Finite simple Moufang loops

by

Petr Vojtěchovský

A dissertation submitted to the graduate faculty in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Mathematics

Major Professor: Jonathan D. H. Smith

Iowa State University

Ames, Iowa

2001

to Kari

Contents

Chapter 1

Introduction

Two out of the four basic arithmetic operations are not associative. This revelation alone should justify the study of non-associative structures, and it is therefore somewhat surprising that many books dealing with non-associativity open with a lengthy defense of their topic—a branch of mathematics where, with a slight hyperbole, parentheses outnumber all other characters combined. Perhaps the human tendency to give more significance to subjects that admit elegant description is responsible for this phenomenon.

The multitude of ways that open up with the transition from associative towards non-associative structures is mindboggling. The change in the order of complexity that one perceives when passing from abelian groups to groups falls short to the change experienced while proceeding from groups to loops (or quasigroups). To restrict one's interest is then not just a matter of taste, but necessity.

Non-associative finite simple Moufang loops form the central topic of this work. The emphasis will be on the connections between groups, composition algebras, combinatorics, and quasigroups. We tried to make this work intelligible for mathematicians working in any of the above areas. Many of the notions we will be discussing are not new; in fact, they are often known under several names and described with different notation. We do not believe it is possible to design new notation which would appeal to everybody. Instead, we will use multiple labels for single objects, depending on the adopted point of view, however, we will always carefully introduce all symbols. As far as the nontrivial notation is concerned, this work is self-contained. The same cannot be said about the results we build on. We have made reasonable effort to refer the reader to easily accessible, standard sources.

Our first comments concern mappings. Most algebraists like to write them to the left of the argument, most loop-theorists to the right. In this regard, we have no preference. In fact, if f is a mapping and x an argument, we write $f(x)$, $(x)f$, xf, and even x^f to denote the image of x under f. This inevitably leads to ambiguity, unless we always say what we mean. Well, we almost always say what we mean. As a rule, mappings written to the right of the argument compose from left to right, and vice versa.

Secondly, the name *non-associative finite simple Moufang loops* is quite long and the concept appears throughout this work. We believe that hard-to-pronounce abbreviations

(such as NFSML) are disturbing for the reader. We therefore give credit to the man who discovered non-associative finite simple Moufang loops, L. Paige, by calling them *Paige loops*. We are not the first to use this term (cf. [40], for instance).

We assume that the reader is familiar with elementary set theory, algebra, universal algebra and their notation. If X is a set, we let $|X|$ denote the cardinality of X. For any universal algebras A, B, we write $A \leq B$ to signify that A is a subalgebra of B. If S is a subset of an algebra A, the smallest subalgebra of A containing S—the *subalgebra of A generated by S*—will be denoted by $\langle S \rangle$. Although there is no mention of A in $\langle S \rangle$, it will be always clear from the context what A is. We sometimes abuse this notation in a natural way. So, if $S = \{s\}$ is a singleton, $\langle s \rangle$ stands for $\langle \{s\} \rangle$. Also, if T is another subset of A, $\langle S, T \rangle$ means $\langle S \cup T \rangle$. The group of all automorphisms of A will be denoted by $\mathrm{Aut}(A)$. If A is isomorphic to B, we write $A \cong B$.

The author used algebra package GAP [22] while working on this thesis, and he is happy to acknowledge it. It proved useful on many occasions. However, only two arguments in this work are actually based on machine computation, and the results obtained in this way have not been invoked later. As its name suggests, GAP's primary application are groups. Nevertheless, its open architecture allows to implement literally any algebraic structure. Appendix A contains several libraries developed by the author. All GAP libraries related to this thesis (and, for that matter, the thesis itself) are available electronically at author's homepage, currently `www.public.iastate.edu/~petr`, and also at `www.math.iastate.edu/~petr`.

Appendix B contains tables that make certain routine calculations easier, and hence the reading more enjoyable.

Let us now recall the basic definitions and properties of quasigroups, loops, Paige loops, and split octonion algebras. More material will be covered later.

1.1 Quasigroups and Loops

Let Q be a set and $\cdot$ a binary operation on Q. Thus $(Q, \cdot)$ is a universal algebra of type $\{2\}$, usually called *groupoid* or *binar*. We will often not mention the binary operation $\cdot$ and simply write Q for $(Q, \cdot)$. As O. Chein remarks in [9], the primary effect of denoting the operation in Q by some symbol is to lengthen most equations, and we will therefore agree to write ab instead of $a \cdot b$.

A groupoid Q is a *quasigroup* if, for a, b, $c \in Q$, the knowledge of any two elements in the equation

$$ab = c \tag{1.1}$$

uniquely specifies the third. (Multiplication tables of quasigroups are known in combinatorics as *Latin squares*.) It is convenient to capture the same idea in terms of *translations*. Let a be an element of Q. A *left translation by a in Q* is the mapping $L(a) : Q \longrightarrow Q$ defined by

$$xL(a) = ax.$$

Symmetrically, the *right translation by a in Q* is the mapping $R(a) : Q \longrightarrow Q$ defined

by

$$xR(a) = xa.$$

It is then easy to see that Q is a quasigroup if and only if every left translation $L(a)$ and every right translation $R(a)$ is a bijection of Q. Hence, in a quasigroup, every translation has an inverse, denoted by $L(a)^{-1}$, $R(a)^{-1}$. The inverse of a translation is not necessarily a translation.

If you work in universal algebra, you might know a different definition of a quasigroup. Namely, an algebra $(Q, \cdot, /, \backslash)$ with three binary operations is called a quasigroup if and only if

$$a \cdot (a\backslash b) = b, \;\; (b/a) \cdot a = b, \;\; a\backslash(a \cdot b) = b, \;\; (b \cdot a)/a = b \tag{1.2}$$

is satisfied for every a, $b \in Q$. These two definitions are equivalent, however, unlike the former one, the latter one guarantees that the class of quasigroups is closed under homomorphic images, and is therefore a variety. (Should you have difficulties remembering (1.2), think of / and $\backslash$ as right division and left division, respectively, and of $\cdot$ as multiplication. Then simplify the left hand sides of every identity in (1.2).)

A quasigroup Q is a *loop* if Q possesses a *neutral element* e, i.e., if

$$ae = a = ea$$

holds for every $a \in Q$. It can be shown by the standard argument that if a neutral element exists, it is unique.

Neither quasigroups nor loops are necessarily associative, and we must be careful when writing down expressions involving complex products. In order to avoid excessive use of parentheses, we employ the following evaluation rules: juxtaposition (as in ab) has the highest priority, followed by $\cdot$, followed by parentheses. Thus, $ab \cdot c$ means: first compute ab and then multiply the result on the right by c. The meaning of more complicated expressions, such as $(ab \cdot c)df$, should now be clear, too.

For a subloop $P \leq Q$ and and element $x \in Q$, let $xP = \{xy;\ y \in P\}$ be the *left coset* corresponding to P and x. Recall the left translation $L(x)$ by x in Q. Since $xP = PL(x)$, and since $L(x)$ is bijective, all left cosets have the same cardinality. Unlike in group theory, two distinct left cosets can have a non-empty intersection. We define *right cosets* in a similar way.

Subloop P is *normal in* Q if

$$xP = Px, \;\; (xP)y = x(Py), \;\; x(yP) = (xy)P$$

holds for every x, $y \in Q$. Normality can be restated in terms of *inner mappings*, much like in group theory. For x, $y \in Q$, consider the mappings

$$\begin{aligned} R(x, y) &= R(xy)^{-1}R(x)R(y), \\ L(x, y) &= L(yx)^{-1}L(x)L(y), \\ T(x) &= R(x)L(x)^{-1}, \end{aligned}$$

where, following our rule, we compose mappings from left to right. The mapping $T(x)$ plays the role of *conjugation*. Both $R(x, y)$, $L(x, y)$ are trivial when Q is a group. To understand what they mean, consult Figure 1.1. Let

$$\mathrm{Inn}(Q) = \langle R(x, y),\, L(x, y),\, T(x);\ x, y \in Q \rangle$$

be the subgroup of $\mathrm{Aut}(Q)$ generated by all inner mappings. Then P is normal in Q if and only if P is invariant under $\mathrm{Inn}(Q)$.

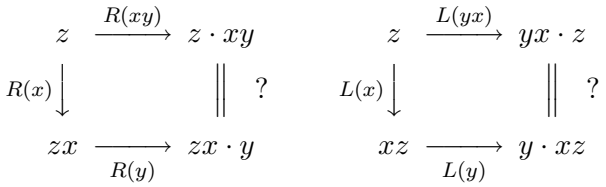

Figure 1.1: Inner mappings $R(x, y)$ and $L(x, y)$

A loop Q is said to be *simple* if Q has no non-trivial normal subloops. Equivalently, Q is simple if Q has no non-trivial congruences.

Finally, the *multiplication group* $\mathrm{Mlt}(Q)$ of a quasigroup Q is defined by

$$\langle L(x),\, R(x);\ x \in Q \rangle.$$

1.2 Moufang Loops

In order to understand the vast variety of loops, one habitually studies only loops satisfying some *weak form of associativity*. A loop L is called a *Moufang loop* if the *Moufang identities*

$$xy \cdot zx = x(yz \cdot x), \tag{1.3}$$
$$x(y \cdot xz) = (xy \cdot x)z, \tag{1.4}$$
$$x(y \cdot zy) = (x \cdot yz)y \tag{1.5}$$

are satisfied for every $x, y, z \in L$. Any of the three identities implies the other two (cf. [35, chapter IV]). The crucial result concerning Moufang loops is the *Moufang Theorem*, first proved by R. Moufang [32]. To state the theorem, we say that $x, y, z \in L$ *associate* if $xy \cdot z = x \cdot yz$. In a Moufang loop, if three elements associate, they associate in any order. It follows directly from the Moufang identities that x, x, y associate for every x, y.

Theorem 1.1 (Moufang Theorem) *Let x, y, z be (not necessarily distinct) elements of a Moufang loop L. Then $\langle x, y, z \rangle$ is an associative subloop of L if and only if x, y, z associate.*

A loop is said to be *power associative* if every element generates an associative subloop, i.e., a group. A loop is said to be *diassociative* if every two elements generate an associative subloop. Both power associativity and diassociativity for Moufang loops follow from the Moufang Theorem. Thanks to power associativity, the expression x^n has a unique interpretation for every non-negative integer n and every $x \in L$. Thanks to diassociativity, we may omit parentheses in expressions involving only powers of two elements.

Moreover, every element of a Moufang loop has a unique, both-sided *inverse*. More precisely, for $x \in L$, there is a unique $y \in L$ such that $xy = yx = e$. This inverse of x will be denoted by x^{-1}. We have therefore defined x^n for every integer n and $x \in L$. Also, the inverse of a translation is a translation when L is Moufang. Namely,

$$L(x)^{-1} = L(x^{-1}), \quad R(x)^{-1} = R(x^{-1}).$$

We define the *commutator* of x, y and the *associator* of x, y, z by

$$[x, y] = x^{-1}y^{-1}xy, \tag{1.6}$$
$$[x, y, z] = (xy \cdot z)^{-1}(x \cdot yz), \tag{1.7}$$

respectively.

The *center* $Z(L)$ of a loop L is the set of all elements of L which commute and associate with all other elements of L.

1.3 Split Octonion Algebras

For every field, there is an 8-dimensional algebra with zero divisors equipped with a non-degenerate quadratic form that permits composition. In this section, we explain the preceding sentence and introduce the needed notation. We will closely follow the exposition of T. A. Springer and F. D. Veldkamp [41], where the subject is treated in greater detail.

Let k be a field of characteristic p or 0, and let V be a vector space over k. Then $f : V \times V \longrightarrow k$ is a *bilinear form* if f is linear in both arguments, i.e., if

$$\begin{aligned} f(u + v, w) &= f(u, w) + f(v, w), \\ f(\lambda u, w) &= \lambda f(u, w) = f(u, \lambda w), \\ f(u, v + w) &= f(u, v) + f(u, w) \end{aligned}$$

holds for every u, v, $w \in V$, $\lambda \in k$. A mapping $N : V \longrightarrow k$ is called a *quadratic form* if

$$N(\lambda u) = \lambda^2 N(u)$$

is satisfied for every $u \in V$, $\lambda \in k$, and if $N(\ ,\ ) : V \times V \longrightarrow k$ defined by

$$N(u, v) = N(u + v) - N(u) - N(v)$$

is a bilinear form. The bilinear form $N(\ ,\ )$ is called the *bilinear form associated with* N. Two quadratic forms N_1 and N_2 on V are *equivalent* if there exists a surjective linear map $t : V \longrightarrow V$ such that

$$N_1(u) = N_2(t(u))$$

for every $u \in V$.

The classification of non-equivalent quadratic forms is a classical subject. We do not need to know the details at this moment, but we have to introduce the notion of *orthogonality* in order to define composition algebras. Assume that f is a bilinear form on V. Two vectors u and v are said to be *orthogonal* if $f(u, v) = 0$. We write $u \perp v$. If W is a subspace of V, the *orthogonal complement of* W *in* V is

$$W^{\perp} = \{v \in V;\ v \perp w \text{ for every } w \text{ in } W\}.$$

The bilinear form f is *non-degenerate* if $V^{\perp} = 0$. A quadratic form N on V is *non-degenerate* if the bilinear form associated with N is non-degenerate.

An *algebra* over a field k is a vector space over k with bilinear multiplication. Specifically, just as in [36], *we do not assume that the multiplication is associative*!

A *composition algebra* C over a field k is an algebra with a neutral element such that there exist a non-degenerate quadratic form N on C which *permits composition*, i.e., such that

$$N(uv) = N(u)N(v)$$

holds for every u, $v \in C$.

Every composition algebra satisfies the Moufang identities (cf. [41, Proposition 1.4.1]), but it is not a quasigroup, of course, because it contains 0. We will identify certain Moufang loops within composition algebras in Section 1.4. Since C is a vector space, it makes sense to speak about the *dimension* of C. One can show that the only possible dimensions of C are 2, 4, and 8; and also 1, provided the characteristic of k is different from 2. Composition algebras of dimension $2n$ are built from composition algebras of dimension n by the so-called *Cayley–Dickson process*, also known as *doubling*. The best known instance of doubling is the construction of complex numbers from real numbers, quaternions from complex numbers, and octonions from quaternions. Starting with a 2-dimensional composition algebra, each application of doubling strips the ensuing algebra of some algebraic property. The first application destroys commutativity, the second associativity. Then the Cayley–Dickson process stops. We say that C is an *octonion algebra* if C has dimension 8. (Octonion algebras can be built in other systematic ways, too. In [14], the multiplication of basis elements is described in a compact way. Dixon [19] uses Galois sequences.)

Every element x of a composition algebra satisfies

$$x^2 - N(x, e)x + N(x)e = 0. \tag{1.8}$$

This is the *minimal equation* for x when x is not a scalar multiple of e. The importance of (1.8) cannot be stressed enough.

For our purposes, it is crucial to look more closely at the quadratic form N of a composition algebra C. If $N(u) = 0$ for some nonzero vector u (i.e., if C contains a

nonzero *isotropic* vector), we say that C is a *split composition algebra*. Otherwise, C is called a *division composition algebra*. Note that split composition algebras are exactly those composition algebras that have zero divisors. The following result is a part [41, Theorem 1.8.1]:

Theorem 1.2 (Existence of Split Octonion Algebras) *There is a unique split octonion algebra for every field.*

Moreover, if k is finite, every octonion algebra constructed over k is split. Let $GF(q)$ be the Galois field of q elements, where q is a prime power. We denote by $\mathbb{O}(q)$ the unique (split) octonion algebra constructed over $GF(q)$. This algebra is the key to the construction of Paige loops. Nevertheless, we will pay more attention to an alternative construction, due to M. Zorn.

1.4 Paige Loops

In 1956, L. Paige [33] constructed one Paige loop for every field GF(q). (Of course, he did not call them Paige loops.) Thirty years later, M. Liebeck [30] showed that there are no other Paige loops. Following Bannai and Song [40], we denote the unique Paige loop constructed over $GF(q)$ by $M^*(q)$. Let us give a brief description of $M^*(q)$ now.

For α, $\beta \in k^3$, let $\alpha \cdot \beta$ denote the standard *dot product*, and $\alpha \times \beta$ the standard *vector product* of α, β. In detail, if $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ and $\beta = (\beta_1, \beta_2, \beta_3)$, we have

$$\begin{aligned} \alpha \cdot \beta &= \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3, \\ \alpha \times \beta &= (\alpha_2\beta_3 - \alpha_3\beta_2,\ \alpha_3\beta_1 - \alpha_1\beta_3,\ \alpha_1\beta_2 - \alpha_2\beta_1). \end{aligned}$$

The *Zorn algebra of vector matrices* $\mathrm{Zrn}(q)$ consists of matrices

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix},$$

where a, $b \in k$, and α, $\beta \in k^3$. The addition is defined entry-wise, and the multiplication is given by the *Zorn multiplication formula*

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha \cdot \delta & a\gamma + d\alpha - \beta \times \delta \\ c\beta + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{pmatrix}. \tag{1.9}$$

(Actually, the original Zorn multiplication formula [48] is different, albeit equivalent. The formula we use can be found in [33], [41, p. 20], and [39, p. 93].) Note that this multiplication differs from the ordinary matrix multiplication only by the two antidiagonal terms $-\beta \times \delta$ and $\alpha \times \gamma$. The Zorn algebra $\mathrm{Zrn}(q)$ is isomorphic to $\mathbb{O}(q)$, and is therefore a split composition algebra. See [28] for details. Since the algebraic structure of any composition algebra uniquely specifies the quadratic form, there must be a unique quadratic form on $\mathrm{Zrn}(q)$ corresponding to the quadratic form N of $\mathbb{O}(q)$. It turns out to be the *determinant*,

$$\det \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} = ab - \alpha \cdot \beta.$$

An element of $\mathrm{Zrn}(q)$ has a multiplicative inverse if and only if its determinant is nonzero. In such a case,

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}^{-1} = \begin{pmatrix} b & -\alpha \\ -\beta & a \end{pmatrix}.$$

All elements of $\mathrm{Zrn}(q)$ with nonzero determinant form a Moufang loop, and so do all elements of $\mathrm{Zrn}(q)$ with determinant 1. Let us denote the latter loop by $M(q)$. The neutral element of $M(q)$ is

$$e = \begin{pmatrix} 1 & (0,\,0,\,0) \\ (0,\,0,\,0) & 1 \end{pmatrix}.$$

The center of $M(q)$ consists of scalar matrices with determinant 1. Thus $Z(M(q)) = \{e, -e\}$. Note that the center is trivial when q is even.

Definition 1.3 *Let $M^*(q)$ be the quotient loop $M(q)/Z(M(q))$.*

The Moufang loop $M^*(q)$ is simple and non-associative, hence a Paige loop. We will not introduce a special notation for the two-element cosets of $M^*(q) = M(q)/Z(M(q))$ when q is odd. We simply write x for $xZ(M(q))$ and tacitly identify x with $-x$. Sometimes the negative sign appears in our computations, but it can be ignored when the equations are interpreted in $M^*(q)$.

An easy argument of Paige [33] shows that $M^*(q)$ has $q^3(q^4-1)$ elements when q is even, and $q^3(q^4-1)/2$ elements when q is odd.

1.5 Summary of Results

After introducing the basic notions, let us briefly outline the results of this work.

Chapter 2 is devoted to generators of Paige loops. We prove that every Paige loop is 3-generated and we list several generating sets for every prime power q. A primitive element of $GF(q)$ is needed to describe these generators, unless q is a prime. The prime case is considered once again in Section 2.2, and generators consisting only of 0, 1 and -1 are found. Thanks to its connection to the real octonions, the case $q = 2$ is of special interest, and is consequently treated in greater detail in Section 2.3. There we also construct an isomorphism between the integral Cayley numbers modulo their center and $M^*(2)$. This result first appeared in [43]. Generators for all values of q are treated in [44].

Automorphisms of octonion algebras are investigated in Chapter 3. We prove on the way that every element of $\mathbb{O}(q)$ can be written as a sum of two elements of norm 1, and that the projective unimodular group $L_2(q)$ contains elements of exactly the same orders as the loop $M^*(q)$. We characterize elements of order 2 and 3 in Section 3.2, and find how many such elements are there in $M(q)$ and $M^*(q)$, respectively. This will allow us to prove that the only Paige loops of exponent 6 are $M^*(2)$ and $M^*(3)$. Several automorphisms of $\mathbb{O}(q)$ (and $M^*(q)$) are constructed in Section 3.3. We focus on two

classes of automorphisms: diagonal automorphisms and conjugations. First, it is shown that

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \mapsto \begin{pmatrix} a & f(\alpha) \\ f(\beta) & b \end{pmatrix}$$

is an automorphism of $\mathbb{O}(q)$ if and only if f is a non-singular orthogonal linear transformation respecting the vector product. Secondly, the conjugation $T(x)$ is an automorphism of $M^*(q)$ if and only if $|x| = 3$.

The natural notion of Hasse constants is introduced in Chapter 4, and some basic properties are derived. Using Hasse constants, we investigate the class of Moufang loops $M_{2n}(G, 2)$. We prove several structural results (e.g., Sylow Theorems), and initiate the theory of presentations for $M_{2n}(G, 2)$. We find compact presentations for all loops $M_{2n}(G, 2)$ with G 2-generated, and we comment on the general case. Chapter 4 is concluded with a visualization of the smallest non-associative Moufang loop $M_{12}(S_3, 2)$, thus offering, as far as we know, the best description of $M_{12}(S_3, 2)$.

Chapter 5 is devoted entirely to the smallest Paige loop $M^*(2)$. We give a complete description of the lattice of subloops of $M^*(2)$. As a consequence, we verify that $M^*(2)$ satisfies the strong Lagrange property. The most interesting facts about $M^*(2)$ are summarized in Theorem 5.27. We rely on the classification of small Moufang loops due to O. Chein. Some of the arguments are of rather detailed nature, nevertheless, all of them can be comfortably carried out by hand. In Section 5.4, we calculate the probability that three randomly chosen elements of $M^*(2)$ actually generate it, and some refinements thereof. This is done with help of a tailored counting technique. There are numerous combinatorial structures based on $\mathbb{O}(2)$ and $M^*(2)$. We investigate two of them more closely: the combinatorial design defined by the overlap of subgroups of type S_3 in $M^*(2)$, and the generalized hexagon of order 2 defined by a certain incidence structure based on the lattice of subloops. It seems that this is the first time the generalized hexagon of order two appears as a natural incidence structure.

Chapter 6 deals with the automorphism groups of Paige loops. It is known that $\mathrm{Aut}(\mathbb{O}(q))$ is the exceptional group $G_2(q)$. We prove in two different ways that the group $\mathrm{Aut}(M^*(2))$ equals $G_2(2)$, and embark on the general case. Here the role of the additive structure and the minimal equation is especially apparent. It is fruitful to look at $\mathbb{O}(q)$ in three ways: as a Zorn vector matrix algebra, as an algebra constructed from $GF(q)$ by three applications of doubling, and as an algebra with elegant quaternion-like multiplication for basis elements. Much to his disappointment, the author was unable to determine the isomorphism type of $\mathrm{Aut}(M^*(q))$ for $q \neq 2$.

A small, but important part of the lattice of subloops of $M^*(q)$ is unveiled in Chapter 7. More specifically, for every prime power q, we find three elements $g_1, g_2, g_3 \in M^*(q)$ such that $\langle g_1, g_2, g_3 \rangle = M^*(q)$, and such that the groups $\langle g_i, g_j \rangle$, for $i \neq j$, are all isomorphic to a certain group $(3, 3 \mid 3, p)$ defined by Edington, Coxeter and Moser. The structure of these groups was not known. They are now completely described by Theorem 7.5. The form of their lattice of subgroups depends on solvability of a certain quadratic congruence, and it can be nicely visualized in terms of affine geometry. The results are based on [45]. We also include a short note on permutation representations of quasigroups.

The investigation of Paige loops is far from finished. The most important open questions can be found in the last chapter.

Chapter 2

Generators

It is remarkable that every finite simple group is 2-generated, i.e., generated by 2 elements. In hindsight, it appears to be an intrinsic property of finite simple groups, however, no proof of this fact based only on the simplicity is known. Instead, the complete list of finite simple groups—obtained from the classification—must be considered class by class, and explicit generators must be found for every group. Decisive steps in this program were made by L. E. Dickson (cf. Dickson Theorem) and by R. Steinberg [42]. The entire effort was concluded in [3], and its history can be found in [47].

Paige loops cannot be 2-generated because they are diassociative but not associative. In view of the results on finite simple groups, it is natural to expect that Paige loops will be generated by a small number of elements. Indeed, we prove in this chapter that every Paige loop is 3-generated.

2.1 Generators for Paige Loops

We adopt the notation of [13] for classical groups. In particular, we use $SL_2(q)$ for the special linear group of 2×2 matrices of determinant 1 over $k = GF(q)$, and $L_2(q)$ for the projective unimodular group $SL_2(q)/Z(SL_2(q))$. We will see later that $M^*(q)$ contains many subgroups isomorphic to $L_2(q)$. Three of them show up in a straightforward way.

Let $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$ be the canonical basis for k^3. For i, $1 \leq i \leq 3$, let $\phi_i : L_2(q) \longrightarrow M^*(q)$ be defined by

$$\phi_i \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & be_i \\ ce_i & d \end{pmatrix}.$$

Since the multiplication in $G_i = \phi_i(L_2(q))$ coincides with the ordinary matrix multiplication (all vector products involved in (1.9) vanish), ϕ_i is an isomorphism.

2.1.1 Generators for $L_2(q)$

With the exception of $(n, q) = (2, 2)$, $(2, 3)$, all groups $L_n(q)$ are simple [26, p. 182], and so 2-generated [3]. The remaining two groups $L_2(2)$, $L_2(3)$ are 2-generated as well.

We will need explicit generators for $L_2(q)$ and $SL_2(q)$. First of all, there is the Dickson Theorem:

Theorem 2.1 (Dickson Theorem) *Let $q \neq 9$ be an odd prime power, or $q = 2$. Then $SL_2(q)$ is generated by*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}, \tag{2.1}$$

where u is a primitive element of $GF(q)$.

The proof can be found in [18], and more recently in [24, pp. 44–55]. Traditionally, Dickson Theorem does not mention the case $q = 2$, despite the fact that (2.1) generate $L_2(2)$. (The group $L_2(2)$ is isomorphic to S_3, hence generated by any two involutions, for instance by (2.1).)

Remark 2.2 *$L_2(4)$ is not generated by* (2.1)*. What about $L_2(2^r)$, $r > 2$?*

A. A. Albert and J. Thompson claim [1, Lemma 8] that for any primitive element u of $GF(q)$, the group $SL_2(q)$ is generated by B, $-B$, and C, where

$$B = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 \\ -1 & u \end{pmatrix}. \tag{2.2}$$

Actually, the claim is not true for $q = 2$ (if $q = 2$, the primitive element $u = \alpha$ equals 1, thus equation (92) in [1, Lemma 8] yields $k = 0$, and then D_j from equation (93) equals I). We still have an impressive result:

Proposition 2.3 (A. A. Albert, J. Thompson, 1959) *Let $q > 2$ be a prime power. Then $L_2(q)$ is generated by* (2.2)*, where u is a primitive element of $GF(q)$.*

The generators (2.2) are especially convenient for our purposes, because $\phi_i(B) = B$ for every i, $1 \leq i \leq 3$; but let us not get ahead of ourselves. It is practical to know some generators that do not involve a primitive element. For that matter, Coxeter and Moser argue in [17] that

Lemma 2.4 *For every prime p, the group $L_2(p)$ is generated by*

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{2.3}$$

The following generators undoubtedly belong to mathematical folklore, but the author was unable to find a reference.

Lemma 2.5 *Let $q = 2^r$, $r > 1$. Then $SL_2(q) = L_2(q)$ is generated by*

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}, \tag{2.4}$$

where u is a primitive element of $GF(q)$.

Proof. Let G be the subgroup of $SL_2(2^r)$ generated by

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}.$$

As u is a primitive element of $k = GF(2^r)$,

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

belongs to G for all $a \in k^* = k \setminus \{0\}$. Note that

$$\begin{pmatrix} a^2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

belongs to G, and thus

$$\begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \in G$$

for all $a \in k^*$ (k is perfect). Because $r > 1$, there are x, $y \in k^*$ such that $x + y = 1$, and consequently

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^2 \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} y & 1 \\ 1 & 0 \end{pmatrix}^{-1} \in G.$$

We also have

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+a & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \in G$$

for every $a \in G$. Finally, consider

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $ad - bc = 1$. First assume that $a \neq 0$. Since

$$M = \begin{pmatrix} 1 & ab \\ ca^{-1} & ad \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},$$

we may assume that $a = 1$. But then

$$M = \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in G.$$

Now assume that $a = 0$. If $d \neq 0$, then

$$M = \begin{pmatrix} d & b \\ b^{-1} & 0 \end{pmatrix}^{-1} \in G.$$

If $d = 0$, we have

$$M = \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in G,$$

and we are through. □

2.1.2 Reducing the number of generators for Paige loops

Within the proof of simplicity of $M^*(q)$, L. Paige showed that $M^*(q)$ is generated by the elements

$$X_\alpha = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \quad Y_\alpha = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}, \tag{2.5}$$

where α runs over k^3. (Combine Lemmas 4.2 and 4.3 of [33].) We now deduce from (2.5) that every $M^*(q)$ is at most 6-generated. Recall the subgroups G_i introduced in Subsection 2.1.1.

Proposition 2.6 *$M^*(q)$ is generated by $G_1 \cup G_2 \cup G_3$.*

Proof. Let Q be the subloop of $M^*(q)$ generated by $G_1 \cup G_2 \cup G_3$. It suffices to prove that Q contains the elements X_α, Y_α for all $\alpha \in k^3$. We show simultaneously that $X_\alpha \in Q$ and $Y_\alpha \in Q$.

Let n denote the number of nonzero entries of α. There is nothing to prove when $n \leq 1$. Suppose that $n = 2$. Without loss of generality, let $\alpha = (a,\ b,\ 0)$ for some a, $b \in k^*$. Verify that

$$\begin{pmatrix} 1 & ae_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & be_2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -abe_3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & (a,b,0) \\ 0 & 1 \end{pmatrix},$$

and thus $X_\alpha \in Q$. Similarly, $Y_\alpha \in Q$. We can therefore assume that Q contains all elements X_α, Y_α with $n \leq 2$.

Let $n = 3$, $\alpha = (a,\ b,\ c)$ for some $a,\ b,\ c \in k^*$. As

$$\begin{pmatrix} 1 & (a,b,0) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & (0,0,c) \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ (-bc,ac,0) & 1 \end{pmatrix} = \begin{pmatrix} 1 & (a,b,c) \\ 0 & 1 \end{pmatrix},$$

X_α belongs to Q. Symmetrically, $Y_\alpha \in Q$, and we are done. □

In fact, $G_1 \cup G_2$ already generates $M^*(q)$. The role of the cross product is especially apparent in the next proposition.

Proposition 2.7 *The subgroup G_3 is contained in the subloop of $M^*(q)$ generated by $G_1 \cup G_2$. In particular, $M^*(q)$ is generated by $G_1 \cup G_2$.*

Proof. As it turns out, all we need are these two equations:

$$\begin{pmatrix} 1 & 0 \\ ue_3 & 1 \end{pmatrix} = -\begin{pmatrix} 0 & e_2 \\ -e_2 & 0 \end{pmatrix} \begin{pmatrix} 1 & ue_1 \\ -u^{-1}e_1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & e_2 \\ -e_2 & 0 \end{pmatrix} \begin{pmatrix} 1 & ue_1 \\ -u^{-1}e_1 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 0 & e_3 \\ -e_3 & 0 \end{pmatrix} = \begin{pmatrix} 0 & e_1 \\ -e_1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -e_2 \\ e_2 & 0 \end{pmatrix}.$$

Note that the left hand sides of these equations are elements of G_3, whereas the right hand sides are products of elements of $G_1 \cup G_2$. If $q = 2$, we are done by Lemma 2.4. If $q > 2$, observe that, calculating in $L_2(q)$,

$$\begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & u \end{pmatrix} = C.$$

Since $B = \phi_i(B)$ for every i, $1 \leq i \leq 3$, we are done by Proposition 2.3. □

2.1.3 Main Result

We are now ready to show that every Paige loop is 3-generated. We present more than one generating set for every $M^*(q)$ with $q \neq 2, 9$.

Theorem 2.8 (Generators for Paige Loops) *Every Paige loop is generated by three elements. When $q > 2$, then*

$$\begin{pmatrix} 0 & (1,0,0) \\ (-1,0,0) & u \end{pmatrix}, \begin{pmatrix} 0 & (0,1,0) \\ (0,-1,0) & u \end{pmatrix}, \begin{pmatrix} u & (0,0,0) \\ (0,0,0) & u^{-1} \end{pmatrix} \tag{2.6}$$

generate $M^*(q)$. When $q \neq 9$ is odd or $q = 2$, then $M^*(q)$ is generated by

$$\begin{pmatrix} 1 & (1,0,0) \\ (0,0,0) & 1 \end{pmatrix}, \begin{pmatrix} 1 & (0,1,0) \\ (0,0,0) & 1 \end{pmatrix}, \begin{pmatrix} 0 & (0,0,u) \\ (0,0,-u^{-1}) & 1 \end{pmatrix}. \tag{2.7}$$

When $q > 2$ is even, then $M^*(q)$ is generated by

$$\begin{pmatrix} 1 & (1,0,0) \\ (1,0,0) & 0 \end{pmatrix}, \begin{pmatrix} 1 & (0,1,0) \\ (0,1,0) & 0 \end{pmatrix}, \begin{pmatrix} u & (0,0,0) \\ (0,0,0) & u^{-1} \end{pmatrix}. \tag{2.8}$$

In all cases, u is a primitive element of $GF(q)$.

Proof. To see that (2.6) generates $M^*(q)$ when $q > 2$, combine Propositions 2.3 and 2.7, and note that $\phi_1(B) = \phi_2(B) = B$.

Assume that $q \neq 9$ is odd, or $q = 2$. Keeping Proposition 2.7 and Dickson Theorem in mind, we only need to obtain the elements

$$\begin{pmatrix} 1 & 0 \\ ue_i & 1 \end{pmatrix},$$

for $i = 1, 2$. Straightforward computation reveals that

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ ue_1 & 1 \end{pmatrix} &= -\begin{pmatrix} 0 & ue_3 \\ -u^{-1}e_3 & 1 \end{pmatrix}^2 \begin{pmatrix} 1 & e_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & ue_3 \\ -u^{-1}e_3 & 1 \end{pmatrix}, \\ \begin{pmatrix} 1 & 0 \\ ue_2 & 1 \end{pmatrix}^{-1} &= -\begin{pmatrix} 0 & ue_3 \\ -u^{-1}e_3 & 1 \end{pmatrix}^2 \begin{pmatrix} 1 & e_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & ue_3 \\ -u^{-1}e_3 & 1 \end{pmatrix}. \end{aligned}$$

Note that the expressions on the right hand side can be evaluated in any order.

Finally, let $q = 2^r$, $r > 1$. Since $\phi_1(B) = \phi_2(B)$, we are done by Lemma 2.5 and Proposition 2.7. □

2.2 Generators for Paige Loops over Prime Fields

We present an alternative set of generators for $M^*(q)$ in case that $q = p$ is a prime. The proof does not require the complicated Dickson Theorem.

Proposition 2.9 (Theorem 2.1**[43])** *Let p be a prime. Then $M^*(p)$ is generated by*

$$U_1 = \begin{pmatrix} 1 & (1,\,0,\,0) \\ 0 & 1 \end{pmatrix},\ U_2 = \begin{pmatrix} 1 & (0,\,1,\,0) \\ 0 & 1 \end{pmatrix},\ X = \begin{pmatrix} 0 & (0,\,0,\,1) \\ (0,\,0,\,-1) & 1 \end{pmatrix}.$$

Proof. First check that

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}. \tag{2.9}$$

Combine (2.3) and (2.9) to see that $L_2(p)$ is generated by

$$U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ V = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Consequently, $M^*(p)$ is generated by $U_1 = \phi_1(U)$, $U_2 = \phi_2(U)$, $V_1 = \phi_1(V)$, and $V_2 = \phi_2(V)$. Now,

$$\begin{aligned} V_2 &= -(XU_1 \cdot XU_2) \cdot X^{-1}U_1, \\ V_1 &= -U_1U_2 \cdot (V_2 \cdot U_1X), \end{aligned}$$

and we are through. □

2.3 Generators for Integral Cayley Numbers

We have seen in Section 1.4 how every Paige loops arises from the octonion algebra $\mathbb{O}(q)$. The loop $M^*(2)$ is exceptional in the sense that it can also be linked to the real octonion algebra $\mathbb{O}$ in a nice way. By *real octonion algebra* we mean the octonion algebra constructed over $\mathbb{R}$ by the *standard* Cayley–Dickson process (see below). We will refer to $\mathbb{O}$ simply as *octonions*. Others prefer different names, such as *algebra of octaves*, or *Cayley numbers*. We will give the details of the construction of $\mathbb{O}(q)$, since we will need them later anyway.

2.3.1 The Cayley–Dickson process = Doubling

We excerpt parts of the material from [41] once again.

Let D be a composition algebra over k with quadratic form N and associated bilinear form $N(\ ,\ )$. We will call N suggestively a *norm*, although the reader should be warned that N does not need to satisfy any of the axioms of a (metric space) norm, especially when D is split. We will see in Section 3.1 that $\mathbb{O}(q)$ has very peculiar metric properties.

For $x \in D$, define the *conjugate* $\overline{x}$ by

$$\overline{x} = N(x,\,e)e - x. \tag{2.10}$$

Pick $\lambda \in k^*$. On $C = D \oplus D$, define the addition entry-wise, multiplication by

$$(x,\,y)(u,\,v) = (xu + \lambda\overline{v}y,\ vx + y\overline{u}),$$

and the norm by

$$N((x, y)) = N(x) - \lambda N(y).$$

This procedure is known as the *Cayley–Dickson process*, or *doubling*. When D is associative and commutative, then C is associative. When D is associative, then C is a composition algebra. Note that the dimension of C is twice that of D. Also note that λ is a parameter in the process. Different values of λ may result in different algebraic properties of C. We speak about *standard Cayley–Dickson process* if $\lambda = -1$.

The octonions $\mathbb{O}$ can be constructed from $\mathbb{R}$ by three applications of the standard Cayley–Dickson process. A more classical approach to the standard Cayley–Dickson process is to introduce a new *unit* in every step, say f, let $C = D \oplus Df$, and define the multiplication by

$$(x + yf)(u + vf) = (xu - \overline{v}y) + (vx + y\overline{x})f,$$

and the norm by

$$N(x + yf) = N(x) + N(y).$$

We can then obtain $\mathbb{O}$ from $\mathbb{R}$ in three steps by adjoining i (to get $\mathbb{C}$), then j (to get $\mathbb{H}$), and finally e. (Here, our notation for the neutral element collides with the usual name for the lastly adjoined unit.) Following Dickson, we can then write a (vector space) basis for $\mathbb{O}$ as 1, i, j, $k = ij$, e, ie, je, ke, where 1 is the neutral element of $\mathbb{O}$, and e is the lastly adjoined unit.

2.3.2 Integral Cayley Numbers

Let C be a composition algebra. A subset S of C is called a *set of integral elements* if it is a maximal subset of C with respect to the following conditions:

(i1) $e \in S$,

(i2) S is closed under multiplication and subtraction,

(i3) $N(a)$ and $a + \overline{a}$ belong to the prime field for every $a \in S$.

This generalizes the definition of a set of integral elements given in [15]. Coxeter explains the meaning of (i3) essentially as follows: in any composition algebra, every element satisfies

$$x^2 - N(x, e)e + N(x)e = 0. \tag{2.11}$$

We recognize that (2.11) is the (minimal) equation (1.8) introduced in Section 1.4. We see immediately from the conjugation formula (2.10) that (2.11) is the same as

$$x^2 - (x + \overline{x})x + N(x)e = 0. \tag{2.12}$$

Thus, the condition (i3) means that the coefficients of (2.11) are in the prime field.

Everybody should be familiar with the integral real numbers (= integers), and the integral complex numbers (= Gauss' integers). We can speak of *the* set of integral

numbers in case of $\mathbb{R}$, $\mathbb{C}$, and even $\mathbb{H}$, because there is a unique set of integral numbers. However, for $\mathbb{O}$, there are 7 isomorphic sets of integral numbers. We will call each of them *integral Cayley numbers*, or *integral octonions*. For the rest of this section, select the one which Coxeter calls J in [15].

2.3.3 An Isomorphism and Generators

Let $J' = \{x \in J;\ N(x) = 1\}$. It is well known that $|J'| = 240$ and that $J'/\{1, -1\}$ is, as a loop, isomorphic to $M^*(2)$. Indeed, J' is probably the best known finite non-associative Moufang loop! Coxeter knew that J is generated by 3 elements by multiplication and subtraction. Since norm permits composition, and since $M^*(2)$ is 3-generated, it is reasonable to expect that J' is 3-generated (by multiplication only), too.

We will use Dickson's notation for $\mathbb{O}$.

Theorem 2.10 (Generators for Integral Cayley Numbers) *Every loop of integral Cayley numbers of unit norm is 3-generated. For J', the generators are i, j, and $h = 1/2(i + j + k + e)$.*

Proof. Define a mapping $\psi : M^*(2) \longrightarrow J'/\{1, -1\}$ by

$$\begin{pmatrix} 0 & e_3 \\ e_3 & 0 \end{pmatrix} \mapsto i,\ \begin{pmatrix} 0 & e_2 \\ e_2 & 0 \end{pmatrix} \mapsto j,\ \begin{pmatrix} 1 & (0,\,1,\,0) \\ (1,\,0,\,1) & 1 \end{pmatrix} \mapsto h.$$

It is rather tedious to check by hand that ψ extends into an isomorphism of $M^*(2)$ onto $J'/\{1, -1\}$. The author used his own GAP libraries (see Appendix A) to confirm the computation. This being said, we can see that $J'/\{1, -1\}$ is generated by i, j, and h. As $i^2 = -1$, we are done. □

The traditional multiplication in $\mathbb{O}$ is cumbersome. For instance, let us verify that e (the unit adjoined to $\mathbb{H}$) equals $-(jh \cdot hi) \cdot kh$. Even if we take advantage of Coxeter's tables [15, p. 576, or p. 28], the computation requires many steps. First, we read off $hi = -1 - ih$. Then

$$\begin{aligned} -(jh \cdot hi) \cdot kh &= (jh + jh \cdot ih) \cdot kh = (jh + k - h - ih) \cdot kh \\ &= jh \cdot kh + k \cdot kh - h \cdot kh - ih \cdot kh \\ &= (-i + h - kh) + (-h) - (k - h) - (j - h - kh) \\ &= -i - j - k + 2h, \end{aligned}$$

which equals e, since $h = 1/2 \cdot (i + j + k + e)$.

On the other hand, multiplication in $M^*(2)$ is easy enough once we know $\psi^{-1}(e)$. One can see that

$$\psi^{-1}(e) = \begin{pmatrix} 0 & (1,\,1,\,1) \\ (1,\,1,\,1) & 0 \end{pmatrix}.$$

See Chapter 6 for more information on additive properties of ψ.

Chapter 3

Automorphisms

Not surprisingly, the group $\mathrm{Aut}(M^*(q))$ is useful in the investigation of $M^*(q)$. We find some automorphisms of $M^*(q)$ and $\mathbb{O}(q)$ needed in Chapter 5, and return to a more detailed investigation of $\mathrm{Aut}(M^*(q))$ and $\mathrm{Aut}(\mathbb{O}(q))$ in Chapter 6.

3.1 Automorphisms of Split Octonion Algebras

Three groups are usually studied in connection with a loop Q: the inner mapping group $\mathrm{Inn}(Q)$, the multiplication group $\mathrm{Mlt}(Q)$, and the automorphism group $\mathrm{Aut}(Q)$. In case of the Paige loop $M^*(q)$, there is another group of interest, namely $\mathrm{Aut}(\mathbb{O}(q))$.

By an *automorphism* of an algebra A over a field k (cf. $A = \mathbb{O}(q)$) we mean a *linear* automorphism, i.e., a bijection f satisfying

$$\begin{array}{rcll} f(x+y) & = & f(x)+f(y), & \text{(additivity)} \\ f(\lambda x) & = & \lambda f(x), & \text{(scalar linearity)} \\ f(xy) & = & f(x)f(y), & \text{(multiplicativity)} \end{array}$$

for every x, $y \in A$, $\lambda \in k$.

3.1.1 Lie Algebras and Groups of Lie Type

It goes beyond the scope of this work to shed light on all the details pertinent to the classification of simple Lie algebras over complex numbers and to the construction of groups of Lie type. We only introduce the notation and the basic concepts. For more details, see [8].

A *Lie algebra* $\mathcal{A}$ is an algebra where the product $[\ ,\ ]$, usually called *Lie bracket*, is bilinear, satisfies $[x, x] = 0$ for every $x \in \mathcal{A}$, and where the *Jacobi identity*

$$[[x, y], z] + [[y, z], x] + [[z, x], y] = 0 \tag{3.1}$$

holds for every x, y, $z \in \mathcal{A}$.

Multiplication in a Lie algebra is *anticommutative*, i.e., $[x, y] = -[y, x]$. An *ideal* $\mathcal{I}$ of $\mathcal{A}$ is a subspace of $\mathcal{A}$ such that $[\mathcal{I}, \mathcal{A}] \subseteq \mathcal{I}$. Lie algebra $\mathcal{A}$ is said to be *simple* if it has no non-trivial ideals.

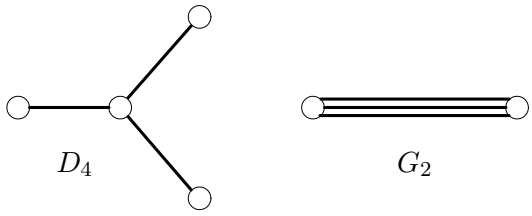

Figure 3.1: The Dynkin diagrams for D_4 and G_2

Simple Lie algebras over $k = \mathbb{C}$ are known to belong to one of nine types—there are four countable families A_i, B_i, C_i, D_i, and five *exceptional Lie algebras* G_2, F_4, E_6, E_7 and E_8. The *Dynkin diagrams* corresponding to the fundamental roots completely characterize each of the simple algebras. We will only deal with Lie algebras of type D_4 and G_2 whose Dynkin diagrams are in Figure 3.1.

To every field k and every simple Lie algebra $\mathcal{A}$ over $\mathbb{C}$, one associates a certain group $\mathcal{A}(k)$, the *Chevalley group* of type $\mathcal{A}$ over k. See [8, Chapter 4]. These groups are also called *groups of Lie type*. We write $G_2(q)$ and $D_4(q)$ to denote the groups $G_2(GF(q))$ and $D_4(GF(q))$, respectively.

The following two results are of importance to us.

Theorem 3.1 (Springer and Veldkamp [41, Ch. 2]) *The automorphism group of the split octonion algebra $\mathbb{O}(q)$ is the Chevalley group $G_2(q)$.*

Theorem 3.2 (Doro [20]) *The multiplication group of $M^*(q)$ is the Chevalley group $D_4(q)$.*

3.1.2 Metric Properties of $\mathbb{O}(q)$

Before we construct several automorphisms of $\mathbb{O}(q)$, we would like to point out how far are the properties of the norm N on $\mathbb{O}(q)$ from the intuitive understanding of (metric) norms.

Theorem 3.3 *In the split octonion algebra $\mathbb{O}(q)$, every element is a sum of two elements of norm one.*

Proof. We identify $\mathbb{O}(q)$ with $\mathrm{Zrn}(q)$, where the norm is given by the determinant. Let

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

be an element of $\mathbb{O}(q)$. First assume that $\beta \neq 0$. Note that for every $\lambda \in k = GF(q)$ there is $\gamma \in k^3$ such that $\gamma \cdot \beta = \lambda$. Pick $\gamma \in k^3$ so that $\gamma \cdot \beta = a + b - ab + \alpha \cdot \beta$. Then

choose $\delta \in \gamma^\perp \cap \alpha^\perp \neq \emptyset$. This choice guarantees that $(a-1)(b-1) - (\alpha - \gamma) \cdot (\beta - \delta) = ab - a - b + 1 - \alpha \cdot \beta + \gamma \cdot \beta = 1$. Thus

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} = \begin{pmatrix} 1 & \gamma \\ \delta & 1 \end{pmatrix} + \begin{pmatrix} a-1 & \alpha - \gamma \\ \beta - \delta & b-1 \end{pmatrix}$$

is the desired decomposition of x into a sum of two elements of norm 1. Note that the above procedure works for every α.

Now assume that $\beta = 0$. If $\alpha \neq 0$, we use a symmetrical argument as before to decompose x. It remains to discuss the case when $\alpha = \beta = 0$. Then the equality

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} a & e_1 \\ -e_1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & -e_1 \\ e_1 & b \end{pmatrix}$$

does the job. □

We will need this result later, although all we really need to know is the weaker statement that $\mathbb{O}(q)$ is generated by elements of norm one (by multiplication and addition).

3.1.3 Restricting Automorphisms

Theorem 3.1 describes the automorphism group of $\mathbb{O}(q)$. We now restrict the automorphisms to the first shell $M(q)$ of $\mathbb{O}(q)$.

Lemma 3.4 *Let $f \in \mathrm{Aut}(\mathbb{O}(q))$. Then $f \restriction M(q) \in \mathrm{Aut}(M(q))$. Moreover, if $f \neq g \in \mathrm{Aut}(\mathbb{O}(q))$, then $f \restriction M(q) \neq g \restriction M(q)$. In particular, $G_2(q)$ is a subgroup of $\mathrm{Aut}(M(q))$.*

Proof. Since $f(uv) = f(u)f(v)$ holds for every u, $v \in \mathbb{O}(q)$, it also holds for u, $v \in M(q)$. Assume that $f \restriction M(q) = g \restriction M(q)$. Since f, $g \in \mathrm{Aut}(\mathbb{O}(q))$ and, by Theorem 3.3, $\mathbb{O}(q) = \langle M(q) \rangle$, we have $f = g$, a contradiction. □

Remark 3.5 *Note that all we needed to assume about f, g was the additivity and multiplicativity, not linearity.*

3.2 Orders of Elements in Paige Loops

We prove that the orders of elements of $M^*(q)$ are the same as the orders of elements of $L_2(q)$. Then we focus on elements of order 2, 3. This *order statistics* can be used sometime for *black box recognition* of Paige loops. See [29] for more information on black box models of groups and algebras.

3.2.1 Orders in $L_2(q)$ versus Orders in $M^*(q)$

Proposition 3.6 explains how to calculate the orders of elements of $M^*(q)$ without using the vector product, hence faster.

Proposition 3.6 *For*

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

in $M^*(q)$*, define* $\tilde{x} \in L_2(q)$ *by*

$$\tilde{x} = \begin{cases} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, & \text{if } (\alpha, \beta) = (0, 0), \\ \begin{pmatrix} a & 1 \\ \alpha \cdot \beta & b \end{pmatrix}, & \text{if } \alpha \neq 0, \\ \begin{pmatrix} a & \alpha \cdot \beta \\ 1 & b \end{pmatrix}, & \text{otherwise.} \end{cases}$$

Then the order of x *in* $M^*(q)$ *is the same as the order of* $\tilde{x}$ *in* $L_2(q)$*.*

Proof. If $(\alpha, \beta) = (0, 0)$, we may consider x as an element of $L_2(q)$. Assume that $(\alpha, \beta) \neq (0, 0)$. Taking the Zorn multiplication formula (1.9) into account, verify that every element of $\langle x \rangle$ has the form

$$\begin{pmatrix} c & s\alpha \\ t\beta & d \end{pmatrix}, \tag{3.2}$$

for some c, d, s, $t \in k$. Furthermore, if $\alpha = 0$ we may assume that $s = 0$, if $\beta = 0$ we may assume that $t = 0$. With this additional convention, every element of $\langle x \rangle$ is uniquely written as (3.2). This allows us to define a mapping $\omega : \langle x \rangle \longrightarrow L_2(q)$ by

$$\omega \begin{pmatrix} c & s\alpha \\ t\beta & d \end{pmatrix} = \begin{cases} \begin{pmatrix} c & s \\ t\alpha \cdot \beta & d \end{pmatrix}, & \text{if } \alpha \neq 0, \\ \begin{pmatrix} c & s\alpha \cdot \beta \\ t & d \end{pmatrix}, & \text{otherwise.} \end{cases}$$

Straightforward computation shows that ω is a homomorphism onto a subgroup of $L_2(q)$. Since the kernel of ω is trivial, ω preserves orders. Now observe that $\tilde{x} = \omega(x)$. $\square$

We have just shown that for every element $x \in M^*(q)$, there is an element $y \in L_2(q)$ such that $|x| = |y|$. The converse is also true.

Theorem 3.7 *Let* $S \subseteq \mathbb{Z}$ *be the set of orders of all elements of* $M^*(q)$*, and let* T *be the set of orders of all elements of* $L_2(q)$*. Then* $S = T$*.*

Proof. Proposition 3.6 shows that $S \subseteq T$. We show that element element y of $L_2(q)$ has the same order as some element $z \in \mathrm{Im}(\omega)$, where ω is the mapping defined in the proof of Proposition 3.6. Let

$$y = \begin{pmatrix} a & c \\ d & b \end{pmatrix}.$$

If $(c, d) = (0, 0)$ then y can be considered as an element of $M^*(q)$. Assume that $c \neq 0$. The case $c = 0$, $d \neq 0$ is similar. Since the mapping

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} \mapsto \begin{pmatrix} r & \lambda s \\ \lambda^{-1}t & u \end{pmatrix}$$

is an automorphism of $L_2(q)$ for every $\lambda \in k^*$, we can assume that $c = 1$. Let $\alpha, \beta \in k^3$ be such that $\alpha \cdot \beta = cd = d$. Then

$$\omega \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} = \begin{pmatrix} a & 1 \\ \alpha \cdot \beta & b \end{pmatrix} = y,$$

and we are done. □

We do not claim that this speeds up the computation of orders dramatically, but it reduces the problem of finding orders of elements of $M^*(q)$ to the theory of groups. For example, since $|L_2(2)| = 6$, it is immediately obvious from Theorem 3.7 that $M^*(2)$ contains only elements of order 1, 2, and 3. More importantly, the set of orders is known for every $L_2(q)$, cf. [26, Ch. II, §8], and therefore also for every $M^*(q)$ now.

A result similar to Theorem 3.7 can be proved for $M(q)$ and $SL_2(q)$.

3.2.2 Counting Elements of Order Two and Three

We will find it convenient to have characterizations of elements of order 2 and 3 in $M(q)$ and $M^*(q)$. All calculations in Lemma 3.8 take place in $M(q)$.

Lemma 3.8 *Let*

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

be an element of $M(q)$. Then:

(i) *For q odd, $x^2 = e$ if and only if $(\alpha, \beta) = (0, 0)$ and $a = b = \pm 1$.*

(ii) *For every q, $x^2 = -e$ if and only if $((\alpha, \beta) = (0, 0)$, $b = a^{-1}$, and $a^2 = -1)$ or $((\alpha, \beta) \neq (0, 0)$, and $b = -a)$.*

(iii) *For q odd, $x^3 = e$ if and only if $((\alpha, \beta) = (0, 0)$, $b = a^{-1}$, and $a^3 = 1)$ or $((\alpha, \beta) \neq (0, 0)$, and $b = -1 - a)$.*

(iv) *For every q, $x^3 = -e$ if and only if $((\alpha, \beta) = (0, 0)$, $b = a^{-1}$, and $a^3 = -1)$ or $((\alpha, \beta) \neq (0, 0)$, and $b = 1 - a)$.*

Proof. Suppose that $(\alpha, \beta) = (0, 0)$. Then $b = a^{-1}$, else $N(x) \neq 1$. Therefore

$$x^m = \begin{pmatrix} a^m & 0 \\ 0 & a^{-m} \end{pmatrix}$$

for every integer m.

For the rest of the proof assume that $(\alpha, \beta) \neq (0, 0)$. We have

$$x^2 = \begin{pmatrix} a^2 + \alpha \cdot \beta & (a+b)\alpha \\ (a+b)\beta & b^2 + \alpha \cdot \beta \end{pmatrix}.$$

If $x^2 = \varepsilon e$, where $\varepsilon = \pm 1$, we must have $b = -a$. Conversely, if $b = -a$, we have $\alpha \cdot \beta = ab - 1 = -a^2 - 1$, and $x^2 = -e$. If $x^3 = \varepsilon e$, then

$$x^2 = \varepsilon x^{-1} = \varepsilon \begin{pmatrix} b & -\alpha \\ -\beta & a \end{pmatrix},$$

and we must have $a + b = -\varepsilon$, i.e., $b = -\varepsilon - a$. Conversely, if $b = -\varepsilon - a$, then $\alpha \cdot \beta = ab - 1 = -1 - \varepsilon a - a^2$, and $b^2 = 1 + 2\varepsilon a + a^2$. Hence

$$x^2 = \begin{pmatrix} -1 - \varepsilon a & -\varepsilon\alpha \\ -\varepsilon\beta & \varepsilon a \end{pmatrix} = \varepsilon x^{-1},$$

i.e., $x^3 = \varepsilon e$. □

We want to count the number of elements of order 2 and 3 in $M(q)$ and $M^*(q)$. It is perhaps not difficult in every particular case, but the general formulas are somewhat complicated. We start with an easy lemma.

Lemma 3.9 *Let $c \in GF(q) = k$. If $c \neq 0$ (resp. $c = 0$), there are $q^2(q^3 - 1)$ (resp. $q^2(q^3 + q - 1)$) ordered pairs (α, β) of vectors $\alpha, \beta \in k^3$ such that $\alpha \cdot \beta = c$.*

Proof. Let $\alpha = (\alpha_1, \alpha_2, \alpha_3)$, $\beta = (\beta_1, \beta_2, \beta_3)$. If $\alpha_1 \neq 0$, and α_2, α_3, β_2, β_3 are arbitrary, there is a unique β_1 such that $\alpha \cdot \beta = c$. We have found $(q-1)q^4$ ordered pairs. Similarly, we find $(q-1)q^3$ ordered pairs when $\alpha_1 = 0$, $\alpha_2 \neq 0$, and additional $(q-1)q^2$ ordered pairs when $\alpha_1 = \alpha_2 = 0$, $\alpha_3 \neq 0$. When $\alpha_1 = \alpha_2 = \alpha_3 = 0$, then $\alpha \cdot \beta = 0$ for every $\beta \in k^3$.

Therefore, if $c \neq 0$, there are $(q-1)(q^4 + q^3 + q^2) = q^2(q^3 - 1)$ ordered pairs. If $c = 0$, there are $q^2(q^3 - 1) + q^3 = q^2(q^3 + q - 1)$ ordered pairs. □

Proposition 3.10 *Let π, ρ, σ, τ be the number of solutions to $x^3 - 1 = 0$, $x^2 + 1 = 0$, $x^2 + x + 1 = 0$, $x^2 - x + 1 = 0$ in $GF(q)$, respectively. Denote by $t_n(q)$, $t_n^*(q)$ the number of elements of order n in $M(q)$, $M^*(q)$, respectively. Let $q_0 = q^2(q^3 + q - 1) - 1$, and $q_1 = q^2(q^3 - 1)$. Then*

$$t_2(q) = \begin{cases} 1, & \text{if } q \text{ is odd,} \\ \rho + \rho q_0 + (q - \rho)q_1 - 1, & \text{if } q \text{ is even,} \end{cases}$$

$$
\begin{aligned}
t_3(q) &= \begin{cases} \pi + \sigma q_0 + (q-\sigma)q_1 - 1, & \text{if } q \text{ is odd,} \\ \pi + \tau q_0 + (q-\tau)q_1 - 1, & \text{if } q \text{ is odd,} \end{cases} \\
t_2^*(q) &= \begin{cases} \frac{1}{2}[\rho + \rho q_0 + (q-\rho)q_1], & \text{if } q \text{ is odd,} \\ \rho + \rho q_0 + (q-\rho)q_1 - 1, & \text{if } q \text{ is even,} \end{cases} \\
t_3^*(q) &= \begin{cases} \pi - 1 + \frac{1}{2}[(\sigma+\tau)q_0 + (2q-\sigma-\tau)q_1], & \text{if } q \text{ is odd,} \\ \pi + \tau q_0 + (q-\tau)q_1 - 1, & \text{if } q \text{ is even.} \end{cases}
\end{aligned}
$$

Proof. Let $p(\mathrm{i}), \ldots, p(\mathrm{iv})$ be the number of elements $x \in M(q)$ satisfying part (i), ..., (iv) of Lemma 3.8, respectively.

Assume that q is even. Then $t_2(q) = p(\mathrm{ii}) - 1$, and $t_3(q) = p(\mathrm{iv}) - 1$. Since $M(q) = M^*(q)$, we also have $t_n^*(q) = t_n(q)$, for $n = 2, 3$.

Assume that q is odd. Then $t_2(q) = p(\mathrm{i}) - 1$, and $t_3(q) = p(\mathrm{iii}) - 1$. Note that $x \in M(q)$ satisfies (i) (resp. (ii)) if and only if $-x$ satisfies (i) (resp. (ii)); and that $y \in M(q)$ satisfies (iii) if and only if $-y$ satisfies (iv). Therefore $t_2^*(q) = 1/2 \cdot (p(\mathrm{i}) - 1 + p(\mathrm{ii}) - 1)$, $t_3^*(q) = 1/2 \cdot (p(\mathrm{iii}) - 1 + p(\mathrm{iv}) - 1)$.

It remains to calculate $p(\mathrm{i}), \ldots, p(\mathrm{iv})$. The right hand sides of parts (i), ..., (iv) consist of two exclusive statements. For $r = \mathrm{ii}, \mathrm{iii}, \mathrm{iv}$, let $p(r)(A)$ (resp. $p(r)(B)$) be the number of elements $x \in M(q)$ satisfying the first (resp. second) statement on the right hand side of (r). Thus, $p(r) = p(r)(A) + p(r)(B)$, for $r = \mathrm{ii}, \mathrm{iii}, \mathrm{iv}$.

Apparently, $p(\mathrm{i})$ equals 1 when q is even, and 2 when q is odd. Also, $p(\mathrm{ii})(A) = \rho$, $p(\mathrm{iii})(A) = \pi$, and $p(\mathrm{iv})(A) = p(\mathrm{iii})(A)$ (since $a^3 = -1$ if and only if $(-a)^3 = 1$).

We proceed to calculate $p(r)(B)$ for $r = \mathrm{ii}, \mathrm{iii}, \mathrm{iv}$. Let $x \in M(q)$ be written as in Lemma 3.8, with $(\alpha, \beta) \neq (0, 0)$. When x satisfies $(r)(B)$, the element b is uniquely determined by a. For instance, x satisfies $(\mathrm{iii})(B)$ if and only if $b = -1 - a$. Since ab equals 1 if and only if $\alpha \cdot \beta = 0$, Lemma 3.9 yields $p(r)(B) = \xi q_0 + (q - \xi)q_1$, where ξ is the number of elements $a \in GF(q)$ for which $ab = 1$. When $r = \mathrm{ii}$, we have $b = -a$, and so $\xi = \rho$. When $r = \mathrm{iii}$, we have $b = -1 - a$, so $\xi = \sigma$. When $r = \mathrm{iv}$, we have $b = 1 - a$, and so $\xi = \tau$.

Therefore, $p(\mathrm{ii}) = \rho + \rho q_0 + (q - \rho)q_1$, $p(\mathrm{iii}) = \pi + \sigma q_0 + (q - \sigma)q_1$, and $p(\mathrm{iv}) = \pi + \tau q_0 + (q - \tau)q_1$. Everything follows. □

The constants π, ρ, σ, and τ are known for every prime power q, of course. We write $a \mid b$ when a divides b, and $a \nmid b$ when it does not.

Lemma 3.11 *Let π, ρ, σ, and τ be as in Proposition* 3.10. *Then*

$$
\pi = \begin{cases} 3, & \text{if } 3 \mid q-1, \\ 1, & \text{otherwise,} \end{cases} \qquad \rho = \begin{cases} 1, & \text{if } q \text{ is even,} \\ 2, & \text{if } 4 \mid q-1, \\ 0, & \text{otherwise,} \end{cases}
$$

$$
\sigma = \begin{cases} 1, & \text{if } 3 \mid q, \\ 2, & \text{if } 3 \mid q-1, \\ 0, & \text{otherwise,} \end{cases} \qquad \tau = \begin{cases} 1, & \text{if } 3 \mid q, \\ 2, & \text{if } 3 \mid q-1, \\ 0, & \text{otherwise.} \end{cases}
$$

Proof. The multiplicative group $GF(q)^*$ is isomorphic to C_{q-1}. Since π counts the number of elements satisfying $x^3 = 1$, its value follows.

An element x satisfies $x^2 + x + 1 = 0$ and $x \neq 1$ if and only if $x^3 = 1$ and $x \neq 1$. Therefore, there are $\pi - 1$ elements satisfying $x^2 + x + 1 = 0$ and $x \neq 1$. The element $x = 1$ solves $x^2 + x + 1 = 0$ if and only if $3 \mid q$. The value of σ follows.

If q is even, there is a unique element satisfying $x^2 = -1$. Assume that q is odd. Then $x^2 = -1$ implies that $|x| = 4$. The value of ρ follows.

Finally, $x = -1$ solves $x^2 - x + 1 = 0$ if and only if $3 \mid q$. Assume that $x \neq -1$. Then $x^2 - x + 1 = 0$ is equivalent to $(x + 1)(x^2 - x + 1) = x^3 + 1 = 0$. Now, $x^3 = -1$ if and only if $(-x)^3 = 1$. The value of τ can thus be calculated from π. □

In particular, Proposition 3.10 and Lemma 3.11 imply that $t_2(q) = t_2^*(q) = q^6 - 1$ when q is even.

Lemma 3.11 suggests the following definition. We say that two prime powers q, q' are $\sim$-*equivalent* if the constants π, ρ, σ, and τ are the same for q, q'. It is easy to see that there are 8 equivalence classes with respect to $\sim$. When q is even, then $q \equiv 1, 2 \pmod 3$ (remember, q is a prime power), and 4 does not divide $q - 1$. When q is odd, then $q \equiv 0, 1, 2 \pmod 3$ and $q - 1 \equiv 0, 2 \pmod 4$. The constants are summarized in Table B.4 for each of these equivalence classes. The smallest class representative is also listed in Table B.4.

Example 3.12 *Let $q = 2$. Then $\pi = 1$, $\tau = 0$, and $q_1 = 4 \cdot 7 = 28$. Therefore $t_2^*(2) = 64 - 1 = 63$ and $t_3^*(2) = 1 + 2 \cdot 28 - 1 = 56$.*

Let $q = 3$. Then $\pi = \sigma = \tau = 1$, $\rho = 0$, $q_0 = 9 \cdot 29 - 1 = 260$, and $q_1 = 9 \cdot 26 = 234$. Therefore $t_2^*(3) = 1/2 \cdot 3 \cdot 234 = 351$, and $t_3^*(3) = 1/2 \cdot (2 \cdot 260 + 4 \cdot 234) = 728$.

Since $M^*(2)$ has $120 = 56 + 63 + 1$ elements and $M^*(3)$ has $3^3(3^4 - 1)/2 = 1080 = 351 + 728 + 1$ elements, we have just demonstrated that both $M^*(2)$, $M^*(3)$ consist of elements of order 1, 2 and 3. There are no other Paige loops with this property, as we will see next.

Lemma 3.13 *The only Paige loops with exponent 6 are $M^*(2)$ and $M^*(3)$.*

Proof. The group $L_2(q)$ has order $q(q - 1)(q + 1)/d$, where d is the greatest common divisor of $q - 1$ and 2 [13, p. x]. Thus q divides $|L_2(q)|$, and $L_2(q)$ contains an element of order p, where $q = p^n$. By Theorem 3.7, so does $M^*(q)$. Therefore $M^*(2)$ can have exponent 6 only if $q = p^n$, where $p = 2, 3$. Unquestionably, one could use Theorem 3.7 and properties of $L_2(q)$ to deduce that $n = 1$. However, we wish to use Proposition 3.10, Lemma 3.11 and Table B.4 instead.

Assume that $p = 2, 3$. Then $q \sim 4, 2, 9$, or 3. Suppose that $q \sim 4$. Then $t = t_2^*(q) + t_3^*(q)$ equals $q^6 - 1 + 2q_0 + (q - 2)q_1 = 2q^6 + q^3 - 3$. This equals to $|M^*(q)| = q^3(q^4 - 1)$ if and only if $s(q) = q^7 - 2q^6 - 2q^3 + 2 = 0$. But $s(4) > 0$, whence $s(q) > 0$ for every $q \sim 4$ (because 4 is the smallest representative, and all coefficients of $s(q)$ are less than 4).

Suppose that $q \sim 2$. Then $t = 2q^6 - q^3 - 1$, hence $t = |M^*(q)| - 1$ if and only if $2q^6 = q^7$. This happens if and only if $q = 2$.

Suppose that $q \sim 9$. Then $t = 1/2 \cdot (3q^6 + q^3 - 2)$, hence $t = |M^*(q)| - 1 = 1/2 \cdot (q^7 - q^3) - 1$ if and only if $q^7 - 3q^6 - 2q^3 = 0$. This is never the case for $q \sim 9$.

Finally, suppose that $q \sim 3$. Then $t = 1/2 \cdot (3q^6 - q^3 - 2)$, hence $t = |M^*(q)| - 1$ if and only if $3q^6 = q^7$. This happens if and only if $q = 3$. □

3.3 Explicit Automorphisms of Split Octonion Algebras and Paige Loops

Let us have a look at two classes of automorphisms of $\mathbb{O}(q)$.

3.3.1 Diagonal Automorphisms

Let $k = GF(q)$, and let $\mathrm{Lie}(q)$ denote the 3-dimensional Lie algebra k^3 where the vector product $\times$ plays the role of Lie bracket. Then $f : k^3 \longrightarrow k^3$ is an element of $\mathrm{Aut}(\mathrm{Lie}(q))$ if and only if f is a linear transformation onto k^3 satisfying

$$f(\alpha \times \beta) = f(\alpha) \times f(\beta)$$

for every α, $\beta \in k^3$. We say that a linear transformation $f : k^3 \longrightarrow k^3$ is *orthogonal* if f preserves the dot product, i.e., if

$$f(\alpha) \cdot f(\beta) = \alpha \cdot \beta$$

holds for every α, $\beta \in k^3$.

Proposition 3.14 (Diagonal Automorphisms of $\mathbb{O}(q)$) *For a non-singular orthogonal linear transformation $f : k^3 \longrightarrow k^3$, let $\widehat{f} : \mathbb{O}(q) \longrightarrow \mathbb{O}(q)$ be the mapping*

$$\widehat{f}\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} = \begin{pmatrix} a & f(\alpha) \\ f(\beta) & b \end{pmatrix}.$$

Then $\widehat{f} \in \mathrm{Aut}(\mathbb{O}(q))$ if and only if $f \in \mathrm{Aut}(\mathrm{Lie}(q))$. For $\lambda \in k^*$, define $\widehat{\lambda} : \mathbb{O}(q) \longrightarrow \mathbb{O}(q)$ by

$$\widehat{\lambda}\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} = \begin{pmatrix} a & \lambda\alpha \\ \lambda^{-1}\beta & b \end{pmatrix}.$$

Then $\widehat{\lambda} \in \mathrm{Aut}(\mathbb{O}(q))$ if and only if $\lambda^3 = 1$.

Proof. Both $\widehat{\lambda}$ and $\widehat{f}$ are clearly linear and preserve the norm. Since f is one-to-one, so is $\widehat{f}$. We have

$$\begin{aligned} &\widehat{f}\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}\widehat{f}\begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} \\ &= \begin{pmatrix} ac + f(\alpha)\cdot f(\delta) & af(\gamma) + df(\alpha) - f(\beta)\times f(\delta) \\ cf(\beta) + bf(\delta) + f(\alpha)\times f(\gamma) & f(\beta)\cdot f(\gamma) + bd \end{pmatrix}. \end{aligned}$$

On the other hand,

$$\widehat{f}\left(\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}\begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix}\right) = \begin{pmatrix} ac+\alpha\cdot\delta & f(a\gamma+d\alpha-\beta\times\delta) \\ f(c\beta+b\delta+\alpha\times\gamma) & \beta\cdot\gamma+bd \end{pmatrix}.$$

The sufficiency is now obvious, and the necessity follows by specializing the elements a, b, c, d, α, β, γ, δ.

Now for the mapping $\widehat{\lambda}$. We have

$$\widehat{\lambda}\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}\widehat{\lambda}\begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac+\alpha\cdot\delta & \lambda(a\gamma+d\alpha)-\lambda^{-2}\beta\times\delta \\ \lambda^{-1}(c\beta+b\delta)+\lambda^2\alpha\times\gamma & \beta\cdot\gamma+bd \end{pmatrix},$$

whereas

$$\widehat{\lambda}\left(\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}\begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix}\right) = \begin{pmatrix} ac+\alpha\cdot\delta & \lambda(a\gamma+d\alpha-\beta\times\delta) \\ \lambda^{-1}(c\beta+b\delta+\alpha\times\gamma) & \beta\cdot\gamma+bd \end{pmatrix}.$$

The result follows. □

Remark 3.15 *We obtain some automorphisms $\widehat{\lambda}$ from Proposition* 3.14 *if and only if $q = 3m+1$. In such a case, we obtain exactly* 2 *nontrivial automorphisms.*

For $f : k^3 \longrightarrow k^3$, let $-f$ be the map *opposite* to f, i.e., $(-f)(\alpha) = -(f(\alpha))$ for all $\alpha \in k^3$. Also, for a permutation $\pi \in S_3$, consider π as a linear transformation on k^3 defined by

$$\pi(\alpha_1, \alpha_2, \alpha_3) = (\alpha_{\pi(1)}, \alpha_{\pi(2)}, \alpha_{\pi(3)}).$$

Apparently, $-S_3 = \{-\pi;\ \pi \in S_3\}$ is a set of non-singular orthogonal linear transformations.

Lemma 3.16 $\widehat{-\pi} \in \mathrm{Aut}(\mathbb{O}(q))$ *for every $\pi \in S_3$.*

Proof. Let $\pi \in S_3$ be the transposition interchanging 1 and 2, and let α, $\beta \in k^3$. Then

$$\pi(\alpha\times\beta) = (\alpha_3\beta_1-\alpha_1\beta_3,\ \alpha_2\beta_3-\alpha_3\beta_2,\ \alpha_1\beta_2-\alpha_2\beta_1),$$

and

$$\pi(\alpha)\times\pi(\beta) = (\alpha_1\beta_3-\alpha_3\beta_1,\ \alpha_3\beta_2-\alpha_2\beta_3,\ \alpha_2\beta_1-\alpha_1\beta_2).$$

Hence $-\pi(\alpha\times\beta) = \pi(\alpha)\times\pi(\beta) = (-\pi)(\alpha)\times(-\pi)(\beta)$. Thanks to the symmetry of S_3, we have shown that $-\pi \in \mathrm{Aut}(\mathrm{Lie}(q))$ for every $\pi \in S_3$. The rest follows from Proposition 3.14. □

There is another obvious automorphism when q is even.

Lemma 3.17 *Define $\partial : \mathbb{O}(q) \longrightarrow \mathbb{O}(q)$ by*

$$\partial\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} = \begin{pmatrix} b & \beta \\ \alpha & a \end{pmatrix}.$$

Then $\partial \in \mathrm{Aut}(\mathbb{O}(q))$ *if and only if* $q = 2^n$.

Proof. The result follows by straightforward calculations. The linearity is obvious. We have

$$\partial \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \partial \begin{pmatrix} a' & \alpha' \\ \beta' & b' \end{pmatrix} = \begin{pmatrix} bb' + \beta \cdot \alpha' & b\beta' + a'\beta - \alpha \times \alpha' \\ b'\alpha + a\alpha' + \beta \times \beta' & \alpha \cdot \beta' + aa' \end{pmatrix},$$

whereas

$$\partial \left(\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \begin{pmatrix} a' & \alpha' \\ \beta' & b' \end{pmatrix} \right) = \begin{pmatrix} bb' + \beta \cdot \alpha' & b\beta' + a'\beta + \alpha \times \alpha' \\ b'\alpha + a\alpha' - \beta \times \beta' & \alpha \cdot \beta' + aa' \end{pmatrix}.$$

These two vector matrices coincide in general only over $GF(2^n)$. □

3.3.2 Conjugations

As in [35, Section III.4], a (*right*) *pseudo-automorphism* of a quasigroup Q is a bijection $f : Q \longrightarrow Q$ such that

$$x^f (y^f c) = (xy)^f c$$

is satisfied for some fixed $c \in Q$ and every $x, y \in Q$. The element c is called a *companion* of f. In general, pseudo-automorphisms can have more companions.

As we have already remarked in the Introduction, the *right nucleus*

$$N_\rho(Q) = \{c;\ [a, b, c] = 0 \text{ for every } a, b \in Q\}$$

coincides with the *nucleus*

$$N(Q) = \{c;\ c \text{ associates with every } a, b \in Q\}$$

when Q is a Moufang loop.

Theorem IV.1.8. of [35] says that the set of all companions of a pseudo-automorphism f of a Moufang loop Q is the coset $cN(Q)$, where c is any of the companions of f. Consequently, every pseudo-automorphism of a Paige loop has a unique companion.

This leads us to the following proposition:

Proposition 3.18 (Conjugations of $M^*(q)$) *For every* $x \in Q = M^*(q)$, *define the conjugation* $T(x) : Q \longrightarrow Q$ *by* $yT(x) = x^{-1}yx$. *Then* $T(x) \in \mathrm{Aut}(Q)$ *if and only if* x *is of order* 3.

Proof. By Theorem IV.1.6 of [35], $T(x)$ is a pseudo-automorphism with companion x^{-3}. If x is of order 3, then $T(x)$ is clearly an automorphism of Q. Conversely, if $T(x) \in \mathrm{Aut}(Q)$, it is a pseudo-automorphism with companions e and x^{-3}. By the uniqueness of the companion, $x^{-1} = e$. □

3.3.3 Conjugations Fixing Chosen Involution

This subsection deals with a specific problem, but we introduce here some general ideas which we will use repeatedly in Chapter 5.

Assume that A is an algebra, $a \in A$, and f, $g \in \mathrm{Aut}(A)$ are such that $f(a) = g(a)$. Then the automorphisms $g^{-1}f$, gf^{-1} fix a. Observe that $f(a) = g(a)$ if and only if $f(h(a)) = g(h(a))$ for every $h \in \mathrm{Aut}(A)$ such that $h(a) = a$.

When q is even, the element

$$x_0 = \begin{pmatrix} 0 & (1,\,1,\,1) \\ (1,\,1,\,1) & 0 \end{pmatrix}$$

belongs to $M^*(q)$. We are interested in x_0 because x_0 is fixed by all automorphisms $\widehat{\pi}$ (where $\pi = -\pi \in S_3$), and by the automorphism ∂. We write $u \sim v$ for two elements u, $v \in M^*(q)$ of order 3, if and only if $x_0T(u) = x_0T(v)$.

For a vector α, let $\mathrm{w}(\alpha)$ be the number of nonzero coordinates of α, the *weight* of α.

For the rest of this section, let $q = 2$.

Proposition 3.19 *Let $v \in M^*(2)$ be an element of order 3. Then*

$$v = \begin{pmatrix} a & \alpha \\ \beta & 1+a \end{pmatrix}$$

for some $a \in k$, α, $\beta \in k^3$, and $v \sim \partial(v)$ if and only if $\mathrm{w}(\alpha - \beta) = 1$.

Proof. The form of v is guaranteed by Lemma 3.8. Let

$$u = \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix}.$$

Then

$$u^{-1} = \begin{pmatrix} d & \gamma \\ \delta & c \end{pmatrix}, \quad \partial(u^{-1}) = \begin{pmatrix} c & \delta \\ \gamma & d \end{pmatrix},$$

and we may therefore assume that $a = 0$ and $\mathrm{w}(\alpha) \geq \mathrm{w}(\beta)$. Since $\det v = \alpha \cdot \beta$, we must have $\alpha \cdot \beta = 1$. Because $\widehat{\pi}$ fixes x_0 for every $\pi \in S_3$, we may further assume that $\alpha_1 = \beta_1 = 1$, where $\alpha = (\alpha_1,\, \alpha_2,\, \alpha_3)$, $\beta = (\beta_1,\, \beta_2,\, \beta_3)$.

Assume, for a while, that $\alpha = \beta$. Then $\partial(v) = v^{-1}$. When $v \sim \partial(v)$, we have $v^{-1}x_0v = vx_0v^{-1}$, or $vx_0v^{-1} = x_0$. But, with $\varphi = (1,\,1,\,1)$,

$$vx_0v^{-1} = \begin{pmatrix} \alpha\cdot\varphi & \alpha\times\varphi \\ \varphi+\alpha\times\varphi & \alpha\cdot\varphi \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ \alpha & 0 \end{pmatrix} = \begin{pmatrix} \alpha\cdot\varphi & - \\ - & \alpha\cdot\varphi \end{pmatrix},$$

thus $\alpha \cdot \varphi = 0$. In other words, $\mathrm{w}(\alpha) \equiv 0 \pmod 2$. Then $\alpha \cdot \alpha = 0$, a contradiction.

We can therefore assume that $\alpha \neq \beta$; moreover, that $\alpha_2 \neq \beta_2$. There are then only three cases to consider, since v must be one of

$$v_0 = \begin{pmatrix} 0 & (1,\,1,\,0) \\ (1,\,0,\,0) & 1 \end{pmatrix}, \quad v_1 = \begin{pmatrix} 0 & (1,\,1,\,1) \\ (1,\,0,\,0) & 1 \end{pmatrix},$$
$$v_2 = \begin{pmatrix} 0 & (1,\,0,\,1) \\ (1,\,1,\,0) & 1 \end{pmatrix}.$$

Check that $v_i \sim \partial(v_i)$ if and only if $i = 0$. $\square$

Let $[v]_\sim$ denote the class of elements equivalent to v in $M^*(2)$.

Lemma 3.20 *Assume that $v \in M^*(2)$ is as in Proposition* 3.19*, and that $v \sim \partial(v)$. Then $[v]_\sim \supseteq \{v,\ \partial(v),\ \widehat{\pi}(v),\ \partial(\widehat{\pi}(v))\}$, where π is the transposition interchanging the two coordinates on which α and β agree.*

Proof. The vectors α, β agree on exactly two positions, by Proposition 3.19. Following the same train of thoughts as in the proof of Proposition 3.19, we may assume that $v = v_0$. Then π is the transposition interchanging 1 and 3. Verify that $v \sim \widehat{\pi}(v)$. Since $\widehat{\pi}(v) \sim \partial(\widehat{\pi}(v))$, we are done. $\square$

Remark 3.21 *Actually, more is true. It is possible to show that $[v]_\sim \neq \{v\}$ if and only if $v \sim \partial(v)$, and that in such a case $[v]_\sim = \{v,\ \partial(v),\ \widehat{\pi}(v),\ \partial(\widehat{\pi}(v))\}$. We will neither prove nor need this fact.*

Chapter 4

Presentations

In order to derive a presentation for a groupoid $A = (A, \cdot)$, one usually needs to introduce a normal form for elements of A written in terms of some generators. Such a normal form is not easy to find when A is not commutative, and even more so when A is not associative. Once a normal form is found, it might be still difficult to come up with presenting relations. Indeed, it is often the case that the only known presentation for a non-associative groupoid is the *table presentation*, i.e., the presentation consisting of all relations $x \cdot y = z$ such that $x \cdot y$ equals z in A, and where x, y run over all elements of A. Table presentations are extremely useful when one constructs a multiplication table for A, however, they are of little use when one needs to identify A as a subgroupoid of another groupoid. To do the latter, it is necessary, in principle, to evaluate all products $x \cdot y$ with x, $y \in A$. It is therefore desirable to have access to presentations with a few presenting relations.

We derive presentations for a certain class of Moufang loops called $M_{2n}(G, 2)$, first studied by O. Chein [9]. Two of these loops will later emerge as subloops of Paige loops.

Thirty years ago, Chein and Pflugfelder [12] proved that the smallest non-associative Moufang loop is of order 12 and is unique up to isomorphism. It coincides with $M = M_{12}(S_3, 2)$. Guided by our presentation for M, we give a new, visual description of M in Section 4.4.

To begin with, we introduce a useful technique for counting in lattices of subalgebras.

4.1 Hasse Constants

Let A, B, C be (universal) algebras, $A \leq C$. For $X \leq C$, let O_X denote the orbit of X under the natural action of $\mathrm{Aut}(C)$ on the set of subalgebras of C isomorphic to X. We will speak of the subalgebras of C isomorphic to X as of *copies* of X in C. We define

$$\begin{aligned} \mathcal{H}_C(B) &= |\{B_0 \leq C;\ B_0 \cong B\}|, \\ \mathcal{H}_C(A|B) &= |\{B_0 \leq C;\ A \leq B_0 \cong B\}|, \\ \mathcal{H}^O_C(A|B) &= |\{B_0 \leq C;\ A \leq B_0,\ B_0 \in O_B\}|. \end{aligned}$$

In words, $\mathcal{H}_C(B)$ counts the number of copies of B in C, $\mathcal{H}_C(A|B)$ counts the number of copies of B in C containing A, and $\mathcal{H}_C^O(A|B)$ counts the number of copies of B in C containing A, and in the same orbit as B.

Yet another description of these constants is perhaps the most appealing. If B is a subalgebra of C, the constant $\mathcal{H}_C(B)$ counts the number of edges connecting C to a copy of B in the complete Hasse diagram of subalgebras of C. The other constants can be interpreted in a similar way. We will therefore refer to these constant jointly as *Hasse constants*.

Note that $\mathcal{H}_C(A|B) = \mathcal{H}_C^O(A|B)$ if $\mathrm{Aut}(C)$ acts transitively on the copies of B in C.

Lemma 4.1 *Let A, B, C be algebras, $A \leq C$. Then:*

(i) *If $B' \cong B$, $C' \cong C$, then $\mathcal{H}_C(B) = \mathcal{H}_{C'}(B')$.*

(ii) *If $A' \in O_A$, $B' \cong B$, then $\mathcal{H}_C(A|B) = \mathcal{H}_C(A'|B')$.*

(iii) *If $A' \in O_A$, $B' \in O_B$, then $\mathcal{H}_C^O(A|B) = \mathcal{H}_C^O(A'|B')$.*

Proof. Part (i) is obvious from the definition of $\mathcal{H}_C(B)$. Also, $\mathcal{H}_C(A|B) = \mathcal{H}_C(A|B')$ holds if $B \cong B'$. Choose $A' \in O_A$, and let $f \in \mathrm{Aut}(C)$ be an automorphism mapping A to A'. Then $\mathcal{H}_C(A|B) = \mathcal{H}_{f(C)}(f(A)|f(B)) = \mathcal{H}_C(A'|f(B)) = \mathcal{H}_C(A'|B)$, where the last equality holds because $B \cong f(B)$. This proves (ii).

Part (iii) is similar. Let $B' \in O_B$. Then $\mathcal{H}_C^O(A|B) = \mathcal{H}_C^O(A|B')$ because $O_B = O_{B'}$. Let $A' \in O_A$, and let $f \in \mathrm{Aut}(C)$ be an automorphism mapping A to A'. Then $\mathcal{H}_C^O(A|B) = \mathcal{H}_{f(C)}^O(f(A)|f(B)) = \mathcal{H}_C^O(A'|f(B)) = \mathcal{H}_C^O(A'|B)$, where the last equality holds because $f(B) \in O_B$. □

Proposition 4.2 *Let A, B, C be algebras, $A \leq C$. Let $A_1, \ldots, A_m$ be representatives from all the orbits $O_{A_1}, \ldots, O_{A_m}$ of the action of $\mathrm{Aut}(C)$ on the copies of A in C. Similarly, let $B_1, \ldots, B_n$ be representatives for B. Then*

$$\mathcal{H}_C(A|B) = \sum_{j=1}^{n} \mathcal{H}_C^O(A|B_j), \tag{4.1}$$

$$\mathcal{H}_B(A) \cdot |O_B| = \sum_{i=1}^{m} |O_{A_i}| \cdot \mathcal{H}_C^O(A_i|B), \tag{4.2}$$

$$\mathcal{H}_B(A) \cdot \mathcal{H}_C(B) = \sum_{i=1}^{m} |O_{A_i}| \cdot \mathcal{H}_C(A_i|B). \tag{4.3}$$

If $\mathrm{Aut}(C)$ acts transitively on the copies of B (i.e., if $n = 1$), then equation (4.2) and (4.3) are the same.

If $\mathrm{Aut}(C)$ acts transitively on the copies of A (i.e., if $m = 1$), then

$$\mathcal{H}_B(A) \cdot |O_B| = \mathcal{H}_C(A) \cdot \mathcal{H}_C^O(A|B), \tag{4.4}$$

$$\mathcal{H}_B(A) \cdot \mathcal{H}_C(B) = \mathcal{H}_C(A) \cdot \mathcal{H}_C(A|B). \tag{4.5}$$

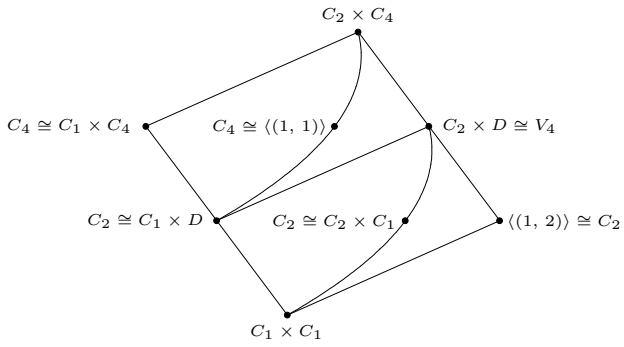

Figure 4.1: Lattice of subgroups of $C_2 \times C_4$

Proof. The proof of (4.1) is straightforward because every copy of B in C belongs to exactly one orbit O_{B_j}.

To establish (4.2), count twice the cardinality t of $\{(A_0,\, B_0);\ A_0 \leq B_0 \in O_B,\, A_0 \cong A\}$. On the one hand,

$$t = \sum_{B_0 \in O_B} \mathcal{H}_{B_0}(A) \overset{4.1(\mathrm{i})}{=} \sum_{B_0 \in O_B} \mathcal{H}_B(A) = \mathcal{H}_B(A) \cdot |O_B|.$$

On the other hand,

$$\begin{aligned} t &= \sum_{A_0 \leq C,\, A_0 \cong A} \mathcal{H}^O_C(A_0|B) \\ &= \sum_{i=1}^{m} \sum_{A_0 \in O_{A_i}} \mathcal{H}^O_C(A_0|B) \overset{4.1(\mathrm{iii})}{=} \sum_{i=1}^{m} |O_{A_i}| \cdot \mathcal{H}^O_C(A_i|B). \end{aligned}$$

The proof of (4.3) is similar to (4.2). Just count twice the cardinality of the set

$$\{(A_0,\, B_0);\ A_0 \leq B_0 \leq C,\, A_0 \cong A,\, B_0 \cong B\}.$$

Equations (4.2) and (4.3) are the same when $n = 1$. When $m = 1$, (4.4) and (4.5) follow immediately from (4.2) and (4.3), respectively. □

Example 4.3 *This example illustrates that the Hasse constant $\mathcal{H}_C(A|B)$ may differ from $\mathcal{H}_C(A'|B)$ even though $A \cong A'$. Let C be the group $C_2 \times C_4$, $C_2 = \{0,\, 1\}$, $C_4 = \{0,\, 1,\, 2,\, 3\}$, and let $D = \{0,\, 2\}$ be the (unique) two-element subgroup of C_4. The lattice of subgroups of C is depicted in Figure* 4.1.

Then with $B = C_4$, $A = C_1 \times D \cong C_2 \times C_1 = A'$, we have $\mathcal{H}_C(A|B) = |\{C_1 \times C_4,\, \langle (1,\, 1) \rangle\}| = 2 \neq 0 = \mathcal{H}_C(A'|B)$.

4.2 The Loops $M_{2n}(G, 2)$

The infinite class of Moufang loops $M_{2n}(G, 2)$ is obtained as follows:

Theorem 4.4 (Chein [10, Theorem 0]) *If L is a finite non-associative Moufang loop for which every minimal set of generators contains an element of order 2, then L contains a non-abelian subgroup G and an element u of order 2 such that each element of L may be uniquely expressed in the form gu^α, where $g \in G$ and $\alpha = 0$ or 1. Furthermore, the product of two elements of L is given by*

$$(g_1u^\delta)(g_2u^\epsilon) = (g_1^\nu g_2^\mu)^\nu u^{\delta+\varepsilon}, \tag{4.6}$$

where $\nu = (-1)^\varepsilon$ and $\mu = (-1)^{\varepsilon+\delta}$.

Conversely, given any non-abelian group G of order n, the loop L constructed as above is a non-associative Moufang loop of order $2n$. It will be denoted by $M_{2n}(G, 2)$.

When speaking of $M_{2n}(G, 2)$, we will always fix the element u.

We are going to prove several structural theorems for $M_{2n}(G, 2)$. Some of them are hinted at in Chein [10]. Let us get started with a rather general observation.

Proposition 4.5 *Let Q be a quasigroup, $G \leq Q$ and $u \in Q \setminus G$ such that Q is the disjoint union of G and Gu. Assume that $Gu \cdot Gu \subseteq G$, and $G \cdot Gu \subseteq Gu$. Let $H \leq Q$. Then either $H \leq G$, or $|H \cap G| = |H \cap Gu|$.*

Proof. Assume that $H \not\leq G$, and let $\{g_1, \ldots, g_m\} = H \cap G$, $\{h_1u, \ldots, h_nu\} = H \cap Gu$, where $g_i, h_j \in G$. Since $g_i \cdot h_1u \neq g_j \cdot h_1u$ for $i \neq j$, we get $n \geq m$. Since $h_iu \cdot h_1u \neq h_ju \cdot h_1u$ for $i \neq j$, we get $m \geq n$. □

Notice that $M_{2n}(G, 2)$ satisfies the assumptions of Proposition 4.5. The following easy lemma tells us something about the local behaviour of $M_{2n}(G, 2)$.

Lemma 4.6 *Let $g, h, k \in G$, and assume that $M_{2n}(G, 2)$ is constructed as in Theorem 4.4. Then*

(i) $|gu| = 2$,

(ii) $g \cdot hu = hg \cdot u$, $gu \cdot h = gh^{-1} \cdot u$, $gu \cdot hu = h^{-1}g$,

(iii) $[g, h, ku] = e$ *if and only if* $[g, h] = e$,

(iv) $[g, hu, ku] = e$ *if and only if* $[g, k^{-1}h] = e$,

(v) $[gu, hu, ku] = e$ *if and only if* $gh^{-1}k = kh^{-1}g$.

Proof. Parts (i) and (ii) follow immediately from (4.6). As for (iii), $g(h \cdot ku) = g(kh \cdot u) = khg \cdot u$, and $gh \cdot ku = kgh \cdot u$. As for (iv), $g(hu \cdot ku) = gk^{-1}h$, and $(g \cdot hu)ku = (hg \cdot u)ku = k^{-1}hg$. Finally, $gu(hu \cdot ku) = gu \cdot k^{-1}h = gh^{-1}k$, and $(gu \cdot hu)ku = h^{-1}g \cdot ku = kh^{-1}g$. □

Lemma 4.7 *The multiplication formula* (4.6) *remains valid if we replace* u *by* xu ($x \in G$). *More precisely, for every* $x \in G$, *we have*

$$(g_1(xu)^\delta)(g_2(xu)^\epsilon) = (g_1^\nu g_2^\mu)^\nu (xu)^{\delta+\varepsilon}, \tag{4.7}$$

where $\nu = (-1)^\varepsilon$ *and* $\mu = (-1)^{\varepsilon+\delta}$.

Proof. We prove (4.7) by considering all possible values of δ and ε. Let s (resp. t) be the left (resp. right) hand side of (4.7). We will use Lemma 4.6 repeatedly. If $\delta = \varepsilon = 0$, we have $s = g_1 g_2$, and $t = g_1 g_2$. If $\delta = 1$ and $\varepsilon = 0$, we have $s = g_1(xu) \cdot g_2 = (xg_1 \cdot u)g_2 = xg_1 g_2^{-1} \cdot u$, and $t = g_1 g_2^{-1} \cdot xu = xg_1 g_2^{-1} \cdot u$. If $\delta = 0$ and $\varepsilon = 1$, we have $s = g_1 \cdot g_2(xu) = g_1(xg_2 \cdot u) = xg_2 g_1 \cdot u$, and $t = (g_1^{-1} g_2^{-1})^{-1} xu = g_2 g_1 \cdot xu = xg_2 g_1 \cdot u$. Finally, if $\delta = \varepsilon = 1$, we have $s = g_1(xu) \cdot g_2(xu) = (xg_1 \cdot u)(xg_2 \cdot u) = (xg_2)^{-1} xg_1 = g_2^{-1} g_1$, and $t = (g_1^{-1} g_2)^{-1} = g_2^{-1} g_1$. □

4.2.1 Sylow Theorems for $M_{2n}(G, 2)$

For a prime p, a finite algebra A is said to be a *p-algebra* if $|A| = p^k$ for some integer k. A p-algebra A is a *Sylow p-subalgebra* of B if $A \leq B$ and A is not a proper subalgebra of any p-algebra $C \leq B$. The set of Sylow p-subalgebras of B will be denoted by $\mathrm{Syl}_p(B)$. Also, let $n_p(B) = |\mathrm{Syl}_p(B)|$.

This definition is motivated by group theory, naturally. In the variety of groups, the six statements (A)–(F), found below, are satisfied. They are usually referred to as *Sylow Theorems*. Part (C) is habitually not mentioned because it follows directly from (D), at least in a variety where every conjugation is an automorphism. We do not have this luxury in the variety of loops. (The loops where every inner mapping is an automorphism are called *A-loops* [6]).

Let A be a finite algebra of order $n = p^s m$, where s is an integer and p is a prime not dividing m. Let us formulate six statements about $\mathrm{Syl}_p(A)$, that are true if A is a group (cf. any book on abstract algebra or group theory, for instance [27, Ch. 5]), but not necessarily for every algebra A.

- (A) Every p-algebra $B \leq A$ of order p^r (with $r < s$) is contained in some p-algebra $C \leq A$ of order p^{r+1}.
- (B) Every Sylow p-subalgebra of A has order p^s.
- (C) All Sylow p-subalgebras of A are isomorphic.
- (D) If it makes sense to speak about conjugations in A, i.e., if A has a unique binary operation $\cdot$ such that every element of A has a two-sided inverse with respect to $\cdot$, then all Sylow p-subalgebras of A are conjugate.
- (E) $n_p(A) \equiv 1 \pmod{p}$.
- (F) $n_p(A)$ divides m.

We would like to see which of these statements are true for the loops $M_{2n}(G, 2)$.

Lemma 4.8 *Let H be a subgroup of $G \leq M_{2n}(G, 2)$. Then $\langle H, gu\rangle \cong \langle H, u\rangle$ for every $g \in G$, and $|\langle H, u\rangle| = 2|H|$. Moreover, $\langle H, gu\rangle$ is associative if and only if H is abelian.*

Proof. By Lemma 4.7, $\langle H, gu\rangle$ behaves just as $\langle H, u\rangle$. By the definition, $\langle H, u\rangle = M_{2|H|}(H, 2)$. □

Lemma 4.9 *Every subloop of $M_{2n}(G, 2)$ is either a subgroup of G or of the form $\langle H, gu\rangle$ for some $H \leq G$ and $g \in G$.*

Proof. Let $L \leq M_{2n}(G, 2)$, $L \not\leq G$. By Proposition 4.5, $H = L \cap G$ has $|L|/2$ elements. If $L = M_{2n}(G, 2)$, there is nothing to prove. Otherwise, pick $g \in L \setminus G$. Then $L = \langle H, gu\rangle$. □

Theorem 4.10 (Sylow Theorems for $M_{2n}(G, 2)$) *Let G be a non-abelian group. Then the non-associative Moufang loop $A = M_{2n}(G, 2)$ satisfies statements (A), (B), (C) and (E), for every prime p. Claim (D) holds if p is odd. Claim (F) holds if and only if p is odd or $p = 2$ and $n_2(G) = 1$.*

Proof. Let L be a Sylow p-subloop of A, $|A| = p^s m$, where p foes not divide m. By Lemma 4.9, either $L \leq G$, or $p = 2$. Assume that p is odd. Then the statements (A)–(E) are satisfied thanks to the classical Sylow Theorems for groups. (We do not claim that the appropriate conjugation is an automorphism of A.) Note that $n = |G| = p^s m/2$. Thus (F) holds, too, since $n_p(A) = n_p(G)$ divides $m/2$, and hence $n_p(A)$ divides m.

Assume that $p = 2$. Then $n = |G| = 2^{s-1}m$. Let $L \leq G$, $|L| = 2^r$, $r < s$. If $L \leq A$, it is contained in $\langle L, u\rangle$, and $|\langle L, u\rangle| = 2^{r+1}$. If $L \not\leq G$, it is of the form $\langle H, gu\rangle$, $H \leq G$, $g \in G$, $|H| = 2^{r-1}$. Since $r - 1 < s - 1$, H is contained in a group $K \leq G$, $|K| = 2^r$. Then $L \leq \langle K, gu\rangle$, $|\langle K, gu\rangle| = 2^{r+1}$. This proves (A). Pick $L \in \mathrm{Syl}_2(A)$, $|L| = 2^r$. If $r > s$, the 2-group $L \cap G \leq G$ has order 2^r or $2^{r-1} > 2^{s-1}$, a contradiction. If $r < s$, then $L \notin \mathrm{Syl}_2(A)$ by (A). This proves (B). The collection $\mathcal{S} = \{\langle H, gu\rangle;\ H \in \mathrm{Syl}_2(G), g \in G\}$ contains $n \cdot n_2(G)/|H| = m \cdot n_2(G)$ distinct Sylow 2-subloops of A, all isomorphic by Lemma 4.7 and by the classical Sylow Theorems. Also, $\mathrm{Syl}_2(A) \subseteq \mathcal{S}$. Therefore (C) holds. Moreover, $n_2(A) = m \cdot n_2(G) \equiv 1 \pmod 2$ because $n_2(G) \equiv 1$ and m is odd. We have proved (E). Finally, $n_2(A)$ divides m if and only if $n_2(G) = 1$. □

Remark 4.11 *Does (D) hold for every loop $A = M_{2n}(G, 2)$ when $p = 2$? It does if G has a unique Sylow 2-subgroup such that $G^2 \cap gH \neq \emptyset$ for every $g \in G \setminus H$. To see this, put $H_1 = \langle H, u\rangle$, and let H_2 be another Sylow 2-subloop of A. By the uniqueness of H, we have $H_2 = \langle H, gu\rangle$ for some $g \in G \setminus H$. Then $H_2 = H \cup H \cdot gu = H \cup gH \cdot u$. There is $x \in G$ such that $x^{-2} \in gH$. We claim that $H_1 T(x) = H_2$. Clearly, $HT(x) = H$. Finally, $uT(x) = x^{-1}ux = x^{-2}u \in gH \cdot u \subseteq H_2$, and we are done.*

4.2.2 A Structural Result for $M_{2n}(G, 2)$

Recall the Hasse constants, and let us further examine the subloop structure of $M_{2n}(G, 2)$.

Proposition 4.12 *Let $M_{2n}(G, 2)$ be constructed as in Theorem 4.4.*

(i) *We have*

$$\mathcal{H}_{M_{2n}(G,2)}(C_m) = \begin{cases} \mathcal{H}_G(C_m), & \text{if } m \neq 2, \\ \mathcal{H}_G(C_2) + n, & \text{if } m = 2. \end{cases}$$

(ii) $\langle H, gu\rangle \cong (C_2)^{k+1}$ *for every* $g \in G$, $H \leq G$, $H \cong (C_2)^k$, $k = 0, 1, \ldots$.

(iii) *For* $k \geq 1$,

$$\mathcal{H}_{M_{2n}(G,2)}((C_2)^k) = \begin{cases} 0, & \text{if } 2^{k-1} \nmid n, \\ \mathcal{H}_G((C_2)^k) + \mathcal{H}_G((C_2)^{k-1}) \cdot n/2^{k-1}, & \text{otherwise.} \end{cases}$$

(iv) $\langle g, hu\rangle \cong S_3$ *for every* $g, h \in G$ *with* $|g| = 3$.

(v) *Assume that G contains an element of order 3, and that S_3 is not a subgroup of G. Then G is the unique subgroup of $M_{2n}(G, 2)$ isomorphic to G, i.e.,* $\mathcal{H}_{M_{2n}(G,2)}(G) = 1$.

Proof. Let $m > 2$. A group isomorphic to C_m must be contained in G, by Lemma 4.6(i). Every loop $\langle gu\rangle$ ($g \in G$) is isomorphic to C_2. This proves (i).

Let $H \leq G$, $H \cong (C_2)^k$, $g \in G$. By Lemmas 4.6 and 4.8, $\langle H, gu\rangle$ is a group of order 2^{k+1} and exponent 2.

To show (iii), let $H \cong (C_2)^k$ be a subgroup of $M_{2n}(G, 2)$ not contained in G. By Proposition 4.5, $H \cap G$ is isomorphic to $(C_2)^{k-1}$. On the other hand, given a subgroup $A \cong (C_2)^{k-1}$ of G and any element g of G, the group $\langle A, gu\rangle$ is isomorphic to $(C_2)^k$, by (ii). This proves (iii).

Let $g \neq h$ be in G, $|g| = 3$. Then $\langle g, hu\rangle \cong S_3$, since $g^3 = (hu)^2 = (g(hu))^2 = e$.

We are going to prove (v). Let $L \neq G$ be a subgroup of $M_{2n}(G, 2)$ isomorphic to G. There is $g \in L$ of order 3. By (i), g is in G. Pick $x \in L \setminus G$. Necessarily, $x = hu$ for some $h \in G$. Then $S_3 \cong \langle g, hu\rangle \leq L$ by (iv), a contradiction. □

4.3 Presentations for $M_{2n}(G, 2)$

The infinite class of Moufang loops of type $M_{2n}(G, 2)$ represents a significant portion of non-associative Moufang loops of small order. Let $\pi(m)$ be the number of isomorphism types of non-associative Moufang loops of order at most m, and let $\sigma(m)$ be the number of non-associative loops of the form $M_{2n}(G, 2)$ of order at most m. Then, according to Chein's classification [10], $\pi(31) = 13$, $\sigma(31) = 8$, $\pi(63) = 158$, $\sigma(63) = 50$. (As Orin Chein kindly notified me, Edgar Goodaire noticed that the loop $M_{12}(S_3, 2) \times C_3$ is missing in [10]. He also observed that $M_{48}(5, 5, 5, 3, 3, 0)$ is isomorphic to $M_{48}(5, 5, 5, 3, 6, 0)$, and $M_{48}(5, 5, 5, 3, 3, 6)$ to $M_{48}(5, 5, 5, 3, 6, 6)$. That is why $\pi(63)$ equals 158, rather than 159.) This demonstrates eloquently the abundance of loops of type $M_{2n}(G, 2)$ among Moufang loops of small order.

We derive compact presentations for $M_{2n}(G,\,2)$ for every finite, two-generated group G. Professor Kenneth Johnson informs me that he has just generalized the construction of $M_{2n}(G,\,2)$, and it seems likely that the methods introduced here will be applicable to his loops as well.

We start with the table presentation

$$gu^{\delta}\cdot hu^{\varepsilon}=(g^{(-1)^{\varepsilon}}h^{(-1)^{\delta+\varepsilon}})^{(-1)^{\varepsilon}}u^{\delta+\varepsilon}\quad(g,\,h\in G;\ \delta,\,\varepsilon=0,\,1). \tag{4.8}$$

for $M_{2n}(G,\,2)$—that is the same as (4.6)—and prove

Theorem 4.13 (Presentation for $M_{2n}(G,\,2)$) *Let $G=\langle x,\,y;\ R\rangle$ be a presentation for a finite group G, where R is a set of relations in generators x, y. Then $M_{2n}(G,\,2)$ is presented by*

$$\langle x,\,y,\,u;\ R,\,u^2=(xu)^2=(yu)^2=(xy\cdot u)^2=e\rangle, \tag{4.9}$$

where e is the neutral element of G.

Let us emphasize that (4.9) is a presentation in the *variety of Moufang loops*, not groups.

The complicated multiplication formula (4.8) merely describes the four cases

$$g\cdot h = gh, \tag{4.10}$$
$$gu\cdot h = gh^{-1}\cdot u, \tag{4.11}$$
$$g\cdot hu = hg\cdot u, \tag{4.12}$$
$$gu\cdot hu = h^{-1}g \tag{4.13}$$

in a compact way (cf. Lemma 4.6). In particular, identities (4.13) and (4.11) imply

$$u^2=e,\ \ gu=ug^{-1}\ (g\in G). \tag{4.14}$$

We claim that (4.14) is equivalent to (4.8). An element $g\in G$ will be called *good* if $gu=ug^{-1}$ can be derived from (4.9).

Lemma 4.14 *If $h\in G$ is good, then* (4.11) *holds. If g, h, $hg\in G$ are good, then* (4.12) *holds. If g, $g^{-1}h$ are good, then* (4.13) *holds.*

Proof. We have $gu\cdot h=(gu\cdot h)u\cdot u=(g\cdot uhu)u=(g\cdot h^{-1}uu)u=gh^{-1}\cdot u$ if h is good. Assume that g, h, hg are good. Then $g\cdot hu=g\cdot uh^{-1}=u\cdot u(g\cdot uh^{-1})=u(ugu\cdot h^{-1})=u\cdot g^{-1}h^{-1}=hg\cdot u$. Finally, when g and $g^{-1}h$ are good, we derive $gu\cdot hu=ug^{-1}\cdot hu=u\cdot g^{-1}h\cdot u=h^{-1}g$. □

Thus (4.14) is equivalent to (4.8). Moreover, in order to prove Theorem 4.13, it suffices to show that every $g\in G$ is good.

Thanks to diassociativity, g^s (s positive integer) is good whenever g is. Since G is finite, g^{-1} is good whenever g is.

Lemma 4.15 *Assume that g, $h \in G$ are good. Then gh is good if and only if hg is.*

Proof. Because of the symmetry, it is enough to prove only one implication. Assume that hg is good. By Lemma 4.14, $g \cdot hu = hg \cdot u$. Using this identity, we obtain $g \cdot hu \cdot g = (hg \cdot u)g$, $gh \cdot ug = h \cdot gug = hu$, $gh = hu \cdot g^{-1}u = uh^{-1} \cdot g^{-1}u = u \cdot h^{-1}g^{-1} \cdot u$, and so $gh \cdot u = u \cdot h^{-1}g^{-1}$. □

Lemma 4.16 *Assume that g, $h \in G$ are good. Then so is ghg.*

Proof. Since g^{-1}, h are good, Lemma 4.14 yields $ug \cdot h = g^{-1}u \cdot h = g^{-1}h^{-1} \cdot u$. Then $u \cdot ghg \cdot u = (ug \cdot h)g \cdot u = (g^{-1}h^{-1} \cdot u)g \cdot u = g^{-1}h^{-1} \cdot ugu = g^{-1}h^{-1}g^{-1}$, and we are done. □

We continue by induction on the *complexity*, or *length*, if you will, of the elements of G, defined below.

For $\varepsilon = 1, -1$, let X_ε be the set of symbols $\{x_1^\varepsilon, \cdots, x_m^\varepsilon\}$, and write $X = X_1 \cup X_{-1}$. Every word w of the free group $F = \langle X \rangle$ can be written uniquely in the form $x_{i_1}^{\varepsilon_1} \cdots x_{i_r}^{\varepsilon_r}$, where $i_j \neq i_{j+1}$, and ε_j is a nonzero integer. Define the *complexity* of w as the ordered pair $c(w) = (r, \sum_{j=1}^r |\varepsilon_j|)$, and order the complexities lexicographically.

From now on, assume that G is two-generated, and write $x = x_1$, $y = x_2$.

Since $xu = ux^{-1}$ and $yu = uy^{-1}$ are presenting relations, both x, y are good, and hence both x^s, y^s are good for every integer s. The last presenting relation $xy \cdot u = u \cdot y^{-1}x^{-1}$ shows that both xy and $y^{-1}x^{-1} = (xy)^{-1}$ are good. Then yx and $x^{-1}y^{-1} = (yx)^{-1}$ are good, by Lemma 4.15. Also, Lemma 4.16 implies that $x^{-1} \cdot xy \cdot x^{-1} = yx^{-1}$ is good. Then $x^{-1}y$, $xy^{-1} = (yx^{-1})^{-1}$ and $y^{-1}x = (x^{-1}y)^{-1}$ are good, by Lemma 4.15. This means that every $g \in G$ with $c(g) < (2, 3)$ is good.

Lemma 4.17 *Every $g \in G$ with $c(g) < (3, 0)$ is good.*

Proof. Suppose there is g that is not good, and let $c(g) = (r, s)$ be as small as possible. We can assume that $g = a^u b^v$, where $\{a, b\} = \{x, y\}$, $s = |u| + |v| > 2$, and $u \neq 0 \neq v$.

Either $|u| > 1$ or $|v| > 1$. Without loss of generality, $u > 1$. (By Lemma 4.15, we can assume that $|u| > 1$. When u is negative, consider the inverse $b^{-v}a^{-u}$ instead, and apply Lemma 4.15 again.) Since $c(a^{u-2}b^v) < (2, s)$, the element $a^{u-2}b^v$ is good, and so is $a^{u-1}b^v a = a \cdot a^{u-2}b^v \cdot a$. As $a^{u-1}b^v$ is good by the induction hypothesis, $a^u b^v a = a \cdot a^{u-1}b^v \cdot a$ is good as well, by Lemma 4.16. Then the decomposition of the good element $a^{u-1}b^v a$ into two good elements $a^{-1} \cdot a^u b^v a$ demonstrates that $a^u b^v a \cdot a^{-1} = a^u b^v$ is good, by Lemma 4.15. We have reached a contradiction. □

To finish the proof, assume there is $g \in G$ that is not good, and let $c(g) = (r, s)$ be as small as possible. By Lemma 4.17, $r \geq 3$. When r is odd, we can write $g = a^{\varepsilon_1}b^{\varepsilon_2}a^{\varepsilon_3} \cdots b^{\varepsilon_{r-1}}a^{\varepsilon_r} = khk$, where $k = a^{\varepsilon_r}$, $h = a^{\varepsilon_1 - \varepsilon_r}b^{\varepsilon_2}a^{\varepsilon_3} \cdots b^{\varepsilon_{r-1}}$, and $\{a, b\} = \{x, y\}$. Since $c(k)$, $c(h) < (r, s)$, both k, h are good, and then g is good by Lemma 4.16.

Assume that r is even. Then $g = a^{\varepsilon_1}b^{\varepsilon_2} \cdots a^{\varepsilon_{r-1}}b^{\varepsilon_r} = khk$, where $k = a^{\varepsilon_1}b^{\varepsilon_r}$, $h = b^{\varepsilon_2 - \varepsilon_r}a^{\varepsilon_3} \cdots b^{\varepsilon_{r-2}}a^{\varepsilon_{r-1} - \varepsilon_1}$. Again, $c(k)$, $c(h) < (r, s)$, thus both k and h are good, and so is g, by Lemma 4.16.

Theorem 4.13 is proved.

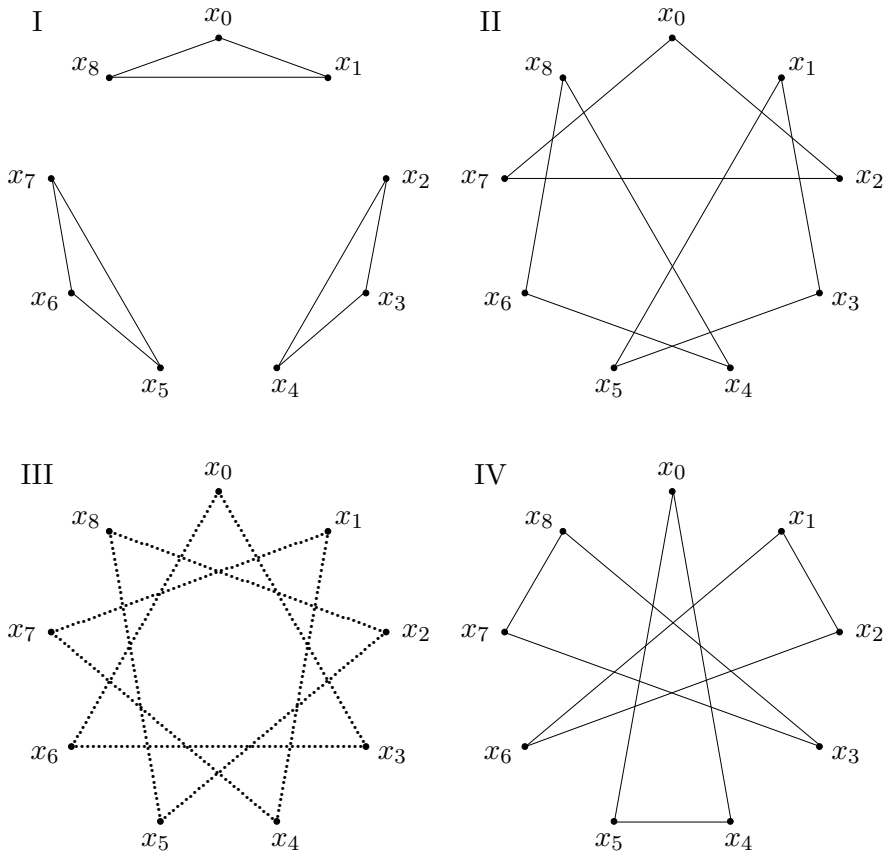

Figure 4.2: Multiplication in $M_{12}(S_3, 2)$

4.4 Visualization of the Smallest Moufang Loop

The multiplication formula (4.8) for $M = M_{12}(S_3, 2)$ is certainly difficult to memorize, and so is the one in [35, Example IV.1.2]. We present a visual description of M.

Note that there are 9 involutions and 2 elements of order 3 in M (cf. [9, Table 3], or Proposition 4.12). We are going to define a 12-element groupoid L and show that it is isomorphic to M.

Look at the four diagrams in Figure 4.2. Think of the vertices $x_0, \ldots, x_8$ as involutions. Let L consists of $e, x_0, \ldots, x_8, y, y^{-1}$, where y is of order 3. Interpret the edges of diagrams I–IV as multiplication rules in the following way. If x_i and x_j are connected by a solid line, let $x_i x_j$ be the third vertex of the (unique) triangle containing both x_i and x_j. If x_i and x_j are not connected by a solid line, we must have $j = i \pm 3$, and then x_i and x_j are connected by a dotted line (in diagram III). Define $x_i x_{i+3} = y$.

These visual rules translate into

$$x_i x_j = \begin{cases} e, & \text{if } i = j, \\ y^{\varepsilon}, & \text{if } j \equiv i + 3\varepsilon \pmod 3, \\ x_{2i-j}, & \text{if } i \equiv 0 \text{ and } i \not\equiv j \pmod 3, \\ x_{(i+j)/2}, & \text{otherwise.} \end{cases} \tag{4.15}$$

This partial multiplication can be extended by properties of Moufang loops. To avoid ambiguity, we postulate that $y^3 = e$, $x_i y = y^{-1} x_i = x_{i+3}$, $y x_i = x_i y^{-1} = x_{i-3}$.

Obviously, L is closed under multiplication and has a neutral element. It is non-associative, since $x_0 x_1 \cdot x_3 = x_8 x_3 = x_7 \neq x_4 = x_0 x_5 = x_0 \cdot x_1 x_3$. Is L isomorphic to M? There is a unique Moufang loop of order 12 [12], so it suffices to check the Moufang identities for L. However, this is not so easy! Instead, we verify directly that L satisfies the multiplication formula (4.8) with some choice of G and u. We suggest using Figure 4.2 rather than (4.15).

Remark 4.18 *It does not suffice to verify* (4.14) *for some choice of* G *and* u *because* (4.14) *is equivalent to* (4.8) *only when it is assumed that* L *is Moufang.*

Put $x = x_0$, and observe that $G = \langle x, y \rangle = \{e, x_0, y, x_3, x_6, y^{-1}\}$ is isomorphic to S_3. Let $u = x_1 \notin G$. We show that (4.10)–(4.13) are satisfied for every $g, h \in G$. Thanks to the symmetry of Figure 4.2, it is enough to consider only $\{g, h\} = \{x_0, x_3\}$, $\{x_0, y\}$.

Identity (4.10) is trivial. Let us prove (4.11). We have $x_0 x_1 \cdot x_3 = x_8 x_3 = x_7 = y x_1 = x_0 x_3^{-1} \cdot x_1$, $x_0 x_1 \cdot y = x_8 y = x_2 = x_6 x_1 = x_o y^{-1} \cdot x_1$, $x_3 x_1 \cdot x_0 = x_5 x_0 = x_4 = y^{-1} x_1 = x_3 x_0^{-1} \cdot x_1$, and $y x_1 \cdot x_0 = x_7 x_0 = x_2 = x_6 x_1 = y x_0^{-1} \cdot x_1$. Similarly for (4.12), (4.13).

Hence L is isomorphic to M. The subloop structure of L is apparent from the visual rules, too. If $j \equiv i + 3 \pmod 3$ then $\langle x_i, x_j \rangle \cong S_3$; otherwise, $\langle x_i, x_j \rangle \cong V_4$, for $i \neq j$.

Chapter 5

The Smallest Paige Loop $M^*(2)$

We have already discussed the importance of $M^*(2) = M^*$ for the real octonions. Most of our effort was originally motivated by this smallest Paige loop, and we have consequently obtained a much more detailed description of M^* than that of other Paige loops. It is therefore appropriate to devote an entire chapter to it.

We will completely describe the lattice of subloops of M^* in the following sense. We list all non-isomorphic subloops of M^*. Given an isomorphism type, we count the orbits of transitivity of the subloops of that type under the natural action of $\mathrm{Aut}(M^*)$. We pick a representative from each orbit. For every member of an orbit, we find an automorphism transforming that member into its orbit representative. For every representative, we enumerate all subloops containing it as a maximal subloop. For any two representatives A, B, we find the Hasse constants $\mathcal{H}_B(A)$ and $\mathcal{H}_{M^*}(A|B)$.

This provides us with a complete local description of the lattice, which can easily be expanded into a global view, especially with the aid of Figure 5.1. From our local description, it is easy to find all copies of B containing A, provided A is maximal in B. If A is not maximal, we have to proceed in several steps. The Hasse constant $\mathcal{H}_{M^*}(A|B)$ tells us when to stop.

The subloops of M^* are quite numerous (there are 1045 of them), so we will also have a look at some combinatorial structures built from their overlap. Our selection is somewhat arbitrary here, but, hopefully, representative.

5.1 Possible Subloops

O. Chein enumerated all Moufang loops of order at most 63 [10]. Since M^* has 120 elements, every proper subloop of M^* can be found in Chein's list. This is a consequence of the following simple Lemma:

Lemma 5.1 (Chein [10, Lemma 0]) *Let H be a subloop of a finite Moufang loop L, and let $u \in L$. If m is the smallest integer such that $u^m \in H$ then $|\langle H, u\rangle| \geq m|H|$.*

We say that a finite power associative loop L has the *weak Cauchy property* if L contains an element of order p for every prime p dividing $|L|$. A finite loop L has the

strong Cauchy property if every subloop of L has the weak Cauchy property.

Not every Moufang loop has the weak Cauchy property. Indeed, it is known that M^* does not, as it contains no element of order 5 (cf. Lemma 3.13). Small Moufang loops have the strong Cauchy property, however.

Theorem 5.2 (Chein [10, Ch. XIV]) *Every Moufang loop of order at most* 63 *has the weak Cauchy property. Thus, every Moufang loop of order at most* 63 *has the strong Cauchy property .*

This result allows us to narrow down the list of possible orders of subloops of M^*.

Corollary 5.3 *Let H be a proper subloop of M^*. Then $|H| = 2^r 3^s$ for some r, s.*

Proof. By Lemma 5.1, $|H| \leq |M^*|/2 = 60$, and so H has the weak Cauchy property, by Theorem 5.2. Since M^* consists of elements of order 1, 2, and 3, we are done. □

Following H. Pflugfelder [35, p. 12], a finite quasigroup Q is said to have the *weak Lagrange property* if $|H|$ divides $|Q|$ for every subquasigroup H of Q. A finite quasigroup Q has the *strong Lagrange property* if every subquasigroup of Q has the weak Lagrange property.

Whether finite Moufang loops satisfy the weak Lagrange property is an excellent open question. G. Glauberman proved [23] that finite Moufang loops of *odd* order have the strong Lagrange property. We proceed to show that M^* has it as well.

5.1.1 Strong Lagrange Property

By Corollary 5.3, a non-trivial subloop of M^* has order 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27, 32, 36, 48 or 54. Let us now focus on the possible orders of *subgroups* of M^*.

Lemma 5.4 *Let a, $b \in M^*$, $|a| = |b| = 3$, $b \notin \langle a \rangle$. Then $\langle a, b \rangle$ contains an involution.*

Proof. We may assume that

$$a = \begin{pmatrix} 1 & \alpha \\ \beta & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & \gamma \\ \delta & 0 \end{pmatrix},$$

for some α_1, α_2, β_1, $\beta_2 \in k^3$. Then

$$ab = \begin{pmatrix} 1 + \alpha \cdot \delta & - \\ - & \beta \cdot \gamma \end{pmatrix}, \quad a^2 b = \begin{pmatrix} \alpha \cdot \delta & - \\ - & \beta \cdot \gamma \end{pmatrix}.$$

By Lemma 3.8, one of ab, $a^2 b$ is of order 3, and the other of order 2. □

We claim that there is no 9-element subgroup in M^*. Assume there is one. Then it is either a cyclic group, or a group of exponent 3. The former is impossible because M^* contains no element of order 9, the latter is impossible by Lemma 5.4.

Consequently, by Sylow Theorems, 9 does not divide the order of any subgroup of M^*.

Every group of order 24 contains an element of order at least 4. This is clearly true for abelian groups. For a contradiction, assume that G is a non-abelian group of order 24 consisting of elements of order 1, 2, 3. Then all Sylow 2-subgroups of G are necessarily isomorphic to $(C_2)^3$. Thus, using [10, Table 1], $G \cong D_6 \times C_2$ or $G \cong A_4 \times C_2$, where D_6 is the 12-element dihedral group, and A_4 the alternating group on 4 points. A contradiction!

Assume that $G \leq M^*$ is a group of order 16. Since G has exponent 2, it is isomorphic to $(C_2)^4$. It is not obvious—at least not to the author—why M^* could not contain such a subgroup. Nevertheless, it does not, and we prove it in Section 5.3. Let us state this fact as a proposition.

Proposition 5.5 $\mathcal{H}_{M^*}((C_2)^4) = 0$.

Since every group of order $32 = 2 \cdot 16$ or $48 = 3 \cdot 16$ contains a subgroup of order 16, there are no subgroups of these orders in M^*. Altogether, if G is a non-trivial subgroup of M^*, it has order 2, 3, 4, 6, 8 or 12. The groups of these orders containing no element of order greater than 3 are: C_2, C_3, V_4, S_3, $(C_2)^3 = E_8$, and A_4. Only two of these groups are non-abelian, namely S_3 and A_4.

O. Chein concludes in [10, Ch. XIII] that every non-associative Moufang loop of order at most 63 which contains no element of order greater than 3 is necessarily of the form $M_{2n}(G, 2)$ for some non-abelian group G. Since $G \leq M_{2n}(G, 2)$, we can possibly find only two non-associative proper subloops in M^*, namely $M_{12}(S_3, 2)$ and $M_{24}(A_4, 2)$. Let us write Mo_{12} and Mo_{24} for $M_{12}(S_3, 2)$, $M_{24}(A_4, 2)$, respectively. (For obvious reasons, we prefer this notation to M_{12}, M_{24}.)

Summarizing our discussion, if H is a non-trivial subloop of M^*, it is isomorphic to

$$C_2,\ C_3,\ V_4,\ S_3,\ E_8,\ A_4,\ Mo_{12},\ Mo_{24}. \tag{5.1}$$

In particular, M^* has the strong Lagrange property.

Proposition 5.6 *M^* satisfies the strong Lagrange property.*

Let us remind the reader that we still have to prove Proposition 5.5. All subloops listed in (5.1) indeed appear as subloops of M^*, as wee shall see in a moment.

5.2 Orbits of Transitivity, Representatives, and Hasse Constants

The detailed discussion of M^* starts here. We consider all possible isomorphism types of subloops of M^*, as found in (5.1). For every isomorphism type H, we investigate the action of $\mathrm{Aut}(M^*)$ on the copies of H, count the orbits of transitivity, pick a representative from each orbit, and calculate the related Hasse constants.

5.2.1 Subloops Isomorphic to C_2

By Lemma 3.8, every involution $x \in M^*$ is of the form

$$\begin{pmatrix} n & \alpha \\ \beta & n \end{pmatrix}$$

for some $n \in \{0, 1\}$, $\alpha, \beta \in k^3$. In order to linearize our notation, we write $x = (\!(\alpha, \beta)\!)$ when the value of n is clear from α, β or when it is not important, and $x = (\!(\alpha, \beta)\!)_n$ otherwise.

Every element $x \in M^*$ of order 3 is of the form

$$\begin{pmatrix} n & \alpha \\ \beta & 1+n \end{pmatrix}$$

for some $n \in \{0, 1\}$, $\alpha, \beta \in k^3$. This time, we write $x = (\!(\!(\alpha, \beta)\!)\!)_n$.

Also, we will sometimes leave out commas and parentheses when writing down vectors. Thus, both 101 and (101) stand for (1, 0, 1).

Proposition 5.7 *Let $x = (\!(\alpha, \beta)\!)_n$, $y = (\!(\gamma, \delta)\!)_m$ be two involutions, $x \neq y$, and $z = (\!(\!(\varepsilon, \varphi)\!)\!)_l$ an element of order 3 in M^*. Then:*

(i) *$[x, y] = e$ if and only if $|xy| = 2$ if and only if $\langle x, y\rangle \cong V_4$ if and only if $\alpha\cdot\delta = \beta\cdot\gamma$.*

(ii) *$[x, y] \neq e$ if and only if $|xy| = 3$ if and only if $\langle x, y\rangle \cong S_3$ if and only if $\alpha\cdot\delta \neq \beta\cdot\gamma$.*

(iii) *x is contained in a copy of S_3 ,*

(iv) *every copy of S_3 contains an involution of the form $(\!(\ ,\ )\!)_0$,*

(v) *$|zx| = 2$ if and only if $\alpha\cdot\varphi + \beta\cdot\varepsilon = n$.*

Proof. The involution x commutes with y if and only if $|xy| = 2$. Since

$$xy = \begin{pmatrix} nm + \alpha\cdot\delta & - \\ - & nm + \beta\cdot\gamma \end{pmatrix},$$

parts (i) and (ii) follow.

Given $x = (\!(\alpha, \beta)\!)_n$, pick $\delta \in \alpha^\perp$, $\gamma \notin \beta^\perp$, and choose $m \in \{0, 1\}$ so that $y = (\!(\gamma, \delta)\!)_m \in M^*$. Then $\langle x, y\rangle \cong S_3$, and (iii) is proved.

Let $G \leq M^*$, $G \cong S_3$, and suppose that $x = (\!(\alpha, \beta)\!)_1$, $y = (\!(\gamma, \delta)\!)_1 \in G$, $x \neq y$. Then

$$xy = \begin{pmatrix} 1 + \alpha\cdot\delta & \alpha + \gamma + \beta\times\delta \\ \beta + \delta + \alpha\times\gamma & 1 + \beta\cdot\gamma \end{pmatrix}.$$

Since $|xy| = 3$, we have $\alpha\cdot\delta \neq \beta\cdot\gamma$. In other words, $\alpha\cdot\delta + \beta\cdot\gamma = 1$. Then the third involution $xyx \in G$ equals

$$\begin{pmatrix} 1 + \alpha\cdot\delta + (\alpha+\gamma)\cdot\beta & - \\ - & - \end{pmatrix} = \begin{pmatrix} \alpha\cdot\beta & - \\ - & - \end{pmatrix}.$$

Now, $\alpha \cdot \beta = 0$ since $\det x = 1$, and we are done with (iv).

Let us prove (v). If $l = 1$, the diagonal entries of zx are $n+\varepsilon\cdot\beta$ and $\varphi\cdot\alpha$, respectively. Thus $|zx| = 2$ if and only if $\alpha \cdot \varphi + \beta \cdot \varepsilon = n$. Similarly for $l = 0$. □

We are going to show that $\mathrm{Aut}(M^*)$ acts transitively on the copies of C_2. As in Subsection 3.3.3, we let

$$x_0 = (\!(111,\, 111)\!)$$

be the canonical involution.

Lemma 5.8 *Let x, $y \in M^*$ be two involutions such that $\langle x, y\rangle = S_3$. Then $T(yx)$ is an automorphism of M^*, and $xT(yx) = y$.*

Proof. Since $|yx| = 3$, $T(yx) \in \mathrm{Aut}(M^*)$, by [35, Theorem IV.1.6]. Also, $xT(yx) = xyxyx = y$. □

The proof of Proposition 5.9 is illustrative and will be imitated many times.

Proposition 5.9 *The group $\mathrm{Aut}(M^*)$ acts transitively on the 63 copies of C_2 in M^*.*

Proof. Whatever α, $\beta \in k^3$ are, exactly one of $(\!(\alpha, \beta)\!)_0$, $(\!(\alpha, \beta)\!)_1$ is an element of M^*, unless both α and β are zero vectors. Thus, $\mathcal{H}_{M^*}(C_2) = 63$.

Let $x = (\!(\alpha, \beta)\!)_n$ be an involution. We describe how to transform x into x_0. By Proposition 5.7(iii), x is contained in a copy of S_3. By Lemma 5.8 and Proposition 5.7(iv), we may assume that $n = 0$.

Let $r = \mathrm{w}(\alpha)$, $s = \mathrm{w}(\beta)$. Using the automorphism ∂ from Lemma 3.17, we can assume that $r \geq s$. We now transform x into x' so that $x' = x_0$, or $x' = x^*$, or $\langle x', x_0\rangle \cong S_3$,or $\langle x', x^*\rangle \cong S_3$, where $x^* = (\!(100,\, 100)\!)$.

If $r \not\equiv s \pmod 2$, then $\langle x, x_0\rangle \cong S_3$. So assume that $r \equiv s$. The following trick will be used throughout the chapter. Every permutation of coordinates can be made into an automorphism of M^*, by Lemma 3.16. The involution x_0 is invariant under all permutations. Since $n = 0$, we must have $s > 0$, and thus $(r, s) = (2, 2)$, $(1, 1)$, $(3, 1)$, or $(3, 3)$. If $(r, s) = (2, 2)$, transform x into $x' = (\!(110,\, 011)\!)$, and note that $\langle x', x^*\rangle \cong S_3$, by Proposition 5.7. If $(r, s) = (1, 1)$, transform x into $x' = x^*$. If $(r, s) = (3, 1)$, transform x into $x' = (\!(111,\, 001)\!)$. Once again, $\langle x', x^*\rangle \cong S_3$. Finally, if $(r, s) = (3, 3)$, we have $x = x' = x_0$.

Now, when $\langle x', x_0\rangle \cong S_3$ or $\langle x', x^*\rangle \cong S_3$, we can permute the involutions so that x' is transformed into x_0 or x^*, using Lemma 5.8.

It remains to show how to transform x^* into x_0. For that matter, consider the element $y = (\!(\!(\!(001,\, 101)\!)\!)\!)_1$, and check that $x_0 = x^*T(y)$. □

Note that the proof of Proposition 5.9 gives a practical way of constructing an automorphism mapping one involution of M^* onto another (also see Appendix A).

Example 5.10 *Let us construct an automorphism f mapping $x = (\!(100,\, 111)\!)$ onto $z = (\!(101,\, 010)\!)$. It suffices to find g, $h \in \mathrm{Aut}(M^*)$ such that $g(x) = x_0$ and $h(z) = x_0$. Then $f = h^{-1}g$.*

The element x has zeros on the diagonal, and satisfies $r = 1$, $s = 3$, $r \equiv s$, $r \leq s$. Thus we look at $\partial(x)$ instead. Following the proof, $\widehat{\pi}(\partial(x)) = x' = (\!(111, 001)\!)$, where π is the transposition $(1, 3)$. Then $\langle x', x^* \rangle \cong S_3$, and $x'T(x^*x') = x^*$. Finally, $x_0 = x^*T(y)$. Altogether, $f = T(y) \circ T(x^*x') \circ (1, 3) \circ \partial$, where we compose from right to left. (We have purposely selected x to be as unpleasant as possible, given the proof of Proposition 5.9.)

Now for h. The element z has ones on the diagonal. Luckily, $\langle x_0, z \rangle \cong S_3$, thus $h = T(x_0 z)$ does the job.

Select $\langle x_0 \rangle$ for the representative among all subloops of M^* isomorphic to C_2.

5.2.2 Subloops Isomorphic to C_3 or S_3

Let

$$y_0 = (\!(\!(011, 110)\!)\!)_1$$

be the canonical element of order 3. We show that $\mathrm{Aut}(M^*)$ acts transitively on the copies of S_3. Since $\mathcal{H}_{S_3}(C_3) = 1$, this will imply that $\mathrm{Aut}(M^*)$ acts transitively on the copies of C_3, too.

Let us first state a technical result.

Lemma 5.11 *Let $v_1 = (\!(\!(010, 110)\!)\!)_0$, $v_2 = (\!(\!(001, 101)\!)\!)_0$. Then both $f_1 : a \mapsto v_2(v_1^{-1}av_1)v_2^{-1}$, $f_2 : a \mapsto v_1(v_2^{-1}av_2)v_1^{-1}$ are automorphisms of M^* fixing x_0.*

Proof. Recall the equivalence $\sim$ for elements of order 3 defined in Subsection 3.3.3. By Proposition 3.19, $v_1 \sim \partial(v_1)$. By Lemma 3.20, $v_1 \sim \widehat{\pi}(v_1)$, where π is the transposition interchanging 2 and 3. In other words, $v_1 \sim v_2$, or $x_0T(v_1) = x_0T(v_2)$. □

Proposition 5.12 *The group $\mathrm{Aut}(M^*)$ acts transitively on the copies of S_3.*

Proof. Let $G \cong S_3$, $G = \langle u, v \rangle$, where $|u| = |v| = 2$. By Proposition 5.9, we can assume that $u = x_0$. Let $v = (\!(\alpha, \beta)\!)_n$, $r = \mathrm{w}(\alpha)$, $s = \mathrm{w}(\beta)$. By Proposition 5.7(ii), we must have $r \not\equiv s \pmod 2$. The automorphism ∂ fixes x_0, and we may thus assume that $r > s$. We will show that v can be transformed into $x_1 = (\!(110, 100)\!)$ without moving x_0.

When $n = 1$, we have $\alpha \cdot \beta = 0$. Taking the permutations of coordinates into account, we may transform v into $x_2 = (\!(010, 000)\!)$ (if $(r, s) = (1, 0)$), $x_3 = (\!(011, 100)\!)$ (if $(r, s) = (2, 1)$), $x_4 = (\!(111, 000)\!)$ (if $(r, s) = (3, 0)$) or $x_5 = (\!(111, 101)\!)$ (if $(r, s) = (3, 2)$). Let f_1, f_2 be as in Lemma 5.11. Check that the involutions $f_1(x_2)$, $f_2(x_3)$, $f_1(x_4)$, and $f_2(x_5)$ are of the form $(\!(\ ,\ )\!)_0$. We may hence assume that $n = 0$.

When $n = 0$, then $s \geq 1$, else $\det v = 0$. This leaves us with $(r, s) = (2, 1)$ or $(3, 2)$. In fact, $(r, s) = (3, 2)$ leads to $\det v = 0$, too. So $(r, s) = (2, 1)$, and we can permute the coordinates of v so that v transforms into x_1. □

In the following lemma, we will see the power of local analysis once again. Also note that we take advantage of Proposition 4.2 for the first time.

Lemma 5.13

$$\begin{array}{lll} \mathcal{H}_{M^*}(C_3) = 28, & \mathcal{H}_{S_3}(C_2) = 3, & \mathcal{H}_{M^*}(C_2|S_3) = 16, \\ \mathcal{H}_{M^*}(S_3) = 336, & \mathcal{H}_{S_3}(C_3) = 1, & \mathcal{H}_{M^*}(C_3|S_3) = 12. \end{array}$$

Proof. By Proposition 5.9, $\mathcal{H}_{M^*}(C_3) = (119 - \mathcal{H}_{M^*}(C_2))/2 = 28$.

Let x be an involution. By Proposition 5.9, the number of involutions y such that $|xy| = 3$ is independent of x. Pick $x = (\!(100, 100)\!)$, and let $\alpha = (\alpha_1, \alpha_2, \alpha_3)$, $\beta = (\beta_1, \beta_2, \beta_3)$, $y = (\!(\alpha, \beta)\!)$. Then $|xy| = 3$ if and only if $\alpha_1 \neq \beta_1$. Thus $(\alpha_1, \beta_1) = (0, 1)$ or $(1, 0)$. Whatever α_2, β_2, α_3, β_3 are, there is a unique n such that $(\!(\alpha, \beta)\!)_n$ is an involution. Therefore, there are 32 involutions y such that $|xy| = 3$. Since $\mathcal{H}_{S_3}(C_2) = 3$, we get $\mathcal{H}_{M^*}(C_2|S_3) = 16$. Then, by (4.3),

$$\mathcal{H}_{M^*}(S_3) = \frac{\mathcal{H}_{M^*}(C_2) \cdot \mathcal{H}_{M^*}(C_2|S_3)}{\mathcal{H}_{S_3}(C_2)} = \frac{63 \cdot 16}{3} = 336.$$

Again by (4.3),

$$\mathcal{H}_{M^*}(C_3|S_3) = \frac{\mathcal{H}_{S_3}(C_3) \cdot \mathcal{H}_{M^*}(S_3)}{\mathcal{H}_{M^*}(C_3)} = \frac{1 \cdot 336}{28} = 12,$$

and we are done. □

With

$$x_1 = (\!(110, 100)\!)$$

from Proposition 5.12, we get $x_0 x_1 = y_0$, justifying our choice of y_0 as the canonical element of order 3. It is reasonable to let $\langle y_0 \rangle$ be the representative for C_3, and $\langle x_0, x_1 \rangle = \langle x_0, y_0 \rangle$ the representative for S_3.

Going back to our promise from the beginning of this chapter, we should now find all copies of S_3 containing the representative $\langle x_0 \rangle$, and all copies of S_3 containing the representative $\langle y_0 \rangle$. Well, we will not list the copies explicitly, just as we did not list all automorphisms mapping a given involution onto x_0. However, the proof of Lemma 5.13 in fact enumerates all copies of S_3 containing the involution $x^* = (\!(100, 100)\!)$. It is easy to adopt the proof for x_0. Or, alternatively, use the automorphism mapping x^* onto x_0. The situation for $\langle y_0 \rangle$ is more complicated, because we have used one of the properties of Hasse constants to calculate $\mathcal{H}_{M^*}(C_3|S_3)$ without resorting to the local analysis. Nevertheless, it is easy to find the twelve copies of S_3 containing $\langle y_0 \rangle$; for instance, by using Proposition 5.7(v). *We will not comment on the local analysis anymore.*

5.2.3 Subloops Isomorphic to A_4

Perhaps it would be more natural to look at the copies of V_4 first, however, the Klein subgroups of M^* are exceptional in the sense that $\mathrm{Aut}(M^*)$ does not act transitively on them (cf. Subsection 5.2.6), rendering the situation less transparent.

Fix

$$z_0 = (((110,\ 100)))_0.$$

Observe that $\mathcal{H}_{A_4}(C_2) = 3$, $\mathcal{H}_{A_4}(C_3) = 4$.

Proposition 5.14 *The group* $\mathrm{Aut}(M^*)$ *acts transitively on the* 63 *copies of* A_4. *Moreover,* $\mathcal{H}_{M^*}(C_2|A_4) = 3$.

Proof. If $G \le M^*$ is isomorphic to C_3 and $u \in M^* \setminus G$ is an involution, then $\langle G,\ u\rangle \cong S_3$ or $\langle G,\ u\rangle \cong A_4$. Since $\mathcal{H}_{M^*}(C_3|S_3) = 12$ and $\mathcal{H}_{S_3}(C_2) = 3$, by Lemma 5.13, there are 36 involutions u in M^* such that $\langle G,\ u\rangle \cong S_3$. Thus, $\mathcal{H}_{M^*}(C_3|A_4) = (63-36)/\mathcal{H}_{A_4}(C_3) = 9$. By (4.3),

$$\mathcal{H}_{M^*}(A_4) = \frac{\mathcal{H}_{M^*}(C_3)\cdot \mathcal{H}_{M^*}(C_3|A_4)}{\mathcal{H}_{A_4}(C_3)} = \frac{28\cdot 9}{4} = 63.$$

Now for the transitivity. Let $G \cong A_4$, $G \le M^*$. By Proposition 5.9, we may assume that $G = \langle x_0,\ z\rangle$, where $|z| = 3$ (and, necessarily, $|x_0 z| = 3$). Let $z = (((\varepsilon,\ \varphi)))_l$, $r = \mathrm{w}(\varepsilon)$, $s = \mathrm{w}(\varphi)$. As $|x_0 z| = 3$, we have $r \not\equiv s$, by Proposition 5.7(v). Also, $r,\ s \ge 1$, else $\det z = 0$. Since $\partial(x_0) = x_0$, we may assume that $r > s$. Then $(r,\ s) = (2,\ 1)$ is the only possibility. Permuting the coordinates of z leaves us with $z_0 = (((110,\ 100)))_0$ or $(((110,\ 100)))_1$. The latter element is just the inverse of z_0. □

Let $\langle x_0,\ z_0\rangle$ be the representative for A_4.

5.2.4 Subloops Isomorphic to Mo_{12}

Table B.2 lists all involutions of M^*, and their relation to x_0. See the table for details.

As we have seen in Section 4.3, the loop Mo_{12} contains 3 copies of S_3 (corresponding to the three dotted triangles in diagram III of Figure 4.2. In symbols, $\mathcal{H}_{Mo_{12}}(S_3) = 3$. Since $\mathrm{Aut}(M^*)$ acts transitively on the copies of S_3, the constant $\mathcal{H}_{M^*}(Mo_{12})$ can be calculated from (4.5) once we know $\mathcal{H}_{M^*}(S_3|Mo_{12})$.

Let us have a look at the representative $G = \langle x_0,\ x_1\rangle \cong S_3$, where $x_0 = (\!(111,\ 111)\!)$, $x_1 = (\!(110,\ 100)\!)$. We want to find a subloop of M^* isomorphic to $M_{12}(G,\ 2)$ and containing G. Thus, we first need to find an involution $u \notin G$ such that $|x_0 u| = |x_1 u| = 2$. This is not a sufficient condition for $\langle G,\ u\rangle$ to be isomorphic to $M_{2n}(G,\ 2)$, but it is a necessary one. (Recall that all elements gu ($g \in G$) of $M_{2n}(G,\ 2)$ are of order 2, by Lemma 4.6(i).)

The only possible candidates for u are the following involutions:

$$\begin{array}{llll}
(\!(000,\ 110)\!)_1, & (\!(001,\ 001)\!)_0, & (\!(010,\ 001)\!)_1, & (\!(100,\ 010)\!)_1,\\
(\!(100,\ 100)\!)_0, & (\!(001,\ 111)\!)_0, & (\!(010,\ 111)\!)_0, & (\!(011,\ 000)\!)_1,\\
(\!(011,\ 110)\!)_0, & (\!(101,\ 011)\!)_0, & (\!(101,\ 101)\!)_1, & (\!(110,\ 011)\!)_1,\\
(\!(110,\ 101)\!)_0, & (\!(111,\ 010)\!)_0, & (\!(111,\ 100)\!)_0. &
\end{array} \tag{5.2}$$

This can be verified easily with the help of Table B.2 and Proposition 5.7(i). Moreover, $x_0 x_1 \cdot u = y_0 u$ must be an involution, too. This additional restriction reduces (5.2) into

$$\begin{array}{lll}
(\!(000,\ 110)\!)_1, & (\!(001,\ 111)\!)_0, & (\!(011,\ 000)\!)_1,\\
(\!(011,\ 110)\!)_0, & (\!(110,\ 011)\!)_0, & (\!(111,\ 100)\!)_0.
\end{array} \tag{5.3}$$

This can be seen with the help of Proposition 5.7(v), where $y_0 = (((011, 110)))_1$ is in place of z, and u is in place of x.

The coset Gu of G in $M_{12}(G, 2)$ consists of 6 involutions. Thus, if some u listed in (5.3) is such that $\langle G, u\rangle = M \cong Mo_{12}$, than there are additional 5 elements u' in (5.3) with $\langle G, u'\rangle = M$. Since there are 6 elements in (5.3), the number $\mathcal{H}_{M^*}(S_3|Mo_{12})$ is at most 1. We show that it is equal to one.

Let

$$u_0 = (\!(000, 110)\!).$$

Lemma 5.15 $\mathcal{H}_{M^*}(S_3|Mo_{12}) = 1$. *In particular,* $\mathrm{Aut}(M^*)$ *acts transitively on the* 112 *copies of* Mo_{12} *in* M^*.

Proof. Check that the presenting relations for Mo_{12} from Theorem 4.13 are satisfied with $x = x_0$, $y = x_1$, and $u = u_0$. This can be done quickly when you realize that $gu = ug^{-1}$ for $g \in G$ if and only if $|gu| = 2$. Hence $\langle G, u_0\rangle = M \cong Mo_{12}$. (The elements of $M \setminus G$ are listed in (5.3).) It follows from the above discussion that there are no more copies of Mo_{12} in M^* containing G, i.e., $\mathcal{H}_{M^*}(S_3|Mo_{12}) = 1$. By Proposition 4.2,

$$\mathcal{H}_{M^*}(Mo_{12}) = \frac{\mathcal{H}_{M^*}(S_3) \cdot \mathcal{H}_{M^*}(S_3|Mo_{12})}{\mathcal{H}_{Mo_{12}}(S_3)} = \frac{336 \cdot 1}{3} = 112.$$

Let M, M' be two copies of Mo_{12} in M^*. Let G (respectively G') be any subgroup of M (respectively M') isomorphic to S_3. By Proposition 5.12, there is $f \in \mathrm{Aut}(M^*)$ mapping G onto G'. As $\mathcal{H}_{M^*}(S_3|Mo_{12}) = 1$, f must map M onto M'. □

Let $\langle x_0, x_1, u_0\rangle = \langle x_0, y_0, u_0\rangle$ be the representative for Mo_{12}.

5.2.5 Subloops Isomorphic to Mo_{24}

Thanks to Proposition 4.12(v) we know that $\mathcal{H}_{Mo_{24}}(A_4) = 1$. We can calculate $\mathcal{H}_{M^*}(Mo_{24})$ as soon as we obtain $\mathcal{H}_{M^*}(A_4|Mo_{24})$.

For this matter, let $G = \langle x_0, z_0\rangle \cong A_4$, where $z_0 = (((110, 100)))_0$ is as in Proposition 5.14. We are trying to find an involution u such that $\langle G, u\rangle \cong Mo_{24}$. If there is such u, we must have $|x_0u| = |x'u| = 2$, where $x' = z_0^{-1}x_0z_0 = (\!(101, 101)\!)$. The third involution of G is $x_0x' = (\!(010, 010)\!)$, Using Table B.2 and Proposition 5.7, we find that there are only 12 involutions $u \neq x_0x'$ such that $|x_0u| = |x'u| = 2$. Namely, u is one of

$$\begin{array}{llll} (\!(000, 101)\!), & (\!(001, 001)\!), & (\!(001, 100)\!), & (\!(100, 001)\!), \\ (\!(100, 100)\!), & (\!(010, 111)\!), & (\!(101, 000)\!), & (\!(011, 011)\!), \\ (\!(011, 110)\!), & (\!(110, 011)\!), & (\!(110, 110)\!), & (\!(111, 010)\!). \end{array} \tag{5.4}$$

Since Mo_{24} contains 12 involutions not contained in A_4, we have just shown that the Hasse constant $\mathcal{H}_{M^*}(A_4|M_{12}(A_4, 2))$ is at most 1.

Let

$$u_1 = (\!(001, 001)\!).$$

Lemma 5.16 *$\mathcal{H}_{M^*}(A_4|Mo_{24}) = 1$, and $\mathrm{Aut}(M^*)$ acts transitively on the 63 copies of Mo_{24} in M^*.*

Proof. We are going to check that $x = x_0$, $y = z_0$, $u = u_1$ satisfy the presenting relations for Mo_{24}, as found in Theorem 4.13. It follows from our choice of u that $|xu| = 2$, and we can see easily that $|yu| = 2$. Now, $xy = (((100, 110)))_1$, and therefore $|xy \cdot u| = 2$, too. Hence $\langle x_0, z_0, u_1\rangle \cong Mo_{24}$, and $\mathcal{H}_{M^*}(A_4|Mo_{24}) = 1$ follows. (The 12 elements of $\langle x_0, z_0, u_1\rangle \setminus \langle x_0, z_0\rangle$ are listed in (5.4).) By (4.5),

$$\mathcal{H}_{M^*}(Mo_{24}) = \frac{\mathcal{H}_{M^*}(A_4) \cdot \mathcal{H}_{M^*}(A_4|Mo_{24})}{\mathcal{H}_{Mo_{24}}(A_4)} = \frac{63 \cdot 1}{1} = 63.$$

Under these circumstances, since $\mathrm{Aut}(M^*)$ acts transitively on the copies of A_4, it also acts transitively on the copies of Mo_{24}. □

Let us calculate a few more Hasse constants.

Lemma 5.17

$$\begin{array}{rclrcl}
\mathcal{H}_{A_4}(C_2) &=& 3, & \mathcal{H}_{M^*}(C_2|A_4) &=& 3,\\
\mathcal{H}_{Mo_{24}}(S_3) &=& 16, & \mathcal{H}_{M^*}(S_3|Mo_{24}) &=& 3,\\
\mathcal{H}_{Mo_{24}}(C_3) &=& 4, & \mathcal{H}_{M^*}(C_3|Mo_{24}) &=& 14,\\
\mathcal{H}_{Mo_{12}}(C_2) &=& 9, & \mathcal{H}_{M^*}(C_2|Mo_{12}) &=& 18,\\
\mathcal{H}_{Mo_{24}}(C_2) &=& 15, & \mathcal{H}_{M^*}(C_2|Mo_{24}) &=& 15,\\
\mathcal{H}_{Mo_{12}}(C_3) &=& 1, & \mathcal{H}_{M^*}(C_3|Mo_{12}) &=& 4.
\end{array}$$

Proof. We have used the equality $\mathcal{H}_{A_4}(C_2) = 3$ many times. $\mathcal{H}_{M^*}(C_2|A_4) = 3$ then follows from (4.5).

Assume that $L \cong S_3$ is a subloop of Mo_{24}. Since $L \not\leq A_4$, we have $|L \cap A_4| = |L \cap A_4u| = 3$, by Proposition 4.5. Thus, every subloop of Mo_{24} isomorphic to S_3 is of the form $\langle g, xu\rangle$, for some g, $x \in A_4$, $|g| = 3$. Each such subgroup can be written in 6 distinct ways as $\langle h, yu\rangle$, where h, $y \in A_4$, $|h| = 3$. Since $\mathcal{H}_{A_4}(C_3) = 4$, we have $\mathcal{H}_{Mo_{24}}(S_3) = 2 \cdot 4 \cdot 12/6 = 16$. Consequently,

$$\mathcal{H}_{M^*}(S_3|Mo_{24}) = \frac{\mathcal{H}_{Mo_{24}}(S_3) \cdot \mathcal{H}_{M^*}(Mo_{24})}{\mathcal{H}_{M^*}(S_3)} = \frac{16 \cdot 63}{336} = 3.$$

By Proposition 4.12(iii), $\mathcal{H}_{Mo_{24}}(C_3) = \mathcal{H}_{A_4}(C_3) = 4$. Therefore, by (4.5), $\mathcal{H}_{M^*}(C_3|Mo_{24}) = 63 \cdot 8/28 = 14$. The remaining six Hasse constants can be calculated in a similar way. Notice that $\mathcal{H}_{Mo_{24}}(C_2) = 15$ follows from Proposition 4.12(i). □

Let $\langle x_0, z_0, u_1\rangle$ be the representative for Mo_{24}.

5.2.6 Subloops Isomorphic to V_4

As announced earlier, we prove that $\mathrm{Aut}(M^*)$ does not act transitively on the copies of V_4. Let us first show that there are at most two orbits of transitivity.

Put

$$u_2 = (\!(100,\, 010)\!).$$

Lemma 5.18 *Let $V_4 \cong \langle u, v\rangle$ be one of the 315 copies of V_4 in M^*. Then there is $f \in \mathrm{Aut}(M^*)$ such that $f(u) = x_0$ and $f(v)$ is one of the two elements u_1, u_2.*

Proof. Recall that $\mathcal{H}_{M^*}(C_2|S_3) = 16$. Therefore, given any involution x, there are $63-1-2\cdot 16 = 30$ involutions y such that $\langle x, y\rangle \cong V_4$. Hence, $\mathcal{H}_{M^*}(V_4) = (63\cdot 30)/(2\cdot 3) = 315$.

By Proposition 5.9, we may assume that $u = x_0$. Write $v = (\!(\alpha, \beta)\!)_n$, $r = \mathrm{w}(\alpha)$, $s = \mathrm{w}(\beta)$. We have $r \equiv s$. Thanks to the automorphism ∂, we may assume that $r \le s$. If $(r, s) = (0, 2)$, transform v into u_0; if $(r, s) = (1, 1)$, into u_1 or u_2, depending on n; if $(r, s) = (1, 3)$, into $u_3 = (\!(001, 111)\!)$; if $(r, s) = (2, 2)$, into $u_4 = (\!(110, 110)\!)$ or $u_5 = (\!(011, 101)\!)$.

Recall the automorphisms f_1, f_2 from Lemma 5.11. Check that $f_1(u_4) = u_1$, and that $f_1(u_3) = u_2$, $f_1(u_5) = u_3$, $f_2(u_5) = \partial(u_0)$. Thus u_4 an be transformed into u_1, and each of u_0, u_3, u_5 can be transformed into u_2. □

Assume, for a while, that $\mathrm{Aut}(M^*)$ acts transitively on the 315 copies of V_4. Then, by (4.5),

$$\mathcal{H}_{M^*}(V_4|A_4) = \frac{\mathcal{H}_{A_4}(V_4)\cdot \mathcal{H}_{M^*}(A_4)}{\mathcal{H}_{M^*}(V_4)} = \frac{1\cdot 63}{315},$$

a contradiction. Hence, by Lemma 5.18, there are 2 orbits of transitivity, with representatives

$$V_4^+ = \langle x_0, u_1\rangle, \quad V_4^- = \langle x_0, u_2\rangle.$$

The proof of Lemma 5.18 also tells us which copies of V_4 belong to $O_{V_4^+}$ and which to $O_{V_4^-}$. In particular, all elements y with $\langle x_0, y\rangle \in O_{V_4^+}$ are denoted by an asterisk in Table B.2.

Lemma 5.19 $\mathcal{H}^O_{M^*}(C_2|V_4^+) = 3$, $\mathcal{H}^O_{M^*}(C_2|V_4^-) = 12$, $|O_{V_4^+}| = 63$, $|O_{V_4^-}| = 252$. *A copy of V_4 is contained in some copy of A_4 if and only if it belongs to $O_{V_4^+}$. More precisely, $\mathcal{H}_{M^*}(V_4^+|A_4) = 1$, $\mathcal{H}_{M^*}(V_4^-|A_4) = 0$.*

Proof. Since $\mathcal{H}_{V_4}(C_2) = 3$ and since there are 6 elements y such that $\langle x_0, y\rangle \in O_{V_4^+}$ (cf. Table B.2), we have $\mathcal{H}^O_{M^*}(C_2|V_4^+) = 6/2 = 3$. Then $\mathcal{H}^O_{M^*}(C_2|V_4^-)$ must be equal to $(30-6)/2 = 12$ (this corresponds to the remaining 24 involutions in set S_2 of Table B.2). By (4.4),

$$\begin{aligned} |O_{V_4^+}| &= \frac{\mathcal{H}_{M^*}(C_2)\cdot \mathcal{H}^O_{M^*}(C_2|V_4^+)}{\mathcal{H}_{V_4}(C_2)} = \frac{63\cdot 3}{3} = 63, \\ |O_{V_4^-}| &= \frac{\mathcal{H}_{M^*}(C_2)\cdot \mathcal{H}^O_{M^*}(C_2|V_4^-)}{\mathcal{H}_{V_4}(C_2)} = \frac{63\cdot 12}{3} = 252. \end{aligned}$$

By (4.2),

$$\begin{aligned} 63 &= \mathcal{H}_{A_4}(V_4)\cdot\mathcal{H}_{M^*}(A_4) = |O_{V_4^+}|\cdot\mathcal{H}_{M^*}(V_4^+|A_4) + |O_{V_4^-}|\cdot\mathcal{H}_{M^*}(V_4^-|A_4) \\ &= 63\cdot\mathcal{H}_{M^*}(V_4^+|A_4) + 252\cdot\mathcal{H}_{M^*}(V_4^-|A_4). \end{aligned}$$

This is only possible when $\mathcal{H}_{M^*}(V_4^+|A_4) = 1$, $\mathcal{H}_{M^*}(V_4^-|A_4) = 0$. □

Lemma 5.20 *$\mathcal{H}_{M^*}(V_4^+|Mo_{12}) = 0$, $\mathcal{H}_{M^*}(V_4^-|Mo_{12}) = 4$.*

Proof. Consider $V_4^+ = \langle x_0, u_1\rangle$. Assume that there is $G \cong S_3$ such that $V_4^+ \le M_{12}(G, 2) = M$. How can the three involutions x_0, u_1, $x_0u_1 = (\!(110, 110)\!)$ of V_4^+ be distributed in the cosets G, Gu of $M_{12}(G, 2)$? Certainly, $V_4^+ \not\le G$. Thus, by Proposition 4.5, exactly one involution must be in G (say g_0), and the remaining two are in Gu (say g_1, g_2).

There is an involution $y \in G$ such that $\langle y, g_0\rangle = G$. Because $G \cong S_3$, we have $|yg_0| = 3$. Also, $|yg_1| = |yg_2| = 2$, by Proposition 4.12(i). We argue that this is impossible.

Write $g_i = (\!(\gamma_i, \gamma_i)\!)$ for appropriate vectors $\gamma_i \in k^3$, $i = 0, 1, 2$, and let $y = (\!(\alpha, \beta)\!)$. Note that, remarkably, $\gamma_0 + \gamma_1 + \gamma_2 = 0$. Since $|yg_0| = 3$, $|yg_1| = |yg_2| = 2$, we have $\alpha\cdot\gamma_0 \ne \beta\cdot\gamma_0$, $\alpha\cdot\gamma_1 = \beta\cdot\gamma_1$, $\alpha\cdot\gamma_2 = \beta\cdot\gamma_2$. Then $0 = \alpha\cdot 0 = \alpha\cdot(\gamma_0+\gamma_1+\gamma_2) \ne \beta\cdot(\gamma_0+\gamma_1+\gamma_2) = \beta\cdot 0 = 0$, a contradiction.

The inevitable conclusion is that V_4^+ is not contained in any copy of Mo_{12}, i.e., $\mathcal{H}_{M^*}(V_4^+|Mo_{12}) = 0$. We proceed to calculate $\mathcal{H}_{M^*}(V_4^-|Mo_{12})$. First observe that Proposition 4.12(iii) implies that $\mathcal{H}_{Mo_{12}}(V_4) = 9$. (We knew it already from Figure 4.2.) We use the same trick as in Lemma 5.19. By (4.3), we have

$$\begin{aligned} 9\cdot 112 &= \mathcal{H}_{Mo_{12}}(V_4)\cdot\mathcal{H}_{M^*}(Mo_{12}) \\ &= |O_{V_4^+}|\cdot\mathcal{H}_{M^*}(V_4^+|Mo_{12}) + |O_{V_4^-}|\cdot\mathcal{H}_{M^*}(V_4^-|Mo_{12}) \\ &= 63\cdot 0 + 252\cdot\mathcal{H}_{M^*}(V_4^-|Mo_{12}). \end{aligned}$$

Hence $\mathcal{H}_{M^*}(V_4^-|Mo_{12}) = 4$. □

We are going to calculate the Hasse constants

$$c^+ = \mathcal{H}_{M^*}(V_4^+|Mo_{24}),\quad c^- = \mathcal{H}_{M^*}(V_4^-|Mo_{24}).$$

The argument is both subtle and detailed, and deserves a careful thought.

Lemma 5.21 *With the above notation for c^+, c^-, we have*

(i) $(c^+, c^-) \in \{(3, 4), (7, 3), (11, 2), (15, 1), (19, 0)\}$,

(ii) $c^+ \le 7$,

(iii) $c^- \le 3$.

Proof. Since $\mathcal{H}_{A_4}(C_2) = 3$ and $\mathcal{H}_{A_4}(V_4) = 1$, we have $\mathcal{H}_{Mo_{24}}(V_4) = 19$, by Proposition 4.12(vi). Formula (4.3) then yields

$$\begin{aligned} 19 \cdot 63 &= \mathcal{H}_{Mo_{24}}(V_4) \cdot \mathcal{H}_{M^*}(Mo_{24}) = |O_{V_4^+}| \cdot c^+ + |O_{V_4^-}| \cdot c^- \\ &= 63c^+ + 252c^- = (c^+ + 4c^-) \cdot 63. \end{aligned}$$

In particular, $c^+ + 4c^- = 19$, and (i) follows.

Let $V_4^+ = \langle x_0, u_1 \rangle$. We are trying to find a group $G \cong A_4$ such that $V_4^+ \leq M_{24}(G, 2)$. We look again at the distribution of the 3 involutions x_0, u_1, x_0u_1 in the cosets G, Gu. There are two possibilities; either $V_4^+ \leq G$, or $|V_4^+ \cap G| = 2$.

Suppose that $V_4^+ \leq G$. As $\mathcal{H}_{A_4}(V_4) = 1$ and $\mathcal{H}_{Mo_{24}}(A_4) = 1$, there is at most one subloop $M \cong Mo_{24}$ such that $V_4^+ \leq M$ in such a case.

Now suppose that $|V_4^+ \cap G| = 2$. Then $V_4^+ \cap G$ is one of the three 2-element subgroups of V_4^+. Let us call it H. Since $\mathcal{H}_{A_4}(C_2) = 3$ and $\mathcal{H}_{Mo_{24}}(A_4) = 1$, there are at most 3 subloops $M \cong M_{24}(G, 2)$ such that $H \leq G \leq M$. Because there are three ways how to choose H in V_4^+, there are at most $3 \cdot 3 = 9$ subloops $M \cong Mo_{24}$ such that $V_4^+ \leq M$.

Altogether, $c^+ \leq 1 + 9 = 10$. By (i), $c^+ \leq 7$, and (ii) is finished,

Let $V_4^- = \langle x_0, u_2 \rangle$. We are trying to find a group $G \cong A_4$ such that $V_4^- \leq M_{24}(G, 2)$. Since $\mathcal{H}_{M^*}(V_4^- | Mo_{24}) = 0$, the group V_4^- is not contained in G, i.e., $|V_4^- \cap G| = 2$. Using the transitivity of $\mathrm{Aut}(M^*)$ on involutions, we can assume that $V_4^- \cap G = \{e, x_0\}$. If there is such a group G, there is also an element

$$y = \begin{pmatrix} c_0 & (\gamma_1, \gamma_2, \gamma_3) \\ (\delta_1, \delta_2, \delta_3) & c_0 + 1 \end{pmatrix}$$

such that

$$|yg_0| = 3, \, |yg_1| = 2, \, |yg_2| = 2. \tag{5.5}$$

(Since we can assume that $\langle x_0, y \rangle = G \cong A_4$.) By Proposition 5.7, the system of equations (5.5) is equivalent to

$$\begin{aligned} \delta_1 + \delta_2 + \delta_3 + \gamma_1 + \gamma_2 + \gamma_3 &= 1, \\ \delta_1 + \gamma_2 &= 1, \\ \delta_2 + \gamma_1 &= 1. \end{aligned} \tag{5.6}$$

In particular, $\gamma_3 + \delta_3 = 1$. There are 4 solutions to (5.6), namely

$$\begin{pmatrix} \gamma_1, \gamma_2, \gamma_3 \\ \delta_1, \delta_2, \delta_3 \end{pmatrix} = \begin{pmatrix} 0, 1, c_1 \\ 0, 1, c_1 + 1 \end{pmatrix}, \; \begin{pmatrix} 1, 0, c_1 \\ 1, 0, c_1 + 1 \end{pmatrix},$$

where $c_1 = 0, 1$. This is easy to see since both $(\gamma_1, \gamma_2) = (0, 0), (1, 1)$ lead to $\det y = 0$. Hence, there are at most 8 candidates for y (with $c_0 = 0, 1$). However, if $\langle g_0, y \rangle$ is isomorphic to A_4, then every element of order 3 in $\langle g_0, y \rangle$ must satisfy (5.6). There are 8 elements of order 3 in A_4, and thus there is at most 1 subloop $M_{24}(G, 2)$ satisfying all of our restrictions.

Because our choice of $x_0 \in V_4^- \cap G$ was one of three equivalent choices, we conclude that $c^- \leq 3$. □

Corollary 5.22 $\mathcal{H}_{M^*}(V_4^+ | Mo_{24})$=7, $\mathcal{H}_{M^*}(V_4^- | Mo_{24})$=3.

5.2.7 Subloops Isomorphic to E_8

Recall the representatives $V_4^+ = \langle x_0, u_1\rangle$, $V_4^- = \langle x_0, u_2\rangle$, and observe that $\langle x_0, u_1, u_2\rangle$ is isomorphic to E_8.

Lemma 5.23 $\mathcal{H}_{M^*}(V_4^+|E_8) = 3$, $\mathcal{H}_{M^*}(V_4^-|E_8) = 1$.

Proof. Let $d^\varepsilon = \mathcal{H}_{M^*}(V_4^\varepsilon|E_8)$. We have seen that both d^+, d^- are positive. An inspection of Table B.2 reveals that there are 12 involutions y such that $|x_0y| = |u_1y| = 2$, $y \notin V_4^+$. Namely, y is one of

$$\begin{array}{llll} a_0 = (\!(000, 110)\!), & a_1 = (\!(010, 010)\!), & a_2 = (\!(010, 100)\!), & a_3 = (\!(100, 010)\!), \\ a_4 = (\!(100, 100)\!), & a_5 = (\!(001, 111)\!), & a_6 = (\!(110, 000)\!), & a_7 = (\!(011, 011)\!), \\ a_8 = (\!(011, 101)\!), & a_9 = (\!(101, 011)\!), & a_{10} = (\!(101, 101)\!), & a_{11} = (\!(111, 001)\!). \end{array} \tag{5.7}$$

This immediately shows that $d^+ \le 3$. Note that $u_2 = a_3$, and check that

$$\begin{aligned} E_8^0 &= V_4^+ \cup \{a_0, a_5, a_6, a_{11}\}, \\ E_8^1 &= V_4^+ \cup \{a_1, a_4, a_7, a_{10}\}, \\ E_8^2 &= V_4^+ \cup \{a_2, a_3, a_8, a_9\} \end{aligned}$$

are all isomorphic to E_8. Thus $d^+ = 3$.

Let us prove that $d^- \le 1$. Yet another inspection of Table B.2 shows that there are 12 involutions y such that $|x_0y| = |u_2y| = 2$, $y \notin V_4^-$. Namely, y is one of

$$\begin{array}{llll} (\!(000, 011)\!), & (\!(001, 001)\!), & (\!(001, 010)\!), & (\!(100, 001)\!), \\ (\!(010, 111)\!), & (\!(101, 000)\!), & (\!(011, 101)\!), & (\!(011, 110)\!), \\ (\!(101, 011)\!), & (\!(110, 101)\!), & (\!(110, 110)\!), & (\!(111, 100)\!). \end{array} \tag{5.8}$$

This means that $d^- \le 3$, but we prove more. The group V_4^- is contained in 4 copies of Mo_{12}. With the notation of Section 4.4, there are nine involutions x_0, …, x_8 in Mo_{12}. We can think of x_0 as x_0 and of u_2 as x_1, say. This is possible thanks to the symmetry. Look at Figure 4.2 and you will see that $|x_0x_2| = |x_1x_2| = 2$ and $|x_0x_5| = |x_1x_5| = 2$. (Also $|x_0x_8| = |x_1x_8| = 2$ but x_8 is in $\langle x_0, x_1\rangle$.) Therefore, every copy of Mo_{12} steals two involutions from the list (5.8). Only 4 elements remain in (5.8), hence $d^- \le 1$. □

Lemma 5.24 *Every copy of E_8 contains a group from $O_{V_4^-}$.*

Proof. Arguing as in the proof of Lemma 5.23, we can assume that E_8 is isomorphic to one of the three groups E_8^i, $i = 0, 1, 2$. Since the representative V_4^- is contained in E_8^2, we proceed only with $i = 0, 1$.

Let π be the transposition $(1, 2)$, $x = (\!(\!(001, 101)\!)\!)_1$, and $y = (\!(\!(101, 100)\!)\!)_1$. Define f, $g \in \mathrm{Aut}(M^*)$ by $f = \widehat{\pi} \circ T(x)$, $g = T(y) \circ T(x)$ (compose from left to right). Then $a_1f = x_0$, $u_1f = (\!(011, 000)\!)$, $a_0g = x_0$, and $u_1g = (\!(000, 011)\!)$. By the proof of Lemma 5.18, both u_1f, u_1g can be mapped onto u_2 without moving x_0. □

Corollary 5.25 *The automorphism group* $\mathrm{Aut}(M^*)$ *acts transitively on the* 63 *copies of* E_8. *Moreover,* $\mathcal{H}_{M^*}(E_8|Mo_{24}) = 3$.

Proof. Let E, E' be two subgroups of M^* isomorphic to E_8. Then there are G, $G' \in O_{V_4^-}$ such that $G \leq E$, $G' \leq E'$, by Lemma 5.24. Since G, G' belong to the same orbit, there is $f \in \mathrm{Aut}(M^*)$ mapping G onto G'. As $\mathcal{H}_{M^*}(V_4^-|E_8) = 1$, f must map E onto E' as well.

By (4.3) and Lemma 5.23,

$$\begin{aligned} 7 \cdot \mathcal{H}_{M^*}(E_8) &= \mathcal{H}_{E_8}(V_4) \cdot \mathcal{H}_{M^*}(E_8) \\ &= |O_{V_4^+}| \cdot d^+ + |O_{V_4^-}| \cdot d^- = 63 \cdot 3 + 1 \cdot 252 = 441. \end{aligned}$$

Hence, $\mathcal{H}_{M^*}(E_8) = 63$. Consequently, (4.5) yields

$$\mathcal{H}_{M^*}(E_8|Mo_{24}) = \frac{\mathcal{H}_{Mo_{24}}(E_8) \cdot \mathcal{H}_{M^*}(Mo_{24})}{\mathcal{H}_{M^*}(E_8)} = \frac{3 \cdot 63}{63} = 3,$$

and we are finished. □

Remark 5.26 *Alternatively, to show that* $\mathrm{Aut}(M^*)$ *acts transitively on the copies of* E_8, *it suffices to prove that every copy of* E_8 *is contained in some* Mo_{24}. *This is enough thanks to Lemma* 5.16 *and Remark* 4.11. *However, this alternative approach does not seem to be easier as far as the numerical calculation is concerned.*

As $\mathcal{H}_{E_8}(C_2) = 7$, we have $\mathcal{H}_{M^*}(C_2|E_8) = 7$, by (4.5).

Let $\langle x_0, u_1, u_2 \rangle$ be the representative for E_8.

5.3 Subloop Lattice

It is about time to prove Proposition 5.5. Assume that $G \cong (C_2)^4$ is a subgroup of M^*. By Corollary 5.25, we can assume that $\langle x_0, u_1, u_2 \rangle \leq G$. Then there must be at least 8 involutions y outside of $\langle x_0, u_1, u_2 \rangle$ in M^* such that $|x_0 y| = |u_1 y| = |u_2 y| = 2$. Each such involution must be listed in both (5.7) and (5.8), a contradiction.

Let us summarize the results obtained in this chapter so far.

Theorem 5.27 (Structural Properties of M^*) *The smallest Paige loop* M^* *is a non-associative simple Moufang loop of order* 120. *It has trivial center and nucleus, and it satisfies the strong Lagrange property but not the weak Cauchy property. The following loops* (*and no other*) *appear as subloops of* M^*: $\{e\}$, C_2, C_3, V_4, S_3, E_8, A_4, Mo_{12}, Mo_{24}, *and* M^*.

The automorphism group $\mathrm{Aut}(M^*)$ *acts transitively on the copies of each of these subloops, with the exception of* V_4. *There are two orbits of transitivity* V_4^+, V_4^- *for* V_4. *With the notational conventions introduced in this chapter, we have the following orbit representatives:* $\langle x_0 \rangle$ *for* C_2, $\langle y_0 \rangle$ *for* C_3, $\langle x_0, u_1 \rangle$ *for* V_4^+, $\langle x_0, u_2 \rangle$ *for* V_4^-, $\langle x_0, y_0 \rangle$ *for* S_3, $\langle x_0, u_1, u_2 \rangle$ *for* E_8, $\langle x_0, z_0 \rangle$ *for* A_4, $\langle x_0, y_0, u_0 \rangle$ *for* Mo_{12}, *and* $\langle x_0, z_0, u_1 \rangle$ *for*

Mo_{24}, where $x_0 = (\!(111, 111)\!)$, $y_0 = (\!(\!(011, 110)\!)\!)_1$, $z_0 = (\!(\!(110, 100)\!)\!)_0$, $u_0 = (\!(000, 110)\!)$, $u_1 = (\!(001, 001)\!)$, and $u_2 = (\!(100, 010)\!)$. The subloop structure and Hasse constants for M^* are summarized in Figure 5.1.

For $p = 2$ and $p = 3$, the Sylow Theorems (A), (B), (C), (E) are true, whereas (F) is false. For $p = 5$, (C), (D), (E), (F) are true, whereas (A), (B) are false; as the Sylow 5-subloop of M^* is trivial.

5.4 Random Generators

As an application of Theorem 5.27 we calculate the probability that three randomly chosen elements of M^* generate M^*, and some refinements thereof. The technique we are about to develop has wide applicability.

5.4.1 Random m-tuples

Let C be a universal algebra and m a positive integer. Given an m-tuple $\mathbf{a} = (a_1, \ldots, a_m)$ of not necessarily distinct elements of C, let $\mathbf{a}^* = \{a_i^*\}_{i=0}^m$ be the sequence of nested subalgebras $a_i^* \leq C$, such that $a_0^* = \{e\}$ and $a_{i+1}^* = \langle a_i^*, a_i \rangle$. Clearly, a_m^* does not depend on the order of the elements $a_1, \ldots, a_m$ in $\mathbf{a}$.

Let $\mathrm{Gen}_m(C)$ be the set of all m-tuples $\mathbf{a} \in C^m$ with $a_m^* = C$, and let $\mathrm{gen}_m(C) = |\mathrm{Gen}_m(C)|$. Then the probability that m randomly chosen elements of C generate C is

$$\gamma_n(C) = |C|^{-m} \cdot \mathrm{gen}_m(C). \tag{5.9}$$

If $\mathrm{Gen}'_m(C) \subseteq \mathrm{Gen}_m(C)$ is the set of m-tuples $\mathbf{a} \in C^m$ with distinct elements, and $\mathrm{gen}'_m(C) = |\mathrm{Gen}'_m(C)|$, then the probability that m randomly chosen distinct elements of C generate C is

$$\gamma'_m(C) = [|C| \cdot (|C| - 1) \cdots (|C| - (m-1))]^{-1} \cdot \mathrm{gen}'_m(C). \tag{5.10}$$

We are now going to refine the above ideas.

Two m-tuples of integers $\mathbf{r} = (r_1, \ldots, r_m)$ and $\mathbf{s} = (s_1, \ldots, s_m)$ are said to be of the *same type* if $r_1, \cdots, r_m$ is a permutation of $s_1, \cdots, s_m$. We say that $\mathbf{a} \in C^m$ is of *type* $\mathbf{s}$ if $(|a_1|, \cdots, |a_m|)$ is of the same type as $\mathbf{s}$.

Let $\mathrm{Gen}_{\mathbf{s}}(C) \subseteq \mathrm{Gen}_m(C)$ be the set of all m-tuples of type $\mathbf{s}$, and $\mathrm{gen}_{\mathbf{s}}(C) = |\mathrm{Gen}_{\mathbf{s}}(C)|$. Similarly, let $\mathrm{Gen}'_{\mathbf{s}}(C) \subseteq \mathrm{Gen}'_m(C)$ be the set of all m-tuples of type $\mathbf{s}$ with distinct entries, and $\mathrm{gen}'_{\mathbf{s}}(C) = |\mathrm{Gen}'_{\mathbf{s}}(C)|$. Then

$$\gamma_{\mathbf{s}}(C) = |C|^{-m} \cdot \mathrm{gen}_{\mathbf{s}}(C)$$

is the probability that m randomly chosen elements $a_1, \ldots, a_m \in C$ generate C and $\mathbf{a} = (a_1, \ldots, a_m)$ is of type $\mathbf{s}$. Similarly,

$$\gamma'_{\mathbf{s}}(C) = [|C| \cdot (|C| - 1) \cdots (|C| - (m-1))]^{-1} \cdot \mathrm{gen}'_{\mathbf{s}}(C)$$

is the probability that m randomly chosen distinct elements $a_1, \ldots, a_m \in C$ generate C and $\mathbf{a} = (a_1, \ldots, a_m)$ is of type $\mathbf{s}$.

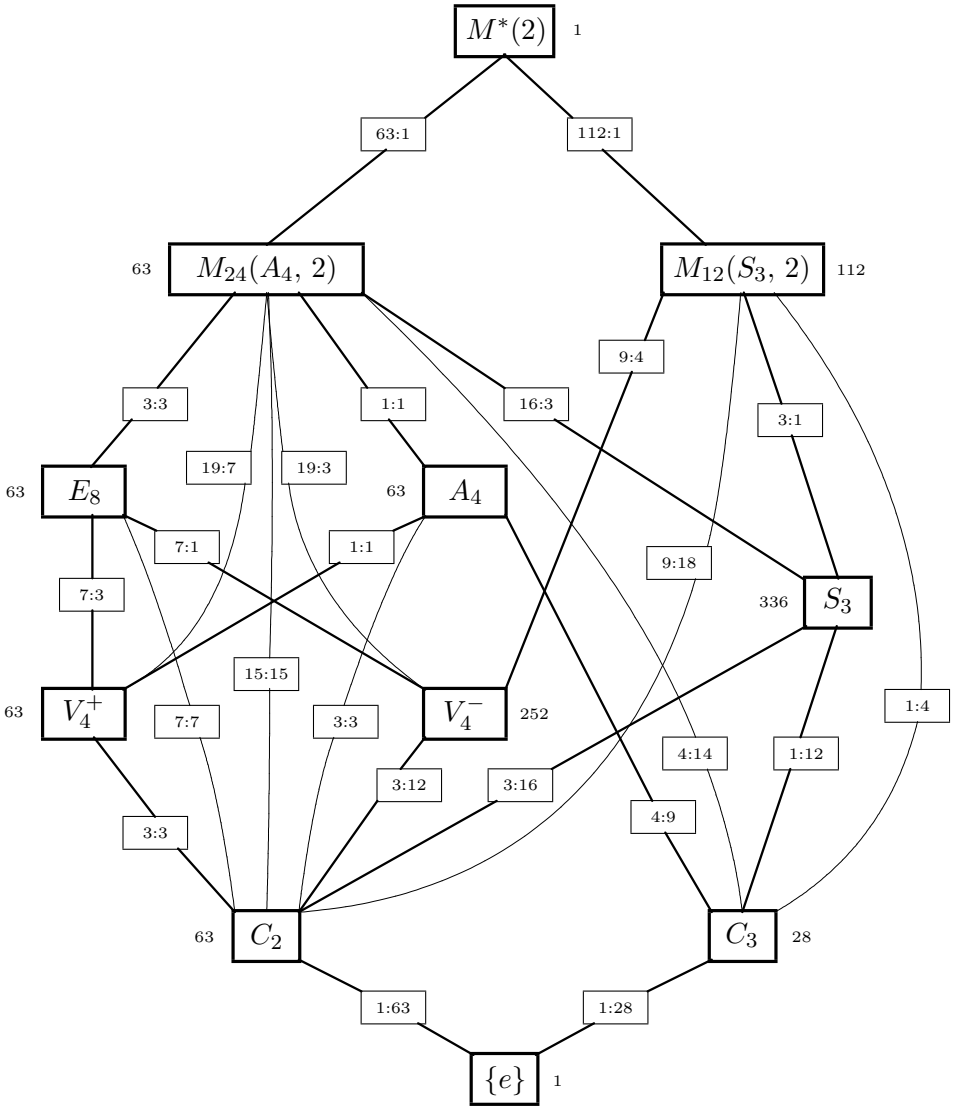

Figure 5.1: The subloop structure and Hasse constants in $M^*(2)$. Two non-trivial representatives A, B are connected by an edge if and only if $\mathcal{H}_{M^*(2)}(A|B) > 0$. If $A = \{e\}$ or $B = M^*(2)$, the two representatives A, B are connected by an edge if and only if a copy of A is maximal in B. The edge connecting A and B is thick if and only if a copy of A is maximal in B. The constants $|O_A|$, $\mathcal{H}_B(A)$, $\mathcal{H}^O_{M^*(2)}(A|B)$ are located in the diagram as follows: $|O_A|$ next to A, $\mathcal{H}_B(A)$ and $\mathcal{H}^O_{M^*(2)}(A|B)$ along the edge connecting A and B, separated by colon.

5.4.2 Links in the Lattice of Subalgebras

For $A,\ B \leq C$, let $\Gamma_n(A,\ B)$ be the cardinality of the set of elements $x \in C$ such that $|x| = n$ and $\langle A,\ x\rangle \in O_B$, where O_B is the orbit of B under the action of $\mathrm{Aut}(C)$ on the copies of B. Put

$$\Gamma(A,\ B) = \sum_{n=1}^{\infty} \Gamma_n(A,\ B).$$

We are going to divide the set $\mathrm{Gen}_m(C)$ into certain equivalence classes. Two m-tuples $\mathbf{a},\ \mathbf{b} \in \mathrm{Gen}_m(C)$ are called *orbit-equivalent* if $a_i^* \in O_{b_i^*}$ for every $i,\ 0 \leq i \leq m$. We write $\mathbf{a} \sim \mathbf{b}$.

The cardinality of the equivalence class $[\mathbf{a}]_\sim$ is easy to calculate with the help of the constants $\Gamma(A,\ B)$.

Lemma 5.28 *With the above notation,*

$$|[\mathbf{a}]_\sim| = \prod_{i=0}^{m-1} \Gamma(a_i^*,\ a_{i+1}^*). \tag{5.11}$$

Proof. Given $a_0^* = \{e\}$, there are $\Gamma(a_0^*,\ a_1^*)$ elements x_1 such that $\langle a_0^*,\ x_1\rangle \in O_{a_1^*}$. Once we are in the orbit $O_{a_i^*}$, we can continue on the way to $O_{a_{i+1}^*}$ by adding one of the $\Gamma(a_i^*,\ a_{i+1}^*)$ elements x_{i+1} to $\langle x_1,\ \ldots,\ x_i\rangle$. □

Since $\mathrm{Gen}_m(C)$ is a disjoint union of equivalence classes $[\mathbf{a}]_\sim \in \mathrm{Gen}_m(C)/\sim$, we have

$$\mathrm{gen}_m(C) = \sum_{[\mathbf{a}]_\sim \in (\mathrm{Gen}_m(C)/\sim)} |[\mathbf{a}]_\sim|. \tag{5.12}$$

Hence, combining (5.11), (5.12) and (5.9), we obtain a practical way of calculating the probability $\gamma_m(C)$.

Example 5.29 *In order to illustrate the theoretical results, let us calculate the probability that two randomly chosen distinct elements of S_3 generate S_3. (It is easy to see that the probability is $(3+6)/15 = 3/5$).*

There are three subgroups isomorphic to C_2 in S_3 (all in one orbit of transitivity), and a unique subgroup isomorphic to C_3. Obviously, $\Gamma(\{e\},\ C_2) = 3$, $\Gamma(\{e\},\ C_3) = 2$, $\Gamma(C_2,\ S_3) = 4$, $\Gamma(C_3,\ S_3) = 3$. Therefore, $\mathrm{gen}_2(S_3) = 3 \cdot 4 + 2 \cdot 3 = 18$. Then $\gamma_2(S_3) = 18/30 = 3/5$, as expected.

From now on, *we will assume that m is the minimal number of generators for C.* Allow us to recall that under this assumption $\mathrm{Gen}_m(C) = \mathrm{Gen}'_m(C)$ and $\mathrm{Gen}_{\mathbf{s}}(C) = \mathrm{Gen}'_{\mathbf{s}}(C)$.

Let $\sim_{\mathbf{s}}$ be the restriction of $\sim$ onto $\mathrm{Gen}_{\mathbf{s}}(C)^2$. We can then refine Lemma 5.28 in an obvious way:

Proposition 5.30 *With the above notation,*

$$|[\mathbf{a}]_{\sim_\mathbf{s}}| = \sum_{\mathbf{k}=(k_1,\ldots,k_m)} \prod_{i=1}^{m-1} \Gamma_{k_i}(a_i^*,\, a_{i+1}^*),$$

where the summation runs over all m-tuples $\mathbf{k}$ of the same type as $\mathbf{s}$.

Again,

$$\mathrm{gen}_\mathbf{s}(C) = \sum_{[\mathbf{a}]_{\sim_\mathbf{s}} \in (\mathrm{Gen}_m(C)/\sim_\mathbf{s})} |[\mathbf{a}]_{\sim_\mathbf{s}}|$$

will be used to calculate $\gamma_\mathbf{s}(C)$.

5.4.3 The Constants $\Gamma_n(A,\, B)$ for M^*

Let $C = M^*$. We are going to find the constants $\Gamma_n(A,\, B)$ for $A < B \leq M^*$.

Clearly, $\Gamma_n(A,\, B)$ vanishes unless $n = 2,\, 3$. Assume that A is a maximal subloop of B, and let r_n the number of elements of order n contained in $B \setminus A$. Then

$$\Gamma_n(A,\, B) = \mathcal{H}^O_{M^*}(A|B) \cdot r_n.$$

This is the connection between Hasse constants and the constants $\Gamma_n(A,\, B)$.

All non-trivial constants $\Gamma_n(A,\, B)$ are summarized in Figure 5.2, where two subloops $A < B$ are connected by a thick, straight edge if A is maximal in B, and by a curved, thin edge when A is not maximal in B but still $B = \langle A,\, x\rangle$ for some $x \in M^*$. The constants $\Gamma_2(A,\, B)$, $\Gamma_3(A,\, B)$ are located along the edges.

For instance, since $\mathcal{H}^O_{M^*}(E_8|Mo_{24}) = 3$ and Mo_{24} contains 8 involutions not contained in E_8, we have $\Gamma_2(E_8,\, Mo_{24}) = 24$.

Counting in this way, we find all constants $\Gamma_n(A,\, B)$ with A maximal in B (using Figure 5.1). Apart from trivialities, the remaining constants to be calculated are

$$\begin{gathered}\Gamma_n(C_2,\, A_4),\ \ \Gamma_n(S_3,\, M^*),\ \ \Gamma_n(A_4,\, M^*),\ \ \Gamma_n(V_4^-,\, M^*)' \\ \Gamma_n(V_4^-,\, Mo_{24}),\ \ \Gamma_n(V_4^+,\, Mo_{24}),\ \ \Gamma_n(V_4^+,\, M^*),\ \ \Gamma_n(E_8,\, M^*),\end{gathered}$$

for $n = 2,\, 3$. Since some invention is needed here, we better show how to obtain all of them.

Let us get started with $\Gamma_n(S_3,\, M^*)$. Let G be a copy of S_3. For any element $x \notin G$, we must have $\langle G,\, x\rangle \cong Mo_{12}$, Mo_{24}, or M^*. Therefore, for $n = 2,\, 3$,

$$\Gamma_n(S_3,\, M^*) = (n-1) \cdot \mathcal{H}_{M^*}(C_n) - \Gamma_n(S_3,\, Mo_{12}) - \Gamma_n(S_3,\, Mo_{24}) - (n-1) \cdot \mathcal{H}_{S_3}(C_n).$$

The terms $(n-1) \cdot \mathcal{H}_{M^*}(C_n)$ and $(n-1) \cdot \mathcal{H}_{S_3}(C_n)$ count the number of elements of order n in M^* and S_3, respectively. (The formula only works when n is a prime.) We get

$$\Gamma_2(S_3,\, M^*) = 63 - 6 - 36 - 3 = 18, \quad \Gamma_3(S_3,\, M^*) = 56 - 0 - 18 - 2 = 36.$$

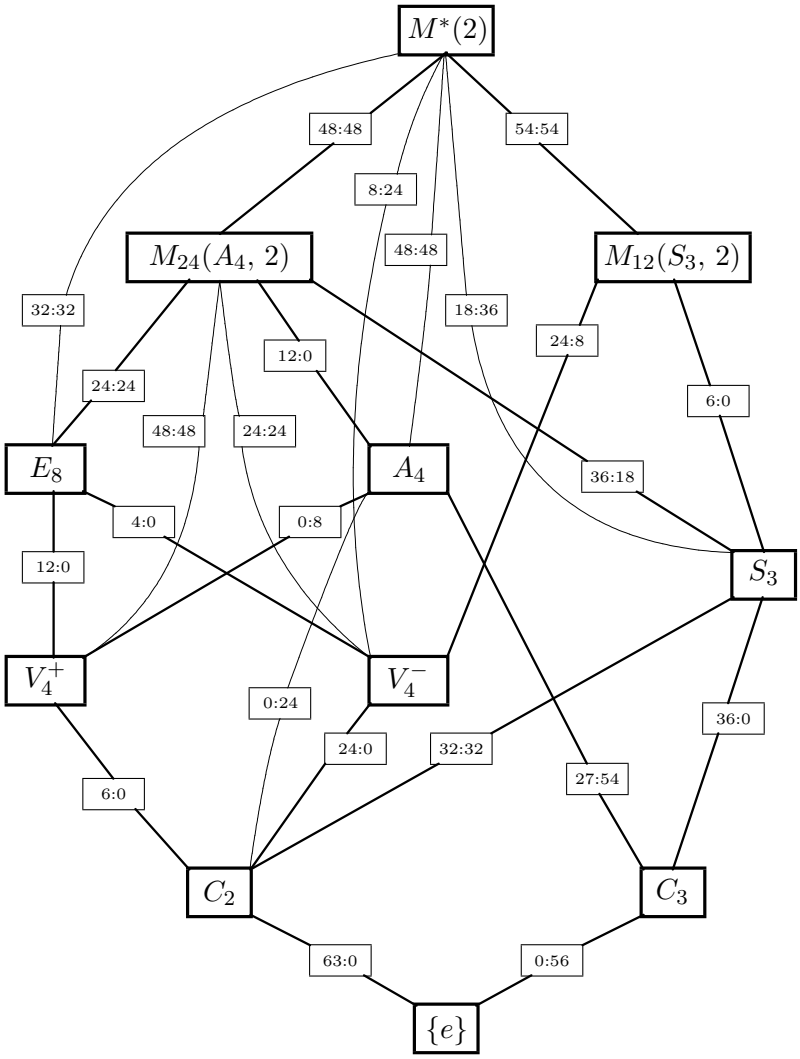

Figure 5.2: The constants $\Gamma_n(A,\,B)$ for $M^*(2)$. If A is maximal in a copy of B, then A and B are connected by a thick, straight line; else by a thin, curved line. The constants $\Gamma_n(A,\,B)$ are located along the edges, separated by colon.

Similarly,

$$\begin{array}{rclrcl} \Gamma_2(C_2,\, A_4) &=& 0, & \Gamma_3(C_2,\, A_4) &=& 24, \\ \Gamma_2(A_4,\, M^*) &=& 48, & \Gamma_3(A_4,\, M^*) &=& 48, \\ \Gamma_2(E_8,\, M^*) &=& 32, & \Gamma_3(E_8,\, M^*) &=& 32. \end{array}$$

A more detailed analysis of the subloop lattice of M^* allows us to calculate the remaining eight constants.

Lemma 5.31 *Let $G \in O_{V_4^-}$, and let M_1, M_2, M_3 be the three copies of Mo_{24} containing G. Then $M_i \cap M_j$ contains no element of order 3, for $i \neq j$, and $M_1 \cap M_2 \cap M_3$ is the unique copy of E_8 containing G. In particular,*

$$\Gamma_3(V_4^-,\, Mo_{24}) = 24,\ \ \Gamma_3(V_4^-,\, M^*) = 24,\ \ \Gamma_2(V_4^-,\, Mo_{24}) = 24,\ \ \Gamma_2(V_4^-,\, M^*) = 8.$$

Proof. Assume there is $x \in M_i \cap M_j$, $|x| = 3$, for some $i \neq j$. Then $M_i = \langle G,\, x\rangle = M_j$, because $\mathcal{H}_{M^*}(V_4^-|A_4) = 0$, a contradiction. Thus $M_1 \cup M_2 \cup M_3$ contains $3 \cdot 8 = 24$ elements x of order 3 such that $\langle G,\, x\rangle \in O_{Mo_{24}}$.

Let H be the unique copy of E_8 containing G. We must have $H = M_1 \cap M_2 \cap M_3$, since $\mathcal{H}_{M^*}(E_8|Mo_{24}) = 3$. Therefore $M_1 \cup M_2 \cup M_3$ contains $3 \cdot (12 - 4) = 24$ involutions x such that $\langle G,\, x\rangle \in O_{Mo_{24}}$. The constants $\Gamma_n(V_4^-,\, M^*)$ are then easy to calculate. $\square$

It is conceivable that there is $G \in O_{V_4^+}$ and $x \in M^*$ such that $\langle G,\, x\rangle = M^*$. It is not so, though.

Lemma 5.32 *In M^*, we have*

$$\Gamma_3(V_4^+,\, Mo_{24}) = 48,\ \ \Gamma_2(V_4^+,\, Mo_{24}) = 48,\ \ \Gamma_3(V_4^+,\, M^*) = 0,\ \ \Gamma_2(V_4^+,\, M^*) = 0.$$

Proof. Pick $G \in O_{V_4^+}$, and let M_1, ..., M_7 be the seven copies of Mo_{24} containing G. We claim that $(M_i \cap M_j)^2 = e$, for $i \neq j$. Assume it is not true, and let x be an element of order 3 contained in $M_i \cap M_j$. Then $A_4 \cong \langle G,\, x\rangle \leq M_i \cap M_j$ shows that $\mathcal{H}_{Mo_{24}}(A_4) \geq 2$, a contradiction. Thus $\bigcup_{i=1}^{7} M_i$ contains all $8 \cdot 7 = 56$ elements of order 3. In particular, for any element x of order 3, we have $\langle G,\, x\rangle \neq M^*$. This translates into

$$\Gamma_3(V_4^+,\, M^*) = 0,\ \ \Gamma_3(V_4^+,\, Mo_{24}) = 56 - \Gamma_3(V_4^+,\, A_4) = 48.$$

We proceed carefully to show that $\Gamma_2(V_4^+,\, M^*) = 0$. The group G is contained in a single copy A of A_4, that is in turn contained in a single copy of Mo_{24}, say M_1. Let H_1, H_2, $H_3 \leq M_1$ be the three copies of E_8 containing G (see the proof of Proposition 4.12). It helps to visualize how the subgroups G, A, H_1, H_2 and H_3 sit in M_1. Observe that $H_1 \cup H_2 \cup H_3 = G \cup Au$, where Au is the second coset of A in M_1. The situation must then look as in Figure 5.3.

Pick M_i, M_j, with $2 \leq i < j \leq 7$. We want to show that $M_i \cap M_j \subseteq M_1$. Thanks to the first part of this Lemma, we know that $M_i \cap M_j \cong V_4$ or (C_2^3). When $M_i \cap M_j \cong V_4$ then, trivially, $M_i \cap M_j = G \leq M_1$. When $M_i \cap M_j \cong E_8$ then $M_i \cap M_j = H_k$ for some $k \in \{1,\, 2,\, 3\}$, else $\mathcal{H}_{M^*}(G|E_8) \geq 4$, a contradiction.

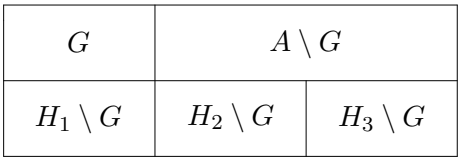

Figure 5.3: The proof of Lemma 5.32

Consequently, $\bigcup_{i=1}^{7} M_i$ contains at least $15 + 6 \cdot 8 = 63$ involutions; 15 in M_1, and additional 8 in each M_i. In particular, $\langle G, x\rangle \neq M^*$ for every involution x. We get

$$\Gamma_2(V_4^+, M^*) = 0, \;\; \Gamma_2(V_4^+, Mo_{24}) = 60 - \Gamma_2(V_4^+, E_8) = 48.$$

This finishes the proof. □

All constants $\Gamma_n(A, B)$ have now been calculated, and we can return to our original question: What is the probability that three randomly chosen elements generate M^*?

5.4.4 Random Generators of Arbitrary Orders

We will use Lemma 5.28 and Equation (5.12) to find $\gamma_3(M^*)$. There are only five orbit-non-equivalent sequences of subalgebras of length 4 in M^*. Namely (look at Figure 5.2),

$$\begin{aligned}
\mathcal{A}_0 &= \{\{e\}, C_2, A_4, M^*\},\\
\mathcal{A}_1 &= \{\{e\}, C_2, V_4^-, M^*\},\\
\mathcal{A}_2 &= \{\{e\}, C_2, S_3, M^*\},\\
\mathcal{A}_3 &= \{\{e\}, C_3, S_3, M^*\},\\
\mathcal{A}_4 &= \{\{e\}, C_3, A_4, M^*\}.
\end{aligned}$$

These sequences and the related constants $\Gamma_n(A, B)$ are visualized in Figure 5.4. Full lines correspond to involutions ($n = 2$), dotted lines to elements of order 3 ($n = 3$).

Proposition 5.33 *Let $\gamma = \gamma_3(M^*)$ (resp. $\gamma' = \gamma_3'(M^*)$) be the probability that 3 randomly chosen (distinct) elements of M^* generate M^*. Then*

$$\gamma = \frac{955,584}{120^3} \doteq 0.553, \;\; \gamma' = \frac{955,584}{120 \cdot 119 \cdot 118} \doteq 0.567.$$

Proof. By (5.12),

$$\mathrm{gen}_3(M^*) = \mathrm{gen}_3'(M^*) = \sum_{i=1}^{4} |[\mathcal{A}_i]_\sim|.$$

By our previous calculation summarized in Figure 5.4, $|[\mathcal{A}_0]_\sim| = 63 \cdot 24 \cdot (48 + 48)$, $|[\mathcal{A}_1]_\sim| = 63 \cdot 24 \cdot (8 + 24)$, $|[\mathcal{A}_2]_\sim| = 63 \cdot (32 + 32) \cdot (18 + 36)$, $|[\mathcal{A}_3]_\sim| = 56 \cdot 36 \cdot (18 + 36)$, and $|[\mathcal{A}_4]_\sim| = 56 \cdot (54 + 27) \cdot (48 + 48)$. Thus $\mathrm{gen}_3(M^*) = 955,584$. We are done by (5.9) and (5.10). □

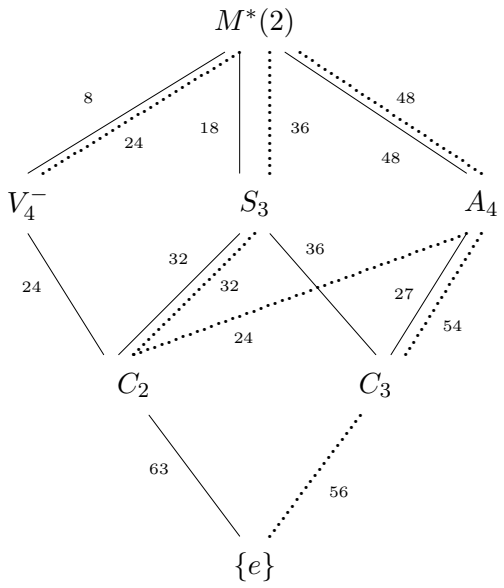

Figure 5.4: Sequences of Subloops in M^*

5.4.5 Random Generators of Given Orders

The only possible types of orders for three generators in M^* are (2, 2, 2), (2, 2, 3), (2, 3, 3), and (3, 3, 3). The sequences of subalgebras corresponding to each of these types are depicted in Figure 5.5. We must be careful, though, since not all combinations of lines in Figure 5.5 correspond to sequences with correct types of orders. We have tried to make the possible continuations clear in Figure 5.5.

Proposition 5.34 *Let* $\mathbf{s} = (s_1, s_2, s_3)$ *be a* 3*-tuple of integers,* $s_1 \leq s_2 \leq s_3$*, and let* $\gamma_{\mathbf{s}} = \gamma_{\mathbf{s}}(M^*)$ *(resp.* $\gamma'_{\mathbf{s}} = \gamma'_{\mathbf{s}}(M^*)$*) be the probability that* 3 *randomly chosen (distinct) elements* a_1*,* a_2*,* a_3 *of* M^* *generate* M^* *and* $(|a_1|, |a_2|, |a_3|)$ *is of type* $\mathbf{s}$*. Then*

$$\gamma_{(2,2,2)} = \frac{48,384}{120^3} \doteq 0.028, \qquad \gamma_{(2,2,3)} = \frac{326,592}{120^3} \doteq 0.189,$$
$$\gamma_{(2,3,3)} = \frac{435,456}{120^3} \doteq 0.252, \qquad \gamma_{(3,3,3)} = \frac{145,152}{120^3} \doteq 0.084,$$
$$\gamma'_{(2,2,2)} = \frac{48,384}{120 \cdot 119 \cdot 118} \doteq 0.029, \qquad \gamma'_{(2,2,3)} = \frac{326,592}{120 \cdot 119 \cdot 118} \doteq 0.194,$$
$$\gamma'_{(2,3,3)} = \frac{435,456}{120 \cdot 119 \cdot 118} \doteq 0.258, \qquad \gamma'_{(3,3,3)} = \frac{145,152}{120 \cdot 119 \cdot 118} \doteq 0.086.$$

Proof. Use Proposition 5.30 and Figure 5.5. □

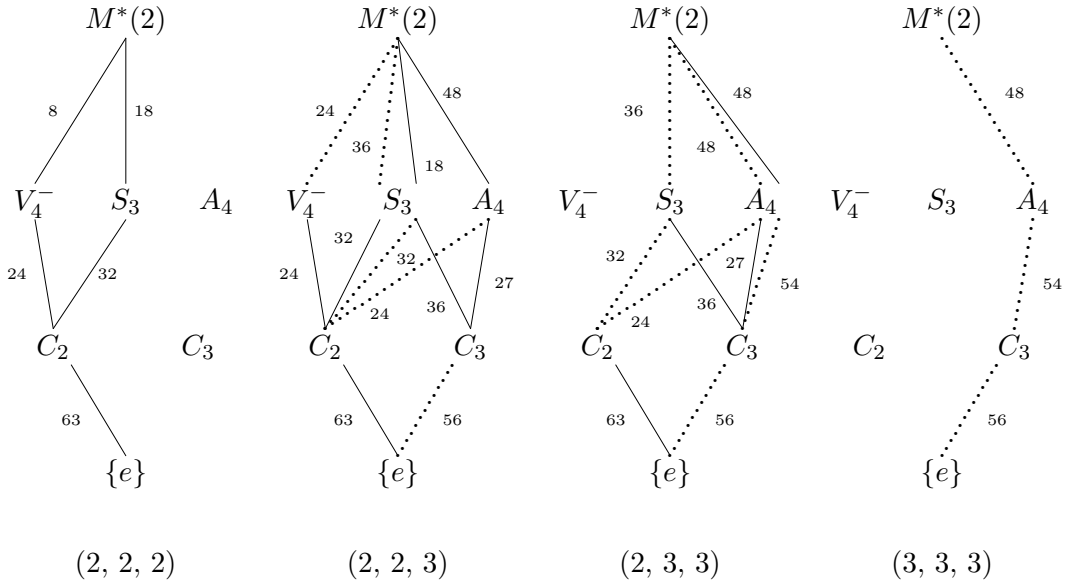

Figure 5.5: The shortest sequences of subloops in M^*

5.5 Combinatorial Structures Related to M^*

We consider two combinatorial structures based on the lattice of subloops of M^*. They further elucidate the complicated structure of the lattice.

5.5.1 A Strongly Regular Graph and its Hadamard Design

By a *graph* $\mathcal{G} = (V(\mathcal{G}), E(\mathcal{G}))$ we mean an unoriented graph with no loops and no multiple edges. The elements of $V(\mathcal{G})$ are called *vertices*, the elements of $E(\mathcal{G})$ are called *edges*. Every edge is represented by a two-element subset of $V(\mathcal{G})$. A vertex $y \in V(\mathcal{G})$ is a *neighbor* of $x \in V(\mathcal{G})$ if $\{x, y\}$ is an edge. Let Nbd x be the set of all neighbors of x in $\mathcal{G}$. The *valency* of x is the cardinality of Nbd x.

A graph $\mathcal{G}$ is said to be *regular* of *degree* n if the valency of each vertex is n. A regular graph is *strongly regular* if there are two constants λ, μ such that $|\text{Nbd } x \cap \text{Nbd } y| = \lambda$ whenever $\{x, y\} \in E(\mathcal{G})$, and $|\text{Nbd } x \cap \text{Nbd } y| = \mu$ whenever $\{x, y\} \notin E(\mathcal{G})$. Such a strongly regular graph will be denoted by srg(v, n, λ, μ), where $v = |V(\mathcal{G})|$. (See van Lint and Wilson [31].)

Lemma 5.35 *Let $V(\mathcal{G})$ be the set of all involutions of M^*, and declare $\{x, y\} \subseteq V(\mathcal{G})$ an edge if $\langle x, y\rangle \cong S_3$ (equivalently, $|xy| = 3$). Then $\mathcal{G} = (V(\mathcal{G}), E(\mathcal{G}))$ is a* srg(63, 32, 16, 16).

Proof. Since $\mathrm{Aut}(M^*)$ acts transitively on the 63 involutions of M^*, $\mathcal{G}$ is a regular graph of degree $n = \mathcal{H}_{M^*}(C_2|S_3) \cdot 2 = 32$.

The proof of Proposition 5.12 in fact shows that $\mathrm{Aut}(M^*)$ acts transitively on the edges of $\mathcal{G}$. To calculate λ, it is then sufficient to count the common neighbors of x_0 and $x_1 = \langle\!\langle 110, 100 \rangle\!\rangle$. A quick inspection of Table B.2 yields $\lambda = 16$.

The group $\mathrm{Aut}(M^*)$ does not act transitively on the non-edges of $\mathcal{G}$ (i.e., on the edges of the complement $\mathcal{G}^c$ of $\mathcal{G}$), nonetheless, every edge of $\mathcal{G}^c$ can be transformed into $\{x_0, u_1\}$ or $\{x_0, u_2\}$, thanks to Lemma 5.18. Therefore, to verify that $\mu = 16$, one only has to check that $|\mathrm{Nbd}\, x_0 \cap \mathrm{Nbd}\, u_i| = 16$, for $i = 1, 2$. Table B.2 comes handy again. □

Remark 5.36 *The following problem seems to be non-trivial: Construct a graph $\mathcal{G}$ of diameter 2 such that $\mathrm{Aut}(\mathcal{G})$ acts transitively on the edges of $\mathcal{G}$, but does not act transitively on the non-edges of $\mathcal{G}$. The graph constructed in Lemma 5.35 is such a graph. (Every strongly regular graph with $\mu > 0$ has diameter 2.)*

When the diameter is bigger than 2, then there are at least 3 orbits of transitivity under the action of $\mathrm{Aut}(\mathcal{G})$ on all pairs of vertices, since every automorphism preserves distance. The simplest graph $\mathcal{G}$ such that $\mathrm{Aut}(\mathcal{G})$ acts transitively on the edges of $\mathcal{G}$ but not on the non-edges of $\mathcal{G}$ is the hexagonal graph C_6.

Every strongly regular graph with $\lambda = \mu$ gives rise to a combinatorial design. Recall that a t-(v, k, λ) *design* is a collection $\mathcal{B}$ of subsets (called *blocks*) of a set $\mathcal{P}$ of v *points*, such that every block contains k points, and every set of t points is contained in exactly λ blocks.

For a strongly regular graph $\mathcal{G} = \mathrm{srg}(v, n, \lambda, \lambda)$, let $\mathcal{P} = V(\mathcal{G})$, $\mathcal{B} = \{\mathrm{Nbd}\ x;\ x \in V(\mathcal{G})\}$. Then $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a 2-(v, n, λ) design. In our case, $\mathcal{D}$ is a 2-(63, 32, 16) design, the complement of the 2-(63, 31, 15) Hadamard design constructed in [31, Example 19.3]. It is known that $\mathcal{D}$ is not a 3-design. (If it were a 3-$(63, 32, \lambda)$ design, we would have, by Theorem 19.3 [31],

$$16 = b_2 = \lambda \begin{pmatrix} 62 \\ 2 \end{pmatrix} / \begin{pmatrix} 31 \\ 2 \end{pmatrix},$$

i.e., $\lambda = 3.93\ldots$ would not be an integer.)

5.5.2 Generalized Hexagons

The *girth* of a graph $\mathcal{G}$ is the length of the shortest cycle (polygon) in $\mathcal{G}$. According to [37], a *generalized hexagon* of order (s, t), $s, t \geq 1$ is a 1-$(v, s+1, t+1)$ design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ whose incidence graph has girth 12 and diameter 6. Up to duality, there are only 2 known generalized hexagons for every prime power q; one of order (q, q), the other of order (q, q^3). When $s = t$, we speak simply of a generalized hexagon of order s. A generalized hexagon of order s can be equivalently defined as follows (cf. [34, p. 42]).

It is an incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B}, I)$ with a symmetric incidence relation satisfying

(i) each point (resp. line = block) is incident with $s + 1$ lines (resp. points),

(ii) $|\mathcal{P}| = |\mathcal{B}| = 1 + s + s^2 + s^3 + s^4 + s^5 = (s^6 - 1)/(s - 1)$,

(iii) 6 is the smallest positive integer k such that $\mathcal{S}$ has a circuit consisting of k (distinct) points and k (distinct) lines.

It is well known (cf. [13]) that the automorphism group of the generalized hexagon of order q described above is the exceptional group $G_2(q)$. Since, as we will see in Chapter 6, $\mathrm{Aut}(M^*) = G_2(2)$, it is natural to search for a generalized hexagon of order 2 in the lattice of subloops of M^*. The aim of this subsection is to persuade the reader that, indeed, there is a generalized hexagon H of order 2 embedded in the lattice. We will construct H, verify axioms (i) and (ii), and leave the verification of (iii) to GAP. The details can be found in Appendix A.

Let $q = 2$. A quick glance at Figure 5.1 shows that there are 3 good candidates for H. Namely, one can see that

$$|O_{C_2}| = |O_{V_4^+}| = |O_{E_8}| = |O_{Mo_{24}}| = 63 = 2^6 - 1,$$

and that

$$\begin{aligned} \mathcal{H}_{V_4}(C_2) &= \mathcal{H}^O_{M^*}(C_2|V_4^+) = \mathcal{H}_{A_4}(C_2) = \mathcal{H}_{M^*}(C_2|A_4) \\ &= \mathcal{H}_{Mo_{24}}(E_8) = \mathcal{H}_{M^*}(E_8|Mo_{24}) = 3 = 2 + 1. \end{aligned}$$

We focus on the incidence between O_{C_2} and $O_{V_4^+}$, however, we suspect that the incidence between O_{C_2} and O_{A_4}, and between O_{E_8} and $O_{Mo_{24}}$ will yield additional two generalized hexagons of order 2.

Proposition 5.37 *Let $\mathcal{P} = O_{C_2}$, $\mathcal{B} = O_{V_4^+}$, $H = (\mathcal{P}, \mathcal{B})$, where the incidence between $\mathcal{P}$ and $\mathcal{B}$ is given by inclusion. Then H is a generalized hexagon of order 2.*

Proof. Axioms (i) and (ii) are clearly satisfied. The author has verified by GAP that (iii) is satisfied, too. See Appendix A for details. □

Chapter 6

Automorphism Groups of Paige Loops

Theorem 3.1 claims that $\mathrm{Aut}(\mathbb{O}(q))$ is the exceptional group $G_2(q)$. Since $G_2(q)$ is a subgroup of $\leq \mathrm{Aut}(M(q))$, by Lemma 3.4, it makes sense to ask whether the equality $G_2(q) = \mathrm{Aut}(M(q))$ holds for some (and possibly all) values of q. Moreover, it is tempting to approach the problem by extending (multiplicative) automorphisms of $M(q)$ into (linear) automorphisms of $\mathbb{O}(q)$.

The additive operation is not well-defined on $M^*(q)$ when q is odd (an element $a \in M^*(q)$ is identified with $-a$, but $a + a = 2a$ in $\mathbb{O}(q)$, whereas $a + (-a) = 0$). Hence, it is not obvious how to extend an automorphism of $M^*(q)$ onto $M(q)$. Nevertheless, when q is even, the two Moufang loops $M^*(q)$ and $M(q)$ coincide, and that is why the investigation of $\mathrm{Aut}(M(q))$ applies to $\mathrm{Aut}(M^*(q))$, too, in such a case.

We prove in two ways that $\mathrm{Aut}(M^*(2)) = G_2(2)$, and offer several results for the general case. We will take advantage of both Zorn's construction of $\mathbb{O}(q)$ and the well-known, clever construction described below.

6.1 Extending Automorphisms from the First Shell

Pick an automorphism g of the (not necessarily simple) Moufang loop $M(q)$. Our ultimate goal is to construct $h \in \mathrm{Aut}(\mathbb{O}(q))$ such that $h \restriction M(q) = g$. If this can be done, we immediately conclude that $\mathrm{Aut}(M(q)) = G_2(q)$ for every q. We like to think of the problem as a notion "orthogonal" to Witt's lemma. Roughly speaking, Witt's lemma deals with extensions of partial isometries from subspaces onto finite-dimensional vector spaces, whereas we are attempting to extend a multiplicative, norm-preserving map from the first shell $M(q)$ into an automorphism (= isometry, by [41, Corollary 1.2.4]) of $\mathbb{O}(q)$. Naturally, $g \in \mathrm{Aut}(M(q))$ is not linear because $M(q)$ is not even closed under addition, however, the analogy with Witt's lemma will become more apparent once we prove that g *is*, in a sense, additive (cf. Proposition 6.14).

6.1.1 A One-step Construction

There is a remarkably compact way of constructing the standard real octonion algebra $\mathbb{O}$ that avoids the iterative Cayley-Dickson process. As in [15], let $B = \{e = e_0, e_1, \ldots, e_7\}$ be a basis whose vectors are multiplied according to

$$\begin{aligned} e_r^2 &= -1, \quad e_{r+7} = e_r, \quad e_r e_s = -e_s e_r, \\ e_{r+1}e_{r+3} &= e_{r+2}e_{r+6} = e_{r+4}e_{r+5} = e_r, \end{aligned}$$

for $r, s \in \{1, \ldots, 7\}$, $r \neq s$. (Alternatively, see [14, p. 122].) The norm $N(u)$ of a vector $u = \sum_{i=0}^{7} a_i e_i \in \mathbb{O}$ is given by $\sum_{i=0}^{7} a_i^2$.

Importantly, all the *structural constants* γ_{ijk}, defined by $e_i \cdot e_j = \sum_{k=0}^{7} \gamma_{ijk} e_k$, are equal to ± 1, and therefore the construction can be imitated over any field k. For $k = GF(q)$, let us denote the ensuing algebra by $\mathbb{O}(q)$. There is no danger of confusion with our previous notation because all octonion algebras over $GF(q)$ are isomorphic.

We now use the basis B of $\mathbb{O}(q)$ to construct a mapping $h : \mathbb{O}(q) \longrightarrow \mathbb{O}(q)$ from g. First of all, B is a subset of $M(q)$, so the values $g(e_i)$ are known for $i = 0, \ldots, 7$. Define $h : \mathbb{O}(q) \longrightarrow \mathbb{O}(q)$ by

$$h(\sum_{i=0}^{7} a_i e_i) = \sum_{i=0}^{7} a_i g(e_i),$$

where a_i are coefficients from $GF(q)$, for $i = 0, \ldots, 7$. Clearly, h is linear. We claim that h is multiplicative.

Using the linearity of h and the multiplicativity of g, we can write

$$\begin{aligned} h(\sum_i a_i e_i \cdot \sum_j b_j e_j) &= h(\sum_{i,j} a_i b_j e_i e_j) \\ &= \sum_{i,j} a_i b_j h(\sum_k \gamma_{ijk} e_k) = \sum_{i,j} a_i b_j \sum_k \gamma_{ijk} g(e_k), \end{aligned}$$

and

$$\begin{aligned} h(\sum_i a_i e_i) \cdot h(\sum_j b_j e_j) &= \sum_i a_i g(e_i) \sum_j b_j g(e_j) \\ &= \sum_{i,j} a_i b_j g(e_i) g(e_j) = \sum_{i,j} a_i b_j g(\sum_k \gamma_{ijk} e_k). \end{aligned}$$

Thus h is multiplicative if and only if

$$\sum_k \gamma_{ijk} g(e_k) = g(\sum_k \gamma_{ijk} e_k) \tag{6.1}$$

holds for every i, j.

Trivially, $g(e) = e$. Then $g(-e) = -e$, because $\{e, -e\}$ is the center of $M(q)$. (We have to use this argument, since we do not assume anything about the linearity of g.) For every i, j, only one out of the 8 structural constants γ_{ijk}, $0 \leq k \leq 7$, is nonzero, and it is equal to ± 1. Therefore (6.1) is satisfied, and h is multiplicative.

By the construction, h coincides with g on B. However, we do not know whether h bijects, and whether it is an extension of g. The fact that $h \restriction B = g \restriction B$ does not guarantee that $h \restriction M(q) = g$, since B does not need to generate $M(q)$ by multiplication. Interestingly enough, it seems to never be the case! The key to answering these questions is to look at the additive properties of g (cf. Section 6.2). Apparently, h bijects once we prove that $h \restriction M(q) = g$.

6.1.2 Multiplication versus Orthogonality

Perhaps the single most important feature of composition algebras is the existence of the minimal equation 2.11. It can be used to establish a beautiful relation between norms of elements in $\mathbb{O}(q)$ and their multiplicative orders.

Lemma 6.1 *Let C be a composition algebra, x, $y \in C$. Then*

$$N(xy, y) = N(x, e)N(y). \tag{6.2}$$

When $N(y) \neq 0$, we have

$$(xy^{-1})^2 - N(x, y)N(y)xy^{-1} + N(xy^{-1})e = 0. \tag{6.3}$$

In particular,

$$(xy^{-1})^2 - N(x, y)xy^{-1} + e = 0 \tag{6.4}$$

whenever $N(x) = N(y) = 1$. In such a case, $(xy^{-1})^2 = -e$ if and only if $N(x, y) = 0$.

Proof. We have $N(xy, y) = N(xy + y) - N(x)N(y) - N(y)$, and $N(xy + y) = N(x + e)N(y) = (N(x, e) + N(x) + N(e))N(y) = N(x, e)N(y) + N(x)N(y) + N(y)$. Equation (6.2) follows.

Substitute xy^{-1} for x into (6.2) to obtain $N(x, y) = N(xy^{-1}, e)N(y)$. The minimal equation

$$(xy^{-1})^2 - N(xy^{-1}, e)xy^{-1} + N(xy^{-1})e = 0$$

for xy^{-1} can then be written as (6.3), provided $N(y) \neq 0$. The rest is easy. □

Lemma 6.2 *Let C be a division composition algebra or $C = \mathbb{O}(q)$. Assume that x, $y \in C$ satisfy $N(x) = N(y) = 1$, $x \neq y$. The following conditions are equivalent:*

(i) $|xy^{-1}| = 3$,

(ii) $(xy^{-1})^2 + xy^{-1} + e = 0$,

(iii) $N(x, y) = -1$,

(iv) $N(x + y) = 1$.

Proof. The equivalence of (ii) and (iii) follows from the uniqueness of the minimal equation (2.11) and from (6.4). Condition (iii) is equivalent to (iv) since $N(x) = N(y) = 1$. It suffices to prove the equivalence of (i) and (ii).

As $(a^3 - e) = (a - e)(a^2 + a + e)$, there is nothing to prove when C has no zero divisors. The implication (ii) $\Rightarrow$ (i) is obviously true in any (composition) algebra. Let us prove (i) $\Rightarrow$ (ii).

Assume that $C = \mathbb{O}(q)$, $|xy^{-1}| = 3$, $x \neq y$, and

$$x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}, \quad y = \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix}.$$

We prove that $N(x + y) = 1$. Direct computation yields $N(x + y) = 2 + r + s$, where $r = ad - \alpha \cdot \delta$, $s = bc - \beta \cdot \gamma$. Also,

$$xy^{-1} = \begin{pmatrix} r & \varepsilon \\ \varphi & s \end{pmatrix}$$

for some ε, $\varphi \in k^3$. Since $(xy^{-1})^3 = e$, we have either ($(\varepsilon, \varphi) = (0, 0)$, $s = r^{-1}$, and $r^3 = 1$), or ($(\varepsilon, \varphi) \neq (0, 0)$, and $s = -1 - r$), by Lemma 3.8. If the latter is true, we immediately get $N(x + y) = 1$. Assume the former is true. Then $r + s = r + r^{-1}$. Also, $r^3 = 1$ implies $r = 1$ or $r^2 + r + 1 = 0$. But $r = 1$ leads to $x = y$, a contradiction. Therefore $r^2 + r + 1 = 0$, i.e., $r + r^{-1} = -1$, and we get $N(x + y) = 1$ again. □

There is a strong bound between the additive and multiplicative structures in composition algebras.

Lemma 6.3 *Let C, x, and y be as in Lemma* 6.2. *Then $N(x + y) = 1$ if and only if $x + y = -xy^{-1}x$.*

Proof. The indirect implication is trivial. Assume that $N(x + y) = 1$. Then $(xy^{-1})^2 + xy^{-1} + e = 0$, and $(xy^{-1})^3 = e$. Thus $yx^{-1} = (xy^{-1})^2 = -xy^{-1} - e$. Multiplying this equality on the right by x yields $y = -xy^{-1}x - x$. □

6.1.3 A Construction using Doubling Triples

Allow us to offer another construction of a possible extension of g. The reader who wishes to arrive at the main results as fast as possible can skip this subsection.

For every q, we find three elements a, b, $c \in M(q)$ such that $e_0 = e$, $e_1 = a$, $e_2 = b$, $e_3 = ab$, $e_4 = c$, $e_5 = ac$, $e_6 = bc$, $e_7 = ab \cdot c$ is a (vector space) basis for $\mathbb{O}(q)$. Using this basis, we define $h : \mathbb{O}(q) \longrightarrow \mathbb{O}(q)$ that agrees with g on a, b, c. We prove that h is linear, and that h is multiplicative if and only if g satisfies a weak form of orthogonality. We then proceed to prove that g satisfies this weak orthogonality. As before, it will not be clear, however, whether h extends g, i.e., whether $h \restriction M(q) = g \restriction M(q)$.

We have seen in Subsection 2.3.1 how composition algebras can be constructed by doubling. In fact, every composition algebra of dimension 4 and 8 can be constructed by doubling. Proposition 6.4 [41, Proposition 1.5.1] and Lemma 6.5 [41, Lemma 1.6.1] tell us how to do it.

Proposition 6.4 *Let C be a composition algebra and D a finite-dimensional composition subalgebra, $D \neq C$. If a is chosen in $D^\perp$ with $N(a) \neq 0$, then $D_1 = D \oplus Da$ is a composition subalgebra of C. Product, norm and conjugation on D_1 are given by the formulas*

$$\begin{aligned}(x + ya)(u + va) &= (xu - N(a)\overline{v}y) + (vx + y\overline{u})a,\\ N(x + ya) &= N(x) + N(a)N(y),\\ \overline{x + ya} &= \overline{x} - ya,\end{aligned}$$

where x, y, u, v are elements of D.

Lemma 6.5 *Let C be a composition algebra over a field k of characteristic 2. If $a \in C$ with $N(a, e) \neq 0$, the linear space $ke \oplus ka$ is a two-dimensional composition subalgebra of C.*

Lemma 6.5 is needed because ke is a composition subalgebra of C if and only if the characteristic of k is not 2. (Remember, we require the norm N of any composition algebra to be non-degenerate.)

So, when the characteristic is even, one can construct C by taking a with $N(a) \neq 0$ and $N(a, e) \neq 0$, thus obtaining the two-dimensional algebra $A = ke \oplus ka$, then taking $b \in A^\perp$ with $N(b) \neq 0$, thus obtaining the four-dimensional algebra $B = A \oplus Ab$, and than taking $c \in B^\perp$ with $N(c) \neq 0$ to construct $C = B \oplus Bc$. When the characteristic is odd, it suffices to take $a \in e^\perp$, $b \in A^\perp$, $c \in B^\perp$ with nonzero norms. We will call such a triple (a, b, c) a *doubling triple*. Additional conditions are usually imposed on doubling triples. For instance, (a, b, c) is called a *basic triple* in [41] if the basis $X = \{e, a, b, ab, c, ac, bc, ab \cdot c\}$ of C has the following properties:

- if the characteristic is odd, X is an orthogonal basis and $N(a)N(b)N(c) \neq 0$,
- if the characteristic is even, $N(e, a) = 1$, $N(b, ab) = N(b)$, $N(c, ac) = N(c)$, $N(bc, ab \cdot c) = N(b)N(c)$, all other inner products between distinct basis vectors are zero, and $N(a)N(b)N(c) \neq 0$.

Basic triples exist in every octonion algebra (cf. [41, Corollary 1.6.3]). Our requirement on (a, b, c) is different. We want to find a doubling triple (a, b, c) satisfying

$$N(a) = N(b) = N(c) = 1. \tag{6.5}$$

This is not always possible, nevertheless, when $C = \mathbb{O}(q)$, it can be done, as we have already seen (recall the basis B). However, we do not wish to use the compact construction of $\mathbb{O}(q)$. Instead, we will construct an explicit doubling triple using the original Zorn's construction.

From now on, we will always assume that $N(a, e) = -1$ when q is even and (a, b, c) is a doubling triple.

Before we start, note that two elements a, b of unit norm are orthogonal if and only if $N(a + b) = 2$, since $N(a, b) = N(a + b) - N(a) - N(b)$.

Lemma 6.6 *In* $\mathbb{O}(q)$,

$$e^\perp \cap M(q) = \left\{ \begin{pmatrix} a & \alpha \\ \beta & -a \end{pmatrix};\ a \in k,\ \alpha,\ \beta \in k^3 \right\} \cap M(q).$$

Proof. Let

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

be an element of $M(q)$. Then $x \perp e$ if and only if

$$N(x+e) = N \begin{pmatrix} 1+a & \alpha \\ \beta & 1+b \end{pmatrix} = 1 + a + b + ab - \alpha \cdot \beta = 2 + a + b$$

equals 2, which happens if and only if $a + b = 0$. □

Proposition 6.7 *If* q *is even, then*

$$a = \begin{pmatrix} 0 & e_1 \\ e_1 & 1 \end{pmatrix},\ b = \begin{pmatrix} 0 & e_2 \\ e_2 & 0 \end{pmatrix},\ c = \begin{pmatrix} 0 & e_3 \\ e_3 & 0 \end{pmatrix}$$

is a doubling triple for $\mathbb{O}(q)$ *such that* $N(a) = N(b) = N(c) = 1$.

Proof. Check that $N(a, e) = -1$. By Lemma 6.6, $a \notin e^\perp$, and $b,\ c \in e^\perp$. Also, $N(a+b) = N(a+c) = N(b+c) = 0$, so $b,\ c \in a^\perp$, and $c \in b^\perp$. It remains to prove that c is orthogonal to ab. Since

$$ab = \begin{pmatrix} 0 & e_3 \\ e_2 + e_3 & 0 \end{pmatrix},$$

we have $N(c + ab) = 0$, and we are done. □

The situation in odd characteristic is more complicated. Since a, b, c must belong to $e^\perp$, we can assume that

$$a = \begin{pmatrix} x & \alpha_1 \\ \alpha_2 & -x \end{pmatrix},\ b = \begin{pmatrix} y & \beta_1 \\ \beta_2 & -y \end{pmatrix},\ c = \begin{pmatrix} z & \gamma_1 \\ \gamma_2 & -z \end{pmatrix}, \tag{6.6}$$

for some $x,\ y,\ z \in k$, $\alpha_1,\ \alpha_2,\ \beta_1,\ \beta_2,\ \gamma_1,\ \gamma_2 \in k^3$, by Lemma 6.6.

Lemma 6.8 *Let* $a,\ b$ *be as in* (6.6). *Then* $N(a) = 1$ *if and only if* $\alpha_1 \cdot \alpha_2 = x^2 - 1$. *If both* $a,\ b$ *belong to* $M(q)$, *then* $a \perp b$ *if and only if* $\alpha_1 \cdot \beta_2 + \beta_1 \cdot \alpha_2 = -2xy$.

Proof. By definition, $N(a) = -x^2 - \alpha_1 \cdot \alpha_2$. Assume that $a,\ b \in M(q)$. Then $N(a+b) = -x^2 - 2xy - y^2 - \alpha_1 \cdot \alpha_2 - \alpha_1 \cdot \beta_2 - \beta_1 \cdot \alpha_2 - \beta_1 \cdot \beta_2 = 2 - 2xy - \alpha_1 \cdot \beta_2 - \beta_1 \cdot \alpha_2$. We have already observed that $a \perp b$ if and only if $N(a+b) = 2$. □

A field element $\rho \in k$ is said to be a *square* if there is $\sigma \in k$ such that $\rho = \sigma^2$. The following number theoretical result proves to be quite useful:

Lemma 6.9 *If $q = 2$ or q is odd then every element of $k = GF(q)$ is a sum of two squares.*

Proof. The lemma is obviously true when $q = 2$. Assume that $q = 2n + 1$ is odd, and pick $\rho \in k$. If ρ is a square, there is nothing to prove, so we may assume that ρ is not a square. In particular, $\rho \neq 0$. Let S be the set of the n squares contained in $k \setminus \{0, \rho\}$. The set $S' = \{\rho - s;\ s \in S\}$ is contained in $k \setminus \{0, \rho\}$, since $\rho - s = 0$ leads to $\rho = s \in S$, and $\rho - s = \rho$ to $s = 0$. But $|S| + |S'| = 2n > 2n - 1 = |k \setminus \{0, \rho\}|$ and, by the pigeon hole principle, there is $r \in S \cap S'$. Then $r = \rho - s$ for some $s \in S$, and $\rho = r + s$ follows. □

Remark 6.10 *As Clifford Bergman pointed out to me, Lemma* 6.9 *cannot be extended to include the case $q = 2^n$, $n > 1$. In even characteristic $(r + s)^2 = r^2 + s^2$, so an element of $GF(2^n)$ is a sum of two squares if and only if it is a square.*

Proposition 6.11 *If q is odd, there is a doubling triple (a, b, c) in $\mathbb{O}(q)$ such that $N(a) = N(b) = N(c) = 1$.*

Proof. Let $\rho \in k$ be such that $-1 - \rho^2$ is a square. Such an element exists by Lemma 6.9, because -1 is a sum of two squares. Put $\alpha_1 = e_1$, $\alpha_2 = -e_1$, $\beta_1 = e_2$, $\beta_2 = -e_2$, $\gamma_1 = \rho e_1 = \gamma_2$, $x = 0$, $y = 0$, and let z be a square root of $-1 - \rho^2$. Define a, b, c as in (6.6), and observe that $1 = N(a) = N(b) = N(c) = -(-1 - \rho^2) - \rho^2$.

By Lemma 6.8, $a \perp b$, $a \perp c$, and $b \perp c$. It remains to verify that $ab \perp c$. Since

$$ab = \begin{pmatrix} 0 & e_1 \\ -e_1 & 0 \end{pmatrix} \begin{pmatrix} 0 & e_2 \\ -e_2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -e_3 \\ e_3 & 0 \end{pmatrix},$$

we have

$$ab + c = \begin{pmatrix} z & (\rho, 0, -1) \\ (\rho, 0, 1) & -z \end{pmatrix},$$

and therefore $N(ab + c) = -(-1 - \rho^2) - \rho^2 + 1 = 2$. □

We now embark on the construction of h—a possible extension of $g \in \mathrm{Aut}(M(q))$.

Proposition 6.12 *Let (a, b, c), (a', b', c') be two doubling triples of a composition algebra C. Then there is an automorphisms of C mapping (a, b, c) onto (a', b', c') if and only if $N(x) = N(x')$, for $x = a, b, c$.*

Proof. The necessity is obvious since every automorphism is an isometry. Let us proof the sufficiency. Let $A = ke \oplus ka$, $B = A \oplus Ab$, $C = B \oplus Bc$, and define $\psi_X : X \longrightarrow X' = \psi_X(X)$ (for $X = A, B, C$) by

$$\begin{aligned} \psi_A(x + ya) &= x + ya', && \text{for } x, y \in k, \\ \psi_B(x + yb) &= \psi_A(x) + \psi_A(y)b', && \text{for } x, y \in A, \\ \psi_C(x + yc) &= \psi_B(x) + \psi_B(y)c', && \text{for } x, y \in B. \end{aligned}$$

We claim that $\psi_X : X \longrightarrow X'$ is an isomorphism. In particular, $\psi_X(\overline{z}) = \overline{\psi_X(z)}$ for every $z \in X$. The case $X = A$ is slightly different from $X = B, C$, because ke does not need to be a composition subalgebra of C, nevertheless the idea is the same.

Every ψ_X is linear by definition. If we prove that ψ_X is multiplicative then ψ_C will automatically be an automorphism, since both (a, b, c) and (a', b', c') give rise to a basis for C.

Let $X = A$. Since $N(a) = N(a')$, the minimal equations for a and a' have the same coefficients (we have $N(a, e) = N(a', e)$ because (a, b, c), (a', b', c') are doubling triples). Routine computation shows that

$$\psi_A(x + ya)\psi_A(u + va) = \psi_A((x + ya)(u + va))$$

for every $x, y, u, v \in k$. Thus ψ_A is an isomorphism.

Let $X = B$. The four-dimensional algebra B is constructed from A by doubling. Therefore, the product on B is defined by

$$(x + yb)(u + vb) = (xu - \overline{v}y) + (vx + y\overline{u})b,$$

for $x, y, u, v \in A$. Similarly, the product on B' is given by

$$(x + yb')(u + vb') = (xu - \overline{v}y) + (vx + y\overline{u})b',$$

for $x, y, u, v \in A'$. One routinely checks that ψ_B is multiplicative, using the fact that the coefficients of the minimal equations for b and b' are the same, and the fact that ψ_A is an isomorphism.

The case $X = C$ is analogous to $X = B$. □

Proposition 6.12 leads us to the following definition. Let (a, b, c) be a doubling triple for $\mathbb{O}(q)$ such that $N(a) = N(b) = N(c) = 1$. We say that $g \in \mathrm{Aut}(M(q))$ is *weakly orthogonal* on (a, b, c) if $(g(a), g(b), g(c))$ is a doubling triple for $\mathbb{O}(q)$, too.

Let $a' = g(a)$, $b' = g(b)$, $c' = g(c)$, and construct ψ_C as in Proposition 6.12. As $N(g(x)) = N(x)$ for $x = a, b, c$, we see that $\psi_C \in \mathrm{Aut}(\mathbb{O}(q))$ if and only if g is weakly orthogonal on (a, b, c).

Corollary 6.13 *Let $g \in \mathrm{Aut}(M(q))$, and let (a, b, c) be a doubling triple for $\mathbb{O}(q)$ with $N(a) = N(b) = N(c) = 1$. Then g is weakly orthogonal on (a, b, c).*

Proof. Since (a, b, c) is a doubling triple, we have $N(b, e) = N(c, e) = N(a, b) = N(a, c) = N(b, c) = 0$. When q is odd, we also have $N(a, e) = 0$. When q is even, we have $N(a, e) = 1$. Be Lemmas 6.1 and 6.2, this is equivalent to $b^2 = c^2 = (ab^{-1})^2 = (ac^{-1})^2 = (bc^{-1})^2 = -e$, and $a^2 = -e$ (resp. $|a| = 3$) if q is odd (resp. even). Because $g \in \mathrm{Aut}(M(q))$, we have $g(b)^2 = g(c)^2 = (g(a)g(b)^{-1})^2 = (g(a)g(c)^{-1})^2 = (g(b)g(c)^{-1})^2 = -e$, and $g(a)^2 = -e$ (resp. $|g(a)| = 3$) if q is odd (resp. even). Then, in turn, $N(g(b), e) = N(g(c), e) = N(g(a), g(b)) = N(g(a), g(c)) = N(g(b), g(c)) = 0$, and $N(g(a), e) = 0$ (resp. $N(g(a), e) = 1$) if q is odd (resp. even). Thus $(g(a), g(b), g(c))$ is a doubling triple (with $N(g(a)) = N(g(b)) = N(g(c)) = 1$). □

In particular, the mapping $\psi = \psi_{\mathbb{O}(q)}$ constructed from g and (a, b, c) is an automorphism of $\mathbb{O}(q)$ satisfying $\psi(x) = g(x)$, for $x = a, b, c$. Thus ψ agrees with g on a basis for $\mathbb{O}(q)$, and it is therefore the only possible candidate for the extension of g into an automorphism of $\mathbb{O}(q)$.

6.2 The Automorphism Group of $M^*(2)$

Finally, we are going to investigate the additive properties of $g \in \mathrm{Aut}(M(q))$.

Proposition 6.14 *Let C be a division composition algebra or $C = \mathbb{O}(q)$, and let $M \subseteq C$ be the set of all elements of norm 1. Assume that $x, y \in M$ are such that $x + y \in M$. Then $g(x + y) = g(x) + g(y)$ for every $g \in \mathrm{Aut}(M)$.*

Proof. If $x = y$, we have $1 = N(x + y) = N(2x) = 4N(x) = 4$. Therefore the characteristic is 3, and $g(x) + g(x) = -g(x) = g(-x) = g(x + x)$.

Assume that $x \neq y$. By Lemma 6.2, $|xy^{-1}| = 3$, and so $|g(x)g(y)^{-1}| = |g(xy^{-1})| = 3$ as well. Then $N(g(x) + g(y)) = 1$, again by Lemma 6.2. Consequently, we use Lemma 6.3 twice to obtain $g(x) + g(y) = -g(x)g(y)^{-1}g(x) = g(-xy^{-1}x) = g(x + y)$. □

We now specialize to $q = 2$, and proceed to prove by the induction on the number of summands that

$$g(\sum_{i=1}^{n} x_i) = \sum_{i=1}^{n} g(x_i)$$

for every $g \in \mathrm{Aut}(M^*(2))$ and $x_1, \ldots, x_n \in M^*(2)$ such that $x_1 + \cdots + x_n \in M^*(2)$.

Lemma 6.15 *Suppose that $x, y \in M^*(2)$, $x \neq y$, are such that none of $x+e$, $y+e$, $x+y$ belongs to $M^*(2)$. Then $\langle x, y\rangle \cong V_4$, and there are $a, b \in M^*(2)$ such that $a + b = e$, and $x + a$, $y + b \in M^*(2)$.*

Proof. We have $N(x + e) = 0$, i.e., $N(x, e) = 0 - 1 - 1 = 0$. Then, by Lemma 6.1, $x^2 = (xe^{-1})^2 = -e = e$. Similarly, $y^2 = (xy^{-1})^2 = e$.

Since $\langle x, y\rangle \cong V_4$, we may assume that $(x, y) = (x_0, u_1)$ or $(x, y) = (x_0, u_2)$, where x_0, u_1, u_2 are as in Lemma 5.18. When $(x, y) = (x_0, u_1)$, let $a = (((011, 010)))_1$, else put $a = (((110, 100)))_1$. In both cases, let $b = e - a$, and verify that $x + a$, $y + b \in M^*(2)$. □

Proposition 6.16 *Let $x_1, \ldots, x_n \in M^*(2)$ be such that $x = \sum_{i=1}^{n} x_i$ belongs to $M^*(2)$. Then*

$$g(\sum_{i=1}^{n} x_i) = \sum_{i=1}^{n} g(x_i).$$

Proof. The case $n = 1$ is trivial, and $n = 2$ is just Proposition 6.14. Assume that $n \geq 3$ and that the Proposition holds for all $m < n$. We can assume that at least two summands x_i are different, say $x_{n-2} \neq x_{n-1}$. Since $g(xx_n^{-1}) = g(x)g(x_n)^{-1}$, we can furthermore assume that $x_n = e$. When at least one of $x_{n-2} + e$, $x_{n-1} + e$, $x_{n-2} + x_{n-1}$ belongs to $M^*(2)$, we are done by the induction hypothesis. Otherwise, Lemma 6.15 applies, and there are $a, b \in M^*(2)$ such that $a+x_{n-2}$, $b+x_{n-1} \in M^*(2)$, and $a+b = e$. Therefore,

$$\begin{aligned} g(x) &= g(x_1 + \cdots + x_{n-3} + (x_{n-2} + a) + (x_{n-1} + b)) \\ &= g(x_1) + \cdots + g(x_{n-3}) + g(x_{n-2} + a) + g(x_{n-1} + b) \\ &= g(x_1) + \cdots + g(x_{n-1}) + g(a) + g(b) \\ &= g(x_1) + \cdots + g(x_{n-1}) + g(a + b), \end{aligned}$$

and we are through. □

Theorem 6.17 (Automorphism Group of $M^*(2)$) *Every automorphism of $M^*(2)$ can be uniquely extended into an automorphism of $\mathbb{O}(2)$. In particular,* $\mathrm{Aut}(M^*(2))$ *is isomorphic to $G_2(2)$.*

Proof. Pick $g \in \mathrm{Aut}(M^*(2))$. Whichever of the two constructions of h do you prefer and use, let $e_0, \ldots, e_7$ be the basis on which g and $h \in \mathrm{Aut}(\mathbb{O}(q))$ coincide. Every element of $M^*(2)$ is a sum of some of the basis elements $e_0, \ldots, e_7$. Hence, by Proposition 6.16, g and h coincide of $M^*(2)$.

This extension is unique, and thus $\mathrm{Aut}(M^*(2)) = \mathrm{Aut}(\mathbb{O}(2))$. Now, $\mathrm{Aut}(\mathbb{O}(2))$ is isomorphic to $G_2(2)$, by Theorem 3.1. □

6.2.1 Combinatorial Proof of $\mathrm{Aut}(M^*(2)) = G_2(2)$

We will establish the equality $\mathrm{Aut}(M^*(2)) = G_2(2)$ again, purely on the grounds of cardinality. The proof is direct, but requires deep knowledge of the lattice of subloops of $M^*(2)$.

Lemma 6.18 $|\mathrm{Aut}(M^*(2))| \leq 12,096$.

Proof. Recall the constants $\Gamma_n(A, B)$ from Section 5.4. Since $x = \Gamma_2(\{e\}, C_2) = 63$, $y = \Gamma_2(C_2, V_4^-) = 24$, $z = \Gamma_2(V_4^-, M^*(2)) = 8$, there are elements $a, b, c \in M^*(2)$ such that $\langle a \rangle \in O_{C_2}$, $\langle a, b \rangle \in O_{V_4^-}$, $\langle a, b, c \rangle = M^*(2)$.

For $S \subseteq M^*(2)$, denote by $G_S = \{f \in \mathrm{Aut}(M^*(2));\ f(s) = s,\ s \in S\}$ the pointwise stabilizer of S, and, for $x \in M^*(2)$, let $O_{S,x}$ be the orbit of x under the action of G_S. We have

$$|\mathrm{Aut}(M^*(2))| = |O_{e,a}| \cdot |G_a| = |O_{e,a}| \cdot |O_{a,b}| \cdot |G_{\langle a,b \rangle}| = |O_{e,a}| \cdot |O_{a,b}| \cdot |O_{\langle a,b \rangle, c}|,$$

since $\langle a, b, c \rangle = M^*(2)$. Now, $|O_{e,a}| \leq x$, $|O_{a,b}| \leq y$, and $|O_{\langle a,b \rangle, c}| \leq z$. Hence $|\mathrm{Aut}(M^*(2))| \leq 63 \cdot 24 \cdot 8 = 12,096$. □

Corollary 6.19 $\mathrm{Aut}(M^*(2)) \cong G_2(2)$.

Proof. By Lemma 3.4 and Theorem 3.1, $\mathrm{Aut}(M^*(2)) \geq G_2(2)$. But $|G_2(2)| = 12,096$ (see [13]). □

Chapter 7

Subloops

The lattice of subloops of $M^*(q)$ is very complicated. We elucidate a small, but important portion of it.

7.1 Subgroups of type $(3, 3 \mid 3, p)$

We have shown in Theorem 2.8, that every $M^*(q)$ is 3-generated, and if $q \neq 9$ is an odd prime power, or if $q = 2$, then the generators can be chosen as

$$g_1 = \begin{pmatrix} 1 & e_1 \\ 0 & 1 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & e_2 \\ 0 & 1 \end{pmatrix}, \quad g_3 = \begin{pmatrix} 0 & ue_3 \\ -u^{-1}e_3 & 1 \end{pmatrix}, \tag{7.1}$$

where u is a primitive element of $k = GF(q)$. In particular, note that g_1, g_2 and g_3 generate $M^*(p)$ for every prime p. We find it more convenient to use another set of generators.

Proposition 7.1 *Let $q \neq 9$ be an odd prime power or $q = 2$. Then $M^*(q)$ is generated by three elements of order three.*

Proof. Let us introduce

$$\begin{aligned} g_4 = g_3 g_1 &= \begin{pmatrix} 0 & (0,0,u) \\ (0,u,-u^{-1}) & 1 \end{pmatrix}, \\ g_5 = g_3 g_2 &= \begin{pmatrix} 0 & (0,0,u) \\ (-u,0,-u^{-1}) & 1 \end{pmatrix}. \end{aligned}$$

It follows from (7.1) that $M^*(q)$ is generated by g_3, g_4, and g_5. These elements are of order 3, by Lemma 3.8. □

The groups $\langle g_3, g_4 \rangle$, $\langle g_3, g_5 \rangle$ and $\langle g_4, g_5 \rangle$ play therefore a prominent role in the subloop lattice. As we prove in Subsection 7.1.2, each of them is isomorphic to the group $(3, 3 \mid 3, p)$, defined below.

7.1.1 The Abstract Groups $(3, 3 \mid 3, p)$

The two-generated abstract groups $(l, m \mid n, k)$ defined by presentations

$$(l, m \mid n, k) = \langle x, y \mid x^l = y^m = (xy)^n = (x^{-1}y)^k \rangle \tag{7.2}$$

were first studied by Edington [21], for some small values of l, m, n and k. The notation we use was devised by Coxeter [16] and Moser [17], and has a deeper meaning that we will not discuss here. From now on, we will always refer to presentation (7.2) when speaking about $(l, m \mid n, k)$.

The starting point for our discussion is Theorem 7.2, due to Edington (Theorem IV, and pages 208–210 [21]. Notice that there is a typo concerning the order of $(3, 3 \mid 3, n)$, and a misprint claiming that $(3, 3 \mid 3, 3)$ is isomorphic to A_4.). For the convenience of the reader, we give a short, modern proof.

Theorem 7.2 (Edington) *The group $G = (3, 3 \mid 3, n)$ exists for every $n \geq 1$, is of order $3n^2$, and is non-abelian when $n > 1$. It contains a normal subgroup $H = \langle x^2y, xy^2 \rangle \cong C_n \times C_n$. In particular, $G \cong C_3$ when $n = 1$, $G \cong A_4$ when $n = 2$, and G is the unique non-abelian group of order 27 and exponent 3 when $n = 3$.*

Proof. Verify that $(3, 3 \mid 3, 1)$ is isomorphic to C_3. Let $n > 1$. Since $x(x^2y)x^{-1} = yx^{-1} = y(x^2u)y^{-1} \in H$, and $x^{-1}(xy^2)x = y^2x = y^{-1}(xy^2)y \in H$, the subgroup H is normal in G. It is an abelian group of order at most n^2 since $x^2y \cdot xy^2 = x(xy)^2y = x(xy)^{-1}y = xy^2 \cdot x^2y$. Clearly, $G/H \cong C_3$ (enumeration of cosets works fine), and hence $|G| = 3|H| \leq 3n^2$.

Let $N = \langle a \rangle \times \langle b \rangle \cong C_n \times C_n$, and $K = \langle f \rangle \leq \mathrm{Aut}(N)$, where f is defined by $f(a) = a^{-1}b$, $f(b) = a^{-1}$. Let E be the semidirect product of N and K via the natural action of K on N. We claim that E is non-abelian, and isomorphic to $(3, 3 \mid 3, n)$ with generators $x = (1, f)$ and $y = (a, f)$. We have $(a, f)^2 = (af(a), f^2) = (b, f^2)$, $(b, f^2)(1, f) = (b, \mathrm{id})$, and $(1, f)(b, f^2) = (a^{-1}, \mathrm{id})$. Thus E is non-abelian, and generated by $(1, f)$, (a, f). A routine computation shows that $(1, f)^3 = (a, f)^3 = ((1, f)(a, f))^3 = ((1, f)^{-1}(a, f))^n = 1$.

The group E proves that $|G| = 3|H| = 3n^2$. In particular, $H \cong C_n \times C_n$. □

We would like to give a detailed description of the lattice of subgroups of $(3, 3 \mid 3, p)$ in term of generators x and y. From a group-theoretical point of view, the groups are rather boring, nevertheless, the lattice can be nicely visualized. The cases $p = 2$ and $p = 3$ cause troubles, and *we exclude them from our discussion for the time being.*

Lemma 7.3 *Let G and H be defined as before. Then H is the Sylow p-subgroup of G, and contains $p + 1$ subgroups $H(i) = \langle h(i) \rangle$, for $0 \leq i < p$, or $p = \infty$, all isomorphic to C_p. We can take*

$$h(i) = x^2y(xy^2)^i, \text{ for } 0 \leq i < p, \text{ and } h(\infty) = xy^2.$$

There are p^2 Sylow 3-subgroups $G(k, l) = \langle g(k, l) \rangle$, for $0 \leq k, l < p$, all isomorphic to C_3. We can take

$$g(k, l) = (x^2y)^{-k}(xy^2)^{-l}x(x^2y)^k(xy^2)^l.$$

Proof. The subgroup structure of H is obvious. Every element of $G \setminus H$ has order 3, so there are p^2 Sylow 3-subgroups of order 3 in G. The subgroup H acts transitively on the set of Sylow 3-subgroups. (By Sylow theorems, G acts transitively on the copies of C_3. As $|G| = 3p^2$, the stabilizer of each C_3 under this action is isomorphic to C_3. Since p and 3 are relatively prime, no element of H can be found in any stabilizer.) This shows that our list of Sylow 3-subgroups is without repetitions, thus complete. □

For certain values of p (see below), there are no other subgroups in G. For the remaining values of p, there are additional subgroups of order $3p$.

If $K \leq G$ has order $3p$, it contains a unique normal subgroup of order p, say $L \leq H$. Since L is normalized by both K and H, it is normal in G. Then G/L is a non-abelian group of order $3p$, and has therefore p subgroups of order 3. Using the correspondence of lattices, we find p subgroups of order $3p$ containing L (the group K is one of them).

Lemma 7.4 *The group $H(i)$ is normal in G if and only if*

$$i^2 + i + 1 \equiv 0 \pmod{p}. \tag{7.3}$$

If $p \equiv 1 \pmod 3$, there are two solutions to (7.3). For other values of p, there is no solution.

Proof. We have

$$\begin{aligned} x^{-1}h(i)x &= x^{-1}x^2y(xy^2)^i x = xy^2y^2(xy^2)^i x \\ &= (xy^2)(y^2x)^{i+1} = (x^2y)^{-(i+1)}(xy^2). \end{aligned}$$

Thus $x^{-1}h(i)x$ belongs to $H(i)$ if and only if $(x^2y)^{-(i+1)i}(xy^2)^i = (x^2y)(xy^2)^i$, i.e., if and only if i satisfies (7.3). Similarly,

$$\begin{aligned} y^{-1}h(i)y &= y^{-1}x^2y(xy^2)^i y = (y^2x)(xy^2)y^2(xy^2)^i y \\ &= (y^2x)(xy^2)(y^2x)^i = (x^2y)^{-(i+1)}(xy^2). \end{aligned}$$

Then $y^{-1}h(i)y$ belongs to $H(i)$ if and only if i satisfies (7.3).

The quadratic congruence (7.3) has either two solutions or none. Pick $a \in GF(p)^*$, $a \neq e$. Then $a^2 + a + e = 0$ if and only if $a^3 = e$, since $a^3 - e = (a-e)(a^2+a+e)$. This simple argument shows that (7.3) has a solution if and only if 3 divides $p-1 = |GF(p)^*|$. □

Theorem 7.5 (The Lattice of Subgroups of $(3, 3 \mid 3, p)$) *For a prime $p > 3$, let $G = (3, 3 \mid 3, p)$, $H = \langle x^2y, xy^2 \rangle$, $h(i) = x^2y(xy^2)^i$ for $0 \leq i < p$, $h(\infty) = xy^2$, $H(i) = \langle h(i) \rangle$, $g(k, l) = (x^2y)^{-k}(xy^2)^{-l}x(x^2y)^k(xy^2)^l$ for $0 \leq k, l < p$, and $G(k, l) = \langle g(k, l) \rangle$.*

Then $H(\infty) \cong C_p$, $H(i) \cong C_p$, $G(k, l) \cong C_3$ are the minimal subgroups of G, and $H(i) \vee H(j) = H \cong C_p \times C_p$ for every $i \neq j$. When 3 does not divide $p-1$, there are no other subgroups in G. Otherwise, there are additional $2p$ non-abelian maximal subgroups of order $3p$; p for each $1 < i < p$ satisfying $i^3 \equiv 1 \pmod p$. These subgroups can be listed as $K(i, l) = H(i) \vee G(0, l)$, for $0 \leq l < p$. Then $H(i) \vee G(k', l') = K(i, l)$ if and

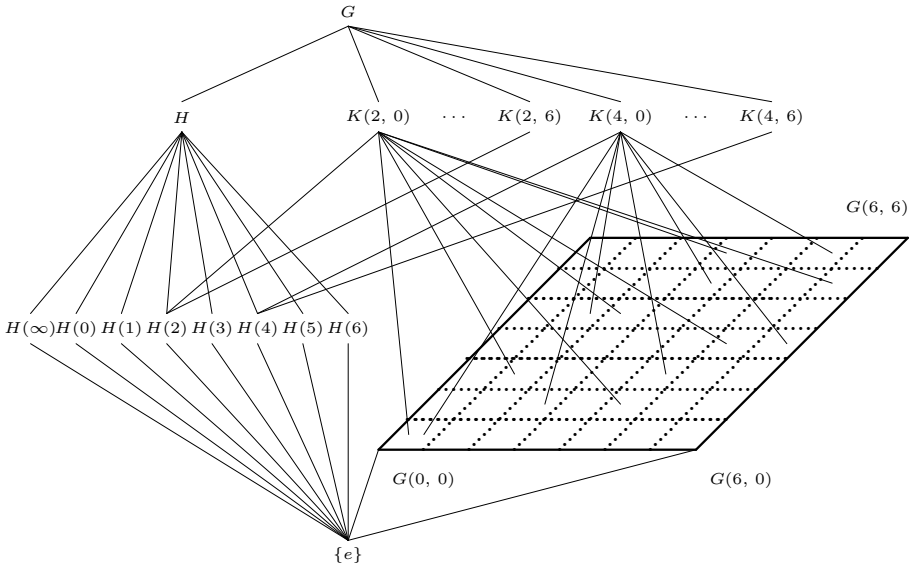

Figure 7.1: The lattice of subgroups of $(3, 3 \mid 3, 7)$

only if $l' - l \equiv ik' \pmod{p}$*; otherwise* $H(i) \vee G(k', l') = G$*. Finally, let* $(k, l) \neq (k', l')$*. Then* $G(k, l) \vee G(k', l') = H(i) \vee G(k, l)$ *if and only if there is* $1 < i < p$ *satisfying* $i^3 \equiv 1 \pmod{p}$ *such that* $l' - l \equiv (k' - k)i \pmod{p}$*; otherwise* $G(k, l) \vee G(k', l') = G$*.*

The group $(3, 3 \mid 3, 2)$ *is isomorphic to* A_4*, the alternating group on* 4 *points, and* $(3, 3 \mid 3, 3)$ *is the unique non-abelian group of order* 27 *and exponent* 3*.*

Proof. Check that $h(i)^{-1}g(k, l)h(i) = g(k+1, l+i)$, and conclude that $H(i) \vee G(k, l) = H(i) \vee G(k', l')$ if and only if $l' - l \equiv i(k' - k) \pmod{p}$. This also implies that, for some $1 < i < p$, $H(i) \vee G(k', l')$ equals $K(i, l)$ if and only if $l' - l \equiv ik' \pmod{p}$ and $i^3 \equiv 1 \pmod{p}$.

Finally, if $S = G(k, l) \vee G(k', l') \neq G$, it contains a unique $H(i) \trianglelefteq G$. Moreover, we have $S = H(i) \vee G(k, l) = H(i) \vee G(k', l')$ solely on the grounds of cardinality, and everything follows. □

We illustrate Theorem 7.5 with $p = 7$. The congruence (7.3) has two solutions, $i = 2$ and $i = 4$. The subgroup lattice of $(3, 3 \mid 3, 7)$ is depicted in the 3D Figure 7.1. The 49 subgroups $G(k, l)$ are represented by a parallelogram that is thought to be in a horizontal position. All lines connecting the subgroups $G(k, l)$ with $K(2, 0)$ and $K(4, 0)$ are drawn. The lines connecting the subgroups $G(k, l)$ with $K(2, j)$, $K(4, j)$, for $1 \leq j < p$, are omitted for the sake of transparency. The best way to add these missing lines is by the means of affine geometry of $GF(p) \times GF(p)$. To determine which groups $G(k, l)$ are connected to the group $K(i, j)$, start at $G(0, j)$ and follow the line with slope i, drawn modulo the parallelogram.

The group A_4 fits the description of Theorem 7.5, too, as can be seen from its lattice

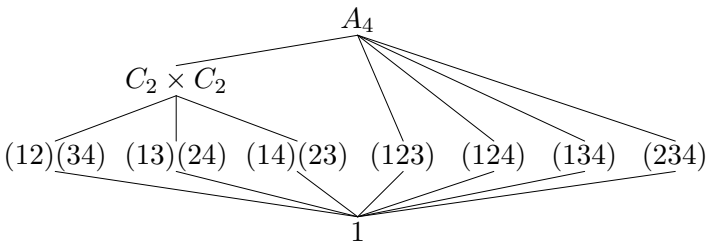

Figure 7.2: The subgroup structure of A_4

of subgroups in Figure 7.2. So does the group $(3, 3 \mid 3, 3)$.

7.1.2 Three Subgroups

We promised to show that each of the subgroups $\langle g_3, g_4\rangle$, $\langle g_3, g_5\rangle$, $\langle g_4, g_5\rangle$ of $M^*(q)$ is isomorphic to $(3, 3 \mid 3, p)$.

Proposition 7.6 *Let g_3, g_4, g_5 be defined as above, $q = 2^r$. Then the three subgroups $\langle g_3, g_4\rangle$, $\langle g_3, g_5\rangle$, $\langle g_4, g_5\rangle$ of $M^*(q)$ are isomorphic to $(3, 3 \mid 3, p)$, if $q \neq 9$ is odd or $q = 2$.*

Proof. We prove that $G_1 = \langle g_3, g_4\rangle \cong (3, 3 \mid 3, p)$; the argument for the other two groups is similar. By Lemma 3.8, we have $g_3^3 = g_4^3 = (g_3g_4)^3 = (g_4g_3)^3 = (g_3^{-1}g_4)^p = (g_3^2g_4)^p = e$. Thus $G_1 \leq (3, 3 \mid 3, p)$. Also, $H_1 = \langle g_3^2g_4, g_3g_4^2\rangle \cong C_p \times C_p$. When $p \neq 3$, we conclude that $|G_1| = 3p^2$, since G_1 contains an element of order 3. When $p = 3$, we check that $g_3 \notin H_1$, and reach the same conclusion. □

We finish this section with a now obvious observation, that in order to describe all subloops of $M^*(q)$, one only has to study the interplay of the isomorphic subgroups $\langle g_3, g_4\rangle$, $\langle g_3, g_5\rangle$, and $\langle g_4, g_5\rangle$.

7.2 Note on Permutation Representation of Quasigroups

The generalization of representation theory from groups to quasigroups was initiated by J. D. H. Smith in [38]. Without recalling the notation, we work out two examples. We rely heavily on the computer computations in GAP.

Example 7.7 *Let $Q = M^*(2)$. We have seen in Chapter 5 that Q contains a maximal subloop P isomorphic to $M_{12}(S_3, 2)$. Since $\mathrm{Aut}(M^*(2))$ acts transitively on the copies of $M_{12}(S_3, 2)$, we do not need to specify P.*

The group $LMlt_Q(P)$ has 648 elements. It acts on Q. There are two orbits of transitivity. One of them contains 12 elements, of course. The other orbit contains

$120 - 12 = 108$ *elements. The transition matrices (see [38]) on* $P \setminus Q$ *have then a quite simple form. Namely,*

$$R_{P\setminus Q}(q) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

if $q \in P$*, and*

$$R_{P\setminus Q}(q) = \begin{pmatrix} 1 & 0 \\ 1/9 & 8/9 \end{pmatrix},$$

if $q \notin P$*. This is not surprising. Whenever there are just two orbits of transitivity, the corresponding transition matrices will be of the form*

$$R_{P\setminus Q}(q) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

if $q \in P$*, and*

$$R_{P\setminus Q}(q) = \begin{pmatrix} 1 & 0 \\ |P|/|Q \setminus P| & (1-|P|)/|Q \setminus P| \end{pmatrix},$$

if $q \notin P$*.*

Example 7.8 *Let again* $Q = M^*(2)$*. This time, pick* P *to be a maximal subloop of type* A_4*. Since* $\mathrm{Aut}(M^*(2))$ *acts transitively on the copies of* A_4*, we do not need to specify* P*.*

Computation reveals that $LMlt_Q(P)$ *has* 9216 *elements, and that there are two orbits of transitivity. Hence, the discussion from Example* 7.7 *applies.*

Chapter 8

Open Problems and Acknowledgement

Some question were answered, many more remain open, yet other came into existence through this work. Let us list some of them now.

1) Does every (finite) Moufang loop have the strong Lagrange property ? The answer is positive if every Paige loop does (see [11]).

2) Is there a finite simple Bol loop that is not Moufang? Assuming all Moufang loops have the strong Lagrange property, there is a non-Moufang finite simple Bol loop if and only if there is a Bol loop that does not have the strong Lagrange property. (*Right*) *Bol loop* is a loop satisfying $(xy \cdot z)y = x(yz \cdot y)$.

3) What are the automorphism groups $\mathrm{Aut}(M^*(q))$ for $q > 2$? In particular, is it true that $\mathrm{Aut}(M^*(q)) = G_2(q)$ for every q? The author suspects that the answer to the latter question is negative.

4) We now know that $\mathrm{Aut}(M^*(q))$ does not have to be simple (since $G_2(2)$ is not). However, $G_2(q)$ is simple for every $q > 2$, and the following question comes inevitably into mind. Is $\mathrm{Aut}(M^*(q))$ simple for every $q > 2$?

5) We have in fact shown that $\mathrm{Aut}(\mathbb{O}(2)) = G_2(2)$ is generated by all permutations (considered as diagonal automorphisms of $\mathbb{O}(2)$), a few conjugations, and by the automorphism ∂. Now, the group $G_2(2)$ is 3-generated. Find three automorphisms of $\mathbb{O}(2)$ generating $\mathrm{Aut}(\mathbb{O}(2))$.

6) In order to disprove the equality $G_2(q) = \mathrm{Aut}(M(q))$, it suffices to find an automorphism $f \in \mathrm{Aut}(M(q))$ and three elements $a, b, c \in M(q)$ such that $a+b+c \in M(q)$ and $f(a) + f(b) + f(c) \neq f(a + b + c)$. Find them, it they exist. Recall that $f(a) + f(b) = f(a + b)$ for every $a, b \in M(q)$ such that $a + b \in M(q)$.

7) Is it always the case that if $B \subseteq M(q)$ is a (vector space) basis for $\mathbb{O}(q)$, then B does not generate $M^*(q)$ by multiplication only? If yes, what does it mean geometrically?

8) Find a simple proof that $(C_2)^4$ is not a subgroup of $M^*(2)$. This will furnish a quick proof of the strong Lagrange property for $M^*(2)$.

9) Find a presentation for every Paige loop, or at least for $M^*(2)$.

10) Is is possible to generalize the presentation from Theorem 4.13 for all loops $M_{2n}(G, 2)$?

11) Is the presentation for $M_{2n}(G, 2)$ found in Theorem 4.13 a minimal presentation? By *minimal presentation* we mean a presentation $\langle X;\ R\rangle$ such that $\langle X;\ S\rangle$ is a bigger algebra than $\langle X;\ R\rangle$ for every proper subset S of R.

12) Are all Sylow 2-subloops of $M_{2n}(G, 2)$ conjugate?

13) Is it possible to generalize the visual description of $M_{2n}(S_3, 2)$ for an infinite class of Moufang loops ?

14) Is there a simple argument proving that the map ψ from Theorem 2.10 is an isomorphism?

15) Show by hand that the incidence structure defined by O_{C_2} and $O_{V_4^+}$ is a generalized hexagon of order 2. What about the other two candidates? A more ambitious goal would be to construct a generalized hexagon of order q based on $M^*(q)$, for every q.

16) Are there three elements $g_1,\ g_2,\ g_3$ such that $\langle g_1,\ g_2,\ g_3\rangle = M^*(q)$ for every q? (I.e., using the Zorn's vector matrix notation, all entries of every g_i must belong to $\{0,\ 1,\ -1\}$.)

17) We have found formulas counting the elements of order 2 and 3 for both $M^*(q)$ and $M(q)$. Extend this result to elements of other orders.

18) The character tables for Paige loops are known, cf. [4]. Are they of some use in the investigation of the subloop structure of $M^*(q)$?

Many people were very helpful during the preparation of this thesis, and I would like to acknowledge their help.

First of all, many thanks to my advisor Jonathan D. H. Smith for his time spent on our (nearly) regular weekly discussions, and for his countless suggestions concerning loops and mathematics in general. Every member of my POS committee commented on the work, especially Clifford Bergman, who pointed me in the correct direction on several occasions.

Orin Chein's classification of small Moufang loops was of major influence on Chapter 5. I thank him for his e-mails concerning the strong Lagrange property and M_k-laws. Also, he brought to my attention the paper [25] by M. L. Merlini Giuliani and César Polcino Milies, where some facts about the subloop structure of $M^*(2) = GLL(F_2)$ are stated without proofs. Briefly, the authors list all subloops of $M^*(2)$, give an example for each isomorphism type, find all maximal subgroups, all maximal subloops (they list E_8 as a possible maximal subloop, although it is not), count the subgroups of order 2 and 3, and give estimates on the Hasse constants $\mathcal{H}_{M^*(2)}(C_2|V_4)$ and $\mathcal{H}_{M^*(2)}(V_4|E_8)$. They also sketch the inclusion between the isomorphism types of subloops in the lattice of subloops of $M^*(2)$. Although I became aware of their paper only after I have finished the work on Chapter 5, I acknowledge that I have later used [25] to confirm my (independent) work.

Gabor Nagy came up with a cunning proof of the fact that $M^*(2)$ is contained in every Paige loop, despite my skepticism in this regard. His comments on the structural constants of the standard real octonion algebra made me rewrite Chapter 6. I must also thank Michael Kinyon for supervising the Loopforum discussion group. It is always inspiring to read about the progress of others, and, yes, I promise I will contribute to the forum more often. More importantly, Michael always seems to know a reference for just what I need. J. D. Phillips invited me on several occasions to present my new results at special sessions he co-organized, and thus made me involved in the loop-theoretical community—I appreciate it very much, particularly because he kept inviting me even after our remarkably unsuccessful bird-watching trip to southern Moravia. Last but not least, I would not be in the States (and thus writing this thesis) if it would not be for Aleš Drápal, my advisor at Charles University in Prague, and my parents. Sincere thanks to all of them.

Appendix A

GAP Libraries

These are some of the GAP 4.1 [22] libraries developed by the author while working on the thesis. All of them, and more, are available electronically at `www.math.iastate.edu/~petr`. All libraries are well documented within the source files.

Representation of Paige Loops in GAP

The finite Zorn vector matrix algebras are implemented in file *paigerep.g*.

```
############################################################################
# REPRESENTATION OF SIMPLE MOUFANG LOOPS, version 1.1
# (set of macros for GAP 4.1)
# written by Petr Vojtechovsky, September 2000
#
# the representation is based on L.Paige: A Class of Simple Moufang Loops
############################################################################

# MATHEMATICAL BACKGROUND
# An element of a simple Moufang loop over field F=GF(q) can be represented as
# a 2x2 matrix whose diagonal entries are elements of F, and whose antidiagonal
# entries are elements of F^3, with "determinant" = 1.
# The operation is written multiplicatively. It does not coincide with the
# usual matrix multiplication. See Paige's article for details.

# DESCRIPTION OF MACROS
# The macros work properly for all Galois fields GF(q). Specify the
# field with function SetFieldSize(q).
# The matrices representing the elements are called "PaigeObj".
# Basic arithmetic operations are defined. The list of methods follows.

# THE LIST OF AUXILIARY FUNCTIONS
# function VectorProduct (x, y)
#   returns the vector product of 3-vectors x and y in the chosen field
# function Det (x)
#   returns the "determinant" of PaigeObj x
# function IsRegularPaige(x)
#   returns TRUE when Det(x)=One(F)
# function SetFieldSize(c)
#   sets the field size to c. c must be a prime power
# function GetFieldSize()
#   returns the field size

q:=2; F:=GF(q);

VectorProduct := function (x, y)
    return [x[2]*y[3]-x[3]*y[2], x[3]*y[1]-x[1]*y[3], x[1]*y[2]-x[2]*y[1]];
```

```
end;

Det := function (x)
    return x![1]*x![4] - x![2]*x![3];
end;

IsRegularPaige := function (x)
    return Det(x)=One(F);
end;

#############################################################################
# DECLARATION PART

F_000:=[Zero(F),Zero(F),Zero(F)];
DeclareCategory("IsPaigeObj",
IsScalar); DeclareCategoryCollections("IsPaigeObj");
DeclareRepresentation("IsPaigeRep", IsPositionalObjectRep, [1, 2, 3, 4]);
DeclareGlobalFunction("PaigeObj");

#############################################################################
# IMPLEMENTATION PART

InstallTrueMethod(IsMultiplicativeElementWithInverse, IsPaigeObj);

InstallGlobalFunction(PaigeObj, function(a,b,c,d)
    return Objectify( NewType( FamilyObj([Zero(F),F_000, F_000,Zero(F)]),
                               IsPaigeObj and IsPaigeRep), [a, b, c, d]);
end);

# neutral element
P_1:=PaigeObj(One(F), F_000, F_000, One(F));

InstallMethod(  PrintObj,
        "for a paige",
        true,
        [ IsPaigeObj and IsPaigeRep],
        0,
        function( x )
            Print("(", x![1], ", ", x![2], ")\n");
            Print("(", x![3], ", ", x![4], ")\n");
end );

InstallMethod(  ViewObj,
        "for a paige",
        true,
        [ IsPaigeObj and IsPaigeRep],
        0,
        function( x )
            Print( "Paige(", x![1], ", ", x![2], ", ",
                     x![3], ", ", x![4], ")");
end);

InstallMethod(  \+,
        "for two paiges",
        IsIdenticalObj,
        [IsPaigeObj and IsPaigeRep, IsPaigeObj and IsPaigeRep],
        0,
        function(A, B)
            return PaigeObj(A![1]+B![1], A![2]+B![2],
                            A![3]+B![3], A![4]+B![4]);
end);

InstallMethod(  \-,
        "for two paiges",
        IsIdenticalObj,
        [IsPaigeObj and IsPaigeRep, IsPaigeObj and IsPaigeRep],
        0,
        function(A, B)
            return PaigeObj(A![1]-B![1], A![2]-B![2],
                            A![3]-B![3], A![4]-B![4]);
end);

InstallMethod(  \*,
        "for two paiges",
```

```
        IsIdenticalObj,
        [IsPaigeObj and IsPaigeRep, IsPaigeObj and IsPaigeRep],
        0,
        function(x, y)
            local a, b, c, d;
            a := x![1]*y![1] + x![2]*y![3];
            b := x![1]*y![2] + x![2]*y![4] - VectorProduct(x![3], y![3]);
            c := x![3]*y![1] + x![4]*y![3] + VectorProduct(x![2], y![2]);
            d := x![3]*y![2] + x![4]*y![4];
        return PaigeObj(a, b, c, d);

end);

InstallMethod(  \=,
        "for two paiges",
        true,
        [IsPaigeObj and IsPaigeRep, IsPaigeObj and IsPaigeRep],
        0,
        function (x, y)
        return (x![1]=y![1] and x![2]=y![2] and x![3]=y![3] and x![4]=y![4])
        or (x![1]=-y![1] and x![2]=-y![2] and x![3]=-y![3] and x![4]=-y![4]);
end);

InstallMethod(  \<, #lexicographical ordering
        "for two paiges",
        true,
        [IsPaigeObj and IsPaigeRep, IsPaigeObj and IsPaigeRep],
        0,
        function (x, y)
        return x![1]<y![1] or (x![1]=y![1] and x![2]<y![2]) or
            (x![1]=y![1] and x![2]=y![2] and x![3]<y![3]) or
            (x![1]=y![1] and x![2]=y![2] and x![3]=y![3] and x![4]<y![4]);
end);

InstallMethod(  OneOp,
        "for a paige",
        true,
        [IsPaigeObj and IsPaigeRep],
        0,
        a -> P_1
);

InstallMethod( InverseOp,
        "for a paige",
        true,
        [IsPaigeObj and IsPaigeRep],
        0,
        a -> PaigeObj(a![4], -a![2], -a![3], a![1])
);

InstallMethod(  \*,
        "for rational and paige",
        true,
        [IsRat, IsPaigeObj and IsPaigeRep],
        0,
        function(x, y) return PaigeObj( x*y![1], x*y![2], x*y![3], x*y![4]);
end);

InstallMethod(  \*,
        "for paige and rational",
        true,
        [IsPaigeObj and IsPaigeRep, IsRat],
        0,
        function(x, y) return PaigeObj( y*x![1], y*x![2], y*x![3], y*x![4]);
end);

InstallMethod(  Order,
            "for paige",
        true,
        [IsPaigeObj and IsPaigeRep],
        0,
        function (x)
            local n, y;
            n:=1; y:=x;
```

```
            while not y=P_1 do
                n:=n+1;
                y:=y*x;
            od;
        return (n);
end);

#changing field size

SetFieldSize := function(c)
    q:=c;
    F:=GF(q);
    P_1:=PaigeObj(One(F),[Zero(F),Zero(F),Zero(F)],
                [Zero(F), Zero(F), Zero(F)], One(F));
end;

GetFieldSize := function()
    return q;
end;
```

File *m2.g* builds the smallest Paige loop $M^*(2)$.

```
##############################################################################
# THE SMALLEST PAIGE LOOP
# (set of macros for GAP 4.1)
# written by Petr Vojtechovsky, September 2000
#
# requires paigerep.g. See paigerep.g for mathematical background.
##############################################################################

f0:=Zero(F);
f1:=One(F);

M2:=Set([]);    #smallest non-associative Moufang loop
M22:=Set([]);   #elements of order 2 in M2
M23:=Set([]);   #elements of order 3 in M2

InitM2:= function()
    local i1, i2, i3, i4, i5, i6, i7, i8, P;
    for i1 in F do for i2 in F do for i3 in F do for i4 in F
      do for i5 in F do for i6 in F do for i7 in F do for i8 in F do
        P:=PaigeObj(i1,[i2,i3,i4],[i5,i6,i7],i8);
        if IsRegularPaige(P) then
            AddSet(M2, P);
            if not i1+i8=f0 then AddSet(M23,P);
                else if not P=P_1 then AddSet(M22,P); fi;
            fi;
        fi;
      od; od; od; od;
    od; od; od; od;
end;

InitM2();
```

Generalized Hexagon of Order Two

Files *genhex.g* and *circuit.g* are used to verify that H introduced in subsection 5.5.2 is a generalized hexagon of order 2. H is constructed in *genhex.g*. It is checked in *circuit.g* that the shortest circuit starting at x_0 has length 6. Since $\mathrm{Aut}(M^*(2))$ acts transitively on the involutions of $M^*(2)$, this means that axiom (iii) of generalized hexagons is satisfied.

```
##############################################################################
# GENERALIZED HEXAGON OF ORDER TWO
# (set of macros for GAP 4.1)
# written by Petr Vojtechovsky, April 2001
##############################################################################
```

```
# requires paigerep.g, m2.g
################################################################################

#MATHEMATICAL BACKGROUND
#See section Generalized Hexagons of my thesis for a definition of a
#generalized hexagon of order q.

#DESCRIPTION OF MACROS
#We construct a generalized hexagon of order two as an incidence structure.
#There are 63 points numbered 1..63, and 63 blocks. The blocks are stored
#in list "block".
#We construct the hexagon in three steps:
#(1) for every involution x we find an automorphism mapping x to x_0
#(2) we identify the three copies of V_4 containing x_0 and belonging to the
#    orbit called V_4^+ in the thesis. We use automorphisms from step (1)
#    to obtain all copies of V_4 in the orbit V_4^+
#(3) using the list of all involutions M22 and the list of the groups in the
#    orbit V_4^+ we construct the incidence structure "block". This strucure
#    turns out to be a generalized hexagon of order 2. We verify this in
#    file circuit.g.
#
#We represent the automorphisms of M^*(2) in a symbolic way as follows:
#Each automorphism is of the form f=[t,F], where t is in [0..4] and F is a list
#of needed data. The meaning of t as is follows:
#   t=0: f is specified point by point, F consists of pairs of elements of
#        M^*(2).
#   t=1: f is a "permutation" as defined in section Diagonal Automorphisms, F
#        contains permuted numbers 1, 2, 3.
#   t=2: f is a conjugation, F contains the element by which we conjugate.
#   t=3: f is a diagonal switch d as described in section Diagonal
#        Automorphisms, F is an empty list
#   t=4: f is a composition of automorphisms, F is the list of factors of f,
#        the first item of F is the automorphism that applies first.

#THE LIST OF FUNCTIONS
#function Weight(w)
#   returns the number of non-zero coordinates of vector w
#function Map(a,f)
#   returns the image of a under f
#function InvertMap(f)
#   returns the inverse mapping to f
#function FindAutomorphism(a)
#   returns an automorphism mapping a to x_0

#SOME GLOBAL VARIABLES
#x_0 : selected involution
#ort : orthonormal basis of GF(2)^3
#V4p : the list of members of the orbit V_4^+
#block: blocks of the generalized hexagon of order 2 on points 1..63
#above: above[i] is the list of blocks containing the involution i

Weight :=function(w)
    local i,j;
    j:=0;
    for i in [1..Length(w)] do if not w[i]=f0 then j:=j+1; fi; od;
    return j;
end;

Map := function(a,f)
    local t, F, g, i;
    t:=f[1]; F:=f[2];
    if t=0 then         #mapping by images
        i:=0;
        repeat  i:=i+1;
        until F[i][1]=a;
        return F[i][2];
    elif t=1 then       #permutation
        return PaigeObj(a![1],[a![2][F[1]],a![2][F[2]],a![2][F[3]]],
                [a![3][F[1]],a![3][F[2]],a![3][F[3]]],a![4]);
    elif t=2 then       #conjugation
        return F[1]^(-1)*a*F[1];
    elif t=3 then       #diagonal switch
        return PaigeObj(a![4],a![3],a![2],a![1]);
    else                #composition
```

```
        for g in F do a:=Map(a,g); od;
        return a;
    fi;
end;

InvertMap := function(f)
    local t,F,G,x;
    t:=f[1]; F:=f[2]; G:=[];
    if t=0 then
        for x in F do Add(G,[x[2],x[1]]); od;
    elif t=1 then
        G:=[Position(F,1), Position(F,2), Position(F,3)];
    elif t=2 then
        G:=[F[1]^(-1)];
    elif t=3 then
        G:=F;
    else
        for x in F do Add(G,InvertMap(x)); od;
        G:=Reversed(G);
    fi;
    return [f[1],G];
end;

x_0:=PaigeObj(f0,[f1,f1,f1],[f1,f1,f1],f0);
ort:=[[f1,f0,f0],[f0,f1,f0],[f0,f0,f1]];

FindAutomorphism := function(a)
    #follows Proposition 5.9
    local F, i, b, r, s, x_1, x_2, x_3, perm;
    F:=[];
    #making sure that a has zeros on the diagonal
    if a![1]=f1 then
        i:=0;
        repeat i:=i+1;
        until (i>3) or (not a![2][i]=a![3][i]);
        if i>3 then     #one of three bad elements: a![2]=a![3], |a![2]|=2
            if a![2][1]=f0 then b:=PaigeObj(f0,[f1,f1,f1],[f0,f1,f0],f0);
                else b:=PaigeObj(f0,[f1,f1,f1],[f1,f0,f0],f0);
            fi;
        else b:=PaigeObj(f0,ort[i],ort[i],f0);
        fi;
        #now <a,b> is isomorphic to S_3. Permute involutions of S_3
        if b=Map(a,[2,[a*b]]) then Add(F,[2,[a*b]]);
            else Add(F,[2,[b*a]]);
        fi;
        a:=b;
    fi;
    #making sure that r>=s
    r:=Weight(a![2]); s:=Weight(a![3]);
    if r<s then
        Add(F,[3,[]]);
        a:=Map(a,[3,[]]);
    fi;
    #last part of Proposition 5.9
    x_1:=PaigeObj(f0,[f1,f0,f0],[f1,f0,f0],f0);
    x_2:=PaigeObj(f0,[f1,f1,f0],[f0,f1,f1],f0);
    x_3:=PaigeObj(f0,[f1,f1,f1],[f0,f0,f1],f0);
    perm:=[[1,[1,2,3]],[1,[1,3,2]],[1,[2,1,3]],
           [1,[2,3,1]],[1,[3,1,2]],[1,[3,2,1]]];
    if (r mod 2=s mod 2) and (not a=x_0) and (not a=x_1) then
        i:=0;
        repeat
            i:=i+1;
            b:=Map(a,perm[i]);
        until b=x_1 or b=x_2 or b=x_3;
        Add(F,perm[i]);
        a:=b;
        #now a=x_1 or <a,x_1> is isomorphic to S_3
        if not a=x_1 then
            if Map(a,[2,[a*x_1]])=x_1 then Add(F,[2,[a*x_1]]);
                else Add(F,[2,[x_1*a]]);
            fi;
            a:=x_1;
        fi;
```

```
    elif not a=x_0 and not a=x_1 then
        if Map(a,[2,[a*x_0]])=x_0 then Add(F,[2,[a*x_0]]);
            else Add(F,[2,[x_0*a]]);
        fi;
        a:=x_0;
    fi;
    if a=x_1 then Add(F,[2,[PaigeObj(f1,[f0,f0,f1],[f1,f0,f1],f0)]]); fi;
    return [4,F];
end;

#Construct all copies of V4^+
V4p:=Set([]);
v:=[PaigeObj(f0,ort[1],ort[1],f0),PaigeObj(f0,ort[2],ort[2],f0),
    PaigeObj(f0,ort[3],ort[3],f0)];
for x in M22 do
    f:=FindAutomorphism(x);
    f:=InvertMap(f);
    for i in [1..3] do
        AddSet(V4p,Set([Map(x_0,f),Map(v[i],f),Map(x_0*v[i],f)]));
    od;
od;

#Construct an abstract incidence structure, generalized hexagon of order 2
block:=[];
for x in V4p do
    Add(block,[Position(M22,x[1]),Position(M22,x[2]),Position(M22,x[3])]);
od;
above:=[];
for i in [1..63] do Add(above,[]); od;
for i in [1..63] do for j in [1..3] do
    Add(above[block[i][j]],i);
od; od;
```

At this moment, we have constructed an incidence structure H. It has blocks

$1,11,42$	$1,18,50$	$1,28,58$	$2,8,46$	$2,17,50$	$2,24,63$
$3,9,42$	$3,16,53$	$3,22,63$	$4,6,46$	$4,14,53$	$4,25,58$
$5,12,38$	$5,22,49$	$5,28,54$	$6,20,62$	$6,21,49$	$7,10,38$
$7,16,57$	$7,18,52$	$8,15,57$	$8,26,54$	$9,20,59$	$9,26,51$
$10,24,55$	$10,25,51$	$11,15,61$	$11,21,55$	$12,14,61$	$12,17,59$
$13,20,37$	$13,24,41$	$13,28,45$	$14,23,41$	$15,19,37$	$16,27,45$
$17,27,43$	$18,23,47$	$19,22,47$	$19,25,43$	$21,27,39$	$23,26,39$
$29,40,41$	$29,48,49$	$29,56,57$	$30,36,37$	$30,48,50$	$30,52,53$
$31,44,45$	$31,48,51$	$31,60,61$	$32,36,38$	$32,40,42$	$32,44,46$
$33,40,43$	$33,52,54$	$33,60,32$	$34,36,39$	$34,56,58$	$34,60,63$
$35,44,47$	$35,52,55$	$35,56,59$			

We proceed to verify that H is a generalized hexagon of order 2.

```
##############################################################################
# CIRCUIT
# (set of macros for GAP 4.1)
# written by Petr Vojtechovsky, April 2001
##############################################################################
# requires genhex.g
##############################################################################

#MATHEMATICAL BACKGROUND
#A circuit is a path in a graph with no repeated edges and only one repeated
#vertex, the starting=terminating vertex.

#DESCRITPION OF MACROS
#We check rather brutally that the shortest circuit consist of 6 points and
#6 edges. We start with a degenerated path consisting of x_0 and keep enlarging
```

```
#it in all possible ways until we reach x_0 again.
#
#Every path is represented as a list [v,e], where v is a list of points
#[v_1,...v_n] and e is a list of blocks (=lines) [e_1,...e_{n-1}]. We always
#have v_i, v_{i+1} in e_i.

#Finding the shortest circuit starting at x_0
posx_0:=Position(M22,x_0);
paths:=[[[posx_0],[]]];
circuit:=false;
length:=0;
repeat
    extpaths:=[];
    for x in paths do                       #path to be extended
        y:=x[1][Length(x[1])];              #last point in the path
        for z in above[y] do                #possible line for extension
            if not z in x[2] then           #good line for extension
                for v in block[z] do        #possible new endpoints
                    if (not v in x[1]) or (v=posx_0 and not v=y) then
                        w:=StructuralCopy(x);
                        Add(w[1],v);
                        Add(w[2],z);
                        Add(extpaths, w);
                        if v=posx_0 then circuit:=true; fi;
                    fi;
                od;
            fi;
        od;
    od;
    length:=length+1;
    paths:=StructuralCopy(extpaths);
until circuit=true;
Print(length);
```

GAP prints 6.

Appendix B

Tables

The following tables can be used to simplify computation. None of them was constructed with aid of computers, and the reader can therefore verify the tables for accuracy easily.

	e	x	y	xy	yx	xyx	u	xu	yu	$(xy)u$	$(yx)u$	$(xyx)u$
e	e	x	y	xy	yx	xyx	u	xu	yu	$(xy)u$	$(yx)u$	$(xyx)u$
x	x	e	xy	y	xyx	yx	xu	u	$(yx)u$	$(xyx)u$	yu	$(xy)u$
y	y	yx	e	xyx	x	xy	yu	$(xy)u$	u	xu	$(xyx)u$	$(yx)u$
xy	xy	xyx	x	yx	e	y	$(xy)u$	yu	$(xyx)u$	$(yx)u$	u	xu
yx	yx	y	xyx	e	xy	x	$(yx)u$	$(xyx)u$	xu	u	$(xy)u$	yu
xyx	xyx	xy	yx	x	y	e	$(xyx)u$	$(yx)u$	$(xy)u$	yu	xu	u
u	u	xu	yu	$(yx)u$	$(xy)u$	$(xyx)u$	e	x	y	yx	xy	xyx
xu	xu	u	$(xy)u$	$(xyx)u$	yu	$(yx)u$	x	e	yx	y	xyx	xy
yu	yu	$(yx)u$	u	xu	$(xyx)u$	$(xy)u$	y	xy	e	xyx	x	yx
$(xy)u$	$(xy)u$	$(xyx)u$	xu	u	$(yx)u$	yu	xy	y	xyx	e	yx	x
$(yx)u$	$(yx)u$	yu	$(xyx)u$	$(xy)u$	u	xu	yx	xyx	x	xy	e	y
$(xyx)u$	$(xyx)u$	$(xy)u$	$(yx)u$	yu	xu	u	xyx	yx	xy	x	y	e

Table B.1: Multiplication table for $M_{12}(S_3,\, 2)$ presented by $\langle x,\, y,\, u;\, x^2 = y^3 = (xy)^2 = u^2 = e,\, xu = ux,\, yu = uy^{-1},\, xy \cdot u = u \cdot (xy)^{-1},\, yx \cdot u = u \cdot (yx)^{-1} \rangle$

S_1	$(\!(111,\ 111)\!)_0$		
S_2			
$S_2(0,\ 2)$	$(\!(000,\ 011)\!)_1$	$(\!(000,\ 101)\!)_1$	$(\!(000,\ 110)\!)_1$
$S_2(1,\ 1)$	$(\!(001,\ 001)\!)_0^*$	$(\!(001,\ 010)\!)_1$	$(\!(001,\ 100)\!)_1$
	$(\!(010,\ 001)\!)_1$	$(\!(010,\ 010)\!)_0^*$	$(\!(010,\ 100)\!)_1$
	$(\!(100,\ 001)\!)_1$	$(\!(100,\ 010)\!)_1$	$(\!(100,\ 100)\!)_0^*$
$S_2(1,\ 3)$	$(\!(001,\ 111)\!)_0$	$(\!(010,\ 111)\!)_0$	$(\!(100,\ 111)\!)_0$
$S_2(2,\ 0)$	$(\!(011,\ 000)\!)_1$	$(\!(101,\ 000)\!)_1$	$(\!(110,\ 000)\!)_1$
$S_2(2,\ 2)$	$(\!(011,\ 011)\!)_1^*$	$(\!(011,\ 101)\!)_0$	$(\!(011,\ 110)\!)_0$
	$(\!(101,\ 011)\!)_0$	$(\!(101,\ 101)\!)_1^*$	$(\!(101,\ 110)\!)_0$
	$(\!(110,\ 011)\!)_0$	$(\!(110,\ 101)\!)_0$	$(\!(110,\ 110)\!)_1^*$
$S_2(3,\ 1)$	$(\!(111,\ 001)\!)_0$	$(\!(111,\ 010)\!)_0$	$(\!(111,\ 100)\!)_0$
S_3			
$S_3(0,\ 1)$	$(\!(000,\ 001)\!)_1$	$(\!(000,\ 010)\!)_1$	$(\!(000,\ 100)\!)_1$
$S_3(0,\ 3)$	$(\!(000,\ 111)\!)_1$		
$S_3(1,\ 0)$	$(\!(001,\ 000)\!)_1$	$(\!(010,\ 000)\!)_1$	$(\!(100,\ 000)\!)_1$
$S_3(1,\ 2)$	$(\!(001,\ 011)\!)_0$	$(\!(001,\ 101)\!)_0$	$(\!(001,\ 110)\!)_1$
	$(\!(010,\ 011)\!)_0$	$(\!(010,\ 101)\!)_1$	$(\!(010,\ 110)\!)_0$
	$(\!(100,\ 011)\!)_1$	$(\!(100,\ 101)\!)_0$	$(\!(100,\ 110)\!)_0$
$S_3(2,\ 1)$	$(\!(011,\ 001)\!)_0$	$(\!(011,\ 010)\!)_0$	$(\!(011,\ 100)\!)_1$
	$(\!(101,\ 001)\!)_0$	$(\!(101,\ 010)\!)_1$	$(\!(101,\ 100)\!)_0$
	$(\!(110,\ 001)\!)_1$	$(\!(110,\ 010)\!)_0$	$(\!(110,\ 100)\!)_0$
$S_3(2,\ 3)$	$(\!(011,\ 111)\!)_1$	$(\!(101,\ 111)\!)_1$	$(\!(110,\ 111)\!)_1$
$S_3(3,\ 0)$	$(\!(111,\ 000)\!)_1$		
$S_3(3,\ 2)$	$(\!(111,\ 011)\!)_1$	$(\!(111,\ 101)\!)_1$	$(\!(111,\ 110)\!)_1$

Table B.2: Involutions of $M^*(2)$ in relation to $x_0 = (\!(111,\ 111)\!)$. The involutions are divided into three sets $S_i = \{y;\ |x_0 y| = i\}$, $i = 1,\ 2,\ 3$. For $i = 2,\ 3$, the sets S_i are further subdivided into $S_i(r,\ s) = \{y \in S_i;\ y = (\!(\alpha,\ \beta)\!),\ \mathrm{w}(\alpha) = r,\ \mathrm{w}(\beta) = s\}$. An involution y is denoted by asterisk if and only if $\langle x_0,\ y\rangle$ is in the orbit V_4^+

	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001		000	100	100	010	010	110	110
010			000	100	001	101	001	101
011				000	011	100	111	011
100					000	010	001	011
101						000	111	101
110							000	110
111								000

Table B.3: The cross product in $GF(2)^3$

q even	yes	yes	no	no	no	no	no	no
q mod 3	1	2	0	1	2	0	1	2
$4 \mid (q-1)$	no	no	yes	yes	yes	no	no	no
min	4	2	9	13	5	3	19	7
π	3	1	1	3	1	1	3	1
ρ	1	1	2	2	2	0	0	0
σ	2	0	1	2	0	1	2	0
τ	2	0	1	2	0	1	2	0

Table B.4: The constants ρ^*, σ^*, τ, ρ and σ for non-equivalent classes of prime powers q, as defined in Section 3.2. The first three rows define the equivalence class. The row labeled *min* contains the smallest representative from each class.

	e	x	y	y^{-1}	xy	$y^{-1}x$	xy^{-1}	yx	yxy^{-1}	xyx	yxy	$y^{-1}xy$
e	e	x	y	y^{-1}	xy	$y^{-1}x$	xy^{-1}	yx	yxy^{-1}	xyx	yxy	$y^{-1}xy$
x	x	e	xy	xy^{-1}	y	yxy	y^{-1}	xyx	$y^{-1}xy$	yx	$y^{-1}x$	yxy^{-1}
y	y	yx	y^{-1}	e	yxy	x	yxy^{-1}	$y^{-1}x$	xyx	xy^{-1}	$y^{-1}xy$	xy
y^{-1}	y^{-1}	$y^{-1}x$	e	y	$y^{-1}xy$	yx	xyx	x	xy^{-1}	yxy^{-1}	xy	yxy
xy	xy	xyx	xy^{-1}	x	$y^{-1}x$	e	$y^{-1}xy$	yxy	yx	y^{-1}	yxy^{-1}	y
$y^{-1}x$	$y^{-1}x$	y^{-1}	$y^{-1}xy$	xyx	e	xy	y	yxy^{-1}	yxy	x	yx	xy^{-1}
xy^{-1}	xy^{-1}	yxy	x	xy	yxy^{-1}	xyx	yx	e	y^{-1}	$y^{-1}xy$	y	$y^{-1}x$
yx	yx	y	yxy	yxy^{-1}	y^{-1}	$y^{-1}xy$	e	xy^{-1}	xy	$y^{-1}x$	x	xyx
yxy^{-1}	yxy^{-1}	$y^{-1}xy$	yx	yxy	xyx	xy^{-1}	$y^{-1}x$	y	e	xy	y^{-1}	x
xyx	xyx	xy	$y^{-1}x$	$y^{-1}xy$	xy^{-1}	yxy^{-1}	x	y^{-1}	y	yxy	e	yx
yxy	yxy	xy^{-1}	yxy^{-1}	yx	x	y	xy	$y^{-1}xy$	$y^{-1}x$	e	xyx	y^{-1}
$y^{-1}xy$	$y^{-1}xy$	yxy^{-1}	xyx	$y^{-1}x$	yx	y^{-1}	yxy	xy	x	y	xy^{-1}	e

Table B.5: Multiplication table for $A_4 = \langle x,\, y;\; x^2 = y^3 = (xy)^3 = e \rangle$

	e	x	y	x^{-1}	y^{-1}	xy	yx	xy^{-1}	yx^{-1}	$x^{-1}y$	$y^{-1}x$	$xy^{-1}x$
e	e	x	y	x^{-1}	y^{-1}	xy	yx	xy^{-1}	yx^{-1}	$x^{-1}y$	$y^{-1}x$	$xy^{-1}x$
x	x	x^{-1}	xy	e	xy^{-1}	$x^{-1}y$	y^{-1}	yx	$y^{-1}x$	y	$xy^{-1}x$	yx^{-1}
y	y	yx	y^{-1}	yx^{-1}	e	x^{-1}	$y^{-1}x$	$x^{-1}y$	xy	$xy^{-1}x$	x	xy^{-1}
x^{-1}	x^{-1}	e	$x^{-1}y$	x	yx	y	xy^{-1}	y^{-1}	$xy^{-1}x$	xy	yx^{-1}	$y^{-1}x$
y^{-1}	y^{-1}	$y^{-1}x$	e	xy	y	yx^{-1}	x	$xy^{-1}x$	x^{-1}	xy^{-1}	yx	$x^{-1}y$
xy	xy	y^{-1}	xy^{-1}	$y^{-1}x$	x	e	$xy^{-1}x$	y	$x^{-1}y$	yx^{-1}	x^{-1}	yx
yx	yx	yx^{-1}	x^{-1}	y	$x^{-1}y$	$xy^{-1}x$	e	$y^{-1}x$	x	y^{-1}	xy^{-1}	xy
xy^{-1}	xy^{-1}	$xy^{-1}x$	x	$x^{-1}y$	xy	$y^{-1}x$	x^{-1}	yx^{-1}	e	yx	y^{-1}	y
yx^{-1}	yx^{-1}	y	$xy^{-1}x$	yx	$y^{-1}x$	y^{-1}	$x^{-1}y$	e	xy^{-1}	x^{-1}	xy	x
$x^{-1}y$	$x^{-1}y$	xy^{-1}	yx	$xy^{-1}x$	x^{-1}	x	yx^{-1}	xy	y	$y^{-1}x$	e	y^{-1}
$y^{-1}x$	$y^{-1}x$	xy	yx^{-1}	y^{-1}	$xy^{-1}x$	xy^{-1}	y	x	yx	e	$x^{-1}y$	x^{-1}
$xy^{-1}x$	$xy^{-1}x$	$x^{-1}y$	$y^{-1}x$	xy^{-1}	yx^{-1}	yx	xy	x^{-1}	y^{-1}	x	y	e

Table B.6: Multiplication table for $A_4 = \langle x,\, y;\; x^3 = y^3 = (xy)^2 = e \rangle$

BIBLIOGRAPHY

[1] A. A. Albert, J. Thompsn, *Two-element generation of the projective unimodular group*, Illinois J. Math. **3** (1959), 421–439.

[2] D. Allcock, *Ideals in the Integral Octaves*, J. of Algebra **220** (1999), no. 2, 396–400.

[3] M. Aschbacher, R. Guralnick, *Some applications of the first cohomology group*, J. of Algebra **90** (1984), no. 2, 446–460.

[4] E. Bannai, S. Song, *The character tables of Paige's simple Moufang loops and their relationship to the character tables of* $PSL(2, q)$, Proc. London. Math. Soc. (3) **58** (1989), issue 2, 209–236.

[5] R. H. Bruck, *Pseudo-Automorphisms and Moufang Loops*, Proc. Amer. Math. Soc. **3**, issue 1 (Feb., 1952), 66–72.

[6] R. H. Bruck, L. J. Paige, *Loops whose inner mappings are automorphisms*, Ann, of Math., second series **63**, issue 2 (Mar., 1956), 308–323.

[7] D. M. Burton, *Elementary Number Theory*, fourth edition, International Series in Pure and Applied Mathematics, The McGraw-Hill Companies, Inc. (1998).

[8] R. W. Carter, *Simple Groups of Lie Type*, Pure and Applied Mathematics **XXVIII**, John Wiley and Sons (1972).

[9] O. Chein, *Moufang Loops of Small Order I*, Trans. Amer. Math. Soc. **188** (1974), 31–51.

[10] O. Chein, *Moufang Loops of Small Order*, Memoirs of the American Mathematical Society **13**, issue 1, no. 197, (1978).

[11] O. Chein, M. Kinyon, A. Rajah, P. Vojtěchovský, *Lagrange Property and Simplicity in Loop Varieties* (tentative title), in preparation.

[12] O. Chein, H. O. Pflugfelder, *The smallest Moufang loop*, Arch. Math. **22** (1971), 573–576.

[13] J. H. Conway et al., *ATLAS of Finite Groups*, Oxford University Press, New York (1985).

[14] J. H. Conway, N. J. A. Sloane, *Sphere packings, lattices and groups.* Second edition. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] **290**, Springer-Verlag, New York (1993).

[15] H. S. M. Coxeter, *Integral Cayley Numbers*, Duke Mathematical Journal **13**, no. 4 (1946). Reprinted in H. S. M. Coxeter, *Twelve Geometric Essays*, Southern Illinois University Press (1968).

[16] H. S. M. Coxeter, *The Abstract Groups* $G^{m,n,p}$, Trans. Amer. Math. Soc. **45**, issue 1 (1939), 73–150.

[17] H. S. M. Coxeter, W. O. J. Moser, *Generators and Relations for Discrete Groups*, fourth edition, A Series of Modern Surveys in Mathematics **14**, Springer-Verlag (1980).

[18] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Teubner (1901); reprinted by Dover (1958).

[19] G. M. Dixon, *Division algebras: octonions, quaternions, complex numbers and the algebraic design of physics.* Mathematics and its Applications **290**, Kluwer Academic Publishers Group, Dordrecht (1994).

[20] S. Doro, *Simple Moufang Loops*, Math. Proc. Camb. Phil. Soc. **83** (1978), 377–392.

[21] W. E. Edington, *Abstract Group Definitions and Applications*, Trans. Amer. Math. Soc. **25**, issue 2 (1923), 193–210.

[22] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.1; Aachen, St Andrews (1999). (Visit http://www-gap.dcs.st-and.ac.uk/~gap).

[23] G. Glauberman, *On Loops of Odd Order*, J. of Algebra **1** (1964), 374–396.

[24] D. Gorenstein, *Finite groups.* Second edition. Chelsea Publishing Co., New York (1980).

[25] M. L. Merlini Giuliani, César Polcino Milies, *On the structure of the simple Moufang loop* $GLL(F_2)$, Nonassociative algebra and its applications : the foirth international converence, Lecture notes in pure and applied mathematics **211**, edited by Roberto Costa, Alexander Grishkov, Henrique Guzzo, Jr., Luiz A. Peresi, 313–319, Marcel Dekker, New York (2000).

[26] B. Huppert, *Endliche Gruppen I*, Springer (1967).

[27] I. M. Isaacs, *Algebra, a graduate course*, Brooks/Cole Publishing Company, Pacific Grove (1994).

[28] N. Jacobson, *Lie algebras.* Republication of the 1962 original. Dover Publications, Inc., New York (1979).

[29] W. M. Kantor, Á. Seress, eds., *Groups and computation III: proceedings of the international conference at the Ohio State University, June* 15–19, 1999, Ohio State University Mathematical Research Institute Publication **8**, Walter de Gruyter, Berlin (2001).

[30] M. W. Liebeck, *The classification of finite simple Moufang loops*, Math. Proc. Camb. Phil. Soc. **102** (1987), 33–47.

[31] J. H. van Lint, R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press (1992).

[32] R. Moufang, *Zur Struktur von Alternativkörpern*, Math. Ann. **110** (1935), 416–430.

[33] L. Paige, *A Class of Simple Moufang Loops*, Proceedings of the American Mathematical Society **7**, issue 3 (1956), 471–482.

[34] S. E. Payne, J. A. Thas, *Finite generalized quadrangles*, Pitman Advances Publishing Program (1984).

[35] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma series in pure mathematics; **7**, Heldermann Verlag Berlin (1990).

[36] R. D. Schafer, *An Introduction to Nonassociative algebras*, Academic Press (1966), New York.

[37] V. de Smet, H. Van Maldeghem, *Ovoids and windows in finite generalized hexagons*, London Math. Soc. Lecture Note Series **191**, Finite Geometry and Combinatorics, proceedings of the Second International Conference at Deinze. Eds. A. Beutelspacher et. al., 131–138, Cambridge University Press (1993).

[38] J. D. H. Smith, *Quasigroup Actions: Markov Chains, Pseudoinverses, and Linear Representations*, Southeast Asian Bulletin of Mathematics **23** (1999), 719–729.

[39] J. D. H. Smith, A. Romanowska, *Post-modern Algebra*, Wiley-Interscience Series in Pure and Applied Mathematics, John Wiley & Sons, Inc. (1999).

[40] S.–Y. Song, *The character tables of certain association schemes*, Ph.D. thesis, Ohio State University.

[41] T. A. Springer, F. D. Veldkamp, *Octonions, Jordan Algebras, and Exceptional Groups*, Springer Monographs in Mathematics, Springer Verlag (2000).

[42] R. Steinberg, *Generators for simple groups*, Canad. J. Math. **14** (1962), 277–283.

[43] P. Vojtěchovský, *Generators of Nonassociative Simple Moufang Loops over Finite Prime Fields*, to appear in J. of Algebra

[44] P. Vojtěchovský, *Generators for Finite Simple Moufang Loops*, submitted.

[45] P. Vojtěchovský, *The Abstract Groups* $(3, 3 \mid 3, p)$*, their Subgroup Structure, and their Significance for Paige Loops*, accepted by Quasigroups and Related Systems.

[46] G. W. Whitehead, *Elements of Homotopy Theory*, Graduate Texts in Mathematics, Springer Verlag (1978).

[47] J. S. Wilson, *Economical generating sets for finite simple groups*. Groups of Lie type and their geometries (Como, 1993), 289–302, London Math. Soc. Lecture Note Ser. **207**, Cambridge Univ. Press, Cambridge (1995).

[48] M. Zorn, *Alternativkörper und quadratische systeme*, Abh. Math. Sem. Univ. Hamburg **9** (1933), 395–402.

Index