$$

Clearly, $\mathscr{W}$ is a S_5-submodule and $\mathscr{U} = \mathscr{U}_1 \oplus \mathscr{U}_2 = \mathscr{T}_1 \oplus \mathscr{T}_2$. We write $\mathscr{G} = G \ltimes \mathscr{U}$ where $J \lhd G$ acts trivially on the S_5-module $\mathscr{U}$. Moreover,

$$\mathscr{J} = O_2(\mathscr{G}) = \langle J, \mathscr{U} \rangle.$$

We will consider the elementary Abelian subgroup $\mathscr{J}$ of $\mathscr{G}$ as an S_5-module over the field $\mathbb{F}_2$. In particular, with some abuse of notation, we will denote the group operation on $\mathscr{J}$ additively and write $\mathscr{J} = J + \mathscr{U}$, etc. It is easy to see that

$$\mathscr{G}/\mathscr{J} \cong S_5 \text{ and } \operatorname{soc}(\mathscr{G}) = J_0 + \mathscr{W}.$$

Moreover, since J_0 and W are non-isomorphic S_5-modules, $J_0 \oplus W$ does not contain diagonal submodules. This implies that for any minimal submodule M of $\mathscr{J}$, we either have $M = J_0$ or $M \leq \mathscr{W}$.

The action of the involution $c \in G \setminus J$ on $\mathscr{U}$ equals the action of the transposition $(12) \in S_5$, hence c interchanges $\mathscr{U}_1, \mathscr{U}_2$. This implies $|C_{\mathscr{U}}(c)| = 16^k$ and $|c^{\mathscr{U}}| = 16^k$; that is, $\mathscr{U}$ is transitive on the involutions in $c\mathscr{U}$. As $G \cong \mathscr{G}/\mathscr{U}$ is transitive on the 80 involutions in $G \setminus J$, and as $\mathscr{U}$ is transitive on the 16^k involutions on $c\mathscr{U}$, $\mathscr{G}$ is transitive on the $80 \cdot 16^k$ involutions in $\mathscr{G} \setminus \mathscr{J}$.

Using Aschbacher's Main Theorem [Asc05] we conclude that a Bol loop folder $(\mathscr{G}, \mathscr{H}, \mathscr{K})$ must have the following properties: The index of $\mathscr{H}$ has to be $96 \cdot 16^k$, that is, $\mathscr{H}$ must have order $40 \cdot 16^k$. The set of involutions $\mathscr{K}$ is the union of $c^{\mathscr{G}}$ and $\mathscr{K} \cap \mathscr{J}$, thus, $|\mathscr{K} \cap \mathscr{J}| = 16 \cdot 16^k$.

There are very many possible choices for $\mathscr{H}$ and $\mathscr{K}$.The most obvious choice is the following.

Proposition 4.13. *Put $\mathscr{H} = H \ltimes \mathscr{T}_1$ and $\mathscr{K} = c^{\mathscr{G}} \cup (J_0 \oplus \mathscr{W})$. Then $(\mathscr{G}, \mathscr{H}, \mathscr{K})$ is a Bol loop folder. Moreover, the homomorphism $\mathscr{G} \to G$ with kernel $\mathscr{U}$ induces a surjective homomorphism between the loop folders $(\mathscr{G}, \mathscr{H}, \mathscr{K})$ and (G, H, K). In other words, the Bol loop corresponding to $(\mathscr{G}, \mathscr{H}, \mathscr{K})$ is an extension of the elementary Abelian group of order 2^{2k} by the loop corresponding to (G, H, K).*

Proof. We apply Proposition 4.5, (a), (c) and (e) are trivial. (b) follows from

$$n_1 = |c^{\mathscr{G}} \cap c\mathscr{J}| = |C_{\mathscr{J}}(c)| = 8|C_{\mathscr{U}}(c)| = 8 \cdot 16^k$$

and $n_0 = |J_0||\mathscr{W}| = 16 \cdot 16^k = 2n_1$. For (d), we use

$$C_{\mathscr{H}\cap\mathscr{J}}(c) = C_{H\cap J+\mathscr{T}_1}(c) = C_{H\cap J}(c) = 1,$$

as by Lemma 4.12, $\mathscr{T}_1 \cap \mathscr{T}_1^c = 0$. □

In the rest of this section, for each integer $k \geq 1$, we modify these $\mathscr{H}$ and $\mathscr{K}$ such that the resulting loop will be simple. Let U^* be a copy of U in $\mathscr{U}$ such that $\mathscr{U} = U^* \oplus U^{k-1}$. We denote the subspaces corresponding to T_i, U_i, W by T_i^*, U_i^*, W^*. Let us define the set $S \subseteq U$ as in Lemma 4.12(ii) and let S^* be the corresponding subset of U^*. In order to construct the new $\mathscr{K}$, we simply replace W^* by S^*.

Let $\psi : J_0 \to T_1^*$ be an isomorphism of F_{20}-modules and define

$$\mathscr{T}_\psi = \{v + \psi(v) + u \mid v \in J_0, u \in T_1^{k-1}\}.$$

Then $\mathscr{T}_\psi$ is normalized by H and we define the new subgroup $\mathscr{H}$ of $\mathscr{G}$ by $\mathscr{H} = H \ltimes \mathscr{T}_\psi$.

Theorem 4.14. *Let $\mathscr{H} = H \ltimes \mathscr{T}_\psi$, $\widetilde{\mathscr{W}} = (\mathscr{W} \setminus W^*) \cup S^*$ and $\mathscr{K} = c^{\mathscr{G}} \cup (J_0 + \widetilde{\mathscr{W}})$. Then the triple $(\mathscr{G}, \mathscr{H}, \mathscr{K})$ is a Bol loop folder such that the corresponding Bol loop is simple of exponent 2.*

Proof. Again, the first statement follows from Proposition 4.5 and Lemma 4.12; one needs to verify hypothesis (a) and (d) of the Proposition only. Again (d) follows from $T_1 \cap T_1^c = 0$.

We prove (a) by showing that $\mathscr{K}_0 = \mathscr{K} \cap \mathscr{H}\,\mathscr{J}$ is a transversal to $\mathscr{H}$ in $\mathscr{H}\,\mathscr{J}$. Since $\mathscr{K}_0 \subset \mathscr{J}$, this is equivalent with the fact that $\mathscr{K}_0 = J_0 + \widetilde{\mathscr{W}}$ is a complement of the subspace

$$\mathscr{H} \cap \mathscr{J} = H \cap J + \mathscr{T}_\psi$$

in $\mathscr{J}$, *i.e.*

$$\mathscr{K}_0 + \mathscr{H} \cap \mathscr{J} = \mathscr{J}.$$

In order to show this, we use the identities

$$\begin{aligned} \mathscr{W} + \mathscr{T}_1 &= \mathscr{U}, \\ J_0 + \mathscr{T}_\psi &= J_0 + \mathscr{T}_1, \\ J_0 + \mathscr{H} \cap \mathscr{J} &= J_0 + H \cap J + \mathscr{T}_\psi \\ &= J_0 + H \cap J + \mathscr{T}_1. \end{aligned}$$

Then

$$\begin{aligned} J_0 + \mathscr{W} + \mathscr{H} \cap \mathscr{J} &= J_0 + \mathscr{W} + H \cap J + \mathscr{T}_\psi \\ &= J_0 + \mathscr{W} + H \cap J + \mathscr{T}_1 \\ &= J_0 + \mathscr{U} + H \cap J \\ &= J + \mathscr{U} \\ &= \mathscr{J}, \end{aligned}$$

that is, $J_0 + \mathscr{W}$ is a complement to $\mathscr{H} \cap \mathscr{J}$ in $\mathscr{J}$ by the order argument $|J_0 + \mathscr{W}||\mathscr{H} \cap \mathscr{J}| = |\mathscr{J}|$.

We constructed $\widetilde{\mathscr{W}}$ from $\mathscr{W}$ by deleting the minimal submodule W^* and replacing it by S^*. Therefore, it is enough to show that this deformations of $\mathscr{W}$ do not change the property of being a complement.

$$\begin{aligned} J_0 + W^* + \mathscr{H} \cap \mathscr{J} &= J_0 + W^* + H \cap J + \mathscr{T}_\psi \\ &= H \cap J + J_0 + W^* + \mathscr{T}_1 \\ &= H \cap J + J_0 + W^* + T_1^* + \mathscr{T}_1 \\ &= H \cap J + J_0 + S^* + T_1^* + \mathscr{T}_1 \\ &= J_0 + S^* + H \cap J + \mathscr{T}_\psi \\ &= J_0 + S^* + \mathscr{H} \cap \mathscr{J} \end{aligned}$$

This proves (a), hence $(\mathscr{G}, \mathscr{H}, \mathscr{K})$ is a Bol loop folder.

It remains to show that the Bol loop $\mathscr{Q}$ corresponding to $(\mathscr{G}, \mathscr{H}, \mathscr{K})$ is simple. Let us therefore assume that $\mathscr{Q} \to \mathscr{Q}^\sharp$ is a nontrivial surjective loop homomorphism and let $(\mathscr{G}^\sharp, \mathscr{H}^\sharp, \mathscr{K}^\sharp)$ be the loop folder of $\mathscr{Q}^\sharp$. Then we have a surjective homomorphism $\alpha : \mathscr{G} \to \mathscr{G}^\sharp$ with $\alpha(\mathscr{H}) = \mathscr{H}^\sharp$ and $\alpha(\mathscr{K}) = \mathscr{K}^\sharp$. Let $\mathscr{N} = \ker \alpha$ and $c^\sharp = \alpha(c) = c\mathscr{N}$. On the one hand, $\mathscr{H}^\sharp$ is core-free, thus,

$$\mathrm{core}_{\mathscr{G}}(\mathscr{H}\mathscr{N}) = \mathscr{N}. \tag{4.2}$$

On the other hand, $\mathscr{N} \leq \mathscr{J}$ since otherwise $\mathscr{H}\mathscr{N} = \mathscr{G}$ and $\mathscr{Q}^\sharp = 1$.

Let us first assume that $J_0 \leq \mathscr{N}$. Since

$$J/J_0 \leq Z(\mathscr{G}/J_0) \lhd \mathscr{G}/J_0 \text{ and } J/J_0 \leq \mathscr{H}\mathscr{N}/J_0,$$

we have $J \leq \mathscr{N}$ by (4.2). In this case the image $G^\sharp$ of $G \leq \mathscr{G}$ is a homomorphic image of $G/J \cong S_5$. Furthermore, if $[c^\sharp, c^{\sharp g}] = 1$ then $c^\sharp c^{\sharp g}$ normalizes a Sylow 5-subgroup of $G^\sharp$, thus, $c^\sharp c^{\sharp g}$ is contained in a conjugate of $\mathscr{H}^\sharp$, and hence $c^\sharp = c^{\sharp g}$ in this case. As the commuting graph of transpositions in S_5 is connected, $c^\sharp = c^{\sharp g}$ for all g. This means $[c, \mathscr{G}] \leq \mathscr{N}$, contradicting to $\mathscr{N} \leq \mathscr{J}$.

Let us now assume $J_0 \not\leq \mathscr{M}$ and let M be a minimal normal subgroup of $\mathscr{G}$ contained in $\mathscr{N}$. Then $M \leq \mathrm{soc}(\mathscr{G}) = J_0 + \mathscr{W}$. Since J_0 and W are non-isomorphic S_5-modules, $J_0 + \mathscr{W}$ contains no submodules isomorphic to J_0 and different from J_0. This implies $M \leq \mathscr{W}$ and, in particular, $\mathscr{N} \cap \mathscr{W} \neq 0$.

Let us take an element $s \in S^* \setminus W^* \subseteq \mathscr{K}$. As W^* and T_0^* are complements in U^*, $s \neq 0$ has the unique decomposition $s = w + t$ with $0 \neq w \in W^*$ and $0 \neq t \in T_1^*$. Furthermore, for $0 \neq j = \psi^{-1}(t) \in J_0$, $j + t \in \mathscr{T}_\psi \leq \mathscr{H}$ holds. We claim that $j + t \in \mathscr{N}$. Indeed, we have the decomposition

$$w = (s + j) + (j + t), \qquad s + j \in \mathscr{K}, j + t \in \mathscr{H}.$$

If $\mathscr{N} \leq U^*$ then $M = W^*$ and $\alpha(s + j) = \alpha(j + t) \in \mathscr{K}^\sharp \cap \mathscr{H}^\sharp = 1$. In particular, $j+t \in \mathscr{N}$. If $\mathscr{N} \not\leq U^*$ then for an arbitrary element $n \in (\mathscr{N} \cap \mathscr{W}) \setminus U^*$, $w+n \in \mathscr{K}$. This means that the element $\alpha(w)$ has two $\mathscr{H}^\sharp\mathscr{K}^\sharp$ decompositions:

$$\alpha(w) = \alpha(w + n) + 0 = \alpha(s + j) + \alpha(j + t).$$

This is only possible if $j + t \in \mathscr{N}$, thus our claim is proved.

Let M' be the S_5-submodule generated by $j + t$, then $J_0 \leq M' \leq \mathscr{N}$ as the irreducible J_0 is not S_5-isomorphic to a submodule of U^*. This contradiction proves the simplicity of $\mathscr{Q}$. □

Remark 4.15. We have seen that there are at least two possibilities for the choice of $\mathscr{H}$. Also in $\widetilde{\mathscr{W}}$, we can replace any minimal submodule W^{**} by an appropriate S^{**}. This shows that there are *many* Bol loops of exponent 2 which live in the same non-solvable group. Many of these loops are simple. Using computer calculations, we were able to construct over 30 nonisomorphic simple Bol loops of exponent 2 in $\mathscr{G}$ in the case $k = 1$.

In fact, this phenomena in not unusual for Bol loops of exponent 2. In [KN02, Section 5] and [Nag06, Theorem 5.5], the authors constructed rich classes of Bol loops of exponent 2 having the same enveloping groups, namely the wreath product $C_2^n \wr C_2$ and the extraspecial 2-group $E^+_{2^{2n+1}}$, respectively. In these cases, a simple parametrization of the conjugacy classes of involutions enabled a description of the associated loops. Unfortunately, the group $\mathscr{G}$ has many conjugacy classes of involutions and these classes have no nice algebraic parametrization. Therefore, we see no way of classifying all simple Bol loops with enveloping group $\mathscr{G}$.

The above remark lets us make another observation. While the class of finite Bol loops of exponent 2 is very rich, the structure of the right multiplication group of a Bol loop of exponent 2 is rather restricted. Differently speaking, while the classification of finite simple Bol loops of exponent 2 seems to be hopeless, we think that the classification of right multiplication groups of such loops could be a meaningful project.

We finish this chapter with the following

Problem 4.16. *Classify those almost simple groups T for which an exponent 2 Bol loop folder (G, H, K) exists such that $T \cong G/O_2(G)$.*

dc_821_13

5. Three results on finite simple Bol loops

At the LOOPS'07 conference in Prague, the author of this dissertation received the following questions on simple Bol loops.

Question 5.1 (A. Greil, München). *Let Q_2 be the 2-dimensional simple Bruck loop defined on the hyperbolic plane and let Q_3 be the 3-dimension simple Bol G-loop obtained by the exact factorization of $PSL_2(\mathbb{R})$. Is Q_2 isomorphic to a subloop of Q_3?*

Question 5.2 (V. Shcherbacov, Chişinău). *Let Q be a finite Bol loop which admits a fixed-point-free automorphism of prime order. Is then Q solvable?*

Question 5.3 (H. Kiechle, Hamburg). *Are there finite non-associative Bol loops with transitive automorphism groups?*

It turns out that all questions have negative answers. Question 3 was recently answered by M. Aschbacher [Asc06, Theorem 1]. Aschbacher's proof is almost purely group theoretical, and uses many deep results from the theory of finite groups including the classification of finite 2-transitive groups. In this chapter, we will present a new proof for the non-existence of finite Bol loops with transitive automorphism group. This proof is of combinatorial nature, it uses a deep classification theorem [CK93, Theorem 1 and 3] of P. J. Cameron and G. Korchmáros concerening 1-factorizations of complete graphs with a doubly transitive automorphism group. Of course, the Cameron-Korchmáros proof also relays on the classification of finite 2-transitive groups. The possibility of the combinatorial argument was first pointed out in [Nag01].

We finish this chapter with a few open problems which are related to simple Bol loops. The content of this chapter is included in [Nag08b]. Theorem 5.7 supports the second claim in **Thesis 2.**

5.1. 2-dimensional subloops and exact factorizations

The hyperbolic plane loop (1.4) can be given by the loop folder (G_2, H_2, K_2), where

$$\begin{aligned} G_2 &= PSL_2(\mathbb{R}), \\ H_2 &= \left\{ \pm \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix} \mid t \in \mathbb{R} \right\}, \\ K_2 &= \left\{ \pm \begin{pmatrix} a & b \\ b & c \end{pmatrix} \mid a > 0, ac - b^2 = 1 \right\}. \end{aligned}$$

Observe that K_2 is given by positive definite symmetric matrices. The polar decomposition of real matrices implies that K_2 is a system of right coset representatives of H_2 in G_2 with $aba \in K_2$ for $a, b \in K_2$. The triple (G_2, H_2, K_2) is a Bol loop folder; we will denote the associated Bol loop by Q_2. Clearly, the loop folder (G_2, H_2, K_2) is faithful.

Let M be a proper subgroup of $PSL_2(\mathbb{R})$ containing H_2. Since the 2-dimensional subgroups of $PSL_2(\mathbb{R})$ are the Borel subgroups and H_2 is not contained in any Borel subgroup, $\dim(M) = 1$ and H_2 is the connected component of M. Moreover, straightforward calculation shows that $N_{G_2}(H_2) = H_2$. Therefore $M = H_2$ is a maximal subgroup of $G_2 = PSL_2(\mathbb{R})$.

Lemma 5.4. *Let (G_0, H_0, K_0) be a Bol loop folder such that $G_0 = \langle K_0 \rangle$ and let us assume that the associated Bol loop is isomorphic to the 2-dimensional hyperbolic loop Q_2. Then H_0 is a maximal subgroup of G_0.*

Proof. As the loop folder (G_2, H_2, K_2) of Q_2 is faithful, we have a surjective homomorphism $G_0 \to G_2$ mapping H_0 to H_2. The kernel $\mathrm{core}_{G_0}(H_0)$ of this homomorphism is contained in H_0. Since H_2 is maximal in G_2, the lemma follows. □

Let $\tau = (G, A, B)$ be an exact factorization triple and define

$$\left\{ \begin{array}{lcl} \mathcal{G} &=& G \times G, \\ \mathcal{H} &=& A \times B, \\ K &=& \{(x, x^{-1}) \mid x \in G\}. \end{array} \right. \tag{5.1}$$

Let Q be the corresponding Bol loop. Then, the underlying set of Q can be naturally identified with the underlying set of the group G. In particular, if G, A, B are Lie groups then Q is a differentiable loop and $\dim(Q) = \dim(G)$.

Lemma 5.5. *Let (G, A, B) be an exact factorization triple and define the loop folder $(\mathcal{G}, \mathcal{H}, K)$ and the loop Q as in* (5.1). *Put $A^* = A \times G$, $B^* = G \times B$ and $K_A = A^* \cap K$, $K_B = B^* \cap K$. Then,*

$$(A^*, \mathcal{H}, K_A) \text{ and } (B^*, \mathcal{H}, K_B)$$

are subloop folders of $(\mathcal{G}, \mathcal{H}, K)$ and the associated subloops are isomorphic to A and B, respectively.

Proof. Let us first observe that

$$K_A = \{(b, b^{-1}) \mid b \in A\}$$

and that (G, B, A) is a Bol loop folder corresponding to the group A. Define the projections $\pi_i : \mathcal{G} = G \times G \to G$. Then π_2 maps A^* to G, $\mathcal{H}$ to B and K_A to A, that is, π_2 induces a homomorphism between the loop folders

$$(A^*, \mathcal{H}, K_A) \text{ and } (G, B, A).$$

Moreover, $\ker \pi_2 \cap A^* = A \times 1 \leq \mathcal{H}$, hence $(A^*, \mathcal{H}, K_A)$ and (G, B, A) determine the same loop. Finally, (G, B, A) and $(\langle A \rangle, A \cap B, A) = (A, 1, A)$ determine the same loop again, which is isomorphic to the group A. Similar argument proves that the subloop corresponding to the loop folder $(B^*, \mathcal{H}, K_B)$ is isomorphic to B. □

Let us now put $G = PSL_2(\mathbb{R})$,

$$\begin{aligned} A &= \left\{ \pm \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix} \mid t \in \mathbb{R} \right\}, \\ B &= \left\{ \pm \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{R} \setminus \{0\}, b \in \mathbb{R} \right\} \end{aligned}$$

of G. Let $(\mathcal{G}_3, \mathcal{H}_3, K_3)$ be the Bol loop folder defined by (5.1) and let us denote by Q_3 the associated simple differentiable Bol G-loop; $\dim(Q_3) = 3$. As the loop folder $(\mathcal{G}_3, \mathcal{H}_3, K_3)$ is faithful we can identify $\mathcal{G}_3, \mathcal{H}_3$ and K_3 with $\mathrm{RMlt}(Q_3), \mathrm{RInn}(Q_3)$ and $\mathrm{RSec}(Q_3)$, respectively.

Theorem 5.6. *The 3-dimensional simple Bol G-loop Q_3 has no subloop isomorphic to the 2-dimensional hyperbolic loop Q_2.*

Proof. Let us assume that the subloop $\tilde{Q} \leq Q_3$ is isomorphic to Q_2 and define the set

$$\tilde{K} = \{R_x \mid x \in \tilde{Q}\}$$

of right multiplication maps corresponding to the elements of $\tilde{Q}$. Put $\tilde{\mathcal{G}} = \langle \tilde{K} \rangle$ and $\tilde{\mathcal{H}} = \tilde{\mathcal{G}} \cap \mathcal{H}_3$, then $(\tilde{\mathcal{G}}, \tilde{\mathcal{H}}, \tilde{K})$ is a loop folder for $\tilde{Q}$ satisfying $\tilde{\mathcal{G}} = \langle \tilde{K} \rangle$. By Lemma 5.4, $\tilde{\mathcal{H}}$ is a maximal subgroup in $\tilde{\mathcal{G}}$.

Define the subgroups

$$M = \{(a, c) \mid a \in G, c \in B\} \text{ and } \tilde{M} = \tilde{\mathcal{G}} \cap M$$

of $\mathcal{G}_3$. Since $M \cong G \times B$, $\dim(M) = 5$ and $\dim(\tilde{M}) \geq \dim(\tilde{\mathcal{G}}) - 1$. However, $\mathcal{H}_3 \leq M$ implies $\tilde{\mathcal{H}} \leq \tilde{M}$. As $\dim(\tilde{\mathcal{H}}) = \dim(\tilde{\mathcal{G}}) - 2$, we obtain that $\tilde{M}$ contains $\tilde{\mathcal{H}}$ properly. This is only possible if $\tilde{M} = \tilde{\mathcal{G}}$, that is, $\tilde{\mathcal{G}} \leq M$.

By Lemma 5.5, $(M, \mathcal{H}_3, M \cap K_3)$ is a subloop folder and the corresponding subloop is isomorphic to the group B. As $\tilde{Q}$ is not isomorphic to a subgroup of B, we obtained a contradiction. □

5.2. Finite simple Bol loops with fixed-point-free automorphisms

By Thompson's famous result [Tho59, Theorem 1], finite groups with fixed-point-free automorphisms of prime order are nilpotent. This motivated Victor Shcherbacov's Question 5.2; the answer relays on the smallest simple Bol loop of exponent 2.

Theorem 5.7. *Let us define G, H, K as in Theorem 4.7 and let Q be the simple Bol loop corresponding to the loop folder (G, H, K). Let a be an element of order 5 in H and let us denote by α the inner automorphism of G induced by a. Then $H^\alpha = H$ and $K^\alpha = K$, thus, α induces an automorphism $\tilde{\alpha}$ of Q. The order of $\tilde{\alpha}$ is 5 and it has no fixed point in $Q \setminus \{1\}$.*

Proof. As K is invariant under conjugation in G, α acts on K. Clearly, $H^\alpha = H$, thus, $\tilde{\alpha}$ is well defined. The action of $\tilde{\alpha}$ is equivalent with the action of α on K. It is therefore enough to show that a does not centralize any element of $K \setminus \{1\}$. However, if $y \in K \cap C_G(a)$ then $y \in H = N_G(\langle a \rangle)$ which implies $y = 1 = K \cap H$. □

5.3. A new proof on finite Bol loops with transitive automorphism group

In this section, we give a new proof for the non-existence of finite Bol loops with transitive automorphism groups. The hard part of the proof is when the loop has exponent 2. We relate this case to 1-factorization of complete graphs and apply deep results of P. J. Cameron and G. Korchmáros [CK93, Theorem 1 and 3] on the automorphism groups of 1-factorizations.

Let Q denote a finite Bol loop such that $\mathrm{Aut}(Q)$ acts transitively on $Q^\sharp = Q \setminus \{1\}$. It is well known that Bol loops are power-associative. Therefore, the orders of elements are well defined and in the case of a finite Bol loop, the orders divide the order of the loop. In particular, each element of $Q^\sharp$ has order p for some prime p. Let us first consider the case when p is odd.

The next lemma is rather *folklore,* as well. It is more general and can be useful in other context, too.

Lemma 5.8. *Let Q be a finite right Bol loop in which every non-trivial element has order p for some odd prime p. Then $\mathrm{RMlt}(Q)$ is a p-group and Q is solvable.*

Proof. Let G be the subgroup of $\mathrm{RMlt}(Q) \times \mathrm{RMlt}(Q)$ which is defined by the set

$$\{(R_x, R_x^{-1}) \mid x \in Q\}.$$

Due to the right inverse property of Q, the map $\sigma : (x, y) \mapsto (y, x)$ leaves G invariant, hence $\sigma \in \mathrm{Aut}(G)$. We consider σ as an element of the semidirect product

$G \ltimes \langle\sigma\rangle$ and claim that the conjugacy class σ^G consists of the elements $\sigma^{(R_x, R_x^{-1})}$. Indeed, using

$$\sigma^{(R_x, R_x^{-1})} = \sigma(R_{x^2}, R_{x^2}^{-1}), \tag{5.2}$$

one can show by a somewhat tedious calculation that

$$\sigma^{(R_x, R_x^{-1})(R_y, R_y^{-1})} = \sigma^{(R_z, R_z^{-1})}$$

holds with $z = ((yx^2)y)^{\frac{1}{2}}$. Notice that $x \mapsto x^{\frac{1}{2}}$ is well defined since every element has odd order.

As the orders of the elements x, R_x and $(R_{x^2}, R_{x^2}^{-1})$ are the same odd prime p, we see that the product of two conjugates of σ has always odd order p. By [Fis64, Satz 4.1], the order of G is a power of p. This implies $\mathrm{RMlt}(Q)$ to be a p-group since it is a homomorphic image of the G. We still have to show that Q is solvable. As $\mathrm{RMlt}(Q)$ is nilpotent, the right inner mapping group of Q is contained in a normal subgroup N of $\mathrm{RMlt}(Q)$. It is straightforward to show that the map

$$Q \to \mathrm{RMlt}(Q)/N, \qquad x \mapsto R_x N$$

is a surjective homomorphism from Q to the p-group $\mathrm{RMlt}(Q)/N$. Since the latter is solvable, Q is solvable as well. □

Remark 5.9. The above lemma holds also for right Bol loops in which the orders of the elements are powers of p; the proof can be used without any change. It was open for a long time if the solvability of Q can be strengthened to nilpotence. The fact that this is not possible was shown by T. Foguel and M. Kinyon [FK10] who constructed a right Bol loop of order 27 and exponent 3 with trivial center.

We can now come to the case of Bol loops of odd order with transitive automorphism groups.

Lemma 5.10. *Let Q be a finite right Bol loop with a transitive automorphism group. Assume that every element of Q has order p with odd prime p. Then Q is an elementary abelian p-group.*

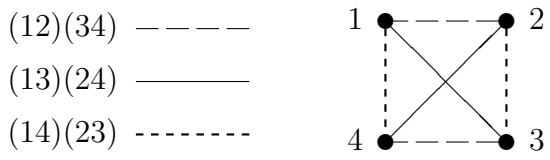
Proof. Let Q' denote the commutator-associator subloop of Q. By Lemma 5.8, Q' is properly contained in Q and $Q \setminus Q' \neq \emptyset$. As Q' is a characteristic normal subloop of Q, we obtain that all non-trivial elements are in $Q \setminus Q'$, thus $Q' = 1$. Hence, Q is an abelian group in which every element have the same order. This proves the lemma. □

Let us now turn to the much harder case when Q consists of elements of order 2. For this, we need the concept of 1-factorization of graphs. (Which is also called a minimal edge coloring.)

Definition 5.11. *Let $\Gamma = (V, E)$ be a finite simple graph. A subset $F \subseteq E$ of edges of Γ is a 1-factor if for any $v \in V$ there is a unique edge $e \in F$ containing v. A 1-factorization of Γ is a partition of the set E of edges into 1-factors $F_1, \ldots, F_k$.*

It is easy to see that the 1-factors of Γ correspond to the involutorial permutations of the set V of vertices. Let n be a positive even integer, put $V = \{1, \dots, n\}$ and denote by K_n the complete graph on V. Let $\mathscr{F} = \{F_1, \dots, F_{n-1}\}$ be a 1-factorization K_n. Let $U_{\mathcal{F}}$ be the set consisting of id_V and the involutorial permutations $u_1, \dots, u_{n-1}$ corresponding to the 1-factors $F_1, \dots, F_{n-1}$, respectively. Then U is a *sharply transitive set* on V, that is, for each $x, y \in V$, there is a unique element $u \in U$ with $x^u = y$.

Conversely, let $U = \{\mathrm{id}_V, u_1, \dots, u_{n-1}\}$ be a sharply transitive set on $V = \{1, \dots, n\}$ such that $u_i^2 = \mathrm{id}_V$ for each $i = 1, \dots, n-1$. Then, the corresponding 1-factors determine a 1-factorization of K_n. The following picture illustrates the correspondence between the 1-factorization of the complete graph K_4 and the involutions of the elementary abelian group of order 4.



The next lemma explains the relationship between Bol loops of exponent 2 and 1-factorizations of the complete graphs.

Lemma 5.12. *Let Q be a finite Bol loop of exponent 2 such that $\mathrm{Aut}(Q)$ acts transitively on $Q^\sharp = Q \setminus \{1\}$. Then the set of right multiplication maps of Q determines a 1-factorization $\mathscr{F}$ of the complete graph K_n with $n = |Q|$. Moreover, the automorphism group of $\mathscr{F}$ acts doubly transitively on the vertices of K_n.*

Proof. Clearly, the set of right multiplication maps of Q consists of involutions and forms a sharply transitive set on Q. Let us identify the elements of Q and the vertices of the complete graph K_n. The 1-factor can be indexed with the elements of $Q^\sharp$: For $x \in Q^\sharp$, the 1-factors F_x consists of the edges $\{y, yx\}$, $y \in Q$.

Let us take an arbitrary element $a \in Q$, then

$$\begin{aligned} F_x^{R_a} &= \{\{y, yx\} \mid y \in Q\}^{R_a} \\ &= \{\{ya, (yx)a\} \mid y \in Q\} \\ &= \{\{ya, (((ya)a)x)a = (ya)((ax)a)\} \mid y \in Q\} \\ &= F_{(ax)a}. \end{aligned}$$

Thus, every right multiplication map R_a is an automorphism of $\mathscr{F}$. Similarly, one shows that for any $\alpha \in \mathrm{Aut}(Q)$, $F_x^\alpha = F_{x^\alpha}$ holds. This implies

$$\mathrm{RMlt}(Q), \mathrm{Aut}(Q) \leq \mathrm{Aut}(\mathscr{F}).$$

Let G be the subgroup of $\mathrm{Sym}(Q)$ generated by $\mathrm{RMlt}(Q)$ and $\mathrm{Aut}(Q)$; clearly G is transitive on Q and $G \leq \mathrm{Aut}(\mathscr{F})$. Moreover, the stabilizer G_1 of 1 contains $\mathrm{Aut}(Q)$, hence G is doubly transitive on Q. □

We are now able to proof our theorem.

Theorem 5.13. *Let Q be a finite right Bol loop and assume that* $\mathrm{Aut}(Q)$ *acts transitively on $Q^\sharp = Q \setminus \{1\}$. Then Q is an elementary abelian p-group for some prime p.*

Proof. We have seen that all non-trivial elements of Q have prime order p. Lemma 5.10 proves the theorem in the case $p > 2$. Assume $p = 2$ and suppose that Q is not elementary abelian. Then by Lemma 5.12, we construct a unique 1-factorization $\mathscr{F}$ of the complete graph K_n with $n = |Q|$ such that $\mathrm{Aut}(\mathscr{F})$ is doubly transitive on the vertices. [CK93, Theorem 3] implies that $n = 6, 12$ or 28 and in all cases $\mathscr{F}$ is unique. As the construction of the 1-factorization is explicitely given in [CK93, Proposition 3], it is straightforward to verify that these 1-factorizations do not correspond to Bol loops. This contradiction proves our theorem. □

5.4. Open problems on simple loops

In this section, we propose five problems which are related to simple Bol loops. The first two problems were proposed by the author at the LOOPS'07 conference in Prague.

Problem 5.14. *Are there simple Bol loops which are neither G-loops nor isotopes of Bruck loops?*

Problem 1 is not reduced to finite Bol loops. By the author's best knowledge all known simple Bol loops are either G-loops or isotopes of Bruck loops. Here by *Bruck loop* we mean a right Bol loop with the automorphic inverse property. We mention that all groups and all known simple Moufang loops are G-loops.

A sufficient but not neccesary condition of the simplicity of a loop is that its right multiplication group acts primitively. Trivial examples of simple loops with imprimitive right multiplication groups are non-abelian simple groups. For non-associative simple Moufang loops, the left, right and full multiplication groups coincide, hence they act primitively on the loop. All known non-Moufang finite simple Bol loops have imprimitive right multiplication group. This motivates the following question.

Problem 5.15. *Is there a finite simple non-Moufang Bol loop where the right multiplication group acts primitively on the loop?*

The first step towards settling Problem 2 can be the following result of E. K. Loginov [Log07]: If the right multiplication group of a Bol loop Q is a finite simple group of Lie type then Q is a finite simple group. Moreover, as Bol loops of prime power order are solvable, $\mathrm{RMlt}(Q)$ cannot be a primitive group of affine type.

The next problem is *folklore* for different loop classes. Lagrange's Theorem was shown for finite Moufang loops by A. Grishkov and Zavarnitsine [GZ05]. It is known that in an equationally defined class of loops, the problem can be reduced to simple loops.

Problem 5.16. *Does Lagrange's Theorem hold for finite Bol loops?*

Let $\mathbb{O}$ be a non-degenerate octonion algebra over the field k. It is well known that modulo the center, the elements of norm 1 form a simple Moufang loop; we call them *classical*. Liebeck's theorem [Lie87b] says that all finite simple non-associative Moufang loops classical with finite ground field. This result was recently extended to locally finite simple Moufang loops by J. I. Hall [Hal07]. Moreover, it also holds for differentiable Moufang loops, see [HS90, IX.6.31. Theorem]. However, no non-classical simple Moufang loops are known.

Problem 5.17. *Do there exist non-classical infinite simple Moufang loops?*

Our last problem was proposed by M. Kinyon at the Mile High Conference 2007 in Denver. It is not directly related to Bol loops. The loop Q is said to be an *A-loop* if all inner maps of Q are automorphisms of Q. Clearly, all groups are A-loops.

Problem 5.18. *Do there exist finite simple non-associative A-loops?*

6. Algebraic Bol loops

Let G be an algebraic group over an algebraically closed field k with closed subgroup H and closed subset K and assume that for each conjugate H^g of H in G, the map

$$H^g \times K \to G, \qquad (h,k) \mapsto hk$$

is a biregular morphism. Then the triple (G,H,K) is an *algebraic loop folder* and the corresponding loop L is a *strongly algebraic* loop.

There is a more natural definition of the concept of algebraic loops, see [Nag03]. A loop L is *algebraic* if L is an algebraic variety over an algebraically closed field k with regular morphisms

$$m : L \times L \to L, \quad \phi : L \times L \to L, \quad \psi : L \times L \to L,$$

such that the identities

$$x = m(e,x) = m(x,e) = m(y,\phi(y,x)) = m(\psi(x,y),y) \tag{6.1}$$

hold for all $x,y \in L$ and some fixed $e \in L$. In this case $m(x,y) = x \cdot y$ is the loop product and $\psi(x,y) = x/y$, $\phi(x,y) = y\backslash x$ are the right and left divisions, respectively.

If the morphisms m,ψ,ϕ are well defined rational maps from $L \times L \to L$ such that the identities (6.1) hold on a Zariski-open subset of $L \times L$ then we shall call L a *local algebraic loop.*

In this chapter, we examine the class of *algebraic right Bol loops.* We explain the relations between the classes of algebraic, strongly algebraic and local algebraic Bol loop. We will show some structure theorems and give many examples.

The results of this chapter have appeared in [GN11].

6.1. Algebraic vs. strongly algebraic loops

One of the main questions in the theory of algebraic loops for a given class of loops is the equivalence of the notion of algebraic and strongly algebraic loops.

It is known that via the *localization process*, any algebraic group determines a formal group. This method works for the class of local algebraic loops, as well, see [Nag02]. A formal algebraic loop over the field k is a system

$$\boldsymbol{\mu}(\boldsymbol{X},\boldsymbol{Y}) = (\mu^i(X_1,\ldots,X_n,Y_1,\ldots,Y_n)), \qquad i = 1,\ldots,n$$

of formal power series in $2n$ variables over k such that the identities

$$\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{0}) = \boldsymbol{\mu}(\boldsymbol{0}, \boldsymbol{X}) = \boldsymbol{X}$$

hold. The integer n is the dimension of the formal loop. If the formal loop $\boldsymbol{\mu}$ is the localization of a local Bol loop, then it clearly satisfies the *formal Bol identity*

$$\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{\mu}(\boldsymbol{\mu}(\boldsymbol{Y}, \boldsymbol{Z}), \boldsymbol{Y})) = \boldsymbol{\mu}(\boldsymbol{\mu}(\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y}), \boldsymbol{Z}), \boldsymbol{Y}).$$

Moreover, any algebraic automorphism of an algebraic loop induces an automorphism of the associated formal loop.

A finite dimensional $\mathbb{R}$-vector space B with trilinear operation $(.,.,.)$ and bilinear operation $[.,.]$ is a *Bol algebra* if

$$\begin{aligned}(x, y, y) = 0, (x, y, z) + (y, z, x) + (z, x, y) = 0\\ ((x, a, b), y, z) + (x, (y, a, b), z) + (x, y, (z, a, b)) = ((x, y, z), a, b)\\ ([x, y], a, b) = [(x, a, b), y] - [x, (y, a, b)] + ([a, b], x, y) + [[a, b], [x, y]]\end{aligned}$$

holds for all $x, y, z, a, b \in B$. L. Sabinin [Sab99] developed a complete theory for local differentiable Bol loops. [Sab99, 5.34 Proposition] says that local differentiable right Bol loops are functorially equivalent to Bol algebras. This functorial equivalence works perfectly between finite dimensional Bol k-algebras and formal Bol loops over fields of characteristic 0. In particular, the automorphisms of a formal Bol loop over a field of characteristic 0 correspond biuniquely to linear automorphisms of the tangent Bol k-algebra. Let X be a variety and G be a group consisting of algebraic transformations of X. We define connectedness and dimension of G as in [Ram64].

Lemma 6.1. *Let L be a global algebraic Bol loop over an algebraically closed field k of characteristic 0 and G a connected group consisting of algebraic automorphisms of L. Then G is biregularly isomorphic to a closed subgroup of $GL_n(k)$ where $n = \dim(L)$. In particular, G is finite dimensional and has a unique structure of an algebraic transformation group on L.*

Proof. Let α be an algebraic automorphism of L and denote by $\boldsymbol{\mu}(\boldsymbol{X}, \boldsymbol{Y})$ the formal Bol loop associated to L. As $\alpha(e) = e$, it has a localization $\boldsymbol{\alpha}(\boldsymbol{T})$ which is a formal automorphism of $\boldsymbol{\mu}$. The action of α on the tangent Bol algebra is given by the Jacobian $(\frac{\partial \boldsymbol{\alpha}^i}{\partial T^j}(\boldsymbol{0}))$ of $\boldsymbol{\alpha}$. Hence, we have an algebraic embedding φ of G into $GL_n(k)$. Let us define the action of G on $GL_n(k)$ by $X^g = X\varphi(g)$. By [Ram64, Lemma 2], the orbit of 1 is a locally closed subvariety of $GL_n(k)$. On the one hand, this orbit is precisely $\mathrm{Im}\varphi$. On the other hand, $\overline{\mathrm{Im}\varphi} = \mathrm{Im}\varphi$ by [Hum75, Proposition 7.4.A]. □

The main result of this sections is the following.

Theorem 6.2. *Let L be a connected algebraic Bol loop over a field k of characteristic 0. Then the right multiplication group $\mathrm{RMlt}(L)$ of L is a connected algebraic group; in particular, L is a strongly algebraic loop.*

Proof. For any $x \in L$, we define the algebraic transformation $\alpha_x = (R_x^{-1}, L_x R_x)$ on $L \times L$. Let G be the group generated by the connected algebraic family $\{\alpha_x \mid x \in L\}$, then G is itself connected. It is easy to see that any element (β_1, β_2) of G can be uniquely extended to an autotopism $(\beta_1, \beta_2, \beta_3)$ of L. Hence, the stabilizer $G_{(e,e)}$ of $(e, e) \in L \times L$ is contained in $\mathrm{Aut}(L)$. We show that G is finite dimensional of dimension at most $n^2 + 2n$ where $n = \dim(L)$. Let $\{\varphi_t \mid t \in T\}$ be an injective family of elements of G with connected variety T of dimension $N > n^2 + 2n$. By [Ram64, Lemma 2], $X = \{\varphi_t(e, e) \mid t \in T\}$ is a locally closed subvariety of $L \times L$. The set $\{t \in T \mid \varphi_t(e, e) = (e, e)\}$ is a closed subvariety of T, let T_0 be a connected component of maximal dimension. As $\dim T_0 + \dim X = \dim T$ and $\dim X \leq 2n$, we have $\dim T_0 > n^2$. However, $\{\varphi_t \mid t \in T_0\}$ is a connected injective algebraic family in $\mathrm{Aut}(L)$, hence a subset of $GL_n(k)$ by Lemma 6.1, a contradiction. The main theorem of [Ram64] implies the claimed result. □

Clearly, if $\mathrm{RMlt}(L)$ is an algebraic transformation group on L, then L can be given by the algebraic loop folder (G, H, K) where $G = \mathrm{RMlt}(L)$, $H = \mathrm{RInn}(L)$ and $K = \{R_x \mid x \in L\}$. Indeed, the decomposition $G \to H \times K$, $g \mapsto hR_x$ with $x = e^g$, $h = gR_x^{-1}$ is a biregular bijection between G and $H \times K$. This implies that in this case, L is strongly algebraic. Conversely, let L be given by a connected algebraic loop folder (G, H, K). We do not destroy the algebraic property of the folder by assuming that H does not contain a proper normal subgroup of G. Then, by identifying L with the coset space G/H, G can be seen as an algebraic transformation group acting on L. Moreover, every right multiplication map of L will be contained in G. Since K is connected, it generates a closed connected subgroup of G, hence $\mathrm{RMlt}(L)$ is a connected algebraic transformation group.

Corollary 6.3. *Let L be an algebraic Bol loop over an algebraically closed field k of characteristic 0. Then L is a strongly algebraic loop.* □

Unfortunately, Lemma 6.1 does not hold when $\mathrm{char}(k) > 0$. More precisely, a connected group of automorphisms of L can have infinite dimension. The rest of the proof works fine. Therefore we have the following

Conjecture 6.4. *Let L be a connected algebraic Bol loop over an algebraically closed field k. Then $\mathrm{RMlt}(L)$ is an algebraic transformation group. In particular, every algebraic Bol loop is strongly algebraic.*

From the proof of Theorem 6.2 follows that in order to show the strong algebraic property, it is sufficient to study the right inner mapping group of an algebraic Bol loop.

Proposition 6.5. *Let L be an algebraic Bol loop over an algebraically closed field k and assume that the right inner mapping group $H = \mathrm{RInn}(L)$ of L is finite dimensional. Then L is strongly algebraic.* □

6.2. Simple algebraic and local algebraic Bol loops

Throughout this section k denotes an algebraically closed field. As all known algebraic Bol loops are strongly algebraic, in the following examples, we will often skip the adjective "strongly". It is known that given any algebraic group G with closed normal subgroup S, one can give the abstract group G/S the structure of (affine) algebraic group, see [Hum75, Section 11 and 12]. This problem is rather subtle already for algebraic groups, and in general the solution is not known for algebraic loops. The next theorem gives a solution for strongly algebraic loops, that is, for loops given by algebraic loop folders. The normality condition for loop folders was given in [Asc05, (2.6)]. A subfolder (G_0, H_0, K_0) corresponds to a normal subloop if and only if

(NC) for each $g \in G$, $k_0 \in K_0$ and $k \in K$, $k_0 k = l_0 k'$ for some $l_0 \in H^g \cap G_0$ and $k' \in K$.

In particular, $K_0 K \subseteq H_0 K$ holds.

Theorem 6.6. *Let (G, H, K) be an algebraic loop folder with corresponding loop L. Let N be a closed normal subloop of L. Then there is an algebraic loop folder $(\bar{G}, \bar{H}, \bar{K})$ such that the corresponding algebraic loop $\bar{L}$ is isomorphic to the abstract factor loop L/N. Moreover, the natural homomorphism $L \to \bar{L} = L/N$ is a regular morphism. The algebraic loop $\bar{L}$ is unique up to algebraic isomorphism.*

Proof. We assume w.l.o.g. that $\mathrm{core}_G(H) = 1$ and identify the homogenous space G/H with L. Let H_1 denote the stabilizer of the the closed set $N \subseteq L$; $H_1 \leq G$ is closed by [Hum75, Proposition 8.2]. $G_0 = \mathrm{core}_G(H_1) = \cap_{g \in G} H_1^g$ is an intersection of closed sets, hence is a closed normal subgroup of G. Write $H_0 = G_0 \cap H$, $K_0 = G_0 \cap K$ for the closed subsets of G. (G_0, H_0, K_0) is the normal subfolder corresponding to the abstract loop homomorphism $L \to L/N$. By the normality condition (NC), $K_0 K = H_0 K$, thus, $G_0 K = H_0 K_0 K \subseteq H_0 K$. As $H_0 \cap K = 1$, this means that the subset $K_1 = G_0 K$ of G is biregularly isomorphic to the subvariety $H_0 \times K$ of $H \times K$. In particular, $G_0 K$ is closed in G, since the varieties G and $H \times K$ are biregularly equivalent.

Let φ be the natural homomorphism $G \to \bar{G} = G/G_0$ and define $\bar{H} = \varphi(H)$ and $\bar{K} = \varphi(K)$. The loop homomorphism $L \to L/N$ corresponds to an abstract folder homomorphism $\varphi : (G, H, K) \to (\bar{G}, \bar{H}, \bar{K})$. In order to see that L/N is algebraic, we have to show that $\bar{H}, \bar{K}$ are closed in $\bar{G}$. Indeed, the respective preimages $H_1 = G_0 H$ and $K_1 = G_0 K$ of $\bar{H}$ and $\bar{K}$ are closed in G. As $\bar{G} = G/G_0$ is endowed with the quotient topology (cf. [Hum75, Section 12]), $\bar{H}$, $\bar{K}$ are closed. This completes the proof. □

The (strongly) algebraic loop L is said to be *simple* if it has no proper closed normal subloops. The most important example of strongly algebraic Bol loops is the Paige loop $M(k)$, for the definition see [Pai56]. It is known that $M(k)$ is a nonassociative simple Moufang loop, its multiplication group is the projective orthogonal group $P\Omega_8^+(k)$.

Now, we give examples of simple algebraic Bol loops. The examples are constructed from an exact factorization $G = AB$ of the group G.

Proposition 6.7. *Let (G, A, B) be an exact factorization triple such that G is an algebraic group over the algebraically closed field k, and A, B are closed subgroups of G. Then the Bol loop $\beta(G, A, B)$ is a strongly algebraic Bol loop.*

Proof. Clearly, G, A, B determine an algebraic Bol loop folder, hence the corresponding loop is strongly algebraic. □

Our main example for a simple strongly algebraic non-Moufang non-Bruck Bol loop is the one in Example 3.14.

The local hyperbolic plane loop

By Weil's theorem [Wei55], any local algebraic group is birationally equivalent to an algebraic group. In this section, we construct a local algebraic Bol loop and prove that it is not birationally equivalent to a global algebraic loop.

The translations of the hyperbolic plane are defined as products of two central symmetries; the set of hyperbolic translations forms a sharply transitive set on the hyperbolic plane, the associated loop is the classical simple Bruck loop given by (1.4). Formal expansion using $x = x_1 + ix_2$, $y = y_1 + iy_2$ gives the formal operation

$$(x_1, x_2) \cdot (y_1, y_2) = (z_1, z_2)$$

with

$$\begin{cases} z_1 &= \dfrac{x_1 + x_1^2 y_1 + y_1 + x_1 y_1^2 + 2y_1 x_2 y_2 + x_2^2 y_1 - y_2^2 x_1}{1 + 2x_1 y_1 + 2x_2 y_2 + x_1^2 y_1^2 + x_2^2 y_2^2 + x_1^2 y_2^2 + x_2^2 y_1^2}, \\ z_2 &= -\dfrac{-x_1^2 y_2 - 2x_1 y_1 y_2 + x_2 y_1^2 - x_2 - x_2^2 y_2 - y_2 - y_2^2 x_2}{1 + 2x_1 y_1 + 2x_2 y_2 + x_1^2 y_1^2 + x_2^2 y_2^2 + x_1^2 y_2^2 + x_2^2 y_1^2}. \end{cases} \tag{6.2}$$

This operation defines a simple local algebraic right Bruck loop on k^2 for any field k. The unit element is $(0, 0)$ and the inverse of (x_1, x_2) is $(-x_1, -x_2)$. Straightforward calculation gives that the right inner map $R_{(y_1,y_2),(z_1,z_2)}$ is

$$(x_1, x_2) \mapsto (ax_1 + bx_2, -bx_1 + ax_2),$$

where

$$\begin{aligned} a &= \frac{z_2^2 y_2^2 + 2z_2 y_2 - z_2^2 y_1^2 + 4z_1 z_2 y_1 y_2 - z_1^2 y_2^2 + z_1^2 y_1^2 + 2z_1 y_1 + 1}{1 + 2z_1 y_1 + 2z_2 y_2 + z_1^2 y_1^2 + z_2^2 y_2^2 + z_2^2 y_1^2 + z_1^2 y_2^2}, \\ b &= \frac{2z_1 z_2 y_2^2 + 2z_1^2 y_1 y_2 - 2z_2^2 y_1 y_2 - 2z_1 z_2 y_1^2 - 2y_1 z_2 + 2z_1 y_2}{1 + 2z_1 y_1 + 2z_2 y_2 + z_1^2 y_1^2 + z_2^2 y_2^2 + z_2^2 y_1^2 + z_1^2 y_2^2}. \end{aligned}$$

Moreover, $a^2 + b^2 = 1$ holds identically. Thus, the right inner maps are contained in a 1-dimensional algebraic group H acting on k^2.

We claim that this local loop is not birationally equivalent to an algebraic loop. Let us assume that $(L, \cdot)$ is an algebraic loop such that $\alpha : k^2 \to L$ is a birational isomorphism. Then $\mathrm{RInn}(L)$ has the structure of a 1-dimensional algebraic transformation group on L. By Proposition 6.5, $G = \mathrm{RMlt}(L)$ is a 3-dimensional algebraic transformation group. Moreover, as L is a simple Bruck loop, G is a simple group, hence $G \cong PSL(2, k)$. Any simple Bruck loop can be given by a loop folder (G, H, K) where $H = C_G(\sigma)$ and $K = \{g \in G \mid g^\sigma = g^{-1}\}$ for an involutorial automorphism σ of G. It is easy to check that $PSL_2(k)$ has no such automorphism. This proves that (6.2) indeed defines a proper local algebraic Bol loop.

6.3. Algebraic solvable Bol loops

In this section, we investigate the relation between solvable (strongly) algebraic groups and and algebraic loop folders (G, H, K) with solvable group G. We first show that the Jordan decomposition is well-defined in the class of power-associative strongly algebraic loops.

Proposition 6.8. *Let L be a connected power-associative strongly algebraic loop. If $x \in L$, there exist unique elements $s, u \in L$ such that: $R_x = R_s R_u$, s and u are contained in a closed Abelian subgroup of L, R_s is semisimple and R_u is unipotent in $\mathrm{RMlt}(L)$. If $\varphi : L \to \bar{L}$ is a morphism of strongly algebraic loops then $\varphi(x)_s = \varphi(x_s)$ and $\varphi(x)_u = \varphi(x_u)$.*

Proof. Let L be given by a faithful algebraic loop folder (G, H, K) with $G = \mathrm{RMlt}(L)$. Since L is power-associative and K closed in G, R_x is contained in a closed Abelian subgroup U of G such that $U \subseteq K$. Let $R_x = s_0 u_0$ be the unique Jordan decomposition of R_x in U. As U is contained in K, there are unique elements $s, u \in L$ such that $s_0 = R_s$, $u_0 = R_u$. Finally, the set $\{y \in L \mid R_y \in U\}$ is a closed Abelian subgroup of L, which contains s, u. The last assertion follows from the fact that morphisms of strongly algebraic loops are equivalent to morphisms of algebraic loop folders, see Theorem 6.6. □

Now, we are able to prove the Lie-Kolchin theorem for strongly algebraic Bol loops.

Theorem 6.9. *Let L be a connected strongly algebraic Bol loop and assume that $\mathrm{RMlt}(L)$ is solvable. Then L has a closed connected solvable normal subloop L_u consisting of the unipotent elements of L. The factor loop L/L_u is a torus. In particular, L is solvable.*

Proof. Let L be given by the faithful algebraic loop folder (G, H, K) with $G = \mathrm{RMlt}(L)$. Let U be the unipotent radical of G and put $U_1 = HU$. We claim that $U_1 \cap K \subseteq U$. Take an arbitrary $R_x \in U_1 \cap K$, $R_x = R_s R_u$ its Jordan decomposition with $R_s, R_u \in U_1 \cap K$. By the Lie-Kolchin theorem, we have the decomposition $H = H_s H_u$ of the solvable algebraic group H; thus, $U_1 = H_s U$ and H_s is a maximal

torus in U_1. This implies that R_s is conjugate to an element of H_s, hence $R_s = 1$ and $R_x = R_u \in U$. Clearly, $(U_1, U_1 \cap H, U_1 \cap K)$ determines a closed subfolder of (G, H, K). Moreover, as it satisfies the normality condition (NC), the corresponding subloop N is normal in L. By $U_1 \cap K = U \cap K$, N consists precisely of the unipotent elements of L. The factor loop L/N has the algebraic loop folder $(G/HU, 1, G/HU)$, thus $L/N \cong G/HU$ is a torus.

In order to show the solvability of L, it remains to deal with the case when L consists of unipotent elements. Then $K \subseteq G_u$ and $G = \langle K \rangle = G_u$ can be assumed. In this case, H is contained in a proper closed normal subgroup M of G and the surjective morphism $(G, H, K) \to (G/M, 1, G/M)$ of algebraic loop folders corresponds to a surjective morphism $L \to G/M$ of algebraic loops. □

Global algebraic Bol loops with trivial center in nilpotent groups

After Theorem 6.9, it is natural to ask about the structure of algebraic Bol loop folders (G, H, K) where G is a connected unipotent group. The following construction shows that the nilpotence of the enveloping group does not imply the nilpotence of the Bol loop even in the strongly algebraic case.

This example was constructed in collaboration with M. A. Reis (São Paulo).

Example 6.10. Let k be a field of characteristic different from 2. Let V be a k-linear space of dimension n and X a k-linear subspace of $\mathrm{End}(V)$ consisting of nilpotent elements. In particular, $x^n = 0$ for all $x \in X$ and the map

$$x \mapsto (1-x)^{-1} = 1 + x + \cdots + x^{n-1}$$

is a k-morphism from X to $\mathrm{End}(V)$. For any $x \in X$, $v \in V$, we denote the image of v under x by xv. Put $G = X \oplus V \oplus V$ and define the operation

$$(x_1, v_1, w_1)(x_2, v_2, w_2) = (x_1 + x_2, v_1 + v_2, w_1 + w_2 + \frac{1}{2}(x_1 v_2 - x_2 v_1)).$$

It is straightforward to see that this operation makes G to a 2-step nilpotent algebraic group with commutator

$$[(x_1, v_1, w_1), (x_2, v_2, w_2)] = (0, 0, x_1 v_2 - x_2 v_1).$$

The set $K = \{(x, v, 0) \mid x \in X, v \in V\}$ consists of the anti-fixed elements of the involutorial automorphism $\sigma : (x, v, w) \mapsto (-x, -v, w)$ of G. Thus, if $x, y \in K$ then $xyx \in K$. Define the subgroup $H = \{(0, w, w) \mid w \in V\}$ of G; then $H \cong (V, +)$. Any element

$$(x, v, w) = \left(0, \left(1 - \frac{x}{2}\right)^{-1} w, \left(1 - \frac{x}{2}\right)^{-1} w\right) \left(x, v - \left(1 - \frac{x}{2}\right)^{-1} w, 0\right)$$

of G can be factorized uniquely as product of elements of H and K. Moreover, the maps

$$G \to H, \qquad (x,v,w) \to \left(0, \left(1-\frac{x}{2}\right)^{-1} w, \left(1-\frac{x}{2}\right)^{-1} w\right),$$
$$G \to K, \qquad (x,v,w) \to \left(x, v - \left(1-\frac{x}{2}\right)^{-1} w, 0\right)$$

are k-morphisms. This implies that the triple (G,H,K) is an algebraic Bol loop folder. The explicit formula for the loop operation is

$$(x_1,v_1)(x_2,v_2) = (x_1+x_2, v_1+v_2-(2-x_1-x_2)^{-1}(x_1v_2-x_2v_1)), \tag{6.3}$$

where the underlying set of the loop is $X \oplus V$.

Now, we give a k-linear subspace X of $\mathrm{End}(V)$ such that Example 6.10 defines an algebraic Bol loop with trivial center. The following construction appeared first in [Sut72]. Let us put $V = k^3$ and

$$X = \left\{ \begin{pmatrix} 0 & s & 0 \\ t & 0 & s \\ 0 & -t & 0 \end{pmatrix} \mid s,t \in k \right\}.$$

For any $x_1 \in X \setminus \{0\}$, there is a $v_2 \in V$ such that $x_1v_2 \neq 0$ and for any $v_1 \in V \setminus \{0\}$ there is an $x_2 \in X$ such that $x_2v_1 \neq 0$. Hence by (6.3), (x_1,v_1) does not commute with $(0,v_2)$ and $(0,v_1)$ does not commute with $(x_2,0)$. This means that the center of the corresponding algebraic Bol loop is trivial.

We remark that by dropping the condition of nilpotency on the elements of X, formula (6.3) gives a local algebraic Bol loop. However, it is not clear in which cases are these local algebraic Bol loops birationally equivalent to global algebraic loops.

Problem 6.11. *What are the necessary and sufficient conditions for a local (solvable) algebraic Bol loop to be birationally equivalent to a global algebraic loop?*

We finish this section with a proposition which gives a condition for the enveloping group of a Bol loop to have nilpotency class 2. The advantage of this result is that it is rather easy to check when the loop operation is given explicitely.

Proposition 6.12. *Let $(L,\cdot)$ be a right Bol loop and define the core $x+y = (yx^{-1})y$ of L. Then the following are equivalent.*

(i) For all $x,y,z \in L$, $((x+y)+1)+z = ((x+z)+1)+y$.

(ii) The group M generated by the maps $P_y = L_yR_y$, $y \in L$, is Abelian.

(iii) The group Γ generated by the autotopisms $\alpha_y = (R_y^{-1}, L_yR_y, R_y)$, $y \in L$, is nilpotent of class at most 2.

(iv) $\mathrm{RMlt}(L)$ *is nilpotent of class at most* 2.

Proof. We have

$$xP_yP_z = (((x+1)+y)+1)+z \quad \text{and} \quad xP_zP_y = (((x+1)+z)+1)+y,$$

hence (i) implies (ii). The projection pr_2 maps Γ onto M, the kernel consists of autotopisms of the form $(L_n, 1, L_n)$ with $n \in N_\lambda$. As for $n \in N_\lambda$, L_n centralizes $\mathrm{RMlt}(L)$, $\ker \mathrm{pr}_2 \leq Z(\Gamma)$. Thus, (ii) implies (iii). Since $\mathrm{RMlt}(L)$ is a homomorphic image of Γ, from (iii) follows (iv). Finally, $R_x + R_y = R_y R_x^{-1} R_y = R_{x+y}$ shows that $y \mapsto R_y$ is an embedding of $(L, +)$ into the core of $\mathrm{RMlt}(L)$. The identity in (i) can be easily shown for groups of nilpotency class 2. □

6.4. Constructions of solvable algebraic Bol loops

In this class of examples, we assume that G is an algebraic group over k which is a semidirect product of the connected algebraic groups A and B; $G = A \rtimes B$. Clearly, $G = AB$ is an exact factorization. Explicit calculation shows that the resulting Bol loop L is isomorphic to the split extension constructed by Johnson and Sharma [JS80]. In particular, if the action of B on A is not Abelian then L is non-Moufang and non-Bruck, see [JS80, Theorem 2].

Take $A = k^n$ and $B = T_n(k)$ the group of $n \times n$ upper triangular matrices; then $G = AB$ is solvable. The following proposition says that the associated Bol loop L is solvable.

Proposition 6.13. *Let $G = AB$ be an exact factorization and $N \leq A$ is normal in G. Define $K = \{(x, x^{-1}) \mid x \in G\} \subseteq G \times G$ and $\bar{K} = \{(xN, x^{-1}N) \mid xN \in G/N\} \subseteq G/N \times G/N$. Then the following hold:*

(i) $\varphi : (G \times G, A \times B, K) \to (G/N \times G/N, A/N \times B, \bar{K})$ *is a surjective morphism of loop folders. The kernel of φ is the normal subfolder $(N \times N, N \times 1, K_N)$ with $K_N = \{(x, x^{-1}) \mid x \in N\}$. The corresponding normal subloop is isomorphic to the group N.*

(ii) If $N \leq Z(G) \cap A$ then $\ker \varphi \leq Z(L)$, where L is the Bol loop associated to the exact factorization $G = AB$.

Proof. We first notice that it is meaningful to speak of the subgroup $A/N \times B$ of $G/N \times G/N$, since $B \cap N = 1$ implies that the image of B in G/N is isomorphic to B. Moreover, G/N is has an exact factorization with subgroups $A/N, B$. We leave to the reader to check that φ is indeed a morphism of loop folders with kernel $(N \times N, N \times 1, K_N)$. The corresponding loop is precisely the group N. This shows (i). To see (ii), assume $N \leq Z(G) \cap A$ and take an arbitrary element (n, n^{-1}) of the transversal belonging to $\ker \phi$. Then $(n, n^{-1})K = K$ implies that the corresponding loop element $x \in L$ is contained in the right and middle nucleus $N_\rho(L) = N_\mu(L)$. Furthermore, by $(n, n^{-1}) \in Z(G \times G)$, the associated loop element x commutes with all elements of L. Thus, $x \in Z(L)$. □

We mention that for solvable algebraic $G = AB$, the solvability of the corresponding Bol loop follows from Theorem 6.9, as well. However, Proposition 6.13 is also useful for the construction of non-Moufang nilpotent algebraic Bol loops. In fact, if A and B are nilpotent groups and $B \leq \mathrm{Aut}(A)$ is not Abelian, then by Proposition 6.13(ii), L is nilpotent.

Finally, we mention that many examples of nilpotent algebraic nonassociative Bruck and Moufang loops are known. For the Moufang case, see [Bru58, Example VII.5.3]. For nilpotent algebraic Bruck loops, one has to consider the operation $x \circ y = x^{\frac{1}{2}} y x^{\frac{1}{2}}$ on any unipotent group G with $\mathrm{char}(k) \neq 2$, cf. [NS02, Section 12].

Part III.

Multiply sharply transitive sets

dc_821_13

7. On the non-existence of sharply transitive sets

A permutation code (or array) of length n and distance d is a set S of permutations of some fixed set Ω of n symbols such that the Hamming distance between each distinct $x, y \in S$ is at least d, see [FD77]. By elementary counting, one has $|S| \leq n(n-1)\cdots d$ and equality holds if and only if for any two tuples $(x_1, \ldots, x_{n-d+1})$, $(y_1, \ldots, y_{n-d+1})$ of distinct symbols, there is a unique element $s \in S$ with $x_1^s = y_1, \ldots, x_{n-d+1}^s = y_{n-d+1}$. Such sets of permutations are called *sharply t–transitive*, where $t = n - d + 1$. It is well known that sharply 1– and 2–transitive sets of permutations correspond to Latin squares and affine planes, respectively [Dem68].

In general, there are very few results on permutation codes and there is a large gap between the lower and upper estimates for $|S|$; see [Tar99], [Qui06]. Most of the known constructions are related to multiply transitive permutation groups. In the 1970's, P. Lorimer started the systematic investigation of the question of existence of sharply 2–transitive sets in finite 2–transitive permutation groups. This program was continued by Th. Grundhöfer, M. E. O'Nan, P. Müller, see [GM09] and the references therein. Some of the 2–transitive permutation groups needed rather elaborated methods from character theory in order to show that they do not contain sharply 2–transitive sets of permutations.

In this chapter, we present some simple combinatorial methods which are useful to exclude the existence of sharply 1– and 2–transitive sets of permutations in given finite permutation groups.

Lemma 7.1, Theorems 7.4, 7.8, 7.10 and Corollary 7.7 support **Thesis 3.** Most of the results of this chapter appeared in the papers [MN11]; the exception is Theorem 7.10 from [MN07]. The essential references to these results are the following.

1) Kantor and Pentilla use Theorem 7.10 to prove the main result of their paper [KP12] on finite projective planes in which every quadrangle lies on a unique Baer subplane.

2) In [HL12], Hiss and Lübeck use [MN07, Lemma 2.1] to show that M_{22} does not contain the multiplication group of a quasigroup. In fact, the original proof of [MN07, Lemma 2.1] is computer based, but it follows immediately from the computer free proof of Theorem 7.5.

7.1. Contradicting subsets

We remind that if S is a sharply t–transitive set of permutations on Ω, then it is also a sharply 1–transitive set of permutations on the set $\Omega^{(t)}$ of t–tuples of pairwise distinct elements from Ω. In other words, the t–transitive permutation group G contains a sharply t–transitive set if and only if in its induced action on $\Omega^{(t)}$, G contains a sharply 1–transitive set.

Let G be a permutation group on the set $\Omega = \{\omega_1, \ldots, \omega_n\}$ and for $g \in G$, denote by $\pi(g)$ the corresponding permutation matrix. Let J denote the $n \times n$ all-one matrix. The existence of sharply transitive sets in G is equivalent to the $\{0,1\}$–solvability of the matrix equation

$$\sum_{g \in G} x_g \pi(g) = J. \tag{7.1}$$

The following simple lemma will be our main tool.

Lemma 7.1. *Let S be a sharply transitive set of permutations on a finite set Ω. Let B and C be arbitrary subsets of Ω. Then $\sum_{g \in S} |B \cap C^g| = |B||C|$.*

Proof. Count the set of triples (b, c, g), where $b \in B$, $c \in C$, $g \in S$ and $c^g = b$, in two ways: If b, c is given, then there is a unique g by sharp transitivity. If g is given, then the number of pairs b, c is $|B \cap C^g|$. □

An immediate consequence is

Lemma 7.2. *Let G be a permutation group on a finite set Ω. Assume that there are subsets B, C of Ω and a prime p such that $p \nmid |B||C|$ and $p \mid |B \cap C^g|$ for all $g \in G$. Then G contains no sharply transitive set of permutations.*

Remark 7.3. It is easy to see that under the assumption of Lemma 7.2, the system (7.1) does not have a solution in the finite field $\mathbb{F}_p$, so in particular (7.1) has no integral solution.

We give several applications of these lemmas. First, we show that in even characteristic, the symplectic group does not contain sharply transitive sets of permutations.

Theorem 7.4. *Let n, m be positive integers, $n \geq 2$, $q = 2^m$. Let $G_1 = PSp(2n, q) \rtimes \mathrm{Aut}(\mathbb{F}_q)$ and $G_2 = Sp(2n, q) \rtimes \mathrm{Aut}(\mathbb{F}_q)$ be permutation groups in their natural permutation actions on $\Omega_1 = PG(2n-1, q)$ and $\Omega_2 = \mathbb{F}_q^{2n} \setminus \{0\}$. Then, G_1 and G_2 do not contain a sharply transitive set of permutations.*

Proof. We deal first with the projective group G_1. Let $\mathcal{E}$ be an elliptic quadric whose quadratic equation polarizes to the invariant symplectic form $\langle ., . \rangle$ of G_1. Let ℓ be a line of $PG(2n-1, q)$ which is nonsingular with respect to $\langle ., . \rangle$. Then for any

$g \in G_1$, ℓ^g is nonsingular, that is, it is not tangent to $\mathcal{E}$. In particular, $|\mathcal{E} \cap \ell^g| = 0$ or 2 for all $g \in G_1$. Furthermore, we have

$$|\mathcal{E}| = \frac{q^{2n-1}-1}{q-1} - q^{n-1}, \qquad |\ell| = q+1,$$

both odd for $n \geq 2$. We apply Lemma 7.2 with $B = \mathcal{E}$, $C = \ell$ and $p = 2$ to obtain the result of the theorem.

In order to show the result for the group G_2, we define the subsets $\mathcal{E}' = \varphi^{-1}(\mathcal{E})$ and $\ell' = \varphi^{-1}(\ell)$, where $\varphi : \Omega_2 \to \Omega_1$ is the natural surjective map. Then,

$$|\mathcal{E}'| = (q-1)|\mathcal{E}|, |\ell'| = (q-1)|\ell| \text{ and } |\mathcal{E}' \cap \ell'| \in \{0, 2(q-1)\}.$$

Hence, Lemma 7.2 can be applied with $B = \mathcal{E}'$, $C = \ell'$ and $p = 2$. □

It was a long standing open problem whether the Mathieu group M_{22} contains a sharply transitive set of permutations, cf. [Gru83]. The negative answer given in the following theorem implies the nonexistence of sharply 2–transitive sets in the Mathieu group M_{23}.

We will use the Witt design $\mathcal{W}_{23}$. This is a $S(4, 7, 23)$–Steiner system. The fact which we use here and again in the proof of Theorem 7.8 is that any two blocks of $\mathcal{W}_{23}$ intersect in 1, 3, or 7 points.

Theorem 7.5. *In its natural permutation representation of degree* 22*, the Mathieu group* M_{22} *does not contain a sharply transitive set of permutations.*

Proof. Let $\Omega' = \{1, \ldots, 23\}$, $\Omega = \{1, \ldots, 22\}$ and $G = M_{22}$ be the stabilizer of $23 \in \Omega'$. Let $B \subset \Omega$ be a block of the Witt design $\mathcal{W}_{23}$, and $C = \Omega \setminus B$. Then, $|B| = 7, |C| = 15$ and for all $g \in G$, $|B \cap C^g| = 0, 4$ or 6. Lemma 7.2 implies the result with $p = 2$. □

We can apply our method for certain alternating groups, as well. The following simple result is somewhat surprising because until now, the symmetric and alternating groups seemed to be out of scope in this problem.

Theorem 7.6. *If* $n \equiv 2, 3 \pmod 4$ *then the alternating group* A_n *does not contain a sharply* 2*–transitive set of permutations.*

Proof. Assume $n \equiv 2, 3 \pmod 4$ and let G be the permutation action of A_n on the set $\Omega^{(2)}$ with $\Omega = \{1, \ldots, n\}$. A sharply 2–transitive set of permutations in A_n corresponds to a sharply transitive set of permutations in G. Define the subsets

$$B = \{(x, y) \mid x < y\}, \qquad C = \{(x, y) \mid x > y\}$$

of $\Omega^{(2)}$. By the assumption on n, $|B| = |C| = n(n-1)/2$ is odd. For any permutation $g \in S_n$, we have

$$|\{(x, y) \mid x < y,\ x^g > y^g\}| \equiv \operatorname{sgn}(g) \pmod 2.$$

This implies $|B \cap C^g| \equiv 0 \pmod 2$ for all $g \in A_n$. Thus, we can apply Lemma 7.2 to obtain the nonexistence of sharply transitive sets in G and sharply 2–transitive sets in A_n. □

Theorems 7.5 and 7.6 can be used to prove the nonexistence of sharply 2–transitive sets in the Mathieu group M_{23}.

Corollary 7.7. *In its natural permutation representation of degree* 23*, the Mathieu group* M_{23} *does not contain a sharply* 2*–transitive set of permutations.*

As the last application of our contradicting subset method, we deal with the stabilizer of the sporadic group Co_3 in its doubly transitive action on 276 points. As a corollary, we obtain a purely combinatorial proof for a theorem by Grundhöfer and Müller saying that Co_3 has no sharply 2–transitive set of permutations. Notice that the original proof used the Atlas of Brauer characters.

Theorem 7.8. *Let* G *be the group* $McL{:}2$ *in its primitive permutation action on* 275 *points. Then,* G *does not contain a sharply transitive set of permutations.*

Proof. Identify G with the automorphism group of the McLaughlin graph Γ, acting on the 275 vertices. We claim that there are subsets B and C of vertices with $|B| = 22$, $|C| = 56$, and $|B \cap C^g| \in \{0, 3, 6, 12\}$ for all $g \in G$. The theorem then follows from Lemma 7.2 with $p = 3$.

In order to describe B and C, we use the construction of Γ based on the Witt design $\mathcal{W}_{23}$, see e.g. [BCN89, 11.4.H]. Let $B \cup \{q\}$ be the 23 points of $\mathcal{W}_{23}$. Let U be the 77 blocks of $\mathcal{W}_{23}$ which contain q, and V be the 176 blocks which do not contain q. The vertices of Γ are the $22 + 76 + 176 = 275$ elements from $B \cup U \cup V$. Adjacency $\sim$ on Γ is defined as follows: The elements in B are pairwise non–adjacent. Furthermore, for $b \in B$, $u, u' \in U$, $v, v' \in V$ define: $b \sim u$ if $b \notin u$, $b \sim v$ if $b \in v$, $u \sim u'$ if $|u \cap u'| = 1$ (so $u \cap u' = \{q\}$), $v \sim v'$ if $|v \cap v'| = 1$, and $u \sim v$ if $|u \cap v| = 3$.

This construction gives the strongly regular graph Γ with parameters $(275, 112, 30, 56)$. Pick two vertices $i \neq j$ which are not adjacent, and let C be the set of vertices which are adjacent to i and j. Then $|C| = 56$. For $g \in G = \mathrm{Aut}(\Gamma)$, C^g is again the common neighborhood of two non–adjacent vertices. Thus without loss of generality we may assume $g = 1$, so we need to show that $|B \cap C| = 0, 3, 6$, or 12. Suppose that $|B \cap C| > 0$. Then there is a vertex $x \in B \cap C$ which is adjacent to i and j. Therefore $i, j \notin B$. Recall that two distinct blocks of $\mathcal{W}_{23}$ intersect in either 1 or 3 points.

We have to consider three cases: First $i, j \in U$. Then $|i \cap j| = 3$ and $q \in i \cap j$. Furthermore, $B \cap C = B \setminus (i \cup j)$, so $|B \cap C| = 12$. Next, if $i, j \in V$, then $|i \cap j| = 3$ and $B \cap C = i \cap j$, so $|B \cap C| = 3$. Finally, if $i \in U$, $j \in V$, then $|i \cap j| = 1$ and $B \cap C = j \setminus i$, so $|B \cap C| = 6$ and we have covered all cases. □

7.2. On 2–transitive symmetric designs

As another application of the lemma we reprove [GM09, Theorem 1.10] without using character theory. In particular, Lorimer's and O'Nan's results [O'N85] about the nonexistence of sharply 2–transitive sets of permutations in $P\Gamma L_k(q)$ $(k \geq 3)$ hold by simple counting arguments.

Theorem 7.9. *Let G be an automorphism group of a nontrivial symmetric design. Then the stabilizer in G of a point does not contain a subset which is sharply transitive on the remaining points. In particular, G does not contain a subset which is sharply 2–transitive on the points of the design.*

Proof. Let $v > k > \lambda$ be the usual parameters of the design. So the set Ω' of points of the design has size v, each block has size k, and two distinct blocks intersect in λ point. We will use the easy relation $(v-1)\lambda = k^2 - k$ (see any book on designs).

Fix $\omega \in \Omega'$, let G_ω be the stabilizer of ω in G, and suppose that $S \subseteq G_\omega$ is sharply transitive on the set $\Omega := \Omega' \setminus \{\omega\}$ of size $v-1$. As each point is contained in $k < v$ blocks, there is a block B with $\omega \notin B$. Apply Lemma 7.1 with $C = B$, so

$$\sum_{g \in S} |B \cap B^g| = |B|^2 = k^2.$$

Let a be the number of $g \in S$ with $B = B^g$. In the remaining $|S| - a = v - 1 - a$ cases we have $B \neq B^g$, hence $|B \cap B^g| = \lambda$.

We obtain $ak + (v-1-a)\lambda = k^2$. Recall that $(v-1)\lambda = k^2 - k$, so

$$a(k - \lambda) = k.$$

Now let B' be a block with $\omega \in B'$. Set $B = C = B' \setminus \{\omega\}$. Then $|B \cap B^g| = k-1$ or $\lambda - 1$. Let b be the frequency of the first case. As above we get $b(k-1) + (v - 1 - b)(\lambda - 1) = (k-1)^2$, which simplifies to

$$b(k - \lambda) = v - k.$$

We obtain:

$$(k-\lambda)^2 \text{ divides } k(v-k), \text{ and } k - \lambda \text{ divides } k + (v-k) = v.$$

On the other hand, the basic relation $(v-1)\lambda = k^2 - k$ is equivalent to $k(v-k) = (v-1)(k-\lambda)$, so $k - \lambda$ divides $v - 1$. Therefore $k - \lambda = 1$, hence $k = v - 1$ and we have the trivial design, contrary to our assumption. □

7.3. Remarks on M_{24}

In the last section, we make two remarks on the Mathieu group M_{24} of degree 24. First, we show that M_{24} cannot be the group of projectivities of a finite non-desarguesian projective plane. Second, we sketch a computer based proof showing that (7.1) has an integer solution for $G = M_{24}$ in its 2-transitive action.

The following result completes the solution of the conjecture in [Dem68, p. 160].

Theorem 7.10. *The group of projectivities of a non-desarguesian projective plane of finite order n contains the alternating group A_{n+1}.*

Proof. By [Gru88], we only have to exclude the case $n = 23$ and $P = M_{24}$. However, if this case would exist, then by [MN07, Lemma 2.2], M_{22} would contain the multiplication group of a loop, which contradicts Theorem 7.5. □

Now we present a computer based approach showing that (7.1) has an integer solution for $G = M_{24}$ in its permutation representation on $\Omega^{(2)}$ with $\Omega = \{1, \ldots, 24\}$. Thus the technique of Sections 2 and 3 cannot answer the question whether M_{24} contains sharply 2–transitive sets of permutations. As the tedious proofs of Lemmas 7.11, 7.12 and Theorem 7.13 are not directly related to the main goal of this chapter, we omit them.

For a subgroup $H \leq G$, we consider the following system (7.2) of linear equations:

> Let $\Omega_1, \Omega_2, \ldots, \Omega_r$ be the orbits of H on $\Omega \times \Omega$, and T be a set of representatives for the action of H on G by conjugation. For $i = 1, 2, \ldots, r$ and $g \in G$ set
>
> $$a_i(g) = |\{(\omega_1, \omega_2) \in \Omega_i | \omega_1^g = \omega_2\}|$$
>
> and consider the system of r linear equations in the variables x_g, $g \in T$:
>
> $$\sum_{g \in T} x_g a_i(g) = |\Omega_i|, \quad i = 1, 2, \ldots, r. \tag{7.2}$$

The system (7.1) is the same as the system (7.2) with $H = 1$. Furthermore, note that $a_i(g)$ depends only on the H–class of g, so the system of equations does not depend on the chosen system T of representatives.

Lemma 7.11. *Let $U \leq V \leq G$ be subgroups of G. If (7.2) has an integral solution for $H = U$, then (7.2) has an integral solution for $H = V$.*

Lemma 7.12. *Let $p^m > 1$ be a power of a prime p, and $R = \mathbb{Z}/p^m\mathbb{Z}$. Suppose that (7.2) has a solution in R for some p'–subgroup H of G. Then also (7.1) is solvable over R.*

The proof of Lemma 7.12 only uses that $|H|$ is a unit in R. So if (7.2) has a rational solution for some $H \leq G$, then (7.1) has a rational solution too. So the rational solubility of (7.1) can be decided by the rational solubility of (7.2) for $H = G$, which gives a very weak condition.

A useful criterion to decide whether (7.1) has an integral solution is

Theorem 7.13. *The following are equivalent:*

(i) The system (7.1) has an integral solution.

(ii) For each prime divisor p of $|G|$, the system (7.2) has an integral solution for some p'–subgroup H of G.

In order to apply this theorem to the action of $G = M_{24}$ on $\Omega^{(2)}$, we first choose a Sylow 2–subgroup H of G. So H is a p'–subgroup of G for each odd prime p. The number of H–orbits on G is 241871. So the number of unknowns is reduced by a factor $|G|/241871 = 1012.2\ldots$. The number of equations is 603. In order to solve this system, one can pick about 270 variables at random, and set the remaining ones to 0. Experiments with the computer algebra system Magma [BCP97] show that this system usually has an integral solution.

It remains to take a $2'$–subgroup of G. For this we let H be the normalizer of a Sylow 23–subgroup. Then $|H| = 253$. This reduces the number of unknowns from $|G| = 244823040$ by a factor of about 253 to 967692. Here, picking 520 unknowns at random usually gives an integral solution.

In both cases, the running time is a few minutes.

There are several modifications of this method. In (7.1) it suffices to consider the sum over the fixed-point-free elements and 1, and likewise in (7.2) (and the lemmas and the theorem), it suffices to consider 1 together with the H–orbits on fixed-poin-free elements. However, even under this assumption, (7.1) still has an integral solution. To do so, one simply sets $x_1 = 1$ and randomly picks the variables x_g for fixed-point-free elements g from T.

Also, Theorem 7.13 and Lemma 7.11 remain true if we replace 'integral' by 'non-negative integral'. So we are faced with an integer linear programming problem. Experiments have shown that (7.2) has a non-negative integral solution for each of the 29 subgroups H of $G = M_{24}$ with $[G : H] \leq 26565$.

dc_821_13

8. On the right multiplication groups of finite quasifields

The first question this chapter asks which finite transitive linear group can occur as right multiplication group of a finite quasifield. It turns out that some of the exceptional finite transitive linear groups may happen to be the right multiplication group of a quasifield. Since these groups are relatively small, in the second part of the chapter, we are able to give an explicit classification of all quasifields whose right multiplication group is an exceptional finite linear group. These results are obtained with computer calculations using the computer algebra system GAP4 [Gap] and the program CLIQUER [NÖ03].

Right multiplication groups of quasifields have not been studied intensively. The most important paper in this field is [Kal87] by M. Kallaher, containing results about finite quasifields with solvable right multiplication groups.

Finally, we notice that our results can be interpreted in the language of the theory of finite loops, as well. *Loops* arise naturally in geometry when coordinatizing point-line incidence structures. Most importantly, the multiplicative structure $(Q^*, \cdot)$ of Q is a loop. In fact, any finite loop $\hat{Q}$ gives rise to a quasifield, provided the right multiplication maps of $\hat{Q}$ generate a group which is permutation isomorphic to a subgroup of $GL(n, q)$, where the latter is considered as a permutation group on the nonzero vectors of $\mathbb{F}_q^n$. Therefore in this chapter, we investigate loops whose right multiplication groups are contained is some finite linear group $GL(n, q)$.

This chapter is almost identical with the paper [Nag13]. Theorem 8.17 supports the first part of **Thesis 4;** the second part follows from the equivalence of sharply transitive sets in $GL(n, p)$ and sharply 2-transitive sets in $AGL(n, p)$, cf. Section 1.8.

8.1. Translation planes, spreads and quasifields

In this section we give the definitions of concepts which are standard in the theory of translation planes. Moreover, we briefly explain the relations between the automorphisms of these mathematical objects.

Let Π be a finite projective plane. By the theorems of Skornyakov-San Soucie and Artin-Zorn [HP73, Theorem 6.18 and 6.20], Π is either Desarguesian or contains at most one translation line. This means that two finite translation planes are isomorphic if and only if the corresponding projective planes are.

The relation between translation planes and quasifields is usually explained using the notion of *(vector space) spreads.*

Definition 8.1. *Let V be a vector space over the field F. We say that the collection σ of subspaces is a spread if (1) $A, B \in \sigma$, $A \neq B$ then $V = A \oplus B$, and (2) every nonzero vector $x \in V$ lies in a unique member of σ. The members of σ are the components of the spread.*

If σ is a spread in V then André's construction yields a translation plane $\Pi(\sigma)$ by setting V as the set of points and the translates of the components of σ as the set of lines of the affine plane. Conversely, if Π is a finite translation plane with origin O then we identify the point set of Π with the group $\mathcal{T}(\Pi)$ of translations. As $\mathcal{T}(\Pi)$ is an elementary Abelian p-group, Π becomes a vector space over (some extension of) $\mathbb{F}_p$ and the lines through O are subspaces forming a spread $\sigma(\Pi)$.

André's construction implies a natural identification of the components of the spread with the parallel classes of the affine lines, and the points at infinity of the corresponding affine plane.

The approach by spreads has many advantages. For us, the most important one is that they allow explicit computations in the group of collineation of the translation plane. Let Π be a nondesarguesian translation plane and let us denote by $\mathcal{T}(\Pi)$ the group of translations of Π. The full group $\mathrm{Aut}(\Pi)$ of collineations contains $\mathcal{T}(\Pi)$ as a normal subgroup. Up to isomorphy, we can choose a unique point of origin O in Π. The stabilizer $\mathcal{C}_O(\Pi)$ of O in $\mathrm{Aut}(\Pi)$ is the *translation complement* of Π with respect to O. The full group $\mathrm{Aut}(\Pi)$ of collineations is the semidirect product of $\mathcal{T}(\Pi)$ and $\mathcal{C}_O(\Pi)$. In particular, $\mathcal{C}_O(\Pi)$ has the structure of a linear group of V. By [JJB07, Theorem 2.27], the collineation group $\mathcal{C}_O(\Pi)$ is essentially the same as the group of automorphisms of the associated spread, that is, there is a natural isomorphism between the two groups. The automorphism group of a spread is defined as follows.

Definition 8.2. *Let σ be a spread in the vector space V. The automorphism group* $\mathrm{Aut}(\sigma)$ *consists of the additive mappings of V that permutes the components of σ among themselves.*

As the translations act trivially on the infinite line, the permutation action of $\mathrm{Aut}(\sigma)$ is equivalent with the action of $\mathrm{Aut}(\Pi)$ on the line at infinity.

Spreads are usually represented by a spread set of matrices. Fix the components A, B of the spread σ with underlying vector space V. The direct sum decomposition $V = A \oplus B$ defines the projections $p_A : V \to A$, $p_B : V \to B$. As for any component $C \in \sigma \setminus \{A, B\}$ we have $A \cap C = B \cap C = 0$, the restrictions of p_A and p_B to C are bijections $C \to A$, $C \to B$. Therefore, the map $u_C : A \to B$, $xu_C = (xp_A^{-1})p_B$ is a linear bijection from A to B. When identifying A, B with $\mathbb{F}_p^k$, u_C can be given in matrix form U_C. The set $\mathcal{S}(\sigma) = \{U_C \mid C \in \sigma\}$ is called the *spread set of matrices representing σ relative to axes* (A, B). This representation depends on the choice of $A, B \in \sigma$. It is also possible to think at a spread set as the collection $\mathcal{S}'(\sigma) = \{u_D u_C^{-1} \mid D \in \sigma\}$ of linear maps $A \to A$, with fixed C.

A spread set $\mathcal{S} \subseteq \hom(A, B)$ can be characterized by the following property: For any elements $x \in A \setminus \{0\}$, $y \in B \setminus \{0\}$, there is a unique map $u \in \mathcal{S}$ such that $xu = y$. Indeed, if $\mathcal{S} = \mathcal{S}(\sigma)$ then $u = u_C$ where C is the unique component containing $x \oplus y$. Conversely, $\mathcal{S}$ defines the spread

$$\sigma(\mathcal{S}) = \{0 \oplus B, A \oplus 0\} \cup \{\{x \oplus xu \mid x \in A\} \mid u \in \mathcal{S}\}$$

with underlying vector space $V = A \oplus B$.

Definition 8.3. *The autotopism group of the spread set $\mathcal{S}$ of $k \times k$ matrices over F consists of the pairs $(T, U) \in GL(k, F) \times GL(k, F)$ such that $T^{-1}\mathcal{S}U = \mathcal{S}$.*

[JJB07, Theorems 5.10] says that autotopisms of spread sets relative to axes (A, B) and automorphism of spreads fixing the components A, B are essentially the same.

By fixing a nondegenerate quadrangle o, e, x, y, any projective plane can be coordinatized by a *planar ternary ring* (PTR), see [HP73]. Let Π be a translation plane and fix affine points o, e and infinite points x, y. Then, the coordinate PTR becomes a *quasifield.*

Definition 8.4. *The finite set Q endowed with two binary operations $+, \cdot$ is called a finite (right) quasifield, if*

(Q1) $(Q, +)$ is an Abelian group with neutral element $0 \in Q$,

(Q2) $(Q \setminus \{0\}, \cdot)$ is a loop,

(Q3) the right distributive law $(x + y)z = xz + yz$ holds, and,

(Q4) $x \cdot 0 = 0$ for each $x \in Q$.

The link between tranlation planes and quasifields can be extended to spread sets, as well. In fact, the set $\mathcal{S}(Q) = \{R_x \mid x \in Q\}$ of nonzero right multiplication maps of Q is a spread set relative to the infinite points of the x- and y-axes of the coordinate system. Collineations correspond to *autotopisms* of the quasifield.

Definition 8.5. *Let $(Q, +, \cdot)$ be a quasifield, $S, T, U : Q \to Q$ bijections such that S, U are additive and $0T = 0$. The triple (S, T, U) is said to be an autotopism of Q if for all $x, y \in Q$, the identity $xS \cdot yT = (x \cdot y)U$ holds.*

It is easy to see that the triple (S, T, U) is an autotopism of the quasifield Q if and only if the pair (S, U) is an autotopism of the associated spread set $\mathcal{S}(Q)$.

We summarize the above considerations in the next proposition.

Proposition 8.6. *Let Π be a translation plane, σ the associated spread. Let A, B be fixed components of σ and a, b the associated infinite points of Π. Let $\mathcal{S}$ be the spread set of σ relative to axes (A, B). Let c, d be arbitrary affine points of Π such that a, b, c, d are in general position, and let $(Q, +, \cdot)$ be the coordinate quasifield of Π with respect to the quadrilateral $abcd$. Then the following groups are isomorphic.*

1. *The autotopism group of* $\mathcal{S}$.
2. *The stabilizer subgroup of the components* A, B *in* $\mathrm{Aut}(\sigma)$.
3. *The stabilizer subgroup of the triangle* abc *in the full collineation group* $\mathrm{Aut}(\Pi)$.
4. *The autotopism group of* Q.

In particular, the structure of the autotopism group of the coordinate quasifield does not depend on the choice of the base points c, d.

8.2. Isotopy, parastrophy and computation

When investigating the isomorphism between translation planes, the *isotopy of quasifields* is a central concept. We borrow the concept of *parastrophy* from the theory of loops in order to define a wider class of equivalence for quasifields.

Definition 8.7. *Let* $\mathcal{S}, \mathcal{S}'$ *be spread sets of matrices in* $GL(d,p)$. *We say that* $\mathcal{S}, \mathcal{S}'$ *are*

1. *isotopes if there are matrices* $T, U \in GL(d,p)$ *such that* $T^{-1}\mathcal{S}U = \mathcal{S}'$ *holds.*
2. *parastrophes if there are matrices* $T, U \in GL(d,p)$ *such that* $T^{-1}\mathcal{S}U = \mathcal{S}'$ *or* $T^{-1}\mathcal{S}U = (\mathcal{S}')^{-1}$ *holds.*

Analogously, we say that the quasifields Q, Q' *are isotopic (parastrophic) if their sets of nonzero right multiplications of matrices are isotopic (parastrophic) as spread sets of matrices.*

In Section 8.1, we explained the method of obtaining the spread set $\mathcal{S}$ of matrices from the spread σ by fixing the components A, B. It follows that interchanging A and B, the resulting spread set of matrices will be $\mathcal{S}^{-1} = \{u^{-1} \mid u \in \mathcal{S}\}$. Hence, $\mathcal{S}$ and $\mathcal{S}^{-1}$ determine isomorphic translation planes. Taking into account [JJB07, Propositions 5.36 and 5.37], we obtain that parastrophic quasifields (or spread sets) determine isomorphic translation planes. On the one hand, the next proposition shows that the right multiplication group of a quasifield is parastrophy invariant. On the other hand, it will give us an effective method for the computation of parastrophy for quasifields with "small" right multiplication group.

Lemma 8.8. *Let* $\mathcal{S}_1, \mathcal{S}_2$ *be spread sets of matrices in* $GL(d,p)$. *Assume that* $1 \in \mathcal{S}_1, \mathcal{S}_2$ *and define the transitive linear groups* $G_1 = \langle \mathcal{S}_1 \rangle$ *and* $G_2 = \langle \mathcal{S}_2 \rangle$ *generated by the spread sets. If* (T, U) *defines a parastrophy between* $\mathcal{S}_1$ *and* $\mathcal{S}_2$ *then* $T^{-1}U \in \mathcal{S}_2$ *and* $T^{-1}G_1T = U^{-1}G_1U = G_2$. *In particular, if* $G_1 = G_2$ *then* $U, T \in N_{GL(d,p)}(G_1)$.

Proof. As $\langle \mathcal{S} \rangle = \langle \mathcal{S}^{-1} \rangle$, it suffices to deal with isotopes. Since $1 \in \mathcal{S}_1$, we have $T^{-1}U = T^{-1}1U \in \mathcal{S}_2$. Moreover, $T^{-1}\mathcal{S}_1T = T^{-1}\mathcal{S}_1U \cdot U^{-1}T = \mathcal{S}_2\, U^{-1}T \subseteq G_2$, which implies $T^{-1}G_1T = G_2$. The equation $U^{-1}G_1U = G_2$ follows from $T^{-1}U \in G_2$. □

We will use the above lemma to compute the classification of quasifields up to parastrophy.

Proposition 8.9. *Let $\mathcal{S}, \mathcal{S}'$ be spread sets of matrices in $GL(d,p)$. Assume that $1 \in \mathcal{S}, \mathcal{S}'$ and $G = \langle \mathcal{S} \rangle = \langle \mathcal{S}' \rangle$. Let G^*, G^{**} be the permutation groups acting on G, where the respective actions are the right regular action of G on itself, and the action of $N_{GL(d,p)}(G)$ on G by conjugation. Let ι be the inverse map $g \mapsto g^{-1}$ on G. Define the permutation group $G^\sharp = \langle G^*, G^{**}, \iota \rangle$ acting on G. Then, $\mathcal{S}, \mathcal{S}'$ are parastrophic if and only if they lie in the same $G^\sharp$-orbit.*

Proof. For any $U \in G$, $T \in N_{GL(d,p)}(G)$, the sets $T^{-1}\mathcal{S}T$, $\mathcal{S}U$ and $\mathcal{S}^{-1}$ are parastrophes of $\mathcal{S}$. Hence, if $\mathcal{S}, \mathcal{S}'$ are in the same $G^\sharp$-orbit then they are parastrophes. Conversely, assume that the pair (T,U) defines an isotopy between $\mathcal{S}$ and $\mathcal{S}'$. By Lemma 8.8, $\mathcal{S}' = T^{-1}\mathcal{S}T \cdot T^{-1}U$ where $T \in N_{GL(d,p)}(G)$ and $T^{-1}U \in G$, that is, they are in the same $G^\sharp$-orbit. The proof goes similarly for the case of parastrophy. □

In general, the explicit computation of the collineation group of a translation plane is very challenging. Another application of Lemma 8.8 is the computation of the autotopism group of a quasifield, that is, the computation of the stabilizer of two infinite points in the full collineation group of the corresponding translation plane.

Proposition 8.10. *Let $\mathcal{S}$ be a spread set of matrices in $GL(d,p)$ with $1 \in \mathcal{S}$ and $G = \langle \mathcal{S} \rangle$. Define the group*

$$H = \{(T,U) \in N_{GL(d,p)}(G)^2 \mid T^{-1}U \in G\}$$

and the permutation action $\Phi : G \times H \to G$ of H on G by

$$\Phi : (X, (T,U)) \mapsto T^{-1}XU.$$

Then, H and Φ are well defined. The isotopism group of $\mathcal{S}$ is the setwise stabilizer of $\mathcal{S}$ in H with respect to the action Φ.

Proof. In order to see that H is a group, take elements $(T,U), (T_1,U_1) \in H$. On the one hand, $(T^{-1})^{-1}U^{-1} = T(T^{-1}U)^{-1}T^{-1} \in TGT^{-1} = G$, which implies $(T^{-1}, U^{-1}) \in H$. On the other hand, $(TT_1, UU_1) \in H$ follows from

$$(TT_1)^{-1}UU_1 = T_1^{-1}(T^{-1}U)T_1 \cdot T_1^{-1}U_1 \in T_1^{-1}GT_1 \cdot G = G.$$

Since $T^{-1}XU = T^{-1}XT \cdot T^{-1}U \in G$ holds for all $X \in G$, H and Φ are well defined. The claim for the autotopism group of $\mathcal{S}$ follows from Lemma 8.8. □

As for an exceptional finite transitive linear group G, $N_{GL(d,p)}(G)$ is also exceptional, it is a small subgroup of $GL(d,p)$ and the autotopism group of $\mathcal{S}$ is computable by GAP4. Using Proposition 8.6, we obtain a straightforward method for computing the stabilizer of two infinite points of our translation planes. However,

the stabilizer of some infinite points is not an invariant of the translation plane in general.

More precisely, let Π be a translation plane with infinite line ℓ_∞ and $P = \{a_1, \ldots, a_t\} \subseteq \ell_\infty$ be a set of infinite points. Denote by $\mathcal{B}_P$ the pointwise stabilizer of P in $\mathrm{Aut}(\Pi)$. In the rest of this section we show that under some circumstances, the structure of $\mathcal{B}_P$ is an invariant of Π. We start with a lemma on general permutation groups.

Lemma 8.11. *Let G be a group acting on the finite set X (not necessarily faithfully). For any $Y \subseteq X$, we denoty by $F(Y)$ the pointwise stabilizer of Y. Let Y_1, Y_2 be subsets of X such that $|Y_1| = |Y_2| < |X|/2$, and suppose that $F(Y_i)$ acts transitively on $X \setminus Y_i$, $i = 1, 2$. Then, there is an element $g \in G$ with $Y_2^g = Y_1$. In particular, the subgroups $F(Y_1), F(Y_2)$ are conjugate in G.*

Proof. Up to the action of G on the orbit Y_2^G, we may assume that $|Y_1 \cap Y_2| \geq |Y_1 \cap Y_2^g|$ for all $g \in G$. Suppose that $Y_1 \neq Y_2$ and take elements $x \in X \setminus (Y_1 \cup Y_2)$, $y_1 \in Y_1 \setminus Y_2$, $y_2 \in Y_2 \setminus Y_1$. As $F(Y_i)$ acts transitively on $X \setminus Y_i$, there are elements $g_1 \in F(Y_1)$, $g_2 \in F(Y_2)$ such that $x^{g_1} = y_2$ and $x^{g_2} = y_1$. Put $h = g_1^{-1} g_2$. Then $h \in F(Y_1 \cap Y_2)$ and $y_2^h = y_1 \in Y_1$. This implies $|Y_1 \cap Y_2^h| > |Y_1 \cap Y_2|$, a contradiction. □

We can apply the lemma for the stabilizer of infinite points of a translation plane.

Proposition 8.12. *Let Π be a translation plane of order q, with infinite line ℓ_∞. For a subset $P \subseteq \ell_\infty$, let $\mathcal{B}_P$ denote the pointwise stabilizer subgroup in* $\mathrm{Aut}(\Pi)$. *Fix the integer $t \leq (q+1)/2$ and define the set*

$$\mathcal{D}_t = \{P \subseteq \ell_\infty \mid |P| = t \text{ and } \mathcal{B}_P \text{ act transitively on } \ell_\infty \setminus P\}.$$

Then, $\mathrm{Aut}(\Pi)$ *acts transitively on $\mathcal{D}_t$. In particular, the structure of $\mathcal{B}_P$ (as a permutation group on $\Pi \cup \ell_\infty$) does not depend on the particular choice $P \in \mathcal{D}_t$.* □

8.3. Sharply transitive sets and permutation graphs

Let G be a permutation group acting on the finite set Ω, $n = |\Omega|$ is the degree of G. The subset $S \subseteq G$ is a *sharply transitive set of permutations* if for any $x, y \in \Omega$ there is a unique element $\sigma \in S$ such that $x\sigma = y$. Sharply transitive sets can be characterized by the property $|S| = |\Omega|$ and, for all $\sigma, \tau \in S$, $\sigma\tau^{-1}$ is fixed point free. In particular, if $1 \in S$ then all $\sigma \in S \setminus \{1\}$ are fixed point free elements of G.

Definition 8.13. *Let G be a finite permutation group. The pair $\mathcal{G} = (V, \mathcal{E})$ is the permutation graph of G, where V is the set of fixed point free elements of G and the edge set $\mathcal{E}$ consists of the pairs (x, y) where $xy^{-1} \in V$.*

The set K of vertices is a *k-clique* if $|K| = k$ and all elements of K are connected. Sharply transitive subsets of G containing 1 correspond precisely the $(n-1)$-cliques of the permutation graph of G. Assume that the action of G on Ω is imprimitive and let Ω' be a nontrivial block of imprimitivity. Let S be a sharply transitive subset of G and define the subset $S' = \{\sigma \in S \mid \Omega'\sigma = \Omega'\}$ of S. Then, the restriction of S' to Ω' is a sharply transitive set on Ω'. We will call Σ' the *subclique corresponding to the block* Ω'.

For the connection between quasifields and sharply transitive sets of matrices see [JJB07, Chapter 8]. In our computations, we represent quasifields by the corresponding sharply transitive set of matrices, or, more precisely by the corresponding (maximal) clique of the permutation graph.

8.4. Finite transitive linear groups

In this section, we give an overview on finite transitive linear groups. The classification is due to C. Hering [Her74; Her85], and to M. W. Liebeck [Lie87a]. For self-contained lists and further details see [HB82, p. XII.7.5] or [JJB07, Theorem 69.7].

Let p be a prime, $V = \mathbb{F}_p^d$, and $\Gamma = GL(d,p)$. Let $G \leq \Gamma$ be a subgroup acting transitively on $V^* = V \setminus \{0\}$. Then $G_0 \trianglelefteq G \leq N_\Gamma(G_0)$, where we have one of the following possibilities for G and G_0:

1.a) $G \leq \Gamma\mathrm{L}(1, p^d)$. In particular, G is solvable.

1.b) $G_0 \cong \mathrm{SL}(d/e, p^e)$ with $2 \leq e \mid d$.

2) $G_0 \cong \mathrm{Sp}(d/e, p^e)$ with $e \mid d$, d/e even.

3) $p = 2$, $d = 6e > 6$, and G_0 is isomorphic to the Chevalley group $G_2(2^e)$. If $d = 6$ then G_0 is isomorphic to $G_2(2)'$. Notice that the Chevalley group $G_2(2)$ is not simple, its commutator subgroup has index two and the isomorphism $G_2(2)' \cong \mathrm{PSU}(3,3)$ holds.

4) There are 27 exceptional finite transitive linear groups, their structure is listed in Table 8.1. The information given in the last column can be used to generate the sporadic examples in the computer algebra systems GAP4 [Gap] in the following way. The split extension of G by the vector group $\mathbb{F}_p^d$ is 2-transitive, hence primitive, and can be loaded from the library of primitive groups using the command `PrimitiveGroup(`p^d`,`k`)`. As $59^2 > 2500$, case (4.i) is not included in this library, but since this group is regular on V^*, it will not be interesting from our point of view.

   We have seven sporadic transitive linear groups which are regular, these are denoted by an asterix. These groups have been found by Dickson and Zassenhaus, and they are also known as the right multiplication groups of the *Zassenhaus nearfields.*

Case	Cond. on p	Cond. on d	G_0	#	Primitive id. of $p^d : G$
(4.a)	$p = 5$	$d = 2$	$\mathrm{SL}(2,3)$	3	$15^*, 18, 19$
(4.b)	$p = 7$	$d = 2$	$\mathrm{SL}(2,3)$	2	$25^*, 29$
(4.c)	$p = 11$	$d = 2$	$\mathrm{SL}(2,3)$	2	$39^*, 42$
(4.d)	$p = 23$	$d = 2$	$\mathrm{SL}(2,3)$	1	59^*
(4.e)	$p = 3$	$d = 4$	$\mathrm{SL}(2,5)$	4	$124, 126, 127, 128$
(4.f)	$p = 11$	$d = 2$	$\mathrm{SL}(2,5)$	2	$56^*, 57$
(4.g)	$p = 19$	$d = 2$	$\mathrm{SL}(2,5)$	1	86
(4.h)	$p = 29$	$d = 2$	$\mathrm{SL}(2,5)$	2	$106^*, 110$
(4.i)	$p = 59$	$d = 2$	$\mathrm{SL}(2,5)$	1	(no id)*
(4.j)	$p = 3$	$d = 4$	2^{1+4}	5	$71, 90, 99, 129, 130$
(4.k)	$p = 2$	$d = 4$	A_6	2	$16, 17$
(4.l)	$p = 2$	$d = 4$	A_7	1	20
(4.m)	$p = 3$	$d = 6$	$\mathrm{SL}(2,13)$	1	396

Table 8.1.: Exceptional finite transitive linear groups

In this chapter, without mentioning explicitly, we consider all finite linear groups as a permutation group acting on the nonzero vectors of the corresponding linear space.

8.5. Non-existence results for finite right quasifields

In this section, let $(Q, +, \cdot)$ be a finite right quasifield of order p^d with prime p. Write $G = \mathrm{RMlt}(Q^*)$ for the right multiplication group of Q. As in Section 8.4, we denote by G_0 a characteristic subgroup of G. Moreover, we denote by S the set of nontrivial right multiplication maps of Q. Then $1 \in S$ and S is a sharply transitive set of permutations in G. We write $\mathcal{G} = (V, \mathcal{E})$ for the permutation graph of G. Remember that $|S| = p^d - 1$ and $S \setminus \{1\}$ is a clique of size $p^d - 2$ in $\mathcal{G}$.

Proposition 8.14. *Assume that G is a transitive linear group belonging to the infinite classes (1)-(3). Then one of the following holds:*

1. $G \leq \Gamma\mathrm{L}(1, p^d)$.
2. $G \triangleright \mathrm{SL}(d/e, p^e)$ *for some divisor $e < d$ of d.*
3. *p is odd and $G \triangleright \mathrm{Sp}(d/e, p^e)$ for some divisor e of d.*

Proof. We have to show that if $p = 2$ then the cases $G_0 \cong \mathrm{Sp}(d/e, p^e)$ and $G_0 \cong G_2(2^e)'$ are not possible. Recall that the transitive linear group $G_2(2^e)$ is a subgroup of $\mathrm{Sp}(6, 2^e)$. The impossibility of both cases follow from [MN11, Theorem 1]. □

Case	p^d	G_0	Orders (primitive id.)
(4.a)	5^2	$\mathrm{SL}(2,3)$	48 (18), *96 (19)*
(4.b)	7^2	$\mathrm{SL}(2,3)$	144 (29)
(4.c)	11^2	$\mathrm{SL}(2,3)$	240 (42)
(4.e)	3^4	$\mathrm{SL}(2,5)$	960 (128)
(4.f)	11^2	$\mathrm{SL}(2,5)$	*600 (57)*
(4.g)	19^2	$\mathrm{SL}(2,5)$	1080 (86)
(4.h)	29^2	$\mathrm{SL}(2,5)$	1680 (110)
(4.l)	2^4	A_7	2520 (20)

Table 8.2.: Exceptional transitive linear groups as right multiplication groups

Proposition 8.15. *If G is an exceptional finite transitive linear group, then it is either a regular linear group or one of those in Table 8.2.*

This proposition is proved in several steps.

(5.1) G cannot be an exceptional transitive linear group of type (4.k) and (4.m).

Computer proof. Assume G of type (4.k) and $G_0 \cong A_6$. Since $A_6 \cong Sp(4,2)' \leq Sp(4,2)$ as permutation groups on $\mathbb{F}_2^4$, [MN11, Theorem 1] applies.

Assume G of type (4.m). Let W be a Sylow 7-group of G and $H = N_G(W)$. Then $|H| = 28$ and H has orbits of length 28. One can find H-orbits A, B of size 28 such that $|A \cap B^g| \in \{0, 6\}$ for all $g \in G$. Again by [MN11, Lemma 2], G does not contain a sharply transitive set of permutations. □

(5.2) G cannot be an exceptional transitive linear group of type (4.e) and order 240 or 480.

Computer proof. We proceed similarly to the cases in (5.1). Assume G of type (4.e) and $|G| \in \{240, 480\}$. Let H be the normalizer of a Sylow 5-group in G. Then $|H| = 40$ and H has orbits A, B of length 40 such that $|A \cap B^g| \in \{0, 24\}$ for all $g \in G$. This proves the claim by [MN11, Lemma 2] with $p = 3$. □

Beside the finite regular linear groups, the remaining exceptional transitive linear groups are those of type (4.j), that is, when G_0 is the extraspecial group E_{32}^+ of order 2^5. In this class, there are five groups, three of them are solvable. The cases of the three solvable group of type (4.j) were left unsolved by M. Kallaher [Kal87], as well. The computation is indeed very tedious even with today's hardware and software.

The construction of the groups of type (4.j) is as follows. Up to conjugacy, $GL(4,3)$ has a unique subgroup L_0 of order 2^5 which is isomorphic to the extraspecial 2-group E_{32}^+, cf. [Hup67, Satz V.16.14.]. The normalizer $L = N_{GL(4,3)}(L_0)$ has order 3840. L has five transitive linear subgroups containing L_0; the orders are

$160, 320, 640, 1920, 3840$. Clearly, it suffices to prove the nonexistence of 79-cliques for the permutation graph of L only.

The action of L is not primitive; it has blocks of imprimitivity of size $2, 8$ and 16. These blocks are unique up to the action of L.

(5.3) Let A be a block of L of size 16. Let K be a 15-clique corresponding to A and assume that the group $\langle K \rangle$ generated by K is not a 2-group. Then, K cannot be extended to a 79-clique of L.

Computer proof. Let A be a block of size 8. Denote by H the setwise stabilizer of A in L; H stabilizes another block B of size 8 and $A \cup B$ is a block of size 16. Let $\mathcal{A}$ be the set of all 7-cliques corresponding to the block A. As $N_L(H)$ operates on the permutation (sub)graph of H, it also acts on $\mathcal{A}$; let $\mathcal{A}_0$ be a set of orbit representatives. We use [Soi12] to compute $\mathcal{A}_0$; $|\mathcal{A}_0| = 98$. Then in all possible ways, we extend the elements of $\mathcal{A}_0$ to 15-cliques corresponding to the block $A \cup B$, let $\mathcal{B}$ denote the set of extended cliques. Finally, we filter out the 15-cliques generating a non-2-group and show that none of them can be extended to a 79-clique. □

We have to deal with subcliques generating a 2-group. An important special case is the following.

(5.4) Up to conjugacy in L, there is a unique 15-clique K^* corresponding to an imprimitivity block of size 16 such that the setwise stabilizer in L has order 192. K^* has the further properties:

1. The subgroup $\langle K^* \rangle$ has order 32.
2. $\langle K^* \rangle$ interchanges two blocks of size 16 and fixes the other three.

Computer proof. Let S be a Sylow 2-subgroup of L. Using [Soi12], one can compute all 15-cliques of the permutation graph of S. Up to conjugacy in S, there are 17923 such cliques, only one of them has stabilizer of size 192. The properties of K^* are obtained by computer calculations. □

(5.5) Let A be a block of L of size 16. Let K be a 15-clique corresponding to A and assume that the group $\langle K \rangle$ generated by K is a 2-group. Then, K cannot be extended to a 79-clique of L.

Computer proof. Let S be a Sylow 2-subgroup of L. S leaves a block of size 16, say A, invariant. We compute the set $\mathcal{A}$ of S-orbit representatives of the 15-cliques of the permutation graph of S. $\mathcal{A}$ contains precisely one element conjugate to K^*, in fact, we assume that $K^* \in \mathcal{A}$.

For all elements $K \in \mathcal{A} \setminus \{K^*\}$, the computer shows within a few seconds that K cannot be extended to a 79-clique. For K^*, the direct computation takes too long, we therefore give a theoretical proof. Let us assume that D is a clique of size 79 in

type	# of cliques	up to parastrophy	proper G	# CCFPs'
(4.a)	4; 8	2; 3	1; 0	1; 0
(4.b)	12	4	2	2
(4.c)	16	4	3	3
(4.e)	27648	32	21	20
(4.f)	6	2	0	0
(4.g)	9	3	3	3
(4.h)	64	9	8	8
(4.l)	450	2	2	1

Table 8.3.: Maximal cliques in exceptional transitive linear groups

the permutation graph of L. We may assume that all subcliques of D corresponding to 16-blocks are conjugate of K^*.

Denote by D_A the subclique of D of size 15, corresponding to A. By (5.4), $\langle D_A \rangle$ interchanges two 16-blocks, say B, B', and leaves the others invariant. Denote by D_B the subclique of D, corresponding to B. Clearly, $D_A \neq D_B$. As $\langle D_B \rangle$ leaves three blocks invariant, there is a 16-block C which is invariant under all elements of $D_A \cup D_B$. However, as $|C| = 16$, D cannot have more than 15 elements mapping C to C, a contradiction to $|D_A \cup D_B| > 15$. □

The claims (5.3), (5.4) and (5.5) imply the following result.

(5.6) G cannot be an exceptional transitive linear group of type (4.j).

The combination of the claims (5.1), (5.2) and (5.6) yields the proof of the Proposition 8.15.

8.6. Exhaustive search for cliques and their invariants

Let $G \leq GL(d, p)$ be a transitive linear group. We use the program CLIQUER [NÖ03] to compute all cliques of size $p^d - 1$ in the permutation graph $\mathcal{G}$ of G. For the exceptional transitive linear groups of Table 8.1, the result is presented in the second column of Table 8.3. Proposition 8.9 allows us to reduce our results on cliques in exceptional transitive linear groups modulo parastrophy, as shown in the third column of Table 8.3. In column 4, we filtered out those cliques which do not generate the whole group G.

In the final step, we compute the *Conway-Charnes fingerprint* of all spread sets of matrices, cf. [CD98; MR95]. The Conway-Charnes fingerprint is an invariant of the translation plane which can be easily computed from any spread set of matrices.

Definition 8.16. *Given a spread set $\mathcal{S} = \{U_1, \ldots, U_{q-1}\}$ of nonzero matrices, one forms a $(q-1) \times (q-1)$ matrix whose (i,j) entry is 0, $+1$ or -1 according as $\det(U_i - U_j)$ is zero, square or nonsquare, respectively. Border this matrix with a leading row and column of 1s (except for the first entry on the diagonal which remains zero) to form a symmetric $q \times q$ matrix A with 0 on the diagonal, and ± 1 in every non-diagonal entry. Finally, form the matrix $F = AA^t$ (with the product being taken in the rational numbers). The fingerprint of the spread set is the multiset of the absolute values of the entries of F.*

The last column of Table 8.3 contains the number of different Conway-Charnes fingerprints of the spread sets of matrices in the corresponding exceptional transitive linear group G. One sees that only for two pairs of spread sets do we obtain the same fingerprint.

Let us denote by Q_1, Q_1' the quasifields of order 3^4 and by Q_2, Q_2' those of order 2^4. We compute the corresponding autotopism groups $\mathcal{A}_1, \mathcal{A}_1'$ and $\mathcal{A}_2, \mathcal{A}_2'$. GAP4 shows that $\mathcal{A}_1$ and $\mathcal{A}_1'$ are nonisomorphic groups of order 640, acting transitively on the 80 points of $\ell_\infty \setminus \{(0), (\infty)\}$. By Proposition 8.12, Q_1, Q_1' determine nonisomorphic translation planes. $\mathcal{A}_2$ and $\mathcal{A}_2'$ are both isomorphic to $\mathrm{PSL}(2,7)$. Both groups fix a third point a, a' of the infinite line and act transitively on the remaining 14 infinite points. Hence, both groups are the stabilizer of a triple of infinite points and Proposition 8.12 applies. As the orbit lengths of $\mathcal{A}_2$ and $\mathcal{A}_2'$ are different, we can conclude that the two translation planes are nonisomorphic.

8.7. Right multiplication groups of finite right quasifields

We compile our results in the following theorem.

Theorem 8.17. *Let $(Q, +, \cdot)$ be a finite right quasifield of order p^d with prime p. Then, for $G = \mathrm{RMlt}(Q^*)$, one of the following holds:*

1. *$G \leq \Gamma\mathrm{L}(1, p^d)$ and the corresponding translation plane is a generalized André plane.*
2. *$G \rhd \mathrm{SL}(d/e, p^e)$ for some divisor $e < d$ of d with $e \neq d$.*
3. *p is odd and $G \rhd \mathrm{Sp}(d/e, p^e)$ for some divisor e of d.*
4. *$p^d \in \{5^2, 7^2, 11^2, 17^2, 23^2, 29^2, 59^2\}$ and G is one of the seven finite sharply transitive linear groups of Zassenhaus [Zas35]. The corresponding translation planes are called Zassenhaus nearfield planes.*
5. *$p^d \in \{5^2, 7^2, 11^2\}$, and G is a solvable exceptional transitive linear group. These quasifields and the corresponding translation planes have been given by M. J. Kallaher [Kal87].*

6. $p^d = 3^4, 19^2$ *or* 29^2*, and the number of translation planes is* 21, 3 *or* 8*, respectively.*

7. $p^d = 16$ *and* $G = A_7$*. The corresponding translation planes are the Lorimer-Rahilly and Johnson-Walker planes.*

Proof. By Proposition 8.14, (1), (2) or (3) holds if G belongs to one of the infinite classes of finite transitive linear groups. If $G \leq \Gamma\mathrm{L}(1, p^d)$ then the corresponding translation plane is a generalized André plane by [Kal87, Theorem 3.1]. (Here the concept of generalized André planes includes the so called *regular nearfield planes,* see [JJB07, Section 8.1].) The cases of the Zassenhaus nearfield planes are in (4). The arguments in Sections 8.5 and 8.6 imply (6) and that there are two quasifields having A_7 as right multiplication group. Moreover, the corresponding translation planes are nonisomorphic. [JK82, Corollary 4.2.1] implies that the two translation planes are the Lorimer-Rahilly and Johnson-Walker planes. □

We close this chapter with two remarks.

1. No quasifield Q is known to the author with $\mathrm{RMlt}(Q^*) \triangleright \mathrm{Sp}(d/e, p^e)$. Even the smallest case of $\mathrm{Sp}(4, 3)$ is computationally challenging.

2. The Lorimer-Rahilly and Johnson-Walker translation planes are known to be polar to each other, that is, one spread set of matrices is obtained by transposing the matrices in the other spread set. (See [JJB07, (29.4.4)].)

The GAP programs used in this chapter are avaible on the author's web page:

`http://www.math.u-szeged.hu/~nagyg/pub/rightmlt.html`

dc_821_13

9. On the multiplication groups of finite semifields

In this chapter, we investigate the following problem: Let G be a finite permutation group on the set Q. Is there a loop operation $x \cdot y$ on Q such that $\mathrm{Mlt}(Q) \leq G$? In particular, we are interested in the cases where G is a projective linear group or a big Mathieu group. Concerning this question, the most general results are due to A. Vesanen [Ves95] and A. Drápal [Drá02], who showed that (a) if $\mathrm{Mlt}(Q) \leq P\Gamma L(2,q)$ ($q \geq 5$), then Q is a cyclic group, and, (b) the answer is negative for the groups $PSp(2n,q)$ ($n \geq 2$), $PU(n,q^2)$ ($n \geq 6$), $PO(n,q)$ ($n \geq 7$ odd), and $PO^{\varepsilon}(n,q)$ ($n \geq 7-\varepsilon$ even). Recall that for the loop Q of units of $\mathbb{O}(\mathbb{F}_q)$ modulo the center, $\mathrm{Mlt}(Q) = P\Omega^{+}(8,q)$.

In [Cam03, Problem 398], A. Drápal asked the above question in the following formulation: Given $n \geq 3$ and a prime power q, does there exist a normalized Latin square such that for the group G generated by the rows and the columns, $PSL(k,q) \leq G \leq P\Gamma L(k,q)$ holds? We answer this question affirmatively when $q^n > 8$. Our construction uses multiplicative loops of semifields and it is unique in the the following sense. Let Q be a finite loop such that $PSL(n,q) \leq M(Q) \leq PGL(n,q)$. Then there is a semifield $\mathbb{S}$ with center $\mathbb{F}_q$ and dimension n over $\mathbb{F}_q$ such that $Q \cong \mathbb{S}^*/Z(\mathbb{S}^*)$.

The results of this chapter have been published in the paper [Nag10]. Theorem 9.4 supports **Thesis 5.** These results had an impact to the following papers:

1) In [Ves13], Vesanen sharpens Theorem 9.4 by showing that the group $PSL(n,q)$ in its natural permutation representation is the multiplication group of a loop if and only if $n \geq 3$, $(n,q) \neq (3,2)$, and $\gcd(n, q-1) = 1$.

2) In [HL12], Hiss and Lübeck investigates finite 2-transitive groups occuring as multiplication groups of quasigroups. They refer to our loop construction in Table 9.1, to Theorem 9.4 and Proposition 9.6 concerning M_{23}. Moreover, they compare their algorithm to our computer algebra methods.

9.1. Finite semifields with large multiplication groups

Using the computer algebra software GAP4 [Gap], the followsing result can easily be checked:

Lemma 9.1. *No exceptional finite transitive linear group can be the group of multiplications of a finite loop.* □

Proposition 9.2. *Let $\mathbb{S}$ be a finite semifield of dimension n over its center $\mathbb{F}_q$. Let G be the group of multiplications of the multiplicative loop $\mathbb{S}^*$. Then $SL(n,q) \leq G \leq GL(n,q)$.*

Proof. Let the socle G_0 of G be $SL(n_0,r)$, $Sp(n_0,r)$ or $G_2(r)$. Then $G \leq \Gamma L(n_0,r)$ and $\mathbb{F}_r$ is a normal subfield of $\mathbb{S}$. The generalized Cartan-Brauer-Hua theorem ([Gru83, Lemma 1.1]) implies that $\mathbb{F}_r$ is central in $\mathbb{S}$, hence $r = q$, $n_0 = n$ and $G \leq GL(n,q)$. Let us assume that $G_0 = Sp(n,q)$ or $G_0 = G_2(q)$. In the latter case $n = 6$ and q is even, hence $G_2(q) < Sp(6,q)$. Indeed, for q even, the 6-dimensional representation of the exceptional Lie group $G_2(q)$ is constructed from its natural 7-dimensional orthogonal representation by using the isomorphism $O(7,q) \cong Sp(6,q)$, cf [Tay92, Theorem 11.9]. Thus, in both cases, the multiplication group of the central factor loop $Q = \mathbb{S}^*/Z(\mathbb{S}^*)$ is contained in $PSp(n,q)$. This contradicts [Ves95, Theorem S]. □

Proposition 9.3. *Let $n \geq 3$ be an integer and q a prime power such that $q^n > 8$. Then, there is a semifield $\mathbb{S}$ such that the multiplication group G of $\mathbb{S}^*$ satisfies $SL(n,q) \leq G \leq GL(n,q)$.*

Proof. By Proposition 9.2, we only have to present a semifield which has dimension n over its center $\mathbb{F}_q$. We distinguish between three cases: (1) $q \geq 3$, (2) $q = 2$ and n is odd, and (3) $q = 2$ and n is even.

In case (1), we can use Albert's twisted fields [Alb61]. Let F be the finite field $\mathbb{F}_{q^n}$. Let $\theta : x \mapsto x^q$ and $\sigma : x \mapsto x^{q^{n-1}}$ be automorphisms of F and $c \in F$ such that $c = x^{q-1}$ has no solution in F. As in [Alb61], the semifield $\mathbb{S} = (F, +, *)$ is defined using the quadruple (F, θ, σ, c) . As $n \geq 3$, $\theta \neq \sigma$ and we can use [Alb61, Theorem 1] to deduce that the center of $\mathbb{S}$ is $\mathbb{F}_q$.

In case (2), we construct a proper binary semifield $\mathbb{S} = (F, +, *)$ of Knuth's type from the fields $F = \mathbb{F}_{2^n}$, $F_0 = \mathbb{F}_2$ and F_0-linear map $f : F \to F_0$. As in [Knu65a, Section 2], we first define $x \circ y = xy + (f(x)y + f(y)x)^2$ and put $x * y = (x/1) \circ (y/1)$ where $x/1$ is given by $(x/1) \circ 1 = x$. Let z be a nonzero element of $Z(\mathbb{S}, +, *)$. Then $(x \circ 1) * ((y \circ 1) * z) = ((x \circ 1) * (y \circ 1)) * z$ implies

$$x \circ (y \circ z/1)/1 = (x \circ y)/1 \circ z/1.$$

We define the maps $\alpha, \beta : \mathbb{S} \to \mathbb{S}$ by

$$\alpha(u) = (u \circ z/1)/1, \qquad \beta(u) = u/1 \circ z/1.$$

Then the above equation has the form

$$x \circ \alpha(y) = \beta(x \circ y),$$

and the triple $(\mathrm{id}, \alpha, \beta)$ defines an autotopism of the pre-semifield $(F, +, \circ)$. By [Knu65a, Theorem 6], $\alpha(u) = z'u$ for some $z' \in F_0$. As $\alpha \neq 0$, this implies $z' = 1$ and $\alpha = \mathrm{id}$. Thus,

$$\begin{aligned} u \circ 1 = \alpha(u) \circ 1 = u \circ z/1 &\implies 1 = z/1 \\ &\implies z = 1 \circ 1 = 1 + (2f(1))^2 = 1. \end{aligned}$$

Hence, $Z(\mathbb{S})$ consists of 0 and 1.

In case (3), put $F = \mathbb{F}_{2^{n/2}}$ and pick elements $f, g \in F$ such that $y^3 + gy + f \neq 0$ for all $y \in F$. Define the multiplication on $\mathbb{S} = F + \lambda F$ by

$$(a + \lambda b)(c + \lambda d) = (ac + b^\sigma d^{\tau^2} f) + \lambda(bc + a^\sigma d + b^\sigma d^\tau g),$$

where $x^\sigma = x^2$ and $\tau = \sigma^{-1}$. As $n \geq 4$, $\sigma \neq \mathrm{id}$ and by [Knu65b, Section 7.4], $\mathbb{S}$ is a semifield with unit element $1 = 1 + \lambda \cdot 0$. Assume that $a + \lambda b \in Z(\mathbb{S})$. If $c \in F$ such that $c^\sigma \neq c$ then

$$ac + \lambda(bc) = (a + \lambda b)c = c(a + \lambda b) = ac + \lambda(c^\sigma b) \iff b = 0.$$

Furthermore,

$$\lambda a = a\lambda = \lambda a^\sigma \iff a = a^\sigma \iff a \in \mathbb{F}_2.$$

This shows $Z(\mathbb{S}) = \mathbb{F}_2$. □

Remarks: It is an easy exercise to show that a semifield cannot have dimension 2 over its center. Moreover, it is also easy to see that no proper semifield of order 8 exists.

9.2. The main result on multiplication groups of semifields

The first part of the following theorem gives a general affirmative answer to Drápal's problem. The second part of the theorem is a partial converse of our construction based on semifields. The proof of this part is basically contained in the proof of [Ves95, Theorem S]. However, as it is not formulated in this way, we present a self-contained proof, using a slightly different notation.

Theorem 9.4. *(a) For any integer $n \geq 3$ and prime power q with $q^n > 8$, there is a loop Q such that $PSL(n, q) \leq \mathrm{Mlt}(Q) \leq PGL(n, q)$.*

(b) Let Q be a loop such that $\mathrm{Mlt}(Q) \leq PGL(n, q)$ with $n \geq 3$. Then there is a semifield $\mathbb{S}$ of dimension n over its center $\mathbb{F}_q$ such that $Q \cong \mathbb{S}^*/Z(\mathbb{S}^*)$.

Proof. Part (a) follows immediately from Proposition 9.2 and 9.3. Let Q be a loop with multiplication group $G = \mathrm{Mlt}(Q) \leq PGL(n, q)$. We simply put $F = \mathbb{F}_q$ and write the elements of $Q = PG(n-1, q)$ in the form xF with $x \in F^n \setminus \{0\}$. Let

us denote the unit element of Q by eF. For any element xF, the left and right translations L_{xF}, R_{xF} are represented by $n \times n$ matrices over F and we assume $L_{eF} = R_{eF} = I$. We have

$$(xF) \cdot (yF) = (xR_{yF})F = (yL_{xF})F,$$

and for all vectors x, y there is a unique nonzero scalar $c_{x,y}$ with

$$xR_{yF} = yL_{xF} \cdot c_{x,y}. \tag{9.1}$$

Clearly, $c_{\lambda x,y} = \lambda c_{x,y}$ holds. For any x, y, z with $x + y \neq 0$, the following yields:

$$zL_{(x+y)F} \cdot c_{x+y,z} = (x+y)R_{zF} = xR_{zF} + yR_{zF} = zL_{xF} \cdot c_{x,z} + zL_{yF} \cdot c_{y,z}.$$

Let us now fix the elements x, y with $x + y \neq 0$ and define the matrices

$$U = L_{(x+y)F}L_{xF}^{-1}, V = L_{yF}L_{xF}^{-1}$$

and the scalars

$$\alpha(z) = \frac{c_{x,z}}{c_{x+y,z}}, \beta(z) = \frac{c_{y,z}}{c_{x+y,z}}.$$

By [Ves95, Lemma A], $\alpha(z)$ and $\beta(z)$ are nonzero constants; in particular, $\alpha(z) = \alpha(e)$ and $\beta(z) = \beta(e)$. Thus, for any $x, y \in F^n \setminus \{0\}$ with $x + y \neq 0$, we have

$$L_{(x+y)F} \cdot c_{x+y,e} = L_{xF} \cdot c_{x,e} + L_{yF} \cdot c_{x,e}. \tag{9.2}$$

Let us now consider the set

$$\mathfrak{L} = \{0\} \cup \{\alpha L_{xF} \mid \alpha \in F^*, x \in F^n \setminus \{0\}\}$$

of matrices. $\mathfrak{L}$ is closed under addition. Indeed, for fixed nonzero scalars α, β and vectors x, y, there are unique scalars λ, μ in F such that $c_{\lambda x,e} = \alpha$, $c_{\mu y,e} = \beta$. Then either $\alpha L_{xF} + \beta L_{yF} = 0 \in \mathfrak{L}$ or by (9.2),

$$\alpha L_{xF} + \beta L_{yF} = c_{\lambda x,e}L_{xF} + c_{\mu y,e}L_{yF} = c_{\lambda x+\mu y,e}L_{(\lambda x+\mu y)F} \in \mathfrak{L}.$$

We make the vector space $V = F^n$ into a semifield in the following way. Denote by T_x the element $c_{x,e}L_{xF}$ of $\mathfrak{L}$. Then by (9.1),

$$eT_x = eL_{xF} \cdot c_{x,e} = xR_{eF} = x.$$

For $x, y \in V$, define $x \circ y = yT_x$.

Claim 1: $(V \setminus \{0\}, \circ)$ is a loop with unit element e.

Clearly, T_e is the identity matrix, hence $e \circ x = xT_e = x$. $x \circ e = eT_x = x$ by definition. The equation $x \circ y = z$ has a unique solution $y = zT_x^{-1}$ in y. Let us fix nonzero vectors y, z and take an element $x_0 \in V$ such that $(x_0F)(yF) = zF$, that is, $yL_{x_0F} = \alpha z$ for some $\alpha \in F$. Then $\alpha^{-1} = c_{\lambda x_0,e}$ for some nonzero scalar λ. With $x = \lambda x_0$, we have $T_x = \alpha^{-1}L_{x_0F}$ and $z = yT_x = x \circ y$.

Claim 2: $(V, +, \circ)$ is a semifield.

Since the left multiplication maps of V are the T_x's, we have left distributivity. Moreover, as $\mathfrak{L}$ is closed under addition, for any $x, y \in V$ there is a unique z such that $T_x + T_y = T_z$. Applying both sides to e, we obtain $z = x + y$. Therefore,

$$(x + y) \circ z = zT_{x+y} = z(T_x + T_y) = zT_x + zT_y = x \circ z + y \circ z.$$

Claim 3: The loop Q is the central factor of V.

Let I denote the identity matrix on V. Then for all $\alpha \in F$, $\alpha I = T_{\alpha e} \in \mathfrak{L}$. Using a trick as above, one can show that $T_{\lambda x} = \lambda T_x$, which implies that $(\lambda x) \circ y = \lambda(x \circ y)$. This means that the right multiplication maps are in $GL(V)$, as well. In particular, the multiplication maps corresponding to the elements λe are centralized by all left and right multiplication maps, thus, $\lambda e \in Z(V)$ for all $\lambda \in F$. By

$$(x \circ y)F = (yT_x)F = (yL_{xF})F = (xF)(yF),$$

the map $\varphi : x \to xF$ is a surjective loop homomorphism. The kernel of φ consists of the elements λe, thus, $\ker \varphi$ is central in V. Since $PSL(n, q) \leq \mathrm{Mlt}(Q)$ acts primitively, Q is a simple loop and the kernel K of the homomorphism is a maximal normal subloop. This proves that $\ker \varphi = Z(V^*)$. □

9.3. Mathieu groups as multiplication groups of loops

In [Drá02], A. Drápal made some remarks on the question whether the Mathieu group can occur as multiplication groups of loops. As noted, there it is rather straigthforward to show that the small Mathieu groups M_{10}, M_{11} are not the multiplication groups of loops. Moreover, extensive computer calculation showed that the same holds for the big Mathieu groups M_{22} and M_{23}. For M_{22}, the computation was independently repeated in [MN07]. Later we proved the result on M_{22} be theoretical argument; in fact it follows from Theorem 7.5. Moreover, we performed an independent verification on M_{23} which gave the same result as Drápal had.

The computation was implemeted in the computer algebra GAP4 [Gap]. In order to reduce the CPU time we used some tricks. First of all, let L be an $n \times n$ normalized Latin square and let $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_n\}$ be the permutations defined by the rows and columns of L, in order. Then $a_1 = b_1 = \mathrm{id}$, $1^{a_i} = 1^{b_i} = i$ and $a_i b_j a_i^{-1} b_j^{-1}$ leaves 1 fixed. Conversely, assume that A, B are sets of permutations of degree n such that

(T1) $\mathrm{id} \in A, B$,

(T2) for all $i \in \{1, \ldots, n\}$ there are unique elements $a \in A$, $b \in B$ such that $i = 1^a = 1^b$, and,

(T3) for all $a \in A$, $b \in B$, $aba^{-1}b^{-1}$ leaves 1 fixed,

then a normalized Latin square can be constructed such that the rows and columns of L determine the elements of A and B. Indeed, for any $i, j \in \{1, \ldots, n\}$, the jth element of the ith row will be j^a, where a is the unique element of A with $1^a = i$.

Let A, B be sets of permutations of degree n satisfying (T1)-(T3) and put $G = \langle A, B \rangle$. Then, the following pairs of sets satisfy (T1)-(T3) as well:

(a) B, A;

(b) A^h, B^h, where $h \in G_1$;

(c) Au^{-1}, uBu^{-1}, where $u \in A$;

(d) vAv^{-1}, Bv^{-1}, where $v \in B$.

This implies the following

Lemma 9.5. *Let L be a Latin square of order n and assume that the rows and columns generate the group G. Let a be an arbitrary row of L. Then for any $a^* \in a^G \cup (a^{-1})^G$ there is a Latin square L^* such that a^* is a row of L^* and the rows and columns of L^* generate G.*

Proof. Let A, B denote the sets of permutations given by the rows and columns of L. If $a^* = a^{-1}$ then define L^* from the sets $A^* = Aa^{-1}, B^* = aBa^{-1}$. Thus, it suffices to deal with the case $a^* = a^g$. We can write $g = hv^{-1}$ where $h \in G_1$, $v \in B$. The sets A^h, B^h determine a Latin square L^h such that a^h is a row of L^h. This means that we can assume that $a^* = vav^{-1}$ where $u \in A$. It follows from (d) that vAv^{-1}, Bv^{-1} determines a Latin square L^* with row a^*. In all cases, the rows and columns generate G. □

Put $G = M_{23} \leq S_{23}$ such that $\{1, \ldots, 7\}$ is a block of the corresponding Witt design D. Let us assume that L is a Latin square such that the rows A and columns B generate G. Let a_{14}, a_{15}, a_{23} be elements of orders 14, 15 and 23 of G, respectively, mapping 1 to 2. Any fixed point free permutation $x \in G$ is conjugate to one of the following elements: $a_{14}, a_{15}, a_{23}, a_{14}^{-1}, a_{15}^{-1}, a_{23}^{-1}$. By Lemma 9.5, we can assume that the second row of L is a_{14}, a_{15} or a_{23}. Define $X = \{(1^g, \ldots, 7^g) \mid g \in G\}$, $|X| = 637\,560$.

On an office PC running GAP4 [Gap], it takes about 72 hours to list all 7×7 submatrices K which have the property that all rows and columns are in X, with given first column and first and second rows. If the second row is determined by a_{14} of a_{15} then the number of such submatrices is about 4000 and it takes 1 hour more to show that none of these submatrices can be extended to a Latin square of order 23 such that the rows and columns are in G. That is, about 150 hours of CPU time suffices to show that no column or row of L can be of order 14 or 15. Thus, we can assume that all rows and columns of L have order 23. Moreover, for any two rows x, y of L, xy^{-1} has order 23, as well. About 3 hours of computation shows that any Latin square with these properties must correspond to a cyclic group of order 23.

We have therefore the following

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	1	4	3	15	18	11	24	8	17	21	20	9	10	22	7	5	19	23	6	12	13	16	14
3	4	1	2	20	17	9	16	23	21	8	14	19	11	6	13	12	5	15	10	24	18	22	7
4	3	2	1	19	22	14	21	11	6	10	5	7	20	23	24	18	13	9	15	17	16	8	12
5	8	7	6	12	10	13	23	15	3	19	2	4	17	14	18	24	21	16	11	20	9	1	22
6	7	8	5	16	9	17	20	1	15	14	18	24	23	19	4	2	22	10	3	13	12	11	21
7	6	5	8	2	3	4	1	18	12	16	10	23	19	17	15	11	20	14	24	22	21	13	9
8	5	6	7	9	16	20	17	21	13	1	23	10	24	3	14	19	2	18	22	11	15	12	4
9	17	20	16	24	11	18	15	19	8	12	7	5	4	13	22	21	23	2	14	1	3	6	10
10	13	23	12	22	19	21	14	5	11	2	24	18	9	4	6	8	1	20	7	16	17	15	3
11	18	15	24	1	4	3	2	14	16	5	9	20	12	7	21	22	8	13	19	10	23	17	6
12	23	13	10	11	24	15	18	7	19	20	22	21	2	9	8	6	16	4	5	3	1	14	17
13	10	12	23	17	20	16	9	4	22	18	19	14	6	24	1	3	11	8	2	5	7	21	15
14	22	19	21	8	7	6	5	13	4	17	1	3	15	16	23	10	9	11	12	18	24	2	20
15	24	11	18	23	13	10	12	17	14	6	21	22	3	8	20	9	7	1	16	2	4	19	5
16	20	17	9	18	15	24	11	12	1	22	4	2	5	21	10	23	14	7	13	6	8	3	19
17	9	16	20	4	1	2	3	10	18	7	15	11	22	5	12	13	6	21	23	19	14	24	8
18	11	24	15	21	14	22	19	16	23	3	13	12	8	1	9	20	4	6	17	7	5	10	2
19	21	14	22	13	23	12	10	6	20	4	17	16	18	2	5	7	3	24	8	15	11	9	1
20	16	9	17	10	12	23	13	2	7	15	8	6	21	11	3	1	24	22	4	14	19	5	18
21	19	22	14	6	5	8	7	20	24	13	11	15	1	12	17	16	10	3	9	4	2	18	23
22	14	21	19	3	2	1	4	24	9	23	16	17	7	10	11	15	12	5	18	8	6	20	13
23	12	10	13	7	8	5	6	22	2	24	3	1	16	18	19	14	15	17	21	9	20	4	11
24	15	18	11	14	21	19	22	3	5	9	6	8	13	20	2	4	17	12	1	23	10	7	16

Table 9.1.: Cayley table of a loop whose multiplication group is M_{24}

Proposition 9.6. *(a) There is no loop Q of order 10 or 22 such that $\mathrm{Mlt}(Q) \leq M_{10}$ or $\mathrm{Mlt}(Q) \leq M_{22}$.*

(b) Let Q be a loop of order 11 or 23 such that $\mathrm{Mlt}(Q) \leq M_{11}$ or $\mathrm{Mlt}(Q) \leq M_{23}$. Then Q is a cyclic group.

(c) There are loops Q_1 and Q_2 of order 12 and 24 such that $\mathrm{Mlt}(Q_1) = M_{12}$ and $\mathrm{Mlt}(Q_2) = M_{24}$.

Proof. The loop Q_1 is Conway's arithmetic progression loop given in [Con88, Section 18]. Q_1 is commutative and its automorphism group is transitive. The multiplication table of the loop Q_2 is given in Table 9.1. Q_2 is noncommutative and $|\mathrm{Aut}(Q_2)| = 5$. □

dc_821_13

Part IV.

Dual nets in projective planes

dc_821_13

10. Projective realizations of 3-nets

In a projective plane a 3-*net* consists of three pairwise disjoint classes of lines such that every point incident with two lines from distinct classes is incident with exactly one line from each of the three classes. If one of the classes has finite size, say n, then the other two classes also have size n, called the *order* of the 3-net.

There is a long history about finite 3-nets in Combinatorics related to affine planes, Latin squares, loops and strictly transitive permutation sets. In this chapter we are dealt with 3-nets in a projective plane $PG(2,\mathbb{K})$ over an algebraically closed field $\mathbb{K}$ which are coordinatized by a group. Such a 3-net, with line classes $\mathcal{A},\mathcal{B},\mathcal{C}$ and coordinatizing group $G=(G,\cdot)$, is equivalently defined by a triple of bijective maps from G to $(\mathcal{A},\mathcal{B},\mathcal{C})$, say

$$\alpha : G \to \mathcal{A},\ \beta : G \to \mathcal{B},\ \gamma : G \to \mathcal{C}$$

such that $a \cdot b = c$ if and only if $\alpha(a),\beta(b),\gamma(c)$ are three concurrent lines in $PG(2,\mathbb{K})$, for any $a,b,c \in G$. If this is the case, the 3-net in $PG(2,\mathbb{K})$ is said to *realize* the group G. In recent years, finite 3-nets realizing a group in the complex plane have been investigated in connection with complex line arrangements and Resonance theory see [FY07; Buz09; PY08; Yuz04; Yuz09].

In the present chapter, combinatorial methods are used to investigate finite 3-nets realizing a group. Since key examples, such as algebraic 3-nets and tetrahedron type 3-nets, arise naturally in the dual plane of $PG(2,\mathbb{K})$, it is convenient to work with the dual concept of a 3-net.

The results of this chapter have been published in the paper [KNP13b]. The details on the classification of low order dual 3-nets are given in [NP13]. The study of the embedding of k-nets into projective planes continued in [KNP13a]. Theorem 10.1 supports **Thesis 6.**

Main result on group realizations

Formally, a *dual* 3-*net* of order n in $PG(2,\mathbb{K})$ consists of a triple $(\Lambda_1,\Lambda_2,\Lambda_3)$ with $\Lambda_1,\Lambda_2,\Lambda_3$ pairwise disjoint point-sets of size n, called *components*, such that every line meeting two distinct components meets each component in precisely one point. A dual 3-net $(\Lambda_1,\Lambda_2,\Lambda_3)$ realizing a group is *algebraic* if its points lie on a plane cubic, and is of *tetrahedron type* if its components lie on the six sides (diagonals)

of a non-degenerate quadrangle such a way that $\Lambda_i = \Delta_i \cup \Gamma_i$ with Δ_i and Γ_i lying on opposite sides, for $i = 1, 2, 3$.

The goal of this chapter is to prove the following classification theorem.

Theorem 10.1. *In the projective plane $PG(2, \mathbb{K})$ defined over an algebraically closed field $\mathbb{K}$ of characteristic $p \geq 0$, let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net of order $n \geq 4$ which realizes a group G. If either $p = 0$ or $p > n$ then one of the following holds.*

(I) *G is either cyclic or the direct product of two cyclic groups, and $(\Lambda_1, \Lambda_2, \Lambda_3)$ is algebraic.*

(II) *G is dihedral and $(\Lambda_1, \Lambda_2, \Lambda_3)$ is of tetrahedron type.*

(III) *G is the quaternion group of order 8.*

(IV) *G has order 12 and is isomorphic to Alt_4.*

(V) *G has order 24 and is isomorphic to Sym_4.*

(VI) *G has order 60 and is isomorphic to Alt_5.*

A computer aided exhaustive search shows that if $p = 0$ then (IV) (and hence (V), (VI)) does not occur, see [NP13].

Theorem 10.1 shows that every realizable finite group can act in $PG(2, \mathbb{K})$ as a projectivity group. This confirms Yuzvinsky's conjecture for $p = 0$.

The proof of Theorem 10.1 uses some previous results due to Yuzvinsky [Yuz09], Urzúa [Urz10], and Blokhuis, Korchmáros and Mazzocca [BKM11].

Our notation and terminology are standard, see [HP73]. In view of Theorem 10.1, $\mathbb{K}$ denotes an algebraically closed field of characteristic p where either $p = 0$ or $p \geq 5$, and any dual 3-net in the present chapter is supposed to be have order n with $n < p$ whenever $p > 0$.

10.1. Some useful results on plane cubics

A nice infinite family of dual 3-nets realizing a cyclic group arises from plane cubics in $PG(2, \mathbb{K})$; see [Yuz04]. The key idea is to use the well known abelian group defined on the points of an irreducible plane cubic, recalled here in the following two propositions.

Proposition 10.2. [HKT08, Theorem 6.104] *A non-singular plane cubic $\mathcal{F}$ can be equipped with an additive group $(\mathcal{F}, +)$ on the set of all its points. If an inflection point P_0 of $\mathcal{F}$ is chosen to be the identity 0, then three distinct points $P, Q, R \in \mathcal{F}$ are collinear if and only if $P + Q + R = 0$. For a prime number $d \neq p$, the subgroup of $(\mathcal{F}, +)$ consisting of all elements g with $dg = 0$ is isomorphic to $C_d \times C_d$ while for $d = p$ it is either trivial or isomorphic to C_p according as $\mathcal{F}$ is supersingular or not.*

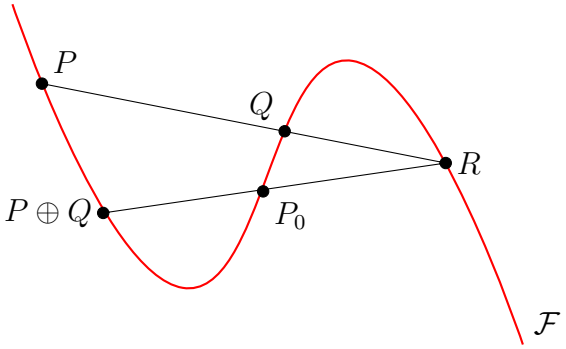


Figure 10.1.: Abelian group law on an elliptic curve

Proposition 10.3. [Yuz04, Proposition 5.6, (1)]. *Let $\mathcal{F}$ be an irreducible singular plane cubic with its unique singular point U, and define the operation $+$ on $\mathcal{F}\setminus\{U\}$ in exactly the same way as on a non-singular plane cubic. Then $(\mathcal{F},+)$ is an abelian group isomorphic to the additive group of $\mathbb{K}$, or the multiplicative group of $\mathbb{K}$, according as P is a cusp or a node.*

If P is a non-singular and non-inflection point of $\mathcal{F}$ then the tangent to $\mathcal{F}$ at P meets $\mathcal{F}$ a point P' other than P, and P' is the *tangential* point of P. Every inflection point of a non-singular cubic $\mathcal{F}$ is the center of an involutory homology preserving $\mathcal{F}$. A classical *Lame configuration* consists of two triples of distinct lines in $PG(2,\mathbb{K})$, say ℓ_1,ℓ_2,ℓ_3 and r_1,r_2,r_3, such that no line from one triple passes through the common point of two lines from the other triple. For $1\le j,k\le 3$, let R_{jk} denote the common point of the lines ℓ_j and r_k. There are nine such common points, and they are called the points of the Lame configuration.

Proposition 10.4. Lame's Theorem. *If eight points from a Lame configuration lie on a plane cubic then the ninth also does.*

10.2. 3-nets, quasigroups and loops

A Latin square of order n is a table with n rows and n columns which has n^2 entries with n different elements none of them occurring twice within any row or column. If $(L,*)$ is a quasigroup of order n then its multiplicative table, also called Cayley table, is a Latin square of order n, and the converse also holds.

For two integers k,n both bigger than 1, let $(G,\cdot)$ be a group of order kn containing a normal subgroup $(H,\cdot)$ of order n. Let $\mathcal{G}$ be a Cayley table of $(G,\cdot)$. Obviously, the rows and the columns representing the elements of $(H,\cdot)$ in $\mathcal{G}$ form a Latin square which is a Cayley table for $(H,\cdot)$. From $\mathcal{G}$, we may extract k^2-1 more Latin squares using the cosets of H in G. In fact, for any two such cosets H_1 and H_2, a Latin square $H_{1,2}$ is obtained by taking as rows (respectively columns) the elements of H_1 (respectively H_2).

Proposition 10.5. *The Latin square $H_{1,2}$ is a Cayley table for a quasigroup isotopic to the group H.*

Proof. Fix an element $t_1 \in H_1$. In $H_{1,2}$, label the row representing the element $h_1 \in H_1$ with $h_1' \in H$ where $h_1 = t_1 \cdot h_1'$. Similarly, for a fixed element $t_2 \in H_2$, label the column representing the element $h_2 \in H_2$ with $h_2' \in H$ where $h_2 = h_2' \cdot t_2$. The entries in $H_{1,2}$ come from the coset $H_1 \cdot H_2$. Now, label the entry h_3 in $H_1 \cdot H_2$ with the element $h_3' \in H$ where $h_3 = t_1 \cdot h_3' \cdot t_2$. Doing so, $H_{1,2}$ becomes a Cayley table for the subgroup $(H, \cdot)$, whence the assertion follows. □

In terms of a dual 3-net, the relationship between 3-nets and quasigroups can be described as follows. Let $(L, \cdot)$ be a loop arising from an embeddable 3-net, and consider its dual 3-net with its components $\Lambda_1, \Lambda_2, \Lambda_3$. For $i = 1, 2, 3$, the points in Λ_i are bijectively labeled by the elements of L. Let (A_1, A_2, A_3) with $A_i \in \Lambda_i$ denote the the triple of the points corresponding to the element $a \in L$. With this notation, $a \cdot b = c$ holds in L if and only if the points A_1, B_2 and C_3 are collinear. In this way, points in Λ_3 are *naturally labeled* when $a \cdot b$ is the label of C_3. Let (E_1, E_2, E_3) be the triple for the unit element e of L. From $e \cdot e = e$, the points E_1, E_2 and E_3 are collinear. Since $a \cdot a = a$ only holds for $a = e$, the points A_1, A_2, A_3 are the vertices of a (non-degenerate) triangle whenever $a \neq e$. Furthermore, from $e \cdot a = a$, the points E_1, A_2 and A_3 are collinear; similarly, $a \cdot e = a$ yields that the points A_1, E_2, and A_3 are collinear. However, the points A_1, A_2 and E_3 form a triangle in general; they are collinear if and only if $a \cdot a = e$, i.e. a is an involution of L.

In some cases, it is useful to relabel the points of Λ_3 replacing the above bijection $A_3 \to a$ from Λ_3 to L by the bijection $A_3 \to a'$ where a' is the inverse of a in $(L, \cdot)$. Doing so, three points A_1, B_2, C_3 with $A_1 \in \Lambda_1$, $B_2 \in \Lambda_2$, $C_3 \in \Lambda_3$ are collinear if and only if $a \cdot b \cdot c = e$ with e being the unit element in $(L, \cdot)$. This new bijective labeling will be called a *collinear relabeling* with respect to Λ_3.

In this chapter we are interested in 3-nets of $PG(2, \mathbb{K})$ which are coordinatized by a group G. If this is the case, we say that the 3-net realizes the group G. In terms of dual 3-nets where $\Lambda_1, \Lambda_2, \Lambda_3$ are the three components, the meaning of this condition is as follows: There exists a triple of bijective maps from G to $(\Lambda_1, \Lambda_2, \Lambda_3)$, say

$$\alpha : G \to \Lambda_1,\ \beta : G \to \Lambda_2,\ \gamma : G \to \Lambda_3$$

such that $a \cdot b = c$ if and only if $\alpha(a), \beta(b), \gamma(c)$ are three collinear points, for any $a, b, c \in G$.

Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net that realizes a group $(G, \cdot)$ of order kn containing a subgroup $(H, \cdot)$ of order n. Then the left cosets of H provide a partition of each component Λ_i into k subsets. Such subsets are called left H-members and denoted by $\Gamma_i^{(1)}, \ldots, \Gamma_i^{(k)}$, or simply Γ_i when this does not cause confusion. The left translation map $\sigma_g : x \mapsto x+g$ preserves every left H-member. The following lemma shows that every left H-member Γ_1 determines a dual 3-subnet of $(\Lambda_1, \Lambda_2, \Lambda_3)$ that realizes H.

Lemma 10.6. *Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net that realizes a group $(G, \cdot)$ of order kn containing a subgroup $(H, \cdot)$ of order n. For any left coset $g \cdot H$ of H in G, let $\Gamma_1 = g \cdot H$, $\Gamma_2 = H$ and $\Gamma_3 = g \cdot H$. Then $(\Gamma_1, \Gamma_2, \Gamma_3)$ is a 3-subnet of $(\Lambda_1, \Lambda_2, \Lambda_3)$ which realizes H.*

Proof. For any $h_1, h_2 \in H$ we have that $(g \cdot h_1) \cdot h_2 = g \cdot (h_1 \cdot h_2) = g \cdot h$ with $h \in H$. Hence, any line joining a point of Γ_1 with a point of Γ_2 meets Γ_3. □

Similar results hold for right cosets of H. Therefore, for any right coset $H \cdot g$, the triple $(\Gamma_1, \Gamma_2, \Gamma_3)$ with $\Gamma_1 = H$, $\Gamma_2 = H \cdot g$ and $\Gamma_3 = H \cdot g$ is a 3-subnet of $(\Lambda_1, \Lambda_2, \Lambda_3)$ which realizes H.

The dual 3-subnets $(\Gamma_1, \Gamma_2, \Gamma_3)$ introduced in Lemma 10.6 play a relevant role. When g ranges over G, we obtain as many as k such dual 3-nets, each being called *a dual 3-net realizing the subgroup H as a subgroup of G.*

Obviously, left cosets and right cosets coincide if and only if H is a normal subgroup of G, and if this is the case we may use the shorter term of coset.

Now assume that H is a normal subgroup of G. Take two H-members from different components, say Γ_i and Γ_j with $1 \leq i < j \leq 3$. From Proposition 10.5, there exists a member Γ_m from the remaining component Λ_m, with $1 \leq m \leq 3$ and $m \neq i, j$, such that $(\Gamma_1, \Gamma_2, \Gamma_3)$ is a dual 3-net of realizing $(H, \cdot)$. Doing so, we obtain k^2 dual 3-subnets of $(\Lambda_1, \Lambda_2, \Lambda_3)$. They are all the dual 3-subnets of $(\Lambda_1, \Lambda_2, \Lambda_3)$ which realize the normal subgroup $(H, \cdot)$ as a subgroup of $(G, \cdot)$.

Lemma 10.7. *Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net that realizes a group $(G, \cdot)$ of order kn containing a normal subgroup $(H, \cdot)$ of order n. For any two cosets $g_1 \cdot H$ and $g_2 \cdot H$ of H in G, let $\Gamma_1 = g_1 \cdot H$, $\Gamma_2 = g_2 \cdot H$ and $\Gamma_3 = (g_1 \cdot g_2) \cdot H$. Then $(\Gamma_1, \Gamma_2, \Gamma_3)$ is a 3-subnet of $(\Lambda_1, \Lambda_2, \Lambda_3)$ which realizes H.*

If g_1 and g_2 range independently over G, we obtain as many as k^2 such dual 3-nets, each being called *a dual 3-net realizing the normal subgroup H as a subgroup of G.*

10.3. The infinite families of dual 3-nets realizing a group

A dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ with $n \geq 4$ is said to be *algebraic* if all its points lie on a (uniquely determined) plane cubic $\mathcal{F}$, called the *associated* plane cubic of $(\Lambda_1, \Lambda_2, \Lambda_3)$. Algebraic dual 3-nets fall into three subfamilies according as the plane cubic splits into three lines, or in an irreducible conic and a line, or it is irreducible.

10.3.1. Proper algebraic dual 3-nets

An algebraic dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ is said to be *proper* if its points lie on an irreducible plane cubic $\mathcal{F}$.

Proposition 10.8. *Any proper algebraic dual 3-net* $(\Lambda_1, \Lambda_2, \Lambda_3)$ *realizes a group* M*. There is a subgroup* $T \cong M$ *in* $(\mathcal{F}, +)$ *such that each component* Λ_i *is a coset* $T + g_i$ *in* $(\mathcal{F}, +)$ *where* $g_1 + g_2 + g_3 = 0$*.*

Proof. We do some computation in $(\mathcal{F}, +)$. Let $A_1, A_2, A_3 \in \Lambda_1$ three distinct points viewed as elements in $(\mathcal{F}, +)$. First we show that the solution of the equation in $(\mathcal{F}, +)$

$$A_1 - A_2 = X - A_3 \tag{10.1}$$

belongs to Λ_1. Let $C \in \Lambda_3$. From the definition of a dual 3-net, there exist $B_i \in \Lambda_2$ such that $A_i + B_i + C = 0$ for $i = 1, 2, 3$. Now choose $C_1 \in \Lambda_3$ for which $A_1 + B_2 + C_1 = 0$, and then choose $A^* \in \Lambda_1$ for which $A^* + B_3 + C_1 = 0$. Now,

$$\begin{aligned} A^* - A_3 &= -B_3 - C_1 - (-B_3 - C) = C - C_1 \\ A_1 - A_2 &= -B_2 - C_1 - (-B_2 - C) = C - C_1 \end{aligned} \tag{10.2}$$

Therefore, A^* is a solution of Equation (10.2).

Now we are in a position to prove that Λ_1 is a coset of a subgroup of $(\mathcal{F}, +)$. For $A_0 \in \Lambda_1$, let $T_1 = \{A - A_0 | A \in \Lambda_1\}$. Since $(A_1 - A_0) - (A_2 - A_0) = A_1 - A_2$, Equation (10.2) ensures the existence of $A^* \in \Lambda_1$ for which $A_1 - A_2 = A^* - A_0$ whenever $A_1, A_2 \in \Lambda_1$. Hence $(A_1 - A_0) - (A_2 - A_0) \in T_1$. From this, T_1 is a subgroup of $(\mathcal{F}, +)$, and therefore Λ_1 is a coset $T + g_1$ of T_1 in $(\mathcal{F}, +)$.

Similarly, $\Lambda_2 = T_2 + g_2$ and $\Lambda_3 = T_3 + g_3$ with some subgroups T_2, T_3 of $(\mathcal{F}, +)$ and elements $g_2, g_3 \in (\mathcal{F}, +)$. It remains to show that $T_1 = T_2 = T_3$. The line through the points g_1 and g_2 meets Λ_3 in a point $t^* + g_3$. Replacing g_3 with $g_3 + t^*$ allows to assume that $g_1 + g_2 + g_3 = 0$. Then three points $g_i + t_i$ with $t_i \in T_i$ is collinear if and only if $t_1 + t_2 + t_3 = 0$. For $t_3 = 0$ this yields $t_2 = -t_1$. Hence, every element of T_2 is in T_1, and the converse also holds. From this, $T_1 = T_2$. Now, $t_3 = -t_1 - t_2$ yields that $T_3 = T_1$. Therefore $T = T_1 = T_2 = T_3$ and $\Lambda_i = T + g_i$ for $i = 1, 2, 3$. This shows that $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizes a group $M \cong T$. □

10.3.2. Triangular dual 3-nets

An algebraic dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ is *regular* if the components lie on three lines, and it is either of *pencil type* or *triangular* according as the three lines are either concurrent, or they are the sides of a triangle.

Lemma 10.9. *Every regular dual* 3*-net of order* n *is triangular.*

Proof. Assume that the components of a regular dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ lie on three concurrent lines. Using homogeneous coordinates in $PG(2, \mathbb{K})$, these lines are assumed to be those with equations $Y = 0, X = 0, X - Y = 0$ respectively, so that the line of equation $Z = 0$ meets each component. Therefore, the points in the components may be labeled in such a way that

$$\Lambda_1 = \{(1, 0, \xi) | \xi \in L_1\},\ \Lambda_2 = \{(0, 1, \eta) | \eta \in L_2\},\ \Lambda_3 = \{(1, 1, \zeta) | \zeta \in L_3\},$$

with L_i subsets of $\mathbb{K}$ containing 0. By a straightforward computation, three points $P = (1, 0, \xi)$, $Q = (0, 1, \eta)$, $R = (1, 1, \zeta)$ are collinear if and only if $\zeta = \xi + \eta$. Therefore, $L_1 = L_2 = L_3$ and $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizes a subgroup of the additive group of $\mathbb{K}$ of order n. Therefore n is a power of p. But this contradicts the hypothesis $p > n$. □

For a triangular dual 3-net, the (uniquely determined) triangle whose sides contain the components is called the *associated* triangle.

Proposition 10.10. *Every triangular dual* 3*-net realizes a cyclic group isomorphic to a multiplicative group of* $\mathbb{K}$*.*

Proof. Using homogeneous coordinates in $PG(2, \mathbb{K})$, the vertices of the triangle are assumed to be the points $O = (0, 0, 1)$, $X_\infty = (1, 0, 0)$, $Y_\infty = (0, 1, 0)$. For $i = 1, 2, 3$, let ℓ_i denote the fundamental line of equation $Y = 0$, $X = 0$, $Z = 0$ respectively. Therefore the points in the components lie on the fundamental lines and they may be labeled in such a way that

$$\Lambda_1 = \{(\xi, 0, 1) | \xi \in L_1\},\ \Lambda_2 = \{(0, \eta, 1) | \eta \in L_2\},\ \Lambda_3 = \{(1, -\zeta, 0) | \zeta \in L_3\}$$

with L_i subsets of $\mathbb{K}^*$ of a given size n. With this setting, three points $P = (\xi, 0, 1)$, $Q = (0, \eta, 1)$, $R = (1, -\zeta, 0)$ are collinear if and only if $\xi\zeta = \eta$. With an appropriate choice of the unity point of the coordinate system, both $1 \in L_1$ and $1 \in L_2$ may also be assumed. From $1 \in L_1$, we have that $L_2 = L_3$. This together with $1 \in L_2$ imply that $L_1 = L_2 = L_3 = L$. Since $1 \in L$, L is a finite multiplicative subgroup of $\mathbb{K}$. In particular, L is cyclic. □

Remark 10.11. In the proof of Proposition 10.10, if the unity point of the coordinate system is arbitrarily chosen, the subsets L_1, L_2 and L_3 are not necessarily subgroups. Actually, they are cosets of (the unique) multiplicative cyclic subgroup H, say $L_1 = aH$, $L_2 = bH$ and $L_3 = cH$, with $ac = b$. Furthermore, since every $h \in H$ defines a projectivity $\varphi_h : x \mapsto hx$ of the projective line, and these projectivities form a group isomorphic to H, it turns out that L_i is an orbit of a cyclic projectivity group of ℓ_i of order n, for $i = 1, 2, 3$.

Proposition 10.12. *Let* $(\Lambda_1, \Lambda_2, \Lambda_3)$ *be a triangular dual* 3*-net. Then every point of* $(\Lambda_1, \Lambda_2, \Lambda_3)$ *is the center of a unique involutory homology which preserves* $(\Lambda_1, \Lambda_2, \Lambda_3)$*.*

Proof. The point $(\xi, 0, 1)$ is the center and the line through Y_∞ and the point $(-\xi, 0, 1)$ and is the axis of the involutory homology φ_ξ associated to the matrix

$$\begin{pmatrix} 0 & 0 & \xi^2 \\ 0 & -\xi & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

With the above notation, if $\xi \in aH$ then h_ξ preserves Λ_1 while it sends any point in Λ_2 to a point in Λ_3, and viceversa. Similarly, for $\eta \in bH$ and $\zeta \in cH$ where ψ_η

and θ_ζ are the involutory homologies associated to the matrices

$$\begin{pmatrix} -\eta & 0 & 0 \\ 0 & 0 & \eta^2 \\ 0 & 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 & 0 \\ \zeta^2 & 0 & 0 \\ 0 & 0 & \zeta \end{pmatrix}.$$

□

With the notation introduced in the proof of Proposition 10.10, let $\Phi_1 = \{\varphi_\xi \varphi_{\xi'} | \xi, \xi' \in aH\}$ and $\Phi_2 = \{\psi_\eta \psi_{\eta'} | \eta, \eta' \in bH\}$. Then both are cyclic groups isomorphic to H. A direct computation gives the following result.

Proposition 10.13. *$\Phi_1 \cap \Phi_2$ is either trivial or has order 3.*

Some useful consequences are stated in the following proposition.

Proposition 10.14. *Let $\Theta = \langle \Phi_1, \Phi_2 \rangle$. Then*

$$|\Theta| = \begin{cases} |H|^2, & \text{when } \gcd.(3, |H|) = 1; \\ \frac{1}{3}|H|^2, & \text{when } \gcd.(3, |H|) = 3. \end{cases}$$

Furthermore, Θ fixes the vertices of the fundamental triangle, and no non-trivial element of Θ fixes a point outside the sides of the fundamental triangle.

We prove another useful result.

Proposition 10.15. *If $(\Gamma_1, \Gamma_2, \Gamma_3)$ and $(\Sigma_1, \Sigma_2, \Sigma_3)$ are triangular dual 3-nets such that $\Gamma_1 = \Sigma_1$, then the associated triangles share the vertices on their common side.*

Proof. From Remark 10.11, Γ_1 is the orbit of a cyclic projectivity group H_1 of the line ℓ containing Γ_1 while the two fixed points of H_1 on ℓ, say P_1 and P_2, are vertices of the triangle containing $\Gamma_1, \Gamma_2, \Gamma_3$.

The same holds for Σ_1 with a cyclic projectivity group H_2, and fixed points Q_1, Q_2. From $\Gamma_1 = \Sigma_1$, the projectivity group H of the line ℓ generated by H_1 and H_2 preserves Γ_1. Let M be the projectivity group generated by H_1 and H_2.

Observe that M is a finite group since it has an orbit of finite size $n \geq 3$. Clearly, $|M| \geq n$ and equality holds if and only if $H_1 = H_2$. If this is the case, then $\{P_1, P_2\} = \{Q_1, Q_2\}$. Therefore, for the purpose of the proof, we may assume on the contrary that $H_1 \neq H_2$ and $|M| > n$.

Now, Dickson's classification of finite subgroups of $PGL(2, \mathbb{K})$ applies to M. From that classification, M is one of the nine subgroups listed as $((1), \ldots, (9)$ in [MV83, Theorem 1] where e denotes the order of the stabilizer M_P of a point P in a short M-orbit, that is, an M-orbit of size smaller than M. Observe that such an M-orbit has size $|M|/e$. There exist a finitely many short M-orbits, and Σ_1 is one of them. It may be that an M-orbit is trivial as it consists of just one point.

Obviously, M is neither cyclic nor dihedral as it contains two distinct cyclic subgroups of the same order $n \geq 3$.

Also, M is not an elementary abelian p-group E of rank ≥ 2, otherwise we would have $|E| = |M| > n$ since the minimum size of a non-trivial E-orbit is $|E|$, see (2) in [MV83, Theorem 1].

From (5) in [MV83, Theorem 1] with $p \neq 2, 3$, the possible sizes of a short Alt_4-orbit are $4, 6$ each larger than 3. On the other hand, Alt_4 has no element of order larger than 3. Therefore, $M \ncong \mathrm{Alt}_4$ for $p \neq 2, 3$.

Similarly, from (5) in [MV83, Theorem 1] with $p \neq 2, 3$, the possible sizes of a short Sym_4-orbit are $6, 8, 12$ each larger than 4. Since Sym_4 has no element of order larger than 4. Therefore, $M \ncong \mathrm{Sym}_4$ for $p \neq 2, 3$.

Again, from (6) in [MV83, Theorem 1] with $p \neq 2, 5$, the possible sizes of a short Alt_5-orbit are $10, 12$ for $p = 3$ while $12, 20, 30$ for $p \neq 2, 3, 5$. Each size exceeds 5. On the other hand Alt_5 has no element of order larger than 5. Therefore, $M \ncong \mathrm{Alt}_5$ for $p \neq 2, 5$.

The group M might be isomorphic to a subgroup L of order qk with $k|(q-1)$ and $q = p^h$, $h \geq 1$. Here L is the semidirect product of the unique (elementary abelian) Sylow p-subgroup of L by a cyclic subgroup of order k. No element in L has order larger than k when $h > 1$ and p when $h = 1$. From (7) in [MV83, Theorem 1], any non-trivial short L-orbit has size q. Therefore $M \cong L$ implies that $h = 1$ and $n = p$. But this is inconsistent with the hypothesis $p > n$.

Finally, M might be isomorphic to a subgroup L such that either $L = PSL(2, q)$ or $L = PGL(2, q)$ with $q = p^h$, $h \geq 1$. No element in L has order larger than $q + 1$. From (7) and (8) in [MV83, Theorem 1], any short L-orbit has size either $q + 1$ or $q(q - 1)$. For $q \geq 3$, if $M \cong L$ occurs then $n = q + 1 \geq p + 1$, a contradiction with the hypothesis $p > n$. For $q = 2$, we have that $|L| = 6$ which is smaller than 12. Therefore $M \ncong L$.

No possibility has arisen for M. Therefore $\{P_1, P_2\} = \{Q_1, Q_2\}$. □

10.3.3. Conic-line type dual 3-nets

An algebraic dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ is of *conic-line type* if two of its three components lie on an irreducible conic $\mathcal{C}$ and the third one lies on a line ℓ. All such 3-nets realize groups and they can be described using subgroups of the projectivity group $PGL(2, \mathbb{K})$ of $\mathcal{C}$. For this purpose, some basic results on subgroups and involutions in $PGL(2, \mathbb{K})$ are useful which essentially depend on the fact that every involution in $PGL(2, \mathbb{K})$ is a perspectivity whose center is a point outside $\mathcal{C}$ and axis is the pole of the center with respect to the orthogonal polarity arising from $\mathcal{C}$. We begin with an example.

Example 10.16. Take any cyclic subgroup C_n of $PGL(2, \mathbb{K})$ of order $n \geq 3$ with $n \neq p$ that preserves $\mathcal{C}$. Let D_n be the unique dihedral subgroup of $PGL(2, \mathbb{K})$ containing C_n. If j is the (only) involution in $\mathcal{Z}(D_n)$ and ℓ is its axis, then the centers of the other involutions in D_n lie on ℓ. We have n involutions in D_n other than j, and the set of the their centers is taken for Λ_1. Take a C_n-orbit $\mathcal{O}$ on $\mathcal{C}$ such that the tangent to $\mathcal{C}$ at any point in $\mathcal{O}$ is disjoint from Λ_1; equivalently, the

D_n-orbit $\mathcal{Q}$ be larger than $\mathcal{O}$. Then $\mathcal{Q}$ is the union of $\mathcal{O}$ together with another C_n-orbit. Take these two C_n-orbits for Λ_2 and Λ_3 respectively. Then $(\Lambda_1, \Lambda_2, \Lambda_3)$ is a conic-line dual 3-net which realizes C_n. It may be observed that ℓ is a chord of $\mathcal{C}$ and the multiplicative group of $\mathbb{K}$ has a subgroup of order n.

The cyclic subgroups C_n form a unique conjugacy class in $PGL(2, \mathbb{K})$. For a cyclic subgroup C_n of $PGL(2, \mathbb{K})$ of order n, the above construction provides a unique example of a dual 3-net realizing C_n. Using the classification of finite subgroups of $PGL(2, \mathbb{K})$ as in the proof of [BKM11, Theorem 6.1], the following result can be proven.

Proposition 10.17. *Up to projectivities, the conic-line dual 3-nets of order n are those described in Example 10.16.*

A corollary of this is the following result.

Proposition 10.18. *A conic-line dual 3-net realizes a cyclic group C_n.*

The result below can be proven with an argument similar to that used in the proof of Proposition 10.15.

Proposition 10.19. *Let $(\Gamma_1, \Gamma_2, \Gamma_3)$ and $(\Delta_1, \Delta_2, \Delta_3)$ be two conic-line type dual 3-nets where Γ_3 lies on the line ℓ and Δ_3 lies on the line s. If $\Gamma_1 = \Delta_1$ then $\ell = s$.*

10.3.4. Tetrahedron type dual 3-nets

In $PG(2, \mathbb{K})$, any non-degenerate quadrangle with its six sides (included the two diagonals) may be viewed as the projection of a tetrahedron of $PG(3, \mathbb{K})$. This suggests to call two sides of the quadrangle *opposite*, if they do not have any common vertex. With this definition, the six sides of the quadrangle are partitioned into three couples of opposite sides. Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net of order $2n$ containing a dual 3-subnet

$$(\Gamma_1, \Gamma_2, \Gamma_3) \tag{10.3}$$

of order n. Observe that $(\Lambda_1, \Lambda_2, \Lambda_3)$ contains three more dual 3-subnets of order n. In fact, for $\Delta_i = \Lambda_i \setminus \Gamma_i$, each of the triples below defines such a subnet:

$$(\Gamma_1, \Delta_2, \Delta_3),\ (\Delta_1, \Gamma_2, \Delta_3),\ (\Delta_1, \Delta_2, \Gamma_3). \tag{10.4}$$

Now, the dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ is said to be *tetrahedron-type* if its components lie on the sides of a non-degenerate quadrangle such that Γ_i and Δ_i are contained in opposite sides, for $i = 1, 2, 3$. Such a non-degenerate quadrangle is said to be *associated* to $(\Lambda_1, \Lambda_2, \Lambda_3)$. Observe that each of the six sides of the quadrangle contains exactly one of the point-sets Γ_i and Δ_i. Moreover, each of the four dual 3-subnets listed in (10.3) and (10.4) is triangular as each of its components, called a *half-set*, lies on a side of a triangle whose vertices are also vertices of the quadrangle. Therefore there are six half-sets in any dual 3-net of tetrahedron type.

Proposition 10.20. *Any tetrahedron-type dual 3-net realizes a dihedral group.*

Proof. The associated quadrangle is assumed to be the fundamental quadrangle of the homogeneous coordinate system in $PG(2,\mathbb{K})$, so that its vertices are O, X_∞, Y_∞ together with the unity point $E = (1,1,1)$. By definition, the subnet (10.3) is triangular. Without loss of generality,

$$\Gamma_1 = \{(\xi,0,1)|\xi \in L_1\},\ \Gamma_2 = \{(0,\eta,1)|\eta \in L_2\},\ \Gamma_3 = \{(1,-\zeta,0)|\zeta \in L_3\}$$

where $L_1 = aH, L_2 = bH, L_3 = cH$ are cosets of H with $ac = b$, see Remark 10.11. We fix such triple $\{a,b,c\}$. Observe that $(a,0,1) \in \Gamma_1$, $(0,b,1) \in \Gamma_2$ and $(1,-c,0) \in \Gamma_3$. Furthermore,

$$\Delta_1 = \{(1,\alpha,1)|\alpha \in M_1\},\ \Delta_2 = \{(\beta,1,1)|\beta \in M_2\},\ \Delta_3 = \{(1,1,\gamma)|\gamma \in M_3\}$$

with M_1, M_2 and M_3 subsets of $\mathbb{K} \setminus \{0,1\}$, each of size n.

An alternative approach to the proof is to lift $(\Lambda_1,\Lambda_2,\Lambda_3)$ to the fundamental tetrahedron of $PG(3,\mathbb{K})$ so that the projection π from the point $P_0 = (1,1,1,1)$ on the plane $X_4 = 0$ returns $(\Lambda_1,\Lambda_2,\Lambda_3)$. For this purpose, it is enough to define the sets lying on the edges of the fundamental tetrahedron:

$$\begin{array}{ll}
\Gamma'_1 = \{(\xi,0,1,0)|\xi \in L_1\}, & \Gamma'_2 = \{(0,\eta,1,0)|\eta \in L_2\},\\
\Gamma'_3 = \{(1,-\zeta,0,0)|\zeta \in L_3\}, & \Delta'_1 = \{(0,\alpha-1,0,-1)|\alpha \in M_1\},\\
\Delta'_2 = \{(\beta-1,0,0,-1)|\beta \in M_2\}, & \Delta'_3 = \{(0,0,\gamma-1,-1)|\gamma \in M_3\},
\end{array}$$

and observe that $\pi(\Gamma'_i) = \Gamma_i$ and $\pi(\Delta'_i) = \Delta_i$ for $i = 1,2,3$. Moreover, a triple (P_1,P_2,P_3) of points with $P_i \in \Gamma_i \cup \Delta_i$ consists of collinear points if and only if if their projection does. Hence, $(\Gamma'_1 \cup \Gamma'_2, \Gamma'_3 \cup \Delta'_1, \Delta'_2 \cup \Delta'_3)$ can be viewed as a "spatial" dual 3-net realizing the same group H. Clearly, $(\Gamma'_1 \cup \Gamma'_2, \Gamma'_3 \cup \Delta'_1, \Delta'_2 \cup \Delta'_3)$ is contained in the sides of the fundamental tetrahedron. We claim that these sides minus the vertices form an infinite spatial dual 3-net realizing the dihedral group $2.\mathbb{K}^*$.

To prove this, parametrize the points as follows.

$$\begin{array}{rcl}
\Sigma_1 & = & \{x_1 = (x,0,1,0), (\varepsilon x)_1 = (0,1,0,x) \mid x \in \mathbb{K}^*\},\\
\Sigma_2 & = & \{y_2 = (1,y,0,0), (\varepsilon y)_2 = (0,0,1,y) \mid y \in \mathbb{K}^*\},\\
\Sigma_3 & = & \{z_3 = (0,-z,1,0), (\varepsilon z)_3 = (1,0,0,-z) \mid z \in \mathbb{K}^*\}.
\end{array} \tag{10.5}$$

Then,

$$\begin{array}{rcl}
x_1, y_2, z_3 \text{ are collinear} & \Leftrightarrow & z = xy,\\
(\varepsilon x)_1, y_2, (\varepsilon z)_3 \text{ are collinear} & \Leftrightarrow & z = xy \Leftrightarrow \varepsilon z = (\varepsilon x)y,\\
x_1, (\varepsilon y)_2, (\varepsilon z)_3 \text{ are collinear} & \Leftrightarrow & z = x^{-1}y \Leftrightarrow \varepsilon z = x(\varepsilon y),\\
(\varepsilon x)_1, (\varepsilon y)_2, z_3 \text{ are collinear} & \Leftrightarrow & z = x^{-1}y \Leftrightarrow z = (\varepsilon x)(\varepsilon y).
\end{array}$$

Thus, $(\Gamma'_1 \cup \Gamma'_2, \Gamma'_3 \cup \Delta'_1, \Delta'_2 \cup \Delta'_3)$ is a dual 3-subnet of $(\Sigma_1,\Sigma_2,\Sigma_3)$ and H is a subgroup of the dihedral group $2.\mathbb{K}^*$. As H is not cyclic but it has a cyclic subgroup of index 2, we conclude that H is itself dihedral. □

10.4. Classification of low order dual 3-nets

An exhaustive computer aided search gives the following results.

Proposition 10.21. *Any dual* 3*-net realizing an abelian group of order* ≤ 8 *is algebraic. The dual of Urzúa's* 3*-nets are the only dual* 3*-net which realize the quaternion group of order* 8*.*

Proposition 10.22. *Any dual* 3*-net realizing an abelian group of order* 9 *is algebraic.*

Proposition 10.23. *If* $p = 0$*, no dual* 3*-net realizes* Alt_4*.*

10.5. Characterizations of the infinite families

Proposition 10.24. *Every dual* 3*-net realizing a cyclic group is algebraic.*

Proof. For $n = 3$, we have that $3n = 9$, and hence all points of the dual 3-net lie on a cubic. Therefore, $n \geq 4$ is assumed.

Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net of order n which realizes the cyclic group $(L, *)$. Therefore, the points of each component are labeled by I_n. After a collinear relabeling with respect to Λ_3, consider the configuration of the following nine points: $0, 1, 2$ from Λ_1, $0, 1, 2$ from Λ_2 and $n-1, n-2, n-3$ from Λ_3. For the seek of a clearer notation, the point with label a in the component Λ_m will be denoted by a_m.

The configuration presents six triples of collinear points, namely

(i) $\{0_1, 1_2, (n-1)_3\},\ \{1_1, 2_2, (n-3)_3\},\ \{2_1, 0_2, (n-2)_3\}$;

(ii) $\{0_1, 2_2, (n-2)_3\},\ \{1_1, 0_2, (n-1)_3\},\ \{2_1, 1_2, (n-3)_3\}$;

Therefore, the corresponding lines form a Lame configuration. Furthermore, the three (pairwise distinct) lines determined by the two triples in (i) can be regarded as a totally reducible plane cubic, say $\mathcal{F}_1$. Similarly, a totally reducible plane curve, say $\mathcal{F}_2$, arises from the triples in (ii). Obviously, $\mathcal{F}_1 \neq \mathcal{F}_2$. Therefore, the nine points of the above Lame configuration are the base points of the pencil generated by $\mathcal{F}_1$ and $\mathcal{F}_2$. Now, define the plane cubic $\mathcal{F}$ to be the cubic from the pencil which contains 3_1.

Our next step is to show that $\mathcal{F}$ also contains each of the points $(n-4)_3$ and 3_2. For this purpose, consider the following six triples of collinear points

(iii) $\{1_1, 2_2, (n-3)_3\},\ \{2_1, 0_2, (n-2)_3\},\ \{3_1, 1_2, (n-4)_3\}$;

(iv) $\{1_1, 1_2, (n-2)_3\},\ \{2_1, 2_2, (n-4)_3\},\ \{3_1, 0_2, (n-3)_3\}$;

Again, the corresponding lines form a Lame configuration. Since eight of its points, namely $1_1, 2_1, 3_1, 0_2, 1_2, 2_2, (n-2)_3, (n-3)_3$ lie on $\mathcal{F}$, Lame's theorem shows that $(n-4)_3$ also lies on $\mathcal{F}$. To show that $3_2 \in \mathcal{F}$, we proceed similarly using the following six triples of collinear points

(v) $\{0_1, 3_2, (n-3)_3\},\ \{1_1, 1_2, (n-2)_3\},\ \{2_1, 2_2, (n-4)_3\}$;

(vi) $\{0_1, 2_2, (n-2)_3\},\ \{1_1, 3_2, (n-4)_3\},\ \{2_1, 1_2, (n-3)_3\}$;

to define a Lame configuration that behaves as before, eight of its points, namely $0_1, 1_1, 2_1, 1_2, 2_2, (n-2)_3, (n-3)_3, (n-4)_3$ lie on $\mathcal{F}$, from Lame's theorem, 3_2 also lies on $\mathcal{F}$.

This completes the proof for $n = 4$. We assume that $n \geq 5$ and show that $(n-5)_3$ lies on $\mathcal{F}$. Again, we use the above argument based on the Lame configuration of the six lines arising from the following six triples of points:

(vii) $\{1_1, 3_2, (n-4)_3\},\ \{2_1, 1_2, (n-3)_3\},\ \{3_1, 2_2, (n-5)_3\}$;

(viii) $\{1_1, 2_2, (n-3)_3\},\ \{2_1, 3_2, (n-5)_3\},\ \{3_1, 1_2, (n-4)_3\}$;

From the previous discussion, eight of these points lie on $\mathcal{F}$. Lame's theorem yields that the ninth, namely $(n-5)_3$, also lies on $\mathcal{F}$. From this we infer that $4_1 \in \mathcal{F}$ also holds. To do this, we repeat the above argument for the Lame configuration arising from the six triples of points

(ix) $\{2_1, 2_2, (n-4)_3\},\ \{3_1, 0_2, (n-3)_3\},\ \{4_1, 1_2, (n-5)_3\}$;

(x) $\{2_1, 1_2, (n-3)_3\},\ \{3_1, 2_2, (n-5)_3\},\ \{4_1, 0_2, (n-4)_3\}$;

Again, we see that eight of these points lie on $\mathcal{F}$. Hence the ninth, namely 4_1, also lies on $\mathcal{F}$, by Lame's theorem.

Therefore, from the hypothesis that $\mathcal{F}$ passes through the ten points

$$0_1, 1_1, 2_1, 3_1, 0_2, 1_2, 2_2, (n-1)_3, (n-2)_3, (n-3)_3,$$

we have deduced that $\mathcal{F}$ also passes through the ten points

$$1_1, 2_1, 3_1, 4_1, 1_2, 2_2, 3_2, (n-2)_3, (n-3)_3, (n-4)_3.$$

Comparing these two sets of ten points shows that the latter derives from the former shifting by $+1$ when the indices are 1 and 2, while by -1 in when the indices are 3. Therefore, repeating the above argument $n-4$ times gives that all points in the dual 3-net lie on $\mathcal{F}$. □

Proposition 10.25. [Yuz04, Theorem 5.4] *If an abelian group G contains an element of order ≥ 10 then every dual 3-net realizing G is algebraic.*

Proposition 10.26. [Yuz04, Theorem 4.2] *No dual 3-net realizes an elementary abelian group of order 2^h with $h \geq 3$.*

Proposition 10.27. [BKM11, Theorem 5.1] *Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net such that at least one component lies on a line. Then $(\Lambda_1, \Lambda_2, \Lambda_3)$ is either triangular or of conic-line type.*

Lemma 10.28. *Let $(\Gamma_1, \Gamma_2, \Gamma_3)$ be an algebraic dual 3-net lying on a plane cubic $\mathcal{F}$. If $\mathcal{F}$ is reducible, then $(\Gamma_1, \Gamma_2, \Gamma_3)$ is either triangle or of conic-line type, according as $\mathcal{F}$ and splits into three lines or into a line and an irreducible conic.*

Proposition 10.29. *Every dual 3-net realizing a dihedral group of order $2n$ with $n \geq 3$ is of tetrahedron type.*

Proof. Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net realizing a dihedral group

$$D_n = \left\langle x, y \mid x^2 = y^n = 1,\ yx = xy^{-1} \right\rangle.$$

Labeling naturally the points in the components Λ_i as indicated in Section 10.2, every $u \in D_n$ defines a triple of points (u_1, u_2, u_3) where $u_i \in \Lambda_i$ for $i = 1, 2, 3$, and viceversa. Doing so, three points $u_1 \in \Lambda_1$, $v_2 \in \Lambda_2$, $w_3 \in \Lambda_3$ are collinear if and only if $uv = w$ holds in D_n.

Therefore, for $1 \leq i \leq n-2$, the triangle with vertices $x_2, (xy)_2, (xy^{-i})_3$ and that with vertices $(1)_3, y_3, (y^{-i})_2$ are in mutual perspective position from the point x_1. For two distinct points u_i and v_j with $u_i \in \Lambda_i$ and $v_j \in \Lambda_j$ and $1 \leq i, j \leq 3$, let $\overline{u_i v_j}$ denote the line through u_i and v_j. From the Desargues theorem, the three diagonal points, that is, the points

$$\begin{aligned} U &= \overline{(x)_2(xy)_2} \cap \overline{(1)_3(y)_3}, \\ (y^i)_1 &= \overline{(x)_2(xy^{-i})_3} \cap \overline{(y^{-i})_2(1)_3}, \\ (y^{i+1})_1 &= \overline{(xy)_2(xy^{-i})_3} \cap \overline{(y^{-i})_2(y)_3}, \end{aligned}$$

are collinear. Hence, a line ℓ_1 contains each point $(1)_1, (y)_1 \ldots, (y^{n-1})_1$ in Λ_1, that is,

$$(1)_1, (y)_1 \ldots, (y^{n-1})_1 \in \ell_1.$$

There are some more useful Desargues configurations. Indeed, the pairs of triangles with vertices

$$\begin{aligned} (x)_2, (xy^{-1})_2, (y^{-i-1})_3 \quad &\text{and} \quad (xy)_3, (x)_3, (y^{-i})_2; \\ (y^i)_2, (y^{i+1})_2, (y^{i+1})_3 \quad &\text{and} \quad (x)_3, (xy)_3, (xy)_2; \\ (xy^i)_2, (xy^{i+1})_2, (y^i)_3 \quad &\text{and} \quad (x)_3, (xy)_3, (1)_2; \\ (1)_2, (y)_2, (x)_3 \quad &\text{and} \quad (y^i)_3, (y^{i+1})_3, (xy^i)_2; \\ (x)_2, (xy)_2, (1)_3 \quad &\text{and} \quad (xy^i)_3, (xy^{i+1})_3, (y^i)_2 \end{aligned}$$

are in mutual perspective position from the points

$$(y^{-1})_1, (xy^{-i})_1, (y^i)_1, (y^i)_1, (y^{-i})_1,$$

respectively. Therefore, there exist five more lines $m_1, \ell_2, m_2, \ell_3, m_3$ such that

$$\{(x)_1, (xy)_1, \ldots, (xy^{n-1})_1\} \subset m_1, \quad \{(1)_2, (y)_2, \ldots, (y^{n-1})_2\} \subset \ell_2,$$
$$\{(x)_2, (xy)_2, \ldots, (xy^{n-1})_2\} \subset m_2, \quad \{(1)_3, (y)_3, \ldots, (y^{n-1})_3\} \subset \ell_3,$$
$$\{(x)_3, (xy)_3, \ldots, (xy^{n-1})_3\} \subset m_3.$$

By Proposition 10.15, the lines $\ell_1, \ldots, m_3$ are the sides of a nondegenarate quadrangle, which shows that the dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ is of tetrahedron type. □

Remark 10.30. From Proposition 10.29, the dual 3-nets given in [PY08, Section 6.2] are of tetrahedron type.

Proposition 10.31. *Let G be a finite group containing a normal subgroup H of order $n \geq 3$. Assume that G can be realized by a dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ and that every dual 3-subnet of $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizing H as a subgroup of G is triangular. Then H is cyclic and $(\Lambda_1, \Lambda_2, \Lambda_3)$ is either triangular or of tetrahedron type.*

Proof. From Proposition 10.10, H is cyclic. Fix an H-member Γ_1 from Λ_1, and denote by ℓ_1 the line containing Γ_1. Consider all the triangles which contain some dual 3-net $(\Gamma_1, \Gamma_2^j, \Gamma_3^s)$ realizing H as a subgroup of G. From Proposition 10.15, these triangles have two common vertices, say P and Q, lying on ℓ_1. For the third vertex R_j of the triangle containing $(\Gamma_1, \Gamma_2^j, \Gamma_3^s)$ there are two possibilities, namely either the side PR_j contains Γ_2^j and the side QR_j contains Γ_3^s, or viceversa. Therefore, every H-member Γ_2^j from Λ_2 (as well as every H-member Γ_3^s from Λ_3) is contained in a line passing through P or Q.

Now, replace Γ_1 by another H-orbit Γ_1^i lying in Λ_1 and repeat the above argument. If ℓ_i is the line containing Γ_1^i and P_i, Q_i denote the vertices then again every H-member Γ_2^j from Λ_2 (as well as every H-member Γ_3^s from Λ_3) is contained in a line passing through P_i or Q_i.

Assume that $\{P, Q\} \neq \{P_i, Q_i\}$. If one of the vertices arising from Γ_1, say P, coincides with one of the vertices, say P_i, arising from Γ_1^i then the line QQ_i must contain either Γ_2^j or Γ_3^s from each $(\Gamma_1, \Gamma_2^j, \Gamma_3^s)$. Therefore, the line QQ_i must contain every H-member from Λ_2, or every H-member from Λ_3. Hence Λ_2 or Λ_3 lies on the line QQ_i. From Proposition 10.27, $(\Lambda_1, \Lambda_2, \Lambda_3)$ is either triangular or conic-line type. The latter case cannot actually occur as Λ_1 contains Γ_1 and hence it contains at least three collinear points.

Therefore $\{P, Q\} \cap \{P_i, Q_i\} = \emptyset$ may be assumed. Then the H-members from Λ_2 and Λ_3 lie on four lines, namely PP_i, PQ_i, QP_i, QQ_i. Observe that these lines may be assumed to be pairwise distinct, otherwise Λ_2 (or Λ_3) is contained in a line, and again $(\Lambda_1, \Lambda_2, \Lambda_3)$ is triangular. Therefore, half of the H-members from Λ_2 lie on one of these four lines, say PQ_i, and half of them on QP_i. Similarly, each of the lines PP_i and QQ_i contain half from the H-members from Λ_3.

In the above argument, any H-member Γ_2 from Λ_2 may play the role of Γ_1. Therefore there exist two lines such that each H-member from Λ_1 lies on one or on other line. Actually, these two lines are PQ and P_iQ_i since each of them contains a H-member from Λ_1. In this case, $(\Lambda_1, \Lambda_2, \Lambda_3)$ is of tetrahedron type. □

Since a dihedral group of order ≥ 8 has a unique cyclic subgroup of index 2 and such a subgroup is characteristic, Propositions 10.31 and 10.20 have the following corollary.

Proposition 10.32. *Let G be a finite group of order $n \geq 12$ containing a normal dihedral subgroup D. If G is realized by a dual 3-net then G is itself dihedral.*

10.6. Dual 3-nets preserved by projectivities

Proposition 10.33. *Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net of order $n \geq 4$ realizing a group G. If every point in Λ_1 is the center of an involutory homology which preserves Λ_1 while interchanges Λ_2 with Λ_3, then either Λ_1 is contained in a line, or $n = 9$. In the latter case, $(\Lambda_1, \Lambda_2, \Lambda_3)$ lies on a non-singular cubic $\mathcal{F}$ whose inflection points are the points in Λ_1.*

Proof. After labeling $(\Lambda_1, \Lambda_2, \Lambda_3)$ naturally, take an element $a \in G$ and denote by φ_a the (unique) involutory homology of center A_1 which maps Λ_2 onto Λ_3. Obviously, φ_a also maps Λ_3 onto Λ_2. Moreover, $\varphi_a(X_2) = Y_3 \Longleftrightarrow a \cdot x = y$, that is, $\varphi_a(X_2) = \varphi_{a'}(X_2') \Longleftrightarrow a \cdot x = a' \cdot x'$, where $G = (G, \cdot)$. Therefore,

$$\varphi_{a'}\varphi_a(X_2) = X_2' \Longleftrightarrow (a'^{-1} \cdot a) \cdot x = x'. \tag{10.6}$$

From this, for any $b \in G$ there exists $b' \in G$ such that

$$\varphi_{a'}\varphi_a(X_2) = \varphi_{b'}\varphi_b(X_2) \tag{10.7}$$

for every $X_2 \in \Lambda_2$, equivalently, for every $x \in G$.

Let Φ be the the projectivity group generated by all products $\varphi_{a'}\varphi_a$ where both a, a' range over G. Obviously, Φ leaves both Λ_2 and Λ_3 invariant. In particular, Φ induces a permutation group on Λ_2. We show that if $\mu \in \Phi$ fixes Λ_2 pointwise then μ is trivial. Since $n > 3$, the projectivity μ has at least four fixed points in $PG(2, \mathbb{K})$. Therefore, μ is either trivial, or a homology. Assume that μ is non-trivial, and let C be the center and c the axis of μ. Take a line ℓ through C that contains a point $P \in \Lambda_3$, and assume that C is a point in Λ_2. Then P is the unique common point of ℓ and Λ_3. Since μ preserves Λ_2, μ must fix P. Therefore, μ fixes Λ_3 pointwise, and hence Λ_3 is contained in c. But then μ cannot fix any point in Λ_2 other than C since the definition of a dual 3-net implies that c is disjoint from Λ_2. This contradiction means that μ is trivial, that is, Φ acts faithfully on Λ_2.

Therefore, (10.7) states that for any $a, a', b \in G$ there exists $b' \in G$ satisfying the equation $\varphi_{a'}\varphi_a = \varphi_{b'}\varphi_b$. This yields that Φ is an abelian group of order n acting on Λ_2 as a sharply transitive permutation group. Also,

$$\Phi = \{\varphi_a\varphi_e \mid a \in G\}$$

where e is the identity of G. Therefore, $\Phi \cong G$, and G is abelian.

Let Ψ be the projectivity group generated by Φ together with some φ_a where $a \in G$. Then $|\Psi| = 2n$ and Ψ comprises the elements in Ψ and the involutory homologies φ_a with a ranging over G. Obviously, Ψ interchanges Λ_2 and Λ_3 while it leaves Λ_1 invariant acting on Λ_1 as a transitive permutation group.

Two cases are investigated according as Φ contains a homology or does not. Observe that Φ contains no elation, since every elation has infinite order when $p = 0$ while it's order is at least p when $p > 0$ but $p > n$ is assumed throughout the chapter.

In the former case, let $\rho \in \Phi$ be a homology with center $C \in \Lambda_1$ and axis c. Since ρ commutes with every element in Φ, the point C is fixed by Φ, and the line is preserved by Φ. Assume that C is also the center of ϕ_a with some $a \in G$. The group of homologies generated by ϕ_a and ρ preserves every line through C and it has order bigger than 2. But then it cannot interchange Λ_2 with Λ_3. Therefore, the center of every ϕ_a with $a \in G$ lies on c. This shows that Λ_1 is contained in c.

In the case where Φ contains no homology, Φ has odd order and $\delta \in \Phi$ has three fixed points which are the vertices of a triangle Δ. Since δ commutes with every element in Φ, the triangle Δ is left invariant by Φ.

If Φ fixes each vertex of δ, then Φ must be cyclic otherwise Ψ would contain a homology. Therefore Ψ is a dihedral group, and we show that Λ_1 is contained in a line. For this purpose, take a generator $\rho = \varphi_a\varphi_b$ of Φ, and consider the line ℓ through the centers of φ_a and φ_b. Obviously, ρ preserves ℓ, and this holds true for every power of ρ. Hence Ψ also preserves ℓ. Since every φ_c is conjugate to φ_a under Ψ, this shows that the center of φ_c must lie on ℓ, as well. Therefore Λ_1 is contained in ℓ.

We may assume that some $\rho \in \Phi$ acts on the vertices of Δ as a 3-cycle. Let Δ' be the triangle whose vertices are the fixed points of ρ. Then $\rho^3 = 1$ since ρ^3 fixes not only the vertices of Δ' but also those of Δ'. Therefore $\Phi = \langle\rho\rangle \times \Theta$ where Θ is the cyclic subgroup of Φ fixing each vertex of Δ. A subgroup of Θ of index ≤ 3 fixes each vertex of Δ', and hence it is trivial. Therefore, $|\Theta| = 3$ and $\Phi \cong C_3 \times C_3$. This shows that $n = 9$ and if Λ_1 is not contained in a line then the configuration of their points, that is the the centers of the homologies in Ψ, is isomorphic to $AG(2, 3)$, the affine plane of order 3. Such a configuration can also be viewed as the set of the nine common inflection points of the non-singular plane cubics of a pencil $\mathcal{P}$, each cubic left invariant by Ψ. For a point $P_2 \in \Lambda_2$, take that cubic $\mathcal{F}$ in $\mathcal{P}$ that contains P_2. Since the orbit of P_2 under the action of Ψ consists of the points in $\Lambda_2 \cup \Lambda_3$, it follows that $\mathcal{F}$ contains each point of $(\Lambda_1, \Lambda, \Lambda_3)$. □

A corollary of Proposition 10.33 is the following result.

Proposition 10.34. *Let* $(\Lambda_1, \Lambda_2, \Lambda_3)$ *be a dual* 3*-net of order* $n \geq 4$ *realizing a group* G*. If every point of* $(\Lambda_1, \Lambda_2, \Lambda_3)$ *is the center of an involutory homology which preserves* $(\Lambda_1, \Lambda_2, \Lambda_3)$*, then* $(\Lambda_1, \Lambda_2, \Lambda_3)$ *is triangular.*

Proof. From Proposition 10.17 and Example 10.16, $(\Lambda_1, \Lambda_2, \Lambda_3)$ is not of conic-line type. For $n = 9$, $(\Lambda_1, \Lambda_2, \Lambda_3)$ does not lie on any non-singular cubic $\mathcal{F}$ since no non-

singular cubic has twenty-seven inflection points. Therefore the assertion follows from Proposition 10.33. □

A useful generalization of Proposition 10.34 is given in the proposition below.

Proposition 10.35. *Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net of order $n \geq 4$ realizing a group G. Let $\mathcal{U}$ be the set of all involutory homologies preserving $(\Lambda_1, \Lambda_2, \Lambda_3)$ whose centers are points of $(\Lambda_1, \Lambda_2, \Lambda_3)$. If $|\mathcal{U}| \geq 3$ and $\mathcal{U}$ contains two elements whose centers lie in different components, then the following assertions hold:*

(i) *every component contains the same number of points that are centers of involutory homologies in $\mathcal{U}$.*

(ii) *the points of $(\Lambda_1, \Lambda_2, \Lambda_3)$ which are centers of involutory homologies in $\mathcal{U}$ form a triangular dual 3-subnet $(\Gamma_1, \Gamma_2, \Gamma_3)$.*

(iii) *Let M be the cyclic subgroup associated to $(\Gamma_1, \Gamma_2, \Gamma_3)$. Then either $(\Lambda_1, \Lambda_2, \Lambda_3)$ is also triangular, or*

$$|G| < \begin{cases} |G:M|^2, & \text{when } \gcd.(3, |G|) = 1; \\ 3|G:M|^2, & \text{when } \gcd.(3, |G|) = 3. \end{cases}$$

Proof. Let $\mathcal{G}$ be the projectivity group preserving $(\Lambda_1, \Lambda_2, \Lambda_3)$. Let (ijk) denote any permutation of (123). As we have already observed in the proof of Proposition 10.33, if $\varphi \in \mathcal{G}$ is an involutory homology with center $P \in \Lambda_i$, then φ preserves Λ_i and interchanges Λ_j with Λ_k. If $\sigma \in \mathcal{G}$ is another involutory homology with center $R \in \Lambda_j$ then $\sigma\varphi\sigma$ is also an involutory homology whose center S is the common point of Λ_k with the line ℓ through P and R. In terms of dual 3-subnets, this yields (i) and (ii). Let m be the order of $(\Gamma_1, \Gamma_2, \Gamma_3)$. For $m = 2$, $(\Gamma_1, \Gamma_2, \Gamma_3)$ is triangular. For $m = 3$, $\Gamma_1 \cup \Gamma_2 \cup \Gamma_3$ is the Hesse configuration, and hence $(\Gamma_1, \Gamma_2, \Gamma_3)$ is triangular. This holds true for $m \geq 4$ by Proposition 10.34 applied to $(\Gamma_1, \Gamma_2, \Gamma_3)$.

To prove (iii), assume that $(\Lambda_1, \Lambda_2, \Lambda_3)$ is not triangular and take a point P from some component, say Λ_3, that does not lie on the sides of the triangle associated to $(\Gamma_1, \Gamma_2, \Gamma_3)$. Since $(\Gamma_1, \Gamma_2, \Gamma_3)$ is triangular, it can play the role of $(\Lambda_1, \Lambda_2, \Lambda_3)$ in Section 10.3.2, and we use the notation introduced there. From the second assertion of Proposition 10.14, the point has as many as $|\Theta|$ distinct images, all lying in Λ_3. Therefore, $|G| = |\Lambda_3| > |\Theta|$. Using Proposition 10.14, $|\Theta|$ can be written in function of $|M|$ giving the assertion □

Let $\mathcal{U}_2$ be the set of all involutory homologies with center in Λ_2 which interchanges Λ_1 and Λ_3. There is a natural injective map Ψ from $\mathcal{U}_2$ to G where $\Psi(\psi) = g$ holds if and only if the point $g_2 \in \Lambda_2$ is the center of ψ.

Proposition 10.36. *Let $(\Lambda_1, \Lambda_2, \Lambda_3)$ be a dual 3-net of order $n \geq 4$ realizing a group G. If $|\mathcal{U}_2| \geq 2$ then the following hold.*

(i) *$\mathcal{U}_2$ is closed by conjugation, that is, $\psi\omega\psi \in \mathcal{U}_2$ whenever $\psi, \omega \in \mathcal{U}_2$.*

(ii) *If* $g, h \in \Psi(\mathcal{U}_2)$ *then* $gh^{-1}g \in \Psi(\mathcal{U}_2)$.

(iii) *If* G *has a cyclic subgroup* H *of order* 6 *with* $|H \cap \Psi(\mathcal{U}_2)| \geq 3$ *and* $1 \in H \cap \Psi(\mathcal{U}_2)$, *then either* $\Psi(\mathcal{U}_2) = H$, *or* $\Psi(\mathcal{U}_2)$ *is the subgroup of* H *of order* 3.

Proof. For $\psi, \omega \in \mathcal{U}_2$, the conjugate $\tau = \psi\omega\psi$ of ω by ψ is also an involutory homology. Let $g = \Psi(\psi)$ and $h = \Psi(\omega)$. Then the center of τ is $\psi(h_2)$. For $x \in G$, the image of x_1 under τ is $y_3 \in \Lambda_3$ with $y = xgh^{-1}g$. This shows that the center of τ is also in Λ_2; more precisely

$$\Psi(\psi\omega\psi) = \Psi(\psi)(\Psi(\omega))^{-1}\Psi(\psi). \tag{10.8}$$

In the case where G has a cyclic subgroup H of order 6, assume the existence of three distinct elements $\psi, \omega\, \rho \in \mathcal{U}_2$ such that $g = \Psi(\psi)$, $h = \Psi(\omega)$, and $r = \Psi(\rho)$ with $g, h, r \in H$. Then H contains $gh^{-1}g$, $hg^{-1}h$, g^2 and h^2. From this assertion (iii) follows. □

10.7. Dual 3-nets containing algebraic 3-subnets of order n with $n \geq 5$.

A key result is the following proposition.

Proposition 10.37. *Let* G *be a group containing a proper abelian subgroup* H *of order* $n \geq 5$. *Assume that a dual* 3*-net* $(\Lambda_1, \Lambda_2, \Lambda_3)$ *realizes* G *such that all its dual* 3*-subnets* $(\Gamma_1^j, \Gamma_2, \Gamma_3^j)$ *realizing* H *as a subgroup of* G *are algebraic. Let* $\mathcal{F}_j$ *be the cubic through the points of* $(\Gamma_1^j, \Gamma_2, \Gamma_3^j)$. *If* $(\Lambda_1, \Lambda_2, \Lambda_3)$ *is not algebraic then* Γ_2 *contains three collinear points and one of the following holds:*

(i) Γ_2 *is contained in a line.*

(ii) $n = 5$ *and there is an involutory homology with center in* Γ_2 *which preserves every* $\mathcal{F}_j$ *and interchanges* Λ_1 *and* Λ_3.

(iii) $n = 6$ *and there are three involutory homologies with center in* Γ_2 *which preserves every* $\mathcal{F}_j$ *and interchanges* Λ_1 *and* Λ_3.

(iv) $n = 9$ *and* Γ_2 *consists of the nine common inflection points of* $\mathcal{F}_j$.

Lemma 10.38. *Let* $A = (A, \oplus)$, $B = (B, +)$ *be abelian groups and consider the injective maps* $\alpha, \beta, \gamma : A \to B$ *such that* $\alpha(x) + \beta(y) + \gamma(z) = 0$ *if and only if* $z = x \oplus y$. *Then,* $\alpha(x) = \varphi(x) + a$, $\beta(x) = \varphi(x) + b$, $\gamma(x) = -\varphi(x) - a - b$ *for some injective homomorphism* $\varphi : A \to B$ *and elements* $a, b \in B$.

Proof. Define $a = \alpha(0)$, $b = \beta(0)$ and $\varphi(x) = -\gamma(x) - a - b$. For $x = 0$, $z = y$, we obtain that $\alpha(0) + \beta(y) + \gamma(y) = 0$ whence $\beta(y) = -\gamma(y) - a = \varphi(y) + b$. Similarly,

for $y = 0$, $z = x$, we obtain that $\alpha(x)+\beta(0)+\gamma(x) = 0$ whence $\alpha(x) = -\gamma(x)-b = \varphi(x) + a$. Finally, for any $x, y \in G$

$$\begin{aligned}\varphi(x) + \varphi(y) - \varphi(x + y) &= \varphi(x) + a + \varphi(y) + b - (\varphi(x + y) + a + b)\\ &= \alpha(x) + \beta(y) + \gamma(x + y) = 0.\end{aligned}$$

Therefore, $\varphi : A \to B$ is a group homomorphism. □

Let $A = (A, \oplus)$ be an abelian group and α, β, γ injective maps from A to $PG(2, \mathbb{K})$. The triple (α, β, γ) is a *realization* of A if the points $\alpha(x), \beta(y), \gamma(z)$ are collinear if and only if $z = x \oplus y$. Since $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizes G, the natural labeling gives rise to a realization (α, β, γ) such that $\alpha(G) = \Lambda_1$, $\beta(G) = \Lambda_2, \gamma(G) = \Lambda_3$. Let $u \in G$. Since H is a subgroup of G, the triple

$$(\alpha_u(x) = \alpha(ux), \beta(y) = \beta(y), \gamma_u(z) = \alpha(uz))$$

provides a realization of H such that

$$\alpha_u(H) = \Gamma_1^u,\ \beta(H) = \Gamma_2,\ \gamma_u(H) = \Gamma_3^u.$$

Therefore, Lemma 10.38 has the following corollary where $(\mathcal{F}_j, *)$ denotes the additive groups of the plane cubic $\mathcal{F}_j$ through the points of $(\Gamma_1^j, \Gamma_2, \Gamma_3^j)$ where, for $u = 1$, we write $(\mathcal{F}, +), \alpha, \beta, \gamma, \Gamma_1, \Gamma_2, \Gamma_3$.

Lemma 10.39. *There exist two realizations from H into $PG(2, \mathbb{K})$, say (α, β, γ) and $(\alpha_j, \beta_j, \gamma_j)$ with*

$$\alpha(H) = \Gamma_1,\ \beta(H) = \Gamma_2,\ \gamma(H) = \Gamma_3,\ \alpha_j(H) = \Gamma_1^j,\ \beta_j(H) = \Gamma_2,\ \gamma_j(H) = \Gamma_3^j$$

such that

$$\begin{gathered}\alpha(x) = \varphi(x) + a, \beta(y) = \varphi(y) + b, \gamma(z) = \varphi(z) + c,\\ \alpha_j(x) = \varphi_j(x) * a_j, \beta_j(y) = \varphi_j(y) * b_j, \gamma_j(z) = \varphi_j(z) * c_j\end{gathered}$$

for every $x, y, z \in H$ where both $\varphi : H \to (\mathcal{F}, +)$ and $\varphi_j : H \to (\mathcal{F}_j, *)$ are injective homomorphisms, and $\varphi(y) + b = \varphi_j(y) * b_j$ for every $y \in H$.

To prove Proposition 10.37 we point out that $3b \in \varphi(H)$ if and only if Γ_2 contains three collinear points. Suppose that $\varphi(x_1)+b, \varphi(x_2)+b, \varphi(x_3)+b$ are three collinear points. Then $\varphi(x_1)+b+\varphi(x_2)+b+\varphi(x_3)+b = 0$ whence $\varphi(x_1+x_2+x_3)+3b = 0$. Therefore $3b \in \varphi(H)$. Conversely, if $\varphi(t) = 3b$, take three pairwise distinct elements $x_1, x_2, x_3 \in H$ such that $x_1+x_2+x_3+t = 0$. Then $\varphi(x_1)+b+\varphi(x_2)+b+\varphi(x_3)+b = 0$. Therefore, the points $\varphi(x_1) + b, \varphi(x_2) + b$ and $\varphi(x_3) + b$ of Γ_2 are collinear. Notice that the element $t = -x_1-x_2-x_3 \in H$ is the same even if we make the computation with φ_j and b_j.

We separately deal with two cases.

10.7.1. Γ_2 contains no three collinear points

By the preceding observation, $3b \notin \varphi(H)$. For any $z \in H$ take four different elements x_1, y_1, x_2, y_2 in H such that

$$z = x_1 \oplus y_1 = x_2 \oplus y_2. \tag{10.9}$$

Then $\varphi(x_1)+b+\varphi(y_1)+b = \varphi(z)+2b = \varphi(x_2)+b+\varphi(y_2)+b$. Let $P_i = \beta(x_i)$, $Q_i = \beta(y_i)$ for $i = 1, 2$. Then $P_i \neq Q_i$ and the lines P_1Q_1 and P_2Q_2 meet in a point S in $\mathcal{F}$ outside Γ_2. The same holds for $\mathcal{F}_j$. Therefore each point S is a common point of $\mathcal{F}$ and $\mathcal{F}_i$ other than those in Γ_2. As S only depends on z which can be freely choosen if $|H| \geq 4$, there are at least n such points S. Hence, $\mathcal{F} \cap \mathcal{F}_j$ contains at least $2n \geq 10$ points. By Bézout's theorem either $\mathcal{F} = \mathcal{F}_j$, or they are reducible. We may assume that the latter case occurs. By Lemma 10.28, we may assume that both $(\Gamma_1, \Gamma_2, \Gamma_3)$ and $(\Gamma_1^j, \Gamma_2, \Gamma_3^j)$ are of conic-line type. Here Γ_2 is contained in an irreducible conic $\mathcal{C}$ which is a common component of $\mathcal{F}$ and $\mathcal{F}_j$. By Proposition 10.19, $\mathcal{F} = \mathcal{F}_j$.

10.7.2. Γ_2 contains three collinear points

This time, $3b \in \varphi(H)$. Let $\varphi(t) = 3b$ with $t \in H$. If either $\mathcal{F}$ or $\mathcal{F}_j$ is reducible, then Γ_2 is contained in a line. Therefore, both $\mathcal{F}$ and $\mathcal{F}_j$ are assumed to be irreducible.

First, suppose in addition that $t \notin 3H$. For any $x \in H$, let $y = 2(\ominus x) \ominus t$. Observe that $y \neq x$. From

$$2(\varphi(x) + b) + \varphi(y) + b = \varphi(t) + \varphi(2x) + \varphi(y) = 0,$$

the point $Q = \beta(y)$ is the tangential point of $P = \beta(x)$ on $\mathcal{F}$. Therefore, β determines the tangents of $\mathcal{F}$ at its points in Γ_2. This holds true for $\mathcal{F}_j$. From Lemma 10.39, $\mathcal{F}$ and $\mathcal{F}_j$ share the tangents at each of their common points in Γ_2. Therefore $|\mathcal{F} \cap \mathcal{F}_j| \geq 2n \geq 10$, and $\mathcal{F} = \mathcal{F}_j$ holds.

It remains to investigate the case where $3b = \varphi(3t_0)$ holds for some $t_0 \in H$. Replacing b by $b - \varphi(t_0)$ shows that $3b = 0$ may be assumed. Therefore, the point $P = \varphi(y) + b$ with $y \in H$ is an inflection point of $\mathcal{F}$ if and only if $3y = 0$. Furthermore, if $3y \neq 0$ then $Q = \varphi(\ominus(2y)) + b$ is the tangential point of P on $\mathcal{F}$. Therefore, β determines the tangents of $\mathcal{F}$ at its points in Γ_2. The same holds true for $\mathcal{F}_j$. By Lemma 10.39, $P = \beta(y)$ is an inflection point of both $\mathcal{F}$ and $\mathcal{F}_j$ or none of them. In the latter case, $\mathcal{F}$ and $\mathcal{F}_j$ have the same tangent at P.

Let m be the number of common inflection points of $\mathcal{F}$ and $\mathcal{F}_j$ lying in Γ_2. Obviously, $P = \varphi(0) + b$ is such a point, and hence $m \geq 1$. On the other hand, m may assume only three values, namely 1, 3 and 9. If $m = 9$, then $\mathcal{F}$ is non-singular and Γ_2 consists of all the nine inflection points of $\mathcal{F}$. The same holds for $\mathcal{F}_j$. If $m = 3$ then $\mathcal{F}$ and $\mathcal{F}_j$ share their tangents at $n - 3$ common points. Therefore, $2n - 3 \leq 9$ whence $n \leq 6$.

If $n = 6$ there are three common inflection points of $\mathcal{F}$ and $\mathcal{F}_j$, and they are collinear. Let H be the additive group of integers modulo 6. Then the inflection

points of $\mathcal{F}$ lying on Γ_2 are $P_i = \varphi(i) + b$ with $i = 0, 2, 4$ while the tangential point of $P_i = \varphi(i) + b$ with $i = 1, 3, 5$ is $P_{-2i} = \varphi(-2i) + b$. Now fix a projective frame with homogeneous coordinates (X, Y, Z) in such a way that

$$P_0 = (1, 0, 1),\ P_1 = (0, 0, 1),\ P_2 = (0, 1, 1),$$
$$P_3 = (0, 1, 0),\ P_4 = (-1, 1, 0),\ P_5 = (1, 0, 0).$$

A straightforward computation shows that $\mathcal{F}_j$ is in the pencil $\mathcal{P}$ comprising the cubics $\mathcal{G}_\lambda$ of equation

$$(X - Z)(Y - Z)(X + Y) + \lambda XYZ = 0, \quad \lambda \in \mathbb{K},$$

with the cubic $\mathcal{G}_\infty$ of equation $XYZ = 0$. The intersection divisor of the plane cubics in $\mathcal{P}$ is $P_0 + P_2 + P_4 + 2P_1 + 2P_3 + 2P_5$. Moreover, the points P_0, P_2, P_4 are inflection points of all irreducible cubics in $\mathcal{P}$, and

$$\psi_0 : (X, Y, Z) \to (Z, -Y, X),$$
$$\psi_2 : (X, Y, Z) \to (-X, Z, Y),$$
$$\psi_4 : (X, Y, Z) \to (Y, X, Z),$$

are the involutory homologies preserving every cubic in $\mathcal{P}$, the center of ψ_i being P_i, for $i = 0, 2, 4$.

If $n = 5$, the zero of H is the only element y with $3y = 0$. This shows that $\mathcal{F}$ (and $\mathcal{F}_j$) has only one inflection point P_0 in Γ_2 and P_0 is not the tangential point of another point in Γ_2. Each of the remaining four points is the the tangential point of exactly one point in Γ_2. These four points may be viewed as the vertices of a quadrangle $P_1P_2P_3P_4$ such that the side P_iP_{i+1} is tangent to $\mathcal{F}$ at P_i for every i with $P_5 = P_1$. Therefore the intersection divisor of $\mathcal{F}$ and $\mathcal{F}_j$ is $P_0+2P_1+2P_2+2P_3+2P_4$, and $\mathcal{F}_j$ is contained in a pencil $\mathcal{P}$.

Fix a projective frame with homogeneous coordinates (X, Y, Z) in such a way that

$$P_1 = (0, 0, 1),\ P_2 = (1, 0, 0),\ P_3 = (1, 1, 1),\ P_4 = (0, 1, 0).$$

Then $P_0 = (1, 1, 0)$. The pencil $\mathcal{P}$ is generated by the cubics $\mathcal{G}$ and $\mathcal{D}$ with equations $Y(X - Z)Z = 0$ and $X(Y - X)(Y - Z) = 0$, respectively. Therefore it consists of cubics G_λ with equation

$$Y^2X - X^2Y + (\lambda - 1)XYZ + X^2Z - \lambda YZ^2 = 0,$$

together with $\mathcal{G} = \mathcal{G}_\infty$. Since the line $Z = 0$ contains three distinct base points of the pencil, P_0 is a non-singular point of $\mathcal{G}_\lambda$ for every $\lambda \in \mathbb{K}$, the tangent ℓ_λ to $\mathcal{G}_\lambda$ at P_0 has equation $-X + Y + \lambda Z = 0$. Assume that Q_0 is an inflection point of $\mathcal{G}_\lambda$. Then ℓ_λ contains no point $P = (X, Y, 1)$ from $\mathcal{G}_\lambda$, that is, the polynomials $Y^2X - X^2Y + (\lambda - 1)XY + X^2 - \lambda Y = 0$ and $-X + Y + \lambda = 0$ have no common solutions. On the other hand, eliminating Y from these polynomials gives λ^2. This

shows that Q_0 is an inflection point for every irreducible cubic in $\mathcal{P}$. Hence $P_0 = Q_0$. Therefore the involutory homology

$$\varphi : (X, Y, Z) \mapsto (-Y + Z, -X + Z, Z)$$

with center P_0 preserves each cubic in $\mathcal{P}$.

This completes the proof of Proposition 10.37.

In the case where H is an abelian normal subgroup of G, we have the following result.

Proposition 10.40. *Let G be a group containing a proper abelian normal subgroup H of order $n \geq 5$. If a dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizes G such that all its dual 3-subnets realizing H as a subgroup of G are algebraic, then either* (I) *or* (II) *of Theorem 10.1 holds.*

Proof. The essential tool in the proof is Proposition 10.37. Assume on the contrary that neither (I) nor (II) occurs.

If every H-member is contained in a line then every dual 3-net realizing H as a subgroup of G is triangular. From Proposition 10.31, either (I) of (II) follows.

Take a H-member not contained in a line. Since H is a normal subgroup, that H-member can play the role of Γ_2 in Proposition 10.37. Therefore, one of the three sporadic cases in Proposition 10.37 holds. Furthermore, from the proof of that proposition, every $\mathcal{F}_j$ is irreducible, and hence neither Γ_1^j nor Γ_3^j is contained in a line. Therefore, no H-member is contained in a line. Since H is a normal subgroup, every 3-subnet $(\Gamma_1^i, \Gamma_2^j, \Gamma_3^s)$ realizing H as a subgroup of G lies in an irreducible plane cubic $\mathcal{F}(i, j)$.

Therefore we can assume that all H-members have the exceptional configurations described in (ii), (iii) or (iv) of Proposition 10.37. We separately deal with the cases $n = 5, 6$ and 9.

10.7.3. $n = 9$

From (iv) of Proposition 10.37, the cubics $\mathcal{F}_j$ share their nine inflection points which form Γ_2. So it is possible to avoid this case by replacing Γ_2 with Γ_1 so that Γ_2 will not have any inflection point of $\mathcal{F}$.

10.7.4. $n = 6$

Every H-member Γ_2 contains three collinear points, say Q_1, Q_2, Q_3, so that Q_r is the center of an involutory homology ψ_r interchanging Λ_1 and Λ_3. Relabeling the points of the dual 3-net permits us to assume that $Q_1 = 1_2$. Then for all $x \in G$, ψ_1 interchanges the points x_1 and x_3. The point $a_2 \in \Lambda_2$ is the intersection of the lines $y_1(ya)_3$, with $y \in G$. These lines are mapped to the lines $(ya)_1 y_3$, which all contain the point $(a^{-1})_2$ of Λ_2. Therefore, the involutory homology ψ_1 leaves Λ_2 invariant. This holds true for all involutory homologies with center in $\Lambda_1 \cup \Lambda_2 \cup$

Λ_3. Since the H-members partition each component of $(\Lambda_1, \Lambda_2, \Lambda_3)$ and every H-member comprises six points, it turns out that half of the points of $(\Lambda_1, \Lambda_2, \Lambda_3)$ are the centers of involutory homologies preserving $(\Lambda_1, \Lambda_2, \Lambda_3)$. Therefore, Proposition 10.35(iii) applies. As in Proposition 10.35, let M denote the subgroup of G such that the dual 3-subnet consisting of the centers of involutory homologies realizes M. As $|G : M| = 2$, 10.35(iii) implies $|G| < 6$, a contradiction.

10.7.5. $n = 5$

The arguments in discussing case $n = 6$ can adapted for case $n = 5$. This time, Proposition 10.37 gives $|G : M| = 5$. By Proposition 10.35(iii), if G contains an element of order 3 then $|G| < 75$, otherwise $|G| < 25$. In the former case, the element of order 3 of G is in $C_G(H)$, hence G contains a cyclic normal subgroup of order 15. Then, $(\Lambda_1, \Lambda_2, \Lambda_3)$ is algebraic by Proposition 10.37. If G has no element of order three then $|G| < 25$ and G contains a normal subgroup of order 10 which is either cyclic or dihedral. By Propositions 10.32 and 10.37 either (I) or (II) of Theorem 10.1 holds. □

A corollary of Proposition 10.40 is the following result.

Theorem 10.41. *Every dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizing an abelian group G is algebraic.*

Proof. By absurd, let n be the smallest integer for which a counter-example $(\Lambda_1, \Lambda_2, \Lambda_3)$ to Theorem 10.41 exists. Since any dual 3-net of order ≤ 8 is algebraic by Propositions 10.21 and 10.24, we have that $n \geq 9$. Furthermore, again by Proposition 10.24, G has composite order. Since n is chosen to be as small as possible, from Proposition 10.40, $|G|$ has only one prime divisor, namely either 2 or 3. Since $|G| \geq 9$, either $|G| = 2^r$ with $r \geq 4$, or $|G| = 3^r$ with $r \geq 2$. In the former case, G has a subgroup M of order 8, and every dual 3-subnet realizing M is algebraic, by Proposition 10.21. But, this together with Proposition 10.40 show that $(\Lambda_1, \Lambda_2, \Lambda_3)$ is not a counter-example. In the latter case G contains no element of order 9 and hence it is an elementary abelian group. But then $(\Lambda_1, \Lambda_2, \Lambda_3)$ is algebraic by Proposition 10.22. □

10.8. Dual 3-nets realizing 2-groups

Proposition 10.42. *Let G be a group of order $n = 2^h$ with $h \geq 2$. If G can be realized by a dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ then one of the following holds.*

(i) *G is cyclic.*

(ii) *$G \cong C_m \times C_k$ with $n = mk$.*

(iii) *G is a dihedral.*

(iv) *G is the quaternion group of order* 8.

Proof. For $n = 4, 8$, the classification follows from Propositions 10.21, 10.29 and [Yuz04, Theorem 4.2]. Up to isomorphisms, there exist fourteen groups of order 16; each has a subgroup H of index 2 that is either an abelian or a dihedral group. In the latter case, G is itself dihedral, by Proposition 10.32. So, Proposition 10.40 applies to G and H yielding that G is abelian. This completes the proof for $n = 16$. By induction on h we assume that Proposition 10.42 holds for $n = 2^h \geq 16$ and we are going to show that this remains true for 2^{h+1}. Let H be a subgroup of G of index 2. Then $|H| = 2^h$ and one of the cases (i), (ii), and (iii) hold for H. Therefore, the assertion follows from Propositions 10.40 and 10.32. □

10.9. Dual 3-nets containing algebraic 3-subnets of order n with $2 \leq n \leq 4$.

It is useful to investigate separately two cases according as $n = 3, 4$ or $n = 2$. An essential tool in the investigation is $M = \mathcal{C}_G(H)$, the centralizer of H in G.

Proposition 10.43. *Let G be a finite group containing a normal subgroup H of order n with $n = 3$ or $n = 4$. Then every dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizing G is either algebraic, or of tetrahedron type, or, G is isomorphic either to the quaternion group of order 8, or to Alt_4, or to Sym_4.*

Proof. First we investigate the case where $M > H$. Take an element $m \in M$ outside H. Then the subgroup T of G generated by m and H is abelian, and larger than H. Since $|H| \geq 3$, then $|T| \geq 6$. If all H-members of $(\Lambda_1, \Lambda_2, \Lambda_3)$ are contained in a line then $(\Lambda_1, \Lambda_2, \Lambda_3)$ is either triangular or of tetrahedron type by Proposition 10.31. Assume that Γ_2 is an H-member which is not contained in a line. Let Γ_2' be the T-member containing Γ_2. We claim that $(\Lambda_1, \Lambda_2, \Lambda_3)$ is algebraic. If not then one of the exceptional cases (iii) or (iv) of Proposition 10.37 must hold. Clearly, in these cases $|H| = 3$. However, the centers of the involutory homologies mentioned in Proposition 10.37 correspond to the points in the H-member Γ_2. As these centers must be collinear, we obtain that Γ_2 is contained in a line, a contradiction.

Assume that $M = H$. Then G/H is an automorphism group H. If H is C_3 or C_4 then $|\mathrm{Aut}(H)| = 2$ and G is either a dihedral group or the quaternion group of order 8. If $H \cong C_2 \times C_2$, then G is a subgroup of Sym_4. The possibilities for G other than H and the dihedral group of order 8 are two, either Alt_4, or Sym_4. Since all these groups are allowed in the proposition, the proof is finished. □

Proposition 10.44. *Let G be a finite group with a central involution which contains no normal subgroup H of order 4. Then a dual 3-net $(\Lambda_1, \Lambda_2, \Lambda_3)$ realizing G is either algebraic or of tetrahedron type.*

Proof. Let H be the normal subgroup generated by the (unique) central involution of G. Two cases are separately investigated according as a minimal normal subgroup $\bar{N}$ of the factor group $\bar{G} = G/H$ is solvable or not. Let σ be the natural homomorphism $G \to \bar{G}$. Let $N = \sigma^{-1}(\bar{N})$.

If $\bar{N}$ is solvable, then $\bar{N}$ is an elementary abelian group of order d^h for a prime d. Furthermore, N is a normal subgroup of G and $\bar{N} = N/H$. If N is abelian, then $|N| \geq 6$ and the assertion follows from Proposition 10.40 and Theorem 10.41.

Bearing this in mind, the case where $d = 2$ is investigated first. Then N has order 2^{h+1} and is a normal subgroup of G. From Proposition 10.42, N is either abelian or it is the quaternion group Q_8 of order 8. We may assume that $N \cong Q_8$. From Proposition 10.42, N is not contained in a larger 2-subgroup of G. Therefore N is a (normal) Sylow 2-subgroup of G. We may assume that G is larger than N. If $M = C_G(N)$ is also larger than N, take an element $t \in M$ of outside N. Then t has odd order ≥ 3. The group T generated by N and t has order $8m$ and its subgroup D generated by t together with an element of N of order 4 is a (normal) cyclic subgroup of M of order $4m$. But this contradicts Proposition 10.40, as T is neither abelian nor dihedral. Therefore $M = N$, and hence G/N is isomorphic to a subgroup L of the automorphism group $\mathrm{Aut}(Q_8)$. Hence $|G|/|N|$ divides 24. On the other hand, since N is a Sylow 2-subgroup of G, $|G/N|$ must be odd. Therefore $|G| = 24$. Two possibilities arise according as either $G \cong SL(2,3)$ or G is the dicyclic group of order 24. The latter case cannot actually occur by Proposition 10.40 as the dicyclic group of order 24 has a (normal) cyclic subgroup of order 12.

To rule the case $G \cong SL(2,3)$ out we relay on Proposition 10.37 and 10.36 since $SL(2,3)$ has four cyclic groups of order 6. For this purpose, we show that every point in Λ_2 is the center of an involutory homology preserving $(\Lambda_1, \Lambda_2, \Lambda_3)$ whence the assertion will follow from Proposition 10.33 applied to Λ_2. With the notation in Section 10.6, (iii) Proposition 10.37 yields that $|\mathcal{U}_2| \geq 3$. With the notation introduced in the proof of Proposition 10.24, we may assume that the point 1_2 is the center of an involutory homology ϵ in $\mathcal{U}_2$. From (iii) of Proposition 10.36 every (cyclic) subgroup of G of order 6 provides (at least) two involutory homologies other than ϵ. Therefore, $|\mathcal{U}_2| \geq 9$, and every point $u_2 \in \Lambda_2$ such that $u^3 = 1$ is the center of an involutory homology in $\mathcal{U}$. A straightforward computation shows that every element in G other than the unique involution e can be written as $gh^{-1}g$ with $g^3 = h^3 = 1$. Thus $|\mathcal{U}| \geq 23$. The involutory homology with center e_2 cannot actually been an exception. To shows this, take an element $g \in G$ of order 4. Then g_2 is the center of an element in $\mathcal{U}$. Since $e = g^2 = g \cdot 1 \cdot g$, this holds true for e_2. Therefore $|\mathcal{U}| = 24$. From (i) of Proposition 10.36, $\mathcal{U}$ also preserves Λ_2. This completes the proof.

Now, the case of odd d is investigated. Since $|H| = 2$ and d are coprime, Zassenhaus' theorem [Hup67, 10.1 Hauptsatz] ensures a complement $W \cong \bar{N}$ such that $N = W \ltimes H = W \times H$. Obviously, W is an abelian normal subgroup of G of order at least 3. The assertion follows from Propositions 10.40 and 10.43.

If $\bar{N}$ is not solvable then it has a non-abelian simple group $\bar{T}$. Let $\bar{S}_2$ be a Sylow 2-subgroup of $\bar{T}$. By Proposition 10.42, the realizable 2-group S_2 is either cyclic,

product of two cyclic groups, dihedral or quaternion of order 8. Thus, $\bar{S}_2$ is either cyclic, product of two cyclic groups or dihedral. As $\bar{T}$ is simple, $\bar{S}_2$ cannot be cyclic. In the remaining cases we can use the classification of finite simple groups of 2-rank 2 to deduce that $\bar{T}$ is either $\bar{T} \cong PSL(2, q^h)$ with an odd prime q and $q^h \geq 5$, or $\bar{T} \cong \mathrm{Alt}_7$, cf. the Gorenstein-Walter theorem [GW65].

If $H \not\leq T'$ then $T = H \times T'$. As $T' \cong \bar{T}$, T' contains an elementary abelian subgroup of order 4, G contains an elementary abelian group of order 8, a contradiction. Therefore, T is a central extension of either $PSL(2, q^h)$, with q^h as before, or Alt_7, with a cyclic group of order 2. From a classical result of Schur [Asc86, Chapter 33], either $T \cong SL(2, q)$ or T is the unique central extension of Alt_7 with a cyclic group of order 2. In the latter case, no dual 3-net can actually realize T since Proposition 10.42 applies, a Sylow 2-subgroup of T being isomorphic to a generalized quaternion group of order 16. To finish the proof it suffices to observe that $SL(2, q^h)$, with q^h as before, contains $SL(2, 3)$ whereas no dual 3-net can realize $SL(2, 3)$ as we have already pointed out. □

10.10. 3-nets and non-abelian simple groups

Proposition 10.45. *If a dual 3-net realizes a non-abelian simple group G then $G \cong \mathrm{Alt}_5$.*

Proof. Let G be a non-abelian simple group, and consider a Sylow 2-subgroup S_2 of G. From Proposition 10.42, S_2 is dihedral since no Sylow 2-subgroup of a non-abelian simple group is either cyclic or the direct product of cyclic groups, see [Gor83, Theorem 2.168], or the quaternion group of order 8 , see [BS59]. From the Gorenstein-Walter theorem [GW65], either $G \cong PSL(2, q^h)$ with an odd prime q and $q^h \geq 5$, or $G \cong \mathrm{Alt}_7$. In the former case, G has a subgroup T of order $q^h(q^h - 1)/2$ containing a normal subgroup of order q^h. Here T is not abelian and is dihedral only for $q^h = 5$. Therefore, Theorem 10.41 and Proposition 10.40 leave only one case, namely $q = 5$. This also shows that Alt_7 cannot occur since Alt_7 contains $PSL(2, 7)$. □

Notice that by Proposition 10.23, computer results [NP13] show that if $p = 0$ then Alt_4 cannot be realized in $PG(2, \mathbb{K})$. This implies that that no dual 3-net can realize Alt_5.

10.11. The proof of Theorem 10.1

Take a minimal normal subgroup H of G. If H is not solvable then H is either a simple group or the product of isomorphic simple groups. From Proposition 10.26, the latter case cannot actually occur as every simple group contains an elementary abelian subgroup of order 4. Therefore, if H is not solvable, $H \cong \mathrm{Alt}_5$ may be assumed by Proposition 10.45. Two cases are considered separately according as

the centralizer $C_G(H)$ of H in G is trivial or not. If $|C_G(H)| > 1$, take a non-trivial element $u \in C_G(H)$ and define U to be the subgroup of G generated by u together with a dihedral subgroup D_5 of H of order 10. Since u centralizes D_5, the latter subgroup is a normal subgroup of U. Hence D_5 a normal dihedral subgroup of U. From Proposition 10.32, M itself must be dihedral. Since the center of a dihedral group has order 2, this implies that u is an involution. Now, the subgroup generated by u together with an elementary abelian subgroup of H of order 4 generate an elementary abelian subgroup of order 8. But this contradicts Proposition 10.26. Therefore, $C_G(H)$ is trivial, equivalently, G is contained in the automorphism group of H. From this, either $G = H$ or $G \cong PGL(2, 5)$. In the latter case, G contains a subgroup isomorphic to the semidirect product of C_5 by C_4. But this contradicts Proposition 10.32. Therefore, if H is not solvable then $H \cong \mathrm{Alt}_5$.

If H is solvable then it is an elementary abelian group of order $d \geq 2$. If d is a power of 2 then $d = 2$ or $d = 4$ and Theorem 10.1 follows from Propositions 10.42 and 10.44. If d is a power of an odd prime, Theorem 10.1 is obtained by Propositions 10.40 and 10.43. □

Bibliography

[Alb43] A. A. Albert. "Quasigroups. I". In: *Transactions of the American Mathematical Society* 54 (1943), 507–519.

[Alb44] A. A. Albert. "Quasigroups. II". In: *Transactions of the American Mathematical Society* 55 (1944), 401–419.

[Alb61] A. A. Albert. "Generalized twisted fields". In: *Pacific Journal of Mathematics* 11 (1961), 1–8.

[Alp86] J. L. Alperin. *Local representation theory*. Vol. 11. Cambridge Studies in Advanced Mathematics. Modular representations as an introduction to the local representation theory of finite groups. Cambridge: Cambridge University Press, 1986.

[Asc86] M. Aschbacher. *Finite group theory*. Vol. 10. Cambridge Studies in Advanced Mathematics. Cambridge: Cambridge University Press, 1986.

[Asc05] M. Aschbacher. "On Bol loops of exponent 2". In: *Journal of Algebra* 288.1 (2005), 99–136.

[Asc06] M. Aschbacher. "Projective planes, loops, and groups". In: *Journal of Algebra* 300.2 (2006), 396–432.

[AKP06] M. Aschbacher, M. K. Kinyon, and J. D. Phillips. "Finite Bruck loops". In: *Transactions of the American Mathematical Society* 358.7 (2006), 3061–3075.

[Bae39] R. Baer. "Nets and groups". In: *Transactions of the American Mathematical Society* 46 (1939), 110–141.

[Bau12] B. Baumeister. "Do finite Bruck loops behave like groups?" In: *Commentationes Mathematicae Universitatis Carolinae* 53.3 (2012), 337–346.

[BS11] B. Baumeister and A. Stein. "The finite Bruck loops". In: *Journal of Algebra* 330 (2011), 206–220.

[BSS11] B. Baumeister, G. Stroth, and A. Stein. "On Bruck loops of 2-power exponent". In: *Journal of Algebra* 327.1 (Feb. 2011), pp. 316–336.

[BS10] B. Baumeister and A. Stein. "Self-invariant 1-factorizations of complete graphs and finite Bol loops of exponent 2". In: *Beiträge zur Algebra und Geometrie. Contributions to Algebra and Geometry* 51.1 (2010), 117–135.

[Bel67] V. D. Belousov. *Foundations of the theory of quasigroups and loops [Osnovy teorii kvazigrupp i lup]*. Izdat. "Nauka", Moscow, 1967.

[BKM11] A. Blokhuis, G. Korchmáros, and F. Mazzocca. "On the structure of 3-nets embedded in a projective plane". In: *Journal of Combinatorial Theory, Series A* 118.4 (May 2011), pp. 1228–1238.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. "The Magma algebra system. I. The user language". In: *Journal of Symbolic Computation* 24.3-4 (1997). Computational algebra and number theory (London, 1993), 235–265.

[BS59] R. Brauer and M. Suzuki. "On finite groups of even order whose 2-Sylow group is a quaternion group". In: *Proceedings of the National Academy of Sciences of the United States of America* 45 (1959), 1757–1759.

[BCN89] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-regular graphs*. Vol. 18. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Berlin: Springer-Verlag, 1989.

[Bru58] R. H. Bruck. *A survey of binary systems*. Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge, Heft 20. Reihe: Gruppentheorie. Berlin: Springer Verlag, 1958.

[Bur78] R. P. Burn. "Finite Bol loops". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 84.3 (1978), 377–385.

[Buz09] M. Á. M. Buzunáriz. "A Description of the Resonance Variety of a Line Combinatorics via Combinatorial Pencils". In: *Graphs and Combinatorics* 25.4 (Nov. 2009), pp. 469–488.

[Cam03] P. J. Cameron. "Research problems from the 18th British Combinatorial Conference". In: *Discrete Mathematics* 266.1-3 (2003). The 18th British Combinatorial Conference (Brighton, 2001), 441–451.

[CK93] P. J. Cameron and G. Korchmáros. "One-factorizations of complete graphs with a doubly transitive automorphism group". In: *The Bulletin of the London Mathematical Society* 25.1 (1993), 1–6.

[CD98] C. Charnes and U. Dempwolff. "The translation planes of order 49 and their automorphism groups". In: *Mathematics of Computation* 67.223 (1998), 1207–1224.

[CPS90] O. Chein, H. O. Pflugfelder, and J. D. H. Smith, eds. *Quasigroups and loops: theory and applications*. Vol. 8. Sigma Series in Pure Mathematics. Berlin: Heldermann Verlag, 1990.

[Con88] J. H. Conway. "The Golay Codes and The Mathieu Groups". In: *Sphere Packings, Lattices and Groups*. Grundlehren der mathematischen Wissenschaften 290. Springer New York, Jan. 1988, pp. 299–330.

[CS03] J. H. Conway and D. A. Smith. *On quaternions and octonions: their geometry, arithmetic, and symmetry*. Natick, MA: A K Peters Ltd., 2003.

[Dem68] P. Dembowski. *Finite geometries*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Berlin: Springer-Verlag, 1968.

[Dem94] U. Dempwolff. "Translation planes of order 27". In: *Designs, Codes and Cryptography. An International Journal* 4.2 (1994), 105–121.

[Dor78] S. Doro. "Simple Moufang loops". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 83.3 (1978), 377–392.

[Drá02] A. Drápal. "Multiplication groups of loops and projective semilinear transformations in dimension two". In: *Journal of Algebra* 251.1 (2002), 256–278.

[FY07] M. Falk and S. Yuzvinsky. "Multinets, resonance varieties, and pencils of plane curves". In: *Compositio Mathematica* 143.4 (2007), 1069–1088.

[Fig06] A. Figula. "Bol loops as sections in semi-simple Lie groups of small dimension". In: *Manuscripta Mathematica* 121.3 (2006), 367–384.

[FS09] A. Figula and K. Strambach. "Subloop incompatible Bol loops". In: *Manuscripta Mathematica* 130.2 (2009), 183–199.

[Fis64] B. Fischer. "Distributive Quasigruppen endlicher Ordnung". In: *Mathematische Zeitschrift* 83 (1964), 267–303.

[FK10] T. Foguel and M. Kinyon. "Uniquely 2-divisible Bol loops". In: *Journal of Algebra and its Applications* 9.4 (2010), 591–601.

[FKP06] T. Foguel, M. K. Kinyon, and J. D. Phillips. "On twisted subgroups and Bol loops of odd order". In: *The Rocky Mountain Journal of Mathematics* 36.1 (2006), 183–212.

[FD77] P. Frankl and M. Deza. "On the maximum number of permutations with given maximal or minimal distance". In: *Journal of Combinatorial Theory. Series A* 22.3 (1977), 352–360.

[Gap] *GAP – Groups, Algorithms, and Programming, Version 4.4.12*. The GAP Group. 2008.

[Giu06] M. Giudici. "Factorisations of sporadic simple groups". In: *Journal of Algebra* 304.1 (2006), 311–323.

[Gla64] G. Glauberman. "On loops of odd order". In: *Journal of Algebra* 1 (1964), 374–396.

[Gla68] G. Glauberman. "On loops of odd order. II". In: *Journal of Algebra* 8 (1968), 393–414.

[Gor83] D. Gorenstein. *The classification of finite simple groups. Vol. 1.* The University Series in Mathematics. Groups of noncharacteristic 2 type. New York: Plenum Press, 1983.

[GW65] D. Gorenstein and J. H. Walter. "The characterization of finite groups with dihedral Sylow 2-subgroups. I". In: *Journal of Algebra* 2 (1965), 85–151.

[GN11] A. Grishkov and G. P. Nagy. "Algebraic Bol loops". In: *Forum Mathematicum* 23.3 (2011), 655–668.

[GZ05] A. N. Grishkov and A. V. Zavarnitsine. "Lagrange's theorem for Moufang loops". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 139.1 (2005), 41–57.

[Gru83] T. Grundhöfer. "Projektivitätengruppen von Translationsebenen". In: *Results in Mathematics. Resultate der Mathematik* 6.2 (1983), 163–182.

[Gru88] T. Grundhöfer. "The groups of projectivities of finite projective and affine planes". In: *Ars Combinatoria* 25.A (1988). Eleventh British Combinatorial Conference (London, 1987), 269–275.

[GM09] T. Grundhöfer and P. Müller. "Sharply 2-transitive sets of permutations and groups of affine projectivities". In: *Beiträge zur Algebra und Geometrie. Contributions to Algebra and Geometry* 50.1 (2009), 143–154.

[Hal07] J. I. Hall. "Central automorphisms of Latin square designs and loops". In: *Quasigroups and Related Systems* 15.1 (2007), 19–46.

[Hei96] S. Heiss. "Invariant 1-factorization of complete graphs". Unpublished manuscript. 1996.

[Her74] C. Hering. "Transitive linear groups and linear groups which contain irreducible subgroups of prime order". In: *Geometriae Dedicata* 2 (1974), 425–460.

[Her85] C. Hering. "Transitive linear groups and linear groups which contain irreducible subgroups of prime order. II". In: *Journal of Algebra* 93.1 (1985), 151–164.

[HKT08] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic curves over a finite field*. Princeton, N.J.; Woodstock, Oxfordshire: Princeton University Press, 2008.

[HL12] G. Hiss and F. Lübeck. "Some remarks on two-transitive permutation groups as multiplication groups of quasigroups". In: *Buildings, finite geometries and groups*. Vol. 10. Springer Proc. Math. New York: Springer, 2012, 81–91.

[HS90] K. H. Hofmann and K. Strambach. "Topological and analytic loops". In: *Quasigroups and loops: theory and applications*. Vol. 8. Sigma Ser. Pure Math. Berlin: Heldermann, 1990, 205–262.

[HP73] D. R. Hughes and F. C. Piper. *Projective planes*. Graduate Texts in Mathematics, Vol. 6. New York: Springer-Verlag, 1973.

[Hum75] J. E. Humphreys. *Linear algebraic groups*. Graduate Texts in Mathematics, No. 21. New York: Springer-Verlag, 1975.

[Hup67] B. Huppert. *Endliche Gruppen. I*. Die Grundlehren der Mathematischen Wissenschaften, Band 134. Berlin: Springer-Verlag, 1967.

[HB82] B. Huppert and N. Blackburn. *Finite groups III*. Springer, 1982.

[JK82] V. Jha and M. J. Kallaher. "On the Lorimer-Rahilly and Johnson-Walker translation planes". In: *Pacific Journal of Mathematics* 103.2 (1982), 409–427.

[JS80] K. V. Johnson and B. L. Sharma. "On a family of Bol loops". In: *Unione Matematica Italiana. Bollettino. Supplemento* 2 (1980), 119–126.

[JS10a] K. W. Johnson and J. D. H Smith. "Matched Pairs, Permutation Representations, and the Bol Property". In: *Communications in Algebra* 38.8 (2010), pp. 2903–2914.

[JS10b] K. W. Johnson and J. D. H. Smith. "On the smallest simple, unipotent Bol loop". In: *Journal of Combinatorial Theory, Series A* 117.6 (Aug. 2010), pp. 790–798.

[JJB07] N. L. Johnson, V. Jha, and M. Biliotti. *Handbook of finite translation planes*. Vol. 289. Pure and Applied Mathematics (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2007.

[Kal87] M. J. Kallaher. "The multiplicative groups of quasifields". In: *Canadian Journal of Mathematics. Journal Canadien de Mathématiques* 39.4 (1987), 784–793.

[KP12] W. M. Kantor and T. Penttila. "Planes in which every quadrangle lies on a unique Baer subplane". In: *Designs, Codes and Cryptography* 65.1-2 (Oct. 2012), pp. 157–161.

[KN02] H. Kiechle and G. P. Nagy. "On the extension of involutorial Bol loops". In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 72 (2002), 235–250.

[Kie02] H. Kiechle. *Theory of K-loops*. Vol. 1778. Lecture Notes in Mathematics. Berlin: Springer-Verlag, 2002.

[KK04] H. Kiechle and M. K. Kinyon. "Infinite simple Bol loops". In: *Commentationes Mathematicae Universitatis Carolinae* 45.2 (2004), 275–278.

[Knu65a] D. E. Knuth. "A class of projective planes". In: *Transactions of the American Mathematical Society* 115 (1965), 541–549.

[Knu65b] D. E. Knuth. "Finite semifields and projective planes". In: *Journal of Algebra* 2 (1965), 182–217.

[KK95] E. Kolb and A. Kreuzer. "Geometry of kinematic K-loops". In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 65 (1995), 189–197.

[KNP13a] G. Korchmáros, G. P. Nagy, and N. Pace. *k-nets embedded in a projective plane over a field*. 2013. eprint: `arXiv:1306.5779`.

[KNP13b] G. Korchmáros, G. P. Nagy, and N. Pace. "3-Nets realizing a group in a projective plane". In: *Journal of Algebraic Combinatorics* (2013), pp. 1–28.

[Lie87a] M. W. Liebeck. "The affine permutation groups of rank three". In: *Proceedings of the London Mathematical Society. Third Series* 54.3 (1987), 477–516.

[Lie87b] M. W. Liebeck. "The classification of finite simple Moufang loops". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 102.1 (1987), 33–47.

[LPS00] M. W. Liebeck, C. E. Praeger, and J. Saxl. "Transitive subgroups of primitive permutation groups". In: *Journal of Algebra* 234.2 (2000). Special issue in honor of Helmut Wielandt, 291–361.

[Log07] E. K. Loginov. "Simple Bol loops". In: *Communications in Algebra* 35.1 (2007), 133–144.

[Lü80] H. Lüneburg. *Translation planes*. Berlin: Springer-Verlag, 1980.

[MV83] D. J. Madden and R. C. Valentini. "The group of automorphisms of algebraic function fields". In: *Journal für die Reine und Angewandte Mathematik* 343 (1983), 162–168.

[Map] *Maplesoft, a division of Waterloo Maple Inc.* Waterloo, Canada, 2013.

[MR95] R. Mathon and G. F. Royle. "The translation planes of order 49". In: *Designs, Codes and Cryptography. An International Journal* 5.1 (1995), 57–72.

[Moo07] G. E. Moorhouse. *Bol loops of small order*. 2007. URL: `http://www.uwyo.edu/moorhouse/pub/bol/`.

[Mor80] B. Mortimer. "The modular permutation representations of the known doubly transitive groups". In: *Proceedings of the London Mathematical Society. Third Series* 41.1 (1980), 1–20.

[Mou35] R. Moufang. "Zur Struktur von Alternativkörpern". In: *Mathematische Annalen* 110.1 (1935), 416–430.

[MN07] P. Müller and G. P. Nagy. "A note on the group of projectivities of finite projective planes". In: *Innovations in Incidence Geometry* 6/7 (Aug. 2007), 291–294.

[MN11] P. Müller and G. P. Nagy. "On the non-existence of sharply transitive sets of permutations in certain finite permutation groups". In: *Advances in Mathematics of Communications* 5.2 (2011), 303–308.

[NP13] G. P. Nagy and N. Pace. "On small 3-nets embedded in a projective plane over a field". In: *Journal of Combinatorial Theory. Series A* 120.7 (2013), 1632–1641.

[Nag98] G. P. Nagy. "Solvability of universal Bol 2-loops". In: *Communications in Algebra* 26.2 (1998), 549–555.

[Nag01] G. P. Nagy. "Burnside problems for Moufang and Bol loops of small exponent". In: *Acta Scientiarum Mathematicarum (Szeged)* 67.3-4 (2001), 687–696.

[Nag02] G. P. Nagy. "Tangential structure of formal Bruck loops". In: *Publicationes Mathematicae Debrecen* 61.1-2 (2002), 87–118.

[Nag03] G. P. Nagy. "Algebraic commutative Moufang loops". In: *Forum Mathematicum* 15.1 (2003), 37–62.

[Nag06] G. P. Nagy. "On the structure and number of small Frattini Bol 2-loops". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 141.3 (2006), 409–419.

[Nag08a] G. P. Nagy. "A class of simple proper Bol loops". In: *Manuscripta Mathematica* 127.1 (2008), 81–88.

[Nag08b] G. P. Nagy. "Some remarks on simple Bol loops". In: *Commentationes Mathematicae Universitatis Carolinae* 49.2 (2008), 259–270.

[Nag09] G. P. Nagy. "A class of finite simple Bol loops of exponent 2". In: *Transactions of the American Mathematical Society* 361.10 (2009), 5331–5343.

[Nag10] G. P. Nagy. "On the multiplication groups of semifields". In: *European Journal of Combinatorics* 31.1 (2010), 18–24.

[Nag13] G. P. Nagy. "Linear groups as right multiplication groups of quasifields". In: *Designs, Codes and Cryptography* (2013), pp. 1–12.

[NV04] G. P. Nagy and M. Valsecchi. "Splitting automorphisms and Moufang loops". In: *Glasgow Mathematical Journal* 46.2 (2004), 305–310.

[NS02] P. T. Nagy and K. Strambach. *Loops in group theory and Lie theory*. Vol. 35. de Gruyter Expositions in Mathematics. Berlin: Walter de Gruyter & Co., 2002.

[NÖ03] S. Niskanen and P. R. J. Östergård. *Cliquer User's Guide: Version 1.0*. Helsinki University of Technology, 2003.

[O'N85] M. E. O'Nan. "Sharply 2-transitive sets of permutations". In: *Proceedings of the Rutgers group theory year, 1983–1984 (New Brunswick, N.J., 1983–1984)*. Cambridge: Cambridge Univ. Press, 1985, 63–67.

[Pai56] L. J. Paige. "A class of simple Moufang loops". In: *Proceedings of the American Mathematical Society* 7 (1956), 471–482.

[PY08] J. V. Pereira and S. Yuzvinsky. "Completely reducible hypersurfaces in a pencil". In: *Advances in Mathematics* 219.2 (2008), 672–688.

[Pfl90] H. O. Pflugfelder. *Quasigroups and loops: introduction*. Vol. 7. Sigma Series in Pure Mathematics. Berlin: Heldermann Verlag, 1990.

[Qui06] J. Quistorff. "A survey on packing and covering problems in the Hamming permutation space". In: *Electronic Journal of Combinatorics* 13.1 (2006), Article 1, 13 pp. (electronic).

[Ram64] C. P. Ramanujam. "A note on automorphism groups of algebraic varieties". In: *Mathematische Annalen* 156 (1964), 25–33.

[Rob76] D. A. Robinson. "Some open questions on Bol loops, mimeographed notes". In: Oberwolfach Conference on Bol and Moufang Loops. 1976.

[Sab99] L. V. Sabinin. *Smooth quasigroups and loops*. Vol. 492. Mathematics and its Applications. Dordrecht: Kluwer Academic Publishers, 1999.

[Soi12] L. H. Soicher. *The GRAPE package for GAP, Version 4.6.1*. 2012.

[Ste68] R. Steinberg. *Endomorphisms of linear algebraic groups*. Memoirs of the American Mathematical Society, No. 80. Providence, R.I.: American Mathematical Society, 1968.

[Sut72] D. Suttles. "A counterexample to a conjecture of Albert". In: *Notices of the American Mathematical Society* 19.5 (1972), A–566.

[Tar99] H. Tarnanen. "Upper bounds on permutation codes via linear programming". In: *European Journal of Combinatorics* 20.1 (1999), 101–114.

[Tay92] D. E. Taylor. *The geometry of the classical groups*. Vol. 9. Sigma Series in Pure Mathematics. Berlin: Heldermann Verlag, 1992.

[Tho59] J. Thompson. "Finite groups with fixed-point-free automorphisms of prime order". In: *Proceedings of the National Academy of Sciences of the United States of America* 45 (1959), 578–581.

[Urz10] G. Urzúa. "On line arrangements with applications to 3-nets". In: *Advances in Geometry* 10.2 (2010), 287–310.

[Ves95] A. Vesanen. "Finite classical groups and multiplication groups of loops". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 117.3 (1995), 425–429.

[Ves13] A. Vesanen. "On the group $PSL(n, q)$ as the multiplication group of a loop". In: *European Journal of Combinatorics* 34.7 (2013), 1078–1080.

[Wei55] A. Weil. "On algebraic groups of transformations". In: *American Journal of Mathematics* 77 (1955), 355–391.

[Wik14] Wikipedia. *Problems in loop theory and quasigroup theory — Wikipedia, The Free Encyclopedia*. [Online; accessed 11-March-2014]. 2014. URL: `http://en.wikipedia.org/w/index.php?title=Problems_in_loop_theory_and_quasigroup_theory&oldid=593818493`.

[Yuz09] S. Yuzvinsky. "A new bound on the number of special fibers in a pencil of curves". In: *Proceedings of the American Mathematical Society* 137.5 (2009), 1641–1648.

[Yuz04] S. Yuzvinsky. "Realization of finite abelian groups by nets in $\mathbb{P}^2$". In: *Compositio Mathematica* 140.6 (2004), 1614–1624.

[Zas35] H. Zassenhaus. "Über endliche Fastkörper". In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 11.1 (1935), 187–220.