Moufang Loops and Groups with Triality are Essentially the Same Thing

J.I. Hall

Author address:

Department of Mathematics, Michigan State University, East Lansing, MI 48824 USA
E-mail address: jhall@math.msu.edu

On peut dire que le *principe de dualité*
de la Géometrie projective est remplacé ici par un *principe de trialité*.
É. Cartan [**Car25**, p. 373]

Contents

Abstract

In 1925 Élie Cartan introduced the principal of triality specifically for the Lie groups of type D_4, and in 1935 Ruth Moufang initiated the study of Moufang loops. The observation of the title was made by Stephen Doro in 1978 who was in turn motivated by work of George Glauberman from 1968. Here we make the statement precise in a categorical context. In fact the most obvious categories of Moufang loops and groups with triality are not equivalent, hence the need for the word "essentially."

Received by the editor October 26, 2016.

2010 *Mathematics Subject Classification.* Primary 20.

Key words and phrases. Moufang loop, triality, octonions.

Introduction

In 1935 Ruth Moufang [**Mou35**] initiated the study of Moufang loops, motivated by her work on highly transitive projective planes and their coordinatizing alternative algebras. A Moufang loop is a set equipped with a binary product having an identity element and cancellation that satisfies the identical relation

$$(xa)(bx) = (x(ab))x\,.$$

As this relation is an immediate consequence of associativity, groups provide a large class of Moufang loops. But, as Moufang noted, the unit loops of alternative algebras give infinitely many nonassociative examples.

In 1925 Élie Cartan [**Car25**] introduced the principal of triality to discuss outer automorphisms of Lie groups of type D_4. The usual duality of a vector space of dimension at least 3 over a field gives rise to an order 2 outer automorphism of its linear group, and Cartan observed that a similar "triality" of 8-dimensional orthogonal space can be used to explain the unexpected order 3 outer automorphisms of groups of type D_4. Cartan also noted a connection with the octonions.

The observation of the title is due to Stephen Doro [**Dor78**] who, in 1978, defined and studied abstract triality for groups—Cartan's triality groups providing nontrivial examples. Doro was motivated by the 1968 work of George Glauberman [**Gla68**] on finite Moufang loops and the 1956 work of Lowell Paige [**Pai56**] on simple Moufang loops. Our title is well accepted and can be found in various forms throughout the literature, for instance [**GrZ06, HaN01, NVo03, Tit58**].[1] The main purpose of the present monograph is to make this observation precise in a categorical context. In fact the most obvious categories of Moufang loops and groups with triality are not equivalent, hence the need for the word "essentially."

Although we have described the work of Cartan and Moufang primarily in algebraic terms, it was inextricably interwoven with geometric motivation and techniques. That will be the case for us as well.

The equivalence of algebraic identities to the existence of various geometric automorphisms and the closure of related configurations goes back over a hundred years. Hilbert [**Hil00**] observed that a large part of classical geometry can be recovered when the axioms of "congruence" are discarded in favor of taking Desargues' Theorem as an axiom. Veblen and Young [**VeY16**] considered automorphisms of

[1] Indeed it is a quote from [**Hal07b**].

projective planes and their relationship to the Desargues configuration. Reidermeister [**Rei29**], Thomsen [**Tho29**], Bol [**Bol37**], and their collaborators, in a remarkable series of papers entitled *"Topologische Fragen der Differentialgeometrie,"* worked on 3-nets (3-webs) of parallel classes of lines in the Euclidean plane. Tits [**Tit58**] studied automorphisms of webs and their connection to groups with triality specifically in the context of the octonions and Cartan's triality groups. See also Bruck [**Bru58**] and Pickert [**Pic55**].

The geometric study was revived in the paper of Funk and P. Nagy [**FuN93**], which describes in detail the relationships between Bol reflections on a 3-net and coordinatizing Bol loops. The approach we take here is closer to that of Hall and G.P. Nagy [**HaN01, Hal07a**] and that of G.P. Nagy and Vojtěchovský [**NVo03**], which discusses the case of simple Moufang loops extensively.

Since the early work in this area dealt with the study of line sets in Euclidean planes, it was naturally phrased in terms of 3-nets. We prefer the equivalent but dual world of Latin square designs and will largely stay there.

The monograph has four parts. In the first part we present the needed category theory and introduce the three main topics of discussion—loops, Latin square designs, and groups with triality. The second part contains the equivalence and nonequivalence results connecting the corresponding categories. The third part presents related issues, and the final part deals with Study's and Cartan's original triality associated with orthogonal geometry and groups in dimension 8 and with the related composition algebras, octonions, and Paige loops.

In Part 1 on *Basics*, we begin in Chapter 1 with category theory. This chapter contains much standard material, such as an introduction to category equivalence, but it also covers several less standard topics of importance here—pointed categories, rank 1 objects, and simplicity. Chapter 2 gives the basics of quasigroup and loop theory, including varieties of loops. Here the most important of these is the variety of Moufang loops mentioned above. Chapter 3 presents Latin square designs. These are the combinatorial/geometric objects that provide the skeleton for all our arguments and constructions. The connection between loops and Latin square designs, even at the categorical level, is given here. A short section provides the deeper link, originally due to Bol [**Bol37**], between the subcategories of Moufang loops and central Latin square designs—those Latin square designs possessing a suitably rich automorphism group. An abstract setting for these automorphisms, motivated by work of Doro [**Dor78**] and Glauberman [**Gla68**], provides the setting for Chapter 4 on abstract groups with triality.

Part 2 gives the arguments regarding *Equivalence* of the categories introduced in Chapters 2 through 4. This is not straightforward, and Chapters 5 through 7 provide the additional machinery and definitions needed for the precise equivalence and nonequivalence results of Chapters 8 and 9.

Part 3 contains *Related* material. Various of the functors guaranteed in the previous part are given concrete constructions. In particular, Chapter 11 gives an elegant map that associates to each Moufang loop a universal group with triality. This allows deeper investigation of the interplay between the loops and associated groups.

Chapter 12 contains discussion of the multiplication groups and autotopisms of general loops. This material could easily have been presented earlier, but we begin its use is in the following Chapter 13. This is relatively long and gives the correspondence between groups with triality, as defined here, and Doro's original formulation [**Dor78**]. Doro's definition, while on the surface different, is seen to be equivalent to one version of that used here.

The material of Chapter 14 was the initial motivation for this work. Doro [**Dor78**] was particularly interested in simple Moufang loops. He was able successfully to move this study to that of simple groups admitting triality automorphisms. With this in hand, Liebeck [**Lie87**] proved that the only nonassociative finite simple Moufang loops are those loops derived by Paige [**Pai56**] from octonion algebras over finite fields. This chapter makes precise and canonical Doro's correspondence between simple Moufang loops and simple groups. It also discusses the relationships between normal subloops of Moufang loops and normal subgroups of the associated groups with triality. In particular we prove that a finite Moufang loop is solvable if and only if its multiplication group is solvable, the converse part of this being a result due to Vesanen [**Ves96**] whose result is valid for all finite loops.

Chapter 15 discusses various other categories and concepts that are adjacent to those discussed here. For instance the 3-nets of Bol and others are seen to be appropriately isomorphic.

Part 4 is devoted to classical or concrete triality. Chapter 16 gives a brief introduction to its three main parts—Study's geometric triality, Cartan's group theoretic triality, and the octonions. Chapter 17 presents the requisite results on orthogonal geometry and groups. Chapter 18 then gives Study's geometric triality and Cartan's group theoretic triality—both in the context of hyperbolic orthogonal 8-space. Chapter 19 discusses composition algebras and their basic classification and structure, including algebraic results that bridge the two classical trialities. It also includes a proof of Hurwitz' theorem on the dimensions of composition algebras. Chapter 20 details Freudenthal's direct connection between octonion algebra and orthogonal triality. The final Chapter 21 then focuses on the Moufang loops that arise from the multiplicative loops of octonion algebras, finishing with a return to Paige's simple Moufang loops.

We close this introduction by discussing the subtleties occasioning the word "essentially" of the title. As already mentioned, loops and Latin square designs are elementary concepts, already seen to be equivalent in Chapter 3. Moufang loops and central Latin square designs are introduced as particularly nice loops and designs, equivalent by Bol's result. There is no correspondingly useful universe containing groups with triality as a subclass. (The category of groups is too big.) Instead the definition for groups with triality is motivated by properties of central Latin square designs and so of Moufang loops. The transition is not completely natural or smooth.

Specifically, two groups with triality that are different, but the same modulo central subgroups, correspond to the same central Latin square design and Moufang loop. Our remedy for this is to define, in Chapter 7, two subcategories of the triality group category—one consisting of groups with trivial center ("adjoint") and the second consisting of groups with center as large as possible ("universal"). The most natural passage from Moufang loops and central Latin square designs to groups with triality—indeed the one that motivates the original definition—is via a map **A** with the adjoint subcategory as its image. In Chapter 5 we define a second map **B** whose image is the universal subcategory.

The map **A**, while obvious and elementary, is not categorical; it is not a functor. On the other hand the map **B** is a functor that ultimately gives the desired equivalence, but it would be hard to describe it as either obvious or elementary. We have the basic bind: the full class of groups with triality is too big; the most accessible subclass is mathematically lacking; and the mathematically satisfactory subclass is obscure. The distinctions are subtle. The issue was already appreciated by Doro and has, through the years, been a source of frequent fuzziness (and occasional inaccuracy). While this monograph does not remove the difficulty, one of the goals is to put it into sharp focus.

I thank the various people whose comments have contributed to and improved this monograph. These include but are not restricted to: Ulrich Meierfrankenfeld, Gabor Nagy, Jonathan D.H. Smith, Petr Vojtěchovský, Richard Weiss, and the late Ernie Shult. I especially thank the editor, Robert Guralnick, and the referee, both of whom were very patient and helpful.

Jonathan I. Hall
East Lansing, Michigan
25 October 2016

Part 1

Basics

Chapter 1

Category Theory

1.1. Basics

We give a brief summary of the category theory and related notation of importance here.

We assume familiarity with the most basic concepts and definitions of category theory, as for instance found in Jacobson [**Jac89**, § 1.1]. We largely follow Jacobson and also Pareigis [**Par70**] although we act on the right:

> *for categories* C, D, $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$, $g \in \mathrm{Hom}_{\mathsf{C}}(B, C)$, *and functor* $\mathbf{F}\colon \mathsf{C} \longrightarrow \mathsf{D}$ *we have* $fg \in \mathrm{Hom}_{\mathsf{C}}(A, C)$, $(fg)\mathbf{F} = f\mathbf{F}g\mathbf{F}$, *and* $1_A\mathbf{F} = 1_{A\mathbf{F}}$.

Many of the categories we consider are *concrete*, which is to say that the objects are sets furnished with decoration (say, a multiplication) and the morphisms are set maps that respect the decoration appropriately. In this situation we may abuse terminology by referring to morphisms as *maps.* Also for clarity we may then write the identity permutation Id_A in place of the identity morphism 1_A, since many of our objects (loops and groups) have a multiplicative identity element, frequently also denoted 1_A.

The morphism $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$ is called *monic* if it is right cancellable:

> *for all* Z *and* $g_1, g_2 \in \mathrm{Hom}_{\mathsf{C}}(Z, A)$, $g_1 f = g_2 f$ *implies* $g_1 = g_2$.

Monic morphisms are the categorical replacements for injective maps.[1] For instance, if ab is monic, then a is monic. (Exercise!) Similarly f is *epic* if it is left cancellable:

> *for all* C *and* $g_1, g_2 \in \mathrm{Hom}_{\mathsf{C}}(B, C)$, $fg_1 = fg_2$ *implies* $g_1 = g_2$.

The morphism f is an *isomorphism* if there is a morphism $g \in \mathrm{Hom}_{\mathsf{C}}(B, A)$ with $fg = 1_A$ and $gf = 1_B$ in which case we write $g = f^{-1}$. Isomorphisms are both monic and epic. The set $\mathrm{End}_{\mathsf{C}}(A) = \mathrm{Hom}_{\mathsf{C}}(A, A)$ of *endomorphisms* of A in C is a monoid under composition. An invertible element of $\mathrm{End}_{\mathsf{C}}(A)$ is then an *automorphism* in C (a C-*automorphism*), and the set of C-automorphisms forms the *automorphism* group of A in C, $\mathrm{Aut}_{\mathsf{C}}(A)$. Functors take isomorphisms to isomorphisms and automorphisms to automorphisms.

[1] Again: we are acting on the right.

Every category C admits the identity functor $\mathbf{1}_{\mathsf{C}}$ taking each object and morphism to itself. This is the special case $\mathsf{C} = \mathsf{D}$ of the inclusion functor $\iota \colon \mathsf{C} \longrightarrow \mathsf{D}$ for any subcategory C of D.

A functor $\mathbf{F} \colon \mathsf{C} \longrightarrow \mathsf{D}$ is *faithful* if the corresponding map $\mathrm{Hom}_{\mathsf{C}}(A, B) \longrightarrow \mathrm{Hom}_{\mathsf{D}}(A\mathbf{F}, B\mathbf{F})$ is always injective and *full* if the same map is always surjective. We call the functor $\mathbf{F}$ *dense* if for every $B \in \mathrm{Obj}\,\mathsf{D}$ there is an $A \in \mathrm{Obj}\,\mathsf{C}$ with $A\mathbf{F}$ isomorphic to B in D. (This is not a standard term.) In particular $\mathbf{1}_{\mathsf{C}}$ is faithful, full, and dense. The inclusion of a subcategory into a category is always faithful, and we call the subcategory *full* if the inclusion is additionally full and *dense* if the inclusion is dense.

1.2. Category equivalence

Two categories C and D are *isomorphic* if there are functors $\mathbf{F} \colon \mathsf{C} \longrightarrow \mathsf{D}$ and $\mathbf{G} \colon \mathsf{D} \longrightarrow \mathsf{C}$ with

$$\mathbf{FG} = \mathbf{1}_{\mathsf{C}} \text{ and } \mathbf{GF} = \mathbf{1}_{\mathsf{D}}\,.$$

Similarly the categories C and D are *equivalent* if there are functors $\mathbf{F} \colon \mathsf{C} \longrightarrow \mathsf{D}$ and $\mathbf{G} \colon \mathsf{D} \longrightarrow \mathsf{C}$ with the weaker

$$\mathbf{FG} \cong \mathbf{1}_{\mathsf{C}} \text{ and } \mathbf{GF} \cong \mathbf{1}_{\mathsf{D}}\,,$$

where $\cong$ indicates natural isomorphism of functors. Here the functor $\mathbf{X} \colon \mathsf{E} \longrightarrow \mathsf{E}$ is *naturally isomorphic*[2] to the identity functor $\mathbf{1}_{\mathsf{E}}$ if:

> *for every* $A \in \mathrm{Obj}\,\mathsf{E}$ *there is an isomorphism* $\chi_A \in \mathrm{Hom}_{\mathsf{E}}(A, A\mathbf{X})$ *such that: for all* $B, C \in \mathrm{Obj}\,\mathsf{E}$ *and each* $f \in \mathrm{Hom}_{\mathsf{E}}(B, C)$*, we have* $f\mathbf{X} = \chi_B^{-1} f \chi_C$*:*

$$\begin{tikzcd}
B \arrow[r, "f"] \arrow[d, "\chi_B"'] & C \arrow[d, "\chi_C"] \\
B\mathbf{X} \arrow[r, "f\mathbf{X}"] & C\mathbf{X}
\end{tikzcd}$$

In this case we say that $(\mathbf{F}, \mathbf{G})$ is a *category equivalence* (or just *equivalence*) of C and D and that $\mathbf{F}$ *gives an equivalence* of C and D. (The functor $\mathbf{F}$ need not determine $\mathbf{G}$ uniquely.)

There are useful reformulations of equivalence.

(1.1). Proposition. *Let* $\mathbf{F}$ *be a functor from* C *to* D*. The following are equivalent:*

(1) *There is a functor* $\mathbf{G} \colon \mathsf{D} \longrightarrow \mathsf{C}$ *with* $(\mathbf{F}, \mathbf{G})$ *a category equivalence.*
(2) *There is a functor* $\mathbf{G} \colon \mathsf{D} \longrightarrow \mathsf{C}$ *with* $\mathbf{FG} \colon \mathsf{C} \longrightarrow \mathsf{C}$ *and* $\mathbf{GF} \colon \mathsf{D} \longrightarrow \mathsf{D}$ *both faithful, full, and dense functors.*
(3) $\mathbf{F}$ *is faithful, full, and dense.*

Proof. Part (2) requires less of $\mathbf{G}$ than (1) does (and indeed for $\mathbf{G}$ as in (2) the pair $(\mathbf{F}, \mathbf{G})$ may not be an equivalence). Part (2) implies (3) by elementary arguments, and (3) implies (1) by [**Jac89**, Prop.1.3]. □

The following alternative view of category equivalence follows easily.

[2] See [**Jac89**, p.23] for the definition of natural isomorphism of arbitrary functors.

(1.2). Corollary. *Two categories are equivalent provided they have isomorphic full, dense subcategories. In particular a category is equivalent to any subcategory that is full and dense.* □

Loosely, two categories are isomorphic if their objects and morphisms are the same up to the changing of names, whereas two categories are equivalent if the isomorphism classes of their objects and morphisms are the same up to the changing of names. For instance, the category of finite sets is equivalent to the category of all finite subsets of the integers (and even to the category of all finite ordinals).

As is always true, isomorphisms respect basic properties. Equivalences usually do too. For instance, the following is an easy exercise.

(1.3). Proposition. *Let $\mathbf{F}\colon \mathsf{C} \longrightarrow \mathsf{D}$ give an equivalence of the categories C and D. If $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ is monic or epic, then $f\mathbf{F}$ is (respectively) monic or epic.* □

1.3. Terminal objects and kernel morphisms

An object A is *terminal* in C when each $\mathrm{Hom}_{\mathsf{C}}(X,A)$ contains a unique morphism. Similarly A is *initial* in C when each $\mathrm{Hom}_{\mathsf{C}}(A,X)$ contains a unique morphism. Terminal (or initial) objects need not exist in C, but if they do then there is a unique isomorphism class of such objects. An object that is both initial and terminal is a *zero object.* For instance, a trivial group is a zero object in the category of groups and a 0 module is a zero object in a module category. Essentially all the categories we shall encounter have terminal objects, although some do not have zero objects.

(1.4). Proposition. *Let $\mathbf{F}\colon \mathsf{C} \longrightarrow \mathsf{D}$ give an equivalence of the categories C and D. If A is a terminal, initial, or zero object of C then $A\mathbf{F}$ is (respectively) terminal, initial, or zero in D.* □

In a category C with terminal objects, a *trivial morphism* is one that factors through a terminal object.

(1.5). Lemma. *If the category C has zero objects, then for each pair of objects $L, M \in \mathrm{Obj}\,\mathsf{C}$ there is a unique trivial C-morphism from L to M.* □

The morphism of the lemma is often denoted $0_{L,M}$, but we shall use this notation sparingly.

Assume that the category C has zero objects. If $\delta \in \mathrm{Hom}_{\mathsf{C}}(Q,M)$ then a *kernel morphism* for δ is a morphism $\alpha \in \mathrm{Hom}_{\mathsf{C}}(N,Q)$ with $\alpha\delta$ trivial and having the property that for any $\lambda \in \mathrm{Hom}_{\mathsf{C}}(L,Q)$ with $\lambda\delta$ trivial there is a unique $\lambda_\alpha \in \mathrm{Hom}_{\mathsf{C}}(L,N)$ with $\lambda = \lambda_\alpha\alpha$:

$$\begin{tikzcd}
L \arrow[d, dashed, "!\,\lambda_\alpha"'] \arrow[dr, "\lambda"] & & \\
N \arrow[r, "\alpha"] & Q \arrow[r, "\delta"] & M
\end{tikzcd}$$

Clearly if α and λ are two kernel morphisms of δ, then there is a unique isomorphism λ_α with $\lambda = \lambda_\alpha\alpha$; that is, kernel morphism are essentially unique.

Kernel morphisms are, of course, categorical substitutes for kernels of homomorphisms in typical situations; see Lemma (2.10) below for a demonstration.

1.4. Pointed categories

There is a uniform technique for promoting a terminal object in a category to zero object status in a related category.

Let C be a category with terminal object O. For A an object of C, any morphism $a \in \mathrm{Hom}_{\mathsf{C}}(O, A)$ is an *anchor* of A (an *O-anchor*). We then define a new category $\mathsf{C}^{\star}_{O}$, a *pointed* category. Its objects are the pairs (A, a) with A an object of C and a an O-anchor of A. For (A, a) and (B, b) in $\mathrm{Obj}\,\mathsf{C}^{\star}_{O}$, the morphism set $\mathrm{Hom}_{\mathsf{C}^{\star}_{O}}((A, a), (B, b))$ consists of those $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$ that additionally have $af = b$. We easily find:

(1.6). Lemma. *$\mathsf{C}^{\star}_{O}$ is a category in which $(O, 1_O)$ is a zero object. If T is a terminal object in C, then $\mathsf{C}^{\star}_{O}$ and $\mathsf{C}^{\star}_{T}$ are isomorphic.* □

We have the forgetful functor from $\mathsf{C}^{\star}_{O}$ to C, taking (A, a) to A and viewing $g \in \mathrm{Hom}_{\mathsf{C}^{\star}_{O}}((A, a), (B, b))$ as an element of $\mathrm{Hom}_{\mathsf{C}}(A, B)$. If O is actually a zero object, then each object of C has a unique anchor, and the forgetful functor gives an isomorphism of C with $\mathsf{C}^{\star}_{O}$.

For each anchor a of A and morphism $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$, the morphism af is the unique anchor b of B for which f induces an element of $\mathrm{Hom}_{\mathsf{C}^{\star}_{O}}((A, a), (B, b))$. Thus, for a fixed anchor a of A, the set of morphisms $\mathrm{Hom}_{\mathsf{C}}(A, B)$ is the disjoint union of the various $\mathrm{Hom}_{\mathsf{C}^{\star}_{O}}((A, a), (B, b))$ as b runs through the anchors of B. In particular, calculations for one of C and $\mathsf{C}^{\star}_{O}$ can often be applied to the other.

(1.7). Lemma. *Let $\mathbf{F}$ be a functor from C to D that takes the terminal object O of C to the terminal object $O\mathbf{F}$ of D. Then $(A, a)\mathbf{F}^{\star} = (A\mathbf{F}, a\mathbf{F})$ and $f\mathbf{F}^{\star} = f\mathbf{F}$ describe a functor $\mathbf{F}^{\star}$ from $\mathsf{C}^{\star}_{O}$ to $\mathsf{D}^{\star}_{O\mathbf{F}}$.*

Proof. As $O\mathbf{F}$ is a terminal object in D, $a\mathbf{F}$ is an $O\mathbf{F}$-anchor of $A\mathbf{F}$ and $(A\mathbf{F}, a\mathbf{F})$ an object of $\mathsf{D}^{\star}_{O\mathbf{F}}$. If $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$ with $af = b$, then

$$a\mathbf{F}^{\star} f\mathbf{F}^{\star} = a\mathbf{F} f\mathbf{F} = (af)\mathbf{F} = b\mathbf{F} = b\mathbf{F}^{\star}\,. \qquad \square$$

(1.8). Corollary. *If the full subcategory C of D contains the terminal object O of D, then the pointed version $\iota^{\star}$ of the inclusion functor ι of C into D is the inclusion functor of $\mathsf{C}^{\star}_{O}$ into $\mathsf{D}^{\star}_{O}$.* □

(1.9). Lemma. *Let $\mathbf{F}$ be a functor from C to D that takes the terminal object O of C to the terminal object $O\mathbf{F}$ of D.*

(a) *If $\mathbf{F}$ is faithful, then $\mathbf{F}^{\star}$ is faithful.*
(b) *If $\mathbf{F}$ is full, then $\mathbf{F}^{\star}$ is full.*
(c) *If $\mathbf{F}$ is full and dense, then $\mathbf{F}^{\star}$ is full and dense.*

Proof. As discussed above, for a fixed object (A, a) of $\mathsf{C}^{\star}_{O}$ we have the disjoint unions:

$$\mathrm{Hom}_{\mathsf{C}}(A, B) = \biguplus_{b} \mathrm{Hom}_{\mathsf{C}^{\star}_{O}}((A, a), (B, b))$$

and

$$\begin{aligned}\mathrm{Hom}_{\mathsf{D}}(A\mathbf{F}, B\mathbf{F}) &= \biguplus_{d} \mathrm{Hom}_{D^{\star}_{O\mathbf{F}}}((A\mathbf{F}, a\mathbf{F}), (B\mathbf{F}, d)) \\ &= \biguplus_{d} \mathrm{Hom}_{D^{\star}_{O\mathbf{F}}}(((A, a)\mathbf{F}^{\star}, (B\mathbf{F}, d))\,,\end{aligned}$$

where not all $O\mathbf{F}$-anchors d of $B\mathbf{F}$ need be of the form $b\mathbf{F}$ for some O-anchor b of B.

The first two parts of the lemma are now immediate.

For part (c), assume $\mathbf{F}$ is full and dense. By the previous part $\mathbf{F}^\star$ is full. Let (X, x) be an object of $D^\star_{O\mathbf{F}}$. As $\mathbf{F}$ is dense, there are an A and isomorphism $i \in \mathrm{Hom}_{\mathsf{D}}(X, A\mathbf{F})$, so that $xi \in \mathrm{Hom}_{\mathsf{D}}(O\mathbf{F}, A\mathbf{F})$ is a $O\mathbf{F}$-anchor of $A\mathbf{F}$. But $\mathbf{F}$ is also full, so there is a O-anchor a of A with $xi = a\mathbf{F}$. Now $(A\mathbf{F}, xi) = (A\mathbf{F}, a\mathbf{F}) = (A, a)\mathbf{F}^\star$ is isomorphic to (X, x) in $D^\star_{O\mathbf{F}}$, and $\mathbf{F}^\star$ is dense. □

(1.10). THEOREM. *Let C be a category containing the terminal object O. If $\mathbf{F}$ gives an equivalence of C and D, then $\mathbf{F}^\star$ gives an equivalence of $\mathsf{C}^\star_O$ and $\mathsf{D}^\star_{O\mathbf{F}}$.*

PROOF. By Proposition (1.4) the equivalence $\mathbf{F}$ takes terminal objects to terminal objects. Also it is faithful, full, and dense by Proposition (1.1). Therefore by the lemma, $\mathbf{F}^\star$ is faithful, full, and dense. Now a second appeal to Proposition (1.1) proves that $\mathbf{F}^\star$ is an equivalence. □

1.5. Rank 1 objects

In a category, monic morphisms correspond to injective maps and epic morphisms to surjective maps. A careful analysis of monics will be presented in Chapter 6.

Epics turn out to be more difficult to handle, so we take a different (and more *ad hoc*) approach to surjectivity. The basic idea is that elements of an object X in the category C correspond to the morphisms of $\mathrm{Hom}_{\mathsf{C}}(A, X)$ where A is "free of rank 1" (interpreted appropriately).

Let A be an object in C. We say that the morphism $f \in \mathrm{Hom}_{\mathsf{C}}(X, Y)$ is *A-surjective* if, for every $a \in \mathrm{Hom}_{\mathsf{C}}(A, Y)$, there is a $b \in \mathrm{Hom}_{\mathsf{C}}(A, X)$ with $a = bf$. If $\mathbf{F}\colon \mathsf{C} \longrightarrow \mathsf{D}$ gives an equivalence, then f is A-surjective if and only if $f\mathbf{F}$ is $A\mathbf{F}$-surjective.

A related concept is the *A-order* of the object X of C, which we define to be $|\mathrm{Hom}_{\mathsf{C}}(A, X)|$. If $\mathbf{F}\colon \mathsf{C} \longrightarrow \mathsf{D}$ gives an equivalence, then the A-order of X equals the $A\mathbf{F}$-order of $X\mathbf{F}$.

The categories we consider have terminal objects. There we define the *terminal-order* of an object X to be its O-order for O terminal. Similarly a *terminal-surjective* morphism is one that is O-surjective. By Proposition (1.4), category equivalences respect terminal-order and terminal-surjectivity.

If a category has zero objects then all morphisms are terminal-surjective and all objects have terminal-order 1, so we need a more subtle concept.

The nonzero object Z of the category C with zero objects will be called a *$\mathbb{Z}$-object* provided:

(i) *for all nonzero A there are nonzero $f \in \mathrm{Hom}_{\mathsf{C}}(Z, A)$;*
(ii) *if $\mathrm{Hom}_{\mathsf{C}}(A, Z)$ contains nonzero morphisms, then there are morphisms $f \in \mathrm{Hom}_{\mathsf{C}}(A, Z)$ and $g \in \mathrm{Hom}_{\mathsf{C}}(Z, A)$ with $gf = 1_Z$;*
(iii) *a nonzero idempotent in $\mathrm{End}_{\mathsf{C}}(Z)$ must be 1_Z.*

Here a *zero morphism* is one that factors through a zero object; that is, a trivial morphism. By Lemma (1.5) every object A in a category with zero has a unique zero endomorphism 0_A. It is idempotent, and A is a nonzero object if and only if $0_A \neq 1_A$.

Condition (ii) says that in some sense Z is free (extensions by Z split). Then (iii) corresponds to Z having rank at most 1 and (i) to Z not having rank 0.

(1.11). LEMMA. *In the category* C *let* Z_1 *be a* $\mathbb{Z}$*-object. Then the object* Z_2 *is a* $\mathbb{Z}$*-object if and only if it is isomorphic to* Z_1.

PROOF. Clearly any object isomorphic to a $\mathbb{Z}$-object is itself a $\mathbb{Z}$-object.

Let Z_1 and Z_2 be $\mathbb{Z}$-objects. As Z_1 is a $\mathbb{Z}$-object and Z_2 is nonzero, the set $\mathrm{Hom}_{\mathsf{C}}(Z_1, Z_2)$ contains nonzero morphisms by (i). As Z_2 is a $\mathbb{Z}$-object, by (ii) there are $f \in \mathrm{Hom}_{\mathsf{C}}(Z_1, Z_2)$ and $g \in \mathrm{Hom}_{\mathsf{C}}(Z_2, Z_1)$ with $gf = 1_{Z_2}$. Therefore $(fg)(fg) = f(gf)g = f(1_{Z_2})g = fg$ is an idempotent in $\mathrm{End}_{\mathsf{C}}(Z_1)$. By (iii) we have $fg = 0_{Z_1}$ or $fg = 1_{Z_1}$. If $fg = 0_{Z_1}$ then

$$1_{Z_2} = gf = (gf)(gf) = g(fg)f = g(0_{Z_1})f = 0_{Z_2}\,,$$

contrary to Z_2 being nonzero. Therefore $fg = 1_{Z_1}$, and f is an isomorphism of Z_1 with Z_2. □

1.6. Simplicity

There seems to be no accepted definition for simplicity of an object in a general category. In an abelian category, a simple object [**Par70**, p.174] is a nonzero object with no nonzero proper subobjects; this is a suitable model for irreducible modules but is not generally appropriate.

All the categories we study possess terminal objects. In such a category, a nonterminal object is *simple* if every morphism from it is either monic or trivial.[3]

(1.12). PROPOSITION. *Let* $\mathbf{F}\colon \mathsf{C} \longrightarrow \mathsf{D}$ *give an equivalence of the categories* C *and* D *with terminal objects. If* A *is a simple object in* C *then* $A\mathbf{F}$ *is a simple object in* D.

PROOF. Let A be a simple object in C with f arbitrary in $\mathrm{Hom}_{\mathsf{D}}(A\mathbf{F}, X)$. By category equivalence there is a $B \in \mathsf{C}$ with X isomorphic to $B\mathbf{F}$ in D, say by $i \in \mathrm{Hom}_{\mathsf{D}}(X, B\mathbf{F})$. Then $fi \in \mathrm{Hom}_{\mathsf{D}}(A\mathbf{F}, B\mathbf{F})$, so there is a $g \in \mathrm{Hom}_{\mathsf{C}}(A, B)$ with $g\mathbf{F} = fi$. As A is simple, either g is monic or it factors through a terminal object in C.

If g is monic then so is $fi = g\mathbf{F}$ by Proposition (1.3). As i is an isomorphism $f = g\mathbf{F}.i^{-1}$ is then monic itself, and we are done. Therefore we may assume that g factors through a terminal object, say $g = ab$ with $a \in \mathrm{Hom}_{\mathsf{C}}(A, O)$ and $b \in \mathrm{Hom}_{\mathsf{C}}(O, B)$ for O a terminal object in C. Then $fi = g\mathbf{F} = a\mathbf{F}b\mathbf{F}$, and $f = a\mathbf{F}(b\mathbf{F}.i^{-1})$ with $a\mathbf{F} \in \mathrm{Hom}_{\mathsf{D}}(A\mathbf{F}, O\mathbf{F})$ and $b\mathbf{F}.i^{-1} \in \mathrm{Hom}_{\mathsf{D}}(O\mathbf{F}, X)$, for $O\mathbf{F}$ a terminal object in D again by Proposition (1.4). □

[3] For abelian categories this definition of simplicity is equivalent to that of [**Par70**, p.174].

Chapter 2

Quasigroups and Loops

2.1. Basics

A *quasigroup* $(Q, \cdot)$ is a nonempty[1] set Q equipped with a binary multiplication $\cdot\colon Q \times Q \longrightarrow Q$ and such that, for each $a \in Q$, the right and left translation maps $\mathrm{R}(a)\colon Q \longrightarrow Q$ and $\mathrm{L}(a)\colon Q \longrightarrow Q$ given by

$$q^{\mathrm{R}(a)} = q \cdot a \quad \text{and} \quad q^{\mathrm{L}(a)} = a \cdot q$$

are permutations of Q. If there is a two-sided identity element $1_Q = 1_{(Q,\cdot)}$ then Q is a *loop.* (We often write Q in place of $(Q, \cdot)$ when the multiplication is clear and also often denote multiplication by juxtaposition.)

The *opposite* of the quasigroup $(Q, \cdot)$ is the quasigroup $(Q, \cdot')$ with multiplication given by $x \cdot' y = y \cdot x$. The opposite of a loop is a loop with the same identity element.

A *homotopism* from the quasigroup $(Q, \cdot)$ to the quasigroup $(R, \circ)$ is a triple (α, β, γ) of maps from Q to R with the property that

$$x^\alpha \circ y^\beta = (x \cdot y)^\gamma$$

for all $x, y \in Q$. A homotopism is an *isotopism* if each of its three maps is a bijection. We have a *principal homotopism* or *principal isotopism* if Q and R are equal as sets and $\gamma = \mathrm{Id}_Q$, the identity permutation of Q.

We let Qgp be the category whose object class consists of all quasigroups, the set $\mathrm{Hom}_{\mathsf{Qgp}}(A, B)$ being that of all homotopisms from the quasigroup A to the quasigroup B. This is clearly a category. The isomorphisms in the category Qgp are precisely the isotopisms, the inverse of (α, β, γ) being $(\alpha^{-1}, \beta^{-1}, \gamma^{-1})$. We let Loop be the full subcategory of Qgp whose object class is that of all loops.

(2.1). Lemma. *Let $(Q, \cdot)$ be a quasigroup. Then (α, β, γ) is a principal isotopism of $(Q, \cdot)$ with a loop $(Q, \circ)$ if and only if there are $a, b \in Q$ with $(\alpha, \beta, \gamma) = (\mathrm{R}(b), \mathrm{L}(a), \mathrm{Id}_Q)$. In that case, the loop identity element is $a \cdot b$.*

[1] As has been pointed out by J.D.H. Smith, there are virtues to admitting the empty set as a quasigroup. For instance, this guarantees that the intersection of subquasigroups is always a subquasigroup—particularly desirable in the varietal setting. But including the empty set renders Corollary (2.2) false, as also pointed out by Professor Smith. We thank him for his observations.

PROOF. ($\Longrightarrow$) Certainly $\gamma = \mathrm{Id}_Q$. Let $1 = 1_{(Q,\circ)}$ be the identity element of the loop $(Q,\circ)$, and set $a = 1^{\alpha^{-1}}$ and $b = 1^{\beta^{-1}}$. Then

$$x^{\alpha^{-1}} \cdot y^{\beta^{-1}} = z \iff x \circ y = z\,.$$

In particular

$$1^{\alpha^{-1}} \cdot z^{\beta^{-1}} = z \iff 1 \circ z = z\,. \quad \text{and} \quad z^{\alpha^{-1}} \cdot 1^{\beta^{-1}} = z \iff z \circ 1 = z\,.$$

Therefore $\beta = \mathrm{L}(a)$, $\alpha = \mathrm{R}(b)$, and $a \cdot b = 1$.

($\Longleftarrow$) (See [**Bru58**, p. 56].) For all $q \in Q$

$$(a \cdot b) \circ q = a^{\mathrm{R}(b)} \circ q = a^{\mathrm{R}(b)} \circ (q^{\mathrm{L}(a)^{-1}})^{\mathrm{L}(a)} = (a \cdot q^{\mathrm{L}(a)^{-1}})^{\mathrm{Id}_Q} = q\,,$$

so $a \cdot b$ is a left identity in quasigroup principal isotope $(Q,\circ)$. Similarly it is a right identity. □

(2.2). COROLLARY. *The inclusion functor gives an equivalence of the categories* Loop *and* Qgp.

PROOF. The inclusion functor ι: Loop $\longrightarrow$ Qgp is faithful and full. By the lemma each quasigroup $(Q,\cdot)$ is isomorphic to a loop $(Q,\circ)$ in Qgp, so inclusion is dense and the result follows from Corollary (1.2). □

In particular we may focus our attention on Loop rather than Qgp without great loss.

A *Latin square* based upon the set Q is a $|Q| \times |Q|$ array in which each element of Q occurs exactly once in each row and exactly once in each column. A particular example is the *Cayley table* (multiplication table) of the quasigroup $(Q,\cdot)$—the cell in the table at the intersection of row a and column b has entry $a \cdot b$. Indeed every Latin square based upon Q can be viewed as the Cayley table of many quasigroups Q, all isotopic. From this point of view, Lemma (2.1) can be easily illustrated:

(2.3). REMARK. *To find one of the $|Q|^2$ principal isotope loops of the given quasigroup $(Q,\cdot)$, select row a and column b of its Cayley table. Use the entries of this row to relabel the columns of the table and the entries of this column to relabel the rows of the table. The new Cayley table is that of a loop principal isotope with identity element $a \cdot b$, the entry at the intersection of the original row a and the original column b.*

2.2. Autotopisms and anti-autotopisms

The Qgp-automorphisms of the quasigroup Q are the *autotopisms* of Q. These are the triples $g = (g_+, g_-, g_0) = (g_+, g_-, g_0)_+$ of permutations g_ϵ of Q with

$$x^{g_+} \cdot y^{g_-} = (xy)^{g_0} \quad \text{for all } x, y \in Q\,,$$

and they form the group $\mathrm{Aut}_{\mathsf{Qgp}}(Q) = \mathrm{Atp}(Q)$—the *autotopism group* of Q. As the subcategory Loop is full in Qgp, for any loop Q the autotopism group is still given by $\mathrm{Atp}(Q) = \mathrm{Aut}_{\mathsf{Qgp}}(Q) = \mathrm{Aut}_{\mathsf{Loop}}(Q)$.

Similarly an *anti-autotopism* of Q is a triple $h = (h_+, h_-, h_0) = (h_+, h_-, h_0)_-$ of permutations h_ϵ of Q with

$$x^{h_+} \cdot y^{h_-} = (yx)^{h_0} \quad \text{for all } x, y \in Q\,.$$

Elementary calculations then give:

(2.4). Proposition. *The set* $\mathrm{AAtp}(Q)$ *of all autotopisms and anti-autotopisms of the quasigroup* Q *form a group, the* anti-autotopism group *of* Q *under the multiplication*

$$(a_+, a_-, a_0)_\alpha \cdot (b_+, b_-, b_0)_\beta = (a_\beta b_+, a_{-\beta} b_-, a_0 b_0)_{\alpha\beta}\,.$$

The autotopism group $\mathrm{Atp}(Q)$ *is normal of index* 1 *or* 2 *in* $\mathrm{AAtp}(Q)$. □

The calculations are aided by the observation that for all subscript choices we have $(ab)_\epsilon = a_{\epsilon\beta} b_\epsilon$.

2.3. Loop homomorphisms and the pointed category $\mathsf{Loop}^\star$

We define a second category of loops, which we denote $\mathsf{Loop}^\star$. Its object class is again all loops (that is, $\mathrm{Obj}\,\mathsf{Loop}^\star = \mathrm{Obj}\,\mathsf{Loop}$), but the morphism set $\mathrm{Hom}_{\mathsf{Loop}^\star}(A, B)$ consists of the loop homomorphisms from A into B. A *loop homomorphism* is a map $\gamma\colon A \longrightarrow B$ from the loop A to the loop B with $(xy)^\gamma = x^\gamma y^\gamma$ for all $x, y \in A$. As the identity is the unique idempotent in a loop, $1_A^\gamma = 1_B$.

Loop homotopisms need not respect the identity, but if $\gamma\colon Q \longrightarrow M$ is a loop homomorphism then $(\alpha, \beta, \gamma) = (\gamma, \gamma, \gamma)$ is a homotopism that additionally has $1_Q^\alpha = 1_Q^\beta = 1_Q^\gamma = 1_M$. We have the converse:

(2.5). Lemma. *Let* $(\alpha, \beta, \gamma)\colon (Q, \cdot) \longrightarrow (M, \circ)$ *be a loop homotopism.*

(a) *If* $1_Q^\alpha = 1_Q^\beta = 1_M$*, then* $1_Q^\gamma = 1_M$ *and* $\alpha = \beta = \gamma$ *is a loop homomorphism from* $(Q, \cdot)$ *to* $(M, \circ)$.

(b) *There is a principal isotopism* $(\alpha_0, \beta_0, \mathrm{Id}_M)\colon (M, \circ) \longrightarrow (M, \times)$ *such that* γ *is a loop homomorphism from* $(Q, \cdot)$ *to* $(M, \times)$*. Specifically*

$$(\gamma, \gamma, \gamma) = (\alpha, \beta, \gamma)(\alpha_0, \beta_0, \mathrm{Id}_M) = (\alpha\alpha_0, \beta\beta_0, \gamma)\,.$$

Proof. (a) We have

$$1_Q^\gamma = (1_Q \cdot 1_Q)^\gamma = 1_Q^\alpha \circ 1_Q^\beta = 1_M \circ 1_M = 1_M\,.$$

Also

$$x^\alpha = x^\alpha \circ 1_M = x^\alpha \circ 1_Q^\beta = (x \cdot 1_Q)^\gamma = x^\gamma\,.$$

Therefore $\alpha = \gamma$ and similarly $\beta = \gamma$.

(b) Set $1_Q^\alpha = a \in M$ and $1_Q^\beta = b \in M$ so that $1_Q^\gamma = a \circ b \in M$. With $\alpha_0 = \mathrm{R}(b)$ and $\beta_0 = \mathrm{L}(a)$ the principal isotopism $(\alpha_0, \beta_0, \mathrm{Id}_M)$ takes $(M, \circ)$ to $(M, \times)$, a loop with identity element $1_{(M,\times)} = a \circ b$ by Lemma (2.1).

Therefore $(\alpha, \beta, \gamma)(\alpha_0, \beta_0, \mathrm{Id}_M) = (\alpha\alpha_0, \beta\beta_0, \gamma)$ is a homotopism from $(Q, \cdot)$ to $(M, \times)$ with each map taking 1_Q to $1_{(M,\times)}$. Part (a) thus implies that $\alpha\alpha_0 = \beta\beta_0 = \gamma$ is a loop homomorphism. □

(2.6). Corollary. *Every loop isotopic to a loop is isomorphic to one of its principal isotopes.* □

For those who now wonder why isotopy never came up in their group theory courses:

(2.7). Corollary. *Every loop that is isotopic to the group* G *is a group that is isomorphic to* G.

Proof. By the previous corollary and Lemma (2.1), we need only examine the image $(G,\circ)$ of G under the principal isotopy $(\mathrm{R}(b),\mathrm{L}(a),\mathrm{Id})$. Consider the map $\varphi\colon G \longrightarrow (G,\circ)$ given by $\varphi(x)=axb$. Then

$$\varphi(xy)=axyb=(axb)b^{-1}\cdot a^{-1}(ayb)=\varphi(x)^{\mathrm{R}(b)^{-1}}\cdot\varphi(y)^{\mathrm{L}(a)^{-1}}=\varphi(x)\circ\varphi(y)\,.\quad\square$$

A particular consequence of Lemma (2.5) is that $\mathsf{Loop}^\star$ is isomorphic to the subcategory of Loop in which all loops remain as objects but we only allow those homotopisms that respect the loop identity elements. We usually identify $\mathsf{Loop}^\star$ with the corresponding subcategory of Loop.

The $\mathsf{Loop}^\star$-automorphism group $\mathrm{Aut}_{\mathsf{Loop}^\star}(Q)$ is the usual group of loop automorphisms—those permutations γ of Q with $x^\gamma y^\gamma=(xy)^\gamma$ for all $x,y\in Q$.

(2.8). Lemma. *The loop $\{1\}$ is a terminal object but is not initial in* Loop. *The loop $\{1\}$ is a zero object in* $\mathsf{Loop}^\star$. *In particular the categories* Loop *and* $\mathsf{Loop}^\star$ *are not equivalent.*

Proof. Objects are sets, and morphisms are induced by set mappings; so $\{1\}$ is certainly terminal. If the loop M contains $e\neq 1_M$, then the homotopism (α,β,γ) from $\{1\}$ to M given by $(1,1,1)^{(\alpha,\beta,\gamma)}=(1,e,e)$ is not the identity map. Therefore $\{1\}$ is not initial in Loop.

The loop $\{1\}$ is a zero object in $\mathsf{Loop}^\star$ by Lemma (2.5). The last sentence then follows from Proposition (1.4). □

The observation from the lemma, that a category with terminal but noninitial objects cannot be equivalent to a category with zero objects, will be made often.

The category $\mathsf{Loop}^\star$ is not completely new to us; it is essentially one of the pointed categories introduced in Section 1.4.

(2.9). Theorem. *The category* $\mathsf{Loop}^\star$ *is equivalent to the pointed category* $\mathsf{Loop}^\star_{\{1\}}$.

Proof. For $Q\in\mathrm{Obj}\mathsf{Loop}^\star=\mathrm{Obj}\mathsf{Loop}$, let $Q\mathbf{E}=(Q,\iota_Q)\in\mathsf{Loop}^\star_{\{1\}}$, where the morphism $\iota_Q=(\iota,\iota,\iota)\in\mathrm{Hom}_{\mathsf{Loop}}(\{1\},Q)$ with $1^\iota=1_Q$. For each $\gamma\in\mathrm{Hom}_{\mathsf{Loop}^\star}(Q,M)$ set $\gamma\mathbf{E}=(\gamma,\gamma,\gamma)$, a morphism in $\mathrm{Hom}_{\mathsf{Loop}^\star_{\{1\}}}((Q,\iota_Q),(M,\iota_M))$ as $1_Q^\gamma=1_M$.

Clearly $\mathbf{E}$ is a faithful functor from $\mathsf{Loop}^\star$ to $\mathsf{Loop}^\star_{\{1\}}$. We claim that it gives an equivalence of the two categories. By Proposition (1.1) we must prove that $\mathbf{E}$ is full and dense.

Any (α,β,γ) of $\mathrm{Hom}_{\mathsf{Loop}^\star_{\{1\}}}((N,\iota_N),(M,\iota_M))$ has $\alpha=\beta=\gamma$, a loop homomorphism from $\mathrm{Hom}_{\mathsf{Loop}^\star}(N,M)$ by Lemma (2.5)(a) (with $Q=N$). Therefore $\mathbf{E}$ is full.

Let $((M,\circ),m)\in\mathsf{Loop}^\star_{\{1\}}$ with $m=(\alpha,\beta,\gamma)$. By Lemma (2.5)(b) (with $Q=\{1\}$) there is a principal isotopism $p=(\alpha_0,\beta_0,\mathrm{Id}_M)$ in $\mathrm{Hom}_{\mathsf{Loop}}((M,\circ),(M,\times))$ such that $mp=(\gamma,\gamma,\gamma)$ is a loop homomorphism from $\{1\}$ to $(M,\times)$. Thus $1^\gamma=1_{(M,\times)}$, $mp=\iota_{(M,\times)}$, and p is an isomorphism of $((M,\circ),m)$ and $((M,\times),\iota_{(M,\times)})$ in $\mathsf{Loop}^\star_{\{1\}}$.

We conclude that $\mathbf{E}$ is dense and so gives the desired equivalence. □

The *kernel* of the loop homomorphism $\delta\colon Q\longrightarrow M$ is the subloop

$$\ker\delta=\{\,k\in Q\mid k^\delta=1_M\,\}\,.$$

This is consistent with the concept of kernel morphisms introduced in Section 1.3.

(2.10). LEMMA. *If $\delta\colon Q \longrightarrow M$ be a loop homomorphism with kernel N, then the injection map $\alpha\colon N \longrightarrow Q$ is a kernel morphism for δ in the category* $\mathsf{Loop}^\star$.

PROOF. Suppose $\lambda\colon L \longrightarrow Q$ is a loop homomorphism with $\lambda\delta$ trivial. That is, the image of each $l \in L$ under $\lambda\delta$ is 1_M. Hence each l^λ is in $\ker\delta = N$, and the map λ_α that takes l to l^λ is a well-defined morphism from L to N. This is the unique such morphism making the diagram commute:

$$\begin{tikzcd}
L \arrow[d, dashed, "\lambda_\alpha"'] \arrow[dr, "\lambda"] & & \\
N \arrow[r, "\alpha"] & Q \arrow[r, "\delta"] & M
\end{tikzcd}$$

We conclude that α is a kernel morphism for δ, as claimed. □

A subloop N of the loop Q is *normal* if it is the kernel of some loop homomorphism. In this case the expected properties hold: N is a normal subloop of the loop Q precisely when set multiplication gives a well-defined coset multiplication

$$Nx \cdot Ny = N(xy)\,,$$

and the quotient loop Q/N is canonically isomorphic to the image of any homomorphism with kernel N. (See [**Bru58**, IV.1 pp.61-2].)

It is sometimes more convenient to think of loop homomorphisms in terms of congruences. A *congruence* $\sim$ on the loop Q is an equivalence relation that additionally has the property

$$x_1 \sim x_2,\ y_1 \sim y_2 \implies x_1y_1 \sim x_2y_2\,.$$

The map that takes every element of Q to its $\sim$-congruence class is a loop homomorphism from Q onto the loop $Q/\sim$ in which, by definition, the product of the class containing x and the class containing y is the class containing xy. Every surjective loop homomorphism δ on Q arises in this way; indeed the image of δ is $Q/\sim$ when we define

$$x \sim y \iff x^\delta = y^\delta\,.$$

The equivalence classes are, of course, the cosets of the corresponding kernel.

2.4. Moufang loops and other loop varieties

We shall be interested in certain varieties of loops—subclasses that are defined through the satisfaction of particular identical relations. For instance, the category of groups arises as the variety of all loops that satisfy identically the associativity relation

$$x(yz) = (xy)z\,.$$

In loops we must distinguish between right inverses and left inverses,

$$x({}^{-1}x) = 1 \quad\text{and}\quad (x^{-1})x = 1\,,$$

as they need not be the same. We say that inverses are *two-sided* if we have any one of the three equivalent identical relations

$${}^{-1}x = x^{-1}\,,\quad (x^{-1})^{-1} = x\,,\quad\text{or}\quad {}^{-1}({}^{-1}x) = x\,.$$

A loop is a *right inverse property loop* if it satisfies the identity

$$(ax)({}^{-1}x) = a$$

and a *left inverse property loop* if it satisfies the identity

$$x^{-1}(xa) = a\,.$$

The loop is an *inverse property loop* if it satisfies both of these identities.

A related property is the *antiautomorphic inverse property*, which holds when we have the identical relation

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

(2.11). Lemma.

(a) *If a loop satisfies either the right or the left inverse property, then inverses are two-sided.*

(b) *An inverse property loop has the antiautomorphic inverse property.*

Proof. (a) Assume $x^{-1}(xa) = a$ identically. Then

$$x^{-1} = x^{-1} \cdot 1 = x^{-1}(x \cdot {}^{-1}x) = {}^{-1}x\,.$$

(b) $a^{-1}x^{-1} = a^{-1}((x^{-1}(xa))(xa)^{-1}) = a^{-1}(a(xa)^{-1}) = (xa)^{-1}$. □

The most important variety of loops for us will be that of *Moufang loops*—those loops that satisfy the identical relation

$$(xa)(bx) = (x(ab))x\,.$$

This is the *Moufang property* or *Moufang identity*, named after Ruth Moufang, who first studied such loops [**Mou35**].

The Moufang property is a consequence of associativity. In particular every group is a Moufang loop. There are also nonassociative examples (see Section 2.5 below). Moufang loops have many nice properties.

(2.12). Proposition. *Let Q be a Moufang loop.*

(a) *Q is an inverse property loop: $(ax)({}^{-1}x) = a$ and $x^{-1}(xa) = a$ for all $x, a \in Q$.*

(b) *Inverses are two-sided and Q satisfies the antiautomorphic inverse property.*

(c) *Q has the flexible property: $(xb)x = x(bx)$ for all $x, b \in Q$.*

(d) *$x(a(xb)) = ((xa)x)b$, for all $x, a, b \in Q$.*

(e) *$b(x(ax)) = ((bx)a)x$, for all $x, a, b \in Q$.*

Proof. This is well known; see [**Bru58**, VII.3.1], [**Pfl90**, IV.1.4].

If we substitute $a = 1$ into the Moufang property $(xa)(bx) = (x(ab))x$, then we find the flexible property $x(bx) = (xb)x$. In particular $(x(ab))x = x((ab)x)$, so the opposite loop of a Moufang loop is again Moufang. As the two inverse properties are opposites of each other, we need only verify one of them to prove that we have an inverse property loop. Substitute $x = a^{-1}$ into the Moufang property to get $ba^{-1} = (a^{-1}a)(ba^{-1}) = (a^{-1}(ab))a^{-1}$, then cancel the factor a^{-1} on the right to obtain the left inverse property $b = a^{-1}(ab)$, as desired. Two-sided inverses and the antiautomorphic inverse property follow by Lemma (2.11).

The last two identities are opposites, so we need only prove one of them. This can be done directly. Instead we defer the proof to Corollary (12.9), which illustrates the use of autotopisms in proving loop identities. □

The last two identities of the proposition can replace the Moufang property in the definition of a Moufang loop. In fact Moufang's original definition [**Mou35**] was slightly different but still equivalent; she studied inverse property loops that satisfy the identical relation

$$x(a(xb)) = (x(ax))b\,.$$

This identity is now called the left Bol property, and a loop satisfying it is a *left Bol loop*. The opposite of a left Bol loop is a *right Bol loop*, characterized by the opposite identical relation $b((xa)x) = ((bx)a)x$.

The flexible property together with Proposition (2.12)(d,e) show that a Moufang loop is both a left and a right Bol loop. Conversely a loop that is both left and right Bol is Moufang, but individually each identity is strictly weaker than the Moufang property. That is, there are Bol loops that are not Moufang, the smallest having order 8.

Part of [**Pfl90**, IV.1] is misleading—without something additional, such as the inverse property or the flexible property, the left Bol identity (denoted there (M_4)) is strictly weaker than the three equivalent Moufang identities (there (M_5), (M_6), and (M_7)). See [**Bru58**, VII.3.1] and [**Pfl90**, IV.1,IV.6] for proofs and further discussion.

(2.13). Proposition.

(a) *The opposite of a Moufang loop is a Moufang loop.*

(b) *Every Moufang loop is power associative: each subloop generated by one elements is a cyclic group.*

(c) (Moufang's Theorem) *Any triple of elements that associates in some order generates a subgroup. Especially each subloop generated by two elements is a group.*

Proof. (a) This is a consequence of the Moufang property and the flexible property of Proposition (2.12)(b).

(b) See [**Pfl90**, IV.6.6] or [**Hal07a**, Cor. 3.10], which gives a proof the spirit of Section 3.3 below.

(c) This is from Moufang's original paper [**Mou35**]. See also [**Bru58**, p.117] and [**Pfl90**, IV.2.10]. □

We have already used part (a) of the proposition, saying that the opposite of a Moufang loop is Moufang, in the proof of Proposition (2.12). We will use it again, often and without reference.

Of course power associativity as in (b) is contained in Moufang's Theorem, but that result is much deeper and difficult. We will not actually make direct appeal to Moufang's Theorem anywhere, but the result is so important that it must be mentioned. For a nice proof due to Drápal, see [**Dra11**].

The category Mouf is the full subcategory of Loop consisting of all Moufang loops. The category $\mathsf{Mouf}^\star$ is then the full subcategory of Moufang loops in $\mathsf{Loop}^\star$. As with general loops, we may identify $\mathsf{Mouf}^\star$ with the corresponding subcategory of Mouf.

(2.14). LEMMA. *The loop $\{1\}$ is a terminal object but not initial in the category* Mouf *and is a zero object in* $\mathsf{Mouf}^\star$. *In particular the categories* Mouf *and* $\mathsf{Mouf}^\star$ *are not equivalent.*

PROOF. The loop $\{1\}$ is a terminal object in Loop and a zero object in $\mathsf{Loop}^\star$ by Lemma (2.8), and it remains so in their full subcategories Mouf and $\mathsf{Mouf}^\star$. The argument for that lemma also shows that $\{1\}$ is terminal but not initial in any full subcategory of Loop that additionally contains a loop with more than one element. For instance, Mouf contains all nontrivial groups and so has the terminal but nonzero object $\{1\}$, while $\mathsf{Mouf}^\star$ contains a zero object. Thus these two categories are not equivalent by Proposition (1.4). □

(2.15). THEOREM. *The categories* $\mathsf{Mouf}^\star$ *and* $\mathsf{Mouf}^\star_{\{1\}}$ *are equivalent.*

PROOF. This follows from the lemma, Theorem (2.9), and Corollary (1.8). □

2.5. Examples

Of course every group is a Moufang loop, but there are other important examples which are not associative.

2.5.1. Paige loops. Moufang [**Mou35**] studied alternative algebras, proving that the Moufang laws are valid in all alternative algebras. Composition algebras are the particular examples possessing a multiplicative norm $\delta(mn) = \delta(m)\delta(n)$. In a composition algebra, an element is a unit if and only if $\delta(m)$ is nonzero. Thus the units form a Moufang loop, and those units u with norm $\delta(u) = 1$ give a normal subloop.

Over the field F a nondegenerate 8-dimensional composition algebra is either a division algebra or is uniquely determined up to isomorphism as the F-algebra of split octonions $\mathrm{Oct}^+(F)$, whose norm 1 subalgebra is denoted $\mathrm{SOct}^+(F)$.

The scalars of $\mathrm{SOct}^+(F)$ form a normal subloop $\{\pm I\}$ of order at most 2, and the *Paige loop* over F is the quotient $\mathrm{PSOct}^+(F) = \mathrm{SOct}^+(F)/\{\pm I\}$. Paige [**Pai56**] proved that all Paige loops are simple (see Theorem (21.14) below), and Liebeck [**Lie87**] proved the converse for finite loops: a finite simple Moufang loop that is not a group is isomorphic to a Paige loop $\mathrm{PSOct}^+(\mathbb{F}_q)$.

We shall return to the octonions and to Paige loops in Part 4, particularly in Chapter 21. See also [**NVo03, Pai56, SpV00**].

2.5.2. Chein's generalized dihedral loops. A second construction of a large number of nonassociative Moufang loops is due to Chein [**Che74**, Theorem 1]. (See also [**Che78**] and [**Cur07**].) See [**Hal06**, §4] for discussion and for a proof of

(2.16). THEOREM. *Let $(Q, \circ)$ be a Moufang loop in which the subloop Q_0 generated by all elements of order not 2 is a proper subloop. Then there is a subgroup H containing Q_0 and an element x of order 2 in $Q \setminus H$ such that each element of Q can be uniquely expressed in the form hx^a, where $h \in H$, $a = 0, 1$; and the product of elements of Q is given by*

$$(h_1x^d) \circ (h_2x^e) = (h_1^n h_2^m)^n x^{d+e}$$

where $n = (-1)^e$ and $m = (-1)^{d+e}$.

Conversely, given a group H, the loop $(Q, \circ)$ constructed as above is a Moufang loop. This loop is a group if and only if the group H is abelian. □

Chein's multiplication is summarized in the following table:

$\circ$	h_2	h_2x
h_1	h_1h_2	$(h_2h_1)x$
h_1x	$(h_1h_2^{-1})x$	$h_2^{-1}h_1$

We call these generalized dihedral loops, since the element x of order 2 inverts all the elements of the normal subgroup H: for $h \in H$ always $x^{-1}hx = xhx = h^{-1}$.

We shall also return to the Chein loops; see page 30 and Theorem (10.2) below.

Chapter 3

Latin Square Designs

As we saw in Section 2.1, the multiplication table of the quasigroup Q is a *Latin square*—a $|Q| \times |Q|$ array in which each element of Q occurs exactly once in each row and exactly once in each column. Latin square designs furnish a geometric setting for these combinatorial objects. They form the geometric bridge between Moufang loops and groups with triality.

3.1. Basics

A *partial linear space* (P, S) consists of a set P, the *point set*, and a set S of subsets of P, the *lines*, the only axiom being that every pair of points from P occur together in at most one line of S. The partial linear space is a *linear space* if every pair of points is in exactly one line. A *subspace* of (P, S) is a partial linear space (P_0, S_0) with $P_0 \subseteq P$ and $S_0 \subseteq S$ such that $L \in S$ with $|L \cap P_0| \geq 2$ implies $L \subseteq P_0$ and $L \in S_0$.

The partial linear spaces of greatest interest here are the Latin square designs. A *Latin square design* (P, S) has its point set partitioned as $P = P^{\mathrm{R}} \cup P^{\mathrm{C}} \cup P^{\mathrm{E}}$ with pairwise disjoint and nonempty *fibers* P^{R}, P^{C}, and P^{E}. The line set S then satisfies:

(i) *every line $l \in S$ contains exactly one point from each of P^{R}, P^{C}, and P^{E};*

(ii) *if p, q are two points not in the same fiber, then there is a unique line $l \in S$ with $p, q \in l$.*

The superscripts are meant to suggest the rows, columns, and entries of the corresponding Latin square, although the definition makes it clear that the role played by entries is really the same as that played by rows and by columns. As convenient, we shall write a line either as a triple $(x, y, z) \in P^{\mathrm{R}} \times P^{\mathrm{C}} \times P^{\mathrm{E}}$ or as a 3-subset $\{x, y, z\} \subseteq P$.

(3.1). Lemma. *Let (P, S) be a Latin square design. The lines through a fixed point of one fiber give a bijection between the other two fibers. In particular, all have the same cardinality $|P^{\mathrm{R}}| = |P^{\mathrm{C}}| = |P^{\mathrm{E}}| = |P|/3$ and so $|S| = |P|^2/9$.* □

The number $|P|/3$ is the *order* of the Latin square design (P, S).

We define a category LSD whose object class consists of all Latin square designs. If (P,S) and (P_0,S_0) are Latin square designs then a morphism $f=(\alpha,\beta,\gamma)$ of $\mathrm{Hom}_{\mathsf{LSD}}((P,S),(P_0,S_0))$ is precisely a triple of maps $\alpha\colon P^{\mathrm{R}}\longrightarrow P_0^{\mathrm{R}}$, $\beta\colon P^{\mathrm{C}}\longrightarrow P_0^{\mathrm{C}}$ and $\gamma\colon P^{\mathrm{E}}\longrightarrow P_0^{\mathrm{E}}$ with the property:

> *if (x,y,z) is a line of S, then $(x,y,z)^f=(x^\alpha,y^\beta,z^\gamma)$ is a line of S_0.*

In particular the set $(P^{\mathrm{R}})^\alpha\cup(P^{\mathrm{C}})^\beta\cup(P^{\mathrm{E}})^\gamma$ carries a Latin square subdesign of (P_0,S_0). If any of α, β, or γ are injections then they all are; in this case we say that f is *injective.*

(3.2). LEMMA. *If a morphism in $\mathrm{Hom}_{\mathsf{LSD}}((P,S),(P_0,S_0))$ is bijective as a map from P to P_0 then it is an isomorphism.*

PROOF. By considering $P^{\mathrm{R}}\times P^{\mathrm{C}}$, a morphism that is bijective on the point set is also bijective on the line set, and therefore has an inverse. □

The category $\mathsf{LSD}^\star$ has as objects the triples (P,S,I) where (P,S) is an object of LSD and I is a fixed line of S. Then $\mathrm{Hom}_{\mathsf{LSD}^\star}((P,S,I),(P_0,S_0,I_0))$ consists of those morphisms of $\mathrm{Hom}_{\mathsf{LSD}}((P,S),(P_0,S_0))$ that take I to I_0.

Any fixed line I can be thought of as a (degenerate) Latin square design of order 1. The category $\mathsf{LSD}^\star$ is also not new.

(3.3). THEOREM. *A Latin square design O of order 1 is a terminal object in LSD but is not initial. The category $\mathsf{LSD}^\star$ is isomorphic to the pointed category $\mathsf{LSD}^\star_O$.*

PROOF. Objects are sets, and morphisms are induced by set mappings, hence O is terminal. If (P,S) is a Latin square design with I_1 and I_2 distinct lines of S, then there are maps φ_i in $\mathrm{Hom}_{\mathsf{LSD}}(O,(P,S))$ with $O^{\varphi_i}=I_i$. Thus O is not initial in LSD.

If $\varphi\in\mathrm{Hom}_{\mathsf{LSD}}(O,(P,S))$ is an anchor, then $\varphi(O)$ is a line I_φ of (P,S). The isomorphism then takes the object (P,S,I_φ) of $\mathsf{LSD}^\star$ to the object $((P,S),\varphi)$ of $\mathsf{LSD}^\star_O$. □

The theorem allows us to identify the categories $\mathsf{LSD}^\star$ and $\mathsf{LSD}^\star_O$.

Let $(Q,\cdot)$ be a quasigroup, and let Q_{R}, Q_{C}, and Q_{E} be disjoint copies of the set Q. The Latin square design $(Q,\cdot)\mathbf{T}=(P_{Q\mathbf{T}},S_{Q\mathbf{T}})$ has point set $P_{Q\mathbf{T}}=Q_{\mathrm{R}}\cup Q_{\mathrm{C}}\cup Q_{\mathrm{E}}$ (so that $P^{\mathrm{R}}_{Q\mathbf{T}}=Q_{\mathrm{R}}$ and so forth), and the triple $(x_R,y_C,z_E)\in Q_{\mathrm{R}}\times Q_{\mathrm{C}}\times Q_{\mathrm{E}}$ is a line of $S_{Q\mathbf{T}}$ precisely when $x\cdot y=z$ as elements of $(Q,\cdot)$. We may at times write (x,y,z) for the triple (x_R,y_C,z_E) of $Q_{\mathrm{R}}\times Q_{\mathrm{C}}\times Q_{\mathrm{E}}$. If $(Q,\cdot)$ is additionally a loop, then we set $(Q,\cdot)\mathbf{T}^\star=(P_{Q\mathbf{T}},S_{Q\mathbf{T}},I_{Q\mathbf{T}})$ where the line $I_{Q\mathbf{T}}$ is $\{(1_Q)_{\mathrm{R}},(1_Q)_{\mathrm{C}},(1_Q)_{\mathrm{E}}\}$.

The design $(Q,\cdot)\mathbf{T}$ is the *Thomsen design* of $(Q,\cdot)$ (after [**Tho29**]). Its associated Latin square is the Cayley table for $(Q,\cdot)$. The Latin square of the quasigroup $(Q,\cdot')$, opposite to $(Q,\cdot)$, is the transpose of that for $(Q,\cdot)$. For the associated Latin square design $(Q,\cdot)\mathbf{T}$, this corresponds to applying the permutation σ that, for every $q\in Q$, interchanges q_{R} and q_C and fixes q_{E}. The resulting Latin square design $(Q,\cdot')\mathbf{T}$ is isomorphic as design to the original, but σ does not induce an LSD-morphism, since it interchanges the indices R and C and the corresponding fibers.

A category LSD^+ with Latin square designs as objects but larger sets of morphisms than LSD will be discussed in Section 15.2 below; there σ is a morphism.

For $f = (\alpha, \beta, \gamma) \in \mathrm{Hom}_{\mathsf{Set}}(Q, M)^3$ let $f\mathbf{T} = (\alpha\mathbf{T}, \beta\mathbf{T}, \gamma\mathbf{T})$ be the map of $\mathrm{Hom}_{\mathsf{Set}}(Q_R, M_R) \times \mathrm{Hom}_{\mathsf{Set}}(Q_C, M_C) \times \mathrm{Hom}_{\mathsf{Set}}(Q_E, M_E)$ given by

$$(x_{\mathrm{R}})^{\alpha\mathbf{T}} = (x^\alpha)_{\mathrm{R}}, \quad (x_{\mathrm{C}})^{\beta\mathbf{T}} = (x^\beta)_{\mathrm{C}}, \quad (x_{\mathrm{E}})^{\gamma\mathbf{T}} = (x^\gamma)_{\mathrm{E}}\,.$$

Clearly $\mathbf{T}$ gives a bijection of the two morphism sets. We next see that the restriction of $\mathbf{T}$ to $\mathrm{Hom}_{\mathsf{Qgp}}(Q, M)$ and to $\mathrm{Hom}_{\mathsf{Loop}^\star}(Q, M)$ (where we shall call it $\mathbf{T}^\star$) turns the Thomsen map into a functor.

(3.4). Theorem.

(a) *The Thomsen map* $\mathbf{T}$ *is a functor that gives an equivalence of the two categories* Qgp *and* LSD.

(b) *The Thomsen map* $\mathbf{T}$ *is a functor that gives an equivalence of the two categories* Loop *and* LSD.

(c) *The Thomsen map* $\mathbf{T}^\star$ *is a functor that gives an equivalence of the two categories* $\mathsf{Loop}^\star$ *and* $\mathsf{LSD}^\star$.

Proof. (a) Let $Q = (Q, \cdot)$ and $M = (M, \circ)$ be two quasigroups. Let $f = (\alpha, \beta, \gamma) \in \mathrm{Hom}_{\mathsf{Set}}(Q, M)^3$, and suppose $x \cdot y = z$. Then

$$\begin{aligned} x^\alpha \circ y^\beta = z^\gamma \iff & \{(x^\alpha)_{\mathrm{R}}, (y^\beta)_{\mathrm{C}}, (z^\gamma)_{\mathrm{E}}\} \in S_{M\mathbf{T}} \\ \iff & \{(x_{\mathrm{R}})^{\alpha\mathbf{T}}, (y_{\mathrm{C}})^{\beta\mathbf{T}}, (z_{\mathrm{E}})^{\gamma\mathbf{T}}\} \in S_{M\mathbf{T}} \\ \iff & \{x_{\mathrm{R}}, y_{\mathrm{C}}, z_{\mathrm{E}}\}^{f\mathbf{T}} \in S_{M\mathbf{T}}\,. \end{aligned}$$

That is, $f \in \mathrm{Hom}_{\mathsf{Qgp}}(Q, M)$ if and only if $f\mathbf{T} \in \mathrm{Hom}_{\mathsf{LSD}}(Q\mathbf{T}, M\mathbf{T})$. Therefore the bijection $\mathbf{T}$ restricts to a map from Qgp to LSD that is full and faithful. It is also clearly functorial.

By Proposition (1.1) it remains to prove that $\mathbf{T}$ is dense. Let (P, S) be a Latin square design, and choose a set Q and bijections $\alpha\colon P^{\mathrm{R}} \longrightarrow Q$, $\beta\colon P^{\mathrm{C}} \longrightarrow Q$, and $\gamma\colon P^{\mathrm{E}} \longrightarrow Q$. We define a multiplication on Q by setting $x^\alpha \cdot y^\beta = z^\gamma$ for each line $(x, y, z) \in S$. If $(\alpha_0, \beta_0, \gamma_0)$ is an isotopism of $(Q, \cdot)$ with $(Q, \circ)$, then $(x, y, z)^f = ((x^{\alpha\alpha_0})_{\mathrm{R}}, (y^{\beta\beta_0})_{\mathrm{C}}, (z^{\gamma\gamma_0})_{\mathrm{E}})$ gives an isomorphism f in LSD of (P, S) with $(Q, \circ)\mathbf{T}$.

Part (b) follows immediately from (a) by Corollary (2.2). Then (c) is a consequence of Theorems (1.10) and (3.3). □

3.2. Central Latin square designs

A particular consequence of Theorem (3.4) is that the automorphism group of $(Q, \cdot)$ in Qgp, $\mathrm{Aut}_{\mathsf{Qgp}}(Q, \cdot)$—that is, the autotopism group $\mathrm{Atp}(Q, \cdot)$—is isomorphic to the automorphism group of $(Q, \cdot)\mathbf{T} = (P, S)$ in LSD, $\mathrm{Aut}_{\mathsf{LSD}}(P, S)$. Here an LSD-automorphism of (P, S) is a triple of permutations, one each for P^{R}, P^{C}, and P^{E}, that take lines of S to lines of S. More generally the *full automorphism group* $\mathrm{Aut}(P, S)$ of (P, S) is the set of all permutations of P that take lines to lines. Any automorphism must take fibers to fibers—they are the equivalence classes under "noncollinearity"—but it may permute the three fibers among themselves. The group $\mathrm{Aut}_{\mathsf{LSD}}(P, S)$ is then the kernel of this action, the normal subgroup of $\mathrm{Aut}(P, S)$ that fixes each fiber globally. The quotient is the subgroup of $\mathrm{Sym}(3)$ induced by $\mathrm{Aut}(P, S)$ upon the set of three fibers. In the category LSD^+, mentioned in the previous section and defined in Section 15.2 below, we do have $\mathrm{Aut}(P,S) = \mathrm{Aut}_{\mathsf{LSD}^+}(P,S)$.

For x a point of the Latin square design (P,S), a *central automorphism* τ_x with *center* x is an automorphism with the property that:

(i) $x^{\tau_x} = x$;
(ii) *if* $\{x,y,z\}$ *is a line of* (P,S) *on* x *then* $y^{\tau_x} = z$ *and* $z^{\tau_x} = y$.

A central automorphism τ_x is not an LSD-automorphism, since it globally fixes the fiber of x but switches the other two fibers.

(3.5). Lemma.

(a) *If there is a central automorphism* τ_x *of* (P,S)*, then it has order* 2 *and is the unique central automorphism with center* x.
(b) *For* g *and* τ_x *automorphisms of* (P,S) *we have* ${\tau_x}^g = \tau_{x^g}$.
(c) *Let* τ_x *and* τ_y *be central automorphisms of* (P,S) *with* $\{x,y,z\}$ *a line. Then* ${\tau_x}^{\tau_y} = \tau_z$*,* $\tau_x\tau_y$ *has order* 3*, and the set of central automorphisms of* (P,S) *is a conjugacy class in* $\mathrm{Aut}(P,S)$*. In particular* $\langle \tau_x, \tau_y \rangle \simeq \mathrm{Sym}(3)$.

Proof. See [**HaN01**, Prop. 2.3] and [**Hal07a**, Prop. 2.3].

If t_1 and t_2 are two central automorphisms of (P,S) with center x, then the automorphism t_1t_2 is trivial on both fibers off x and so is the identity automorphism. Therefore if there is a central automorphism with center x, then it is unique and has order 2.

For g an automorphism of (P,S) the conjugate ${\tau_x}^g$ is clearly a central automorphism of (P,S) with center x^g. Therefore by uniqueness ${\tau_x}^g = \tau_{x^g}$. In particular if x and y are in different fibers and $\{x,y,z\}$ is a line of S with τ_x and τ_y central automorphisms, then

$$\tau_x\tau_y\tau_x = {\tau_y}^{\tau_x} = \tau_z = {\tau_x}^{\tau_y} = \tau_y\tau_x\tau_y$$

and therefore

$$(\tau_x\tau_y)^3 = (\tau_x\tau_y\tau_x)(\tau_y\tau_x\tau_y) = {\tau_z}^2 = 1$$

and $\langle \tau_x, \tau_y \rangle \simeq \mathrm{Sym}(3)$.

As stated, a conjugate of a central automorphism is a central automorphism. If u and v are arbitrary points of P then either they are in different fibers, so that τ_u and τ_v are conjugate in $\langle \tau_u, \tau_v \rangle \simeq \mathrm{Sym}(3)$, or u and v are in the same fiber and then τ_u and τ_v are both conjugate to τ_w, where $w \in \{x,y\}$ is not in the fiber of u and v. Thus the set of all central automorphisms is a conjugacy class of $\mathrm{Aut}(P,S)$. □

(3.6). Corollary.

(a) *If* (P,S) *admits central automorphisms with centers* x *and* y *from different fibers, then the set* P_0 *of all centers of central automorphisms of* (P,S) *is the point set of a subdesign* (P_0,S_0) *of* (P,S).
(b) *If* f *is in* $\mathrm{Hom}_{\mathsf{LSD}}((P,S),(P_0,S_0))$ *and there is a central automorphism* τ_x *of* (P,S)*, then there is a unique central automorphism* τ_{x^f} *of* (P_0,S_0). □

Let $\mathrm{CAut}(P,S)$ be the subgroup of $\mathrm{Aut}(P,S)$ that is generated by all the central automorphisms of (P,S). Clearly this is a normal subgroup of $\mathrm{Aut}(P,S)$.

Of course there may be points x for which there is no central automorphism at x. Let CLSD be the full subcategory of LSD consisting of those Latin square designs that admit a central automorphism at every point. The category $\mathsf{CLSD}^\star$ is then the full subcategory of $\mathsf{LSD}^\star$ whose objects are the (P, S, I) with (P, S) an object of CLSD. The objects of CLSD and $\mathsf{CLSD}^\star$ will be called *central Latin square designs.* In this case the automorphism group $\mathrm{Aut}(P, S)$ induces the full $\mathrm{Sym}(3)$ on the set of fibers. Indeed $\mathrm{Aut}(P, S) = \mathrm{Aut}_{\mathsf{CLSD}}(P, S) \rtimes I$, where $I = \langle \tau_x, \tau_y \rangle \simeq \mathrm{Sym}(3)$, for any x and y from different fibers.

(3.7). Theorem. *The Latin square design O of order 1 belongs to CLSD. The category $\mathsf{CLSD}^\star$ is isomorphic to the pointed category $\mathsf{CLSD}^\star_O$.*

Proof. The first sentence is clear. The isomorphism of $\mathsf{LSD}^\star$ and $\mathsf{LSD}^\star_O$ given under Theorem (3.3) restricts to an isomorphism of $\mathsf{CLSD}^\star$ and $\mathsf{CLSD}^\star_O$. □

(3.8). Lemma. *If (P, S) is a central Latin square design, then the centralizer of $\mathrm{CAut}(P, S)$ in $\mathrm{Aut}(P, S)$ is 1.*

Proof. If c is in the centralizer, then $\tau_x = {\tau_x}^c = \tau_{x^c}$, for all $x \in P$, by Lemma (3.5). That is, c fixes all points of P and so is the identity. □

3.3. The correspondence between Mouf and CLSD

The next theorem is at the heart of the topic, and there are proofs in the literature from various points of view. The original proof is probably that of Bol [**Bol37**] from 1937, which is phrased in the language of 3-nets (that is, Latin square designs with the roles of points and lines interchanged; see Section 15.1). Funk and Nagy [**FuN93**] rekindled interest in such topics.

(3.9). Theorem. *Let Q be a loop. Then Q is a Moufang loop if and only if the Latin square design $Q\mathbf{T}$ admits a central automorphism τ_x with center x, for each of its points x.*

In this section we give a brief proof of the theorem in the spirit of [**HaN01, Hal07a**].

Clearly any Latin square design isomorphic to a member of CLSD belongs itself to CLSD. Therefore this theorem and Theorem (3.4) give immediately the following known result [**Pfl90**, Theorem IV.4.2]:

(3.10). Corollary. *Any loop isotopic to a Moufang loop is itself a Moufang loop.* □

Before we prove the theorem, we render it categorically.

(3.11). Theorem. *The Thomsen functor $\mathbf{T}$ gives an equivalence of the two categories Mouf and CLSD, and the functor $\mathbf{T}^\star$ gives an equivalence of the two categories $\mathsf{Mouf}^\star$ and $\mathsf{CLSD}^\star$.*

Proof. By Theorem (3.9) the loop Q is Moufang if and only if $Q\mathbf{T}$ is in CLSD if and only if $Q\mathbf{T}^\star$ is in $\mathsf{CLSD}^\star$. Therefore upon restriction $\mathbf{T}$ is a functor from Mouf to CLSD, and $\mathbf{T}^\star$ is a functor from $\mathsf{Mouf}^\star$ to $\mathsf{CLSD}^\star$. Furthermore, each of these categories is a full subcategory of, respectively, Loop, LSD, $\mathsf{Loop}^\star$, and $\mathsf{CLSD}^\star$ that is closed under isomorphism in the parent category. Therefore the restrictions of $\mathbf{T}$ and $\mathbf{T}^\star$ to the subcategories Mouf and $\mathsf{Mouf}^\star$ remain full, faithful, and dense. That is, they give the desired equivalences by Proposition (1.1). □

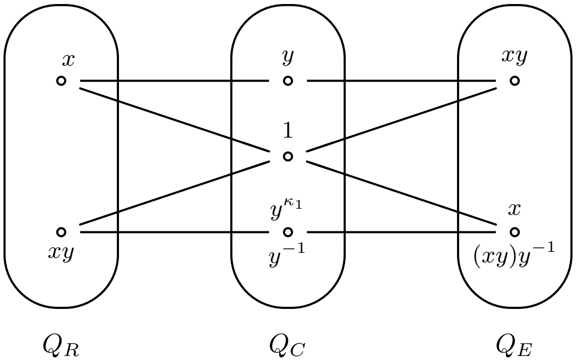
In working with central automorphisms of the Thomsen designs $Q\mathbf{T}$ we may streamline the notation by writing ρ_x for τ_{x_R}, κ_x for τ_{x_C}, and ϵ_x for τ_{x_E}.

The rest of this section is devoted to a proof of Theorem (3.9).

(3.12). LEMMA. *Let $Q = (Q, \cdot)$ be a loop.*

(a) $\kappa_1 \in \mathrm{Aut}(Q\mathbf{T})$ *if and only if Q has the right inverse property $(xy)({}^{-1}y) = x$ for all $x, y \in Q$. In this case inverses are two-sided and $x_C^{\kappa_1} = x_C^{-1}$.*
(b) $\rho_1 \in \mathrm{Aut}(Q\mathbf{T})$ *if and only if Q has the left inverse property $x^{-1}(xy) = y$ for all $x, y \in Q$. In this case inverses are two-sided and $x_R^{\rho_1} = x_R^{-1}$.*
(c) $\epsilon_1 \in \mathrm{Aut}(Q\mathbf{T})$ *if and only if Q has the antiautomorphic inverse property $(xy)^{-1} = y^{-1}x^{-1}$ for all $x, y \in Q$. In this case inverses are two-sided and $x_E^{\epsilon_1} = x_E^{-1}$.*

PROOF. (a) Assume that κ_1 is an automorphism of $Q\mathbf{T}$, and let $x, y \in Q$. The two lines $\{x_R, 1_C, x_E\}$ and $\{xy_R, 1_C, xy_E\}$ are mapped to themselves by κ_1.



The image of the line $\{x_R, y_C, xy_E\}$ under κ_1 is then the line

$$\{x_R^{\kappa_1}, y_C^{\kappa_1}, xy_E^{\kappa_1}\} = \{x_E, y_C^{\kappa_1}, xy_R\} = \{xy_R, y_C^{\kappa_1}, x_E\}\,.$$

In the special case $x = 1$, this line is $\{y_R, y_C^{\kappa_1}, 1_E\}$. As $\{y_R, ({}^{-1}y)_C, 1_E\}$ is always a line, we must have $y_C^{\kappa_1} = ({}^{-1}y)_C$. Repeating this, we find $y_C = y_C^{\kappa_1\kappa_1} = ({}^{-1}({}^{-1}y))_C$. In particular $y = {}^{-1}({}^{-1}y)$, so inverses are two-sided.

Therefore in the general case the image line becomes $\{xy_R, y_C^{-1}, x_E\}$. But $\{xy_R, y_C^{-1}, (xy)y_E^{-1}\}$ is certainly a line of $Q\mathbf{T}$. We conclude that $x = (xy)y^{-1}$, the right inverse property.

Now assume that L has the right inverse property. In particular, inverses are two-sided by Lemma (2.11). The line $\{x_R, y_C, xy_E\}$ is a generic line of $Q\mathbf{T}$, and the picture above shows that its image under κ_1 is also a line (with the image of y_C under κ_1 defined to be y_C^{-1}). Therefore this κ_1 is a central automorphism of $Q\mathbf{T}$.

(b) This is equivalent to (a) for the opposite loop $(Q, \circ)$ given by $x \circ y = y \cdot x$ for all $x, y \in Q$.

(c) For arbitrary $x, y \in Q$ we always have in $Q\mathbf{T}$ the lines $(y^{-1}, y, 1)$ and $(x, {}^{-1}x, 1)$. Therefore the generic line (x, y, xy) would have as image under $\epsilon_1 \in \mathrm{Aut}(Q\mathbf{T})$ the line $(y^{-1}, {}^{-1}x, (xy_{\mathrm{E}})^{\epsilon_1})$. In this case setting $x = 1$ gives us $(y_{\mathrm{E}})^{\epsilon_1} = y_{\mathrm{E}}^{-1}$, while setting $y = 1$ gives $(x_{\mathrm{E}})^{\epsilon_1} = {}^{-1}x_{\mathrm{E}}$. Therefore ϵ_1 is in $\mathrm{Aut}(Q\mathbf{T})$ if and only if $(y^{-1}, x^{-1}, (xy)^{-1})$ is a line for all $x, y \in Q$, in which case inverses are two-sided. □

If ρ_1 and κ_1 $(= \rho_1\epsilon_1\rho_1)$ and ϵ_1 $(= \rho_1\kappa_1\rho_1)$ are automorphisms of $Q\mathbf{T}$, then the lemma tells us that Q is an inverse property loop. Furthermore it says that an inverse property loop always has two-sided inverses (as seen previously in Lemma (2.11)) and satisfies the antiautomorphic inverse property $(xy)^{-1} = y^{-1}x^{-1}$.

(3.13). Lemma. *Let Q be an inverse property loop. Then, for the element x of Q, we have $\epsilon_x \in \mathrm{Aut}(Q\mathbf{T})$ if and only if we have $(xa)(bx) = (x(ab))x$ for all a, b in Q. In this case $(xy)x = x(yx)$ and $y_{\mathrm{E}}^{\epsilon_x} = ((xy^{-1})x)_{\mathrm{E}} = (x(y^{-1}x))_{\mathrm{E}}$ for all y in Q.*

Proof. As we are in an inverse property loop, inverses are two-sided by Lemma (3.12) (or Lemma (2.11)).

Let x, a, b be arbitrary in the inverse property loop Q. We always have in $Q\mathbf{T}$ the lines (xa, a^{-1}, x) by the right inverse property and (b^{-1}, bx, x) by the left inverse property. The line $(b^{-1}, a^{-1}, (ab)^{-1})$ is the image of the generic line (a, b, ab) under ϵ_1—the antiautomorphic inverse property.

Suppose ϵ_x is an automorphism of $Q\mathbf{T}$. The image of the line $(b^{-1}, a^{-1}, (ab)^{-1})$ under ϵ_x would then be $(xa, bx, ((ab)^{-1})^{\epsilon_x})$. Setting $b = 1$ we find $(a_{\mathrm{E}}^{-1})^{\epsilon_x} = ((xa)x)_{\mathrm{E}}$ for all a whereas $a = 1$ gives $(b_{\mathrm{E}}^{-1})^{\epsilon_x} = (x(bx))_{\mathrm{E}}$.

As $(xa, bx, (xa)(bx))$ is always a line of $Q\mathbf{T}$, we see that ϵ_x is an automorphism of $Q\mathbf{T}$ if and only if $(xa)(bx)$ is equal to $((ab)^{-1})^{\epsilon_x}$ for all a, b. That is, if and only if $(xa)(bx) = (x(ab))x$ for all a, b. □

Proof of Theorem (3.9).

A Moufang loop is an inverse property loop by Proposition (2.12), so by Lemma (3.12) ρ_1 and κ_1 are automorphisms of $Q\mathbf{T}$. Next by Lemma (3.13) all ϵ_x are automorphisms. But then so are all $\rho_x = \kappa_1\epsilon_x\kappa_1$ and $\kappa_x = \rho_1\epsilon_x\rho_1$. This gives the forward direction of the theorem.

If all ρ_x, κ_x, and ϵ_x are automorphisms of $Q\mathbf{T}$, then especially Q is an inverse property loop by Lemma (3.12). Therefore by Lemma (3.13) the identity $(xa)(bx) = (x(ab))x$ holds for all $x, a, b \in Q$, and Q is a Moufang loop. □

3.4. Cayley tables of groups

Every Latin square is the Cayley table of a quasigroup. It is natural to wonder when the Latin square is the Cayley table of a group. According to [**DeK74**], the result goes back at least to Frolov [**Fro90**] and Brandt [**Bra27**], although in the loop theory community it is commonly associated with Reidermeister [**Rei29**]. (See Section 15.1 for further discussion.) Our treatment follows [**DeK74**, p.18-19].

For the Latin square E with rows and columns indexed by the set Q with the cell in row r and column c containing entry $e_{r,c}$ consider:

> **(QC) The Quadrangle Condition.** *In all cases, if $e_{au} = e_{cw}$, $e_{av} = e_{cx}$, and $e_{bu} = e_{dw}$, then $e_{bv} = e_{cx}$.*

That is, whenever in the Cayley table below we encounter the pattern seen above, then in fact $4 = 5$.

$\cdot$		u		v				w		x	
	$\ddots$		$\ddots$		$\ddots$		$\ddots$		$\ddots$		$\ddots$
a	$\dots$	1	$\dots$	2	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
	$\ddots$		$\ddots$		$\ddots$		$\ddots$		$\ddots$		$\ddots$
b	$\dots$	3	$\dots$	4	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
	$\ddots$		$\ddots$		$\ddots$		$\ddots$		$\ddots$		$\ddots$
	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
	$\ddots$		$\ddots$		$\ddots$		$\ddots$		$\ddots$		$\ddots$
c	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	1	$\dots$	2	$\dots$
	$\ddots$		$\ddots$		$\ddots$		$\ddots$		$\ddots$		$\ddots$
d	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	3	$\dots$	5	$\dots$
	$\ddots$		$\ddots$		$\ddots$		$\ddots$		$\ddots$		$\ddots$

(3.14). THEOREM. *The Latin square E is the Cayley table of a group if and only if it satisfies the Quadrangle Condition* **(QC)**.

PROOF. If E is the Cayley table of a group, then

$$e_{bv} = bv = bu(au)^{-1}av = dw(cw)^{-1}cx = dx = e_{dx}\,.$$

Now assume that E has the Quadrangle Condition, and select one of the loops with Cayley table E as was done in Section 2.1—choose a cell (say, the upper-lefthand corner) and then label the columns of E with the entries in that row and the rows with the entries in that column. The identity e of the loop is the entry from the original cell.

We claim that this loop is a group. Indeed, for arbitrary r, s, t, first look at the intersections of rows e and r and columns s and st to see the entries

$$\begin{array}{cc} s & st \\ rs & r(st) \end{array}$$

Next look at the intersections of rows s and rs and columns e and t and now find

$$\begin{array}{cc} s & st \\ rs & (rs)t \end{array}^{\cdot}$$

The Quadrangle Condition then gives $r(st) = (rs)t$, as claimed. □

In the proof, the specific choice of cell was not crucial. This is explained by Corollary (2.7) above.

Chapter 4

Groups with Triality

Lemma (3.5) motivates the following definition:

(4.1). Definition. *Let D be a conjugacy class of elements of order 2 in the group $G = \langle D \rangle$; and let $\pi\colon G \longrightarrow \mathrm{Sym}(3)$, the symmetric group on $\{1, 2, 3\}$, be a surjective group homomorphism. Further assume that*

$(*)$ *for all $d, e \in D$, if $d^\pi \neq e^\pi$, then $|de| = 3$.*

Then we say that (G, D, π) is a group with triality *or* triality group*. The normal subgroup $\ker \pi$ of index 6 in G is the* base group *of (G, D, π).*

We may abuse this by calling G itself a group with triality or a triality group when D and π are evident. The definition (in a different form—see Section 13.1 below) goes back to Doro [**Dor78**] and Glauberman [**Gla68**]. We shall refer to our triality and that of Doro-Glauberman as *abstract triality* in contrast to the motivating *concrete triality* of Cartan [**Car25**], which will be the topic of Part 4.

In Section 4.2.4 we shall see that the pair G and D does not always determine the map π uniquely, and similarly G and π need not determine D.

4.1. Basics

For each $d, e \in D$ with $d^\pi \neq e^\pi$ the condition $(*)$ is equivalent to $S = \langle d, e \rangle \simeq \mathrm{Sym}(3)$. In particular G is the split extension $\ker \pi \rtimes S$. Furthermore d and e are conjugate within $\langle d, e \rangle$, so it would have been enough to require D to be a normal set, conjugacy following directly.

If (G, D, π) and (G_0, D_0, π_0) are two groups with triality, then a *triality homomorphism* $f\colon (G, D, \pi) \longrightarrow (G_0, D_0, \pi_0)$ is a group homomorphism $f\colon G \longrightarrow G_0$ that additionally has $D^f \subseteq D_0$ and $\pi = f\pi_0$. We then have the category TriGrp whose object class is all groups with triality and whose morphisms are the triality homomorphisms.

Let (P, S) be a central Latin square design. Set $D = \{\, \tau_x \mid x \in P \,\}$ and $G = \langle D \rangle = \mathrm{CAut}(P, S)$, a normal subgroup of $\mathrm{Aut}(P, S)$. Further define the homomorphism $\pi\colon G \longrightarrow \mathrm{Sym}(3)$ to extend the map

$$\tau_x \mapsto \begin{cases} (2,3) & \text{for } x \in P^{\mathrm{R}} \\ (1,3) & \text{for } x \in P^{\mathrm{C}} \\ (1,2) & \text{for } x \in P^{\mathrm{E}} \end{cases}$$

Then $(P,S)\mathbf{A} = (G,D,\pi)$ is a group with triality by Lemma (3.5). The base group $\ker\pi$ is the intersection of $\mathrm{Aut}_{\mathsf{CLSD}}(P,S)$ with $\mathrm{CAut}(P,S)$.

Conversely, let (G,D,π) be a group with triality. Set $P = P_{(G,D,\pi)} = D$ with

$$P^{\mathrm{R}} = D \cap (2,3)^{\pi^{-1}}, \quad P^{\mathrm{C}} = D \cap (1,3)^{\pi^{-1}}, \quad P^{\mathrm{E}} = D \cap (1,2)^{\pi^{-1}}.$$

We let $S = S_{(G,D,\pi)}$ be the union of all the 3-subsets T^u of $P = D$ for $u \in \mathrm{Hom}_{\mathsf{TriGrp}}((\mathrm{Sym}(3), T, \mathrm{Id}_{\mathrm{Sym}(3)}), (G,D,\pi))$, where $T = \{(2,3),(1,3),(1,2)\}$. That is, the 3-subset T_0 of D is a line of $S_{(G,D,\pi)}$ precisely when $\langle T_0\rangle \simeq \mathrm{Sym}(3)$ is a complement to $\ker\pi$ in G. Then $(G,D,\pi)\mathbf{C} = (P,S)$ is a central Latin square design with the various elements of D naturally acting as central automorphisms by conjugation (hence the center of G acts trivially).

Because of the remarks of the previous paragraph, we call the various subgroups $I = \mathrm{Sym}(3)^u$ for $u \in \mathrm{Hom}_{\mathsf{TriGrp}}((\mathrm{Sym}(3), T, \mathrm{Id}_{\mathrm{Sym}(3)}), (G,D,\pi))$ the *lines* of the group with triality (G,D,π). A G-conjugate of a line is also a line. If I is a line, then D is the G-class containing the transpositions of I and π factors through the isomorphism of I with $\mathrm{Sym}(3)$.

(4.2). Lemma. *Let (G,D,π) be a group with triality.*

(a) *If the subgroup H of G contains a line I, then $H_0 = \langle I^H\rangle$ is itself a triality group with respect to the class $D_0 = D \cap H_0 = D \cap H$ and the projection π_0 equal to the restriction of π to H_0.*

(b) *If $f\colon (G,D,\pi) \longrightarrow (G_0,D_0,\pi_0)$ is a triality homomorphism, then* $\ker f$ *is a normal subgroup of G that is contained in* $\ker\pi$*.*

(c) *Conversely, let K be a normal subgroup of G that is contained in* $\ker\pi$*. Then there is a surjective triality homomorphism $f\colon (G,D,\pi) \longrightarrow (G_0,D_0,\pi_0)$ with* $\ker f = K$ *and (G_0,D_0,π_0) uniquely determined up to triality isomorphism.*

Proof. (a) This is clear.

(b) As $\pi = f\pi_0$ we must have $\ker f \le \ker\pi$.

(c) Set $G_0 = G/K$. The class D_0 is uniquely determined as that containing DK/K. Because $K \le \ker\pi$, the map π can be factored through $G/K = G_0$ as $f\pi_0$ for $\pi_0\colon G_0 \longrightarrow \mathrm{Sym}(3)$. Since f is surjective, $\pi = f\pi_0$ determines π_0 uniquely. □

We have a second category $\mathsf{TriGrp}^\star$ of groups with triality whose object class consists of all (G,D,π,I) with (G,D,π) is a group with triality and I a line in G. Again we can realize this category as a pointed category.

(4.3). Theorem. *The group with triality*

$$O = (\mathrm{Sym}(3), \{(2,3),(1,3),(1,2)\}, \mathrm{Id}_{\mathrm{Sym}(3)})$$

is a terminal object in TriGrp *but is not initial. The category* $\mathsf{TriGrp}^\star$ *is isomorphic to the pointed category* $\mathsf{TriGrp}^\star_O$*.*

Proof. As every morphism from (G,D,π) must be compatible with π, the object O is certainly terminal. The Cayley tables of nontrivial groups give nontrivial central Latin square designs hence triality groups (G,D,π) with $\ker\pi \ne 1$. In that case we can find distinct $d, e_1, e_2 \in D$ with $d^\pi \neq e_1^\pi = e_2^\pi$. For the lines $I_i = \langle d, e_i \rangle$ there are maps φ_i in $\mathrm{Hom}_{\mathsf{TriGrp}}(O, (G, D, \pi))$ with $O^{\varphi_i} = I_i$. Thus O is not initial in TriGrp.

If $\varphi \in \mathrm{Hom}_{\mathsf{TriGrp}}(O, (G, D, \pi))$ is an anchor, then $\varphi(O)$ is a line I_φ of (G, D, π). The isomorphism then takes the object (G, D, π, I_φ) of $\mathsf{TriGrp}^\star$ to $((G, D, \pi), \varphi)$ of $\mathsf{TriGrp}^\star_O$. □

The theorem allows us to identify the categories $\mathsf{TriGrp}^\star$ and $\mathsf{TriGrp}^\star_O$.

For $f \in \mathrm{Hom}_{\mathsf{TriGrp}}((G, D, \pi), (G_0, D_0, \pi_0))$, let $f\mathbf{C}$ act as the restriction map $f|_D$ on $P_{(G,D,\pi)} = D$ and as the corresponding induced map on $S_{(G,D,\pi)} = S$. If additionally $I^f = I_0$ so that $f \in \mathrm{Hom}_{\mathsf{TriGrp}^\star}((G, D, \pi, I), (G_0, D_0, \pi_0, I_0))$, set $D^{f\mathbf{C}^\star} = D^{f\mathbf{C}}$, $S^{f\mathbf{C}^\star} = S^{f\mathbf{C}}$, and $(I \cap D)^{f\mathbf{C}^\star} = I_0 \cap D_0$.

(4.4). Proposition.

(a) $\mathbf{C}\colon \mathsf{TriGrp} \longrightarrow \mathsf{CLSD}$ *is a faithful, dense functor.*

(b) $\mathbf{C}^\star\colon \mathsf{TriGrp}^\star \longrightarrow \mathsf{CLSD}^\star$ *is a faithful, dense functor.*

Proof. We first check $f\mathbf{C} \in \mathrm{Hom}_{\mathsf{CLSD}}((G, D, \pi)\mathbf{C}, (G_0, D_0, \pi_0)\mathbf{C})$. That is, for each $\{x, y, z\}$ is in $S_{(G,D,\pi)}$ we must make sure that $\{x, y, z\}^f$ belongs to $S_{(G_0,D_0,\pi_0)}$. As $\{x, y, z\}$ is in $S_{(G,D,\pi)}$, for $T = \{(2, 3), (1, 3), (1, 2)\}$ the definition gives a morphism $u \in \mathrm{Hom}_{\mathsf{TriGrp}}((\mathrm{Sym}(3), T, \mathrm{Id}_{\mathrm{Sym}(3)}), (G, D, \pi))$ with $\{x, y, z\} = T^u$. But then

$$\{x, y, z\}^f = (T^u)^f = T^{uf}$$

for uf in $\mathrm{Hom}_{\mathsf{TriGrp}}((\mathrm{Sym}(3), T, \mathrm{Id}_{\mathrm{Sym}(3)}), (G_0, D_0, \pi_0))$. That is, $\{x, y, z\}^f$ belongs to $S_{(G_0,D_0,\pi_0)}$, as desired.

For f as given and $g \in \mathrm{Hom}_{\mathsf{TriGrp}}((G_0, D_0, \pi_0), (G_1, D_1, \pi_1))$, we have

$$(fg)\mathbf{C} = fg|_D = f|_D\, g|_{D_0} = f\mathbf{C}g\mathbf{C}\,;$$

and $\mathbf{C}$ is indeed a functor.

Let $f, g \in \mathrm{Hom}_{\mathsf{TriGrp}}((G, D, \pi), (G_0, D_0, \pi_0))$. Then

$$f\mathbf{C} = g\mathbf{C} \iff f|_D = g|_D \iff f|_{\langle D \rangle} = g|_{\langle D \rangle} \iff f = g$$

since $G = \langle D \rangle$. Therefore $\mathbf{C}$ is faithful.

Finally $\mathbf{C}$ is dense as $(P, S) \in \mathsf{CLSD}$ is always isomorphic to $((P, S)\mathbf{A})\mathbf{C}$, giving (a).

Lemma (1.9) then gives us (b). □

In Proposition (7.12) below we shall see that neither $\mathbf{C}$ nor $\mathbf{C}^\star$ is full.

4.2. Examples

4.2.1. Wreath products. For H a group, the full *wreath product* $H \wr \mathrm{Sym}(n)$ is the split extension of the direct sum $B = \bigoplus_{i=1}^n H_i$, the *base group* of the wreath product, by the symmetric group $\mathrm{Sym}(n)$, naturally permuting the factors of the base with action given by $h_i^g = h_{i.g}$ for each $h \in H$ and $g \in \mathrm{Sym}(n)$.

Routine calculations give

(4.5). Proposition. *For arbitrary $k, h \in H$ and distinct indices a, b, c, d (as possible), we have:*

(a) $(a, b)^{H \wr \mathrm{Sym}(n)} \cap B(a, b) = \{\, h_a^{-1} h_b (a, b) \mid h \in H \,\}$;

(b) $\big(k_a^{-1}k_b(a,b)\big)^{h_a^{-1}h_b(c,d)} = k_a^{-1}k_b(a,b)$;

(c) $\big(k_a^{-1}k_b(a,b)\big)^{h_b^{-1}h_c(b,c)} = (kh)_a^{-1}(kh)_b(a,c)$;

(d) $\big(k_a^{-1}k_b(a,b)\big)^{h_a^{-1}h_b(a,b)} = (hk^{-1}h)_a^{-1}(hk^{-1}h)_b(a,b)$. □

The following elementary result is due to Zara [**Zar85**] and is also implicit (for $n = 3$) in Tits [**Tit58**] and Doro [**Dor78**]. (See also [**Hal06**].)

(4.6). THEOREM. *Let H be a group and let D be the conjugacy class of the full wreath product $H \wr \mathrm{Sym}(n)$ containing the transposition class of $\mathrm{Sym}(n)$, for $n \geq 3$, and set $\mathrm{Wr}(H, n) = \langle D\rangle$. Let the associated projection homomorphism be $\eta\colon H \wr \mathrm{Sym}(n) \longrightarrow \mathrm{Sym}(n)$.*

(a) *There is a bijection between H and $D \cap Bd$ for each $d \in D$.*
(b) *For all $d, e \in D$, if $|d^\eta e^\eta| = 2$ then $|de| = 2$.*
(c) *For all $d, e \in D$, if $|d^\eta e^\eta| = 3$ then $|de| = 3$.*
(d) *The quotient $(H \wr \mathrm{Sym}(n))/\mathrm{Wr}(H, n)$ is isomorphic to H/H'.*

PROOF. For $t, r \in T$, if $|t^\eta r^\eta| = 2$, then $t^\eta = (a, b)$ and $r^\eta = (c, d)$ for distinct a, b, c, d. Therefore $t^r = t$ by Proposition (4.5)(b), so $|tr| = 2$, giving (b).

If $|t^\eta r^\eta| = 3$, then there are $h, k \in H$ and distinct a, b, c with $t = k_a^{-1}k_b(a, b)$ and $r = h_b^{-1}h_c(b, c)$. By Proposition (4.5)(c), $t^r = (kh)_a^{-1}(kh)_c(a, c)$. Also by Proposition (4.5)(c)

$$r^t = \big((h^{-1})_c^{-1}(h^{-1})_b(c,b)\big)^{(k^{-1})_b^{-1}(k^{-1})_a(b,a)} = (h^{-1}k^{-1})_c^{-1}(h^{-1}k^{-1})_a(c,a)\,.$$

Therefore $r^t = (kh)_a^{-1}(kh)_c(a, c) = t^r$, so that $(tr)^3 = (trt)(rtr) = (r^t)(t^r) = 1$, giving (c).

By (c), the conjugacy class of transpositions remains a class in $\mathrm{Wr}(H, n)$, so (a) follows from Proposition (4.5)(a).

By Proposition (4.5)(d), the group $\mathrm{Wr}(H, n)$ contains the derived group $B' = \oplus_{i=1}^n H_i'$, while the image of $B\cap\mathrm{Wr}(H, n)/B'$ is spanned by the images of the various $h_a^{-1}h_b$ by Proposition (4.5)(c). Therefore $B/B\cap\mathrm{Wr}(H, n) \simeq (H\wr\mathrm{Sym}(n))/\mathrm{Wr}(H, n)$ is a copy of H/H', as in (d). □

This immediately gives

(4.7). COROLLARY. *Let D be the transposition class of $H \wr \mathrm{Sym}(3)$ or $H \wr \mathrm{Sym}(4)$, respectively, and let G be the subgroup generated by D—respectively $\mathrm{Wr}(H, 3)$ and $\mathrm{Wr}(H, 4)$.*

(a) *(G, D, π) is a group with triality, where in the first case π is η and in the second π is η followed by the projection from $\mathrm{Sym}(4)$ onto $\mathrm{Sym}(3)$.*
(b) *$|D|$ is equal to $3|H|$ for $\mathrm{Wr}(H, 3)$ and $6|H|$ for $\mathrm{Wr}(H, 4)$.*
(c) *The quotients $(H\wr\mathrm{Sym}(3))/\mathrm{Wr}(H, 3)$ and $(H\wr\mathrm{Sym}(4))/\mathrm{Wr}(H, 4)$ are isomorphic to H/H'. In particular if H is perfect then $H \wr \mathrm{Sym}(3) = \mathrm{Wr}(H, 3)$ and $H \wr \mathrm{Sym}(4) = \mathrm{Wr}(H, 4)$.* □

Not surprisingly the corresponding loop $\mathrm{Wr}(H, 3)$**CS** is the group H, as we shall verify in Theorem (10.1) below. The loops $\mathrm{Wr}(H, 4)$**CS** are precisely the Chein generalized dihedral loops of Theorem (2.16); see Theorem (10.2) below as well as [**GrZ06**, Prop. 1] and [**Hal06**, §4].

4.2.2. Weyl groups.

This entire monograph could be viewed as a riff on the tame observation that the Weyl group of type A_2 is the symmetric group of degree 3.

(4.8). PROPOSITION.

(a) $\mathrm{W}(A_2) = \langle\, r, c \mid r^2 = c^2 = 1,\ (rc)^3 = 1\,\rangle \simeq \mathrm{Sym}(3)$.
(b) $\mathrm{W}(\widetilde{A}_2) = \langle\, r, c, e \mid r^2 = c^2 = e^2 = 1,\ (rc)^3 = (re)^3 = (ce)^3 = 1\,\rangle \simeq \mathbb{Z}^2 \rtimes \mathrm{Sym}(3)$.
(c) $\mathrm{W}(A_3) = \langle\, r_1, r_2, c \mid r_i^2 = c^2 = 1, (r_ic)^3 = 1,\ (r_ir_j)^2 = 1\,\rangle \simeq \mathrm{Sym}(4)$.
(d) $\mathrm{W}(D_4) = \langle\, r_1, r_2, r_3, c \mid r_i^2 = c^2 = 1, (r_ic)^3 = 1,\ (r_ir_j)^2 = 1\,\rangle \simeq Z_2^3 \rtimes \mathrm{Sym}(4)$.
(e) $\mathrm{W}(\widetilde{D}_4) = \langle\, r_1, r_2, r_3, r_4, c \mid r_i^2 = c^2 = 1, (r_ic)^3 = 1, (r_ir_j)^2 = 1.\,\rangle \simeq \mathbb{Z}^4 \rtimes \mathrm{W}(D_4)$.

PROOF. See for instance [**Hum90**]. These all can be calculated directly without difficulty. □

In each of these Weyl groups the generators belong to the same conjugacy class, the reflection class D. The projection maps π given by

$$r\,,\ r_i \mapsto r \quad c \mapsto c \quad e \mapsto rcr$$

describe homomorphisms of each onto $\mathrm{W}(A_2) \simeq \mathrm{Sym}(3)$.

We write $\mathrm{W}_n(\widetilde{A}_2)$ and $\mathrm{W}_n(\widetilde{D}_4)$ for the quotients (respectively) of $\mathrm{W}(\widetilde{A}_2)$ and $\mathrm{W}(\widetilde{D}_4)$ by n times their root lattice subgroups—$n\mathbb{Z}^2$ and $n\mathbb{Z}^4$. These are isomorphic to (respectively) $Z_n^2 \rtimes \mathrm{Sym}(3)$ and $Z_n^4 \rtimes \mathrm{W}(D_4)$; for instance $\mathrm{W}_2(\widetilde{A}_2) \simeq \mathrm{Sym}(4)$.

Keeping Corollary (4.7) in mind, we easily find the following lemmas.

(4.9). LEMMA.

(a) $\mathrm{W}(\widetilde{A}_2) \simeq \mathrm{Wr}(\mathbb{Z}, 3) \simeq \mathbb{Z}^2 \rtimes \mathrm{Sym}(3)$ *is a group with triality.*
(b) *The center of* $\mathrm{W}_n(\widetilde{A}_2)$ *is cyclic of order* $\gcd(n, 3)$.
(c) $\mathrm{W}_4(\widetilde{A}_2) \simeq \mathrm{Wr}(Z_4, 3) \simeq Z_4^2 \rtimes \mathrm{Sym}(3)$ *is a group with triality containing* 12 *transpositions. It has trivial center.* □

(4.10). LEMMA. $\mathrm{W}(D_4) \simeq \mathrm{Wr}(Z_2, 4)$ *is a group with triality containing* 12 *transpositions. It has center of order* 2 *and* $\mathrm{W}(D_4)/\mathrm{Z}(\mathrm{W}(D_4)) \simeq \mathrm{Wr}(Z_2 \times Z_2, 3)$. □

(4.11). LEMMA.

(a) $\mathrm{W}(\widetilde{D}_4) \simeq \mathrm{Wr}(\,D_\infty, 4) \simeq \mathbb{Z}^4 \rtimes \mathrm{W}(D_4)$ *is a group with triality. (Here* D_∞ *is a dihedral group of infinite order.)*
(b) $\mathrm{W}_3(\widetilde{D}_4) \simeq \mathrm{Wr}(\mathrm{Sym}(3), 4) \simeq Z_3^4 \rtimes \mathrm{W}(D_4)$ *is a group with triality containing* 36 *transpositions. It has trivial center and has no triality subgroups* $\mathrm{W}_4(\widetilde{A}_2)$ *or* $\mathrm{W}(D_4)/\mathrm{Z}(\mathrm{W}(D_4))$. □

4.2.3. Cartan's triality groups.

Cartan's triality group $\mathrm{P}\Omega_8^+(F) \rtimes \mathrm{Sym}(3)$ of type D_4 [**Car25**] over F is a group with triality in our sense, as verified by Tits [**Tit58**]. This is concrete triality (mentioned at the beginning of this chapter) and the example that motivated Doro's original terminology [**Dor78**]. We shall return to the group and its triality in Part 4 below, particularly in Chapter 18. (See also [**GrZ06, Hal11, NVo03**].)

4.2.4. Nonuniqueness.

The group $G = 3^n \rtimes 2$ gives an example of a group with triality (G, D, π) in which G and D do not determine π uniquely as $\ker \pi$ may be chosen to be any subgroup of index 3 in the normal subgroup 3^n. The group $G = \mathrm{W}(D_4)$ gives an example where G and π do not determine D uniquely. Indeed, if z is an element of order 2 in the center of (G, D, π), then (G, zD, π) is also a group with triality.

4.3. Normal subgroups in the base group and wreath products

In Doro's [**Dor78**] original treatment of groups with triality (G, D, π, I), the focus was actually the base group $K = \ker \pi$, admitting a group I isomorphic to Sym(3) acting in a prescribed fashion, as will be described precisely in the introduction to Chapter 13. There we call the pair (K, I) a *group admitting triality* to distinguish it from the group with triality $G = K \rtimes I$.

Recall that the *second center* of the group G, denoted $\mathrm{Z}_2(G)$, is the preimage in G of $\mathrm{Z}(G/\mathrm{Z}(G))$.

(4.12). Lemma. *Let (G, D, π) be a group with triality and I a line with $D \cap I = \{d, e, f\}$. Further let K be a normal subgroup of G that is contained in $\ker \pi$.*

(a) *$G' = \langle\, ab \mid a, b \in D\,\rangle$ of index 2 in G and $\mathrm{Z}(G)G'' \le \ker \pi$.*
(b) *$\ker \pi = [\ker \pi, I] = \langle\, ab \mid a, b \in D\,,\ a \ker \pi = b \ker \pi\,\rangle$.*
(c) *$K\mathrm{Z}(G) = \ker \pi$ if and only if $K = \ker \pi$.*
(d) *$D \cap Kd = d^K = d^{[K,I]}$, and for $H = [K, I]I$ the triple $(H, D \cap H, \pi|_H)$ is a group with triality.*
(e) *$\mathrm{Z}(G) = \mathrm{Z}_2(G)$ and $D \cap \mathrm{Z}(G)d = \{d\}$.*
(f) *$[K, G] = [K, G, G] = \langle\, ab \mid a, b \in D,\ Ka = Kb\,\rangle$.*

Proof.

(a) Any group generated by a conjugacy class of involutions has derived group of index at most 2. Here $G^\pi \simeq \mathrm{Sym}(3)$.
(b) Set $K = \langle\, ab \mid a, b \in D\,,\ a \ker \pi = b \ker \pi\,\rangle$. The subgroup $[\ker \pi, I]I$ is contained in $K \rtimes I$ and contains all D and so equals G. In particular $\ker \pi = [\ker \pi, I] = K$.
(c) This follows immediately from the previous part.
(d) For $d_0 \in D \cap Kd$ the group $\langle d_0, e\rangle$ is symmetric of degree three, so d_0, e, and d are all conjugate within $KI = IK$. Therefore

$$D \cap KI = \{d, e, f\}^{IK} = \{d, e, f\}^K = D \cap I^K$$

and $D \cap Kd = d^K$.

The subgroup $[K, I]I$ of KI contains I^K and so is equal to $\langle D \cap KI\rangle$. As before $D \cap KI = \{d, e, f\}^{[K,I]}$ and $d^K = D \cap Kd = d^{[K,I]}$. Indeed this shows for $[K, I]I = H$ that $D \cap H = d^H$ generates H and so H is a group with triality.
(e) For $K = \mathrm{Z}_2(G)$, from (d)

$$\{d\} \subseteq D \cap \mathrm{Z}_2(G)d = d^{\mathrm{Z}_2(G)} = d^{[\mathrm{Z}_2(G), I]} \subseteq d^{\mathrm{Z}(G)} = \{d\}\,.$$

Especially $\mathrm{Z}_2(G)$ centralizes every $d \in D$ and so centralizes $G = \langle D\rangle$, hence $\mathrm{Z}(G) \le \mathrm{Z}_2(G) \le \mathrm{Z}(G)$.
(f) Since the conjugacy class D generates G,

$$[K, G] = \langle\, [K, b] \mid b \in D\,\rangle = \langle\, [K, J] \mid J \text{ a line}\,\rangle\,.$$

By (b) and (d) we have $[K,J]=[K,J,J]$ for all lines J, so $[K,G]=[K,G,G]$. Then

$$\begin{aligned}[K,G] &= \langle\, [K,b] \mid b\in D\,\rangle \\ &= \langle\, k^{-1}bkb \mid b\in D,\ k\in K\,\rangle \\ &= \langle\, b^k b \mid b\in D,\ k\in K\,\rangle \\ &= \langle\, ab \mid a,b\in D,\ a\in Kb\,\rangle\end{aligned}$$

by (d), as desired. □

(4.13). Proposition. *Let (G,D,π) be a group with triality, and set $K=\ker\pi$. The action of G by conjugation on the class D gives a group homomorphism from G to $M\wr\mathrm{Sym}(3)$ with kernel equal to $\mathrm{Z}(G)$. Then $K/\mathrm{Z}(G)$ is the intersection of $G/\mathrm{Z}(G)$ with the wreath product base group $M_1\oplus M_2\oplus M_3$; and, for each i, the projection of $K/Z(G)$ onto M_i is a surjection.*

Proof. As before, let $I\simeq\mathrm{Sym}(3)$ be a line with $I\cap D=\{r,c,e\}$.

The group $G=\langle D\rangle$ acts on the class D by conjugation with kernel $\mathrm{C}_G(D)=\mathrm{Z}(G)$. By the lemma, this permutation action is imprimitive, respecting the equivalence relation with classes $D\cap Kr=r^K$, $D\cap Kc=c^K$, and $D\cap Ke=e^K$. Here I permutes the three classes as $\mathrm{Sym}(3)$ and K the kernel of this action. This gives the desired wreath product action, where M is the group induced by K on any one of the equivalence classes. □

The proposition motivates our calling $\ker\pi$ the base group of the group with triality (G,D,π). The group M will be discussed in Section 12.3. Some care must be taken. For instance for the triality groups $\mathrm{Wr}(H,3)$ of the previous section, the corresponding group M will rarely be isomorphic to H. Indeed if H is nonabelian and simple, then M is isomorphic to $H\times H$.

Part 2

Equivalence

Chapter 5

The Functor **B**

We already have the most familiar version of “essential equivalence”:

$$\begin{tikzcd}\mathsf{Mouf} \arrow[r, shift left, "\mathbf{T}"] & \mathsf{CLSD} \arrow[l, shift left, "\mathbf{S}"] \arrow[r, shift left, "\mathbf{A}"] & \mathsf{TriGrp} \arrow[l, shift left, "\mathbf{C}"]\end{tikzcd}$$

Here $(\mathbf{T}, \mathbf{S})$ is the equivalence of Mouf and CLSD guaranteed by Theorem (3.11), and $\mathbf{A}$ and $\mathbf{C}$ are the “automorphism” and “central design” maps of Chapter 4.

From the categorical point of view this is incomplete and imperfect. Proposition (4.4) above said that $\mathbf{C}$ is a functor, but Corollary (7.11) below will show that it does not give an equivalence. More seriously, the map $\mathbf{A}$ is not a functor (as we shall see in Corollary (9.20) below).

In this chapter we construct a functor $\mathbf{B}$ to take the place of $\mathbf{A}$. As with $\mathbf{T}$ we initially construct $\mathbf{B}$ as a functor from LSD to TriGrp and then examine its restriction to the subcategory CLSD.

5.1. A presentation

(5.1). Presentation. *For the Latin square design (P, S), the group $\mathrm{G}(P, S)$ has the following presentation:*

Generators:

$\tilde{p}$, for arbitrary $p \in P$;

Relations:

for arbitrary $p \in P$ and $\{p, q, r\} \in S$:

(1) $\tilde{p}^2 = 1$;

(2) $\tilde{p}\tilde{q}\tilde{p} = \tilde{r}$.

In the remaining lemmas of this section, let (P, S) be a fixed but arbitrary Latin square design.

(5.2). Lemma. *The map*

$$\tilde{x} \mapsto \begin{cases} (2,3) & \text{for } x \in P^{\mathrm{R}} \\ (1,3) & \text{for } x \in P^{\mathrm{C}} \\ (1,2) & \text{for } x \in P^{\mathrm{E}} \end{cases}$$

extends to a homomorphism $\pi_{(P,S)}$ of $\mathrm{G}(P, S)$ onto $\mathrm{Sym}(3)$. For every line $I \in S$, the subgroup $\langle \tilde{I} \rangle$ is isomorphic to $\mathrm{Sym}(3)$ and is a complement to $\ker \pi_{(P,S)}$.

Proof. The line $I = \{p, q, r\}$ of S meets each of P^{R}, P^{C}, P^{E} exactly once. Therefore the image of I is $\{(2,3), (1,3), (1,2)\}$. Certainly we have $(2,3)^2 = (1,3)^2 = (1,2)^2 = 1$, and in all cases we also have $(a,b)(a,c)(a,b) = (b,c)$. Therefore the group $\mathrm{G}(P,S)$ maps onto $\mathrm{Sym}(3)$ with the restriction to each subgroup $\langle \tilde{p}, \tilde{q}, \tilde{r}\rangle$ an isomorphism. □

(5.3). Lemma. *$\tilde{P} = \{\, \tilde{p} \mid p \in P\,\}$ is a conjugacy class of elements of order 2 in $\mathrm{G}(P,S)$, and $(\mathrm{G}(P,S), \tilde{P}, \pi_{(P,S)})$ is a group with triality. Every line of $(\mathrm{G}(P,S), \tilde{P}, \pi_{(P,S)})$ is $\langle \tilde{I}\rangle$ for some line I of S.*

Proof. The previous lemma implies that $\tilde{P}$ consists of elements of order 2. Also elements $\tilde{q}$ and $\tilde{r}$ with different images under $\pi_{(P,S)}$ are conjugate, so $\tilde{P}$ is contained in a single conjugacy class.

Since $\tilde{P}$ is a generating set, it itself is a class provided $\tilde{p}^{\tilde{a}} \in \tilde{P}$ for all $p, a \in P$. This is clear by the relations when p and a are from different fibers, so we assume they are in the same fiber. Let $\{p, q, r\} \in S$. Then, as just mentioned, $\tilde{q}^{\tilde{a}}$ and $\tilde{r}^{\tilde{a}}$ both belong to $\tilde{P}$; so $\tilde{p}^{\tilde{a}} = \tilde{q}^{\tilde{a}}\tilde{r}^{\tilde{a}}\tilde{q}^{\tilde{a}}$ does as well.

We thus have $\tilde{P}$ a conjugacy class of elements of order 2 in the group $\mathrm{G}(P,S) = \langle \tilde{P}\rangle$ and $\pi_{(P,S)} \colon G \longrightarrow \mathrm{Sym}(3)$ a surjective group homomorphism. Furthermore, for every $\tilde{p}, \tilde{q} \in \tilde{P}$ with $\tilde{p}^{\pi(P,S)} \neq \tilde{q}^{\pi(P,S)}$, the order of $\tilde{p}\tilde{q}$ is 3, as can be checked within $\langle \tilde{p}, \tilde{q}\rangle \simeq \mathrm{Sym}(3)$. That is, $(\mathrm{G}(P,S), \tilde{P}, \pi_{(P,S)})$ is a group with triality.

Let T be a line of $(\mathrm{G}(P,S), \tilde{P}, \pi_{(P,S)})$ with $T \cap \tilde{P} = \{x, y, z\}$. Then there are p, q in different fibers of P with $x = \tilde{p}$ and $y = \tilde{q}$. There is a line I of S with $I = \{p, q, r\}$ so that $T_0 = \langle \tilde{p}, \tilde{q}, \tilde{r}\rangle$ is a line of $(\mathrm{G}(P,S), \tilde{P}, \pi_{(P,S)})$. As $T \cap T_0$ contains the generators $x = \tilde{p}$ and $y = \tilde{q}$ we must have $z = \tilde{r}$ and $T = T_0 = \langle \tilde{p}, \tilde{q}, \tilde{r}\rangle = \langle \tilde{I}\rangle$.
□

(5.4). Lemma. *The map $t \colon P \longrightarrow \tilde{P}$ given by $p^t = \tilde{p}$ is a bijection if and only if (P,S) is a central Latin square design. In this case the induced map $t \colon I \mapsto \langle \tilde{I}\rangle$ gives a bijection of the set S of lines of (P,S) and the set of lines of $(\mathrm{G}(P,S), \tilde{P}, \pi_{(P,S)})$.*

Proof. If (P,S) is a central Latin square design, then by Lemma (3.5) the bijection $\tilde{p} \mapsto \tau_p$ extends to a homomorphism from $\mathrm{G}(P,S)$ onto $\mathrm{CAut}(P,S)$. Therefore the bijection $p \mapsto \tau_p$ factors through t, which thus must also be a bijection.

Conversely, assume that t is a bijection. Choose a fixed but arbitrary a in the fiber P^{X}, and define $\alpha \in \mathrm{Sym}(P)$ by $x^{\alpha} = (\tilde{x}^{\tilde{a}})^{t^{-1}}$ for all $x \in P$. Let $\{p, q, r\} \in S$. Then $\langle \tilde{p}, \tilde{q}, \tilde{r}\rangle$ is a line of $(\mathrm{G}(P,S), \tilde{P}, \pi_{(P,S)})$ as is

$$\langle \tilde{p}, \tilde{q}, \tilde{r}\rangle^{\tilde{a}} = \langle \tilde{p}^{\tilde{a}}, \tilde{q}^{\tilde{a}}, \tilde{r}^{\tilde{a}}\rangle = \langle \widetilde{p^{\alpha}}, \widetilde{q^{\alpha}}, \widetilde{r^{\alpha}}\rangle\,.$$

As t is a bijection, $\{p^{\alpha}, q^{\alpha}, r^{\alpha}\} = \{p, q, r\}^{\alpha} \in S$; so α is an automorphism of (P,S). Since α acts as τ_a on $P \setminus P^{\mathrm{X}}$, we have $\alpha = \tau_a$ by Lemma (3.5).

By the previous lemma the map induced by t from S to the line set of the group $(\mathrm{G}(P,S), \tilde{P}, \pi_{(P,S)})$ is surjective. When t is bijective on P it must also be injective on S. □

5.2. The functor B

Let the map $\mathbf{B} \colon \mathsf{ObjLSD} \longrightarrow \mathsf{ObjTriGrp}$ be given by

$$(P,S)\mathbf{B} = (\mathrm{G}(P,S), \tilde{P}, \pi_{(P,S)})\,.$$

Similarly $\mathbf{B}^\star\colon \mathrm{Obj}\mathsf{LSD}^\star \longrightarrow \mathrm{Obj}\mathsf{TriGrp}^\star$ is given by

$$(P,S,I)\mathbf{B} = (\mathrm{G}(P,S), \tilde{P}, \pi_{(P,S)}, \langle \tilde{I} \rangle)\,.$$

Set $G = (\mathrm{G}(P,S), \tilde{P}, \pi_{(P,S)})$ and $G_0 = (\mathrm{G}(P_0,S_0), \tilde{P}_0, \pi_{(P_0,S_0)})$, and suppose $\varphi = (\alpha,\beta,\gamma)$ is in $\mathrm{Hom}_{\mathsf{LSD}}((P,S),(P_0,S_0))$. Let f from $\tilde{P} = P^t$ to $\tilde{P}_0 = P_0^{t_0}$ be given by

$$(x^t)^f = \tilde{x}^f = \begin{cases} \widetilde{x^\alpha} = (x^\alpha)^{t_0} & \text{for } x \in P^{\mathrm{R}} \\ \widetilde{x^\beta} = (x^\beta)^{t_0} & \text{for } x \in P^{\mathrm{C}} \\ \widetilde{x^\gamma} = (x^\gamma)^{t_0} & \text{for } x \in P^{\mathrm{E}} \end{cases}$$

This is summarized in a commutative diagram:

$$\begin{tikzcd}
P \arrow[r, "t"] \arrow[d, "\varphi"'] & \tilde{P} = D \arrow[d, "f\ (=\varphi\mathbf{B})"] \\
P_0 \arrow[r, "t_0"] & \tilde{P}_0 = D_0
\end{tikzcd}$$

As we shall next see, the map f on D uniquely determines the morphism $\varphi\mathbf{B} \in \mathrm{Hom}_{\mathsf{TriGrp}}(G,G_0)$. Therefore it will only be a mild abuse to replace f with $\varphi\mathbf{B}$ in the above commutative diagram (as indicated parenthetically).

(5.5). Lemma.

(a) *f extends uniquely to $\varphi\mathbf{B} \in \mathrm{Hom}_{\mathsf{TriGrp}}(G,G_0)$.*

(b) *If $(P,S),(P_0,S_0)$ are both designs in CLSD, then the map $\varphi \mapsto \varphi\mathbf{B}$ is a bijection of $\mathrm{Hom}_{\mathsf{LSD}}((P,S),(P_0,S_0))$ and $\mathrm{Hom}_{\mathsf{TriGrp}}(G,G_0)$ uniquely determined by $t^{-1}\varphi t_0 = \varphi\mathbf{B}|_{\tilde{P}}$.*

Proof. (a) By definition $\pi_{(P,S)} = f\pi_{(P_0,S_0)}$ on $\tilde{P}$ and $\tilde{P}^f \subseteq \tilde{P}_0$. Therefore we need only prove that f extends to a group homomorphism from $\mathrm{G}(P,S) = \langle \tilde{P} \rangle$ to $\mathrm{G}(P_0,S_0)$. It suffices to show that each relation of $\mathrm{G}(P,S)$ is mapped to a relation valid in $\mathrm{G}(P_0,S_0)$.

Clearly $(\tilde{x}^f)^2 = 1$ for each $\tilde{x} \in \tilde{P}$.

Let $(p,q,r) \in P^{\mathrm{R}} \times P^{\mathrm{C}} \times P^{\mathrm{E}}$ be a line of S. The relation $\tilde{p}\tilde{q}\tilde{p} = \tilde{r}$ for $\mathrm{G}(P,S)$ becomes under f the candidate relation $\tilde{p}^f\tilde{q}^f\tilde{p}^f = \tilde{r}^f$; that is, $p^{tf}q^{tf}p^{tf} = r^{tf}$.

The set $\{p,q,r\}^\varphi = \{p^\alpha, q^\beta, r^\gamma\}$ is a line of S_0, and so $T_0 = \langle p^{\alpha t_0}, q^{\beta t_0}, r^{\gamma t_0} \rangle$ is a line of $(\mathrm{G}(P_0,S_0), \tilde{P}_0, \pi_{(P_0,S_0)})$ with $T_0 \cap \tilde{P}_0 = \{p^{\alpha t_0}, q^{\beta t_0}, r^{\gamma t_0}\}$. Within T_0 we calculate that

$$p^{tf}q^{tf}p^{tf} = p^{\alpha t_0}q^{\beta t_0}p^{\alpha t_0} = r^{\gamma t_0} = r^{tf}\,,$$

as required. The images under f of the other $\mathrm{G}(P,S)$ relations $\tilde{a}\tilde{b}\tilde{a} = \tilde{c}$ associated with the line $\{p,q,r\} = \{a,b,c\}$ can be verified within $T_0 = \langle p^{tf}, q^{tf}, r^{tf} \rangle \simeq \mathrm{Sym}(3)$ as well.

(b) Under (a) we have seen that the restriction f of $\varphi\mathbf{B}$ to $\tilde{P}$ satisfies

$$t\varphi\mathbf{B}|_{\tilde{P}} = tf = \varphi t_0\,.$$

The previous lemma tells us that t and t_0 are bijections on P and P_0 and respect lines. As $\mathrm{G}(P,S)$ is generated by $\tilde{P}$, the morphisms φ and $\varphi\mathbf{B}$ uniquely determine each other via

$$t^{-1}\varphi t_0 = \varphi\mathbf{B}|_{\tilde{P}} \quad \text{and} \quad \varphi = t(\varphi\mathbf{B}|_{\tilde{P}})t_0^{-1}\,. \qquad \square$$

Suppose $\varphi^\star$ is in $\mathrm{Hom}_{\mathsf{LSD}^\star}((P,S,I),(P_0,S_0,I_0))$. By the forgetful functor, we have also $\varphi^\star$ in $\mathrm{Hom}_{\mathsf{LSD}}((P,S),(P_0,S_0))$. Then $\varphi^\star\mathbf{B}$ naturally induces

$$\varphi^\star\mathbf{B}^\star \in \mathrm{Hom}_{\mathsf{TriGrp}^\star}((\mathrm{G}(P,S),\tilde{P},\pi_{(P,S)},\langle\tilde{I}\rangle),(\mathrm{G}(P_0,S_0),\tilde{P_0},\pi_{(P_0,S_0)},\langle\tilde{I_0}\rangle))\,.$$

(5.6). Theorem.

(a) $\mathbf{B}\colon \mathsf{LSD} \longrightarrow \mathsf{TriGrp}$ *is a functor that is additionally full and faithful when restricted to the subcategory* CLSD.

(b) $\mathbf{B}^\star\colon \mathsf{LSD}^\star \longrightarrow \mathsf{TriGrp}^\star$ *is a functor that is additionally full and faithful when restricted to the subcategory* $\mathsf{CLSD}^\star$.

Proof. We have $\mathbf{B}$ defined on LSD and $\mathbf{B}^\star$ on $\mathsf{LSD}^\star$, but we must prove functoriality.

Let φ be in $\mathrm{Hom}_{\mathsf{LSD}}((P,S),(P_0,S_0))$ and φ_0 in $\mathrm{Hom}_{\mathsf{LSD}}((P_0,S_0),(P_1,S_1))$. Let f denote the restriction of $\varphi\mathbf{B}$ to $\tilde{P}$ and f_0 the restriction of $\varphi_0\mathbf{B}$ to $\tilde{P_0}$. From Lemma (5.5) we have $tf = \varphi t_0$ and $t_0 f_0 = \varphi_0 t_1$. Therefore

$$tff_0 = \varphi t_0 f_0 = \varphi\varphi_0 t_1\,.$$

This implies $\varphi\varphi_0\mathbf{B}|_{\tilde{P}} = ff_0 = \varphi\mathbf{B}|_{\tilde{P}}\varphi_0\mathbf{B}|_{\tilde{P_0}}$, hence $\varphi\varphi_0\mathbf{B} = \varphi\mathbf{B}\varphi_0\mathbf{B}$. We conclude that $\mathbf{B}$ is a functor, as is $\mathbf{B}^\star$.

By Lemma (5.5)(b), on the subcategory CLSD the functor $\mathbf{B}$ is full and faithful, and so $\mathbf{B}^\star$ on $\mathsf{CLSD}^\star$ is also by Lemma (1.9). □

In Proposition (7.12) below we shall see that $\mathbf{B}$ from CLSD is not dense, nor is $\mathbf{B}^\star$ from $\mathsf{CLSD}^\star$.

Chapter 6

Monics, Covers, and Isogeny in TriGrp

We now have a more categorical version of "essential equivalence":

$$\begin{tikzcd} \mathsf{Mouf} \arrow[r, shift left, "\mathbf{T}"] & \mathsf{CLSD} \arrow[l, shift left, "\mathbf{S}"] \arrow[r, shift left, "\mathbf{B}"] & \mathsf{TriGrp} \arrow[l, shift left, "\mathbf{C}"] \end{tikzcd}$$

Unfortunately, the pair $(\mathbf{B},\mathbf{C})$ still does not guarantee equivalence. The functor $\mathbf{BC}$ on CLSD is indeed faithful, full, and dense. However $\mathbf{CB}$ on TriGrp, while faithful (as $\mathbf{C}$ and $\mathbf{B}$ are), is neither full nor dense. The study of the functor $\mathbf{U} = \mathbf{CB}$ and its image in TriGrp will be the main topic of the next chapter. This requires a careful study in the present chapter of the monic morphisms in TriGrp.

6.1. A fibered product

Let (G_1, D_1, π_1, I_1) and (G_2, D_2, π_2, I_2) be groups with triality. Then $G_1 \times G_2$ is not a triality group, but we can easily construct one from it by taking an index 6 subgroup $(\ker \pi_1 \times \ker \pi_2) \rtimes I$, where $I \simeq \mathrm{Sym}(3)$ sits on the diagonal of $I_1 \times I_2$. The resulting group with triality is nearly the direct product and corresponds (under $\mathbf{CS}$) to the direct product of the associated Moufang loops. This is the degenerate case $N_i = \ker \pi_i$ of the following fibered product construction.

(6.1). Proposition. *Let (G_1, D_1, π_1, I_1) and (G_2, D_2, π_2, I_2) be objects in $\mathsf{TriGrp}^\star$. For $i \in \{1, 2\}$ assume there are normal subgroups N_i of G_i contained in $\ker \pi_i$ such that, for $\bar{G}_i = G_i/N_i$, the two groups with triality $(\bar{G}_1, \bar{D}_1, \bar{\pi}_1, \bar{I}_1)$ and $(\bar{G}_2, \bar{D}_2, \bar{\pi}_2, \bar{I}_2)$ are isomorphic via $\delta \colon \bar{G}_1 \longrightarrow \bar{G}_2$.*

Let H be the subgroup $\{ (g_1, g_2) \mid \bar{g}_1^\delta = \bar{g}_2 \}$ of $G_1 \times G_2$, the δ-diagonal modulo $N_1 \times N_2$. In H set $D_\infty = \{ (d_1, d_2) \mid d_1 \in D_1,\ d_2 \in D_2,\ \bar{d}_1^\delta = \bar{d}_2 \}$ and $G_\infty = \langle D_\infty \rangle$. Further let $I_\infty = \langle D_\infty \cap (I_1 \times I_2) \rangle$, isomorphic to $\mathrm{Sym}(3)$ via $\pi_\infty = (\pi_1 \times \pi_2)|_{G_\infty}$.

Then $(G_\infty, D_\infty, \pi_\infty, I_\infty)$ is a group with triality in $\mathsf{TriGrp}^\star$. For $\{i, j\} = \{1, 2\}$, the projection a_i onto (G_i, D_i, π_i, I_i) is a surjective triality homomorphism with kernel $G_\infty \cap N_j \geq [N_j, I_\infty] = [N_j, I_j]$.

Proof. Most of this is clear from the definitions. Certainly $G_\infty / G_\infty \cap N_j \simeq G_i$. If $d = (d_1, d_2) \in D_\infty \cap I$ and $n \in N_1$, then $[n, d_2] = 1$ and

$$[n, d_1] = [n, d] = (d_1, d_2)^n (d_1, d_2) = (d_1^n, d_2)(d_1, d_2) \in N_1 \cap G_\infty$$

as $(d_1^n)^\delta = d_1^\delta = d_2$.

The elements of the normal set D_∞ in H and G_∞ have order 2 and generate G_∞. The map π_∞ is onto $\mathrm{Sym}(3) \simeq I_\infty$ with $(D_\infty)^{\pi_\infty} = \{(2,3),(1,3),(1,2)\}$. When we have proven that $|de| = 3$, for all $d, e \in D_\infty$ with $d^{\pi_\infty} \neq e^{\pi_\infty}$, we will be done since this implies that $\langle d, e\rangle \simeq \mathrm{Sym}(3)$ and hence D_∞ is a single class.

Let $d = (d_1, d_2)$ and $e = (e_1, e_2)$ be in D_∞ with $d^{\pi_\infty} = s \neq t = e^{\pi_\infty}$, so that $d_1^{\pi_1} = d_2^{\pi_2} = s \neq t = e_1^{\pi_1} = e_2^{\pi_2}$. Therefore in $G_1 \times G_2$

$$((d_1,d_2)(e_1,e_2))^3 = (d_1e_1, d_2e_2)^3 = ((d_1e_1)^3, (d_2e_2)^3) = (1,1)\,.\square$$

6.2. Monics in TriGrp

(6.2). Proposition. *Let C be a full subcategory of* TriGrp *containing a terminal object and such that the corresponding pointed category $\mathsf{C}^\star$ is closed under the fibered product of Proposition (6.1). Let (G, D, π) and (G_0, D_0, π_0) be groups in C, and let f be a triality homomorphism from (G, D, π, I) to (G_0, D_0, π_0, I_0). The following are equivalent:*

(1) *f is monic in C.*
(2) *f is monic in $\mathsf{C}^\star$.*
(3) *$\ker f$ is central in G.*
(4) *The restriction $f\colon D \longrightarrow D_0$ is an injection.*

Proof. (1) $\Longrightarrow$ (2): Suppose that f is not monic in $\mathsf{C}^\star$, and let $a, b \in \mathrm{Hom}_{\mathsf{C}^\star}((G_1, D_1, \pi_1, I_1), (G, D, \pi, I))$ with $a \neq b$ and $af = bf$. Forgetting the special lines, we then have $a, b \in \mathrm{Hom}_{\mathsf{C}}((G_1, D_1, \pi_1), (G, D, \pi))$ with $a \neq b$ and $af = bf$; that is, f is not monic in C.

(2) $\Longrightarrow$ (3): Assume f is monic in $\mathsf{C}^\star$ and set $N = \ker f$. Let (G_1, D_1, π_1, I_1) and (G_2, D_2, π_2, I_2) be two copies of (G, D, π, I) and form the fibered product $(G_\infty, D_\infty, \pi_\infty, I_\infty)$ over $G/N\ (\leq G_0)$ as in Proposition (6.1). By hypothesis the triality group $(G_\infty, D_\infty, \pi_\infty, I_\infty)$ is in $\mathsf{C}^\star$. If a_1 and a_2 are (upon identification of G, G_1, and G_2) the two projections onto (G, D, π, I) described in the proposition, then $a_1 f = a_2 f$ as maps from $(G_\infty, D_\infty, \pi_\infty, I_\infty)$ to (G_0, D_0, π_0, I_0). Since f is monic in $\mathsf{C}^\star$, this forces $a_1 = a_2$. Especially $G_\infty \cap N_1 = \ker a_2 = \ker a_1 = G_\infty \cap N_2$. The factors N_1 and N_2 intersect trivially, therefore $G_\infty \cap N_1 = G_\infty \cap N_1 \cap N_2 = 1$. In particular $[N_1, I_1] = [N_1, I_\infty] \leq G_\infty \cap N_1 = 1$; that is, $[N, I] = 1$. As N is normal and $G = \langle I^G \rangle$, this gives $N \leq \mathrm{Z}(G)$.

(3) $\Longrightarrow$ (4): This follows from Lemma (4.12)(e).

(4) $\Longrightarrow$ (1): Let a and b be triality homomorphisms from (G_1, D_1, π_1) to (G, D, π) with $af = bf$ taking (G_1, D_1, π_1) to (G_0, D_0, π_0). For arbitrary but fixed $d_1 \in D_1$ let $(d_1^a)^f = d_1^{af} = d_1^{bf} = (d_1^b)^f$, an element of D_0. As f is an injection of D into D_0, we have $d_1^a = d_1^b$. Thus a and b agree on D_1 and so on $G_1 = \langle D_1 \rangle$. That is, $a = b$. $\square$

Of course in this proposition the main case of interest is $\mathsf{C} =$ TriGrp, but we will use the result for proper subcategories as well.

6.3. Covers and isogeny

If f is a surjective triality homomorphism from (G, D, π) to (G_0, D_0, π_0) with $\ker f$ contained in $\mathrm{Z}(G)$, then we say that f is a *covering map* and (G, D, π) is a *cover* of (G_0, D_0, π_0).

(6.3). Lemma.

(a) *If* $\zeta_0\colon (G_0, D_0, \pi_0) \longrightarrow (G_1, D_1, \pi_1)$ *and* $\zeta_1\colon (G_1, D_1, \pi_1) \longrightarrow (G_2, D_2, \pi_2)$ *are covering maps, then* $\zeta_0\zeta_1\colon (G_0, D_0, \pi_0) \longrightarrow (G_2, D_2, \pi_2)$ *is a covering map.*

(b) *The triality homomorphism* $f\colon (G, D, \pi) \longrightarrow (G_0, D_0, \pi_0)$ *is a covering map if and only if the restriction* $f\colon D \longrightarrow D_0$ *is a bijection.*

Proof. (a) The composition $\zeta_0\zeta_1$ is a surjective triality homomorphism whose kernel is contained in $\mathrm{Z}_2(G_0) = \mathrm{Z}(G_0)$ by Lemma (4.12).

(b) By Proposition (6.2) the kernel of f is central if and only if the restriction of f to D is injective. In this case, f will be surjective if and only if the restriction is also surjective. □

We say that two groups with triality (G, D, π) and (G_0, D_0, π_0) are *isogenous* if there is an *isogeny* from D to D_0—a bijection $\psi\colon D \longrightarrow D_0$ with $d^\psi e^\psi d^\psi = (ded)^\psi$, for all $d, e \in D$ with $d^\pi \neq e^\pi$. We also ask that $\pi|_D = \psi\pi_0$ (although this is not strictly necessary as an arbitrary ψ with the first condition can be concatenated with conjugation by an element of a line to get a bijection that additionally has this second condition). The inverse $\psi^{-1}\colon D_0 \longrightarrow D$ of the isogeny ψ is also an isogeny. Isogeny gives an equivalence relation on Obj TriGrp that can be viewed as a weakened form of isomorphism.

By Lemma (6.3) a covering map is a triality homomorphism f for which the restriction $\psi = f|_D$ is an isogeny. We shall soon discover that all isogenies are associated with covers. Indeed we find that isogeny is the transitive extension of the symmetrized covering relation.

Chapter 7

Universals and Adjoints

We return to study of the functor $\mathbf{U} = \mathbf{CB}$. This leads to the important full subcategories of TriGrp consisting of its universal and its adjoint objects.

7.1. Universal and adjoint groups

(7.1). Presentation. *For a group with triality (G, D, π), the group G^{U} has the following presentation:*

Generators:

$\tilde{d}$, *for arbitrary* $d \in D$;

Relations:

for arbitrary $d, e \in D$ *with* $d^\pi \neq e^\pi$:

(1) $\tilde{d}^2 = 1$;

(2) $\tilde{d}\tilde{e}\tilde{d} = \widetilde{ded}$.

(7.2). Theorem.

(a) *Set* $D^{\mathrm{U}} = \{\, \tilde{d} \mid d \in D \,\}$, *and define the map* π^{U} *on* D^{U} *by* $\tilde{d}^{\pi^{\mathrm{U}}} = d^\pi$. *Then* π^{U} *extends uniquely to a homomorphism from* G^{U} *onto* $\mathrm{Sym}(3)$, *and* $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ *is a group with triality.*

(b) *The map* $\tilde{d} \mapsto d$ *is a bijection of the conjugacy class* D^{U} *with* D *that extends to a covering map* $\zeta_G^{\mathrm{U}} \colon (G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}}) \longrightarrow (G, D, \pi)$.

(c) $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}}) = (G, D, \pi)\mathbf{U}$.

Proof. Statement (a) follows immediately from (c). Also, given (c) the map $\tilde{d} \mapsto d$ is a bijection by Lemma (5.4), and (b) then follows from Lemma (6.3).

It remains to prove (c). By Presentations (5.1) and (7.1) both triality groups $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ and $(G, D, \pi)\mathbf{U} = (G, D, \pi)\mathbf{CB}$ are generated by the set $\{\, \tilde{d} \mid d \in D \,\}$ and satisfy the relations $\tilde{d}^2 = 1$ for $d \in D$. The remaining relations are

Relation (5.1)(2): $\tilde{d}\tilde{e}\tilde{d} = \tilde{f}$, for $\{d, e, f\}$ a line of $(G, D, \pi)\mathbf{C}$

for $(G, D, \pi)\mathbf{U}$, and

Relation (7.1)(2): $\tilde{d}\tilde{e}\tilde{d} = \widetilde{ded}$, for $d, e \in D$ with $d^\pi \neq e^\pi$

for $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$.

However $\{d,e,f\}$ is a line of $(G,D,\pi)\mathbf{C}$ if and only if in (G,D,π) we have $I=\langle d,e,f\rangle \simeq \mathrm{Sym}(3)$ with $\{d,e,f\}=I\cap D$ and $d^\pi \neq e^\pi$. In this case $ded=f$, so the relations of (5.1)(2) and (7.1)(2) are equivalent. □

The triality groups $(G^{\mathrm{U}},D^{\mathrm{U}},\pi^{\mathrm{U}})$ have an important universal mapping property.

(7.3). Theorem. *Let (G,D,π) and (H,E,ρ) be groups with triality, and let $\psi\colon D \longrightarrow E$ have the two properties:*

(i) $d^\psi e^\psi d^\psi = (ded)^\psi$*, for all* $d,e\in D$ *with* $d^\pi \neq e^\pi$

(ii) $\pi|_D = \psi\rho$

(a) *There is a unique morphism*

$$\psi^{\mathrm{U}} \in \mathrm{Hom}_{\mathsf{TriGrp}}((G^{\mathrm{U}},D^{\mathrm{U}},\pi^{\mathrm{U}}),(H^{\mathrm{U}},E^{\mathrm{U}},\rho^{\mathrm{U}}))$$

with $\zeta_G^{\mathrm{U}}\psi = \psi^{\mathrm{U}}\zeta_H^{\mathrm{U}}$ *as maps from* D^{U} *to* E*; that is, the following diagram commutes:*

$$\begin{tikzcd}
D^{\mathrm{U}} \arrow[r, "\psi^{\mathrm{U}}"] \arrow[d, "\zeta_G^{\mathrm{U}}"'] & E^{\mathrm{U}} \arrow[d, "\zeta_H^{\mathrm{U}}"] \\
D \arrow[r, "\psi"] & E
\end{tikzcd}$$

(b) *There is a unique morphism*

$$\psi_0 \in \mathrm{Hom}_{\mathsf{TriGrp}}((G^{\mathrm{U}},D^{\mathrm{U}},\pi^{\mathrm{U}}),(H,E,\rho))$$

with $\zeta_G^{\mathrm{U}}\psi = \psi_0$ *on* D^{U}.

Proof. (a) For $d\in D$, we have $\tilde{d}^{\zeta_G^{\mathrm{U}}\psi} = d^\psi \in E$. As ζ_H^{U} is a bijection of E^{U} and E, to make the diagram commute we must set

$$\tilde{d}^{\psi^{\mathrm{U}}} = \widetilde{d^\psi}\,.$$

Therefore if there is a morphism ψ^{U} as described, then it is uniquely determined as the extension of this map on the generating set D^{U} to all of G^{U}.

We need to check that the relations of (7.1) defining G^{U} are taken by ψ^{U} to relations valid in H^{U}. The image of D^{U} is within E^{U}, so all these images certainly square to 1 in H^{U}. Consider now the relation $\tilde{d}\tilde{e}\tilde{d} = \widetilde{ded}$ with $d^\pi \neq e^\pi$, hence $(d^\psi)^\rho \neq (e^\psi)^\rho$:

$$\begin{aligned}
\tilde{d}^{\psi^{\mathrm{U}}}\tilde{e}^{\psi^{\mathrm{U}}}\tilde{d}^{\psi^{\mathrm{U}}} &= \widetilde{d^\psi}\,\widetilde{e^\psi}\,\widetilde{d^\psi} && \text{by definition;}\\
&= \widetilde{d^\psi e^\psi d^\psi} && \text{in } H^{\mathrm{U}};\\
&= \widetilde{(ded)^\psi} && \text{by hypothesis;}\\
&= \widetilde{ded}^{\,\psi^{\mathrm{U}}} && \text{again by definition.}
\end{aligned}$$

Thus the defining relations for G^{U} are respected by ψ^{U}, which therefore extends to a homomorphism from G^{U} to H^{U}.

By construction the homomorphism ψ^{U} takes D^{U} into E^{U}. Therefore to prove that ψ^{U} is a TriGrp-morphism from $(G^{\mathrm{U}},D^{\mathrm{U}},\pi^{\mathrm{U}})$ to $(H^{\mathrm{U}},E^{\mathrm{U}},\rho^{\mathrm{U}})$, it remains to observe that on D^{U}

$$\pi^{\mathrm{U}} = \zeta_G^{\mathrm{U}}\pi = \zeta_G^{\mathrm{U}}\psi\rho = \psi^{\mathrm{U}}\zeta_H^{\mathrm{U}}\rho = \psi^{\mathrm{U}}\rho^{\mathrm{U}}\,.$$

(b) The condition $\zeta^{\mathrm{U}}_G\psi = \psi_0$ on D^{U} determines ψ_0 uniquely on a generating set of G^{U}, so there is at most one such morphism. But $\psi_0 = \psi^{\mathrm{U}}\zeta^{\mathrm{U}}_H$ has the desired property. □

A map ψ as in the theorem has all the properties of an isogeny except it is not required to be bijective. (We resist the temptation to call it a homogeny.) Of course isogenies are examples, but also the restriction to D of any morphism from (G, D, π) gives an example. We examine these two special cases.

(7.4). THEOREM. *For each $\varphi \in \mathrm{Hom}_{\mathsf{TriGrp}}((G, D, \pi), (H, E, \rho))$, there is a unique $\varphi^{\mathrm{U}} \in \mathrm{Hom}_{\mathsf{TriGrp}}((G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}}), (H^{\mathrm{U}}, E^{\mathrm{U}}, \rho^{\mathrm{U}}))$ with $\zeta^{\mathrm{U}}_G\varphi = \varphi^{\mathrm{U}}\zeta^{\mathrm{U}}_H$:*

$$\begin{tikzcd}
G^{\mathrm{U}} \arrow[r, "\varphi^{\mathrm{U}}"] \arrow[d, "\zeta^{\mathrm{U}}_G"'] & H^{\mathrm{U}} \arrow[d, "\zeta^{\mathrm{U}}_H"] \\
G \arrow[r, "\varphi"] & H
\end{tikzcd}$$

PROOF. Set $\psi = \varphi|_D$. The morphism $\zeta^{\mathrm{U}}_G\varphi$ from G^{U} to H has, as its restriction to the class D^{U}, the map

$$\zeta^{\mathrm{U}}_G|_{D^{\mathrm{U}}}\varphi = \zeta^{\mathrm{U}}_G\varphi|_D = \zeta^{\mathrm{U}}_G\psi\,.$$

Theorem (7.3) then guarantees that $\zeta^{\mathrm{U}}_G\varphi = \psi^{\mathrm{U}}\zeta^{\mathrm{U}}_H$ as TriGrp-morphisms and that $\varphi^{\mathrm{U}} = \psi^{\mathrm{U}}$ is the unique morphism with this property. □

(7.5). THEOREM.

(a) *If ψ is an isogeny from (G, D, π) to (H, E, ρ), then the morphism ψ^{U} is an isomorphism of $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ and $(H^{\mathrm{U}}, E^{\mathrm{U}}, \rho^{\mathrm{U}})$.*

(b) *If φ is a covering map from (H, E, ρ) to (G, D, π), then ζ^{U}_G factors through φ; that is, there is a unique triality homomorphism ζ from $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ to (H, E, ρ) with $\zeta^{\mathrm{U}}_G = \zeta\varphi$. Furthermore ζ itself is a covering map.*

PROOF. (a) By Theorem (7.3) there is a morphism ψ^{U} from G^{U} to H^{U} with $\zeta^{\mathrm{U}}_G\psi = \psi^{\mathrm{U}}\zeta^{\mathrm{U}}_H$ on D^{U} and a morphism $(\psi^{-1})^{\mathrm{U}}$ from H^{U} to G^{U} with $\zeta^{\mathrm{U}}_H\psi^{-1} = (\psi^{-1})^{\mathrm{U}}\zeta^{\mathrm{U}}_G$ on E^{U}. Therefore, as a map from D^{U} to D we have

$$\zeta^{\mathrm{U}}_G = \zeta^{\mathrm{U}}_G\psi\psi^{-1} = \psi^{\mathrm{U}}\zeta^{\mathrm{U}}_H\psi^{-1} = \psi^{\mathrm{U}}(\psi^{-1})^{\mathrm{U}}\zeta^{\mathrm{U}}_G\,.$$

As ζ^{U}_G restricts to a bijection of D^{U} and D, the morphism $\psi^{\mathrm{U}}(\psi^{-1})^{\mathrm{U}}$ is the identity map on the generating class D^{U} for G^{U}. Thus $\psi^{\mathrm{U}}(\psi^{-1})^{\mathrm{U}} = 1_{(G,D,\pi)}$, and similarly $(\psi^{-1})^{\mathrm{U}}\psi^{\mathrm{U}} = 1_{(H,E,\rho)}$. We conclude that ψ^{U} is an isomorphism.

(b) As φ is a cover, $\varphi|_E$ is an isogeny (by Lemma (6.3)(b)). Let $\psi = \varphi|_E^{-1}$ be the inverse isogeny from D to E. By Theorem (7.3), there is a unique morphism ζ from $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ to (H, E, ρ) with $\zeta^{\mathrm{U}}_G\psi = \zeta$ on D^{U}. That is, the morphism ζ is unique subject to $\zeta^{\mathrm{U}}_G = \zeta\psi^{-1}$ on D^{U}. The class D^{U} generates G^{U}, so ζ is in turn unique subject to $\zeta^{\mathrm{U}}_G = \zeta\varphi$ on all G^{U}. As $\zeta^{\mathrm{U}}_G|_{D^{\mathrm{U}}}$ and ψ are both bijections, so is $\zeta|_{D^{\mathrm{U}}}$. Again by Lemma (6.3)(b) the map ζ is a cover. □

We call $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ (or any group with triality isomorphic to it) a *universal group with triality.* The two preceding theorems express universal properties of the universal groups with triality. Theorem (7.4) says that any morphism between groups with triality lifts uniquely to a morphism between the corresponding universal groups.

The second part of Theorem (7.5) says that the group with triality $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ is a universal central extension of (G, D, π) in TriGrp. This is particularly satisfying since, in the category of groups, universal central extensions exist generally only for perfect groups [**Asc00**, (33.4)]; existence for perfect H is proven via a presentation that encodes the full Cayley table of H. In Presentation (7.1) we only needed to encode the transform table for the conjugacy class D of (G, D, π), so the presentation is simpler and the construction works in all cases.

(7.6). PROPOSITION.

(a) *The triality group* (G_0, D_0, π_0) *is isogenous to* (G, D, π) *if and only if the groups* $(G_0^{\mathrm{U}}, D_0^{\mathrm{U}}, \pi_0^{\mathrm{U}})$ *and* $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ *are isomorphic.*

(b) *The triality group* (G_0, D_0, π_0) *is isogenous to* (G, D, π) *if and only if there is a covering map* $\zeta\colon (G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}}) \longrightarrow (G_0, D_0, \pi_0)$.

(c) *The triality group* $((G^{\mathrm{U}})^{\mathrm{U}}, (D^{\mathrm{U}})^{\mathrm{U}}, (\pi^{\mathrm{U}})^{\mathrm{U}})$ *is isomorphic to* $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$.

PROOF. (a) By Theorem (7.5) isogeny of (G_0, D_0, π_0) and (G, D, π) gives isomorphism of $(G_0^{\mathrm{U}}, D_0^{\mathrm{U}}, \pi_0^{\mathrm{U}})$ and $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$. Conversely, if $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ and $(G_0^{\mathrm{U}}, D_0^{\mathrm{U}}, \pi_0^{\mathrm{U}})$ are isomorphic via φ, then the map $(\zeta_G^{\mathrm{U}}|_{D^{\mathrm{U}}})^{-1}\varphi\zeta_{G_0}^{\mathrm{U}}$ is an isogeny from (G, D, π) to (G_0, D_0, π_0).

(b) By Lemma (6.3) if ζ is a cover, then $\zeta|_D$ is an isogeny. Conversely, if ψ is an isogeny from (G, D, π) to (G_0, D_0, π_0), then by Theorem (7.5) $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ and $(G_0^{\mathrm{U}}, D_0^{\mathrm{U}}, \pi_0^{\mathrm{U}})$ are isomorphic via ψ^{U}; so $\psi^{\mathrm{U}}\zeta_{G_0}^{\mathrm{U}}$ is a covering map from G^{U} to G_0.

(c) As $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ and (G, D, π) are isogenous, this follows from (a). □

The above results tell us that the universal groups with triality (G, D, π) are precisely those for which ζ_G^{U} is an isomorphism and equally well those that are (up to isomorphism) in the range of the functor $\mathbf{U}$. Each isogeny class contains a unique universal group up to isomorphism.

We can now make precise our statement at the end of the previous chapter that all isogenies are associated with covers. Specifically, suppose that (G_1, D_1, π_1) and (G_2, D_2, π_2) are isogenous. Then there are a universal group (G, D, π) and covering maps ζ_i from G to G_i. Each $\zeta_i|_D$ is an isogeny, and $(\zeta_1|_D^{-1})(\zeta_2|_D)$ is a specific isogeny from (G_1, D_1, π_1) to (G_2, D_2, π_2). In particular isogeny is the equivalence relation generated by covering through symmetry and transitivity.

Loosely, two isogenous triality groups are the same up to centers. Within each isogeny class the universal group is the unique largest group up to isomorphism, and all others are covered by it. In each isogeny class there is also a unique smallest group up to isomorphism, and it is covered by all the others. This is the adjoint group, which we next define.

Consider the map ζ taking G to $G/\mathrm{Z}(G) = G^{\mathrm{A}}$. Lemma (4.2) and Proposition (6.2) then give a covering map $\zeta\colon (G, D, \pi) \longrightarrow (G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$ with π^{A} uniquely determined by $\pi = \zeta\pi^{\mathrm{A}}$. Again by Proposition (6.2) the triality groups (G, D, π) and $(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$ are isogenous. We call $(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$ (or any group with triality that is isomorphic to it) an *adjoint group with triality.* As we shall see below, every triality group that is isogenous to (G, D, π) has central quotient isomorphic to $(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$.

The adjoint groups with triality have a particularly elementary characterization.

(7.7). Proposition.

(a) *The group with triality* (G, D, π) *is adjoint if and only if* $\mathrm{Z}(G) = 1$*. In particular* $((G^{\mathrm{A}})^{\mathrm{A}}, (D^{\mathrm{A}})^{\mathrm{A}}, (\pi^{\mathrm{A}})^{\mathrm{A}})$ *is equal to* $(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$.

(b) *The groups with triality* $(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$ *and* $(G, D, \pi)\mathbf{CA}$ *are isomorphic.*

Proof. (a) If $\mathrm{Z}(G) = 1$ then clearly $(G, D, \pi) = (G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$ is adjoint. On the other hand, by Lemma (4.12)(e) the adjoint group G^{A} has trivial center and $(G^{\mathrm{A}})^{\mathrm{A}} = G^{\mathrm{A}}$.

(b) By design the element d of D and G acts as τ_d on $(G, D, \pi)\mathbf{C}$. Therefore there is a triality homomorphism from (G, D, π) to $(G, D, \pi)\mathbf{CA}$ that restricts to a bijection on D. By Proposition (6.2) the group $(G, D, \pi)\mathbf{CA}$ is covered by (G, D, π), and by Lemma (3.8) it has trivial center. Therefore $(G, D, \pi)\mathbf{CA}$ is isomorphic to the full central quotient of (G, D, π), namely $(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$. □

Proposition (7.7) is the adjoint counterpart to Theorem (7.2). Compare the following with Proposition (7.6).

(7.8). Proposition.

(a) *The triality group* (G_0, D_0, π_0) *is isogenous to* (G, D, π) *if and only if the groups* $(G_0^{\mathrm{A}}, D_0^{\mathrm{A}}, \pi_0^{\mathrm{A}})$ *and* $(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$ *are isomorphic.*

(b) *The triality group* (G_0, D_0, π_0) *is isogenous to* (G, D, π) *if and only if there is a covering map* $\zeta\colon (G_0, D_0, \pi_0) \longrightarrow (G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$.

Proof. (a) If (G_0, D_0, π_0) is isogenous to (G, D, π), then by Proposition (7.6) the groups $(G_0^{\mathrm{U}}, D_0^{\mathrm{U}}, \pi_0^{\mathrm{U}})$ and $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ are isomorphic and cover (G_0, D_0, π_0) and (G, D, π). These in turn cover $(G_0^{\mathrm{A}}, D_0^{\mathrm{A}}, \pi_0^{\mathrm{A}})$ and $(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$. Therefore by Lemma (6.3) the group $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ covers both adjoint groups $(G_0^{\mathrm{A}}, D_0^{\mathrm{A}}, \pi_0^{\mathrm{A}})$ and $(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$. By Proposition (7.7) these groups are isomorphic, both being full central quotients of $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$

Conversely if $(G_0^{\mathrm{A}}, D_0^{\mathrm{A}}, \pi_0^{\mathrm{A}})$ and $(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$ are isomorphic, then by Proposition (7.6)

$$\begin{aligned}(G_0^{\mathrm{U}}, D_0^{\mathrm{U}}, \pi_0^{\mathrm{U}}) &\simeq ((G_0^{\mathrm{A}})^{\mathrm{U}}, (D_0^{\mathrm{A}})^{\mathrm{U}}, (\pi_0^{\mathrm{A}})^{\mathrm{U}}) \\ &\simeq ((G^{\mathrm{A}})^{\mathrm{U}}, (D^{\mathrm{A}})^{\mathrm{U}}, (\pi^{\mathrm{A}})^{\mathrm{U}}) \simeq (G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})\,.\end{aligned}$$

Therefore (G_0, D_0, π_0) and (G, D, π) are isogenous by Proposition (7.6).

(b) If (G_0, D_0, π_0) is isogenous to (G, D, π), then by (a) the groups with triality $(G_0^{\mathrm{A}}, D_0^{\mathrm{A}}, \pi_0^{\mathrm{A}})$ and $(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$ are isomorphic; but by definition the group (G_0, D_0, π_0) covers $(G_0^{\mathrm{A}}, D_0^{\mathrm{A}}, \pi_0^{\mathrm{A}})$. Conversely, if (G_0, D_0, π_0) covers the group $(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$, then by Lemma (6.3) both (G_0, D_0, π_0) and (G, D, π) are isogenous to $(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$; so they are isogenous to each other. □

7.2. Universal and adjoint categories

The universal triality group category $\mathsf{UTriGrp}$ is defined to be the full subcategory of TriGrp with object class consisting of the universal groups with triality. The category $\mathsf{UTriGrp}^\star$ is the corresponding full subcategory of $\mathsf{TriGrp}^\star$. By Theorem (7.2) the universal functor $\mathbf{U} = \mathbf{CB}$ is a functor from TriGrp to $\mathsf{UTriGrp}$ taking (G, D, π) to $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$. Similarly let $\mathbf{U}^\star$ be the functor from $\mathsf{TriGrp}^\star$ to $\mathsf{UTriGrp}^\star$ taking (G, D, π, I) to $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}}, I^{\mathrm{U}})$, where $I^{\mathrm{U}} = \langle \tilde{c}, \tilde{d}, \tilde{e}\rangle$ for $I = \langle c, d, e\rangle$ with $c, d, e \in D$.

The adjoint categories $\mathsf{ATriGrp}$ and $\mathsf{ATriGrp}^\star$ are the full subcategories of TriGrp and $\mathsf{TriGrp}^\star$ consisting of those objects that are adjoint.

(7.9). Theorem. *The group with triality*

$$O = (\mathrm{Sym}(3), \{(2,3),(1,3),(1,2)\}, \mathrm{Id}_{\mathrm{Sym}(3)})$$

is both universal and adjoint, so it is a terminal object in $\mathsf{UTriGrp}$ *and* $\mathsf{ATriGrp}$ *but is not initial. The category* $\mathsf{UTriGrp}^\star$ *is isomorphic to the pointed category* $\mathsf{UTriGrp}^\star_O$*, and the category* $\mathsf{ATriGrp}^\star$ *is isomorphic to the pointed category* $\mathsf{ATriGrp}^\star_O$*.*

Proof. The triality group $\mathrm{Sym}(3)$ is adjoint as it has trivial center and universal by its presentation as $\mathrm{W}(A_2)$. Therefore it is also terminal in the full subcategories $\mathsf{UTriGrp}$ and $\mathsf{ATriGrp}$. The proof from Theorem (4.3) that $\mathrm{Sym}(3)$ is not initial goes over to the full subcategories, as there are groups with triality not isomorphic to the universal and adjoint $\mathrm{Sym}(3)$; and the isomorphism of $\mathsf{TriGrp}^\star$ and $\mathsf{TriGrp}^\star_O$ given there restricts to isomorphisms of the corresponding subcategories. □

(7.10). Theorem. *For groups with triality* (G_1, D_1, π_1) *and* (G_2, D_2, π_2) *the following are equivalent:*

(1) (G_1, D_1, π_1) *and* (G_2, D_2, π_2) *are isogenous in* TriGrp.
(2) $(G_1, D_1, \pi_1)\mathbf{U}$ *and* $(G_2, D_2, \pi_2)\mathbf{U}$ *are isomorphic in* $\mathsf{UTriGrp}$.
(3) $(G_1^{\mathrm{A}}, D_1^{\mathrm{A}}, \pi_1^{\mathrm{A}})$ *and* $(G_2^{\mathrm{A}}, D_2^{\mathrm{A}}, \pi_2^{\mathrm{A}})$ *are isomorphic in* $\mathsf{ATriGrp}$.
(4) $(G_1, D_1, \pi_1)\mathbf{C}$ *and* $(G_2, D_2, \pi_2)\mathbf{C}$ *are isomorphic in* CLSD.
(5) $(G_1, D_1, \pi_1)\mathbf{CS}$ *and* $(G_2, D_2, \pi_2)\mathbf{CS}$ *are isomorphic in* Mouf.

Proof. Statements (1) and (2) are equivalent by Theorem (7.2) and Proposition (7.6). Statements (1) and (3) are equivalent by Proposition (7.8).

Statements (4) and (5) are equivalent as $\mathbf{S}$ is a category equivalence.

Statement (1) implies (4) by Lemma (4.12)(e), while (4) implies (2) as $\mathbf{U} = \mathbf{CB}$ and $\mathbf{B}$ is a functor. □

(7.11). Corollary. *The functor* $\mathbf{C}$ *does not give an equivalence of the categories* TriGrp *and* CLSD*.*

Proof. By Lemma (4.10) the triality groups $\mathrm{W}(D_4)$ and $\mathrm{W}(D_4)/\mathrm{Z}(\mathrm{W}(D_4))$ are nonisomorphic but isogenous. By the theorem $\mathbf{C}$ takes these to isomorphic objects in CLSD. But equivalences take nonisomorphic objects to nonisomorphic objects. □

Similarly we have

(7.12). Proposition.

(a) *The map* $\mathbf{U} = \mathbf{CB}$ *is a faithful functor from* TriGrp *to* TriGrp *but is neither full nor dense.*
(b) *The map* $\mathbf{U}^\star = \mathbf{C}^\star\mathbf{B}^\star$ *is a faithful functor from* $\mathsf{TriGrp}^\star$ *to* $\mathsf{TriGrp}^\star$ *but is neither full nor dense.*
(c) *The functors* $\mathbf{C}$ *and* $\mathbf{C}^\star$ *are not full on* TriGrp *and* $\mathsf{TriGrp}^\star$*.*
(d) *The functors* $\mathbf{B}$ *and* $\mathbf{B}^\star$ *are not dense on* CLSD *and* $\mathsf{CLSD}^\star$*.*

Proof. $\mathbf{C}$ is a faithful and dense functor from TriGrp to CLSD by Proposition (4.4) while $\mathbf{B}$ is a faithful and full functor from CLSD to TriGrp by Theorem (5.6). This gives the faithful part of (a), and a similar argument gives the corresponding part of (b).

The group $\mathrm{W}(D_4)$ is universal (as revealed by its presentation in Proposition (4.8)) and is isogenous but not isomorphic to $\mathrm{W}(D_4)/\mathrm{Z}(\mathrm{W}(D_4))$ by Lemma (4.10). Therefore the isomorphism class of $\mathrm{W}(D_4)/\mathrm{Z}(\mathrm{W}(D_4))$ is not represented in the image of $\mathbf{U}$ or $\mathbf{U}^\star$, and these functors are not dense. Furthermore $(\mathrm{W}(D_4)/\mathrm{Z}(\mathrm{W}(D_4)))^{\mathrm{U}}$ and $\mathrm{W}(D_4)^{\mathrm{U}}$ are isomorphic in TriGrp and $\mathsf{TriGrp}^\star$ (both to $\mathrm{W}(D_4)$, in fact), and this isomorphism cannot be the image under $\mathbf{U}$ or $\mathbf{U}^\star$ of any morphism from $\mathrm{W}(D_4)/\mathrm{Z}(\mathrm{W}(D_4))$ to $\mathrm{W}(D_4)$; the functors are also not full.

As $\mathbf{C}$ and $\mathbf{C}^\star$ are dense while $\mathbf{B}$ and $\mathbf{B}^\star$ are full, but $\mathbf{U} = \mathbf{CB}$ and $\mathbf{U}^\star = \mathbf{C}^\star\mathbf{B}^\star$ are neither, $\mathbf{C}$ and $\mathbf{C}^\star$ are not full and $\mathbf{B}$ and $\mathbf{B}^\star$ are not dense. □

As $(\mathrm{Sym}(3), \{(2,3),(1,3),(1,2)\}, \mathrm{Id}_{\mathrm{Sym}(3)})$ is both universal and adjoint, Theorem (7.10) gives us immediately

(7.13). Theorem. *For groups with triality (G_1, D_1, π_1, I_1) and (G_2, D_2, π_2, I_2) the following are equivalent:*

(1) (G_1, D_1, π_1, I_1) *and* (G_2, D_2, π_2, I_2) *are isogenous in* $\mathsf{TriGrp}^\star$.
(2) $(G_1, D_1, \pi_1, I_1)\mathbf{U}^\star$ *and* $(G_2, D_2, \pi_2, I_2)\mathbf{U}^\star$ *are isomorphic in* $\mathsf{UTriGrp}^\star$.
(3) $(G_1^{\mathrm{A}}, D_1^{\mathrm{A}}, \pi_1^{\mathrm{A}}, I_1^{\mathrm{A}})$ *and* $(G_2^{\mathrm{A}}, D_2^{\mathrm{A}}, \pi_2^{\mathrm{A}}, I_2^{\mathrm{A}})$ *are isomorphic in* $\mathsf{ATriGrp}^\star$.
(4) $(G_1, D_1, \pi_1, I_1)\mathbf{C}^\star$ *and* $(G_2, D_2, \pi_2, I_2)\mathbf{C}^\star$ *are isomorphic in* $\mathsf{CLSD}^\star$.
(5) $(G_1, D_1, \pi_1, I_1)\mathbf{C}^\star\mathbf{S}^\star$ *and* $(G_2, D_2, \pi_2, I_2)\mathbf{C}^\star\mathbf{S}^\star$ *are isomorphic in* $\mathsf{Mouf}^\star$. □

The previous two theorems might look better were we to define a map $\mathbf{V}$ from TriGrp to $\mathsf{ATriGrp}$ by

$$\mathbf{V} = \mathbf{CA} \quad \text{with} \quad (G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}}) \simeq (G, D, \pi)\mathbf{V}\,,$$

in parallel to our earlier definition of the map $\mathbf{U}$ from TriGrp to $\mathsf{UTriGrp}$ given by

$$\mathbf{U} = \mathbf{CB} \quad \text{with} \quad (G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}}) = (G, D, \pi)\mathbf{U}\,.$$

We resist this temptation, since unlike $\mathbf{U}$ the map $\mathbf{CA}$ is not a functor. Indeed in Corollary (9.20) below we prove that $\mathbf{A}$ is not a functor precisely by observing that this would force $\mathbf{CA}$ to be a functor and then deriving a contradiction.

If a morphism is monic (or epic) then it certainly remains monic (or epic) in any subcategory. But in passage to the subcategory we may have lost some morphisms and so promoted other morphisms to monic (or epic) status. We now prove that in the subcategories $\mathsf{ATriGrp}$ and $\mathsf{UTriGrp}$ of TriGrp there are no monic surprises.

(7.14). Proposition. *Let (G, D, π) and (G_0, D_0, π_0) be groups in* $\mathsf{ATriGrp}$, *and let f be a triality homomorphism from (G, D, π, I) to (G_0, D_0, π_0, I_0). The following are equivalent:*

(1) *f is monic in* $\mathsf{ATriGrp}$.
(2) *f is monic in* $\mathsf{ATriGrp}^\star$.
(3) *f is monic in* TriGrp.
(4) *f is monic in* $\mathsf{TriGrp}^\star$.
(5) *f is an injection of G into G_0.*
(6) *the restriction $f\colon D \longrightarrow D_0$ is an injection.*

Proof. The objects of $\mathsf{ATriGrp}^\star$ are characterized within $\mathsf{TriGrp}^\star$ as those with trivial center, so the full subcategory $\mathsf{ATriGrp}^\star$ is closed under the fibered product of Proposition (6.1). Therefore this result follows directly from Proposition (6.2) as $\mathrm{Z}(G) = 1$. □

(7.15). Proposition. *Let (G, D, π) and (G_0, D_0, π_0) be groups in* $\mathsf{UTriGrp}$*, and let f be a triality homomorphism from (G, D, π, I) to (G_0, D_0, π_0, I_0). The following are equivalent:*

(1) *f is monic in* $\mathsf{UTriGrp}$.
(2) *f is monic in* $\mathsf{UTriGrp}^\star$*.*
(3) *f is monic in* TriGrp.
(4) *f is monic in* $\mathsf{TriGrp}^\star$*.*
(5) $\ker f$ *is central in G.*
(6) *The restriction $f\colon D \longrightarrow D_0$ is an injection.*

Proof. The category $\mathsf{UTriGrp}^\star$ is not closed under the fibered product. Instead we show directly that f is monic in $\mathsf{UTriGrp}^\star$ if and only if it is monic in $\mathsf{TriGrp}^\star$. With that, the forgetful functor and Proposition (6.2) give the full result.

As already mentioned, if f is monic in $\mathsf{TriGrp}^\star$ then it is monic in the subcategory $\mathsf{UTriGrp}^\star$.

Now assume that f in monic in $\mathsf{UTriGrp}^\star$, and let g_1 and g_2 be $\mathsf{TriGrp}^\star$ morphisms from (G_1, D_1, π_1, I_1) to (G, D, π, I) with $g_1 f = g_2 f$. Then the $g_i\mathbf{U}^\star$ are morphisms from $(G_1, D_1, \pi_1, I_1)\mathbf{U}^\star$ to $(G, D, \pi, I)\mathbf{U}^\star \simeq (G, D, \pi, I)$ with

$$g_1\mathbf{U}^\star f\mathbf{U}^\star = (g_1 f)\mathbf{U}^\star = (g_2 f)\mathbf{U}^\star = g_2\mathbf{U}^\star f\mathbf{U}^\star\,.$$

By Proposition (1.1) the restriction of the functor $\mathbf{U}^\star$ to $\mathsf{UTriGrp}^\star$ is an equivalence, and especially $f\mathbf{U}^\star$ is monic in the subcategory as f is. Therefore in $\mathsf{UTriGrp}^\star$ we find $g_1\mathbf{U}^\star = g_2\mathbf{U}^\star$. By Proposition (7.12) the functor $\mathbf{U}^\star$ is faithful, so $g_1 = g_2$. This proves that f is still monic in the supercategory $\mathsf{TriGrp}^\star$. □

Chapter 8

Moufang Loops and Groups with Triality are Essentially the Same Thing

More precisely we have the following two theorems.

(8.1). Theorem. *The categories* Mouf*,* CLSD*, and* UTriGrp *are equivalent.*

(8.2). Theorem. *The categories* Mouf**,* CLSD**, and* UTriGrp* *are equivalent.*

As in Lemma (2.14), the categories from the two different theorems cannot be equivalent to each other, since the categories of the second theorem all have zero objects while none of the categories in the first theorem do.

Theorem (8.2) follows from Theorem (8.1) as the categories in the second theorem are equivalent to the pointed versions of those in the first theorem. The relevant references are Theorems (1.10), (2.15), (3.7), and (7.9).

8.1. A category equivalence

By Theorem (3.11) we know that Mouf and CLSD are equivalent via **T**. We wish to construct equivalences according to:

$$\begin{tikzcd}
\mathsf{Mouf} \arrow[r, shift left, "\mathbf{T}"] & \mathsf{CLSD} \arrow[l, shift left, "\mathbf{S}"] \arrow[r, shift left, "\mathbf{B}"] & \mathsf{UTriGrp} \arrow[l, shift left, "\mathbf{C}"]
\end{tikzcd}$$

In a certain sense this has been done already via "proof by definition." Namely in Theorem (5.6) we showed that **B** is faithful and full as a functor from CLSD to TriGrp. By restricting to UTriGrp, the image of **B**, we have effectively defined **B** to be additionally dense as a functor from CLSD to UTriGrp. Thus **B** gives an equivalence of CLSD and UTriGrp by Proposition (1.1). Rather than fill in the details of this argument, we prove something that is more concrete.

(8.3). Proposition. *The pair of functors* $(\mathbf{B}, \mathbf{C})$ *is a category equivalence of* CLSD *and* UTriGrp*.*

Proof. We must prove:

(i) *For every* $(G, D, \pi) \in$ UTriGrp *we can choose an isomorphism* $\chi_{(G,D,\pi)}$ *in* $\mathrm{Hom}_{\mathsf{UTriGrp}}((G, D, \pi), (G, D, \pi)\mathbf{CB})$ *such that:*

for all

$$(G_1, D_1, \pi_1),\ (G_2, D_2, \pi_2) \in \mathsf{UTriGrp}$$

and each

$$f \in \mathrm{Hom}_{\mathsf{UTriGrp}}((G_1, D_1, \pi_1), (G_2, D_2, \pi_2))\,,$$

we have

$$f\mathbf{CB} = \chi^{-1}_{(G_1,D_1,\pi_1)} f \chi_{(G_2,D_2,\pi_2)}\,.$$

(ii) *For every* $(P, S) \in \mathsf{CLSD}$ *we can choose an isomorphism* $\delta_{(P,S)}$ *in* $\mathrm{Hom}_{\mathsf{CLSD}}((P, S), (P, S)\mathbf{BC})$ *such that:*
for all

$$(P_3, S_3), (P_4, S_4) \in \mathsf{CLSD}$$

and each

$$\varphi \in \mathrm{Hom}_{\mathsf{CLSD}}((P_3, S_3), (P_4, S_4))\,,$$

we have

$$\varphi\mathbf{BC} = \delta^{-1}_{(P_3,S_3)} \varphi \delta_{(P_4,S_4)}\,.$$

The morphism f of $\mathrm{Hom}_{\mathsf{UTriGrp}}((G_1, D_1, \pi_1), (G_2, D_2, \pi_2))$ is completely and uniquely determined by its restriction taking the set D_1 to the set D_2. Also φ of $\mathrm{Hom}_{\mathsf{CLSD}}((P_3, S_3), (P_4, S_4))$ is determined by its action mapping the set P_3 to P_4. In a similar manner, the functor $\mathbf{C}$ is completely and uniquely determined on each object (G, D, π) of $\mathsf{UTriGrp}$ by the identity inclusion $\iota\colon D \longrightarrow D = P_{(G,D,\pi)} = P$ given by $d \mapsto d$. The functor $\mathbf{B}$ is determined on each object (P, S) of CLSD by the bijection $t\colon P \longrightarrow \tilde{P} = D$ given by $p \mapsto \tilde{p} = p^t$. The morphisms $f\mathbf{C}$ and $\varphi\mathbf{B}$ are then uniquely determined by the commutative diagrams

$$\begin{tikzcd}
D_1 \arrow[r, "\iota_1"] \arrow[d, "f"'] & D_1 = P_1 \arrow[d, "f\mathbf{C}"] & P_3 \arrow[r, "t_3"] \arrow[d, "\varphi"'] & \tilde{P}_3 = D_3 \arrow[d, "\varphi\mathbf{B}"] \\
D_2 \arrow[r, "\iota_2"] & D_2 = P_2 & P_4 \arrow[r, "t_4"] & \tilde{P}_4 = D_4
\end{tikzcd}$$

For (i), given $(G, D, \pi) \in \mathsf{UTriGrp}$ the morphism $\chi_{(G,D,\pi)}$ is the element of $\mathrm{Hom}_{\mathsf{UTriGrp}}((G, D, \pi), (G, D, \pi)\mathbf{CB})$ uniquely determined by

$$\chi_{(G,D,\pi)}|_D = \iota_{(G,D,\pi)} t_{(G,D,\pi)\mathbf{C}}\,.$$

Thus $(G, D, \pi)^{\chi_{(G,D,\pi)}} = (G, D, \pi)\mathbf{U}$, which is isomorphic to (G, D, π) by Proposition (7.6)(c). Furthermore, with $f\mathbf{C} = \varphi$, $P_1 = P_3$, and $P_2 = P_4$, we glue the diagrams together at the middle to get

$$f\mathbf{CB} = \varphi\mathbf{B} = t_1^{-1}\iota_1^{-1} f \iota_2 t_2 = \chi_1^{-1} f \chi_2\,,$$

as required for (i).

For (ii), given $(P, S) \in \mathsf{CLSD}$ the morphism $\delta_{(P,S)}$ is the unique element of $\mathrm{Hom}_{\mathsf{CLSD}}((P, S), (P, S)\mathbf{BC})$ determined by

$$\delta_{(P,S)}|_P = t_{(P,S)}\iota_{(P,S)\mathbf{B}}\,.$$

As $t_{(P,S)}$ (by Lemma (5.4)) and $\iota_{(P,S)\mathbf{B}}$ are both bijections, so is their composition $\delta_{(P,S)}$. Then by Lemma (3.2) the morphism $\delta_{(P,S)}$ is an isomorphism.

With $\varphi\mathbf{B} = f$, $D_3 = D_1$, and $D_4 = D_2$, we now glue the outsides of the diagrams together and get

$$\varphi\mathbf{BC} = f\mathbf{C} = \iota_3^{-1} t_3^{-1} \varphi t_4 \iota_4 = \delta_3^{-1} \varphi \delta_4\,,$$

as required for (ii). □

This proves Theorem (8.1) and so also Theorem (8.2), as discussed above.

8.2. Monics

In Propositions (6.2), (7.14), and (7.15) we studied monic morphisms in the category of groups with triality and found that they are close to injective.

(8.4). Theorem. *In* Mouf, $\mathsf{Mouf}^\star$, CLSD, *and* $\mathsf{CLSD}^\star$ *a morphism is monic if and only if it is injective on the appropriate underlying set.*

Proof. This is immediate from Proposition (7.15) and Theorems (7.2), (7.10), (7.13), (8.1), and (8.2). □

On the other hand, it is likely that in these categories epic morphisms need not be surjective.

Chapter 9

Moufang Loops and Groups with Triality are Not Exactly the Same Thing

On the other hand, the basic categories Mouf and TriGrp are not equivalent, nor are Mouf* and TriGrp*.

(9.1). Theorem. *The category* Mouf *is not equivalent to the category* TriGrp *or to the category* ATriGrp*.*

(9.2). Theorem. *The category* Mouf* *is not equivalent to the category* TriGrp* *or to the category* ATriGrp**.*

(9.3). Theorem. *No two of the categories* TriGrp*,* UTriGrp*, and* ATriGrp *are equivalent.*

(9.4). Theorem. *No two of the categories* TriGrp**,* UTriGrp**, and* ATriGrp* *are equivalent.*

By Theorems (8.1) and (8.2) the categories Mouf and UTriGrp are equivalent, as are Mouf* and UTriGrp*. Therefore Theorems (9.1) and (9.2) are actually contained in Theorems (9.3) and (9.4).

Furthermore using Theorem (1.10) we could deduce Theorem (9.3) from Theorem (9.4). Therefore this last theorem is the only one that requires proof. That is not quite the approach we take.

9.1. Mouf and TriGrp are not equivalent

By Theorem (8.1) the categories Mouf and UTriGrp are equivalent. Therefore to prove that Mouf is not equivalent to TriGrp it is enough to prove that UTriGrp is not equivalent to TriGrp. At the same time we prove that ATriGrp is not equivalent to TriGrp.

By Theorem (1.10) these results are immediate consequences of the nonequivalence of the corresponding pointed categories, to be proved in the next section. Thus this short section is not necessary. Nevertheless we provide it, since it follows the same path as the later arguments but with simpler details.

Each category TriGrp, UTriGrp, and ATriGrp has an object O that is terminal but not initial, namely $O = (\mathrm{Sym}(3), \{(2,3),(1,3),(1,2)\}, \mathrm{Id}_{\mathrm{Sym}(3)})$.

Recall from Section 1.5 that the morphism f from (G, D, π) to (G_0, D_0, π_0) is terminal-surjective if, for every $a \in \mathrm{Hom}_{\mathsf{TriGrp}}(O, (G_0, D_0, \pi_0))$, there is a $b \in \mathrm{Hom}_{\mathsf{TriGrp}}(O, (G, D, \pi))$ with $a = bf$. Equally well the terminal-order of the triality group (G, D, π) is $|\mathrm{Hom}_{\mathsf{TriGrp}}(O, (G, D, \pi))|$. Category equivalences respect terminal-order and terminal-surjectivity. Terminal-surjectivity and terminal-order are also unchanged by passage to full subcategories such as $\mathsf{UTriGrp}$ and $\mathsf{ATriGrp}$ within TriGrp.

(9.5). Proposition.

(a) *(G, D, π) has terminal-order $|D|^2/9$. In particular (G, D, π) is a terminal object if and only if it has terminal-order* 1.

(b) *For the map $f \in \mathrm{Hom}_{\mathsf{TriGrp}}((G, D, \pi), (G_0, D_0, \pi_0))$ the following are equivalent:*
  (1) *f is terminal-surjective.*
  (2) *$f|_D : D \longrightarrow D_0$ is surjective.*
  (3) *$f : G \longrightarrow G_0$ is surjective.*

Proof. (a) (Compare Lemma (3.1).) Each line I is uniquely determined by $t_1 = I \cap (2, 3)^{\pi^{-1}}$ and $t_2 = I \cap (1, 3)^{\pi^{-1}}$. There are $|D|/3$ choices each for t_1 and t_2.

(b) As G is generated by the class D and G_0 is generated by the class D_0 which contains D^f, f is surjective if and only if $f|_D$ is onto D_0. Let $d_0 \in D_0$, and choose a line $I_0 = \langle d_0, e_0 \rangle$ in G_0. Then there is a line $I = O^\iota$ with $O^{\iota f} = I^f = I_0$ if and only if there are $d, e \in D$ with $I = \langle d, e \rangle$ and $d^f = d_0$, $e^f = e_0$. That is, f is terminal-surjective if and only if $f|_D$ is onto D_0. □

Since a covering map from (G, D, π) is precisely a triality homomorphism whose restriction to D is a bijection, Proposition (6.2) gives directly:

(9.6). Corollary. *A morphism of* TriGrp *is monic and terminal-surjective if and only if it is a cover.* □

An important consequence of the corollary is that isogeny in TriGrp can be recognized categorically. Indeed the corollary gives a categorical characterization of covering, and isogeny is the equivalence relation generated by (symmetrized) covering.

Isogenous objects within the full subcategories $\mathsf{UTriGrp}$ or $\mathsf{ATriGrp}$ of TriGrp are isomorphic, therefore we immediately have:

(9.7). Corollary. *In the categories* $\mathsf{UTriGrp}$ *and* $\mathsf{ATriGrp}$ *a morphism is monic and terminal-surjective if and only if it is an isomorphism.* □

(9.8). Corollary. *In* TriGrp *the map* $\mathrm{W}(D_4) \longrightarrow \mathrm{W}(D_4)/\mathrm{Z}(\mathrm{W}(D_4))$ *is a monic and terminal-surjective morphism but is not an isomorphism.*

Proof. This is immediate from Lemma (4.10). □

By the previous two corollaries TriGrp cannot be category equivalent to $\mathsf{UTriGrp}$ or $\mathsf{ATriGrp}$. This provides half of Theorem (9.1), as Mouf and $\mathsf{UTriGrp}$ are equivalent, and two-thirds of Theorem (9.3).

9.2. $\mathsf{Mouf}^\star$ and $\mathsf{TriGrp}^\star$ are not equivalent

By Theorem (8.2) the categories $\mathsf{Mouf}^\star$ and $\mathsf{UTriGrp}^\star$ are equivalent. Therefore to prove that $\mathsf{Mouf}^\star$ is not equivalent to $\mathsf{TriGrp}^\star$ we may prove instead that

$\mathsf{UTriGrp}^\star$ is not equivalent to $\mathsf{TriGrp}^\star$. At the same time we show that $\mathsf{ATriGrp}^\star$ is not equivalent to $\mathsf{TriGrp}^\star$.

The proof is in spirit the same as that of the previous section, but the details are messier. The categories $\mathsf{TriGrp}^\star$, $\mathsf{UTriGrp}^\star$, and $\mathsf{ATriGrp}^\star$ again have the object $O = (\mathrm{Sym}(3), \{(2,3),(1,3),(1,2)\}, \mathrm{Id}_{\mathrm{Sym}(3)}, \mathrm{Sym}(3))$, but it is now a zero object—both terminal and initial. In this case all objects have O-order 1 and every morphism is O-surjective, so we must look elsewhere.

Recall various categorical concepts from Section 1.5. The nonzero object Z of a category C with zero objects is a $\mathbb{Z}$-object provided it satisfies:

(i) *for all nonzero A there are nonzero $f \in \mathrm{Hom}_{\mathsf{C}}(Z, A)$;*

(ii) *if $\mathrm{Hom}_{\mathsf{C}}(A, Z)$ contains nonzero morphisms, then there are morphisms $f \in \mathrm{Hom}_{\mathsf{C}}(A, Z)$ and $g \in \mathrm{Hom}_{\mathsf{C}}(Z, A)$ with $gf = 1_Z$;*

(iii) *a nonzero idempotent in $\mathrm{End}_{\mathsf{C}}(Z)$ must be 1_Z.*

In C there is at most one isomorphism class of $\mathbb{Z}$-objects by Lemma (1.11).

Let Z be a $\mathbb{Z}$-object in C. The morphism $f \in \mathrm{Hom}_{\mathsf{C}}(X, Y)$ is $\mathbb{Z}$-surjective if, for every $a \in \mathrm{Hom}_{\mathsf{C}}(Z, Y)$, there is a $b \in \mathrm{Hom}_{\mathsf{C}}(Z, X)$ with $a = bf$. The $\mathbb{Z}$-order of the object X of C is $|\mathrm{Hom}_{\mathsf{C}}(A, X)|$. Both $\mathbb{Z}$-order and $\mathbb{Z}$-surjectivity are unaffected by category equivalence or passage to full subcategories containing zero objects.

The following proposition motivates the terminology.

(9.9). Proposition.

(a) *In $\mathsf{Mouf}^\star$ the group $(\mathbb{Z}, +)$ is a $\mathbb{Z}$-object.*

(b) *In $\mathsf{Mouf}^\star$ the Moufang loop L has $\mathbb{Z}$-order $|L|$. In particular L is a zero object if and only if it has $\mathbb{Z}$-order 1.*

(c) *In $\mathsf{Mouf}^\star$ a morphism is $\mathbb{Z}$-surjective if and only if it is surjective on the appropriate underlying set.*

Proof. Recall from Proposition (2.13) that Moufang loops are power associative; that is, a subloop generated by a single element is a cyclic subgroup. Therefore, for every element $x \in L$, the map $\iota_x \colon 1 \mapsto x$ extends uniquely to a morphism $\iota_x \in \mathrm{Hom}_{\mathsf{Mouf}^\star}(\mathbb{Z}, L)$, and every morphism of $\mathrm{Hom}_{\mathsf{Mouf}^\star}(\mathbb{Z}, L)$ has this form. In particular, $|\mathrm{Hom}_{\mathsf{Mouf}^\star}(\mathbb{Z}, L)|$ is the number of such ι_x, namely $|L|$, giving (b) (subject to (a)).

Similarly for (c), let $f \in \mathrm{Hom}_{\mathsf{C}}(X, Y)$. Then every ι_y, for $y \in Y$, factors as $\iota_x f$, for some $x \in X$, if and only if the map $f \colon X \longrightarrow Y$ is surjective at the set level.

It remains to prove (a):

(i) There are nonzero morphisms in $\mathrm{Hom}_{\mathsf{C}}(\mathbb{Z}, A)$ if and only if $|A| \neq 1$. That is, if and only if A is not a zero object in $\mathsf{Mouf}^\star$.

(ii) Every $f_0 \in \mathrm{Hom}_{\mathsf{Mouf}^\star}(A, \mathbb{Z})$ has image $m\mathbb{Z}$ for some integer m, and the map is nonzero precisely when m is not 0. Let f_0 be a nonzero map with image $m\mathbb{Z}$, and choose an element a of the loop A with $a^{f_0} = m$. Then $a^f = 1$ extends to a surjective morphism $f \colon A \longrightarrow \mathbb{Z}$. The map $g = \iota_a \in \mathrm{Hom}_{\mathsf{Mouf}^\star}(\mathbb{Z}, A)$ given by $1^g = a$ then has $1^{gf} = (1^g)^f = a^f = 1$. Therefore $gf = \mathrm{Id}_{\mathbb{Z}}$, as desired.

(iii) Each endomorphism of $\mathbb{Z}$ is multiplication by some fixed integer m. Therefore the only nonzero idempotent is given by $m = 1$. □

(9.10). Proposition.

(a) *In* $\mathsf{TriGrp}^\star$ *the group* $\mathrm{W}(\tilde{A}_2)$ *is a* $\mathbb{Z}$*-object.*

(b) *In* $\mathsf{TriGrp}^\star$ *the group* (G,D,π,I) *has* $\mathbb{Z}$*-order* $|D|/3$*. In particular the group* (G,D,π,I) *is a zero object if and only if it has* $\mathbb{Z}$*-order* 1*.*

Proof. Let (W,D_W,π_W,I_W) be the triality group

$$W=\mathrm{W}(\widetilde{A}_2)=\langle\, r,c,e \mid r^2=c^2=e^2=1,\,(rc)^3=(re)^3=(ce)^3=1\,\rangle$$

of Lemma (4.9), where we set $D_W=r^W$, $I_W=\langle r,c\rangle$, and

$$r^{\pi_W}=(2,3),\ c^{\pi_W}=(1,3),\ (rcr)^{\pi_W}=e^{\pi_W}=(1,2)\,.$$

(i) In the group with triality (G,D,π,I) let $I=\langle x,y\rangle$ with $x^\pi=(2,3)$ and $y^\pi=(1,3)$. For every element $w\in D_{(1,2)}=(1,2)^{\pi^{-1}}\cap D$, the map

$$r^{\iota_w}=x,\quad c^{\iota_w}=y,\quad e^{\iota_w}=w$$

extends uniquely to $\iota_w\in\mathrm{Hom}_{\mathsf{TriGrp}^\star}((W,D_W,\pi_W,I_W),(G,D,\pi,I))$, giving every morphism of this set. Therefore there are nonzero morphisms if and only if $D_{(1,2)}\neq\{xyx\}$. That is, if and only if (G,D,π,I) is not a zero object in $\mathsf{TriGrp}^\star$. Equally well $|\mathrm{Hom}_{\mathsf{TriGrp}^\star}((W,D_W,\pi_W,I_W),(G,D,\pi,I))|=|D_{(1,2)}|=|D|/3$, giving (b) (subject to (a)).

(ii) Every $f_0\in\mathrm{Hom}_{\mathsf{TriGrp}^\star}((G,D,\pi,I),(W,D_W,\pi_W,I_W))$ has image $m\mathbb{Z}^2\rtimes I_W$ for some integer m, and the map is nonzero precisely when m is not 0. Let f_0 be such a nonzero map. In particular $x^{f_0}=r$ and $y^{f_0}=c$. Choose an element w of D with $w^{f_0}=(m,m)rcr$. Then $x^f=r$, $y^f=c$, $w^f=e$ extends to a surjective map $f\colon(G,D,\pi,I)\longrightarrow(W,D_W,\pi_W,I_W)$.

The map g in $\mathrm{Hom}_{\mathsf{TriGrp}^\star}((W,D_W,\pi_W,I_W),(G,D,\pi,I))$ given by $r^g=x$, $c^g=y$, $e^g=w$ then has $r^{gf}=r$, $c^{gf}=c$, $e^{gf}=e$. That is, $gf=1_{(G,D,\pi,I)}$, as desired.

(iii) Each endomorphism of $\mathbb{Z}^2\rtimes I_W$ taking I_W to itself is completed by multiplication of $\mathbb{Z}^2$ by some fixed integer m. Therefore the only nonzero idempotent is given by $m=1$ and so is $1_{(W,D_W,\pi_W,I_W)}$. □

The adjoint group with triality $\mathrm{W}(\widetilde{A}_2)$ is also universal since any cover must be generated by three transpositions satisfying the same defining relations as $\mathrm{W}(\widetilde{A}_2)$. From this it is not hard to show that each $\mathrm{W}_n(\widetilde{A}_2)$ is universal (although it is adjoint only when 3 does not divide n by Lemma (4.9)).

(9.11). Proposition. *For* $f\in\mathrm{Hom}_{\mathsf{TriGrp}^\star}((G,D,\pi,I),(G_0,D_0,\pi_0,I_0))$ *the following are equivalent:*

(1) f *is* $\mathbb{Z}$*-surjective.*

(2) $f|_D\colon D\longrightarrow D_0$ *is surjective.*

(3) $f\colon G\longrightarrow G_0$ *is surjective.*

Proof. As G is generated by the class D and G_0 is generated by the class D_0 which contains D^f, f is surjective if and only if $f|_D$ is onto D_0.

Let $w_0\in D_0$ with $w_0^{\pi_0}=t\in\mathrm{Sym}(3)$, and let $I_0=\langle x_0,y_0\rangle$ with $x_0^{\pi_0}\neq t\neq y_0^{\pi_0}$. Thus $r^{\iota_0}=x_0$, $c^{\iota_0}=y_0$, $r^{\iota_0}=w_0$ extends to a morphism ι_0 to (G_0,D_0,π_0,I_0) from $\mathrm{W}(\widetilde{A}_2)$, realized as (W,D_W,π_W,I_W) as above.

Any morphism ι from (W,D_W,π_W,I_W) to (G,D,π,I) is described by $r^\iota=x$, $c^\iota=y$, and $e^\iota=w$ where $w^\pi=t$ and $I=\langle x,y\rangle$. The map f is $\mathbb{Z}$-surjective if and only if for every ι_0 there is an ι with $\iota_0 = \iota f$. This is true in turn if and only if for each $w_0 \in D_0$ there is a $w \in D$ with $w^f = w_0$. Thus f is $\mathbb{Z}$-surjective if and only if $f|_D$ is onto D_0. □

This together with Proposition (6.2) again gives three corollaries.

(9.12). Corollary. *A morphism in* $\mathsf{TriGrp}^\star$ *is monic and* $\mathbb{Z}$*-surjective if and only if it is a cover.* □

As before, an important consequence is that isogeny in $\mathsf{TriGrp}^\star$ can be recognized categorically. The corollary gives a categorical characterization of covering, and isogeny is the equivalence relation generated by (symmetrized) covering.

(9.13). Corollary. *In the categories* $\mathsf{UTriGrp}^\star$ *and* $\mathsf{ATriGrp}^\star$ *a morphism is monic and* $\mathbb{Z}$*-surjective if and only if it is an isomorphism.* □

(9.14). Corollary. *In* $\mathsf{TriGrp}^\star$ *the map* $\mathrm{W}(D_4) \longrightarrow \mathrm{W}(D_4)/\mathrm{Z}(\mathrm{W}(D_4))$ *is a monic and* $\mathbb{Z}$*-surjective morphism but is not an isomorphism.*

Proof. This is again immediate from Lemma (4.10). □

The two corollaries say that $\mathsf{TriGrp}^\star$ cannot be category equivalent to $\mathsf{UTriGrp}^\star$ or $\mathsf{ATriGrp}^\star$. This provides half of Theorem (9.2), as $\mathsf{Mouf}^\star$ and $\mathsf{UTriGrp}^\star$ are equivalent, and two-thirds of Theorem (9.4).

9.3. $\mathsf{Mouf}^\star$ and $\mathsf{ATriGrp}^\star$ are not equivalent

Theorem 3.6 of [**HaN01**] suggests (but fortunately does not state) that the categories Mouf and $\mathsf{ATriGrp}^\star$ are equivalent. This is certainly not the case. ($\mathsf{ATriGrp}^\star$ has zero objects while Mouf has terminal objects that are not initial.) However this does raise the question as to whether Mouf and $\mathsf{ATriGrp}$ are equivalent and, similarly, $\mathsf{Mouf}^\star$ and $\mathsf{ATriGrp}^\star$.

This seems unlikely, as it would say that $\mathsf{UTriGrp}$ and $\mathsf{ATriGrp}$ or $\mathsf{UTriGrp}^\star$ and $\mathsf{ATriGrp}^\star$ are equivalent. On the other hand, the arguments of the previous two sections will fail since $\mathbf{U}\colon \mathsf{ATriGrp} \longrightarrow \mathsf{UTriGrp}$ and $\mathbf{U}^\star\colon \mathsf{ATriGrp}^\star \longrightarrow \mathsf{UTriGrp}^\star$ are faithful functors that are dense (indeed give bijections of isomorphism classes) and respect the appropriate orders and surjections.

In the previous two sections, we used the fact that the groups with triality $\mathrm{W}(D_4)$ and $\mathrm{W}(D_4)/\mathrm{Z}(\mathrm{W}(D_4))$ are isogenous but not isomorphic. We then needed to realize this categorically. Here the crucial observation we use is more complicated:

> *The adjoint group with triality* $\mathrm{W}_3(\widetilde{D}_4)$ *contains as a subgroup the universal group* $\mathrm{W}(D_4)$*, but it does not contain as a subgroup the adjoint group* $\mathrm{W}(D_4)/\mathrm{Z}(\mathrm{W}(D_4))$*.*

The categorical rendering is correspondingly more complicated.

(9.15). Proposition.

(a) *There are, up to isomorphism and up to isotopism, exactly two loops of order* 4*: the cyclic and elementary abelian groups of order* 4*.*

(b) *There are, up to isomorphism and up to isotopism, exactly six Moufang loops of order* 12*. Each has a subloop of order* 4*.*

Proof. (a) It is an easy and pleasant exercise to see that there are only two types of 4×4 Latin squares.

(b) Chein and Pflugfelder [**ChP71**] proved that the Moufang loops of order 12 are (up to isomorphism) the five groups of order 12 and one nonassociative Moufang loop of order 12, the smallest nonassociative Moufang loop. That loop is, in fact, $\mathrm{W}_3(\widetilde{D}_4)\mathbf{CS}$ and has $\mathrm{W}(D_4)\mathbf{CS}$ as a subloop of order 4. Each group of order 12 has Sylow 2-subgroups of order 4. □

In the category C, a subobject of the object B is defined as an appropriate equivalence class of monic morphisms $f \in \mathrm{Hom}_{\mathsf{C}}(X, B)$ for various isomorphic X; see [**Jac89**, p.18]. We only need a weaker (and somewhat abused) version of this. We say that B has X as a *subobject* if there is at least one monic morphism in $\mathrm{Hom}_{\mathsf{C}}(X, B)$. Category equivalences take subobjects (in this sense) to subobjects.

(9.16). Corollary.

(a) *In* $\mathsf{Mouf}^\star$ *there are, up to isomorphism, exactly two loops having* $\mathbb{Z}$*-order* 4*: the cyclic and elementary abelian groups of order* 4*.*

(b) *In* $\mathsf{Mouf}^\star$ *there are, up to isomorphism, exactly six Moufang loops having* $\mathbb{Z}$*-order* 12*. Each has a subloop of* $\mathbb{Z}$*-order* 4*.*

Proof. Part (a) and the first sentence of (b) are immediate from the corresponding parts of the proposition. Let the Moufang loop Q of $\mathbb{Z}$-order (and order) 12 have the subloop X. That is, there is a monic map $f \in \mathrm{Hom}_{\mathsf{Mouf}^\star}(X, Q)$. By Theorem (8.4) the map f is injective. Therefore L has a subloop isomorphic to X, and the result is completed by the last sentence of the proposition. □

(9.17). Corollary.

(a) *In* $\mathsf{UTriGrp}^\star$ *there are, up to isomorphism, exactly two triality groups having* $\mathbb{Z}$*-order* 4*:* $\mathrm{W}_4(\tilde{A}_2)$ *and* $\mathrm{W}(D_4)$*.*

(b) *In* $\mathsf{ATriGrp}^\star$ *there are, up to isomorphism, exactly two triality groups having* $\mathbb{Z}$*-order* 4*:* $\mathrm{W}_4(\tilde{A}_2)$ *and* $\mathrm{W}(D_4)/\mathrm{Z}(\mathrm{W}(D_4))$*.*

Proof. By Theorem (8.2) and the previous corollary, there are only two isomorphism classes of universal triality groups with $\mathbb{Z}$-order 4. By Lemmas (4.9) and (4.10) one contains $\mathrm{W}_4(\tilde{A}_2)$, with trivial center, and the other $\mathrm{W}(D_4)$ with center of order 2. This gives (a), and (b) follows immediately. □

Similarly by Theorem (8.2):

(9.18). Corollary. *In* $\mathsf{UTriGrp}^\star$ *there are, up to isomorphism, exactly six triality groups with* $\mathbb{Z}$*-order* 12*. Each has a triality subgroup of* $\mathbb{Z}$*-order* 4*.* □

On the other hand:

(9.19). Lemma. *In* $\mathsf{ATriGrp}^\star$ *the group with triality* $\mathrm{W}_3(\widetilde{D}_4)$ *has* $\mathbb{Z}$*-order* 12 *and has no triality subgroup of* $\mathbb{Z}$*-order* 4*.*

Proof. By Lemma (4.11) the group $\mathrm{W}_3(\widetilde{D}_4)$ is adjoint and has $\mathbb{Z}$-order 12. For it to have in $\mathsf{ATriGrp}^\star$ a subgroup of $\mathbb{Z}$-order 4 there would need to be a monic map to it from either $\mathrm{W}_4(\widetilde{A}_2)$ or $\mathrm{W}(D_4)/\mathrm{Z}(\mathrm{W}(D_4))$ by Corollary (9.17). By Proposition (7.14) such a monic map is an injection. But $\mathrm{W}_3(\widetilde{D}_4)$ does not have triality subgroups $\mathrm{W}_4(\widetilde{A}_2)$ or $\mathrm{W}(D_4)/\mathrm{Z}(\mathrm{W}(D_4))$, again by Lemma (4.11). □

The lasts two corollaries show that $\mathsf{UTriGrp}^\star$ and $\mathsf{ATriGrp}^\star$ are not equivalent. This completes the proof of nonequivalence stated in Theorem (9.4) and also that of Theorem (9.2), since $\mathsf{Mouf}^\star$ and $\mathsf{UTriGrp}^\star$ are equivalent.

Furthermore, by Theorems (2.15) and (7.9) the categories of Theorems (9.2) and (9.4) may be thought of as the pointed counterparts to the categories of Theorems (9.1) and (9.3), which thus are also nonequivalent by Theorem (1.10), completing the proof of those theorems.

Similar arguments to those of this section lead to the following, which was promised in Chapter 5.

(9.20). Corollary. *The map* $\mathbf{A}\colon \mathsf{CLSD} \longrightarrow \mathsf{TriGrp}$ *is not a functor.*

Proof. Let W be the triality group $\mathrm{W}(D_4)$ and $\overline{W}$ the corresponding adjoint group $\mathrm{W}(D_4)/\mathrm{Z}(\mathrm{W}(D_4))$ as in Lemma (4.10). Let T be the adjoint group $\mathrm{W}_3(\widetilde{D}_4)$ as in Lemma (4.11).

Next let $(P,S) = W\mathbf{C} \simeq \overline{W}\mathbf{C}$ and $(P_T,S_T) = T\mathbf{C}$, so that

$$(P,S)\mathbf{A} = W\mathbf{CA} \simeq \overline{W}\mathbf{CA} \simeq \overline{W}$$

and

$$(P_T,S_T)\mathbf{A} = T\mathbf{CA} \simeq T\,.$$

The group $\mathrm{W}_3(\widetilde{D}_4)$ is the split extension of a 3-group by $\mathrm{W}(D_4)$, so in TriGrp there are morphisms

$$W \xrightarrow{f} T \xrightarrow{g} W$$

with $fg = 1_W$. As $(P,S) = W\mathbf{C}$ and $(P_T,S_T) = T\mathbf{C}$ we then have in CLSD

$$(P,S) \xrightarrow{f\mathbf{C}} (P_T,S_T) \xrightarrow{g\mathbf{C}} (P,S)$$

with $f\mathbf{C}g\mathbf{C} = 1_{(P,S)}$.

Were $\mathbf{A}$ to be a functor, then $\mathbf{CA}$ would also be a functor and we would get new morphisms in TriGrp:

$$(P,S)\mathbf{A} \xrightarrow{f\mathbf{CA}} (P_T,S_T)\mathbf{A} \xrightarrow{g\mathbf{CA}} (P,S)\mathbf{A}$$

with $f\mathbf{CA}g\mathbf{CA} = 1_{(P,S)\mathbf{A}}$. That is, there would be in TriGrp morphisms

$$\overline{W} \xrightarrow{f_0} T \xrightarrow{g_0} \overline{W}$$

with $f_0g_0 = 1_{\overline{W}}$. But $T \simeq \mathrm{W}_3(\widetilde{D}_4)$ has no subgroup $\mathrm{W}(D_4)/\mathrm{Z}(\mathrm{W}(D_4))$ by Lemma (4.11), so there are no such morphisms. □

Part 3

Related Topics

Chapter 10

The Functors **S** and **M**

We already have concrete constructions of the equivalences $\mathbf{T}$, $\mathbf{B}$, and $\mathbf{C}$, even on the parent categories Loop, LSD, and TriGrp. In this chapter and the next we discuss more precisely the remaining $\mathbf{S}$, $\mathbf{M}$, and $\mathbf{G}$ and their pointed versions.

$$\begin{tikzcd}
\mathsf{Mouf} \arrow[rr, shift left, "\mathbf{G}"] \arrow[dr, shift left, "\mathbf{T}"] & & \mathsf{UTriGrp} \arrow[ll, shift left, "\mathbf{M}"] \arrow[dl, shift left, "\mathbf{C}"] \\
& \mathsf{CLSD} \arrow[ul, shift left, "\mathbf{S}"] \arrow[ur, shift left, "\mathbf{B}"] &
\end{tikzcd}$$

10.1. S and S*

We first define the functor $\mathbf{S}^\star$ from its parent category $\mathsf{LSD}^\star$ to $\mathsf{Loop}^\star$. This then leads to $\mathbf{S}$ from LSD to Loop as well as the restrictions of $\mathbf{S}^\star$ to $\mathsf{CLSD}^\star$ and $\mathbf{S}$ to CLSD.

Let $(P, S) \in \mathsf{LSD}$ with I a line of S. We identify (P, S) with an isomorphic Latin square design by renaming its points. First relabel the elements of P^{E} as $\{ x_{\mathrm{E}} \mid x \in Q \}$ for a set Q with $1 \in Q$ so that $1_{\mathrm{E}} = I \cap P^{\mathrm{E}}$. Next we let $I = (1_{\mathrm{R}}, 1_{\mathrm{C}}, 1_{\mathrm{E}})$; and, more generally, for each $x \in Q$, rename the points $x_{\mathrm{R}} \in P^{\mathrm{R}}$ and $x_{\mathrm{C}} \in P^{\mathrm{C}}$ according to

$$(x_{\mathrm{R}}, 1_{\mathrm{C}}, x_{\mathrm{E}}),\ (1_{\mathrm{R}}, x_{\mathrm{C}}, x_{\mathrm{E}}) \in S\,.$$

We can now define on Q the structure $(Q, \cdot)$ whose binary operation is given by

$$(x_{\mathrm{R}}, y_{\mathrm{C}}, (x \cdot y)_{\mathrm{E}}) \in S\,.$$

As (P, S) is a Latin square design, $(Q, \cdot)$ is in fact a loop with identity element 1. We set $(Q, \cdot) = (P, S, I)\mathbf{S}^\star$.

If $f \in \mathrm{Hom}_{\mathsf{LSD}^\star}((P,S,I),(P_0,S_0,I_0))$ with $M = (P_0,S_0,I_0)\mathbf{S}^\star$ then $f\mathbf{S}^\star \in \mathrm{Hom}_{\mathsf{Mouf}^\star}(Q,M)$ is the homotopism (α,β,γ) given by

$$\begin{aligned} x^\alpha &= x_0 \quad \text{where} \quad x_{\mathrm{R}}^f = (x_0)_{\mathrm{R}}\,, \\ y^\beta &= y_0 \quad \text{where} \quad y_{\mathrm{C}}^f = (y_0)_{\mathrm{C}}\,, \\ z^\gamma &= z_0 \quad \text{where} \quad z_{\mathrm{E}}^f = (z_0)_{\mathrm{E}}\,. \end{aligned}$$

This completes the description of $\mathbf{S}^\star$. For $\mathbf{S}$, we must define the various $(P,S)\mathbf{S}$ and $f\mathbf{S}$ for $f \in \mathrm{Hom}_{\mathsf{LSD}}((P,S),(P_0,S_0))$.

For each $(P,S) \in \mathsf{LSD}$ choose a line $I = I_{(P,S)}$. Then we set $(P,S)\mathbf{S} = (P,S,I_{(P,S)})\mathbf{S}^\star$. (Recall that we are viewing $\mathsf{Loop}^\star$ as a subcategory of Loop.) For every $g \in \mathrm{Hom}_{\mathsf{LSD}}((P,S),(P_0,S_0))$ there is a unique line $I_0 = I^g_{(P,S)}$ in S_0 with $g_{I_{(P,S)}} \in \mathrm{Hom}_{\mathsf{LSD}^\star}((P,S,I_{(P,S)}),(P_0,S_0,I_0))$. (Note that I_0 need not be equal to $I_{(P_0,S_0)}$.) We then set $g\mathbf{S} = g_{I_{(P,S)}}\mathbf{S}^\star$. As the initial choice of $I_{(P,S)}$ was arbitrary, this fabrication of the functor $\mathbf{S}$ from $\mathbf{S}^\star$ is not canonical; however replacing $I_{(P,S)}$ by some other line I of (P,S) replaces $(P,S)\mathbf{S}$ by a loop isotope. Since isotopism is isomorphism in the category Loop, this does not cause a problem for our construction of the equivalence $\mathbf{S}$.[1]

By design $(P,S,I)\mathbf{S}^\star\mathbf{T}^\star$ and (P,S,I) are isomorphic. Therefore by Theorem (3.9) the restriction of $\mathbf{S}^\star$ to $\mathsf{CLSD}^\star$ has its image in $\mathsf{Mouf}^\star$, and correspondingly the restriction of $\mathbf{S}$ to CLSD has its image in Mouf.

10.2. M and M*

We effectively construct the functors $\mathbf{M}^\star$ from $\mathsf{TriGrp}^\star$ to $\mathsf{Mouf}^\star$ and $\mathbf{M}$ from TriGrp to Mouf as the compositions $\mathbf{M}^\star = \mathbf{C}^\star\mathbf{S}^\star$ and $\mathbf{M} = \mathbf{CS}$.

Let (G,D,π) be a group with triality. For the line $I = I_{(G,D,\pi)}$, we set

$$r_1 = I \cap (2,3)^{\pi^{-1}} \qquad c_1 = I \cap (1,3)^{\pi^{-1}} \qquad e_1 = I \cap (1,2)^{\pi^{-1}}\,.$$

We then let $(1,2)^{\pi^{-1}} = \{\, e_h \mid h \in Q \,\}$ for a set Q (with $1 \in Q$).

Next for each $x \in Q$ set

$$r_x = \langle c_1, e_x\rangle \cap (2,3)^{\pi^{-1}} \quad \text{and} \quad c_y = \langle r_1, e_y\rangle \cap (1,3)^{\pi^{-1}}\,.$$

We define on Q the structure $(Q,\cdot)$ with binary operation given by

$$e_{x\cdot y} = \langle r_x, c_y\rangle \cap (1,2)^{\pi^{-1}}\,.$$

As $\langle r_x, c_y\rangle = \langle r_x, e_{x\cdot y}\rangle = \langle e_{x\cdot y}, c_y\rangle$ intersects D in $\{r_x, c_y, e_{x\cdot y}\}$, any two of x, y and $x\cdot y$ determine the remaining one uniquely; so $(Q,\cdot)$ is a loop with identity element 1. Furthermore by construction the elements of D act as a full collection of central automorphisms on the Latin square design $Q\mathbf{T}$, so by Theorem (3.9) the loop Q is a Moufang loop. We set $(Q,\cdot) = (G,D,\pi,I)\mathbf{M}^\star$ and so $(Q,\cdot) = (G,D,\pi)\mathbf{M}$.

If $f \in \mathrm{Hom}_{\mathsf{TriGrp}^\star}((G,D,\pi,I),(G_0,D_0,\pi_0,I_0))$ with the Moufang loop $M = (G_0,D_0,\pi_0,I_0)\mathbf{M}^\star$ then $f\mathbf{M}^\star \in \mathrm{Hom}_{\mathsf{Mouf}^\star}(Q,M)$ is the homotopism (α,β,γ) given

[1] At the highest level, we are invoking the Axiom of Choice in these arguments. But at the lowest level, for any particular Latin square we are merely choosing a cell to play the roll of the identity, as in Remark (2.3) and our proof of Theorem (3.14).

by

$$\begin{aligned} x^\alpha &= x_0 \quad \text{where} \quad r_x^f = r_{x_0} \\ y^\beta &= y_0 \quad \text{where} \quad c_y^f = c_{y_0} \\ z^\gamma &= z_0 \quad \text{where} \quad e_z^f = e_{z_0} \,. \end{aligned}$$

For $g \in \mathrm{Hom}_{\mathsf{TriGrp}}((G,D,\pi),(G_0,D_0,\pi_0))$ there is a unique line $I_0 = I^g$ of the triality group (G_0,D_0,π_0) with g inducing $g_I \in \mathrm{Hom}_{\mathsf{TriGrp}^\star}((G,D,\pi,I),(G_0,D_0,\pi_0,I_0))$. In this case we let $g\mathbf{M}$ be $g_I\mathbf{M}^\star$ viewed as an element of $\mathrm{Hom}_{\mathsf{Mouf}}(Q,M)$.

As an example, we consider the triality groups introduced in Section 4.2.1—the wreath products $\mathrm{Wr}(H,3)$ for H a group. A version of this is already in Doro's paper [**Dor78**, p. 385].

(10.1). THEOREM. *Let H be a group and D the conjugacy class of the full wreath product $H \wr \mathrm{Sym}(3)$ containing the transposition class of* $\mathrm{Sym}(3)$*. Set* $\mathrm{Wr}(H,3) = \langle D\rangle$*, and let π be the projection homomorphism from the wreath product and* $\mathrm{Wr}(H,3)$ *to* $\mathrm{Sym}(3)$*. Then the Moufang loop*

$$(\mathrm{Wr}(H,3),D,\pi,\mathrm{Sym}(3))\mathbf{M}^\star$$

is isomorphic to the group H.

PROOF. We construct the loop $(Q,\cdot)$ as above. Set

$$r_1 = (2,3)\,, \quad c_1 = (1,3)\,, \quad e_1 = (2,3)\,.$$

Next $(1,2)^{\pi^{-1}} = \{\, e_h \mid h \in Q \,\}$ is given by

$$e_h = h_1^{-1}h_2(1,2)\,, \quad \text{for } h \in H\,,$$

by Proposition (4.5)(a). In particular we may identify the set Q with H.

For each $x \in H$ we define

$$r_x = \langle c_1, e_x\rangle \cap (2,3)^{\pi^{-1}} = (1,3)x_1^{-1}x_2(1,2)(1,3) = x_3^{-1}x_2(3,2)$$

and

$$c_y = \langle r_1, e_y\rangle \cap (1,3)^{\pi^{-1}} = (2,3)y_1^{-1}y_2(1,2)(2,3) = y_1^{-1}y_3(1,3)\,.$$

Finally the product $x \cdot y$ of the two elements $x, y \in Q = H$ is given by

$$\begin{aligned} e_{x\cdot y} &= \langle r_x, c_y\rangle \cap (1,2)^{\pi^{-1}} \\ &= (x_3^{-1}x_2(3,2))(y_1^{-1}y_3(1,3))(x_3^{-1}x_2(3,2)) \\ &= x_3^{-1}x_2y_1^{-1}y_2(3,2)x_1^{-1}x_2(1,3)(3,2) \\ &= x_3^{-1}x_2y_1^{-1}y_2x_1^{-1}x_3(3,2)(1,3)(3,2) \\ &= (xy)_1^{-1}(xy)_2(1,2) \\ &= e_{xy}\,. \end{aligned}$$

Thus $x \cdot y = xy$, and the loop $(Q,\cdot)$ is isomorphic to the group H. □

We do not prove the following similar theorem here, but results equivalent to it can be found in [**GrZ06**, Prop. 1] and [**Hal06**, §4].

(10.2). THEOREM. *Let H be a group and D the conjugacy class of the full wreath product $H \wr \mathrm{Sym}(4)$ containing the transposition class of* $\mathrm{Sym}(4)$*. Set*

$\mathrm{Wr}(H,4) = \langle D\rangle$, *and let* π *be the homomorphism from the wreath product and* $\mathrm{Wr}(H,4)$ *to the quotient* $\mathrm{Sym}(3)$ *of* $\mathrm{Sym}(4)$. *Then the Moufang loop*

$$(\mathrm{Wr}(H,4), D, \pi, \mathrm{Sym}(3))\mathbf{M}^{\star}$$

is isomorphic to the Chein generalized dihedral loop having H *of index* 2, *as constructed in Theorem (2.16).*

Chapter 11

The Functor **G**

In this chapter we give a construction of the functors **G** and $\mathbf{G}^\star$. We then discuss the properties of universal groups with triality in terms of their associated Moufang loops.

11.1. G and G*

The functor **TB** gives an equivalence of Mouf and $\mathsf{UTriGrp}$ by taking the loop Q to the universal group with triality $\mathrm{G}(P_{Q\mathbf{T}}, S_{Q\mathbf{T}})$. We wish a more direct and simpler version of this functor.

(11.1). Presentation. *For the quasigroup Q, the group G_Q has the following presentation:*

Generators:

r_x, c_x, *and* e_x *for arbitrary* $x \in Q$;

Relations:

for arbitrary $x, y \in Q$:

(1) $\mathsf{r}_x^2 = \mathsf{c}_x^2 = \mathsf{e}_x^2 = 1$;

(2) $\mathsf{r}_x\mathsf{c}_y\mathsf{r}_x = \mathsf{c}_y\mathsf{r}_x\mathsf{c}_y = \mathsf{e}_{xy}$.

The map

$$\mathsf{r}_x \longrightarrow (2,3) \quad \mathsf{c}_x \longrightarrow (1,3) \quad \mathsf{e}_x \longrightarrow (1,2)$$

gives a homomorphism onto Sym(3). Thus the relation (2) effectively says that, for each pair $x, y \in Q$, the subgroup $\langle \mathsf{r}_x, \mathsf{c}_y, \mathsf{e}_{xy} \rangle$ is isomorphic to Sym(3).

We have immediately:

(11.2). Lemma. *If $(\alpha, \beta, \gamma)\colon Q \longrightarrow M$ is an surjective homotopism of the quasigroups Q and M, then the map*

$$\mathsf{r}_x \longrightarrow \mathsf{r}_{x^\alpha} \quad \mathsf{c}_x \longrightarrow \mathsf{c}_{x^\beta} \quad \mathsf{e}_x \longrightarrow \mathsf{e}_{x^\gamma}$$

extends uniquely to a surjective homomorphism of groups from G_Q to G_M. Especially an isotopism (α, β, γ) extends uniquely to an isomorphism of G_Q an G_M. □

In particular by Lemma (2.1) it is always possible to replace the quasigroup Q of the presentation with a loop.

(11.3). Theorem. *For a loop Q the groups G_Q and $\mathrm{G}(P_{Q\mathbf{T}}, S_{Q\mathbf{T}})$ are isomorphic universal groups with triality under the map*

$$\mathsf{r}_x \xrightarrow{\iota} \widetilde{x}_{\mathrm{R}} \quad \mathsf{c}_x \xrightarrow{\iota} \widetilde{x}_{\mathrm{C}} \quad \mathsf{e}_x \xrightarrow{\iota} \widetilde{x}_{\mathrm{E}}$$

The transposition class of the universal group with triality G_Q is its generating set $D_Q = \{\, \mathsf{r}_x, \mathsf{c}_x, \mathsf{e}_x \mid x \in Q \,\}$ and the map $\pi_Q \colon D \longrightarrow \mathrm{Sym}(3)$ is given by

$$\mathsf{r}_x \mapsto (2,3) \quad \mathsf{c}_x \mapsto (1,3) \quad \mathsf{e}_x \mapsto (1,2)\,.$$

For every $x, y \in Q$ the restriction of π_Q is an isomorphism of $\langle \mathsf{r}_x, \mathsf{c}_y, \mathsf{e}_{xy} \rangle$ and $\mathrm{Sym}(3)$*. Especially $I_Q = \langle \mathsf{r}_1, \mathsf{c}_1, \mathsf{e}_1 \rangle$ is a line of the group with triality $(\mathrm{G}_Q, D_Q, \pi_Q)$.*

The loop Q is a Moufang loop if and only if each of the maps

$$x \mapsto \mathsf{r}_x\,, \quad x \mapsto \mathsf{c}_x\,, \quad x \mapsto \mathsf{e}_x$$

is a bijection of Q and the corresponding subset $D_Q \cap (i,j)^{\pi_Q^{-1}}$ of G_Q.

Proof. Clearly the map ι is a bijection of the generating sets for the two corresponding free groups, so we must show that ι takes the relations (11.1) for G_Q to relations valid in $\mathrm{G}(P_{Q\mathbf{T}}, S_{Q\mathbf{T}})$ and conversely that ι^{-1} takes the relations (5.1) for $\mathrm{G}(P_{Q\mathbf{T}}, S_{Q\mathbf{T}})$ to relations valid in G_Q. This is clearly the case for the relations (11.1)(1) and (5.1)(1) which merely state that all generators square to the identity.

Consider first the relations

$$\mathsf{r}_x\mathsf{c}_y\mathsf{r}_x = \mathsf{e}_{xy} \quad \text{and} \quad \mathsf{c}_y\mathsf{r}_x\mathsf{c}_y = \mathsf{e}_{xy}$$

of (11.1)(2). Under ι these become

$$\widetilde{x}_{\mathrm{R}}\widetilde{y}_{\mathrm{C}}\widetilde{x}_{\mathrm{R}} = \widetilde{xy}_{\mathrm{E}} \quad \text{and} \quad \widetilde{y}_{\mathrm{C}}\widetilde{x}_{\mathrm{R}}\widetilde{y}_{\mathrm{C}} = \widetilde{xy}_{\mathrm{E}}\,.$$

As $\{\widetilde{x}_{\mathrm{R}}, \widetilde{y}_{\mathrm{C}}, \widetilde{xy}_{\mathrm{E}}\}$ is a line of $(P_{Q\mathbf{T}}, S_{Q\mathbf{T}})$, both of these are relations under (5.1)(2).

Conversely, for each line $\{\widetilde{x}_{\mathrm{R}}, \widetilde{y}_{\mathrm{C}}, \widetilde{xy}_{\mathrm{E}}\}$ of $(P_{Q\mathbf{T}}, S_{Q\mathbf{T}})$ we have the following six relations of (5.1)(2) and their images under ι^{-1}:

$$\begin{aligned}
\widetilde{x}_{\mathrm{R}}\widetilde{y}_{\mathrm{C}}\widetilde{x}_{\mathrm{R}} = \widetilde{xy}_{\mathrm{E}} &\xrightarrow{\iota^{-1}} \mathsf{r}_x\mathsf{c}_y\mathsf{r}_x = \mathsf{e}_{xy}\\
\widetilde{y}_{\mathrm{C}}\widetilde{x}_{\mathrm{R}}\widetilde{y}_{\mathrm{C}} = \widetilde{xy}_{\mathrm{E}} &\xrightarrow{\iota^{-1}} \mathsf{c}_y\mathsf{r}_x\mathsf{c}_y = \mathsf{e}_{xy}\\
\widetilde{x}_{\mathrm{R}}\widetilde{xy}_{\mathrm{E}}\widetilde{x}_{\mathrm{R}} = \widetilde{y}_{\mathrm{C}} &\xrightarrow{\iota^{-1}} \mathsf{r}_x\mathsf{e}_{xy}\mathsf{r}_x = \mathsf{c}_y\\
\widetilde{y}_{\mathrm{C}}\widetilde{xy}_{\mathrm{E}}\widetilde{y}_{\mathrm{C}} = \widetilde{x}_{\mathrm{R}} &\xrightarrow{\iota^{-1}} \mathsf{c}_y\mathsf{e}_{xy}\mathsf{c}_y = \mathsf{r}_x\\
\widetilde{xy}_{\mathrm{E}}\widetilde{y}_{\mathrm{C}}\widetilde{xy}_{\mathrm{E}} = \widetilde{x}_{\mathrm{R}} &\xrightarrow{\iota^{-1}} \mathsf{e}_{xy}\mathsf{c}_y\mathsf{e}_{xy} = \mathsf{r}_x\\
\widetilde{xy}_{\mathrm{E}}\widetilde{x}_{\mathrm{R}}\widetilde{xy}_{\mathrm{E}} = \widetilde{y}_{\mathrm{C}} &\xrightarrow{\iota^{-1}} \mathsf{e}_{xy}\mathsf{r}_x\mathsf{e}_{xy} = \mathsf{c}_y\,.
\end{aligned}$$

In particular, the first two relations from (5.1)(2) are sent by ι^{-1} to relations of (11.1)(2). Indeed the subgroup $\langle\, \mathsf{r}_x, \mathsf{c}_y, \mathsf{e}_{xy} \rangle$ of G_Q satisfies the relations

$$\mathsf{r}_x^2 = \mathsf{c}_y^2 = 1 \quad \text{and} \quad (\mathsf{r}_x\mathsf{c}_y)^3 = (\mathsf{r}_x\mathsf{c}_y\mathsf{r}_x)(\mathsf{c}_y\mathsf{r}_x\mathsf{c}_y) = \mathsf{e}_{xy}^2 = 1$$

and so is a homomorphic image of $\mathrm{W}(A_2) \simeq \mathrm{Sym}(3)$. On the other hand π_Q clearly is a homomorphism of G_Q onto $\mathrm{Sym}(3)$, so π_Q restricts to an isomorphism of $\langle \mathsf{r}_x, \mathsf{c}_y, \mathsf{e}_{xy} \rangle$ and $\mathrm{Sym}(3)$, as claimed.

Now all the relations of (5.1)(2) are sent by ι^{-1} to relations that hold within $\langle \mathsf{r}_x, \mathsf{c}_y, \mathsf{e}_{xy} \rangle \simeq \mathrm{Sym}(3)$. Therefore ι gives an isomorphism of G_Q with $\mathrm{G}(P_{Q\mathbf{T}}, S_{Q\mathbf{T}})$.

From Lemma (5.3) and Proposition (8.3) we know that $\mathrm{G}(P_{Q\mathbf{T}}, S_{Q\mathbf{T}})$ is a universal group with triality whose transposition class is $\{\, \widetilde{x}_{\mathrm{R}}, \widetilde{x}_{\mathrm{C}}, \widetilde{x}_{\mathrm{E}} \mid x \in Q \,\}$ and that its projection map π is determined by

$$\widetilde{x}_{\mathrm{R}} \mapsto (2,3) \quad \widetilde{x}_{\mathrm{C}} \mapsto (1,3) \quad \widetilde{x}_{\mathrm{E}} \mapsto (1,2)\,.$$

Therefore under the isomorphism ι^{-1} the group G_Q is a universal group with triality whose transposition class is

$$\{\, \widetilde{x}_{\mathrm{R}}, \widetilde{x}_{\mathrm{C}}, \widetilde{x}_{\mathrm{E}} \mid x \in Q \,\}^{\iota^{-1}} = \{\, \mathsf{r}_x, \mathsf{c}_x, \mathsf{e}_x \mid x \in Q \,\}$$

and whose projection map π_Q is $\iota\pi$.

By Lemma (5.4) the loop Q is Moufang precisely when there is a bijection between the points of the Latin square design and the elements of the generating conjugacy class. □

As a consequence of the theorem, we may set $Q\mathbf{G} = (\mathrm{G}_Q, D_Q, \pi_Q)$. For the morphism $(\alpha, \beta, \gamma) \in \mathrm{Hom}_{\mathsf{Loop}}(Q, M)$ the corresponding morphism of $\mathsf{UTriGrp}$ is $(\alpha, \beta, \gamma)\mathbf{G} = (a, b, c)$ given by

$$\mathsf{r}_x^a = \mathsf{r}_{x^\alpha} \quad \mathsf{c}_x^b = \mathsf{c}_{x^\beta} \quad \mathsf{e}_x^c = \mathsf{e}_{x^\gamma}\,.$$

Recalling that $I_Q = \langle \mathsf{r}_1, \mathsf{c}_1, \mathsf{e}_1 \rangle$, we define $Q\mathbf{G}^\star = (\mathrm{G}_Q, D_Q, \pi_Q, I_Q)$. The theorem then immediately gives:

(11.4). Corollary.

(a) *$Q\mathbf{G}$ and $Q\mathbf{TB}$ are isomorphic in* TriGrp *and* $\mathsf{UTriGrp}$.
(b) *$Q\mathbf{G}^\star$ and $Q\mathbf{T}^\star\mathbf{B}^\star$ are isomorphic in* $\mathsf{TriGrp}^\star$ *and* $\mathsf{UTriGrp}^\star$. □

11.2. Properties of universal groups

The following properties of universal groups coming from Moufang loops will be of interest in Section 13.1. By Proposition (2.12) every Moufang loop is an inverse property loop, has two-sided inverses, and satisfies the antiautomorphic inverse property $(xy)^{-1} = y^{-1}x^{-1}$. In particular, part (a) of the proposition below is unambiguous as stated.

(11.5). Proposition. *Let $G = \mathrm{G}_Q$ for Q a Moufang loop, and let $K = \ker \pi_Q$. Set $\eta = \mathsf{r}_1$, $\sigma = \mathsf{c}_1$, $\epsilon = \mathsf{e}_1$, and $\mu = \eta\sigma = \sigma\epsilon$. Further let $H = \mathrm{C}_K(\eta)$, the subgroup of all elements of K that commute with η. For each $x \in Q$ define $\mathrm{R}_x = \mathsf{c}_x\mathsf{c}_1$ and then set $R = \{\, \mathrm{R}_x \mid x \in Q \,\}$.*

(a) *For distinct x, y in Q we have $\mathrm{R}_x \neq \mathrm{R}_y$ and $\mathrm{R}_x^{-1} = \mathrm{R}_{x^{-1}}$.*
(b) *The set R equals $\{\, [k, \sigma] \mid k \in K \,\}$ and is a set of right (and left) coset representatives for H in K.*
(c) *$\mathrm{R}_x\mathrm{R}_y \in H\mathrm{R}_{xy}$.*
(d) *$\mathrm{R}_{xy} = \mathrm{R}_y^{-\mu^2}\mathrm{R}_x\mathrm{R}_y^{-\mu} = \mathrm{R}_x^{-\mu}\mathrm{R}_y\mathrm{R}_x^{-\mu^2}$.*

Proof. (a) As Q is Moufang, if $x \neq y$ then $\mathsf{c}_x \neq \mathsf{c}_y$ by Theorem (11.3). Therefore $\mathrm{R}_x = \mathsf{c}_x\mathsf{c}_1 \neq \mathsf{c}_y\mathsf{c}_1 = \mathrm{R}_y$. Also

$$\begin{aligned}
\mathrm{R}_x^{-1} &= \mathsf{c}_1\mathsf{c}_x \\
&= \mathsf{c}_1(\mathsf{e}_x\mathsf{e}_x)\mathsf{c}_x(\mathsf{e}_x\mathsf{e}_x) \\
&= \mathsf{c}_1\mathsf{e}_x(\mathsf{e}_x\mathsf{c}_x\mathsf{e}_x)\mathsf{e}_x \\
&= \mathsf{c}_1\mathsf{e}_x\mathsf{r}_1\mathsf{e}_x \\
&= \mathsf{c}_1\mathsf{e}_x(\mathsf{c}_1\mathsf{c}_1)\mathsf{r}_1(\mathsf{c}_1\mathsf{c}_1)\mathsf{e}_x(\mathsf{c}_1\mathsf{c}_1) \\
&= (\mathsf{c}_1\mathsf{e}_x\mathsf{c}_1)(\mathsf{c}_1\mathsf{r}_1\mathsf{c}_1)(\mathsf{c}_1\mathsf{e}_x\mathsf{c}_1)\mathsf{c}_1 \\
&= \mathsf{r}_x\mathsf{e}_1\mathsf{r}_x\mathsf{c}_1 \\
&= \mathsf{c}_{x^{-1}}\mathsf{c}_1 = \mathrm{R}_{x^{-1}}\,.
\end{aligned}$$

(b) The group K acts transitively by conjugation on $\mathsf{r}_1^K \subseteq \{\, \mathsf{r}_x \mid x \in Q \,\}$ with stabilizer $H = \mathrm{C}_K(\mathsf{r}_1) = \mathrm{C}_K(\eta)$. Because $(\mathsf{c}_x\mathsf{c}_1)^\pi = 1$, each R_x of R belongs to K with $\mathsf{r}_1^{\mathrm{R}_x} = \mathsf{r}_1^{\mathsf{c}_x\mathsf{c}_1} = \mathsf{e}_x^{\mathsf{c}_1} = \mathsf{r}_x$. Therefore $\mathsf{r}_1^K = \{\, \mathsf{r}_x \mid x \in Q \,\}$ and $R = \{\, \mathrm{R}_x \mid x \in Q \,\}$ is a set of right coset representatives for H. Furthermore

$$\mathsf{c}_1^K = (\mathsf{r}_1^{\mathsf{e}_1})^K = (\mathsf{r}_1^K)^{\mathsf{e}_1} = \{\, \mathsf{r}_x^{\mathsf{e}_1} \mid x \in Q \,\} = \{\, \mathsf{c}_z \mid z \in Q \,\}\,,$$

and so $R = \{\, [k, \mathsf{c}_1] \mid k \in K \,\} = \{\, [k, \sigma] \mid k \in K \,\}$. Finally R is closed under inverses (by (a)), so it is also a set of left coset representatives.

(c) We must prove that $\mathrm{R}_x\mathrm{R}_y\mathrm{R}_{xy}^{-1} \in H = \mathrm{C}_K(\eta)$. That is, we must show that $(\mathsf{c}_x\mathsf{c}_1)(\mathsf{c}_y\mathsf{c}_1)(\mathsf{c}_{xy}\mathsf{c}_1)^{-1} = \mathsf{c}_x\mathsf{c}_1\mathsf{c}_y\mathsf{c}_{xy}$ centralizes r_1. Indeed

$$\mathsf{r}_1^{\mathsf{c}_x\mathsf{c}_1\mathsf{c}_y\mathsf{c}_{xy}} = \mathsf{e}_x^{\mathsf{c}_1\mathsf{c}_y\mathsf{c}_{xy}} = \mathsf{r}_x^{\mathsf{c}_y\mathsf{c}_{xy}} = \mathsf{e}_{xy}^{\mathsf{c}_{xy}} = \mathsf{r}_1\,.$$

(d) We have

$$\begin{aligned}
\mathrm{R}_y^{-\mu^2}\mathrm{R}_x\mathrm{R}_y^{-\mu} &= ((\mathsf{c}_y\mathsf{c}_1)^{-1})^{\mathsf{c}_1\mathsf{r}_1}(\mathsf{c}_x\mathsf{c}_1)((\mathsf{c}_y\mathsf{c}_1)^{-1})^{\mathsf{r}_1\mathsf{c}_1} \\
&= (\mathsf{r}_1\mathsf{c}_1)(\mathsf{c}_1\mathsf{c}_y)(\mathsf{c}_1\mathsf{r}_1)(\mathsf{c}_x\mathsf{c}_1)(\mathsf{c}_1\mathsf{r}_1)(\mathsf{c}_1\mathsf{c}_y)(\mathsf{r}_1\mathsf{c}_1) \\
&= \mathsf{r}_1(\mathsf{c}_1\mathsf{c}_1)\mathsf{c}_y\mathsf{c}_1\mathsf{r}_1\mathsf{c}_x(\mathsf{c}_1\mathsf{c}_1)\mathsf{r}_1\mathsf{c}_1\mathsf{c}_y\mathsf{r}_1\mathsf{c}_1 \\
&= \mathsf{r}_1\mathsf{c}_y\mathsf{c}_1(\mathsf{r}_1\mathsf{c}_x\mathsf{r}_1)\mathsf{c}_1\mathsf{c}_y\mathsf{r}_1\mathsf{c}_1 \\
&= \mathsf{r}_1\mathsf{c}_y(\mathsf{c}_1\mathsf{e}_x\mathsf{c}_1)\mathsf{c}_y\mathsf{r}_1\mathsf{c}_1 \\
&= \mathsf{r}_1(\mathsf{c}_y\mathsf{r}_x\mathsf{c}_y)\mathsf{r}_1\mathsf{c}_1 \\
&= (\mathsf{r}_1\mathsf{e}_{xy}\mathsf{r}_1)\mathsf{c}_1 \\
&= \mathsf{c}_{xy}\mathsf{c}_1 = \mathrm{R}_{xy}\,.
\end{aligned}$$

This gives the first equality. The second can be proved in a similar way, but it also follows from the first if we use $\mathrm{R}_{ab}^{-1} = \mathrm{R}_{(ab)^{-1}} = \mathrm{R}_{b^{-1}a^{-1}}$ from (a). □

We also have new versions of the universal functors $\mathbf{U}^\star$ and $\mathbf{U}$.

(11.6). Theorem.

(a) *For every group with triality (G, D, π, I) the groups*

$$(G, D, \pi, I)\mathbf{M}^\star\mathbf{G}^\star \text{ and } (G, D, \pi, I)\mathbf{U}^\star$$

are isomorphic in $\mathsf{TriGrp}^\star$ *and* $\mathsf{UTriGrp}^\star$*. In particular, every universal group with triality (G, D, π, I) is isomorphic to $Q\mathbf{G}^\star$ for the Moufang loop $Q = (G, D, \pi, I)\mathbf{M}^\star$. Furthermore for every Moufang loop Q, we have $Q\mathbf{G}^\star\mathbf{M}^\star$ isomorphic to Q.*

(b) *For every group with triality* (G, D, π) *the groups*

$$(G, D, \pi)\mathbf{MG} \textit{ and } (G, D, \pi)\mathbf{U}$$

are isomorphic in TriGrp *and* $\mathsf{UTriGrp}$. *In particular, every universal group with triality* (G, D, π) *is isomorphic to* $Q\mathbf{G}$ *for the Moufang loop* $Q = (G, D, \pi)\mathbf{M}$. *Furthermore for every Moufang loop* Q, *we have* $Q\mathbf{GM}$ *isomorphic to* Q.

Proof. On (G, D, π, I) the functor $\mathbf{M}^\star\mathbf{G}^\star$ is realized by

$$r_x \overset{\iota}{\mapsto} \mathsf{r}_x \quad c_x \overset{\iota}{\mapsto} \mathsf{c}_x \quad e_x \overset{\iota}{\mapsto} \mathsf{e}_x$$

taking (G, D, π, I) to the universal group with triality $Q\mathbf{G}^\star$ for the Moufang loop $Q = (G, D, \pi, I)\mathbf{M}^\star$. The inverse map

$$\mathsf{r}_x \overset{\iota^{-1}}{\mapsto} r_x \quad \mathsf{c}_x \overset{\iota^{-1}}{\mapsto} c_x \quad \mathsf{e}_x \overset{\iota^{-1}}{\mapsto} e_x\,.$$

is a bijection on D and respects the relations of $Q\mathbf{G}^\star$, so it is a cover by Lemma (6.3). If (G, D, π, I) itself is universal, this is an isomorphism.

In the transition from the Moufang loop Q to $Q\mathbf{G}^\star$, each element x of Q gives rise to the three generators r_x, c_x, and e_x of $Q\mathbf{G}^\star = (G, D, \pi, I_{Q\mathbf{G}^\star})$, while each pair $x, y \in Q$ leads to the line $\langle \mathsf{r}_x, \mathsf{c}_y, \mathsf{e}_{xy}\rangle$. In particular we have the special line $I_{Q\mathbf{G}^\star} = \langle \mathsf{r}_1, \mathsf{c}_1, \mathsf{e}_1\rangle$. To construct $Q\mathbf{G}^\star\mathbf{M}^\star = (Q\mathbf{G}^\star)\mathbf{M}^\star$ we first (see Section 10.2) set

$$r_1 = \mathsf{r}_1 \qquad c_1 = \mathsf{c}_1 \qquad e_1 = \mathsf{e}_1\,,$$

and then let $\{\, \mathsf{e}_x \mid x \in Q \,\} = (1, 2)^{\pi^{-1}} = \{\, e_z \mid z \in M \,\}$ for some set M in bijection with Q via, say, $z \mapsto \bar{z} \in Q$, taking care that $1 \in M$ with $\bar{1} = 1$. Next for each $z \in M$ we must set

$$r_z = \langle c_1, e_z\rangle \cap (2, 3)^{\pi^{-1}} = \mathsf{r}_{\bar{z}} \quad \text{and} \quad c_z = \langle r_1, e_z\rangle \cap (1, 3)^{\pi^{-1}} = \mathsf{c}_{\bar{z}}\,.$$

The set M then receives the loop structure $(M, \circ)$ given by

$$\mathsf{e}_{\overline{u\circ v}} = e_{u\circ v} = \langle r_u, c_v\rangle \cap (1, 2)^{\pi^{-1}} = \langle \mathsf{r}_{\bar{u}}, \mathsf{c}_{\bar{v}}\rangle \cap \{\, \mathsf{e}_{\bar{z}} \mid z \in M \,\} = \mathsf{e}_{\bar{u}\bar{v}}\,.$$

As Q is a Moufang loop, different $x \in Q$ give different e_x. Therefore for all $u, v \in M$ we have $\overline{u \circ v} = \bar{u}\bar{v}$; that is, the bijection of M and Q given by $z \mapsto \bar{z}$ is an isomorphism of the loops Q and $(M, \circ) = Q\mathbf{G}^\star\mathbf{M}^\star$.

The second part of the theorem follows immediately from the first. □

11.3. Another presentation

A presentation related to that of (11.1) and Theorem (11.3) appears in [**Hal06**, (2.5)], parameterized there by an integer n and a group Q. If we specialize that presentation to $n = 3$ and allow Q to be a loop, we get:

(11.7). Presentation. *For a loop* Q, *the group* $\mathrm{G}(Q)$ *has the following presentation:*

Generators:

for arbitrary $x \in Q$ *and distinct* $a, b \in \{1, 2, 3\}$*:*

$\langle\!\langle x\,;\, a\,, b\rangle\!\rangle$.

Relations:

for arbitrary $x, y \in Q$ *and distinct* $a, b, c \in \{1, 2, 3\}$*:*

(1) $\langle\!\langle x\,;\, a\,, b\rangle\!\rangle^2 = 1$*;*

(2) $\langle\!\langle x\,;\, a\,, b\rangle\!\rangle = \langle\!\langle x^{-1}\,;\, b\,, a\rangle\!\rangle$*;*

(3) $\langle\!\langle x\,;\, a\,, b\rangle\!\rangle^{\langle\!\langle y\,;\, b\,, c\rangle\!\rangle} = \langle\!\langle xy\,;\, a\,, c\rangle\!\rangle$.

Theorem 4.1 of [**Hal06**] states that, for Q a Moufang loop, the above group $\mathrm{G}(Q)$ is a universal group with triality. The proof was not given, other similar results in the literature instead being cited. Here we give a proof in a precise form of a more general result.

Recall that a loop has the antiautomorphic inverse property when it satisfies the identical relation $(xy)^{-1} = y^{-1}x^{-1}$. By Proposition (2.12) Moufang loops are inverse property loops and satisfy the antiautomorphic inverse property.

(11.8). THEOREM. *Let Q be a loop with the antiautomorphic inverse property. Then the groups $\mathrm{G}(Q)$ and G_Q are isomorphic universal groups with triality under the maps*

$$\{\langle\!\langle x\,;\,2\,,3\rangle\!\rangle, \langle\!\langle x^{-1}\,;\,3\,,2\rangle\!\rangle\} \xrightarrow{\iota_1} \mathsf{r}_x \xrightarrow{\iota_2} \langle\!\langle x\,;\,2\,,3\rangle\!\rangle\,,$$
$$\{\langle\!\langle x\,;\,3\,,1\rangle\!\rangle, \langle\!\langle x^{-1}\,;\,1\,,3\rangle\!\rangle\} \xrightarrow{\iota_1} \mathsf{c}_x \xrightarrow{\iota_2} \langle\!\langle x\,;\,3\,,1\rangle\!\rangle\,,$$
$$\{\langle\!\langle x\,;\,2\,,1\rangle\!\rangle, \langle\!\langle x^{-1}\,;\,1\,,2\rangle\!\rangle\} \xrightarrow{\iota_1} \mathsf{e}_x \xrightarrow{\iota_2} \langle\!\langle x\,;\,2\,,1\rangle\!\rangle\,.$$

(11.9). PROPOSITION. *Let Q be a loop. The group G_Q is a homomorphic image of $\mathrm{G}(Q)$ under the map*

$$\{\langle\!\langle x\,;\,2\,,3\rangle\!\rangle, \langle\!\langle x^{-1}\,;\,3\,,2\rangle\!\rangle\} \xrightarrow{\iota_1} \mathsf{r}_x$$
$$\{\langle\!\langle x\,;\,3\,,1\rangle\!\rangle, \langle\!\langle x^{-1}\,;\,1\,,3\rangle\!\rangle\} \xrightarrow{\iota_1} \mathsf{c}_x$$
$$\{\langle\!\langle x\,;\,2\,,1\rangle\!\rangle, \langle\!\langle x^{-1}\,;\,1\,,2\rangle\!\rangle\} \xrightarrow{\iota_1} \mathsf{e}_x$$

PROOF. The generators of $\mathrm{G}(Q)$ are mapped to those of G_Q, so we need only check that the relations (11.7) are respected by the map ι_1. This is clearly the case for (11.7)(1-2).

Consider the six relations $\langle\!\langle x\,;\,a\,,b\rangle\!\rangle^{\langle\!\langle y\,;\,b\,,c\rangle\!\rangle} = \langle\!\langle xy\,;\,a\,,c\rangle\!\rangle$ of (11.7)(3). The relation $\langle\!\langle x\,;\,2\,,3\rangle\!\rangle^{\langle\!\langle y\,;\,3\,,1\rangle\!\rangle} = \langle\!\langle xy\,;\,2\,,1\rangle\!\rangle$ is mapped to $\mathsf{r}_x^{\mathsf{c}_y} = \mathsf{e}_{xy}$, valid in G_Q by (11.1)(2). Also

$$\langle\!\langle 1\,;\,3\,,1\rangle\!\rangle^{\langle\!\langle 1\,;\,2\,,3\rangle\!\rangle} = \langle\!\langle 1\,;\,1\,,3\rangle\!\rangle^{\langle\!\langle 1\,;\,3\,,2\rangle\!\rangle} = \langle\!\langle 1\,;\,1\,,2\rangle\!\rangle = \langle\!\langle 1\,;\,2\,,1\rangle\!\rangle$$

is mapped to $\mathsf{c}_1^{\mathsf{r}_1} = \mathsf{e}_1$. Therefore the subgroup $S = \langle \langle\!\langle 1\,;\,2\,,3\rangle\!\rangle, \langle\!\langle 1\,;\,3\,,1\rangle\!\rangle \rangle$ of $\mathrm{G}(Q)$ is isomorphic to $\mathrm{Sym}(3)$ and is mapped isomorphically to the subgroup $S^{\iota_2} = \langle \mathsf{r}_1, \mathsf{c}_1\rangle$ of G_Q.

For fixed x and y, the subgroup S acts regularly on the set of six relations $\langle\!\langle x\,;\,a\,,b\rangle\!\rangle^{\langle\!\langle y\,;\,b\,,c\rangle\!\rangle} = \langle\!\langle xy\,;\,a\,,c\rangle\!\rangle$. After verifying that

$$\mathsf{r}_x^{\mathsf{r}_1} = \mathsf{r}_{x^{-1}} \quad \mathsf{c}_x^{\mathsf{c}_1} = \mathsf{c}_{x^{-1}} \quad \mathsf{e}_x^{\mathsf{e}_1} = \mathsf{e}_{x^{-1}}\,,$$

we can use the action of S^{ι_2} to check that the images of these six relations under ι_1 remain valid. □

PROOF OF THEOREM (11.8).

In view of (11.7)(2) the maps ι_i are inverse bijections of generating sets for the appropriate free groups. As we already have Proposition (11.9), we now need only check that ι_2 gives a homomorphism from G_Q to $\mathrm{G}(Q)$. This we do by checking that the relations (11.1) are respected by the map ι_2. This is clearly the case for (11.1)(1), but we must check the two parts of (11.1)(2).

We have

$$(\mathsf{c}_y\mathsf{r}_x\mathsf{c}_y)^{\iota_2} = \langle\!\langle y\,;\,3\,,1\rangle\!\rangle\langle\!\langle x\,;\,2\,,3\rangle\!\rangle\langle\!\langle y\,;\,3\,,1\rangle\!\rangle = \langle\!\langle xy\,;\,2\,,1\rangle\!\rangle = \mathsf{e}_{xy}^{\iota_2}\,.$$

Therefore the relation $\mathsf{c}_y\mathsf{r}_x\mathsf{c}_y = \mathsf{e}_{xy}$ remains true under ι_2.

Similarly

$$\begin{aligned}(\mathsf{r}_x\mathsf{c}_y\mathsf{r}_x)^{\iota_2} &= \langle\!\langle x\,;\,2\,,3\rangle\!\rangle\langle\!\langle y\,;\,3\,,1\rangle\!\rangle\langle\!\langle x\,;\,2\,,3\rangle\!\rangle\\ &= \langle\!\langle x^{-1}\,;\,3\,,2\rangle\!\rangle\langle\!\langle y^{-1}\,;\,1\,,3\rangle\!\rangle\langle\!\langle x^{-1}\,;\,3\,,2\rangle\!\rangle\\ &= \langle\!\langle y^{-1}x^{-1}\,;\,1\,,2\rangle\!\rangle = \langle\!\langle (y^{-1}x^{-1})^{-1}\,;\,2\,,1\rangle\!\rangle\\ &= \langle\!\langle xy\,;\,2\,,1\rangle\!\rangle = \mathsf{e}_{xy}^{\iota_2}\,,\end{aligned}$$

as desired. In passing to the last line, we have used the assumption that Q satisfies the antiautomorphic inverse property. □

It is unclear whether or not Theorem (11.8) is valid for all loops Q, but the antiautomorphic inverse identity appears prominently in the present proof that $\mathrm{G}(Q)$ is a group with triality. As the following proposition shows, the crucial cases would be right inverse property loops that are not antiautomorphic, that is, are not inverse property loops. Gabor Nagy [**Nag11**] has done calculations showing that for right Bol loops of order 8 and 16 the conclusion of Theorem (11.8) remains valid.

The following proposition should be compared with Theorem (13.25) below.

(11.10). PROPOSITION. *Let Q be a loop, and consider the group* $\mathrm{G}(Q)$*, as presented in (11.7). For $x, y \in Q$ and arbitrary $a, b, c, d \in$ with $a \neq b$, $c \neq d$, we have*

$$\langle\!\langle x\,;\,a\,,b\rangle\!\rangle = \langle\!\langle y\,;\,a\,,b\rangle\!\rangle \iff \langle\!\langle x\,;\,c\,,d\rangle\!\rangle = \langle\!\langle y\,;\,c\,,d\rangle\!\rangle\,.$$

In this case we write $x \sim y$. The equivalence relation $\sim$ is a congruence on the loop Q, and $Q/\!\sim$ is an right inverse property loop.

PROOF. Again, the action of $S = \langle\langle\!\langle 1\,;\,2\,,3\rangle\!\rangle, \langle\!\langle 1\,;\,3\,,1\rangle\!\rangle\rangle \simeq \mathrm{Sym}(3)$ shows that if $\langle\!\langle x\,;\,a\,,b\rangle\!\rangle = \langle\!\langle y\,;\,a\,,b\rangle\!\rangle$ holds for one pair $a \neq b$ then it holds for all such pairs, giving the equivalence relation. For $\langle\!\langle x_1\,;\,a\,,b\rangle\!\rangle = \langle\!\langle x_2\,;\,a\,,b\rangle\!\rangle$ and $\langle\!\langle y_1\,;\,b\,,c\rangle\!\rangle = \langle\!\langle y_2\,;\,b\,,c\rangle\!\rangle$, we find

$$\langle\!\langle x_1y_1\,;\,a\,,c\rangle\!\rangle = \langle\!\langle x_1\,;\,a\,,b\rangle\!\rangle^{\langle\!\langle y_1\,;\,b\,,c\rangle\!\rangle} = \langle\!\langle x_2\,;\,a\,,b\rangle\!\rangle^{\langle\!\langle y_2\,;\,b\,,c\rangle\!\rangle} = \langle\!\langle x_2y_2\,;\,a\,,c\rangle\!\rangle\,.$$

Therefore the equivalence relation is a congruence.

Two applications of (11.7)(3) yield

$$\langle\!\langle x\,;\,a\,,b\rangle\!\rangle = \langle\!\langle x^{-1}\,;\,b\,,a\rangle\!\rangle = \langle\!\langle (x^{-1})^{-1}\,;\,a\,,b\rangle\!\rangle\,,$$

so inverses are two-sided in the quotient $Q/\sim$.

Next as $\langle\!\langle x\,;\,a\,,b\rangle\!\rangle^{\langle\!\langle y\,;\,b\,,c\rangle\!\rangle} = \langle\!\langle xy\,;\,a\,,c\rangle\!\rangle$ with $\langle\!\langle y\,;\,b\,,c\rangle\!\rangle$ of order 2,

$$\langle\!\langle x\,;\,a\,,b\rangle\!\rangle = \langle\!\langle xy\,;\,a\,,c\rangle\!\rangle^{\langle\!\langle y\,;\,b\,,c\rangle\!\rangle} = \langle\!\langle xy\,;\,a\,,c\rangle\!\rangle^{\langle\!\langle y^{-1}\,;\,c\,,b\rangle\!\rangle} = \langle\!\langle (xy)y^{-1}\,;\,a\,,b\rangle\!\rangle\,.$$

Hence $x \sim (xy)y^{-1}$, and $Q/\sim$ has the right inverse property. □

Chapter 12

Multiplication Groups and Autotopisms

The material in this chapter certainly qualifies as "basic" and could have been presented right after Chapter 4.

12.1. Multiplication and inner mapping groups

For $x \in Q$, a quasigroup, we define the *left multiplication* map $\mathrm{L}(x)$, given by

$$a^{\mathrm{L}(x)} = xa\,,$$

and similarly the *right multiplication* map $\mathrm{R}(x)$, given by

$$a^{\mathrm{R}(x)} = ax\,.$$

Within $\mathrm{Sym}(Q)$ (the symmetric group on the set Q), we then define the *right multiplication group*

$$\mathrm{Mlt}_{\mathrm{R}}(Q) = \langle\, \mathrm{R}(x) \mid x \in Q\,\rangle\,,$$

the *left multiplication group*

$$\mathrm{Mlt}_{\mathrm{L}}(Q) = \langle\, \mathrm{L}(x) \mid x \in Q\,\rangle\,,$$

and the *multiplication group*

$$\mathrm{Mlt}(Q) = \langle\, \mathrm{R}(x), \mathrm{L}(x) \mid x \in Q\,\rangle = \langle\, \mathrm{Mlt}_{\mathrm{R}}(Q), \mathrm{Mlt}_{\mathrm{L}}(Q)\rangle.$$

Many properties of a loop can be easily described in terms of its translation maps and multiplication groups.

(12.1). Proposition. *Let Q be a loop.*

(a) $\mathrm{Mlt}_{\mathrm{R}}(Q)$*,* $\mathrm{Mlt}_{\mathrm{L}}(Q)$*, and* $\mathrm{Mlt}(Q)$ *are transitive subgroups of* $\mathrm{Sym}(Q)$*.*
(b) *Q is a group if and only if* $\mathrm{Mlt}_{\mathrm{R}}(Q)$ *is semiregular.*
(c) *Q is an abelian group if and only if* $\mathrm{Mlt}(Q)$ *is abelian.*

Proof.

(a) $1^{\mathrm{R}(x)} = x = 1^{\mathrm{L}(x)}$.
(b) If Q is a group, then $\mathrm{Mlt}_{\mathrm{R}}(Q)$ is the right regular representation of Q. Conversely always $1^{\mathrm{R}(xy)} = xy = (1^{\mathrm{R}(x)})^{\mathrm{R}(y)}$, therefore semiregularity forces $\mathrm{R}(xy) = \mathrm{R}(x)\mathrm{R}(y)$. That is, for all $z \in Q$, we have $z(xy) = (zx)y$. Hence Q is associative and a group.

(c) If Q is an abelian group, then $\mathrm{Mlt}(Q) = \mathrm{Mlt}_{\mathrm{R}}(Q) = \mathrm{Mlt}_{\mathrm{L}}(Q)$ is the regular representation of Q. Conversely, if $\mathrm{Mlt}(Q)$ is abelian then transitivity forces it to be regular. Therefore Q is a group by (a) and is isomorphic to $\mathrm{Mlt}_{\mathrm{R}}(Q)$, a subgroup of the abelian group $\mathrm{Mlt}(Q)$. □

Identities in the loop Q often correspond to identities in $\mathrm{Mlt}(Q)$.

(12.2). Proposition. *Let Q be a loop.*

(a) *Q is a left inverse property loop* $\iff$ $\mathrm{L}(x)^{-1} = \mathrm{L}(x^{-1})$ *for all* $x \in Q$.
(b) *Q is a right inverse property loop* $\iff$ $\mathrm{R}(x)^{-1} = \mathrm{R}({}^{-1}x)$ *for all* $x \in Q$.
(c) *Q has the flexible property* $\iff$ $\mathrm{L}(x)\,\mathrm{R}(x) = \mathrm{R}(x)\,\mathrm{L}(x)$ *for all* $x \in Q$. □

As $x = 1^{\mathrm{L}(x)} = 1^{\mathrm{R}(x)}$ for every loop

$$\mathrm{L}(x) = \mathrm{L}(y) \iff x = y \iff \mathrm{R}(x) = \mathrm{R}(y)\,.$$

We get a quick proof of the already observed

(12.3). Corollary. *If the loop Q has the left or right inverse property, then inverses are two-sided.*

Proof. With the left inverse property

$$\mathrm{L}(x) = (\mathrm{L}(x)^{-1})^{-1} = \mathrm{L}(x^{-1})^{-1} = \mathrm{L}((x^{-1})^{-1})\,,$$

hence $x = (x^{-1})^{-1}$. □

Certain more complicated identities in $\mathrm{Mlt}(Q)$ will be important in the next chapter.

(12.4). Proposition. *Let Q be a Moufang loop. For all $x \in Q$ define $\mathrm{P}(x) = \mathrm{R}(x)^{-1}\,\mathrm{L}(x)^{-1}$. Then for all $x, y \in Q$ we have:*

(a) $\mathrm{P}(x)\,\mathrm{R}(xy)\,\mathrm{L}(x) = \mathrm{R}(y)$, $\mathrm{R}(x)\,\mathrm{L}(xy)\,\mathrm{P}(x) = \mathrm{L}(y)$, $\mathrm{L}(x)\,\mathrm{P}(xy)\,\mathrm{R}(x) = \mathrm{P}(y)$.
(b) $\mathrm{P}(x)\,\mathrm{L}(yx)\,\mathrm{R}(x) = \mathrm{L}(y)$, $\mathrm{L}(x)\,\mathrm{R}(yx)\,\mathrm{P}(x) = \mathrm{R}(y)$, $\mathrm{R}(x)\,\mathrm{P}(yx)\,\mathrm{L}(x) = \mathrm{P}(y)$.

Proof. By Proposition (12.2) we have

$$\mathrm{P}(x) = \mathrm{R}(x)^{-1}\,\mathrm{L}(x)^{-1} = \mathrm{L}(x)^{-1}\,\mathrm{R}(x)^{-1} = \mathrm{R}(x^{-1})\,\mathrm{L}(x^{-1}) = \mathrm{L}(x^{-1})\,\mathrm{R}(x^{-1})$$

and

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

The Moufang identity $(xy)(zx) = (x(yz))x$ becomes

$$z^{\mathrm{R}(x)\,\mathrm{L}(xy)} = z^{\mathrm{L}(y)\,\mathrm{P}(x)^{-1}} \quad \text{and} \quad y^{\mathrm{L}(x)\,\mathrm{R}(zx)} = y^{\mathrm{R}(z)\,\mathrm{P}(x)^{-1}}\,,$$

hence $\mathrm{R}(x)\,\mathrm{L}(xy)\,\mathrm{P}(x) = \mathrm{L}(y)$ as in (a) and $\mathrm{L}(x)\,\mathrm{R}(zx)\,\mathrm{P}(x) = \mathrm{R}(z)$ as in (b).

Inverting the first of these leads to

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

giving $\mathrm{P}(x)\,\mathrm{L}(yx)\,\mathrm{R}(x) = \mathrm{L}(y)$ as in (b).

In this we set $x = uv$ and $y = u^{-1}$ to find

$$\begin{aligned}\mathrm{L}(u)^{-1} &= \mathrm{L}(u^{-1})\\ &= \mathrm{P}(uv)\,\mathrm{L}(u^{-1}(uv))\,\mathrm{R}(uv)\\ &= \mathrm{P}(uv)(\mathrm{L}(v)\,\mathrm{R}(uv))\\ &= \mathrm{P}(uv)(\mathrm{R}(u)\,\mathrm{P}(v)^{-1})\,,\end{aligned}$$

so $\mathrm{P}(v) = \mathrm{L}(u)\,\mathrm{P}(uv)\,\mathrm{R}(u)$ as in (a).

The final two identities come from inverting two of those already verified. Alternatively, the identities of (b) are exactly those of (a) when interpreted in the Moufang loop opposite to Q. □

The *inner mapping group* $\mathrm{Inn}(Q)$ is the stabilizer of the identity 1_Q in the multiplication group $\mathrm{Mlt}(Q)$ of the loop Q.

(12.5). PROPOSITION. *Let Q be a loop.*

(a) $\mathrm{Inn}(Q) = \langle\, \mathrm{R}(x)\,\mathrm{R}(y)\,\mathrm{R}(xy)^{-1}, \mathrm{R}(x)\,\mathrm{L}(y)\,\mathrm{R}(yx)^{-1} \mid x, y \in Q\,\rangle\,.$

(b) $\mathrm{Inn}(Q) = \langle\, \mathrm{L}(y)\,\mathrm{R}(y)^{-1}, \mathrm{R}(x)\,\mathrm{R}(y)\,\mathrm{R}(xy)^{-1}, \mathrm{L}(x)\,\mathrm{L}(y)\,\mathrm{L}(yx)^{-1} \mid x, y \in Q\,\rangle\,.$

PROOF. This is an easy consequence of the Reidermeister rewriting process [**Bog08**, p. 69], discussed also in Section 13.2 on page 95 below.

(a) The group $\mathrm{Mlt}(Q)$ has the generating set $X = \{\, \mathrm{L}(x), \mathrm{R}(x) \mid x \in Q\,\}$. Its subgroup $I = \mathrm{Inn}(Q)$ has, as a right transversal, the coset representative set $T = \{\, \mathrm{R}(x) \mid x \in Q\,\}$.

Let $w = \prod_{i=1}^{n} g_i(x_i) \in \mathrm{Inn}(Q)$, so that $1^w = 1$ with each $g_i \in \{\mathrm{R}, \mathrm{L}, \mathrm{R}^{-1}, \mathrm{L}^{-1}\}$. We wish to rewrite w as a product of elements or inverses of elements from the set

$$H = \{\, \mathrm{R}(x)\,\mathrm{R}(y)\,\mathrm{R}(xy)^{-1}, \mathrm{R}(x)\,\mathrm{L}(y)\,\mathrm{R}(yx)^{-1} \mid x, y \in Q\,\}$$

by scanning w from left to right, inserting words $\mathrm{R}(z)^{-1}\,\mathrm{R}(z)$ as appropriate. To do this, we must identify coset representatives from T for each product tu^{ϵ} with $t \in T$, $u \in X$, and $\epsilon = \pm 1$.

Specifically,

$$(1x)y = xy\,, \text{ hence } \mathrm{R}(x)\,\mathrm{R}(y) \in I\,\mathrm{R}(xy) \text{ and } \mathrm{R}(x)\,\mathrm{R}(y)\,\mathrm{R}(xy)^{-1} \in I\,,$$

and

$$y(1x) = yx\,, \text{ hence } \mathrm{R}(x)\,\mathrm{L}(y) \in I\,\mathrm{R}(yx) \text{ and } \mathrm{R}(x)\,\mathrm{L}(y)\,\mathrm{R}(yx)^{-1} \in I\,.$$

Next, letting the equation $x = by$ determine b from the pair x, y,

$$1^{\mathrm{R}(x)\,\mathrm{R}(y)^{-1}} = 1^{\mathrm{R}(by)\,\mathrm{R}(y)^{-1}} = (by)^{\mathrm{R}(y)^{-1}} = b = 1^{\mathrm{R}(b)}\,,$$

indicating that

$$\mathrm{R}(x)\,\mathrm{R}(y)^{-1}\,\mathrm{R}(b)^{-1} = \mathrm{R}(by)\,\mathrm{R}(y)^{-1}\,\mathrm{R}(b)^{-1} \in I\,,$$

something we already knew since

$$\mathrm{R}(by)\,\mathrm{R}(y)^{-1}\,\mathrm{R}(b)^{-1} = (\mathrm{R}(b)\,\mathrm{R}(y)\,\mathrm{R}(by)^{-1})^{-1}\,.$$

Again if $x = ya$ defines a, then

$$1^{\mathrm{R}(x)\,\mathrm{L}(y)^{-1}} = 1^{\mathrm{R}(ya)\,\mathrm{L}(y)^{-1}} = (ya)^{\mathrm{L}(y)^{-1}} = a = 1^{\mathrm{R}(a)}\,,$$

corresponding to

$$\mathrm{R}(x)\,\mathrm{L}(y)^{-1}\,\mathrm{R}(a)^{-1} = \mathrm{R}(ya)\,\mathrm{L}(y)^{-1}\,\mathrm{R}(a)^{-1} = (\mathrm{R}(a)\,\mathrm{L}(y)\,\mathrm{R}(ya)^{-1})^{-1} \in I\,.$$

Now for $\mathrm{X} \in \{\mathrm{R}, \mathrm{L}\}$ and $\epsilon = \pm 1$, let $w = \mathrm{R}(x)\,\mathrm{X}(y)^\epsilon \prod_{i=3}^n g_i(x_i)$, where if needed we set $g_1(x_1) = \mathrm{R}(1)$. Then we can rewrite the initial segment of w:

$$\mathrm{R}(x)\,\mathrm{X}(y)^\epsilon = \mathrm{R}(x)\,\mathrm{X}(y)^\epsilon(\mathrm{R}(z)^{-1}\,\mathrm{R}(z)) = (\mathrm{R}(x)\,\mathrm{X}(y)^\epsilon\,\mathrm{R}(z)^{-1})\,\mathrm{R}(z)\,.$$

Here $\mathrm{R}(x)\,\mathrm{X}(y)^\epsilon\,\mathrm{R}(z)^{-1} = h^\epsilon = h_1$ for $h \in H \subset \mathrm{Inn}(Q)$ with the appropriate z equal to one of xy, yx, b, or a. Then $w = h_1\,\mathrm{R}(z) \prod_{i=3}^n g_i(x_i)$, and we can proceed with rewriting $w_1 = \mathrm{R}(z) \prod_{i=3}^n g_i(x_i)$, a shorter word in the generators than the original w.

Continuing in this fashion, we ultimately arrive at $w = (\prod_{i=1}^{n-1} h_i)\,\mathrm{R}(z)$ where each h_i or its inverse is one of the elements of H. We then have

$$1 = 1^w = 1^{(\prod_{i=1}^{n-1} h_i)\,\mathrm{R}(z)} = 1^{\mathrm{R}(z)} = z\,,$$

so in fact $w = \prod_{i=1}^{n-1} h_i$. Therefore $\langle H \rangle = \mathrm{Inn}(Q)$, as claimed in (a).

(b) With $x = 1$

$$\mathrm{R}(x)\,\mathrm{L}(y)\,\mathrm{R}(yx)^{-1} = \mathrm{R}(1)\,\mathrm{L}(y)\,\mathrm{R}(y1)^{-1} = \mathrm{L}(y)\,\mathrm{R}(y)^{-1}\,.$$

Furthermore

$$(\mathrm{L}(x)\,\mathrm{R}(x)^{-1})(\mathrm{R}(x)\,\mathrm{L}(y)\,\mathrm{R}(yx)^{-1})(\mathrm{L}(yx)\,\mathrm{R}(yx)^{-1})^{-1} = \mathrm{L}(x)\,\mathrm{L}(y)\,\mathrm{L}(yx)^{-1}\,.\square$$

The generating set of Proposition (12.5)(b) is the usual, preferred set ([**Bru58**, p. 61],[**Pfl90**, I.5.2]). In it, the elements of the second and third types speak to associativity in Q; in particular, for an associative loop Q they always vanish. That is, if Q is a group then the generators of the first (and only nontrivial) type are conjugations, and $\mathrm{Inn}(Q)$ is the inner automorphism group of Q. This motivates the following result.

(12.6). PROPOSITION. *In the loop Q, the subloop N is normal if and only if it is invariant under the action of* $\mathrm{Inn}(Q)$.

PROOF. Using the definition of normality (from page 13) and the previous proposition, we recast this as:

> *For all $n_1, n_2 \in N$ and $x, y \in Q$, there is an $n_3 \in N$ with $(n_1x)(n_2y) = n_3(xy)$*
>
> $$\Updownarrow$$
>
> *for all $n \in N$ and $x, y \in Q$, we have $n^{\mathrm{R}(x)\,\mathrm{R}(y)\,\mathrm{R}(xy)^{-1}} \in N$ and $n^{\mathrm{R}(y)\,\mathrm{L}(x)\,\mathrm{R}(xy)^{-1}} \in N$.*

($\Downarrow$) Set $n_1 = n$ and $n_2 = 1$. Then

$$n^{\mathrm{R}(x)\,\mathrm{R}(y)} = (nx)y = (n_1x)(n_2y) = n_3(xy) = n_3^{\mathrm{R}(xy)}$$

and $n^{\mathrm{R}(x)\,\mathrm{R}(y)\,\mathrm{R}(xy)^{-1}} = n_3 \in N$. Similarly with $n_1 = 1$ and $n_2 = n$

$$n^{\mathrm{R}(y)\,\mathrm{L}(x)} = x(ny) = (n_1x)(n_2y) = n_3(xy) = n_3^{\mathrm{R}(xy)}$$

and $n^{\mathrm{R}(y)\,\mathrm{L}(x)\,\mathrm{R}(xy)^{-1}} = n_3 \in N$.

($\Uparrow$) We have, with all n_i in N,

$$\begin{aligned}(n_1x)(n_2y) &= n_1^{\mathrm{R}(x)\,\mathrm{R}(n_2y)} = n_4^{\mathrm{R}(x(n_2y))} = n_4(x(n_2y))\\ &= n_4(n_2^{\mathrm{R}(y)\,\mathrm{L}(x)}) = n_4(n_5^{\mathrm{R}(xy)}) = n_4(n_5(xy))\\ &= n_4^{\mathrm{R}(n_5(xy))} = n_6^{\mathrm{R}(n_5)\,\mathrm{R}(xy)} = (n_6n_5)(xy)\\ &= n_3(xy)\,.\square\end{aligned}$$

Our original definition of subloop normality was qualitative: a subloop is normal when it is the kernel of some homomorphism. This proposition now gives us a quantitative definition: a subloop is normal when it is invariant under the inner mapping group.

12.2. Autotopisms

Recall from Section 2.2 that an autotopism of the quasigroup Q is a Qgp-automorphism; that is, a triple (α, β, γ) of permutations of Q with $x^\alpha y^\beta = (xy)^\gamma$ for all $x, y \in Q$. They form the group $\mathrm{Aut}_{\mathsf{Qgp}}(Q) = \mathrm{Atp}(Q)$—the autotopism group of Q. As noted in Section 3.2, the category equivalence of Theorem (3.4) implies that $\mathrm{Atp}(Q)$ is isomorphic to $\mathrm{Aut}_{\mathsf{LSD}}(Q\mathbf{T})$, the automorphism group of $Q\mathbf{T}$ in LSD, a normal subgroup of index at most six in $\mathrm{Aut}(Q\mathbf{T})$, the full automorphism group of $Q\mathbf{T}$.

(12.7). Proposition. *The loop Q is a Moufang loop if and only if the triple*

$$(\mathrm{L}(x), \mathrm{R}(x), \mathrm{L}(x)\,\mathrm{R}(x))$$

is an autotopism of Q for every $x \in Q$.

Proof. We have

$$(xa)(bx) = (a^{\mathrm{L}(x)})(b^{\mathrm{R}(x)})$$

and

$$(x(ab))x = (ab)^{\mathrm{L}(x)\,\mathrm{R}(x)}\,.$$

□

In a sense, this result was at the heart of our proof of Lemma (3.13). Indeed, let Q be an inverse property loop for which ϵ_x is an automorphism of $Q\mathbf{T}$. The equation $a \cdot b = ab$ in Q becomes the line (a, b, ab) of $Q\mathbf{T}$. The image of this line under ϵ_1 is $(b^{-1}, a^{-1}, (ab)^{-1})$; and, as in the proof of that lemma, the image of this line under ϵ_x is $(xa, bx, ((ab)^{-1})^{\epsilon_x}) = (xa, bx, (x(ab))x)$. That is,

$$(a, b, ab)^{\epsilon_1\epsilon_x} = (xa, bx, (x(ab))x)\ ,$$

which gives the first part of Proposition (12.8) below. The other parts of that proposition can be proven is a similar fashion and also are interpretations of the first part in conjugates of Q, inverse property loops by Lemma (3.12). (See Section 15.2 for discussion of conjugates. Compare the proposition with [**Hal07a**, Prop. 3.15].)

Note that, for all u and v from Q, the elements $\rho_u\rho_v$, $\kappa_u\kappa_v$, and $\epsilon_u\epsilon_v$ induce LSD-automorphisms of $Q\mathbf{T}$ and hence autotopisms of Q.

(12.8). Proposition. *Let Q be an inverse property loop.*

(a) *If* $\epsilon_x \in \mathrm{Aut}(Q\mathbf{T})$ *for some* x *of* Q*, then the element* $\epsilon_1\epsilon_x$ *induces on* $Q\mathbf{T}$ *the automorphism* $(\mathrm{L}(x), \mathrm{R}(x), \mathrm{L}(x)\,\mathrm{R}(x))$ *which is thus an autotopism of* Q*.*

(b) *If* $\rho_x \in \mathrm{Aut}(Q\mathbf{T})$ *for some* x *of* Q*, then the element* $\rho_1\rho_x$ *induces on* $Q\mathbf{T}$ *the automorphism* $(\mathrm{R}(x)\,\mathrm{L}(x), \mathrm{L}(x^{-1}), \mathrm{L}(x))$ *which is thus an autotopism of* Q*.*

(c) *If* $\kappa_x \in \mathrm{Aut}(Q\mathbf{T})$ *for some* x *of* Q*, then the element* $\kappa_1\kappa_x$ *induces on* $Q\mathbf{T}$ *the automorphism* $(\mathrm{R}(x^{-1}), \mathrm{L}(x)\,\mathrm{R}(x), \mathrm{R}(x))$ *which is thus an autotopism of* Q*.* □

We now have the deferred proof of two identities from Proposition (2.12).

(12.9). Corollary. *In the Moufang loop* Q *we have* $x(a(xb)) = ((xa)x)b$*, for all* $x, a, b \in Q$*, and similarly* $b(x(ax)) = ((bx)a)x$*, for all* $x, a, b \in Q$*.*

Proof. By the proposition we have the autotopism $(\mathrm{R}(x)\,\mathrm{L}(x), \mathrm{L}(x^{-1}), \mathrm{L}(x))$ of Q. When applied to $a \cdot c = ac$, this yields

$$(x(ax))(x^{-1}c) = x(ac)\,.$$

Set $b = x^{-1}c$, so that $xb = c$ by the left inverse property. Then

$$(x(ax))b = x(a(xb))\,.$$

An application of the flexible property $x(ax) = (xa)x$ now gives the first of the desired identities. The second follows immediately, as the opposite of a Moufang loop is a Moufang loop. □

12.3. Moufang multiplication groups, nuclei, and special autotopisms

We return to the triality base group of adjoint groups with triality, thought of in Section 4.2.1 as a subgroup of the base group of a wreath product $M \wr \mathrm{Sym}(3)$. Here we see that M is the multiplication group of the corresponding Moufang loop.

(12.10). Lemma. *Let* Q *be a Moufang loop and* K *the base group of the adjoint group with triality* $Q\mathbf{TA}$*. Then* $K = \langle\, \rho_1\rho_x,\ \kappa_1\kappa_x,\ \epsilon_1\epsilon_x \mid x \in Q\,\rangle$ *is a normal subgroup of* $\mathrm{Atp}(Q)$*.*

Proof. The observation on generation is immediate from the more general Lemma (4.12)(b). The rest follows from remarks in the previous section and Proposition (12.8). □

The group K of the lemma will be called the *special autotopism group* of Q and be denoted $\mathrm{SAtp}(Q)$, its elements being *special autotopisms.* The corresponding adjoint group with triality

$$\mathrm{G}_Q\,/\mathrm{Z}(\mathrm{G}_Q) = Q\mathbf{TA} = \mathrm{SAtp}(Q) \rtimes \mathrm{Sym}(3)$$

will correspondingly be denoted $\mathrm{TAtp}(Q)$.

(12.11). Proposition. *Let* Q *be a Moufang loop. Then* $\mathrm{SAtp}(Q)$ *induces on each fiber of the Latin square design* $Q\mathbf{T}$ *the multiplication group* $\mathrm{Mlt}(Q)$*.*

Proof. Proposition (12.8) says that, for fixed x, the generators $\epsilon_1\epsilon_x$, $\rho_1\rho_x$, and $\kappa_1\kappa_x$ induce on the fibers $Q\mathbf{T}^{\mathrm{R}}$, $Q\mathbf{T}^{\mathrm{C}}$, and $Q\mathbf{T}^{\mathrm{E}}$, respectively, the subgroup

$$\begin{aligned}\langle \mathrm{L}(x), \mathrm{R}(x)\rangle =&\langle \mathrm{L}(x), \mathrm{R}(x)\,\mathrm{L}(x), \mathrm{R}(x^{-1})\rangle = \langle \mathrm{R}(x), \mathrm{L}(x^{-1}), \mathrm{L}(x)\,\mathrm{R}(x)\rangle\\ =&\ \langle \mathrm{L}(x)\,\mathrm{R}(x), \mathrm{L}(x), \mathrm{R}(x)\rangle\,.\end{aligned}$$

Therefore K induces $\langle\, \mathrm{L}(x), \mathrm{R}(x) \mid x \in Q \,\rangle = \mathrm{Mlt}(Q)$ on each fiber. □

If we want full information about the base group, then we need to know not only the group it induces on each fiber but also what the kernel of that action is.

In an arbitrary loop (indeed quasigroup) Q the *right nucleus* $\mathrm{Nuc}^{\rho}(Q)$ is the set of all z with

$$(ab)z = a(bz) \text{ for all } a, b \in Q\,.$$

Similarly the *left nucleus* $\mathrm{Nuc}^{\lambda}(Q)$ is the set of all x with

$$(xb)c = x(bc) \text{ for all } b, c \in Q\,,$$

and the *middle nucleus* $\mathrm{Nuc}^{\mu}(Q)$ is the set of all y with

$$(ay)c = a(yc) \text{ for all } a, c \in Q\,.$$

A particular consequence of the next proposition is that each of these is a subloop of Q, indeed a subgroup.

The *nucleus* of Q is then $\mathrm{Nuc}(Q) = \mathrm{Nuc}^{\lambda}(Q) \cap \mathrm{Nuc}^{\mu}(Q) \cap \mathrm{Nuc}^{\rho}(Q)$, the set of all elements of Q that associate with all elements of Q is all possible ways. The relevance of this here is the following proposition.

(12.12). Proposition. *Let Q be a loop.*

(a) *The bijection $z \longleftrightarrow (\mathrm{Id}_Q, \mathrm{R}(z), \mathrm{R}(z))$ gives an isomorphism between the right nucleus $\mathrm{Nuc}^{\rho}(Q)$ of Q and that subgroup of $\mathrm{Atp}(Q)$ consisting of all autotopisms of the form (Id_Q, Y, Z). Especially $\mathrm{R}(z^{-1}) = \mathrm{R}(z)^{-1}$ for all $z \in \mathrm{Nuc}^{\rho}(Q)$.*

(b) *The bijection $z \longleftrightarrow (\mathrm{L}(z^{-1}), \mathrm{Id}_Q, \mathrm{L}(z^{-1}))$ gives an isomorphism between the left nucleus $\mathrm{Nuc}^{\lambda}(Q)$ of Q and that subgroup of $\mathrm{Atp}(Q)$ consisting of all autotopisms of the form (X, Id_Q, Z). Especially $\mathrm{L}(z^{-1}) = \mathrm{L}(z)^{-1}$ for all $z \in \mathrm{Nuc}^{\lambda}(Q)$.*

(c) *The bijection $z \longleftrightarrow (\mathrm{R}(z), \mathrm{L}(z^{-1}), \mathrm{Id}_Q)$ gives an isomorphism between the middle nucleus $\mathrm{Nuc}^{\mu}(Q)$ of Q and that subgroup of $\mathrm{Atp}(Q)$ consisting of all autotopisms of the form (X, Y, Id_Q). Especially $\mathrm{R}(z^{-1}) = \mathrm{R}(z)^{-1}$ and $\mathrm{L}(z^{-1}) = \mathrm{L}(z)^{-1}$ for all $z \in \mathrm{Nuc}^{\mu}(Q)$.*

Proof. (a) Assume (Id_Q, Y, Z) is an autotopism. As $1 \cdot a = a$ always, we have

$$a^Y = 1 \cdot a^Y = 1^{\mathrm{Id}_Q} \cdot a^Y = a^Z\,;$$

that is, $Y = Z$. Set $z = 1^Y = 1^Z$. Then $a \cdot 1 = a$ gives $a^{\mathrm{Id}_Q} \cdot 1^Y = a^Z$ or $a \cdot z = a^Z$; that is $Y = Z = \mathrm{R}(z)$. Finally $a \cdot b = ab$ yields $a^{\mathrm{Id}_Q} \cdot b^Y = (ab)^Z$ or $a(bz) = (ab)z$, and z is in the right nucleus Nuc^{ρ}.

Now assume $z \in \mathrm{Nuc}^{\rho}$. Then

$$a^{\mathrm{Id}_Q} \cdot b^{\mathrm{R}(z)} = a(bz) = (ab)z = (ab)^{\mathrm{R}(z)}$$

always, and $(\mathrm{Id}_Q, \mathrm{R}(z), \mathrm{R}(z))$ is an autotopism of Q.

For x and y in $\mathrm{Nuc}^{\rho}(Q)$ we have always

$$a^{\mathrm{R}(x)\,\mathrm{R}(y)} = (ax)y = a(xy) = a^{\mathrm{R}(xy)}\,,$$

so $z \mapsto \mathrm{R}(z)$ is a homomorphism of quasigroups, hence loops, hence groups. (It is worth noticing that this only uses $y \in \mathrm{Nuc}^{\rho}(Q)$.)

Certainly each $(\mathrm{Id}_Q, Y, Z)^{-1} = (\mathrm{Id}_Q, \mathrm{R}(z)^{-1}, \mathrm{R}(z)^{-1})$ is in this subgroup, and so must be equal to $(\mathrm{Id}_Q, \mathrm{R}(w), \mathrm{R}(w))$ for some $w \in \mathrm{Nuc}^{\rho}(Q)$. Then $z^{-1} = 1^{\mathrm{R}(z)^{-1}} = 1^{\mathrm{R}(w)} = w$.

(b) This follows by applying (a) to the opposite loop, except we find that $z \mapsto \mathrm{L}(z)$ is an anti-isomorphism of groups, so we must compose it with inversion to get an isomorphism $z \mapsto \mathrm{L}(z)^{-1} = \mathrm{L}(z^{-1})$.

(c) An autotopism (X, Y, Id_Q) is a principal autotopism of Q. Therefore by Lemma (2.1) there are z and w with $wz = 1$ and $X = \mathrm{R}(z)$ and $Y = \mathrm{L}(w)$. Applied to $1 \cdot 1 = 1$ this gives $z \cdot w = 1$, so in fact $w = z^{-1}$ is a two-sided inverse for z.

The autotopism $(X, Y, \mathrm{Id}_Q)^{-1} = (\mathrm{R}(z)^{-1}, \mathrm{L}(z^{-1})^{-1}, \mathrm{Id}_Q)$ is also principal and so equals $(\mathrm{R}(w), \mathrm{L}(w^{-1}), \mathrm{Id}_Q)$ for some w, which can only be z^{-1}. When applied to $1 \cdot b = b$, this gives $z^{-1}(zb) = b$ for all $b \in Q$.

Let a and b be arbitrary in Q, and set $c = zb$. Then

$$a(zb) = (ac)^{\mathrm{Id}_Q} = a^X \cdot c^Y = a^{\mathrm{R}(z)} c^{\mathrm{L}(z^{-1})} = (az)(z^{-1}(zb)) = (az)b\,.$$

That is, z belongs to the middle nucleus $\mathrm{Nuc}^{\mu}(Q)$.

Conversely, for $z \in \mathrm{Nuc}^{\mu}(Q)$ and $b \in Q$

$$z^{-1}(z(z^{-1}b)) = (z^{-1}z)(z^{-1}b) = z^{-1}b\,,$$

so by cancellation $z(z^{-1}b) = b$ always. Now for arbitrary $a, b \in Q$

$$a^{\mathrm{R}(z)} \cdot b^{\mathrm{L}(z^{-1})} = (az) \cdot (z^{-1}b) = a(z(z^{-1}b)) = ab = (ab)^{\mathrm{Id}_Q}\,;$$

that is, $(\mathrm{R}(z), \mathrm{L}(z^{-1}), \mathrm{Id}_Q)$ is an autotopism.

As before the associated bijection $z \mapsto \mathrm{R}(z)$ gives an isomorphism and $z \mapsto \mathrm{L}(z)$ an anti-isomorphism, so we are done. □

(12.13). Corollary. ([**Bru58**, Theorem VII.2.1],[**Pfl90**, IV.1.5,7])

(a) *Let Q be a left inverse property loop. Then* $\mathrm{Nuc}^{\lambda}(Q) = \mathrm{Nuc}^{\mu}(Q)$ *is a subgroup of Q.*

(b) *Let Q be a right inverse property loop. Then* $\mathrm{Nuc}^{\rho}(Q) = \mathrm{Nuc}^{\mu}(Q)$ *is a subgroup of Q.*

(c) *Let Q be a loop with the antiautomorphic inverse property. Then* $\mathrm{Nuc}^{\rho}(Q) = \mathrm{Nuc}^{\lambda}(Q)$ *is a subgroup of Q.*

(d) *Let Q be an inverse property loop. Then* $\mathrm{Nuc}(Q) = \mathrm{Nuc}^{\lambda}(Q) = \mathrm{Nuc}^{\mu}(Q) = \mathrm{Nuc}^{\rho}(Q)$ *is a subgroup of Q.*

Proof. (See [**Bru58**, Theorem VII.2.] and [**Pfl90**, Theorem I.4.3].) By Lemma (3.12), Q is a left inverse property loop if and only if $\mathrm{Aut}(Q\mathbf{T})$ contains the automorphism ρ_1. But the map ρ_1 interchanges autotopisms of the form (X, Y, Id_Q) and (W, Id_Q, Z), thought of as automorphisms of the Latin square design $Q\mathbf{T}$. This gives (a), and similar arguments yield (b) and (c) hence (d). □

(12.14). Lemma. *Let Q be a Moufang loop. Then* $\mathrm{Nuc}(Q) = \mathrm{Nuc}^{\lambda}(Q) = \mathrm{Nuc}^{\mu}(Q) = \mathrm{Nuc}^{\rho}(Q)$ *is a normal subgroup of Q.*

Proof. (See [**Bru58**, Theorem VII.2.] and [**Pfl90**, Corollary IV.1.7].) Every Moufang loop is an inverse property loop, so by the corollary all we need is a demonstration that $\mathrm{Nuc}(Q)$ is normal in the Moufang loop Q.

By Propositions (12.5) and (12.6), this will be the case provided that, for every $z \in \mathrm{Nuc}(Q)$ and $a, b \in Q$, we can show

$$z^{\mathrm{R}(a)\,\mathrm{R}(b)\,\mathrm{R}(ab)^{-1}} \in \mathrm{Nuc}(Q)\,, \quad z^{\mathrm{L}(a)\,\mathrm{L}(b)\,\mathrm{L}(ba)^{-1}} \in \mathrm{Nuc}(Q)\,, \quad z^{\mathrm{L}(a)\,\mathrm{R}(a)^{-1}} \in \mathrm{Nuc}(Q)\,.$$

As $z \in \mathrm{Nuc}^{\lambda}(Q) \cap \mathrm{Nuc}^{\rho}(Q)$, the first two come easily; indeed

$$z^{\mathrm{R}(a)\,\mathrm{R}(b)\,\mathrm{R}(ab)^{-1}} = z = z^{\mathrm{L}(a)\,\mathrm{L}(b)\,\mathrm{L}(ba)^{-1}}\,.$$

Since Q is Moufang, it admits the autotopism $(\mathrm{L}(a), \mathrm{R}(a), \mathrm{L}(a)\,\mathrm{R}(a))$ by Proposition (12.7). As z is in the nucleus, we also have the autotopism $(\mathrm{Id}_Q, \mathrm{R}(z), \mathrm{R}(z))$ by Proposition (12.12)(a). Therefore we have a third autotopism

$$\begin{aligned}(\mathrm{L}(a), \mathrm{R}(a), \mathrm{L}(a)\,\mathrm{R}(a))\,&(\mathrm{Id}_Q, \mathrm{R}(z), \mathrm{R}(z))\,(\mathrm{L}(a), \mathrm{R}(a), \mathrm{L}(a)\,\mathrm{R}(a))^{-1}\\ &= (\mathrm{L}(a)\,\mathrm{L}(a)^{-1}, \mathrm{R}(a)\,\mathrm{R}(z)\,\mathrm{R}(a)^{-1}, *)\\ &= (\mathrm{Id}_Q, \mathrm{R}(a)\,\mathrm{R}(z)\,\mathrm{R}(a)^{-1}, *)\,,\end{aligned}$$

where in these last two lines we do not need the third mapping specifically. Again by Proposition (12.12)(a) there is a w in the (right) nucleus with $\mathrm{R}(a)\,\mathrm{R}(z)\,\mathrm{R}(a)^{-1} = \mathrm{R}(w)$. Indeed

$$w = 1^w = 1^{\mathrm{R}(a)\,\mathrm{R}(z)\,\mathrm{R}(a)^{-1}} = (az)a^{-1}\,.$$

Therefore $z^{\mathrm{L}(a)\,\mathrm{R}(a)^{-1}} = (az)a^{-1} \in \mathrm{Nuc}(Q)$, as desired. □

(12.15). THEOREM. *Let Q be a Moufang loop and $K = \mathrm{SAtp}(Q)$, the special autotopism group and the base group of the adjoint group with triality* $\mathrm{TAtp}(Q)$. *There are isomorphic groups A_1, A_2, and A_3 such that:*

(a) *A_1 is the kernel of the projection of K onto one of its three coordinates and so is normal in K with K/A_1 isomorphic to* $\mathrm{Mlt}(Q)$*;*

(b) *A_2 is normal in* $\mathrm{Mlt}(Q)$*;*

(c) *A_3 is normal in Q and is contained in the nucleus of Q.*

Indeed the three kernels A_1 are

$$\begin{aligned}&\{\,(\mathrm{Id}_Q, \mathrm{R}(z), \mathrm{R}(z)) \mid z \in A_3\,\}\,,\\ &\{\,(\mathrm{L}(z), \mathrm{Id}_Q, \mathrm{L}(z)) \mid z \in A_3\,\}\,,\\ &\{\,(\mathrm{R}(z), \mathrm{L}(z^{-1}), \mathrm{Id}_Q)) \mid z \in A_3\,\}\,.\end{aligned}$$

In particular A_2 may be taken to be the image of either of the two kernels not A_1.

PROOF. Let A_1 be the kernel of the homomorphism from K onto $\mathrm{Mlt}(Q)$ given by Proposition (12.11), where we (somewhat arbitrarily) choose A_1 to be those elements of K having the form (Id_Q, Y, Z) as autotopisms of Q. This gives (a).

By Proposition (12.12)(a), A_1 is then isomorphic to a subgroup A_3 of the nucleus of Q via $z \longleftrightarrow (\mathrm{Id}_Q, \mathrm{R}(z), \mathrm{R}(z))$. By Proposition (12.8) the element $k = \epsilon_1\epsilon_x$ of K acts as the autotopism $(\mathrm{L}(x), \mathrm{R}(x), \mathrm{L}(x)\,\mathrm{R}(x))$. Hence, as in the proof of Lemma (12.14),

$$k(\mathrm{Id}_Q, \mathrm{R}(z), \mathrm{R}(z))k^{-1} = (\mathrm{Id}_Q, \mathrm{R}((xz)x^{-1}), \mathrm{R}((xz)x^{-1})) \in A_1\,.$$

Thus the nuclear subgroup A_3 is fixed by all $\mathrm{L}(x)\,\mathrm{R}(x)^{-1}$ as well as being fixed pointwise by all $\mathrm{R}(x)\,\mathrm{R}(y)\,\mathrm{R}(xy)^{-1}$ and $\mathrm{L}(x)\,\mathrm{L}(y)\,\mathrm{L}(yx)^{-1}$. Therefore A_3 is normal in Q by Propositions (12.5) and (12.6), completing (c).

Finally the subgroup $A_1^{\kappa_1} = \{\,(\mathrm{R}(z), \mathrm{L}(z^{-1}), \mathrm{Id}_Q)) \mid z \in A_3\,\}$ is normal in K and isomorphic to A_1 (and A_3), while meeting A_1 trivially; so its image A_2 in $\mathrm{Mlt}(Q) \simeq K/A_1$ is normal and isomorphic to A_1, as needed for (b). □

(12.16). COROLLARY. *The Moufang loop Q is finite if and only if* G_Q *is finite if and only if* $\mathrm{Mlt}(Q)$ *is finite.*

Proof. As $\mathrm{Mlt}(Q)$ is a transitive subgroup of $\mathrm{Sym}(Q)$, the (arbitrary) loop Q is finite if and only if $\mathrm{Mlt}(Q)$ is finite. By Theorem (12.15) for Moufang Q

$$|\,\mathrm{Mlt}(Q)| \leq |\,\mathrm{G}_Q/\mathrm{Z}(\mathrm{G}_Q)| \leq 6|\,\mathrm{Mlt}(Q)|^2\,,$$

so $\mathrm{Mlt}(Q)$ is finite if and only if $\mathrm{G}_Q/\mathrm{Z}(\mathrm{G}_Q)$ is finite. If $\mathrm{G}_Q/\mathrm{Z}(\mathrm{G}_Q)$ is infinite, then certainly G_Q is infinite. If $\mathrm{G}_Q/\mathrm{Z}(\mathrm{G}_Q)$ is finite, then G'_Q is finite by a classical result of Schur [**Rob82**, 10.1.4]. As $\mathrm{Z}(\mathrm{G}_Q) \leq \mathrm{G}'_Q$ by Lemma (4.12), both $\mathrm{Z}(G)$ and G_Q are finite. □

(12.17). Corollary. (Glauberman [**Gla68**, Theorem 6]) *If Q is a Moufang loop with trivial nucleus, then* $\mathrm{Mlt}(Q)$ *admits a group of automorphisms* $\mathrm{Sym}(3)$ *in such a way that* $\mathrm{Mlt}(Q) \rtimes \mathrm{Sym}(3)$ *is a group with triality.*

Proof. In Theorem (12.15) if the nucleus of Q is trivial then the isomorphic groups A_3 and A_1 are both trivial. That is, when the nucleus is trivial, $\mathrm{Mlt}(Q)$ is isomorphic to the triality base group and so naturally admits $\mathrm{Sym}(3)$ giving a group with triality. □

The question then arises, when exactly does the multiplication group of a Moufang loop naturally admit the triality? The difficulty is that the nucleus can be nontrivial but with the corresponding subgroups of $\mathrm{Atp}(Q)$ intersecting $\mathrm{SAtp}(Q)$ trivially. The question has been studied by Phillips [**Phi94, Phi99**] but is not completely solved.

(12.18). Proposition. *Let Q be a Moufang loop. Then the universal group with triality* G_Q *is solvable if and only if the multiplication group* $\mathrm{Mlt}(Q)$ *is solvable.*

Proof. The group G_Q is a central extension of the adjoint group with triality $\mathrm{TAtp}(Q)$, so a further equivalent statement would be the solvability of $\mathrm{TAtp}(Q)$ or indeed of its base group K. By Theorem (12.15) the group K has a normal subgroup A such that K/A is isomorphic to $\mathrm{Mlt}(Q)$ with A in turn isomorphic to a normal subgroup of $\mathrm{Mlt}(Q)$. In particular K is solvable if and only if $\mathrm{Mlt}(Q)$ is solvable, as desired. □

Chapter 13

Doro's Approach

We have discussed groups with triality (G, D, π). In Doro's original treatment [**Dor78**] of abstract triality for groups the main object of study is the base group K, the kernel of the homomorphism π, which admits a group Sym(3), the image of π, inducing automorphisms in a prescribed manner.

Specifically, Doro defined a group with triality to be a group K that admits an action of $I \simeq \mathrm{Sym}(3)$ as a (not necessarily faithful) group of automorphisms such that, for σ of order 2 and μ of order 3 in I, we have

(i) $[k, \sigma][k, \sigma]^{\mu}[k, \sigma]^{\mu^2} = 1$, *for all* $k \in K$*;*

(ii) $K = [K, I]$.

In order to avoid confusion, we will in this case say that the group K *admits the triality* I. Doro proved that the set $\{\, [k, \sigma] \mid k \in K \,\}$ naturally carries the structure of a Moufang loop; see Theorem (13.4)(a) below.

The group Sym(3) acts regularly by conjugation on the set of its ordered pairs consisting of an element of order 2 and an element of order 3. Therefore the above conditions are actually independent of the specific choices of the elements σ and μ.

As we shall see in this chapter Doro's viewpoint is basically the same as ours for $\mathsf{TriGrp}^{\star}$. This is relatively easy to check except for the specifics regarding universal groups, which take up a lot of the chapter.

13.1. Doro's categories

Let objects of the category Doro be triples (K, I, ι_I) with K admitting the triality I and $\iota_I \colon I \simeq \mathrm{Sym}(3)$ an isomorphism, so that K canonically admits the triality $\mathrm{Sym}(3) = I^{\iota_I}$. The pair (φ, ι) belongs to $\mathrm{Hom}_{\mathsf{Doro}}((K, I, \iota_I), (H, J, \iota_J))$ when $\iota \colon I \longrightarrow J$ is an isomorphism with $\iota_I = \iota\iota_J$ and $\varphi \colon K \longrightarrow H$ is a compatible Sym(3)-homomorphism: for all $a \in I$ and $k \in K$

$$(k^a)^{\varphi} = (k^{\varphi})^{a^{\iota}} \quad \text{or equivalently} \quad (k^{a^{i_I}})^{\varphi} = (k^{\varphi})^{a^{\iota i_J}} \, .$$

Doro [**Dor78**, p. 383] actually introduced a slightly different category, which he called $\mathcal{T}$. Doro's $\mathcal{T}$ is isomorphic to the full subcategory of Doro whose objects are those (K, I, ι_I) with $I = \mathrm{Sym}(3)$ and $\iota_I = \mathrm{Id}_{\mathrm{Sym}(3)}$. As this subcategory $\mathcal{T}$ is full and dense, it is equivalent to Doro by Corollary (1.2).

The following observation is due to Richard Parker [**Lie87**, Lemma 3.2].

(13.1). Lemma. *Let $I \simeq \mathrm{Sym}(3)$ act on the group K. Further let σ and η have order 2 in I so that $\mu = \eta\sigma$ has order 3. Then for $k \in K$ we have $[k,\sigma][k,\sigma]^{\mu}[k,\sigma]^{\mu^2} = (\sigma^k\eta)^3$ in $K \rtimes I$.*

Proof. Let $\epsilon = \sigma\eta\sigma$ be the third element of order 2 in I. Then $\eta = \sigma\epsilon\sigma = \epsilon\sigma\epsilon$ and $\mu = \sigma\epsilon$, so that

$$\begin{aligned}[k,\sigma][k,\sigma]^{\mu}[k,\sigma]^{\mu^2} &= (k^{-1}\sigma k\sigma).\epsilon\sigma(k^{-1}\sigma k\sigma)\sigma\epsilon.\sigma\epsilon(k^{-1}\sigma k\sigma)\epsilon\sigma \\ &= (k^{-1}\sigma k)(\sigma\epsilon\sigma)(k^{-1}\sigma k)(\sigma\sigma)(\epsilon\sigma\epsilon)(k^{-1}\sigma k)(\sigma\epsilon\sigma) \\ &= (\sigma^k\eta)^3 \,. \square\end{aligned}$$

(13.2). Theorem.

(a) *Let $(G,D,\pi,I) \in \mathsf{TriGrp}^{\star}$. Then $(K,I,\iota_I) \in \mathsf{Doro}$ where $K = \ker\pi$ and $\iota_I = \pi|_I$.*

(b) *Let $(K,I,\iota_I) \in \mathsf{Doro}$. Then $(G,D,\pi,I) \in \mathsf{TriGrp}^{\star}$ where $G = K \rtimes I$, $D = \sigma^G$ for σ of order 2 in I, and $g^{\pi} = s^{\iota_I}$ for $g = ks$ with $k \in K$ and $s \in I$.*

Proof. For (a) the group G is generated by D, so G is contained in and thus equal to $[K,I]I$. Therefore $K = [K,I]$, and the rest follows from the lemma.

In (b) as $K = [K,I]$, we have $G = KI = [K,I]I = I^G = \langle D\rangle$. Let η be a second element of order 2 in I and $d,e \in D$ with $d^{\pi} \neq e^{\pi}$. There is a $t \in I$ such that $(de)^t = \sigma^m\eta^n$ with $m,n \in K$. But then $|de| = |\sigma^k\eta|$ for $k = mn^{-1} \in K$, and the lemma again applies. □

We therefore immediately have:

(13.3). Theorem. *The categories Doro and $\mathsf{TriGrp}^{\star}$ are isomorphic.* □

After a long and tiring journey, we have finally arrived at Doro's original construction of a Moufang loop from a group admitting triality.

(13.4). Theorem. *Let $(K,I,\iota_I) \in \mathsf{Doro}$. Choose distinct elements σ,η of order 2 in I and set $\mu = \eta\sigma$.*

(a) **(Doro [Dor78**, Theorem 1**])** *Let $R = \{\, [k,\sigma] \mid k \in K \,\}$ and $H = \mathrm{C}_K(\eta)$. Then R is a set of right coset representatives for H in K. If we define a binary product on R by*

$$m \circ n = p \quad \text{for} \quad mn \in Hp\,,$$

then $(R,\circ)$ is a Moufang loop.

(b) **(Grishkov and Zavarnitsine [GrZ06**, Lemma 2**])** *For $(R,\circ)$ as in* (a) *we have $m \circ n = n^{-\mu^2}mn^{-\mu} = m^{-\mu}nm^{-\mu^2}$.*

(c) *Let $(G,D,\pi,I) \in \mathsf{TriGrp}^{\star}$ with $G = K \rtimes I$, $D = \sigma^G$, and $(ks)^{\pi} = s^{\iota_I}$ for $k \in K, s \in I$. Then $(R,\circ)$ as defined in* (a) *is isomorphic to the Moufang loop $(G,D,\pi,I)\mathbf{M}^{\star}$.*

Proof. By Theorem (13.2) we have $(G,D,\pi,I) \in \mathsf{TriGrp}^{\star}$ as claimed in (c). As $H \geq \mathrm{Z}(G)$ and $[k,\sigma] = [k\mathrm{Z}(G),\sigma]$ for all $k \in K$, we may, without loss of generality, assume that $(G,D,\pi,I) \in \mathsf{UTriGrp}^{\star}$. By Theorem (11.6) there is a Moufang loop Q with (G,D,π,I) isomorphic to $Q\mathbf{G}^{\star}$ and then $(G,D,\pi,I)\mathbf{M}^{\star}$ isomorphic to $Q\mathbf{G}^{\star}\mathbf{M}^{\star}$ and hence to Q.

Part (c) is now a consequence of Proposition (11.5) parts (a), (b), and (c). Part (a) then follows from the present (c) and (11.5)(b) again, while (b) comes from (11.5)(d). □

The adjoint category $\mathsf{ATriGrp}^\star$ is the full subcategory of $\mathsf{TriGrp}^\star$ consisting of those objects (G, D, π, I) with $Z(G) = 1$. For $(K, I, \iota_I) \in \mathsf{Doro}$, let $Z_I(K) = Z(K) \cap C_K(I)$ so that $Z_I(K) = Z(K \rtimes I)$. We then let ADoro be the full subcategory of Doro of those (K, I, ι_I) with $Z_I(K) = 1$.

(13.5). THEOREM. *The categories* ADoro *and* $\mathsf{ATriGrp}^\star$ *are isomorphic.* □

Using Theorem (13.4)(a), Doro [**Dor78**, p. 383] defined a functor M from his category $\mathcal{T}$ of groups admitting triality to the category $\mathsf{Mouf}^\star$ of Moufang loops (with loop homomorphisms as morphisms). This functor can be thought of as our functor $\mathbf{M}^\star$ composed with the isomorphism of Theorem (13.3). Although Doro did not expressly define adjoint or universal subcategories of the category $\mathcal{T}$, he did deal with adjoint and universal groups as important objects. For instance, in his Corollary 1 to Theorem 2 Doro noted that if two groups G_1 and G_2 admitting the triality I give isomorphic Moufang loops $M(G_1)$ and $M(G_2)$, then the corresponding adjoint groups $G_1/Z_I(G_1)$ and $G_2/Z_I(G_2)$ are isomorphic groups admitting triality. The current Proposition (7.8) is a version of Doro's corollary.

Doro also defined a functor G from $\mathsf{Mouf}^\star$ to $\mathcal{T}$ that assigns to each Moufang loop a universal group admitting triality. Doro's functor G is defined via a presentation parametrized by Q, as is our functor $\mathbf{G}^\star$. Doro showed that the corresponding map is a functor and that the groups in its image have $M(G(Q))$ isomorphic to Q and are appropriately universal subject to that.

The rest of this chapter is devoted to proof and discussion of the fact that Doro's universal functor G and our $\mathbf{G}^\star$ are basically the same. We do this by proving that Doro's universal group admitting triality, which we shall call $\mathrm{K}(Q)$ rather than $G(Q)$, is canonically isomorphic to the kernel K_Q of π_Q, where (G_Q, D_Q, π_Q, I_Q) is our universal group with triality $Q\mathbf{G}^\star$ from Section 11.1.

The treatment is long for two reasons. We squeeze out as much generality as we can by considering arbitrary loops Q, only at the end specializing to Moufang loops. But even without the generality, a full proof would take us a while, since we give a full account of the use of the Reidermeister-Schreier method to move from our defining presentation of the group G_Q to its normal subgroup K_Q of index 6.

We begin with Doro's presentation [**Dor78**, p. 383].

(13.6). PRESENTATION. *Let Q be a Moufang loop. The group* $\mathrm{K}(Q)$ *has the following presentation:*

Generators:
for arbitrary $x \in Q$:
R_x, L_x, *and* P_x ;

Relations:
for arbitrary $x, y \in Q$:
(1) $R_1 = L_1 = P_1 = 1$;
(4) $P_xR_yL_x = R_{x^{-1}y}$; $R_xL_yP_x = L_{x^{-1}y}$; $L_xP_yR_x = P_{x^{-1}y}$;
(5) $L_yR_xP_y = R_{xy^{-1}}$; $P_yL_xR_y = L_{xy^{-1}}$; $R_yP_xL_y = P_{xy^{-1}}$;
(6) $P_xL_xR_x = 1$;
(7) $P_xP_yP_x = P_{xyx}$; $L_xL_yL_x = L_{xyx}$; $R_xR_yR_x = R_{xyx}$.

The reason behind our strange numbering should become apparent later.

(13.7). THEOREM. **(Doro [Dor78**, Theorem 2]**)** *Let Q be a Moufang loop. The group $\mathrm{K}(Q) = [\mathrm{K}(Q), I]$ of Presentation (13.6) admits the triality group of automorphisms $I = \langle \sigma, \mu \rangle \simeq \mathrm{Sym}(3)$ acting via:*

$$R_x \overset{\sigma}{\longleftrightarrow} R_x^{-1} \quad \textit{and} \quad L_x \overset{\sigma}{\longleftrightarrow} P_x^{-1}$$

$$R_x \xrightarrow{\mu} P_x \xrightarrow{\mu} L_x \xrightarrow{\mu} R_x\,.$$

Each of the maps

$$x \mapsto R_x \qquad x \mapsto L_x \qquad x \mapsto P_x$$

is a bijection of Q with the corresponding subset of the generators.

We let UDoro be the full subcategory of Doro consisting of those objects from Doro isomorphic to those of Theorem (13.7).

(13.8). THEOREM. *The categories* UDoro *and* UTriGrp* *are isomorphic.*

Theorems (13.7) and (13.8) are immediate consequences of Theorem (13.3) and the following theorem which will be proven in Section 13.4 below.

(13.9). THEOREM. *Let Q be a Moufang loop, and let K_Q be the kernel of the map π_Q on the universal group with triality G_Q of Section 11.1. Then K_Q has the following presentation:*

Generators:

for arbitrary $x \in Q$:

R_x, L_x, *and* P_x;

Relations:

for arbitrary $x, y \in Q$:

(1) $R_1 = L_1 = P_1 = 1$;

(4) $P_xR_yL_x = R_{x^{-1}y}$; $R_xL_yP_x = L_{x^{-1}y}$; $L_xP_yR_x = P_{x^{-1}y}$;

(5) $L_yR_xP_y = R_{xy^{-1}}$; $P_yL_xR_y = L_{xy^{-1}}$; $R_yP_xL_y = P_{xy^{-1}}$;

(6) $P_xL_xR_x = 1$;

(7) $P_xP_yP_x = P_{xyx}$; $L_xL_yL_x = L_{xyx}$; $R_xR_yR_x = R_{xyx}$.

In fact the relations (6) *and* (7) *are consequences of relations* (1), (4), *and* (5).

As a subgroup of G_Q, the chosen generators of K_Q are $R_x = \mathsf{c}_x\mathsf{c}_1$, $L_x = \mathsf{e}_1\mathsf{e}_x$, and $P_x = \mathsf{r}_x\mathsf{r}_1$, for $x \in Q$.

The group $K_Q = [K_Q, I_Q]$ admits the triality group of automorphisms $I_Q = \langle \sigma, \mu \rangle \simeq \mathrm{Sym}(3)$ acting via:

$$R_x \overset{\sigma}{\longleftrightarrow} R_x^{-1} \quad \textit{and} \quad L_x \overset{\sigma}{\longleftrightarrow} P_x^{-1}$$

$$R_x \xrightarrow{\mu} P_x \xrightarrow{\mu} L_x \xrightarrow{\mu} R_x\,.$$

Each of the maps

$$x \mapsto R_x \qquad x \mapsto L_x \qquad x \mapsto P_x$$

is a bijection of Q with the corresponding subset of the generators.

13.2. A presentation of the base group

The next theorem is the central result of the universality work in this chapter. Starting from Presentation (11.1) for the universal group G_Q, we find a presentation for $\ker \pi_Q$, its normal subgroup of index 6. To do this we use the Reidermeister-Schreier method, largely following the treatment of Bogopolski [**Bog08**, §§2.8-9].

(13.10). THEOREM. *Let Q be a loop, and let K_Q be the kernel of the map π_Q on G_Q. Then K_Q has the following presentation:*

Generators:
for arbitrary $x \in Q$:
R_x, L_x, *and* P_x ;

Relations:
for arbitrary $x, y \in Q$:
(1) $R_1 = L_1 = P_1 = 1$;
(2) $P_x R_{xy} L_x = R_y$; $R_x L_{xy} P_x = L_y$; $L_x P_{xy} R_x = P_y$;
(3) $L_y R_{xy} P_y = R_x$; $P_y L_{xy} R_y = L_x$; $R_y P_{xy} L_y = P_x$.

As a subgroup of G_Q, the chosen generators of K_Q are $R_x = \mathsf{c}_x\mathsf{c}_1$, $L_x = \mathsf{e}_1\mathsf{e}_x$, and $P_x = \mathsf{r}_x\mathsf{r}_1$, for $x \in Q$.

The group $K_Q = [K_Q, I_Q]$ admits the triality group of automorphisms $I_Q = \langle \mathsf{c}_1, \mathsf{e}_1 \rangle = \langle \sigma, \mu \rangle \simeq \mathrm{Sym}(3)$ with $\sigma = \mathsf{c}_1$ and $\mu = \mathsf{c}_1\mathsf{e}_1$ acting via:

$$R_x \overset{\sigma}{\longleftrightarrow} R_x^{-1} \quad \textit{and} \quad L_x \overset{\sigma}{\longleftrightarrow} P_x^{-1}$$

$$R_x \xrightarrow{\mu} P_x \xrightarrow{\mu} L_x \xrightarrow{\mu} R_x \,.$$

Let Q be a loop, and let G be the free group generated by

$$X = \{\, \mathsf{r}_x, \mathsf{c}_x, \mathsf{e}_x \mid x \in Q \,\}\,.$$

With reference to Presentation (11.1) for the group G_Q, we let R be the set of relators

$$\begin{aligned} \mathsf{r}_x^2\,,\ \mathsf{c}_x^2\,,\ \mathsf{e}_x^2 &\quad \text{for all } x \in Q\,, \\ \mathsf{r}_x\mathsf{c}_y\mathsf{r}_x\mathsf{e}_{xy}^{-1}\,,\ \mathsf{c}_y\mathsf{r}_x\mathsf{c}_y\mathsf{e}_{xy}^{-1} &\quad \text{for all } x, y \in Q\,. \end{aligned}$$

The kernel J of the canonical map from G to $\mathrm{G}_Q = \langle\, X \mid R \,\rangle$ is then the normal closure within G of the relator set R.

Next let K be the preimage in G of K_Q, the kernel of the homomorphism π_Q on G_Q (as defined in Theorem (11.3)). Therefore K has index 6 in G, and a particularly nice set of coset representatives for K in G is

$$T = \{1, \mathsf{r}_1, \mathsf{c}_1, \mathsf{e}_1, \mathsf{e}_1\mathsf{r}_1, \mathsf{e}_1\mathsf{c}_1\}\,.$$

The kernel K_Q is thus isomorphic to the quotient K/J, and J is the normal closure within K of the set of elements $\bigcup_{t\in T}\{\, trt^{-1} \mid r \in R \,\}$.

The construction of a presentation of K_Q from that for G_Q is a two step process. First we construct (following Schreier) a convenient set of free generators for the subgroup K of G. Then we use the Reidermeister rewriting process to write the various trt^{-1} as words in those generators, giving a complete set of relators.

For each $g \in G$ we let $\overline{g}$ be the unique element of T with $g \in K\overline{g}$. As the set of coset representatives T is a Schreier transversal (that is, every initial segment of a member of T also belongs to T), Theorem 8.10 of [**Bog08**] tells us that the group

K is freely generated within G by the set of nonidentity elements $tg(\overline{tg})^{-1}$ for $t \in T$ and $g \in X$. The appropriate coset representatives $\overline{tg}$ are easy to tabulate:

$\overline{tg}$	r_x	c_x	e_x
1	r_1	c_1	e_1
r_1	1	$\mathsf{e}_1\mathsf{r}_1$	$\mathsf{e}_1\mathsf{c}_1$
c_1	$\mathsf{e}_1\mathsf{c}_1$	1	$\mathsf{e}_1\mathsf{r}_1$
e_1	$\mathsf{e}_1\mathsf{r}_1$	$\mathsf{e}_1\mathsf{c}_1$	1
$\mathsf{e}_1\mathsf{r}_1$	e_1	r_1	c_1
$\mathsf{e}_1\mathsf{c}_1$	c_1	e_1	r_1

We then list and name the elements $tg(\overline{tg})^{-1}$ in:

$t \in T$	$g \in X$	$tg(\overline{tg})^{-1}$	Name
1	r_x	$\mathsf{r}_x\mathsf{r}_1^{-1}$	$P_{\mathsf{r},x}$
r_1	r_x	$\mathsf{r}_1\mathsf{r}_x$	$P^-_{\mathsf{r},x}$
c_1	r_x	$\mathsf{c}_1\mathsf{r}_x(\mathsf{e}_1\mathsf{c}_1)^{-1}$	$L^-_{\mathsf{r},x}$
e_1	r_x	$\mathsf{e}_1\mathsf{r}_x(\mathsf{e}_1\mathsf{r}_1)^{-1}$	$R^-_{\mathsf{r},x}$
$\mathsf{e}_1\mathsf{r}_1$	r_x	$\mathsf{e}_1\mathsf{r}_1\mathsf{r}_x\mathsf{e}_1^{-1}$	$R_{\mathsf{r},x}$
$\mathsf{e}_1\mathsf{c}_1$	r_x	$\mathsf{e}_1\mathsf{c}_1\mathsf{r}_x\mathsf{c}_1^{-1}$	$L_{\mathsf{r},x}$
1	c_x	$\mathsf{c}_x\mathsf{c}_1^{-1}$	$R_{\mathsf{c},x}$
r_1	c_x	$\mathsf{r}_1\mathsf{c}_x(\mathsf{e}_1\mathsf{r}_1)^{-1}$	$L^-_{\mathsf{c},x}$
c_1	c_x	$\mathsf{c}_1\mathsf{c}_x$	$R^-_{\mathsf{c},x}$
e_1	c_x	$\mathsf{e}_1\mathsf{c}_x(\mathsf{e}_1\mathsf{c}_1)^{-1}$	$P^-_{\mathsf{c},x}$
$\mathsf{e}_1\mathsf{r}_1$	c_x	$\mathsf{e}_1\mathsf{r}_1\mathsf{c}_x\mathsf{r}_1^{-1}$	$L_{\mathsf{c},x}$
$\mathsf{e}_1\mathsf{c}_1$	c_x	$\mathsf{e}_1\mathsf{c}_1\mathsf{c}_x\mathsf{e}_1^{-1}$	$P_{\mathsf{c},x}$
1	e_x	$\mathsf{e}_x\mathsf{e}_1^{-1}$	$L^-_{\mathsf{e},x}$
r_1	e_x	$\mathsf{r}_1\mathsf{e}_x(\mathsf{e}_1\mathsf{c}_1)^{-1}$	$R_{\mathsf{e},x}$
c_1	e_x	$\mathsf{c}_1\mathsf{e}_x(\mathsf{e}_1\mathsf{r}_1)^{-1}$	$P_{\mathsf{e},x}$
e_1	e_x	$\mathsf{e}_1\mathsf{e}_x$	$L_{\mathsf{e},x}$
$\mathsf{e}_1\mathsf{r}_1$	e_x	$\mathsf{e}_1\mathsf{r}_1\mathsf{e}_x\mathsf{c}_1^{-1}$	$P^-_{\mathsf{e},x}$
$\mathsf{e}_1\mathsf{c}_1$	e_x	$\mathsf{e}_1\mathsf{c}_1\mathsf{e}_x\mathsf{r}_1^{-1}$	$R^-_{\mathsf{e},x}$

As motivation for the names from the final column, refer to Proposition (12.8) and momentarily set

$$\begin{aligned} L &= \epsilon_1\epsilon_x = (\mathrm{L}(x), \mathrm{R}(x), \mathrm{L}(x)\,\mathrm{R}(x))\,, \\ R^{-1} &= \kappa_1\kappa_x = (\mathrm{R}(x^{-1}), \mathrm{L}(x)\,\mathrm{R}(x), \mathrm{R}(x))\,, \\ P^{-1} &= \rho_1\rho_x = (\mathrm{R}(x)\,\mathrm{L}(x), \mathrm{L}(x^{-1}), \mathrm{L}(x))\,. \end{aligned}$$

Then the names refer to the first entry of the corresponding autotopism and

$$RLP = RPL = LRP = LPR = PRL = PLR = (\mathrm{Id}_Q, \mathrm{Id}_Q, \mathrm{Id}_Q)\,.$$

(13.11). PROPOSITION. *The subgroup K of G is freely generated by the non-identity elements of*

$$\begin{aligned} &R_{\mathsf{r},x},\ R^-_{\mathsf{r},x},\ L_{\mathsf{r},x},\ L^-_{\mathsf{r},x},\ P_{\mathsf{r},x},\ P^-_{\mathsf{r},x}\,,\\ &R_{\mathsf{c},x},\ R^-_{\mathsf{c},x},\ L_{\mathsf{c},x},\ L^-_{\mathsf{c},x},\ P_{\mathsf{c},x},\ P^-_{\mathsf{c},x}\,,\\ &R_{\mathsf{e},x},\ R^-_{\mathsf{e},x},\ L_{\mathsf{e},x},\ L^-_{\mathsf{e},x},\ P_{\mathsf{e},x},\ P^-_{\mathsf{e},x}\,. \end{aligned}$$

for all $x \in Q$. The only identity elements among these are

$$P_{\mathsf{r},1}\,,\ R^-_{\mathsf{r},1}\,,\ R_{\mathsf{c},1}\,,\ P^-_{\mathsf{c},1}\,,\ L^-_{\mathsf{e},1}\,.$$

PROOF. For each $x \in Q$ we have the eighteen elements of K named in the previous table. Of these, only those with $x = 1$ have any chance of being the identity in the free group G generated by X. When we check the eighteen elements $tg(\overline{tg})^{-1}$ with $g \in \{\mathsf{r}_1, \mathsf{c}_1, \mathsf{e}_1\}$, we find the identity only in five cases:

$$\begin{gathered} P_{\mathsf{r},1} = \mathsf{r}_1\mathsf{r}_1^{-1} = 1\,;\ R^-_{\mathsf{r},1} = \mathsf{e}_1\mathsf{r}_1(\mathsf{e}_1\mathsf{r}_1)^{-1} = 1\,;\ R_{\mathsf{c},1} = \mathsf{c}_1\mathsf{c}_1^{-1} = 1;\\ P^-_{\mathsf{c},1} = \mathsf{e}_1\mathsf{c}_1(\mathsf{e}_1\mathsf{c}_1)^{-1} = 1\,;\ L^-_{\mathsf{e},1} = \mathsf{e}_1\mathsf{e}_1^{-1} = 1. \qquad \square \end{gathered}$$

The Reidermeister rewriting process (which has been discussed earlier starting on page 81) is relatively simple. Starting with one of the conjugated relator words trt^{-1}, written as a product of letters from $X \cup X^{-1}$, we scan the word starting from the front; subwords $s^{-1}s$, for $s \in T$, are inserted in such a way that ever increasing initial segments of the word are products of generators of the subgroup K (from Proposition (13.11)) or their inverses. For instance, the relator $\mathsf{r}_x^2 = \mathsf{r}_x\mathsf{r}_x$ begins with r_x; this is not one of our subgroup generators, but $\mathsf{r}_x\mathsf{r}_1^{-1} = P_{\mathsf{r},x}$ is. Therefore we rewrite as follows:

$$\mathsf{r}_x\mathsf{r}_x = \mathsf{r}_x(\mathsf{r}_1^{-1}\mathsf{r}_1)\mathsf{r}_x = (\mathsf{r}_x\mathsf{r}_1^{-1})\,\mathsf{r}_1\mathsf{r}_x = P_{\mathsf{r},x}\,\mathsf{r}_1\mathsf{r}_x = P_{\mathsf{r},x}P^-_{\mathsf{r},x}\,.$$

That trt^{-1} belongs to K and indeed to J is not very important for the rewriting process. Indeed, we can scan any word in the letters $X \cup X^{-1}$ from beginning to end in the same way, the result being a rewritten version of the corresponding element of G as a product of generators of K or their inverses, followed by a single coset representative from T; for instance $\mathsf{r}_x = (\mathsf{r}_x\mathsf{r}_1^{-1})\mathsf{r}_1 = P_{\mathsf{r},x}\mathsf{r}_1$. If the word happens to belong to the subgroup K (as all the elements trt^{-1} of J certainly do), then that coset representative must turn out to be the identity, as in the example displayed above.

There are five basic relator types r for G_Q and six members t of the transversal T. Therefore there are thirty different types of word trt^{-1} to be rewritten, one of which was discussed above. We give several representative examples, the first in detail:

$$t = \mathsf{e}_1\mathsf{c}_1,\ r = \mathsf{c}_y\mathsf{r}_x\mathsf{c}_y\mathsf{e}_{xy}^{-1}\ :$$

$$\begin{aligned}
\mathsf{e}_1\mathsf{c}_1.\mathsf{c}_y\mathsf{r}_x\mathsf{c}_y\mathsf{e}_{xy}^{-1}.(\mathsf{e}_1\mathsf{c}_1)^{-1} &= \mathsf{e}_1\mathsf{c}_1\mathsf{c}_y(\mathsf{e}_1^{-1}\mathsf{e}_1)\mathsf{r}_x\mathsf{c}_y\mathsf{e}_{xy}^{-1}(\mathsf{e}_1\mathsf{c}_1)^{-1}\\
&= (\mathsf{e}_1\mathsf{c}_1\mathsf{c}_y\mathsf{e}_1^{-1})\,\mathsf{e}_1\mathsf{r}_x\mathsf{c}_y\mathsf{e}_{xy}^{-1}(\mathsf{e}_1\mathsf{c}_1)^{-1}\\
&= P_{\mathsf{c},y}.\mathsf{e}_1\mathsf{r}_x\mathsf{c}_y\mathsf{e}_{xy}^{-1}(\mathsf{e}_1\mathsf{c}_1)^{-1}\\
&= P_{\mathsf{c},y}.\mathsf{e}_1\mathsf{r}_x((\mathsf{e}_1\mathsf{r}_1)^{-1}(\mathsf{e}_1\mathsf{r}_1))\mathsf{c}_y\mathsf{e}_{xy}^{-1}(\mathsf{e}_1\mathsf{c}_1)^{-1}\\
&= P_{\mathsf{c},y}.(\mathsf{e}_1\mathsf{r}_x(\mathsf{e}_1\mathsf{r}_1)^{-1})(\mathsf{e}_1\mathsf{r}_1)\mathsf{c}_y\mathsf{e}_{xy}^{-1}(\mathsf{e}_1\mathsf{c}_1)^{-1}\\
&= P_{\mathsf{c},y}R^{-}_{\mathsf{r},x}.(\mathsf{e}_1\mathsf{r}_1)\mathsf{c}_y\mathsf{e}_{xy}^{-1}(\mathsf{e}_1\mathsf{c}_1)^{-1}\\
&= P_{\mathsf{c},y}R^{-}_{\mathsf{r},x}.(\mathsf{e}_1\mathsf{r}_1)\mathsf{c}_y(\mathsf{r}_1^{-1}\mathsf{r}_1)\mathsf{e}_{xy}^{-1}(\mathsf{e}_1\mathsf{c}_1)^{-1}\\
&= P_{\mathsf{c},y}R^{-}_{\mathsf{r},x}.((\mathsf{e}_1\mathsf{r}_1)\mathsf{c}_y\mathsf{r}_1^{-1})\mathsf{r}_1\mathsf{e}_{xy}^{-1}(\mathsf{e}_1\mathsf{c}_1)^{-1}\\
&= P_{\mathsf{c},y}R^{-}_{\mathsf{r},x}L_{\mathsf{c},y}.\mathsf{r}_1\mathsf{e}_{xy}^{-1}(\mathsf{e}_1\mathsf{c}_1)^{-1}\\
&= P_{\mathsf{c},y}R^{-}_{\mathsf{r},x}L_{\mathsf{c},y}(R^{-}_{\mathsf{e},xy})^{-1}\,;
\end{aligned}$$

$$t = \mathsf{r}_1,\ r = \mathsf{c}_x\mathsf{c}_x\ :$$

$$\begin{aligned}
\mathsf{r}_1.\mathsf{c}_x\mathsf{c}_x.\mathsf{r}_1^{-1} &= \mathsf{r}_1\mathsf{c}_x(\mathsf{e}_1\mathsf{r}_1)^{-1}(\mathsf{e}_1\mathsf{r}_1)\mathsf{c}_x\mathsf{e}_1^{-1}\\
&= L^{-}_{\mathsf{c},x}L_{\mathsf{c},x}\,;
\end{aligned}$$

$$t = \mathsf{e}_1\mathsf{c}_1,\ r = \mathsf{e}_x\mathsf{e}_x\ :$$

$$\begin{aligned}
\mathsf{e}_1\mathsf{c}_1.\mathsf{e}_x\mathsf{e}_x.(\mathsf{e}_1\mathsf{c}_1)^{-1} &= \mathsf{e}_1\mathsf{c}_1\mathsf{e}_x(\mathsf{r}_1^{-1}\mathsf{r}_1)\mathsf{c}_x(\mathsf{e}_1\mathsf{c}_1)^{-1}\\
&= (\mathsf{e}_1\mathsf{c}_1\mathsf{e}_x\mathsf{r}_1^{-1})(\mathsf{r}_1\mathsf{c}_x(\mathsf{e}_1\mathsf{c}_1)^{-1})\\
&= R^{-}_{\mathsf{e},x}R_{\mathsf{e},x}\,;
\end{aligned}$$

$$t = \mathsf{c}_1,\ r = \mathsf{r}_x\mathsf{c}_y\mathsf{r}_x\mathsf{e}_{xy}^{-1}\ :$$

$$\begin{aligned}
\mathsf{c}_1.\mathsf{r}_x\mathsf{c}_y\mathsf{r}_x\mathsf{e}_{xy}^{-1}.\mathsf{c}_1^{-1} &= \mathsf{c}_1\mathsf{r}_x(\mathsf{e}_1\mathsf{c}_1)^{-1}(\mathsf{e}_1\mathsf{c}_1)\mathsf{c}_y(\mathsf{e}_1^{-1}\mathsf{e}_1)\mathsf{r}_x(\mathsf{e}_1\mathsf{r}_1)^{-1}(\mathsf{e}_1\mathsf{r}_1)\mathsf{e}_{xy}^{-1}\mathsf{c}_1^{-1}\\
&= (\mathsf{c}_1\mathsf{r}_x(\mathsf{e}_1\mathsf{c}_1)^{-1})((\mathsf{e}_1\mathsf{c}_1)\mathsf{c}_y\mathsf{e}_1^{-1})(\mathsf{e}_1\mathsf{r}_x(\mathsf{e}_1\mathsf{r}_1)^{-1})(\mathsf{e}_1\mathsf{r}_1)\mathsf{e}_{xy}^{-1}\mathsf{c}_1^{-1}\\
&= L^{-}_{\mathsf{r},x}P_{\mathsf{c},y}R^{-}_{\mathsf{r},x}(P_{\mathsf{e},xy})^{-1}\,.
\end{aligned}$$

Reidermeister-Schreier now gives us a first approximation to Theorem (13.10).

(13.12). PROPOSITION. *The group K_Q has the following presentation:*

Generators:

for arbitrary $x \in Q$:

$R_{\mathsf{r},x},\ R^{-}_{\mathsf{r},x},\ L_{\mathsf{r},x},\ L^{-}_{\mathsf{r},x},\ P_{\mathsf{r},x},\ P^{-}_{\mathsf{r},x}\,,$
$R_{\mathsf{c},x},\ R^{-}_{\mathsf{c},x},\ L_{\mathsf{c},x},\ L^{-}_{\mathsf{c},x},\ P_{\mathsf{c},x},\ P^{-}_{\mathsf{c},x}\,,$
$R_{\mathsf{e},x},\ R^{-}_{\mathsf{e},x},\ L_{\mathsf{e},x},\ L^{-}_{\mathsf{e},x},\ P_{\mathsf{e},x},\ P^{-}_{\mathsf{e},x}\,.$

Relations:

for arbitrary $x, y \in Q$:

(0) *for arbitrary* $\mathsf{a} \in \{\mathsf{r},\mathsf{c},\mathsf{e}\}$ *and* $W \in \{R, L, P\}$,
$W_{\mathsf{a},x}W^{-}_{\mathsf{a},x} = W^{-}_{\mathsf{a},x}W_{\mathsf{a},x} = 1$;

(1) $P_{\mathsf{r},1} = R^{-}_{\mathsf{r},1} = R_{\mathsf{c},1} = P^{-}_{\mathsf{c},1} = L^{-}_{\mathsf{e},1} = 1$;

(2) $P_{\mathsf{r},x}L^{-}_{\mathsf{c},y}R_{\mathsf{r},x}(L^{-}_{\mathsf{e},xy})^{-1} = P^{-}_{\mathsf{r},x}R_{\mathsf{c},y}L^{-}_{\mathsf{r},x}(R_{\mathsf{e},xy})^{-1} =$
$L^{-}_{\mathsf{r},x}P_{\mathsf{c},y}R^{-}_{\mathsf{r},x}(P_{\mathsf{e},xy})^{-1} = R^{-}_{\mathsf{r},x}L_{\mathsf{c},y}P^{-}_{\mathsf{r},x}(L_{\mathsf{e},xy})^{-1} =$
$R_{\mathsf{r},x}P^{-}_{\mathsf{c},y}L_{\mathsf{r},x}(P^{-}_{\mathsf{e},xy})^{-1} = L_{\mathsf{r},x}R^{-}_{\mathsf{c},y}P_{\mathsf{r},x}(R^{-}_{\mathsf{e},xy})^{-1} = 1$;

(3) $R_{\mathsf{c},y}L^{-}_{\mathsf{r},x}P_{\mathsf{c},y}(L^{-}_{\mathsf{e},xy})^{-1} = L^{-}_{\mathsf{c},y}R_{\mathsf{r},x}P^{-}_{\mathsf{c},y}(R_{\mathsf{e},xy})^{-1} =$

$$\begin{gathered}R^-_{\mathsf{c},y}P_{\mathsf{r},x}L^-_{\mathsf{c},y}(P_{\mathsf{e},xy})^{-1} = P^-_{\mathsf{c},y}L_{\mathsf{r},x}R^-_{\mathsf{c},y}(L_{\mathsf{e},xy})^{-1} = \\ L_{\mathsf{c},y}P^-_{\mathsf{r},x}R_{\mathsf{c},y}(P^-_{\mathsf{e},xy})^{-1} = P_{\mathsf{c},y}R^-_{\mathsf{r},x}L_{\mathsf{c},y}(R^-_{\mathsf{e},xy})^{-1} = 1.\end{gathered}$$

PROOF. The generators are those of Proposition (13.11), including those that represent the identity. The relations (1) set those five identity generators to 1.

The eighteen elements $t\mathsf{r}_x\mathsf{r}_xt^{-1}$, $t\mathsf{c}_x\mathsf{c}_xt^{-1}$, and $t\mathsf{e}_x\mathsf{e}_xt^{-1}$ after rewriting become the eighteen relation types of (0), three of these having been discussed above.

The six elements $t\mathsf{r}_x\mathsf{c}_y\mathsf{r}_x\mathsf{e}_{xy}^{-1}t^{-1}$ after rewriting give the six relation types of (2), an example appearing above. Finally the six elements $t\mathsf{c}_y\mathsf{r}_x\mathsf{c}_y\mathsf{e}_{xy}^{-1}t^{-1}$ give the six relation types of (3), one example appearing in detail above. □

We now concern ourselves with simplifying this presentation.

(13.13). LEMMA. *For all $W \in \{R, L, P\}$, all $\mathsf{a} \in \{\mathsf{r}, \mathsf{c}, \mathsf{e}\}$, and all $x \in Q$, we have $W^{-1}_{\mathsf{a},x} = W^-_{\mathsf{a},x}$.*

PROOF. This is immediate from the relations (0) in the proposition. □

(13.14). LEMMA. *For all $W \in \{R, L, P\}$ and all $\mathsf{a} \in \{\mathsf{r}, \mathsf{c}, \mathsf{e}\}$, we have $W_{\mathsf{a},1} = 1$.*

PROOF. By Lemma (13.13) and the relations (1), we have five of the nine desired identities:

$$P_{\mathsf{r},1} = R_{\mathsf{r},1} = R_{\mathsf{c},1} = P_{\mathsf{c},1} = L_{\mathsf{e},1} = 1\,.$$

The relations (2) and (3) then give

$$R^{-1}_{\mathsf{r},1}L_{\mathsf{c},1}P^{-1}_{\mathsf{r},1} = P^{-1}_{\mathsf{c},1}L_{\mathsf{r},1}R^{-1}_{\mathsf{c},1} = L_{\mathsf{e},1} = 1\,,$$

so that $L_{\mathsf{c},1} = L_{\mathsf{r},1} = 1$. Finally by (2)

$$R_{\mathsf{e},1} = P^{-1}_{\mathsf{r},1}R_{\mathsf{c},1}L^{-1}_{\mathsf{r},1} = 1 \quad\text{and}\quad P_{\mathsf{e},1} = L^{-1}_{\mathsf{r},1}P_{\mathsf{c},1}R^{-1}_{\mathsf{r},1} = 1\,. \qquad \square$$

(13.15). LEMMA. *For all $W \in \{R, L, P\}$, all $\mathsf{a}, \mathsf{b} \in \{\mathsf{r}, \mathsf{c}, \mathsf{e}\}$, and all $z \in Q$, we have $W_{\mathsf{a},z} = W_{\mathsf{b},z}$.*

PROOF. By Lemma (13.13) and the relations in (2) and (3), for each W there are appropriate U and V with

$$U^{-1}_{\mathsf{r},x}W_{\mathsf{c},z}V^{-1}_{\mathsf{r},x} = W_{\mathsf{e},xz} \quad\text{and}\quad V^{-1}_{\mathsf{c},y}W_{\mathsf{r},z}U^{-1}_{\mathsf{c},y} = W_{\mathsf{e},zy}\,.$$

By Lemma (13.14), when we set $x = y = 1$ we get

$$W_{\mathsf{c},z} = U^{-1}_{\mathsf{r},1}W_{\mathsf{c},z}V^{-1}_{\mathsf{r},1} = W_{\mathsf{e},z} = V^{-1}_{\mathsf{c},1}W_{\mathsf{r},z}U^{-1}_{\mathsf{c},1} = W_{\mathsf{r},z}\,. \qquad \square$$

PROOF OF THEOREM (13.10). Lemma (13.15) tells us that, for a given $x \in Q$, each of the nine generators $W_{\mathsf{a},x}$ from Proposition (13.12) can be replaced by the corresponding generator W_x from Theorem (13.10). Furthermore the nine generators $W^-_{\mathsf{a},x}$ and the relations (0) of the proposition can be deleted, provided that in the remaining relations we replace each $W^-_{\mathsf{a},x}$ with $W^{-1}_{\mathsf{a},x} = W^{-1}_x$. The list of names preceding Proposition (13.11) then gives the stated correspondence $R_x = \mathsf{r}_x\mathsf{r}_1$, $L_x = \mathsf{e}_1\mathsf{e}_x$, and $P_x = \mathsf{c}_x\mathsf{c}_1$.

The five relations of (1) in the proposition now become the three relations of (1) in the theorem.

After the replacements, the inverse of each of the six relators of (2) from the proposition is a conjugate of a second relator of (2). Taking just one relation from each such pair, we are left with

$$P_x^{-1}R_yL_x^{-1}R_{xy}^{-1} = R_x^{-1}L_yP_x^{-1}L_{xy}^{-1} = L_x^{-1}P_yR_x^{-1}P_{xy}^{-1} = 1\,.$$

These are clearly equivalent to the relations (2) in the theorem.

Similarly the relations (3) in the proposition reduce to

$$L_y^{-1}R_xP_y^{-1}R_{xy}^{-1} = P_y^{-1}L_xR_y^{-1}L_{xy}^{-1} = R_y^{-1}P_xL_y^{-1}P_{xy}^{-1} = 1\,,$$

which are equivalent to those of (3) in the theorem.

By Theorem (13.2) the group K_Q admits the group $I_Q = \langle \mathsf{c}_1, \mathsf{e}_1\rangle \simeq \mathrm{Sym}(3)$ as a triality group of automorphisms. It remains to verify the action of its generators $\sigma = \mathsf{c}_1$ and $\mu = \mathsf{c}_1\mathsf{e}_1$, which we do within G_Q. (This could also be done using the Reidermeister-Schreier process.)

$$\begin{aligned}
R_x^\sigma = R_{\mathsf{c},x}^{\mathsf{c}_1} &= \mathsf{c}_1^{-1}(\mathsf{c}_x\mathsf{c}_1^{-1})\mathsf{c}_1 = \mathsf{c}_1^{-1}\mathsf{c}_x\\
&= (\mathsf{c}_1^2)^{-1}\mathsf{c}_1\mathsf{c}_x = \mathsf{c}_1\mathsf{c}_x\\
&= R_{\mathsf{c},x}^{-} = R_x^{-1}\,;\\
L_x^\sigma = L_{\mathsf{r},x}^{\mathsf{c}_1} &= \mathsf{c}_1^{-1}(\mathsf{e}_1\mathsf{c}_1\mathsf{r}_x\mathsf{c}_1^{-1})\mathsf{c}_1 = \mathsf{c}_1^{-1}\mathsf{e}_1\mathsf{c}_1\mathsf{r}_x\\
&= (\mathsf{c}_1^2)^{-1}\mathsf{c}_1(\mathsf{c}_1\mathsf{r}_1\mathsf{c}_1)\mathsf{c}_1\mathsf{r}_x = \mathsf{r}_1\mathsf{c}_1^2\mathsf{r}_x = \mathsf{r}_1\mathsf{r}_x\\
&= P_{\mathsf{r},x}^{-} = P_x^{-1}\,;\\
R_x^\mu = R_{\mathsf{c},x}^{\mathsf{c}_1\mathsf{e}_1} &= \mathsf{e}_1^{-1}\mathsf{c}_1^{-1}(\mathsf{c}_x\mathsf{c}_1^{-1})\mathsf{c}_1\mathsf{e}_1 = \mathsf{e}_1^{-1}\mathsf{c}_1^{-1}\mathsf{c}_x\mathsf{e}_1\\
&= (\mathsf{e}_1^2)^{-1}\mathsf{e}_1(\mathsf{c}_1^2)^{-1}\mathsf{c}_1\mathsf{c}_x\mathsf{e}_1 = \mathsf{e}_1\mathsf{c}_1\mathsf{c}_x\mathsf{e}_1\\
&= P_{\mathsf{c},x} = P_x\,;\\
P_x^\mu = P_{\mathsf{r},x}^{\mathsf{c}_1\mathsf{e}_1} &= \mathsf{e}_1^{-1}\mathsf{c}_1^{-1}(\mathsf{r}_x\mathsf{r}_1^{-1})\mathsf{c}_1\mathsf{e}_1\\
&= \mathsf{e}_1(\mathsf{e}_1^2)^{-1}(\mathsf{c}_1^2)^{-1}\mathsf{c}_1\mathsf{r}_x\mathsf{c}_1^2\mathsf{r}_1(\mathsf{r}_1^2)^{-1}\mathsf{c}_1\mathsf{e}_1\\
&= \mathsf{e}_1(\mathsf{c}_1\mathsf{r}_x\mathsf{c}_1)(\mathsf{c}_1\mathsf{r}_1\mathsf{c}_1)\mathsf{e}_1 = \mathsf{e}_1\mathsf{e}_x\mathsf{e}_1\mathsf{e}_1 = \mathsf{e}_1\mathsf{e}_x\\
&= L_{\mathsf{c},x} = L_x\,.
\end{aligned}$$

It remains to prove $K_Q = [K_Q, \langle\sigma,\mu\rangle]$. First note that with $x = 1$ the identity $L_y^{-1}R_xP_y^{-1}R_{xy}^{-1} = 1$ yields $L_y^{-1}P_y^{-1} = R_y$. This implies

$$[L_x, \sigma] = L_x^{-1}L_x^\sigma = L_x^{-1}P_x^{-1} = R_x\,.$$

Therefore $[K_Q, \langle\sigma,\mu\rangle]$ contains R_x and so also $R_x^\mu = P_x$ and $P_x^\mu = L_x$, for all $x \in Q$, a full set of generators for K_Q. □

Some useful identities are a consequence.

(13.16). PROPOSITION. *In K_Q we have the following, for all $\{U, V, W\} = \{R, L, P\}$ and $x, y \in Q$.*

(a) $U_xV_xW_x = 1$, *and in particular* $U_xV_x = V_xU_x = W_x^{-1}$.
(b) $W_{x^{-1}} = W_x^{-1} = W_{^{-1}x}$.
(c) $W_{xy}^{-1} = W_{y^{-1}x^{-1}}$.
(d) $W_xW_yW_x = W_{(xy)x} = W_{x(yx)}$.

PROOF. (a) Either $U_xV_{xy}W_x = V_y$ or $U_xV_{yx}W_x = V_y$, and in both cases $y = 1$ gives the identity.

(b) Choose U and V so that

$$U_x W_{xy} V_x = W_y \quad \text{and} \quad V_x W_{zx} U_x = W_z \,.$$

With $y = {}^{-1}x$ and $z = x^{-1}$, the previous part gives

$$W_x^{-1} = U_x V_x = W_{{}^{-1}x} \quad \text{and} \quad W_x^{-1} = V_x U_x = W_{x^{-1}} \,.$$

(c) From $U_x W_{xy} V_x = W_y$ and $V_z W_{vz} U_z = W_v$ we find first

$$W_{xy} = U_x^{-1} W_y V_x^{-1} \quad \text{and} \quad W_{vz} = V_z^{-1} W_v U_z^{-1} \,,$$

then next

$$\begin{aligned} W_{xy}^{-1} &= (U_x^{-1} W_y V_x^{-1})^{-1} = V_x W_y^{-1} U_x \\ &= V_{x^{-1}}^{-1} W_{y^{-1}} U_{x^{-1}}^{-1} = W_{y^{-1}x^{-1}} \,. \end{aligned}$$

(d) Again assume $U_x W_{xy} V_x = W_y$ so that

$$W_x W_y W_x = W_x U_x W_{xy} V_x W_x = V_x^{-1} W_{xy} U_x^{-1} = W_{(xy)x} \,,$$

where we have used the first part of the lemma and an identity from the proof of the previous part. The rest of this part follows from a similar argument. □

13.3. Equivalent presentations

We give several presentations for K_Q. The presentation (I) is that of Theorem (13.10). The presentation (II) is essentially Doro's presentation; see Theorem (13.9). The presentation (III) is shorter than the others, a property that might be helpful in applications.

(13.17). THEOREM. *Let Q be a loop. Consider the group K with the following presentation:*

Generators:

R_x, L_x, and P_x for arbitrary $x \in Q$;

Relations:

(1) $R_1 = L_1 = P_1 = 1$.

Then each of the following additional sets of relations gives the same quotient of K, namely the kernel K_Q of π_Q:

(I) *for arbitrary $x, y \in Q$,*

(2) $P_x R_{xy} L_x = R_y$; $R_x L_{xy} P_x = L_y$; $L_x P_{xy} R_x = P_y$.

(3) $L_y R_{xy} P_y = R_x$; $P_y L_{xy} R_y = L_x$; $R_y P_{xy} L_y = P_x$.

(II) *for arbitrary $x, y \in Q$,*

(4) $P_x R_y L_x = R_{(x^{-1})y}$; $R_x L_y P_x = L_{(x^{-1})y}$; $L_x P_y R_x = P_{(x^{-1})y}$.

(5) $L_y R_x P_y = R_{x({}^{-1}y)}$; $P_y L_x R_y = L_{x({}^{-1}y)}$; $R_y P_x L_y = P_{x({}^{-1}y)}$.

(III) *for arbitrary $x, y \in Q$,*

(2) $P_x R_{xy} L_x = R_y$; $R_x L_{xy} P_x = L_y$; $L_x P_{xy} R_x = P_y$.

(8) $R_{xy}^{-1} = R_{y^{-1}x^{-1}}$; $L_{xy}^{-1} = L_{y^{-1}x^{-1}}$; $P_{xy}^{-1} = P_{y^{-1}x^{-1}}$.

There are many other related and equivalent sets of relations. In (III) the relation set (2) could be replaced by any one of (3), (4), or (5). Also since the subscripts of (8) contain six left inverses, each of which might be replaced by a right inverse, there are 64 variants of (8) which could be considered. The theorem remains true with any of these in place of (8); see Remark (13.22).

By substituting $y = 1$ into (8) we get

(9) for all $x \in Q$, $R_x^{-1} = R_{x^{-1}}$, $L_x^{-1} = L_{x^{-1}}$, $P_x^{-1} = P_{x^{-1}}$.

There are three left inverses in the subscripts of (9), so it has eight variants, all valid within K_Q by Proposition (13.16). (In fact it is not hard to prove that any one of the eight variants implies all of the others; see the proof of Lemma (13.19) below.)

(13.18). LEMMA. *Let N be a quotient group of K that additionally satisfies* (4) *and* (5) *for all $x, y \in Q$. Then* (9) *holds within N.*

PROOF. For each W, we may choose U and V so that in N

$$U_x W_y V_x = W_{(x^{-1})y} \quad \text{and} \quad U_x V_y W_x = V_{y({}^{-1}x)} \, .$$

In the first $y = 1$ gives $U_x V_x = W_{x^{-1}}$, and in the second $y = x$ gives $U_x V_x = W_x^{-1}$. □

(13.19). LEMMA. *Let N be a quotient group of K that additionally satisfies* (9)*. Then within N:*

(a) (2) *holds for all $x, y \in Q$ if and only if* (4) *holds for all $x, y \in Q$.*
(b) (3) *holds for all $x, y \in Q$ if and only if* (5) *holds for all $x, y \in Q$.*

PROOF. Set $z = {}^{-1}x$ so that $x = z^{-1}$. Then $U_x = U_{z^{-1}} = U_z^{-1} = U_{{}^{-1}x}^{-1}$; that is, $U_x^{-1} = U_{{}^{-1}x}$ and similarly $V_x^{-1} = V_{{}^{-1}x}$. Thus

$$\begin{aligned} W_y = U_x W_{xy} V_x &\iff U_x^{-1} W_y V_x^{-1} = W_{xy} \\ &\iff U_{{}^{-1}x} W_y V_{{}^{-1}x} = W_{xy} \iff U_z W_y V_z = W_{(z^{-1})y} \, . \end{aligned}$$

Therefore, given (9), we have (2) if and only if we have (4). The other case is similar. □

(13.20). LEMMA. *Let N be a quotient group of K that additionally satisfies* (8)*. Then* (2) *holds for all $x, y \in Q$ if and only if* (3) *holds for all $x, y \in Q$.*

PROOF. As (8) implies (9) we have

$$P_x R_{xy} L_x = R_y \iff L_x^{-1} R_{xy}^{-1} P_x^{-1} = R_y^{-1} \iff L_{x^{-1}} R_{y^{-1}x^{-1}} P_{x^{-1}} = R_{y^{-1}} \, .$$

Therefore the first relation in (2) holds for all $x, y \in Q$ if and only if the first relation in (3) holds for all $x, y \in Q$, and the other two cases are similar. □

PROOF OF THEOREM (13.17). By Proposition (13.16)(b) and Lemma (13.18), the relations (9) hold under both (I) and (II). Therefore (I) and (II) are equivalent by Lemma (13.19), Next (I) implies (III) by Proposition (13.16)(c), and (III) imples (I) by Lemma (13.20). □

(13.21). LEMMA. *Let N be a quotient group of K that additionally satisfies* (2) *or* (3)*. Then the equivalence relation*

$$x \sim y \iff R_x = R_y \, , L_x = L_y \, , \text{ and } P_x = P_y \, .$$

is a congruence on Q.

PROOF. Assume that (2) holds in N, the case (3) being similar. Thus for each W there are appropriate choices for U and V with $U_x W_{xy} V_x = W_x$ or, equivalently, $W_{xy} = U_x^{-1} W_y V_x^{-1}$. Therefore when $x_1 \sim x_2$ and $y_1 \sim y_2$, we have

$$W_{x_1 y_1} = U_{x_1}^{-1} W_{y_1} V_{x_1}^{-1} = U_{x_2}^{-1} W_{y_2} V_{x_2}^{-1} = W_{x_2 y_2} \, . \square$$

(13.22). Remark. *The lemma leads to a proof that in Theorem (13.17) we could replace the relations* (2) *and* (3) *of* (I) *for* K_Q *by any one of* (2)-(5) *together with any one of the* 64 *variants of* (8). *Indeed, each of these variants has* (9) *(and all its eight variants) as a consequence, therefore by Lemma (13.19) we only need consider the variant together with* (2) *or* (3). *But then the lemma together with all variants of* (9) *gives all variants of* (8), *in particular* (8) *itself. This and Lemma (13.20) now show that the new pair is equivalent to the pair* (2) *and* (8) *of* (III) *and so to* (2) *and* (3) *of* (I).

13.4. Moufang loops

Most of Theorem (13.9) follows directly from Theorem (13.10) and material from the previous section. What is new is the last assertion that, for the Moufang loop Q, the maps $x \mapsto W_x$ are bijections. That came naturally for Doro, since he designed his presentation with a certain image in mind, namely the multiplication group $\mathrm{Mlt}(Q)$. Indeed the properties of the multiplication group such as those we found in Proposition (13.16) provided the motivation for Doro's presentation.

(13.23). Proposition. *Let Q be a Moufang loop. Then the map given by*

$$R_x \mapsto \mathrm{R}(x)\,, \quad L_x \mapsto \mathrm{L}(x)\,, \quad P_x \mapsto \mathrm{R}(x)^{-1}\,\mathrm{L}(x)^{-1}$$

extends to a homomorphism from K_Q *onto* $\mathrm{Mlt}(Q)$.

Proof. Doro used the properties of the translation maps corresponding to the relations of Theorem (13.9) as motivation for his presentation. We instead verify that the images of the relation sets

(1) $R_1 = L_1 = P_1 = 1$;
(2) $P_x R_{xy} L_x = R_y$; $R_x L_{xy} P_x = L_y$; $L_x P_{xy} R_x = P_y$;
(3) $L_y R_{xy} P_y = R_x$; $P_y L_{xy} R_y = L_x$; $R_y P_{xy} L_y = P_x$.

of Theorem (13.10) are valid in $\mathrm{Mlt}(Q)$.

The translation maps $\mathrm{R}(1)$ and $\mathrm{L}(1)$ are the identity permutation of Q as is $\mathrm{P}(1) = \mathrm{R}(1)^{-1}\,\mathrm{L}(1)^{-1}$. Thus the relations of (1) are taken to relations of $\mathrm{Mlt}(Q)$. The relations of (2) are mapped to the three identities of Proposition (12.4)(a), while those of (3) are mapped to the identities of Proposition (12.4)(b) (with x and y switched). □

Proof of Theorem (13.9). By Theorem (13.17), the relations (1), (4), and (5) of Theorem (13.9) are equivalent to the relations (1), (2), and (3) of Theorem (13.10), and so by that theorem they present K_Q. Furthermore the additional relations (6) and (7) are consequences of the relations of the previous sentence by Proposition (13.16)(a,d). The action of I_Q is that of Theorem (13.10) as is the form of the generators.

It remains to prove bijectivity for the thee maps $x \mapsto W_x$. For an arbitrary loop Q, the map $\mathrm{R}(x)$ takes 1 to x; so for distinct x and y in Q, the right translations $\mathrm{R}(x)$ and $\mathrm{R}(y)$ are distinct permutations of Q. That is, the map $x \mapsto \mathrm{R}(x)$ is a bijection. By the proposition, for Moufang Q the bijection $x \mapsto \mathrm{R}(x)$ factors through the map $x \mapsto R_x$, which is therefore also a bijection. The action of μ now guarantees that all three of the maps $x \mapsto W_x$ are bijections, as required.

A second proof of bijectivity comes from

$$x \mapsto \mathsf{c}_x \mapsto \mathsf{c}_x \mathsf{c}_1 = R_x\,,\ x \mapsto \mathsf{e}_x \mapsto \mathsf{e}_1 \mathsf{e}_x = L_x\,,\ x \mapsto \mathsf{r}_x \mapsto \mathsf{r}_x \mathsf{r}_1 = P_x$$

being bijections by Theorem (11.3). □

Doro's argument [**Dor78**, p. 384] for bijectivity of the maps $x \mapsto W_x$ is misleading. He focused on the maps $\mathrm{P}(x) = \mathrm{R}(x)^{-1}\,\mathrm{L}(x)^{-1}$ and ultimately asserted that $x \mapsto P_x$ is a bijection. As we have seen, this is true. But it is not as immediate as the corresponding statement for $x \mapsto R_x$ (or $x \mapsto L_x$), since there are Moufang loops (for instance, elementary abelian 2-groups) for which the map $x \mapsto \mathrm{P}(x)$ is not a bijection even though $x \mapsto P_x$ is.[1]

The next two results show that the bijectivity of the maps $x \mapsto W_x$ in Theorem (13.10) characterizes Q as a Moufang loop.

(13.24). Proposition. *Let Q be a loop, and let K_Q be the kernel of the map π_Q, as presented in Theorem (13.10). Let $W \in \{R, L, P\}$. Then $W_{(xy)(zx)} = W_{(x(yz))x}$ in K_Q, for all $x, y, z \in Q$.*

Proof. We only prove this for $W = R$, the other cases then following from the action of μ. In our verification, we use freely the various parts of Proposition (13.16), particularly $W_{x^{-1}} = W_x^{-1}$. We also use various identities such as $U_z W_{zv} V_z = W_v$, sometimes in the form $W_{zv} = U_{z^{-1}} W_v V_{z^{-1}}$.

$$\begin{aligned}
R_{(xy)(zx)} &= P_{xy}^{-1} R_{zx} L_{xy}^{-1} \\
&= P_{y^{-1}x^{-1}} R_{zx} L_{y^{-1}x^{-1}} \\
&= (L_y P_{x^{-1}} R_y) P_{z^{-1}} R_x L_{z^{-1}} (R_y L_{x^{-1}} P_y) \\
&= R_x (R_{x^{-1}} L_y P_{x^{-1}}) R_y P_{z^{-1}} R_x L_{z^{-1}} R_y (L_{x^{-1}} P_y R_{x^{-1}}) R_x \\
&= R_x L_{xy} R_y P_{z^{-1}} R_x L_{z^{-1}} R_y P_{xy} R_x \\
&= R_x P_{y^{-1}} (P_y L_{xy} R_y) P_{z^{-1}} R_x L_{z^{-1}} (R_y P_{xy} L_y) L_{y^{-1}} R_x \\
&= R_x P_{y^{-1}} L_x P_{z^{-1}} R_x L_{z^{-1}} P_x (R_{z^{-1}} R_z) L_{y^{-1}} R_x \\
&= R_x P_{y^{-1}} (L_x P_{z^{-1}} R_x)(L_{z^{-1}} P_x R_{z^{-1}}) R_z L_{y^{-1}} R_x \\
&= R_x P_{y^{-1}} P_{x^{-1}z^{-1}} P_{zx} R_z L_{y^{-1}} R_x \\
&= R_x (P_{y^{-1}} R_z L_{y^{-1}}) R_x \\
&= R_x R_{yz} R_x \\
&= R_{(x(yz))x} \qquad \square
\end{aligned}$$

(13.25). Theorem. *Let Q be a loop, and let K_Q be the kernel of the map π_Q, as presented in Theorem (13.10). For $x, y \in Q$ we have*

$$R_x = R_y \iff L_x = L_y \iff P_x = P_y\,.$$

In this case we write $x \sim y$. The equivalence relation $\sim$ is a congruence on the loop Q, and $Q/{\sim}$ is the largest Moufang quotient of Q.

Proof. The action of μ guarantees that for $x, y \in Q$ we have

$$R_x = R_y \iff L_x = L_y \iff P_x = P_y\,.$$

Let $\sim$ be the associated equivalence relation. By Lemma (13.21) the relation $\sim$ is in fact a congruence on Q. By Proposition (13.23) the largest Moufang quotient of

[1] Thanks go to Petr Vojtěchovský for pointing out the possible confusion.

Q is a quotient of $Q/\sim$. On the other hand, by Proposition (13.24) the quotient $Q/\sim$ is itself a Moufang loop. □

Chapter 14

Normal Structure

A primary motivation for this work was the wish to formalize the relationships between the normal structure of Moufang loops and of groups with triality, particular simplicity in each class.

14.1. Simplicity

Recall from Chapter 2 that the subloop M of the loop Q is normal if there is a loop homomorphism with kernel M and that the nonidentity loop Q is simple if its only normal subloops are the identity and itself. Also, from Chapter 1, a nonterminal object in a category is simple if every morphism from it is either monic or trivial.

(14.1). THEOREM. *Let Q be a Moufang loop. The following are equivalent:*

(1) *Q is simple.*
(2) *Q is simple in* Mouf.
(3) *Q is simple in* $\mathsf{Mouf}^\star$.

PROOF. (1) $\Longrightarrow$ (2): Let Q be simple and consider $f \in \mathrm{Hom}_{\mathsf{Mouf}}(Q, A)$. By Lemma (2.5) there is a B and an isomorphism $i \in \mathrm{Hom}_{\mathsf{Mouf}}(A, B)$ with $fi \in \mathrm{Hom}_{\mathsf{Mouf}^\star}(Q, B)$. By simplicity of Q the kernel of fi is 1_Q or Q. If $\ker fi = 1_Q$, then $g = fi$ is injective hence monic, and so $f = gi^{-1}$ is also monic. If $\ker fi = Q$, then for the zero object $O = \{1\}$ of $\mathsf{Mouf}^\star$, we have $fi = eo$ where $\{e\} = \mathrm{Hom}_{\mathsf{Mouf}^\star}(Q, O) \subseteq \mathrm{Hom}_{\mathsf{Mouf}}(Q, O)$ and $\{f\} = \mathrm{Hom}_{\mathsf{Mouf}^\star}(O, B) \subseteq \mathrm{Hom}_{\mathsf{Mouf}}(O, B)$. Thus $f = eoi^{-1}$ factors through the terminal object O of Mouf.

(2) $\Longrightarrow$ (3): The category $\mathsf{Mouf}^\star$ is a subcategory of Mouf with the same object class and same terminal objects. Monic morphisms in Mouf remain monic in $\mathsf{Mouf}^\star$. Thus an object that is simple in Mouf remains simple in $\mathsf{Mouf}^\star$.

(3) $\Longrightarrow$ (1): Suppose Q is simple in $\mathsf{Mouf}^\star$, and let $f\colon Q \longrightarrow M$ be a loop homomorphism. Then $f \in \mathrm{Hom}_{\mathsf{Mouf}^\star}(Q, M)$, so f is either trivial or monic. If f is trivial, then it factors $f = eo$ where $\{e\} = \mathrm{Hom}_{\mathsf{Mouf}^\star}(Q, O)$ and $\{o\} = \mathrm{Hom}_{\mathsf{Mouf}^\star}(O, M)$ for O a zero object in $\mathsf{Mouf}^\star$. Thus $\ker f = \ker e = Q$. On the other hand, if f is monic, then it is injective by Theorem (8.4) and so $\ker f = 1_Q$. Therefore the only

kernels of loop homomorphisms from Q are Q and 1_Q, and Q is a simple Moufang loop. □

The group with triality (G, D, π) or (G, D, π, I) is terminal precisely when G is isomorphic to $\mathrm{Sym}(3)$. We say that the group with triality (G, D, π) or (G, D, π, I) with $G \not\simeq \mathrm{Sym}(3)$ is *triality quasisimple* provided the only normal subgroups of G properly contained in $\ker \pi$ are the subgroups of $\mathrm{Z}(G)$. It is further *triality simple* provided the only normal subgroup of G properly contained in $\ker \pi$ is the identity; that is, it is triality simple provided it is triality quasisimple and has trivial center.

(14.2). THEOREM. *A triality group is simple in* TriGrp *if and only if it is triality quasisimple.*

PROOF. For the group (G, D, π) to be simple in TriGrp, all morphisms from it are either monic or trivial. A morphism is trivial when it factors through a terminal object, so as loop homomorphism it has image a copy of $\mathrm{Sym}(3)$ and kernel equal to $\ker \pi$. By Proposition (6.2) a morphism is monic precisely when as a loop homomorphism it has central kernel. Therefore nonterminal (G, D, π) is simple in TriGrp if and only if all the normal subgroups of G contained properly in $\ker \pi$ are central; that is, when (G, D, π) is triality quasisimple. □

(14.3). THEOREM. *Let (G, D, π, I) be a group with triality. The following are equivalent:*

(1) *(G, D, π) is triality quasisimple.*
(2) *(G, D, π) is simple in* TriGrp.
(3) *(G, D, π, I) is triality quasisimple.*
(4) *(G, D, π, I) is simple in* $\mathsf{TriGrp}^\star$.
(5) *$(G, D, \pi)\mathbf{U}$ is triality quasisimple.*
(6) *$(G, D, \pi)\mathbf{U}$ is simple in* $\mathsf{UTriGrp}$.
(7) *$(G, D, \pi, I)\mathbf{U}^\star$ is triality quasisimple.*
(8) *$(G, D, \pi, I)\mathbf{U}^\star$ is simple in* $\mathsf{UTriGrp}^\star$.
(9) *$(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$ is triality simple.*
(10) *$(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$ is simple in* $\mathsf{ATriGrp}$.
(11) *$(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}}, I^{\mathrm{A}})$ is triality simple.*
(12) *$(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}}, I^{\mathrm{A}})$ is simple in* $\mathsf{ATriGrp}^\star$.

PROOF. The previous theorem gives: (1) $\Longleftrightarrow$ (2). The remaining equivalences follow from elementary observations:

(i) The definitions of triality quasisimplicity and simplicity for (G, D, π, I) make no reference to I. Therefore (1) $\Longleftrightarrow$ (3), (5) $\Longleftrightarrow$ (7), (9) $\Longleftrightarrow$ (11).
(ii) By Lemma (4.12)(c),(e) triality quasisimplicity is an isogeny invariant, and only the adjoint group has trivial center. Therefore (1) $\Longleftrightarrow$ (5), (1) $\Longleftrightarrow$ (9).
(iii) For the category C from $\{\mathsf{TriGrp}, \mathsf{UTriGrp}, \mathsf{ATriGrp}\}$ and an object (G, D, π) of C that contains the line I, the forgetful functor between $\mathsf{C}^\star$ and C preserves terminal objects—(G, D, π) is terminal if and only if $G \simeq \mathrm{Sym}(3)$ if and only if (G, D, π, I) is terminal. Furthermore we have noted in Section 1.4 that

$$\mathrm{Hom}_{\mathsf{C}}((G, D, \pi), (G_0, D_0, \pi_0))$$

is the disjoint union over the lines I_0 of (G_0, D_0, π_0) of the sets

$$\mathrm{Hom}_{\mathsf{C}^\star}((G, D, \pi, I), (G_0, D_0, \pi_0, I_0))\,.$$

By Propositions (6.2), (7.14), and (7.15) the monic morphisms in these sets are those that induce injections of D into D_0. Therefore the original set is composed entirely of trivial morphisms (ones that factor through terminal objects) and monic morphisms if and only if the the same is true of each of the sets in the disjoint union. Thus (G, D, π) is simple in C if and only if (G, D, π, I) is simple in $\mathsf{C}^\star$. This gives (2) $\Longleftrightarrow$ (4), (6) $\Longleftrightarrow$ (8), (10) $\Longleftrightarrow$ (12).

(iv) So far we have three connected components under the relation $\Longleftrightarrow$, namely (6) $\Longleftrightarrow$ (8), (10) $\Longleftrightarrow$ (12), and the rest. To complete the connection and the theorem we add two further equivalent statements:

(5.5) $(G, D, \pi)\mathbf{U}$ *is simple in* TriGrp.

(9.5) $(G^{\mathrm{A}}, D^{\mathrm{A}}, \pi^{\mathrm{A}})$ *is simple in* TriGrp.

Since we have already proven (1) $\Longleftrightarrow$ (2) we have (5) $\Longleftrightarrow$ (5.5) and (9) $\Longleftrightarrow$ (9.5) immediately. To show (5.5) $\Longleftrightarrow$ (6) and (9.5) $\Longleftrightarrow$ (10), and thereby complete our proof of the theorem, we must observe that the objects (G, D, π) of $\mathsf{UTriGrp}$ and $\mathsf{ATriGrp}$ that are simple are exactly those that are already simple within TriGrp. But this is clear since the terminal objects of the three categories coincide, and by Propositions (6.2), (7.14), and (7.15) the monic morphisms from (G, D, π) in each category are precisely those that are injective on D. □

We now have a categorical proof of one of Doro's basic results.

(14.4). Theorem. (Doro [**Dor78**, Corollary 2.2]) *The Moufang loop Q is simple if and only if* $\mathrm{TAtp}(Q) = \mathrm{G}_Q/\mathrm{Z}(\mathrm{G}_Q)$ *is triality simple.*

Proof. By Theorem (14.1) the Moufang loop Q is simple as a loop if and only if it is simple in $\mathsf{Mouf}^\star$. Proposition (1.12) then says that this is the case if and only if $Q\mathbf{G}^\star$ is simple in $\mathsf{UTriGrp}^\star$. By Theorem (14.3) this is true if and only if $\mathrm{TAtp}(Q) = \mathrm{G}_Q/\mathrm{Z}(\mathrm{G}_Q)$ is triality simple. □

(14.5). Theorem. (Doro [**Dor78**], Nagy and Valsecchi [**NVa04**]) *Let (G, D, π, I) be triality simple. Set $M = (G, D, \pi, I)\mathbf{M}^\star$. Then exactly one of:*

(1) $G \simeq (Z_3 \times Z_3) \rtimes Z_2$ *and M is a cyclic group of order* 3.

(2) $G \simeq \mathrm{W}_p(\widetilde{A}_2) \simeq Z_p^2 \rtimes \mathrm{Sym}(3)$*, and M is a cyclic group of order p, a prime not equal to* 3.

(3) $\ker \pi$ *is a nonabelian simple group, and M is nonabelian, nonassociative, and simple.*

(4) *G is isomorphic to the wreath product $M \wr \mathrm{Sym}(3)$ of Section 4.2.1, and M is a nonabelian simple group,*

Proof. We only sketch the proof. Set $K = \ker \pi$. Then either K is a finite elementary abelian p-group (for some prime p) or K is the direct product of $k \in \{1, 2, 3, 6\}$ copies of a nonabelian simple group H permuted transitively by I under conjugation. (For finite G this is immediate as K is characteristically simple; for arbitrary G this comes from elementary arguments—see [**NVo03**].)

If K is abelian, then by Proposition (4.8)(b) the triality simple group G is $\mathrm{W}_p(\widetilde{A}_2)/\mathrm{Z}(\mathrm{W}_p(\widetilde{A}_2))$ for some prime p. This and Lemma (4.9) give (1) and (2).

Doro gave short and elementary proofs that $k = 6$ cannot occur (also a consequence of Proposition (4.8)(b) and that $k = 3$ leads to (4). The case $k = 1$ is then (3).

Doro also gave a complicated argument proving that $k = 2$ cannot occur for finite nonabelian simple H. Later Nagy and Valsecchi gave an elementary proof that $k = 2$ gives a contradiction for arbitrary nonabelian simple H. □

The following elegant consequence may be well-known, but we have been unable to find it in the literature. See [**NVa04**, Theorem 4.3] for the forward direction.

(14.6). Corollary. *Let M be a Moufang loop. Then M is nonassociative and simple if and only if* $\mathrm{Mlt}(M)$ *is nonabelian and simple.*

Proof. For M a nonassociative simple Moufang loop, $\mathrm{SAtp}(M)\,(=\ker\pi)$ is nonabelian simple by the previous two theorem. But $\mathrm{Mlt}(M)$ is an image of $\mathrm{SAtp}(M)$ by Proposition (12.11).

For the converse, assume that $H = \mathrm{Mlt}(M)$ is a nonabelian simple group. By Theorem (12.15) either H equals $\mathrm{SAtp}(M)$ or $\mathrm{SAtp}(M)$ contains the two normal subgroups $H_1 = \{\, (\mathrm{Id}, h, h) \mid h \in H \,\}$ and $H_2 = \{\, (h, \mathrm{Id}, h) \mid h \in H \,\}$, both isomorphic to H. But in that case $[H_1, H_2] = \{\, (\mathrm{Id}, \mathrm{Id}, h) \mid h \in H \,\}$ is also isomorphic to H within $\mathrm{Atp}(M)$, a clear contradiction.

We conclude that if $\mathrm{Mlt}(M)$ is nonabelian simple, then $\mathrm{TAtp}(M)$ is triality simple. In the first two cases of the theorem M is an abelian group, so $\mathrm{Mlt}(M)$ is also abelian by Proposition (12.1). In the last case of the theorem M itself is a nonabelian simple group. But there $\mathrm{Mlt}(M)$ is isomorphic to $M \times M$, being the product of the left-regular and right-regular permutation representations of M.

We are left with case (3) of the theorem, and M is a nonassociative simple Moufang loop. □

14.2. Short exact sequences

In many contexts a version of the fundamental First Isomorphism Theorem reveals the image of a homomorphism as canonically isomorphic to a quotient by its kernel. This is unavailable in arbitrary categories, but here we are able to use kernel morphisms in $\mathsf{Mouf}^\star$ and $\mathsf{TriGrp}^\star$ effectively to relate short exact sequences of Moufang loops and images of groups with triality.

(14.7). Theorem. *Let*

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\alpha"] & Q \arrow[r, "\delta"] & M \arrow[r] & 1 \end{tikzcd}$$

be a short exact sequence of Moufang loops. Then we have a short exact sequence of groups

$$\begin{tikzcd} 1 \arrow[r] & K_{N,Q} \arrow[r, "\alpha'"] & \mathrm{G}_Q \arrow[r, "\delta'"] & \mathrm{G}_M \arrow[r] & 1 \end{tikzcd}$$

where $\delta' = \delta\mathbf{G}^\star$ is a morphism of groups with triality that has kernel (as group homomorphism) $K_{N,Q} = \langle K_0^{\mathrm{G}_Q}\rangle = \langle K_0^{K_Q}\rangle$ for $K_0 = [K_{N,Q}, I_Q]$, a central quotient of K_N, the kernel of π_N on G_N.

Proof. Apply the functor $\mathbf{G}^\star$ to the given exact sequence in $\mathsf{Mouf}^\star$ to find the following sequence in $\mathsf{UTriGrp}^\star$:

$$\begin{tikzcd} \mathrm{Sym}(3) \arrow[r] & \mathrm{G}_N \arrow[r, "\alpha^\star"] & \mathrm{G}_Q \arrow[r, "\delta^\star"] & \mathrm{G}_M \arrow[r] & \mathrm{Sym}(3)\,. \end{tikzcd}$$

Here the first morphism can be taken to be the injection of I_N into G_N and the last to be projection onto I_M.

As the original loop sequence is exact, any two consecutive morphisms in it have trivial composition. This is respected by $\mathbf{G}^\star$. In particular, $\alpha^\star\delta^\star$ is a trivial morphism from G_N to G_M. The morphism α is injective hence monic in $\mathsf{Mouf}^\star$ by Theorem (8.4), therefore $\alpha^\star$ is monic; and so at the group level its kernel is central by Proposition (6.2). Similarly surjective δ is $\mathbb{Z}$-surjective by Proposition (9.9), thus $\delta^\star$ is $\mathbb{Z}$-surjective hence surjective by Proposition (9.11). (See also Lemma (11.2).)

The map $\alpha\colon N \longrightarrow Q$ is a kernel morphism for $\delta\colon Q \longrightarrow M$ in $\mathsf{Mouf}^\star$ by Lemma (2.10). Therefore $\alpha^\star\colon \mathrm{G}_N \longrightarrow \mathrm{G}_Q$ is a kernel morphism for $\delta^\star\colon \mathrm{G}_Q \longrightarrow \mathrm{G}_M$ in $\mathsf{UTriGrp}^\star$. That is, for every $\gamma^\star\colon G \longrightarrow \mathrm{G}_Q$ with $\gamma^\star\delta^\star$ trivial, there is a unique $\gamma^\star_{\alpha^\star}\colon G \longrightarrow \mathrm{G}_N$ with $\gamma^\star = \gamma^\star_{\alpha^\star}\alpha^\star$:

$$\begin{tikzcd}
G \arrow[d, dashed, "\gamma^\star_{\alpha^\star}"'] \arrow[dr, "\gamma^\star"] & & \\
\mathrm{G}_N \arrow[r, "\alpha^\star"] & \mathrm{G}_Q \arrow[r, "\delta^\star"] & \mathrm{G}_M
\end{tikzcd}$$

Set $\delta' = \delta^\star$, and let the short exact sequence of groups

$$\begin{tikzcd}
1 \arrow[r] & K_{N,Q} \arrow[r, "\alpha'"] & \mathrm{G}_Q \arrow[r, "\delta'"] & \mathrm{G}_M \arrow[r] & 1
\end{tikzcd}$$

define the normal subgroup $K_{N,Q}$ of G_Q. As $\delta^\star$ is a morphism, $K_{N,Q} \leq \ker \pi_Q$.

Set $G_0 = \langle I_Q^{K_{N,Q}} \rangle$, so that (G_0, D_0, π_0, I_Q) is a group with triality for $D_0 = D_Q \cap G_0$ and π_0 the restriction of π_Q to G_0. The injection $\gamma\colon G_0 \longrightarrow \mathrm{G}_Q$ is in particular monic. As $G_0 = \langle I_Q^{K_{N,Q}} \rangle = [K_{N,Q}, I_Q]I_Q$ and $\ker \pi_0 \geq G_0 \cap K_{N,Q}$, we have $\ker \pi_0 = [K_{N,Q}, I_Q] = K_0$.

Consider the universal group with triality G_0^{U} and the corresponding map $\gamma^{\mathrm{U}}\colon G_0^{\mathrm{U}} \longrightarrow \mathrm{G}_Q$, monic because its kernel is central in G_0^{U}. As $\gamma\delta^\star$ is trivial, so is $\gamma^{\mathrm{U}}\delta^\star$. Therefore as above there is a unique map $\beta = \gamma^{\mathrm{U}}_{\alpha^\star}$ with $\gamma^{\mathrm{U}} = \gamma^{\mathrm{U}}_{\alpha^\star}\alpha^\star = \beta\alpha^\star$, where, since γ^{U} is monic, its initial factor β is also monic. (See the exercise on page 3.)

$$\begin{tikzcd}
G_0^{\mathrm{U}} \arrow[d, dashed, "\beta=\gamma^{\mathrm{U}}_{\alpha^\star}"'] \arrow[dr, "\gamma^{\mathrm{U}}"] & & \\
\mathrm{G}_N \arrow[r, "\alpha^\star"] & \mathrm{G}_Q \arrow[r, "\delta^\star"] & \mathrm{G}_M
\end{tikzcd}$$

Let G_1 be the image of G_N under $\alpha^\star$. As $\alpha^\star\delta^\star$ is trivial, the triality group G_1 is contained in G_0. We let ι be the corresponding injection. Then we have most of the diagram

$$\begin{tikzcd}
\mathrm{G}_N \arrow[d, "(\alpha^\star)^{\mathrm{U}}"'] \arrow[ddd, dashed, bend right=70, "\mathrm{Id}_{G_N}"'] \arrow[dddr, dashed, "(\alpha^\star)^{\mathrm{U}}\iota^{\mathrm{U}}\gamma^{\mathrm{U}}=\alpha^\star"] & & \\
G_1^{\mathrm{U}} \arrow[d, "\iota^{\mathrm{U}}"'] & & \\
G_0^{\mathrm{U}} \arrow[d, "\beta"'] \arrow[dr, "\gamma^{\mathrm{U}}"] & & \\
\mathrm{G}_N \arrow[r, "\alpha^\star"] & \mathrm{G}_Q \arrow[r, "\delta^\star"] & \mathrm{G}_M
\end{tikzcd}$$

The diagonal $(\alpha^\star)^{\mathrm{U}}\iota^{\mathrm{U}}\gamma^{\mathrm{U}}$ from G_N to G_Q takes I_N to I_Q. It also has K_N in its kernel, since $\gamma^{\mathrm{U}}\delta^\star$ is trivial. Therefore in fact $(\alpha^\star)^{\mathrm{U}}\iota^{\mathrm{U}}\gamma^{\mathrm{U}}$ is equal to $\alpha^\star$. As $\alpha^\star$ is a kernel morphism for $\delta^\star$, uniqueness forces $(\alpha^\star)^{\mathrm{U}}\iota^{\mathrm{U}}\beta$ from G_N to G_N to be the identity morphism $\mathrm{Id}_{\mathrm{G}_N}$.

The identity $\mathrm{Id}_{\mathrm{G}_N} = (\alpha^\star)^{\mathrm{U}}\iota^{\mathrm{U}}\beta$ is certainly surjective, so its final factor β is as well. We have already noted that β is monic. Therefore by Proposition (9.11) and Corollary (9.13) the morphism β is an isomorphism of the groups G_0^{U} and G_N in $\mathsf{UTriGrp}^\star$.

If ζ is the natural covering map from G_0^{U} to G_0, then $\beta^{-1}\zeta$ is a covering map from G_N to G_0. In particular $\ker\pi_0 = K_0$ is a central quotient of $\ker\pi_N = K_N$, as claimed.

As I_Q normalizes K_0 we have $\langle K_0^{\mathrm{G}_Q}\rangle = \langle K_0^{K_Q}\rangle$, so it remains to prove $K_{N,Q} = \langle K_0^{\mathrm{G}_Q}\rangle$. By definition $K_0 = [K_{N,Q}, I_Q]$, so $K_{N,Q}$ contains the normal subgroup $K_1 = \langle K_0^{\mathrm{G}_Q}\rangle$ of G_Q. For $g \in \mathrm{G}_Q$,

$$K_1 \geq K_0^g = [K_{N,Q}, I_Q]^g = [K_{N,Q}, I_Q^g]\,.$$

Therefore $K_1 \geq [K_{N,Q}, \mathrm{G}_Q]$ and $K_{N,Q}/K_1$ is central in $\mathrm{G}_Q\,/K_1$. As G_Q is universal, $K_1 = K_{N,Q}$ by Lemma (4.12)(e), as desired. □

We have immediately a version in Doro's context.

(14.8). Corollary. *Let*

$$1 \longrightarrow N \xrightarrow{\alpha} Q \xrightarrow{\delta} M \longrightarrow 1$$

be a short exact sequence of Moufang loops. Then we have a short exact sequence of groups

$$1 \longrightarrow K_{N,Q} \xrightarrow{\alpha'} K_Q \xrightarrow{\delta'} K_M \longrightarrow 1$$

where $\delta' = \delta\mathbf{G}^\star$ is a morphism of groups admitting the triality I_Q that has kernel (as group homomorphism) $K_{N,Q} = \langle K_0^{K_Q}\rangle$ for $K_0 = [K_{N,Q}, I_Q]$, a central quotient of K_N, the kernel of π_N on G_N. □

Conversely, we have an expanded version of Doro's [**Dor78**, Corollary 1.1].

(14.9). Theorem. *Let (G, D, π) be a group with triality and K be a normal subgroup that is contained in* $\ker\pi$. *Then there is a short exact sequence of Moufang loops*

$$1 \longrightarrow N \xrightarrow{\alpha} Q \xrightarrow{\delta} M \longrightarrow 1$$

and a related commutative diagram of groups

$$\begin{tikzcd}
1 \arrow[r] & K_{N,Q} \arrow[r, "\alpha'"] \arrow[d, "\lambda"] & \mathrm{G}_Q \arrow[r, "\delta'"] \arrow[d, "\chi"] & \mathrm{G}_M \arrow[r] \arrow[d, "\mu"] & 1 \\
1 \arrow[r] & K \arrow[r] & G \arrow[r] & H \arrow[r] & 1
\end{tikzcd}$$

whose rows are exact and whose vertical maps have central kernels. Indeed, we may take $Q = G\mathbf{M}^\star$ and $M = H\mathbf{M}^\star$ with χ and μ the associated covers by the universal groups $\mathrm{G}_Q = G\mathbf{M}^\star\mathbf{G}^\star$ and $\mathrm{G}_M = H\mathbf{M}^\star\mathbf{G}^\star$. The image of $K_{N,Q}$ under λ is $[K, G]$.

Proof. Let $H = G/K$, a group with triality. By Theorem (11.6) the universal groups G^{U} and H^{U} are naturally isomorphic to the groups $G\mathbf{M}^\star\mathbf{G}^\star$ and $H\mathbf{M}^\star\mathbf{G}^\star$. We have

$$\begin{tikzcd}
1 \arrow[r] & K \arrow[r] & G \arrow[r] \arrow[d, "\mathbf{M}^\star"] & H \arrow[r] \arrow[d, "\mathbf{M}^\star"] & 1 \\
1 \arrow[r] & N \arrow[r, "\alpha"] & Q \arrow[r, "\delta"] \arrow[d, "\mathbf{G}^\star"] & M \arrow[r] \arrow[d, "\mathbf{G}^\star"] & 1 \\
1 \arrow[r] & K_{N,Q} \arrow[r, "\alpha'"] \arrow[d, dashed, "\lambda"] \arrow[dr, dashed, "\alpha'\chi"] & \mathrm{G}_Q \arrow[r, "\delta'"] \arrow[d, "\chi"] & \mathrm{G}_M \arrow[r] \arrow[d, "\mu"] & 1 \\
1 \arrow[r] & K \arrow[r, "\alpha''"] & G \arrow[r, "\delta''"] & H \arrow[r] & 1
\end{tikzcd}$$

Here χ and μ are the appropriate covers, and we may take the maps α, α', and α'' to be injections. As $\alpha'\delta'$ is trivial, so is $\alpha'\delta'\mu = \alpha'\chi\delta''$. Therefore $\alpha'\chi$ factors through K as $\lambda\alpha''$. As α' is injective and χ has central kernel, so does λ.

It remains to prove $K_{N,Q}^\lambda = [K, G]$. We already know $K_{N,Q}^\lambda \leq [K, G]$, so we must show λ takes $K_{N,Q}$ onto $[K, G]$. By Lemma (4.12)

$$[K, G] = \langle\, de \mid d, e \in D,\ e \in Kd \,\rangle\,.$$

As χ is a cover, by Lemma (6.3) the map $(d_\chi)^\chi = d$ describes a bijection (indeed isogeny) between the elements d_χ of D_Q and the elements d of D. Suppose $e \in Kd$ so that de is one of the chosen generators of $[K, G]$. Then

$$1_H = (de)^{\alpha''\delta''} = (de)^{\delta''} = d^{\delta''}e^{\delta''} = (d_\chi^\chi)^{\delta''}(e_\chi^\chi)^{\delta''} = d_\chi^{\chi\delta''}e_\chi^{\chi\delta''} = d_\chi^{\delta'\mu}e_\chi^{\delta'\mu} = (d_\chi^{\delta'}e_\chi^{\delta'})^\mu.$$

That is, $d_\chi^{\delta'}e_\chi^{\delta'}$ is in the kernel of μ and the two elements $d_\chi^{\delta'}$ and $e_\chi^{\delta'}$ of D_M are in the same coset of $\ker\mu$. As μ is a cover, its kernel is central in G_M; so by Lemma (4.12)(e) we must have $d_\chi^{\delta'} = e_\chi^{\delta'}$. Therefore $1_{\mathrm{G}_M} = d_\chi^{\delta'}e_\chi^{\delta'} = (d_\chi e_\chi)^{\delta'}$, and $d_\chi e_\chi \in \ker\delta' = K_{N,Q}$. Then

$$(d_\chi e_\chi)^\lambda = (d_\chi e_\chi)^{\lambda\alpha''} = (d_\chi e_\chi)^{\alpha'\chi} = (d_\chi e_\chi)^\chi = d_\chi^\chi e_\chi^\chi = de\,.$$

Hence each of the chosen generators of $[K, G]$ is in $K_{N,Q}^\lambda$, and the map λ takes $K_{N,Q}$ onto $[K, G]$ as desired. □

14.3. Solvable Moufang loops

Following the standard definition for groups, a Moufang loop Q is *solvable* [**Gla68**, p. 397] if it possesses a finite series of subloops

$$1 = Q_0 \leq\ \cdots\ \leq Q_i \leq Q_{i+1} \leq\ \cdots\ \leq Q_n = Q$$

in which each Q_i is normal in Q_{i+1} with the quotient Q_{i+1}/Q_i an abelian group.[1]

(14.10). Theorem. *Let Q be a Moufang loop whose universal group with triality G_Q is solvable. Then Q is solvable of derived length at most k, the derived length of the base group $\ker\pi_Q/\mathrm{Z}(\mathrm{G}_Q) = K_Q/\mathrm{Z}(\mathrm{G}_Q)$ of the adjoint group $\mathrm{G}_Q/\mathrm{Z}(\mathrm{G}_Q)$..*

[1] For arbitrary loops a stronger definition of solvability is more appropriate; for a thorough discussion of this, see Stanovský and Vojtěchovský [**SVo14**].

Proof. The proof is by induction on k. When $k = 0$ we have $\ker \pi_Q = \mathrm{Z}(\mathrm{G}_Q) = 1$, hence $Q = 1$ as needed.

Assume $k \geq 1$ and let K be the preimage of the last term in the derived series of $K_Q/\mathrm{Z}(\mathrm{G}_Q)$. Consider the commutative diagram of Theorem (14.9):

$$\begin{tikzcd}
1 \arrow[r] & K_{N,Q} \arrow[r, "\alpha'"] \arrow[d, "\lambda"] & \mathrm{G}_Q \arrow[r, "\delta'"] \arrow[d, "\mathrm{Id}"] & \mathrm{G}_M \arrow[r] \arrow[d, "\mu"] & 1 \\
1 \arrow[r] & K \arrow[r] & \mathrm{G}_Q \arrow[r] & H \arrow[r] & 1
\end{tikzcd}$$

associated with the short exact sequence of Moufang loops

$$1 \longrightarrow N \xrightarrow{\alpha} Q \xrightarrow{\delta} M \longrightarrow 1$$

for $M = H\mathbf{M}^\star$ and N the kernel of the loop homomorphism δ. Here μ is the cover of H by G_M, hence $H/\mathrm{Z}(H)$ and $\mathrm{G}_M/\mathrm{Z}(\mathrm{G}_M)$ are isomorphic. In particular $\ker \pi_M/\mathrm{Z}(\mathrm{G}_M)$ has derived length less than k, so by induction M is solvable with derived length at most $k-1$.

As α', Id, and the map from K to G_Q are all injections, so is λ.

Following Theorem (14.7) where $K_0 = [K_{N,Q}, I_Q]$, the composition

$$K_N \xrightarrow{\alpha^\star} K_0 \xrightarrow{\iota} K_{N,Q} \xrightarrow{\lambda} K$$

has central kernel. Extend this by I_N and I_Q, as appropriate, to

$$\mathrm{G}_N \xrightarrow{\alpha^\star} G_0 \xrightarrow{\iota} K_{N,Q}.I_Q \xrightarrow{\lambda} K.I_Q$$

where by the definition of K we have $K' \leq \mathrm{Z}(\mathrm{G}_Q)$ and especially I_Q centralizes K'. Then

$$\mathrm{G}_N \xrightarrow{\alpha^\star} G_0 = \langle I_Q^{K_{N,Q}} \rangle \xrightarrow{\lambda} \langle I_Q^K \rangle$$

still has central kernel, so the adjoint group with triality $\mathrm{G}_N/\mathrm{Z}_2(\mathrm{G}_N) = \mathrm{G}_N/\mathrm{Z}(\mathrm{G}_N)$ (by Lemma (4.12)(e)) has abelian base group. Therefore by Theorem (12.15) the multiplication group $\mathrm{Mlt}(N)$ is also an abelian group. But then by Proposition (12.1) the Moufang loop N is also an abelian group. Therefore the Moufang loop Q itself is solvable of derived length at most $k = 1 + (k-1)$, as required. □

(14.11). Corollary. *Let Q be a Moufang loop whose multiplication group is solvable. Then Q is solvable.*

Proof. This is an immediate consequence of Proposition (12.18) and Theorem (14.10). □

Vesanen [**Ves96**] proved the corollary for arbitrary loops that are finite. We also have its converse for finite Moufang loops.

(14.12). Theorem. *Let Q be a finite solvable Moufang loop. Then the groups G_Q and $\mathrm{Mlt}(Q)$ are solvable.*

Proof. The proof is by induction on k, the derived length of Q. If $k = 0$ then $Q = 1$, in which case $\mathrm{G}_Q = I_Q \simeq \mathrm{Sym}(3)$ and $\mathrm{Mlt}(Q) = 1$, both solvable.

Now assume $k \geq 1$. Let N be a normal abelian subgroup of Q with $M = Q/N$ of derived length $k-1$. Consider the associated short exact sequence of groups from Theorem (14.7):

$$1 \longrightarrow K_{N,Q} \xrightarrow{\alpha'} \mathrm{G}_Q \xrightarrow{\delta'} \mathrm{G}_M \longrightarrow 1$$

As M has derived length $k-1$, G_M is solvable by induction. Also $K_{N,Q} = \langle K_0^{\mathrm{G}_Q} \rangle$ where $K_0 = [K_{N,Q}, I_Q]$ is a normal subgroup of $K_{N,Q}$ that is a central quotient of $\ker \pi_N$. As N is an abelian group, by Proposition (12.1) the group $\mathrm{Mlt}(N)$ is solvable (indeed abelian). Therefore by Proposition (12.18) G_N and its section K_0 are both solvable. Now

$$K_{N,Q} = \langle K_0^{\mathrm{G}_Q} \rangle = \langle\, [K_{N,Q}, I_Q]^g \mid g \in \mathrm{G}_Q \,\rangle = \langle\, [K_{N,Q}, I_Q^g] \mid g \in \mathrm{G}_Q \,\rangle\,.$$

There are at most $|Q|^2$ distinct conjugates I_Q^g in G_Q, a finite number by assumption. Therefore $K_{N,Q}$ is generated by finitely many G_Q-conjugates of the solvable normal subgroup K_0 and so is solvable itself.

As G_M and $K_{N,Q}$ are both solvable, G_Q is solvable. Its section $\mathrm{Mlt}(Q)$ is then also solvable; see again Proposition (12.18). □

Chapter 15

Some Related Categories and Objects

15.1. 3-nets

In the early 20th Century Hilbert, Reidermeister, Thomsen, Moufang, Bol and others [**Hil00, Rei29, Tho29, Mou35, Bol37**] studied quasigroups and loops in the context of algebraic systems that might coordinatize geometries, in particular 3-nets, which are dual to Latin square designs. The algebraic properties of the loops thus corresponded to certain geometric properties, in particular the closure of certain geometric configurations. For instance, the projective planes that can be coordinatized by a field are precisely those that satisfy Desargues' Theorem [**VeY16**].

A 3-net is a partial linear space that is dual to a Latin square design. That is, a 3-*net* (S, P) is a *point set* S together with a set P of subsets of S called *lines*—the line set being partitioned $P = P^{\mathrm{R}} \cup P^{\mathrm{C}} \cup P^{\mathrm{E}}$ into pairwise disjoint *parallel classes*—and satisfying:

(i) *every point* $l \in S$ *is contained in exactly one line from each parallel class* P^{R}*,* P^{C}*, and* P^{E}*;*

(ii) *if* p, q *are two lines not in the same parallel class, then they intersect at a unique point* $l \in S$*.*

We thus see that a 3-net is the same as a Latin square design (as in Chapter 3) except that the roles of points and lines have been interchanged; that is, the two concepts are dual to each other. Most of the early work in this area was done in terms of nets; see [**Bol37, Tho29**].

We can thus easily define the dual category $\mathsf{3Net}$ of 3-nets and have the following.

(15.1). Theorem. *The categories* $\mathsf{3Net}$ *and* LSD *are isomorphic.* □

Bol [**Bol37**] considered the existence of certain automorphisms for nets and related these to coordinatization of the net by a Moufang loop. This study was revived by Funk and Nagy [**FuN93**] who gave the automorphisms in question the name *Bol reflections.* In fact, they are precisely the net automorphisms dual to central automorphisms of Latin square designs. Accordingly we have the category BRNet of Bol reflection 3-nets, those 3-nets that admit all possible Bol reflections. The category isomorphism thus restricts to the appropriate subcategories.

(15.2). THEOREM. *The categories* BRNet *and* CLSD *are isomorphic.* □

It is often convenient to choose a particular point $l \in S$ of a Bol net as *origin*. The corresponding pointed categories are $\mathsf{3Net}^\star$ and $\mathsf{BRNet}^\star$.

(15.3). THEOREM.

(a) *The categories* $\mathsf{3Net}^\star$ *and* $\mathsf{LSD}^\star$ *are isomorphic.*
(b) *The categories* $\mathsf{BRNet}^\star$ *and* $\mathsf{CLSD}^\star$ *are isomorphic.* □

15.2. Categories of conjugates

Many of the categories C that we have encountered can be meaningfully enlarged to categories C^+ with the same object class but additional morphisms.

The most natural is the category LSD^+ enlarging LSD. If (P,S) and (P_0,S_0) are two Latin square designs, thus objects of LSD and so also LSD^+, then a morphism φ of $\mathrm{Hom}_{\mathsf{LSD}^+}((P,S),(P_0,S_0))$ is a map $\varphi\colon P \longrightarrow P_0$ such that

$$\ell \in S \implies \ell^\varphi \in S_0\,.$$

Recall that for such a φ to be an LSD-morphism it must additionally have three parts (α,β,γ) for which

$$\varphi|_{P^{\mathrm{R}}} = \alpha\colon P^{\mathrm{R}} \longrightarrow P_0^{\mathrm{R}}\,,\ \varphi|_{P^{\mathrm{C}}} = \beta\colon P^{\mathrm{C}} \longrightarrow P_0^{\mathrm{C}}\,,\ \varphi|_{P^{\mathrm{E}}} = \gamma\colon P^{\mathrm{E}} \longrightarrow P_0^{\mathrm{E}}\,.$$

As the fibers of (P,S) and (P_0,S_0) are their equivalence classes under noncollinearity, an arbitrary φ must map the fiber set of (P,S) to that of (P_0,S_0), but in doing so it may induce a nontrivial permutation on the label set $\{\mathrm{R},\mathrm{C},\mathrm{E}\}$, whereas a LSD-morphism is required to act trivially. For instance, taking the transpose of a Latin square corresponds to an LSD^+-isomorphism but not an LSD-morphism.

In particular, we see that $\mathrm{Aut}_{\mathsf{LSD}^+}(P,S)$ is the full automorphism group of the Latin square design, whereas $\mathrm{Aut}_{\mathsf{LSD}}(P,S)$ is a normal subgroup of index d, the order of the subgroup of $\mathrm{Sym}(\mathrm{R},\mathrm{C},\mathrm{E})$ induced by the full automorphism group. Indeed, LSD^+ could be viewed as LSD with the isomorphism class of (P,S) enlarged to contain $6/d$ of the LSD-classes. In particular, the isomorphism classes in CLSD are left unchanged, although central automorphisms are now morphisms in CLSD^+, a full subcategory of LSD^+.

Consider next the category TriGrp and the corresponding TriGrp^+. Recall that if (G,D,π) and (G_0,D_0,π_0) are two groups with triality, then a morphism $f\colon (G,D,\pi) \longrightarrow (G_0,D_0,\pi_0)$ is a group homomorphism $f\colon G \longrightarrow G_0$ that additionally has $D^f \subseteq D_0$ and $\pi = f\pi_0$. This last condition says that the following diagram commutes:

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & G_0 \arrow[d, "\pi_0"] \\ \mathrm{Sym}(3) \arrow[r, "\mathrm{Id}_{\mathrm{Sym}(3)}"] & \mathrm{Sym}(3) \end{tikzcd}$$

In TriGrp^+ a morphism between these two groups will be a group homomorphism $f\colon G \longrightarrow G_0$ that has $D^f \subseteq D_0$ and for which the following diagram commutes

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & G_0 \arrow[d, "\pi_0"] \\ \mathrm{Sym}(3) \arrow[r, "\sigma_f"] & \mathrm{Sym}(3) \end{tikzcd}$$

where σ_f may be an arbitrary automorphism of $\mathrm{Sym}(3)$. As was the case for CLSD^+, isomorphism classes are left unchanged since σ is an inner automorphism and can always be induced by an element of G. (See related remarks on page 43 in the context of isogeny.)

It remains to consider the various extensions of Qgp and its subcategories. A morphism in Qgp^+ from $(Q,\cdot)$ to $(R,\circ)$ is a triple of maps $\varphi = (\alpha_1,\alpha_2,\alpha_3)$ from Q to R together with a permutation $\sigma \in \mathrm{Sym}(3)$ such that

$$q_1 \cdot q_2 = q_3 \implies q_{1^\sigma}^{\alpha_{1^\sigma}} \circ q_{2^\sigma}^{\alpha_{2^\sigma}} = q_{3^\sigma}^{\alpha_{3^\sigma}}\ ,$$

for $q_1, q_2, q_3 \in Q$. It is easiest to think of this as a two-step process

$$(Q,\cdot) \xrightarrow{\varphi} (R,\star) \xrightarrow{\sigma} (R,\circ)\,,$$

where $\varphi = (\alpha_1,\alpha_2,\alpha_3)$ is a homotopism from $(Q,\cdot)$ to $(R,\star)$ (and so a Qgp-morphism) and the permutation σ is viewed as a special Qgp^+-isomorphism given by

$$r_1 \star r_2 = r_3 \quad\iff\quad r_{1^\sigma} \circ r_{2^\sigma} = r_{3^\sigma}\ .$$

In this case, $(R,\star)$ and $(R,\circ)$ are called *conjugates* (or *parastrophes*) of each other.

We already saw a common example of conjugacy on page 21 in Section 3.1. If $\sigma = (1,2)(3)$, then

$$r_1 \star r_2 = r_3 \quad\iff\quad r_2 \circ r_1 = r_3\,,$$

and $(R,\star)$ and $(R,\circ)$ are opposite quasigroups.

15.3. Groups enveloping triality

It has become relatively common [**GrZ06, Mik93, NVo03**] to weaken Doro's definition of a group K admitting the triality I by dropping the requirement that $[K,I]=K$. This is not a serious change, since in any event $[K,I,I]=[K,I]$ (see Proposition (15.4)(c) below). Therefore this expanded idea of a group admitting triality has Doro's form at its heart.

In the context of our definition of a triality group (G,D,π) (or (G,D,π,I)) the corresponding change is to repeat definition (4.1) nearly as is, dropping only the requirement that the conjugacy class D generates G. We will say that the group E *envelopes triality* if it satisfies this weakened version of (4.1), and we will write $(\!(E,D,\pi)\!)$ or $(\!(E,D,\pi,I)\!)$ as appropriate. In this event, the normal subgroup $G=\langle D\rangle$ gives rise to groups with triality $(G,D,\pi|_G)$ and $(G,D,\pi|_G,I)$ as before, since elements of D are conjugate via the various $\mathrm{Sym}(3)$ subgroups that they generate. We say that $(\!(E,D,\pi)\!)$ and $(\!(E,D,\pi,I)\!)$ *envelope* the groups with triality $(G,D,\pi|_G)$ and $(G,D,\pi|_G,I)$ or any triality groups isomorphic to them. Furthermore, if M is a Moufang loop isomorphic to $(G,D,\pi)\mathbf{M}$ or $(G,D,\pi,I)\mathbf{M}^\star$ (as appropriate), then we say that $(\!(E,D,\pi)\!)$ and $(\!(E,D,\pi,I)\!)$ *envelope* M.

(15.4). PROPOSITION. *Let $(\!(E,D,\pi_E)\!)$ be a group enveloping triality, and set $P=\ker\pi_E$, $G=\langle D\rangle$, and $\pi=\pi_E|_G$.*

(a) *(G,D,π) is a group with triality; $E=PG$; and $\mathrm{C}_E(D)=\mathrm{C}_P(D)=\mathrm{C}_E(G)$ is a normal subgroup of E with $G\cap\mathrm{C}_E(D)=\mathrm{Z}(G)$.*

(b) *$\pi_E=\pi|^E$ is uniquely determined from P and (G,D,π) via $(pg)^{\pi_E}=g^{\pi_E}=g^\pi$ for $p\in P$ and $g\in G$.*

(c) *For I a line of (G,D,π), we have $E=P\rtimes I$ and* $\ker\pi=[P,I]=[P,I,I]$.

Proof. All this is evident except for (c). We have $\ker\pi = G \cap P$, hence $E = PG = P \rtimes I$. As $G = \langle I^E\rangle = \langle I^P\rangle = [P,I] \rtimes I$, we also have $\ker\pi = [P,I]$. Furthermore modulo its normal subgroup $[P,I,I]$, G is a group with triality that is a central extension of $[P,I]/[P,I,I]$ by $I \simeq \mathrm{Sym}(3)$. Thus $[P,I]/[P,I,I]$ is trivial by Lemma (4.12), and $[P,I] = [P,I,I]$. □

We now have the category ETriGrp whose object class consists of all groups enveloping triality. A morphism f of $\mathrm{Hom}_{\mathsf{ETriGrp}}((\!(E,D,\pi)\!),(\!(E_0,D_0,\pi_0)\!))$ is again a group homomorphism $f\colon E \longrightarrow E_0$ that additionally has $D^f \subseteq D_0$ and $\pi = f\pi_0$. We similarly have the category $\mathsf{ETriGrp}^\star$ with objects $(\!(E,D,\pi,I)\!)$ for I a line of $(\langle D\rangle, D, \pi|_{\langle D\rangle})$. A morphism from (E,D,π,I) to (E_0,D_0,π_0,I_0) additionally satisfies $I^f = I_0$.

There is virtue in these new definitions. If (G,D,π,I) is a group with triality, and H is a subgroup of G that contains I, then H still might not be a group with triality. On the other hand if $(\!(E,D,\pi,I)\!)$ is a group enveloping triality and H is a subgroup containing I, then $(\!(H, D\cap H, \pi|_H, I)\!)$ also envelopes triality. Thus the new concept can be helpful inductively. On the other hand, we have lost some control. If $(\!(E,D,\pi)\!)$ is a group enveloping triality and A is any group, then $(\!(A\times E, \{1_A\}\times D, \pi|^{A\times E})\!)$ also envelopes triality. In particular, each group with triality has arbitrarily large enveloping groups. Thus within ETriGrp there is no obvious counterpart to the subcategory UTriGrp of TriGrp.

There is a counterpart to ATriGrp. We call the group $(\!(E,D,\pi)\!)$ *faithful* if $\mathrm{C}_E(D) = 1$. Let AETriGrp be the full subcategory of ETriGrp consisting of the faithful groups enveloping triality. Then by Proposition (15.4) the intersection of AETriGrp with TriGrp is precisely the adjoint subcategory ATriGrp. There is of course a corresponding pointed category $\mathsf{AETriGrp}^\star$.

Grishkov and Zavarnitsine [**GrZ06**] (following in part Mikheev [**Mik93**]) noted the existence of faithful groups enveloping triality and possessing a "universal injective" property:

(15.5). Theorem.

(a) *For every adjoint group with triality* (G,D,π) *there is a faithful enveloping group* $(\!(G^{\mathrm{AE}}, D^{\mathrm{AE}}, \pi^{\mathrm{AE}})\!)$ *with the property:*

If $(\!(E_0,D_0,\pi_0)\!)$ *faithfully envelopes* (G,D,π) *via the triality isomorphism* f *of* $(\langle D_0\rangle, D_0, \pi_0|_{\langle D_0\rangle})$ *with* (G,D,π)*, then* f *extends to a morphism* φ *that is an injection of the faithful group* $(\!(E_0,D_0,\pi_0)\!)$ *into* $(\!(G^{\mathrm{AE}}, D^{\mathrm{AE}}, \pi^{\mathrm{AE}})\!)$*.*

(b) *For every adjoint group with triality* (G,D,π,I) *there is a faithful enveloping group* $(\!(G^{\mathrm{AE}}, D^{\mathrm{AE}}, \pi^{\mathrm{AE}}, I^{\mathrm{AE}})\!)$ *with the property:*

If $(\!(E_0,D_0,\pi_0,I_0)\!)$ *faithfully envelopes* (G,D,π,I) *via the triality isomorphism* f *of* $(\langle D_0\rangle, D_0, \pi_0|_{\langle D_0\rangle}, I_0)$ *with* (G,D,π,I)*, then* f *extends to a morphism* φ *that is an injection of the group* $(\!(E_0,D_0,\pi_0,I_0)\!)$ *into* $(\!(G^{\mathrm{AE}}, D^{\mathrm{AE}}, \pi^{\mathrm{AE}}, I^{\mathrm{AE}})\!)$*.*

(c) *In* (a) *and* (b) *we may take* G^{AE} *to be* $\mathrm{Aut}((G,D,\pi)\mathbf{C})$*, the full automorphism group of the Latin square design* $(G,D,\pi)\mathbf{C}$ *associated with* (G,D,π)*. In this case* $D^{\mathrm{AE}} = D$ *is the class of central automorphisms,* $\pi^{\mathrm{AE}} = \pi|^{G^{\mathrm{AE}}}$*,* $I^{\mathrm{AE}} = I$*, and* $P^{\mathrm{AE}} = \mathrm{Aut}_{\mathsf{LSD}}((G,D,\pi)\mathbf{C})$*.*

Proof. The first two parts follow from the third. Because of the definition of the functor $\mathbf{C}$, each transposition d of D plays two roles. It is an element of $P_{(G,D,\pi)}$, the point set of $(G,D,\pi)\mathbf{C}$, but it also acts on $D = P_{(G,D,\pi)}$ by conjugation as the central automorphism of $(G,D,\pi)\mathbf{C}$ with center the point d.

Suppose for $(\!(E_0, D_0, \pi_0, I_0)\!)$ with $G_0 = \langle D_0 \rangle$ there is an isomorphism f of $(G_0, D_0, \pi_0|_{\langle D_0\rangle}, I_0)$ with (G, D, π, I). Then for each $g \in E_0$ the map $g^\varphi \colon d \mapsto d^{f^{-1}gf}$ defines an action of g on $D = D^{\mathrm{AE}} = P_{(G,D,\pi)}$. If d and e are in D with $\langle d, e\rangle$ a line of (G,D,π,I), then $\langle d,e\rangle^{g^\varphi} = \langle d^{g^\varphi}, e^{g^\varphi}\rangle$ is also a line of (G,D,π,I), because $\langle d^{f^{-1}}, e^{f^{-1}}\rangle$ and $\langle d^{f^{-1}g}, e^{f^{-1}g}\rangle$ are lines of $(G_0, D_0, \pi_0|_{\langle D_0\rangle}, I_0)$. Therefore g^φ takes lines of $(G,D,\pi)\mathbf{C}$ to lines and so is an automorphism of the Latin square design.

The map $\varphi \colon E \longrightarrow \mathrm{Aut}((G,D,\pi)\mathbf{C})$ given by $g \mapsto g^\varphi$ is then easily a group homomorphism with $P^\varphi \le \mathrm{Aut}_{\mathsf{LSD}}((G,D,\pi)\mathbf{C})$. If $g^\varphi = h^\varphi$, the element $(gh^{-1})^\varphi$ is trivial on D, and hence $(d^{f^{-1}})^{gh^{-1}} = d^{f^{-1}}$ for all $d \in D$. Thus, as f is a bijection, gh^{-1} acts trivially by conjugation on D_0. That is, $gh^{-1} \in \mathrm{C}_{E_0}(D_0)$, a trivial group as $(\!(E_0, D_0, \pi_0, I_0)\!)$ is faithful. We conclude that φ is an injection.

For each $y \in G_0$, $x \in D_0$, and $x^f = a \in D$,

$$a^{y^f} = (x^f)^{y^f} = (x^y)^f = ((a^{f^{-1}})^y)^f = a^{f^{-1}yf} = a^{y^\varphi}\,.$$

Therefore $\varphi|_{\langle D_0\rangle} = f$, and φ extends f to all of E_0. In particular $D_0^\varphi = D = D^{\mathrm{AE}}$, the class of central automorphisms, and $I_0^\varphi = I_0^f = I = I^{\mathrm{AE}}$ (as in (b)).

To complete the proof that φ is a morphism, we must show $\pi_0 = \varphi\pi^{\mathrm{AE}}$, knowing that $\pi_0|_{G_0} = f\pi$. First, for $p \in P_0 = \ker \pi_0$ and $a \in D$,

$$(a^{p^\varphi})^\pi = (a^{f^{-1}pf})^\pi = (a^{f^{-1}p})^{f\pi} = (a^{f^{-1}p})^{\pi_0} = ((a^{f^{-1}})^p)^{\pi_0} = (a^{f^{-1}})^{\pi_0} = a^\pi\,.$$

That is, $P_0^\varphi \le P^{\mathrm{AE}} = \ker \pi^{\mathrm{AE}}$. Thus for $x = pg \in E_0$ with $p \in P_0$ and $g \in G_0$,

$$x^{\varphi\pi^{\mathrm{AE}}} = (pg)^{\varphi\pi^{\mathrm{AE}}} = (p^\varphi g^\varphi)^{\pi^{\mathrm{AE}}} = (g^\varphi)^{\pi^{\mathrm{AE}}} = (g^f)^{\pi^{\mathrm{AE}}} = g^{f\pi} = g^{\pi_0} = (pg)^{\pi_0} = x^{\pi_0}\,,$$

as desired. □

Here in the statement "extends" and "injection" are not categorical concepts (although using arguments similar to ones from earlier chapters we could render them so).

The work of Grishkov and Zavarnitsine [**GrZ06**] is phrased in terms of the expanded version of Doro's groups admitting triality. Accordingly, if $(\!(E, D, \pi, I)\!)$ is in $\mathsf{ETriGrp}^\star$, then we construct the object (P, I, ι_I) of the isomorphic category EDoro with $P = \ker \pi$ and $\iota_I = \pi|_I$. We also have the isomorphic faithful subcategories $\mathsf{AETriGrp}^\star$ and AEDoro. The corresponding faithful and universally injective object $(P^{\mathrm{AE}}, I^{\mathrm{AE}}, \iota^{\mathrm{AE}}_{I^{\mathrm{AE}}})$, discussed by Grishkov and Zavarnitsine [**GrZ06**], then has $P^{\mathrm{AE}} = \mathrm{Aut}_{\mathsf{LSD}}((G,D,\pi)\mathbf{C})$, the group of LSD-automorphisms of $(G,D,\pi)\mathbf{C}$, and $\iota^{\mathrm{AE}}_{I^{\mathrm{AE}}} = \pi^{\mathrm{AE}}|_{I^{\mathrm{AE}}}$. If $(G,D,\pi)\mathbf{M}$ (isomorphic to $(G,D,\pi)\mathbf{CS}$) is the Moufang loop M, then the universal faithful enveloping kernel P^{AE} is in turn isomorphic to the autotopism group of M, $\mathrm{Atp}(M) = \mathrm{Aut}_{\mathsf{Loop}}(M)$. See Section 3.2 above and also [**GrZ06, Hal10**].

15.4. Tits' symmetric $\mathcal{T}$-geometries

This section is based upon §§3-4 of [**Tit58**]. A *$\mathcal{T}$-geometry* is a tripartite graph $\mathcal{T}$ with nonempty parts $\mathcal{T}^1$, $\mathcal{T}^2$, $\mathcal{T}^3$ and satisfying, for $\{i,j,k\} = \{1,2,3\}$:

> *for every nonadjacent pair $p_i \in \mathcal{T}^i$ and $p_j \in \mathcal{T}^j$, there is a unique $p_k \in \mathcal{T}^k$ that is adjacent to both p_i and p_j.*

Incidence of p_i and p_j will be written as $p_i \sim p_j$.

In particular a $\mathcal{T}$-geometry is connected of diameter at most 3. There are many examples.

(15.6). Example. (Gated $\mathcal{T}$-geometries) *Let $\mathcal{U}$ be a tripartite graph with parts $\mathcal{U}_1$, $\mathcal{U}_2$, and $\mathcal{U}_3$ and having the property:*

> *if $p_i \sim p_j \sim p_k$, for $p_i \in \mathcal{U}_i$, $p_j \in \mathcal{U}_j$, $p_k \in \mathcal{U}_k$ and $\{i,j,k\} = \{1,2,3\}$, then $p_i \sim p_k$.*

This is the case precisely when any connected component that meets each $\mathcal{U}_l$ nontrivially is complete.

For each i let $\mathcal{T}^i = \mathcal{U}_i \cup \{\infty_i\}$, where ∞_i is a new vertex, a "gate." For $\{i,j,k\} = \{1,2,3\}$ let the gate ∞_i be adjacent to every vertex of $\mathcal{T}^j$ and $\mathcal{T}^k$. The tripartite graph $\mathcal{T} = \mathcal{T}^1 \uplus \mathcal{T}^2 \uplus \mathcal{T}^3$ is then a $\mathcal{T}$-geometry.

In particular any complete tripartite graph $K_{m,n,p}$ is a $\mathcal{T}$-geometry [**Tit58**, §4.1].

(15.7). Example. T*he* 6*-cycle C_6 is a $\mathcal{T}$-geometry, where the $\mathcal{T}^i$ are the various antipodal pairs of vertices.*

Among the above examples of $\mathcal{T}$-geometries, the complete tripartite graphs $K_{m,m,m}$ and the cycle C_6 have large automorphism groups.

Specifically, consider the subgroup Sym(3) of Aut(C_6) whose three elements of order 2 are the reflections of the 6-cycle that fix none of its vertices. If a is one such element, then a fixes $\mathcal{T}^i$, switches $\mathcal{T}^j$ and $\mathcal{T}^k$ (for an appropriate numbering of the three parts of C_6), and has the following three properties:

(i) *for all $p_j \in \mathcal{T}^j$, p_j and p_j^a are adjacent;*
(ii) *if $p_i \in \mathcal{T}^i$ is adjacent simultaneously to p_j $(\in \mathcal{T}^j)$ and p_j^a $(\in \mathcal{T}^k)$, then $p_i^a = p_i$;*
(iii) $a^2 = 1$.

Of course for C_6, the second property holds trivially.

Similarly, consider the complete graph $K_{m,m,m}$. Here the wreath product $\mathrm{Sym}(m)^3 \rtimes \mathrm{Sym}(3)$ acts on the associated $\mathcal{T}$-geometry with each involution a of the wreathing quotient Sym(3) having the three properties above. In this example, the first property is essentially trivial but the second is very strong, saying that a fixes each vertex of the part it leaves invariant.

We call an automorphism a of the $\mathcal{T}$-geometry $\mathcal{T}$ acting as in (i)-(iii) above a *symmetry* of $\mathcal{T}$. We denote by D_i the set of symmetries of $\mathcal{T}$ that leave part $\mathcal{T}^i$ fixed and switch $\mathcal{T}^j$ and $\mathcal{T}^k$. Further set $\Delta = D_1 \cup D_2 \cup D_3$. In Aut$(\mathcal{T})$ a conjugate of a symmetry is again a symmetry, so Δ is a normal set of elements of order 2.

The automorphisms of D_i induce the permutation $(i)(j,k)$ on the parts of $\mathcal{T}$. Tits [**Tit58**, §3.2] calls $\mathcal{T}$ a *symmetric $\mathcal{T}$-geometry* provided all permutations of $\{1,2,3\}$ are induced by Aut$(\mathcal{T})$. Thus C_6 and $K_{m,m,m}$ are symmetric.

We next have Tits' "Fundamental Lemma" [**Tit58**, §3.3]:

(15.8). Lemma. *Let $\{i,j,k\} = \{1,2,3\}$. If $a \in D_i$ and $b \in D_j$, then*

(a) *$aba = bab \in D_k$;*
(b) $(ab)^3 = 1$.

Proof. As a conjugate of a symmetry is a symmetry, both $a^{-1}ba = aba$ and bab are in D_k, inducing the permutation $(k)(i,j)$. It remains to prove

$$1 = (aba)(bab) = (ab)^3\,.$$

First let $p \in \mathcal{T}^k$. Then $p \sim p^b$ by (i), hence $p^{ab} \sim p^{bab}$. Similarly $p^{ba} \sim (p^{ba})^b = p^{bab}$ as $p^{ba} \in \mathcal{T}^i$. That is,

$$p^{ab} \sim p^{bab} \sim p^{ba}\,,$$

and by symmetry

$$p^{ba} \sim p^{aba} \sim p^{ab}\,.$$

If $p^{ab} \not\sim p^{ba}$, then by the defining axiom for $\mathcal{T}$-spaces $p^{bab} = p^{aba}$ and $p^{(ab)^3} = p$. On the other hand, if $p^{ab} \sim p^{ba}$ this would combine with $p^{ab} \sim p^{bab} = (p^{ba})^b$ (from above) to give $p^{ab} = (p^{ab})^b = p^a$ by (ii). That is, $p^{aba} = p$ and by symmetry $p^{bab} = p$; again $p^{bab} = p^{aba}$ and $p^{(ab)^3} = p$. Therefore for $p \in \mathcal{T}^k$ we always have $p^{(ab)^3} = p$.

This in turn implies that

$$(p^{ab})^{(ab)^3} = p^{(ab)^4} = (p^{(ab)^3})^{ab} = p^{ab}$$

and

$$(p^{(ab)^2})^{(ab)^3} = p^{(ab)^5} = (p^{(ab)^3})^{(ab)^2} = p^{(ab)^2}\,.$$

We conclude that $(ab)^3$ is trivial on $\mathcal{T}^k$ and additionally on $(\mathcal{T}^k)^{ab} \cup (\mathcal{T}^k)^{(ab)^2} = \mathcal{T}^i \cup \mathcal{T}^j$. That is, $(ab)^3 = 1$, as desired. □

(15.9). Corollary. *Let $H \leq \mathrm{Aut}(\mathcal{T})$ with $D = H \cap \Delta$ meeting at least two of D_1, D_2, and D_3. Then $\mathcal{T}$ is symmetric, and (G, D, π) is a group with triality, where $G = \langle D \rangle$ and π takes each symmetry of D_i to the permutation $(i)(j,k)$.* □

The consequences of the previous lemma and corollary for $\mathcal{T} = K_{m,m,m}$, where the full automorphism group is the wreath product $\mathrm{Aut}(\mathcal{T}) = \mathrm{Sym}(m)^3 \rtimes \mathrm{Sym}(3)$, were detailed by Tits [**Tit58**, §4.1] and later (and independently) rediscovered by Doro [**Dor78**] and Zara [**Zar85**]. This is the case $n = 3$ of Theorem (4.6) above.

While symmetric $\mathcal{T}$-geometries give rise to groups with triality, the converse seems not to hold in general. For many groups with triality there are no obvious $\mathcal{T}$-geometries upon which they act symmetrically. Nevertheless this approach gives a nice proof in Theorem (18.13) below that Cartan's triality group $\mathrm{P}\Omega_8^+(F) \rtimes \mathrm{Sym}(3)$ is a group with triality in our sense.

Tits has a second paper [**Tit59**] also devoted to triality. Although that paper is probably more famous than [**Tit58**], it is less central here. It focuses on identifying all conjugacy classes of elements of order 3 in the outer automorphism groups of orthogonal groups of dimension 8, not just the special class that we study here.

15.5. Latin chamber systems covered by buildings

The work in this section is motivated by a result of Meierfrankenfeld, Stroth, and Weiss [**MSW13**].

Let $\Delta = (V, A, \varphi)$ be a graph with vertex set V and edge set A, additionally provided with an edge-coloring $\varphi\colon A \longrightarrow I$.

The graph Δ is a *chamber system* provided that, for each color $i \in I$, the subgraph with vertex set V and edge set $\varphi^{-1}(i)$ is a disjoint union of complete subgraphs containing at least two vertices each. The connected components of these monochromatic subgraphs are the *panels* of the chamber system. Chamber systems were introduced by Tits in the fundamental paper [**Tit81**].

The vertices of the graph are the *chambers* of the chamber system. A *gallery* is a path $c_0, c_1, \ldots, c_d$ in the chamber system. The gallery is *simple* if $c_j \neq c_{j+1}$ for $0 \leq j < d$, in which case d is its *length*. The *type* of a gallery is the corresponding sequence of edge colors $\varphi(c_0c_1), \varphi(c_1c_2), \ldots, \varphi(c_jc_{j+1}), \ldots, \varphi(c_{d-1}c_d)$.

The number of colors is the *rank* of the chamber system, and a chamber system of rank 3 will be called, following [**MSW13**], a *Latin chamber system* provided:

any two panels of different colors intersect in a unique chamber.

The color set I will be taken to be $\{\mathrm{R}, \mathrm{C}, \mathrm{E}\}$.

We have immediately

(15.10). Lemma.

(a) *If (V, A, φ) is a Latin chamber system, then (V, N) is a* 3*-net, where the line set N is the set of panels and two lines are parallel when they have the same color.*

(b) *If (S, P) is a* 3*-net, then (S, A, φ) is a Latin chamber system, where the edges of A are given by collinearity in the* 3*-net, an edge receiving as color the name of the parallel class of the unique line containing it.* □

The lemma actually describes an isomorphism between the categories $\mathsf{3Net}$ of 3-nets and LCS of Latin chamber systems.

Latin chamber systems occur in [**MSW13**] as special sorts of chamber systems with Coxeter diagram $A_1 \times A_1 \times A_1$. A basic question to ask whenever considering a chamber system with Coxeter diagram is whether or not its universal 2-cover is a building. Proposition 4.2 of [**MSW13**] effectively states:

(15.11). Theorem. *For a Latin chamber system, the following two statements are equivalent:*

(1) *its universal* 2*-cover is a building;*

(2) *every loop that coordinatizes it, as* 3*-net, is a group.*

The proof in [**MSW13**] replaces (1) with the equivalent condition:

> **(R)** *whenever two simple galleries of the same reduced type are homotopic, they coincide.*

The equivalence of (1) and **(R)** for chamber systems with Coxeter diagrams is Theorem 3 of [**Tit81**].

The diameter of a Latin chamber system is two. If a pair of galleries share a panel, then their distance is at most one. If they do not, then any panel on one intersects a panel on the other, and a minimal length gallery connecting the two has length two.

In a chamber system with Coxeter diagram, galleries of *reduced type* are generalizations of minimal galleries. The Coxeter group W with diagram $A_1 \times A_1 \times A_1$ is elementary abelian of order 8 with presentation

$$\langle\, \mathrm{R}, \mathrm{C}, \mathrm{E} \mid \mathrm{R}^2 = \mathrm{C}^2 = \mathrm{E}^2 = 1\,,\ \mathrm{RC} = \mathrm{CR},\ \mathrm{RE} = \mathrm{ER},\ \mathrm{CE} = \mathrm{EC}\,\rangle\,.$$

The reduced types in this case are the words in the alphabet $\{\mathrm{R}, \mathrm{C}, \mathrm{E}\}$ that minimally represent elements of the Coxeter group W, that is, that contain no repeated letter. Thus simple galleries of reduced type have length at most three. The minimal galleries are those with reduced type of length at most two.

The empty type (word) of length 0 corresponds to the identity element of the Coxeter group and the length 0 gallery from any chamber to itself. The types of length 1 are the generators $\mathrm{R}, \mathrm{C}, \mathrm{E}$ of the Coxeter group, and a gallery with one of these types moves from one chamber of a panel to another.

The six types of length two come in three pairs, corresponding to relations in the Coxeter group: RC = CR, RE = ER, CE = EC. In a Latin chamber system, for the gallery c_0, c_1, c_2 of one of these types MN there is a corresponding and uniquely determined gallery c_0, c_1', c_2 with the same end chambers but of type NM. For example, if we think of the chambers c_0 and c_2 as two cells of a Latin square in different rows and different columns, then we can get from c_0 to c_2 via c_1, the cell in the row of c_0 that is also in the column of c_2; this is a gallery of type RC. But there is also a unique gallery of type CR connecting c_0 and c_2, namely, the gallery that travels by way of c_1', the cell in the same column as c_0 that is also in the same row as c_2.

Let

$$c_0 \longrightarrow \cdots c_{j-1} \xrightarrow{M} c_j \xrightarrow{N} c_{j+1} \cdots \longrightarrow c_d$$

be an arbitrary simple gallery whose subgallery c_{j-1}, c_j, c_{j+1} has type MN. The passage from this gallery to the corresponding gallery

$$c_0 \longrightarrow \cdots c_{j-1} \xrightarrow{N} c_j' \xrightarrow{M} c_{j+1} \cdots \longrightarrow c_d$$

is called an *elementary homotopy*. Two galleries are *homotopic*[1] if it is possible to pass from one to the other by a finite number of elementary homotopies. Homotopy is then an equivalence relation on the set of all simple galleries. As elementary homotopies only affect chambers in the interior of the gallery, two homotopic galleries must have the same initial and terminal chambers.

The homotopy class of a gallery of length 0 or 1 contains only that gallery. The discussion above shows that in Latin chamber systems, the homotopy class of a gallery of type MN contains only two galleries—the original and the gallery of type NM that results from an elementary homotopy—since the only elementary homotopy available for the second gallery is the move back to the first.

Therefore in a Latin chamber system, two simple and homotopic galleries of the same reduced type of length at most two are in fact the same. That is, condition **(R)** is satisfied for the minimal galleries. A proof of Theorem (15.11) will thus depend upon the analysis of reduced galleries of length three.

[1] The terminology here should not be confused with the similar sounding but unrelated concept of 'homotopism' introduced in Chapter 2.

Proof of Theorem (15.11).

We shall show that condition **(R)** is equivalent to the Reidermeister Quadrangle Condition **(QC)** of Section 3.4 for the associated 3-net and Latin square. Then Theorem (3.14) proves the theorem.

Recall from page 25 the Quadrangle Condition, which says that, whenever we encounter the following pattern in a Latin square, we must have $4 = 5$. Theorem (3.14) states that this is equivalent to the Latin square being the multiplication table of a group.

$$\begin{array}{c|ccccccccccc}
 & & u & & v & & & & w & & x & \\
\hline
 & \ddots & & \ddots & & \ddots & & \ddots & & \ddots & & \ddots \\
a & \cdots & 1 & \cdots & 2 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
 & \ddots & & \ddots & & \ddots & & \ddots & & \ddots & & \ddots \\
b & \cdots & 3 & \cdots & 4 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
 & \ddots & & \ddots & & \ddots & & \ddots & & \ddots & & \ddots \\
 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
 & \ddots & & \ddots & & \ddots & & \ddots & & \ddots & & \ddots \\
c & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1 & \cdots & 2 & \cdots \\
 & \ddots & & \ddots & & \ddots & & \ddots & & \ddots & & \ddots \\
d & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 3 & \cdots & 5 & \cdots \\
 & \ddots & & \ddots & & \ddots & & \ddots & & \ddots & & \ddots
\end{array}$$

The Latin square is visually a good representation of the associated 3-net and Latin chamber system. The cells of Latin square correspond to the points of the 3-net and to the chambers of the Latin chamber system. The various rows then constitute the lines of the parallel class labelled R and also the panels with color R. The columns give the parallel class C and the panels colored C. Finally the entries in the cells identify the lines of the diagonal parallel class E and the panels colored E.

In aid of our proof we add further labels to our Latin square, letting z be the column with entry $e_{bz} = 5$, then 6 the entry e_{az}, and finally f the row with $e_{fx} = 6$:

$$\begin{array}{c|ccccccccccc}
 & & u & & v & & z & & w & & x & \\
\hline
 & \ddots & & \ddots & & \ddots & & \ddots & & \ddots & & \ddots \\
a & \cdots & \mathbf{1} & \cdots & \mathbf{2} & \cdots & 6 & \cdots & \cdots & \cdots & \cdots & \cdots \\
 & \ddots & & \ddots & & \ddots & & \ddots & & \ddots & & \ddots \\
b & \cdots & \mathbf{3} & \cdots & \mathbf{4} & \cdots & 5 & \cdots & \cdots & \cdots & \cdots & \cdots \\
 & \ddots & & \ddots & & \ddots & & \ddots & & \ddots & & \ddots \\
f & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 6 & \cdots \\
 & \ddots & & \ddots & & \ddots & & \ddots & & \ddots & & \ddots \\
c & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \mathbf{1} & \cdots & \mathbf{2} & \cdots \\
 & \ddots & & \ddots & & \ddots & & \ddots & & \ddots & & \ddots \\
d & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \mathbf{3} & \cdots & \mathbf{5} & \cdots \\
 & \ddots & & \ddots & & \ddots & & \ddots & & \ddots & & \ddots
\end{array}$$

The cells of the Latin square, hence points of the 3-net and chambers of the Latin chamber system, are identified by triples (r, c, e), where r is the row index, c is the column index, and e is the entry.

We consider a sequence of elementary homotopies starting with an appropriate gallery of type REC:

$$(a, u, 1) \xrightarrow{\mathrm{R}} (a, v, 2) \xrightarrow{\mathrm{E}} (c, x, 2) \xrightarrow{\mathrm{C}} (d, x, 5)$$

$$(a, u, 1) \xrightarrow{\mathrm{E}} (c, w, 1) \xrightarrow{\mathrm{R}} (c, x, 2) \xrightarrow{\mathrm{C}} (d, x, 5)$$

$$(a, u, 1) \xrightarrow{\mathrm{E}} (c, w, 1) \xrightarrow{\mathrm{C}} (d, w, 3) \xrightarrow{\mathrm{R}} (d, x, 5)$$

$$(a, u, 1) \xrightarrow{\mathrm{C}} (b, u, 3) \xrightarrow{\mathrm{E}} (d, w, 3) \xrightarrow{\mathrm{R}} (d, x, 5)$$

$$(a, u, 1) \xrightarrow{\mathrm{C}} (b, u, 3) \xrightarrow{\mathrm{R}} (b, z, 5) \xrightarrow{\mathrm{E}} (d, x, 5)$$

$$(a, u, 1) \xrightarrow{\mathrm{R}} (a, z, 6) \xrightarrow{\mathrm{C}} (b, z, 5) \xrightarrow{\mathrm{E}} (d, x, 5)$$

$$(a, u, 1) \xrightarrow{\mathrm{R}} (a, z, 6) \xrightarrow{\mathrm{E}} (f, x, 6) \xrightarrow{\mathrm{C}} (d, x, 5)$$

The first and last are homotopic, simple galleries of reduced type REC from the chamber $(a, u, 1)$ to $(d, x, 5)$. If we assume condition **(R)** then they must be equal. In that case $(a, v, 2) = (a, z, 6)$, which gives $v = z$ and $2 = 6$. (Also $(c, x, 2) = (f, x, 6)$ hence $c = f$.) Therefore $(b, v, 4) = (b, z, 4) = (b, z, 5)$, and we conclude that $4 = 5$. This shows that the condition **(R)** indeed implies the Reidermeister Quadrangle Condition **(QC)**.

Conversely, if we assume **(QC)**, then we must have $4 = 5$, hence in turn $v = z$, $2 = 6$, and $f = c$. Thus the eight cells labelled in the Latin square form the eight corners of a cube in the 3-net and chamber system. (It is no coincidence that the cube is exactly the thin chamber system corresponding to the Coxeter diagram $A_1 \times A_1 \times A_1$.)

Consider a gallery with initial chamber $(a, u, 1)$ and terminal chamber $(d, x, 4) = (d, x, 5)$ and having as type one of the six permutations of REC. Any elementary homotopy leaves us with a gallery all of whose chambers come from the eight of the cube appearing in the **(QC)** configuration. That is, we cannot escape this cube using elementary homotopies. But within it, there is a unique gallery with these end chambers and having each of the six possible types. This together with the remarks preceding this proof on minimal galleries shows that **(QC)** implies **(R)**, as desired. □

Part 4

Classical Triality

Chapter 16

An introduction to concrete triality

There are classical and well-studied relationships among duality of finite dimensional vector spaces, order 2 outer automorphisms of the general linear groups (Lie type A_n), and algebras with involution.

This chapter is an introduction to Part 4, which is devoted to discussion of the more specialized relationships among Study's triality of hyperbolic orthogonal 8-space, Cartan's order 3 outer automorphisms of orthogonal groups (Lie type D_4), and Moufang's alternative algebras, such as the octonions of Cayley and Graves and the split octonions of Zorn. This we have termed *classical triality* as the topic is now over a hundred years old. An alternative would be *concrete triality*, as a contrast to the *abstract triality* of Chapter 4.

16.1. Study's triality

Quadratic forms are meant to model squared-length in Euclidean space. Thus the map $q\colon V \longrightarrow F$ is a *quadratic form* on the finite dimensional F-space V provided

$$q(\alpha x) = \alpha^2 q(x)\,,$$

for all $\alpha \in F$ and $x \in V$, and the associated form $h\colon V \times V \longrightarrow F$

$$h(x,y) = q(x+y) - q(x) - q(y)$$

is bilinear. An important and motivating example is the vector space $\mathrm{Mat}_2(F)$ of 2×2 matrices over F with q the determinant function.

For $W \subseteq V$, we define the F-subspace $W^\perp = \{x \in V \mid h(x,w) = 0,\, w \in W\}$. The form q is *nondegenerate* if $V^\perp = 0$. At the other extreme, a subspace is *singular* if the restriction of q (and so h) to S is identically 0. In nondegenerate (V,q), the largest dimension a singular subspace can have is $\dim V/2$. If nondegenerate V has a singular subspace of exactly this dimension, then (V,q) is a *hyperbolic space* or *split*, $\mathrm{Mat}_2(F)$ again providing an example.

Study [**Stu12, Stu13**] noticed a fascinating property of (real) hyperbolic 8-space. Let $\mathcal{T}$ be the graph whose vertices are the singular 1-spaces and singular 4-spaces. A singular 1-space is adjacent in $\mathcal{T}$ to each singular 4-space containing it and to no other 1-spaces. Two singular 4-spaces are adjacent if their intersection has dimension 3.

Study observed (of course, in other terms) that this graph is tripartite (one part consisting of all the 1-spaces) and that it admits an automorphism of order 3 that permutes the three parts of the graph transitively. This is *Study's triality*, valid over arbitrary fields F.

16.2. Cartan's triality

Cartan [**Car25**], motivated by Weinstein's calculation [**Wei23**] of the automorphism group of $\mathrm{GL}_n(\mathbb{R})$, discussed the automorphism groups of arbitrary Lie groups. He observed that automorphisms are linear in nature unless related to nontrivial graph automorphisms of the associated Dynkin diagram. (Recall that $\mathrm{Aut}(\mathbb{R}) = 1$.) This brought him to the diagrams A_l with $l \geq 2$, D_l with $l \geq 4$, and E_6. The first case is that handled by Weinstein with nontrivial graph automorphisms induced by correlations of the underlying space, the transpose-inverse giving an example. Similarly for E_6 the outer automorphisms are induced by correlations of the 27-space on which the group acts, preserving a cubic form. For D_l with $l \geq 5$, the nontrivial graph automorphism group has order 2 and is induced by orthogonal reflections.

This leaves D_4. According to Cartan, *"Ce cas est le plus interssant."* The automorphism group of the D_4 graph is $\mathrm{Sym}(3)$, with orthogonal reflections again inducing an element of order 2. But Cartan also constructed automorphisms of $\mathrm{D}_4(\mathbb{R}) = \mathrm{P}\Omega_8^+(\mathbb{R})$ inducing graph automorphisms of order 3.

In particular, Cartan discussed (rediscovered?) Study's geometric observation (without reference) and introduced the term "triality" to describe it (see page iii). As $\mathrm{P}\Omega_8^+(\mathbb{R})$ certainly acts on Study's graph $\mathcal{T}$, the automorphism group of that graph contains *Cartan's triality* group $\mathrm{P}\Omega_8^+(\mathbb{R}) \rtimes \mathrm{Sym}(3)$, which also generalizes to arbitrary fields F.

16.3. Composition algebras and the octonions

An *F-algebra A* is a vector space over F that admits a bilinear (but not necessarily associative) multiplication. A *composition algebra* is an algebra with identity possessing a nondegenerate quadratic form q admitting composition, which is to say that

$$q(mn) = q(m)q(n)$$

for all $m, n \in A$. In a composition algebra, an element is a unit if and only if $q(m)$ is nonzero. The units form a loop, and those units u with norm $q(u) = 1$ give a normal subloop, as do the scalars. Composition algebras are alternative algebras, and so their loops of units are Moufang loops.

In the earlier parts of this monograph, we used geometry (central Latin square designs) to bridge the gap between Moufang loops (algebra) and groups with triality. In this part, things go a little differently. We use composition algebras, particularly the split octonions, to connect Study's geometric triality and Cartan's group theoretic triality. Both Study [**Stu12, Stu13**] and Cartan [**Car25**] make use of 8-dimensional algebras, Cartan explicitly referring to Cayley algebras.

Composition algebras of dimension 8 are the Cayley or octonion algebras, which are of particular interest here. Historically, the first such algebra was that of the

Cayley-Graves compact real octonions[1] [**SpV00**, p. 23]. For us, the most prominent examples will instead be the split octonions (defined over arbitrary fields), as exemplified by Zorn's vector matrices [**Zor31**]. The Cayley-Graves octonions and the real split octonions are the two real forms of the complex octonions, which must be split.

16.4. Freudenthal's triality

The trialities of Study and Cartan are largely concerned with hyperbolic space; that is, with the split octonions. A version of algebraic triality that goes back at least to the famous 1951 Utrecht notes of Freudenthal (finally published in 1985 [**Fre51, Vel85**]) has the advantage of speaking to all octonion algebras O simultaneously.

In Chapter 20 we study Freudenthal's version, which states that for every similarlity g from the general orthogonal group $\mathrm{GO}(O)$ there are companions $h, k \in \mathrm{GO}(O)$ such that, either

$$x^h y^k = (xy)^g \quad \text{for all } x, y \in O$$

or

$$x^h y^k = (yx)^g \quad \text{for all } x, y \in O\,.$$

Consideration of this version leads to an elementary presentation of the spinor norm and the associated spin group in the special case of orthogonal spaces that support octonion algebras.

16.5. Moufang loops from octonion algebras

The study of Moufang loops began with the study of alternative algebras, of which octonion algebras provide the basic nonassociative examples.

Moufang [**Mou33**] and M. Hall [**Hll43, Hll49**] proved that projective planes in which the Little Theorem of Desargues holds are precisely those coordinatized by alternative division algebras. Moufang [**Mou35**] then studied arbitrary alternative rings, proving among other things that they satisfy the identical relation

$$(\alpha\beta)(\gamma\alpha) = (\alpha((\beta\gamma)\alpha)$$

which we now know as the Moufang identity.

In [**Mou35**] Moufang initiated the subject of Moufang loops, which she called "quasigroups," proving her remarkable theorem that three elements of a Moufang loop that associate in any order must generate an associative subloop—a group.

In our final Chapter 21 we study the Moufang loops that arise from the unit loops in octonion algebras. All known simple nonassociative Moufang loops occur as sections of such unit loops. Of special interest are the Paige loops [**Pai56**], which come from the split octonions. By a theorem of Liebeck [**Lie87**], following on from Doro's original work [**Dor78**], every finite, nonassociative, simple Moufang loop is a Paige loop.

[1] In situations such as this, the word "compact" does not refer to algebra itself but to its automorphism group, which is compact since the invariant form is positive definite.

Chapter 17

Orthogonal Spaces and Groups

Classical, concrete triality lives in the realm of orthogonal 8-space and the groups and algebras associated with it.

17.1. Orthogonal geometry

Throughout this chapter F will be a commutative field and V will be a finite dimensional vector space over F. For any subset W of V, we let $\langle W \rangle \leq V$ be the F-subspace of V spanned by W.

Let $q\colon V \longrightarrow F$ be a *quadratic form* on the F-space V. That is,

$$q(\alpha x) = \alpha^2 q(x)\,,$$

for all $\alpha \in F$ and $x \in V$, and the associated form $h = h_q\colon V \times V \longrightarrow F$, given by

$$h(x,y) = q(x+y) - q(x) - q(y)\,,$$

is bilinear (and symmetric). For any subspace W of V, the restriction of q to W is a quadratic form on W. We call (V,q) an *orthogonal space* or a *quadratic space*. The associated bilinear form h_q will typically be abbreviated to h.

Always $h(x,x) = 2q(x)$. So in characteristic other than 2, the bilinear form h determines q. That is not the case in characteristic 2 where $h(x,x)$ is always 0: h is a *symplectic form*.

If K is an extension of F, then q extends naturally to a quadratic form $q|^K$ on the tensor product $K \otimes_F V = V|^K$. Indeed for any totally ordered set $(I,<)$ and basis $\mathcal{I} = \{\, x_i \mid i \in I \,\}$ of the E-space W, any map $q_I\colon \mathcal{I} \longrightarrow E$ and Gram matrix $\{\, h(x_i,x_j) \in E \mid i < j \,\}$ extends by "linearity" to a unique quadratic form q^W on W.

For $W \subseteq V$, we let $W^\perp = \{x \in V \mid h(x,w) = 0,\ w \in W\}$, an F-subspace of V. The form q is *nondegenerate* if $V^\perp = 0$.

(17.1). Lemma. *Let q be a quadratic form on the finite dimensional F-space V with associated bilinear form h.*

(a) *For each $x \in V$, let $\lambda_x\colon V \longrightarrow F$ be given by $y^{\lambda_x} = h(x,y)$. Then $\lambda\colon V \longrightarrow V^*$ given by $x \mapsto \lambda_x$ is an homomorphism of F-vector spaces. It is an isomorphism if and only if (V,q) is nondegenerate.*

(b) *If* (V, q) *is nondegenerate then* $\dim_F U + \dim_F U^\perp = \dim_F V$ *for each subspace* U*.*

(c) *If* (V, q) *is nondegenerate and* $U \cap U^\perp = 0$*, then* $V = U \oplus U^\perp$ *(which we may write as* $U \perp U^\perp$*).*

(d) (V, q) *is nondegenerate if and only if* $(K \otimes_F V, q|^K)$ *is nondegenerate.*

Proof. The first part is routine, given the definitions. The rest then follows directly. □

A subset S of V is *singular* (or sometimes even *totally singular*) if the restriction of q to S is identically 0. If U is a singular subspace, then q induces a quadratic form on the quotient space $U^\perp/U$, nondegenerate if (V, q) is nondegenerate.

A vector that is not singular is *nonsingular*, and a space (V, q) in which all nonzero vectors are nonsingular is an *asingular space.*

Let (V, q_V) and (W, q_W) be quadratic spaces over F. An *isometry* from (V, q_V) to (W, q_W) is an invertible $g \in \mathrm{Hom}_F(V, W)$ with

$$q_W(v^g) = q_V(v)\,, \text{ for all } v \in V\,.$$

Thus two quadratic F-spaces are essentially the same precisely when they are *isometric.*

One dimensional quadratic spaces Fx are easy to describe: for all $y = \alpha x \in Fx$ we have $q(y) = d\alpha^2$ for the constant $d = q(x)$. (Characteristic 2 quadratic 1-spaces are always degenerate.) The structure of 2-dimensional spaces is crucial.

(17.2). Proposition. *Let* (V, q) *be a quadratic* F*-space of dimension* 2*.*

(a) *If* $0 \neq x \in V$ *is singular with* $x^\perp = V$*, then* (V, q) *is degenerate and, for* $y \in V \setminus Fx$*, we have* $q(\beta x + \gamma y) = e\gamma^2$ *where* $e = q(y)$ *is a constant.*

(b) *If* $0 \neq x \in V$ *is singular with* $x^\perp \neq V$*, then* (V, q) *is nondegenerate and there are exactly two* 1*-spaces in* V *consisting of singular vectors. In this case, we have a basis of singular vectors* x *and* y *with* $h(x, y) = 1$*, hence* $q(\beta x+\gamma y) = \beta\gamma$*. Especially, for each* $\alpha \in F$ *there are* $z \in V$ *with* $q(z) = \alpha$*.*

(c) *If all nonzero vectors of* V *are nonsingular, then there is a quadratic extension* K *of* F *for which the extension* $q|^K$ *of* q *to* $K \otimes_F V = V|^K$ *has nonzero singular vectors and so falls under* (a) *or* (b)*.*

In this case (V, q) *is isometric to* K *(as* F*-space) provided with the quadratic form* $q_K(\kappa) = d\kappa\bar{\kappa}$*, where the bar denotes Galois conjugation in* K *over* F *and* $d \in F$ *is fixed and nonzero. If* K *is separable over* F *then* (V, q) *is nondegenerate; if* K *is inseparable over* F *(which forces* $\mathrm{char} F = 2$*) then* $V = V^\perp$*.*

Proof. (a) This is immediate from the remarks about spaces of dimension 1.

(b) As $q(x) = 0$, $h(x, x) = 0$; so for $w \notin \langle x\rangle = x^\perp$ we have $h(x, w) \neq 0$. If necessary, replace w by a scalar multiple so that $h(x, w) = 1$. Consider $y = \beta x + w$. Then

$$h(x, y) = h(x, w) = 1\,, \text{ and } q(y) = q(\beta x) + q(w) + h(\beta x, w) = q(w) + \beta\,.$$

Therefore $\beta = -q(w)$ gives a second 1-space $\langle y\rangle$ of singular vectors and all other nonzero vectors are nonsingular. Finally

$$q(\beta x + \gamma y) = q(\beta x) + q(\gamma y) + h(\beta x, \gamma y) = 0 + 0 + \beta\gamma = \beta\gamma\,.$$

In particular $q(\alpha x + y) = \alpha$.

(c) Choose a basis $\{u, v\}$ of V with $q(u) = d$, $q(v) = f$, and $h(u, v) = e$. Then $q(\beta u+\gamma v) = d\beta^2+e\beta\gamma+f\gamma^2$. As there are no singular vectors in V, the polynomial $dz^2 + ez + f$ is irreducible of degree 2 in $F[z]$ but has a root α in the quadratic extension $K = F(\alpha)$ of F.

When we identify V with the F-space K via the linear isomorphism given by $u \mapsto 1$ and $v \mapsto -\alpha$, so that $\beta u + \gamma v \mapsto \beta - \alpha\gamma = \kappa$, we find

$$q_K(\kappa) = q(\beta u + \gamma v) = \\ d\beta^2 + e\beta\gamma + f\gamma^2 = d(\beta - \alpha\gamma)(\beta - \bar{\alpha}\gamma) = d(\beta - \alpha\gamma)\overline{(\beta - \alpha\gamma)} = d\kappa\bar{\kappa}\,.$$

The space $(V|^K, q|^K)$ contains the singular 1-space spanned by $\alpha u + v$ and so comes under (a) or (b). We have $V|^K = K(\alpha u+v)\oplus Kv$ with $h|^K(\alpha u+v, \alpha u+v) = 0$. We calculate

$$\begin{aligned} h|^K(\alpha u + v, -v) &= q|^K(\alpha u + v - v) - q|^K(\alpha u + v) - q|^K(-v) \\ &= \alpha^2 q(u) - 0 - q(-v) \\ &= d\alpha^2 - f \\ &= d\alpha^2 - f - (d\alpha^2 + e\alpha + f) \\ &= -e\alpha - 2f\,. \end{aligned}$$

As $dz^2 + ez + f$ is irreducible of degree 2 in $F[z]$, necessarily $d \neq 0 \neq f \in F$. But $\alpha \notin F$, so the quantity $-e\alpha - 2f$ is zero if and only if $e = 0$ and $\mathrm{char}(F) = 2$. This is in turn the case if and only if the polynomial and K are both inseparable over F.

Thus if K is separable over F then $(V|^K, q|^K)$ is nondegenerate as in (b), and (V, q) is also nondegenerate by Lemma (17.1)(d). If K is inseparable over F, then $V|^K = K(\alpha u + v) \perp Kv$ with $h|^K(v, v) = h(v, v) = 2q(v) = 0$. Thus $h|^K$ and h as well are identically 0, and $V = V^\perp$. □

In part (b) of the proposition, V is a *hyperbolic 2-space*. The basis pair $\{x, y\}$ of singular vectors x and y with $h(x, y) = 1$ is a *hyperbolic pair*. The hyperbolic pairs in V are precisely the pairs $\{\beta^{-1}x, \beta y\}$ for nonzero β in F.

(17.3). COROLLARY. *If (V, q) is a nondegenerate quadratic space of dimension 2 over the algebraically closed field F, then (V, q) is hyperbolic.*

PROOF. Nondegeneracy puts us in (b) or (c) of the proposition, while algebraic closure implies that no quadratic extension K as in (c) exists. □

(17.4). COROLLARY. *If (V, q) is a nondegenerate quadratic space of dimension at least 3 over the finite field $\mathbb{F}_r$, then V contains nonzero singular vectors.*

PROOF. Choose x and y in V with $h(x, y) \neq 0$, and set $H = \langle x, y\rangle$. If H contains singular vectors, then we are done. Otherwise, by the proposition nondegenerate H is a copy of $\mathbb{F}_{r^2}$ with quadratic form $q(\kappa) = d\kappa^{1+r}$ for nonzero $d \in \mathbb{F}_r$. The map $\kappa \mapsto \kappa^{1+r}$ is a surjective homomorphism from the cyclic multiplicative subgroup of $\mathbb{F}_{r^2}$ of order $r^2 - 1$ to the order $r - 1$ multiplicative subgroup of its subfield $\mathbb{F}_r$. In particular for $0 \neq z \in H^\perp$, there is a $w \in H$ with $q(w) = -q(z)$; so $w + z$ is a nonzero singular vector. □

17.2. Hyperbolic orthogonal spaces

The orthogonal space (V,q) admits the *hyperbolic basis* $\mathcal{H} = \{\dots, f_i, g_i, \dots\}$ $(1 \le i \le m)$ provided for all i,j,l:

$$q(f_i) = q(g_j) = h(f_i,f_l) = h(g_j,g_l) = 0\,,\ h(f_i,g_j) = \delta_{i,j}\,.$$

Especially the dimension $2m$ of V is even and q is nondegenerate. The integer m is the *index* of the form.

A hyperbolic 2-space of course provides an example, but so does the 4-dimensional F-space $\mathrm{Mat}_2(F)$ of 2×2 matrices over F with q the determinant function There the four matrix units form a hyperbolic basis (up to sign).

If (V,q) has a hyperbolic basis, then we say that q and V are *split* or *hyperbolic.*

(17.5). Proposition. *If q is a nondegenerate quadratic form on the F-space V of finite dimension, then the following are equivalent:*

(1) *V has a hyperbolic basis.*

(2) *V is a perpendicular direct sum of hyperbolic 2-spaces.*

(3) *Every maximal singular subspace has dimension $\dim_F(V)/2$.*

(4) *There are maximal singular subspaces M and N with $V = M \oplus N$.*

(5) *There is a singular subspace of dimension at least $\dim_F(V)/2$.*

(6) *For any basis χ of the totally singular subspace X, V has a hyperbolic basis containing χ.*

Proof. (1) and (2) are clearly equivalent, and both are consequences of (6). (5) is a consequence of all the others. If the hyperbolic basis of (1) is the one given above, then the spaces $M = \langle \dots, f_i \dots \rangle$ and $N = \langle \dots, g_i, \dots \rangle$ are maximal singular with $V = M \oplus N$, as in (4).

Also (6) implies (3) as every singular subspace spanned by a subset of a hyperbolic basis is contained in such a maximal singular subspace of dimension $\dim_F(V)/2$.

It remains to prove that (5) implies (6), which we do by induction on $\dim(V)$ with Proposition (17.2) providing the initial step. (The case of dimension 1 being trivial since nondegenerate 1-spaces contain no nonzero singular vectors.) If M is a singular subspace of dimension at least $\dim(V)/2$ and z is singular, then $z^\perp \cap M$ contains a hyperplane of M and singular $\langle z, z^\perp \cap M\rangle$ has dimension at least that of M. Thus, if necessary replacing M or enlarging χ, we may assume that $M \cap \chi$ is nonempty. Let $x \in M \cap \chi$. Then, for any y in $(\chi \setminus \{x\})^\perp$ but not its hyperplane $\chi^\perp$, the 2-space $\langle x,y\rangle$ is hyperbolic by Proposition (17.2). Nondegenerate $\langle x,y\rangle^\perp$ contains $M \cap y^\perp$ and $\chi \setminus \{x\}$. By induction $\chi \setminus \{x\}$ embeds in a hyperbolic basis of $\langle x,y\rangle^\perp$, and therefore χ is in a hyperbolic basis of V. □

(17.6). Corollary. *The two finite dimensional hyperbolic spaces (V,q_V) and (W,q_W) over F are isometric if and only if they have the same dimension.*

Proof. Both spaces have hyperbolic bases, and it is possible to map one of these to the other by an invertible linear transformation if and only if they have the same cardinality. □

(17.7). Proposition. *If (V,q) is a nondegenerate quadratic space of dimension $2m$ over the algebraically closed field F, then (V,q) is hyperbolic and unique up to isometry (indeed similarity).*

Proof. This follows by induction from the previous corollary and Corollary (17.3). □

As arbitrary F can be tensored up to an algebraically closed field, the proposition provides a tool for reducing general questions to the hyperbolic case.

(17.8). Proposition. *Let the quadratic form q be hyperbolic on the F-space V of dimension $2m$.*

(a) *Every singular $(m-1)$-space is contained in exactly two singular m-spaces.*
(b) *Let W be a maximal singular subspace, and let S be a singular subspace not contained in W. Then for every $s \in S \setminus W$ there is a unique maximal singular subspace T with $s \in T$ and $W \cap T$ of dimension $m-1$. The space T is $\langle s, s^\perp \cap W\rangle$, and $\dim_F(S \cap T) = 1 + \dim_F(S \cap W)$.*

Proof. (a) If U has codimension 1 in a maximal singular subspace, then $U^\perp/U$ is a hyperbolic 2-space; so (a) follows from Proposition (17.2).

(b) As $s \notin W$, $s^\perp \cap W$ is a hyperplane of W and $T = \langle s, s^\perp \cap W\rangle$ is a singular m-space. It is unique since any T as described must contain s, whence $T \cap W \leq s^\perp \cap W$.

The hyperplane $T \cap W = s^\perp \cap W$ of T contains $S \cap W$, so the dimension of $S \cap T$ is equal to that of $S \cap W$ or exceeds it by 1. But $s \in T \setminus W$. □

(17.9). Proposition. *Let the quadratic form q be hyperbolic on the F-space V of dimension $2m$.*

The graph $(\mathcal{M}, \sim)$ on the set $\mathcal{M}$ of maximal singular subspaces, with two such adjacent when their intersection has codimension 1 in each, is connected and bipartite of diameter m. In this graph, the distance between two maximal singular subspaces M and N equals the codimension of $M \cap N$ in each.

Proof. We first claim that, for all $S \in \mathcal{M}$ and $T_1 \sim T_2$ in $\mathcal{M}$, we have

$$|\dim(S \cap T_1) - \dim(S \cap T_2)| = 1\,.$$

Let $U = T_1 \cap T_2$ of codimension 1 in each, and set $R = S \cap U$. If necessary passing to $R^\perp/R$, we may assume $R = 0$ in proving the claim. Then $U^\perp$ has dimension $m+1$ and so intersects S nontrivially. Therefore $T = \langle U, U^\perp \cap S\rangle$ is totally singular of dimension m. By the previous proposition, T is equal to exactly one of T_1 or T_2. Thus

$$\{\dim(S \cap T_1), \dim(S \cap T_2)\} = \{0, 1\}\,,$$

giving the claim.

Let $d(M,N)$ be the distance between M,N in $(\mathcal{M}, \sim)$. Again by the previous proposition, $d(M,N) \leq m - \dim(M \cap N)$. In particular the graph is connected.

To prove $d(M,N) = m - \dim(M \cap N)$, we induct on $d(M,N)$. The result is true by definition for $d(M,N) = 0, 1$. Suppose $d(M,N) = d$, and choose a $T \in \mathcal{M}$ with $T \sim N$ and $d(T,M) = d-1$. Then by induction $d-1 = m - \dim(M \cap T)$. By the preceding paragraph and the claim $d \leq m - \dim(M \cap N) = (d-1) \pm 1 \leq d$, as desired.

It remains to prove $(\mathcal{M}, \sim)$ bipartite. Otherwise, there is a minimal cycle $\mathcal{C}$ of odd length, say $2k+1$. But for $S \in \mathcal{C}$, the two vertices T_1 and T_2 at distance k from S in $\mathcal{C}$ are adjacent with $\dim(S \cap T_1) - \dim(S \cap T_2) = 0$, contradicting the earlier claim. □

17.3. Oriflamme geometries

Let (V, q) be a hyperbolic orthogonal space of dimension $2m$. Consider the graph $(\Gamma, \sim)$ whose vertices are the nonzero singular spaces of V. Two singular spaces are *incident* (that is, adjacent in Γ) precisely when

> *one is properly contained in the other* or *they both have dimension m and intersect in a $(m-1)$-space.*

This graph is $(m+1)$-partite by Proposition (17.9) above, with the collection $\mathcal{M}$ of m-spaces falling into two parts $\mathcal{M}^\rho$ and $\mathcal{M}^\lambda$ while the remaining singular subspaces provide a part $\mathcal{S}_k$ for each dimension $1 \leq k \leq m-1$.

The associated *oriflamme geometry* or D_m*-geometry* is this graph with the part $\mathcal{S}_{m-1}$ (the vertices of dimension $m-1$) removed. We can recover the graph $(\Gamma, \sim)$ from its oriflamme geometry, since by Proposition (17.8) there is a bijection between the spaces of $\mathcal{S}_{m-1}$ and the edges between $\mathcal{M}^\rho$ and $\mathcal{M}^\lambda$ in which a singular $(m-1)$-space is incident precisely with the endpoints of its edge and the spaces of smaller dimension incident to both of those endpoints.

By Corollary (17.6) a D_m-geometry over F is uniquely determined up to isomorphism by m and F.

17.4. Orthogonal groups

Let q be a quadratic form on V. An *isometry* of (V, q) is a $g \in \mathrm{GL}(V)$ with

$$q(v^g) = q(v)\,, \text{ for all } v \in V\,.$$

The full *isometry group* of (V, q) is then $\mathrm{O}(V, q)$, the *orthogonal group.* A *similarity* of (V, q) is a $g \in \mathrm{GL}(V)$ with

$$q(v^g) = \mu_g q(v)\,, \text{ for all } v \in V\,,$$

for some nonzero constant *multiplier* $\mu_g \in F$. The full *similarity group* of (V, q) is $\mathrm{GO}(V, q)$, the *general orthogonal group.*

An isometry g is precisely a similarity with $\mu_g = 1$. Indeed the map $\mu\colon g \mapsto \mu_g$ is a homomorphism from $\mathrm{GO}(V, q)$ to $\mathbb{F}$ with kernel $\mathrm{O}(V, q)$. Each nonzero scalar transformations αI is a similarity with multiplier α^2, but only $\pm I$ are isometries. The scalars subgroups are central, and we write $\mathrm{PO}(V, q)$ for the *projective orthogonal group* $\mathrm{O}(V, q)/\{\pm I\}$ and $\mathrm{PGO}(V, q)$ for the *projective similarity group* $\mathrm{GO}(V, q)/F^\times I$.

Similarly, a *similarity* of the associated bilinear form $h = h_q$ is a $g \in \mathrm{GL}(V)$ with

$$h(v^g, w^g) = \mu_g h(v, w)\,,$$

for all $v, w \in V$ and some nonzero constant $\mu_g \in F$. An *isometry* g of h is then a similarity with $\mu_g = 1$.

Clearly an isometry (or similarity) of q gives one of h. In characteristic 2 the converse is not true in general.

For the linear transformation t on V, we set $[V, t] = V^{t-1}$ and $\mathrm{C}_V(t) = \{\, v \in V \mid v^t = v \,\}$.

(17.10). Lemma. *Let t be an isometry of the nondegenerate quadratic space (V, q). Then $[V, t] = \mathrm{C}_V(t)^\perp$.*

Proof. For all $v \in V$ and fixed w,

$$\begin{aligned} h(v^{t-1}, w) &= h(v^t, w) - h(v, w) \\ &= h(v^t, w) - h(v^t, w^t) \\ &= h(v^t, w^{1-t}) . \end{aligned}$$

As q and h are nondegenerate and t invertible, $w \in [V, t]^\perp$ if and only if $w \in \mathrm{C}_W(t)$. □

(17.11). Proposition. *Let (V, q) be a nondegenerate quadratic space over F.*

(a) *Let t be an isometry with $\dim_F[V, t] = 1$. Then there is a nonsingular $x \in V$ with $[V, t] = \langle x \rangle$ and*

$$t\colon v \mapsto v - q(x)^{-1} h(v, x)x .$$

(b) *Conversely, for every nonsingular $x \in V$ the map*

$$\mathrm{s}_x\colon v \mapsto v - q(x)^{-1} h(v, x)x .$$

is an isometry of order 2 of the quadratic form q on V (and so also of h) with $[V, \mathrm{s}_x] = \langle x \rangle$. If the characteristic of F is not 2, then the symmetry s_x is the reflection in the hyperplane $x^\perp = \mathrm{C}_V(\mathrm{s}_x)$.

(c) *$\mathrm{s}_x = \mathrm{s}_y$ if and only if $y = \alpha x$ for some nonzero $\alpha \in F$.*

(d) *If g is an isometry of (V, q), then $g^{-1}\,\mathrm{s}_x\, g = \mathrm{s}_{x^g}$.*

(e) *For $W \le V$, $W^{\mathrm{s}_x} = W$ if and only if $x \in W$ or $W \le x^\perp$.*

Proof. Consider an arbitrary linear transformation $t\colon V \longrightarrow V$ with $[V, t] = \langle x \rangle$, for some nonzero $x \in V$. The kernel of the map $v \mapsto v^{t-1}$ is then $\mathrm{C}_V(t)$, a hyperplane of V. The image of v is $(v^\tau)x$, for some linear functional τ on V with $\ker \tau = \mathrm{C}_V(t)$.

By the previous lemma, for t to have any chance at all of being an isometry, we must have $\mathrm{C}_V(t) = x^\perp$; so we may assume $v^\tau = \beta h(v, x)$ for some nonzero constant β, and

$$t\colon v \mapsto v + \beta h(v, x)x .$$

Now t is an isometry of (V, q) if and only if $q(v^t) = q(v)$ for all $v \in V$. We calculate

$$\begin{aligned} q(v^t) - q(v) &= q(v + \beta h(v, x)x) - q(v) \\ &= q(v) + q(\beta h(v, x)x) + h(v, \beta h(v, x)x) - q(v) \\ &= \beta^2 h(v, x)^2 q(x) + \beta h(v, x)h(v, x) \\ &= \beta h(v, x)^2(\beta q(x) + 1) . \end{aligned}$$

This is 0 whenever $v \in x^\perp$, but for $v \notin x^\perp$ this is 0 if and only if $\beta q(x)+1 = 0$. That is, t is an isometry if and only if $\beta = -q(x)^{-1}$; especially, x must be nonsingular.

We have $t = \mathrm{s}_x$, and

$$\begin{aligned} x^{\mathrm{s}_x} &= x - q(x)^{-1} h(x, x)x = x - q(x)^{-1}(q(2x) - q(x) - q(x))x \\ &= x - q(x)^{-1}(2q(x))x = -x . \end{aligned}$$

In particular, for arbitrary $v \in V$ with $\gamma = v^\tau \in F$,

$$v^{\mathrm{s}_x^2 -1} = v^{(\mathrm{s}_x -1)(\mathrm{s}_x +1)} = (\gamma x)^{\mathrm{s}_x +1} = (\gamma x)^{\mathrm{s}_x} + \gamma x = -(\gamma x) + \gamma x = 0 .$$

That is, the isometry s_x has order 2. Furthermore, we see that in characteristic other than 2 the element s_x is precisely reflection in the hyperplane $x^\perp$.

If $\mathrm{s}_x = \mathrm{s}_y$, then certainly

$$Fx = [V, \mathrm{s}_x] = [V, \mathrm{s}_y] = Fy$$

and $y = \alpha x$, for some constant α, nonzero as $\mathrm{s}_y \neq 1_V$. On the other hand, if $y = \alpha x$ then

$$q(y)^{-1}h(v,y)y = q(\alpha x)^{-1}h(v,\alpha x)\alpha x = \alpha^{-2}\alpha^2 q(x)^{-1}h(v,x)x$$

and $\mathrm{s}_x = \mathrm{s}_y$.

For any isometries f and g we have $[V,f]^g = [V^g, f^g] = [V, f^g]$. If $f = \mathrm{s}_x$ then $[V, \mathrm{s}_x^g]$ has dimension 1, and the only possibility is $\mathrm{s}_x^g = \mathrm{s}_{x^g}$.

Finally, if s_x-invariant W is not in $x^\perp = \mathrm{C}_W(\mathrm{s}_x)$, then $0 \neq W^{t-1} \leq Fx$ of dimension 1, hence $x \in W$. The converse is easy. □

The isometry s_x is a *symmetry* of (V,q).

(17.12). PROPOSITION. *Let (V,q) be a hyperbolic space over of finite dimension $2m$ over F.*

(a) *The group $\mathrm{GO}(V,q)$ induces automorphisms of the bipartite graph $(\mathcal{M}, \sim)$ (of Proposition (17.9)) whose vertex set $\mathcal{M}$ consists of all singular m-subspaces, two such adjacent provided their intersection has codimension 1 in each.*

(b) *If s_x is a symmetry of $\mathrm{O}(V,q)$ and $M \in \mathcal{M}$ is a singular m-space, then $M \sim M^{\mathrm{s}_x}$. In particular symmetries switch the two parts, so $\mathrm{O}(V,q)$ and $\mathrm{GO}(V,q)$ have normal subgroups of index 2 that globally fix the two parts of the bipartition.*

(c) *For $m \geq 2$, the kernel of the action of $\mathrm{GO}(V,q)$ on $(\mathcal{M}, \sim)$ consists of the scalars.*

PROOF. Part (a) is clear. $M = M^\perp$ for every maximal singular space, so $x^\perp \cap M$ is a hyperplane of M that is equal to $M \cap M^{\mathrm{s}_x}$. Thus $M \sim M^{\mathrm{s}_x}$, giving (b).

For (c) first note that every singular 1-space is the intersection of those singular m-spaces containing it, so $\mathrm{GO}(V,q)$ acts on the set of all singular 1-spaces. The kernel of the action on $(\mathcal{M}, \sim)$ then fixes each 1-space. Easy and familiar linear algebra next says that an element g of this kernel is scalar on each maximal singular subspace. As $m \geq 2$ and $(\mathcal{M}, \sim)$ is connected, the scalar in question is the same for all maximal singular subspaces; and g is scalar on all of V. □

The subgroup of index 2 within $\mathrm{O}(V,q)$ found in the theorem will be written as $\mathrm{SO}(V,q)$ and is the *special orthogonal group*. At this stage this definition only applies to hyperbolic spaces (V,q). The groups induced on $(\mathcal{M}, \sim)$ are the corresponding matrix groups modulo their scalar subgroups and are the projective groups, respectively, $\mathrm{PGO}(V,q)$ and $\mathrm{PO}(V,q)$ (both already seen) and the new *projective special orthogonal group* $\mathrm{PSO}(V,q)$, which is $\mathrm{SO}(V,q)/\{\pm I\}$. Again, this last is presently only defined in the hyperbolic case.[1]

As we saw in Corollary (17.6), a finite dimensional hyperbolic space is characterized up to isometry by its dimension $2m$ and defining field F. Therefore in the hyperbolic case, the groups defined above may be, and often will be, written as $\mathrm{GO}^+_{2m}(F)$, $\mathrm{O}^+_{2m}(F)$, $\mathrm{SO}^+_{2m}(F)$, $\mathrm{PGO}^+_{2m}(F)$, $\mathrm{PO}^+_{2m}(F)$, and $\mathrm{PSO}^+_{2m}(F)$, these parameters determining the groups up to isomorphism.

[1] But see Section 20.2.

17.5. Chevalley groups $\mathrm{D}_n(F)$

In the previous section we investigated isometries t with $[V,t] = V(t-1)$ of dimension 1, because they are "small"—they are close to being the identity. Proposition (17.12) showcases one difficulty with the resulting orthogonal symmetries—they are not in the derived subgroup of the group they generate. Especially they do not sit as "low down" in the group as they might. A related issue is that they are associated with the nonsingular parts of the associated geometry whereas the oriflamme D_m-geometry is constructed out of singular pieces. These failings were forced on us by our quest for an isometry t with $[V,t]$ of dimension 1.

We now investigate isometries g with $L = [V,g]$ of dimension 2. There are three cases to consider, depending upon the dimension of the intersection of L with $L^\perp = \mathrm{C}_V(g)$ (by Lemma (17.10)). If that dimension is 0, then L is nondegenerate, $V = L \oplus L^\perp$, and the appropriate isometries are those from $\mathrm{O}(L, q|_L)$ extended to all of V by $\mathrm{Id}\,|_{L^\perp}$.

In the remaining two cases, there is (at least) a 1-space $\langle u\rangle \le L \cap L^\perp$. Then g must globally stabilize the series $\langle u\rangle \le \langle u\rangle^\perp \le L$, acting trivially on the 1-spaces $\langle u\rangle$ and $L/\langle u\rangle^\perp$. For singular u, the isometries g that additionally are trivial on the quotient $\langle u\rangle^\perp/\langle u\rangle$ are the *Siegel elements* of $\mathrm{O}(V,q)$. These are the correct "low, small" elements to study [**Tay92**] when investigating the normal structure of the orthogonal group in the presence of nonzero singular vectors.[2]

In the happiest situation, when L is totally singular (and, in particular, contained in $L^\perp$), there is a basis u, v of L with

$$g\colon x \mapsto x + h(x,v)u - h(x,v)v\,.$$

This element g is a *long root element* of $\mathrm{O}(V,q)$.

Elementary calculation shows that long root elements enjoy, and indeed are characterized by, the following properties:

(17.13). PROPOSITION. *Consider the nondegenerate quadratic space (V,q).*

(a) *The isometry g is a long root element if and only if $V(g-1) = L$ is totally singular of dimension 2 and $V(g-1)^2 = 0$.*
(b) *The set R_L of all long root elements g with $[V,g] = L$ together with the identity is a subgroup of $\mathrm{O}(V,q)$ isomorphic to $(F,+)$.*
(c) *The elements of R_L act trivially on $L^\perp$. For each singular $x \in V \setminus L^\perp$, there is a unique 1-space $\langle y\rangle$ in $x^\perp \cap L$, and R_L stabilizes and is regular on the 1-spaces of $\langle x,y\rangle \setminus \langle y\rangle$.* □

The subgroups R_L are the *long root subgroups*. For hyperbolic forms (at least) they sit in $\mathrm{SO}(V,q)$ by the last part of the lemma. We also use the language of long root elements and long root subgroups for their (isomorphic) images in the corresponding projective groups. Especially, within the projective hyperbolic orthogonal groups $\mathrm{PSO}^+_{2m}(F)$ the subgroup generated by all long root subgroups is the *Chevalley group* $\mathrm{D}_m(F)$, and we take this as our definition of $\mathrm{D}_m(F)$ (see [**Ree57**]).

[2] The asingular case is much more varied and difficult.

17.6. Orthogonal groups in dimension 8

We present some important results about orthogonal groups and geometries in dimension 8, the proofs of which we either postpone or do not provide at all.

(17.14). THEOREM. (CARTAN) *Let (V, q) be a nondegenerate, finite dimensional quadratic space that is asingular. Then $\mathrm{O}(V, q)$ is generated by its symmetries.* □

This result has a famous extension, the Cartan-Dieudonné Theorem, which says that almost all orthogonal groups are generated by their symmetries; see [**Asc00**, (22.7)] and [**Tay92**, Cor. 11.42]. We need one further special case:

(17.15). THEOREM. *Let (V, q) be hyperbolic of dimension 8. Then $\mathrm{O}(V, q) = \mathrm{O}_8^+(F)$ is generated by its symmetries.* □

The *spinor norm* on $\mathrm{SO}_8^+(F)$ is the homomorphism with image $F^\times/(F^\times)^2$ that is given by

$$\prod_i \mathrm{s}_{x_i} \mapsto \prod_i q(x_i)(F^\times)^2\,.$$

By Theorem (17.15), every element of $\mathrm{SO}_8^+(F)$ can be factored as $\prod_i \mathrm{s}_{x_i}$. Such factorizations will not be unique, so it is unclear whether or not the spinor norm as described is a well-defined homomorphism. This is the case even more generally. A proof requires work and will be given later (Theorem (20.9)) in the cases of interest to us.

The group $\Omega_8^+(F)$ is defined to be the kernel of the spinor norm, with central quotient $\mathrm{P}\Omega_8^+(F)$. But for the moment[3] the first part of the next theorem can be thought of as giving the definition of $\Omega_8^+(F)$.

(17.16). THEOREM.

(a) $\Omega_8^+(F) = \mathrm{O}_8^+(F)'$, *the derived subgroup, which is perfect.*

(b) $\mathrm{P}\Omega_8^+(F) = \mathrm{PSO}_8^+(F)'$ *is simple.*

(c) $\mathrm{P}\Omega_8^+(F) = \mathrm{D}_4(F)$, *the subgroup generated by the long root subgroups.*

PROOF. (a) Taylor [**Tay92**, 11.51] proves that the kernel of the spinor norm on $\mathrm{SO}_8^+(F)$ is equal to the derived group $\mathrm{O}_8^+(F)'$. He also shows in [**Tay92**, 11.47] that this derived group is perfect.

(b) The group $\mathrm{PO}_8^+(F)' = \mathrm{P}\Omega_8^+(F)$ is simple by [**Tay92**, Theorem 11.48].

(c) By [**Tay92**, Theorem 11.46] the derived group $\mathrm{O}_8^+(F)'$ is generated by the Siegel elements of $\mathrm{O}_8^+(F)$. In particular, the group $\mathrm{D}_4(F)$, generated by the long root subgroups, is a nontrivial normal subgroup of $\mathrm{PO}_8^+(F)$ contained in $\mathrm{PO}_8^+(F)'$. As this latter group is simple we must have $\mathrm{P}\Omega_8^+(F) = \mathrm{PO}_8^+(F)' = \mathrm{D}_4(F)$. (Ree [**Ree57**, §6] proved $\mathrm{D}_4(F) = \mathrm{PO}_8^+(F)'$ in the Chevalley context.) □

[3] and often in the literature: [**Asc00**, p. 89], [**Tay92**, p. 136]

Chapter 18

Study's and Cartan's Triality

Study's triality [**Stu12, Stu13**] is that of hyperbolic 8-space; see Theorem (18.5) below. Cartan's triality group [**Car25**] is then the corresponding group

$$\mathrm{P}\Omega_8^+(F) \rtimes \mathrm{Sym}(3) = \mathrm{D}_4(F) \rtimes \mathrm{Sym}(3)\,;$$

see Theorem (18.13) below.

We will use the approach of Tits [**Tit58**] to prove that Cartan's triality group is a group with triality in our sense. This group was the motivating example for Doro [**Dor78**] in introducing this terminology.

18.1. Triality geometries and Study's triality

Let (V, q) be a hyperbolic quadratic space of dimension 8 over the field F.

Recall from Section 17.3 that the associated oriflamme D_4-geometry is the 4-partite graph $\mathcal{D}_4$ with parts the singular 1-spaces $\mathcal{S}_1$, the singular 2-spaces $\mathcal{S}_2$, and the two classes $\mathcal{M}^\lambda$ and $\mathcal{M}^\rho$ of singular 4-spaces (as in Proposition (17.9)), with adjacency being given by containment except that $M \in \mathcal{M}^\lambda$ is adjacent to $N \in \mathcal{M}^\rho$ precisely when $M \cap N$ has dimension 3.

The associated *triality graph* $\mathcal{T}(V, q)$ is the induced tripartite subgraph $\mathcal{T} = \mathcal{T}^1 \cup \mathcal{T}^2 \cup \mathcal{T}^3$ of $\mathcal{D}_4$, with parts $\mathcal{T}^1 = \mathcal{S}_1$, $\mathcal{T}^2 = \mathcal{M}^\lambda$, and $\mathcal{T}^3 = \mathcal{M}^\rho$.

(18.1). Theorem. *Let $\{i, j, k\} = \{1, 2, 3\}$. For every nonincident pair $p_i \in \mathcal{T}^i$ and $p_j \in \mathcal{T}^j$, there is a unique $p_k \in \mathcal{T}^k$ that is incident to both p_i and p_j.*

Proof. There are two distinct cases: $\{i, j\} = \{1, 2\}$ and $\{i, j\} = \{2, 3\}$.

The case $\{i, j\} = \{1, 2\}$ is contained in Proposition (17.8)(b) with $p_1 = S$, $p_2 = U$, and $p_3 = T = \langle S, S^\perp \cap U\rangle$.

The case $\{i, j\} = \{2, 3\}$ comes from Proposition (17.9): as p_2 and p_3 are not incident, their intersection must have dimension 1—the unique singular 1-space $p_1 = p_2 \cap p_3 \in \mathcal{T}^1$ incident to both p_2 and p_3. □

(18.2). Corollary. *The graph $\mathcal{T}$ is a $\mathcal{T}$-geometry in the sense of Section 15.4.*

Proof. This is immediate from Theorem (18.1). □

We shall see in Theorem (18.7) below that $\mathcal{T}$ is furthermore a symmetric $\mathcal{T}$-geometry, again in the sense of Section 15.4.

We first observe that, as with the associated oriflamme D_4-geometry, the triality graph is determined uniquely up to isomorphism by F, again by Corollary (17.6).

(18.3). LEMMA.

(a) *For each singular* 2*-space* $L \in \mathcal{S}_2$*, let* $\mathcal{T}_L$ *be the subgraph of* $\mathcal{T}$ *of those singular* 1*-spaces and* 4*-spaces incident to* L*. Then* $\mathcal{T}_L$ *is a complete tripartite subgraph of* $\mathcal{T}$*, with each part of cardinality* $|K|+1$ *(a projective line).*

(b) *If* T *is a complete tripartite (or bipartite) subgraph of* $\mathcal{T}$ *meeting at least two parts of* $\mathcal{T}$ *in at least two vertices, then there is a unique singular* 2*-space* $L \in \mathcal{S}_2$ *with* $T \subseteq \mathcal{T}_L$*.*

PROOF. The singular 1-spaces incident to L are certainly incident to any singular subspace containing it. Now let $M \in \mathcal{T}_L \cap \mathcal{T}^2$ and $N \in \mathcal{T}_L \cap \mathcal{T}^3$. $M \cap N$ has odd codimension in each (see Proposition (17.9)(b)) and dimension at least 2. Thus $\dim(M \cap N) = 3$, and M and N are incident in $\mathcal{T}$. This proves $\mathcal{T}_L$ to be complete tripartite. For (a) it remains to show that each $\mathcal{T}_L \cap \mathcal{T}^i$ (for $i = 1, 2, 3$) has the structure of a projective line over K. This is clear for $i = 0$. Consider a singular 3-space H containing L. This represents an arbitrary singular 1-space in the quotient orthogonal geometry $L^\perp/L$, split of dimension 4. By Proposition (17.9)(a), this is contained in exactly two maximal 4-spaces, one in $\mathcal{T}^2$ and the other in $\mathcal{T}^3$. Thus each $\mathcal{T}_L \cap \mathcal{T}^i$, for $i = 2, 3$, induces a partition of the singular 1-spaces of the geometry $L^\perp/L$ into singular 2-spaces. As M/L runs through the 1-spaces of $(\mathcal{T}_L \cap \mathcal{T}^2)/L$, the 2-space $N/L \in (\mathcal{T}_L \cap \mathcal{T}^3)/L$ meets each in exactly one singular 1-space. Projectively, we have the two transverse rulings of the Klein quadric associated with $L^\perp/L$.

For (b), first suppose distinct $\langle x\rangle, \langle y\rangle \in T \cap \mathcal{T}^1$ and distinct $M, M' \in T \cap \mathcal{T}^2$. Then $\langle x\rangle, \langle y\rangle$ are contained in M; so they span a singular 2-space L, which in turn is incident to any 4-space incident to both $\langle x\rangle$ and $\langle y\rangle$, including all those of T. By the previous paragraph $M \cap M' = L$; so any singular 1-space of T, being incident to both M and M', must also belong to L. Thus $T \subseteq \mathcal{T}_L$, as desired. The case in which T is known to meet both $\mathcal{T}^2$ and $\mathcal{T}^3$ in sets of size at least 2 is similar. This completes (b). □

(18.4). PROPOSITION.

(a) *Define a new set of vertices,* $\mathcal{L}$*, whose elements are the maximal complete tripartite subgraphs* $\mathcal{T}_L$ *of* $\mathcal{T}$*, and connect each new vertex* $\mathcal{T}_L$ *to the vertices of* $\mathcal{T}_L$ *in* $\mathcal{T}$*. Then the new* 4*-partite graph* $\mathcal{T} \cup \mathcal{L}$ *is isomorphic to* $\mathcal{D}_4$ *via the identity on* $\mathcal{T}$ *and the correspondence* $L \leftrightarrow \mathcal{T}_L$*.*

(b) *The automorphism groups of the* 4*-partite graph* $\mathcal{D}_4$ *and the tripartite graph* $\mathcal{T}$ *leave the various parts fixed globally and are isomorphic under the restriction of an automorphism of* $\mathcal{D}_4$ *to the vertices of its subgraph* $\mathcal{T}$*.*

PROOF. Part (a) is immediate from the lemma.

(b) First consider $\mathcal{T}$ and $\mathrm{Aut}(\mathcal{T})$. If two distinct vertices of $\mathcal{T}^i$ are collinear (that is, both adjacent in $\mathcal{D}_4$ to a vertex L of $\mathcal{S}_2$), then as in Lemma (18.3) they lie in the complete tripartite subgraph $\mathcal{T}_L$ of $\mathcal{T}$. If two distinct vertices of $\mathcal{T}^i$ are not collinear, then they have no common neighbors in $\mathcal{T}$ (indeed in $\mathcal{D}_4$). On the other hand, two nonadjacent vertices of $\mathcal{T}$ not together in one of the $\mathcal{T}^i$ have exactly one common neighbor by Theorem (18.1). Therefore $\mathrm{Aut}(\mathcal{T})$ respects the tripartition of $\mathcal{T}$ into the $\mathcal{T}^i$. By (a) each automorphism of $\mathcal{T}$ extends to an automorphism of $\mathcal{D}_4$.

Now examine $\mathcal{D}_4$ and $\mathrm{Aut}(\mathcal{D}_4)$. For every vertex $L \in \mathcal{S}_2$, the neighborhood of L in $\mathcal{D}_4$ is the complete tripartite graph $\mathcal{T}_L$. No vertex of $\mathcal{D}_4$ not in $\mathcal{S}_2$ has a complete multipartite neighborhood in $\mathcal{D}_4$ (for instance, because its neighborhood in $\mathcal{S}_2$ is very large). Therefore $\mathrm{Aut}(\mathcal{D}_4)$ globally fixes the part $\mathcal{S}_2$, and thus every automorphism of $\mathcal{D}_4$ acts on $\mathcal{T} = \mathcal{D}_4 \setminus \mathcal{S}_2$. If two automorphisms g and h of $\mathcal{D}_4$ have the same restriction to $\mathcal{T}$, then gh^{-1} fixes each vertex of each $\mathcal{T}^i$. In this case, every maximal tripartite subgraph of $\mathcal{T}$ is fixed, hence every subgraph $\mathcal{T}_L$ is fixed and so every vertex of $\mathcal{S}_2$ is fixed. That is, $gh^{-1} = 1$ and $g = h$. □

In the next chapter we extensively study the algebra of the octonions. During this, an algebraic proof of the following Theorem (18.5)(b) will emerge and be stated as Theorem (19.29). Thus here we sketch a geometric proof of the equivalent Theorem (18.5)(a). This proof is due to Cameron [**Cam92**] with modifications due to Shult (personal communication).

(18.5). THEOREM.

(a) (STUDY'S TRIALITY) *The automorphism group of the oriflamme* D_4*-geometry permutes the three parts* $\mathcal{S}_1$*,* $\mathcal{M}^\rho$*, and* $\mathcal{M}^\lambda$ *transitively.*

(b) *The automorphism group of the graph* $\mathcal{T}$ *permutes the three parts* $\mathcal{T}^1$*,* $\mathcal{T}^2$*, and* $\mathcal{T}^3$ *transitively.*

PROOF. These two statements are equivalent by Proposition (18.4). We proceed in a series of steps.

(i) *For each* $i \in \{1,2,3\}$*, the vertices of* $\mathcal{T}^i$ *will be called i-points. For each* $L \in \mathcal{S}_2$ *let the i-line* L^i *be* $\mathcal{T}_L \cap \mathcal{T}^i$*, and set* $\mathcal{L}^i = \{\, L^i \mid L \in \mathcal{L}\,\}$*. Then* $(\mathcal{T}^i, \mathcal{L}^i)$ *is a partial linear space (as defined in Section 3.1). We say that two i-points are collinear if they are together in an i-line. That is, two distinct i-points are collinear when they are in a common singular* 2*-space for* $i = 1$ *and when they intersect in a singular* 2*-space for* $i \in \{2,3\}$*.*

PROOF. The only thing that needs proving is that $(\mathcal{T}^i, \mathcal{L}^i)$ is a partial linear space. For $i = 1$ this is clear, since L^i consists precisely of the $|F| + 1$ singular 1-spaces of the singular 2-space L. For $i = 2, 3$, this is also true as then L^i consists of the $|F|+1$ singular 4-spaces from $\mathcal{T}^i$ that pairwise intersect in the singular 2-space L. □

(ii) *There is no i-point collinear with all other i-points. For each i-line* L^i*, the i-point p is collinear either with all i-points of* L^i *or with a unique i-point of* L^i*. That is, each partial linear space* $(\mathcal{T}^i, \mathcal{L}^i)$ *is a nondegenerate* polar space. *(See* [**Shu11**, p. 168]*.)*

PROOF. As (V, q) is nondegenerate and hyperbolic, the first sentence is immediate. When i=1 the second sentence is also clear, as the singular 2-space L is either inside the hyperplane $p^\perp$ or intersects it in a singular 1-space.

Now suppose $i \in \{2,3\}$ so that p is a singular 4-space and L^i is the set of all singular 4-spaces that contain the singular 2-space L and meet p in a subspace of dimension 0, 2, or 4. Choose a q in L^i that meets p in a subspace of minimum dimension. If this dimension is anything but 0, then p is collinear with all the i-points of L^i, as desired. Assume then that p and q intersect trivially, and so $V = p \oplus q$ with $L \le q \le L^\perp$. Thus $L^\perp \cap p = M$, a second singular 2-space. Therefore $r = M \oplus L$ is the unique singular 4-space containing L and meeting p in a subspace of dimension 2. That is, r is the unique i-point of L^i that is collinear with p. □

(iii) *The residue in $\mathcal{D}_4$ of each i-point p (that is, the neighborhood of p) is isomorphic to $A_{3,2}(F)$, the A_3-incidence geometry of* 1*-spaces,* 2*-spaces, and* 3*-spaces of F^4, with the* 2*-spaces of F^4 being in bijection with $\mathcal{L}_p$ (the neighborhood of p in $\mathcal{L}$). The* 1*-spaces and* 3*-spaces are in bijection with those maximal linear subspaces of $(\mathcal{T}^i, \mathcal{L}^i)$ on p.*

Proof. This is clear for $i \in \{2, 3\}$. For $i = 1$ the residue is a D_3-oriflamme geometry. The graphs A_3 and D_3 are the same, and in this case the result is well-known. □

(iv) *With $\{1, 2, 3\} = \{i, j, k\}$, the partial linear spaces $(\mathcal{T}^i, \mathcal{L}^i)$ and $(\mathcal{T}^j, \mathcal{L}^j)$ are isomorphic.*

Proof. This is the heart of the argument. By (iii) each polar space $(\mathcal{T}^i, \mathcal{L}^i)$ is "hyperbolic of rank 4 over the field F." As such, it is uniquely determined up to isomorphism, this being a special case of a far-reaching theorem of Tits on buildings. We sketch direct arguments of Cameron and Shult that handle the specific case of interest here.

By symmetry we may assume $i = 1$, $j = 2$, and $k = 3$.

Cameron [**Cam92**, Prop. 7.4.2 and 8.5.1] sketches an argument based upon the following simple observation: for two singular 4-spaces A and B in $\mathcal{T}^k$ with trivial intersection, we have $V = A \oplus B$. The geometries $(\mathcal{T}^i, \mathcal{L}^i)$ and $(\mathcal{T}^j, \mathcal{L}^j)$ can then be identified relative to this sum.

For the i-point a within A the space $\langle a, a^\perp \cap B\rangle$ is a j-point incident to B. Conversely, any j-point meeting B in a 3-space must meet A in a 1-space or 3-space, hence a 1-space—an i-point. Similarly there is a bijection between i-points incident to B and j-points incident to A.

On the other hand, any j-point not incident to A or B must meet both in 1-spaces, that is, i-points a_0 and b_0, say. Then the i-line $L = \langle a_0, b_0\rangle$ is incident to a_0 and b_0 and the $|F| - 1$ distinct i-points of L not incident to A or B. But L is also a j-line and in $(\mathcal{T}^j, \mathcal{L}^j)$ is incident to the j-points $\langle L, L^\perp \cap A\rangle$ and $\langle L, L^\perp \cap B\rangle$ and to $|F| - 1$ additional j-points incident to neither A nor B. At this stage we have seen all i-points and all j-points and have come close (up to factors $|F| - 1$) to establishing a bijection between them. Using (ii) and (iii) we can define this bijection precisely and then recognize it as the desired isomorphism of $(\mathcal{T}^i, \mathcal{L}^i)$ and $(\mathcal{T}^j, \mathcal{L}^j)$.

Of course, the preceding paragraphs present a sketch of a sketch within our sketch, and some readers may feel unsatisfied! We can alternatively quote a Theorem of Tits—proven by elementary methods relatively early (Theorem 7.5.13) in Shult's delightful book [**Shu11**]—that says two nondegenerate polar spaces of rank at least 3 with isomorphic point cones are isomorphic via a map that takes the chosen point of the first to that of the second. By definition, in a polar space the cone of a point is the subspace of all points collinear with it. Therefore the isomorphism of i-cones and j-cones is a refinement of (iii); and, after verification of the isomorphism, Tits' theorem applies to give us (iv). □

(v) *There is an automorphism of $\mathcal{D}_4$ that takes $\mathcal{T}^i$ to $\mathcal{T}^j$. That is, the automorphism group is transitive on the set $\{\mathcal{T}^1, \mathcal{T}^2, \mathcal{T}^3\}$, as desired for the theorem.*

Proof. This is similar to Proposition (18.4). For $\{a, b, c\} = \{1, 2, 3\}$, Step (iii) allows us to reconstruct from the polar space $(\mathcal{T}^c, \mathcal{L}^c)$ the two classes of maximal linear, indeed projective, subspaces $\mathcal{T}^a$ and $\mathcal{T}^b$ (equivalence determined by even intersection codimension) and their incidences in a unique fashion.

Therefore the isomorphism of $(\mathcal{T}^i, \mathcal{L}^i)$ and $(\mathcal{T}^j, \mathcal{L}^j)$ from the previous step extends to an automorphism of $\mathcal{D}_4$. □

In Theorem (19.29) and Proposition (19.30) below we shall construct a subgroup of the automorphism group of the oriflamme geometry and the graph $\mathcal{T}$ that is isomorphic to Sym(3) and acts as such on the set $\{\mathcal{T}^1, \mathcal{T}^2, \mathcal{T}^3\}$. The existence of such subgroups is also an easy consequence of the fact that $\mathcal{T}$ is a symmetric $\mathcal{T}$-geometry, proven in Theorem (18.7).

(18.6). Theorem. *Let $i = 1$ and $\{j, k\} = \{2, 3\}$. For each nonsingular n, the automorphism g induced by the symmetry s_n of $\mathrm{O}(V, q)$ has the following properties.*

(a) *g fixes $\mathcal{T}^i$ and and each p_j of $\mathcal{T}^j$ is incident to p_j^g, which belongs to $\mathcal{T}^k$.*

(b) *If $p_i \in \mathcal{T}^i$ is incident to both $p_j \in \mathcal{T}^j$ and $p_j^g \in \mathcal{T}^k$, then $p_i^g = p_i$.*

(c) *$g^2 = 1$.*

Proof. Part (a) is contained in Proposition (17.12). Part (c) holds as all symmetries have order 2 by Proposition (17.11).

For (b), if the singular 1-space p_1 is incident to the incident pair of singular 4-spaces p_2 and $p_3 = p_2^{\mathrm{s}_x}$, then it is in the hyperplane $p_2 \cap p_3$ of each. But $p_2 \cap p_3 = p_2 \cap n^\perp = p_3 \cap n^\perp$, so $p_1 \leq n^\perp$ is fixed by $g = \mathrm{s}_n$. □

(18.7). Theorem. *The graph $\mathcal{T}$ is a symmetric $\mathcal{T}$-geometry in the sense of Section 15.4. Let D be the conjugacy class of $\mathrm{Aut}(\mathcal{T})$ that contains the symmetries s_n of Theorem (18.6), and set $G = \langle D \rangle$. Let π be the homomorphism from G to the group $\mathrm{Sym}(3)$ induced on the three parts of $\mathcal{T}$ and taking each symmetry of D_i to the permutation $(i)(j, k)$. Then the triple (G, D, π) is a group with triality.*

Proof. This follows from Corollary (15.9) and results of this section, specifically Corollary (18.2), Theorem (18.5), and Theorem (18.6). □

18.2. Cartan's triality

As in the previous section, (V, q) is a hyperbolic quadratic space of dimension 8 over the field F. Its tripartite triality graph $\mathcal{T} = \mathcal{T}(V, q)$ has parts $\mathcal{T}^1 = \mathcal{S}_1$, $\mathcal{T}^2 = \mathcal{M}^\lambda$, and $\mathcal{T}^3 = \mathcal{M}^\rho$. The associated D_4-graph is $\mathcal{D}_4 = \mathcal{T} \cup \mathcal{S}_2$.

As the isomorphism type of $\mathcal{T}(V, q)$ is uniquely determined by the field, we may write $\mathcal{T}(F)$ in its place.

(18.8). Theorem. $\mathrm{D}_4(F) \leq \mathrm{PGO}_8^+(F) \leq \mathrm{Aut}(\mathcal{T}(F)) \leq \mathrm{Aut}(\mathrm{D}_4(F))$.

A large part of the theorem comes quickly. As seen in Proposition (17.12), the group $\mathrm{GO}(V, q)$ acts on $\mathcal{T}(F)$, permuting the singular 1-spaces of $\mathcal{T}^1 = \mathcal{S}_1$ and the maximal singular 4-spaces of $\mathcal{T}^2 \cup \mathcal{T}^3$, preserving adjacency with kernel consisting of the scalars. Thus $\mathrm{PGO}_8^+(F) \leq \mathrm{Aut}(\mathcal{T}(F))$, and $\mathrm{PGO}_8^+(F)$ contains the normal subgroup $\mathrm{D}_4(F)$ generated by long root subgroups. To prove the remainder of the theorem, we show that $\mathrm{D}_4(F)$ is normal in $\mathrm{Aut}(\mathcal{T}(F))$ with trivial centralizer. In doing this, we will make use of the isomorphism of Proposition (18.4)(a), identifying the graph $\mathcal{D}_4 = \mathcal{T} \cup \mathcal{S}_2$ with the graph $\mathcal{T} \cup \mathcal{L}$, where $\mathcal{L}$ is the set of maximal tripartite subgraphs of $\mathcal{T}$ (with at least two parts of size greater than 1), $\mathcal{L}$ being in bijection with $\mathcal{S}_2$ via $\mathcal{T}_L \leftrightarrow L$.

In fact, $\mathrm{Aut}(\mathcal{T}(F))$ and $\mathrm{Aut}(\mathrm{D}_4(F))$ are always equal. All we lack for a proof is that $\mathrm{Aut}(\mathrm{D}_4(F))$ stabilizes the class of long root subgroups in $\mathrm{D}_4(F)$. To prove this would take us a bit far afield. One proof makes use of Chow and Dieudonné's [**Cho49, Die51**] determination of the automorphism group of the polar space $(\mathcal{T}^1, \mathcal{L}^1)$ from our proof of Theorem (18.5).

Let $T \in \mathcal{L}$ be a maximal complete tripartite subgraph of $\mathcal{T}$. For each vertex x of $\mathcal{T}$, let x^+ denote the set of all vertices adjacent to x. Then T^+ is the union of all t^+ for $t \in T$. Especially $T \subseteq T^+$. An element of $\mathrm{Aut}(\mathcal{T}(F))$ will be called a root element for T if it fixes each vertex of T^+. For fixed T, the root elements for T form a subgroup, the root subgroup, R_T of $\mathrm{Aut}(\mathcal{T}(F))$.

We have immediately:

(18.9). LEMMA. *Let $T \in \mathcal{L}$.*

(a) *If $S \in \mathcal{L}$ with $R_S = R_T$ then $S = T$.*

(b) *As T meets each of $\mathcal{T}^i$ nontrivially, R_T fixes each of the parts $\mathcal{T}^i$ globally.*

(c) *For each $g \in \mathrm{Aut}(\mathcal{T}(F))$ we have $R_T^g = R_{T^g}$. Especially $\langle R_T \mid T \in \mathcal{L} \rangle$ is a normal subgroup of $\mathrm{Aut}(\mathcal{T}(F))$.* □

(18.10). PROPOSITION. *Let $T \in \mathcal{L}$.*

(a) *For each $v \in \mathcal{T}^i \setminus T^+$ There is a unique vertex $t = t_v \in \mathcal{T}^i \cap T$ at distance 2 from v, and there is a unique member $S = S_v$ of $\mathcal{L}$ containing v and t.*

(b) *Let $v \in \mathcal{T}^1 \setminus T^+$, and let $t = t_v \in \mathcal{T}^1$ and $S = S_v \in \mathcal{L}$ be as found in* (a). *The root group R_T fixes $(S \cap \mathcal{T}^1) \setminus \{t\}$ globally.*

PROOF. We often do calculations in the orthogonal space (V, q).[1]

(a) Let $L \in \mathcal{S}_2$ with $T = \mathcal{T}_L$. First take $v \in \mathcal{T}^1 \setminus T^+$. If v were perpendicular to all L, then $\langle v, L \rangle$ would be in one of the 4-spaces of T, hence v would be in T^+, against assumption. Therefore the hyperplane $v^\perp$ of V meets L in a unique 1-space t. Especially $U = \langle v, t \rangle \in \mathcal{S}_2$, and $S = \mathcal{T}_U$ is the unique member of $\mathcal{L}$ containing v and t.

If instead v is a 4-space in $\mathcal{T}^i$, for $i \neq 1$, then $v \notin T^+$ is equivalent to $v \cap L = 0$. Thus $K = L^\perp \cap v$ is a 2-space and $t = K \oplus L \in \mathcal{T}^i \cap T$ with $S = \mathcal{T}_K$.

(b) Let M and N be two distinct 4-spaces of $S \cap \mathcal{T}^2$. As $t \in U = M \cap N$ we have $M, N \in T^+$, so M and N are fixed by each $g \in R_T$. But then

$$v^g \in (M \cap N)^g = M \cap N = U\,,$$

hence $v^g \in (S \cap \mathcal{T}^1) \setminus \{t\}$, as claimed. □

(18.11). PROPOSITION. *For each $T \in \mathcal{L}$, the root group R_T is semiregular on $\mathcal{T}^1 \setminus T^+$.*

PROOF. As in the previous proposition, let $v \in \mathcal{T}^1 \setminus T^+$. There are a unique $t \in \mathcal{T}^1 \cap T$ at distance 2 from v and a unique $S \in \mathcal{L}$ containing v and t. Let $L \in \mathcal{S}_2$ with $T = \mathcal{T}_L$.

[1] This is why we focus on the easily accessible $\mathcal{T}^1$, even though by Study's Triality all the $\mathcal{T}^i$ are equivalent.

Let $g \in R_T$ with $v^g = v$. We must prove that g is the identity.

We first claim that g fixes each vertex of v^+. Let $M \in \mathcal{T}^i \cap v^+$. If $M \in T^+$, then g fixes it by the definition of the root subgroup R_T. So we may assume $M \notin T^+$. Choose $r \in T \cap \mathcal{T}^1$ with $r \neq t$. Then r and v are not perpendicular, so $M = v \oplus Q$ for $Q = r^\perp \cap M$. The singular 4-space $N = r \oplus Q \in \mathcal{T}^{3-i}$ is thus adjacent to M (as they meet in Q), in T^+ (as it contains r), and not adjacent to v (again, as it contains r). Therefore M is the unique vertex of the $\mathcal{T}$-geometry $\mathcal{T}$ adjacent to both v and N. As g fixes v and $N \in T^+$, it also fixes M. This gives the claim.

As every singular 2-space is the intersection of all the singular 4-spaces containing it, for any singular 2-space U on v, the root element g fixes $U \setminus \{v\}$ globally.

We next show that g fixes each vertex of $\mathcal{T}^1$. This is the case for $\mathcal{T}^1 \cap T^+$ by definition. Suppose that $p \in \mathcal{T}^1 \setminus T^+$ with v and p perpendicular, but $U = \langle v, p \rangle$ not containing t. Then U is fixed globally by g as is $\langle p, t_p \rangle \cap \mathcal{T}^1 = S_p \cap \mathcal{T}^1$ (by the previous proposition), so g fixes $p = U \cap (S_p \cap \mathcal{T}^1)$. Especially, when p and $t = t_p$ are perpendicular (which does happen), the element g fixes each vertex of $\langle p, t \rangle = S_p \cap \mathcal{T}^1$. Reversing the roles of v and p, we also see from this case that each vertex of $S \cap \mathcal{T}^1$ is fixed by g. Every vertex of $\mathcal{T}^1 \setminus T^+$ not perpendicular to t is perpendicular to one of the vertices of $(S \cap \mathcal{T}^1) \setminus \{t\}$, so all such are fixed by g. Exchanging t for another element of $T \cap \mathcal{T}^1$, we find that g is trivial on all $\mathcal{T}^1 \setminus T^+$ and so on $\mathcal{T}^1$.

Next, if $M \in \mathcal{T}^2 \cup \mathcal{T}^3$, then

$$(M^g)^+ \cap \mathcal{T}^1 = (M^+)^g \cap \mathcal{T}^1 = (M^+ \cap \mathcal{T}^1)^g = M^+ \cap \mathcal{T}^1 \,,$$

hence $M^g = M$. That is, g trivial on all $\mathcal{T}$, and $g = 1$ as desired. □

(18.12). Lemma. *For $T \in \mathcal{L}$, let $L \in \mathcal{S}_2$ be given by $T = \mathcal{T}_L$. Then $R_T = R_L \leq \mathrm{PGO}_8^+(F)$, the long root subgroup for L.*

Proof. By Proposition (17.13)(c), the long root subgroup R_L induces a subgroup of the root group R_T that is transitive on $(S_v \cap \mathcal{T}^1) \setminus \{t_v\}$ for each $v \in \mathcal{T}^1 \setminus T^+$.

Let $h \in R_T$, then for $v \in \mathcal{T}^1 \setminus T^+$ we have $w = v^h \in S_v \setminus \{t_v\}$ by Proposition (18.10)(b). Choose $r \in R_L$ with $v^r = w$, and set $g = hr^{-1} \in R_T$. Then

$$v^g = v^{hr^{-1}} = w^{r^{-1}} = v \,.$$

By Proposition (18.11) we find $g = 1$ hence $h = r$. □

Proof of Theorem (18.8).

As discussed directly after the statement of the theorem, here we need only prove that $\mathrm{D}_4(F)$ is normal in $\mathrm{Aut}(\mathcal{T}(F))$ with trivial centralizer.

By Lemmas (18.9) and (18.12) the group

$$\langle\, R_T \mid T \in \mathcal{L} \,\rangle = \langle\, R_L \mid L \in \mathcal{S}_2 \,\rangle = \mathrm{D}_4(F)$$

is normal in $\mathrm{Aut}(\mathcal{T}(F))$.

If z centralizes this subgroup, then for all $T \in \mathcal{L}$ we have $R_T = R_T^z = R_{T^z}$. Therefore $T = T^z$ for all $T \in \mathcal{L}$, and z is trivial on $\mathcal{L}$. But every vertex of $\mathcal{T}$ is the intersection of the members of $\mathcal{L}$ containing it, so z is trivial on $\mathcal{T}$. That is, $z = 1$. □

(18.13). Theorem. (Cartan's triality) *For the field F, the group $\mathrm{D}_4(F) = \mathrm{P}\Omega_8^+(F)$ admits as outer automorphism the group $\mathrm{Sym}(3)$ with its elements of order*

3 *not induced by semilinear automorphisms of* F^8*. The split extension*

$$\mathrm{P}\Omega_8^+(F) \rtimes \mathrm{Sym}(3) = \mathrm{D}_4(F) \rtimes \mathrm{Sym}(3)$$

is a group with triality, with π *equal to projection onto* $\mathrm{Sym}(3)$ *and* D *the conjugacy class containing the transpositions of* $\mathrm{Sym}(3)$*.*

Proof. Following Theorem (18.7), let E be the conjugacy class of $\mathrm{Aut}(\mathcal{T}(F))$ containing those automorphisms induced by the symmetries s_n of $\mathrm{O}(V, q)$. Set $G = \langle E \rangle$, and let π be the homomorphism from G to the group $\mathrm{Sym}(3)$ induced on the three parts of $\mathcal{T}(F)$, so that the triple (G, E, π) is a group with triality, as in Theorem (18.7).

For $d, e \in E$ with

$$S = \langle d, e \rangle \simeq \langle d, e \rangle^\pi = \mathrm{Sym}(3)\,,$$

by Theorem (18.8) in $\mathrm{Aut}(\mathcal{T}(F))$ the group S normalizes simple $\mathrm{D}_4(F) = \mathrm{P}\Omega_8^+(F)$ (using Theorem (17.16)). The element de of order 3 takes $\mathcal{S}_1 = \mathcal{T}^1$ to either $\mathcal{T}^2$ or $\mathcal{T}^3$, in both cases consisting of totally singular 4-spaces, and so is not induced by a semilinear automorphism of the underlying space F^8.

The subset D of E that is the conjugacy class of d and e in the semidirect product remains a class of 3-transpositions with projection map the restriction of the original π. As $\mathrm{D}_4(F) = \mathrm{P}\Omega_8^+(F)$ is simple, the class generates the full semidirect product, which is thus a group with triality. □

Chapter 19

Composition Algebras

Composition algebras are beautiful objects whose loops of units provide important examples of Moufang loops. They also form a bridge between Study's and Cartan's triality. In particular a central motivation for this chapter is Theorem (19.29), which provides our algebraic proof of of Study's triality—Theorem (18.5).

Here we are mainly interested in properties of the composition algebras of dimension 8, the octonion algebras, although a short detour in our arguments provides a proof of Hurwitz' Theorem on the dimensions of arbitrary composition algebras.

Much of the material in this chapter comes from [**Hal00**]. Those notes were motivated by and drew a great deal from an early version [**BuC97**] of Chapter 5 of [**Coh13**]. In turn, the final version of that chapter incorporates material that was introduced in the notes.

19.1. Composition algebras

An *algebra* over the field F is a F-vector space A combined with a bilinear product $\pi\colon\ A \times A \longrightarrow A$. The algebra *admits composition* with respect to the quadratic form $q\colon A \longrightarrow F$ provided

$$q(x)q(y) = q(xy)\,,$$

for all $x, y \in A$. A *composition algebra* is an algebra admitting composition with respect to a nondegenerate quadratic form q. We follow [**SpV00**] in requiring our composition algebras A to have a multiplicative identity element $1 = 1_A$. In this case $q(1) = q(1)^2 = 1$ since q is nondegenerate. The opposite of a composition is also a composition algebra.

An immediate consequence of the composition law is that an invertible element of A, a *unit* of A, must be by nonsingular. In composition algebras the converse is also true (see Corollary (19.8) below). Therefore if all nonzero elements of a composition algebra A are nonsingular, then all nonzero elements are invertible and A is a *division algebra.* If A is not a division algebra, then q is actually hyperbolic (Lemma (19.11)). In this case, the composition algebra is called *split.*

Moufang [**Mou35**] studied alternative algebras, of which composition algebras are examples. She proved (see Theorem (19.23) below) that alternative hence composition algebras satisfy the Moufang identities. Therefore their loops of units provide interesting examples of Moufang loops.

We now give some examples of composition algebras. (Indeed, in the split case, these are the only examples; see Theorems (19.21) and (19.22) below.)

19.1.1. Composition algebras of dimension 1**,** 2**, and** 4**.** A composition algebra of dimension 1 is just a field with $q(x) = x^2$ and is not split. (As q is required to be nondegenerate, the field cannot have characteristic 2.)

A composition algebra of dimension 4 is usually called a *quaternion* algebra. The canonical example of a split composition F-algebra of dimension 4 is the associative algebra $\mathrm{Mat}_2(F)$ of all 2×2 matrices over F with $q(x) = \det(x)$:

$$\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ab - cd\,.$$

The diagonal matrices of $\mathrm{Mat}_2(F)$ give a nondegenerate split subalgebra of dimension 2. This is of course isomorphic to $F \oplus F$ with $(a, d)(x, w) = (ax, dw)$ and $q((a, d)) = ad$. (An example of a nonsplit composition algebra of dimension 2 over F is a separable quadratic extensions K of F proved with the Galois norm: $q(\alpha) = \alpha\bar{\alpha}$; see Theorem (19.21).)

Additionally the scalar matrices give a subalgebra $F1$ of dimension 1.

19.1.2. Spilt composition algebras of dimension 8**.** Composition algebras of dimension 8 are called *octonion algebras.*[1] The originals is the real, compact algebra $\mathbb{O}$ due to Graves (1843, unpublished) and Cayley (1845) [**SpV00**, p. 23]. A version of its construction can be found at the end of Section 19.4.

A specific split octonion algebra $\mathrm{Oct}^+(F)$ is provided by *Zorn's vector matrices* [**Zor31**]

$$m = \begin{bmatrix} a & \vec{b} \\ \vec{c} & d \end{bmatrix}$$

with $a, d \in F$ and $\vec{b}, \vec{c} \in F^3$. Multiplication is given by

$$\begin{bmatrix} a & \vec{b} \\ \vec{c} & d \end{bmatrix} \begin{bmatrix} x & \vec{y} \\ \vec{z} & w \end{bmatrix} = \begin{bmatrix} ax + \vec{b} \cdot \vec{z} & a\vec{y} + w\vec{b} \\ x\vec{c} + d\vec{z} & \vec{c} \cdot \vec{y} + dw \end{bmatrix} + \begin{bmatrix} 0 & \vec{c} \times \vec{z} \\ -\vec{b} \times \vec{y} & 0 \end{bmatrix}$$

using the standard dot (inner) and cross (outer, exterior, vector) products of 3-vectors. The associated quadratic form is the norm (or determinant)

$$q(m) = ad - \vec{b} \cdot \vec{c}\,.$$

For any $\vec{v}$ with $\vec{v} \cdot \vec{v} = k \neq 0$ the subalgebra of all

$$m = \begin{bmatrix} a & b\vec{v} \\ ck^{-1}\vec{v} & d \end{bmatrix}$$

is a copy of the quaternion algebra $\mathrm{Mat}_2(F)$.

Zorn (and others) gave a slightly different version of these matrices, replacing the entry $\vec{c}$ with its negative. This gives the more symmetrical norm form

[1] With this terminology we follow [**SpV00**]. Composition algebras with an identity element and having dimension 8 are often called *Cayley algebras.*

$q(m) = ad + \vec{b} \cdot \vec{c}$ but makes the connection with standard matrix multiplication and determinants less clear.

(19.1). THEOREM. $\mathrm{Oct}^+(F)$ *with the notation and operations defined above is a split octonion algebra.*

PROOF. The set is closed under addition and multiplication with identity element

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} .$$

The dot and cross products are bilinear, so we do have an F-algebra. The map q is a quadratic form on the F-space $\mathrm{Oct}^+(F)$, easily seen to be nondegenerate (for instance, only 0 is perpendicular to each of the eight matrix units) and so hyperbolic since, for instance, the elements

$$m = \begin{bmatrix} a & \vec{0} \\ \vec{c} & 0 \end{bmatrix}$$

form a singular 4-space.

It remains to check (following [**BuC97, Coh13**]) that the form admits composition. This is not difficult and depends upon certain identities involving the dot and cross products:

Let $\vec{a}, \vec{b}, \vec{c}, \vec{d} \in F^3$. *Then*

(i) $\vec{a} \cdot \vec{b} = \vec{b} \cdot \vec{a}$.

(ii) $\vec{a} \times \vec{b} = -(\vec{b} \times \vec{a})$ *and* $\vec{a} \times \vec{a} = 0$.

(iii) $\vec{a} \cdot (\vec{a} \times \vec{b}) = 0$.

(iv) $(\vec{a} \times \vec{b}) \cdot (\vec{c} \times \vec{d}) = (\vec{a} \cdot \vec{c})(\vec{b} \cdot \vec{d}) - (\vec{a} \cdot \vec{d})(\vec{b} \cdot \vec{c})$. □

Especially, as found in Theorem (19.23) below, the loop of units of $\mathrm{Oct}^+(F)$ is a Moufang loop.

19.2. General structure

Essentially by definition, for an arbitrary F-algebra A the *translation maps*

$$\mathrm{L}(a) \colon x \mapsto ax \quad \text{and} \quad \mathrm{R}(a) \colon x \mapsto xa$$

yield linear transformations—the left and right *adjoint maps*. When $a \in F$, the maps $\mathrm{L}(a)$ and $\mathrm{R}(a)$ are just scalar multiplication by a on the F-space A.

For the rest of this section we will assume that A is a composition F-algebra with associated norm $q \colon A \longrightarrow F$. In this case, the translations have additional structure.

(19.2). LEMMA. *For all* $a, x \in A$, *the composition law can be written as*

$$q(x^{\mathrm{L}(a)}) = q(a)q(x) = q(x^{\mathrm{R}(a)}) .$$

Especially, in the language of Section 17.4, for nonsingular a *the invertible translation maps* $\mathrm{L}(a)$ *and* $\mathrm{R}(a)$ *are similarities* g *with scaling factor* $\mu_g = q(a)$. □

The remarks of the lemma extend to the associated bilinear form $h(\cdot,\cdot)$.

(19.3). LEMMA. *For all* $a, x, y \in A$,

(a) $h(xa, ya) = h(ax, ay) = q(a)h(x, y)$.

(b) $h(x, y)h(w, z) = h(xz, yw) + h(xw, yz)$.

Proof. (a)

$$\begin{aligned} h(ax,ay) &= q(ax+ay)-q(ax)-q(ay) \\ &= q(a)q(x+y)-q(a)q(x)-q(a)q(y) \\ &= q(a)h(x,y)\,. \end{aligned}$$

(b) We use the previous part in calculating

$$\begin{aligned} 0 &= q(x+y)q(w+z)-q((x+y)(w+z)) \\ &= h(x,y)h(w,z)-h(xz,yw)+h(xw,yz)\,. \qquad \square \end{aligned}$$

(19.4). Lemma. *If K is an extension field for F, then the algebra $K \otimes_F A$ also is a composition algebra with respect to the induced quadratic form.*

Proof. The multiplication and forms on A admit unique extension to $K \otimes_F A$ by bilinearity. To show that the induced form admits composition, we must prove the extended law

$$q(\textstyle\sum_{i=1}^m \alpha_i x_i)q(\sum_{j=1}^m \alpha_j z_j) = q((\sum_{i=1}^m \alpha_i x_i)(\sum_{j=1}^m \alpha_j z_j))\,,$$

where the α_i form an F-basis for K and $x_i, z_j \in A$.

Consider first the situation with only two summands:

$$q(\alpha x+\beta y)q(\alpha w+\beta z) = q((\alpha x+\beta y)(\alpha w+\beta z))\,,$$

for all $x, y, w, z \in A$ and $\alpha, \beta \in K$. By the composition law and the previous lemma, we have

$$\begin{aligned} &q(\alpha x+\beta y)q(\alpha w+\beta z)-q((\alpha x+\beta y)(\alpha w+\beta z)) \\ &\qquad\qquad = \alpha\beta(h(x,y)h(w,z)-h(xz,yw)-h(xw,yz))\,. \end{aligned}$$

By Lemma (19.3) the righthand side is 0, and we have the desired composition law in this special case.[2]

The general case then takes a similiar shape and follows from composition and multiple applications of Lemma (19.3). □

As an immediate corollary of Proposition (17.2) and Lemma (19.4), we have

(19.5). Corollary. *If A has dimension at least 2 over F then, by tensoring with an appropriate separable quadratic extension K, we get a composition algebra $K \otimes_F A$ containing nonzero singular elements.* □

We define the operation of *conjugation* on A by

$$x \mapsto = -x^{\mathrm{s}_1} = -x + h(x,1)1\,,$$

where s_1 is a symmetry of the quadratic F-space (A,q), as found in Proposition (17.11).

For instance, in the split quaternion algebra of 2×2 matrices we have the familiar

$$\overline{\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}} = \begin{bmatrix} \delta & -\beta \\ -\gamma & \alpha \end{bmatrix}.$$

This formula then carries over to Zorn's representation of the split octonions.

[2] The most important case of the lemma is that where K is a quadratic extension of F and the special case of composition is all that is needed.

(19.6). Lemma.

(a) $\bar{\bar{x}} = x$
(b) *$q(x) = q(\bar{x})$ and $h(x,y) = h(\bar{x},\bar{y})$*

Proof. These are direct consequences of $\bar{x} = -x^{\mathrm{s}_1}$. □

(19.7). Proposition.

(a) *$\bar{x}(xy) = q(x)y = (yx)\bar{x}$. In particular $\bar{x}x = q(x)1 = x\bar{x}$.*
(b) *$\bar{x}(yz) + \bar{y}(xz) = h(x,y)z$ and $(zy)\bar{x} + (zx)\bar{y} = h(x,y)z$.*
(c) *$\bar{x}y + \bar{y}x = h(x,y)1$ and $y\bar{x} + x\bar{y} = h(x,y)1$.*
(d) *$h(x,\bar{v}y) = h(vx,y)$ and $h(x,y\bar{v}) = h(xv,y)$.*

Proof. In each case, we only prove the first identity. We first prove (d):

$$\begin{aligned} h(x,\bar{v}y) &= h(x,(h(1,v)-v)y) \\ &= h(x,y)h(1,v) - h(x,vy) \\ &= h(x,y)(q(1+v) - q(1) - q(v)) - h(x,vy) \\ &= h((1+v)x,(1+v)y) - h(x,y) - h(vx,vy) - h(x,vy) \\ &= h(vx,y)\,. \end{aligned}$$

Next, from (d)

$$\begin{aligned} h(\bar{x}(xy),z) &= h(xy,xz) \\ &= q(x)h(y,z) \\ &= h(q(x)y,z)\,, \end{aligned}$$

for all z. Therefore by nondegeneracy $\bar{x}(xy) = q(x)y$, giving (a).

We linearize (a) to get (b):

$$\begin{aligned} (\bar{x}+\bar{y})((x+y)z) &= q(x+y)z \\ \bar{x}(xz) + \bar{y}(yz) + \bar{x}(yz) + \bar{y}(xz) &= q(x)z + q(y)z + h(x,y)z \\ \bar{x}(yz) + \bar{y}(xz) &= h(x,y)z\,. \end{aligned}$$

Part (c) is the special case $z = 1$ of (b). □

The first part of the proposition immediately gives:

(19.8). Corollary. *The following are equivalent:*

(1) *x is nonsingular.*
(2) *x is invertible.*
(3) *x has inverse $q(x)^{-1}\bar{x}$.*
(4) *$\mathrm{R}(x)$ is invertible.*
(5) *$\mathrm{L}(x)$ is invertible.*

When all these hold, $q(x)^{-1}\bar{x}$ is a 2-sided inverse and we have the "inverse property" identities:

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

for all y. □

(19.9). Corollary.

(a) *$x^2 - h(x,1)x + q(x) = 0$.*
(b) *$\overline{xy} = \bar{y}\bar{x}$.*
(c) (Alternative Law) *$x(xy) = x^2y$ and $(xy)y = xy^2$.*

Proof. By definition $\bar{x}x = (-x + h(x,1)1)x = -x^2 + h(x,1)x$, so (a) follows directly from Proposition (19.7)(a).

For (b), we use Proposition (19.7)(d) many times:

$$\begin{array}{rclcl} h(\overline{xy}, z) & = & h(1, (xy)z) & = & h(\bar{z}, xy) \\ & = & h(\bar{z}\bar{y}, x) & = & h(\bar{y}, zx) \\ & = & h(\bar{y}\bar{x}, z) & & \end{array}$$

for all z. Therefore, by nondegeneracy, $\overline{xy} = \bar{y}\bar{x}$.

(c) By Proposition (19.7)

$$\begin{aligned} \bar{x}(xy) &= q(x)y \\ (-x + h(x,1))(xy) &= q(x)y \\ -x(xy) &= q(x)y - h(x,1)xy \\ -x(xy) &= (q(x) - h(x,1)x)y \\ -x(xy) &= (-x^2)y\,. \end{aligned}$$

So we have the right alternative identity $x(xy) = x^2y$, and the left alternative identity follows in the opposite algebra. □

(19.10). Corollary. *For nonscalar x, the 2-space $F1 \oplus Fx$ is always a commutative and associative subalgebra. Especially it is a composition subalgebra of dimension 2 when nondegenerate.* □

19.3. Hurwitz' Theorem in a restricted version

We now additionally assume that A is a finite dimensional composition algebra over F with respect to nondegenerate q.

(19.11). Lemma. *If x is a nonzero singular vector in A, then there exist singular vectors y with $h(x,y) \neq 0$. Furthermore, for any such pair $\{x,y\}$, always $A = xA \oplus yA = Ax \oplus Ay$ with each xA and Ax maximal singular. In particular, (A,q) is hyperbolic.*

Proof. For all singular x, the subspaces xA and Ax are both singular since $q(xA) = 0 = q(Ax)$.

By Proposition (17.2) any nondegenerate 2-subspace containing x contains a hyperbolic pair $\{x,y\}$. Especially $x+y$ is nonsingular. Thus by Corollary (19.8)

$$A = A^{\mathrm{L}(x+y)} = (x+y)A \leq xA + yA \leq A\,.$$

That is, $A = xA + yA$. As q is nondegenerate $xA \cap yA = 0$, and both are maximal singular. Therefore $A = xA \oplus yA$, and q is hyperbolic by Proposition (17.5).

A similar argument proves the claims for Ax and Ay. (Here and elsewhere, lefthanded and righthanded versions of a result can be proven by similar arguments or seen to be equivalent using Corollary (19.9)(b). Equally well, the opposite of a composition algebra is again a composition algebra. In any event, we may only give one version.) □

From now on we will assume that the set $\mathcal{S}$ of nonzero singular vectors is not empty. By the lemma (A,q) is hyperbolic. As before $\mathcal{S}_1$ is the set of singular 1-spaces of A, and $\mathcal{M}$ is the set of all maximal singular subspaces of A. Let m be the dimension of each member of $\mathcal{M}$, so that A has F-dimension $2m$.

(19.12). LEMMA.

(a) *If $x \in \mathcal{S}$, then the image of* $\mathrm{L}(x)$ *is xA and its kernel is $\bar{x}A$.*

(b) *If $x \in \mathcal{S}$, then the image of* $\mathrm{R}(x)$ *is Ax and its kernel is $A\bar{x}$.*

PROOF. Certainly the image of $\mathrm{L}(x)$ is xA. By Proposition (19.7)(a) the m-space $\bar{x}A$ is contained in the kernel of $\mathrm{L}(x)$, which has dimension $2m - m = m$. □

(19.13). LEMMA. *Assume $m \geq 2$. Let $x, y \in \mathcal{S}$.*

(a) *If $xy = 0$, then $xA \cap Ay = x(y^\perp) = (x^\perp)y$ of codimension* 1 *in each.*

(b) *$xA \neq Ay$.*

PROOF. By Proposition (19.7)(b), for all $a \in A$,

$$\bar{x}(ay) + \bar{a}(xy) = h(x,a)y\,,$$

and by Lemma (19.12)

$$xA \cap Ay = \ker \mathrm{L}(\bar{x}) \cap Ay\,.$$

(a) If $xy = 0$ then $\bar{x}(ay) = h(x,a)y$. Thus $xA \cap Ay = (x^\perp)y$ and also $x^\perp \geq \ker \mathrm{R}(y) = A\bar{y}$. As $x^\perp$ has codimension 1 in A, the codimension of $(x^\perp)y$ in $Ay = \operatorname{im} \mathrm{R}(y)$ is 1.

(b) If $xA = Ay$ then $\bar{a}(xy) = h(x,a)y$, so $A(xy) \leq \langle y \rangle$ has dimension at most 1. By Corollary (19.8) and Lemma (19.12), for nonzero w the linear transformation $\mathrm{R}(w)$ has rank m or $2m$. As we are assuming $m \geq 2$, this forces $xy = 0$ and so contradicts (a). □

(19.14). LEMMA. *Assume $m \geq 2$.*

(a) *Let x be singular and U a maximal singular subspace with $xA \cap U$ of codimension* 1 *in each. Then there is a singular y with $xy = 0$, $U = Ay$, and $xA \cap U = xA \cap Ay = x(y^\perp) = (x^\perp)y$.*

(b) *Let x be singular and U a maximal singular subspace with $Ax \cap U$ of codimension* 1 *in each. Then there is a singular y with $yx = 0$, $U = yA$, and $Ax \cap U = yA \cap Ax = y(x^\perp) = (y^\perp)x$.*

PROOF. We only prove (a). Let $U_0 = U \cap xA$, of codimension 1 in each. Let W be the preimage of U_0 under $\mathrm{L}(x)$, so that W has codimension 1 in A. By Lemma (19.12), $\ker(\mathrm{L}(x)) = \bar{x}A$ is contained in W. As W has codimension 1 in A, there is a y, uniquely determined up to scalar multiple, with $W = y^\perp$, hence $U_0 = W^{\mathrm{L}(x)} = xW = x(y^\perp)$. Furthermore, $\langle y \rangle = W^\perp \subseteq (\bar{x}A)^\perp = \bar{x}A$, hence $y \in \mathcal{S}$. Also $0 = xy \in x(\bar{x}A)$, by Proposition (19.7) or Lemma (19.12).

By the previous paragraph and Lemma (19.13), we have

$$xA \cap Ay = x(y^\perp) = U_0 = xA \cap U\,.$$

Therefore $Ay = U$ by Proposition (17.8)(a). □

(19.15). PROPOSITION. *Assume $m \geq 2$. For every maximal singular subspace U, there is a singular x with U equal to one of xA or Ax. The two parts of the incidence graph $(\mathcal{M}, \sim)$ on the set $\mathcal{M}$ of maximal singular subspaces are $\mathcal{M}^\rho = \{Ax \,|\, x \in \mathcal{S}\}$ and $\mathcal{M}^\lambda = \{xA \,|\, x \in \mathcal{S}\}$.*

PROOF. Consider the two sets of maximal singular subspaces $\{Ax \,|\, x \in \mathcal{S}\}$ and $\{xA \,|\, x \in \mathcal{S}\}$. They are disjoint by Lemma (19.13). By Lemma (19.14) every edge on yA in the incidence graph $(\mathcal{M}, \sim)$ goes to $\{Ax \,|\, x \in \mathcal{S}\}$, and every edge of $(\mathcal{M}, \sim)$ on Ay goes to $\{xA \,|\, x \in \mathcal{S}\}$. By Proposition (17.9) $(\mathcal{M}, \sim)$ is bipartite and connected, so these sets are the two parts of the bipartition. □

(19.16). Lemma. *Assume $m \geq 3$. Let $x, y \in \mathcal{S}$ be with $\langle x\rangle \neq \langle y\rangle$.*

(a) If $h(x,y) = 0$ then $xA \cap yA$ has codimension 2 in each and $Ax \cap Ay$ has codimension 2 in each.

(b) $xA \neq yA$ and $Ax \neq Ay$.

Proof. Let U_0 be singular of dimension $m-1\,(\geq 2)$ and containing $\langle x, y\rangle$. By Lemma (19.14) and Proposition (19.15), there are $w, z \in \mathcal{S}$ with $U_0 = wA \cap Az$. As $\langle x, y\rangle \subseteq Az$, we have $x\bar{z} = y\bar{z} = 0$ by Lemma (19.12). Therefore $xA \cap A\bar{z}$ and $yA \cap A\bar{z}$ both have dimension $m-1$ by Lemma (19.13). This implies that $xA \cap yA$ has dimension at least $m-2$. The dimension of $xA \cap yA$ cannot be $m-1$ by Lemmas (19.13) and (19.14), so (a) will follow from (b).

If $xA = yA$, then $h(x,y) = 0$; so in proving (b) we may make use of the previous paragraph. By Lemma (19.13) again $xA \cap A\bar{z} = yA \cap A\bar{z}$ equals the $m-1$ space $(x^{\perp})\bar{z} = (y^{\perp})\bar{z}$. Its preimage under $\mathrm{R}(\bar{z})$ is then $x^{\perp} = y^{\perp}$. This forces $\langle x\rangle = \langle y\rangle$, which is not the case.

Starting again with $\bar{w}x = \bar{w}y = 0$, we find the rest of the lemma. □

(19.17). Corollary. *Assume $m \geq 3$. Then the map $\langle x\rangle \mapsto Ax$ gives a bijection of $\mathcal{S}_1$ and $\mathcal{M}^{\rho}$ and $\langle x\rangle \mapsto xA$ gives a bijection of $\mathcal{S}_1$ and $\mathcal{M}^{\lambda}$.*

Proof. This follows from Lemmas (19.13) and (19.16) and Proposition (19.15). □

We now can prove Hurwitz' Theorem (in the split, finite dimensional case).

(19.18). Theorem. (Hurwitz' Theorem—restricted version) *A finite dimensional, split composition algebra A has dimension 2, 4, or 8.*

Proof. Since q is hyperbolic, the dimension $2m$ is even. We must prove that m is 1, 2, or 4. Assume that m is at least 3. Consider the part $\mathcal{M}^{\lambda} = \{xA \,|\, x \in \mathcal{S}\}$ of the graph $(\mathcal{M}, \sim)$ and distances within it.

By Propositions (17.9) and (19.15), the distance from xA to yA in $(\mathcal{M}, \sim)$ is even and equal to the codimension of $xA \cap yA$ in each. Every even number in the range 0 to m must be realized, since $(\mathcal{M}, \sim)$ is connected of diameter m. But by Lemmas (19.11) and (19.16), the only distances realized within $\mathcal{M}^{\lambda} = \{xA \,|\, x \in \mathcal{S}\}$ are 0 (when $\langle x\rangle = \langle y\rangle$), 2 (when $h(x,y) = 0$ but $\langle x\rangle \neq \langle y\rangle$), and m (when $h(x,y) \neq 0$). This forces m to be even and $2 \geq m-2\,(\geq 1)$. That is, $m = 4$. □

19.4. Doubling and Hurwitz' Theorem in its general version

The fundamental result is

(19.19). Proposition. *Let B be a composition subalgebra of a composition algebra. Choose $t \in B^{\perp}$ with $q(t) = -\gamma \neq 0$. Then $A = B + Bt = B \oplus Bt = B \perp Bt$ is a composition subalgebra of dimension twice that of B and with multiplication given by*

$$(u + vt)(x + yt) = (ux + \gamma\bar{y}v) + (yu + v\bar{x})t\,,$$

for $u, v, x, y \in B$. If B is split, then A is split.

Proof. See Springer and Veldkamp [**SpV00**, Proposition 1.5.1].

For $w, z \in B$, we have by Proposition (19.7)(d), $h(w, zt) = h(\bar{w}z, t) = 0$. Therefore $A = B + Bt$ is the perpendicular direct sum of nondegenerate B and Bt. As $\gamma \neq 0$, Bt has dimension equal to that of B (by Corollary (19.8)) and is itself nondegenerate by similarity. Therefore A is nondegenerate.

It remains to prove that A satisfies the stated multiplication rule. For $w, z \in B$ and $r, s \in Bt$, we have the fundamental identities:

(i) $r = -\bar{r}$;
(ii) $zr = r\bar{z}$;
(iii) $(wz)r = z(wr)$;
(iv) $(wr)s = (rs)w$.

The first is clear, since $h(r, 1) = 0$. For the second, we start with Proposition (19.7)(b):

$$(wz)r + (w\bar{r})\bar{z} = h(\bar{r}, z)w = 0$$

hence $(wz)r = -(w\bar{r})\bar{z} = (wr)\bar{z}$ by (i). Specializing to $w = 1$ gives (ii). We then in turn have $(wz)r = (wr)\bar{z} = z(wr)$ by (ii), and this is (iii).

For (iv), we again use Proposition (19.7)(b):

$$(rs)w + (r\bar{w})\bar{s} = h(\bar{w}, s)r = 0$$

Hence $(rs)w = -(r\bar{w})\bar{s} = (r\bar{w})s = (wr)s$ by (i) and (ii).

Therefore

$$\begin{aligned}(u + vt)(x + yt) &= ux + u(yt) + (vt)x + (vt)(yt)\,; \\ &= ux + (yu)t + \bar{x}(vt) + (t(yt))v \qquad \text{by } (iii), (ii), (iv)\,; \\ &= ux + (yu)t + (v\bar{x})t - (\bar{t}(t\bar{y}))v \qquad \text{by } (iii), (i), (ii)\,; \\ &= ux + (yu)t + (v\bar{x})t - (q(t)\bar{y})v \qquad \text{by (19.7)(a)}\,; \\ &= (ux + \gamma\bar{y}v) + (yu + v\bar{x})t\,;\end{aligned}$$

as desired. □

(19.20). Corollary. *Let β be an automorphism of B, and let t_1 and t_2 in $B^\perp$ with $q(t_1) = q(t_2) \neq 0$. Then there is a unique automorphism α of A with $\alpha|_B = \beta$ and $\alpha(t_1) = t_2$.* □

(19.21). Theorem. *Let C be a composition algebra over F.*

(a) *If $\dim_F C = 1$ then $C = F$ with $q(u) = u^2$.*
(b) *If $\dim_F C > 1$ then C contains composition subalgebras of dimension 2, which can be chosen split if C is split.*
(c) *If C is split of dimension 2, then C is isomorphic to the commutative, associative algebra $F \oplus F$ with hyperbolic form $q((u, v)) = uv$.*
(d) *If C is nonsplit of dimension 2, then there is a separable quadratic extension K of F and C is isomorphic, as F-composition algebra, to K provided with the quadratic form $q(a) = a\bar{a}$, where the bar denotes Galois conjugation in K over F.*
(e) *If C is split of dimension 4 over F, then it is isomorphic to the associative algebra $\mathrm{Mat}_2(F)$ with q the usual determinant function.*
(f) *If C is split of dimension 8 over F, then it is unique up to isomorphism and contains split composition subalgebras of dimension 4.*

Proof. The first part is clear. For C of dimension greater than 1 each 2-subspace $F \oplus Fx$ is a subalgebra by Corollary (19.10). If C is split, then there are singular x in $C \setminus 1^\perp$. For each of these, $F1 \oplus Fx$ is a split composition subalgebra by

Proposition (17.2)(b). If C is nonsplit, then by Proposition (17.2)(c) the subalgebra $F1 \oplus Fx$ is nondegenerate for all nonscalar $x \in C \setminus 1^{\perp}$.

Let C have dimension 2. By Corollary (19.9) for $b \in C \setminus F1$ we have $C = F[b] \simeq F[z]/(z^2 - h(b,1)z + q(b))$. Therefore as F-algebra C can be identified with $F \oplus F$ or $K = F(b)$, a quadratic field extension of F. In the second case $C = K$ is a nonsplit division algebra.

If C is $F \oplus F$, then $(1,0)(0,1) = 0$; so C is split and the two summands are singular 1-spaces in C. As $(1,0) + (0,1) = (1,1) = 1$,

$$h((1,0),(0,1)) = q((1,1)) - q((1,0)) - q((0,1)) = 1 - 0 - 0 = 1\,.$$

That is, $x = (1,0)$ and $y = (0,1)$ form a hyperbolic pair in C. Furthermore

$$q((u,v)) = q((u,0)) + q((0,v)) + h((u,0),(0,v)) = 0 + 0 + uv1 = uv\,.$$

In particular split C of dimension 2 is uniquely determined up to isomorphism, as described under (c).

Next suppose nonsplit C is $K = F(b)$, a quadratic field extension of F. As C is nondegenerate, the polynomial $z^2 - h(b,1)z + q(b)$ and field K are both separable over F by Proposition (17.2). In particular $a \neq \bar{a}$ and conjugation in the composition algebra C induces the nonidentity element of the Galois group of K over F. By Proposition (19.7)(a) we have $a\bar{a} = q(a)$ for all $a \in C$.

Let C be split of dimension 4 or 8. By (b) it contains a hyperbolic subalgebra $H = F1 \oplus Fx$. As C itself is split hyperbolic, $H^{\perp}$ contains nonsingular vectors with all possible values by Proposition (17.2). Therefore by Proposition (19.19) and Corollary (19.20) it has a 4-dimensional split subalgebra C_4, unique up to isomorphism. As $\mathrm{Mat}_2(F)$ with q the determinant function is visibly a split composition algebra of dimension 4, we are done with (e).

If C has dimension 8, then again $C_4^{\perp}$ contains nonsingular vectors with all possible values. Proposition (19.19) and Corollary (19.20) tell us that the algebra $C = C_8$ is uniquely determined up to isomorphism. □

We now prove the general version of Hurwitz' theorem.

(19.22). Theorem. (Hurwitz' Theorem—general version) *A composition algebra has dimension* 1, 2, 4, *or* 8 *over the field* F.

Proof. Assume C does not have dimension 1, 2, 4, or 8. By Corollary (19.5) and Lemma (19.11) we may assume that the composition algebra is split (if necessary, replacing F by a quadratic extension).

By Proposition (19.19) and Theorem (19.21) the algebra C contains a composition subalgebra of dimension 8 that is proper and split. Then one more application of Proposition (19.19) yields a split composition (sub)algebra of dimension 16. This contradicts our restricted version of Hurwitz' Theorem, Theorem (19.18). □

Proposition (19.19) has an important converse: "Dickson's doubling construction." If B is an arbitrary F-algebra with identity and admitting composition with respect to the form q_B, and if γ is a arbitrary nonzero element of F, then this formula turns $A = B \oplus Bt$ into a F-algebra with identity that may admit composition with respect to the quadratic form $q_A(x + yt) = q_B(x) - \gamma q_B(y)$. Conjugation is given by $\overline{x + yt} = \bar{x} - yt$.

For a split composition algebra, every possible value γ is attained by q on each nondegenerate split subspace. A standard uniqueness, existence, nonexistence proof for split composition algebras uses this construction:

(1) start from $F = A_1$ itself, commutative and associative with the conjugation map trivial (in characteristic 2, must start with A_2);
(2) the double of A_1 is A_2, a uniquely determined composition algebra of dimension 2, which is commutative and associative but has nontrivial conjugation;
(3) A_2 has unique double A_4, a composition algebra of dimension 4, associative but no longer commutative;
(4) A_4 doubles to a unique algebra A_8 of dimension 8, which still admits composition but is now neither commutative nor associative;
(5) finally, from A_8 the double A_{16} of dimension 16 no longer admits composition.

We have all that is needed for a formal proof, but see Springer and Veldkamp [**SpV00**, Proposition 1.5.3] for the details.

The doubling construction can be expressed nicely in 2×2 matrix form:

$$\begin{bmatrix} u & v \\ \gamma\bar{v} & \bar{u} \end{bmatrix} \begin{bmatrix} x & y \\ \gamma\bar{y} & \bar{x} \end{bmatrix} = \begin{bmatrix} ux + \gamma\bar{y}v & yu + v\bar{x} \\ \gamma x\bar{v} + \gamma\bar{u}\bar{y} & \gamma\bar{v}y + \bar{x}\bar{u} \end{bmatrix} .$$

The selection $\gamma = -1$ then gives the usual matrix construction of the complex numbers $\mathbb{C}$ from the reals $\mathbb{R}$ and Hamilton's quaternion division algebra $\mathbb{H}$ from the complexes, finishing with the Cayley-Graves division algebra $\mathbb{O}$ of real, compact octonions.

On the other hand, starting again with $A = \mathbb{R}$ but instead choosing $\gamma = 1$ leads us to the unique real, split composition algebras $\mathbb{R} \oplus \mathbb{R}$, $\mathrm{Mat}_2(\mathbb{R})$, and $\mathrm{Oct}^+(\mathbb{R})$.

From the matrix version, we easily see that when the algebra B is commutative and conjugation is trivial, the resulting A is commutative. As long as B is commutative, the product on A is just the regular matrix product and so is associative. Less obvious but still true is that for associative B admitting composition, the algebra A admits composition with respect to the "determinant" form $x\bar{x} - \gamma\bar{y}y$.

19.5. Commuting and associating

Hamilton found that a crucial step in going from the complex numbers to the quaternions was giving up on commutativity. Similarly Graves (and Cayley) realized that moving to the next level, the octonions, required sacrificing associativity. To what extent are these higher dimensional composition algebras commutative and associative?

By Corollary (19.9)(c) a composition algebra is an alternative algebra, so the following is contained in results of Moufang [**Mou35**]. In all composition algebras the Moufang identities are easy to verify and hold for all elements, not just the units of the algebra.

(19.23). Theorem. *In the composition algebra C, we have the Moufang identities*

$$(xa)(bx) = (x(ab))x\,, \quad ((xa)x)b = x(a(xb))\,, \quad ((ax)b)x = a(x(bx))\,,$$

for all $a, b, x \in C$. Especially, by setting $a = 1$ in either the first or third of the Moufang identities, we get the flexible identity

$$(xb)x = x(bx)\,.$$

Proof. We only prove the first Moufang identity; the others follow similarly. Our proof follows [**SpV00**, Prop. 1.4.1]. For arbitrary $z \in V$, we use parts of Lemma (19.3) and Proposition (19.7) to calculate

$$\begin{aligned}
h((x(ab))x-(xa)(bx), z) &= h((x(ab))x, z) - h((xa)(bx), z)\\
&= h(x(ab), z\bar{x}) - h(xa, z(\bar{x}\bar{b}))\\
&= h(x, z)h(ab, \bar{x}) - h(x\bar{x}, z(ab)) - (h(x, z)h(a, \bar{x}\bar{b}) - h(x(\bar{x}\bar{b}), za))\\
&= h(x(\bar{x}\bar{b}), za) - h(x\bar{x}, z(ab))\\
&= q(x)(h(\bar{b}, za) - h(\bar{z}, ab))\\
&= q(x)(h(\bar{z}\bar{b}, a) - h(\bar{z}\bar{b}, a))\\
&= 0
\end{aligned}$$

As q and h are nondegenerate, this gives $(x(ab))x = (xa)(bx)$, as desired. □

At times we use the flexible identity implicitly to write xbx in place of $(xb)x$ or $x(bx)$.

In sympathy with our definitions for quasigroups and loops (on page 85), we define nuclei for composition algebras. Given subsets S and T of the algebra C, the *right associator* for S in T, written $\mathrm{Nuc}^{\rho}_T(S)$, is the set of all $z \in T$ with

$$(ab)z = a(bz) \text{ for all } a, b \in S\,.$$

For instance, with M the Moufang loop of units in C, we have $\mathrm{Nuc}^{\rho}_M(M) = \mathrm{Nuc}^{\rho}(M)$, the right nucleus of the loop M. The *right nucleus* of the algebra C is $\mathrm{Nuc}^{\rho}_C(C) = \mathrm{Nuc}^{\rho}(C)$, the right associator for C in C.

Similarly the *left associator* for S in T is the set $\mathrm{Nuc}^{\lambda}_T(S)$ of all $x \in T$ with

$$(xb)c = x(bc) \text{ for all } b, c \in S\,,$$

The *left nucleus* of C is then $\mathrm{Nuc}^{\lambda}_C(C) = \mathrm{Nuc}^{\lambda}(C)$. Also the *middle associator* for S in T is the set $\mathrm{Nuc}^{\mu}_T(S)$ of all $y \in T$ with

$$(ay)c = a(yc) \text{ for all } a, c \in S\,,$$

the *middle nucleus* being $\mathrm{Nuc}^{\mu}_C(C) = \mathrm{Nuc}^{\mu}(C)$. The *associator* for S in T is then

$$\mathrm{Nuc}_T(S) = \mathrm{Nuc}^{\lambda}_T(S) \cap \mathrm{Nuc}^{\mu}_T(S) \cap \mathrm{Nuc}^{\rho}_T(S)$$

with the *nucleus* of C being $\mathrm{Nuc}_C(C) = \mathrm{Nuc}(C)$.

In a similar vein, the *centralizer* of S in T, written $\mathrm{C}_T(S)$ consists of all $t \in T$ with

$$st = ts \text{ for all } s \in S\,.$$

The centralizer of C is then $\mathrm{C}_C(C) = \mathrm{C}(C)$. Finally, the *center* of C is the intersection of its centralizer and nucleus: $\mathrm{Z}(C) = \mathrm{C}(C) \cap \mathrm{Nuc}(C)$.

(19.24). Proposition. *Let C be a composition algebra over F.*

(a) *The centralizer* $\mathrm{C}(C)$ *of C is an F-subspace of C.*

(b) *The various nuclei* $\mathrm{Nuc}^{*}(C)$ *and center* $\mathrm{Z}(C)$ *of C are F-subalgebras of C.*

(c) *If K is an extension field of F, then* $\mathrm{C}(C) = C \cap \mathrm{C}(C|^K)$ *and* $\mathrm{Nuc}^*(C) = C \cap \mathrm{Nuc}^*(C|^K)$.

Proof. Commutativity is tested by the commutator $c(x,y) = xy - yx$ and associativity by the associator $a(x,y,z) = (xy)z - x(yz)$, both F-multilinear. Thus the centralizer and nuclei can be characterized in terms of these vanishing appropriately on an F-basis. In particular the centralizer $\mathrm{C}(C)$ and nuclei $\mathrm{Nuc}^*(C)$ are F-subspaces of C and sit within those of $C|^K = K \otimes_F C$, for all extensions K of F.

We must check that the nuclei are closed under multiplication and so are subalgebras. Consider, for instance $u, v \in \mathrm{Nuc}^\mu(C)$. We have, for all $a, c \in C$:

$$\begin{aligned}
(a(uv))c &= ((au)v)c && \text{as } u \in \mathrm{Nuc}^\mu(C)\,;\\
&= (au)(vc) && \text{as } v \in \mathrm{Nuc}^\mu(C)\,;\\
&= a(u(vc)) && \text{as } u \in \mathrm{Nuc}^\mu(C)\,;\\
&= a((uv)c) && \text{as } v \in \mathrm{Nuc}^\mu(C)\,.
\end{aligned}$$

That is, $uv \in \mathrm{Nuc}^\mu(C)$, as desired. Within the associative subalgebra $\mathrm{Nuc}(C)$, a product of centralizing elements is centralizing. □

(19.25). Proposition.

(a) *A composition algebra of dimension* 1 *or* 2 *is always commutative and associative.*

(b) *A composition algebra C of dimension* 4 *over F is always associative and its center* $\mathrm{Z}(C)$ *is its subalgebra* $F1$.

Proof. The first part is clear from Theorem (19.21).

Assume C has dimension 4. By Corollary (19.5) and the previous proposition, there is an extension K of F (separable of degree at most 2) with the nucleus and center of C inside the nucleus and center, respectively, of the split algebra $C|^K$. By Theorem (19.21) this algebra is isomorphic to $\mathrm{Mat}_2(K)$, associative with center equal to its dimension 1 subalgebra of scalar matrices. □

(19.26). Proposition. *In the octonion algebra O the F-subspace*

$$M = \{\, m \in O \mid x(my) - (xm)y \in F1\,,\ \textit{for all } x, y \in O \,\}$$

is equal to $F1$, the subspace of central scalars.

Proof. The set M is an F-subspace of O and contains $F1$. As in the previous proposition, Corollary (19.5) and Proposition (19.24) allow us to reduce to the case of split octonions. We need only consider Zorn's vector matrices

$$\begin{bmatrix} a & \vec{b} \\ \vec{c} & d \end{bmatrix}$$

with $a, d \in F$ and $\vec{b}, \vec{c} \in F^3$; see Section 19.1.2.

It is enough to show that if the vector matrix

$$m = \begin{bmatrix} f & \vec{b} \\ \vec{c} & 0 \end{bmatrix} = \begin{bmatrix} a & \vec{b} \\ \vec{c} & d \end{bmatrix} - \begin{bmatrix} d & \vec{0} \\ \vec{0} & d \end{bmatrix}$$

belongs to M, then $m = 0$. Let

$$\vec{e}_1 = (1,0,0)\,,\ \vec{e}_2 = (0,1,0)\,,\ \vec{e}_3 = (0,0,1)\,,\ \vec{b} = (b_1, b_2, b_3)\,,\ \vec{c} = (c_1, c_2, c_3)\,.$$

For $\{i,j,k\}=\{1,2,3\}$

$$\begin{aligned} &\begin{bmatrix} 0 & \vec{e}_i \\ \vec{0} & 0 \end{bmatrix}\left(\begin{bmatrix} f & \vec{b} \\ \vec{c} & 0 \end{bmatrix}\begin{bmatrix} 0 & \vec{e}_j \\ \vec{0} & 0 \end{bmatrix}\right)- \\ &\qquad\left(\begin{bmatrix} 0 & \vec{e}_i \\ \vec{0} & 0 \end{bmatrix}\begin{bmatrix} f & \vec{b} \\ \vec{c} & 0 \end{bmatrix}\right)\begin{bmatrix} 0 & \vec{e}_j \\ \vec{0} & 0 \end{bmatrix} \\ &\qquad= \begin{bmatrix} b_k & c_j\vec{e}_i - c_i\vec{e}_j \\ \pm f\vec{e}_k & b_k \end{bmatrix}. \end{aligned}$$

Assuming $m \in M$, we must have $f=0$ and $\vec{c}=\vec{0}$. Furthermore

$$\begin{aligned} &\begin{bmatrix} 0 & \vec{0} \\ \vec{e}_i & 0 \end{bmatrix}\left(\begin{bmatrix} 0 & \vec{b} \\ \vec{0} & 0 \end{bmatrix}\begin{bmatrix} 0 & \vec{0} \\ \vec{e}_j & 0 \end{bmatrix}\right)- \\ &\qquad\left(\begin{bmatrix} 0 & \vec{0} \\ \vec{e}_i & 0 \end{bmatrix}\begin{bmatrix} 0 & \vec{b} \\ \vec{0} & 0 \end{bmatrix}\right)\begin{bmatrix} 0 & \vec{0} \\ \vec{e}_j & 0 \end{bmatrix} \\ &\qquad= \begin{bmatrix} 0 & \vec{0} \\ b_j\vec{e}_i - b_i\vec{e}_j & 0 \end{bmatrix}, \end{aligned}$$

and $\vec{b}=\vec{0}$ as well. Thus $m=0$, as desired. □

(19.27). THEOREM. *An octonion algebra O over F has* $\mathrm{C}(O)=\mathrm{Z}(O)=\mathrm{Nuc}^{\mu}(C)=\mathrm{Nuc}(O)=F1$.

PROOF. Again, using Corollary (19.5) and Proposition (19.24) we reduce to the case of split octonions, realized as vector matrices as before.

The only vector matrices that commute with all diagonal matrices are the diagonal matrices themselves. Of these, the only ones that commute with the matrices

$$\begin{bmatrix} 0 & \vec{e} \\ \vec{0} & 0 \end{bmatrix}$$

are the scalar matrices, which commute with everything. We conclude $\mathrm{C}(O)=F1$.

The middle nucleus of O is contained in the subspace M of the previous proposition. Therefore by that proposition the middle nucleus and the nucleus are equal to $F1$. Then also $\mathrm{Z}(O)=\mathrm{C}(O)\cap\mathrm{Nuc}(O)=F1$. □

It is no surprise that additional calculation along the same lines shows that $\mathrm{Z}(O)$ is equal to each of the nuclei of O.

19.6. Algebraic triality for the split octonions

We return to the notation of Section 19.3, although here we restrict our attention to the triality case of the split octonions A with $2m=8$. The associated triality graph is $\mathcal{T}=\mathcal{T}^1\uplus\mathcal{T}^2\uplus\mathcal{T}^3$ where $\mathcal{T}^1=\mathcal{S}_1$, $\mathcal{T}^2=\mathcal{M}^{\lambda}$, and $\mathcal{T}^3=\mathcal{M}^{\rho}$. By Corollary (18.2) this is a $\mathcal{T}$-geometry.

(19.28). LEMMA. *For $\langle x\rangle,\langle y\rangle\in\mathcal{T}^1$, the following are equivalent:*
(1) $xy=0$;
(2) $\langle y\rangle \sim \bar{x}A$;
(3) $\langle x\rangle \sim A\bar{y}$;
(4) $\langle \bar{y}\rangle \sim Ax$;
(5) $\langle \bar{x}\rangle \sim yA$;
(6) $xA \sim Ay$;

(7) $\bar{y}A \sim A\bar{x}$.

Proof. By Lemma (19.12), $\bar{x}A$ is the kernel of $\mathrm{L}(x)$, so $y \in \bar{x}A$ if and only if $xy = 0$. Similarly $\langle x \rangle \in A\bar{y} = \ker(\mathrm{R}(y))$ if and only if $xy = 0$. Also $\langle \bar{y} \rangle \in Ax$ if and only if $\bar{y}\bar{x} = 0$ if and only if $xy = 0$ by Corollary (19.9)(b), and similarly for $\langle \bar{x} \rangle \in yA$.

By Lemmas (19.13), (19.14), and (19.16) the intersection $xA \cap Ay$ has codimension 1 in each if and only if $xy = 0$, and similarly $\bar{y}A \cap A\bar{x}$ has codimension 1 in each if and only if $\bar{y}\bar{x} = 0$. □

Define on $\mathcal{T}$ the map τ, for all $\langle x \rangle \in \mathcal{T}^1$:

$$\langle x \rangle \xrightarrow{\tau} \bar{x}A \xrightarrow{\tau} A\bar{x} \xrightarrow{\tau} \langle x \rangle \,.$$

The map τ is well-defined by Corollary (19.17). The following theorem gives us the promised algebraic proof of Theorem (18.5)(b).

(19.29). Theorem. *The map τ is an automorphism of $\mathcal{T}$ of order 3, a triality automorphism—transitive on the set $\{\mathcal{T}^1, \mathcal{T}^2, \mathcal{T}^3\}$.*

Proof. We have τ acting on pairs:

$$(\langle y \rangle, \bar{x}A) \xrightarrow{\tau} (\bar{y}A, A\bar{x}) \xrightarrow{\tau} (A\bar{y}, \langle x \rangle) \xrightarrow{\tau} (\langle y \rangle, \bar{x}A) \,.$$

By the lemma, any one of these is an edge of $\mathcal{T}$ if and only if $xy = 0$, in which case they are all edges. Therefore τ is an automorphism of the graph $\mathcal{T}$. □

Let κ be the permutation of $\mathcal{T}$ determined by the conjugation map in A:

$$\kappa(\langle x \rangle) = \langle \bar{x} \rangle;\ \kappa(xA) = A\bar{x};\ \kappa(Ax) = \bar{x}A \,.$$

(19.30). Proposition. *κ is an automorphism of $\mathcal{T}$ of order 2 that inverts the triality automorphism τ.*

Proof. We have on pairs

$$(\langle y \rangle, \bar{x}A) \overset{\kappa}{\longleftrightarrow} (\langle \bar{y} \rangle, Ax) \text{ and } (\bar{y}A, A\bar{x}) \overset{\kappa}{\longleftrightarrow} (Ay, xA) \,.$$

Again by Lemma (19.28), any of these pairs is an edge if and only if $xy = 0$, in which case all are edges. Furthermore

$$\langle x \rangle \xrightarrow{\kappa} \langle \bar{x} \rangle \xrightarrow{\tau} xA \xrightarrow{\kappa} A\bar{x} \,,$$

and so forth, leading to

$$\langle x \rangle \xrightarrow{\kappa\tau\kappa} A\bar{x} \xrightarrow{\kappa\tau\kappa} \bar{x}A \xrightarrow{\kappa\tau\kappa} \langle x \rangle \,.$$

Therefore $\kappa\tau\kappa = \tau^{-1}$, as claimed. □

By Proposition (17.11) the map κ arises naturally, induced by the negative of the orthogonal symmetry s_1 on A.

The following will be of use later.

(19.31). Proposition. *Let $X \in \mathcal{T}^i$ and z be an invertible (that is, nonsingular) element of A. Then both $Xz = X^{\mathrm{R}(z)}$ and $zX = X^{\mathrm{L}(z)}$ belong to $\mathcal{T}^i$.*

Proof. Let y be singular. Then $q(yz) = q(zy) = q(y)q(z) = 0$, so the result holds for $i = 1$.

We need only consider the case $i = 2$. As y is singular and z is invertible, both $(yA)z$ and $z(yA)$ are singular 4-spaces. We must determine their classes. Let a

be arbitrary in A so that $(ya)z$ is an arbitrary element of $(yA)z$. We make use of Proposition (19.7):

$$\begin{aligned}(ya)z &= -(y\bar{z})\bar{a} + h(\bar{z},a)y\\ &= -(y\bar{z})\bar{a} + h(\bar{z},a)q(z)^{-1}q(z)y\\ &= -(y\bar{z})\bar{a} + h(\bar{z},a)q(z)^{-1}(y\bar{z})z\\ &= (y\bar{z})(-\bar{a} + h(\bar{z},a)q(z)^{-1}z)\,.\end{aligned}$$

That is, $(yA)z = (y\bar{z})A \in \mathcal{T}^2$. Similarly

$$\begin{aligned}z(ya) &= -\bar{y}(\bar{z}a) + h(\bar{z},y)a\\ &= -\bar{y}(\bar{z}a) + h(\bar{z},y)q(z)^{-1}q(z)a\\ &= -\bar{y}(\bar{z}a) + h(\bar{z},y)q(z)^{-1}z(\bar{z}a)\\ &= (-\bar{y} + q(z)^{-1}h(\bar{z},y)z)(\bar{z}a)\,,\end{aligned}$$

whence $z(yA) = wA \in \mathcal{T}^2$ for singular

$$w = -\bar{y} + q(z)^{-1}h(\bar{z},y)z = -\bar{y}^{\mathrm{s}_z}$$

by Proposition (17.11). □

Chapter 20

Freudenthal's Triality

One common version of triality for the octonion algebra O goes back at least to Freudenthal [**Fre51**]. It states that for each $g \in \mathrm{GO}(O)$ there are $h, k \in \mathrm{GO}(O)$ such that either

$$x^h y^k = (xy)^g \quad \text{for all } x, y \in O$$

or

$$x^h y^k = (yx)^g \quad \text{for all } x, y \in O\,.$$

In Theorem (20.5) we present this as a statement about the existence of certain autotopisms and anti-autotopisms.

One good aspect of this treatment is that the split and division octonion algebras are handled simultaneously. Tits [**Tit58**, §4.3] also discusses descent and the division algebras as forms of the split algebras.

20.1. Some calculations

It is reasonably clear that the concepts of autotopism and anti-autotopism, defined initially for quasigroups Q in Section 2.2, have natural interpretations for A any algebra. The triple of permutations $(c_+, c_-, c_0)_+ \in \mathrm{Sym}(A)^3$ is an *autotopism* of A provided

$$x^{c_+} y^{c_-} = (xy)^{c_0} \quad \text{for all } x, y \in A$$

and $(c_+, c_-, c_0)_-$ is an *anti-autotopism* of A provided

$$x^{c_+} y^{c_-} = (yx)^{c_0} \quad \text{for all } x, y \in A$$

These again form a group $\mathrm{AAtp}(A)$ under the multiplication

$$(a_+, a_-, a_0)_\alpha \cdot (b_+, b_-, b_0)_\beta = (a_\beta b_+, a_{-\beta} b_-, a_0 b_0)_{\alpha\beta}\,,$$

within which the autotopisms form a normal subgroup $\mathrm{Atp}(A)$ of index at most 2.

The following lemma will be used without reference.

(20.1). Lemma. *Let (A, q) be a composition algebra. If $(g_+, g_-, g)_\epsilon \in \mathrm{AAtp}(A)$ and $\alpha, \beta, \gamma \in F^\times$ with $\alpha\beta = \gamma$, then $(\alpha g_+, \beta g_-, \gamma g)_\epsilon \in \mathrm{AAtp}(A)$.* □

Recall from Theorem (19.23) that the flexible identity $(ab)a = a(ba)$ allows us to write aba unambiguously in the next lemma.

(20.2). Lemma. *Let a be a nonsingular element of the composition algebra (A, q). For each $x \in O$:*

(a) $x^{\mathrm{s}_a} = -q(a)^{-1}a\bar{x}a$. *Especially* $x^{\mathrm{s}_1} = -\bar{x}$.

(b) $x^{\mathrm{s}_1\,\mathrm{s}_a} = q(a)^{-1}axa$.

Proof. Part (a) immediately gives (b). By Proposition (19.7)(c)

$$\begin{aligned} x^{\mathrm{s}_a} &= x - q(a)^{-1}h(x,a)a \\ &= x - q(a)^{-1}(x\bar{a} + a\bar{x})a \\ &= x - q(a)^{-1}(x\bar{a})a - q(a)^{-1}(a\bar{x})a \\ &= x - q(a)^{-1}q(a)x - q(a)^{-1}(a\bar{x})a \\ &= -q(a)^{-1}a\bar{x}a\,. \qquad \square \end{aligned}$$

(20.3). Proposition. *Let a be a nonsingular element of the composition algebra (A, q).*

(a) $(-q(a)^{-1}\,\mathrm{s}_1\,\mathrm{L}(a)\,,\,\mathrm{s}_1\,\mathrm{R}(a)\,,\,\mathrm{s}_a)_- \in \mathrm{AAtp}(A)\backslash\mathrm{Atp}(A)$. *Especially* $(-\,\mathrm{s}_1, \mathrm{s}_1, \mathrm{s}_1)_- \in \mathrm{AAtp}(A) \setminus \mathrm{Atp}(A)$.

(b) $(q(a)^{-1}\,\mathrm{L}(a)\,,\,\mathrm{R}(a)\,,\,\mathrm{s}_1\,\mathrm{s}_a) \in \mathrm{Atp}(A)$.

(c) $(\mathrm{L}(a)\,\mathrm{R}(a)\,,\,\mathrm{L}(a)^{-1},\,\mathrm{L}(a)) \in \mathrm{Atp}(A)$.

(d) $(\mathrm{R}(a)^{-1},\,\mathrm{R}(a)\,\mathrm{L}(a)\,,\,\mathrm{R}(a)) \in \mathrm{Atp}(A)$.

Proof. (a) By the previous lemma and the Moufang identity

$$\begin{aligned} (xy)^{\mathrm{s}_a} &= -q(a)^{-1}a\overline{xy}a \\ &= -q(a)^{-1}a(\bar{y}\bar{x})a \\ &= -q(a)^{-1}(a\bar{y})(\bar{x}a) \\ &= -q(a)^{-1}(y^{\mathrm{s}_1\,\mathrm{L}(a)})(x^{\mathrm{s}_1\,\mathrm{R}(a)})\,. \end{aligned}$$

(b) $(q(a)^{-1}\,\mathrm{L}(a), \mathrm{R}(a), \mathrm{s}_1\,\mathrm{s}_a)_+$

$$= (-1,-1,1)_+(-\,\mathrm{s}_1, \mathrm{s}_1, \mathrm{s}_1)_-(-q(a)^{-1}\,\mathrm{s}_1\,\mathrm{L}(a), \mathrm{s}_1\,\mathrm{R}(a), \mathrm{s}_a)_-\ .$$

(c) By Corollary (19.8) and a Moufang identity from Theorem (19.23) with $z = a^{-1}y$:

$$\begin{aligned} ((ax)a)z &= a(x(az)) \\ ((ax)a)(a^{-1}y) &= a(x(a(a^{-1}y)) \\ ((ax)a)(a^{-1}y) &= a(xy) \\ x^{\mathrm{L}(a)\,\mathrm{R}(a)}y^{\mathrm{L}(a)^{-1}} &= (xy)^{\mathrm{L}(a)}\,, \end{aligned}$$

and (d) is (c) in the opposite algebra A^{op}. □

20.2. Freudenthal's triality

For the octonion algebra O we denote its loop of units $\mathrm{GOct}(O)$, the *general octonion loop*. By Corollary (19.8) it consists of the nonsingular vectors in O and is a Moufang loop by Theorem (19.23).

Recall from Lemma (19.2) that for $a \in \mathrm{GOct}(O)$ the linear transformations $\mathrm{L}(a)$ and $\mathrm{R}(a)$ are similarities of the octonion algebra (O, q) with multiplier $q(a)$.

(20.4). Proposition. *Let O be an octonion algebra.*

(a) $\mathrm{O}(O) = \langle\, \mathrm{s}_b \mid b \in \mathrm{GOct}(O)\,\rangle$.
(b) $\mathrm{GO}(O) = \langle\, \mathrm{L}(a),\, \mathrm{s}_b \mid a, b \in \mathrm{GOct}(O)\,\rangle = \langle\, \mathrm{R}(a),\, \mathrm{s}_b \mid a, b \in \mathrm{GOct}(O)\,\rangle$.
(c) *The image of the homomorphism* $\mu\colon \mathrm{GO}(O) \longrightarrow F^\times$ *given by* $g \mapsto \mu_g$ *is* $q(O)^\times$, *the multiplicative group of all nonzero values taken by the form* q.

Proof. (a) As O is a composition algebra, it is either asingular or split by Lemma (19.11)). Therefore by the Cartan-Dieudonné Theorem, in one of the versions (17.14) and (17.15), we have $\mathrm{O}(O) = \langle\, \mathrm{s}_b \mid b \in \mathrm{GOct}(O)\,\rangle$.

(b) Let $g \in \mathrm{GO}(O)$ and set $1^g = a^{-1} \in \mathrm{GOct}(O)$. Then also $g\,\mathrm{R}(a), g\,\mathrm{L}(a) \in \mathrm{GO}(O)$ with

$$1^{g\,\mathrm{R}(a)} = (a^{-1})^{\mathrm{R}(a)} = a^{-1}a = 1$$

and

$$1^{g\,\mathrm{L}(a)} = (a^{-1})^{\mathrm{L}(a)} = aa^{-1} = 1\,,$$

so in fact $g\,\mathrm{R}(a), g\,\mathrm{L}(a) \in \mathrm{O}(O)$. As g was chosen arbitrarily in $\mathrm{GO}(O)$, (a) yields

$$\mathrm{GO}(O) = \langle\, \mathrm{L}(a),\, \mathrm{s}_b \mid a, b \in \mathrm{GOct}(O)\,\rangle = \langle\, \mathrm{R}(a),\, \mathrm{s}_b \mid a, b \in \mathrm{GOct}(O)\,\rangle\,.$$

(c) follows immediately from (b). □

The next theorem presents the fundamental existence and uniqueness properties that constitute Freudenthal's version of triality.

(20.5). Theorem. (Freudenthal's triality) *Let O be an octonion algebra and $g \in \mathrm{GO}(O)$.*

(a) *There exist a sign $\epsilon \in \{\pm\}$ and permutations g_+, g_- from* $\mathrm{Sym}(O)$ *such that $(g_+, g_-, g)_\epsilon$ is in* $\mathrm{AAtp}(O)$.
(b) *If $(g_+, g_-, g)_\epsilon$ and $(h_+, h_-, g)_\delta$ both belong to* $\mathrm{AAtp}(O)$, *then $\delta = \epsilon = \epsilon_g$ is uniquely determined. Furthermore $g_+, g_- \in \mathrm{GO}(O)$, and there is a scalar $\beta \in F^\times$ with $h_+ = \beta^{-1} g_+$ and $h_- = \beta g_-$.*

Proof. (a) By Proposition (20.4)(b)

$$\mathrm{GO}(O) = \langle\, \mathrm{L}(a),\, \mathrm{s}_b \mid a, b \in \mathrm{GOct}(O)\,\rangle = \langle\, \mathrm{R}(a),\, \mathrm{s}_b \mid a, b \in \mathrm{GOct}(O)\,\rangle\,.$$

Part (a) then follows by Proposition (20.3)(a,c,d). Note that the permutations g_+ and g_- given by the proposition belong to $\mathrm{GO}(O)$.

(b) As just observed, there are examples with $g_+, g_- \in \mathrm{GO}(O)$; so we only need to prove the uniqueness claims.

Suppose that $(g_+, g_-, g)_\epsilon$ and $(h_+, h_-, g)_\delta$ are both in $\mathrm{AAtp}(O)$. Then $\mathrm{AAtp}(O)$ also contains

$$(g_+, g_-, g)_\epsilon^{-1}(h_+, h_-, g)_\delta = (k_+, k_-, 1)_{\epsilon\delta}\,,$$

for appropriate $k_+, k_- \in \mathrm{Sym}(O)$. That is, for all $x, y \in O$

$$x^{k_+}y^{k_-} \quad \text{equals} \quad xy \text{ if } \epsilon\delta = + \quad \text{and} \quad yx \text{ if } \epsilon\delta = -\,.$$

Set $a = 1^{k_+}$ and $b = 1^{k_-}$. Then

$$1 = 1 \cdot 1 = 1^{k_+}1^{k_-} = ab\,,$$

hence $a, b \in \mathrm{GOct}(O)$ with $a^{-1} = b$. Also

$$x = x^{k_+}1^{k_-} = x^{k_+}b \quad \text{and} \quad y = 1^{k_+}y^{k_-} = ay^{k_-}\,,$$

so that $k_+ = \mathrm{R}(b)^{-1} = \mathrm{R}(b^{-1})$ and $k_- = \mathrm{L}(a)^{-1} = \mathrm{L}(a^{-1})$ (where we have used Corollary (19.8)).

That is,

$$(xb^{-1})(by) \quad \text{equals} \quad xy \text{ always} \quad \text{or} \quad yx \text{ always}, \quad \text{as appropriate.}$$

First suppose $\epsilon\delta = -$, so that $(xb^{-1})(by) = yx$ always. With $x = b$ this says that $yb = by$ for all $y \in O$, so b is in the centralizer of O. By Theorem (19.27) the element b is a central scalar in O. But then $xy = (xb^{-1})(by) = yx$ always, and O is commutative, a contradiction. We conclude that the case $\epsilon\delta = -$, which is to say $\epsilon \neq \delta$, does not occur. Therefore $\delta = \epsilon = \epsilon_g$ is uniquely determined by g.

When $\epsilon\delta = +$, set $z = xb^{-1}$ so that $zb = x$. For all z, y we have

$$z(by) = ((zb)b^{-1})(by) = (zb)y\,.$$

That is, b is in the middle nucleus of O, which is the set of central scalars again by Theorem (19.27). Thus $b = \beta \in F^\times$ and $a = \beta^{-1}$, as claimed. □

Similar arguments extend the uniqueness property to say that if any one of the entries in $(h, k, g)_\epsilon \in \mathrm{AAtp}(O)$ belongs ot $\mathrm{GO}(O)$ then the other two do as well and are determined up to appropriate scalars.

Let the *special general orthogonal group* $\mathrm{SGO}(O)$ be the normal subgroup of $\mathrm{GO}(O)$ consisting of all all $g \in \mathrm{GO}(O)$ with $\epsilon_g = +$. Additionally let the *special orthogonal group*[1] $\mathrm{SO}(O)$ be the intersection $\mathrm{O}(O) \cap \mathrm{SGO}(O)$.

(20.6). Proposition.

(a) $\mathrm{SGO}(O) = \langle\, \mathrm{L}(a),\, \mathrm{s}_1\, \mathrm{s}_b \mid a, b \in \mathrm{GOct}(O)\,\rangle = \langle\, \mathrm{R}(a),\, \mathrm{s}_1\, \mathrm{s}_b \mid a, b \in \mathrm{GOct}(O)\,\rangle$ *has index* 2 *in* $\mathrm{GO}(O)$ *with* $\mathrm{GO}(O) = \langle \mathrm{s}_b \rangle\, \mathrm{SGO}(O)$ *for each* $b \in \mathrm{GOct}(O)$.

(b) $\mathrm{SGO}(O) = \langle\, \mathrm{L}(a), \mathrm{R}(a) \mid a \in \mathrm{GOct}(O)\,\rangle$.

(c) $\mathrm{SO}(O) = \langle\, \mathrm{s}_1\, \mathrm{s}_b \mid b \in \mathrm{GOct}(O)\,\rangle$ *has index* 2 *in* $\mathrm{O}(O)$ *with* $\mathrm{O}(O) = \langle \mathrm{s}_b \rangle \mathrm{SO}(O)$ *for each* $b \in \mathrm{GOct}(O)$.

(d) *For* $(g_+, g_-, g)_\epsilon \in \mathrm{AAtp}(O)$ *with* $g \in \mathrm{SGO}(O)$, *we have* $\epsilon_g = +$ *and* $g_+, g_- \in \mathrm{SGO}(O)$.

Proof. (a) By the previous theorem, the map $g \mapsto \epsilon_g 1$ is a well-defined homomorphism from $\mathrm{GO}(O)$ to the cyclic group of order 2. By Proposition (20.3)(a) the anti-autotopism $(-q(a)^{-1}\, \mathrm{s}_1\, \mathrm{L}(a)\,,\, \mathrm{s}_1\, \mathrm{R}(a)\,,\, \mathrm{s}_a)_-$ is in $\mathrm{AAtp}(A) \setminus \mathrm{Atp}(A)$. Therefore this homomorphism is surjective with kernel $\mathrm{SGO}(O)$ of index 2 in $\mathrm{GO}(O)$, and $\mathrm{GO}(O) = \langle \mathrm{s}_b \rangle\, \mathrm{SGO}(O)$ for each $b \in \mathrm{GOct}(O)$. Part (a) then follows from Propositions (20.3)(c,d) and (20.4)(b) as $\mathrm{s}_a\, \mathrm{s}_b = (\mathrm{s}_1\, \mathrm{s}_a)^{-1}(\mathrm{s}_1\, \mathrm{s}_b)$.

(b) By Lemma (20.2)(b)

$$\mathrm{s}_1\, \mathrm{s}_a = q(a)^{-1}\, \mathrm{L}(a)\, \mathrm{R}(a) = \mathrm{L}(q(a)^{-1})\, \mathrm{L}(a)\, \mathrm{R}(a)\,,$$

so this follows from (a).

[1] Up to now we have only defined the special orthogonal group $\mathrm{SO}(V, q)$ for hyperbolic spaces. Again here we only define it under specialized circumstances—there is a supported octonion algebra. General definitions do exist. In characteristic other than 2 it can be (and often is) defined as the group of orthogonal transformations having determinant 1. Every orthogonal transformation has determinant ±1, and symmetries have determinant −1.

Every nondegenerate quadratic space can be embedded in a hyperbolic space, so the products of even numbers of symmetries always form a normal subgroup of index 2 in the group generated by all symmetries (even in characteristic 2). By the Cartan-Dieudonné Theorem in its full generality, this group is almost always the full orthogonal group; so $\mathrm{SO}(V, q) = \langle\, \mathrm{s}_a\, \mathrm{s}_b \mid q(a) \neq 0 \neq q(b)\,\rangle$, as in the third part of the proposition, is a reasonable definition that can also be found in the literature.

(c) Propositions (20.4)(a) gives $\mathrm{O}(O) = \langle\, \mathrm{s}_b \mid b \in \mathrm{GOct}(O)\,\rangle$, hence $\mathrm{SO}(O) = \langle\, \mathrm{s}_1\, \mathrm{s}_b \mid b \in \mathrm{GOct}(O)\,\rangle$ has index 2.

(d) By Proposition (20.3)(b-d) this holds for $g \in \{\mathrm{s}_1\, \mathrm{s}_b\,,\, \mathrm{L}(a)\,,\, \mathrm{R}(a)\}$. Therefore by (a) it holds for all $\mathrm{SGO}(O)$. □

Define the *Freudenthal group* of O to be

$$\mathrm{Frd}(O) = \{\, (g_+, g_-, g)_\epsilon \in \mathrm{AAtp}(O) \mid g \in \mathrm{GO}(O)\,\}\,,$$

as in the theorem. We then have the *special Freudenthal group*

$$\mathrm{SFrd}(O) = \{\, (g_+, g_-, g)_+ \in \mathrm{Atp}(O) \mid g \in \mathrm{SGO}(O)\,\} = \mathrm{Frd}(O) \cap \mathrm{SGO}(O)^3\,.$$

The results in this section and projection onto the final coordinate then immediately yield two short exact sequences for group central extensions:

(20.7). THEOREM.

(a) $$1 \longrightarrow F^\times \longrightarrow \mathrm{Frd}(O) \longrightarrow \mathrm{GO}(O) \longrightarrow 1\,.$$

(b) $$1 \longrightarrow F^\times \longrightarrow \mathrm{SFrd}(O) \longrightarrow \mathrm{SGO}(O) \longrightarrow 1\,.$$ □

20.3. The spin kernel and spin group

The spinor norm and spin group can be defined for any (nondegenerate) orthogonal space, but this would necessitate the introduction of the Clifford algebra (as in [**Asc00**]) or other machinery (for instance, as in [**Tay92**]) which we otherwise do not need. Here we only treat the spaces and groups associated with octonion algebras, making heavy use of the composition algebra structure. For us this treatment is sufficient, convenient, and elegant.

(20.8). PROPOSITION. *Let O be an octonion algebra. For each $g \in \mathrm{SGO}(O)$ choose $(g_+, g_-, g) \in \mathrm{SFrd}(O)$. Then for each $\epsilon \in \{\pm\}$ the map $\sigma_\epsilon \colon \mathrm{SGO}(O) \longrightarrow F^\times/(F^\times)^2$ given by*

$$\sigma_\epsilon(g) = \mu_{g_\epsilon}(F^\times)^2$$

is well-defined and gives a homomorphism from $\mathrm{SGO}(O)$ to the elementary abelian 2-group $F^\times/(F^\times)^2$.

The image of σ_ϵ is $q(O)^\times(F^\times)^2$. Especially σ_ϵ is surjective if O is split.

PROOF. By Theorem (20.5) the elements g_ϵ are well-defined up to a scalar β_ϵ. But if $q(x^{g_\epsilon}) = \mu_{g_\epsilon} q(v)$ for all $x \in O$, then

$$q(x^{\beta_\epsilon g_\epsilon}) = q(\beta_\epsilon x^{g_\epsilon}) = \beta_\epsilon^2 q(x^{g_\epsilon}) = \beta_\epsilon^2 \mu_{g_\epsilon} q(v)$$

for all $x \in O$. Thus $\mu_{\beta_\epsilon g_\epsilon} = \beta_\epsilon^2 \mu_{g_\epsilon}$ and $\sigma_\epsilon(\beta_\epsilon g_\epsilon) = \sigma_\epsilon(g_\epsilon)$; as a map, σ_ϵ is well-defined.

Consider $(g_+, g_-, g)_+, (h_+, h_-, h)_+ \in \mathrm{SFrd}(O)$ with product

$$(g_+h_+, g_-h_-, gh)_+ = ((gh)_+, (gh)_-, gh)_+ \in \mathrm{Atp}(O)\,.$$

Because μ is a homomorphism,

$$\begin{aligned} \sigma_\epsilon(gh) &= \mu_{(gh)_\epsilon}(F^\times)^2 \\ &= \mu_{g_\epsilon}\mu_{h_\epsilon}(F^\times)^2 \\ &= \mu_{g_\epsilon}(F^\times)^2\, \mu_{h_\epsilon}(F^\times)^2 \\ &= \sigma_\epsilon(g)\sigma_\epsilon(h)\,. \end{aligned}$$

Therefore σ_ϵ is indeed a homomorphism.

By Proposition (20.4) its image is $q(O)^\times(F^\times)^2$. As hyperbolic forms realize all possible values (by Proposition (17.2)(b)), this is surjective for split O. □

We defined the spinor norm for hyperbolic 8-space in Section 17.6, although we did not verify our claims about it. Now we both define it for arbitrary octonion algebras and prove that it has the desired properties.

(20.9). THEOREM. *Let O be an octonion algebra. On the group* $\mathrm{SO}(O) = \langle\, \mathrm{s}_1\, \mathrm{s}_b \mid b \in \mathrm{GOct}(O)\, \rangle$, *the spinor norm σ given by*

$$\sigma\colon \prod_i \mathrm{s}_{x_i} \mapsto \prod_i q(x_i)(F^\times)^2\,,$$

is a well-defined homomorphism from $\mathrm{SO}(O)$ *to* $F^\times/(F^\times)^2$. *Indeed, σ is the restriction to* $\mathrm{SO}(O)$ *of both of the homomorphisms σ_+ and σ_- from Proposition (20.8). The image of σ is $q(O)^\times(F^\times)^2$. Especially, σ is surjective if O is split.*

PROOF. From Proposition (20.3)(b), for nonsingular $x \in O$

$$(q(x)^{-1}\,\mathrm{L}(x)\,,\,\mathrm{R}(x)\,,\,\mathrm{s}_1\,\mathrm{s}_x) \in \mathrm{Atp}(O)\,.$$

Therefore

$$\sigma_+(\mathrm{s}_1\,\mathrm{s}_x) = \sigma_-(\mathrm{s}_1\,\mathrm{s}_x) = \sigma(\mathrm{s}_1\,\mathrm{s}_x) = q(x)(F^\times)^2\,,$$

as required.

Let $g \in \mathrm{SO}(O)$ and let $g = \prod_{i=1}^m \mathrm{s}_{x_i}$ be one of its factorizations. Here $m = 2k$ is even by Proposition (20.6)(a,c), so we have

$$g = \prod_{j=1}^k (\mathrm{s}_1\,\mathrm{s}_{x_{2j-1}})^{-1}(\mathrm{s}_1\,\mathrm{s}_{x_{2j}})$$

and then

$$\begin{aligned}\sigma_\epsilon(g) &= \sigma_\epsilon\Bigg(\prod_{j=1}^k (\mathrm{s}_1\,\mathrm{s}_{x_{2j-1}})^{-1}(\mathrm{s}_1\,\mathrm{s}_{x_{2j}})\Bigg)\\ &= \prod_{j=1}^k \sigma_\epsilon(\mathrm{s}_1\,\mathrm{s}_{x_{2j-1}})^{-1}\sigma_\epsilon(\mathrm{s}_1\,\mathrm{s}_{x_{2j}})\\ &= \prod_{j=1}^k q(x_{2j-1})(F^\times)^2 q(x_{2j})(F^\times)^2\\ &= \prod_{i=1}^m q(x_i)(F^\times)^2 = \sigma(g)\,.\end{aligned}$$

We conclude that σ is well-defined since σ_+ and σ_- are. Furthermore, for $g, h \in \mathrm{SO}(O)$,

$$\sigma(gh) = \sigma_\epsilon(gh) = \sigma_\epsilon(g)\sigma_\epsilon(h) = \sigma(g)\sigma(h)\,,$$

and σ is a homomorphism.

Finally $\sigma(\mathrm{s}_1\,\mathrm{s}_x) = q(x)(F^\times)^2$, so the image of σ is $q(O)^\times(F^\times)^2$. This is all of $F^\times/(F^\times)^2$ for split and hyperbolic (O, q), again by Proposition (17.2)(b). □

The *spin kernel* (or *reduced orthogonal group*) is $\Omega(O)$, the kernel of the spinor norm on $\mathrm{SO}(O)$. When O is split, the isomorphism class is uniquely determined by the field F and we may write $\Omega^+(O)$ or even $\Omega_8^+(F)$ (as seen in Section 17.6). The center is $\{\pm\operatorname{Id}\}$ (see below) and the corresponding central quotients are the respective projective groups $\mathrm{P}\Omega(O)$, $\mathrm{P}\Omega^+(O)$, and $\mathrm{P}\Omega_8^+(F)\,(=\mathrm{D}_4(F)\,)$.

For $g \in \Omega(O)$, consider a corresponding $(g_+, g_-, g)_+ \in \operatorname{Atp}(O)$. Then by Theorem (20.5) in fact $(g_+, g_-, g)_+$ belongs to $\operatorname{SFrd}(O)$ and

$$\mu_{g_+}\mu_{g_-} = \mu_g = 1 \text{ and } \mu_{g_\epsilon}(F^\times)^2 = \sigma(g) = (F^\times)^2\,.$$

Therefore there is a $\beta \in F$ with $\mu_{g_+} = \beta^{-2}$ and $\mu_{g_-} = \beta^2$. For $h_+ = \beta g_+$ and $h_- = \beta^{-1} g_-$ we find

$$(h_+, h_-, g) \in \operatorname{Atp}(O) \cap \operatorname{SO}(O)^3 = \operatorname{SFrd}(O) \cap \operatorname{SO}(O)^3\,.$$

Define the *spin group* $\operatorname{Spin}(O)$ to be the group $\operatorname{SFrd}(O) \cap \operatorname{SO}(O)^3$ ($= \operatorname{Atp}(O) \cap \operatorname{SO}(O)^3$). In the split case, this is $\operatorname{Spin}_8(F)$.

(20.10). THEOREM. *Let O be an octonion algebra. Then the projection π onto the third coordinate gives an exact sequence*

$$1 \longrightarrow \{\pm\operatorname{Id}\} \longrightarrow \operatorname{Spin}(O) \xrightarrow{\pi} \Omega(O) \longrightarrow 1\,.$$

This is a central extension. More precisely $\langle(-\operatorname{Id}, -\operatorname{Id}, \operatorname{Id}), (-\operatorname{Id}, \operatorname{Id}, -\operatorname{Id})\rangle$ is the center of $\operatorname{Spin}(O)$ *with image the center* $\{\pm\operatorname{Id}\}$ *of* $\Omega(O)$.

PROOF. Above we saw that for every $g \in \Omega(O)$ there is an $(h_+, h_-, g) \in \operatorname{Spin}(O)$. On the other hand, if $(h_+, h_-, g) \in \operatorname{Spin}(O)$, then $\sigma(g) = \sigma_\epsilon(h_\epsilon)$ is trivial; so $g \in \Omega(O)$. Therefore projection is a surjective homomorphism. The kernel consists of all $(k_+, k_-, \operatorname{Id})$ with $k_\epsilon \in \operatorname{SO}(O)$. By Theorem (20.5) this is precisely the central subgroup $\{\pm(-\operatorname{Id}, -\operatorname{Id}, \operatorname{Id})\}$. The central subgroup $\{\pm(-\operatorname{Id}, \operatorname{Id}, -\operatorname{Id})\}$ of $\operatorname{Spin}(F)$ then has image the scalar subgroup $\{\pm\operatorname{Id}\}$ of $\Omega(O)$. Indeed, this is its full center (say, by Proposition (21.3)(a) below). □

Some care must be take with context for the spin group. In the literature one can find statements to the effect that the spin group is a double cover of the special orthogonal group. As the theorem suggests, this holds only when the spinor norm is the trivial map. This is often not the case (for instance, when F is a finite field of odd characteristic) but does occur in certain important circumstances. If the field F is algebraically closed, as in the context of algebraic groups, then $F^2 = F$ and the spinor norm must be trivial. Similarly, in the theory of Lie groups we may implicitly be restricted to the real field $\mathbb{R}$ and the standard Euclidean form, where the nonzero value set is equal to $\mathbb{R}^+ = (\mathbb{R}^\times)^2$ and the spinor norm is again trivial.

Chapter 21

The Loop of Units in an Octonion Algebra

In the matrix algebra $\mathrm{Mat}_2(F)$ the group of units is $\mathrm{GL}_2(F)$. It has scalar center $F^\times I$ and dually a determinant homomorphism with kernel $\mathrm{SL}_2(F)$. The determinant of the scalars gives all squares, and the center meets $\mathrm{SL}_2(F)$ in $\{\pm I\}$. We have the projective quotients $\mathrm{PGL}_2(F)$ and $\mathrm{PSL}_2(F)$, the latter almost always simple. In view of Zorn's vector matrices, an octonion algebra O, particularly if split, might be viewed as a generalization of $\mathrm{Mat}_2(F)$. Various similar loop sections exist within the Moufang loop of units of O. In the split case their analysis goes well. But just as the division rings that are forms of $\mathrm{Mat}_2(F)$ are more exotic, so the structure and properties of division algebras O are more elusive.

21.1. Loop sections of octonion algebras

We discuss the appropriate generalizations of the center and the determinant.

The composition algebra (A, q) over the field F will usually be written A with the form q and field F implicit. An octonion algebra O over F may at times be denoted $\mathrm{Oct}(F)$. Especially $\mathrm{Oct}^+(F)$ is a split octonion algebra over F. Theorem (19.21) tells us that an algebra $\mathrm{Oct}^+(F)$ is uniquely determined up to isomorphism. A particular model for $\mathrm{Oct}^+(F)$ is that of Zorn's vector matrices, discussed at length in Section 19.1.2.

By Corollary (19.8) an element m of $\mathrm{Oct}(F)$ is invertible if and only if $q(m) \neq 0$. Recall that the corresponding loop of units, the *general octonion loop* or *unit octonion loop*, is denoted $\mathrm{GOct}(O)$ or $\mathrm{GOct}(F)$ and is a nonassociative Moufang loop by Theorem (19.23). In the split case we write $\mathrm{GOct}^+(F)$ for the loop of units in $\mathrm{Oct}^+(F)$. In the nonsplit case $\mathrm{GOct}(O) = O \setminus \{0\}$, so that O is a *division algebra*.

Since q admits composition, it is a loop homomorphism from $\mathrm{GOct}(O)$ to $F^\times$. Its kernel, denoted $\mathrm{SOct}(O)$ or $\mathrm{SOct}(F)$, is the normal subloop consisting of all units having norm 1. This is the *special octonion loop* or *norm* 1 *octonion loop*. In the split case $\mathrm{GOct}^+(F)$ this is $\mathrm{SOct}^+(F)$ and the map to $F^\times$ is surjective by Proposition (17.2)(b).

The utility of results like the following was first observed by P. Vojtěchovský; see [**NVo03**, Theorem 7.1].

(21.1). PROPOSITION. *The composition algebra A is spanned by its subloop of elements with norm* 1 *unless it is isomorphic to one of the split algebras $\mathbb{F}_2 \oplus \mathbb{F}_2$ or $\mathbb{F}_3 \oplus \mathbb{F}_3$.*

PROOF. This is trivial if the dimension is 1.

Consider the split case. For $F \oplus F$ with form $q((a,b)) = ab$, the norm 1 loop is the subgroup $S = \{\, (a, a^{-1}) \mid a \in F^\times \,\}$. It contains $1 = (1,1)$, so S spans A unless $F^\times = \{\, a \in F \mid a = a^{-1} \,\}$, that is, unless F is $\mathbb{F}_2$ or $\mathbb{F}_3$. In those two cases the full algebra is not spanned by S.

In dimension 4, the split algebra $\mathrm{Mat}_2(F)$ is always spanned by the four norm 1 matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}.$$

In dimension 8, the split algebra A is $\mathrm{Mat}_2(F) \perp \mathrm{Mat}_2(F)t$ as in Proposition (19.19). We may choose t with $q(t) = 1$ by Proposition (17.2), as q is hyperbolic on A. Since $\mathrm{Mat}_2(F)$ is spanned by elements of norm 1, so is $\mathrm{Mat}_2(F)t$ and finally A as well.

We may now assume that our composition algebra A is nonsplit; that is, is a division algebra. In particular, for every nonscalar $x \in A \setminus 1^\perp$, the subspace $F1 \oplus Fx$ is a nonsplit composition subalgebra by Proposition (17.2) and Corollary (19.10). All such subalgebras generate A, so we are reduced to consideration of 2-dimensional nonsplit composition algebras.

By Theorem (19.21) there is a separable quadratic extension K of F such A is isomorphic as composition algebra to K provided with the quadratic norm $q(a) = aa^\gamma$, where γ acts as Galois conjugation in K over F. As $1 \cdot 1^\gamma = 1$, the claim that K is spanned by its norm 1 elements is equivalent to the claim that not all norm 1 elements are in the fixed subfield F. Assume the opposite, for a contradiction.

For $a \in K^\times$ the commutator $a^{-1}a^\gamma$ has norm 1 and so belongs to $F^\times$ by assumption. Each norm aa^γ is fixed by γ and so also belongs to F. We conclude that all (nonzero) squares $a^2 = aa^\gamma(a^{-1}a^\gamma)^{-1}$ belong to F. Let $a \in K \setminus F$. We then have $b = a^2 \in F$ and also $(a+1)^2 = a^2 + 2a + 1 \in F$. Therefore $2a \in F$. As $a \notin F$, this can only happen in characteristic 2. In that case, a is a root of the inseparable polynomial $z^2 + b \in F[z]$. This is a contradiction, since K is separable over F. □

For each $(g_+, g_-, g_0)_\epsilon \in \mathrm{Frd}(O)$, the permutations g_δ from $\mathrm{Sym}(O)$ in fact belong to $\mathrm{GO}(O)$ by Theorem (20.5). In particular for nonsingular a the image a^{g_δ} is also nonsingular. That is, the elements of $\mathrm{Frd}(O)$ in their action on O^3 leave $\mathrm{GOct}(O)^3$ invariant and indeed induce autotopisms or anti-autotopisms of $\mathrm{GOct}(O)$. We can therefore consider the homomorphism given by restriction from O to the invariant $\mathrm{GOct}(O)$. The proposition immediately gives:

(21.2). COROLLARY. *The restriction map* $\mathrm{Frd}(O) \longrightarrow \mathrm{AAtp}(\mathrm{GO}(O))$ *is an injective homomorphism.* □

(21.3). PROPOSITION. *Let O be an octonion algebra over F.*

(a) *If $g \in \mathrm{SO}(O)$ takes each $x \in \mathrm{SOct}(O)$ to $\pm x$, then g is a scalar from $\{\pm \mathrm{Id}\}$.*
(b) *If $g \in \mathrm{GO}(O)$ leaves invariant each* 1*-space Fx with $q(x) \neq 0$, then g is a scalar from $F^\times$* Id.

PROOF. As O is spanned by $\mathrm{SOct}(O)$ (Proposition (21.1)), it is enough in both parts to prove that the function $\alpha\colon \mathrm{SOct}(O) \longrightarrow F$, given by $x^g = \alpha_x x$, is a constant function $\alpha_x = \alpha$. For $F = \mathbb{F}_2$ we must have $\alpha_x = 1$, and g is the identity; we are done. For $F = \mathbb{F}_3$, the only possible scalars α_x are ± 1, so the element g has order 2 (or 1), and the hypotheses say that every $x \in \mathrm{SOct}(O)$ is in one of the eigenspaces $\mathrm{C}_O(g)$ and $[O, g]$. But $|\,\mathrm{SOct}(O)| = 2160$ while $3^6 - 1 = 728$ and $3^7 - 1 = 2186$, so easily the only possibilities are $O = \mathrm{C}_O(g)$ or $O = [O, g]$; that is, g is a scalar as claimed. Thus in proving (a) and (b) we may assume $|F| \geq 4$.

(a) Here $\alpha_x = \pm 1$. In particular we may assume that $\mathrm{char} F \neq 2$.

By Lemma (17.10) the space O is the perpendicular direct sum of its two eigenspaces $\mathrm{C}_O(g)$ and $[O, g]$. By hypothesis every element of $\mathrm{SOct}(O)$ belongs to one or the other eigenspace. We may assume (for a contradiction) that both are nontrivial.

By Proposition (21.1) there are $x \in \mathrm{C}_O(g)$ and $y \in [O, g]$ with $q(x) = q(y) = 1$. Choose nonzero $a, b \in F$ with $a^2 = 1 + b^2$ (always possible as $|F| \geq 4$). Then $v = x + by$ has $q(v) = 1 + b^2 = a^2$. Thus $a^{-1}v$ is in $\mathrm{SOct}(O)$ but in neither of the eigenspaces $\mathrm{C}_O(g)$ and $[O, g]$, the desired contradiction.

(b) As before α from $\mathrm{GOct}(O)$ to $F^\times$ is given by $x^g = \alpha_x x$. By Proposition (17.2), if a 2-subspace of O contains nonsingular vectors then it has at most two singular 1-spaces, so it contains a basis x, y of nonsingular vectors such that $x + y$ is also nonsingular (as $|F| \geq 4$). But then

$$x^g + y^g = (x+y)^g \implies \alpha_x x + \alpha_y y = \alpha_{x+y}(x+y) = \alpha_{x+y} x + \alpha_{x+y} y\,,$$

so $\alpha_x = \alpha_{x+y} = \alpha_y$. Thus α is constant on each 2-space containing nonsingular vectors. Applied to the subalgebras $F1 \oplus Fx$, this shows that the map α is a constant on $\mathrm{GOct}(O)$. Therefore g is a scalar linear transformation by Proposition (21.1). □

(21.4). THEOREM.

(a) $\mathrm{Nuc}(\mathrm{GOct}(F)) = \mathrm{C}(\mathrm{GOct}(F)) = \mathrm{Z}(\mathrm{GOct}(F)) = F^\times 1$.

(b) $\mathrm{Nuc}(\mathrm{SOct}(F)) = \mathrm{C}(\mathrm{SOct}(F)) = \mathrm{Z}(\mathrm{SOct}(F)) = \{\pm 1\}$.

PROOF. By Proposition (21.1) the nucleus of $\mathrm{GOct}(F)$ and that of $\mathrm{SOct}(F)$ are nuclear in $\mathrm{Oct}(F)$, so they consist of central scalars by Theorem (19.27). This is similarly true for the centralizer of $\mathrm{GOct}(F)$. In particular the nonzero scalar subgroup $F^\times 1$ of $\mathrm{GOct}(F)$ is equal to the normal central subgroup $\mathrm{Nuc}(\mathrm{GOct}(F)) = \mathrm{C}(\mathrm{GOct}(F)) = \mathrm{Z}(\mathrm{GOct}(F))$.

For the scalar b we have $q(b) = b^2 q(1) = b^2$. Especially the only scalars of norm 1 are ± 1, and thus $\mathrm{Nuc}(\mathrm{SOct}(F)) = \mathrm{C}(\mathrm{SOct}(F)) = \mathrm{Z}(\mathrm{SOct}(F))$ is the normal, central, scalar subgroup $\{\pm 1\}$ of order 1 or 2. □

The quotient loop $\mathrm{GOct}(F))/F^\times 1$ is $\mathrm{PGOct}(F)$, the *projective general octonion loop*, especially $\mathrm{PGOct}^+(F)$ in the split case. Similarly the quotient $\mathrm{SOct}(F)/\{\pm 1\}$ is the *projective special octonion loop* $\mathrm{PSOct}(F)$. In particular we have $\mathrm{PSOct}^+(F)$, usually called a *Paige loop* since Paige [**Pai56**] first studied these loops carefully, proving that they are simple Moufang loops.[1] Alternative notation is $\mathrm{PGOct}(O)$ and $\mathrm{PSOct}(O)$.

[1] Notation for the Paige loops varies. For instance, they are $\mathrm{M}(F)$ in [**Dor78**], $\mathrm{M}^*(F)$ in [**NVo03**], and $\mathrm{PSLL}(F)$ in [**Gag06**].

(21.5). Theorem. *The loops* $\mathrm{PGOct}(F)$ *and* $\mathrm{PSOct}(F)$ *have trivial nucleus.*

Proof. Let n be a preimage in $\mathrm{GOct}(O)$ of an element of the nucleus of L, one of these loops. Then by Proposition (21.1) it belongs to the subspace

$$M = \{\, m \in O \mid x(my) - (xm)y \in F1\,,\ \text{for all } x, y \in O\,\}$$

of Proposition (19.26). By that proposition n is a central scalar and so has trivial image in the loop L. □

(21.6). Theorem. *The norm map* $q\colon \mathrm{GOct}(O) \longrightarrow F^\times$ *is a surjective homomorphism in* $\mathsf{Loop}^\star$. *Therefore there is a surjective homomorphisms in* $\mathsf{TriGrp}^\star$ *from the universal group with triality* $\mathrm{GOct}(O)\mathbf{G} = \mathrm{G}_{\mathrm{GOct}(O)}$ *to* $(F^\times \times F^\times) \rtimes \mathrm{Sym}(3)$.

Proof. By Lemma (11.2) the universal group with triality $G = \mathrm{G}_{\mathrm{GOct}(O)}$ has as quotient in $\mathsf{TriGrp}^\star$ the universal group $H = \mathrm{G}_{F^\times}$ for the $\mathsf{Mouf}^\star$-image $F^\times$. By Corollary (4.7) this last group has quotient $(F^\times \times F^\times) \rtimes \mathrm{Sym}(3)$. □

21.2. Octonion multiplication and triality groups

Let O be an octonion algebra over F. In this section for the loops L among $\mathrm{GOct}(O)$, $\mathrm{PGOct}(O)$, $\mathrm{SOct}(O)$, and $\mathrm{PSOct}(O)$ we approach the multiplication group $\mathrm{Mlt}(L)$ and the associated universal group with triality G_L. The results are not definitive. Especially, the identification of the center $\mathrm{Z}(\mathrm{G}_L)$ is difficult for any Moufang loop; we do not address that here. We would be happy to find each corresponding adjoint group with triality $\mathrm{TAtp}(L)$, defined by

$$\mathrm{TAtp}(L) = \mathrm{G}_L\,/\mathrm{Z}(\mathrm{G}_L) = L\mathbf{TA} = \mathrm{SAtp}(L) \rtimes \mathrm{Sym}(3)$$

or its base, the special autotopism group $\mathrm{SAtp}(L)$. Even with that we are not entirely successful.

There is, however, some good news. By Theorem (12.15) the multiplication group $\mathrm{Mlt}(L)$ is a quotient of $\mathrm{SAtp}(L)$ by an A isomorphic to a subgroup of the nucleus of L. In the previous section we have proven that each L has a relatively elementary nucleus. Indeed $\mathrm{PGOct}(O)$ and $\mathrm{PSOct}(O)$ have trivial nuclei, so for these two loops $\mathrm{Mlt}(L) = \mathrm{SAtp}(L)$.

(21.7). Theorem. *For the octonion algebra O, the multiplication group of its loop of units* $\mathrm{GOct}(O)$ *is the special general orthogonal group* $\mathrm{SGO}(O)$.

Proof. We found in Proposition (20.6)(b) that within $\mathrm{GO}(O)$ the linear transformation group $\langle\, \mathrm{L}(a), \mathrm{R}(a) \mid a \in \mathrm{GOct}(O)\,\rangle$ is $\mathrm{SGO}(O)$. By Proposition (21.1) this action is faithful when restricted to $\mathrm{GOct}(O)$. We conclude that $\mathrm{Mlt}(O) = \mathrm{SGO}(O)$. □

(21.8). Corollary. $\mathrm{Mlt}(\mathrm{PGOct}(F)) = \mathrm{SAtp}(\mathrm{PGOct}(F)) = \mathrm{PSGO}(O)$.

Proof. As $\mathrm{PGOct}(F)$ has trivial nucleus (by Theorem (21.5)) we have

$$\mathrm{Mlt}(\mathrm{PGOct}(F)) = \mathrm{SAtp}(\mathrm{PGOct}(F))$$

by Theorem (12.15). Let $N = F^\times 1$, the nucleus of $\mathrm{GOct}(F)$. Each translation $\mathrm{L}(x)$ and $\mathrm{R}(y)$ of $\mathrm{Mlt}(\mathrm{GOct}(F))$ induces the translation $\mathrm{L}(Nx)$ and $\mathrm{R}(Ny)$ on $\mathrm{PGOct}(F) = \mathrm{GOct}(F)/N$. Accordingly

$$\mathrm{L}(x) \mapsto \mathrm{L}(Nx) \qquad \mathrm{R}(y) \mapsto \mathrm{R}(Ny)$$

gives a surjective homomorphism from $\mathrm{Mlt}(\mathrm{GOct}(F))$ onto $\mathrm{Mlt}(\mathrm{PGOct}(F))$. The kernel of this homomorphism is induced by linear transformations from $\mathrm{SGO}(O) = \mathrm{Mlt}(\mathrm{GOct}(F))$ that leave each 1-space of $\mathrm{GOct}(F)$ invariant. Therefore by Proposition (21.3)(b) the kernel consists of the scalar subgroup $F^\times 1$ and

$$\mathrm{Mlt}(\mathrm{PGOct}(F)) = \mathrm{SGO}(O)/F^\times 1 = \mathrm{PSGO}(O)\,,$$

as claimed. □

(21.9). THEOREM. *The group admitting triality* $\mathrm{SAtp}(\mathrm{GOct}(O))$ *is equal to* $\mathrm{SFrd}(O)$*, identified with its image in* $\mathrm{Atp}(\mathrm{GOct}(O))$ *via Corollary (21.2). Especially there is a short exact sequence*

$$1 \longrightarrow F^\times \longrightarrow \mathrm{SAtp}(\mathrm{GOct}(O)) \longrightarrow \mathrm{SGO}(O) \longrightarrow 1\,.$$

PROOF. By the previous theorem and Proposition (12.11)

$$\mathrm{SAtp}(\mathrm{GOct}(O)) \le \{\, (g_+, g_-, g) \in \mathrm{Atp}(\mathrm{GOct}(O)) \mid g \in \mathrm{SGO}(O)\,\} = \mathrm{SFrd}(O),$$

with both $\mathrm{SAtp}(\mathrm{GOct}(O))$ and $\mathrm{SFrd}(O)$ projecting in the last coordinate to $\mathrm{Mlt}(O) = \mathrm{SGO}(O)$. Therefore

$$\mathrm{SFrd}(O) = \mathrm{SAtp}(\mathrm{GOct}(O))M\,,$$

where $M = \{\, (f, f^{-1}, \mathrm{Id}) \mid f \in F^\times\,\}$ is the kernel of projection in $\mathrm{SFrd}(O)$ onto its third coordinate. Indeed it is that same kernel in all $\mathrm{Atp}(O)$ by Theorem (20.5). Now within $\mathrm{Atp}(\mathrm{GOct}(O))$ we see that $M \le \mathrm{SAtp}(F^\times 1) \le \mathrm{SAtp}(\mathrm{GOct}(O))$. Thus $\mathrm{SFrd}(O) = \mathrm{SAtp}(\mathrm{GOct}(O))$ and the short exact sequence

$$1 \longrightarrow F^\times \longrightarrow \mathrm{SFrd}(O) \longrightarrow \mathrm{SGO}(O) \longrightarrow 1\,.$$

of Theorem (20.7) becomes that of the theorem. □

In view of Theorem (21.9), it is tempting to think that for the subloop $\mathrm{SOct}(O)$ the corresponding group admitting triality is $\mathrm{Atp}(\mathrm{SOct}(O)) \cap \mathrm{SO}(O)^3 = \mathrm{Spin}(O)$ so that the multiplication group would be $\Omega(O)$. We shall see in the next section that this does happen in the split case, but we cannot prove it in general. The difficulty arises because earlier we were able to use the Cartan-Dieudonné Theorem to prove $\langle\, \mathrm{s}_1\, \mathrm{s}_a \mid q(a) \neq 0\,\rangle = \mathrm{SO}(O)$ hence $\langle\, \mathrm{L}(a), \mathrm{R}(a) \mid q(a) \neq 0\,\rangle = \mathrm{SGO}(O)$, whereas now we only have $\langle\, \mathrm{s}_1\, \mathrm{s}_a \mid q(a) = 1\,\rangle \le \langle\, \mathrm{L}(a), \mathrm{R}(a) \mid q(a) = 1\,\rangle \le \Omega(O)$.

Define the normal subgroup $\Omega^1(O)$ of $\mathrm{O}(O)$ to be the subgroup generated by all products $\mathrm{s}_1\, \mathrm{s}_a$ for $q(a) = 1$, equivalently $q(a) \in (F^\times)^2$. The spinor norm is trivial on each element $\mathrm{s}_1\, \mathrm{s}_a$, so we have $\Omega^1(O) \le \Omega(O)$.

(21.10). THEOREM. *Let O be an octonion algebra. The multiplication group of* $\mathrm{SOct}(O)$ *is is a nonscalar normal subgroup of* $\Omega(O)$ *that contains* $\Omega^1(O)$*.*

PROOF. By Proposition (21.1), the embedding of

$$\mathrm{Mlt}(\mathrm{SOct}(O)) = \langle\, \mathrm{L}(a), \mathrm{R}(a) \mid q(a) = 1\,\rangle$$

in $\mathrm{Mlt}(\mathrm{GOct}(O))$ and $\mathrm{Mlt}(O)$ is an injection.

The similarities $\mathrm{L}(a)$ and $\mathrm{R}(a)$ are isometries when $q(a) = 1$ and so belong to $\mathrm{SO}(O) = \mathrm{O}(O) \cap \mathrm{SGO}(O)$ by Proposition (20.6). Therefore by Proposition (12.11) $\mathrm{SAtp}(\mathrm{SOct}(O)) \le \mathrm{Atp}(O) \cap \mathrm{SO}(O)^3$ which is $\mathrm{Spin}(O)$ (Theorem (20.10)). From the third coordinate of this, we learn that $\mathrm{Mlt}(\mathrm{SOct}(O))$ is a normal subgroup of $\Omega(O)$, clearly nonscalar by Proposition (21.1).

By Lemma (20.2)(b), for all $x \in O$ and $q(a) = 1$

$$x^{\mathrm{s}_1\,\mathrm{s}_a} = q(a)^{-1}axa = axa = x^{\mathrm{L}(a)\,\mathrm{R}(a)}\,,$$

so the normal subgroup $\Omega^1(O)$ of $\mathrm{O}(O)$ is contained in $\mathrm{Mlt}(\mathrm{SOct}(O))$. □

By Theorem (21.4)(b) the loop $\mathrm{SOct}(O)$ has nucleus $\{\pm 1\}$, and the subgroup $\{\pm\,\mathrm{Id}\}$ of scalars in $\Omega(O)$ is in the kernel of the natural map from $\mathrm{Mlt}(\mathrm{SOct}(O))$ to $\mathrm{Mlt}(\mathrm{PSOct}(O))$. Indeed by Proposition (21.3)(a) it is equal to that kernel and to the center of $\Omega(O)$ (see Theorem (20.10)).

Let $\mathrm{P}\Omega(O)$ and $\mathrm{P}\Omega^1(O)$ be the images of $\Omega(O)$ and $\Omega^1(O)$ in $\mathrm{PSO}(O)$. The remarks of the previous paragraph give

(21.11). Corollary. *Let O be an octonion algebra. Then* $\mathrm{Mlt}(\mathrm{PSOct}(O)) = \mathrm{SAtp}(\mathrm{PSO}(O))$ *is a nontrivial normal subgroup of* $\mathrm{P}\Omega(O)$ *that contains* $\mathrm{P}\Omega^1(O)$*.*
□

21.3. The split octonions

In the case of the split octonions O over F we can provide complete results in the cases that were not resolved in the previous section. It is no surprise that we encounter Cartan's group with triality again.

Nagy and Vojtěchovský [**NVo03**] calculated the multiplication groups of the special split octonion loops $\mathrm{SOct}^+(F)$ and the Paige loops $\mathrm{PSOct}^+(F)$. They observed that these results are "folklore" but are rarely (if ever, before [**NVo03**]) provided with a complete proof. At least for finite Paige loops, the results are already implicit in Doro's paper [**Dor78**].

(21.12). Theorem.

(a) $\mathrm{Mlt}(\mathrm{SOct}^+(F)) = \Omega_8^+(F)$.
(b) $\mathrm{SAtp}(\mathrm{SOct}^+(F)) = \mathrm{Spin}_8(F)$.
(c) $\mathrm{TAtp}(\mathrm{SOct}^+(F)) = \mathrm{Spin}_8(F) \rtimes \mathrm{Sym}(3)$.

Proof. From Theorem (21.10) we have the nonscalar subgroup $\Omega^1(O)$ contained in $\mathrm{Mlt}(\mathrm{SOct}(O))$, both normal in $\Omega(O) = \Omega_8^+(F)$. By Theorem (17.16) this last group is quasisimple. Therefore

$$\Omega^1(O) = \mathrm{Mlt}(\mathrm{SOct}(O)) = \Omega_8^+(F)\,,$$

as claimed under (a).

As in proof of Theorem (21.10), Proposition (12.11) yields

$$\mathrm{SAtp}(\mathrm{SOct}^+(O)) \le \mathrm{Atp}(O) \cap \mathrm{SO}(O)^3 = \mathrm{Spin}_8(F)$$

with the projection of $\mathrm{SAtp}(\mathrm{SOct}^+(O))$ onto each coordinate equal to $\Omega_8^+(F) = \mathrm{Mlt}(\mathrm{SOct}^+(F))$ by (a). Especially $(-\mathrm{Id}, -\mathrm{Id}, \mathrm{Id}) \in \mathrm{SAtp}(\mathrm{SOct}^+(O))$, so

$$\mathrm{SAtp}(\mathrm{SOct}^+(O)) = \langle(-\mathrm{Id}, -\mathrm{Id}, \mathrm{Id})\rangle\,\mathrm{SAtp}(\mathrm{SOct}^+(O)) = \mathrm{Spin}_8(F)\,,$$

as in (b). Part (c) follows directly. □

(21.13). Theorem.

(a) $\mathrm{Mlt}(\mathrm{PSOct}^+(F)) = \mathrm{SAtp}(\mathrm{PSOct}^+(F)) = \mathrm{P}\Omega_8^+(F)$.
(b) $\mathrm{TAtp}(\mathrm{PSOct}^+(F)) = \mathrm{P}\Omega_8^+(F) \rtimes \mathrm{Sym}(3)$.

Proof. From Theorem (21.11) we have the nontrivial subgroup $\mathrm{P}\Omega^1(O)$ contained in $\mathrm{Mlt}(\mathrm{PSOct}(O))$, both normal in $\mathrm{P}\Omega(O) = \mathrm{P}\Omega_8^+(F)$. By Theorem (17.16) this last group is simple. □

21.4. Simple Moufang loops

It is fitting that we finish this lengthy monograph by returning to Paige's early and fundamental paper [**Pai56**]. Its main result is:

(21.14). THEOREM. *For every field F, the Moufang loop* $\mathrm{PSOct}^{+}(F)$ *is simple.*

PROOF. By Theorem (21.13) $\mathrm{Mlt}(\mathrm{PSOct}^{+}(F)) = \mathrm{P}\Omega_8^{+}(F)$, which is simple by Theorem (17.16). The result follows from Corollary (14.6). □

A converse to Paige's theorem has been conjectured, namely that all nonassociative simple Moufang loops are isomorphic to $\mathrm{PSOct}(O)$ for some octonion algebra O. Liebeck [**Lie87**] proved this for finite Moufang loops and Hall [**Hal07b**] for locally finite Moufang loops (that is, Moufang loops in which every finite subset generates a finite subloop). Under these hypotheses only the split case occurs (Corollary (17.4)), so the nonassociative simple Moufang loops encountered are Paige loops.

(21.15). THEOREM. (LIEBECK [**Lie87**] (HALL [**Hal07b**])) *A (locally) finite simple Moufang loop is either associative—and so is a simple group—or is isomorphic to a Paige loop* $\mathrm{PSOct}^{+}(F)$ *over a (locally) finite field F.* □

Following Doro's plan [**Dor78**] and Theorem (14.5)(3), Liebeck searched the list of nonabelian finite simple groups H, looking for triality simple groups $H \rtimes \mathrm{Sym}(3)$. He proved that the only examples are $\mathrm{P}\Omega_8^{+}(F) \rtimes \mathrm{Sym}(3)$ over finite fields F. The associated loops are then the Paige loops $\mathrm{PSOct}^{+}(F)$.

Two additional observations of Paige [**Pai56**] are consequences of Corollary (14.6). They point up the distinction between the uniformity of the split case, as seen in Paige's Theorem (21.14), and the sensitivity of the nonsplit case to the arithmetic of the underlying field.

(21.16). COROLLARY.

(a) *Let $\mathbb{O}$ be the real compact octonions (the original Cayley-Graves octonions). Then* $\mathrm{Mlt}(\mathrm{PSOct}(\mathbb{O})) = \mathrm{P}\Omega(\mathbb{O}) = \mathrm{PSO}(\mathbb{O})$ *is simple (as is well-known), and in particular* $\mathrm{PSOct}(\mathbb{O})$ *is simple.*

(b) *Let $\mathbb{O}_t$ denote the real compact octonions tensored up to the field $\mathbb{R}((t))$ of Laurent series. Then* $\mathrm{Mlt}(\mathrm{PSOct}(\mathbb{O}_t))$ *is not simple* [**Die48**]*, and in particular* $\mathrm{PSOct}(\mathbb{O}_t)$ *is not simple.* □

Bibliography

[Asc00] M. Aschbacher, "Finite Group Theory," Second edition, Cambridge Studies in Advanced Mathematics, **10**, Cambridge University Press, Cambridge, 2000.

[Bog08] O. Bogopolski, "Introduction to Group Theory." EMS Textbooks in Mathematics, European Mathematical Society, Zürich, 2008.

[Bol37] G. Bol, *Gewebe und Gruppen (Topologische Fragen der Differentialgeometrie 65.)*, Math. Ann., **114** (1937), 414–431.

[Bra27] H. Brandt, *Verallgemeinierung des Gruppenbegriffs*, Math. Ann., **96** (1927), 360–366.

[Bru58] R.H. Bruck, "A Survey of Binary Systems," Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft **20**, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1958.

[BuC97] F. Buekenhout and A.M. Cohen, *Chapter 15: Generalized hexagons*, draft book chapter, 1997.

[Cam92] P.J. Cameron, "Projective and Polar Spaces," QMW Math Notes **13**, Queen Mary and Westfield College, 1992.

[Car25] É. Cartan, *Le principe de dualité et la théorie des groupes simples et semi-simple*, Bull. Sc. Math., **49** (1925), 361–374.

[Che74] O. Chein, *Moufang loops of small order. I*, Trans. Amer. Math. Soc., **188** (1974), 31–51.

[Che78] O. Chein, *Moufang loops of small order*, Mem. Amer. Math. Soc., **13** (1978), no. 197.

[ChP71] O. Chein and H. Pflugfelder, *The smallest Moufang loop*, Arch. Math. (Basel), **22** (1971), 573–576.

[Cho49] W.L. Chow, *On the geometry of algebraic homogeneous spaces*, Ann. of Math. (Series 2), **50** (1949), 32–67.

[Coh13] A.M. Cohen, "Diagram Geometry," draft, 23 August 2013.

[Cur07] R.T. Curtis, *Construction of a family of Moufang loops*, Math. Proc. Cambridge Philos. Soc., **142** (2007), 233–237.

[DeK74] J. Dénes, A.D. Keedwell, "Latin Squares and their Applications," Academic Press, New York-London, 1974.

[Die48] J. Dieudonné, "Sur les Groupes Classiques," Actualités Sci. Ind., **1040**, Hermann et Cie., Paris, 1948.

[Die51] J. Dieudonné, *Algebraic homogeneous spaces over fields of characteristic two*, Proc. Amer. Math. Soc., **2** (1951), 295–304.

[Dor78] S. Doro, *Simple Moufang loops*, Math. Proc. Cambridge Philos. Soc., **83** (1978), 377–392.

[Dra11] A. Drápal, *A simplified proof of Moufang's theorem*, Proc. Amer. Math. Soc., **139** (2011), 93–98.

[Fre51] H. Freudethal, *Oktaven, Ausnahmegruppen und Oktavengeometrie*, Geom. Dedicata, **19** (1985), 7–63.

[Fro90] M. Frolov, *Recherches sur les permutations carrées*, J. Math. Spec., (3) **4** (1890), 8–11.

[FuN93] M. Funk and P.T. Nagy, *On collineation groups generated by Bol reflections*, J. Geom., **48** (1993), 63–78.

[Gag06] S.M. Gagola III, *Subloops of the unit octonions*, Acta Sci. Math. (Szeged), **72** (2006), 837–861.

[Gla68] G. Glauberman, *On loops of odd order, II*, J. Algebra, **8** (1968), 393–414.

[GrZ06] A.N. Grishkov and A.V. Zavarnitsine, *Groups with triality*, J. Algebra Appl., **5** (2006), 441–463.

[Hal00] J.I. Hall, *Notes on composition algebras*, 2000 (revised 2012):
`www.math.msu.edu/~jhall/research/research.html`

[Hal06] J.I. Hall, *A characterization of the full wreath product*, J. Algebra 300 (2006), 529–554.

[Hal07a] J.I. Hall, *Central automorphisms of Latin squares and loops*, Quasigroups and Related Systems **15** (2007), 19–46.

[Hal07b] J.I. Hall, *Locally finite simple Moufang loops*, Turkish J. Math. **31** (2007), 45–61.

[Hal10] J.I. Hall, *On Mikheev's construction of enveloping groups*, Comm. Math. Univ. Carolinae **51** (2010), 245–252.

[Hal11] J.I. Hall *Central automorphisms, Z^*-theorems, and loop structure*, Quasigroups and Related Systems **19** (2011), 69–108.

[Hal12] J.I. Hall, *Triality (after Tits)*, 2012:
`www.math.msu.edu/~jhall/research/research.html`

[HaN01] J.I. Hall and G.P. Nagy, *On Moufang* 3*-nets and groups with triality*, Acta Sci. Math. (Szeged), **67** (2001), 675–685.

[Hll43] M. Hall, Jr., *Projective planes*, Trans. Amer. Math. Soc., **54** (1943), 229–277,

[Hll49] M. Hall, Jr., *Correction to "Projective planes,"* Trans. Amer. Math. Soc., **65** (1949), 473–474.

[Hil00] D. Hilbert, *Les principes fondamentaux de la géométrie*, Ann. Sci. École Norm. Sup. (3), **17** (1900), 103–209.

[Hum90] J.E. Humphreys, "Reflection Groups and Coxeter Groups," Cambridge Studies in Advanced Mathematics, **29**, Cambridge University Press, Cambridge, 1990.

[Jac89] N. Jacobson, "Basic Algebra II," Second edition, W.H. Freeman and Company, New York, 1989.

[Lie87] M.W. Liebeck, *The classification of finite simple Moufang loops*, Math. Proc. Cambridge Philos. Soc., **102** (1987), 33–47.

[MSW13] U. Meierfrankenfeld, G. Stroth, R.M. Weiss, *Local identification of spherical buildings and finite simple groups of Lie type*, Math. Proc. Cambridge Philos. Soc., **154** (2013), 527–547.

[Mik93] P.O. Mikheev, *Groups that envelop Moufang loops*, Uspekhi Mat. Nauk, **48** (1993), 191–192; translation in Russian Math. Surveys, **48** (1993), 195–196.

[Mou33] R. Moufang, *Alternativkörper und der Satz vom vollständigen Vierseit (D_9)*, Abh. Math. Sem. Univ. Hamburg, **9** (1933), 207–222.

[Mou35] R. Moufang, *Zur Struktur von Alternativkörpern*, Math. Ann., **110** (1935), 416–430.

[Nag11] G.P. Nagy, *personal communication*, August 2011.

[NVa04] G.P. Nagy and M. Valsecchi, *Splitting automorphisms and Moufang loops*, Glasg. Math. J., **46** (2004), 305–310.

[NVo03] G.P. Nagy and P. Vojtěchovský, *Octonions, simple Moufang loops and triality*, Quasigroups Related Systems, **10** (2003), 65–94.

[Pai56] L.J. Paige, *A class of simple Moufang loops*, Proc. Amer. Math. Soc., **7** (1956), 471–482.

[Par70] B. Pareigis, "Categories and Functors," Academic Press, New York-London, 1970.

[Pfl90] H.O. Pflugfelder, "Quasigroups and Loops: Introduction," Sigma Series in Pure Mathematics, **7**, Heldermann Verlag, Berlin, 1990.

[Phi94] J.D. Phillips, *Moufang loops and groups with biality*, Boll. Un. Mat. Ital. B **8** (1994), no. 3, 755–768.

[Phi99] J.D. Phillips, *Moufang loop multiplication groups with triality*, Rocky Mountain J. Math., **29** (1999), 1483–1490.

[Pic55] G. Pickert, "Projektive Ebenen," Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Bercksichtigung der Anwendungsgebiete, **LXXX**, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1955.

[Ree57] R. Ree, *On some simple groups defined by C. Chevalley*, Trans. Amer. Math. Soc. **84** (1957), 392–400.

[Rei29] K. Reidermeister, *Topologische Fragen der Differentialgeometrie. V. Gewebe und Gruppen*, Math. Z., **29** (1929), 427–435.

[Rob82] D.J.S. Robinson, "A Course in the Theory of Groups," Graduate Texts in Mathematics, **80**, Springer-Verlag, New York-Heidelberg-Berlin, 1982.

[Shu11] E.E. Shult, "Points and Lines. Characterizing the Classical Geometries," Universitext, Springer, Heidelberg, 2011.

[SpV00] T.A. Springer and F.D. Veldkamp, "Octonions, Jordan Algebras and Exceptional Groups," Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[SVo14] D. Stanovský and P. Vojtěchovský, *Commutator theory for loops*, J. Algebra, **399** (2014), 290–322.

[Stu12] E. Study, *Gruppen zweiseitiger Kollineationen*, Nachr. Ges. Wiss. Göttingen, (1912), 453–479.

[Stu13] E. Study, *Grundlagen und Ziele der analytischen Kinematik*, Sitzber. Berliner Math. Gesellschaft, **12** (1913), 36–60.

[Tay92] D.E. Taylor, "The Geometry of the Classical Groups," Sigma Series in Pure Mathematics, **9**, Heldermann Verlag, Berlin, 1992.

[Tho29] G. Thomsen, *Topologische Fragen der Differentialgeometrie XII, Schnittpunktssätze in ebenen Geweben*, Abh. Math. Semin. Univ. Hambg., **7** (1929), 99–106.

[Tit58] J. Tits, *Sur la trialité et les algèbres d'octaves*, Acad. Roy. Belg. Bull. Cl. Sci., **44** (1958), 332–350.

[Tit59] J. Tits, *Sur la trialité et certains groupes qui s'en déduisent*, Inst. Hautes Études Sci. Publ. Math., 1959.

[Tit81] J. Tits, *A local approach to buildings*, in: "The Geometric Vein: The Coxeter Festschrift," eds.: C. Davis, B. Grünbaum and F.A. Sherk, Springer-Verlag, New York-Berlin 1981, 519–547.

[VeY16] O. Veblen and J.W. Young, "Projective Geometry, Vol. 1" Ginn and Co., Boston, 1916.

[Vel85] F.D. Veldkamp, *In honor of Hans Freudenthal on his eightieth birthday*, Geom. Dedicata **19** (1985), 2–5.

[Ves96] A. Vesanen, *Solvable groups and loops*, J. Algebra, **180** (1996), 862–876.

[Wei23] A. Weinstein, *Fundamentalsatz der Tensorrechnung*, Math. Zeit., **16** (1923), 78–91.

[Zar85] F. Zara, "Classification des couples fischeriens," Thése, Amiens, 1985.

[Zor31] M. Zorn, *Theorie der alternativen Ringe*, Abh. Math. Sem. Hamburg Univ., **8** (1931), 123–147

Index