Some Classes of E-Minimal Algebras of Affine Type: Nilpotent Squags, p-Groups and Nilpotent SQS-Skeins

by

Andreas Guelzow

A thesis submitted to the FACULTY OF GRADUATE STUDIES of the UNIVERSITY OF MANITOBA in partial fulfillment of the requirements of the degree of

Doctor of Philosophy

ISBN 0-315-76773-1

SOME CLASSES OF E-MINIMAL ALGEBRAS OF AFFINE TYPE: NILPOTENT SQUAGS, p-GROUPS AND NILPOTENT SQS-SKEINS

BY

ANDREAS GUELZOW

A thesis submitted to the Faculty of Graduate Studies of the University of Manitoba in partial fulfillment of the requirements of the degree of

DOCTOR OF PHILOSOPHY

Abstract

Several classes of E-minimal algebras of affine type are investigated: finite nilpotent squags, finite nilpotent SQS-skeins and finite p-groups. (Squags arise from the co-ordinatization of Steiner triple systems and SQS-skeins from Steiner quadruple systems.) We present several representation and construction theorems for these algebras of the type given by Klossek for distributive squags. As a consequence of these theorems we are able to show that for every k larger than 1 there are infinitely many finite subdirectly irreducible (distributive) squags of nilpotence class k. Moreover we show that the variety of SQS-skeins is not locally finite by constructing a sequence of 4-generated nilpotent SQS-skeins of strictly increasing cardinality (and nilpotence class). We also investigate the variety of semi-boolean SQS-skeins, i.e. SQS-skeins satisfying the identity $q(x,u,q(y,u,z)) = q(q(x,u,y),u,z)$, and show that it contains the variety of boolean SQS-skeins as proper subvariety, thereby disputing the popular belief that above identity characterizes boolean SQS-skeins. Semi-boolean SQS-skeins can be described as those SQS-skeins that correspond to Steiner quadruple systems whose derived Steiner triple systems are all projective geometries.

Acknowledgements

This dissertation would have been impossible without the support of several people and organizations.

I would like to thank Prof. Dr. Heinrich Werner and Prof. Dr. Bernhard Ganter for awakening in me the interest in Universal Algebra and Combinatorics. As advisor to my Diplom-thesis, Heinrich Werner suggested to me to investigate distributive squags; this investigation has finally led to this thesis. I am also thankful to my current advisor Prof. Dr. Robert W. Quackenbush for discussing with me my ideas, for suggesting different approaches, for raising interesting and stimulating questions and for providing me with his experience.

I appreciate the financial support given to me by the Government of Canada through the World University Service of Canada, by the Faculty of Graduate Studies of the University of Manitoba, by the Department of Mathematics and Astronomy and by Prof. Dr. R. W. Quackenbush.

At last I would like to thank my wife Dona for her moral support, for believing in me, for the patience she showed while waiting for the completion of this dissertation, and for getting used to the peculiarities some mathematicians tend to exhibit, and my fellow graduate student† and close friend David Kaminski who, while he studied at this university, discussed with me my research and thereby allowed me to clarify and organize my thoughts, although he was working in a completely different mathematical field (asymptotical analysis).

---

† David is currently a professor in the Department of Mathematical Sciences at the University of Lethbridge.

Table of Contents

Table of Figures

1. Introduction

In the early nineteen hundred eighties P. P. Pálfy, P. Pudlák, R. McKenzie, D. Hobby and others investigated the structure of finite algebras with the use of tame congruence theory. Their results were collected and presented in (Hobby, McKenzie 1988). One of the classes of finite algebras considered is the class of E-minimal algebras: a finite algebra $\langle A;\Omega\rangle$ is called E-minimal if and only if $|A| > 1$ and every unary idempotent algebraic function on $\langle A;\Omega\rangle$ is either constant or the identity. It has been shown that there are exactly 5 types of E-minimal algebras, in fact every E-minimal algebra with at least 3 elements is either of affine or unary type. The exact definitions of these terms are presented in chapter 8 of this thesis. We will be exclusively concerned with E-minimal algebras of affine type, especially with the following three classes of examples: finite nilpotent squags, finite nilpotent SQS-skeins and finite p-groups.

Both squags and SQS-skeins arise from the co-ordinatization of Steiner Systems: the former are obtained from Steiner triple systems and the latter from Steiner quadruple systems. While SQS-skeins have not been extensively studied, the theory of nilpotent squags includes the theory of distributive squags. The latter are polynomially equivalent to exponent-3 commutative Moufang loops, which were thoroughly investigated by R. H. Bruck in (Bruck 1971). In (Klossek 1975) S. Klossek translated this theory into the language of distributive squags (kommutative Spiegelungsräume) and added several representation and construction theorems. We will first introduce the co-ordinatization of Steiner Systems in chapter 4 and then discuss nilpotent squags in chapter 5. We are able to generalize Klossek's representation theorem for any finite nilpotent squag and answer some of her open questions. For example, we are able to show that for every $n > 1$ there are infinitely many finite subdirectly irreducible squags of nilpotence class exactly n.

In chapter 6 we turn to the theory of SQS-skeins and are able to present representation and construction theorems that are analogous to the theorems for squags. Moreover, we will prove constructively, that the free SQS-skein with four generators is neither finite nor nilpotent. As for nilpotent squags we are also able to prove constructively that for every $n > 1$ there are infinitely many finite subdirectly irreducible SQS-skeins of nilpotence class exactly n. In (Mendelsohn 1975), (Quackenbush 1975) and (Lindner, Rosa 1978) it is claimed to be well known that the SQS-skeins satisfying the added equation $q(x,u,q(y,u,z)) = q(q(x,u,y),u,z)$ are exactly the SQS-skeins corresponding to the boolean groups. We will provide a counterexample to this 'folklore'. The class of SQS-skeins satisfying the above condition shall be called semi-boolean SQS-skeins; it can also be characterized as the class of all those SQS-skeins whose corresponding Steiner quadruple systems have only derived Steiner triple systems that are projective geometries over GF(2). The class of semi-boolean SQS-skeins appears to be quite analogous to the class of distributive squags among all nilpotent squags, but it has yet to be proven that every semi-boolean SQS-skein is even nilpotent.

Chapter 7 contains a short excursion into the theory of finite p-groups. Again we can give a representation theorem for these algebras that is similar to the theorems for squags and SQS-skeins. For p-groups of maximal class we are even able to improve our representation theorem. We have chosen to include this short discussion of p-groups in this thesis since it shows that some of the nice properties of finite nilpotent SQS-skeins and finite nilpotent squags cannot be generalized to all E-minimal algebras of affine type.

In chapter 8 finally, we will investigate generalizations of some of the theorems presented in earlier chapters into the theory of E-minimal algebras of affine type. While many of the proofs in the earlier chapters become superfluous once we have

verified these more general statements, we have retained them since they provide a clearer insight into the structure of the specific algebras than the more general ones.

In chapter 9 we conclude this thesis by discussing some of the questions that we were unable to answer and whose further investigation appears worthwhile.

2. Notation

In this paper we will mainly use the notations as introduced in (Grätzer 1979 [1968]). We assume that the reader is familiar with the concepts introduced in this book. Below we will review a few of the most important notations and introduce those that are different from (Grätzer 1979 [1968]).

An algebra $\mathbf{A}$ shall be written as $\mathbf{A} = \langle A;\Omega\rangle$, where A is the underlying non-empty set and Ω the set of (finitary) operations of $\mathbf{A}$. If Ω is indexed by the elements of I (i.e. $\Omega = \{F^i \mid i\in I\}$) or if $\Omega = \{F_1,F_2,\ldots,F_n\}$ is finite, we will also write $\langle A;F^i:i\in I\rangle$ or $\langle A;F_1,F_2,\ldots,F_n\rangle$ respectively. If $H \subseteq A$ then $[H]_{\mathbf{A}}$ denotes the set generated by H in the algebra $\mathbf{A}$, i.e. $\langle [H]_{\mathbf{A}};\Omega\rangle$ is the smallest subalgebra of $\mathbf{A}$ whose universe (the underlying set) contains H.

In universal algebra, some mathematicians use the expression '*polynomial*' interchangeable with '*term function*' while to others a '*polynomial*' is exactly an '*algebraic function*'. Contrary to the usage in (Grätzer 1979 [1968]), in this thesis '*algebraic function*' and '*polynomial*' shall be synonyms, i.e. polynomials are those functions that arise from term functions by substituting some variables with constants from A. The set of all term functions on $\mathbf{A}$ shall be denoted by $\mathrm{Clo}(\mathbf{A})$ and the set of all polynomials by $\mathrm{Pol}(\mathbf{A})$. $\mathrm{Clo}_n(\mathbf{A})$ and $\mathrm{Pol}_n(\mathbf{A})$ will represent the sets of all n-ary term functions and polynomials respectively.

The congruence lattice of the algebra $\mathbf{A}$ will be denoted by $\mathbb{C}(\mathbf{A})$. The largest and smallest elements in $\mathbb{C}(\mathbf{A})$ will be denoted by ι_A and ω_A respectively. If $X \subseteq A$ then $\Theta^{\mathbf{A}}(X)$ denotes the smallest congruence on $\mathbf{A} = \langle A;\Omega\rangle$ identifying all elements in X. If it is clear from the context which operations are considered we will also just write $\Theta^A(X)$ instead of $\Theta^{\mathbf{A}}(X)$. A *quotient* in $\mathbb{C}(\mathbf{A})$ or of $\mathbf{A}$ is any pair (α,β) of distinct elements in $\mathbb{C}(\mathbf{A})$ such that $\alpha < \beta$. If β even covers α then (α,β) is called a *prime*

quotient in $\mathbb{C}(\mathbb{A})$ or of $\mathbb{A}$. For any congruence $\alpha \in \mathbb{C}(\langle A;\Omega\rangle)$ and every $x \in A$ the expression $[x]\alpha$ denotes the set $\{y \in A \mid x\alpha y\}$.

δ_{ik} will denote the Kronecker symbol, i.e. $\delta_{ik}= 0$ if $i \neq k$ and $\delta_{ik} = 1$ if $i = k$. Moreover $\mathbb{Z}$ will denote the set of all integers and $\mathbb{N}$ the set of all non-negative integers (including 0). In some of the calculations in this thesis, it will be obvious that the values of certain expressions do not influence the final result. If these expressions are also complicated or lengthy, we will replace them by the symbol '?'.

3. Universal Algebraic Concepts

3.1. The Commutator

In 1976 Jonathan Smith's book on Mal'cev varieties was published. In this book Smith generalized the group theoretic concept of the commutator to the theory of Mal'cev varieties, i.e. varieties that have permutable congruences. With this concept he also generalized such notions as the 'centre' of an algebra, 'nilpotence' and 'centralizer'. A short time later Joachim Hagemann and Christian Herrmann extended the theory of the commutator to modular varieties. In (Gumm 1980) Heinz Peter Gumm presented an elegant introduction into the commutator theory, which is especially nice since it motivates the commutator geometrically. The definition in this paper will follow along the introduction in (Gumm 1980). A more complete introduction into commutator theory can be found in (Freese and McKenzie 1987). (A 1981 preprint of this book is known as *'the commutator, an overview'*.)

DEFINITION 3.1.1 Let $\mathfrak{V}$ be any congruence modular variety and let $\mathbf{A} \in \mathfrak{V}$. Let α and β be congruences on $\mathbf{A}$.
Then the congruence $\Theta^{\alpha}(\{((x,x),(y,y))\,|\,x\beta y\})$ is denoted by Δ_{α}^{β} and $[\alpha,\beta] = \{(b,c)\,|\,(b,b)\,\Delta_{\alpha}^{\beta}(b,c)\}$ is called the *commutator* of α and β.

THEOREM 3.1.2 *Let $\mathfrak{V}$ be any congruence modular variety and let $\mathbf{A} \in \mathfrak{V}$. Let α and β be congruences on $\mathbf{A}$. Properties of the congruence Δ_{α}^{β} are:*

(1) $(a,b)\,\Delta_{\alpha}^{\beta}(c,d) \Rightarrow (a\beta b \;\&\; c\alpha d \;\&\; d\beta b \;\&\; b\alpha a)$

(2) $(a,b)\,\Delta_{\alpha}^{\beta}(c,d) \Rightarrow (b,a)\,\Delta_{\alpha}^{\beta}(d,c)$

(3) $a\beta b \Rightarrow (a,a)\,\Delta_{\alpha}^{\beta}(b,b)$

THEOREM 3.1.4 *Let $\mathfrak{V}$ be any congruence modular variety and let $\mathbb{A} \in \mathfrak{V}$. Let α and β be congruences on $\mathbb{A}$. Properties of the commutator $[\alpha,\beta]$ are:*

(1) $[\alpha,\beta]$ *is a congruence on* $\mathbb{A}$.

(2) $[\alpha,\beta] \leq \alpha \cap \beta$

(3) $[\alpha,\beta] = \{(x,y) \mid (x,x)\ \Delta_{\alpha}^{\beta}\ (y,x)\}$

(4) $[\alpha,\beta] = \{(x,y) \mid \exists z\ ((z,x)\ \Delta_{\alpha}^{\beta}\ (z,y))\}$

(5) $[\alpha,\beta] = \{(x,y) \mid \exists z\ ((x,z)\ \Delta_{\alpha}^{\beta}\ (y,z))\}$

(6) $[\alpha,\beta] = \{(x,y) \mid \exists z\ ((z,z)\ \Delta_{\alpha}^{\beta}\ (x,y))\}$

(7) $[\alpha,\beta] = [\beta,\alpha]$

(8) $\gamma \leq \alpha \Rightarrow [\gamma,\beta] \leq [\alpha,\beta]$ *for all congruences* γ *on* $\mathbb{A}$.

THEOREM 3.1.5 *Let $\mathfrak{V}$ be any congruence modular variety and let $\mathbb{A},\mathbb{B} \in \mathfrak{V}$. Let α and β be congruences on $\mathbb{A}$ and let $\phi:\mathbb{A} \twoheadrightarrow \mathbb{B}$ be a surjective homomorphism. Then $\phi([\alpha,\beta]) \leq [\phi(\alpha),\phi(\beta)]$.*

The inequality in theorem 3.1.5 can be sharpened to an equality if the kernel of the homomorphism is known:

THEOREM 3.1.6 *Let $\mathfrak{V}$ be any congruence modular variety and let $\mathbb{A},\mathbb{B} \in \mathfrak{V}$. Let α and β be congruences on $\mathbb{A}$ and let $\phi:\mathbb{A} \twoheadrightarrow \mathbb{B}$ be a surjective homomorphism with kernel* $\ker\phi$. *Then:*

$$\phi([\alpha,\beta] \vee \ker\phi) = [\phi(\alpha \vee \ker\phi), \phi(\beta \vee \ker\phi)]$$

COROLLARY 3.1.7 *Let $\mathfrak{V}$ be any congruence modular variety and let $\mathbb{A},\mathbb{B} \in \mathfrak{V}$. Let α,β and γ be congruences on $\mathbb{A}$ such that $\gamma \subseteq \alpha \cap \beta$. Then:*

$$([\alpha,\beta] \vee \gamma)/\gamma = [\alpha/\gamma, \beta/\gamma]$$

THEOREM 3.1.8 *Let $\mathfrak{V}$ be any congruence modular variety and let $\mathbb{A},\mathbb{B} \in \mathfrak{V}$. Let α,β and γ be congruences on $\mathbb{A}$. Then $[\alpha,\beta] \leq \gamma$ if and only if $[\pi_\gamma(\alpha),\pi_\gamma(\beta)] = \omega_{\mathbb{A}/\gamma}$, where π_γ is the canonical homomorphism from $\mathbb{A}$ onto $\mathbb{A}/\gamma$.*

A very useful (and well known) syntactical description of the commutator is given by the *term condition*:

THEOREM 3.1.9 *Let $\mathfrak{V}$ be any congruence modular variety and let $\mathbb{A} \in \mathfrak{V}$. Let α and β be congruences on $\mathbb{A}$. Then $[\alpha,\beta]$ is the smallest congruence on $\mathbb{A}$ such that for all terms $\tau(x_0,x_1,\ldots,x_n)$, $(x,y) \in \beta$ and $(a_1,b_1),\ldots,(a_n,b_n) \in \alpha$ we have:*

$$\tau(x,a_1,\ldots,a_n)\ [\alpha,\beta]\ \tau(x,b_1,\ldots,b_n) \Rightarrow \tau(y,a_1,\ldots,a_n)\ [\alpha,\beta]\ \tau(y,b_1,\ldots,b_n)$$

The proofs of these theorems have been omitted since, with the exception of 3.1.6 and 3.1.7, they can be found in (Gumm 1980) or (Gumm 1983). A proof for theorem 3.1.6 is contained in (Freese and McKenzie 1987).

3.2. Nilpotence

In group theory non-commutative groups can be classified by "how far they are from being commutative (abelian)" using the notion of nilpotence. As mentioned above, Smith (1976), Gumm (1980), etc. have also generalized this group theoretic notion of nilpotence:

DEFINITION 3.2.1 Given an algebra $\langle S; \Omega \rangle$ in a congruence modular variety $\mathfrak{V}$ we define a sequence $\{\phi_i\}_{i=0,1,\ldots}$ of congruences on $\langle S; \Omega \rangle$ by:

$$\begin{aligned} \phi_0 &= \iota_S \\ \phi_{n+1} &= [\phi_n, \iota_S] \end{aligned}$$

This sequence is called the *lower central series* of $\langle S; \Omega \rangle$. If $\phi_k = \omega_S$ and $\phi_{k-1} \neq \omega_S$ then $\langle S; \Omega \rangle$ is said to be *nilpotent of class k*. The *universal algebraic centre* $\zeta(\langle S; \Omega \rangle)$ of $\langle S; \Omega \rangle$ is defined as the largest congruence ϕ on $\langle S; \Omega \rangle$ such that $[\phi, \iota_S] = \omega_S$.

Let $\mathfrak{V}_{(k)}$ denote the class of all algebras in $\mathfrak{V}$ that are nilpotent of class k or less, i.e. $\mathfrak{V}_{(1)} \subseteq \mathfrak{V}_{(2)} \subseteq \mathfrak{V}_{(3)} \subseteq \ldots \subseteq \mathfrak{V}$.

THEOREM 3.2.2 *Let $\mathfrak{V}$ be any congruence modular variety. Then all $\mathfrak{V}_{(k)}$ $(k \geq 1)$ are congruence permutable varieties.*

A proof of this theorem may be found in (Gumm 1980). An alternative definition of nilpotence can be given using the concept of the 'upper central series':

DEFINITION 3.2.3 Let $\mathfrak{V}$ be any congruence modular variety and $\langle S; \Omega \rangle \in \mathfrak{V}$. Then the series $\xi_0 \leq \xi_1 \leq \xi_2 \leq \ldots \leq \xi_n \leq \ldots$ of congruences on $\langle S; \Omega \rangle$ defined by:

a) $\xi_0 = \omega_S$ and

b) ξ_n is that congruence above ξ_{n-1} on $\langle S; \Omega \rangle$ such that

$$\xi_n / \xi_{n-1} = \zeta\left(\left\langle S / \xi_{n-1} ; \Omega \right\rangle\right)$$

is called the *upper central series* of $\langle S; \Omega \rangle$.

For Mal'cev varieties Smith (1976) has proven the following theorem. It can similarly be proven for modular varieties. (This theorem appears to be known, but the author was unable to find any reference to it.)

THEOREM 3.2.4 *Let $\mathfrak{V}$ be any congruence modular variety and let $\{\xi_i\}_{i=0,1,\ldots}$ be the upper central series of $\langle S; \Omega \rangle \in \mathfrak{V}$. Then $\langle S; \Omega \rangle$ is nilpotent of class k if and only if $\xi_k = \iota_S$ and $\xi_{k-1} \neq \iota_S$.*

In the proof of this theorem we require the following lemma:

LEMMA 3.2.5 *Let $\mathfrak{V}$ be any congruence modular variety and let $\{\xi_i\}_{i=0,1,\ldots}$ and $\{\phi_i\}_{i=0,1,\ldots}$ be the upper and lower central series of $\langle S;\Omega\rangle \in \mathfrak{V}$. If $\phi_j \le \xi_i$ then $\phi_{j+1} \le \xi_{i-1}$ and $\phi_{j-1} \le \xi_{i+1}$.*

Proof of Lemma 3.2.5: Let $\phi_j \le \xi_i$. By definitions 3.2.1 and 3.2.3 ξ_i is the largest congruence on $\langle S;\Omega\rangle$ such that $\omega_{S/\xi_{i-1}} = \left[\xi_i/\xi_{i-1}, \iota_S/\xi_{i-1}\right]$. By theorem 3.1.6 this implies:

$$\omega_{S/\xi_{i-1}} = \left[\xi_i/\xi_{i-1}, \iota_S/\xi_{i-1}\right] = \left(\left[\xi_i,\iota_S\right] \vee \xi_{i-1}\right)/\xi_{i-1}$$

Therefore $$\xi_{i-1} \ge \left[\xi_i,\iota_S\right] \ge \left[\phi_j,\iota_S\right] = \phi_{j+1}$$

and moreover $\left[\phi_{j-1}/\xi_i, \iota_S/\xi_i\right] = \left(\left[\phi_{j-1},\iota_S\right] \vee \xi_i\right)/\xi_i = \left(\phi_j \vee \xi_i\right)/\xi_i = \xi_i/\xi_i = \omega_{S/\xi_i}$.

Since ξ_{i+1} is defined as the largest congruence with the property $\left[\xi_{i+1}/\xi_i, \iota_S/\xi_i\right] = \omega_{S/\xi_i}$ we get: $\phi_{j-1} \le \xi_{i+1}$. □

Proof of Theorem 3.2.4: Let $\{\phi_i\}_{i=0,1,\ldots}$ be the lower central series of $\langle S;\Omega\rangle$. It is then sufficient to show that $\phi_i = \omega_S$ if and only if $\xi_i = \iota_S$ for all i.

Assume $\xi_i = \iota_S$. Clearly $\phi_0 \le \xi_i$. By repeated application of lemma 3.2.5 we get finally $\phi_i \le \xi_0 = \omega_S$. Therefore $\phi_i = \omega_S$. Vice versa, let us assume $\phi_i = \omega_S$. Then $\phi_i \le \xi_0$ and again by lemma 3.2.5 we get $\phi_0 \le \xi_i$. Since $\phi_0 = \iota_S$ this implies $\xi_i = \iota_S$. □

Since the upper central series of an algebra $\mathbf{S}$ has obviously one term more than the upper central series of $\mathbf{S}/\zeta(\mathbf{S})$ (provided $\mathbf{S}$ is not already of nilpotence class 1) theorem 3.2.4 yields a corollary that will become useful in section 3.4.:

COROLLARY 3.2.6 *Let $\mathfrak{V}$ be any congruence modular variety and let $\mathbb{S} = \langle S; \Omega \rangle \in \mathfrak{V}$ with $\mathbb{S} \neq \zeta(\mathbb{S})$. Then $\mathbb{S}$ is nilpotent of class k if and only if $\mathbb{S}/\zeta(\mathbb{S})$ is nilpotent of class k–1.*

As a simple consequence of theorem 3.2.4 and lemma 3.2.5 we can get the following two corollaries that describe the relationship between the upper and the lower central series of a nilpotent algebra in a congruence modular variety. Figure 1 shows this relationship in the congruence lattice of such an algebra of nilpotence class 4.

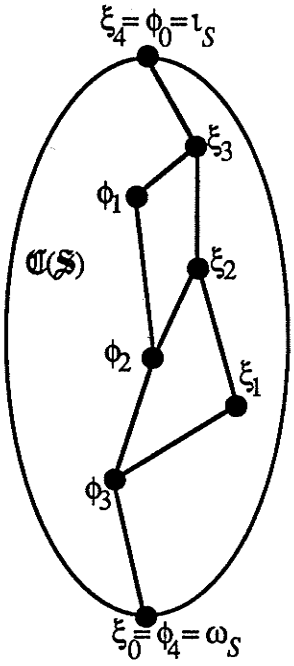


Figure 1
Upper and lower central series of an algebra of nilpotence class 4.

COROLLARY 3.2.7 *Let $\mathfrak{V}$ be any congruence modular variety and let $\mathbb{S} = \langle S; \Omega \rangle \in \mathfrak{V}$ be nilpotent of class k. Let $\{\xi_i\}_{i=0,1,\ldots}$ and $\{\phi_i\}_{i=0,1,\ldots}$ be the upper and lower central series of $\mathbb{S}$. Then $\phi_i \leq \xi_{k-i}$ for all i=0,1,…,k.*

COROLLARY 3.2.8 *Let $\mathfrak{V}$ be any congruence modular variety and let $\mathbb{S} = \langle S; \Omega \rangle \in \mathfrak{V}$ be nilpotent of class $k > 0$. Let $\{\xi_i\}_{i=0,1,\ldots}$ and $\{\phi_i\}_{i=0,1,\ldots}$ be the upper and lower central series of $\mathbb{S}$. Then $\phi_i \not\leq \xi_{k-i-1}$ for all i=0,1,…,k–1.*

Proof of Corollary 3.2.7: By theorem 3.2.4 $\xi_k = \iota_S = \phi_0$, i.e. $\xi_k \geq \phi_0$. The statement of the corollary follows by repeated application of lemma 3.2.5. □

Proof of Corollary 3.2.8: Suppose $\xi_{k-i-1} \geq \phi_0$. By repeated application of lemma 3.2.5 we get $\xi_{k-1} \geq \phi_i = \iota_S$. This contradicts theorem 3.2.4 since $\mathbb{S}$ is of nilpotence class k. □

Note that it is not possible to improve these corollaries since it is possible to construct nilpotent algebras in a modular variety such that each of the following conditions holds for some i in at least one of these algebras:

$$\xi_{k-i-1} < \phi_i,$$
$$\xi_{k-i-1} \vee \phi_i = \xi_{k-i} \text{ with } \phi_i \neq \xi_{k-i}, \text{ and}$$
$$\phi_i = \xi_{k-i}.$$

When determining whether certain nilpotent algebras are subdirectly irreducible we will require the following lemma and its corollary:

LEMMA 3.2.9 *Let $\mathbb{V}$ be any congruence modular variety and let $\mathbb{S} = \langle S; \Omega \rangle \in \mathbb{V}$ be nilpotent. Let $\alpha \in \mathbb{C}(\mathbb{S})$. Then*

$$\alpha \neq \omega_S \Leftrightarrow \alpha \cap \zeta(\mathbb{S}) \neq \omega_S .$$

COROLLARY 3.2.10 *Let $\mathbb{V}$ be any congruence modular variety and let $\mathbb{S} = \langle S; \Omega \rangle \in \mathbb{V}$ be nilpotent. Then $\mathbb{S}$ is subdirectly irreducible if and only if for all $C \subseteq \{\alpha \in \mathbb{C}(\mathbb{S}) \mid \alpha \leq \zeta(\mathbb{S})\}$:*

$$\bigcap C = \omega_S \Rightarrow \exists \alpha \in C \text{ such that } \alpha = \omega_S .$$

Lemma 3.2.9 is an exercise in (Freese, McKenzie 1987). We will therefore omit the proof.

Proof of Corollary 3.2.10: Since an algebra $\mathbb{S} = \langle S; \Omega \rangle$ is called subdirectly irreducible if for all $C \subseteq \mathbb{C}(\mathbb{S})$ the implication $(\bigcap C = \omega_S \Rightarrow \exists \alpha \in C$ such that $\alpha = \omega_S)$ holds, corollary 3.2.10 is an obvious consequence of lemma 3.2.9.

By corollary 3.2.10, a description of the centre of a given algebra is useful in determining whether that algebra is subdirectly irreducible. The next theorem will yield such a description. Before we are able to present it, we have to recall the definition of a Gumm difference term:

DEFINITION 3.2.11 Let $\mathfrak{V}$ be any variety. A ternary term $d(x,y,z)$ is called a *Gumm difference term* if it satisfies the following two conditions:

(a) $d(x,y,z) = y$ is an identity in $\mathfrak{V}$.

(b) If $(x,y) \in \theta \in \mathfrak{C}(\mathbb{A})$ for some $\mathbb{A} \in \mathfrak{V}$, then $d(x,y,y)\ [\theta,\theta]\ x$.

It is well known that every modular variety has a Gumm difference term. Note that in a permutable variety the Mal'cev term is a Gumm difference term.

THEOREM 3.2.12 *Let $\mathfrak{V}$ be a modular variety and $\langle A,\Omega\rangle = \mathbb{A} \in \mathfrak{V}$. Let $d(x,y,z)$ be a Gumm difference term. Then $a\ \zeta(\mathbb{A})\ b$ if and only if*

(1) $$f(d(r_1(a,b),r_1(b,b),c_1),\ldots,d(r_n(a,b),r_n(b,b),c_n)) = d(f(r_1(a,b),\ldots,r_n(a,b)),f(r_1(b,b),\ldots,r_n(b,b)),f(\mathbf{c}))$$

and

(2) $$d(r(a,b),r(b,b),r(b,b)) = r(a,b)$$

for all $f \in \Omega$, all $\mathbf{c} = (c_1,\ldots,c_n) \in A^n$ (n being the arity of f) and all binary term functions $r(x,y),r_1(x,y),\ldots,r_n(x,y)$.

A proof of theorem 3.2.12 can be found in (Freese, McKenzie 1987). As mentioned above, in every permutable variety the Mal'cev polynomial is a Gumm difference term. Since it always satisfies 3.2.12 (2), we get:

COROLLARY 3.2.13 *Let $\mathfrak{V}$ be a permutable variety with Mal'cev term $p(x,y,z)$ and let $\langle A,\Omega\rangle = \mathbb{A} \in \mathfrak{V}$. Then $a\ \zeta(\mathbb{A})\ b$ if and only if*

$$f(p(r_1(a,b),r_1(b,b),c_1),\ldots,p(r_n(a,b),r_n(b,b),c_n)) =$$
$$p(f(r_1(a,b),\ldots,r_n(a,b)),f(r_1(b,b),\ldots,r_n(b,b)),f(c))$$

for all $f \in \Omega$, *all* $\mathbf{c} = (c_1,\ldots,c_n) \in A^n$ (*n being the arity of f*) *and all binary term functions* $r_1(x,y),\ldots,r_n(x,y)$.

3.3. The Vaughan-Lee Description of the Commutator

At the Fourth International Conference on Universal Algebra and Lattice Theory at Puebla, Mexico in 1982 M. R. Vaughan-Lee presented a paper on nilpotence in permutable varieties (Vaughan-Lee 1983). In this paper Vaughan-Lee introduces a new description of the commutator for varieties of unital algebras with permutable weakly regular congruences.

The results as presented in (Vaughan-Lee 1983) are valid for a variety $\mathfrak{V}$ satisfying the following conditions:

(1) $\mathfrak{V}$ is a variety of Ω-algebras where Ω is a finite set of finitary operations containing a single nullary operation 0.

(2) $\mathfrak{V}$ is congruence permutable.

(3) $\mathfrak{V}$ is weakly congruence regular, i.e. for every $\langle A; \Omega\rangle$ in $\mathfrak{V}$ every congruence of $\langle A; \Omega\rangle$ is uniquely determined by its 0 class.

(4) Every algebra $\langle A; \Omega\rangle$ is unital, i.e. $\{0\}$ is a subalgebra of $\langle A; \Omega\rangle$. (This is equivalent to the requirement that $f(0,0,\ldots,0) = 0$ is a law in $\mathfrak{V}$ for all $f \in \Omega$.)

Examples of varieties satisfying above conditions are: the variety of groups $\langle G; +,-,0\rangle$ and the variety of pointed squags $\langle S; \bullet, e\rangle$.

In group theory the 0-class of the universal algebraic commutator can be described by the values of the group theoretic commutator term $-x-y+x+y$. For varieties satisfying the above conditions (1) to (4) this notion can be generalized as follows:

DEFINITION 3.3.1A Let $\mathfrak{V}$ be a variety satisfying above conditions (1) to (4). A term $\tau(x_0,x_1,\ldots,x_{n-1})$ is called a *commutator term* in $\mathfrak{V}$ if for each $i \in \{0,1,\ldots,n-1\}$:

$$0 \quad = \quad \tau(x_0,x_1,\ldots,x_{i-1},0,x_{i+1},\ldots,x_{n-1})$$

is a law in $\mathfrak{V}$. The commutator term $\tau(x_0,x_1,\ldots,x_{n-1})$ is said to involve n variables.

(Vaughan-Lee, 1983) mentions that the same results can also be proven without the requirements that the algebras in $\mathfrak{V}$ have an equationally defined constant. The proofs of the generalized theorems are presented in (Freese and McKenzie 1987, ch. 14). In this case the concept of a commutator or commutator term has to be defined as follows:

DEFINITION 3.3.1B Let $\mathfrak{V}$ be a congruence permutable variety. A term $\tau(x_0,x_1,\ldots,x_{n-1},z)$ is called a *commutator term* in $\mathfrak{V}$ if for each $i \in \{0,1,\ldots,n-1\}$

$$z \quad = \quad \tau(x_0,x_1,\ldots,x_{i-1},z,x_{i+1},\ldots,x_{n-1},z)$$

is a law in $\mathfrak{V}$.

We will present some of the results from (Vaughan-Lee 1983) in the setting of (Freese and McKenzie 1987). We will omit the proofs that can be found in (Freese and McKenzie 1987). An important tool is the following generalization of a lemma well known in group theory:

LEMMA 3.3.2 (HIGMAN'S LEMMA) *Let $\mathfrak{V}$ be a congruence permutable and nilpotent variety, i.e. a variety such that every algebra $\mathbb{A} = \langle A,\Omega\rangle$ in $\mathfrak{V}$ is nilpotent. Let $\mathbb{F} = \langle F,\Omega\rangle$ be the free algebra in $\mathfrak{V}$ with generators $z,x_0,x_1,\ldots$ and for every set $S \subseteq \mathbb{N}$ let $\delta_S:\mathbb{F}\to\mathbb{F}$ be the endomorphism defined by:*

$$\delta_S(x_i) = \begin{cases} x_i & \text{if } i \notin S \\ z & \text{if } i \in S \end{cases} \quad \text{and } \delta_S(z) = z$$

Let $\tau(x_0,x_1,\ldots,x_n)$ and $\sigma(x_0,x_1,\ldots,x_m)$ be arbitrary terms in $\mathfrak{V}$. Then there is a finite set C of commutator terms such that for all $S \subseteq \mathbb{N}$:

(1) the identity $\delta_S(\tau) \approx \delta_S(\sigma)$ together with the identities of $\mathfrak{V}$ implies the law: $\delta_S(\omega(x_0,x_1,\ldots,x_k,z)) \approx z$ for all $\omega \in C$, and

(2) the pair $\left(\delta_S(\tau),\delta_S(\sigma)\right)$ is contained in the congruence generated by $\left\{\left(\delta_S\left(\omega\left(x_0,x_1,\ldots,x_k,z\right)\right),z\right) \middle| \ \omega \in C\right\}$ in the free algebra $\mathfrak{F} = \langle F,\Omega\rangle$ in $\mathfrak{V}$ with generators $z, x_0, x_1,\ldots$.

Higmann's Lemma in (Freese and McKenzie 1987) is formulated only for $S = \varnothing$, but the proof itself shows above formulation, which is essentially the same as in (Vaughan-Lee 1983). Using Higmann's Lemma in this stronger formulation we can show that definition 3.3.1 is appropriate, i.e. these commutator terms describe the universal algebraic commutator:

THEOREM 3.3.3 *Let $\mathfrak{V}$ be a congruence permutable and nilpotent variety. Let $\mathfrak{A} = \langle A; \Omega\rangle$ be an algebra in $\mathfrak{V}$. Let ϕ and ψ be congruences on $\mathfrak{A}$. Then* $[\phi,\psi] =$

$$\Theta^{\mathfrak{A}}\left(\left\{\left(z,\tau(x_0,x_1,\ldots,x_{n-1},z)\right) \middle| \ \tau \in \mathbb{K}(\mathfrak{V}) \ \&\ x_0\phi z \ \&\ x_1\psi z \ \&\ x_0,x_1,\ldots,x_{n-1},z \in A\right\}\right)$$

where $\mathbb{K}(\mathfrak{V})$ denotes the set of all commutator terms of $\mathfrak{V}$ involving at least the three variables x_0 , x_1 and z.

To prove this theorem we require a lemma from (Freese and McKenzie 1987):

LEMMA 3.3.4 *Let $\mathfrak{A} = \langle A; \Omega\rangle$ be a nilpotent algebra of class k in a congruence permutable variety $\mathfrak{V}$ with lower central series $\{\phi_i\}_{i=0,1,\ldots}$. Let $p(x,y,z)$ be the Mal'cev polynomial for this variety and let $f_n(x,y,z)$ be a term defined recursively by:*

$$f_0(x,y,z) = y \qquad \textit{and}$$
$$f_{n+1}(x,y,z) = p\Big(y,p\Big(y,x,p\Big(f_n(x,y,z),y,z\Big)\Big),f_n(x,y,z)\Big)$$

Then for all n and all x,y,b,c ∈ A we have:

(1) $f_n(p(x,b,c),b,c) \;\phi_n\; x$ *and*

(2) $p(f_n(y,b,c),b,c) \;\phi_n\; y$

and therefore

(3) $f_k(p(x,b,c),b,c) = x$ *and*

(4) $p(f_k(y,b,c),b,c) = y$

Proof of theorem 3.3.3 This proof follows closely along the line of the corresponding proof in (Vaughan-Lee 1983). We will abbreviate:

$$\Theta = \Theta^{\mathfrak{A}}\Big(\Big\{\big(z,\tau(x_0,x_1,\ldots,x_{n-1},z)\big)\Big\| \ \tau\in\mathfrak{T}(\mathfrak{V}) \ \&\ x_0\phi z \ \&\ x_1\psi z \ \&\ x_0,x_1,\ldots,x_{n-1},z\in A)\Big\}\Big)$$

First we will show that $\Theta \le [\phi,\psi]$, i.e. $z\ [\phi,\psi]\ \tau(x_0,x_1,\ldots,x_{n-1},z)$ for all $\tau \in \mathfrak{T}(\mathfrak{V})$ & $x_0\phi z$ & $x_1\psi z$.

Obviously $\tau(z,z,x_2\ldots,x_{n-1},z) = z\ [\phi,\psi]\ z = \tau(z,x_1,\ldots,x_{n-1},z)$. Since $(z,x_0) \in \phi$ and $(z,x_1), (x_2,x_2),\ldots, (x_n,x_n) \in \psi$ we may conclude by theorem 3.1.9 :

$$z = \tau(x_0,z,\ldots,x_{n-1},z) \quad [\phi,\psi] \quad \tau(x_0,x_1,\ldots,x_{n-1},z)$$
$$\text{i.e. } \Theta \le [\phi,\psi].$$

Now suppose $\tau(x_0,x_1,\ldots,x_n)$ is any term, $(c,d) \in \psi$ and $(a_1,b_1),\ldots,(a_n,b_n) \in \phi$ such that $\tau(c,a_1,\ldots,a_n)\ \Theta\ \tau(c,b_1,\ldots,b_n)$. We will show that $\tau(d,a_1,\ldots,a_n)\ \Theta\ \tau(d,b_1,\ldots,b_n)$ since this implies $\Theta \ge [\phi,\psi]$.

Since $\mathfrak{A}$ is in a nilpotent variety it is nilpotent of class k for some positive integer k. Let $p(x_0,x_1,x_2)$ be the Mal'cev polynomial in $\mathfrak{V}$ and $f_k(x_0,x_1,x_2)$ the polynomial defined in lemma 3.3.4.

Then $f_k(z,c,z) = c$ since $z = p(c,c,z)$ and

$f_k(\mu,c,z) = d$ with $\mu = p(d,c,z)$.

Note that $\mu = p(d,c,z)\ \psi\ p(c,c,z) = z.$

Similarly we get for all $i = 1,2,\ldots$:

$$f_k(z,a_i,z) = a_i \quad \text{since} \quad z = p(a_i,a_i,z) \quad \text{and}$$

$$f_k(\nu_i,a_i,z) = b_i \quad \text{with} \quad \nu_i = p(b_i,a_i,z) \quad \text{and}$$

$$\nu_i = p(n_i,a_i,z)\ \phi\ p(a_i,a_i,z) = z.$$

Now define with $\mathbf{s} = (s_1,\ldots,s_n)$ and $\mathbf{t} = (t_1,\ldots,t_n)$ the term function κ:

$$\kappa(r,\mathbf{s},\mathbf{t},t_{n+1},t_{n+2}) = \tau\left(f_k(r,t_{n+1},t_{n+2}),f_k(s_1,t_1,t_{n+2}),\ldots f_k(s_n,t_n,t_{n+2})\right)$$

Then

$$\tau(c,a_1,\ldots,a_n) = \kappa(z,\mathbf{z},\mathbf{a},c,z)$$

$$\tau(c,b_1,\ldots,b_n) = \kappa(z,\nu,\mathbf{a},c,z)$$

$$\tau(d,a_1,\ldots,a_n) = \kappa(\mu,\mathbf{z},\mathbf{a},c,z)$$

$$\tau(d,b_1,\ldots,b_n) = \kappa(\mu,\nu,\mathbf{a},c,z)$$

where $\nu = (\nu_1,\ldots,\nu_n)$, $\mathbf{a} = (a_1,\ldots,a_n)$ and $\mathbf{z} = (z,\ldots,z)$ with:

$\mu\ \psi\ z$ and $\nu\ \phi\ \mathbf{z}$ componentwise.

Consider the two terms $\kappa(x_0,(x_1,\ldots,x_n),(x_{n+1},\ldots,x_{n+n}),x_{2n+1},z)$ and $\lambda(x_0,\ldots,x_{2n+1},z) =$

$p(\kappa(z,\mathbf{z},(x_{n+1},\ldots,x_{n+n}),x_{2n+1},z),\ \kappa(z,(x_1,\ldots,x_n),(x_{n+1},\ldots,x_{n+n}),x_{2n+1},z),$

$\kappa(x_0,\mathbf{z},(x_{n+1},\ldots,x_{n+n}),x_{2n+1},z)).$

By Higmann's Lemma (Theorem 3.3.2), there exists a finite set C of commutator terms such that in the free algebra in $\mathfrak{V}$ with generators $z,x_0,x_1,\ldots$ the pair $\left(\lambda(x_0,\ldots,x_{2n+1},z),\kappa(x_0,(x_1,\ldots,x_n),(x_{n+1},\ldots,x_{2n}),x_{2n+1},z)\right)$ is contained in the congruence generated by $\left\{\left(\delta_S(\omega(x_0,x_1,\ldots,x_k,z)),z\right)\middle|\ \omega\in C\right\}$. Since $\mu\ \psi\ z$ and $\nu_1\ \phi\ z$ and since

$$\Theta = \Theta^{\mathbf{A}}\left(\left\{\left(z,\tau(x_0,x_1,\ldots,x_{n-1},z)\right)\middle|\ \tau\in\mathbb{K}(\mathfrak{V})\ \&\ x_0\psi z\ \&\ x_1\phi z\ \&\ x_0,x_1,\ldots,x_{n-1},z\in A)\right\}\right)$$

we know therefore that in $\mathbf{A}$: $\lambda(\mu,\nu,\ldots,\nu,a_1,\ldots,a_n,c,z)\ \Theta\ \kappa(\mu,\nu,\mathbf{a},c,z)$, i.e.:

$$p(\kappa(z,\mathbf{z},\mathbf{a},c,z),\kappa(z,\nu,\mathbf{a},c,z),\kappa(\mu,\mathbf{z},\mathbf{a},c,z))\ \Theta\ \kappa(\mu,\nu,\mathbf{a},c,z)$$

therefore $p(\tau(c,a_1,\ldots,a_n),\tau(c,b_1,\ldots,b_n),\tau(d,a_1,\ldots,a_n))\ \Theta\ \tau(d,b_1,\ldots,b_n)$.

Since we have assumed that $\tau(c,a_1,\ldots,a_n)\ \Theta\ \tau(c,b_1,\ldots,b_n)$ we get immediately:

$$\tau(d,a_1,\ldots,a_n)\ \Theta\ \tau(d,b_1,\ldots,b_n)$$

and therefore $\Theta \geq [\phi,\psi]$. We have shown that $\Theta = [\phi,\psi]$. □

While (Vaughan-Lee 1983) and (Freese and McKenzie 1987) use this description of the commutator to show that certain algebras are finitely based we will use it in a different context.

3.4. Representing Nilpotent Algebras

In (Freese and McKenzie 1987) a description of the structure of an algebra over its centre is given. By induction, this will allow us to describe the basic structure of any nilpotent algebra in a modular variety, especially in those varieties in which the structure of the algebras of nilpotence class 1 is well known. To present this description we have first to discuss the concept of an associated group:

DEFINITION 3.4.1 Let $\mathfrak{V}$ be a modular variety and let $\mathbb{A} \in \mathfrak{V}$. $\mathbb{A} = \langle A;\Omega\rangle$ is called *abelian* if and only if $[\iota_A,\iota_A] = \omega_A$, i.e. if and only if $\mathbb{A}$ is nilpotent of class 1.

DEFINITION 3.4.2 Let $\mathbb{A} = \langle A;\Omega\rangle$ be any algebra (not necessarily in a modular variety). $\mathbb{A}$ is called *affine* if and only if there exists an abelian group $\langle A;+,-\rangle = \mathbb{A}'$ and a ternary term function $\tau(x,y,z)$ of $\mathbb{A}$ such that

(1) $\tau(x,y,z) = x - y + z$ for all $x,y,z \in A$ and

(2) $\{(x,y,z,u) \mid x + y = z + u\}$ is a subalgebra of $\mathbb{A}^4$.

If this abelian group exists it is called the *group associated with* $\mathbb{A}$ and the term function τ is called a *difference function for* $\mathbb{A}$.

In a modular variety these two concepts coincide. This has been proven first by Christian Herrmann in (Herrmann 1979). Proofs of this difficult theorem can also be found in (Taylor 1982) and (Gumm 1980):

THEOREM 3.4.3 *In a modular variety, every abelian algebra is affine, and conversely .*

The next definition yields the construction used in (Freese and McKenzie 1987) to describe an algebra over its centre:

DEFINITION 3.4.4 Let $\mathfrak{Q} = \langle Q; F^i : i \in I \rangle$ and $\mathfrak{B} = \langle B; F^i : i \in I \rangle$ be algebras in the modular variety $\mathfrak{V}$. Let $\mathfrak{Q}$ be abelian with associated group $\langle Q; +, -, 0 \rangle$. Suppose for each $i \in I$ we are given a map $T_i : B^{n(i)} \to Q$ where $n(i)$ is the arity of F^i. Let $\mathbf{T}$ denote the system of such maps $(T_i : i \in I)$. Then $\mathfrak{A} = \mathfrak{B} \otimes^{\mathbf{T}} \mathfrak{Q}$ is defined to be the algebra $\langle B \times Q ; F^i : i \in I \rangle$ with:

$$F^i((b_1,q_1),\ldots,(b_n,q_n)) = (F^i(b_1,\ldots,b_n), F^i(q_1,\ldots,q_n) + T_i(b_1,\ldots,b_n))$$

where $b_k \in B$, $q_k \in Q$ for all k and each F^i is evaluated in the appropriate algebra.

In (Freese and McKenzie 1987) B and Q are exchanged. The author of this paper has chosen to use this version to be consistent with certain representation theorems presented in (Klossek 1975) which will be discussed below. Obviously, the algebra defined in 3.4.4 need not belong to the variety $\mathfrak{V}$. But in (Freese and McKenzie 1987) this construction has been used to describe the structure of the non-abelian algebras in a congruence modular variety $\mathfrak{V}$:

THEOREM 3.4.5 *Let $\mathfrak{A} \in \mathfrak{V}$, where $\mathfrak{V}$ is a congruence modular variety. Let $\mathfrak{B} = \mathfrak{A}/\zeta(\mathfrak{A})$. Then there exists an abelian algebra $\mathfrak{Q} \in \mathfrak{V}$ and a system $\mathbf{T}$ of maps as described above such that $\mathfrak{A} \cong \mathfrak{B} \otimes^{\mathbf{T}} \mathfrak{Q}$ and the centre of $\mathfrak{B} \otimes^{\mathbf{T}} \mathfrak{Q}$ is the kernel of the projection onto $\mathfrak{B}$.*

It is clear that the projection onto $\mathfrak{B}$ is always a homomorphism. A relatively simple corollary to this theorem is:

COROLLARY 3.4.6 *An algebra in a congruence modular variety is nilpotent of class 2 or less if and only if it can be represented as (i.e. is isomorphic to)* $\mathbb{Q}_1 \otimes^{\mathbf{T}} \mathbb{Q}_2$ *where* $\mathbb{Q}_1$ *and* $\mathbb{Q}_2$ *are abelian algebras in* $\mathfrak{V}$.

By induction over the class of nilpotence (using corollary 3.2.6), one implication of this corollary can easily be extended. The proof of the second implication of Corollary 3.4.6 seems to require the knowledge that $\mathbb{Q}_1$ is also abelian. We can therefore write:

COROLLARY 3.4.7 *If an algebra* $\mathbb{A} = \langle A; F^i : i \in I \rangle$ *in a congruence modular variety is nilpotent of class n then it is isomorphic to:*

$$\left(\left(\cdots\left(\left(\mathbb{Q}_1 \otimes^{\mathbf{T}^1} \mathbb{Q}_2\right) \otimes^{\mathbf{T}^2} \mathbb{Q}_3\right)\cdots\right) \otimes^{\mathbf{T}^{n-1}} \mathbb{Q}_n\right)$$

where $\mathbb{Q}_1, \mathbb{Q}_2, \ldots, \mathbb{Q}_n$ *are abelian algebras in* $\mathfrak{V}$ *and* $\mathbf{T}^1, \mathbf{T}^2, \ldots, \mathbf{T}^{n-1}$ *are some appropriate systems of maps as described in 3.4.4. Moreover, if* $\omega_A = \xi_0 \le \xi_1 \le \xi_2 \le \ldots \le \xi_n = \iota_A$ *is the upper central series of* $\mathbb{A}$ *then for any* $k \in \{0, \ldots, n\}$ ξ_{n-k} *corresponds to the kernel of the projection onto* $\left(\left(\cdots\left(\left(\mathbb{Q}_1 \otimes^{\mathbf{T}^1} \mathbb{Q}_2\right) \otimes^{\mathbf{T}^2} \mathbb{Q}_3\right)\cdots\right) \otimes^{\mathbf{T}^{k-1}} \mathbb{Q}_k\right)$.

We will see in a later chapter that although this representation doesn't appear to provide much information on the structure of an arbitrary nilpotent algebra in a congruence modular variety, for certain varieties it yields valuable information, especially if the structure of the abelian algebras is easy to describe — as for groups, squags and SQS-skeins.

It is easy to see that the algebra $\left(\left(\cdots\left(\left(\mathbb{Q}_1 \otimes^{\mathbf{T}^1} \mathbb{Q}_2\right) \otimes^{\mathbf{T}^2} \mathbb{Q}_3\right)\cdots\right) \otimes^{\mathbf{T}^{n-1}} \mathbb{Q}_n\right)$ can also be given as $\left\langle \prod_{k=1}^{n} Q_k; F^i : i \in I \right\rangle$ with

$$F^i((q_{1,1},q_{1,2},\ldots,q_{1,n}),\ldots,(q_{m,1},q_{m,2},\ldots,q_{m,n})) =$$

$$\begin{pmatrix} F_1^i(q_{1,1},\ldots,q_{m,1}), \\ F_2^i(q_{1,2},\ldots,q_{m,2}) + T_i^1(q_{1,1},\ldots,q_{m,1}), \\ F_3^i(q_{1,3},\ldots,q_{m,3}) + T_i^2((q_{1,1},q_{1,2}),\ldots,(q_{m,1},q_{m,2})), \\ \vdots \qquad\qquad\qquad \vdots \\ F_n^i(q_{1,n},\ldots,q_{m,n}) + T_i^{n-1}((q_{1,1},\ldots,q_{1,n-1}),\ldots,(q_{m,1},\ldots,q_{m,n-1})) \end{pmatrix}$$

if F^i is m-ary and F_k^i is F^i evaluated in $\mathfrak{Q}_k = \langle Q_k ; F^i : i \in I \rangle$.

4. Co-ordinatizations of Steiner Systems

Two of the main examples in this paper are the classes of nilpotent squags and nilpotent SQS-skeins. Since squags and SQS-skeins arise from the co-ordinatization of certain Steiner systems a short review of this topic shall be given. A good survey of different algebras corresponding to Steiner systems can be found in (Ganter and Werner 1980).

A Steiner system of type (t,k) is a pair (P,B) of finite sets, where B is a set of k element subsets of P such that every t-element subset of P is contained in exactly one element of B. While the elements of P are usually called points, the elements of B are called blocks (or lines). A Steiner system of type (2,3) is also called a Steiner triple system (STS) and a Steiner system of type (3,4) is called a Steiner quadruple system (SQS).

Steiner triple systems can be represented using one of three types of algebras: near boolean algebras, sloops or squags. The first method of co-ordinatizing is due to R. W. Quackenbush, the remaining two to R. H. Bruck. Steiner quadruple systems are usually represented by SQS-skeins. This concept is due to T. Evans.

4.1. Near Boolean Algebras

Let (P,B) be a Steiner triple system. Let P' be a set disjoint from P such that $|P| = |P'|$. Let 0 and 1 be two symbols neither in P nor in P'. Let $': P \to P'$ be a bijection and $Q = P \cup P' \cup \{0,1\}$. On Q let us define two binary operations $\wedge$ and $\vee$ in such a way that for every block b in B the algebra $\langle b \cup b' \cup \{0,1\}; \wedge,\vee,',0,1\rangle$ is a boolean algebra where $b' = \{x' \mid x \in b\}$. Note that this is possible since each pair of elements $x,y \in P, x \neq y$ is in exactly one block $b \in B$. It is clear that the algebra $\langle Q; \wedge,\vee,',0,1\rangle$ is

a near boolean algebra, i.e. an algebra satisfying all equations in two variables that are satisfied in all boolean algebras.

Vice versa, let $\langle Q; \wedge,\vee,',0,1\rangle$ be a finite near boolean algebra and $P \subset Q\backslash\{0,1\}$ such that $P \cup P' = Q\backslash\{0,1\}$ and $P \cap P' = \varnothing$ where $P' = \{p' \mid p \in P\}$. If $x,y \in P, x \neq y$ then $\langle\{x,y\}\rangle$ denotes the subalgebra of $\langle Q; \wedge,\vee,',0,1\rangle$ generated by x and y. $\langle\{x,y\}\rangle$ is a boolean algebra, therefore $\langle\{x,y\}\rangle \cap P\backslash\{x,y\}$ contains either exactly one element (that we will call z) or a unique element z that is the join of two atoms of $\langle\{x,y\}\rangle$. Then let B be defined as: $B = \{\{x,y,z\} \mid x,y \in P, x \neq y, z$ chosen as described above$\}$. It can be shown that (P,B) is a Steiner triple system.

4.2. Sloops

Steiner triple systems can also be co-ordinatized by sloops. A sloop (or Steiner loop) is a commutative loop satisfying the equation $x \bullet (x \bullet y) = y$. Let (P,B) be again a Steiner triple system. Let e be a symbol not contained in P. Let $S = P \cup \{e\}$. The binary operation $\bullet$ be defined on S by:

$$x \bullet x = e, \qquad e \bullet e = e$$

$$x \bullet e = x = e \bullet x$$

$$x \bullet y = \text{the third point on the block through } x \text{ and } y$$

for all $x,y \in P, x \neq y$. It is easy to see that the resulting algebra $\langle S; \bullet, e\rangle$ is a sloop.

Conversely, given a sloop $\langle S; \bullet, e\rangle$ we can define:

$$P = S\backslash\{e\} \qquad \text{and}$$

$$B = \left\{\{x,y,x\bullet y\} \middle| x,y \in S\backslash\{e\}, x \neq y\right\}$$

Then (P,B) is a Steiner triple system.

4.3. Squags

In this thesis we will be mainly interested in the co-ordinatization of Steiner triple systems by squags. Given a Steiner triple (P,B) system we can define a binary operation $\cdot$ on the set of points as follows:

$$\begin{aligned} x \cdot x &= x, \\ x \cdot y &= \text{the third point on the block through } x \text{ and } y \end{aligned}$$

for all $x,y \in P, x \neq y$. The resulting groupoid is called a squag. The (equational) class of all squags is defined by the equations:

$$\begin{aligned} x \cdot x &= x \\ x \cdot y &= y \cdot x \\ x \cdot (x \cdot y) &= y \end{aligned} \tag{4.3.1}$$

Conversely, given a finite squag $\langle S; \cdot \rangle$, i.e. a groupoid satisfying the equations (4.3.1), we can construct a Steiner Triple System by taking the elements of S as points and the sets $\{x, y, (x \cdot y)\}$ with $x \neq y$ and $x, y \in S$ as blocks. Therefore squags correspond exactly to Steiner triple systems.

In 1960 M. Hall, Jr. investigated which Steiner triple systems are transitive on triangles. In (Hall 1960) he showed that there are exactly two classes of such Steiner triple systems. The first class consists of all systems whose subplanes (i.e. subdesigns generated by a triangle) are the projective plane of order 2. He showed that these are exactly the projective geometries over GF(2). The second class is the class of all Steiner triple systems whose subplanes are the affine (9-element) plane over GF(3) (See figure 2). This class obviously contains all affine geometries over GF(3). But contrary to the first case there are also non-affine Steiner triple systems belonging to this class. As M. Hall, Jr. has proven, the smallest non-affine Steiner triple system whose subplanes are affine planes over GF(3) has 81 elements. This system is

unique and we will refer to it and to the corresponding squag as H_{81} and $HALL_{81}$ respectively. Every Steiner triple systems in this second class (whether affine or not) will be called *Hall triple system (HTS)*, although some authors use this name for the non-affine systems only. It can be shown that the squags associated with Hall triple systems are exactly the (self-) distributive squags, i.e. those groupoids satisfying the following four equations:

$$\begin{aligned} x \cdot x &= x \\ x \cdot y &= y \cdot x \\ x \cdot (x \cdot y) &= y \\ x \cdot (y \cdot z) &= (x \cdot y) \cdot (x \cdot z) \end{aligned} \qquad \textbf{(4.3.2)}$$

(Distributive squags are also called commutative reflection spaces (kommutative Spiegelungsräume), e.g. by Loos and Klossek, or symmetric distributive quasigroups, e.g. by Deza.) Conversely, the Steiner triple system corresponding to a given finite distributive squag is also always a Hall triple system.

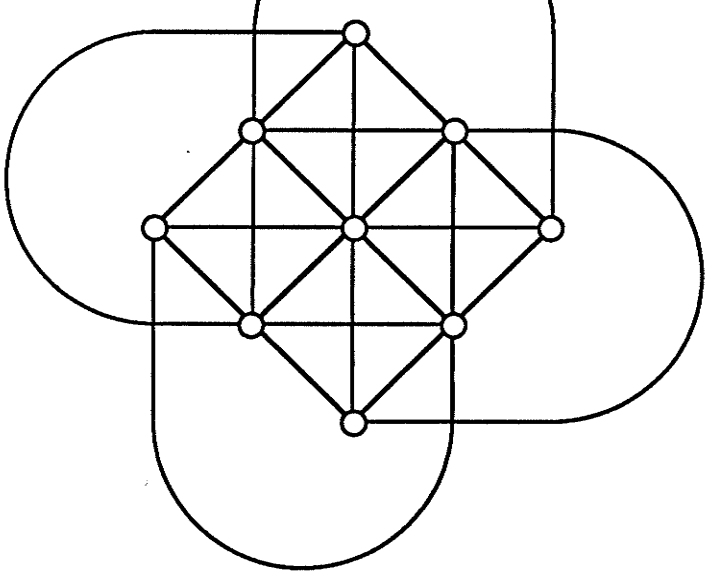


Figure 2:
Affine plane over GF(3)

It is easy to verify that these distributive squags are functionally equivalent to commutative Moufang loops of exponent 3. In (Bruck 1971) Bruck presents an extended theory for commutative Moufang loops of exponent 3, which was first translated into

the language of distributive squags and then expanded by Klossek in (Klossek 1975). Some results of this paper will be presented in the next chapter.

4.4. SQS-Skeins

Let (P,B) be a Steiner quadruple system, i.e. a Steiner system of type (3,4). Then we can define on P a ternary operation q by

$$\begin{aligned} q(x,x,y) &= y \\ q(x,y,x) &= y \\ q(y,x,x) &= y \text{ and} \\ q(x,y,z) &= \text{4th point on the block through } x,y \text{ and } z \end{aligned}$$

for all $x \neq y \neq z \neq x$ in P.

The algebras $\langle P; q\rangle$ obtained in this way are called SQS-skeins. The class of all SQS-skeins is defined by the equations:

$$\begin{aligned} q(x,x,y) &= y \\ q(x,y,z) &= q(x,z,y) \\ q(x,y,z) &= q(y,x,z) \text{ and} \\ q(x,y,q(x,y,z)) &= z \end{aligned} \qquad \textbf{(4.4.1)}$$

Conversely, given any SQS-skein $\langle P; q\rangle$ i.e. any algebra of type $\langle 3\rangle$ satisfying the equations (4.4.1) we can define a set B of blocks on P by:

$$B = \left\{ \{x,y,z,q(x,y,z)\} \middle| x,y,z \in P,\ x \neq y \neq z \neq x \right\}$$

It is straightforward to verify that (P,B) is indeed a Steiner quadruple system.

In chapter 7 we will take a closer look at nilpotent SQS-skeins.

5. Squags

5.1. Basic Properties

It is well known—and was first proven in (Ganter, Werner 1975 A)—that the class of all squags is a congruence uniform, regular, coherent, permutable and modular variety, i.e. all congruence classes of the same congruence are of identical size, each congruence class determines the congruence uniquely, each subalgebra that contains a congruence class of a congruence is the union of congruence classes of this congruence, etc. Moreover, every congruence class is a subalgebra, but there may be subalgebras which are not congruence classes for any congruence (i.e. this variety is not hamiltonian).

5.2. Medial Squags

In (Hall 1960) M. Hall, Jr. has shown that the affine Hall triple systems (i.e. Hall triple systems that are affine spaces over GF(3)) are those Hall triple systems which are transitive on 4-tuples of non-planar points. As a consequence the (distributive) squags corresponding to affine Hall triple systems are exactly those satisfying the *medial* or *surcommutative law*:

$$(x \cdot y) \cdot (z \cdot u) \quad = \quad (x \cdot z) \cdot (y \cdot u) \tag{5.2.1}$$

Note that the medial law implies the distributive law, by choosing $x = y$.

As mentioned above, the smallest non-affine Hall triple system is H_{81}. Therefore it corresponds to the smallest distributive squag violating (5.2.1). This algebra was first discussed by G. Bol in (Bol 1973). It can be given as follows: $HALL_{81} = \langle V;\bullet\rangle$ where $V = (\mathrm{GF}(3))^4$ and $\bullet$ is defined by

$$(x \bullet y)_i = \begin{cases} -x_i - y_i & \text{if } i \neq 4 \\ -x_4 - y_4 + (x_1 - y_1)\begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix} & \text{if } i = 4 \end{cases} \qquad \text{for } i = 1,\ldots,4$$

It can easily be checked that this structure is a distributive squag and that the medial law (5.3.1) is not satisfied for $x = (0,0,0,0)$, $y = (0,1,0,1)$, $z = (1,1,0,1)$, and $u = (1,0,1,0)$.

5.3. The Squag Commutator for Distributive Squags

In group theory nilpotence refers to the commutative law: groups that are nilpotent of class 1 are commutative, etc. In the theory of distributive squags nilpotence refers to the medial law instead of the commutative law. Let $\mathfrak{S} = \langle S;\cdot\rangle$ be a distributive squag and $e \in S$. Then define $f_e(a,b,c)$ to be the polynomial:

$$f_e(a,b,c) \quad = \quad ((e \cdot a) \cdot (b \cdot c)) \cdot (((e \cdot c) \cdot (b \cdot a)) \cdot e) \qquad \textbf{(5.3.1)}$$

If e, a ,b and c generate a medial subalgebra of $\mathfrak{S}$ then clearly $f_e(a,b,c) = e$. If at least two of the four variables are identical the generated subalgebra must be contained in a plane, i.e. it is medial and $f_e(a,b,c) = e$ holds. If $\mathfrak{A} = \langle A;\cdot\rangle$, $\mathfrak{B} = \langle B;\cdot\rangle$ and $\mathfrak{C} = \langle C;\cdot\rangle$ are normal subalgebras of $\mathfrak{S}$, i.e. subalgebras which are congruence classes of some congruences (possibly of a different congruence for each of A, B, and C), and $e \in A \cap B \cap C$ then $f_e(\mathfrak{A},\mathfrak{B},\mathfrak{C})$ denotes the subalgebra generated by $\{f_e(a,b,c) \mid a \in A \;\&\; b \in B \;\&\; c \in C\}$. It can be shown that $f_e(\mathfrak{A},\mathfrak{B},\mathfrak{C})$ is even a normal subalgebra. Similar to the original definition of the commutator in the theory of groups, the squag theoretic commutator of two normal subalgebras $\mathfrak{A}$ and $\mathfrak{B}$ of $\mathfrak{S} = \langle S;\cdot\rangle$ that contain a common element e (corresponding to the constant 0 in groups) can be defined as the (normal) subalgebra $\langle f_e(\mathfrak{A},\mathfrak{S},\mathfrak{B});\cdot\rangle$. For congruences we can therefore define:

DEFINITION 5.3.2 Let $\mathbb{S} = \langle S;\cdot\rangle$ be a distributive squag and $e \in S$. Let α and β be congruences on $\mathbb{S}$. Then the *squag theoretic commutator* of α and β will be denoted as $[\alpha,\beta]^S$ and is defined as

$$[\alpha,\beta]^S = \Theta^{\mathbb{S}}\left(\left\{(e,f_e(a,b,c)) \middle| a\alpha e \;\&\; b\in S \;\&\; b\beta e\right\}\right).$$

It is clear that this squag theoretic commutator is a congruence. It is presently not known whether this squag theoretic commutator coincides with the universal algebraic one, but the author has proven in (Gülzow 1983):

THEOREM 5.3.3 *Let $\mathbb{S} = \langle S;\cdot\rangle$ be a distributive squag. Let α and β be any congruences on $\mathbb{S}$. Then*

$$[\alpha,\beta] \;\geq\; [\alpha,\beta]^S \quad \textit{and} \quad [\iota_S,\beta] \;=\; [\iota_S,\beta]^S$$

This theorem is also a consequence of the Vaughan-Lee description of the commutator. Using this concept of a commutator the notion of nilpotence can be defined as before:

DEFINITION 5.3.4 Let $\mathbb{S} = \langle S;\cdot\rangle$ be any distributive squag. Then define:

$$\mathbb{S}_0 = \mathbb{S}$$
$$\mathbb{S}_{n+1} = f_e(\mathbb{S}_n,\mathbb{S},\mathbb{S})$$

with $\mathbb{S}_n = \langle S_n;\cdot\rangle$. If $S_k = \{e\}$ and $S_{k-1} \neq \{e\}$ then $\mathbb{S}$ is said to be *of nilpotence class k*. Moreover, we will consider the trivial (i.e. 1-element) squag $\langle\{e\};\cdot\rangle$ to be of nilpotence class 1.

Theorem 5.3.3 clearly ensures that this concept of nilpotence coincides with the universal algebraic concept as defined in 3.2.1.

Using 5.3.4 and 5.3.1 one can easily verify that the distributive squags of nilpotence class 1 are exactly those satisfying the medial law 5.3.1, i.e those squags corresponding to the affine spaces over GF(3).

DEFINITION 5.3.5 The (squag theoretic) *centre* $\zeta'(\mathfrak{S})$ of the distributive squag $\mathfrak{S} = \langle S;\cdot\rangle$ is defined to be the congruence generated by:

$$\left\{(e,x)\in S^2 \middle| f_e(x,b,c)=e \text{ for all } b\in S \;\&\; c\in S\right\}$$

which is equal to:

$$\left\{(e,x)\in S^2 \middle| (e\cdot x)\cdot(b\cdot c)=(e\cdot c)\cdot(b\cdot x) \text{ for all } b\in S \;\&\; c\in S\right\}$$

It is easy to see that $\zeta(\mathfrak{S}) \supseteq \zeta'(\mathfrak{S})$. A short proof verifies $\zeta(\mathfrak{S}) \subseteq \zeta'(\mathfrak{S})$. We have therefore:

THEOREM 5.3.6 *The universal algebraic centre of a distributive squag and its squag theoretical centre coincide.*

In the variety of distributive squags the centre also allows us to recognize whether a given distributive squag is subdirectly irreducible:

THEOREM 5.3.7 *Let* $\mathfrak{S} = \langle S;\cdot\rangle$ *be a distributive squag and let* $e \in S$. *Then* $|[e]\zeta(\mathfrak{S})| = 3$ *if and only if* $\mathfrak{S}$ *is subdirectly irreducible.*

A proof of this theorem can be found in (Klossek 1975, 4.4). We will prove a generalization of theorem 5.3.7 in section 5.6. Another important congruence related to the concept of nilpotence is:

DEFINITION 5.3.8 The *Frattini congruence* $\mathfrak{T}(\mathfrak{S})$ of the squag $\mathfrak{S}$ is defined as the intersection of all maximal congruence relations of $\mathfrak{S}$.

In (Soublin 1971) J. P. Soublin has proven that for a distributive squag $\mathfrak{S}$, $\mathfrak{T}(\mathfrak{S})$ is the smallest congruence ϕ such that $\mathfrak{S}/_{\gamma}$ is of nilpotence class 1. Therefore every simple distributive squag is medial. This implies that the 3-element distributive squag is the only simple distributive squag and, as a consequence, it is also the only simple nilpotent squag.

5.4. The Theorem of Bruck and Slaby

In (Bruck 1971) Bruck presents the generalization of a theorem previously proven by T. Slaby that—translated into the theory of distributive squags—gives a relationship between the numbers of generators of a distributive squag and its class of nilpotence:

> **THEOREM 5.4.1** *An n-generated distributive squag is of nilpotence class at most n–2.*

The lengthy proof of this theorem can be found in (Bruck 1971). It relies heavily on the structure of the commutator polynomial (5.3.1). Note that this theorem implies that every finitely generated distributive squag is nilpotent, i.e. every finite distributive squag is nilpotent. An arbitrary infinite distributive squag may or may not be nilpotent.

L. Bénéteau has shown in (Bénéteau 1980 A) that the above limit is the best possible:

> **THEOREM 5.4.2** *For $n \geq 3$, the free n-generated distributive squag is of nilpotence class n–2.*

While it was the original goal of the research leading to this thesis to generalize theorem 5.4.1 and possibly 5.4.2 we were unable to succeed. In fact a result that we obtained for nilpotent SQS-skeins shows that they cannot be generalized for all E-minimal algebras of affine type.

5.5. Free Distributive Squags

In (Bruck 1971) the following important result has been proven:

> **THEOREM 5.5.1** *Let $\mathfrak{S} = \langle S;\bullet\rangle$ be a finitely generated distributive squag. Then S is finite and moreover $|S| = 3^m$ for some integer m.*

COROLLARY 5.5.2 *The variety of distributive squags is locally finite.*

Let $\mathfrak{N}$ denote the class of all distributive squags. We will now consider the class $\mathfrak{N}_k$ of all distributive squags of nilpotence class at most k. It is known from universal algebra that $\mathfrak{N}$ and $\mathfrak{N}_k$ are varieties for every k. Therefore in each $\mathfrak{N}_k$ and for every positive integer n there exists a free n-generated distributive squag $\mathcal{S}_{k,n}$ in $\mathfrak{N}_k$. Let us denote the free n-generated distributive squag in $\mathfrak{N}$ with $\mathcal{S}_n$. By theorem 5.5.1 $\mathcal{S}_{k,n}$ and $\mathcal{S}_n$ are both finite. Since by theorem 5.4.2 $\mathcal{S}_n$ (with $n\geq 3$) is of nilpotence class $n-2$ we know that $\mathcal{S}_n = \mathcal{S}_{k,n}$ for all $n\geq 3$ and all $k \geq n-2$.

In general, the size of $\mathcal{S}_{k,n}$ is unknown. Only for very small k has this size been determined:

$$\log_3\left(\left|\mathcal{S}_{1,n}\right|\right) = n-1 \qquad \text{(affine geometries over GF(3))}$$

$$\log_3\left(\left|\mathcal{S}_{2,n}\right|\right) = n-1+\binom{n-1}{3} \qquad \text{(Bruck 1971)}$$

$$\log_3\left(\left|\mathcal{S}_{3,n}\right|\right) = n-1+\binom{n-1}{3}+4\binom{n-1}{4}+4\binom{n-1}{5} \qquad \text{(Bénéteau 1980 A)}$$

$$\log_3\left(\left|\mathcal{S}_{4,n}\right|\right) = n-1+\binom{n-1}{3}+4\binom{n-1}{4}+14\binom{n-1}{5}+30\binom{n-1}{6}+20\binom{n-1}{7} \qquad \text{(Smith 1984)}$$

From these formulae we can calculate the size of the free distributive squags in $\mathfrak{N}$: $|\mathcal{S}_1| = 3^0$, $|\mathcal{S}_2| = 3^1$, $|\mathcal{S}_3| = 3^2$, $|\mathcal{S}_4| = 3^4$, $|\mathcal{S}_5| = 3^{12}$ and $|\mathcal{S}_6| = 3^{49}$.

5.6. Nilpotent Squags

In section 5.4 we have seen that every distributive squag is nilpotent. This raises the question whether there are any non-distributive squags that are also nilpotent. Before we will answer this question positively by providing an example, we need to charac-

terize the centre of a squag—the characterization given in 5.3.5 and 5.3.6 is only valid for distributive squags—and the squags that are of nilpotence class 1.

LEMMA 5.6.1 *Let* $\mathbb{S} = \langle S;\cdot\rangle$ *be a squag. Then* $a\ \zeta(\mathbb{S})\ b$ *if and only if for all* $c,d \in S$ *the following five identities hold:*

a) $c\cdot d = ((((a\cdot c)\cdot b)((a\cdot d)\cdot b))\cdot b)\cdot a$

b) $c\cdot d = (((((a\cdot b)\cdot c)\cdot b)\cdot(((a\cdot b)\cdot d)\cdot b))\cdot b)\cdot(a\cdot b)$

c) $c\cdot d = ((a\cdot c)\cdot b)\cdot(((a\cdot b)\cdot d)\cdot b)$

d) $c\cdot d = ((((a\cdot c)\cdot b)\cdot d)\cdot b)\cdot(a\cdot b)$

e) $c\cdot d = ((((((a\cdot b)\cdot d)\cdot b)\cdot c)\cdot b)\cdot a$

Proof: The statement of this lemma follows immediately from corollary 3.2.13 if we observe that the Mal'cev polynomial is given by $p(x,y,z) = (x\cdot z)\cdot y$ and the only binary term functions are x, y, and $x\cdot y$. □

THEOREM 5.6.1 *The squag* $\mathbb{S}$ *is of nilpotence class* 1 *if and only if* $\mathbb{S}$ *is medial.*

Proof: Since every medial squag is of nilpotence class 1 in the variety of distributive squags, it is obviously also of nilpotence class 1 in the variety of all squags. Suppose $\mathbb{S} = \langle S;\cdot\rangle$ is of nilpotence class 1. Then $[\iota_S,\iota_S] = \omega_S$. Let $\tau(x_1,x_2,x_3,x_4,x_5)$ be the term function given by:

$$\tau(x_1,x_2,x_3,x_4,x_5) \;=\; (x_2\cdot((x_1\cdot x_3)\cdot(x_4\cdot x_5)))\cdot((x_1\cdot x_4)\cdot(x_3\cdot x_5))$$

By theorem 3.1.9 the following implication holds for all $x,y,a_1,a_2,a_3,a_4,b_1,b_2,b_3,b_4 \in S$:

$$\tau(x,a_1,a_2,a_3,a_4) = \tau(x,b_1,b_2,b_3,b_4) \;\Rightarrow\; \tau(y,a_1,a_2,a_3,a_4) = \tau(y,b_1,b_2,b_3,b_4).$$

Let a,b,c,d,e be some arbitrary elements in S. Let $x = c\cdot d$, $a_1 = b_1 = b_2 = b_3 = b_4 = e$, $y = a$, $a_2 = b$, $a_3 = c$, and $a_4 = d$. Then this implication becomes

$$\tau(c\cdot d,e,b,c,d) = \tau(c\cdot d,e,e,e,e) \;\Rightarrow\; \tau(a,e,b,c,d) = \tau(a,e,e,e,e).$$

Since $\tau(c\cdot d,e,e,e,e) = (e\cdot(((c\cdot d)\cdot e)\cdot(e\cdot e)))\cdot(((c\cdot d)\cdot e)\cdot(e\cdot e)) = (e\cdot(c\cdot d))\cdot(c\cdot d) = e$ and $\tau(c\cdot d,e,b,c,d) = (e\cdot(((c\cdot d)\cdot b)\cdot(c\cdot d)))\cdot(((c\cdot d)\cdot c)\cdot(b\cdot d)) = (e\cdot b)\cdot(d\cdot(b\cdot d)) = (e\cdot b)\cdot b = e$, the left hand side of the latter implication is always true and we have

$$(e\cdot((a\cdot b)\cdot(c\cdot d)))\cdot((a\cdot c)\cdot(b\cdot d)) = \tau(a,e,b,c,d) = \tau(a,e,e,e,e) = e,$$

therefore $$e\cdot((a\cdot b)\cdot(c\cdot d)) = e\cdot((a\cdot c)\cdot(b\cdot d))$$

and finally $$(a\cdot b)\cdot(c\cdot d) = (a\cdot c)\cdot(b\cdot d).$$

Since this equations holds for all $a,b,c,d \in S$ the squag $\mathbf{S} = \langle S;\cdot\rangle$ is medial. □

We will now show that there are indeed non-distributive, but nilpotent squags by constructing a 27-element example. Let $S = \mathrm{GF}(3)^3$ and let $\cdot$ be a binary operation on S defined by:

$$\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}\cdot\begin{pmatrix}y_1\\y_2\\y_3\end{pmatrix} = \begin{pmatrix} -x_1 - y_1 \\ -x_2 - y_2 \\ -x_3 - y_3 + \left({x_1}^2 - 1\right)\left({y_1}^2 - 1\right)(x_2 - y_2)^2 \end{pmatrix}$$

It is immediately clear that $\langle S;\cdot\rangle$ satisfies the identities $x\cdot x = x$ and $x\cdot y = y\cdot x$. Let us consider the identity $x\cdot(x\cdot y) = y$. Obviously $(x\cdot(x\cdot y))_i = y_i$ for all $i \in \{1,2\}$. If $x_1 \neq 0$, i.e. ${x_1}^2 = 1$, then it is also clear that $(x\cdot(x\cdot y))_3 = y_3$. Therefore assume $x_1 = 0$. Then we have:

$$\begin{aligned}(x\cdot(x\cdot y))_3 &= -x_3 - (x\cdot y)_3 + (-1)\left((x\cdot y)_1{}^2 - 1\right)(x_2 - (x\cdot y)_2)^2 \\ &= y_3 + \left({y_1}^2 - 1\right)(x_2 - y_2)^2 - \left({y_1}^2 - 1\right)(x_2 - (-x_2 - y_2))^2 \\ &= y_3 + \left({y_1}^2 - 1\right)(x_2 - y_2)^2 - \left({y_1}^2 - 1\right)(x_2 - y_2)^2 \\ &= y_3\end{aligned}$$

$\langle S;\cdot\rangle$ is therefore a squag. It is not distributive since:

$$\begin{pmatrix}0\\0\\0\end{pmatrix}\cdot\left(\begin{pmatrix}0\\1\\0\end{pmatrix}\cdot\begin{pmatrix}1\\0\\0\end{pmatrix}\right) = \begin{pmatrix}0\\0\\0\end{pmatrix}\cdot\begin{pmatrix}2\\2\\0\end{pmatrix} = \begin{pmatrix}1\\1\\0\end{pmatrix}$$

but $$\left(\left(\begin{pmatrix}0\\0\\0\end{pmatrix}\cdot\begin{pmatrix}0\\1\\0\end{pmatrix}\right)\cdot\left(\begin{pmatrix}0\\0\\0\end{pmatrix}\cdot\begin{pmatrix}1\\0\\0\end{pmatrix}\right)\right)=\begin{pmatrix}0\\2\\1\end{pmatrix}\cdot\begin{pmatrix}2\\0\\0\end{pmatrix}=\begin{pmatrix}1\\1\\2\end{pmatrix}$$

It remains to be verified that $\langle S;\cdot\rangle$ is nilpotent. Let π_2 be the projection onto the first two components. It is clear that the image of π_2 is a medial squag, by theorem 5.6.2 it is therefore nilpotent of class 1. If we can show that $\zeta(\langle S;\cdot\rangle) \supseteq \ker(\pi_2)$, then $\langle S;\cdot\rangle$ is nilpotent of class at most 2.

Suppose $\begin{pmatrix}w_1\\w_2\\w_3\end{pmatrix}\in\left[\begin{pmatrix}0\\0\\0\end{pmatrix}\right]\pi_3$ then $\begin{pmatrix}w_1\\w_2\\w_3\end{pmatrix}=\begin{pmatrix}0\\0\\w_3\end{pmatrix}$.

Using lemma 5.6.1 it is straightforward to verify, that in fact

$$\begin{pmatrix}0\\0\\w_3\end{pmatrix}\in\left[\begin{pmatrix}0\\0\\0\end{pmatrix}\right]\zeta(\langle S;\cdot\rangle).$$

Since the variety of squags is regular, this implies $\ker(\pi_2) \subseteq \zeta(\langle S;\cdot\rangle)$. Since $\langle S;\cdot\rangle$ is not distributive, it cannot be medial; by theorem 5.6.2 it is therefore not of nilpotence class 1. $\langle S;\cdot\rangle$ is a non-distributive squag of nilpotence class 2. In the remainder of this thesis, we will call this squag A_{27} .

5.7. Some Representation Theorems

In (Klossek 1975) two representation theorems for distributive squags are presented. Applying a theorem from (Freese and McKenzie 1987) we can find two further representation theorems, that are even valid for all nilpotent squags. Moreover, these theorems will answer an open question from (Klossek 1975). We will first present—without proof—the two theorems of (Klossek 1975):

FIRST REPRESENTATION THEOREM 5.7.1 *Let* $\mathfrak{S} = \langle S;\cdot\rangle$ *be a finite distributive squag generated by* $A = \{a_1,a_2,\ldots,a_n\}$ *and not by any proper*

subset of A. Then there exists an m-dimensional vector space V ($m \geq n-1$) *and 2m-ary polynomials* $p_i(x_1,\ldots,x_m, y_1,\ldots,y_m)$ *for* $n \leq i \leq m$ *over* GF(3) *without constant term such that*

1) *Every monomial of every* p_i *contains elements of both sets* $\{x_1,\ldots,x_m\}$ *and* $\{y_1,\ldots,y_m\}$.

2) $\mathfrak{S}$ *is isomorphic to* $\mathfrak{V} = \langle V;\square\rangle$ *where*

$$(x \square y)_i = \begin{cases} -x_i - y_i & \text{if } 1 \leq i < n \\ -x_i - y_i + p_i(x,y) & \text{if } n \leq i \leq m \end{cases}$$

3) $\mathfrak{I}(\mathfrak{S})$ *(the Fratini congruence) is the kernel of the projection onto the first n–1 components. This projection is a homomorphism.*

4) *The isomorphism* $\phi : \mathfrak{S} \to \mathfrak{V}$ *can be chosen such that for all i with* $1 \leq i \leq t$ $\phi(a_i) = e_{i-1}$ *where* $(e_i)_k = \delta_{ik}$ *for* $k = 1,\ldots,m$.

SECOND REPRESENTATION THEOREM 5.7.2 *Let* $\mathfrak{S} = \langle S;\cdot\rangle$ *be a finite distributive squag generated by* $A = \{a_1,a_2,\ldots,a_n\}$ *and not by any proper subset of A. Let* $\left|[a_1]\zeta(\mathfrak{S})\right| = 3^r$ *and* $\zeta(\mathfrak{S}) \subseteq \mathfrak{I}(\mathfrak{S})$. *Then there exists an m-dimensional vector space V* ($m \geq n-1$) *and 2m-ary polynomials* $p_i(x_1,\ldots,x_m,y_1,\ldots,y_m)$ *for* $n \leq i \leq m$ *over* GF(3) *without constant term such that*

1) *Every monomial of every* p_i *contains elements of both sets* $\{x_1,\ldots,x_m\}$ *and* $\{y_1,\ldots,y_m\}$.

2) *For* $n \leq l \leq m - r$ *the polynomial* $p_l(x_1,\ldots,x_m,y_1,\ldots,y_m)$ *does not depend on* $x_{m-r+1},\ldots,x_m$ *and* $y_{m-r+1},\ldots,y_m$.

3) $\mathfrak{S}$ *is isomorphic to* $\mathfrak{V} = \langle V;\square\rangle$ *where*

$$(x \square y)_i = \begin{cases} -x_i - y_i & \text{if } 1 \leq i < n \\ -x_i - y_i + p_i(x,y) & \text{if } n \leq i \leq m \end{cases}$$

4) $\mathfrak{I}(\mathfrak{S})$ *is the kernel of the projection onto the first* $n-1$ *components. This projection is a squag homomorphism.*

5) $\zeta(\mathfrak{S})$ *is the kernel of the projection onto the first* $m-r$ *components, this projection is also a squag homomorphism.*

6) *The isomorphism* $\phi : \mathfrak{S} \to \mathfrak{V}$ *can be chosen such that* $\phi(a_i) = e_{i-1}$ *for all* i *with* $1 \le i \le n$ *where* $(e_i)_k = \delta_{ik}$ *for* $k = 1,\ldots,m$.

Using corollary 3.4.7, the following representation theorem for arbitrary nilpotent squags can be proven:

THIRD REPRESENTATION THEOREM 5.7.3 *Let* $\mathfrak{S} = \langle S;\cdot\rangle$ *be a finite squag of nilpotence class* k. *Then there exists an* m*–dimensional vector space* V *and polynomials* $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ *for* $1 \le i \le m$ *over* GF(3) *without constant term and a sequence* $1 \le n_1 < \ldots < n_k = m$ *of integers such that*

1) *For* $n_s < i \le n_{s+1}$ $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ *does not depend on* x_t *and* y_t *for all* t *with* $n_s < t \le m$.

2) $\mathfrak{V} = \langle V;\square\rangle$ *is isomorphic to* $\mathfrak{S}$ *where*

$$(x \square y)_i \quad = \quad -x_i - y_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$$

for all $i \in \{1,\ldots,m\}$ *with* $p_t \equiv 0$ *for all* $t \in \{1,\ldots,n_1\}$.

3) $\zeta(\mathfrak{V})$ *corresponds to the kernel of the projection onto the first* n_{k-1} *components of* $\langle V;\square\rangle$, *this projection is a squag homomorphism.*

4) *If* $\omega_S = \xi_0 \le \xi_1 \le \xi_2 \le \ldots \le \xi_k = \iota_S$ *is the upper central series of* $\langle S;\cdot\rangle$ *then for any* $j \in \{0,1,\ldots,k\}$ *the congruence* ξ_j *corresponds to the kernel of the projection onto the first* n_{k-j} *components of* $\langle V;\square\rangle$.

Proof: If $k = 1$, $\mathfrak{S}$ corresponds to an affine space over GF(3) and it is straightforward to verify the statement of the theorem. In this case $p_i \equiv 0$ for all i. Therefore we will assume that $k > 1$.

By corollary 3.4.7 there is a collection of finite squags $\mathfrak{Q}_1 = \langle Q_1;\cdot\rangle$, $\mathfrak{Q}_2 = \langle Q_2;\cdot\rangle,\ldots,$ $\mathfrak{Q}_k = \langle Q_k;\cdot\rangle$ of nilpotence class 1 and maps $T^1,T^2,\ldots,T^{k-1}$ such that $\mathfrak{S}$ is isomorphic to:

$$\left\langle \prod_{i=1}^{k} Q_i \;;\square \right\rangle$$

with $(r_1,r_2,\ldots,r_k) \square (q_1,q_2,\ldots,q_k) =$

$$\left(r_1\cdot q_1,(r_2\cdot q_2)+T^1(r_1,q_1),\ldots,(r_k\cdot q_k)+T^{k-1}((r_1,r_2,\ldots,r_{k-1}),(q_1,q_2,\ldots,q_{k-1}))\right)$$

where each T^j: $\left(\prod_{i=1}^{j} Q_i\right)^2 \to Q_{j+1}$.

Since all $\mathfrak{Q}_i$ are of nilpotence class 1 they are medial and correspond to affine spaces over GF(3). Therefore each $\mathfrak{Q}_i$ is isomorphic to $\langle \mathrm{GF}(3)^{m_i};\bullet\rangle$ for some $m_i \geq 1$ with $\left(r_1,\ldots,r_{m_i}\right)\bullet\left(q_1,\ldots,q_{m_i}\right)=\left(-r_1-q_1,\ldots,-r_{m_i}-q_{m_i}\right)$. Now define $n_1 = m_1$, $n_i = n_{i-1} + m_i$ for all $i = 2,3,\ldots,k$ and $m = n_k$. Then $1 < n_1 <\ldots< n_k$.

Each T^i can then be considered a mapping from $\mathrm{GF}(3)^{2n_i}$ to $\mathrm{GF}(3)^{m_{i+1}}$. We can further define p_{n_i+j} as the jth component of T^i and $p_i \equiv 0$ if $t \in \{1,\ldots,n_1\}$. Since p_{n_i+j} is a mapping from $\mathrm{GF}(3)^{2n_i}$ to GF(3) it can be written as a polynomial over GF(3).

Using these notations, $\mathfrak{S}$ is isomorphic to $\mathfrak{V} = \langle \mathrm{GF}(3)^{n_k};\square\rangle$ where

$$(x \square y)_i \quad = \quad -x_i - y_i + p_i(x_1,\ldots,x_{n_s},y_1,\ldots,y_{n_s}) \text{ if } n_s < i \leq n_{s+1}.$$

Since $0 = (0,0,\ldots,0)_i = ((0,0,\ldots,0) \square (0,0,\ldots,0))_i = -0 - 0 + p_i(0,\ldots,0) = p_i(0,\ldots,0)$ we can conclude that none of the polynomials p_i has a constant term.

From corollary 3.4.7 we get immediately 3) and 4). □

Note that, as an immediate consequence of this representation theorem, the size of every nilpotent squag is a power of 3.

It is clear that there may be different representations satisfying the conditions of theorem 5.7.3 for any given squag $\mathfrak{S}$. These representations can obviously only differ in the choice of the polynomials p_i, $i= 1,\ldots,m$. In the following discussion we will denote the set of all possible families $(p_i \mid i=1,\ldots,m)$ of polynomials satisfying 5.7.3 with $\mathfrak{T}$. We will now show that we can always choose these polynomials such that every monomial of p_i must contain at least one of $x_1,x_2,\ldots,x_{i-1}$ and one of $y_1,y_2,\ldots,y_{i-1}$.

LEMMA 5.7.4 *The polynomials p_i in theorem 5.6.3 can be chosen such that for all i $p_i(x_1,x_2,\ldots,x_{i-1},0,0,\ldots,0) = 0$.*

To prove lemma 5.7.4 we require the following lemma:

LEMMA 5.7.5 *Let V be an m-dimensional vector space over* GF(3) *and let $\langle V;\bullet\rangle$ be a squag such that*

$$(x \bullet y)_i \quad = \quad -x_i - y_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$$

for $i = 1,\ldots,m$ where the $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ are polynomials over GF(3). *Let k be a fixed number in $\{2,\ldots,m\}$ and let $P(x_1,\ldots,x_{k-1})$ be another polynomial in* GF(3). *Let $\blacklozenge$ be a binary operation on V defined by:*

$$(x \blacklozenge y)_i = \begin{cases} (x \bullet y)_i & \text{if } i<k \\ (x \bullet y)_k + P(x_1,\ldots,x_{k-1}) + P(y_1,\ldots,y_{k-1}) + P\big((x \bullet y)_1,\ldots,(x \bullet y)_{k-1}\big) & \text{if } i=k \\ -x_i-y_i+p_i\big(x_1,\ldots,x_{k-1},x_k-P(x_1,\ldots,x_{k-1}), x_{k+1},\ldots,x_{i-1},y_1,\ldots,y_{k-1}, y_k-P(y_1,\ldots,y_{k-1}),y_{k+1},\ldots,y_{i-1}\big) & \text{if } i>k \end{cases}$$

and let ϕ:$V \to V$ be defined by :

$$\left[\phi((x_1,\ldots,x_m))\right]_i = \begin{cases} x_i & \text{if } i \neq k \\ x_k + P(x_1,\ldots,x_{k-1}) & \text{if } i = k \end{cases}$$

Then ϕ:$\langle V;\bullet\rangle \rightarrowtail\!\!\!\!\rightarrow \langle V;\blacklozenge\rangle$ is an isomorphism and ϕ^{-1} is given by:

$$\left[\phi^{-1}((x_1,\ldots,x_m))\right]_i = \begin{cases} x_i & \text{if } i \neq k \\ x_k - P(x_1,\ldots,x_{k-1}) & \text{if } i = k \end{cases}$$

Moreover, if $\langle V;\bullet\rangle$ satisfies the conditions 3) and 4) of theorem 5.7.3 then $\langle V;\blacklozenge\rangle$ also satisfies these conditions.

Proof of Lemma 5.7.5: From the definition of ϕ it is immediately clear that ϕ is a bijection and that ϕ^{-1} is given as described. To prove that ϕ is even an isomorphism, we will show that for every i $(1 \leq i \leq m)$:

$$\left[\phi(\phi^{-1}((x_1,\ldots,x_m)) \bullet \phi^{-1}((y_1,\ldots,y_m)))\right]_i = \left[(x_1,\ldots,x_m) \blacklozenge (y_1,\ldots,y_m)\right]_i \qquad \textbf{(5.7.6)}$$

5.7.6 holds clearly for $1 \leq i < k$. At first we will show 5.7.6 holds for $i = k$:

$$\Big(\phi\big(\phi^{-1}((x_1,\ldots,x_m)) \bullet \phi^{-1}((y_1,\ldots,y_m))\big)\Big)_k$$

$$= \Big(\phi\Big(\big(x_1,\ldots,x_k - P(x_1,\ldots,x_{k-1}),\ldots,x_m\big) \bullet \big(y_1,\ldots,y_k - P(y_1,\ldots,y_{k-1}),\ldots,y_m\big)\Big)\Big)_k$$

$$= \Big(\phi\Big(\big((x \bullet y)_1,(x \bullet y)_2,\ldots,(x \bullet y)_{k-1},$$
$$-x_k + P(x_1,\ldots,x_{k-1}) - y_k + P(y_1,\ldots,y_{k-1}) + p_k(x_1,\ldots,x_{k-1},y_1,\ldots,y_{k-1}),\ldots\big)\Big)\Big)_k$$

$$= -x_k - y_k + p_k(x_1,x_2,\ldots,x_{k-1},y_1,y_2,\ldots,y_{k-1}) + P(x_1,\ldots,x_{k-1}) + P(y_1,\ldots,y_{k-1})$$
$$+ P\big((x \bullet y)_1,(x \bullet y)_2,\ldots,(x \bullet y)_{k-1}\big)$$

$$= \big((x_1,\ldots,x_m) \blacklozenge (y_1,\ldots,y_m)\big)_k$$

If $i > k$ then we get similarly:

$$\Big(\phi\big(\phi^{-1}((x_1,\ldots,x_m))\bullet\phi^{-1}((y_1,\ldots,y_m))\big)\Big)_i$$

$$=\Big(\phi\Big(\big(x_1,\ldots,x_k-P(x_1,\ldots,x_{k-1}),\ldots,x_m\big)\bullet\big(y_1,\ldots,y_k-P(y_1,\ldots,y_{k-1}),\ldots,y_m\big)\Big)\Big)_i$$

$$=-x_i-y_i+p_i\big(x_1,\ldots,x_i-P(x_1,\ldots,x_{k-1}),\ldots,x_{i-1},y_1,\ldots,y_i-P(y_1,\ldots,y_{k-1}),\ldots,y_{i-1}\big)$$

$$=\big((x_1,\ldots,x_m)\blacklozenge(y_1,\ldots,y_m)\big)_i$$

i.e. 5.7.6 holds for all $i \in \{1,\ldots,m\}$. Therefore ϕ is an isomorphism.

If $\langle V;\bullet\rangle$ satisfies the conditions 3) and 4) of theorem 5.7.3 then $\langle V;\blacklozenge\rangle$ also satisfies these conditions since ϕ and the projection onto the first j components commute for every j. (This is immediately clear from the definition of ϕ.) □

Proof of Lemma 5.7.4: Suppose the conditions of lemma 5.7.3 are satisfied. To prove this lemma we will first define a concept of an *improved* family of polynomials and then show that for every family $(p_i \mid i=1,\ldots,m)$ in $\mathfrak{T}$ not satisfying the condition

$$p_i(x_1,x_2,\ldots,x_{i-1},0,0,\ldots,0) \quad = \quad 0 \qquad \text{for all } i=1,\ldots,m \qquad \textbf{(5.7.7)}$$

we can find an improved family $(q_i \mid i=1,\ldots,m)$ in $\mathfrak{T}$. Note that for $i=1$ the property $p_i(x_1,x_2,\ldots,x_{i-1},0,0,\ldots,0) = 0$ is always satisfied.

In this proof, the *weight* of a point $x \in \mathrm{GF}(3)^m$ shall be the number of non-zero coordinates of x. We define a mapping $\tau:\mathfrak{T}\to\mathbb{N}\times\mathbb{N}\times\mathbb{N}$ as follows: Let $\mathbf{p} = (p_i \mid i=1,\ldots,m) \in \mathfrak{T}$ be a family of polynomials. If $\mathbf{p}$ satisfies 5.7.7 then $\tau(\mathbf{p}) = (m+1,0,0)$, otherwise $\tau(\mathbf{p}) = (a,b,c)$ where a is the smallest number such that

$$p_a(x_1,x_2,\ldots,x_{a-1},0,0,\ldots,0) \quad \neq \quad 0 \qquad \text{for some } (x_1,x_2,\ldots,x_m) \in \mathrm{GF}(3)^m,$$

b is the smallest number such that there exists an $(x_1,x_2,\ldots,x_m) \in \mathrm{GF}(3)^m$ of weight b with $p_a(x_1,x_2,\ldots,x_{a-1},0,0,\ldots,0) \neq 0$, and c is the number of such points of weight b. On $\mathbb{N}\times\mathbb{N}\times\mathbb{N}$ we can define a total ordering $\leq$ by:

$$(a,b,c) \leq (\alpha,\beta,\gamma) \Leftrightarrow \begin{cases} a < \alpha & \text{or} \\ a = \alpha \text{ and } b < \beta & \text{or} \\ a = \alpha \text{ and } b = \beta \text{ and } c \geq \gamma \end{cases}$$

Via τ this total ordering $\leq$ on $\mathbb{N}\times\mathbb{N}\times\mathbb{N}$ induces a partial ordering $\leq_\tau$ on $\mathfrak{T}$ by $\mathbf{p} \leq_\tau \mathbf{q}$ if and only if $\left[\tau(\mathbf{p}) \leq \tau(\mathbf{q}) \text{ and } \tau(\mathbf{p}) \neq \tau(\mathbf{q})\right]$ or $\mathbf{p} = \mathbf{q}$. We write $\mathbf{p} <_\tau \mathbf{q}$ and say a family $\mathbf{q} \in \mathfrak{T}$ is *improved* over $\mathbf{p} \in \mathfrak{T}$ if $\mathbf{p} \leq_\tau \mathbf{q}$ and $\mathbf{p} \neq \mathbf{q}$.

From the definition of τ it is clear that the families in $\mathfrak{T}$ that satisfy 5.7.7 are maximal elements in $\langle \mathfrak{T}; <_\tau \rangle$. In the next part of this proof we are going to show that no other families in $\mathfrak{T}$ are maximal elements by constructing for every $\mathbf{p} \in \mathfrak{T}$ that does not satisfy 5.7.7 a $\mathbf{q} \in \mathfrak{T}$ such that $\mathbf{q}$ is improved over $\mathbf{p}$.

Suppose $\mathbf{p} = (p_i \mid i=1,\ldots,m) \in \mathfrak{T}$ does not satisfy 5.7.7 and $\tau(\mathbf{p}) = (k,b,c)$ with $1 < k \leq m$, $b > 0$ and $c > 0$. Let $(w_1,w_2,\ldots,w_m) \in \mathrm{GF}(3)^m \setminus \{(0,\ldots,0)\}$ be a point of weight b such that $0 \neq p_k(w_1,w_2,\ldots,w_{k-1},0,0,\ldots,0)$. Obviously $w_i = 0$ for all $i = k,\ldots,m$. Let $a_1 < a_2 < \ldots < a_b$ be those integers such that for all i:

$$w_i = 0 \quad \Leftrightarrow \quad i \notin I = \{a_1,a_2,\ldots,a_b\}.$$

Let $K = p_k(w_1,w_2,\ldots,w_{k-1},0,0,\ldots,0)$ and let $P(x_1,\ldots,x_{k-1}) = -K\left(\prod_{j\in I} x_j(w_j - x_j)\right)$.

Note that, since $\mathbf{p} \in \mathfrak{T}$, $\langle V, \square_{\mathrm{p}} \rangle$ is isomorphic to $\mathfrak{S}$ where

$$(x \square_{\mathrm{p}} y)_i = -x_i - y_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) \text{ for all } i \in \{1,\ldots,m\}.$$

Now define $\mathbf{q} = (q_i \mid i=1,\ldots,m)$ by:

- if $1 \leq i < k$ then $q_i(x_1,x_2,\ldots,x_{i-1},y_1,y_2,\ldots,y_{i-1}) = p_i(x_1,x_2,\ldots,x_{i-1},y_1,y_2,\ldots,y_{i-1})$
- if $i = k$ then $q_i(x_1,x_2,\ldots,x_{i-1},y_1,y_2,\ldots,y_{i-1}) =$

$$p_i(x_1,x_2,\ldots,x_{i-1},y_1,y_2,\ldots,y_{i-1}) + P(x_1,\ldots,x_{k-1}) + P(y_1,\ldots,y_{k-1}) + P\big((x \square_{\mathrm{p}} y)_1,(x \square_{\mathrm{p}} y)_2,\ldots,(x \square_{\mathrm{p}} y)_{k-1}\big)$$

- if $m \geq i > k$ then $q_i(x_1,x_2,\ldots,x_{i-1},y_1,y_2,\ldots,y_{i-1}) =$

$$p_i\big(x_1,\ldots,x_i - P(x_1,\ldots,x_{k-1}),\ldots,x_{i-1},y_1,\ldots,y_i - P(y_1,\ldots,y_{k-1}),\ldots,y_{i-1}\big)$$

Lemma 5.7.5 implies that $\langle V, \square_{\mathrm{p}} \rangle$ is isomorphic to $\langle V, \square_{\mathrm{q}} \rangle$ with:

$$(x \square_{\mathrm{q}} y)_i = -x_i - y_i + q_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) \text{ for all } i \in \{1,\ldots,m\}$$

Therefore $\mathbf{q}$ satisfies 5.7.3.3). Lemma 5.7.5 yields also that 5.7.3.4) and 5) are satisfied for $\langle V,\square_q\rangle$. Due to the minimality of b, $P(x_1,\ldots,x_{k-1})$ depends only on the variables that $p_k(x_1,x_2,\ldots,x_{k-1},y_1,y_2,\ldots,y_{k-1})$ also depends on. Therefore $\mathbf{q}$ satisfies 5.7.3.2).

Therefore $\mathbf{q} \in \mathfrak{T}$. It remains to be shown that $\mathbf{p} <_\tau \mathbf{q}$. Recall that $\tau(\mathbf{p}) = (k,b,c)$ and suppose $\tau(\mathbf{q}) = (d,e,f)$. From the construction it is clear that $d \geq k$. If $d > k$ we are done. Therefore assume $d = k$. By the definition of q_k, the minimality of b and since $|I|=b$, for every point $(x_1,\ldots,x_m) \in V$ of weight less than b we have:

$$q_k(x_1,\ldots,x_{k-1},0,\ldots,0) \quad = \quad 0 + p_k(x_1,\ldots,x_{k-1},0,\ldots,0) = 0.$$

This implies $e \geq b$. If $e > b$ we are done. Therefore assume $e = b$.

We know $\qquad p_k(w_1,\ldots,w_{k-1},0,\ldots,0) \quad = \quad K \quad \neq \quad 0. \qquad$ **(5.7.8)**

Now consider the product $(0,0,\ldots,0)\square_p(w_1,\ldots,w_{k-1},0,\ldots,0) = (z_1,\ldots,z_m)$. Obviously $z_i = -w_i$ for all i with $1 \leq i \leq k-1$ and $z_k = K$. (There is nothing that could be said about z_i for $i > k$.) By 4.3.1 we get:

$$(-w_1,-w_2,\ldots,-w_{k-1},K,z_{k+1},\ldots,z_m)\square_p(0,0,\ldots,0) \quad = \quad (w_1,\ldots,w_{k-1},0,\ldots,0)$$

The kth component of this equation yields:

$$-K + p_k(-w_1,\ldots,-w_{k-1},0,\ldots,0) \quad = \quad 0 \qquad \text{or}$$

$$p_k(-w_1,\ldots,-w_{k-1},0,\ldots,0) \quad = \quad K \quad \neq \quad 0 \qquad \textbf{(5.7.9)}$$

Note that the point $(-w_1,\ldots,-w_{k-1},0,\ldots,0) \in V$ has weight b since $(w_1,\ldots,w_{k-1},0,\ldots,0)$ has weight b.

Now let $(x_1,\ldots,x_{k-1},0,\ldots,0) \in V$ be a point of weight b s.t. $p_k(x_1,\ldots,x_{k-1},0,\ldots,0) = 0$. Recall that $a_1<a_2<\ldots<a_b$ are those integers such that for all i:

$$w_i = 0 \quad \Leftrightarrow \quad i \notin I = \{a_1,a_2,\ldots,a_b\}.$$

If one of $x_{a_1},x_{a_2},\ldots,x_{a_b}$ is zero then by the definition of q_k:

$$q_k(x_1,\ldots,x_{k-1},0,\ldots,0) \quad = \quad 0 + p_k(x_1,\ldots,x_{k-1},0,\ldots,0) \quad = \quad 0$$

If the $x_{a_1},x_{a_2},\ldots,x_{a_b}$ are all non-zero then $x_i = 0$ for all $i \notin I$ & $1 \le i \le k-1$ since the weight of $(x_1,\ldots,x_{k-1},0,\ldots,0)$ is b. Because of 5.7.8 and 5.7.9 we have:

$$(x_1,\ldots,x_{k-1},0,\ldots,0) \neq (w_1,\ldots,w_{k-1},0,\ldots,0) \quad \text{and}$$

$$(x_1,\ldots,x_{k-1},0,\ldots,0) \neq (-w_1,\ldots,-w_{k-1},0,\ldots,0).$$

Then there must be $u \in I$ and $v \in I$ such that $x_u = w_u$ and $x_v = -w_v$. But then:

$$q_k(x_1,\ldots,x_{k-1},0,\ldots,0) = 0 + p_k(x_1,\ldots,x_{k-1},0,\ldots,0) = 0\,.$$

Finally:

$q_k(w_1,w_2,\ldots,w_{k-1},0,0,\ldots,0)$

$$= p_k(w_1,\ldots,w_{k-1},0,\ldots,0) - K\left(\prod_{j\in I} w_j(w_j-w_j)\right) - K\left(\prod_{j\in I} 0(w_j-0)\right)$$

$$- K\left(\prod_{j\in I}\left(w_j+0-p_j(w_1,\ldots,w_{j-1},0,\ldots,0)\right)\left(-w_j-w_j-0+p_j(w_1,\ldots,w_{j-1},0,\ldots,0)\right)\right)$$

$$= K - K\left(\prod_{j\in I} 0\right) - K\left(\prod_{j\in I} 0\right) - K\left(\prod_{j\in I} w_j w_j\right)$$

$$= K - K\left(\prod_{j\in I} 1\right) = 0$$

and

$q_k(-w_1,-w_2,\ldots,-w_{k-1},0,0,\ldots,0)$

$$= p_k(-w_1,\ldots,-w_{k-1},0,\ldots,0) - K\left(\prod_{j\in I} -w_j(w_j+w_j)\right) - K\left(\prod_{j\in I} 0(w_j-0)\right)$$

$$- K\left(\prod_{j\in I}\left(-w_j-p_j(-w_1,\ldots,-w_{j-1},0,\ldots,0)\right)\left(-w_j+w_j+p_j(-w_1,\ldots,-w_{j-1},0,\ldots,0)\right)\right)$$

$$= K - K\left(\prod_{j\in I} w_j w_j\right) - K\left(\prod_{j\in I} 0\right) - K\left(\prod_{j\in I} 0\right)$$

$$= K - K\left(\prod_{j\in I} 1\right) = 0$$

We have shown that every point $(x_1,\ldots,x_{k-1},0,\ldots,0) \in V$ of weight b such that $p_k(x_1,\ldots,x_{k-1},0,\ldots,0) = 0$ also satisfies $q_k(x_1,\ldots,x_{k-1},0,\ldots,0) = 0$. Moreover we have shown that there are two points $(x_1,\ldots,x_{k-1},0,\ldots,0)$, $(y_1,\ldots,y_{k-1},0,\ldots,0) \in V$ of weight b such that:

$$p_k(x_1,\ldots,x_{k-1},0,\ldots,0) \neq 0 \quad \& \quad p_k(y_1,\ldots,y_{k-1},0,\ldots,0) \neq 0 \qquad \text{but}$$
$$q_k(x_1,\ldots,x_{k-1},0,\ldots,0) = 0 \quad \& \quad q_k(y_1,\ldots,y_{k-1},0,\ldots,0) = 0$$

i.e. $c \geq f+2 > f$. (In fact it can be proved that $c = f+2$.) This means $\mathbf{p} <_\tau \mathbf{q}$. As we have mentioned above this implies that all maximal points in $\langle \mathfrak{T}; \leq_\tau \rangle$ are satisfying 5.7.7. Since $\mathfrak{T}$ is finite it has at least one maximal point, i.e. the polynomials p_i in Theorem 5.7.3 can be chosen such that for all i: $p_i(x_1,x_2,\ldots,x_{i-1},0,0,\ldots,0) = 0$. □

The polynomial p_3 in our example A_{27} does not satisfy the condition in this lemma since $p_3(0,1,0,0) = (0^2-1)\,(0^2-1)\,(1-0)^2 = 1 \neq 0$. It is relatively simple to find a representation of A_{27} such that the polynomials satisfy this condition:

Let P be the constant polynomial 1. By lemma 5.7.5, the algebra $\langle \mathrm{GF}(3)^3, \blacklozenge \rangle$ with the binary operation $\blacklozenge$ defined by

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \blacklozenge \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} -x_1 - y_1 + 1 + 1 + 1 \\ -x_2 - y_2 \\ -x_3 - y_3 + \left((x_1+1)^2 - 1\right)\left((y_1+1)^2 - 1\right)(x_2 - y_2)^2 \end{pmatrix}$$

$$= \begin{pmatrix} -x_1 - y_1 \\ -x_2 - y_2 \\ -x_3 - y_3 + x_1\,(x_1-1)\,y_1\,(y_1-1)(x_2-y_2)^2 \end{pmatrix}$$

is isomorphic to A_{27} and it is obvious that $p_i(x_1,x_2,\ldots,x_{i-1},0,0,\ldots,0) = 0$ holds for all i.

For distributive squags we are able to specify the type of polynomials even more closely, but we first have to examine some additional property of the polynomials described in 5.7.4:

LEMMA 5.7.10 *Let* V *be an m-dimensional vector space over* GF(3) *and let* $\langle V;\bullet\rangle$ *be a squag with*

$$(x \bullet y)_i \quad = \quad -x_i - y_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$$

for $i = 1,\ldots,m$ *where the* $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ *are polynomials over* GF(3) *such that for all* i $p_i(0,\ldots,0,y_1,\ldots,y_{i-1}) = 0$.

Then for all $(x_1,\ldots,x_m), (y_1,\ldots,y_m) \in V$:

$$|\{j \mid x_j \neq 0\} \cup \{j \mid y_j \neq 0\}| \leq 1 \Rightarrow \quad \forall i \; p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) = 0\,.$$

For the proof of this and the following lemma we require the notation:

DEFINITION 5.7.11 Let V be an m-dimensional vector space over GF(3). Then $s_{(n)}$ denotes the point $(x_1,\ldots,x_m) \in V$ with $x_n = s$ and $x_k = 0$ if $k \neq n$ and $(s_1,s_2)_{(n_1,n_2)}$ denotes the point $(x_1,\ldots,x_m) \in V$ with $x_{n_1} = s_1$, $x_{n_2} = s_2$ and $x_k = 0$ if $k \notin \{n_1,n_2\}$. Any point $(x_1,\ldots,x_m) \in V$ with $x_{n_1} = s_1$, $x_{n_2} = s_2$, $x_{n_3} = s_3$ and $x_k = 0$ if $k \notin \{n_1,n_2\}$ & $k < n_3$ will be denoted by $(s_1,s_2,s_3)_{(n_1,n_2,n_3,\ldots)}$. (The latter expression will therefore indicate one of several possible points.)

Proof of lemma 5.7.10: If $|\{j \mid x_j \neq 0\} \cup \{j \mid y_j \neq 0\}| = 0$ then the equation $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) = 0$ is a special case of $p_i(0,\ldots,0,y_1,\ldots,y_{i-1}) = 0$. We can therefore consider the case $\{j \mid x_j \neq 0\} \cup \{j \mid y_j \neq 0\} = \{k\}$ and the polynomial $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ (i.e. for the remainder of this proof i and k will be fixed). If $i \leq k$ we have again a special case of $p_i(0,\ldots,0,y_1,\ldots,y_{i-1}) = 0$. We may therefore assume that $i > k$.

Since $p_i(0,\ldots,0,y_1,\ldots,y_{i-1}) = 0$ we have $1_{(k)} \bullet 0_{(k)} = 2_{(k)}$. Since every 2-generated squag has three elements, $\{0_{(k)}, 1_{(k)}, 2_{(k)}\}$ is a subalgebra of $\langle V,\bullet\rangle$.

Now suppose $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) \neq 0$ for $(x_1,\ldots,x_m) = s_{(k)}$ and $(y_1,\ldots,y_m) = t_{(k)}$. Then:

$$\left[s_{(k)} \bullet t_{(k)}\right]_i = p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) \neq 0.$$

Since $k < i$ this implies: $s_{(k)} \bullet t_{(k)} \notin \{0_{(k)}, 1_{(k)}, 2_{(k)}\}$ which is a contradiction.
Therefore $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) = 0$. □

Before we will use this lemma to 'improve' the polynomials in the representation of an distributive squag even further, we will consider an obvious consequence of this lemma regarding the existence of small nilpotent squags: Since p_2 depends at most on x_1 and y_1 lemma 5.7.10 implies that $p_2 = 0$ and we have:

> **COROLLARY 5.7.12** *Every nilpotent squag with 3 or 9 elements is medial.*

(In fact, this corollary does not provide us with new information. It is well known that the 9 element squag is unique, i.e. it is the medial one.)

This corollary allows us to deduce that above example A_{27} is even a subdirectly irreducible squag, since otherwise it would have to be the subdirect product of smaller nilpotent squags, at least one of which being non-medial.

As previously indicated, for a distributive squag we can 'improve' the polynomials in the representation even further:

LEMMA 5.7.13 *If the squag* $\mathfrak{S} = \langle S;\cdot\rangle$ *is distributive then the polynomials* p_i *in theorem 5.7.3 can be chosen such that for all* i *and all* $(x_1,\ldots,x_m), (y_1,\ldots,y_m) \in V$:

$$p_i(x_1,x_2,\ldots,x_{i-1},0,0,\ldots,0) = 0 \qquad \textit{and}$$

$$|\{j\,|\,x_j \neq 0\}\cup\{j\,|\,y_j \neq 0\}| \leq 2 \Rightarrow p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) = 0\,.$$

Proof: The proof of this lemma is very similar to the proof of lemma 5.7.4:

Let $\mathfrak{R}$ be the set of all families $(p_i\,|\,i=1,\ldots,m)$ of polynomials satisfying the conditions of lemma 5.7.3 and the condition:

$$p_i(x_1,x_2,\ldots,x_{i-1},0,0,\ldots,0) \;=\; 0 \qquad \text{for all } i = 1,\ldots,m \text{ and } (x_1,\ldots,x_m) \in V \qquad \textbf{(5.7.14)}$$

By lemma 5.7.4 we know that $\mathfrak{R}$ is non-empty.

We will first define a new concept of an *improved* family of polynomials and then show that for every family $\mathbf{p} = (p_i\,|\,i=1,\ldots,m)$ in $\mathfrak{R}$ not satisfying the condition:

$$|\{j\,|\,x_j \neq 0\}\cup\{j\,|\,y_j \neq 0\}| \leq 2 \;\Rightarrow\; \forall i\; p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) = 0 \qquad \textbf{(5.7.15)}$$

we can find an improved family $(q_i\,|\,i=1,\ldots,m)$ in $\mathfrak{R}$. Note that by lemma 5.7.11 the weaker condition:

$$|\{j\,|\,x_j \neq 0\}\cup\{j\,|\,y_j \neq 0\}| \leq 1 \;\Rightarrow\; \forall i\; p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) = 0$$

is always satisfied.

We define a mapping $\tau:\mathfrak{R}\to\mathbb{N}\times\mathbb{N}$ as follows: Let $\mathbf{p} = (p_i\,|\,i=1,\ldots,m) \in \mathfrak{R}$ be a family of polynomials. If $\mathbf{p}$ satisfies 5.7.15 then $\tau(\mathbf{p}) = (m+1,0)$, otherwise $\tau(\mathbf{p}) = (a,b)$ where a is the smallest number such that $p_a(x_1,\ldots,x_{a-1},y_1,\ldots,y_{a-1}) \neq 0$ for some $(x_1,x_2,\ldots,x_m),(y_1,y_2,\ldots,y_m) \in \mathrm{GF}(3)^m$ with $\{j\,|\,x_j \neq 0\}\cup\{j\,|\,y_j \neq 0\} = \{r,s\}$ (from lemma 5.7.11 it is clear that $r \neq s$) and b is the number of possible sets $\{r,s\}$. On $\mathbb{N}\times\mathbb{N}$ we can define a total ordering $\leq$ by:

$$(a,b) \;\leq\; (\alpha,\beta) \qquad \Leftrightarrow \qquad \begin{cases} a < \alpha & \text{or} \\ a = \alpha \text{ and } b \geq \beta \end{cases}$$

Via τ this total ordering $\leq$ on $\mathbb{N}\times\mathbb{N}$ induces a partial ordering $\leq_\tau$ on $\mathfrak{R}$ by $\mathbf{p} \leq_\tau \mathbf{q}$ if and only if $\left[\tau(\mathbf{p}) \leq \tau(\mathbf{q}) \text{ and } \tau(\mathbf{p}) \neq \tau(\mathbf{q})\right]$ or $\mathbf{p} = \mathbf{q}$. We write $\mathbf{p} <_\tau \mathbf{q}$ and say a family $\mathbf{q} \in \mathfrak{R}$ is *improved* over $\mathbf{p} \in \mathfrak{R}$ if $\mathbf{p} \leq_\tau \mathbf{q}$ and $\mathbf{p} \neq \mathbf{q}$.

From the definition of τ it is clear that the families in $\mathfrak{R}$ that satisfy 5.7.15 are maximal elements in $\langle\mathfrak{R};<_\tau\rangle$. In the next part of this proof we are going to show that no other families in $\mathfrak{T}$ are maximal elements by constructing for every $\mathbf{p} \in \mathfrak{R}$ that does not satisfy 5.7.15 a $\mathbf{q} \in \mathfrak{R}$ such that $\mathbf{q}$ is improved over $\mathbf{p}$.

Suppose $\mathbf{p} = (p_i \mid i=1,\ldots,m) \in \mathfrak{R}$ does not satisfy 5.7.15 and $\tau(\mathbf{p}) = (k,b)$ with $1< k \leq m$ and $b > 0$. Let $(u_1,u_2,\ldots,u_m),(v_1,v_2,\ldots,v_m) \in \mathrm{GF}(3)^m$ with:

$$p_k(u_1,\ldots,u_{k-1},v_1,\ldots,v_{k-1}) \neq 0 \text{ and } \{j \mid u_j \neq 0\} \cup \{j \mid v_j \neq 0\} = \{r,s\}.$$

As mentioned above, $r \neq s$. Therefore let us assume $r < s$. By lemma 5.7.11 we have also $s < k$. Since $\mathbf{p} \in \mathfrak{R}$, $\langle V,\square_\mathrm{p}\rangle$ is isomorphic to $\mathfrak{S}$ where

$$(x \square_\mathrm{p} y)_i = -x_i - y_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) \text{ for all } i \in \{1,\ldots,m\}.$$

By 5.7.14:
$$(0,0)_{(r,s)} \square_\mathrm{p} (0,1)_{(r,s)} = (0,2)_{(r,s)} \quad \text{and}$$
$$(0,0)_{(r,s)} \square_\mathrm{p} (1,0)_{(r,s)} = (2,0)_{(r,s)}$$

The three points $(0,0)_{(r,s)}$, $(0,1)_{(r,s)}$, and $(1,0)_{(r,s)}$ will therefore generate a 9-element subplane (subalgebra) of $\langle V,\square_\mathrm{p}\rangle$. Due to the minimality of k we know:

$$(1,0)_{(r,s)} \square_\mathrm{p} (0,1)_{(r,s)} = (2,2,K)_{(r,s,k,\ldots)} \quad \text{and}$$
$$(1,0)_{(r,s)} \square_\mathrm{p} (0,2)_{(r,s)} = (2,1,L)_{(r,s,k,\ldots)}$$

where

$$p_k(x_1,\ldots,x_{k-1},y_1,\ldots,y_{k-1}) = \begin{cases} K & \text{if } (x_1,\ldots,x_m) = (1,0)_{(r,s)} \text{ and } (y_1,\ldots,y_m) = (0,1)_{(r,s)} \\ L & \text{if } (x_1,\ldots,x_m) = (1,0)_{(r,s)} \text{ and } (y_1,\ldots,y_m) = (0,2)_{(r,s)} \end{cases}$$

By 5.7.14 we may conclude:

$$(0,0)_{(r,s)} \square_\mathrm{p} (2,2,K)_{(r,s,k,\ldots)} = (1,1,-K)_{(r,s,k,\ldots)} \quad \text{and}$$
$$(0,0)_{(r,s)} \square_\mathrm{p} (2,1,L)_{(r,s,k,\ldots)} = (1,2,-L)_{(r,s,k,\ldots)}$$

Since the subplane generated by $(0,0)_{(r,s)}$, $(0,1)_{(r,s)}$, and $(1,0)_{(r,s)}$ is the 9-element affine plane we have the situation as shown in figure 3. Recall that three different points x, y and z lie on one line if and only if

$$x \,¤_p\, y = z$$

In the figure, the index of a pair is (r,s) and of a triple $(r,s,k,\ldots)$.

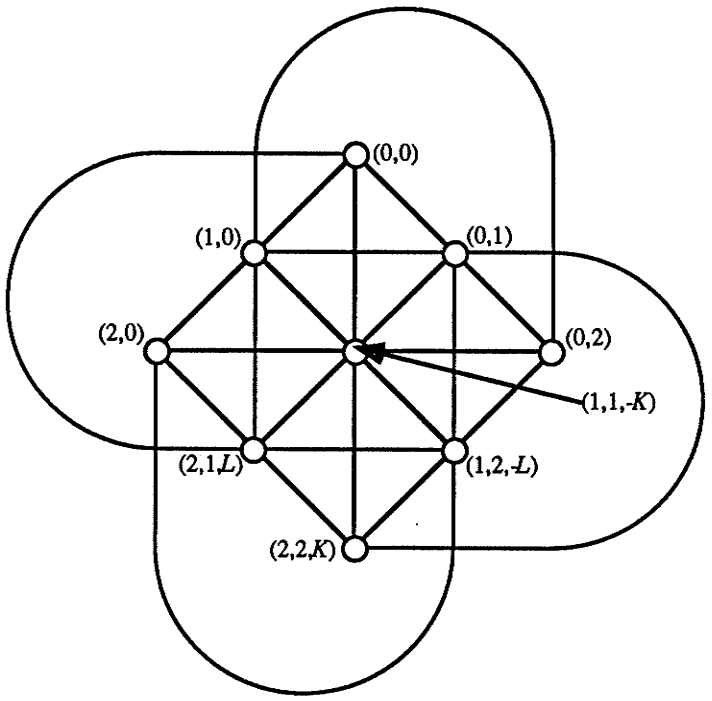


Figure 3:
Subplane generated by $(0,0)_{(r,s)}$, $(0,1)_{(r,s)}$, and $(1,0)_{(r,s)}$.

As in the proof of lemma 5.7.4 we will now define a polynomial $P(x_1,\ldots,x_{k-1})$:

Let $$P(x_1,\ldots,x_{k-1}) = L\cdot\left(x_r^2x_s - x_s^2x_r\right) - K\cdot\left(x_r^2x_s + x_s^2x_r\right) \qquad \textbf{(5.7.16)}$$

Then define $\mathbf{q} = (q_i \mid i=1,\ldots,m)$ by:

- if $1 \le i < k$ then $q_i(x_1,x_2,\ldots,x_{i-1},y_1,y_2,\ldots,y_{i-1}) = p_i(x_1,x_2,\ldots,x_{i-1},y_1,y_2,\ldots,y_{i-1})$
- if $i = k$ then $q_i(x_1,x_2,\ldots,x_{i-1},y_1,y_2,\ldots,y_{i-1}) =$

$$p_i(x_1,x_2,\ldots,x_{i-1},y_1,y_2,\ldots,y_{i-1}) + P(x_1,\ldots,x_{k-1}) + P(y_1,\ldots,y_{k-1})$$
$$+ P\left(-x_1-y_1,-x_2-y_2+p_2(x_1,y_1),\ldots,-x_{k-1}-y_{k-1}+p_{k-1}(x_1,\ldots,y_{k-2})\right)$$

- if $m \ge i > k$ then $q_i(x_1,x_2,\ldots,x_{i-1},y_1,y_2,\ldots,y_{i-1}) =$

$$p_i\left(x_1,\ldots,x_i - P(x_1,\ldots,x_{k-1}),\ldots,x_{i-1},y_1,\ldots,y_i - P(y_1,\ldots,y_{k-1}),\ldots,y_{i-1}\right)$$

Lemma 5.7.5 implies that $\langle V,¤_p\rangle$ is isomorphic to $\langle V,¤_q\rangle$ with:

$$(x \,¤_q\, y)_i = -x_i - y_i + q_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) \text{ for all } i \in \{1,\ldots,m\}$$

Therefore $\mathbf{q}$ satisfies 5.7.3.2). Lemma 5.7.5 yields also that 5.7.3.3) and 4) are satisfied for $\langle V,\mathrm{p}_{\mathbf{q}}\rangle$. Since $P(x_1,\ldots,x_{k-1})$ depends only on variables, on which $p_k(x_1,x_2,\ldots,x_{k-1},y_1,y_2,\ldots,y_{k-1})$ also depends, $\mathbf{q}$ satisfies 5.7.3.1).

By 5.7.16 $P(0,\ldots,0) = 0$ and $P(-x_1,\ldots,-x_{k-1}) = -P(x_1,\ldots,x_{k-1})$, therefore we get:

$q_i(x_1,x_2,\ldots,x_{i-1},0,0,\ldots,0) \quad = \quad 0 \qquad\qquad$ for all $i = 1,\ldots,m$ and $(x_1,\ldots,x_m) \in V$

i.e. $\mathbf{q}$ satisfies 5.7.14 .

Therefore $\mathbf{q} \in \mathfrak{R}$. It remains to be shown that $\mathbf{p} <_\tau \mathbf{q}$. Recall that $\tau(\mathbf{p}) = (k,b)$ and suppose $\tau(\mathbf{q}) = (d,e)$. From the construction it is clear that $d \geq k$. If $d > k$ we are done. Therefore assume $d = k$. Now suppose:

$\{j \mid w_j \neq 0\} \cup \{j \mid z_j \neq 0\} = \{o,t\} \neq \{r,s\} \quad \& \quad p_k(w_1,\ldots,w_{k-1},z_1,\ldots,z_{k-1}) = 0$

Since $\{o,t\} \neq \{r,s\}$ we have $w_r = 0 = z_r$ or $w_s = 0 = z_s$. In either case:

$$
\begin{aligned}
&q_k(w_1,w_2,\ldots,w_{k-1},z_1,z_2,\ldots,z_{k-1}) \\
&\quad = p_k(w_1,w_2,\ldots w_{k-1},z_1,z_2,\ldots,z_{k-1}) + P(w_1,\ldots,w_{k-1}) + P(z_1,\ldots,z_{k-1}) \\
&\qquad + P\big(-w_1-z_1,-w_2-z_2+p_2(w_1,z_1),\ldots,-w_{k-1}-z_{k-1}+p_{k-1}(w_1,\ldots,z_{k-2})\big) \\
&\quad = 0+0+0+P\big(-w_1-z_1,-w_2-z_2,\ldots,-w_{k-1}-z_{k-1}\big) = 0
\end{aligned}
$$

Note that due to the minimality of k: $p_2(w_1,z_1) = \ldots = p_{k-1}(w_1,\ldots,z_{k-2}) = 0$.

The image of the subplane generated by $(0,0)_{(r,s)}$, $(0,1)_{(r,s)}$, and $(1,0)_{(r,s)}$ in $\langle V,\mathrm{p}_{\mathrm{p}}\rangle$ under the isomorphism ϕ is given in figure 4. The calculation is straightforward. Again, the index of a pair is (r,s) and of a triple $(r,s,k,\ldots)$.

Now suppose $\{j \mid w_j \neq 0\} \cup \{j \mid z_j \neq 0\} = \{r,s\}$. Then $(w_1,\ldots,w_m)$ and $(z_1,\ldots,z_m)$ are in the subplane shown in figure 4. We get immediately:

$q_k(w_1,\ldots,w_{k-1},z_1,\ldots,z_{k-1}) = 0$. Since $p_k(u_1,\ldots,u_{k-1},v_1,\ldots,v_{k-1}) \neq 0$ and because of $\{j \mid u_j \neq 0\} \cup \{j \mid v_j \neq 0\} = \{r,s\}$ we get $q_k(u_1,\ldots,u_{k-1},v_1,\ldots,v_{k-1}) = 0$.

Therefore $b > e$ and $\mathbf{p} <_\tau \mathbf{q}$.

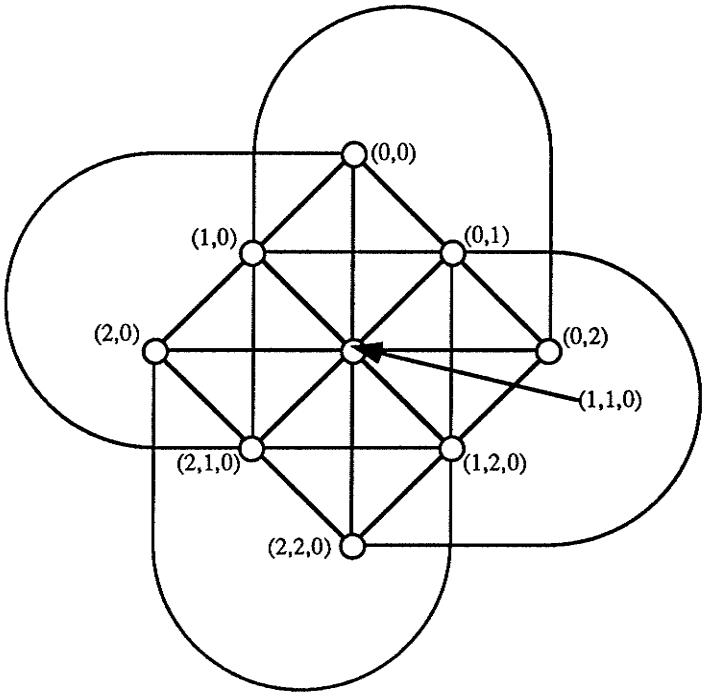


Figure 4:
Image of the subplane generated by $(0,0)_{(r,s)}$, $(0,1)_{(r,s)}$, and $(1,0)_{(r,s)}$ in $\langle V,\square_p\rangle$.

As in the proof of lemma 5.7.4 this implies that the maximal elements of $\langle \mathfrak{R};\leq_\tau\rangle$ satisfy 5.7.15. Since the finite poset $\langle \mathfrak{R};\leq_\tau\rangle$ must have at least one maximal element, we are done. □

Using these lemmas and some further arguments we can formulate a stronger version of theorem 5.7.3:

FOURTH REPRESENTATION THEOREM 5.7.17 *Let $\mathfrak{S} = \langle S;\cdot\rangle$ be a finite squag of nilpotence class k. Then there exists an m–dimensional vector space V, for every i $(1 \leq i \leq m)$ a polynomial $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ over* GF(3), *and an increasing sequence $n_1 < \ldots < n_k = m$ of integers such that*

1) *For $n_s < i \leq n_{s+1}$ $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ does not depend on x_t and y_t for all t with $n_s < t \leq m$.*

2) *$\mathfrak{V} = \langle V;\square\rangle$ is isomorphic to $\mathfrak{S}$ where*

$$(x \square y)_i = -x_i - y_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$$

for all $i \in \{1,\ldots,m\}$ with $p_t \equiv 0$ for all $t \in \{1,\ldots,n_1\}$.

3) $\zeta(\mathfrak{A})$ *corresponds to the kernel of the projection onto the first* n_{k-1} *components of* $\langle V;\Box\rangle$, *this projection is a squag homomorphism.*

4) *If* $\omega_S = \xi_0 \le \xi_1 \le \xi_2 \le \ldots \le \xi_k = \iota_S$ *is the upper central series of* $\langle S;\cdot\rangle$ *then for any* $j \in \{0,1,\ldots,k\}$ *the congruence* ξ_j *corresponds to the kernel of the projection onto the first* n_{k-j} *components of* $\langle V;\Box\rangle$.

5) *For all i and all* $(x_1,\ldots,x_m), (y_1,\ldots,y_m) \in V$:

$$p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) = p_i(y_1,\ldots,y_{i-1},x_1,\ldots,x_{i-1})$$

6) *For all i and all* $(x_1,\ldots,x_m) \in V$: $p_i(x_1,\ldots,x_{i-1},0,\ldots,0) = 0$.*(i.e. no* $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ *has a constant term and every monomial of it contains elements from* $\{x_1,\ldots,x_m\}$ *and from* $\{y_1,\ldots,y_m\}$.*)*

7) *For all* $(x_1,\ldots,x_m), (y_1,\ldots,y_m) \in V$:

$$|\{j \mid x_j \neq 0\} \cup \{j \mid y_j \neq 0\}| \le 1 \Rightarrow \forall i\ p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) = 0\ .$$

8) *If* $k > 1$ *then* $n_1 \ge 2$.

If $\mathfrak{S} = \langle S;\cdot\rangle$ *is distributive, the polynomials* p_i *also satisfy*

9) *For all* $(x_1,\ldots,x_m), (y_1,\ldots,y_m) \in V$:

$$|\{j \mid x_j \neq 0\} \cup \{j \mid y_j \neq 0\}| \le 2 \Rightarrow \forall i\ p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) = 0\ .$$

10) *For all i and all* $(x_1,\ldots,x_m), (y_1,\ldots,y_m) \in V$:

$$p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) = -p_i(-x_1,\ldots,-x_{i-1},-y_1,\ldots,-y_{i-1})$$

(i.e. all monomials in $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ *have an odd number of factors.)*

11) *If* $k > 1$ *then* $n_1 \ge 3$.

Proof: Theorem 5.7.3, together with lemmas 5.7.4, 5.7.10, and 5.7.13, yields theorem 5.7.17 except parts 3, 5, 8, 10, 11, and the second half of 6.

Part 3 is a consequence of part 4. Part 5 follows immediately from the commutativity of the squag operation and implies together with the first half of part 6 that its second part is also true.

To verify part 10, suppose $\mathfrak{S}$ is distributive and consider the following equation:

$$0_{(1)} \,\square\, ((x_1,\ldots,x_m) \,\square\, (y_1,\ldots,y_m)) \;=\; (0_{(1)} \,\square\, (x_1,\ldots,x_m)) \,\square\, (0_{(1)} \,\square\, (y_1,\ldots,y_m)) \quad \textbf{(5.7.18)}$$

Because of the distributivity 5.7.18 is satisfied for every $(x_1,\ldots,x_m)$, $(y_1,\ldots,y_m) \in V$. The ith component of the lefthand side evaluates to:

$$\left(0_{(1)} \,\square\, ((x_1,\ldots,x_m) \,\square\, (y_1,\ldots,y_m))\right)_i = x_i + y_i - p_i\,(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$$

and the same component of the righthand side to:

$$\left((0_{(1)} \,\square\, (x_1,\ldots,x_m)) \,\square\, (0_{(1)} \,\square\, (y_1,\ldots,y_m))\right)_i = x_i + y_i + p_i\,(-x_1,\ldots,-x_{i-1},-y_1,\ldots,-y_{i-1})$$

Part 10 is therefore correct.

To prove 8 and 11, suppose that $\mathfrak{S}$ (and therefore $\mathfrak{V}$) is of nilpotence class $k > 1$. Then consider the image $\langle \mathrm{GF}(3)^{n_2};\square_2 \rangle$ of the projection of $\mathfrak{V}$ onto its first n_2 components. From the construction we know that this algebra is of nilpotence class 2, i.e. it is not medial. Therefore there are points $x = (x_1,x_2,\ldots,x_{n_2})$, $y = (y_1,y_2,\ldots,y_{n_2})$, $z = (z_1,z_2,\ldots,z_{n_2})$ and $w = (w_1,w_2,\ldots,w_{n_2})$ such that

$$(w \,\square_2\, x) \,\square_2\, (y \,\square_2\, z) \;\neq\; (w \,\square_2\, y) \,\square_2\, (w \,\square_2\, z).$$

This inequality must hold in at least one component, say in component j. Due to the definition of the operation $\square_2$ we know $n_1 < j \leq n_2$. Now consider the projection $\pi : \langle \mathrm{GF}(3)^{n_2};\square_2 \rangle \twoheadrightarrow \langle \mathrm{GF}(3)^{1+n_1};\square_3 \rangle$ defined by:

$$\pi(u_1,u_2,\ldots,u_{n_1},\ldots,u_{n_2}) = (u_1,u_2,\ldots,u_{n_1},u_j)$$

where $\square_3$ is given by :

$$(u \,\square_3\, v)_i \;=\; \begin{cases} -u_i - v_i & \text{if } i \leq n_1 \\ -u_i - v_i + p_j(u_1,u_2,\ldots,u_{n_1},v_1,v_2,\ldots,v_{n_1}) & \text{if } i = n_1 + 1 \end{cases}$$

It is easy to verify that this is indeed a homomorphism since p_j depends only on the first n_1 components. Since the inequality had held in the jth component we get

$$(\pi(w)\ \square_3\ \pi(x))\ \square_3\ (\pi(y)\ \square_3\ \pi(z)) \quad \neq \quad (\pi(w)\ \square_3\ \pi(y))\ \square_3\ (\pi(x)\ \square_3\ \pi(z)),$$

i.e. $\langle \mathrm{GF}(3)^{1+n_1};\square_3 \rangle$ is not medial and is an homomorhic image of $\mathfrak{V}$; it must be of nilpotence class 2. By corollary 5.7.12 the smallest squag of nilpotence class 2 has $3^3 = 27$ elements, therefore $n_1 \geq 2$. Moreover, if $\mathfrak{V}$ is distributive so is its homomorphic image $\langle \mathrm{GF}(3)^{1+n_1};\square_3 \rangle$. Since, as mentioned in section 4.3, the smallest distributive squag of nilpotence class 2 (the squag H_{81}) has $3^4 = 81$ elements, we have shown that $n_1 \geq 3$. □

The existence of the squag A_{27} shows that parts 9 and 11 cannot be proven for non-distributive squags, since both of them would imply that A_{27} must be medial.

We will see in chapter 8 that the representation given in 5.7.17 exactly describes the nilpotent squags, since the following theorem is a special case of a theorem proven there:

THEOREM 5.7.19 *Let $\langle V;\cdot \rangle$ be a finite squag having the following properties:*

1) *V is an m-dimensional vectorspace over* GF(3).

2) *There exists a positive integer k and an increasing sequence* $0 = n_0 < n_1 < \ldots < n_k = m$ *of integers such that the binary operation* $\cdot$ *is given by:*

$$(x\cdot y)_i \;=\; x_i + y_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$$

where all $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ *are polynomials over* GF(3) *and each* p_i *does not depend on* $x_{n_t+1},\ldots,x_m,y_{n_t+1},\ldots,y_m$, $z_{n_t+1},\ldots,z_m$ *for* $n_t < i \leq n_{t+1}$.

Then $\langle V;\cdot \rangle$ is nilpotent of class at most k.

In section 3 we had seen that whether a distributive squag is subdirectly irreducible, can be recognized in the size of the centre: theorem 5.3.7 stated that a distributive

squag is subdirectly irreducible if and only if the size of any or every centre class is 3. The representation given in theorem 5.7.17 allows the proof of the same theorem for nilpotent squags in general:

THEOREM 5.7.20 *Let $\mathbb{S} = \langle S;\cdot\rangle$ be a finite nilpotent squag and let $e \in S$. Then $\mathbb{S}$ is subdirectly irreducible if and only if $|[e]\zeta(\mathbb{S})| = 3$.*

Proof: Since $\mathbb{S}$ is a nilpotent squag, it has a representation as described in theorem 5.7.17. Suppose $\mathbb{S}$ is subdirectly irreducible and $n_{k-1} \leq m-2$. Then the two mappings:

$$\pi_{\underline{m}}\left(\begin{pmatrix} x_1 \\ \vdots \\ x_{m-1} \\ x_m \end{pmatrix}\right) = \begin{pmatrix} x_1 \\ \vdots \\ x_{m-1} \\ 0 \end{pmatrix} \text{ and } \pi_{\underline{\underline{m-1}}}\left(\begin{pmatrix} x_1 \\ \vdots \\ x_{m-2} \\ x_{m-1} \\ x_m \end{pmatrix}\right) = \begin{pmatrix} x_1 \\ \vdots \\ x_{m-2} \\ 0 \\ x_m \end{pmatrix}$$

are homomorphisms and have kernels that are smaller than $\zeta(\mathbb{S})$ and that intersect in ω_S. This contradicts 3.2.10, i.e. $n_{k-1} = m-1$. But this implies that each class of $\zeta(\mathbb{S})$ has size 3. On the other hand, if each class of $\zeta(\mathbb{S})$ has size 3, then the only congruences below $\zeta(\mathbb{S})$ are $\zeta(\mathbb{S})$ itself and ω_S. By corollary 3.2.10 this implies that $\mathbb{S}$ is subdirectly irreducible. □

5.8. Construction of Nilpotent Squags

In (Klossek 1975) some methods are described that will allow us to construct arbitrarily large but finite subdirectly irreducible distributive squags of a given nilpotence class $k \geq 2$ if one subdirectly irreducible distributive squag in this class is known. We will first present these methods as theorem 5.8.1 and 5.8.2:

THEOREM 5.8.1 *Let V be an n-dimensional vector space over* GF(3) *and let $\langle V;\bullet\rangle$ be a subdirectly irreducible distributive squag of nilpotence class k such that*

$$(x \bullet y)_i \quad = \quad -x_i - y_i + p_i(x_1,\ldots,x_{n-1},y_1,\ldots,y_{n-1})$$

for $i = 1,\ldots,n$ where the p_i are polynomials over GF(3) *with:*

a) $$p_1 \quad = \quad 0$$

b) $$p_i(0,\ldots,0,0,\ldots,0) \quad = \quad 0 \qquad \text{for } i = 1,\ldots,n$$

c) $$p_i(x_1,0,\ldots,0,y_1,0,\ldots,0) \quad = \quad 0 \qquad \text{for } i = 1,\ldots,n$$

d) $\zeta\big(\langle V;\bullet\rangle\big)$ *is the kernel of the projection onto the first $n-1$ components.*

Then the $n+2$ dimensional vector space V' with the operation $\blacklozenge$ defined by

$$\big(u \blacklozenge v\big)_i = \begin{cases} -u_i - v_i & \text{if } i \le 3 \\ -u_i - v_i + p_{i-2}(u_3,\ldots,u_{n+1},v_3,\ldots,v_{n+1}) & \text{if } 4 \le i \le n+1 \\ -u_i - v_i + p_{i-2}(u_3,\ldots,u_{n+1},v_3,\ldots,v_{n+1}) & \\ \qquad + p(u_1,u_2,u_3,v_1,v_2,v_3) & \text{if } i = n+2 \end{cases}$$

with $p(u_1,u_2,u_3,v_1,v_2,v_3) = (u_3 - v_3)\begin{vmatrix} u_1 & v_1 \\ u_2 & v_2 \end{vmatrix}$ *is a subdirectly irreducible distributive squag of nilpotence class k and $\zeta\big(\langle V';\blacklozenge\rangle\big)$ is the kernel of the projection onto the first $n+1$ components.*

THEOREM 5.8.2 *Let V be an n-dimensional vector space over* GF(3) *and let $\langle V;\bullet\rangle$ be a subdirectly irreducible distributive squag of nilpotence class k such that*

$$(x \bullet y)_i \quad = \quad -x_i - y_i + p_i(x_1,\ldots,x_{n-1},y_1,\ldots,y_{n-1})$$

for $i = 1,\ldots,n$ *where the* p_i *are polynomials over* GF(3) *with:*

a) $p_i(0,0,\ldots,0,y_1,y_2,\ldots,y_{n-1}) \quad = \quad 0 \qquad$ *for* $i = 1,\ldots,n$

b) $\zeta(\langle V;\bullet\rangle)$ *is the kernel of the projection onto the first* $n-1$ *components.*

Let V' *be an m-dimensional vector space over* GF(3) *and let* $\langle V';\blacklozenge\rangle$ *be a subdirectly irreducible distributive squag of nilpotence class j such that*

$$(x \blacklozenge y)_i \quad = \quad -x_i - y_i + q_i(x_1,\ldots,x_{m-1},y_1,\ldots,y_{m-1})$$

for $i = 1,\ldots,m$ *where the* q_i *are polynomials over* GF(3) *with:*

a) $q_i(0,0,\ldots,0,y_1,y_2,\ldots,y_{m-1}) \quad = \quad 0 \qquad$ *for* $i = 1,\ldots,m$

b) $\zeta(\langle V';\blacklozenge\rangle)$ *is the kernel of the projection onto the first* $m-1$ *components.*

Then the $n+m-1$ *dimensional vector space* V'' *with the operation* $*$ *defined by*

$$(u*v)_i = \begin{cases} -u_i - v_i + p_i(u_1,\ldots,u_{n-1},v_1,\ldots,v_{n-1}) & \text{if } 1 \le i \le n-1 \\ \left(\begin{array}{l} -u_i - v_i \\ +q_{i-(n-1)}(u_n,\ldots,u_{n+m-2},v_n,\ldots,v_{n+m-2}) \end{array}\right) & \text{if } n \le i \le n+m-2 \\ \left(\begin{array}{l} -u_i - v_i + p_n(u_1,\ldots,u_{n-1},v_1,\ldots,v_{n-1}) \\ +q_m(u_n,\ldots,u_{n+m-2},v_n,\ldots,v_{n+m-2}) \end{array}\right) & \text{if } i = n+m-1 \end{cases}$$

is a subdirectly irreducible distributive squag of nilpotence class $\max\{k,j\}$.

Since every nilpotence class of distributive squags has to contain at least one subdirectly irreducible squag and this squag can be represented as described in 5.7.17, we can answer an open question of (Klossek 1975) by concluding from 5.8.1 or 5.8.2:

> **COROLLARY 5.8.3** *For every $k \geq 2$ there are infinitely many finite subdirectly irreducible distributive squags of nilpotence class k.*

Klossek was unable to prove this corollary, since her general representation theorems, i.e. theorems 5.7.1 and 5.7.2 in this chapter, did not provide all the properties required for these construction theorems.

6. SQS-Skeins

6.1. Basic Properties

In section 4.4 we introduced the concept of an SQS-skein as a co-ordinatization of a Steiner quadruple system. Let us recall the definition:

DEFINITION 6.1.1 An algebra $\langle S; q\rangle$ of type (3) satisfying the equations

$$\begin{aligned} q(x,x,y) &= y \\ q(x,y,z) &= q(x,z,y) \\ q(x,y,z) &= q(y,z,x) \text{ and} \\ q(x,y,q(x,y,z)) &= z \end{aligned}$$

is called an *SQS-skein.*

An extensive discussion of SQS-skeins can be found in (Armanious 1980), where they are called *Steiner Ternare.* These algebras are sometimes also called *idempotent totally symmetric 3-quasigroups* or *Steiner 3-quasigroups*, e.g. in (Lindner, Rosa 1978).

Since the ternary operation of an SQS-skein itself is a Mal'cev polynomial, it is immediately clear that the variety of SQS-skeins is congruence permutable and modular. Moreover, it is congruence uniform, coherent and regular. A proof of the latter statement is given in (Armanious 1980).

In (Hanani 1960) the possible size of a Steiner quadruple system was investigated. Due to the correspondence between Steiner quadruple systems and SQS-skeins as described in 4.4. we get the following lemma:

LEMMA 6.1.2 *If* $\langle S; q\rangle$ *is an SQS-skein then* $|S| \equiv 2$ *or* $4 \pmod 6$ *or* $|S| = 1$.

Note that lemma 6.1.2 does not exclude any power of 2 as the possible size of an SQS-skein.

Let us consider the subalgebras of an SQS-skein $\langle S; q\rangle$. The defining identities in 6.1.1 imply that every one or two element subset of S forms a subalgebra of $\langle S; q\rangle$. If α is any congruence on the SQS-skein $\langle S; q\rangle$ and $a, b, c \in [d]\alpha$ for some $d \in S$, then $q(a,b,c)\ \alpha\ q(d,d,d) = d$ and therefore $q(a,b,c) \in [d]\alpha$. This means that every congruence class is a subalgebra. In fact we even have:

LEMMA 6.1.3 *If α is a congruence on the SQS-skein $\langle S; q\rangle$ and $\langle T; q\rangle$ a subalgebra of $\langle S; q\rangle$ then $[T]\alpha = \bigcup_{s\in S} [s]\alpha$ is the universe of a subalgebra of $\langle S; q\rangle$.*

A proof of 6.1.3 is contained in (Armanious 1980). Note that this lemma implies immediately that the union of two congruence classes (of the same congruence) is a subalgebra, since—as noted above—every 2-element set is a subalgebra.

While every congruence class is a subalgebra, the converse is not true. An SQS-skein may have subalgebras that are not congruence classes. As in the theory of groups we will call every subalgebra that is a congruence class of some congruence a *normal* subalgebra. The next lemma will characterize these normal subalgebras and describe the associated congruence:

LEMMA 6.1.4 *A subalgebra $\langle N; q\rangle$ of an SQS-skein $\langle S; q\rangle$ is a normal subalgebra (i.e. is the congruence class for some congruence on $\langle S; q\rangle$) if and only if for some $a \in N$ and all $x_1, x_2, x_3, y_1, y_2, y_3 \in S$:*

$$\Big(\forall i \in \{1,2,3\}\ \ q(a, x_i, y_i) \in N\Big) \Rightarrow q(a, q(x_1, x_2, x_3), q(y_1, y_2, y_3)) \in N$$

If $\langle N; q\rangle$ is a normal subalgebra of an SQS-skein $\langle S; q\rangle$, then N is a class of the congruence θ_N defined by:

$$\theta_N = \{(x,y) \in S^2 \mid q(a, x, y)) \in N\} \text{ for some } a \in N.$$

If a subalgebra $\langle N; q\rangle$ of $\langle S; q\rangle$ is sufficiently large (in relation to S) then it is always a normal subalgbra:

LEMMA 6.1.5 *Let $\langle N; q\rangle$ be a subalgebra of the SQS-skein $\langle S; q\rangle$ such that $|S| = \frac{1}{2}|N|$. Then $\langle N; q\rangle$ is a normal subalgebra of $\langle S; q\rangle$.*

Proofs of lemmas 6.1.4 and 6.1.5 can be found in (Armanious 1980).

6.2. Boolean and Semi-Boolean SQS-Skeins

We will precede the discussion of nilpotent SQS-skeins with the study of a subvariety of the variety of SQS-skeins:

DEFINITION 6.2.1 An SQS-skein $\langle S; q\rangle$ satisfying the equation:

$$q(x,u,q(y,u,z)) = q(x,y,z)$$

is called a *boolean* SQS-skein.

In the context of Steiner Quadruple Systems this equation means that if two blocks (of 4 points each) intersect in two points then the remaining four points form a block. (Figure 5.)

In (Quackenbush 1975) a boolean SQS-skein is defined to be an SQS-skein satisfying the equation

$$q(x,u,q(y,u,z)) \quad = \quad q(q(x,u,y),u,z) \qquad \textbf{(6.2.2)}$$

It is immediately clear that the equation 6.2.2 is satisfied by all boolean SQS-skeins as defined in 6.2.1. Since we are able to provide an example of an SQS-skein satisfy-

ing 6.2.2 but failing to be boolean, we will introduce the following name for Quackenbush's version of boolean SQS-skeins:

DEFINITION 6.2.3 An SQS-skein $\langle S; q\rangle$ satisfying the equation:

$$q(x,u,q(y,u,z)) = q(q(x,u,y),u,z)$$

is called a *semi-boolean* SQS-skein.

At the end of this section, lemma 6.2.9 will justify the choice of the expression "semi-boolean", since semi-boolean SQS-skeins satisfy half of the main property of boolean SQS-skeins. As indicated above, we have:

THEOREM 6.2.4 *The variety of boolean SQS-skeins is a proper sub-variety of the variety of semi-boolean SQS-skeins.*

Proof: As mentioned previously, boolean SQS-skeins form a subvariety of the variety of semi-boolean SQS-skeins. To show that this subvariety is proper we will construct an SQS-skein $H_{16} = \langle H; q\rangle$ that is semi-boolean, but not boolean. (We have chosen the name H_{16} since this SQS-skein is very similar to the distributive squag H_{81} as defined in 5.2. and will play an analogous role.)

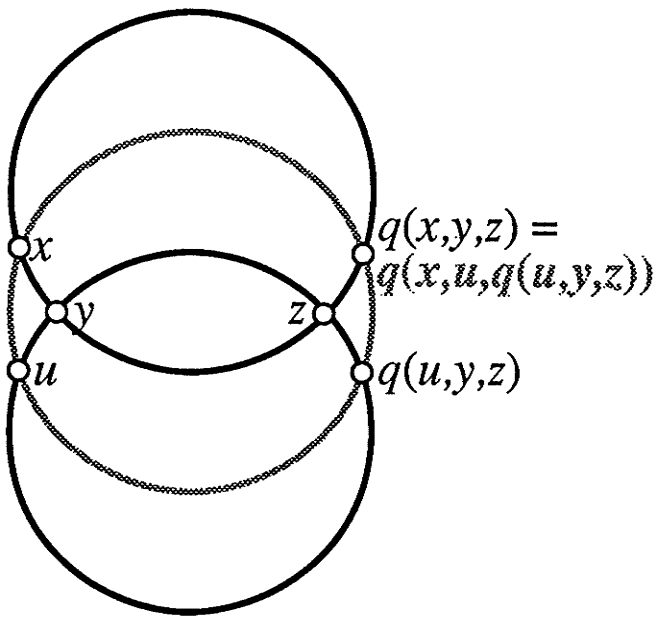


Figure 5:
Intersecting blocks in a boolean SQS-skein

Let H be a 4-dimensional vectorspace over GF(2) and let q be the ternary operation on H given by:

$$q\left(\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix},\begin{pmatrix}y_1\\y_2\\y_3\\y_4\end{pmatrix},\begin{pmatrix}z_1\\z_2\\z_3\\z_4\end{pmatrix}\right)=\begin{pmatrix}x_1+y_1+z_1\\x_2+y_2+z_2\\x_3+y_3+z_3\\x_4+y_4+z_4+\begin{vmatrix}x_1&y_1&z_1\\x_2&y_2&z_2\\x_3&y_3&z_3\end{vmatrix}\end{pmatrix}$$

It is straightforward to verify that $\langle H; q\rangle$ is indeed an SQS-skein. (Note that only one of the defining equations requires some work.) It is not boolean since:

$$q\left(\begin{pmatrix}0\\1\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\1\\0\end{pmatrix},q\left(\begin{pmatrix}0\\0\\1\\0\end{pmatrix},\begin{pmatrix}1\\0\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\0\\0\end{pmatrix}\right)\right)=\begin{pmatrix}1\\1\\0\\1\end{pmatrix}\neq\begin{pmatrix}1\\1\\0\\0\end{pmatrix}=q\left(\begin{pmatrix}0\\1\\0\\0\end{pmatrix},\begin{pmatrix}1\\0\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\0\\0\end{pmatrix}\right)$$

It is also easy to verify that this SQS-skein is semi-boolean. We have (omitting a few steps):

$$q(x,u,q(y,u,z))=\begin{pmatrix}x_1+y_1+z_1\\x_2+y_2+z_2\\x_3+y_3+z_3\\x_4+y_4+z_4+\begin{vmatrix}x_1+z_1&y_1&u_1\\x_2+z_2&y_2&u_2\\x_3+z_3&y_3&u_3\end{vmatrix}+\begin{vmatrix}x_1&u_1&z_1\\x_2&u_2&z_2\\x_3&u_3&z_3\end{vmatrix}\end{pmatrix}=q(x,u,q(y,u,z))$$

□

We will encounter the SQS-skein H_{16} soon again. In 4.4. we had outlined the relationship between SQS-skeins and Steiner quadruple systems. Obviously this SQS-skein H_{16} must also correspond to such a quadruple system. It is given in figure 6.

The main results of (Quackenbush 1975) and (Armanious 1980) on boolean SQS-skeins are given in the following three theorems:

THEOREM 6.2.5 *An SQS-skein $\langle S; q\rangle$ is boolean if and only if there exists a boolean group $\langle S; +,0\rangle$ such that $q(x,y,z) = x + y + z$.*

0	1	2	3	0	4	9	D	1	2	9	A	1	A	D	E	2	7	A	F	3	A	E	F	5	9	B	F
0	1	4	5	0	4	A	E	1	3	4	E	1	B	C	E	2	9	C	F	4	5	6	F	5	A	B	C
0	1	6	7	0	4	B	F	1	3	5	F	1	B	D	F	2	9	D	E	4	5	7	E	5	C	E	F
0	1	8	9	0	5	8	D	1	3	6	C	2	3	4	D	2	B	C	D	4	5	8	9	6	7	8	9
0	1	A	B	0	5	9	C	1	3	7	D	2	3	5	C	2	B	E	F	4	5	C	D	6	7	E	F
0	1	C	D	0	5	A	F	1	3	8	A	2	3	6	F	3	4	5	A	4	6	7	D	6	9	A	D
0	1	E	F	0	5	B	E	1	3	9	B	2	3	7	E	3	4	6	9	4	6	8	A	6	9	B	C
0	2	4	6	0	6	8	E	1	4	6	B	2	3	8	9	3	4	8	F	4	6	C	E	6	A	B	F
0	2	5	7	0	6	9	F	1	4	7	A	2	3	A	B	3	4	B	C	4	7	8	B	6	C	D	F
0	2	8	A	0	6	A	C	1	4	8	D	2	4	5	B	3	5	7	9	4	7	C	F	7	9	A	C
0	2	9	B	0	6	B	D	1	4	9	C	2	4	7	9	3	5	8	E	4	9	A	F	7	9	B	D
0	2	C	E	0	7	8	F	1	5	6	A	2	4	8	E	3	5	B	D	4	9	B	E	7	A	B	E
0	2	D	F	0	7	9	E	1	5	7	B	2	4	A	C	3	6	7	A	4	A	B	D	7	C	D	E
0	3	4	7	0	7	A	D	1	5	8	C	2	5	6	9	3	6	8	D	4	D	E	F	8	9	A	B
0	3	5	6	0	7	B	C	1	5	9	D	2	5	8	F	3	6	B	E	5	6	7	C	8	9	C	D
0	3	8	B	1	2	4	F	1	6	8	F	2	5	A	D	3	7	8	C	5	6	8	B	8	9	E	F
0	3	9	A	1	2	5	E	1	6	9	E	2	6	7	B	3	7	B	F	5	6	D	E	8	A	C	E
0	3	C	F	1	2	6	D	1	7	8	E	2	6	8	C	3	9	C	E	5	7	8	A	8	A	D	F
0	3	D	E	1	2	7	C	1	7	9	F	2	6	A	E	3	9	D	F	5	7	D	F	8	B	C	F
0	4	8	C	1	2	8	B	1	A	C	F	2	7	8	D	3	A	C	D	5	9	A	E	8	B	D	E

Figure 6: The Steiner quadruple system corresponding to H_{16}.

THEOREM 6.2.6 *The variety $\mathbb{A}_0$ of all boolean SQS-skeins is generated by the unique 2-element SQS-skein. $\mathbb{A}_0$ is the unique atom in the lattice of subvarieties of the variety $\mathbb{A}$ of all SQS-skeins.*

THEOREM 6.2.7 *The variety $\mathbb{A}$ of all SQS-skeins is the class of all algebras of type (3) satisfying all identities in three variables that are satisfied in $\mathbb{A}_0$.*

Proofs of the last three theorems can also be found in (Armanious 1980). The following lemma, describing the possible sizes of boolean SQS-skeins, is an immediate corollary of theorem 6.2.5:

COROLLARY 6.2.8 *If $\langle S; q\rangle$ is a finite boolean SQS-skein then $|S| = 2^r$ for some non-negative integer r. Vice versa, if r is any non-negative integer, then there exists (up to isomorphisms) a unique boolean SQS-skein $\langle S; q\rangle$ satisfying $|S| = 2^r$.*

In the remainder of this chapter we will refer to the unique boolean SQS-skein of size 2^r with B_r.

The following lemma justifies the choice of the expression "semi-boolean" since it is about half of theorem 6.2.5. We will omit the proof, because it follows immediately from the defining equations:

LEMMA 6.2.9 *If $\langle S; q\rangle$ is a semi-boolean SQS-skein then for every $0 \in S$ the algebra $\langle S; +,0\rangle$ with $x + y = q(x,y,0)$ is a boolean group.*

This lemma immediately yields a generalization of the first part of corollary 6.2.8:

COROLLARY 6.2.10 *If $\langle S; q\rangle$ is a finite semi-boolean SQS-skein then $|S| = 2^r$ for some non-negative integer r.*

6.3. Nilpotent SQS-Skeins

As in the theory of squags the original definition of nilpotence of SQS-skeins is the universal algebraic one. We have already discussed the SQS-skeins of nilpotence class 1 since:

THEOREM 6.3.1 *The boolean SQS-skeins are exactly the SQS-skeins of nilpotence class* 1.

A simple consequence of 3.4.7, 6.2.8 and 6.3.1 is the following theorem:

THEOREM 6.3.2 *If $\langle S; q\rangle$ is a finite nilpotent SQS-skein then $|S| = 2^r$ for some non-negative integer r.*

Theorems 6.3.1 and 6.3.2 are both consequences of the discussion in (Armanious 1980). Note that the converse of theorem 6.3.2 is not true, since it was shown in

(Armanious 1980) that there exists a 16-element SQS-skein that is not nilpotent. The same thesis also answers the question about the size of the smallest nilpotent SQS-skein that is not boolean: it has 16 elements (and is obviously of nilpotence class 2), it is not necessarily unique. An example of such an SQS-skein is the already discussed H_{16}. To verify that H_{16} is indeed nilpotent, we note that each of the sets

$$\{(x_1,x_2,x_3,x_4) \mid x_i = 0\} \text{ for } i = 1,2,3$$

$$\{(x_1,x_2,x_3,x_4) \mid x_i = 1\} \text{ for } i = 1,2,3$$

$$\{(x_1,x_2,x_3,x_4) \mid x_1 = x_2\},\ \{(x_1,x_2,x_3,x_4) \mid x_1 = x_3\},\ \{(x_1,x_2,x_3,x_4) \mid x_2 = x_3\}$$

$$\{(x_1,x_2,x_3,x_4) \mid x_1 = x_2+1\},\ \{(x_1,x_2,x_3,x_4) \mid x_1 = x_3+1\},\ \{(x_1,x_2,x_3,x_4) \mid x_2 = x_3+1\}$$

has eight elements and is the universe of a subalgebra of H_{16}, i.e. this SQS-skein has at least 12 8-element subalgebras. (By (Gibbons 1976) H_{16} has therefore either 14 or 30 such subalgebras.) Since it has been shown in (Armanious 1980) that every SQS-skein of cardinality 16 with more than 6 8-element subalgebras is nilpotent of class 1 or 2, we know that H_{16} is nilpotent of class 2.

Alternatively we can determine the centre of H_{16} . This is relatively easy due to the following consequence of corollary 3.2.13:

LEMMA 6.3.3 *Let $\mathbb{S} = \langle S; q\rangle$ be an SQS-skein. Then $a\ \zeta(\mathbb{S})\ b$ if and only if for all $c_1,c_2,c_3 \in S$:*

$$q(q(a,b,c_1),c_2,c_3) \;=\; q(a,b,q(c_1,c_2,c_3))$$

Proof: Since every 2-element subset of an SQS-skein is a subalgebra, the 2-generated free SQS-skein has only two elements. Therefore there are only two binary term functions (none of which is essentially binary): $r_1(x,y) = x$ and $r_2(x,y) = y$. Moreover, the ternary operation q itself is a Mal'cev polynomial. After omitting the equations that are obviously satisfied by all elements in every SQS-skein, corollary 3.2.13 yields:

$a\ \zeta(\mathfrak{S})\ b$ if and only if:

(1) $q(q(a,b,c_1),c_2,c_3) = q(a,b,q(c_1,c_2,c_3))$ for all $c_1,c_2,c_3 \in S$ and

(2) $q(q(a,b,c_1),q(a,b,c_2),c_3) = q(c_1,c_2,c_3)$ for all $c_1,c_2,c_3 \in S$ and

(3) $q(q(a,b,c_1),q(a,b,c_2),q(a,b,c_3)) = q(a,b,q(c_1,c_2,c_3))$ for all $c_1,c_2,c_3 \in S$

We will complete the proof by showing that (1) implies (2) and (3). Suppose (1) holds for all $c_1,c_2,c_3 \in S$. Then:

$$\begin{aligned} q(q(a,b,c_1),q(a,b,c_2),c_3) &= q(a,b,q(c_1,q(a,b,c_2),c_3)) && \text{by (1)} \\ &= q(a,b,q(a,b,q(c_2,c_1,c_3))) && \text{by (1)} \\ &= q(c_1,c_2,c_3) \end{aligned}$$

i.e. (2) holds for all $c_1,c_2,c_3 \in S$. Moreover:

$$\begin{aligned} q(q(a,b,c_1),q(a,b,c_2),q(a,b,c_3)) &= q(c_1,c_2,q(a,b,c_3)) && \text{by (2)} \\ &= q(a,b,q(c_1,c_2,c_3)) && \text{by (1)} \end{aligned}$$

i.e. (3) holds for all $c_1,c_2,c_3 \in S$. □

By lemma 6.3.3 $\begin{pmatrix} w_1 \\ \vdots \\ w_4 \end{pmatrix} \in \left[\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}\right] \zeta(H_{16})$ if and only if

$$q\left(q\left(\begin{pmatrix} w_1 \\ \vdots \\ w_4 \end{pmatrix},\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},\begin{pmatrix} c_1^{(1)} \\ \vdots \\ c_4^{(1)} \end{pmatrix}\right),\begin{pmatrix} c_1^{(2)} \\ \vdots \\ c_4^{(2)} \end{pmatrix},\begin{pmatrix} c_1^{(3)} \\ \vdots \\ c_4^{(3)} \end{pmatrix}\right) = q\left(\begin{pmatrix} w_1 \\ \vdots \\ w_4 \end{pmatrix},\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},q\left(\begin{pmatrix} c_1^{(1)} \\ \vdots \\ c_4^{(1)} \end{pmatrix},\begin{pmatrix} c_1^{(2)} \\ \vdots \\ c_4^{(2)} \end{pmatrix},\begin{pmatrix} c_1^{(3)} \\ \vdots \\ c_4^{(3)} \end{pmatrix}\right)\right)$$

$$\text{for all } \begin{pmatrix} c_1^{(1)} \\ \vdots \\ c_4^{(1)} \end{pmatrix},\begin{pmatrix} c_1^{(2)} \\ \vdots \\ c_4^{(2)} \end{pmatrix},\begin{pmatrix} c_1^{(3)} \\ \vdots \\ c_4^{(3)} \end{pmatrix} \in H_{16}$$

i.e.

$$\begin{pmatrix} w_1+c_1^{(1)}+c_1^{(2)}+c_1^{(3)} \\ w_2+c_2^{(1)}+c_2^{(2)}+c_2^{(3)} \\ w_3+c_3^{(1)}+c_3^{(2)}+c_3^{(3)} \\ w_4+c_4^{(1)}+c_4^{(2)}+c_4^{(3)}+\begin{vmatrix} w_1+c_1^{(1)} & c_1^{(2)} & c_1^{(3)} \\ w_2+c_2^{(1)} & c_2^{(2)} & c_2^{(3)} \\ w_3+c_3^{(1)} & c_3^{(2)} & c_3^{(3)} \end{vmatrix} \end{pmatrix} = \begin{pmatrix} w_1+c_1^{(1)}+c_1^{(2)}+c_1^{(3)} \\ w_2+c_2^{(1)}+c_2^{(2)}+c_2^{(3)} \\ w_3+c_3^{(1)}+c_3^{(2)}+c_3^{(3)} \\ w_4+c_4^{(1)}+c_4^{(2)}+c_4^{(3)}+\begin{vmatrix} c_1^{(1)} & c_1^{(2)} & c_1^{(3)} \\ c_2^{(1)} & c_2^{(2)} & c_2^{(3)} \\ c_3^{(1)} & c_3^{(2)} & c_3^{(3)} \end{vmatrix} \end{pmatrix}$$

This is clearly equivalent to

$$\begin{vmatrix} w_1 & c_1^{(2)} & c_1^{(3)} \\ w_2 & c_2^{(2)} & c_2^{(3)} \\ w_3 & c_3^{(2)} & c_3^{(3)} \end{vmatrix} = 0 \text{ for all } \begin{pmatrix} c_1^{(2)} \\ c_2^{(2)} \\ c_3^{(2)} \end{pmatrix} \times \begin{pmatrix} c_1^{(3)} \\ c_2^{(3)} \\ c_3^{(3)} \end{pmatrix} \in \mathrm{GF}(2)^3$$

which happens exactly if $w_1 = w_2 = w_3 = 0$.

We have shown that $\zeta(H_{16}) = \ker(\pi_3)$ where π_3 is the projection onto the first three components. Since the image of π_3 is a boolean SQS-skein, H_{16} is nilpotent of class 2.

The nilpotence of H_{16} also follows immediately from theorem 6.4.4 which we will present and prove in the next section.

Since our example H_{16} is both nilpotent (of class 2) and semi-boolean, we are faced with the two questions whether every semi-boolean SQS-skein is nilpotent and whether every SQS-skein of nilpotence class 2 is semi-boolean. We can answer the latter question negatively by considering the following example $A_{16} = \langle A; q \rangle$:

Let $A = \mathrm{GF}(2)^4$ and q be a ternary operation on A defined by

$$q\left(\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix},\begin{pmatrix}y_1\\y_2\\y_3\\y_4\end{pmatrix},\begin{pmatrix}z_1\\z_2\\z_3\\z_4\end{pmatrix}\right)=\begin{pmatrix}x_1+y_1+z_1\\x_2+y_2+z_2\\x_3+y_3+z_3\\x_4+y_4+z_4+x_1y_1z_1\begin{vmatrix}x_2&y_2&z_2\\x_3&y_3&z_3\\1&1&1\end{vmatrix}\end{pmatrix}$$

It is easy to verify that $A_{16} = \langle A; q\rangle$ is indeed an SQS-skein. It is not semi-boolean (and therefore not boolean) since:

$$q\left(\begin{pmatrix}1\\0\\0\\0\end{pmatrix},\begin{pmatrix}1\\1\\0\\0\end{pmatrix},q\left(\begin{pmatrix}0\\0\\0\\0\end{pmatrix},\begin{pmatrix}1\\1\\0\\0\end{pmatrix},\begin{pmatrix}0\\1\\1\\0\end{pmatrix}\right)\right)=q\left(\begin{pmatrix}1\\0\\0\\0\end{pmatrix},\begin{pmatrix}1\\1\\0\\0\end{pmatrix},\begin{pmatrix}1\\0\\1\\0\end{pmatrix}\right)=\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$$

$$\neq\begin{pmatrix}1\\1\\1\\0\end{pmatrix}=q\left(\begin{pmatrix}0\\1\\0\\0\end{pmatrix},\begin{pmatrix}1\\1\\0\\0\end{pmatrix},\begin{pmatrix}0\\1\\1\\0\end{pmatrix}\right)=q\left(q\left(\begin{pmatrix}1\\0\\0\\0\end{pmatrix},\begin{pmatrix}1\\1\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\0\\0\end{pmatrix}\right),\begin{pmatrix}1\\1\\0\\0\end{pmatrix},\begin{pmatrix}0\\1\\1\\0\end{pmatrix}\right)$$

Via similar calculations as for H_{16}, lemma 6.3.3 yields that

$$\begin{pmatrix}w_1\\\vdots\\w_4\end{pmatrix}\in\left[\begin{pmatrix}0\\\vdots\\0\end{pmatrix}\right]\zeta\left(A_{16}\right)\text{ if and only if}$$

$$a_1\begin{vmatrix}c_2^{(1)}&c_2^{(2)}&c_2^{(3)}\\c_3^{(1)}&c_3^{(2)}&c_3^{(3)}\\1&1&1\end{vmatrix}+\left(a_1+c_1^{(1)}\right)\begin{vmatrix}a_2&c_2^{(2)}&c_2^{(3)}\\a_3&c_3^{(2)}&c_3^{(3)}\\0&1&1\end{vmatrix}=0$$

$$\text{for all }\begin{pmatrix}c_1^{(1)}\\\vdots\\c_4^{(1)}\end{pmatrix},\begin{pmatrix}c_1^{(2)}\\\vdots\\c_4^{(2)}\end{pmatrix},\begin{pmatrix}c_1^{(3)}\\\vdots\\c_4^{(3)}\end{pmatrix}\in A_{16}$$

The choice $c_1^{(1)} = a_1$ shows that $a_1 = 0$. Choosing $c^{(1)} = c^{(2)}$ yields further $a_2 = a_3 = 0$. This proves that again $\zeta(A_{16}) = \ker(\pi_3)$, π_3 being the projection onto the first three components. Since the image of π_3 is a boolean SQS-skein, A_{16} must be of nilpotence class 2. (Note that this will also follow immediately from theorem 6.4.4.) This example yields the following lemma:

LEMMA 6.3.4 *The variety of SQS-skein of nilpotence class at most 2 is not a subclass of the variety of all semi-boolean SQS-skeins.*

The SQS-skein A_{16} is essentially one of the Steiner quadruple systems described in (Armanious n.d.). Armanious considers the direct product of an SQS-skein with the 2-element boolean SQS-skein and modifies one of the 8-element subskeins. In figure 7, the blocks within the modified subskein are marked by a grey underlay.

0 1 2 3	0 4 9 D	1 2 D E	1 7 9 F	2 6 B F	3 9 D F	5 7 D F
0 1 4 5	0 4 A E	1 3 4 6	1 7 A C	2 7 8 D	4 5 6 7	5 9 B F
0 1 6 7	0 4 B F	1 3 5 F	1 B D F	2 7 9 C	4 5 8 9	6 7 8 9
0 1 8 9	0 5 8 D	1 3 7 D	2 3 4 5	2 7 A F	4 5 A B	6 7 A B
0 1 A B	0 5 9 C	1 3 8 A	2 3 6 7	2 7 B E	4 5 C D	6 7 C D
0 1 C D	0 5 A F	1 3 9 B	2 3 8 9	3 4 8 F	4 5 E F	6 7 E F
0 1 E F	0 5 B E	1 3 C E	2 3 A B	3 4 9 E	4 6 8 A	7 9 B D
0 2 4 6	0 6 8 E	1 4 8 D	2 3 C D	3 4 A D	4 6 9 B	8 9 A B
0 2 5 7	0 6 9 F	1 4 9 C	2 3 E F	3 4 B C	4 6 C E	8 9 C D
0 2 8 A	0 6 A C	1 4 A F	2 4 8 E	3 5 7 9	4 6 D F	8 9 E F
0 2 9 B	0 6 B D	1 4 B E	2 4 9 F	3 5 8 E	4 7 8 B	8 A C E
0 2 C E	0 7 8 F	1 5 7 B	2 4 A C	3 5 A C	4 7 9 A	8 A D F
0 2 D F	0 7 9 E	1 5 8 C	2 4 B D	3 5 B D	4 7 C F	8 B C F
0 3 4 7	0 7 A D	1 5 9 D	2 5 8 F	3 6 8 D	4 7 D E	8 B D E
0 3 5 6	0 7 B C	1 5 A E	2 5 9 E	3 6 9 C	5 6 8 B	9 A C F
0 3 8 B	1 2 4 7	1 6 8 F	2 5 A D	3 6 A F	5 6 9 A	9 A D E
0 3 9 A	1 2 5 6	1 6 9 E	2 5 B C	3 6 B E	5 6 C F	9 B C E
0 3 C F	1 2 8 B	1 6 A D	2 6 8 C	3 7 8 C	5 6 D E	A B C D
0 3 D E	1 2 9 A	1 6 B C	2 6 9 D	3 7 A E	5 7 8 A	A B E F
0 4 8 C	1 2 C F	1 7 8 E	2 6 A E	3 7 B F	5 7 C E	C D E F
1 3 5 7	1 3 D F	1 5 B F	1 7 B D 9 B D F	3 5 9 F	3 7 9 D	5 7 9 B

Figure 7: The Steiner quadruple system corresponding to A_{16}.
Exchanging the grey blocks with the blocks below the separating line, creates the 16-element boolean SQS-skein.

6.4. Representation of Nilpotent SQS-Skeins

As in the theory of squags we can again use corollary 3.4.7 to give a representation of any finite nilpotent SQS-skein. Since the abelian SQS-skeins (i.e. the SQS-skeins of nilpotence class 1) are the boolean SQS-skeins, they can easily be described as boolean groups:

LEMMA 6.4.1 *Let $\mathfrak{S} = \langle S; q\rangle$ be a finite abelian SQS-skein (i.e. a finite SQS-skein of nilpotence class 1). Let m be the non-negative integer with $|S| = 2^m$. Then there exists an m–dimensional vector space V over* GF(2) *such that $\mathfrak{V} = \langle V;t\rangle$ is isomorphic to $\mathfrak{S}$ where*

$$(t(x,y,z))_i = x_i + y_i + z_i$$

It is clear that this lemma is a simple consequence of 6.2.2. For arbitrary finite nilpotent SQS-skeins we can therefore obtain the following representation theorem:

THEOREM 6.4.2 *Let $\mathfrak{S} = \langle S; q\rangle$ be a finite SQS-skein of nilpotence class $k > 0$. Let m be the non-negative integer with $|S| = 2^m$ and, for some element a of S, let $|[a]\zeta(\mathfrak{S})| = 2^r$. Then there exists an m–dimensional vector space V over* GF(2) *and a family of polynomials:*

$$p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$$

over GF(2) *for $1 \le i \le m$ and an increasing sequence $n_0 < n_1 < \ldots < n_k$ of integers such that*

1) $0 = n_0, 3 \le n_1, n_{k-1} = m-r$ *and* $n_k = m$

2) *For $n_s < i \le n_{s+1}$ $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$ does not depend on x_t, y_t, and z_t for all t with $n_s < t \le m$.*

3) *$\mathfrak{V} = \langle V;t\rangle$ is isomorphic to $\mathfrak{S}$ where*

$$(t(x,y,z))_i = x_i + y_i + z_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$$

for all $i \in \{1,\ldots,m\}$ with $p_t \equiv 0$ for all $t \in \{1,\ldots,n_1\}$.

4) *For all i and all* $(x_1,\ldots,x_m), (y_1,\ldots,y_m), (z_1,\ldots,z_m) \in V$*:*

$$p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1}) = p_i(y_1,\ldots,y_{i-1},x_1,\ldots,x_{i-1},z_1,\ldots,z_{i-1}) = p_i(y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1},x_1,\ldots,x_{i-1})$$

5) *For all i and all* $(x_1,\ldots,x_m) \in V$ $p_i(x_1,\ldots,x_{i-1},0,\ldots,0) = 0$ *(i.e. no* $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$ *has a constant term and every monomial of it contains elements from at least two of the sets* $\{x_1,\ldots,x_m\}$, $\{y_1,\ldots,y_m\}$ *and* $\{z_1,\ldots,z_m\}$*.)*

6) *If* $\omega_S = \xi_0 \leq \xi_1 \leq \xi_2 \leq \ldots \leq \xi_k = \iota_S$ *is the upper central series of* $\mathfrak{V}$ *then for any* $j \in \{0,\ldots,k\}$ *the congruence* ξ_j *corresponds to the kernel of the projection onto the first* n_{k-j} *components of* $\mathfrak{V}$*.*

7) $\zeta(\mathfrak{V})$ *corresponds to the kernel of the projection onto the first* $m-r$ *components of* $\mathfrak{V}$*, this projection is a homomorphism.*

8) $\mathfrak{V}$ *is subdirectly irreducible if and only if* $n_{k-1} = m-1$*.*

Proof: The main part of theorem 6.4.2 follows again from corollary 3.4.7. Since the details are essentially the same as in the proofs of theorems 5.6.3 and 6.2.3 we will omit that part of the proof. Nevertheless we will have to prove parts 4, 5, and 8, and the fact that $n_1 \geq 3$.

Let us assume that $n_1 < 3$. It is clear that the projection onto the first 3 components is a homomorphism and its image is a finite nilpotent SQS-skein of size $2^3 = 8$. Since $n_1 < 3$ this SQS-skein cannot be nilpotent of class 1, but this contradicts the above mentioned fact that the smallest non-boolean nilpotent SQS-skein has 16 elements.

Parts 4 and 5 follow immediately from the fact that :

$$t((0,\ldots,0),(0,\ldots,0),y) = y,$$
$$t(x,y,z) = t(x,z,y),$$

and $$t(x,y,z) = t(y,x,z)$$

for all $x,y,z \in V$ since $\langle V;t\rangle$ is an SQS-skein.

Part 8 follows from corollary 3.2.10: Suppose $\mathfrak{V}$ is subdirectly irreducible and $n_{k-1} \leq m-2$. Then the two mappings:

$$\pi_{\overline{m}}\left(\begin{pmatrix} x_1 \\ \vdots \\ x_{m-1} \\ x_m \end{pmatrix}\right) = \begin{pmatrix} x_1 \\ \vdots \\ x_{m-1} \\ 0 \end{pmatrix} \text{ and } \pi_{\overline{\overline{m-1}}}\left(\begin{pmatrix} x_1 \\ \vdots \\ x_{m-2} \\ x_{m-1} \\ x_m \end{pmatrix}\right) = \begin{pmatrix} x_1 \\ \vdots \\ x_{m-2} \\ 0 \\ x_m \end{pmatrix}$$

are homomorphisms and have kernels that are below $\zeta(\mathfrak{V})$ and that intersect in ω_V. This contradicts 3.2.10, i.e. $n_{k-1} = m-1$. Now suppose $n_{k-1} = m-1$. Then the size of any class of $\zeta(\mathfrak{V})$ is 2, therefore the only congruences below $\zeta(\mathfrak{V})$ are $\zeta(\mathfrak{V})$ itself and ω_V. But by corollary 3.2.10 this implies that $\mathfrak{V}$ is subdirectly irreducible. □

Part 8) of theorem 6.4.2 can in fact be formulated directly for all nilpotent SQS-skeins:

COROLLARY 6.4.3: *Let $\mathbb{S} = \langle S; q\rangle$ be a finite nilpotent SQS-skein. Then $\mathbb{S}$ is subdirectly irreducible if and only if $|[a]\zeta(\mathbb{S})| = 2$ for some element $a \in S$.*

COROLLARY 6.4.4 *Let $\langle V;t\rangle$ be a finite subdirectly irreducible and nilpotent SQS-skein such that V is an m-dimensional vectorspace over* GF(2) *and t is given by:*

$$(t(x,y,z))_i = x_i + y_i + z_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$$

where all $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$ are polynomials over GF(2). *Then $\zeta(\langle V;t\rangle) = \ker(\pi_{m-1})$, where π_{m-1} denotes the projection onto the first m–1 components of V.*

Proof: Since p_m does not depend on x_m , y_m and z_m it is clear that $\ker(\pi_{m-1})$ is a congruence. By 3.2.9 $\zeta(\langle V;t\rangle) \cap \ker(\pi_{m-1}) \neq \omega_V$, therefore $[\mathbf{0}]\zeta(\langle V;t\rangle) \cap [\mathbf{0}]\ker(\pi_{m-1}) \neq \varnothing$ and by 6.4.3 $|[\mathbf{0}]\zeta(\langle V;t\rangle)| = 2 = |[\mathbf{0}]\ker(\pi_{m-1})|$ which implies immediately that $\zeta(\langle V;t\rangle) = \ker(\pi_{m-1})$. □

We will use this corollary several times in the remainder of this chapter. The representation given in 6.4.2 is very useful since even the converse is true:

THEOREM 6.4.5 *Let $\langle V;t\rangle$ be a finite SQS-skein having the following properties:*

1) *V is an m-dimensional vectorspace over* GF(2).

2) *There exists a positive integer k and an increasing sequence* $0 = n_0 < n_1 < \ldots < n_k = m$ *of integers such that the ternary operation t is given by:*

$$(t(x,y,z))_i = x_i + y_i + z_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$$

where all $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$ *are polynomials over* GF(2) *and each* p_i *does not depend on* $x_{n_t+1},\ldots,x_m,y_{n_t+1},\ldots,y_m,$ $z_{n_t+1},\ldots,z_m$ *for* $n_t < i \leq n_{t+1}$.

Then $\langle V;t\rangle$ is nilpotent of class at most k.

It is clear that this theorem immediately implies that the SQS-skein discussed at the end of the previous section is nilpotent of class at most 2. Analogous theorems can also be proven for squags (see 5.7.19) and p-groups. All three theorems are a consequence of a more general theorem which we will present and prove in chapter 8; we have nevertheless chosen to present this proof since it provides—in this simpler situation—a better insight into the structure of these algebras.

While proving theorem 6.4.5 we will rely heavily on the Vaughan-Lee representation of the commutator as described in 3.3. We need therefore a good description of the commutator terms in the variety of SQS-skeins. This description is given by the following two lemmas:

LEMMA 6.4.6 *Let $\langle V;t\rangle$ be a finite SQS-skein having the following properties:*

1) *V is an m-dimensional vectorspace over* GF(2).

2) *There exists a positive integer k and an increasing sequence* $0 = n_0 < n_1 < \ldots < n_k = m$ *of integers such that the ternary operation t is given by:*

$$(t(x,y,z))_i = x_i + y_i + z_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$$

where all $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$ *are polynomials over* GF(2) *and each* p_i *does not depend on* $x_{n_t+1},\ldots,x_m,y_{n_t+1},\ldots,y_m$, $z_{n_t+1},\ldots,z_m$ *for* $n_t < i \le n_{t+1}$.

For every $i = 1,\ldots,m$ *let* $f(i)$ *be the integer such that* $f(i) = n_r < i \le n_{r+1}$ *for some r. If* $\tau(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(j)})$ *is a term function on* $\langle V;t\rangle$ *then it is given by*

$$\left(\tau(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(j)})\right)_i = \left(\sum_{h=1}^{j} r_h x_i^{(h)}\right) + s_i\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{f(i)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(j)} \\ \vdots \\ x_{f(i)}^{(j)} \end{pmatrix}\right)$$

where $r_1,\ldots,r_j \in$ GF(2) *and the* s_i *are polynomials over* GF(2) *in the variables* $x_1^{(1)},\ldots,x_{f(i)}^{(1)},\ldots,x_1^{(j)},\ldots,x_{f(i)}^{(j)}$.

Proof: We will prove 6.4.6 by induction over the number of operations occurring in τ. If τ is a projection then 6.4.6 is obviously true.

Now suppose

$$\tau(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(j)}) = t(\tau_1(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(j)}),\ldots,\tau_3(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(j)}))$$

where τ_1, τ_2, and τ_3 satisfy 6.4.6, i.e. for $l \in \{1,2,3\}$:

$$\left(\tau_l(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(j)})\right)_i = \left(\sum_{h=1}^{j} r_h^{(l)} x_i^{(h)}\right) + s_i^{(l)}\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{f(i)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(j)} \\ \vdots \\ x_{f(i)}^{(j)} \end{pmatrix}\right)$$

Then $\left(\tau(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(j)})\right)_i =$

$$\sum_{l=1}^{3}\left(\left(\sum_{h=1}^{j} r_h^{(l)} x_i^{(h)}\right) + s_i^{(l)}\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{f(i)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(j)} \\ \vdots \\ x_{f(i)}^{(j)} \end{pmatrix}\right) + P_i\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{f(i)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(j)} \\ \vdots \\ x_{f(i)}^{(j)} \end{pmatrix}\right)\right)$$

$$= \left(\sum_{h=1}^{j}\left(\sum_{l=1}^{3} r_h^{(l)}\right) x_i^{(h)}\right) + \left(\sum_{l=1}^{3} s_i^{(l)}\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{f(i)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(j)} \\ \vdots \\ x_{f(i)}^{(j)} \end{pmatrix}\right) + P_i\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{f(i)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(j)} \\ \vdots \\ x_{f(i)}^{(j)} \end{pmatrix}\right)\right)$$

where P_i is an appropriate composition of p_i, $(\tau_1)_1,\ldots,(\tau_1)_{f(i)}$, $(\tau_2)_1,\ldots,(\tau_2)_{f(i)}$, and $(\tau_3)_1,\ldots,(\tau_3)_{f(i)}$. Note that $\sum_{l=1}^{3} r_h^{(l)}$ does not depend on i. This proves 6.4.6 for all term functions τ. □

LEMMA 6.4.7 *Let $\langle V;t\rangle$ be a finite SQS-skein having the following properties:*

1) V is an m-dimensional vectorspace over GF(2).

2) There exists a positive integer k and an increasing sequence $0 = n_0 < n_1 < \ldots < n_k = m$ *of integers such that the ternary operation t is given by:*

$$(t(x,y,z))_i = x_i + y_i + z_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$$

where all $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$ *are polynomials over* GF(2) *and each* p_i *does not depend on* $x_{n_t+1},\ldots,x_m,y_{n_t+1},\ldots,y_m$, $z_{n_t+1},\ldots,z_m$ *for* $n_t < i \le n_{t+1}$.

For every $i = 1,\ldots,m$ *let* $f(i)$ *be the integer such that* $f(i) = n_r < i \le n_{r+1}$ *for some* r. *If* $\tau(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(j)})$ *is a commutator term with* $j \ge 2$ *then it is given on* $\langle V;t\rangle$ *by*

$$\left(\tau(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(j)},z)\right)_i = z_i + s_i\left(\begin{pmatrix}x_1^{(1)}\\ \vdots \\ x_{f(i)}^{(1)}\end{pmatrix},\ldots,\begin{pmatrix}x_1^{(j)}\\ \vdots \\ x_{f(i)}^{(j)}\end{pmatrix},\begin{pmatrix}z_1\\ \vdots \\ z_{f(i)}\end{pmatrix}\right)$$

where the s_i *are polynomials over* GF(2) *in the variables* $x_1^{(1)},\ldots,x_{f(i)}^{(1)}$, $\ldots,x_1^{(j)},\ldots,x_{f(i)}^{(j)}$ *satisfying*

$$\left(\exists h\in\{1,\ldots,j\} : \begin{pmatrix}x_1^{(h)}\\ \vdots \\ x_{f(i)}^{(h)}\end{pmatrix} = \begin{pmatrix}z_1\\ \vdots \\ z_{f(i)}\end{pmatrix}\right) \Rightarrow s_i\left(\begin{pmatrix}x_1^{(1)}\\ \vdots \\ x_{f(i)}^{(1)}\end{pmatrix},\ldots,\begin{pmatrix}x_1^{(j)}\\ \vdots \\ x_{f(i)}^{(j)}\end{pmatrix},\begin{pmatrix}z_1\\ \vdots \\ z_{f(i)}\end{pmatrix}\right) = 0$$

for all $i \in \{1,\ldots,m\}$

Proof: Let τ be a commutator term. By lemma 6.4.6 τ can be written as:

$$\left(\tau(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(j)},z)\right)_i = \left(\sum_{h=1}^{j} r_h x_i^{(h)}\right) + rz_i + s_i\left(\begin{pmatrix}x_1^{(1)}\\ \vdots \\ x_{f(i)}^{(1)}\end{pmatrix},\ldots,\begin{pmatrix}x_1^{(j)}\\ \vdots \\ x_{f(i)}^{(j)}\end{pmatrix},\begin{pmatrix}z_1\\ \vdots \\ z_{f(i)}\end{pmatrix}\right)$$

We will first prove $r_h = 0$ for all $h \in \{1,\ldots,j\}$. Let $\mathbf{0} = (0,\ldots,0)$. Since τ is a commutator term and $j \ge 2$, for all $x^{(2)},x^{(3)},\ldots,x^{(j)} \in V$ the following equation holds:

$$0 = (\mathbf{0})_1 = \left(\tau(\mathbf{0},x^{(2)},x^{(3)},\ldots,x^{(j)},\mathbf{0})\right)_1 = r_1 0 + \left(\sum_{h=2}^{j} r_h x_1^{(h)}\right) + r0 + s_1 = s_1 + \sum_{h=2}^{j} r_h x_1^{(h)}$$

Therefore $s_1 = 0$ and $r_h = 0$ for all $h \in \{2,\ldots,j\}$. Since $j \geq 2$, we get similarly for all $x^{(1)} \in V$:

$$0 = (\mathbf{0})_1 = \left(\tau(x^{(1)},\mathbf{0},x^{(3)},\ldots,x^{(j)},\mathbf{0})\right)_1 = r_1 x_1^{(1)} + r\mathbf{0} = r_1 x_1^{(1)}$$

i.e. $r_1 = 0$, therefore $r_h = 0$ for all $h \in \{1,\ldots,j\}$. The fact that $r = 1$ follows now immediately from:

$$z_1 = \left(\tau(z,x^{(2)},x^{(3)},\ldots,x^{(j)},z)\right)_1 = rz_1$$

We have shown that τ is given by:

$$\left(\tau(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(j)},z)\right)_i = z_i + s_i\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{f(i)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(j)} \\ \vdots \\ x_{f(i)}^{(j)} \end{pmatrix},\begin{pmatrix} z_1 \\ \vdots \\ z_{f(i)} \end{pmatrix}\right)$$

Suppose $\begin{pmatrix} x_1^{(h)} \\ \vdots \\ x_{f(i)}^{(h)} \end{pmatrix} = \begin{pmatrix} z_1 \\ \vdots \\ z_{f(i)} \end{pmatrix}$, then:

$$z_i = \left(\tau(x^{(1)},\ldots,x^{(h-1)},z,x^{(h+1)},\ldots,x^{(j)},z)\right)_i$$

$$= \left(\tau\left(x^{(1)},\ldots,\begin{pmatrix} x_1^{(h)} \\ \vdots \\ x_{f(i)}^{(h)} \\ z_{f(i)+1} \\ \vdots \\ z_m \end{pmatrix},\ldots,x^{(j)},z\right)\right)_i = z_i + s_i\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{f(i)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(j)} \\ \vdots \\ x_{f(i)}^{(j)} \end{pmatrix},\begin{pmatrix} z_1 \\ \vdots \\ z_{f(i)} \end{pmatrix}\right)$$

and therefore $s_i\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{f(i)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(j)} \\ \vdots \\ x_{f(i)}^{(j)} \end{pmatrix},\begin{pmatrix} z_1 \\ \vdots \\ z_{f(i)} \end{pmatrix}\right) = 0$, i.e. we have proven 6.4.7.

□

Since $\pi_{n_{l-1}}(z) = \pi_{n_{l-1}}(x^{(1)})$ and $f(i) \le n_{l-1}$ this implication yields

$$s_i\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{f(i)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(j)} \\ \vdots \\ x_{f(i)}^{(j)} \end{pmatrix},\begin{pmatrix} z_1 \\ \vdots \\ z_{f(i)} \end{pmatrix}\right) = 0$$

and therefore $\left(\tau(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(j)},z)\right)_i = z_i$ for all $i \le n_l$. This implies $\pi_{n_l}(z) = \pi_{n_l}(\tau(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(j)},z))$, i.e. 6.4.9 and consequently 6.4.8 have been proven.

To complete the proof of 6.4.5 we only have to observe that, for $h = k$, 6.4.8 implies $\phi_k \subseteq \ker(\pi_{n_k}) = \ker(\pi_m) = \omega_V$, therefore $\phi_k = \omega_V$. This means $\langle V;t\rangle$ is nilpotent of class at most k. □

In the next two sections we will consider generating sets of several SQS-skeins. To facilitate this, we will now prove a lemma that provides generating sets for SQS-skeins represented as in the preceding theorems. Note that this generating set is usually not minimal. In fact, it is only minimal if the SQS-skein is boolean.

LEMMA 6.4.10 *Let* $\mathfrak{V} = \langle V;t\rangle$ *be a finite SQS-skein having the following properties:*

1) *V is an m-dimensional vectorspace over* GF(2).

2) *The ternary operation t is given by:*

$$(t(x,y,z))_i = x_i + y_i + z_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$$

where all $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$ *are polynomials over* GF(2).

Let $e_0, e_1, e_2, \ldots, e_m$ *be the elements in V given by* $(e_j)_i = \delta_{ji}$. *Then for every* $h \in \{0,1,\ldots,m\}$:

$$\{x \in V \mid \forall i \le h: x_i = 0\} = [\{e_0\} \cup \{e_j \mid h < j \le m\}]_{\mathfrak{V}}$$

Especially: $$V = [\{e_0,e_1,e_2,\ldots,e_m\}]_{\mathfrak{V}}$$

Proof: Note that for all i and all $x = (x_1,\ldots,x_m) \in V$: $p_i(x_1,\ldots,x_{i-1},0,\ldots,0,0,\ldots,0) = 0$ since $t(x,e_0,e_0) = x$. Let $h \in \{0,1,\ldots,m\}$ and let $z \in \{x \in V \mid \forall i \le h: x_i = 0\}$. Now define $g: [\{e_0\} \cup \{e_j \mid l < j \le m\}]_{\mathfrak{V}} \to \{0,\ldots,m\}$ by:

$$g(x) = \begin{cases} 0 \text{ if } x_1 \neq z_1 \\ j \text{ if } x_{j+1} \neq z_{j+1} \text{ and } x_i = z_i \text{ for all } i \in \{1,\ldots,j\} \\ m \text{ if } x_i = z_i \text{ for all } i \in \{1,\ldots,m\} \end{cases}$$

Note that $g(x) = m$ if and only if $x = z$. Since $\{0,\ldots,m\}$ is finite, there exists a $y \in [\{e_0\} \cup \{e_j \mid h < j \le m\}]_{\mathfrak{V}}$ s.t. $g(y) \ge g(x)$ for all $x \in [\{e_0\} \cup \{e_j \mid h < j \le m\}]_{\mathfrak{V}}$. Obviously $g(y) \ge g(e_l) \ge h$. We will show that $g(y) = m$, i.e. $y = z$.

Suppose $g(y) < m$. Then $y_{g(y)+1} \neq z_{g(y)+1}$, i.e. $y_{g(y)+1} + 1 = z_{g(y)+1}$. Consider the element $t(y,e_0,e_{g(y)+1}) \in [\{e_0\} \cup \{e_j \mid h < j \le m\}]_{\mathfrak{V}}$:

$$\left(t(y,e_0,e_{g(y)+1})\right)_i$$

$$= \begin{cases} y_i + 0 + 0 + p_i(y_1,\ldots,y_{i-1},0,\ldots,0) = y_i & = z_i \quad \text{if } i \le g(y) \\ y_{g(y)+1} + 0 + 1 + p_i(y_1,\ldots,y_{i-1},0,\ldots,0) = y_{g(y)+1} + 1 & = z_{g(y)+1} \text{ if } i = g(y)+1 \end{cases}$$

This implies that $g(t(y,e_0,e_{g(y)+1})) \ge g(y) + 1 > g(y)$, which is a contradiction to the maximality of $g(y)$. Therefore $g(y) = m$ and $z = y \in [\{e_0\} \cup \{e_j \mid h < j \le m\}]_{\mathfrak{V}}$.

We have shown that $\{x \in V \mid \forall i \le h: x_i = 0\} \subseteq [\{e_0\} \cup \{e_j \mid h < j \le m\}]_{\mathfrak{V}}$. Since obviously $\{x \in V \mid \forall i \le h: x_i = 0\} \supseteq [\{e_0\} \cup \{e_j \mid h < j \le m\}]_{\mathfrak{V}}$ we are done. □

6.5. Construction of Nilpotent SQS-Skeins

In chapter 5.8 we have presented some construction methods for distributive squags. We are able to provide similar methods for nilpotent SQS-skeins:

THEOREM 6.5.1: *Let* $\mathfrak{V}_1 = \langle V;t^{(1)}\rangle$ *and* $\mathfrak{V}_2 = \langle V;t^{(2)}\rangle$ *be finite SQS-skeins having the following properties:*

1) $V = \mathrm{GF}(2)^m$ *for some* $m \geq 1$.

2) The operations $t^{(j)}$ *are given by:*

$$(t^{(j)}(x,y,z))_i = x_i + y_i + z_i + p_i^{(j)}(x,y,z)$$

where $j = 1,2$ *and* $i = 1,\ldots,m$.

3) For all $k = 1,\ldots,m$ *and* $j = 1,2$ *the following holds:*

If for some i $p_i^{(j)}(x,y,z)$ *depends on* z_k *then* $p_k^{(2-j)}(x,y,z) = 0$.

Then $\mathfrak{V} = \langle V;t\rangle$ *with*

$$(t(x,y,z))_i = x_i + y_i + z_i + p_i^{(1)}(x,y,z) + p_i^{(2)}(x,y,z)$$

is also an SQS-skein. Moreover, if both $\mathfrak{V}_1$ *and* $\mathfrak{V}_2$ *are boolean (semi-boolean) then* $\mathfrak{V}$ *is also boolean (semi-boolean).*

Proof: We have to show that $\mathfrak{V}$ satisfies the four defining equations of 6.1.1: Let x, y, $z \in V$ and $1 \leq i \leq m$. Then:

$$\begin{aligned}
(t(x,x,y))_i &= x_i + x_i + y_i + p_i^{(1)}(x,x,y) + p_i^{(2)}(x,x,y) \\
&= x_i + x_i + y_i + (x_i + x_i + y_i + p_i^{(1)}(x,x,y)) + (x_i + x_i + y_i + p_i^{(2)}(x,x,y)) \\
&= y_i + (t^{(1)}(x,x,y))_i + (t^{(2)}(x,x,y))_i \\
&= y_i + (y)_i + (y)_i \\
&= y_i
\end{aligned}$$

i.e. $t(x,x,y) = y$

Similarly we can prove $t(x,y,z) = t(x,z,y)$ and

$t(x,y,z) = t(y,z,x)$.

Note that for the proofs of these three equations we do not require condition 3.

For the proof of the remaining equation we define: $\mathbf{p}^{(j)}: V^3 \to V$ $(j = 1,2)$ to be the function given by: $(\mathbf{p}^{(j)}(x,y,z))_i = p_i^{(j)}(x,y,z)$. Note that condition 3 implies that for all $x,y,z,u,v,w \in V$ and $j = 1,2$:

$$\mathbf{p}^{(j)}\Big(x,y,z+\mathbf{p}^{(2-j)}(u,v,w)\Big) \;=\; \mathbf{p}^{(j)}(x,y,z)$$

Then we get: $t(x,y,t(x,y,z)) = t\Big(x,y,x+y+z+\mathbf{p}^{(1)}(x,y,z)+\mathbf{p}^{(2)}(x,y,z)\Big)$

$$= \left\{ \begin{array}{l} x+y+x+y+z+\mathbf{p}^{(1)}(x,y,z)+\mathbf{p}^{(2)}(x,y,z) \\ +\,\mathbf{p}^{(1)}\Big(x,y,x+y+z+\mathbf{p}^{(1)}(x,y,z)+\mathbf{p}^{(2)}(x,y,z)\Big) \\ +\mathbf{p}^{(2)}\Big(x,y,x+y+z+\mathbf{p}^{(1)}(x,y,z)+\mathbf{p}^{(2)}(x,y,z)\Big) \end{array} \right\}$$

$$= \left\{ \begin{array}{l} x+y+x+y+z+\mathbf{p}^{(1)}(x,y,z)+\mathbf{p}^{(2)}(x,y,z) \\ +\,\mathbf{p}^{(1)}\Big(x,y,x+y+z+\mathbf{p}^{(1)}(x,y,z)\Big)+\mathbf{p}^{(2)}\Big(x,y,x+y+z+\mathbf{p}^{(2)}(x,y,z)\Big) \end{array} \right\}$$

$$= z + \left\{ \begin{array}{l} x+y+x+y+z+\mathbf{p}^{(1)}(x,y,z)+\mathbf{p}^{(1)}\Big(x,y,x+y+z+\mathbf{p}^{(1)}(x,y,z)\Big) \\ +\,x+y+x+y+z+\mathbf{p}^{(2)}(x,y,z)+\mathbf{p}^{(2)}\Big(x,y,x+y+z+\mathbf{p}^{(2)}(x,y,z)\Big) \end{array} \right\}$$

$$= z+t^{(1)}\Big(x,y,x+y+z+\mathbf{p}^{(1)}(x,y,z)\Big)+t^{(2)}\Big(x,y,x+y+z+\mathbf{p}^{(2)}(x,y,z)\Big)$$

$$= z+t^{(1)}\Big(x,y,t^{(1)}(x,y,z)\Big)+t^{(2)}\Big(x,y,t^{(2)}(x,y,z)\Big)$$

$$= z+z+z \;=\; z$$

i.e. we have shown that $\mathfrak{V} = \langle V;t\rangle$ is indeed an SQS-skein. We can show similarly to the proof of the last equation, that $\mathfrak{V}$ is boolean or semi-boolean provided both $\mathfrak{V}_1$ and $\mathfrak{V}_2$ are boolean or semi-boolean respectively. □

Note that the operation t defined in 6.5.1 can also be given as:

$$t(x,y,z) \;=\; x + y + z + t^{(1)}(x,y,z) - t^{(2)}(x,y,z)$$

The main part of the next construction theorem is in fact a corollary of the last theorem. This is the analogue to theorem 5.8.2 for distributive squags.

THEOREM 6.5.2 *For each* $j \in \{1,2\}$ *let* V_j *be an* m_j*-dimensional vector space over* GF(2) *and let* $\langle V_j;t^{(j)}\rangle$ *be a subdirectly irreducible SQS-skein of nilpotence class* k_j *such that*

$$t^{(j)}(x,y,z) = x_i + y_i + z_i + p_i^{(j)}(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$$

for $i = 1,\ldots,m_j$ *where the* $p_i^{(j)}$ *are polynomials over* GF(2).

Then $\langle V;t\rangle$ *is a subdirectly irreducible SQS-skein of nilpotence class* $\max\{k_1,k_2\}$ *where* V *is an* m_1+m_2-1 *dimensional vector space over* GF(2) *and the ternary operation* t *is defined by*

$$(t(x,y,z))_i = \begin{cases} \left(t^{(1)}\left(\begin{pmatrix} x_1 \\ \vdots \\ x_{m_1-1} \\ x_{m_1+m_2-1}\end{pmatrix},\begin{pmatrix} y_1 \\ \vdots \\ y_{m_1-1} \\ y_{m_1+m_2-1}\end{pmatrix},\begin{pmatrix} z_1 \\ \vdots \\ z_{m_1-1} \\ z_{m_1+m_2-1}\end{pmatrix}\right)\right)_i & \text{if } 1 \le i \le m_1-1 \\ \left(t^{(2)}\left(\begin{pmatrix} x_{m_1} \\ \vdots \\ x_{m_1+m_2-1}\end{pmatrix},\begin{pmatrix} y_{m_1} \\ \vdots \\ y_{m_1+m_2-1}\end{pmatrix},\begin{pmatrix} z_{m_1} \\ \vdots \\ z_{m_1+m_2-1}\end{pmatrix}\right)\right)_{i-m_1+1} & \text{if } m_1 \le i \le m_1+m_2-2 \\ \begin{pmatrix} x_i+y_i+z_i \\ +\left(t^{(1)}\left(\begin{pmatrix} x_1 \\ \vdots \\ x_{m_1-1} \\ x_{m_1+m_2-1}\end{pmatrix},\begin{pmatrix} y_1 \\ \vdots \\ y_{m_1-1} \\ y_{m_1+m_2-1}\end{pmatrix},\begin{pmatrix} z_1 \\ \vdots \\ z_{m_1-1} \\ z_{m_1+m_2-1}\end{pmatrix}\right)\right)_{m_1} \\ -\left(t^{(2)}\left(\begin{pmatrix} x_{m_1} \\ \vdots \\ x_{m_1+m_2-1}\end{pmatrix},\begin{pmatrix} y_{m_1} \\ \vdots \\ y_{m_1+m_2-1}\end{pmatrix},\begin{pmatrix} z_{m_1} \\ \vdots \\ z_{m_1+m_2-1}\end{pmatrix}\right)\right)_{m_2} \end{pmatrix} & \text{if } i = m_1+m_2-1 \end{cases}$$

Proof: The fact that $\langle V;t\rangle$ is an SQS-skein follows immediately from theorem 6.5.1 with $\mathfrak{V}_j$ isomorphic to the direct product of $\langle V_j;t_j\rangle$ with the boolean SQS-skein $B_{m(2-j)-1}$.

By theorem 6.4.5 $\langle V;t\rangle$ is nilpotent. It is easy to see that $\langle\{x \in V \mid \forall i\ (i < m_1 \Rightarrow x_i = 0)\};t\rangle$ and $\langle\{x \in V \mid \forall i\ (m_1 \le i < m_1+m_2-1 \Rightarrow x_i = 0)\};t\rangle$ are subalgebras of $\langle V;t\rangle$. Moreover, these algebras are obviously isomorphic to $\langle V_1;t_1\rangle$ and $\langle V_2;t_2\rangle$ respectively. Therefore $\langle V;t\rangle$ contains subalgebras that are nilpotent of class k_1 and k_2, it must therefore be nilpotent of class at least $\max\{k_1, k_2\}$. By corollary 3.2.6, the algebras

$$\langle V_1,t_1\rangle \Big/ \zeta\Big(\langle V_1,t_1\rangle\Big) \quad \text{and} \quad \langle V_2,t_2\rangle \Big/ \zeta\Big(\langle V_2,t_2\rangle\Big)$$

are nilpotent of class k_1-1 and k_2-1 respectively. Their direct product is therefore of nilpotence class $\max\{k_1, k_2\}-1$. As a consequence of corollary 6.4.4 it is isomorphic to the image of the projection $\pi_{m_1+m_2-2}$ onto the first m_1+m_2-2 components of $\langle V;t\rangle$. $\pi_{m_1+m_2-2}$ is obviously a homomorphism with the property that the classes of its kernel have 2 elements each. By lemma 3.2.9 this implies $\zeta(\langle V;t\rangle) \supseteq \ker(\pi_{m_1+m_2-2})$. Therefore $\langle V;t\rangle$ is indeed nilpotent of class $\max\{k_1, k_2\}$.

By corollary 6.4.3, if $\zeta(\langle V;t\rangle) = \ker(\pi_{m_1+m_2-2})$ then $\langle V;t\rangle$ is subdirectly irreducible, and this proof is complete. We will now prove that $\zeta(\langle V;t\rangle) \subseteq \ker(\pi_{m_1+m_2-2})$.

Suppose $w \in [\mathbf{0}]\zeta(\langle V;t\rangle)$ where $\mathbf{0} = (0,\ldots,0)$. Let

$$w^{(1)} = \begin{pmatrix} w_1 \\ \vdots \\ w_{m_1-1} \\ w_{m_1+m_2-1} \end{pmatrix} \quad \text{and} \quad w^{(2)} = \begin{pmatrix} w_{m_1} \\ \vdots \\ w_{m_1+m_2-2} \\ w_{m_1+m_2-1} \end{pmatrix}$$

Then $w^{(j)} \in [\mathbf{0}]\zeta(\langle V_j;t^{(j)}\rangle)$. We will show this fact for $j = 2$. The proof for $j = 1$ is nearly identical. By lemma 6.3.3 it is sufficient to verify that for all $c^{(1)}, c^{(2)}, c^{(3)} \in V_2$ the following equation holds:

$$t^{(2)}(t^{(2)}(\mathbf{0},w^{(2)},c^{(1)}),c^{(2)},c^{(3)}) \quad = \quad t^{(2)}(\mathbf{0},w^{(2)},t^{(2)}(c^{(1)},c^{(2)},c^{(3)})) \qquad \textbf{(6.5.3)}$$

For $l \in \{1,2,3\}$ let $\mathbf{c}^{(l)} \in V$ be defined by $(\mathbf{c}^{(l)})_i = \begin{cases} 0 & \text{if } i < m_1 \\ (c^{(l)})_{i-m_1+1} & \text{if } i \geq m_1 \end{cases}$.

Since $w \in [\mathbf{0}]\zeta(\langle V;t\rangle)$, by lemma 6.3.3 the following equation is satisfied:

$$t(t(\mathbf{0},w,\mathbf{c}^{(1)}),\mathbf{c}^{(2)},\mathbf{c}^{(3)}) \quad = \quad t(\mathbf{0},w,t(\mathbf{c}^{(1)},\mathbf{c}^{(2)},\mathbf{c}^{(3)})) \qquad \textbf{(6.5.4)}$$

We observe that for $1 \leq i < m_2$ obviously

$$(t(t(\mathbf{0},w,\mathbf{c}^{(1)}),\mathbf{c}^{(2)},\mathbf{c}^{(3)}))_{i+m_1-1} \quad = \quad (t^{(2)}(t^{(2)}(\mathbf{0},w^{(2)},c^{(1)}),c^{(2)},c^{(3)}))_i$$

$$(t(\mathbf{0},w,t(\mathbf{c}^{(1)},\mathbf{c}^{(2)},\mathbf{c}^{(3)})))_{i+m_1-1} \quad = \quad (t^{(2)}(\mathbf{0},w^{(2)},t^{(2)}(c^{(1)},c^{(2)},c^{(3)})))_i$$

i.e. 6.5.4 implies 6.5.3 for all but possibly the last component. Let us now consider this last component. We have for $1 \leq i < m_j$ $(j \in \{1,2\})$:

$$\left(t^{(j)}\left(\begin{pmatrix}0\\\vdots\\0\\a\end{pmatrix},\begin{pmatrix}x_1\\\vdots\\x_{m_j}\end{pmatrix},\begin{pmatrix}0\\\vdots\\0\\b\end{pmatrix}\right)\right)_i = 0+x_i+0+p_i^{(j)}(0,\ldots,0,x_1,\ldots,x_{i-1},0,\ldots,0)$$

$$= \left(t^{(j)}\left(\mathbf{0},\begin{pmatrix}x_1\\\vdots\\x_{m_j}\end{pmatrix},\mathbf{0}\right)\right)_i = x_i \qquad \textbf{(6.5.5)}$$

and

$$\left(t^{(j)}\left(\begin{pmatrix}0\\\vdots\\0\\a\end{pmatrix},\begin{pmatrix}x_1\\\vdots\\x_{m_j}\end{pmatrix},\begin{pmatrix}0\\\vdots\\0\\b\end{pmatrix}\right)\right)_{m_j} = a+x_{m_j}+b+p_{m_j}^{(j)}(0,\ldots,0,x_j,\ldots,x_{m_j-j},0,\ldots,0)$$

$$= a+b+\left(t^{(j)}\left(\mathbf{0},\begin{pmatrix}x_1\\\vdots\\x_{m_j}\end{pmatrix},\mathbf{0}\right)\right)_{m_j} = a+b+x_{m_j}$$

6.5.5 implies that for $1 \leq i < m_1$ $(t(\mathbf{c}^{(1)},\mathbf{c}^{(2)},\mathbf{c}^{(3)}))_i = 0$ and $(t(\mathbf{0},w,\mathbf{c}^{(1)}))_i = w_i$.

Moreover for $m_1 \le i \le m_1+m_2-1$:

$$\left(t(\mathbf{0},w,\mathbf{c}^{(1)})\right)_i = \left\{ \begin{array}{ll} \left(t^{(2)}\left(\mathbf{0},w^{(2)},c^{(1)}\right)\right)_{i-m_1+1} & \text{if } m_1 \le i < m_1+m_2-1 \\ \left(\begin{array}{c} w_i+c^{(1)}_{m_2} \\ +\left(t^{(1)}\left(\mathbf{0},w^{(1)},\begin{pmatrix}0\\ \vdots \\ 0 \\ c^{(1)}_{m_2}\end{pmatrix}\right)\right)_{m_1} \\ -\left(t^{(2)}\left(\mathbf{0},w^{(2)},c^{(1)}\right)\right)_{m_2} \end{array} \right) & \text{if } i=m_1+m_2-1 \end{array} \right\}$$

$$= \left\{ \begin{array}{ll} \left(t^{(2)}\left(\mathbf{0},w^{(2)},c^{(1)}\right)\right)_{i-m_1+1} & \text{if } m_1 \le i < m_1+m_2-1 \\ w_i+w^{(1)}_{m_1}+\left(t^{(2)}\left(\mathbf{0},w^{(2)},c^{(1)}\right)\right)_{m_2} & \text{if } i=m_1+m_2-1 \end{array} \right\}$$

$$= \left(t^{(2)}\left(\mathbf{0},w^{(2)},c^{(1)}\right)\right)_{i-m_1+1}$$

and

$$\left(t(\mathbf{c}^{(1)},\mathbf{c}^{(2)},\mathbf{c}^{(3)})\right)_i = \left\{ \begin{array}{ll} \left(t^{(2)}\left(c^{(1)},c^{(2)},c^{(3)}\right)\right)_{i-m_1+1} & \text{if } m_1 \le i < m_1+m_2-1 \\ \left(\begin{array}{c} c^{(1)}_{m_2}+c^{(2)}_{m_2}+c^{(3)}_{m_2} \\ +\left(t^{(1)}\left(\begin{pmatrix}0\\ \vdots \\ 0 \\ c^{(1)}_{m_2}\end{pmatrix},\begin{pmatrix}0\\ \vdots \\ 0 \\ c^{(2)}_{m_2}\end{pmatrix},\begin{pmatrix}0\\ \vdots \\ 0 \\ c^{(3)}_{m_2}\end{pmatrix}\right)\right)_{m_1} \\ -\left(t^{(2)}\left(c^{(1)},c^{(2)},c^{(3)}\right)\right)_{m_2} \end{array} \right) & \text{if } i=m_1+m_2-1 \end{array} \right\}$$

$$= \left(t^{(2)}\left(c^{(1)},c^{(2)},c^{(3)}\right)\right)_{i-m_1+1}$$

We can now calculate:

$$\left(t\left(\mathbf{0},w,t\left(\mathbf{c}^{(1)},\mathbf{c}^{(2)},\mathbf{c}^{(3)}\right)\right)\right)_{m_1+m_2-1}$$

$$=\left\{\begin{array}{c}\left(t(\mathbf{c}^{(1)},\mathbf{c}^{(2)},\mathbf{c}^{(3)})\right)_{m_1+m_2-1}+w_{m_1+m_2-1}+\left(t^{(2)}\left(\mathbf{0},w^{(2)},\begin{pmatrix}\left(t(\mathbf{c}^{(1)},\mathbf{c}^{(2)},\mathbf{c}^{(3)})\right)_{m_1}\\ \vdots \\ \left(t(\mathbf{c}^{(1)},\mathbf{c}^{(2)},\mathbf{c}^{(3)})\right)_{m_1+m_2-1}\end{pmatrix}\right)\right)_{m_2}\\ +\left(t^{(1)}\left(\mathbf{0},w^{(1)},\begin{pmatrix}0\\ \vdots \\ 0\\ \left(t(\mathbf{c}^{(1)},\mathbf{c}^{(2)},\mathbf{c}^{(3)})\right)_{m_1+m_2-1}\end{pmatrix}\right)\right)_{m_1}\end{array}\right\}$$

$$=\left\{\begin{array}{c}\left(t^{(2)}(c^{(1)},c^{(2)},c^{(3)})\right)_{m_2}+w_{m_1+m_2-1}+\left(t^{(2)}\left(\mathbf{0},w^{(2)},t^{(2)}(c^{(1)},c^{(2)},c^{(3)})\right)\right)_{m_2}\\ +\left(t^{(2)}(c^{(1)},c^{(2)},c^{(3)})\right)_{m_2}+w^{(1)}_{m_1}\end{array}\right\}$$

$$=\left(t^{(2)}\left(\mathbf{0},w^{(2)},t^{(2)}(c^{(1)},c^{(2)},c^{(3)})\right)\right)_{m_2}$$

and

$$\left(t\left(t(\mathbf{0},w,\mathbf{c}^{(1)}),\mathbf{c}^{(2)},\mathbf{c}^{(3)}\right)\right)_{m_1+m_2-1}$$

$$=\left\{\begin{array}{c}\left(t(\mathbf{0},w,\mathbf{c}^{(1)})\right)_{m_1+m_2-1}+c^{(2)}_{m_2}+c^{(3)}_{m_2}+\left(t^{(2)}\left(\begin{pmatrix}\left(t(\mathbf{0},w,\mathbf{c}^{(1)})\right)_{m_1}\\ \vdots \\ \left(t(\mathbf{0},w,\mathbf{c}^{(1)})\right)_{m_1+m_2-1}\end{pmatrix},c^{(2)},c^{(3)}\right)\right)_{m_2}\\ +\left(t^{(1)}\left(\begin{pmatrix}\left(t(\mathbf{0},w,\mathbf{c}^{(1)})\right)_1\\ \vdots \\ \left(t(\mathbf{0},w,\mathbf{c}^{(1)})\right)_{m_1-1}\\ \left(t(\mathbf{0},w,\mathbf{c}^{(1)})\right)_{m_1+m_2-1}\end{pmatrix},\begin{pmatrix}0\\ \vdots \\ 0\\ c^{(2)}_{m_2}\end{pmatrix},\begin{pmatrix}0\\ \vdots \\ 0\\ c^{(3)}_{m_2}\end{pmatrix}\right)\right)_{m_1}\end{array}\right\}$$

$$= \left\{ \begin{array}{c} (t(\mathbf{0},w,\mathbf{c}^{(1)}))_{m_1+m_2-1} + c^{(2)}_{m_2} + c^{(3)}_{m_2} + \left(t^{(2)} \left(t^{(2)}(\mathbf{0},w^{(2)},c^{(1)}),c^{(2)},c^{(3)} \right) \right\|_{m_2} \\ + (t(\mathbf{0},w,\mathbf{c}^{(1)}))_{m_1+m_2-1} + c^{(2)}_{m_2} + c^{(3)}_{m_2} \end{array} \right\}$$

$$= \left(t^{(2)} \left(t^{(2)}(\mathbf{0},w^{(2)},c^{(1)}),c^{(2)},c^{(3)} \right) \right\|_{m_2}$$

i.e. $\left(t\left(\mathbf{0},w,t(\mathbf{c}^{(1)},\mathbf{c}^{(2)},\mathbf{c}^{(3)})\right) \right\|_{m_1+m_2-1} = \left(t^{(2)} \left(\mathbf{0},w^{(2)},t^{(2)}(c^{(1)},c^{(2)},c^{(3)}) \right) \right\|_{m_2}$

and $\left(t\left(t(\mathbf{0},w,\mathbf{c}^{(1)}),\mathbf{c}^{(2)},\mathbf{c}^{(3)} \right) \right\|_{m_1+m_2-1} = \left(t^{(2)} \left(t^{(2)}(\mathbf{0},w^{(2)},c^{(1)}),c^{(2)},c^{(3)} \right) \right\|_{m_2}$

Therefore by 6.5.4 we may conclude 6.5.3, i.e. $w^{(2)} \in [\mathbf{0}]\zeta(\langle V_2;t^{(2)}\rangle)$ and similarly $w^{(1)} \in [\mathbf{0}]\zeta(\langle V_1;t^{(1)}\rangle)$. Since by corollary 6.4.4 these two centers are the kernels of the projections onto the first $m_2 - 1$ and $m_1 - 1$ components resp., this implies that for all $i < m_1 + m_2 - 1 \;\; w_i = 0$. Therefore $w \in [\mathbf{0}]\ker(\pi_{m_1+m_2-2})$ which finally shows that $\zeta(\langle V;t\rangle) \subseteq \ker(\pi_{m_1+m_2-2})$.

By theorem 6.4.5 $\langle V;t\rangle$ is nilpotent, therefore $2 \leq |[\mathbf{0}]\zeta(\langle V;t\rangle)| \leq |[\mathbf{0}]\ker(\pi_{m_1+m_2-2})| = 2$. This implies $\zeta(\langle V;t\rangle) = \ker(\pi_{m_1+m_2-2})$. □

Before we present an analogue to the construction theorem 5.8.1, we will prove a lemma necessary for the proofs in the remainder of this section:

LEMMA 6.5.6 *Let W be an m-dimensional vector space over* GF(2) *with $m > 1$ and let*

$$s(x,y,z) \;=\; x_i + y_i + z_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$$

for $i = 1,\ldots,m$ where all the p_i are polynomials over GF(2). *If $\langle W;s\rangle$ is an SQS-skein then the following statements hold:*

a) for all $i \in \{1,\ldots,m\}$ and all $a_1,\ldots,a_{i-1},x_1,\ldots,x_{i-1} \in$ GF(2):

$$p_i(a_1,\ldots,a_{i-1},a_1,\ldots,a_{i-1},x_1,\ldots,x_{i-1}) = 0.$$

b) *for all* $i \in \{1,\ldots,m\}$, *all* $j \in \{1,\ldots,i\}$ *and all* $a_1,\ldots,a_{j-1},a_{j+1},\ldots,a_{i-1}$, $x,y,z \in$ GF(2):

$$p_i(a_1,\ldots,a_{j-1},x,a_{j+1},\ldots,a_{i-1},a_1,\ldots,a_{j-1},y,a_{j+1},\ldots,a_{i-1},$$
$$a_1,\ldots,a_{j-1},z,a_{j+1},\ldots,a_{i-1}) = 0.$$

Proof: Part (a) of this lemma follows immediately from the identity $s(x,x,z) = z$. Part (b) is obvious if we observe that

$$\left|\left\langle \begin{pmatrix} a_1 \\ \vdots \\ a_{j-1} \\ x \\ a_{j+1} \\ \vdots \\ a_m \end{pmatrix}, \begin{pmatrix} a_1 \\ \vdots \\ a_{j-1} \\ y \\ a_{j+1} \\ \vdots \\ a_m \end{pmatrix}, \begin{pmatrix} a_1 \\ \vdots \\ a_{j-1} \\ z \\ a_{j+1} \\ \vdots \\ a_m \end{pmatrix} \right\rangle\right| = 2$$

and therefore

$$s\left(\begin{pmatrix} a_1 \\ \vdots \\ a_{j-1} \\ x \\ a_{j+1} \\ \vdots \\ a_m \end{pmatrix}, \begin{pmatrix} a_1 \\ \vdots \\ a_{j-1} \\ y \\ a_{j+1} \\ \vdots \\ a_m \end{pmatrix}, \begin{pmatrix} a_1 \\ \vdots \\ a_{j-1} \\ z \\ a_{j+1} \\ \vdots \\ a_m \end{pmatrix}\right) \in \left\langle \begin{pmatrix} a_1 \\ \vdots \\ a_{j-1} \\ x \\ a_{j+1} \\ \vdots \\ a_m \end{pmatrix}, \begin{pmatrix} a_1 \\ \vdots \\ a_{j-1} \\ y \\ a_{j+1} \\ \vdots \\ a_m \end{pmatrix}, \begin{pmatrix} a_1 \\ \vdots \\ a_{j-1} \\ z \\ a_{j+1} \\ \vdots \\ a_m \end{pmatrix} \right\rangle$$

□

THEOREM 6.5.7 *Let* W *be an* m*-dimensional vector space over* GF(2) *with* $m > 1$ *and let* $\langle W;s\rangle$ *be a subdirectly irreducible SQS-skein of nilpotence class* $k > 1$ *such that*

$$s(x,y,z) = x_i + y_i + z_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$$

for $i = 1,\ldots,m$ *where all the* p_i *are polynomials over* GF(2). *If* V *is an* $m+2$ *dimensional vector space over* GF(2) *and if* t *is the ternary operation given by*

$$\big(t(x,y,z)\big)_i = \begin{cases} x_i+y_i+z_i & \text{if } 1\le i\le 2 \\ \left(s\left(\begin{pmatrix} x_3 \\ \vdots \\ x_{m+2}\end{pmatrix},\begin{pmatrix} y_3 \\ \vdots \\ y_{m+2}\end{pmatrix},\begin{pmatrix} z_3 \\ \vdots \\ z_{m+2}\end{pmatrix}\right)\right)_{i-2} & \text{if } 3\le i\le m+1 \\ \left(\left(s\left(\begin{pmatrix} x_3 \\ \vdots \\ x_{m+2}\end{pmatrix},\begin{pmatrix} y_3 \\ \vdots \\ y_{m+2}\end{pmatrix},\begin{pmatrix} z_3 \\ \vdots \\ z_{m+2}\end{pmatrix}\right)\right)_m + \begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix}\right) & \text{if } i=m+2 \end{cases}$$

then $\langle V;t\rangle$ is a subdirectly irreducible SQS-skein of nilpotence class k.

The proof of this theorem is very similar to the proof of theorem 6.5.2. Since some of the details are quite different, we will present it nevertheless.

Proof: The fact that $\langle V;t\rangle$ is an SQS-skein follows from theorem 6.5.1 with $\mathfrak{V}_1$ isomorphic to the direct product of $\langle W;s\rangle$ with the boolean SQS-skein B_2 and $\mathfrak{V}_1$ isomorphic to the direct product of H_{16} with B_{m-1}. Theorem 6.5.1 is applicable in this case since by lemma 6.5.6 $p_1 = 0$.

By theorem 6.4.5 $\langle V;t\rangle$ is nilpotent. It is easy to see that $\langle\{x \in V \mid x_1 = x_2 = 0)\};t\rangle$ is a subalgebra of $\langle V;t\rangle$ isomorphic to $\langle W;s\rangle$. Therefore $\langle V;t\rangle$ must be nilpotent of class at least k. By corollary 3.2.6, the algebra $\langle W,s\rangle/\zeta(\langle W,s\rangle)$ is nilpotent of class $k-1 \ge 1$, i.e. its direct product with B_2 is also of nilpotence class $k-1$. Since by corollary 6.4.4 this direct product is isomorphic to the image of the projection onto the first $m+1$ components, we may conclude—as in the proof of the previous theorem—that $\langle V;t\rangle$ is nilpotent of class k.

It remains to be shown that $\langle V;t\rangle$ is subdirectly irreducible. As before it is sufficient to prove that $\zeta(\langle V;t\rangle) \subseteq \ker(\pi_{m+1})$.

Suppose $w \in [\mathbf{0}]\zeta(\langle V;t\rangle)$ where $\mathbf{0} = (0,\ldots,0)$. Let

$$\widetilde{w} = \begin{pmatrix} w_3 \\ \vdots \\ w_{m+2} \end{pmatrix} \in W$$

We will prove that $\widetilde{w} \in [\mathbf{0}]\zeta(\langle W;s\rangle)$. By lemma 6.3.3 it is sufficient to verify that for all $c^{(1)}, c^{(2)}, c^{(3)} \in W$ the following equation holds:

$$s(s(\mathbf{0},\widetilde{w},c^{(1)}),c^{(2)},c^{(3)}) \quad = \quad s(\mathbf{0},\widetilde{w},s(c^{(1)},c^{(2)},c^{(3)})) \qquad \textbf{(6.5.8)}$$

For $l \in \{1,2,3\}$ let $\mathbf{c}^{(l)} \in V$ be defined by $(\mathbf{c}^{(l)})_i = \begin{cases} 0 & \text{if } i \le 2 \\ (c^{(l)})_{i-2} & \text{if } i < 2 \end{cases}$.

Since $w \in [\mathbf{0}]\zeta(\langle V;t\rangle)$, by lemma 6.3.3 the following equation is satisfied:

$$t(t(\mathbf{0},w,\mathbf{c}^{(1)}),\mathbf{c}^{(2)},\mathbf{c}^{(3)}) \quad = \quad t(\mathbf{0},w,t(\mathbf{c}^{(1)},\mathbf{c}^{(2)},\mathbf{c}^{(3)})) \qquad \textbf{(6.5.9)}$$

We will first evaluate $t(\mathbf{0},w,\mathbf{c}^{(1)})$ and $t(\mathbf{c}^{(1)},\mathbf{c}^{(2)},\mathbf{c}^{(3)})$ and both sides of 6.5.9:

$$\left(t(\mathbf{0},w,\mathbf{c}^{(1)})\right)_i = \begin{cases} w_i & \text{if } i \le 2 \\ \left(s(\mathbf{0},\widetilde{w},c^{(1)})\right)_{i-2} & \text{if } 3 \le i \le m+2 \end{cases}$$

$$\left(t\left(t(\mathbf{0},w,\mathbf{c}^{(1)}),\mathbf{c}^{(2)},\mathbf{c}^{(3)}\right)\right)_i = \begin{cases} w_i & \text{if } i \le 2 \\ \left(s\left(s(\mathbf{0},\widetilde{w},c^{(1)}),c^{(2)},c^{(3)}\right)\right)_{i-2} & \text{if } 3 \le i < m+2 \\ \left(s\left(s(\mathbf{0},\widetilde{w},c^{(1)}),c^{(2)},c^{(3)}\right)\right)_m + \begin{vmatrix} w_1 & 0 & 0 \\ w_2 & 0 & 0 \\ ? & c_1^{(2)} & c_1^{(3)} \end{vmatrix} & \text{if } i = m+2 \end{cases}$$

$$= \begin{cases} w_i & \text{if } i \le 2 \\ \left(s\left(s(\mathbf{0},\widetilde{w},c^{(1)}),c^{(2)},c^{(3)}\right)\right)_{i-2} & \text{if } 3 \le i \le m+2 \end{cases}$$

$$\left(t(\mathbf{c}^{(1)},\mathbf{c}^{(2)},\mathbf{c}^{(3)})\right)_i = \begin{cases} 0 & \text{if } i \le 2 \\ \left(s(c^{(1)},c^{(2)},c^{(3)})\right)_{i-2} & \text{if } 3 \le i \le m+2 \end{cases}$$

$$\left(t\left(\mathbf{0},w,t(\mathbf{c}^{(1)},\mathbf{c}^{(2)},\mathbf{c}^{(3)})\right)\right)_i = \begin{cases} w_i & \text{if } i \le 2 \\ \left(s\left(\mathbf{0},\widetilde{w},s(c^{(1)},c^{(2)},c^{(3)})\right)\right)_{i-2} & \text{if } 3 \le i \le m+2 \end{cases}$$

These calculations show that 6.5.9 implies 6.5.8, i.e. $\widetilde{w} \in [\mathbf{0}]\zeta(\langle W;s\rangle)$. Since by corollary 6.4.4 $\zeta(\langle W;s\rangle)$ is the kernel of the projection onto the first m–1 components of W, we can conclude that for all $1 \le i \le m-1$ $\widetilde{w}_i = w_{i+2} = 0$.

By lemma 6.5.6 $p_i(x_1,0,\ldots,0,y_1,0,\ldots,0,z_1,0,\ldots,0) = 0$ for all i. Using this property and the fact that $w_i = 0$ for all $i \in \{3,\ldots,m+1\}$, it can similarly be shown that:

$$\begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ w_{m+2} \end{pmatrix} \in [\mathbf{0}]\zeta(H_{16})$$

i.e. $w_i = 0$ for all $i \in \{1,\ldots,m+1\}$. Therefore $w \in \ker(\pi_{m+1})$ — we have shown that $\zeta(\langle V;t\rangle) \subseteq \ker(\pi_{m+1})$. □

The last two theorems furnish tools that allow us to construct SQS-skeins within a given nilpotence class, i.e. to create a new SQS-skeins of nilpotence class k provided we already know an SQS-skein of this class. We will now turn to the question of building an SQS-skein of a higher class. The first answer to this question was given in (Armanious n.d.). Armanious constructed an SQS-skein of nilpotence class k from an SQS-skein of class k–1 by considering the Steiner quadruple system corresponding to the direct product of the latter SQS-skein with B_1 and rearranging an appropriate subsystem. The next theorem presents this construction using the easier accessible representation that we have developed in this section:

THEOREM 6.5.10 *Let $\langle W;s\rangle$ be an SQS-skein such that W is an m-dimensional vector space over* GF(2) *with $m \geq 3$ and*

$$s(x,y,z) = x_i + y_i + z_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1})$$

for $i = 1,\ldots,m$ where all the p_i are polynomials over GF(2). *Let $1 \leq j < m$. If V is an $m+1$ dimensional vector space over* GF(2) *and if t is the ternary operation given by*

$$\big(t(x,y,z)\big)_i = \begin{cases} \left(s\left(\begin{pmatrix}x_1\\\vdots\\x_m\end{pmatrix},\begin{pmatrix}y_1\\\vdots\\y_m\end{pmatrix},\begin{pmatrix}z_1\\\vdots\\z_m\end{pmatrix}\right)\right)_i & \text{if } 1\leq i\leq m \\ x_{m+1}+y_{m+1}+z_{m+1}+\begin{vmatrix}x_j & y_j & z_j\\ x_m & y_m & z_m\\ 1 & 1 & 1\end{vmatrix}\prod_{\substack{l=1\\l\neq j}}^{m-1}\left(x_l y_l z_l\right) & \text{if } i=m+1 \end{cases}$$

then $\langle V;t\rangle$ is an SQS-skein which is not semi-boolean. If $\langle W;s\rangle$ is subdirectly irreducible and of nilpotence class k, then $\langle V;t\rangle$ is also subdirectly irreducible, but of nilpotence class $k+1$.

Proof: It is immediately clear that in $\langle V;t\rangle$ the equations $t(x,x,y) = y$ and $t(x,y,z) = t(x,z,y) = t(y,z,x)$ hold. First we will show that $t(x,y,t(x,y,z)) = z$. Suppose π_m is the projection onto the first m components of V. Then for $1 \leq i \leq m$ we have:

$$(t(x,y,t(x,y,z)))_i = (s(\pi_m(x),\pi_m(y),s(\pi_m(x),\pi_m(y),\pi_m(z))))_i = (\pi_m(z))_i = z_i$$

Moreover:

$$\big(t(x,y,t(x,y,z))\big)_{m+1} = x_{m+1}+y_{m+1}+\big(t(x,y,z)\big)_{m+1}+\begin{vmatrix}x_j & y_j & \big(t(x,y,z)\big)_j\\ x_m & y_m & \big(t(x,y,z)\big)_m\\ 1 & 1 & 1\end{vmatrix}\prod_{\substack{l=1\\l\neq j}}^{m-1}\left(x_l y_l \big(t(x,y,z)\big)_l\right)$$

$$= \left(\begin{array}{l} z_{m+1} + \begin{vmatrix} x_j & y_j & z_j \\ x_m & y_m & z_m \\ 1 & 1 & 1 \end{vmatrix} \prod_{\substack{l=1 \\ l\neq j}}^{m-1} (x_l y_l z_l) \\ \\ + \begin{vmatrix} x_j & y_j & \left(x_j+y_j+z_j+p_j(x_1,\ldots,z_{j-1})\right) \\ x_m & y_m & \left(x_m+y_m+z_m+p_m(x_1,\ldots,z_{m-1})\right) \\ 1 & 1 & 1 \end{vmatrix} \prod_{\substack{l=1 \\ l\neq j}}^{m-1} \left(x_l y_l \left(x_l+y_l+z_l+p_l(x_1,\ldots,z_{l-1})\right)\right) \end{array} \right)$$

If $0 \in \{x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_{m-1},y_1,\ldots,y_{j-1},y_{j+1},\ldots,y_{m-1}\}$ then both products are zero, therefore $(t(x,y,t(x,y,z)))_{m+1} = z_{m+1}$. Now assume that $0 \notin \{x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_{m-1}, y_1,\ldots,y_{j-1},y_{j+1},\ldots,y_{m-1}\}$, i.e. $\{x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_{m-1},y_1,\ldots,y_{j-1},y_{j+1},\ldots,y_{m-1}\} = \{1\}$. Then by lemma 6.5.6 $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1}) = p_i(1,\ldots,1,z_1,\ldots,z_{i-1}) = 0$ for all $i \leq j$. This yields

$(t(x,y,t(x,y,z)))_{m+1} =$

$$\left(\begin{array}{l} z_{m+1} + \left(\begin{vmatrix} x_j & y_j & z_j \\ x_m & y_m & z_m \\ 1 & 1 & 1 \end{vmatrix} \prod_{\substack{l=1 \\ l\neq j}}^{m-1} z_l \right) + \begin{vmatrix} x_j & y_j & x_j+y_j+z_j \\ x_m & y_m & \left(x_m+y_m+z_m+p_m(x_1,\ldots,z_{m-1})\right) \\ 1 & 1 & 1 \end{vmatrix} \\ \\ \left(\prod_{l=1}^{j-1} z_l\right)\left(\prod_{l=j+1}^{m-1} \left(z_l+p_l(x_1,\ldots,z_{l-1})\right)\right) \end{array} \right)$$

If there exists an $i \in \{1,\ldots,j-1\}$ such that $z_i = 0$ then again we get $(t(x,y,t(x,y,z)))_{m+1} = z_{m+1}$ since the products $\prod_{l=1}^{j-1} z_l$ become 0.

Otherwise suppose that $z_i = 1$ for all $i \in \{1,\ldots,j-1\}$ and that there exists an $i \in \{j+1,\ldots,m-1\}$ such that $z_i = 0$. Let f denote the minimal such index i. Then by lemma 6.5.6:

$p_f(x_1,\ldots,x_{f-1},y_1,\ldots,y_{f-1},z_1,\ldots,z_{f-1}) = p_f(1,\ldots,1,x_j,1,\ldots,1,1,\ldots,1,y_j,1,\ldots,1,\ 1,\ldots,1) = 0$

and we get:

$$\prod_{\substack{l=1\\ l\neq j}}^{m-1} z_l = 0 \text{ and } \prod_{l=j+1}^{m-1} \left(z_l + p_l(x_1,\ldots,z_{l-1})\right) = 0$$

i.e. $(t(x,y,t(x,y,z)))_{m+1} = z_{m+1}$.

Finally we have to consider the case $z_i = 0$ for all $i \in \{1,\ldots,j-1,j+1,\ldots,m-1\}$. By lemma 6.5.6. we have for all $1 \le i \le m$

$p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1},z_1,\ldots,z_{i-1}) = p_i(1,\ldots,1,x_j,1,\ldots,1,1,\ldots,1,y_j,1,\ldots,1,\ 1,\ldots,1) = 0$

and therefore

$$\begin{aligned}\left(t(x,y,t(x,y,z))\right)_{m+1} &= z_{m+1} + \begin{vmatrix} x_j & y_j & z_j \\ x_m & y_m & z_m \\ 1 & 1 & 1 \end{vmatrix} + \begin{vmatrix} x_j & y_j & x_j+y_j+z_j \\ x_m & y_m & x_m+y_m+z_m \\ 1 & 1 & 1 \end{vmatrix} \\ &= z_{m+1} + \begin{vmatrix} x_j & y_j & z_j \\ x_m & y_m & z_m \\ 1 & 1 & 1 \end{vmatrix} + \begin{vmatrix} x_j & y_j & z_j \\ x_m & y_m & z_m \\ 1 & 1 & 1 \end{vmatrix} \\ &= z_{m+1}\end{aligned}$$

We have shown that $\langle V;t\rangle$ is indeed an SQS-skein.

Before we prove that $\langle V;t\rangle$ is not semi-boolean, we will evaluate an expression which we will have to use twice: **(6.5.11)**

$$t\left(t\left(\begin{pmatrix}0\\\vdots\\0\\0_j\\0\\\vdots\\0\\x_m\\x_{m+1}\end{pmatrix},\begin{pmatrix}0\\\vdots\\0\\0_j\\0\\\vdots\\0\\0\\0\end{pmatrix},\begin{pmatrix}1\\\vdots\\1\\0_j\\1\\\vdots\\1\\1\\0\end{pmatrix}\right),\begin{pmatrix}1\\\vdots\\1\\0_j\\1\\\vdots\\1\\1\\0\end{pmatrix},\begin{pmatrix}1\\\vdots\\1\\1_j\\1\\\vdots\\1\\1\\0\end{pmatrix}\right) = t\left(\begin{pmatrix}1\\\vdots\\1\\0_j\\1\\\vdots\\1\\x_m+1\\x_{m+1}\end{pmatrix},\begin{pmatrix}1\\\vdots\\1\\0_j\\1\\\vdots\\1\\1\\0\end{pmatrix},\begin{pmatrix}1\\\vdots\\1\\1_j\\1\\\vdots\\1\\1\\0\end{pmatrix}\right)$$

$$= t\left(\begin{pmatrix} 1 \\ \vdots \\ 1 \\ 0_j \\ 1 \\ \vdots \\ 1 \\ x_m+1 \\ x_{m+1} \end{pmatrix}, \begin{pmatrix} 1 \\ \vdots \\ 1 \\ 0_j \\ 1 \\ \vdots \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ \vdots \\ 1 \\ 1_j \\ 1 \\ \vdots \\ 1 \\ 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ \vdots \\ 1 \\ 1_j \\ 1 \\ \vdots \\ 1 \\ x_m+1 \\ x_{m+1}+\begin{vmatrix} 1 & 1\,0 \\ x_m+1 & 1\,1 \\ 1 & 1\,1 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \\ 1_j \\ 1 \\ \vdots \\ 1 \\ x_m+1 \\ x_{m+1}+x_m \end{pmatrix}$$

where the index j indicates the jth component.

Now consider the following elements:

$$x = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \end{pmatrix}, \mathbf{0} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ 0 \end{pmatrix}, z = \begin{pmatrix} 1 \\ \vdots \\ 1 \\ 1 \\ 0 \end{pmatrix} \text{ and } u = \begin{pmatrix} 1 \\ \vdots \\ 1 \\ 0_j \\ 1 \\ \vdots \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

By 6.5.11 we get $$t(t(x,u,\mathbf{0}),u,z) = \begin{pmatrix} 1 \\ \vdots \\ 1 \\ 0 \\ 1 \end{pmatrix}$$ but

$$(t(x,u,t(\mathbf{0},u,z)))_{m+1} = \left(t\left(x,u,\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1_j \\ ? \\ \vdots \\ ? \\ 0 \end{pmatrix}\right)\right)_{m+1} = 0$$

i.e. $$t(t(x,u,\mathbf{0}),u,z) \neq t(x,u,t(\mathbf{0},u,z))$$

this SQS-skein is not semi-boolean.

Now suppose $\langle W;s\rangle$ is subdirectly irreducible and of nilpotence class k. By theorem 6.4.5 $\langle V;t\rangle$ is nilpotent. Since the image under the projection onto the first m components is obviously isomorphic to $\langle W;s\rangle$ and the kernel of this projection is a minimal non-trivial congruence, we may conclude as before that $\langle V;t\rangle$ is nilpotent of class k or $k+1$ and $\zeta(\langle V;t\rangle) \supseteq \ker(\pi_{m+1})$.

Suppose $w \in [\mathbf{0}]\zeta(\langle V;t\rangle)$ where $\mathbf{0} = (0,\ldots,0)$. Let π_m be the projection onto the first m components of V. We will prove that $\pi_m(w) \in [\mathbf{0}]\zeta(\langle W;s\rangle)$. By lemma 6.3.3 it is sufficient to verify that for all $c^{(1)}, c^{(2)}, c^{(3)} \in W$ the following equation holds:

$$s(s(\mathbf{0},\pi_m(w),c^{(1)}),c^{(2)},c^{(3)}) \quad = \quad s(\mathbf{0},\pi_m(w),s(c^{(1)},c^{(2)},c^{(3)})) \qquad \textbf{(6.5.12)}$$

For $l \in \{1,2,3\}$ let $\mathbf{c}^{(l)} \in V$ be defined by $(\mathbf{c}^{(l)})_i = \begin{cases} (c^{(l)})_i & \text{if } i \le m \\ 0 & \text{if } i = m \end{cases}$.

Since $w \in [\mathbf{0}]\zeta(\langle V;t\rangle)$, by lemma 6.3.3 the following equation is satisfied:

$$t(t(\mathbf{0},w,\mathbf{c}^{(1)}),\mathbf{c}^{(2)},\mathbf{c}^{(3)}) \quad = \quad t(\mathbf{0},w,t(\mathbf{c}^{(1)},\mathbf{c}^{(2)},\mathbf{c}^{(3)}))$$

By application of the projection π_m on both sides of this equation, we immediately get 6.5.12, i.e. $\pi_m(w) \in [\mathbf{0}]\zeta(\langle W;s\rangle)$. Since by corollary 6.4.4 $\zeta(\langle W;s\rangle)$ is the kernel of the projection onto the first $m-1$ components of $\langle W;s\rangle$ we may conclude $w_i = 0$ for all $i = 1,\ldots,m-1$. By lemma 6.3.3 we have

$$t\left(t\left(\begin{pmatrix}0\\\vdots\\0\\0_j\\0\\\vdots\\0\\w_m\\w_{m+1}\end{pmatrix},\begin{pmatrix}0\\\vdots\\0\\0_j\\0\\\vdots\\0\\0\\0\end{pmatrix},\begin{pmatrix}1\\\vdots\\1\\0_j\\1\\\vdots\\1\\1\\0\end{pmatrix}\right),\begin{pmatrix}1\\\vdots\\1\\0_j\\1\\\vdots\\1\\1\\0\end{pmatrix},\begin{pmatrix}1\\\vdots\\1\\1_j\\1\\\vdots\\1\\1\\0\end{pmatrix}\right) = t\left(\begin{pmatrix}0\\\vdots\\0\\0_j\\0\\\vdots\\0\\w_m\\w_{m+1}\end{pmatrix},\begin{pmatrix}0\\\vdots\\0\\0_j\\0\\\vdots\\0\\0\\0\end{pmatrix},t\left(\begin{pmatrix}1\\\vdots\\1\\0_j\\1\\\vdots\\1\\1\\0\end{pmatrix},\begin{pmatrix}1\\\vdots\\1\\0_j\\1\\\vdots\\1\\1\\0\end{pmatrix},\begin{pmatrix}1\\\vdots\\1\\1_j\\1\\\vdots\\1\\1\\0\end{pmatrix}\right)\right)$$

The left hand side of this equation is just 6.5.11, and the right hand side can be evaluated easily. We obtain

$$\begin{pmatrix} 1 \\ \vdots \\ 1 \\ 1_j \\ 1 \\ \vdots \\ 1 \\ w_m+1 \\ w_{m+1}+w_m \end{pmatrix} = t\left(\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0_j \\ 0 \\ \vdots \\ 0 \\ w_m \\ w_{m+1} \end{pmatrix}, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0_j \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ \vdots \\ 1 \\ 1_j \\ 1 \\ \vdots \\ 1 \\ 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ \vdots \\ 1 \\ 1_j \\ 1 \\ \vdots \\ 1 \\ w_m+1 \\ w_{m+1} \end{pmatrix}$$

i.e. $w_m = 0$. Therefore $w \in \ker(\pi_{m+1})$, we have shown $\zeta(\langle V;t\rangle) = \ker(\pi_{m+1})$. By corollary 6.4.3 this implies that $\langle V;t\rangle$ is subdirectly irreducible, and by 3.2.6 that $\langle V;t\rangle$ is nilpotent of class k–1. □

Using these construction theorems we are able to construct SQS-skeins of nilpotence class k and size 2^n for all $k > 1$ and $n \geq k+2$. Note that corollary 6.2.8 already states that for every $n \geq 0$ there exists an SQS-skein of nilpotence class 1 and size 2^n, but this SQS-skein is only subdirectly irreducible if $n = 1$.

THEOREM 6.5.13: *For every $k > 1$ and every $n \geq k + 2$ there exists an subdirectly irreducible SQS-skein of size 2^n and nilpotence class k.*

Proof: Before we can proceed with the main part of this proof we have to construct an SQS-skein of nilpotence class 2 and size 2^5. Let $A_{32} = \langle A;q\rangle$ where $A = (\mathrm{GF}(2))^5$ and q is given by

$$q\left(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \end{pmatrix}, \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \end{pmatrix}\right) = \begin{pmatrix} x_1+y_1+z_1 \\ x_2+y_2+z_2 \\ x_3+y_3+z_3 \\ x_4+y_4+z_4 \\ x_5+y_5+z_5+x_2y_2z_2x_3y_3z_3\begin{vmatrix} x_1 & y_1 & z_1 \\ x_4 & y_4 & z_4 \\ 1 & 1 & 1 \end{vmatrix} \end{pmatrix}$$

It follows immediately from theorem 6.5.10 that A_{32} is an SQS-skein, created from B_4, that is not semi-boolean. By 6.4.5 it is nilpotent of class 1 or 2. Since it is not semi-

boolean, it cannot be of nilpotence class 1, i.e. it is of nilpotence class 2. Let π_4 be the projection onto the first four components. As before it is clear that $\ker(\pi_4) \subseteq \zeta(A_{32})$. We will show that in fact $\ker(\pi_4) = \zeta(A_{32})$. Suppose $w \in [\mathbf{0}]\zeta(A_{32})$ with $\mathbf{0} = (0,\ldots,0)$. By lemma 6.3.3 for all $c^{(j)} \in A$ with $j = 1,2,3$

$$q(q(\mathbf{0},w,c^{(1)}),c^{(2)},c^{(3)}) \quad = \quad q(\mathbf{0},w,q(c^{(1)},c^{(2)},c^{(3)})).$$

Evaluation of these expressions yields

$$\left(c_2^{(1)}+w_2\right)c_2^{(2)}c_2^{(3)}\left(c_3^{(1)}+w_3\right)c_3^{(2)}c_3^{(3)}\begin{vmatrix} c_1^{(1)}+w_1 & c_1^{(2)} & c_1^{(3)} \\ c_4^{(1)}+w_4 & c_4^{(2)} & c_4^{(3)} \\ 1 & 1 & 1 \end{vmatrix} \tag{6.5.14}$$

$$= c_2^{(1)}c_2^{(2)}c_2^{(3)}c_3^{(1)}c_3^{(2)}c_3^{(3)}\begin{vmatrix} c_1^{(1)} & c_1^{(2)} & c_1^{(3)} \\ c_4^{(1)} & c_4^{(2)} & c_4^{(3)} \\ 1 & 1 & 1 \end{vmatrix}$$

Choosing $c_2^{(2)}=c_2^{(3)}=c_3^{(2)}=c_3^{(3)}=1$ & $c_2^{(1)}=c_3^{(1)}=0$ shows that

$$w_2\,w_3\begin{vmatrix} c_1^{(1)}+w_1 & c_1^{(2)} & c_1^{(3)} \\ c_4^{(1)}+w_4 & c_4^{(2)} & c_4^{(3)} \\ 1 & 1 & 1 \end{vmatrix} = 0$$

for all remaining choices of $c^{(j)}$, i.e. $w_2\,w_3 = 0$. If we change our selection to $c_3^{(1)}=1$ we obtain instead

$$w_2\left(w_3+1\right)\begin{vmatrix} c_1^{(1)}+w_1 & c_1^{(2)} & c_1^{(3)} \\ c_4^{(1)}+w_4 & c_4^{(2)} & c_4^{(3)} \\ 1 & 1 & 1 \end{vmatrix} = 0$$

for all remaining choices of $c^{(j)}$, i.e. $w_2\,(w_3 + 1) = 0$. This implies $w_2 = 0$. Similarly we can deduce $w_3 = 0$. If we now choose $c_2^{(1)}=c_2^{(2)}=c_2^{(3)}=c_3^{(1)}=c_3^{(2)}=c_3^{(3)}=1$ then 6.5.14 yields

$$\begin{vmatrix} w_1 & c_1^{(2)} & c_1^{(3)} \\ w_4 & c_4^{(2)} & c_4^{(3)} \\ 0 & 1 & 1 \end{vmatrix} = 0$$

for all remaining choices of $c^{(j)}$, i.e. $w_1 = w_4 = 0$. This implies $w \in \ker(\pi_4)$. We have shown $\ker(\pi_4) = \zeta(A_{32})$. By corollary 6.4.3 A_{32} is subdirectly irreducible. We are now ready to proceed with the main part of the proof.

Let $k \geq 2$, $n \geq k+2 \geq 4$ and $m = n-(k-2)$. Then $m \geq 4$.

We note first that A_{16} and A_{32} are subdirectly irreducible SQS-skeins of nilpotence class 2 and of size 2^4 and 2^5 respectively. If m is even we apply the construction theorem 6.5.7 $\frac{m-4}{2}$ times to A_{16} and obtain an subdirectly irreducible SQS-skein of nilpotence class 2 and size 2^m. If m is odd we can construct a subdirectly irreducible SQS-skein of nilpotence class 2 and size 2^m by applying the same theorem $\frac{m-5}{2}$ times to A_{32}. Therefore for any $m = n-(k-2)$ there exists an subdirectly irreducible SQS-skein $\mathfrak{Z}_m$ of nilpotence class 2 and size 2^m.

Starting with $\mathfrak{Z}_m$ and applying theorem 6.5.10 $(k-2)$ times we have finally constructed a subdirectly irreducible SQS-skein of nilpotence class $2+(k-2) = k$ and size $2^{m+(k-2)} = 2^{n-(k-2)+(k-2)} = 2^n$. □

6.6. Examples

In this section we will investigate several examples of SQS-skeins. In all of these examples, given an SQS-skein $\langle V;q\rangle$ where V is an vectorspace over GF(2), $e_j \in V$ shall denote the element given by $(e_j)_i = \delta_{ji}$ for $j = 0,1,2,\ldots$ and $i = 1,2,\ldots$. Note that $e_0 = \mathbf{0} = (0,\ldots,0)$.

In the previous sections we have already discussed the SQS-skeins B_n, H_{16}, A_{16}, and A_{32}. We will now complete their investigation.

EXAMPLE 6.6.1: *Let n be any positive integer. Let B_n be the algebra $\langle B;q\rangle$ given by $B = (\mathrm{GF}(2))^n$ and*

$$(q(x,y,z))_i \quad = \quad x_i + y_i + z_i \qquad \text{for all } i = 1,\ldots,n$$

Then B_n is an SQS-skein of nilpotence class 1, which is generated by the $n+1$ elements $e_0, e_1, e_2,\ldots, e_n$. B_n is subdirectly irreducible if and only if $n = 1$.

Proof: The properties of B_n follow immediately from theorem 6.2.5, lemma 6.4.10 and corollary 6.4.3, since $\zeta(B_n) = \iota_{B_n}$. □

EXAMPLE 6.6.2: *Let H_{16} be the algebra $\langle H;q\rangle$ given by $H = (\mathrm{GF}(2))^4$ and*

$$q\left(\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix},\begin{pmatrix}y_1\\y_2\\y_3\\y_4\end{pmatrix},\begin{pmatrix}z_1\\z_2\\z_3\\z_4\end{pmatrix}\right) = \begin{pmatrix} x_1+y_1+z_1 \\ x_2+y_2+z_2 \\ x_3+y_3+z_3 \\ x_4+y_4+z_4+\begin{vmatrix}x_1 & y_1 & z_1\\ x_2 & y_2 & z_2\\ x_3 & y_3 & z_3\end{vmatrix}\end{pmatrix}$$

Then H_{16} is a semi-boolean, subdirectly irreducible SQS-skein of nilpotence class 2, which is generated by the four elements e_0, e_1, e_2, and e_3.

Proof: We have already seen in 6.2. and 6.3. that H_{16} is a semi-boolean SQS-skein of nilpotence class 2 with $\zeta(H_{16}) = \ker(\pi_3)$ where π_3 is the projection onto the first 3 components. By corollary 6.4.3 H_{16} is subdirectly irreducible. By lemma 6.4.10 H_{16} is generated by the 5 elements e_0, e_1, e_2, e_3, and e_4. It remains to be verified that in fact $e_4 \in [\{e_0, e_1, e_2, e_3\}]_{H_{16}}$. This is true since $q(q(e_1,e_0,q(e_2,e_0,e_3)),e_0,q(e_1,e_2,e_3)) =$

$$q\left(q\left(e_1,e_0,\begin{pmatrix}0\\1\\1\\0\end{pmatrix}\right),e_0,q(e_1,e_2,e_3)\right) = q\left(\begin{pmatrix}1\\1\\1\\0\end{pmatrix},e_0,\begin{pmatrix}1\\1\\1\\1\end{pmatrix}\right) = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = e_4$$

□

EXAMPLE 6.6.3: *Let A_{16} be the algebra $\langle A;q\rangle$ given by $A = (\mathrm{GF}(2))^4$ and*

$$q\left(\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix},\begin{pmatrix}y_1\\y_2\\y_3\\y_4\end{pmatrix},\begin{pmatrix}z_1\\z_2\\z_3\\z_4\end{pmatrix}\right)=\begin{pmatrix}x_1+y_1+z_1\\x_2+y_2+z_2\\x_3+y_3+z_3\\x_4+y_4+z_4+x_1y_1z_1\begin{vmatrix}x_2&y_2&z_2\\x_3&y_3&z_3\\1&1&1\end{vmatrix}\end{pmatrix}$$

Then A_{16} is a subdirectly irreducible SQS-skein of nilpotence class 2, which is generated by the four elements e_0, e_1, e_2, and e_3 and which is not semi-boolean.

Proof: We have already seen in 6.3. that A_{16} is an SQS-skein of nilpotence class 2, which is not semi-boolean, with $\zeta(A_{16}) = \ker(\pi_3)$ where π_3 is the projection onto the first 3 components. Corollary 6.4.3 shows again that A_{16} is subdirectly irreducible and lemma 6.4.9 yields that A_{16} is generated by the 5 elements e_0, e_1, e_2, e_3, and e_4. It remains to be verified that in fact $e_4 \in [\{e_0, e_1, e_2, e_3\}]_{A_{16}}$. This is true since

$$q(q(q(e_1,e_0,e_2),q(e_1,e_0,e_3),q(q(e_1,e_0,e_2),e_0,e_3)),e_0,e_1)$$

$$=q\left(q\left(\begin{pmatrix}1\\1\\0\\0\end{pmatrix},\begin{pmatrix}1\\0\\1\\0\end{pmatrix},q\left(\begin{pmatrix}1\\1\\0\\0\end{pmatrix},e_0,e_3\right)\right),e_0,e_1\right)=q\left(q\left(\begin{pmatrix}1\\1\\0\\0\end{pmatrix},\begin{pmatrix}1\\0\\1\\0\end{pmatrix},\begin{pmatrix}1\\1\\1\\0\end{pmatrix}\right),e_0,e_1\right)$$

$$=q\left(\begin{pmatrix}1\\0\\0\\1\end{pmatrix},e_0,e_1\right)=\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=e_4$$

□

EXAMPLE 6.6.4: *Let A_{32} be the algebra $\langle A;q\rangle$ given by $A = (\mathrm{GF}(2))^5$ and*

$$q\left(\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\end{pmatrix},\begin{pmatrix}y_1\\y_2\\y_3\\y_4\\y_5\end{pmatrix},\begin{pmatrix}z_1\\z_2\\z_3\\z_4\\z_5\end{pmatrix}\right)=\begin{pmatrix}x_1+y_1+z_1\\x_2+y_2+z_2\\x_3+y_3+z_3\\x_4+y_4+z_4\\x_5+y_5+z_5+x_2y_2z_2x_3y_3z_3\begin{vmatrix}x_1&y_1&z_1\\x_4&y_4&z_4\\1&1&1\end{vmatrix}\end{pmatrix}$$

Then A_{32} is a subdirectly irreducible SQS-skein of nilpotence class 2, which is generated by the five elements e_0, e_1, e_2, e_3, and e_4 and which is not semi-boolean.

Proof: We have already seen in the proof of 6.5.13 that A_{32} is a subdirectly irreducible SQS-skein of nilpotence class 2, which is not semi-boolean. Lemma 6.4.9 yields that A_{32} is generated by the 6 elements e_0, e_1, e_2, e_3, e_4, and e_5. It remains to be verified that in fact $e_5 \in [\{e_0, e_1, e_2, e_3, e_4\}]_{A_{32}}$. This is true since

$$q(q(q(q(e_1,e_0,e_2),e_0,e_3),q(e_2,e_0,e_3),q(q(e_2,e_0,e_3),e_0,e_4)),q(e_1,e_0,e_2),q(e_3,e_0,e_4))$$

$$= q\left(q\left(q\left(q\begin{pmatrix}1\\1\\0\\0\\0\end{pmatrix},e_0,e_3\right),\begin{pmatrix}0\\1\\1\\0\\0\end{pmatrix},q\left(\begin{pmatrix}0\\1\\1\\0\\0\end{pmatrix},e_0,e_4\right)\right),\begin{pmatrix}1\\1\\0\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\1\\1\\0\end{pmatrix}\right)\right)$$

$$= q\left(q\left(\begin{pmatrix}1\\1\\1\\0\\0\end{pmatrix},\begin{pmatrix}0\\1\\1\\0\\0\end{pmatrix},\begin{pmatrix}0\\1\\1\\1\\0\end{pmatrix}\right),\begin{pmatrix}1\\1\\0\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\1\\1\\0\end{pmatrix}\right)$$

$$= q\left(\begin{pmatrix}1\\1\\1\\1\\1\end{pmatrix},\begin{pmatrix}1\\1\\0\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\1\\1\\0\end{pmatrix}\right)=\begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix}=e_5$$

□

We will now consider an infinite sequence of 4-generated SQS-skeins of increasing size and nilpotence class. The existence of this sequence shows that the free 4-generated SQS-skein must be infinite and cannot be nilpotent.

EXAMPLE 6.6.5: *Let* $N_4 = \langle (\mathrm{GF}(2))^4 ; q^{(4)} \rangle = A_{16}$ *as given in example 6.6.3. For* $n > 4$ *let* N_n *be the algebra* $\langle (\mathrm{GF}(2))^n ; q^{(n)} \rangle$ *where* $q^{(n)}$ *is given by*

$$\left(q^{(n)}(x,y,z)\right)_i = \begin{cases} \left(q^{(n-1)}\left(\begin{pmatrix} x_1 \\ \vdots \\ x_{n-1} \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_{n-1} \end{pmatrix}, \begin{pmatrix} z_1 \\ \vdots \\ z_{n-1} \end{pmatrix}\right)\right)_i & \text{if } 1 \le i < n \\ x_n + y_n + z_n + \begin{vmatrix} x_{n-2} & y_{n-2} & z_{n-2} \\ x_{n-1} & y_{n-1} & z_{n-1} \\ 1 & 1 & 1 \end{vmatrix} \prod_{l=1}^{n-2} (x_l y_l z_l) & \text{if } i = n \end{cases}$$

Then each N_n *is a subdirectly irreducible SQS-skein of nilpotence class* $(n-2)$, *which is not semi-boolean. Moreover, each* N_n *is generated by the four elements* e_0, e_1, e_2, *and* e_3.

Proof: The first part of this statement follows immediately from example 6.6.3 and the fact that for $n > 4$ N_n is constructed from N_{n-1} by the construction method described in theorem 6.5.10.

It remains to be shown that each N_n is generated by the four elements e_0, e_1, e_2, and e_3. We will first show that for every $i \in \{4,\ldots,n\}$ $e_i \in [\{e_0, e_1, e_2, \ldots, e_{i-1}\}]_{N_n}$.

Let 1_t^s denote the element in $(\mathrm{GF}(2))^n$ given by $\left(1_t^s\right)_i = \begin{cases} 0 \text{ if } i < t \\ 1 \text{ if } t \le i \le s \\ 0 \text{ if } s < i \end{cases}$. Note that for any s $1_s^s = e_s$.

Since $q^{(n)}\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}, e_0\right) = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$ obviously $1_t^s \in [\{e_0,\ldots,e_{i-1}\}]_{N_n}$ for all $0 \le t \le s < i$.

Let us now consider the expression $q^{(n)}(1_1^{i-1},1_1^{i-2},1_1^{i-3})$.

$$\text{If } j<i-2 \text{ then } \left(q^{(n)}(1_1^{i-1},1_1^{i-2},1_1^{i-3})\right)_j = \begin{cases} 1+1+1=1 & \text{if } j\le 3 \\ 1+1+1+1\begin{vmatrix}1&1&1\\1&1&1\\1&1&1\end{vmatrix}=1 & \text{if } j>3 \end{cases}.$$

$$\text{If } j=i-2 \text{ then } \left(q^{(n)}(1_1^{i-1},1_1^{i-2},1_1^{i-3})\right)_j = \begin{cases} 1+1+0=0 & \text{if } j\le 3 \\ 1+1+0+1\begin{vmatrix}1&1&1\\1&1&1\\1&1&1\end{vmatrix}=0 & \text{if } j>3 \end{cases}.$$

$$\text{If } j=i-1 \text{ then } \left(q^{(n)}(1_1^{i-1},1_1^{i-2},1_1^{i-3})\right)_j = \begin{cases} 1+0+0=1 & \text{if } j\le 3 \\ 1+0+0+1\begin{vmatrix}1&1&1\\1&1&0\\1&1&1\end{vmatrix}=1 & \text{if } j>3 \end{cases}.$$

$$\text{If } j=i \text{ then } \left(q^{(n)}(1_1^{i-1},1_1^{i-2},1_1^{i-3})\right)_j = 0+0+0+1\begin{vmatrix}1&1&0\\1&0&0\\1&1&1\end{vmatrix}=1 \text{ and}$$

$$\text{if } j>i \text{ then } \left(q^{(n)}(1_1^{i-1},1_1^{i-2},1_1^{i-3})\right)_j = 0+0+0+0\begin{vmatrix}?&0&0\\0&0&0\\1&1&1\end{vmatrix}=0.$$

Therefore $q^{(n)}(1_1^{i-1},1_1^{i-2},1_1^{i-3}) = q^{(n)}(1_{i-1}^{i},1_1^{i-3},e_0)$ and we get

$$q^{(n)}(q^{(n)}(q^{(n)}(1_1^{i-1},1_1^{i-2},1_1^{i-3}),1_1^{i-3},e_0),e_{i-1},e_0)$$
$$= q^{(n)}(q^{(n)}(q^{(n)}(1_{i-1}^{i},1_1^{i-3},e_0),1_1^{i-3},e_0),e_{i-1},e_0)$$
$$= q^{(n)}(1_{i-1}^{i},e_{i-1},e_0) = e_i$$

Since for every $i \in \{4,\ldots,n\}$ and all $0 \le t \le s \le i$ $1_t^s \in [\{e_0, e_1, e_2,\ldots, e_{i-1}\}]_{N_n}$ this equation implies that for every $i \in \{4,\ldots,n\}$ $e_i \in [\{e_0, e_1, e_2,\ldots, e_{i-1}\}]_{N_n}$. Since by lemma 6.4.10 N_n is generated by $\{e_0, e_1, e_2,\ldots, e_n\}$, we can deduce that N_n is in fact generated by $\{e_0, e_1, e_2, e_3\}$. □

As mentioned above, the existence of this sequence of SQS-skeins permits some conclusions about the free 4-generated SQS-skein:

COROLLARY 6.6.6: *The free 4-generated SQS-skein is infinite and neither nilpotent nor semi-boolean.*

COROLLARY 6.6.7: *The variety of SQS-skeins is not locally finite.*

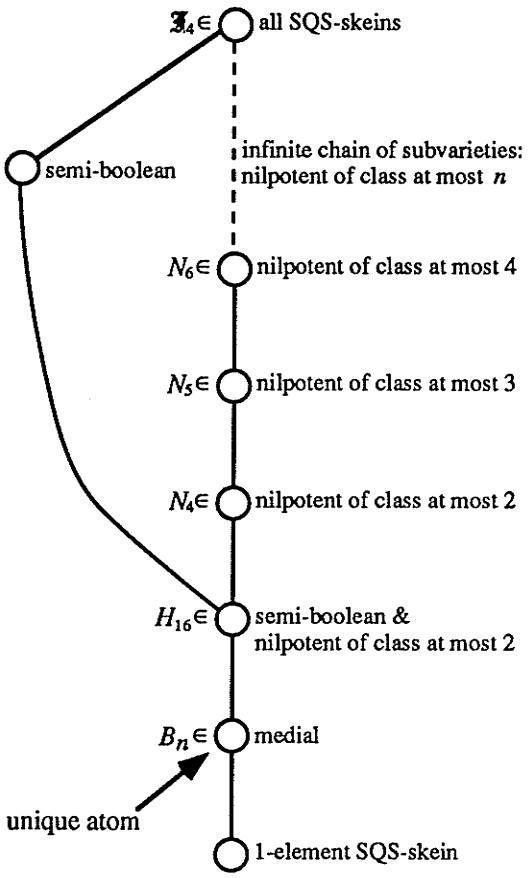


Figure 8:
A part of the subvariety lattice of the variety of SQS-skeins.

These examples allow us to take a glance at the structure of the subvariety lattice of the variety of SQS-skeins. Figure 8 shows those subvarieties that we have shown to be different from all others included with the exceptions that we have not constructed a semi-boolean SQS-skein that is not nilpotent of class at most 2. In this figure $\mathfrak{F}_4$ indicates the free 4-generated SQS-skein.

6.7. Derived Steiner Triple Systems

We have previously seen that distributive squags can be characterized combinatorically as those squags that correspond to Steiner Triple Systems whose subplanes are isomorphic to the 9-element affine plane. A similar description can be given for semi-

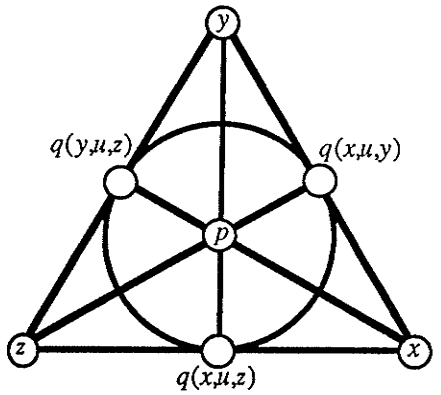
boolean SQS-skeins. We will first define the concept of a derived Steiner triple system as a certain "substructure" of a Steiner quadruple system:

> **Definition 6.7.1:** Let (P,B) be a Steiner quadruple system and $u \in P$ be an arbitrary point in P. Then the Steiner triple system $(P\backslash\{u\}, B')$ with $B' = \{\{x,y,z\} \mid x,y,z \in P\backslash\{u\} \;\&\; \{x,y,z,u\} \in B\}$ is called a *derived Steiner triple system of* (P,B).

We can now state and proof the following characterization of semi-boolean SQS-skeins:

> **THEOREM 6.7.2:** *Let $\mathcal{S} = \langle S;q\rangle$ be a SQS-skein with the corresponding Steiner quadruple system (S,B). $\mathcal{S}$ is semi-boolean if and only if all derived Steiner triple systems of (S,B) are projective geometries over GF(2).*

Proof: Suppose all derived Steiner triple systems of (S,B) are projective geometries over GF(2). Let $u, x, y, z \in S$. If $|\{u, x, y, z\}| < 4$ or $\{u, x, y, z\}$ form a subalgebra of $\mathcal{S}$ then $q(x,u,q(y,u,z)) = q(q(x,u,y),u,z)$ since every four element SQS-skein is boolean. Otherwise, consider the derived triple system $(P\backslash\{u\},B')$ where B' is given by $B' = \{\{a,b,c\} \mid a,b,c \in P\backslash\{u\} \;\&\; \{a,b,c,u\} \in B\}$. In $(P\backslash\{u\},B')$ x, y, and z are not collinear. Since this triple system is a projective geometry over GF(2), the subplane generated by x, y, and z has seven elements and is shown in figure 9. It is straightforward to verify that in fact $q(x,u,q(y,u,z)) = q(q(x,u,y),u,z)$, i.e. $\mathcal{S}$ is semi-boolean.



$q(q(x,u,y),u,z) = p = q(x,u,q(y,u,z))$

Figure 9:
A subplane in a projective geometry over GF(2).

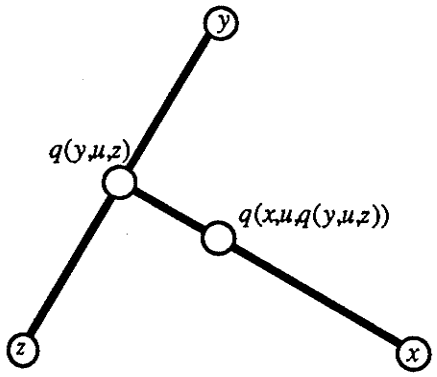


Figure 10:
In a derived Steiner triple system
of a semi-boolean SQS-skein (1).

Now suppose that $\mathcal{S}$ is semi-boolean. Let $u \in S$ and let x, y and z be three non-collinear points in the derived Steiner triple system $(P\backslash\{u\},B')$. We will show that the subplane generated by x, y and z is the projective plane of order two (i.e. the Fano plane).

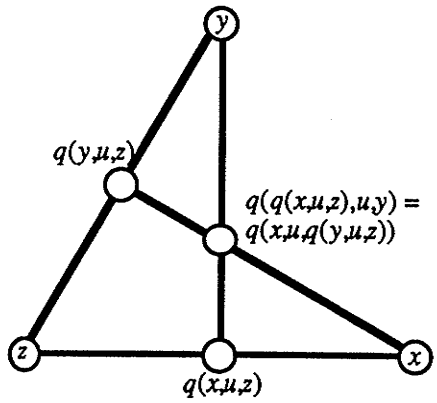


Figure 11:
In a derived Steiner triple system
of a semi-boolean SQS-skein (2).

The third point on the line through y and z is $q(y,u,z)$ and the third point on the line passing through $q(y,u,z)$ and x is $q(x,u,q(y,u,z))$ (figure 10). (Note that we are now not concerned with the question whether the points that appear distinct in the figures are in fact different; we will consider this question at the end of the proof.) Similarly, the third point on the line through x and z is $q(x,u,z)$ and the third point on the line passing through $q(x,u,z)$ and y is $q(q(x,u,z),u,y)$. Since $\mathcal{S}$ is semi-boolean, $q(q(x,u,z),u,y) = q(x,u,q(z,u,y)) = q(x,u,q(y,u,z))$ (figure 11). Using the same argument again and since $q(q(x,u,y),u,z) = q(x,u,q(y,u,z))$, we obtain figure 12. Since $q(q(x,u,z),u,q(y,u,z)) = q(x,u,q(z,u,q(y,u,z))) = q(x,u,y)$ we reach

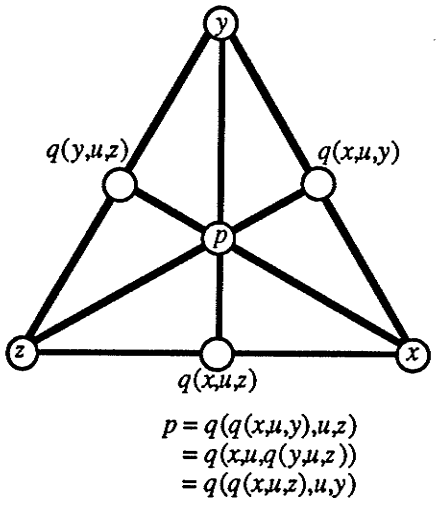


Figure 12:
In a derived Steiner triple system
of a semi-boolean SQS-skein (3).

the subplane shown in figure 13. It is easy to verify that this configuration contains all lines determined by at least two of the included points, i.e. it is indeed the complete subplane generated by x,y and z.

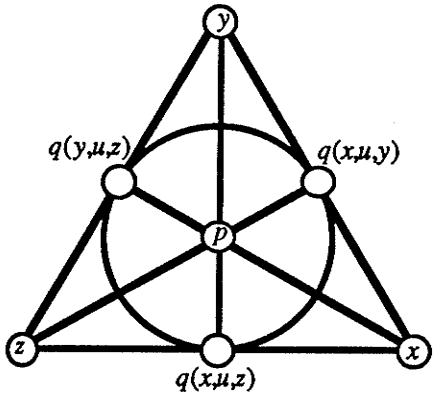


Figure 13:
A plane in a derived Steiner triple system of a semi-boolean SQS-skein.

The configuration shown in figure 13 is obviously the projective plane of order 2 (the Fano plane). Since the Fano plane is the smallest Steiner triple system that contains at least three non-collinear points, we can conclude that the subplane generated by x,y and z is this projective plane of order 2, i.e. the different points in figure 13 are in fact distinct. As we have mentioned in 4.3, Hall showed in (Hall 1960) that the Steiner triple systems whose subplanes are the projective plane of order 2 are exactly the projective geometries over GF(2). We may conclude that the derived Steiner triple systems of a Steiner quadruple system corresponding to a semi-boolean SQS-skein are projective geometries over GF(2). □

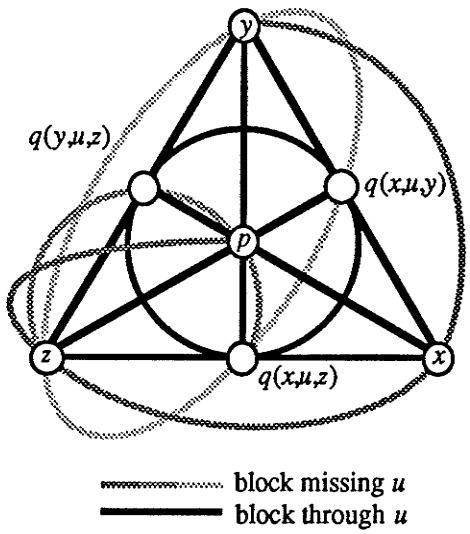


Figure 14:
A plane in a derived Steiner triple system of a boolean SQS-skein.

The boolean identity 6.2.1 cannot be expressed within a derived Steiner triple system. It describes in which way these systems are assembled to form the Steiner quadruple system. Figure 14 shows the meaning of this equation for the points x, y and z of the last proof. Note that the 'grey' blocks

miss u and are therefore not part of the derived Steiner triple system considered. Several blocks missing u have been omitted. They can be obtained from an existing block by rotating it about the centre of the configuration by 60° or 120°.

7. p-Groups

7.1. Basic Properties and Definitions

In this paper we are considering groups only as algebras of type $\langle 2,1,0\rangle$, i.e.:

DEFINITION 7.1.1 An algebra $\langle G;\cdot,^{-1},1\rangle$ of type $\langle 2,1,0\rangle$ is called a *group* if the following equations are satisfied in $\langle G;\cdot,^{-1},1\rangle$:

$$\begin{aligned} a\cdot(b\cdot c) &= (a\cdot b)\cdot c \\ a\cdot 1 = a &= 1\cdot a \\ a\cdot(a^{-1}) = 1 &= (a^{-1})\cdot a \end{aligned}$$

A group $\langle G;\cdot,^{-1},1\rangle$ is called *commutative* if in $\langle G;\cdot,^{-1},1\rangle$ the following equation is satisfied:

$$a\cdot b = b\cdot a$$

A group $\langle G;\cdot,^{-1},1\rangle$ is called *cyclic* if it is generated by one element.

Since the universal algebraic theory of the commutator has been developed as a generalization of the group-theoretic commutator it is not surprising that the commutator and the centre can be easily described in group-theoretic terms:

THEOREM 7.1.2 *Let $\mathfrak{G} = \langle G;\cdot,^{-1},1\rangle$ be a group and let α and β be two congruences on $\mathfrak{G}$. Then*

a) the commutator $[\alpha,\beta]$ is the unique congruence satifying the condition: $[1][\alpha,\beta] = \{aba^{-1}b^{-1} \mid a\alpha 1\beta b \;\&\; a,b \in G\}$ and

b) the centre $\zeta(\mathfrak{G})$ is the unique congruence satisfying the condition: $[1]\zeta(\mathfrak{G}) = \{x \mid x \in G \;\&\; ax = xa \text{ for all } a \in G\}$.

It is well known that the commutative groups are exactly the abelian groups. Moreover the finite abelian groups are exactly the direct products of cyclic groups. Every cyclic group is one of:

$\langle \mathbb{Z};+,-,0\rangle$	the additive group of integers
$\langle \{0,\ldots,p-1\};+_p,-_p,0\rangle$	the set of integers $0,\ldots p-1$ under addition modulo p for every positive integer $p \geq 2$.

Every finite cyclic group $\langle \{0,\ldots,p-1\},+_p,-_p,0\rangle$ satisfies the equation $px = 0$. (The expression px stands for the sum $((\ldots((x + x) + x) +\ldots) + x)$ in which x occurs p times. Similarly, we will denote the product $((\ldots((x \cdot x) \cdot x) \cdot\ldots) \cdot x)$, x occurring p times, with x^p.) A generalization of this concept is:

DEFINITION 7.1.3 A group $\langle G;\cdot,^{-1},1\rangle$ satisfying the equation $x^p = 1$ is called a *group of exponent p*. Groups of exponent 2 are also called *Boolean groups*.

DEFINITION 7.1.4 Given a group $\mathfrak{G} = \langle G;\cdot,^{-1},1\rangle$ an element $x \in G$ is said to have *order n* if $x^n = 1$ and for all j:

$$1 \leq j < n \quad \Rightarrow \quad x^j \neq 1$$

If G is finite then $|G|$ is called the order of $\mathfrak{G}$.

It is known that the order of any element in a finite group divides the order of the group. It is also known that these definitions imply that the order of any element in a group $\langle G;\cdot,^{-1},1\rangle$ of exponent p must divide p. Since the only element in $\langle G;\cdot,^{-1},1\rangle$ with order 1 is the element 1, every element other than 1 in a group $\langle G;\cdot,^{-1},1\rangle$ of exponent p where p is prime must have order p itself. A more general concept is:

DEFINITION 7.1.5 A group $\langle G;\cdot,^{-1},1\rangle$ in which every element $x \neq 1$ has the order p^k where k is some positive integer (depending on x) is called a *p-group*.

In the remainder of this chapter we will be mainly concerned with p-groups for prime p. Note that for every prime p every group of exponent p including the cyclic group $\langle\{0,\ldots,p-1\};+_p,-_p,0\rangle$ is a p-group. Every homomorphic image, subalgebra (i.e. subgroup) and finite direct product of p-groups (p prime and fixed) is again a p-group, Nevertheless, the class $\mathfrak{G}_p$ of all p-groups does not form a subvariety of the variety of all groups. Every variety within $\mathfrak{G}_p$ is congruence permutable, uniform and regular.

We have previously seen that every finite distributive squag is nilpotent. Similarly, it is also known that:

> **THEOREM 7.1.6** *Every finite p-group is nilpotent and if* $\langle G;\cdot,^{-1},1\rangle$ *is a finite p-group with* $|G| = p^k$ *then* $\langle G;\cdot,^{-1},1\rangle$ *is nilpotent of class at most* $k-1$.

but while the variety of distributive squags is locally finite, we have here:

> **THEOREM 7.1.7** *The class of all p-groups* $\mathfrak{G}_p$ *(p prime and fixed) is not locally finite.*

i.e. a finitely generated p-group may be infinite. The question whether this can happen is known as the generalized Burnside problem. It was answered in (Golod, 1965 [1964]). Golod gave a non-constructive proof that for every prime p there exist a finitely generated infinite p-group. In (Grigorčuk 1980) the construction of a 3-generated infinite 2-group was presented and (Gupta and Sidki 1983) gives constructions of 2-generated infinite p-groups for every odd prime p. The original Burnside problem was posed in (Burnside 1902): "*Is every group with a finite number of generators and satisfying an identical relation* $x^n = 1$ *finite?* " This question was first answered negatively in (Adian and Novikov 1968) for all odd $n \geq 4381$. The limit for n has been improved in (Adian 1979 [1975]) to $n \geq 665$ (n odd).

For certain classes of groups of exponent p more can be said: Every Boolean group is abelian, every finitely generated group of exponent 3 is finite and every group of exponent 3, whether finitely generated or not, is even nilpotent of class at most 3. Moreover, every finitely generated group of exponent 4 is also finite and therefore nilpotent. But in this case it cannot be extended to the infinitely generated groups of exponent 4.

The finitely generated infinite p-groups behave very differently from their finite counterpart since the following theorem holds:

THEOREM 7.1.8 *No finitely generated infinite p-group is nilpotent.*

Theorem 7.1.8 is really a corollary of the more general theorem that a nilpotent group is finite if it is generated by a finite number of elements each having finite order. It allows us to describe a locally finite class of p-groups:

COROLLARY 7.1.9 *Any variety consisting solely of nilpotent p-groups is locally finite.*

Proofs for theorems 7.1.6 and 7.1.8 can be found in every standard group theory textbook. Corollary 7.1.9 follows immediately from 7.1.8.

We will see in the next sections that the limit on the nilpotence class given by theorem 7.1.6 is only slightly better than the most obvious one. Theorem 5.4.1 has given us an upper bound of the nilpotence class of an n-generated distributive squag as a function of the number of generators n — theorem 5.4.2 even proved that this was the best possible bound. The question arises whether such a bound can also be given for p-groups. The existence of a recursive upper bound for the nilpotence class of an n-generated finite group of prime exponent p has already been shown by Adian and Razborov. A rather shorter proof of this fact due to E. I. Zel'manov can be found in (Kostrikin 1989).

M. F. Newman and J. Wiegold have found a bound for the nilpotence class of algebras in the variety $\mathfrak{A}_2^2 = \mathfrak{A}_2\mathfrak{A}_2$ where $\mathfrak{A}_2$ is the variety generated by $\langle\{0,1\};+_2,-_2,0\rangle$ and the product of two group varieties is defined to be the variety of all groups that are extensions of a group in the first factor by a group in the second factor. Their bound was first published in (Neumann 1967, theorem 34.53):

THEOREM 7.1.10 *In the variety $\mathfrak{A}_2^2$ every n-generator group is nilpotent of class at most $(n+1)$ for every $n \geq 2$.*

This theorem is a consequence of their result (also published in (Neumann 1967, 34.52)) that whenever the group $\mathfrak{A} = \langle A;+,-,0\rangle$ is metabelian (soluble of class 2)—i.e. it satisfies the commutator identity $\left[[\iota_A,\iota_A]\,,\,[\iota_A,\iota_A]\right] = \omega_A$ —and for $k = 2$ and $k = 3$ all the k-generator subgroups of $\mathfrak{A}$ are nilpotent of class at most $k + 1$, then the same is true for all values of k.

7.2. A Representation Theorem

As in the theories of nilpotent squags and nilpotent SQS-skeins we can use corollary 3.4.7 to give a representation of any finite p-group provided we have found a similar representation for all finite abelian p-groups. Since every finite abelian p-group is the direct product of cyclic groups of order p^n (p prime), we will first consider such a cyclic group of order p^n:

THEOREM 7.2.1 *Let $\mathfrak{G} = \langle G;+,-,0\rangle$ be a cyclic group of order p^n (p prime). Then there exists an n–dimensional vector space V and polynomials $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ and $q_i(x_1,\ldots,x_{i-1})$ over $\mathrm{GF}(p)$ for $1 \leq i \leq n$ such that*

1) $\mathfrak{V} = \langle V;+,-,\mathbf{0}\rangle$ *is isomorphic to $\mathfrak{G}$ where*

$$(x + y)_i \quad = \quad x_i + y_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})\,,$$

$$(-x)_i = -x_i + q_i(x_1,\ldots,x_{i-1}),$$

and $\mathbf{0}_i = 0$

for all $i \in \{1,\ldots,n\}$ *with* $p_1 \equiv 0 \equiv q_1$.

2) *For all* i *and all* $(x_1,\ldots,x_n), (y_1,\ldots,y_n) \in V$:

$$p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) = p_i(y_1,\ldots,y_{i-1},x_1,\ldots,x_{i-1})$$

3) *For all* i *and all* $(x_1,\ldots,x_n) \in V$ $p_i(x_1,\ldots,x_{i-1},0,\ldots,0) = 0$ *(i.e. no* $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ *has a constant term and every monomial of it contains elements from* $\{x_1,\ldots,x_n\}$ *and from* $\{y_1,\ldots,y_n\}$.*)*

4) *For all* i $q_i(0,\ldots,0) = 0$ *(i.e. no* $q_i(x_1,\ldots,x_{i-1})$ *has a constant term.)*

Proof: The representation described is simply the base p representation $x_n\ldots x_1$ where the polynomials p_i and q_i are the carry-over functions. It is clear that these functions depend only on the lower valued digits — note that they indeed depend on all lower valued digits since p_i has to consider the value of p_{i-1}. Properties 2, 3, and 4 are consequences of the equations $x + y = y + x$, $x + \mathbf{0} = \mathbf{0}$, and $-\mathbf{0} = \mathbf{0}$. □

Since every finite abelian p-group is the direct product of cyclic groups of order p^n we immediately get the following corollary:

COROLLARY 7.2.2 *Let* $\mathfrak{G} = \langle G;+,-,0\rangle$ *be an abelian p-group of order* p^n *(p prime). Then there exists an n–dimensional vector space V and polynomials* $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ *and* $q_i(x_1,\ldots,x_{i-1})$ *over* GF(p) *for* $1 \le i \le n$ *such that*

1) $\mathfrak{V} = \langle V;+,-,\mathbf{0}\rangle$ *is isomorphic to* $\mathfrak{G}$ *where*

$$(x + y)_i = x_i + y_i + p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}),$$

$$(-x)_i = -x_i + q_i(x_1,\ldots,x_{i-1}),$$

and $\mathbf{0}_i = 0$

for all $i \in \{1,\ldots,n\}$ *with* $p_1 = 0 = q_1$.

2) *For all i and all* $(x_1,\ldots,x_n), (y_1,\ldots,y_n) \in V$

$$p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}) = p_i(y_1,\ldots,y_{i-1},x_1,\ldots,x_{i-1})$$

3) *For all i and all* $(x_1,\ldots,x_n) \in V$ $p_i(x_1,\ldots,x_{i-1},0,\ldots,0) = 0$ *(i.e. no* $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ *has a constant term and every monomial of it contains elements from* $\{x_1,\ldots,x_n\}$ *and from* $\{y_1,\ldots,y_n\}$.*)*

4) *For all i* $q_i(0,\ldots,0) = 0$ *(i.e. no* $q_i(x_1,\ldots,x_{i-1})$ *has a constant term.)*

As a consequence of this corollary and of corollary 3.4.7 we get (as in the case of theorem 5.6.3):

REPRESENTATION THEOREM 7.2.3 *Let* $\mathfrak{G} = \langle G;+,-,0\rangle$ *be p-group of order* p^m *(p prime) of nilpotence class k. Let* $|[0]\zeta(\mathfrak{G})| = p^r$. *Then there exists an m–dimensional vector space V and polynomials* $q_i(x_1,\ldots,x_{i-1})$ *and* $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ *over* GF(p) *without constant term for all i with* $1 \le i \le m$ *and an increasing sequence* $n_1 < \ldots < n_k$ *of integers such that*

1) $n_1 \ge 2$, $n_{k-1} = m-r$ *and* $n_k = m$

2) $\mathfrak{V} = \langle V;+,-,\mathbf{0}\rangle$ *is isomorphic to* $\mathfrak{G}$ *where*

$$\begin{aligned} (x+y)_i &= x_i +_p y_i +_p p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}), \\ (-x)_i &= -_p x_i +_p q_i(x_1,\ldots,x_{i-1}), \\ \text{and} \qquad \mathbf{0}_i &= 0 \end{aligned}$$

for all $i \in \{1,\ldots,m\}$ *with* $p_1 = 0 = q_1$.

3) *For all i and all* $(x_1,\ldots,x_m) \in V$ $p_i(x_1,\ldots,x_{i-1},0,\ldots,0) = 0$ *and* $p_i(0,\ldots,0,x_1,\ldots,x_{i-1}) = 0$ *(i.e. no* $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ *has a constant term and every monomial of it contains elements from* $\{x_1,\ldots,x_m\}$ *and from* $\{y_1,\ldots,y_m\}$.*)*

4) *For all* i $q_i(0,\ldots,0) = 0$ *(i.e. no* $q_i(x_1,\ldots,x_{i-1})$ *has a constant term.)*

5) $\zeta(\mathfrak{V})$ *corresponds to the kernel of the projection onto the first* $m-r$ *components of* $\mathfrak{V}$*, this projection is a group homomorphism.*

6) *If* $\omega_S = \xi_0 \leq \xi_1 \leq \xi_2 \leq \ldots \leq \xi_k = \iota_S$ *is the upper central series of* $\mathfrak{V}$ *then for any* $j \in \{0,\ldots,k\}$ *the congruence* ξ_j *corresponds to the kernel of the projection onto the first* n_{k-j} *components of* $\mathfrak{V}$.

Note that the requirement $|[0]\zeta(\mathfrak{G})| = p^r$ is not a restriction for this theorem but a definition of the variable r. We will illustrate this representation theorem in section 7.4.

Proof: If $k = 1$ $\mathfrak{G}$ is an abelian p-group with $m = r$ and $\zeta(\mathfrak{G}) = G$. Theorem 7.2.3 follows then immediately from corollary 7.2.2. Therefore we will assume that $k > 1$.

By corollary 3.4.7 there is a collection of finite p-groups $\mathfrak{Q}_1 = \langle Q_1;+,-,0\rangle$, $\mathfrak{Q}_2 = \langle Q_2;+,-,0\rangle$, …, $\mathfrak{Q}_k = \langle Q_k;+,-,0\rangle$ of nilpotence class 1 and maps T_e^j for $e = 1,2,3$ and $j = 1,\ldots,k-1$ such that:

$$\mathfrak{G} \text{ is isomorphic to } \left\langle \prod_{i=1}^{k} Q_i \;;+,-,\mathbf{0} \right\rangle \text{ with:}$$

$$(r_1,r_2,\ldots,r_k) + (s_1,s_2,\ldots,s_k) =$$

$$\left(r_1+s_1, r_2+s_2+T_1^1\left(r_1,s_1\right),\ldots, r_k+s_k+T_1^{k-1}\left((r_1,\ldots,r_{k-1}),(s_1,\ldots,s_{k-1})\right)\right)$$

$$-(s_1,s_2,\ldots,s_k) = \left(-s_1,-s_2+T_2^1(s_1),\ldots,-s_k+T_2^{k-1}(s_1,\ldots,s_{k-1})\right)$$

$$\mathbf{0} = \left(0,0+T_3^1,\ldots,0+T_3^{k-1}\right) = \left(0,T_3^1,\ldots,T_3^{k-1}\right)$$

where $T_1^j : \left(\prod_{i=1}^{j} Q_i\right)^2 \to Q_{j+1}$, $T_2^j : \prod_{i=1}^{j} Q_i \to Q_{j+1}$, and $T_3^j : \varnothing \to Q_{j+1}$, i.e. $T_3^j \in Q_{j+1}$.

We can assume that $T_3^j = 0$ for all j, since otherwise we may consider the isomorphic algebra $\left\langle \prod_{i=1}^{k} Q_i \;;+^*,-^*,\mathbf{0}^* \right\rangle$ with:

$$(r_1,r_2,\ldots,r_k) +^* (s_1,s_2,\ldots,s_k) =$$

$$\begin{pmatrix} r_1+s_1, \\ r_2+s_2+T_3^1+T_1^1\left(r_1,s_1\right), \\ \vdots \\ r_k+s_k+T_3^{k-1}+T_1^{k-1}\left(\left(r_1,r_2+T_3^1,\ldots,r_{k-1}+T_3^{k-2}\right),\left(s_1,s_2+T_3^1,\ldots,s_{k-1}+T_3^{k-2}\right)\right) \end{pmatrix}$$

$$-^* (s_1,s_2,\ldots,s_k) = \left(-s_1,-s_2-2T_3^1+T_2^1(s_1),\ldots,-s_k-2T_3^{k-1}+T_2^{k-1}\left(s_1,s_2+T_3^1\ldots,s_{k-1}+T_3^{k-2}\right)\right)$$

$$\mathbf{0}^* = (0,0,\ldots,0) .$$

This algebra $\left\langle \prod_{i=1}^{k} \mathfrak{Q}_i ;+^*,-^*,\mathbf{0}^* \right\rangle$ is isomorphic to $\mathfrak{G}$ since the bijection:

$$\phi: \left\langle \prod_{i=1}^{k} \mathfrak{Q}_i ;+,-,\mathbf{0} \right\rangle \hookrightarrow\!\!\!\!\rightarrow \left\langle \prod_{i=1}^{k} \mathfrak{Q}_i ;+^*,-^*,\mathbf{0}^* \right\rangle$$

given by $\phi\left((s_1,s_2,\ldots,s_k)\right) = (s_1,s_2-T_3^1,\ldots,s_k-T_3^{k-1})$ can easily be checked to be an isomorphism.

Since all $\mathfrak{Q}_i$ are of nilpotence class 1 they can be represented as described in corollary 7.2.3, i.e. each $\mathfrak{Q}_i$ is isomorphic to $\left\langle \mathrm{GF}(p)^{m_i};+^i,-^i,\mathbf{0}^i \right\rangle$ for some $m_i \geq 1$ with:

$$\left(\left(r_1,\ldots,r_{m_i}\right)+^i\left(s_1,\ldots,s_{m_i}\right)\right)_j = r_j +_p s_j +_p p_j^i(r_1,\ldots,r_{j-1},s_1,\ldots,s_{j-1})$$

$$\left(-^i\left(s_1,\ldots,s_{m_i}\right)\right)_j = -_p s_j +_p q_j^i(s_1,\ldots,s_{j-1})$$

$$\mathbf{0}^i = (0,0,\ldots,0)$$

for all j and appropriate families of polynomials $\{p_j^i(r_1,\ldots,r_{j-1},s_1,\ldots,s_{j-1}) \mid j = 1,\ldots,m_i\}$ and $\{q_j^i(s_1,\ldots,s_{j-1}) \mid j = 1,\ldots,m_i\}$. Now define $n_1 = m_1$, $n_i = n_{i-1} + m_i$ for all $i = 2,\ldots,k$ and $m = n_k$. Then $1 < n_1 <\ldots< n_k$. Each T_1^j and T_2^j can then be considered a mapping from $\mathrm{GF}(p)^{2n_j}$ or $\mathrm{GF}(p)^{2n_j}$ to $\mathrm{GF}(p)^{m_{j+1}}$. We can further define t_{i,n_j+h} as the hth component of T_i^j and $t_{i,h}\equiv 0$ if $h \in \{1,\ldots,n_1\}$. Since t_{i,n_j+h} is a mapping from $\mathrm{GF}(p)^{2n_j}$ to $\mathrm{GF}(p)$ it can be considered a polynomial over $\mathrm{GF}(p)$.

Using these notations, $\mathfrak{G}$ is isomorphic to $\mathfrak{V} = \langle \mathrm{GF}(p)^m; +, -, \mathbf{0} \rangle$ where

$$((r_1,r_2,\ldots,r_k) + (s_1,s_2,\ldots,s_k))_g =$$
$$r_g +_p s_g +_p p_g^j(r_1,\ldots,r_{g-1},s_1,\ldots,s_{g-1}) +_p t_{1,n_j+h}(r_1,\ldots,r_{n_j},s_1,\ldots,s_{n_j})$$
$$(-(s_1,s_2,\ldots,s_k))_g = -_p s_g +_p q_g^j(s_1,\ldots,s_{g-1}) +_p t_{2,n_j+h}(s_1,\ldots,s_{n_j})$$
$$\mathbf{0} = (0,0,\ldots,0)$$

if $g = n_j + h$ and $h \in \{1,\ldots,m_{j+1}\}$.

Obviously this implies part 1 and all of part 2 except $n_1 \geq 2$.

The inequality $n_1 \geq 2$ follows from theorem 7.1.6 and the fact that the projection π_2 onto the first two components is obviously a homomorphism. Suppose $n_1 = 1$, then the image of π_2 is a p-group of nilpotence class 2 and size p^2 which contradicts theorem 7.1.6.

Parts 5 and 6 are true since they are true for the original construction as described by corollary 3.4.7 and the possible changes to this construction are all within a fixed component, i.e. they do not change the kernel of any projection onto the first n components. $(x + \mathbf{0} = x)$ and $(\mathbf{0} + x = x)$ imply part 3, while $(-\mathbf{0} = \mathbf{0})$ implies part 4. □

It is interesting to note that the representation as described in theorem 7.2.3 is quite similar to an intermediate construction used in the proof of the theorem that there exists a representation of every finitely generated torsion-free nilpotent group as a group of uni-triangular matrices over $\mathbb{Z}$ as given in (Kargapolov, Merzljakov 1979, theorem 17.2.5). Note that torsion-free groups are the opposite of p-groups since a group is called torsion-free if there is only one element of finite order.

This theorem even provides a representation of an arbitrary finite nilpotent group since by the Burnside-Wielandt theorem a finite group is nilpotent if and only if it is the direct product of its Sylow p-subgroups, i.e. the finite nilpotent groups are exactly the direct products of finite p-groups (p prime). The statement and proof of the Burnside-

Wielandt theorem can be found in many group-theory textbooks, e.g. in (Kargapolov, Merzljakov 1979).

7.3. p-Groups of Maximal Class

It has been shown by C. C. Sims in (Sims 1965) that the number of non-isomorphic groups of order p^n is (asymptotically) given by $p^{A(n)\,n^3}$ where $A(n) = \frac{2}{27} + O(n^{-1/3})$. Due to this multiplicity, special classes of p-groups are being investigated separately. One of these classes are the p-groups of maximal class:

DEFINITION 7.3.1 A p-group of order p^m with $m \geq 3$ and nilpotence class $m-1$ is called a *p-group of maximal class.*

In view of theorem 7.1.6 a p-group of maximal class has the largest nilpotence class possible for its order. For any such p-group we are able to specify exactly the sequence $n_1 < \ldots < n_{m-1}$ of numbers described in the representation theorem 7.2.3 and we can formulate the following theorem:

REPRESENTATION THEOREM 7.3.2 *Let $\mathfrak{G} = \langle G;+,-,0\rangle$ be p-group of order p^m (p prime) of maximal class, i.e. of nilpotence class $k = m-1$. Then there exists an m-dimensional vector space V and polynomials $q_i(x_1,\ldots,x_{i-1})$ and $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ over GF(p) without constant term for $1 \leq i \leq m$ such that*

1) $\mathfrak{V} = \langle V;+,=,\mathbf{0}\rangle$ *is isomorphic to $\mathfrak{G}$ where*

$$\begin{aligned} (x+y)_i &= x_i +_p y_i +_p p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1}), \\ (=x)_i &= -_p x_i +_p q_i(x_1,\ldots,x_{i-1}), \\ \text{and} \qquad \mathbf{0}_i &= 0 \end{aligned}$$

for all $i \in \{1,\ldots,n\}$ with $p_1 \equiv 0 \equiv q_1$.

2) *For all* i *and all* $(x_1,\ldots,x_n) \in V$ $p_i(x_1,\ldots,x_{i-1},0,\ldots,0) = 0$ *and* $p_i(0,\ldots,0,x_1,\ldots,x_{i-1}) = 0$ *(i.e. no* $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ *has a constant term and every monomial of it contains elements from* $\{x_1,\ldots,x_n\}$ *and from* $\{y_1,\ldots,y_n\}$*.)*

3) *For all* $i \geq 3$ $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ *depends on* x_{i-1} *or* y_{i-1}*.*

4) *For all* i $q_i(0,\ldots,0) = 0$ *(i.e. no* $q_i(x_1,\ldots,x_{i-1})$ *has a constant term.)*

5) $\zeta(\mathfrak{V})$ *corresponds to the kernel of the projection onto the first* $m-1$ *components of* $\mathfrak{V}$*, this projection is a group homomorphism.*

6) *If* $\omega_S = \xi_0 \leq \xi_1 \leq \xi_2 \leq \ldots \leq \xi_k = \iota_S$ *is the upper central series and* $\omega_S = \phi_k \leq \phi_{k-1} \leq \phi_{k-2} \leq \ldots \leq \phi_0 = \iota_S$ *the lower central series of* $\mathfrak{V}$ *then for any* $j \in \{0,\ldots,k\}$ $\xi_j = \phi_{k-j}$ *and for any* $j \in \{0,\ldots,k-1\}$ *this congruence* ξ_j *corresponds to the kernel of the projection onto the first* $m-j$ *components of* $\mathfrak{V}$*.*

Proof: The representation $\mathfrak{V} = \langle V;+,-,\mathbf{0}\rangle$ is exactly the representation given by theorem 7.2.3. Consider the sequence $2 \leq n_1 < n_2 < \ldots < n_k = m$ given by that theorem. Since for p-groups of maximal class $k = m-1$, we must have $n_j = j+1$ for all $j \in \{1,\ldots,k\}$. The remaining statements of this theorem follow immediately except part 3 and the claim $\xi_j = \phi_{k-j}$ for all $j \in \{0,\ldots,k\}$ in part 6.

The fact $\xi_j = \phi_{k-j}$ for all $j \in \{0,\ldots,k\}$ is well known for p-groups of maximal class (e.g. see (Huppert 1967, lemma 14.2)) but we can easily prove it using only universal algebraic arguments and this representation:

Obviously $\xi_j = \phi_{k-j}$ for $j \in \{0,k\}$ since $\xi_0 = \omega_S = \phi_k$ and $\xi_k = \iota_S = \phi_0$. Let us assume that we have already proven $\xi_j = \phi_{k-j}$ for all $j \in \{0,\ldots,i\}$. We will show that $\xi_i = \phi_{k-i}$ for $0 < i < k$. Since $\xi_i \geq \xi_{i-1} = \phi_{k-i+1} \leq \phi_{k-i}$ it is sufficient to prove:

$$\xi_i/\xi_{i-1} = \phi_{k-i}/\phi_{k-i+1} \tag{7.3.3}$$

By 3.2.7 we may conclude that $\xi_i \geq \phi_{k-i}$ and therefore

$$\xi_i/\xi_{i-1} \geq \phi_{k-i}/\phi_{k-i+1} \tag{7.3.4}$$

hence $$[0]\left(\xi_i/\xi_{i-1}\right) \supseteq [0]\left(\phi_{k-i}/\phi_{k-i+1}\right)$$

From part 6 of theorem 7.2.3 we get that

$$\left|[0]\left(\xi_i/\xi_{i-1}\right)\right| = p$$

Since ϕ_{k-i}/ϕ_{k-i+1} is a subalgebra (subgroup) this implies

$$\left|[0]\left(\phi_{k-i}/\phi_{k-i+1}\right)\right| = p \text{ or } 1$$

If $\left|[0]\left(\phi_{k-i}/\phi_{k-i+1}\right)\right| = 1$ then $\phi_{k-i} = \phi_{k-i+1}$ and therefore $i \leq 0$ which contradicts the fact that $0 < i < k$.

Therefore $$\left|[0]\left(\phi_{k-i}/\phi_{k-i+1}\right)\right| = p = \left|[0]\left(\xi_i/\xi_{i-1}\right)\right|$$

and we get $$[0]\left(\phi_{k-i}/\phi_{k-i+1}\right) \lhd [0]\left(\xi_i/\xi_{i-1}\right) \tag{7.3.5}$$

7.3.4 and 7.3.5 together imply immediately 7.3.3, i.e we have proven $\xi_j = \phi_{k-j}$ for all $j \in \{0,\ldots,k\}$.

It remains to prove part 3. Suppose there exists at least one $i \geq 3$ such that $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ does not depend on x_{i-1} and y_{i-1}. By theorem 7.3.2 the element $(a_1,\ldots,a_m)$ with $a_j = 0$ if $j \neq i-1$ and $a_{i-1} = 1$ is not in the kernel of $\xi_{m-i+1} = \zeta\left(\mathfrak{V}/\xi_{m-i}\right)$. Let $(b_1,\ldots,b_m)$ be an arbitrary element in V. Then for $j < i$ we have:

$$\begin{aligned}((a_1,\ldots,a_m) + (b_1,\ldots,b_m))_j &= a_j +_p b_j +_p p_j(a_1,\ldots,a_{j-1},b_1,\ldots,b_{j-1}) \\ &= a_j +_p b_j +_p p_j(0,\ldots,0,b_1,\ldots,b_{j-1}) \\ &= a_j +_p b_j +_p 0 \qquad \text{by part 2} \\ &= b_j +_p a_j +_p p_j(b_1,\ldots,b_{j-1},0,\ldots,0)\end{aligned}$$

$$= b_j +_p a_j +_p p_j(b_1,\ldots,b_{j-1},a_1,\ldots,a_{j-1})$$

$$= ((b_1,\ldots,b_m) + (a_1,\ldots,a_m))_j \qquad \text{and}$$

$$((a_1,\ldots,a_m) + (b_1,\ldots,b_m))_i \quad = a_i +_p b_i +_p p_i(a_1,\ldots,a_{i-1},b_1,\ldots,b_{i-1})$$

$$= a_i +_p b_i +_p p_i(0,\ldots,0,1,b_1,\ldots,b_{i-1})$$

$$= a_i +_p b_i +_p p_i(0,\ldots,0,0,b_1,\ldots,b_{i-1})$$

since p_i does not depend on x_{i-1}

$$= a_i +_p b_i +_p 0 \qquad \text{by part 2}$$

$$= b_i +_p a_i +_p p_i(b_1,\ldots,b_{i-1},0,\ldots,0,0)$$

$$= b_i +_p a_i +_p p_i(b_1,\ldots,b_{i-1},0,\ldots,0,1)$$

since p_i does not depend on y_{i-1}

$$= b_i +_p a_i +_p p_i(b_1,\ldots,b_{i-1},a_1,\ldots,a_{i-1})$$

$$= ((b_1,\ldots,b_m) + (a_1,\ldots,a_m))_i$$

Therefore $((a_1,\ldots,a_m) + (b_1,\ldots,b_m))\ \xi_{m-i}\ ((b_1,\ldots,b_m) + (a_1,\ldots,a_m))$.

Since $(b_1,\ldots,b_m)$ was chosen arbitrarily, theorem 7.1.2 implies that $(a_1,\ldots,a_m)$ is in the kernel of $\xi_{m-i+1} = \zeta\left(\mathfrak{A}/\xi_{m-i}\right)$ which is a contradiction! We have shown that for all $i \geq 3$ $p_i(x_1,\ldots,x_{i-1},y_1,\ldots,y_{i-1})$ depends on at least one of x_{i-1} and y_{i-1}. □

7.4. Examples

In this section we will illustrate the representation theorems of sections 7.2 and 7.3 by presenting representations of some well known finite groups. We will begin with a trivial example, a boolean group:

EXAMPLE 7.4.1 (KLEIN'S FOUR-GROUP) *Klein's four-group is the unique 4-element boolean (i.e. exponent 2) group. It can be given as:* $\langle \mathrm{GF}(2)^2, \dotplus, -, \mathbf{0}\rangle$ *where*

$$\begin{pmatrix}x_1\\x_2\end{pmatrix} \dotplus \begin{pmatrix}y_1\\y_2\end{pmatrix} = \begin{pmatrix}x_1+y_1\\x_2+y_2\end{pmatrix},\quad -\begin{pmatrix}x_1\\x_2\end{pmatrix} = \begin{pmatrix}x_1\\x_2\end{pmatrix} \quad \textit{and} \quad \mathbf{0} = \begin{pmatrix}0\\0\end{pmatrix}.$$

Our next example is only slightly more complicated. It is the smallest 2-group that is not boolean, i.e. that is not an exponent 2 group:

EXAMPLE 7.4.2 *The cyclic group of order 4 can be given as:*

$\langle \mathrm{GF}(2)^2, \dotplus, -, \mathbf{0} \rangle$ *where*

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \dotplus \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1+y_1 \\ x_2+y_2+x_1y_1 \end{pmatrix}, \quad -\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2+x_1 \end{pmatrix} \quad \textit{and} \quad \mathbf{0} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Examples 7.4.1 and 7.4.2 are abelian groups, i.e. groups of nilpotence class 1. The next two examples are of nilpotence class 2:

EXAMPLE 7.4.3 *The 8-element dihedral group $\mathfrak{D}_4$ can be given as:*

$\langle \mathrm{GF}(2)^3, \dotplus, -, \mathbf{0} \rangle$ *where*

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \dotplus \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_1+y_1 \\ x_2+y_2 \\ x_3+y_3+x_2y_2+x_1y_2 \end{pmatrix}, \quad -\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3+x_2\,(1+x_1) \end{pmatrix}$$

$$\textit{and} \quad \mathbf{0} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

It is generated by the two elements e_1 and e_2; e_1 has order 2 and e_2 has order 4. The centre of this group is the kernel of the projection onto the first two components.

This group is of maximal class and subdirectly ireducible. Note that it looks like the direct product of the 2-element boolean group and the cyclic group of order 4 with the added polynomial terms x_1y_2 and x_1x_2. Similarly, we can represent $\mathfrak{D}_8$, the 16-element dihedral group:

EXAMPLE 7.4.4 *The 16-element dihedral group $\mathfrak{D}_8$ can be given as:* $\langle \mathrm{GF}(2)^4, \dotplus, -, \mathbf{0} \rangle$ *where*

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \dotplus \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} x_1+y_1 \\ x_2+y_2 \\ x_3+y_3+x_2y_2+x_1y_2 \\ x_4+y_4+x_3y_3+x_2x_3y_2+x_2y_2y_3+x_1\left(y_2+y_3+(x_3+y_3+x_2)y_2\right) \end{pmatrix},$$

$$-\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3+x_2(1+x_1) \\ x_4+(x_2+x_3+x_2x_3)(1+x_1) \end{pmatrix} \quad \textit{and} \quad \mathbf{0} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

It is generated by the two elements e_1 and e_2; e_1 has order 2 and e_2 has order 8. The centre of this group is the kernel of the projection onto the first three components.

This group is also subdirectly irreducible and of maximal class, i.e. it is nilpotent of class 3. Our last example is a group that is nilpotent of class 2, subdirectly irreducible, but not of maximal class:

EXAMPLE 7.4.5 *The group $G = G(X, Y \mid X^8 = 1, Y^2 = 1, YXYX^3 = 1)$ can be given as* $\langle \mathrm{GF}(2)^4, \dotplus, -, \mathbf{0} \rangle$ *where*

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \dotplus \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} x_1+y_1 \\ x_2+y_2 \\ x_3+y_3+x_2y_2 \\ x_4+y_4+x_3y_3+x_2x_3y_2+x_2y_2y_3+x_1y_2 \end{pmatrix},$$

$$-\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 + x_2 \\ x_4 + x_2 + x_3 + x_2x_3 + x_1x_2 \end{pmatrix} \quad \textit{and} \quad \mathbf{0} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

It is generated by the two elements $Y = e_1$ and $X = e_2$. The centre of this group is the kernel of the projection onto the first two components.

Note that the group in the last example is subdirectly irreducible, but the centre is not a minimal congruence. This implies that the equivalent theorem to 5.7.20 and 6.4.3 is not true for p-groups.

We have omitted the proofs that the representations given in examples 7.4.1 to 7.4.5 are indeed correct since it is very easy to see: Examples 7.4.1 and 7.4.2 are immediately clear. 7.4.3 and 7.4.4 follow from the representation of the dihedral group $\mathfrak{D}_n$ as the group of 2×2 matrices $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ over $\mathbb{Z}_n$ with $a = \pm 1$ (see for example (Kargapolov, Merzljakov 1979 [1977])). 7.4.5 finally follows from the representation of the group G as a semidirect product of $\mathbb{Z}_8$ with $\mathbb{Z}_2$ (see (Weinstein 1977, example 4.7)). The other mentioned properties of these groups are also proven in (Weinstein 1977).

8. E-Minimal Algebras of Affine Type

8.1. Minimal and E-Minimal Algebras

In this chapter we will consider E-minimal algebras of affine type. This concept arose from the investigation of finite algebras by Pálfy, Pudlák, Hobby and McKenzie. Most of their results were collected and presented in (Hobby, McKenzie 1988). In this section, and the beginning of the next, we will present those definitions and theorems that are needed for our work. We omit all proofs, since they can be found in (Hobby, McKenzie 1988). We will see that finite nilpotent squags, finite nilpotent SQS-skeins and finite p-groups are examples of E-minimal algebras and we will be able to generalize some of the results that we have obtained earlier in this thesis.

The main concepts are given in the following three definitions:

DEFINITION 8.1.1 Let (δ,θ) be a congruence quotient of the finite algebra $\mathbf{A} = \langle A;\Omega\rangle$. $\mathbf{A}$ is called (δ,θ)-*minimal* if and only if every unary polynomial $f \in \mathrm{Pol}_1(\mathbf{A})$ is either a permutation of A or satisfies the condition: $f(\theta) \subseteq \delta$.

DEFINITION 8.1.2 A finite algebra $\mathbf{A} = \langle A;\Omega\rangle$ is called *minimal* if and only if $\mathbf{A}$ is (ω_A,ι_A)-minimal (i.e. if $|A| > 1$ and every non-constant unary polynomial $f \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A).

DEFINITION 8.1.3 Let $\mathbf{A} = \langle A;\Omega\rangle$ be a finite algebra. Then $\mathrm{E}(\mathbf{A})$ denotes the set of all unary polynomials $e \in \mathrm{Pol}_1(\mathbf{A})$ satisfying $e(x) = e(e(x))$ for all $x \in A$. The finite algebra $\mathbf{A}$ is called *E-minimal* if and only if $|A| > 1$ and every non-constant $e \in \mathrm{E}(\mathbf{A})$ is the identity on A, i.e. $e(x) = x$ for all $x \in A$.

It has been shown that every minimal algebra is of one of five types:

DEFINITION 8.1.4 Let $\mathbf{A} = \langle A;\Omega\rangle$ be a minimal algebra.

1) $\mathbf{A}$ is of *unary type*, or type 1, if and only if $\mathrm{Pol}(\mathbf{A}) = \mathrm{Pol}(\langle A;\Pi\rangle)$ for a subgroup $\Pi \subseteq \mathrm{Sym}(\mathbf{A})$.
2) $\mathbf{A}$ is of *affine type*, or *type* 2, if and only if $\mathbf{A}$ is polynomially equivalent (i.e. functionally equivalent) to a vectorspace.
3) $\mathbf{A}$ is of *boolean type*, or *type* 3, if and only if $\mathbf{A}$ is polynomially equivalent to a 2-element boolean algebra.
4) $\mathbf{A}$ is of *lattice type*, or *type* 4, if and only if $\mathbf{A}$ is polynomially equivalent to a 2-element lattice.
5) $\mathbf{A}$ is of *semilattice type*, or *type* 5, if and only if $\mathbf{A}$ is polynomially equivalent to a 2-element semilattice.

THEOREM 8.1.5 *A finite algebra is minimal if and only if it is of one of the types* 1 *to* 5.

Similarly, it has also be shown that every E-minimal algebra is of one of five types. To present this result, we require some further concepts:

DEFINITION 8.1.6 Let $\mathbf{A} = \langle A;\Omega\rangle$ be (δ,θ)-minimal. A subset $N \subseteq A$ is called a (δ,θ)-*trace of* $\mathbf{A}$ if and only if there exists an $x \in N$ such that $N = [x]\theta \neq [x]\delta$.

DEFINITION 8.1.9 Let $\mathbf{A} = \langle A;\Omega\rangle$ be an arbitrary algebra, $\alpha \in \mathrm{Con}(\mathbf{A})$, $h \in \mathrm{Pol}_n(\mathbf{A})$, and $N \subseteq A$. Then

1) $\alpha\big|_N = \alpha \cap (N \times N)$ denotes the congruence α restricted to N.

2) $h\big|_N = \{(x_0,\ldots,x_{n-1},h(x_0,\ldots,x_{n-1})) \mid (x_0,\ldots,x_{n-1}) \in N^n\}$ denotes the n-ary polynomial h restricted to N. Note that the description of h may still contain constants from A that are not in N.

3) $\mathrm{Pol}(\mathbf{A})\big|_N$ is the set of all $h\big|_N$ such that for some n, $h \in \mathrm{Pol}_n(\mathbf{A})$ and $h(N^n) \subseteq N$.

4) $\mathbf{A}\big|_N = \left\langle N ; \mathrm{Pol}(\mathbf{A})\big|_N \right\rangle$ is called the *algebra induced on N by* $\mathbf{A}$.

DEFINITION 8.1.8 Let $\mathbf{A} = \langle A;\Omega\rangle$ be (δ,θ)-minimal. Let $i \in \{1,2,3,4,5\}$. We say that $\mathbf{A}$ is *(δ,θ)-minimal of type i* if and only if for every (δ,θ)-trace N, $\left(\mathbf{A}\big|_N\right)\Big/\left(\delta\big|_N\right)$ is a minimal algebra of type i.

Using these definitions we can describe the possible types of an E-minimal algebra as follows:

DEFINITION 8.1.9 Let $\mathbf{A}$ be an E-minimal algebra.

1) $\mathbf{A}$ has *unary type* (*type* 1) if and only if $\mathbf{A}$ is (δ,θ)-minimal of type 1 for every prime congruence quotient (δ,θ) of $\mathbf{A}$.

2) $\mathbf{A}$ has *affine type* (*type* 2) if and only if $\mathbf{A}$ is (δ,θ)-minimal of type 2 for every prime congruence quotient (δ,θ) of $\mathbf{A}$.

3) $\mathbf{A}$ has *boolean type* (*type* 3), *lattice type* (*type* 4), or *semilattice type* (*type* 5) if and only if it is a 2-element minimal algebra of the same type.

THEOREM 8.1.10 *Every E-minimal algebra is of one of the following types: unary, affine, boolean, lattice or semilattice type.*

We are only interested in E-minimal algebras of affine type, since finite nilpotent squags, finite nilpotent SQS-skeins and finite p-groups can be shown to be of this type.

In (Hobby, McKenzie 1988) the following properties of E-minimal algebras of affine type have been proven:

THEOREM 8.1.11 *Any finite algebra $\mathbf{A}$ with more than one element is E-minimal of affine type if and only if $\mathbf{A}$ satisfies the following two conditions:*

1) *$\mathbf{A}$ has a Mal'cev polynomial and*

2) *$\mathbf{A}$ has a congruence quotient (δ,θ) such that it is (δ,θ)-minimal of type 2.*

THEOREM 8.1.12 *Every E-minimal algebra of affine type is nilpotent.*

In the proof of this theorem in (Hobby, McKenzie 1988) an even stronger property of E–minimal algebras of affine type has been shown:

LEMMA 8.1.13 *Let $\mathbf{A}$ be an E-minimal algebra of affine type and let $\alpha,\beta \in \mathbb{C}(\mathbf{A})$ such that α covers β. Then $[\iota_A,\alpha] < \beta$. Moreover:*

$$[\iota_A,\alpha] \leq \bigcap \{\gamma \in \mathbb{C}(\mathbf{A}) \mid \alpha \text{ covers } \gamma\}.$$

The proof of lemma 8.1.14 is an exercise in (Hobby, McKenzie 1988):

LEMMA 8.1.14 *Every E-minimal algebra of affine type has a Mal'cev term operation that is one–to–one in each variable when the others are held fixed.*

A simple, but useful consequence is the following corollary:

COROLLARY 8.1.15 *Every E-minimal algebra of affine type is congruence uniform and congruence regular.*

Proof: Let $\mathbf{A}$ be an E-minimal algebra of affine type. Let $d(x,y,z)$ be the Malcev term operation on $\mathbf{A}$ described in lemma 8.1.13. Then for every a and b in $\mathbf{A}$ and every congruence ϕ on $\mathbf{A}$ the term function $f(x) = d(a,x,b)$ maps $[a]\phi$ into $[b]\phi$ and $[b]\phi$ into $[a]\phi$. Since f is one-to-one $[a]\phi$ and $[b]\phi$ have the same cardinality. Since the algebra is finite and $f([a]\phi) \subseteq [b]\phi$ this also implies congruence regularity. □

Note that the congruence uniformity also follows from theorems 8.1.11 and 8.1.12 and the fact that every nilpotent algebra in a congruence modular variety is congruence uniform. For a proof of the latter statement see (Freese, McKenzie 1987).

8.2. Representation of E-Minimal Algebras of Affine Type

Already in (Hobby, McKenzie 1988) a representation of E-minimal algebras of affine types has been given:

DEFINITION 8.2.1 Let GF(q) be a finite field and m be any positive integer. Then $\mathfrak{E}(q,m)$ denotes the algebra $\langle \mathrm{GF}(q)^m;\Omega\rangle$ where Ω is the set of all operations f on $\mathrm{GF}(q)^m$ satisfying the following condition (provided the arity of f is n):

There exist $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathrm{GF}(q)$ and polynomials $h_1, h_2, \ldots, h_m$ over GF(q), such that h_i is $n\cdot(i-1)$-ary and for all $x^{(1)}, x^{(2)}, \ldots, x^{(n)} \in \mathrm{GF}(q)^m$:

$$(f(x^{(1)}, x^{(2)}, \ldots, x^{(n)}))_i = \left(\sum_{j=1}^{n} \lambda_j x_i^{(j)}\right) + h_i\left(x_1^{(1)}, x_2^{(1)}, \ldots, x_{i-1}^{(1)}, x_1^{(2)}, \ldots, x_1^{(n)}, \ldots, x_{i-1}^{(n)}\right)$$

for all $i = 1, 2, \ldots, m$. f will be denoted by $[\lambda_1,\ldots,\lambda_n; h_1,\ldots,h_m]^q$.

THEOREM 8.2.2 *For any finite, non-trivial algebra* $\mathfrak{A}$ *the following are equivalent:*

1) $\mathfrak{A}$ *is E-minimal of affine type.*

2) $\mathfrak{A}$ *is Mal'cev and isomorphic to a reduct of some algebra* $\mathfrak{T}(q,k)$*, where* k *is the height of* $\mathrm{Con}(\mathfrak{A})$.

The following corollary is an immediate consequence of this theorem and our representation theorems 5.7.3, 6.4.2 and 7.2.3. Note that the sequence of kernels of the projections onto the first m, m–1, m–2,... components respectively form a maximal chain in the congruence lattice of those algebras.

COROLLARY 8.2.3 *All finite nilpotent squags, finite nilpotent SQS-skeins and finite p-groups are E-minimal algebras of affine type.*

We will now consider some generalizations of theorems and lemmas that we have already proven for finite p-groups, finite nilpotent SQS-skeins, and finite nilpotent squags. We will begin with a more detailed description of the representation given by theorem 8.2.2.

COROLLARY 8.2.4 *Let* $\mathfrak{A} = \langle A; \{f_i \mid i \in I\}\rangle$ *be an E-minimal algebra of affine type and of nilpotence class k. Then there exist an m-dimensional vector space V over a finite field* $\mathrm{GF}(q)$*, for every* $i \in I$ *an operation* $[\lambda_1^{(i)},\ldots,\lambda_{n_i}^{(i)};h_1^{(i)},\ldots,h_m^{(i)}]^q$ *where* n_i *is the arity of* f_i*, and a sequence* $1 \leq m_1 < \ldots < m_k = m$ *of integers such that:*

1) $\mathfrak{V} = \langle V; \{[\lambda_1^{(i)},\ldots,\lambda_{n_i}^{(i)};h_1^{(i)},\ldots,h_m^{(i)}]^q \mid i \in I\}\rangle$ *is isomorphic to* $\mathfrak{A}$.

2) $\zeta(\mathfrak{V})$ *corresponds to the kernel of the projection onto the first* m_{k-1} *components of V, this projection is a homomorphism.*

3) *If* $\omega_V = \xi_0 \leq \xi_1 \leq \xi_2 \leq \ldots \leq \xi_k = \iota_V$ *is the upper central series of* $\mathfrak{V}$ *then for any* $j \in \{0,1,\ldots,k\}$ *the congruence* ξ_j *is the kernel of the projection onto the first* m_{k-j} *components of* V.

Proof: This corollary follows immediately from the proof of theorem 8.2.2 in (Hobby, McKenzie 1988), since the construction of the $\mathfrak{T}(q,k)$ proceeds along an arbitrary maximal chain in $\mathfrak{C}(\mathbb{A})$ and $\xi_0 \leq \xi_1 \leq \xi_2 \leq \ldots \leq \xi_k$ can be extended to such a chain. □

In the theory of squags we had seen that we can move among different representations of a fixed squag by using certain easily described isomorphisms (see lemma 5.7.5). We had used this fact to prove the existence of especially nice representations (see lemmata 5.7.4 and 5.7.13). We are able to generalize this tool to the theory of E-minimal algebras:

LEMMA 8.2.5 *Let* V *be an* m*-dimensional vector space over the finite field* GF(q) *and let* $\mathfrak{V} = \langle V; \{ f_i \mid i \in I \} \rangle$ *be an E-minimal algebra of affine type with* $f_i = [\lambda_1^{(i)},\ldots,\lambda_{n_i}^{(i)};h_1^{(i)},\ldots,h_m^{(i)}]^q$ *for all* $i \in I$. *Let* k *be a fixed number in* $\{2,\ldots,m\}$ *and let* $P(x_1,\ldots,x_{k-1})$ *be another polynomial over* GF(q). *For every* $i \in I$ *and every* $j \in \{k,\ldots,m\}$ *define:*

• *if* $j=k$ *then*

$$\widehat{h_j^{(i)}}\left(x_1^{(1)},x_2^{(1)},\ldots,x_{j-1}^{(1)},\ldots,x_1^{(n_i)},\ldots,x_{j-1}^{(n_i)}\right)$$

$$= P\left(\left(f_i(\mathbf{x}^{(1)},\ldots,\mathbf{x}^{(n_i)})\right)_1,\ldots,\left(f_i(\mathbf{x}^{(1)},\ldots,\mathbf{x}^{(n_i)})\right)_{k-1}\right)$$

$$- \sum_{t=1}^{n_i} \lambda_t P\left(x_1^{(t)},\ldots,x_{k-1}^{(t)}\right) + h_j^{(i)}\left(x_1^{(1)},\ldots,x_{j-1}^{(n_i)}\right)$$

$$\text{where } \mathbf{x}^{(s)} = \left(x_1^{(s)},\ldots,x_{k-1}^{(s)},0,\ldots,0\right)$$

• *if* $j>k$ *then* $\widehat{h}_j^{(i)}\left(x_1^{(1)},x_2^{(1)},\ldots,x_{j-1}^{(1)},\ldots,x_1^{(n_i)},\ldots,x_{j-1}^{(n_i)}\right)$

$$= h_j^{(i)}\begin{pmatrix} x_1^{(1)},\ldots,x_{k-1}^{(1)},x_k^{(1)}-P\left(x_1^{(1)},\ldots,x_{k-1}^{(1)}\right),x_{k+1}^{(1)},\ldots,x_{j-1}^{(1)}, \\ \ldots, \\ x_1^{(n_i)},\ldots,x_{k-1}^{(n_i)},x_k^{(n_i)}-P\left(x_1^{(n_i)},\ldots,x_{k-1}^{(n_i)}\right),x_{k+1}^{(n_i)},\ldots,x_{j-1}^{(n_i)} \end{pmatrix}$$

Then $\widehat{f}_i=[\lambda_1^{(i)},\ldots,\lambda_{n_i}^{(i)};h_1^{(i)},\ldots,h_{k-1}^{(i)},\widehat{h}_k^{(i)},\ldots,\widehat{h}_m^{(i)}]^q$ *is an operation on the field* GF(q) *in the sense of definition 8.2.1.*

Let $\widehat{\mathfrak{V}}=\langle V;\{\widehat{f}_i\,|\,i\in I\}\rangle$ *and let* $\phi: V\to V$ *be defined by :*

$$[\phi((x_1,\ldots,x_m))]_j=\begin{cases}x_j & \text{if } j\neq k\\ x_k+P(x_1,\ldots,x_{k-1}) & \text{if } j=k\end{cases}$$

Then $\phi:\mathfrak{V}\longrightarrow\!\!\!\!\rightarrow\widehat{\mathfrak{V}}$ *is an isomorphism and* ϕ^{-1} *is given by:*

$$\left[\phi^{-1}((x_1,\ldots,x_m))\right]_j=\begin{cases}x_j & \text{if } j\neq k\\ x_k-P(x_1,\ldots,x_{k-1}) & \text{if } j=k\end{cases}$$

Moreover, if $\mathfrak{V}$ *satisfies the conditions 2) and 3) of corollary 8.2.4 then* $\widehat{\mathfrak{V}}$ *also satisfies these conditions.*

Proof: From the definition of ϕ it is immediately clear that ϕ is a bijection and that its inverse ϕ^{-1} is given as described. It is straightforward to verify that each polynomial $\widehat{h}_j^{(i)}$ depends only on the variables $x_1^{(1)},x_2^{(1)},\ldots,x_{j-1}^{(1)},\ldots,x_1^{(n_i)},\ldots,x_{j-1}^{(n_i)}$, i.e. $\widehat{f}_i$ is an operation on the field GF(q) in the sense of definition 8.2.1. As in the proof of lemma 5.7.5 it is easy to show that ϕ is even an isomorphism.

Moreover, if $\mathfrak{V}$ satisfies the conditions 2) and 3) of theorem 8.2.4 then $\widehat{\mathfrak{V}}$ also satisfies these conditions since ϕ and the projection onto the first j components commute for every j. (This is immediately clear from the definition of ϕ.) □

We can now use this tool to show that the representation in corollary 8.2.4 can be chosen such that any arbitrary element $a\in A$ can be mapped onto $\mathbf{0}=(0,\ldots0)$:

THEOREM 8.2.6 *The representation in corollary 8.2.4 can be chosen such that the isomorphism from the algebra* $\mathfrak{A} = \langle A; \{f_i \mid i \in I\}\rangle$ *to* $\mathfrak{V} = \langle \mathrm{GF}(q)^m; \{g_i \mid i \in I\}\rangle$ *maps any fixed point* $a \in A$ *to* $\mathbf{0} = (0,\ldots,0)$.

Proof: Let $\phi : \mathfrak{A} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathfrak{V}_0$ be any representation of $\mathfrak{A}$ as given by corollary 8.2.4. Let $\phi_1, \phi_2, \ldots, \phi_m$ be the sequence of isomorphisms and $\mathfrak{V}_1, \mathfrak{V}_2, \ldots \mathfrak{V}_m$ the sequence of algebras obtained from lemma 8.2.5 for $\phi_i : \mathfrak{V}_{i-1} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathfrak{V}_i$, $k = i$ and $P = (\phi(a))_k$. Let $\psi = \phi_m \circ \phi_{m-1} \circ \ldots \circ \phi_1 \circ \phi : \mathfrak{A} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathfrak{V}_m$. Then $\psi : \mathfrak{A} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathfrak{V}_m$ is a representation as described by 8.2.4 and $(\psi(a))_i = (\phi_i(a))_i = (\phi(a))_i - (\phi(a))_i = 0$. □

As we have seen in the proofs of 5.7.4 and 5.7.13, this tool—lemma 8.2.5—is also useful to improve the representation given by corollary 8.2.4 within the theory of specific E-minimal algebras of affine type, e.g. finite nilpotent squags.

In section 6.4 (lemma 6.4.7) we presented a description of the commutator terms for finite nilpotent SQS-skeins. Since this description is based on a representation theorem analogous to 8.2.4, we are able to generalize this description.

LEMMA 8.2.7 *Let* V *be an* m*-dimensional vector space over the finite field* $\mathrm{GF}(q)$ *and let* $\mathfrak{V} = \langle V; \{f_i \mid i \in I\}\rangle$ *be an E-minimal algebra of affine type with* $f_i = [\lambda_1^{(i)},\ldots,\lambda_{n_i}^{(i)}; h_1^{(i)},\ldots,h_m^{(i)}]^q$ *for all* $i \in I$. *Let* $k \in \{1,\ldots,m\}$ *and let* $0 = m_0 < m_1 < \ldots < m_k = m$ *be a finite sequence of integers. For every* $j = 1,\ldots,m$ *let* $m(j)$ *be the integer such that* $m(j) = m_r < j \leq m_{r+1}$ *for some* r. *Moreover, suppose that for all* $i \in I$ *and* $j \in \{1,\ldots,m\}$ *the polynomial* $h_j^{(i)}$ *depends only on* $x_1^{(1)}, x_2^{(1)},\ldots,x_{m(j)}^{(1)},\ldots,x_1^{(n_i)},\ldots,x_{m(j)}^{(n_i)}$.

Then every t*-ary term function* $\tau(x^{(1)}, x^{(2)}, x^{(3)},\ldots, x^{(t)})$ *on* $\mathfrak{V}$ *is given by*

$$\left(\tau(x^{(1)},x^{(2)},\ldots,x^{(t)})\right)_j = \left(\sum_{h=1}^{t} r_h x_j^{(h)}\right) + s_j\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{m(j)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(t)} \\ \vdots \\ x_{m(j)}^{(t)} \end{pmatrix}\right)$$

where $r_1,\ldots,r_t \in \mathrm{GF}(q)$ *and the* s_j *are polynomials over* $\mathrm{GF}(q)$ *in the variables* $x_1^{(1)},\ldots, x_{m(j)}^{(1)},\ldots, x_1^{(t)},\ldots, x_{m(j)}^{(t)}$.

Proof: We will prove 8.2.7 by induction over the number of operations occurring in τ.

If τ is a projection then 8.2.7 is obviously true.

Now suppose

$$\tau(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(t)}) = f_i(\tau^{(1)}(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(t)}),\ldots,\tau^{(n_i)}(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(t)}))$$

where $\tau^{(1)}$ to $\tau^{(n_i)}$ satisfy 8.2.7, i.e. for $l \in \{1,\ldots,n_i\}$:

$$\left(\tau^{(l)}(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(t)})\right)_j = \left(\sum_{h=1}^{t} r_h^{(l)} x_j^{(h)}\right) + s_j^{(l)}\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{m(j)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(t)} \\ \vdots \\ x_{m(j)}^{(t)} \end{pmatrix}\right)$$

Then $\left(\tau(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(t)})\right)_i =$

$$\sum_{l=1}^{n_i} \lambda_l^{(i)} \cdot \left(\left(\sum_{h=1}^{t} r_h^{(l)} x_j^{(h)}\right) + s_j^{(l)}\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{m(j)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(t)} \\ \vdots \\ x_{m(j)}^{(t)} \end{pmatrix}\right)\right) + P_j\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{m(j)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(j)} \\ \vdots \\ x_{m(j)}^{(j)} \end{pmatrix}\right)$$

$$= \left(\sum_{h=1}^{t}\left(\sum_{l=1}^{n_i} \lambda_l^{(i)} \cdot r_h^{(l)}\right) x_j^{(h)}\right) +$$

$$\left(\sum_{l=1}^{n_i} s_j^{(l)}\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{m(j)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(t)} \\ \vdots \\ x_{m(j)}^{(t)} \end{pmatrix}\right) + P_j\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{m(j)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(t)} \\ \vdots \\ x_{m(j)}^{(t)} \end{pmatrix}\right)\right)$$

where P_j is an appropriate composition of ${\tau^{(1)}}_1,\ldots,{\tau^{(1)}}_{m(j)},\ldots,{\tau^{(n_i)}}_1,\ldots,{\tau^{(n_i)}}_{m(j)}$ and $h_j^{(i)}$. Note that $\left(\sum_{l=1}^{n_i} \lambda_l^{(i)} \cdot r_h^{(l)}\right)$ does not depend on j. This proves 8.2.7 for all term functions τ. □

LEMMA 8.2.8 *Let V be an m-dimensional vector space over the finite field* GF(q) *and let $\mathfrak{A} = \langle V;\{ f_i \mid i\in I\}\rangle$ be an E-minimal algebra of affine type with $f_i = [\lambda_1^{(i)},\ldots,\lambda_{n_i}^{(i)};h_1^{(i)},\ldots,h_m^{(i)}]^q$ for all $i \in I$. Let $k \in \{1,\ldots,m\}$ and let $0 = m_0 < m_1 < \ldots < m_k = m$ be a finite sequence of integers. For every $j = 1,\ldots,m$ let $m(j)$ be the integer such that $m(j) = m_r < j \le m_{r+1}$ for some r. Moreover, suppose that for all $i \in I$ and $j \in \{1,\ldots,m\}$ the polynomial $h_j^{(i)}$ depends only on $x_1^{(1)}, x_2^{(1)},\ldots,x_{m(j)}^{(1)},\ldots,x_1^{(n_i)},\ldots,x_{m(j)}^{(n_i)}$.*

Then every $(t+1)$-ary commutator term $\tau(x^{(1)}, x^{(2)}, x^{(3)},\ldots, x^{(t)}, z)$ on $\mathfrak{A}$ with $t \ge 2$ is given by

$$\left(\tau(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(t)},z)\right)_j = z_j + s_j\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{m(j)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(t)} \\ \vdots \\ x_{m(j)}^{(t)} \end{pmatrix},\begin{pmatrix} z_1 \\ \vdots \\ z_{m(j)} \end{pmatrix}\right)$$

where the s_j are polynomials over GF(q) *in the variables $x_1^{(1)},\ldots, x_{m(j)}^{(1)}$, $\ldots, x_1^{(t)},\ldots, x_{m(j)}^{(t)}$ satisfying (for all $j \in \{1,\ldots,m\}$):*

$$\left(\exists h\in\{1,\ldots,t\} : \begin{pmatrix} x_1^{(h)} \\ \vdots \\ x_{m(j)}^{(h)} \end{pmatrix} = \begin{pmatrix} z_1 \\ \vdots \\ z_{m(j)} \end{pmatrix}\right) \Rightarrow s_j\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{m(j)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(t)} \\ \vdots \\ x_{m(j)}^{(t)} \end{pmatrix},\begin{pmatrix} z_1 \\ \vdots \\ z_{m(j)} \end{pmatrix}\right) = 0$$

Proof: Let τ be a commutator term. By lemma 8.2.7 τ can be written as:

$$\left(\tau(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(t)},z)\right)_j = \left(\sum_{h=1}^{t} r_h x_j^{(h)}\right) + r z_j + s_j\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{m(j)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(t)} \\ \vdots \\ x_{m(j)}^{(t)} \end{pmatrix},\begin{pmatrix} z_1 \\ \vdots \\ z_{m(j)} \end{pmatrix}\right)$$

We will first prove $r_h = 0$ for all $h \in \{1,\ldots,t\}$. Let $\mathbf{0} = (0,\ldots,0)$. Since τ is a commutator term and $t \geq 2$, for all $x^{(2)},x^{(3)},\ldots,x^{(j)} \in V$ the following equation holds:

$$0 = (\mathbf{0})_1 = \left(\tau(\mathbf{0},x^{(2)},x^{(3)},\ldots,x^{(t)},\mathbf{0})\right)_1 = r_1 0 + \left(\sum_{h=2}^{t} r_h x_1^{(h)}\right) + r0 + s_1 = s_1 + \sum_{h=2}^{t} r_h x_1^{(h)}$$

Therefore $s_1 = 0$ and $r_h = 0$ for all $h \in \{2,\ldots,t\}$. Since $t \geq 2$, we get similarly for all $x^{(1)} \in V$:

$$0 = (\mathbf{0})_1 = \left(\tau(x^{(1)},\mathbf{0},x^{(3)},\ldots,x^{(t)},\mathbf{0})\right)_1 = r_1 x_1^{(1)} + r0 = r_1 x_1^{(1)}$$

i.e. $r_1 = 0$, therefore $r_h = 0$ for all $h \in \{1,\ldots,t\}$. The fact that $r = 1$ follows now immediately from:

$$z_1 = \left(\tau(z,x^{(2)},x^{(3)},\ldots,x^{(t)},z)\right)_1 = rz_1$$

We have shown that τ is given by:

$$\left(\tau(x^{(1)},x^{(2)},x^{(3)},\ldots,x^{(t)},z)\right)_j = z_j + s_j\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{m(j)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(t)} \\ \vdots \\ x_{m(j)}^{(t)} \end{pmatrix},\begin{pmatrix} z_1 \\ \vdots \\ z_{m(j)} \end{pmatrix}\right)$$

Suppose $\begin{pmatrix} x_1^{(h)} \\ \vdots \\ x_{m(j)}^{(h)} \end{pmatrix} = \begin{pmatrix} z_1 \\ \vdots \\ z_{m(j)} \end{pmatrix}$ for some $h \in \{1,\ldots,t\}$, then:

$$z_j = \left(\tau(x^{(1)},\ldots,x^{(h-1)},z,x^{(h+1)},\ldots,x^{(t)},z)\right)_j$$

$$= \left(\tau\left(x^{(1)},\ldots,\begin{pmatrix} x_1^{(h)} \\ \vdots \\ x_{m(j)}^{(h)} \\ z_{m(j)+1} \\ \vdots \\ z_m \end{pmatrix},\ldots,x^{(t)},z\right)\right)_j = z_j + s_j\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{m(j)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(t)} \\ \vdots \\ x_{m(j)}^{(t)} \end{pmatrix},\begin{pmatrix} z_1 \\ \vdots \\ z_{m(j)} \end{pmatrix}\right)$$

and therefore $s_j\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{m(j)}^{(1)} \end{pmatrix},\ldots,\begin{pmatrix} x_1^{(t)} \\ \vdots \\ x_{m(j)}^{(t)} \end{pmatrix},\begin{pmatrix} z_1 \\ \vdots \\ z_{m(j)} \end{pmatrix}\right) = 0$, i.e. we have proven 8.2.8.

□

As we had already mentioned in the context of theorem 5.7.19 and in analogy to theorem 6.4.5 the dependency of the polynomials in the representation theorem 8.2.2 allows us to determine an upper bound for the class of nilpotency of a given E-minimal algebra of affine type:

THEOREM 8.2.9 *Let V be an m-dimensional vector space over the finite field* GF(q) *and let $\mathfrak{V} = \langle V;\{ f_i \mid i\in I\}\rangle$ be an E-minimal algebra of affine type with $f_i = [\lambda_1^{(i)},\ldots,\lambda_{n_i}^{(i)};h_1^{(i)},\ldots,h_m^{(i)}]^q$ for all $i \in I$. Let $k \in \{1,\ldots,m\}$ and let $0 = m_0 < m_1 < \ldots < m_k = m$ be a finite sequence of integers. For every $j = 1,\ldots,m$ let $m(j)$ be the integer such that $m(j) = m_r < j \leq m_{r+1}$ for some r. Moreover, suppose that for all $i \in I$ and $j \in \{1,\ldots,m\}$ the polynomial $h_j^{(i)}$ depends only on $x_1^{(1)}, x_2^{(1)},\ldots,x_{m(j)}^{(1)},\ldots,x_1^{(n_i)},\ldots,x_{m(j)}^{(n_i)}$.*

Then $\mathfrak{V}$ is nilpotent of class at most k.

We have chosen to present two proofs for this theorem since they use quite different tools. The first proof is analogous to the proof for 6.4.5 while the second uses the property of E-minimal algebras described in 8.1.13, i.e. that the commutator $[\iota_A,\alpha]$ is below or equal to the intersection of all congruences covered by α.

Proof 1 of Theorem 8.2.9: We will first prove the following claim by induction over h:

(8.2.10) For all $h = 0,\ldots,k$ the following holds: if π_{m_h} is the projection onto the first m_h components then $\phi_h \subseteq \ker(\pi_{m_h})$ where $\{\phi_i\}_{i=1,2,\ldots}$ is the lower central series of $\mathfrak{V}$.

If $h = 0$, then $\phi_h = \phi_0 = \iota_V = \ker(\pi_0) = \ker(\pi_{m_h})$, i.e. 8.2.10 holds for $h = 0$.

Suppose 8.2.10 is true for all $h < l$. We will show that $\phi_l \subseteq \ker(\pi_{m_l})$. By 3.3.3 and since $\phi_l = [\phi_{l-1}, \iota_V]$ it is sufficient to show that:

(8.2.11) for all commutator terms $\tau(x^{(1)}, x^{(2)}, x^{(3)}, \ldots, x^{(t)}, z)$ with $t \geq 2$ and all $x^{(1)}, x^{(2)}, x^{(3)}, \ldots, x^{(t)}, z \in V$ with $\pi_{m_{l-1}}(z) = \pi_{m_{l-1}}(x^{(1)})$:

$$\pi_{m_l}(z) = \pi_{m_l}(\tau(x^{(1)}, x^{(2)}, x^{(3)}, \ldots, x^{(t)}, z))$$

Let $\tau(x^{(1)}, x^{(2)}, x^{(3)}, \ldots, x^{(t)}, z)$ be any commutator term with $t \geq 2$ and let $x^{(1)}, x^{(2)}, x^{(3)}, \ldots, x^{(t)}, z \in V$ with $\pi_{m_{l-1}}(z) = \pi_{m_{l-1}}(x^{(1)})$. Let $j \leq m_l$. Then $m(j) \leq m_{l-1}$, where $m(j)$ is defined as in the statement of lemma 8.2.8. By this lemma we have:

$$\left(\tau(x^{(1)}, x^{(2)}, x^{(3)}, \ldots, x^{(t)}, z)\right)_j = z_j + s_j\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{m(j)}^{(1)} \end{pmatrix}, \ldots, \begin{pmatrix} x_1^{(t)} \\ \vdots \\ x_{m(j)}^{(t)} \end{pmatrix}, \begin{pmatrix} z_1 \\ \vdots \\ z_{m(j)} \end{pmatrix}\right) \quad \text{with}$$

$$\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{m(j)}^{(1)} \end{pmatrix} = \begin{pmatrix} z_1 \\ \vdots \\ z_{m(j)} \end{pmatrix} \Rightarrow s_j\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{m(j)}^{(1)} \end{pmatrix}, \ldots, \begin{pmatrix} x_1^{(t)} \\ \vdots \\ x_{m(j)}^{(t)} \end{pmatrix}, \begin{pmatrix} z_1 \\ \vdots \\ z_{m(j)} \end{pmatrix}\right) = 0$$

Since $\pi_{m_{l-1}}(z) = \pi_{m_{l-1}}(x^{(1)})$ and $m(j) \leq m_{l-1}$ this implication yields

$$s_j\left(\begin{pmatrix} x_1^{(1)} \\ \vdots \\ x_{m(j)}^{(1)} \end{pmatrix}, \ldots, \begin{pmatrix} x_1^{(t)} \\ \vdots \\ x_{m(j)}^{(t)} \end{pmatrix}, \begin{pmatrix} z_1 \\ \vdots \\ z_{m(j)} \end{pmatrix}\right) = 0$$

and therefore $\left(\tau(x^{(1)}, x^{(2)}, x^{(3)}, \ldots, x^{(t)}, z)\right)_j = z_j$ for all $j \leq m_l$. This implies $\pi_{m_l}(z) = \pi_{m_l}(\tau(x^{(1)}, x^{(2)}, x^{(3)}, \ldots, x^{(t)}, z))$, i.e. 8.2.11 and consequently 8.2.10 have been proven.

To complete the proof of 8.2.9 we only have to observe that, for $h = k$, 8.2.10 implies $\phi_k \subseteq \ker(\pi_{m_k}) = \ker(\pi_m) = \omega_V$, therefore $\phi_k = \omega_V$. This means that $\mathfrak{V}$ is nilpotent of class at most k. □

Proof 2 of Theorem 8.2.9: Let π_{m_h} be the projection onto the first m_h components of V. We will first prove that for all $h = 0,\ldots,k-1$:

(8.2.12) $$\left[\iota_V, \ker\left(\pi_{m_h}\right)\right] \leq \ker\left(\pi_{m_{h+1}}\right)$$

For $m_h < l \leq m_{h+1}$ let $\pi_{m_h,l}$ be the projection given by

$$\pi_{m_h,l}\left(\begin{pmatrix} x_1 \\ \vdots \\ x_{m_h} \\ x_{m_h+1} \\ \vdots \\ x_{l-1} \\ x_l \\ x_{l+1} \\ \vdots \\ x_m \end{pmatrix}\right) = \begin{pmatrix} x_1 \\ \vdots \\ x_{m_h} \\ x_{m_h+1} \\ \vdots \\ x_{l-1} \\ x_{l+1} \\ \vdots \\ x_{m_{h+1}} \end{pmatrix}$$

Since the polynomials $h_j^{(i)}$ depend only on $x_1^{(1)}, x_2^{(1)}, \ldots, x_{m(j)}^{(1)}, \ldots, x_1^{(n_i)}, \ldots, x_{m(j)}^{(n_i)}$ the kernel of $\pi_{m_h,l}$ is a congruence. It is clear that, since $\ker(\pi_0) > \ker(\pi_1) > \ldots > \ker(\pi_m)$ is a maximal chain of congruences on $\mathfrak{V}$, $\ker(\pi_0) > \ker(\pi_1) > \ldots > \ker(\pi_{m_h}) > \ker(\pi_{m_h,l}) > \ker(\pi_{m_h,l}) \cap \ker(\pi_{m_h+1}) > \ldots > \ker(\pi_{m_h,l}) \cap \ker(\pi_{l-1}) > \ker(\pi_{l+1}) > \ldots > \ker(\pi_m)$ is also a maximal chain. Therefore π_{m_h} covers $\pi_{m_h,l}$ and we get by lemma 8.1.13:

$$\left[\iota_A, \ker\left(\pi_{m_h}\right)\right] \leq \bigcap \left\{ \gamma \in \mathfrak{C}(\mathfrak{A}) \;\middle|\; \ker\left(\pi_{m_h}\right) \text{ covers } \gamma \right\}$$

$$\leq \bigcap \left\{ \ker\left(\pi_{m_h,l}\right) \middle|\; m_h < l \leq m_{h+1} \right\} = \ker\left(\pi_{m_{h+1}}\right)$$

i.e. 8.2.12 has been proven.

Now let $\{\phi_i\}_{i=1,2,\ldots}$ be the lower central series of $\mathfrak{V}$. By induction over h we will show that $\phi_h \leq \ker(\pi_{m_h})$ for all $h = 0,1,\ldots,k$. This statement is immediately clear for $h = 0$. Now suppose it is true for $i = h-1$, i.e. $\phi_{h-1} \leq \ker(\pi_{m_{h-1}})$. By 8.2.12 and 3.1.4 (8) we have therefore:

$$\begin{aligned}\phi_h = \left[\iota_V, \phi_{h-1}\right] &\leq \left[\iota_V, \ker\left(\pi_{m_{h-1}}\right)\right] \\ &\leq \ker\left(\pi_{m_h}\right)\end{aligned}$$

which proves $\phi_h \leq \ker(\pi_{m_h})$ for all $h = 0,1,\ldots,k$. For $h = k$ this means $\phi_k \leq \ker(\pi_{m_k}) = \ker(\pi_m) = \omega_V$, i.e. $\mathfrak{V}$ is nilpotent of class at most k. □

Note that this theorem 8.2.9 implies theorem 5.7.19. We had omitted the proof of the latter theorem since it is a consequence of the former.

8.3. Subdirectly Irreducible E-Minimal Algebras of Affine Type

For finite nilpotent squags and finite nilpotent SQS-skeins we had seen that our representation can be used to characterize the subdirectly irreducible algebras: a finite nilpotent squag or finite nilpotent SQS-skein is subdirectly irreducible if and only if in its representation $n_{k-1} = m-1$, i.e. every class of the centre contains q elements (see theorem 5.7.20, theorem 6.4.2 part 8 and corollary 6.4.3). Example 7.4.5 showed that this is not necessarily true for p-groups, i.e. it can't be true for all E-minimal algebras of affine type. Nevertheless, one implication still holds:

THEOREM 8.3.1 *Let $\mathfrak{A} = \langle A; \{f_i \mid i \in I\}\rangle$ be an E-minimal algebra of affine type with $|[x]\zeta(\mathfrak{A})| = q$ for some element $x \in A$ and some prime q. Then $\mathfrak{A}$ is subdirectly irreducible.*

Proof: By theorems 8.2.4 and 8.2.6 there exists an m-dimensional vector space V over a finite field GF(q'), for every i $\in$ I an operation $[\lambda_1^{(i)},\ldots,\lambda_{n_i}^{(i)};h_1^{(i)},\ldots,h_m^{(i)}]^{q'}$ as described above with n_i being the arity of f_i, and an isomorphism

$$\phi : \mathfrak{A} \rightarrowtail\!\!\!\!\rightarrow \mathfrak{V} = \langle V;\{[\lambda_1^{(i)},\ldots,\lambda_{n_i}^{(i)};h_1^{(i)},\ldots,h_m^{(i)}]^{q'} \mid i\in I\}\rangle$$

such that $\zeta(\mathfrak{V})$ corresponds to the kernel of the projection onto the first n components of V and $\phi(x) = (0,\ldots,0)$. Since $|[x]\zeta(\mathfrak{A})| = q$ and q is prime, we may conclude immediately that $q = q'$ and $n = m-1$. Consider the sequence of congruences $\alpha_0 > \alpha_1 >\ldots> \alpha_m$ defined by $\alpha_j = \ker(\pi_j)$ where π_j is the projection onto the first j components of V. Note that $\alpha_{m-1} = \zeta(\mathfrak{V})$. By 8.2.2 this sequence of congruences is maximal. Therefore $\zeta(\mathfrak{V})$ is an atom in $\mathfrak{C}(\mathfrak{V})$. By 3.2.10 $\mathfrak{V}$ and $\mathfrak{A}$ are subdirectly irreducible. □

9. Open Questions

9.1. The Theorem of Bruck and Slaby

The research leading to this dissertation was initiated by the question whether the theorem of Bruck and Slaby (theorem 5.4.1) can be generalized to a larger variety of algebras. The author was unable to find a generalization, but would therefore like to pose the following question: Which additional properties must be required of $\mathfrak{V}$ to ensure the correctness of the following statement: If $\mathfrak{V}$ is an E-minimal variety of affine type, i.e. a variety in which every finite algebra is an E-minimal algebra of affine type, then then there exists a function $f(n) = (a\ n + c)$ such that every n-generated algebra in $\mathfrak{V}$ is of nilpotence class at most $f(n)$.

More specifically it should be investigated whether any variety of nilpotent squags is locally finite, and—in the case of an affirmative answer—whether a theorem similar to the theorem of Bruck and Slaby can be proven for said variety.

9.2. The Commutator

By theorem 5.3.3 the squag theoretic commutator (defined by a single commutator term) coincides with the universal algebraic commutator if one of the congruences is ι. While the author believes this also to be true if none of the congruences is ι, this is still an unsettled question. Note that any counterexample must have at least 243 elements, since the statement is trivial for medial squags and known to be true for the unique non-medial 81-element squag (H_{81}).

It is well known that the universal algebraic commutator for groups coincides with the group theoretic commutator which is defined using a single commutator term. A positive answer of the question mentioned in the previous paragraph will obviously raise

the question whether in every E-minimal variety of affine type the commutator can be defined with one or a finite number of commutator terms. Note that theorem 3.3.3 states that the commutator in every congruence permutable and nilpotent variety can be defined by all (i.e. possibly infinitely many) commutator terms.

9.3. Semi-Boolean SQS-Skeins

Since it was believed that the semi-boolean SQS-skeins are exactly the SQS-skeins that arise from boolean groups (a statement which we have shown to be incorrect), the variety of semi-boolean SQS-skeins has escaped investigation. The immediate questions are whether every semi-boolean SQS-skein is nilpotent (and we can therefore apply the theory of nilpotent SQS-skeins) and whether this variety is locally finite. If these questions can be answered positively, then the semi-booloean SQS-skeins may behave similar as the distributive squags and it would be reasonable to explore whether they in fact have the same properties. It would be especially interesting to know whether there are semi-boolean SQS-skeins of every nilpotence class and whether an analogue of the theorem of Bruck and Slaby can be proven. Note that both semi-boolean SQS-skeins and distributive squags can be selected from among the SQS-skeins and squags respectively by properties of the corresponding designs (see theorem 6.7.2 and section 4.3).

9.4. Construction Theorems

Of all the construction theorems in this thesis only one allows the formation of an algebra (a nilpotent SQS-skein) that has a larger class of nilpotence than any of the algebras required for it. Since this theorem therefore allows the construction of SQS-skeins of arbitrary large nilpotence class it would be useful to have similar theorems for nilpotent squags, distributive squags and semi-boolean SQS-skeins.

Bibliography

ADIAN, S. I.

1979 [1975] *The burnside problem and identities in groups*. Translated from the Russian by J. Lennox and J. Wiegold. Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. **95**. Berlin, Heidelberg, and New York: Springer-Verlag. Originally published as *Проблема Бернсаидства в Группах.* (Moscow: Nauka, 1975).

ADIAN, S. I., and P. S. NOVIKOV

1968 Infinite periodic groups I–III. *Izv. Akad. Nauk. SSSR Ser. Mat.* **32**, no. 1: 214–244, no. 2: 251–524, no. 3: 709–731.

ARMANIOUS, M. H.

1980 *Algebraische Theorie der Quadrupelsysteme*. Dissertation. Fachbereich der Mathematik der Technischen Hochschule Darmstadt, Federal Republic of Germany.

1989 A Die Varietät der auflösbaren Ternare der Ordnung 2. *Beiträge zur Algebra und Geometrie*. **28**: 33–37.

1989 B Classification of Steiner Quadruple Systems of Cardinality 32. *Beiträge zur Algebra und Geometrie*. **28**: 39–50.

n.d. Existence of nilpotent SQS-skeins of class *n*. Preprint.

BASS, H.

1972 The degree of polynomial growth of finitely generated nilpotent groups. *Proc. London Math. Soc.* **25**, no. 3: 603–614.

BÉNÉTEAU, L.

1975 A Boucles de Moufang d'exposant 3 et quasi-groupes de Steiner distributifs. *C. R. Acad. Sc. Paris* **281**, Série A: 75–76.

1975 B Classification des espaces barycentrés et des espaces planairement affines. *C. R. Acad. Sc. Paris* **281**, Série A: 9–11.

1977 A Les groupes de Fischer au sens restreint: dimension, et classe de nilpotence du dérivé. *C. R. Acad. Sc. Paris* **285**, Série A: 693–695.

1977 B Les groupes de Fischer au sens restreint: majorants pour l'ordre en fonction de la dimension. *C. R. Acad. Sc. Paris* **285**, Série A: 735–737.

1980 A Free commutative Moufang loops and anticommutative graded rings. *Journal of Algebra* **67**: 1–35.

1980 B Topics about 3-Moufang loops and Hall triple systems. *Simon Stevin* **67**, no. 2: 107–124.

1980 C Le quotients de Frattini d'une boucle de Moufang commutative. *C. R. Acad. Sc. Paris* **290**, Série A: 443–446.

1980 D Une classe particulière de matroïdes parfaits. Proc. colloque franco-canadien de Combinatoire, Juin 1979, *Annals of Discrete Mathematics* **8**: 229–232.

1981 A *Contribution à l'étude de Moufang commutatives et des espaces apparentés*. Thèse d'Etat, Universite de Provence, Marseille, France.

1981 B Les systèmes triples de Hall de dimension 4. *Europ. J. Combinatorics* **2**: 205 - 212.

1981 C Ordre minimum des boucles de Moufang de classe 2 (resp. 3). *Annales Faculté des Sciences Toulouse* **3**: 75–88.

1982 The geometry of distributive quasigroups. *Rendiconti del Seminario Matematico di Brescia* **70**: 57–65.

1983 A Hall triple systems and related topics. In *Proceedings of the International Conference on Combinatorial Geometries and their Applications*. Ed. by A. Barlotti, P. V. Ceccherini, and G. Lallini. *Annals of Discrete Mathematics* **18**: 55–60.

1983 B L'irréductibilité centrale dans les boucles de Moufang commutatives et dans les systèmes triples de Hall. *Discrete Mathematics* **45**: 31–44.

1983 C Quasigroupes distributifs provenant de certaines algebres. *Communications in Algebra* **11**, no. 9: 913–935.

1983 D Quelques consequences de la locale nilpotence des boucles de Moufang commutatives. *Communications in Algebra* **11**, no. 15: 1725 - 1753.

1983 E Une conjecture sur les suites centrales d'une boucle de Moufang commutative libre. *Note di Mathematica* **3**: 45–53.

1984 A The Hall triple systems of small class. *Europ. J. Combinatorics* **5**: 1–5.

1984 B 3-Abelian groups and commutative Moufang loops. *Europ. J. Combinatorics* **5**: 193 –196.

BÉNÉTEAU, L., and J. LACAZE

1980 Groupes d'automorphismes des boucles de Moufang commutatives. *Europ. J. Combinatorics* **1**: 299–309.

BERMAN, J., and BLOK, W. J.

1987 Free spectra of nilpotent varieties. *Algebra Universalis* **24**: 279–282.

BOL, G.

1937 Gewebe und Gruppen. *Mathematische Annalen* **114**: 414–431.

BRUCK, R. H.

1971 *A survey of binary systems*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, vol. **20**. New York, Heidelberg, and Berlin: Springer-Verlag.

FREESE, R. S., and R. N. MCKENZIE

1987 *Commutator theory for congruence modular varieties*. London Mathematical Society Lecture Note Series, **125**. Cambridge: Cambridge University Press.

DAY, A., and H. P. GUMM

n.d. Some characterization of the commutator. Preprint.

GANTER, B., and H. WERNER

1975 A Equational Classes of Steiner Systems. *Algebra Universalis* **5**: 125–140.

1975 B Equational Classes of Steiner Systems II. Proc. Conf. Algebraic Aspects of Combinatorics, Toronto 1975. *Congressus Numerantium* **XIII**: 283–285.

1980 Co-ordinatizing Steiner systems. *Annals of Discrete Mathematics* **7**: 3–24.

GIBBONS, P. B.

1976 *Computing techniques for the construction and analysis of block designs*. Ph.D. thesis, University of Toronto.

GOLOD, E. S.

1965 [1964] On nil-algebras and finitely approximable p-groups. *Amer. Math. Soc. Transl.*, **48**, Ser. 2: 103–106. Originally published in Russian in *Izv. Akad. Nauk. SSSR Ser. Mat.* **28** (1964): 273–276.

GRÄTZER, G.

1979 [1968] *Universal algebra.* 2nd ed. New York, Heidelberg, and Berlin: Springer-Verlag. Originally published in the University Series in Higher Mathematics (D. Van Nostrand Company, 1968).

GRIGORČUK, R. I.

1980 On the Burnside problem for periodic groups. *Functional Anal. Appl.* **14**: 41–43. Originally published in Russian in *Funkcional. Anal. i Priložen.* **14**: 53–54.

GÜLZOW, A.

1983 *Die verschiedenen Nilpotenzbegriffe in der Theorie der distributiven Squags im Vergleich.* Diplomarbeit, Gesamthochschule Kassel, Universität des Landes Hessen, Federal Republic of Germany.

GUMM, H. P.

1980 An easy way to the commutator in modular varieties. *Arch. Math.* **34**: 220–228.

1983 *Geometrical methods in congruence modular algebras.* Mem. Amer. Math. Soc., **45**. Providence, RI: American Mathematical Society.

GUPTA, N. D., and S. SIDKI

1983 On the Burnside problem for periodic groups. *Math. Z.* **182**: 385–388.

HALL, M., JR.

1960 Automorphisms of Steiner triple systems. *IBM Journal of Research and Development*: 460–472.

HANANI, H.

1960 On quadruple systems. *Canad. J. Math.* **12**: 145–157.

HARTLEY, B.

1984 Topics in the Theory of Nilpotent Groups. In *Group Theory, essays for Philip Hall.* Ed. by K. W. Gruenberg and J. E. Roseblade. London: Academic Press.

HERRMANN, CH.

1979 Affine algebras in congruence modular varieties. *Acta Sci. Math. (Szeged)* **41**: 119–125.

HOBBY, D., and R. MCKENZIE

1988 *The structure of finite algebras.* Contemporary Mathematics. Vol. **76**. Providence, RI: American Mathematical Society.

HUPPERT, B.

1967 *Endliche Gruppen I.* Die Grundlehren der mathematischen Wissenschaften. Vol. **134**. Berlin, Heidelberg, and New York: Springer-Verlag.

KARGAPOLOV, M. I., and MERZLJAKOV, JU. I.

1979 [1977] *Fundamentals of the Theory of Groups.* Translated from the Second Russian Edition by R. G. Burns. Graduate Texts in Mathematics, vol. **62**. Berlin, Heidelberg, and New York: Springer-Verlag. Originally published as *Основы Теории Групп.* (Moscow: Nauka, 1977).

KEPKA, T.

1978 Distributive Steiner quasigroups of order 3^5. *Commentationes Mathematicae Universitatis Carolinae* **19,** no. 2: 389–401.

KLOSSEK, S.

1975 Kommutative Spiegelungsräume. *Mitteilungen aus dem mathematischen Seminar Gießen,* **117**.

KOSTRIKIN, A. I.

1989 *Around Burnside*. Translated from the Russian by J. Wiegold. Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, vol. **20**. Berlin, Heidelberg, and New York: Springer-Verlag. Originally published as *Вокруг бернсайда*.

LINDNER, CH. C., and ROSA, A.

1978 Steiner Quadruple Systems — A Survey. *Discrete Mathematics* **21**: 147–181.

LOOS, O.

1967 Spiegelungsräume und homogene symmetrische Räume. *Mathematische Zeitschrift* **99**: 141–170.

MENDELSOHN, E.

1975 On the Groups of Automorphisms of Steiner Triple And Quadruple Systems. Proceedings of the Conference on Algebraic Aspects of Combinatorics, University of Toronto 1975. *Congressus Numerantium*. **XIII**: 255–264.

NEUMANN, H.

1967 *Varieties of Groups*. Ergebnisse der Mathematik und ihrer Grenzgebiete, New Series, vol. **37**. New York: Springer-Verlag.

QUACKENBUSH, R. W.

1975 Algebraic aspects of Steiner quadruple systems. Proceedings of the Conference on Algebraic Aspects of Combinatorics, University of Toronto 1975. *Congressus Numerantium*. **XIII**: 265–268.

1976 Varieties of Steiner loops and Steiner quasigroups. *Can. J. Math.* **28**, no. 6: 1187–1198.

1980 Algebraic speculations about Steiner systems. *Annals of Discrete Mathematics* **7**:25–36.

ROTH, R. L., JR.

1979 *Hall Triple Systems and Commutative Moufang Exponent 3 Loops*. Dissertation, The Ohio State University.

SIDKI, S.

1987 On a 2-generated infinite 3-group. Parts 1, 2. *Journal of Algebra* **110**: 13–23, 24–55.

SIMS, C. C.

1965 Enumerating p-groups. *Proc. London Math. Soc.* **15**, no. 3: 151–166.

SMITH, J. D. H.

1976 *Mal'cev varieties*. Lecture Notes in Mathematics. Vol. **554**. Berlin, Heidelberg, and New York: Springer-Verlag.

1978 On the nilpotence class of commutative Moufang loops. *Math. Proc. Camb. Phil. Soc.* **84**: 387–404.

1984 Two enumeration principles for free algebras. *Acta Univ. Carolin. Math. Phys.* **25**, no. 1: 53–58.

SOUBLIN, J. P.

1971 Étude algébrique de la notion moyenne. *Journal de Mathématiques pures et appliquees* **50**.

TAYLOR, W.

1982 Some applications of the term condition. *Algebra Universalis* **14**: 11–24.

VAUGHAN-LEE, M. R.

1983 Nilpotence in permutable varieties. In *Universal Algebra and Lattice Theory*. Edited by R. S. Freese and O. C. Garcia. Lecture Notes in Mathematics. Berlin, Heidelberg, New York, and Tokyo: Springer-Verlag.

WEINSTEIN, M.

1977 *Examples of groups*. Passaic, N. J.: Polygonal Publishing House.

Index

Bold numbers indicate the page of the definition or introduction of a term. All symbols (except fixed names for algebras such as B_n) are collected at the end of this index.