The Structure of Composition Algebras

(Die Struktur von Kompositionsalgebren)

Dissertation
zur Erlangung des akademischen Grades
eines Doktors der Technischen Wissenschaften

vorgelegt von
Dipl.-Ing. Erhard Aichinger

Angefertigt am Institut für Algebra, Stochastik und
wissensbasierte mathematische Systeme
der technisch-naturwissenschaftlichen Fakultät
der Johannes Kepler Universität Linz

bei
O.Univ.-Prof. Dr. Günter Pilz

Gefördert durch ein Doktorandenstipendium der
österreichischen Akademie der Wissenschaften

Linz, im Mai 1998

Begutachter:

Prof.Dr.Günter Pilz
Institut für Algebra, Stochastik und wissenbasierte mathematische Systeme
Johannes Kepler Universität Linz, Österreich

Prof.Dr.Kalle Kaarli
Institut für Mathematik
Universität Tartu, Estland

Vorwort

Als ich im Mai 1994 mit der Arbeit an meiner Dissertation begann, wollte ich Kompositionsringe untersuchen. Kompositionsringe entstehen, wenn man die Menge aller Funktionen auf einem Ring mit den Operationen der punktweisen Addition und Multiplikation, sowie mit der Operation der Hintereinanderausführung von Funktionen versieht.

Ein Anliegen der Algebraiker ist es, interessante und erstaunliche Eigenschaften einer Klasse von Algebren herzuleiten. Verfolgen wir diese Arbeit am Beispiel der Fastkörper: Fastkörper sind zunächst durch recht steril klingende Bedingungen definiert. Sie sind jene algebraische Strukturen, die bei der Koordinatisierung bestimmter projektiver Ebenen auftreten. Es ist nun H. Zassenhaus gelungen, alle endlichen Fastkörper zu beschreiben: man erhält diese schönen Strukturen durch Verdrehen der Körpermultiplikation eines endlichen Körpers — bis auf sieben Ausnahmefastkörper, die Zassenhaus explizit angeben konnte.

Kompositionsringe haben mit Fastringen gemeinsam, daß sie als Algebren von Funktionen auf einer anderen Algebra entstehen. Daher hoffte ich, den Kompositionsringen mit den Werkzeugen der Fastringtheorie, besonders mit den Dichtesätzen, erfolgreich zu Leibe rücken. Natürlich war schon einiges über Kompositionsringe bekannt: Man wußte, daß jeder Kompositionsring als Kompositionsring von Funktionen auf einem Ring aufgefaßt werden kann, was Cayleys Satz in der Gruppentheorie entspricht. I. Adler hatte im Jahr 1962 alle Kompositionsringe von Funktionen auf einem Körper bestimmt, die zumindest jede konstante Funktion enthalten. Die Dichtesätze in der Hand, glaubte ich, einige weitere Fragen klären zu können. Darunter war zum Beispiel die Bestimmung aller einfachen Kompositionsringe. Was mir dazu eingefallen ist, erfährt der Leser im fünften Kapitel dieser Dissertation.

Gleichzeitig interessierte ich mich für ein anderes Problem: Wie lassen sich Polynomfunktionen auf Gruppen und auf universellen Algebren beschreiben? Welche Funktionen lassen sich von Polynomfunktionen an einer gewissen Anzahl von Stellen interpolieren? Eine Bedingung, die eine Polynomfunktion erfüllen muß, ist, daß sie Kongruenzen erhält. Also ist es natürlich, zu fragen, wann jede kongruenzerhaltende Funktion eine Polynomfunktion ist. Algebren, bei denen das der Fall ist, nennen wir *affin vollständig*. Herrn K. Kaarli verdanke ich den Hinweis, daß eines der bedeutendsten Resultate zu diesem Thema in einer Arbeit von J. Hagemann und Chr. Herrmann enthalten ist. Da deren Arbeit aber

Konzepte verwendet, die erst später gründlich studiert wurden, so zum Beispiel die Kommutatortheorie für universelle Algebren, lassen sich die Resultate heute eindringlicher als zur Zeit ihrer Entstehung formulieren. Zum anderen sind mir die Beweise in dieser Arbeit bis heute ein Rätsel. Da also kein Weg an Hagemanns und Herrmanns Resultaten vorbeiführte, sah ich mich gezwungen, sie erneut zu beweisen. Dazu habe ich die Beweise, daß bestimmte Ringe und Gruppen affin vollständig sind, in die Sprache der universellen Algebra übersetzt. Dort, wo diese Übertragung den Inhalt verschleiert hat, habe ich auch die Beweise angegeben, von denen ich ausgegangen bin. Ich habe meine Einsicht in diese Resultate durch die universelle Sichtweise aber doch wesentlich verbessern können. Im letzten Kapitel dieser Arbeit habe ich die Resultate von Hagemann und Herrmann über affin vollständige Algebren noch einmal kurz zusammengestellt.

Eigentlich bin ich zum Kommutator aber ganz anders als durch die universelle Algebra gekommen: Was man bei der Interpolation einer Funktion auf einem Körper mithilfe der Multiplikation schafft, geht in der universellen Algebra mithilfe des Kommutators. Multiplikationen auf Algebren, die eine Körpermultiplikation imitieren, wurden schon von H.K. Kaiser verwendet. Den Dichtesatz für Fastringe kann man recht anschaulich beweisen, wenn man Funktionen in passender Weise multipliziert. Auch S.D. Scott multiplizierte, allerdings nicht Elemente oder Funktionen, sondern Ideale in Ω-Gruppen. In dieser Arbeit erkläre ich, wie sich diese Multiplikationen auf den Kommutator, wie er in der universellen Algebra studiert wird, zurückführen lassen.

G. Betsch, S.V. Polin, D. Ramakotaiah und H. Wielandt haben eine sehr systematischen Strukturtheorie der Fastringe geschaffen, die sich auf Interpolationsresultaten aufbauen läßt. Welche Auswirkungen können also die Interpolationsaussagen der universellen Algebra auf die Strukturtheorie von Kompositionsringen, oder überhaupt auf andere Algebren, die den Fastringen ähnlich sind, haben? Da ich Verallgemeinerungen dieser Interpolationsresultate zur Verfügung hatte, konnte ich viele Resultate von Fastringen auf "rechtsdistributive universellen Algebren", die dann Kompositionsalgebren heißen, übersetzen. Die wesentliche Botschaft dieser Arbeit ist, daß sich viel aus der Fastringtheorie auf die rechtsdistributiven Algebren hinüberretten läßt, deren Addition sich zumindest in einer Hinsicht wie eine Gruppenoperation verhält: die Kongruenzen der additiven Struktur dieser Algebra müssen bezüglich des Relationsprodukts vertauschbar sein. Das ist schon bei Loops, das sind "nichtassoziative Gruppen", immer der Fall. Diese Verallgemeinerungen sind aber nicht nur für jene Algebren fruchtbar, deren additive Struktur ärmer als die der Fastringe ist. Was sie bringen, kommt auch dann heraus, wenn man die universell algebraischen Resultate auf Kompositionsringe anwendet.

Während der Entwicklungen der theoretischen Resultate habe ich immer wieder einzelne Fragestellungen am Computer untersucht. Die brauchbaren Programme stehen im Paket SONATA für das Gruppentheoriesystem GAP, und sind daher nicht in dieser Arbeit enthalten.

Ich danke Günter Pilz für die Betreuung und der österreichischen Akademie der Wissenschaften für die Finanzierung dieser Arbeit; ebenso danke ich Kalle Kaarli und Paweł Idziak für hilfreiche Anleitungen und meinen Kollegen Franz Binder, Tim Boykett, Jürgen Ecker und Christof Nöbauer für zahlreiche Diskussionen und Kommentare. Den Dank für private Unterstützung möchte ich persönlich abstatten; lediglich meinen Eltern Gertraud und Bruno Aichinger sei die Freude nicht verwehrt, hier namentlich erwähnt zu werden.

Linz, im Mai 1998

Preface

When I started to work on this thesis four years ago, my idea was to investigate composition rings. Those arise if one provides the set of all functions on a ring with the operations of pointwise addition and multiplication and with the operation of functional composition.

An algebraist's goal is to detect interesting and surprising properties of a class of algebras. Near-fields provide a good example for the algebraists' work: reading the way they are defined, they might seem as yet another structure of the "quasi-, infra-, semi-, hemi-, para-, skew-, near-" type. On a closer view, one finds out that near-fields naturally arise in the coordinatization of certain projective planes. It was H.Zassenhaus who succeeded in describing all finite near-fields: these beautiful structures can be constructed from finite fields by doing some harm to the multiplication – except for seven sporadic near-fields that Zassenhaus managed to describe explicitly.

Composition rings and near-rings have in common that they are algebras of functions on another algebra. This suggested to me that the tools of near-ring theory, especially the density theorems, might prove useful also for composition rings. What was known about composition rings? It was known that every composition ring can be embedded into a composition ring of functions on a ring. This corresponds to Cayley's result in group theory. In 1962, I.Adler determined all composition rings of functions on a field that contain all constant functions. Using the density theorems, I hoped to settle some other questions. Among these is the determination of all simple composition rings. What I have been able to do in this direction can be found in the fifth chapter of this thesis.

At the same time, I was interested in the following type of questions: How can one describe and distinguish polynomial functions on groups and universal algebras? Which functions can be interpolated by a polynomial function at a fixed number of places? We know that every polynomial function preserves the congruences of an algebra. So we may ask on which algebras every congruence preserving function is polynomial. Algebras where this is the case have been called *affine complete*. K.Kaarli pointed out to me that J.Hagemann and Chr.Herrmann have proved a central result on this topic. Since they have used concepts that were to be studied more thouroghly only later, such as the theory of commutators in universal algebra, their results can be formulated more easily today. On the other hand, Hagemann's and Herrmann's proofs are difficult to follow. Given the

importance of these results, I have provided new proofs for them, which I have obtained by translating the proofs that certain classes of groups are affine complete into the language of universal algebra. What we thereby gain in generality is sometimes outweighed by added notational complications, so, at some places, I have included the original proofs. However, to me, the universal algebraic viewpoint is often the clearest one.

In this thesis, the commutator plays an important role. The first place where I met commutator theory, however, was not universal algebra: if one tries to interpolate functions, then what one can do in fields using the field multiplication can often be done in universal algebras using commutators. Multiplications that emulate field multiplications have already been studied by H.K.Kaiser. The density theorem for near-rings can be proved in an intuitive way by introducing a suitable way of multiplying functions. And also S.D.Scott liked to multiply, but not elements in an algebras or functions, but rather ideals in Ω-groups. In the present thesis I explain what these multiplications have to do with commutators in universal algebra.

G.Betsch, S.V.Polin, D.Ramakotaiah, and H.Wielandt have developed a very systematic structure theory for near-rings that can be based on interpolation results. So it seemed likely that the interpolation results in universal algebra might have impacts on the structure of composition rings or other similar universal algebras. And really – many results for near-rings can be translated to "right distributive universal algebras", which are called "composition algebras". One of the central messages of the present thesis is that many results for near-rings still hold for structures whose "addition" behaves like a group operation at least in one respect: the congruences of the additive structure must commute with respect to the relation product. This is already the case for loops; these are "non-associative groups". These generalizations are not only fertile for those algebras that have less structure than near-rings. What they are good for also comes out if one applies the universal algebraic results to composition rings.

During the theoretical part of this research, I have computed lots of examples on the computer. The usable functions arising from this enterprise can be found in the package SONATA for the group theory system GAP, and are therefore not contained in this thesis.

I want to thank Günter Pilz for supervising, and the Austrian Academy of Science for financing the work on this thesis. Kalle Kaarli and Paweł Idziak have provided helpful suggestions, and Franz Binder, Tim Boykett, Jürgen Ecker, and Christof Nöbauer have spent a lot of time discussing this material with me. Also personally I owe a great deal to several persons, but the reader will allow me to thank them personally; at this place I just want to thank my parents, Gertraud and Bruno Aichinger, for their support.

Linz, May 1998

Contents

Vorwort 1

Preface 5

Chapter 1. Prerequisites 9
1. Algebras and Varieties 9
2. Congruences and Mal'cev conditions 11
3. Commutators 16
4. Abelian algebras 18
5. Neutral algebras 20
6. Ω-groups 21
7. Various concepts of commutator operations for Ω-groups 23
8. Abelian Ω-groups 28

Chapter 2. An interpolation result for function algebras 29
1. Function algebras 29
2. The interpolation result 29

Chapter 3. Composition algebras 39
1. Adding composition 39
2. Local interpolation algebras 43
3. Modules of composition algebras 50
4. The structure of composition algebras with constants 58
5. The structure of some composition algebras with a left identity 70

Chapter 4. Tame composition algebras on Ω-groups 83
1. Tame near-rings 83

Chapter 5. Composition Rings 89
1. The definition of composition rings 89
2. Simple Zero-Symmetric Composition Rings 90
3. Composition rings with constants 95

Chapter 6. On Hagemann's and Herrmann's characterization of strictly affine complete algebras 103
1. Varieties generated by algebras that have only neutral subalgebras 103
2. Strictly affine complete algebras 105
3. Affine complete algebras 108
4. Some consequences for polynomial interpolation 109

Bibliography 113

CHAPTER 1

Prerequisites

In the present chapter, we give a brief repetition of the algebraic and notational prerequisites that we shall need in the sequel. We write $\mathbb{N}$ for the set of natural numbers $\{1, 2, 3, \ldots\}$, $\mathbb{N}_0$ for $\mathbb{N} \cup \{0\}$, and $\mathbb{Z}$ for the set of integers. A set whose cardinality is finite or countably infinite will be called *countable*.

1. Algebras and Varieties

We use the notation of [**Ihr93**], which is very similar to the notation used in standard references on universal algebra such as [**BS81**] and [**MMT87**]. A short and concise introduction to the notions of universal algebra is also given in [**HM88**, pp.5-16]. An *n-ary operation* on a set A is a function from A^n to A. A *type of algebras* is a pair $\tau = (\mathcal{F}, \sigma)$, where $\mathcal{F}$ is a set and σ a function from $\mathcal{F}$ to $\mathbb{N}_0$. The elements of $\mathcal{F}$ are called *operation symbols*, for $f \in \mathcal{F}$, the number $\sigma(f)$ denotes the *arity* of f. The element f is then called a *$\sigma(f)$-ary operation symbol*. The set $\mathcal{F}_n := \{f \in \mathcal{F} \mid \sigma(f) = n\}$ is called the set of *all n-ary operation symbols*.

An *algebra* of type $(\mathcal{F}, \sigma)$ is a pair $\mathbf{A} = (A, F)$, where A is a non-empty set and $F = (f_{\mathbf{A}} \mid f \in \mathcal{F})$ is a family of operations on A, where an operation $f_{\mathbf{A}} : A^{\sigma(f)} \to A$ is assigned to each $f \in \mathcal{F}$. The set A is called the *universe* of $\mathbf{A}$ and the elements of F are called *fundamental operations* of $\mathbf{A}$. For the algebra $\mathbf{A} = (A, F)$ with $F = (f_1, f_2, \ldots)$ we will also write $(A; f_1, f_2, \ldots)$ if it is clear how the operations $f_1, f_2, \ldots$ are assigned to the operation symbols in $\mathcal{F}$. A subset B of A is called *subuniverse* of $\mathbf{A}$ iff it is closed under all fundamental operations of $\mathbf{A}$. The algebra $\mathbf{B}$ is called a *subalgebra* of $\mathbf{A}$ iff $\mathbf{A}$ and $\mathbf{B}$ are of the same type, the universe B of $\mathbf{B}$ is a subuniverse of $\mathbf{A}$, and each fundamental operation of $\mathbf{B}$ is the restriction of the corresponding fundamental operation of $\mathbf{A}$. Sometimes, we want to forget about some operations of the algebra $\mathbf{A}$: If $\mathbf{A}$ is an algebra of type $(\mathcal{F}_1, \sigma_1)$ and $\mathbf{B}$ is an algebra of type $(\mathcal{F}_2, \sigma_2)$, then $\mathbf{B}$ is *a reduct* of $\mathbf{A}$ iff $B = A$, $\mathcal{F}_2 \subseteq \mathcal{F}_1$ and and for all operation symbols ω in $\mathcal{F}_2$, we have $\omega_{\mathbf{B}} = \omega_{\mathbf{A}}$. If $\mathbf{B}$ is a reduct of $\mathbf{A}$, then $\mathbf{A}$ is called an *expansion* of $\mathbf{B}$.

We will now define three notions that will be important throughout this thesis: These are *terms*, *term functions* and *polynomial functions*. The definitions of these notions can also be found in [**MMT87**, Definitions 4.120, 4.2, and 4.4] and [**Ihr93**, Definitions 6.2.1, 6.2.6, and 6.2.10]. We adopt [**BS81**, Definitions 10.1,10.2, and 13.3]. Let $(\mathcal{F}, \sigma)$ be a type, and let X be a set. In this

context, we call the elements of X *variables*. Then the set $T(X)$ of *terms of type* $(\mathcal{F}, \sigma)$ *over* X is the smallest set such that

(1) $X \cup \{f \in \mathcal{F} \mid \sigma(f) = 0\} \subseteq T(X)$. This means that every variable and every nullary function symbol is a term.
(2) If $p_1, p_2, \ldots, p_n \in T(X)$ and f is an n-ary function symbol of $\mathcal{F}$, then the "string" $f(p_1, p_2, \ldots, p_n)$ is an element of $T(X)$.

Let $X = \{x_1, x_2, \ldots, x_k\}$, and let $\mathbf{A}$ be an algebra of type $(\mathcal{F}, \sigma)$. Then every term t of the same type induces a function from A^k to A. This function is denoted by $t_{\mathbf{A}}$, and is defined as follows:

(1) If $t = x_i$, then

$$t_{\mathbf{A}}(a_1, a_2, \ldots, a_k) = a_i \text{ for all } a_1, a_2, \ldots, a_k \in A.$$

(2) If $t = f$ with $f \in \mathcal{F}, \sigma(f) = 0$, then

$$t_{\mathbf{A}}(a_1, a_2, \ldots, a_k) = f_{\mathbf{A}}() \text{ for all } a_1, a_2, \ldots, a_k \in A.$$

(3) If $t = f(t^{(1)}, t^{(2)}, \ldots, t^{(n)})$ with $f \in \mathcal{F}, \sigma(f) = n$, and all $t^{(i)} \in T(X)$, then

$$t_{\mathbf{A}}(a_1, a_2, \ldots, a_k) = f_{\mathbf{A}}(t^{(1)}_{\mathbf{A}}(a_1, a_2, \ldots, a_k), t^{(2)}_{\mathbf{A}}(a_1, a_2, \ldots, a_k), \ldots, t^{(n)}_{\mathbf{A}}(a_1, a_2, \ldots, a_k))$$

for all $a_1, a_2, \ldots, a_k \in A$.

Every such function is called a *k-ary term function*. The set of all k-ary term functions on $\mathbf{A}$ will be abbreviated by $\mathsf{T}_k(\mathbf{A})$.

Polynomial functions arise from term functions by plugging in some constants: A function $p : A^k \to A$ is called a *k-ary polynomial function* on $\mathbf{A}$ iff there exist $n \geq 0$, $b_1, b_2, \ldots, b_n \in A$, and a $k+n$-ary term function f on $\mathbf{A}$ such that

$$p(a_1, a_2, \ldots, a_k) = f(a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_n) \text{ for all } a_1, a_2, \ldots, a_k \in A.$$

The set of all k-ary polynomial functions on $\mathbf{A}$ will be abbreviated by $\mathsf{P}_k(\mathbf{A})$.

Small boldface letters stand for vectors; hence $\mathbf{a}$ stands for $(a_1, a_2, \ldots, a_k)$.

A class of algebras of the same type $(\mathcal{F}, \sigma)$ is called a *variety* iff it is closed under the formation of direct products, subalgebras and homomorphic images. This is the case iff the class can be described using identites:

DEFINITION 1.1. Let $\mathbf{A}$ be an algebra and let $t^{(1)}, t^{(2)}$ be terms of type $(\mathcal{F}, \sigma)$ over the variables $x_1, x_2, \ldots, x_k$. Then $t^{(1)} = t^{(2)}$ is an *identity* of $\mathbf{A}$ iff for all $\mathbf{a} \in A^k$ we have $t^{(1)}_{\mathbf{A}}(\mathbf{a}) = t^{(2)}_{\mathbf{A}}(\mathbf{a})$.

For example, the group $\mathbf{G} = (G; +)$ is abelian iff $x_1 + x_2 = x_2 + x_1$ is an identity of $\mathbf{G}$.[1]

2. Congruences and Mal'cev conditions

The set of all congruences of an algebra $\mathbf{A}$ is denoted by $Con\,\mathbf{A}$. For two congruences α and β of $\mathbf{A}$, we denote the largest equivalence relation that is contained in both α and β by $\alpha \wedge \beta$. It is given by

$$\alpha \wedge \beta = \alpha \cap \beta.$$

It is easy to see that $\alpha \wedge \beta$ is again a congruence on $\mathbf{A}$. We denote the smallest equivalence relation that contains both α and β by $\alpha \vee \beta$. It is given by

$$\alpha \vee \beta = \\ \alpha \cup \beta \cup (\alpha \circ \beta) \cup (\beta \circ \alpha) \cup (\alpha \circ \beta \circ \alpha) \cup (\beta \circ \alpha \circ \beta) \cup (\alpha \circ \beta \circ \alpha \circ \beta) \cup \cdots .$$

Here $\alpha \circ \beta$ denotes the relation product $\{(a, b) \mid \exists z \in A : (a, z) \in \alpha \text{ and } (z, b) \in \beta\}$. The relation $\alpha \vee \beta$ is again a congruence on $\mathbf{A}$. Now $(Con\,\mathbf{A}; \wedge, \vee)$ is a lattice. We abbreviate this lattice by $\mathbf{Con\ A}$. In this thesis, we are mainly considered with algebras whose congruences satisfy $\alpha \circ \beta = \beta \circ \alpha$, which is the case for all groups. If $\alpha \circ \beta = \beta \circ \alpha$, we have $\alpha \vee \beta = \alpha \circ \beta$.

For $\alpha \in Con\,\mathbf{A}$ and $a \in A$, the set $\{a' | (a', a) \in \alpha\}$ is denoted by a/α. The congruence relation $\{(a, a) | a \in A\}$ will usually be denoted by $\mathbf{0_A}$, the congruence relation $A \times A$ by $\mathbf{1_A}$. The congruence generated by (a, b) with $a, b \in A$ will be denoted by $\Theta_{\mathbf{A}}(a, b)$. Let Θ be a congruence on the algebra $\mathbf{A}$. If $a, b \in A$ are congruent modulo Θ, we shall write $(a, b) \in \Theta$, $a \overset{\Theta}{\equiv} b$, or $a \equiv b \pmod{\Theta}$. For $\mathbf{a}, \mathbf{b} \in A^k$, we say $\mathbf{a} \equiv \mathbf{b} \pmod{\Theta}$ iff $a_i \equiv b_i \pmod{\Theta}$ for $i = 1, 2, \ldots, k$. Furthermore, by $\Theta_{\mathbf{A}}(\mathbf{a}, \mathbf{b})$ we denote the congruence on $\mathbf{A}$ generated by $(a_1, b_1), (a_2, b_2), \ldots, (a_k, b_k)$.

Let $(\mathbf{A}_i)_{i \in I}$ be a family of algebras of the same type. Then a subalgebra $\mathbf{D}$ of $\prod_{i \in I} \mathbf{A}_i$ is a *subdirect product* of the family $\mathbf{A}_i$ iff for each $i \in I$ the projection from $\mathbf{D}$ to the ith component is surjective.

In this section, we look at functions that go from some set D into an algebra $\mathbf{A}$. Of course, we cannot compose two functions of that kind (unless we imitate the construction of sandwich near-rings); but we will nevertheless get a useful interpolation result. Let $\mathbf{A}$ be a universal algebra and let D be a set. We form the algebra $\mathbf{A}^D$ that consists of all functions from D to A with operations defined pointwisely. This algebra is called the *direct product of* $\mathbf{A}$*, indexed by* D. A subalgebra $\mathbf{B}$ of $\mathbf{A}^D$ forms a *subdirect product* iff for all $d \in D$ the mapping $\pi_d : B \to A$, $b \mapsto b(d)$ is surjective. We also call every subalgebra of $\mathbf{A}^D$ a *function algebra from* D *to* $\mathbf{A}$.

[1] We will sometimes see groups as algebras with one binary operation $+$; at other times, groups will be regarded as algebras with a binary operation $+$, a unary operation $-$ of forming the inverse, and a nullary operation 0 giving the identity of the group.

Let D and A be sets, and let F be a subset of A^D. For each cardinal number n we form the set $\mathsf{L}_n F$ of all functions with domain D that can be interpolated at n places by a function in F. Formally, this reads as follows:

DEFINITION 1.2. Let D and A be sets, and let F be a subset of A^D. Then for every cardinal number n we define the set $\mathsf{L}_n F$ by

$$\mathsf{L}_n F := \{l : D \to A \,|\, \forall S \subseteq D \,:\, |S| \leq n \Rightarrow \exists f \in F : f|_S = l|_S\}.$$

Clearly, for all cardinals s, b with $s \leq b$ we have $F \subseteq \mathsf{L}_b F \subseteq \mathsf{L}_s F \subseteq A^D$.

We shall make use of the following two ternary partial functions on an algebra $\mathbf{A}$. The *Mal'cev operation* m of $\mathbf{A}$ is defined on $\{(x,y,y) \,|\, x,y \in A\} \cup \{(y,y,x) \,|\, x,y \in A\}$ by

$$m(y,y,x) = m(x,y,y) = x.$$

The *Pixley operation* p of $\mathbf{A}$ is defined on $\{(x,y,y) \,|\, x,y \in A\} \cup \{(x,y,x) \,|\, x,y \in A\} \cup \{(y,y,x) \,|\, x,y \in A\}$ by

$$p(x,y,y) = p(x,y,x) = p(y,y,x) = x.$$

We abbreviate the Pixley operation on $\mathbf{A}$ by $\mathsf{Pix}(\mathbf{A})$ and the Mal'cev operation on $\mathbf{A}$ by $\mathsf{Mal}(\mathbf{A})$. On some algebras, the Mal'cev and the Pixley operations are restrictions of term functions. For example, on every group $\mathbf{G}$ we have $\mathsf{Mal}(\mathbf{G})(x,y,z) = x - y + z$. On the two element field $\mathbf{GF}(2)$, we can write the Pixley operation as $\mathsf{Pix}(\mathbf{GF}(2))(x,y,z) = x + z + xy + xz + yz$.

For any partial function f, we denote its domain by $\mathsf{dom}(f)$.

The importance of Mal'cev and Pixley operations lies in the following fact: If an algebra has a term function which is a Mal'cev operation or a Pixley operation, then its congruences behave in a certain way. We are going to make this more precise in the following two propositions. We call an algebra *congruence permutable* if for each pair (α, β) of congruences of $\mathbf{A}$ the relation product $\alpha \circ \beta$ is equal to the product $\beta \circ \alpha$. If α and β fulfil $\alpha \circ \beta = \beta \circ \alpha$, then their join in the lattice $\mathbf{Con}\ \mathbf{A}$ is given by $\alpha \vee \beta = \alpha \circ \beta$ [**Ihr93**, Bemerkung 5.1.4].

PROPOSITION 1.3 (cf. [**Ihr93**, Satz 6.4.2]). *If* $\mathsf{Mal}(\mathbf{A})$ *can be interpolated at each subset of its domain with at most two elements by a term function in* $\mathsf{T}_3(\mathbf{A})$*, then* $\mathbf{A}$ *is congruence permutable.*

Proof: We fix $\alpha, \beta \in Con\,\mathbf{A}$. Let $(a,b) \in \alpha \circ \beta$. Let $c \in A$ be such that $(a,c) \in \alpha$ and $(c,b) \in \beta$. Now let t be a term function on $\mathbf{A}$ that interpolates the Mal'cev operation $\mathsf{Mal}(\mathbf{A})$ at (a,b,b) and (b,b,c). Then we have:

$$a = t(a,b,b) \overset{\beta}{\equiv} t(a,b,c) \overset{\alpha}{\equiv} t(b,b,c) = c.$$

This implies $(a,b) \in \beta \circ \alpha$. □

We call an algebra *arithmetical* if it is congruence permutable and if its lattice of congruences is distributive. This is for example the case in the ring of integers.

Other algebras with the same property can be found with the help of the following proposition:

PROPOSITION 1.4 (cf. [**Ihr93**, Satz 6.4.8]). *If* $\mathsf{Pix}(\mathbf{A})$ *can be interpolated at every subset of its domain with at most four elements by a term function in* $\mathsf{T}_3(\mathbf{A})$*, then* $\mathbf{A}$ *is arithmetical.*

Proof: Since the Mal'cev operation on an algebra is a restriction of the Pixley operation, Proposition 1.3 yields that $\mathbf{A}$ is congruence permutable. For proving that **Con A** is a distributive lattice, lattice theory (in particular, [**MMT87**, Theorem 2.51]) tells that that it is sufficient to prove

$$\alpha \wedge (\beta \vee \gamma) \leq (\alpha \wedge \beta) \vee (\alpha \wedge \gamma) \text{ for all } \alpha, \beta, \gamma \in \mathit{Con}\,\mathbf{A}.$$

We fix $\alpha, \beta, \gamma \in \mathit{Con}\,\mathbf{A}$ and $a, b \in A$ such that $(a, b) \in \alpha \wedge (\beta \vee \gamma)$. Since $\mathbf{A}$ is congruence permutable, $\beta \vee \gamma$ is equal to $\beta \circ \gamma$, and therefore we have a $c \in A$ such that $(a, c) \in \beta$ and $(c, b) \in \gamma$. Let p be term function on $\mathbf{A}$ that interpolates the Pixley operation at $\{(a, a, b), (a, b, b), (a, c, a), (a, a, a)\}$. Then we have the following relations:

(1) $a = p(a, a, a) = p(a, p(a, c, a), a) \overset{\alpha}{\equiv} p(a, p(a, c, b), b)$. This holds because of $(a, b) \in \alpha$.
(2) $a = p(a, b, b) = p(a, p(a, a, b), b) \overset{\beta}{\equiv} p(a, p(a, c, b), b)$. This holds because of $(a, c) \in \beta$.
(3) $p(a, p(a, c, b), b) \overset{\alpha}{\equiv} p(b, p(b, c, b), b) = b$.
(4) $p(a, p(a, c, b), b) \overset{\gamma}{\equiv} p(a, p(a, b, b), b) = p(a, a, b) = b$. This holds because of $(b, c) \in \gamma$.

Putting together the first two congruences, we obtain

$$a \equiv p(a, p(a, c, b), b) \pmod{\alpha \wedge \beta}.$$

Putting together the third and the fourth congruence, we obtain

$$p(a, p(a, c, b), b) \equiv b \pmod{\alpha \wedge \gamma}.$$

Altogether, we get $(a, b) \in (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$, which we had to prove. □

For $\mathbf{A}$, let $\mathcal{SP}_f\mathbf{A}$ denote the class of all subalgebras of direct products of finitely many copies of $\mathbf{A}$. The following term conditions describe whether the class $\mathcal{SP}_f\mathbf{A}$ is congruence permutable or arithmetical. (A class of algebras is congruence permutable (arithmetical) iff each of its members has this property.)

PROPOSITION 1.5. *For a universal algebra* $\mathbf{A}$*, the following are equivalent.*

(1) $\mathcal{SP}_f\mathbf{A}$ *is congruence permutable.*
(2) $\mathsf{Mal}(\mathbf{A})$ *can be interpolated at every finite subset of its domain by a term function on* $\mathbf{A}$*.*

Proof: (1) $\Rightarrow$ (2): Let D be a finite subset of $\mathsf{dom}\,(\mathsf{Mal}\,(\mathbf{A}))$, and let $\mathbf{T}$ be the function algebra from D to $\mathbf{A}$ with universe $\{t|_D \,|\, t \in \mathsf{T}_3\,(\mathbf{A})\}$. Since $\mathbf{T} \in \mathcal{SP}_f\mathbf{A}$, it is congruence permutable. Let $\overline{x}, \overline{y}, \overline{z}$ be the elements of $\mathbf{T}$ defined by $\overline{x}(d_1, d_2, d_3) = d_1, \overline{y}(d_1, d_2, d_3) = d_2, \overline{z}(d_1, d_2, d_3) = d_3$. We define two congruences Θ_1, Θ_2 on $\mathbf{T}$ by

$$\Theta_1 := \{(t_1, t_2) \,|\, \forall x, y \in D : t_1(x, y, y) = t_2(x, y, y)\}$$
$$\Theta_2 := \{(t_1, t_2) \,|\, \forall x, y \in D : t_1(y, y, x) = t_2(y, y, x)\}.$$

Then we have $\overline{x} \equiv \overline{y} \pmod{\Theta_2}$ and $\overline{y} \equiv \overline{z} \pmod{\Theta_1}$. Altogether, this gives

$$\overline{x} \equiv \overline{z} \pmod{\Theta_2 \circ \Theta_1},$$

and hence, by congruence permutablility,

$$\overline{x} \equiv \overline{z} \pmod{\Theta_1 \circ \Theta_2}.$$

This yields an element $m \in T$ with $\overline{x} \equiv m \pmod{\Theta_1}$ and $m \equiv \overline{z} \pmod{\Theta_2}$. The last two conditions imply that m interpolates $\mathsf{Mal}\,(\mathbf{A})$ on D: in fact, for all $x, y \in D$ we have $\overline{x}(x, y, y) = m(x, y, y)$ and hence $x = m(x, y, y)$; in the same way we get $m(y, y, x) = \overline{z}(y, y, x) = x$.
(2) $\Rightarrow$ (1): Let $\mathbf{B}$ be a subalgebra of $\mathbf{A}^k$ for some natural number $k \in \mathbb{N}$. We want to show that $\mathbf{B}$ is congruence permutable. For this, it is sufficient to show that $\mathsf{Mal}\,(\mathbf{B})$ can be interpolated at every finite subset D of its domain by a function in $\mathsf{T}_3\,(\mathbf{B})$. (Actually, by Proposition 1.3, we could even restrict ourselves to the case that D has two elements.) We define D' to be the subset of A^3 given by

$$D' := \{(x_i, y_i, z_i) \,|\, (\mathbf{x}, \mathbf{y}, \mathbf{z}) \in D;\, i = 1, 2, \ldots, k\}.$$

The set D' is finite and a subset of the domain of the Mal'cev operation on $\mathbf{A}$; hence there is a term t such that the induced term function $t_{\mathbf{A}}$ interpolates the Mal'cev operation $\mathsf{Mal}\,(\mathbf{A})$ on D'. Then one can easily convince oneself that the function $t_{\mathbf{B}}$, which is the function that t induces on $\mathbf{B}$, interpolates $\mathsf{Mal}\,(\mathbf{B})$ on D. □

Proposition 1.6. *For a universal algebra* $\mathbf{A}$*, the following are equivalent.*

(1) $\mathcal{SP}_f\mathbf{A}$ *is arithmetical.*
(2) $\mathsf{Pix}\,(\mathbf{A})$ *can be interpolated at every finite subset of its domain by a term function on* $\mathbf{A}$*.*

Proof: (1) $\Rightarrow$ (2): Let D be a finite subset of $\mathsf{dom}\,(\mathsf{Pix}\,(\mathbf{A}))$, and let $\mathbf{T}$ be the function algebra from D to $\mathbf{A}$ with universe $\{t|_D \,|\, t \in \mathsf{T}_3\,(\mathbf{A})\}$. Since $\mathbf{T} \in \mathcal{SP}_f\mathbf{A}$, it is arithmetical. Let $\overline{x}, \overline{y}, \overline{z}, \Theta_1, \Theta_2$ be as in the proof of Proposition 1.5 and let Θ_3 be the congruence on $\mathbf{T}$ defined by

$$\Theta_3 := \{(t_1, t_2) \,|\, \forall x, y \in D : t_1(x, y, x) = t_2(x, y, x)\}.$$

As above, we have $\overline{x} \equiv \overline{z} \pmod{\Theta_1 \circ \Theta_2}$. It is obvious that we also have $\overline{x} \equiv \overline{z} \pmod{\Theta_3}$. Altogether, we get $\overline{x} \equiv \overline{z} \pmod{(\Theta_1 \circ \Theta_2) \wedge \Theta_3}$, and therefore, by arithmeticity, $\overline{x} \equiv \overline{z} \pmod{(\Theta_1 \wedge \Theta_3) \circ (\Theta_2 \wedge \Theta_3)}$. Hence there exists an element

p in T such that $\overline{x} \equiv p \pmod{\Theta_1 \wedge \Theta_3}$ and $p \equiv \overline{z} \pmod{\Theta_2 \wedge \Theta_3}$. The first condition gives $p(x, y, y) = x$ and $p(x, y, x) = x$; the second gives $p(y, y, x) = x$ and, again, $p(x, y, x) = x$. Hence p interpolates the Pixley operation at D.
(2) $\Rightarrow$ (1): We replace "Mal'cev operation" with "Pixley operation" and repeat the proof of (2) $\Rightarrow$ (1) of Proposition 1.5. □

Given an algebra $\mathbf{A}$ and a subset D of A^3, we say that a ternary function f is *a Mal'cev function on D* iff $f(\mathbf{x}) = \mathsf{Mal}(\mathbf{A})(\mathbf{x})$ for all $\mathbf{x} \in D \cap \mathsf{dom}(\mathsf{Mal}(\mathbf{A}))$. We say that f is *a Pixley function on D* iff $f(\mathbf{x}) = \mathsf{Pix}(\mathbf{A})(\mathbf{x})$ for all $\mathbf{x} \in D \cap \mathsf{dom}(\mathsf{Pix}(\mathbf{A}))$. Actually, Proposition 1.5 tells the following: $\mathcal{SP}_f\mathbf{A}$ is congruence permutable if and only if there is a Mal'cev function $f \in \mathsf{T}_3(\mathbf{A})$ on D for every finite subset D of A^3.

If the class $\mathcal{SP}_f\mathbf{A}$ is congruence permutable, the following helpful lemma makes it easy to check for relations whether they are congruences.

LEMMA 1.7. *Let $\mathbf{A}$ be an algebra for which $\mathcal{SP}_f\mathbf{A}$ is congruence permutable. Let ρ be a relation on A such that*

(1) *ρ is a reflexive relation.*
(2) *For all $\mathbf{a}, \mathbf{b} \in A^2$ with $\mathbf{a} \equiv \mathbf{b} \pmod{\rho}$, and $p \in \mathsf{P}_2(\mathbf{A})$ we have $p(\mathbf{a}) \equiv p(\mathbf{b}) \pmod{\rho}$.*

Then ρ is a congruence relation on $\mathbf{A}$.

This lemma is of course applicable to all algebras that lie in a congruence permutable variety.

Proof: By assumption, ρ is reflexive.[2]

For symmetry, we assume that (a, b) lies in ρ. Let $t \in \mathsf{T}_3(\mathbf{A})$ be the term function that interpolates the Mal'cev function on $\{(a, a, b), (a, b, b)\}$, and let p be the polynomial function in $\mathsf{P}_2(\mathbf{A})$ defined by

$$p(x, y) := t(a, x, b).$$

Then condition (2) gives that $(p(a, a), p(b, b))$ lies in ρ. But we have $(p(a), p(b)) = (t(a, a, b), t(a, b, b)) = (b, a)$, and hence (b, a) lies in ρ.

For showing that ρ is transitive, we assume that (a, b) and (b, c) lie in ρ. Let $t \in \mathsf{T}_3(\mathbf{A})$ be the term function that interpolates the Mal'cev function on $\{(a, c, c), (b, b, c)\}$, and let p be the polynomial function in $\mathsf{P}_2(\mathbf{A})$ defined by

$$p(x, y) := t(x, y, c).$$

Since ρ is symmetric, we know that (c, b) lies in ρ. Hence condition (2) gives that $(p(a, c), p(b, b))$ lies in ρ. But we have $(p(c), p(b)) = (t(a, c, c), t(b, b, c)) = (a, c)$, and hence (a, c) lies in ρ. This shows that ρ is also transitive. Hence ρ is an equivalence relation.

[2]One can weaken the first condition from "ρ is reflexive" to "ρ is not the empty set".

For showing that ρ is a congruence, let $(a, b) \in \rho$ and let f be an n-ary fundamental operation of $\mathbf{A}$. We fix $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n \in A$ and show
(2.1)
$$f(x_1, x_2, \ldots, x_{i-1}, a, x_{i+1}, \ldots, x_n) \equiv f(x_1, x_2, \ldots, x_{i-1}, b, x_{i+1}, \ldots, x_n) \pmod{\rho}.$$
We consider the binary polynomial function defined by

$$p(u, v) := f(x_1, x_2, \ldots, x_{i-1}, u, x_{i+1}, \ldots, x_n).$$

(Of course, the polynomial function p does not depend on v.) By the fact that ρ is preserved under binary polynomial functions, we have $p(a, a) \equiv p(b, b) \pmod{\rho}$, which implies (2.1). □

3. Commutators

In the textbook [**FM87**] on the theory of commutators in universal algebra, several commutator operations are defined. The commutator definition that we are going to use in the present thesis is the one of [**HM88**, p.42, Exercises 3.8 (3)]. The same definition can also be found in [**MMT87**, p.252]. For congruence modular varieties, this commutator operation is the same as the operation denoted by $[.,.]$ in [**FM87**, p.29].

Definition 1.8 ([**MMT87**, Definition 4.150]). Let α, β be two congruence relations on the universal algebra $\mathbf{A}$. Then the commutator $[\alpha, \beta]$ of α and β is the smallest congruence η on $\mathbf{A}$ for which the following condition holds:

For all $k \in \mathbb{N}$, $t \in \mathsf{T}_k(\mathbf{A})$, $a, b \in A$, $\mathbf{c}, \mathbf{d} \in A^{k-1}$ we have

$$\left.\begin{array}{l} a \equiv b \pmod{\alpha} \\ \mathbf{c} \equiv \mathbf{d} \pmod{\beta} \\ t(a, \mathbf{c}) \equiv t(a, \mathbf{d}) \pmod{\eta} \end{array}\right\} \Longrightarrow t(b, \mathbf{c}) \equiv t(b, \mathbf{d}) \pmod{\eta}. \tag{3.1}$$

At first glance, it is not obvious that a smallest congruence with these properties really exists. The reason for the existence of a smallest congruence with these properties is given in [**MMT87**, Lemma 4.149].

Commutators are the universal algebraic formulation of concepts that had been widely used in classical algebra before: The concept specializes to the concept of commutator subgroups of two normal subgroups in the theory of groups, and to the ideal product in the case of rings [**MMT87**, p.258, Exercises 11 and 12]. A description of the commutator in certain algebras with group reduct is given in Proposition 1.24.

We want to recall briefly the main properties of the commutator operation $[.,.] : Con\,\mathbf{A} \times Con\,\mathbf{A} \to Con\,\mathbf{A}$ for congruence modular varities (cf. [**FM87**, Proposition 4.3]). We assume that $\mathbf{A}$ is an algebra living in a congruence modular variety and that α, β, γ are congruences of $\mathbf{A}$.

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

(2) $[\alpha, \beta] \leq \alpha \wedge \beta$
(3) $\alpha \leq \beta \Rightarrow [\alpha, \gamma] \leq [\beta, \gamma]$
(4) $[\alpha \vee \beta, \gamma] = [\alpha, \gamma] \vee [\beta, \gamma]$
(5) (cf. [**FM87**, Proposition 4.4 (1)]) If f is an epimorphism from $\mathbf{A}$ onto $\mathbf{B}$, then we have

$$\varphi^{-1}\big([\varphi(\alpha \vee \ker f), \varphi(\beta \vee \ker f)]\big) = [\alpha, \beta] \vee \ker f. \tag{3.2}$$

Here φ is the mapping from the congruences of $\mathbf{A}$ above $\ker f$ to the congruences of $\mathbf{B}$ defined as follows:

$$\varphi(\alpha) := \{(f(a_1), f(a_2)) \mid (a_1, a_2) \in \alpha\}.$$

By the diamond lemma, φ is a bijection, and therefore it is meaningful to speak also of its inverse φ^{-1}. We observe that the first commutator in (3.2) is taken in $Con\,\mathbf{B}$ and the second one in $Con\,\mathbf{A}$.

We want to give one application of this "commutator calculus", in which group theorists will discover a known lemma due to H. Wielandt.

LEMMA 1.9 (Wielandt). *Let $\mathbf{A}$ be an algebra in a congruence modular variety; and let $\alpha, \beta, \gamma \in Con\,\mathbf{A}$. Then we have*

$$[(\alpha \vee \gamma) \wedge (\beta \vee \gamma), (\alpha \vee \gamma) \wedge (\beta \vee \gamma)] \leq (\alpha \wedge \beta) \vee \gamma.$$

In group theory, this lemma reads as follows: If A, B, C are normal subgroups of the group $(G; +)$, then the group defined by

$$((A + C) \cap (B + C))/((A \cap B) + C)$$

is abelian. H. Wielandt proved a stronger version of this result [**Pil83**, Proposition 2.23].

Proof:

$$\begin{aligned}
[(\alpha \vee \gamma) \wedge (\beta \vee \gamma), (\alpha \vee \gamma) \wedge (\beta \vee \gamma)] &\leq [\alpha \vee \gamma, \beta \vee \gamma] \\
&= [\alpha, \beta] \vee [\alpha, \gamma] \vee [\gamma, \beta] \vee [\gamma, \gamma] \\
&\leq [\alpha, \beta] \vee \gamma \\
&= (\alpha \wedge \beta) \vee \gamma.
\end{aligned}$$

□

DEFINITION 1.10. An algebra $\mathbf{A}$ is called *abelian* iff $[\mathbf{1_A}, \mathbf{1_A}] = \mathbf{0_A}$.

Let us single out abelian algebras in some interesting varieties. All statements will be consequences of Proposition 1.29.

(1) A group is abelian iff it satisfies the equation $x + y = y + x$.
(2) A ring is abelian iff it satisfies the equation $x \cdot y = 0$.
(3) A near-ring [**Pil83**] is abelian iff it satisfies the equations $x + y = y + x$ and $x \circ y = x \circ 0$. All those near-rings can be obtained as follows:
    Start with an abelian group $\mathbf{G}$ and and an endomorphism e on $\mathbf{G}$ that satisfies $e \circ e = e$. Then define $x \circ y = e(x)$.

What we call an abelian near-ring is not what is called an abelian near-ring in classical near-ring theory. We stay consistent with universal algebra terminology; another motivation to distinguish near-rings that satisfy the identites $x + y = y + x$ and $x \circ y = x \circ 0$ is given by [**IK79**].

(4) Let $\mathbf{R}$ be a ring. Then every $\mathbf{R}$-module is abelian.

Furthermore, from the definition of commutators one sees that every algebra that has only unary fundamental operations is abelian.

4. Abelian algebras

DEFINITION 1.11. Let $\mathbf{A} = (A; +)$ be a group with identity element 0. Then a function $f : A^k \to A$ is called *affine* with respect to $+ :\Leftrightarrow$

$$\forall \mathbf{x}, \mathbf{y} \in A^k : f(\mathbf{x} + \mathbf{y}) - f(\mathbf{y}) = f(\mathbf{x}) - f(\mathbf{0}).$$

Here we have used $a - b$ as an abbreviation of $a + (-b)$, and $\mathbf{a} + \mathbf{b}$ as abbreviation of $(a_1 + b_1, a_2 + b_2, \ldots, a_k + b_k)$.

Actually, affine functions are the sum of a homomorphism and a constant function:

PROPOSITION 1.12. *Let $\mathbf{A} = (A; +)$ be a group. Then a function $f : A^k \to A$ is affine with respect to $+$ iff the function g defined by $g(\mathbf{x}) := f(\mathbf{x}) - f(\mathbf{0})$ is a homomorphism from A^k to A.*

Proof: If f is affine, we can compute

$$\begin{aligned} g(\mathbf{x} + \mathbf{y}) &= f(\mathbf{x} + \mathbf{y}) - f(\mathbf{0}) \\ &= f(\mathbf{x} + \mathbf{y}) - f(\mathbf{y}) + f(\mathbf{y}) - f(\mathbf{0}) \\ &= f(\mathbf{x}) - f(\mathbf{0}) + f(\mathbf{y}) - f(\mathbf{0}) \\ &= g(\mathbf{x}) + g(\mathbf{y}). \end{aligned}$$

On the other hand, if $\mathbf{x} \mapsto f(\mathbf{x}) - f(\mathbf{0})$ is a homomorphism, we have

$$\begin{aligned} f(\mathbf{x} + \mathbf{y}) - f(\mathbf{y}) &= f(\mathbf{x} + \mathbf{y}) - f(\mathbf{0}) + f(\mathbf{0}) - f(\mathbf{y}) \\ &= f(\mathbf{x}) - f(\mathbf{0}) + f(\mathbf{y}) - f(\mathbf{0}) + f(\mathbf{0}) - f(\mathbf{y}) \\ &= f(\mathbf{x}) - f(\mathbf{0}). \end{aligned}$$

This proves the result. □

Now we can state the main result about abelian algebras in congruence permutable varieties. Compare also [**MMT87**, Theorem 4.155].

PROPOSITION 1.13 ([**Gum79**]). *Let $\mathbf{A}$ be an abelian algebra in a congruence permutable variety with Mal'cev term d. Let 0 be any element in A and define an addition on $\mathbf{A}$ by*

$$a + b := d_{\mathbf{A}}(a, 0, b).$$

Then the following conditions hold:

(1) $(A;+)$ *is an abelian group,*
(2) *The inverse of* a *in the group* $(A;+)$ *is given by* $-a := d(0,a,0)$.
(3) *We have* $d_{\mathbf{A}}(a,b,c) = a + (-b) + c$ *for all* $a,b,c \in A$.
(4) *Every polynomial function* $p \in \mathsf{P}_k(\mathbf{A})$ *is affine with respect to* $+$.

Proof: [**Ihr93**, Satz 8.3.4]. □

For the converse, we have the following well-known result:

PROPOSITION 1.14. *Let* $\mathbf{A}$ *be an algebra of type* $(\mathcal{F},\sigma)$ *with a function* $+ \in \mathsf{P}_2(\mathbf{A})$ *such that* $(A;+)$ *is an abelian group and all fundamental operations of* $\mathbf{A}$ *are affine with respect to* $+$. *Then* $\mathbf{A}$ *is abelian.*

Proof: We observe that under these assumptions not only the fundamental operations, but actually all polynomial functions on $\mathbf{A}$ are affine with respect to $+$. We use the definition of commutators given in Definition 1.8 for proving $[\mathbf{1_A},\mathbf{1_A}] = \mathbf{0_A}$. Let $k \in \mathbb{N}$, $a,b \in A$, $\mathbf{c},\mathbf{d} \in A^{k-1}$, and let $t \in \mathsf{T}_k(\mathbf{A})$ such that $t(a,\mathbf{c}) = t(a,\mathbf{d})$. The function t is affine and we get

$$t(a,\mathbf{c}) = t(a,\mathbf{0}) - t(0,\mathbf{0}) + t(0,\mathbf{c}).$$

In the same way, we get

$$t(a,\mathbf{d}) = t(a,\mathbf{0}) - t(0,\mathbf{0}) + t(0,\mathbf{d}).$$

Hence the equality $t(a,\mathbf{c}) = t(a,\mathbf{d})$ implies $t(0,\mathbf{c}) = t(0,\mathbf{d})$. Therefore we have

$$\begin{aligned} t(b,\mathbf{c}) &= t(b,\mathbf{0}) - t(0,\mathbf{0}) + t(0,\mathbf{c}) \\ &= t(b,\mathbf{0}) - t(0,\mathbf{0}) + t(0,\mathbf{d}) \\ &= t(b,\mathbf{d}). \end{aligned}$$

This implies $[\mathbf{1_A},\mathbf{1_A}] = \mathbf{0_A}$. □

Just for getting familiar with these notations, let us do a little exercise. A more general version of this result is given in [**MMT87**, Lemma 4.153]. As in [**MMT87**, p.39], we use $\mathbf{M_3}$ to denote the diamond lattice with five elements.

LEMMA 1.15 ([**MMT87**]). *Let* $\mathbf{A}$ *be an algebra in a congruence modular variety that has congruences* $\alpha_1,\alpha_2,\alpha_3$ *with the property that* $\{\mathbf{0_A},\alpha_1,\alpha_2,\alpha_3,\mathbf{1_A}\}$ *is the universe of a sublattice of* $\mathbf{Con\ A}$ *isomorphic to the diamond lattice* $\mathbf{M_3}$. *Then* $\mathbf{A}$ *is abelian.*

Proof: We have

$$\begin{aligned} [\mathbf{1_A},\mathbf{1_A}] &= [\alpha_1 \vee \alpha_2, \alpha_1 \vee \alpha_3] \\ &= [\alpha_1,\alpha_1] \vee [\alpha_1,\alpha_3] \vee [\alpha_2,\alpha_1] \vee [\alpha_2,\alpha_3] \\ &= [\alpha_1,\alpha_1] \vee \mathbf{0_A} \\ &= [\alpha_1,\alpha_1]. \end{aligned}$$

Hence we have

$$[\mathbf{1_A},\mathbf{1_A}] \leq \alpha_1.$$

For the same reason, we have $[\mathbf{1_A}, \mathbf{1_A}] \leq \alpha_2$ and therefore $[\mathbf{1_A}, \mathbf{1_A}] \leq \alpha_1 \wedge \alpha_2 = \mathbf{0_A}$. This proves that $\mathbf{A}$ is abelian. □

5. Neutral algebras

DEFINITION 1.16. An algebra $\mathbf{A}$ in which all congruences α, β satisfy $[\alpha, \beta] = \alpha \wedge \beta$ is called *neutral*.

Let us give some examples of neutral algebras:

(1) Let $\mathbf{R}$ be a finite ring which is isomorphic to a direct product of fields. Then $\mathbf{R}$ is neutral.
(2) A finite group is neutral if and only if it has a principal series in which all the factors are non-abelian.
(3) Every simple non-abelian algebra is neutral.
(4) Every Boolean algebra is neutral [**MMT87**, p.258, Exercise 5].
(5) Every semilattice is neutral [**MMT87**, p.258, Exercise 5].

Furthermore, it is proved in [**FM87**, Exercise 8.3] that a variety $\mathcal{V}$ of congruence modular algebras is congruence distributive iff every algebra of $\mathcal{V}$ is neutral. A single neutral algebra in a congruence modular variety has distributive congruences [**FM87**, Exercise 8.1].

For checking whether an algebra is neutral we do not have to check all pairs of congruences:

LEMMA 1.17. *Let $\mathbf{A}$ be a universal algebra. Then $\mathbf{A}$ is neutral iff $[\alpha, \alpha] = \alpha$ for all $\alpha \in Con\,\mathbf{A}$.*

Proof: The "only if"-part is obvious. For the "if"-part, let β and γ be two congruences of $\mathbf{A}$. By its definition, the commutator is monotonous in both arguments, i.e., $\alpha_1 \leq \alpha_2$ and $\beta_1 \leq \beta_2$ implies $[\alpha_1, \beta_1] \leq [\alpha_2, \beta_2]$. Hence we have $[\beta, \gamma] \geq [\beta \wedge \gamma, \beta \wedge \gamma] = \beta \wedge \gamma$. □

Let us quickly repeat two properties of neutral algebras that we need in the sequel.

PROPOSITION 1.18 ([**FM87**, Exercise 8.2]). *Let $(\mathbf{A}_i)_{i \in I}$ be a family of finitely many neutral algebras in a congruence modular variety, and let $\mathbf{D}$ be a subdirect product of $(\mathbf{A}_i)_{i \in I}$. Then $\mathbf{D}$ is neutral.*

DEFINITION 1.19 ([**BS81**, Definition 11.5]). Let $\mathbf{D}$ be a subdirect product of $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$. Then $\mathbf{D}$ is *skew-free* iff for every congruence $\theta \in Con\,\mathbf{D}$ there are congruences $\theta_1, \theta_2, \ldots, \theta_n$ with $\theta_i \in Con\,\mathbf{A}_i$ such that

$$\theta = (\theta_1 \times \theta_2 \times \cdots \times \theta_n) \cap D^2.$$

In this definition, we use the notation

$$\theta_1 \times \theta_2 \times \cdots \times \theta_n$$

for the relation ψ on A^n defined by

$$((a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n)) \in \psi :\Leftrightarrow (a_i, b_i) \in \theta_i \text{ for } i = 1, \ldots, n.$$

PROPOSITION 1.20. *Let $(\mathbf{A}_i)_{i=1,\ldots,n}$ be a family of finitely many neutral algebras in a congruence modular variety, and let $\mathbf{D}$ be a subdirect product of $(\mathbf{A}_i)_{i=1,\ldots,n}$. Then $\mathbf{D}$ is skew-free.*

Proof: By [**BS81**, Lemma 11.6] it is sufficient to prove that for every congruence $\theta \in Con\mathbf{D}$ we have

$$\theta = \bigcap_{i=1}^{n} (\theta \vee \rho_i), \tag{5.1}$$

where ρ_i is the kernel of the projection of $\mathbf{D}$ to $\mathbf{A}_i$. But by Proposition 1.18 and the fact that neutral algebras in congruence modular varieties have distributive congruences, (5.1) can be rewritten as

$$\theta = \theta \vee \bigcap_{i=1}^{n} \rho_i,$$

which is true because $\bigcap_{i=1}^{n} \rho_i = \mathbf{0_D}$. □

6. Ω-groups

Ω-groups are groups with further operations which fulfil one restriction: For each $k \in \mathbb{N}_0$ and for every k-ary fundamental operation ω of an Ω-group, we claim

$$\omega(0, 0, \ldots, 0) = 0.$$

Ω-groups were introduced by [**Hig56**], and are also studied in [**Kur65**]. Many algebraic structures can be seen as Ω-groups, such as e.g. groups, rings, near-rings, and ring modules. One of the pleasant facts about Ω-groups is that a congruence on an Ω-group is completely described by the congruence class of 0. Actually, the congruence class of 0 is always a subalgebra of the Ω-group. Those subuniverses of an Ω-group that arise as congruence classes of 0 for some congruence are called *ideals*. Ideals can easily be described by intrinsic properties; these topics are discussed, e.g., in [**Kur65**] or [**Pil84**]. Before continuing our discussion of Ω-groups, let us first give a clean definition of Ω-groups:

DEFINITION 1.21. Let $\Omega = (\mathcal{F}, \sigma)$ be a type. Then an algebra $\mathbf{V}$ of type Ω is called an Ω-*group* iff

(1) The set $\mathcal{F}$ of operation symbols contains the elements $+$, $-$ and 0.
(2) The operation symbol $+$ is binary, $-$ is unary, and 0 is nullary.
(3) The algebra $(V; +_{\mathbf{V}}, -_{\mathbf{V}}, 0_{\mathbf{V}})$ is a group.
(4) The set $\{0\}$ is a subuniverse of $\mathbf{V}$, i.e., for all $k \in \mathbb{N}_0$ and for all k-ary fundamental operations ω of $\mathbf{V}$ we have

$$\omega(0, 0, \ldots, 0) = 0. \tag{6.1}$$

Using vector notation, (6.1) can be written as $\omega(\mathbf{0}) = 0$. So, one can say that an Ω-group is an algebra with a group reduct and a one element subuniverse $\{0\}$.

For reason of simplicity, we will write $+, -, 0$ for $+_{\mathbf{V}}, -_{\mathbf{V}}, 0_{\mathbf{V}}$, and we will use $-$ also as a binary operation symbol in the usual way. As in Definition 1.11, we will also use $+$ for the componentwise addition in $\mathbf{V}^k$.

DEFINITION 1.22. A non-empty subset I of V is called *an ideal* of $\mathbf{V}$ iff for all $k \in \mathbb{N}_0$, for all k-ary fundamental operations ω of $\mathbf{V}$, for all $\mathbf{i} \in I^k$, and for all $\mathbf{v} \in V^k$ we have

$$\omega(\mathbf{v} + \mathbf{i}) - \omega(\mathbf{v}) \in I.$$

For a subset S of V, the smallest ideal of $\mathbf{V}$ that contains S is denoted by $\mathcal{I}_{\mathbf{V}}(S)$. We will also write $\mathcal{I}_{\mathbf{V}}(v)$ for $\mathcal{I}_{\mathbf{V}}(\{v\})$.

Note that an ideal I is automatically a subuniverse of $\mathbf{V}$ (take $\mathbf{v} := \mathbf{0}$), and furthermore a normal subgroup of $(V; +, -, 0)$. This holds because if we take $v \in V$, $i \in I$, and $\omega(\mathbf{x}) := x_1 + x_2$, and if we choose $\mathbf{w} := \binom{v}{0}$ and $\mathbf{j} := \binom{i}{0}$, we have

$$\begin{aligned}\omega(\mathbf{w} + \mathbf{j}) - \omega(\mathbf{w}) &= (v + i + 0 + 0) - (v + 0)\\ &= v + i - v.\end{aligned}$$

But this is precisely the closure property that a normal subgroup has to fulfill.

Let $Id\,\mathbf{V}$ be the set of all ideals of $\mathbf{V}$. It is not too hard to see that for ideals $I, J \in Id\,\mathbf{V}$, the sets $I \cap J$ and $I + J := \{i + j \mid i \in I, j \in J\}$ are again ideals of $\mathbf{V}$. Furthermore, the structure $(Id\,\mathbf{V}; \cap, +)$ is a lattice, and the mapping γ defined by

$$\begin{array}{rccc}\gamma & : & Id\,\mathbf{V} & \longrightarrow & Con\,\mathbf{V}\\ & & I & \longmapsto & \gamma(I)\end{array} \tag{6.2}$$

with

$$v_1 \equiv v_2 \pmod{\gamma(I)} :\Leftrightarrow v_1 - v_2 \in I$$

is a lattice isomorphism from **Id V** to **Con V**.

Of course, the commutator notation for universal algebras is immediately available for the congruences of Ω-groups; however, we want to have a commutator operation for ideals, and not only for congruences. Then the commutator operation on the set $Id\,\mathbf{V}$ should behave in a way that the mapping γ defined in (6.2) is also a homomorphism from $(Id\,\mathbf{V}; \cap, +, [.,.])$ to $(Con\,\mathbf{V}; \wedge, \vee, [.,.])$. Hence we define the commutator of two ideals A, B of $\mathbf{V}$ by

$$[A, B] := \gamma^{-1}([\gamma(A), \gamma(B)]).$$

A nicer description of the commutator using polynomial functions is given in Proposition 1.24. There is another thing that we should pay attention to: Let $\mathbf{V}$ be an Ω-group and let $\mathbf{W}$ be a subalgebra of $\mathbf{V}$. Suppose that $\mathbf{V}$ has an ideal I with $I \subseteq W$. It is easy to see that I is then also an ideal of $\mathbf{W}$. However, if we write $[I, I]$, it is not clear whether the commutator has to be taken in the algebra

$\mathbf{V}$ or in its subalgebra $\mathbf{W}$. We will therefore write $[I, I]_{\mathbf{V}}$ if the commutator is taken in $\mathbf{V}$, and $[I, I]_{\mathbf{W}}$ if the commutator is taken in $\mathbf{W}$.

Note that a similar distinction is not vital for congruences, because a congruence relation α on $\mathbf{V}$ can never be a congruence on a proper subalgebra $\mathbf{W}$ of $\mathbf{V}$. This holds simply because for every $v \in V - W$, the pair (v, v) is in α, and therefore α is not even a subset of $W \times W$.

7. Various concepts of commutator operations for Ω-groups

The importance of the concept of commutators has already been observed in [**Hig56**] and [**Kur65**]. However, their definition gives a commutator concept which is different from the commutator arising from the universal algebra commutator due to [**Smi76**] and [**FM87**], which is the concept that we use in the present thesis. Still, it must be said that Higgins's commutators coincide with the universal algebra commutators for the important cases of groups or rings. Many years later, Stuart D. Scott felt the necessity of a good concept of commutators for Ω-groups [**Sco97**]; and he introduced an ideal multiplication that differed from the commutator of [**Hig56**]. His definition proved sucessful in his work – which is not too surprising, because we will show that the *Scott-commutator* is actually a re-invention of the universal algebra commutator. A very similar characterization of the commutator operation using polynomials can be found in [**GU84**].

Nevertheless, we think it is instructive to give a short comparision of the various commutator concepts in the following section, before forsaking Higgins's concept of commutators for the rest of this work, and staying exclusively with the universal algebra concept that has proved most successful. For this discussion, let $\mathbf{V}$ always be an Ω-group and let A and B be two ideals of $\mathbf{V}$.

For introducing Scott's commutator concept and comparing it to the one used in universal algebra, we need the following set of *zero-symmetric* polynomials on an Ω-group $\mathbf{V}$.

Definition 1.23. Let $k \in \mathbb{N}$ with $k \geq 2$, and let $\mathbf{V}$ be an Ω-group. Then $\mathsf{ZP}_k(\mathbf{V})$ is defined by

$$\mathsf{ZP}_k(\mathbf{V}) := \{p \in \mathsf{P}_k(\mathbf{V}) \mid p(v, \mathbf{0}) = p(0, \mathbf{w}) = 0 \text{ for all } v \in V, \mathbf{w} \in V^{k-1}\}.$$

A polynomial function is in $\mathsf{ZP}_k(\mathbf{V})$ if it is zero whenever either the first argument or all the other arguments are zero. These polynomial functions can be used as multiplications: note that in every ring $\mathbf{R}$, the function $(x, y) \mapsto x \cdot y$ lies in $\mathsf{ZP}_2(\mathbf{R})$. In groups, $(x, y) \mapsto x + y - x - y$ is an example of such a zero-symmetric polynomial function. For a near-ring $\mathbf{N}$, the function $(x, y) \mapsto x \circ y - x \circ 0$ lies in $\mathsf{ZP}_2(\mathbf{N})$. These polynomial functions can be used to describe the commutator:

Proposition 1.24. *Let $\mathbf{V}$ be an Ω-group, let k be a natural number with $k \geq 2$, and let A, B be ideals of $\mathbf{V}$. We define a set S_k as follows:*

$$S_k := \{p(a, \mathbf{b}) \mid p \in \mathsf{ZP}_k(\mathbf{V}), a \in A, \mathbf{b} \in B^{k-1}\}.$$

Then the ideal of $\mathbf{V}$ *that is generated by* S_k *is equal to* $[A, B]_{\mathbf{V}}$.

For $k = 2$ this proposition yields that the commutator of A and B is generated by all elements $p(a, b)$, where a is taken in A, b in B, and p is a binary polynomial function of $\mathbf{V}$ with the property $p(x, 0) = p(0, x) = 0$ for all $x \in V$. This is the actual definition given by Stuart Scott [**Sco97**].

Proof: Let k be a natural number with $k \geq 2$. We will prove the following subset relations:

$$[A, B]_{\mathbf{V}} \subseteq \mathcal{I}_{\mathbf{V}}(\bigcup_{j\in\mathbb{N}, j\geq 2} S_j) \subseteq \mathcal{I}_{\mathbf{V}}(S_2) \subseteq \mathcal{I}_{\mathbf{V}}(S_k) \subseteq [A, B]_{\mathbf{V}} \tag{7.1}$$

Let us start with the first relation, namely with

$$[A, B]_{\mathbf{V}} \subseteq \mathcal{I}_{\mathbf{V}}(\bigcup_{j\in\mathbb{N}, j\geq 2} S_j). \tag{7.2}$$

Let

$$\gamma(\mathcal{I}_{\mathbf{V}}(\bigcup_{j\in\mathbb{N}, j\geq 2}))$$

be the congruence corresponding to the ideal

$$\mathcal{I}_{\mathbf{V}}(\bigcup_{j\in\mathbb{N},\, j\geq 2} S_j),$$

and let α and β be the congruences $\gamma(A)$ and $\gamma(B)$ which correspond to A and B. What we are going to show is

$$[\alpha, \beta] \subseteq \gamma(\mathcal{I}_{\mathbf{V}}(\bigcup_{j\in\mathbb{N},\, j\geq 2} S_j)). \tag{7.3}$$

By the definition of the commutator operation, we know that $[\alpha, \beta]$ is the smallest congruence η satisfying the implication given in Definition (1.8). Therefore, we are done if we show that this implication also holds for

$$\eta := \gamma(\mathcal{I}_{\mathbf{V}}(\bigcup_{j\in\mathbb{N},\, j\geq 2} S_j)).$$

To this end, we take $n \in \mathbb{N}$, a term function $t \in \mathsf{T}_n(\mathbf{A})$, two elements a, b of V with $a \equiv b \pmod{\alpha}$ and two vectors $\mathbf{c}, \mathbf{d}$ of V^{n-1} with $\mathbf{c} \equiv \mathbf{d} \pmod{\beta}$. We assume that

$$t(a, \mathbf{c}) \equiv t(a, \mathbf{d}) \pmod{\eta}.$$

Now we define the following polynomial function $q \in \mathsf{P}_n(\mathbf{V})$.

$$q(x, \mathbf{y}) := -t(a + x, \mathbf{c}) + t(a + x, \mathbf{c} + \mathbf{y}) - t(a, \mathbf{c} + \mathbf{y}) + t(a, \mathbf{c}).$$

Since $q(0, \mathbf{y}) = q(x, \mathbf{0}) = 0$ for all $x \in V, \mathbf{y} \in V^{n-1}$, the definition of S_n tells us that $q(-a + b, -\mathbf{c} + \mathbf{d})$ lies in S_n, and hence we have

$$q(-a + b, -\mathbf{c} + \mathbf{d}) \equiv 0 \pmod{\eta}.$$

Replacing q with its definition, this is equivalent to

$$-t(b,\mathbf{c})+t(b,\mathbf{d})-t(a,\mathbf{d})+t(a,\mathbf{c})\equiv 0 \pmod{\eta}.$$

This implies $t(b,\mathbf{c})\equiv t(b,\mathbf{d}) \pmod{\eta}$. Therefore, η lies above the commutator $[\alpha,\beta]$, which proves (7.2).

Now we prove the next inclusion of (7.1), namely

$$\gamma(\mathcal{I}_{\mathbf{V}}(\bigcup_{j\in\mathbb{N},\,j\geq 2} S_j)) \subseteq \gamma(\mathcal{I}_{\mathbf{V}}(S_2)). \tag{7.4}$$

We will prove the following fact by induction on n:

$$\forall n\geq 2 \,:\, S_n \subseteq \mathcal{I}_{\mathbf{V}}(S_2) \tag{7.5}$$

Base case $n=2$: Obvious.

Induction step $n>2$: Let $a\in A$, $\mathbf{b}\in B^{n-1}$ and let $q\in \mathsf{P}_n(\mathbf{V})$ with $q(0,\mathbf{y})=q(x,\mathbf{0})=0$ for all $x\in V,\mathbf{y}\in V^{n-1}$. We have to prove

$$q(a,\mathbf{b})\in\mathcal{I}_{\mathbf{V}}(S_2). \tag{7.6}$$

We now write the vector $\mathbf{b}$ as $(b_1,\mathbf{b}^R)$. From the equation

$$q(a,\mathbf{b})=q(a,b_1,\mathbf{b}^R)-q(a,0,\mathbf{b}^R)+q(a,0,\mathbf{b}^R),$$

we see that it is sufficient for (7.6) to prove

$$q(a,b_1,\mathbf{b}^R)-q(a,0,\mathbf{b}^R)\in\mathcal{I}_{\mathbf{V}}(S_2) \tag{7.7}$$

and

$$q(a,0,\mathbf{b}^R)\in\mathcal{I}_{\mathbf{V}}(S_2). \tag{7.8}$$

Considering the polynomial $r(x,y):=q(x,y,\mathbf{b}^R)-q(x,0,\mathbf{b}^R)$ we see that r lies in $\mathsf{ZP}_2(\mathbf{V})$, and therefore $r(a,b_1)$ is in $\mathcal{I}_{\mathbf{V}}(S_2)$. But this is just the condition given in (7.7). For proving (7.8), we observe that the polynomial function $s\in\mathsf{P}_{n-1}(\mathbf{V})$ defined by $s(x,\mathbf{y}):=q(x,0,\mathbf{y})$ ($x\in V$, $\mathbf{y}\in V^{n-2}$) is zero whenever either $x=0$ or $\mathbf{y}=\mathbf{0}$. By induction hypothesis, it follows that $s(a,\mathbf{b}^R)$ is in S_2. Hence we also have the condition given in (7.8). This finishes the proof of (7.6).

Altogether, we have proved the second inclusion in (7.4). Let us now attack the third inclusion of (7.1), namely

$$\mathcal{I}_{\mathbf{V}}(S_2)\subseteq\mathcal{I}_{\mathbf{V}}(S_k). \tag{7.9}$$

In order to prove this inclusion, it is sufficient to prove $S_2\subseteq S_k$. But this can be seen immediately: Let p be in $\mathsf{ZP}_2(\mathbf{V})$, $a\in A$ and $b\in B$. We will show that $p(a,b)$ lies in S_k. To this end, we define a polynomial $q\in\mathsf{P}_k(\mathbf{V})$ by

$$q(x,\mathbf{y}):=p(x,y_1).$$

Then $p(a,b)=q(a,b,b,\ldots b)$, and q lies in $\mathsf{ZP}_k(\mathbf{V})$. Therefore $p(a,b)$ also lies in S_k, which finishes the proof of (7.9).

The fourth inclusion of (7.1) is

$$\mathcal{I}_{\mathbf{V}}(S_k) \subseteq [A, B]_{\mathbf{V}} \tag{7.10}$$

We show that the generators of $\mathcal{I}_{\mathbf{V}}(S_k)$ lie in $[A, B]_{\mathbf{V}}$. For that purpose, let $p \in \mathsf{ZP}_k(\mathbf{V})$, $a \in A$, $\mathbf{b} \in B^{k-1}$. We can find a natural number $n \geq k$, a vector $\mathbf{v}$ in V^{n-k}, and a term function t in $\mathsf{T}_n(\mathbf{V})$ such that the polynomial function p can be written as

$$p(x, \mathbf{y}) = t(x, \mathbf{y}, \mathbf{v}).$$

Note that $\mathbf{v}$ is the vector of elements of V that appear in a term representation of the polyonomial function p. Since $p \in \mathsf{ZP}_2(\mathbf{V})$, we have

$$t(a, \mathbf{0}, \mathbf{v}) = t(0, \mathbf{b}, \mathbf{v}).$$

Setting $a' := 0, b' := a$, and defining the vectors $\mathbf{c}'$ and $\mathbf{d}'$ in V^{n-1} by $\mathbf{c}' := (\mathbf{b}, \mathbf{v})$ and $\mathbf{d}' := (\mathbf{0}, \mathbf{v})$, we get

$$t(a', \mathbf{c}') = t(0, \mathbf{b}, \mathbf{v}) = p(0, \mathbf{b}) = 0.$$

Similarly, we get

$$t(a', \mathbf{d}') = t(0, \mathbf{0}, \mathbf{v}) = p(0, \mathbf{0}) = 0.$$

By the definition of the commutator, we get

$$t(b', \mathbf{c}') \equiv t(b', \mathbf{d}') \pmod{[A, B]_{\mathbf{V}}}.$$

This means

$$t(a, \mathbf{b}, \mathbf{v}) \equiv t(a, \mathbf{0}, \mathbf{v}) \pmod{[A, B]_{\mathbf{V}}},$$

which gives $p(a, b) \in [A, B]$. This finishes the proof (7.1). □

We are now going to give some consequences of Proposition 1.24.

COROLLARY 1.25. *Let l and m be natural numbers. Each of the following sets generates the commutator $[A, B]_{\mathbf{V}}$ of the ideals A and B of $\mathbf{V}$:*

1. $G_1 := \{p(\mathbf{a}, \mathbf{b}) \mid \mathbf{a} \in A^l, \mathbf{b} \in B^m, p \in \mathsf{P}_{l+m}(\mathbf{V}), \forall \mathbf{x} \in A^l, \mathbf{y} \in B^m : p(\mathbf{0}, \mathbf{y}) = p(\mathbf{x}, \mathbf{0}) = 0\}$
2. $G_2 := \{p(\mathbf{a}, \mathbf{b}) \mid \mathbf{a} \in A^l, \mathbf{b} \in B^m, p \in \mathsf{P}_{l+m}(\mathbf{V}), p(\mathbf{0}, \mathbf{b}) = p(\mathbf{a}, \mathbf{0}) = p(\mathbf{0}, \mathbf{0}) = 0\}$
3. $G_3 := \{-p(a, 0) + p(a, b) - p(0, b) + p(0, 0) \mid a \in A, b \in B, p \in \mathsf{P}_2(\mathbf{V})\}$.

Proof: Since G_1 depends on l and m, let us write $G_1(l, m)$ for G_1 in this proof. We first prove

$$\mathcal{I}_{\mathbf{V}}(G_1(l, m)) = [A, B]_{\mathbf{V}}. \tag{7.11}$$

Now we proof $\subseteq$ by induction on l. If $l = 1$, then the set G_1 is equal to set S_{l+1} defined in Proposition 1.24. For $l > 1$, we write $\mathbf{a}$ as $(a_1, \mathbf{a}^R)$, and then we have

$$p(\mathbf{a}, \mathbf{b}) = p(a_1, \mathbf{a}^R, \mathbf{b}) - p(0, \mathbf{a}^R, \mathbf{b}) + p(0, \mathbf{a}^R, \mathbf{b}).$$

It is easy to see that that $p(a_1, \mathbf{a}^R, \mathbf{b}) - p(0, \mathbf{a}^R, \mathbf{b})$ lies in $G_1(1, m)$. We also see that $p(0, \mathbf{a}^R, \mathbf{b})$ lies in $G_1(l - 1, m)$. Now induction hypothesis gives that both summands lie in $[A, B]_{\mathbf{V}}$.

For $\supseteq$, let s be in S_2, where S_2 is the set defined in Proposition 1.24. Then s can be written as $p(a,b)$ with $a \in A$, $b \in B$, and $p \in \mathsf{ZP}_2(\mathbf{V})$. Obviously, the polynomial function $p' \in \mathsf{P}_{l+m}(\mathbf{V})$ defined by

$$p'(\mathbf{x},\mathbf{y}) := p(\underbrace{x,x,\ldots,x}_{l \text{ times}},\underbrace{y,y,\ldots,y}_{m \text{ times}})$$

is 0 if $\mathbf{x}$ or $\mathbf{y}$ is zero. Hence $s = p(a,b)$ lies in G_1. This finishes the proof of (7.11).

For proving that G_2 generates $[A,B]_{\mathbf{V}}$, we observe that $G_1 \subseteq G_2$. We will now whow that G_1 is actually equal to G_2. To this end, let g_2 be an element of G_2. Then g_2 can be written as $g_2 = p(\mathbf{a},\mathbf{b})$ with $\mathbf{a} \in A^l$, $\mathbf{b} \in B^m$ and $p \in \mathsf{P}_{l+m}(\mathbf{V})$, where $p(\mathbf{a},\mathbf{0}) = p(\mathbf{0},\mathbf{b}) = 0$. Now we define the polynomial $q \in \mathsf{P}_{l+m}(\mathbf{V})$ by

$$q(\mathbf{x},\mathbf{y}) := -p(\mathbf{x},\mathbf{0}) + p(\mathbf{x},\mathbf{y}) - p(\mathbf{0},\mathbf{y}) + p(\mathbf{0},\mathbf{0}).$$

By the fact that $q(\mathbf{x},\mathbf{y})$ is zero whenever $\mathbf{x}$ or $\mathbf{y}$ is zero, we see that $q(\mathbf{a},\mathbf{b})$ lies in G_1. But $q(\mathbf{a},\mathbf{b}) = p(\mathbf{a},\mathbf{b})$, and hence g_2 lies in G_1.

For proving that G_3 generates $[A,B]_{\mathbf{V}}$, we prove that G_3 is equal to the set S_2 defined in Proposition 1.24. It is obvious that S_2 is a subset of G_3. For the other side, let $-p(a,0)+p(a,b)-p(0,b)+p(0,0)$ be a typical element of G_3. Then the polynomial function $q \in \mathsf{P}_2(\mathbf{V})$ defined by

$$q(x,y) := -p(x,0) + p(x,y) - p(0,y) + p(0,0)$$

lies in $\mathsf{ZP}_2(\mathbf{V})$. Therefore $q(a,b)$ lies in S_2. □

Now we want to compare this notion of commutators to the commutators studied in Kurosh's book [**Kur65**]. There, the following commutator operation is defined:

Definition 1.26 ([**Kur65**]). Let $\mathbf{V}$ be an Ω-group, and let A and B be ideals of $\mathbf{V}$. Then for each k-ary fundamental operation ω of $\mathbf{V}$, and for all $\mathbf{x},\mathbf{y} \in V^k$, we define

$$[\mathbf{x};\mathbf{y};\omega] := -\omega(\mathbf{a}) - \omega(\mathbf{b}) + \omega(\mathbf{a}+\mathbf{b}).$$

Then we define $\mathbf{K}(A,B)$ to be the ideal of $\mathbf{V}$ generated by the set

$$\{[\mathbf{a};\mathbf{b};\omega] \mid \omega \text{ is a } k\text{-ary fundamental operation of } \mathbf{V},\ \mathbf{a} \in A^k, \mathbf{b} \in B^k\}.$$

Since every generator of $\mathbf{K}(A,B)$ obviously lies in the set G_1 defined in Corollary 1.25, we know that $\mathbf{K}(A,B) \subseteq [A,B]_{\mathbf{V}}$. The other inclusion does not necessarily hold:

Proposition 1.27. *There is an Ω-group $\mathbf{V}$ with ideals A and B such that*

$$\mathbf{K}(A,B) \neq [A,B]_{\mathbf{V}}.$$

Proof of Proposition 1.27: We take $\mathbf{V} := (\mathbb{Z}_4;+,\varphi)$, where $(\mathbb{Z}_4,+)$ is the cyclic group of order 4 with the elements $\{0,1,2,3\}$. The binary operation φ is defined by $\varphi(1,1) = 2$ and $\varphi(x,y) = 0$ else. Now we consider $A = B := \{0,2\}$. The set A is an ideal of $\mathbf{V}$ because it is a normal subgroup of $(\mathbb{Z}_4;+)$ and φ is a

compatible, i.e., congruence preserving function on $(\mathbb{Z}_4;+)$, because it maps $\mathbb{Z}_4$ into a minimal normal subgroup of $(\mathbb{Z}_4;+)$.

Since φ is trivial on A, each of the generators of $\mathbf{K}(A,B)$ given in Definition 1.26 is equal to 0. From this it follows that $\mathbf{K}(A,B)=\{0\}$.

Now let us compute $[A,B]_{\mathbf{V}}$. We consider the polynomial

$$p(x,y) := -\varphi(1,y+1)+\varphi(x+1,y+1)-\varphi(x+1,1)+2.$$

It can easily be seen that p lies in $\mathsf{ZP}_2(\mathbf{V})$. From $p(2,2)=-\omega(1,3)+\omega(3,3)-w(3,1)+2=2$ we see that $2\in[A,A]$. □

We close with one important application of the commutator.

PROPOSITION 1.28. *Let $p\in\mathsf{P}_2(\mathbf{V})$ with $p(0,0)=0$, $a\in A$, $b\in B$. Then*

$$p(a,b)\equiv p(a,0)+p(0,b)\pmod{[A,B]_{\mathbf{V}}}. \tag{7.12}$$

Proof of Proposition 1.28: We consider the polynomial $q(x,y):=p(x,y)-p(0,y)-p(x,0)$. Then we see that $q\in\mathsf{ZP}_2(\mathbf{V})$. Hence $q(a,b)\in[A,B]_{\mathbf{V}}$, which implies the congruence stated in 7.12. □

8. Abelian Ω-groups

In this section, we describe abelian Ω-groups.

PROPOSITION 1.29. *Let $\mathbf{V}$ be an algebra of type $(\mathcal{F},\sigma)$ such that $+,-,0$ of arity $2,1,0$, resp., lie in $\mathcal{F}$. Furthermore, we suppose that $(V;+,-,0)$ is a group. Then the following are equivalent.*

1. *$\mathbf{V}$ is an abelian algebra in the sense of Definition 1.10*
2. *$(V;+,-,0)$ is an abelian group, and for all $k\in\mathbb{N}_0$, all k-ary fundamental operations of $\mathbf{V}$ are affine with respect to $+$.*

Proof: (1) ⇒ (2) follows from Proposition 1.13 and the fact that the Mal'cev term for the variety generated by $\mathbf{V}$ is given by $d(x,y,z):=x+(-y)+z$.

(2) ⇒ (1) follows from Proposition 1.14. □

If $\mathbf{V}$ is an Ω-group, then we know that each fundamental operation of $\mathbf{V}$ fixes 0, and hence we can restate Proposition 1.29 as follows:

PROPOSITION 1.30. *An Ω-group $\mathbf{V}$ is abelian (in the sense of Definition 1.10) iff the group $(V;+,-,0)$ is an abelian group and for all $k\in\mathbb{N}_0$, all k-ary fundamental operations of $\mathbf{V}$ are homomorphisms from $(V;+,-,0)^k$ to $(V;+,-,0)$.*

From now on, "abelian" will always mean "abelian in the sense of Definition 1.10".

CHAPTER 2

An interpolation result for function algebras

In this chapter, we are going to prove and explain several important interpolation results due to [**HH82**]. Proposition 2.2 will be crucial for the entire interpolation and structure theory that we shall develop in this thesis.

1. Function algebras

Recalling the definition of function algebras from a set D to the algebra $\mathbf{A}$, we notice that a function algebra from D to $\mathbf{A}$ is just a subalgebra of the cartesian product $\mathbf{A}^D$; we prefer to view its elements as functions. This is mainly because of the following result.

2. The interpolation result

In this section, we give an interpolation result of the type

Interpolation at 2 places $\Rightarrow$ Interpolation at n places.

Due to the importance of this result, we shall first state and prove it for Ω-groups. Then we will give the universal version of this result.

2.1. The interpolation result for Ω-groups.

PROPOSITION 2.1. *Let D be a set, and let $\mathbf{V}$ be an Ω-group. Let $\mathbf{F}$ be a function algebra from D to $\mathbf{V}$, i.e., a subalgebra of $\mathbf{V}^D$. Assume that all subalgebras of $\mathbf{V}$ are neutral. Let l be a function from D to V that can be interpolated at each subset S of D with $|S| \leq 2$ by a function in F. Then l can be interpolated at every finite subset of D by a function in F.*

Proof: We show that for $n \in \mathbb{N}$, $n \geq 2$, each function in V^D that can be interpolated at n points by a function in F can also be interpolated at $n+1$ points by a function in F. In other words, we show $\mathsf{L}_n F \subseteq \mathsf{L}_{n+1} F$.

For this purpose, we fix $n \geq 2$, $l \in \mathsf{L}_n F$, and $x_1, x_2, \ldots, x_{n+1} \in D$. We want to construct a function $f \in F$ that interpolates l at $x_1, x_2, \ldots, x_{n+1}$.

To start with, we choose a function $s_1 \in F$ that interpolates l at $x_1, x_2, \ldots, x_n$. Then we are left with a function $l_1 \in \mathsf{L}_n F$ defined by $l_1 := l - s_1$, which is zero on

$x_1, x_2, \ldots, x_n$. For finding the function in F that interpolates l_1, it is sufficient to prove $B = S$, where B und S are the two subsets of V that are given by

$$\begin{aligned} B &:= \{l(x_{n+1}) \,|\, l \in \mathsf{L}_n F \text{ and } l(x_i) = 0 \text{ for } i = 1, \ldots, n\} \\ S &:= \{f(x_{n+1}) \,|\, f \in F \text{ and } f(x_i) = 0 \text{ for } i = 1, \ldots, n\}. \end{aligned}$$

Since $F \subseteq \mathsf{L}_n F$, it is easy to see that $S \subseteq B$.

We shall now show

$$B \subseteq S. \tag{2.1}$$

First of all we prove that B is an ideal of $\mathbf{W}$, which is defined as the subalgebra of $\mathbf{V}$ with universe

$$W := \{f(x_{n+1}) \,|\, f \in F\}.$$

We check the ideal property given in Definition 1.22. To this end, let ω be a k-ary operation symbol of $\mathbf{V}$, let $\mathbf{v} \in W^k$, and let $\mathbf{b} \in B^k$. We want to show that $\omega_{\mathbf{V}}(\mathbf{v} + \mathbf{b}) - \omega_{\mathbf{V}}(\mathbf{v})$ lies in B. By the definition of B, we can find a function l_j in $\mathsf{L}_n F$ for each $j = 1, 2, \ldots, k$ that satisfies the following condition:

$$l_j(x_{n+1}) = b_j \text{ and } l_j(x_i) = 0 \text{ for } i = 1, 2, \ldots, n.$$

Since $\mathbf{v} \in W^k$, there are functions $f_1, f_2, \ldots, f_j \in F$ for $j = 1, 2, \ldots, k$ that satisfy

$$f_j(x_{n+1}) = v_j.$$

We write $\mathbf{l}$ for $(l_1, l_2, \ldots, l_k)$, and we write $\mathbf{f}$ for $(f_1, f_2, \ldots, f_k)$. Furthermore, $\mathbf{l}(x_{n+1})$ abbreviates the vector $\big(l_1(x_{n+1}), l_2(x_{n+1}), \ldots, l_k(x_{n+1})\big)$, and $\mathbf{f}(x_{n+1})$ abbreviates the vector $\big(f_1(x_{n+1}), f_2(x_{n+1}), \ldots, f_k(x_{n+1})\big)$.

Now we can write $\omega_{\mathbf{V}}(\mathbf{v} + \mathbf{b}) - \omega_{\mathbf{V}}(\mathbf{v})$ as

$$\omega_{\mathbf{V}}\big(\mathbf{l}(x_{n+1}) + \mathbf{f}(x_{n+1})\big) - \omega_{\mathbf{V}}\big(\mathbf{l}(x_{n+1})\big). \tag{2.2}$$

But taking

$$g := \omega_{\mathbf{V}^D}(\mathbf{l} + \mathbf{f}) - \omega_{\mathbf{V}^D}(\mathbf{f}),$$

we can write the expression in Equation (2.2) as $g(x_{n+1})$. Furthermore, it is easy to see that $\mathsf{L}_n F$ is a subuniverse $\mathbf{V}^D$. (A similar result will be proved in Proposition 3.11.) Hence $g \in \mathsf{L}_n F$. We also see that $g(x_i) = 0$ for $i = 1, 2, \ldots, n$. Altogether, we see that $g(x_{n+1})$ lies in B. Therefore, B is really an ideal of $\mathbf{W}$.

In the same way, we see that S is an ideal of $\mathbf{W}$. Now suppose that S is not equal to B. By the assumptions, $\mathbf{W}$ is neutral, and hence the commutator $[B, B]_{\mathbf{W}}$ is equal to B. By the characterization of the commutator via binary polynomial functions in Proposition 1.24, we know that $[B, B]_{\mathbf{W}}$ is generated by the elements $p(b_1, b_2)$, where p is a polynomial function in $\mathsf{ZP}_2(\mathbf{W})$, and b_1, b_2 lie in B. Since we have supposed $S \neq B$, and since by assumption we have $B = [B, B]_{\mathbf{W}}$, we know that S is a proper subset of $[B, B]_{\mathbf{W}}$. This inclusion can only be proper if at least one of these generators of $[B, B]_{\mathbf{W}}$ of the form $p(b_1, b_2)$ does not lie in S. In other words, there must be a binary polynomial function $p \in \mathsf{ZP}_2(\mathbf{W})$ and

two elements $b_1, b_2 \in B$ with $p(b_1, b_2) \notin S$. Since b_1 lies in B, the definition of B allows to construct a function $f \in F$ such that

$$f(x_{n+1}) = b_1 \text{ and } f(x_i) = 0 \text{ for } i = 1, 2, \ldots, n-1.$$

In the same way, we construct a function $g \in F$ such that

$$g(x_{n+1}) = b_2 \text{ and } g(x_n) = 0.$$

We take $r \in \mathbb{N}$, $t \in \mathsf{T}_{r+2}(\mathbf{V})$, and $\mathbf{v} \in W^r$ such that for all $x, y \in W$ we have

$$t(\mathbf{v}, x, y) = p(x, y).$$

Since $\mathbf{v} \in W^r$, there is a function e_j in F for each $j = 1, 2, \ldots, r$ such that

$$e_j(x_{n+1}) = v_j.$$

We will write $\mathbf{e}$ for $(e_1, e_2, \ldots, e_r)$. Furthermore, for a k-ary term function t of $\mathbf{V}$ and mappings $f_1, f_2, \ldots, f_k$ from F to F, we write $t(f_1, f_2, \ldots, f_k)$ for the mapping on V that maps v to $t(f_1(v), f_2(v), \ldots, f_k(v))$. Using these simplifications of notation, we define a function $h \in F$ by

$$h := -t(\mathbf{e}, f, 0) + t(\mathbf{e}, f, g) - t(\mathbf{e}, 0, g) + t(\mathbf{e}, 0, 0).$$

It is easy to calculate that we have $h(x_i) = 0$ for $i = 1, 2, \ldots, n$. For $h(x_{n+1})$, we obtain

$$\begin{aligned} h(x_{n+1}) &= -t(\mathbf{v}, b_1, 0) + t(\mathbf{v}, b_1, b_2) - t(\mathbf{v}, 0, b_2) + t(\mathbf{v}, 0, 0) \\ &= -p(b_1, 0) + p(b_1, b_2) - p(0, b_2) + p(0, 0) \\ &= p(b_1, b_2). \end{aligned}$$

Hence $h(x_{n+1})$ is not an element of S. But since h lies in F and is zero on $x_1, x_2, \ldots, x_n$, this contradicts the definition of S. Hence the assumption $S \neq B$ leads to a contradiction, and therefore the inclusion (2.1) is fulfilled. But $S = B$ immediately allows us to interpolate l_1 at $x_1, x_2, \ldots, x_{n+1}$. □

Note that the restriction that all fundamental operations on an Ω-group preserve 0 is not essential in this proof. Instead of Ω-groups, we might in fact consider any algebra with group reduct. In all those algebras, the congruences are determined by the congruence classes of 0, although these 0-classes then need not be subalgebras. For generalizing the proof, we would also have to check that the characterization of the commutator in Proposition 1.24 carries over to any algebra with group reduct. Instead of doing this, we immediately switch to a more general version of the same result, stated in the language of universal algebra.

2.2. The interpolation result for universal algebras.

PROPOSITION 2.2. *Let D be a set, and let $\mathbf{F}$ be a function algebra from D to $\mathbf{A}$. Assume that all subalgebras of $\mathbf{A}$ are neutral and that the class $\mathcal{SP}_f\mathbf{A}$ is congruence permutable. Let l be a function from D to A that can be interpolated at each subset S of D with $|S| \leq 2$ by a function in F. Then l can be interpolated at every finite subset of D by a function in F.*

This Proposition follows immediately from the literature if $\mathbf{A}$ lies in a congruence modular variety. In this case we can give the following proof:

Proof I: Let $x_1, x_2, \ldots, x_n \in D$, and let l be a function that can be interpolated at every subset of D with not more than two elements by a function in F.

We consider the following algebra $\mathbf{G}$ that arises from restricting the functions in F to $X := \{x_1, x_2, \ldots, x_n\}$. Formally, $\mathbf{G}$ is defined by

$$G := \{f|_X \mid f \in F\}.$$

G is a subuniverse of the direct product $\mathbf{A}^X$ and the operations of $\mathbf{G}$ are defined such that $\mathbf{G}$ becomes a subalgebra of $\mathbf{A}^X$.

We have to find a function $g \in G$ that satisfies

$$\begin{array}{rcl} g(x_1) & = & l(x_1) \\ g(x_2) & = & l(x_2) \\ & \vdots & \\ g(x_n) & = & l(x_n). \end{array}$$

Since l can be interpolated at each 1-element subset of D by an element in F, there are functions $g_1, g_2, \ldots, g_n \in G$ such that $g_i(x_i) = l(x_i)$ for $i = 1, 2, \ldots, n$.

Now let ζ_i be the congruence on $\mathbf{G}$ defined by

$$(g, h) \in \zeta_i :\Leftrightarrow g(x_i) = h(x_i).$$

Of course, ζ_i is just the kernel of the x_i th projection.

Then we have to find $g \in G$ as a solution of

$$\begin{array}{rcll} g & \equiv & l_1 & (\mathrm{mod}\ \zeta_1) \\ g & \equiv & l_2 & (\mathrm{mod}\ \zeta_2) \\ & \vdots & & \\ g & \equiv & l_n & (\mathrm{mod}\ \zeta_n). \end{array} \tag{2.3}$$

By the assumptions, every subsystem of the system in Equation (2.3) that consists of two congruences has a solution g in G.

We shall now prove that the algebra $\mathbf{G}$ is arithmetical, i.e., the congruences of $\mathbf{G}$ are permutable and **Con G** is a distributive lattice: then the Chinese Remainder Theorem gives that the whole system in Equation (2.3) has a solution; and this solution is the function g we are looking for.

Since X is finite, and since $\mathbf{G}$ is a subalgebra of $\mathbf{A}^X$, we get that $\mathbf{G}$ is in $\mathcal{SP}_f\mathbf{A}$, and hence congruence permutable.

For showing that **Con G** is distributive, we show that it is neutral. For that purpose, we define Φ by

$$\begin{array}{rcccl} \Phi & : & G & \longrightarrow & \underbrace{A \times A \times \cdots \times A}_{n \text{ times}} \\ & & g & \longmapsto & (g(x_1), g(x_2), \ldots, g(x_n)). \end{array}$$

Since Φ is injective, we see that $\mathbf{G}$ is a subdirect product of the algebras $\mathbf{B}_i$, where $\mathbf{B}_i$ is the subalgebra of $\mathbf{A}$ with universe $B_i := \{g(x_i) \mid g \in G\}$. By assumption, every algebra $\mathbf{B}_i$ is neutral. Now [**FM87**, Exercise 8.2] gives that a subdirect product of finitely many neutral algebras is neutral. Therefore $\mathbf{G}$ is neutral, and we are done. □

Remark: When we use the results of Chapter 8 of [**FM87**], we have to bear in mind that all the results in that chapter presuppose that we are working in congruence modular varieties. As Paweł Idziak remarked, in the non-congruence modular case Proof I breaks at the point where we say that $\mathbf{G}$ is neutral and hence congruence distributive. In the general case, a neutral algebra does not necessarily have a distributive congruence lattice.

We now give an elementary proof of Proposition 2.2 that does obviously not make use of congruence modularity.
Proof II: We show that for $n \in \mathbb{N}$, $n \geq 2$, each function in A^D that can be interpolated at n points by a function in F can also be interpolated at $n+1$ points by a function in F. In other words, we show $\mathsf{L}_n F \subseteq \mathsf{L}_{n+1} F$.

For this purpose, we fix $n \geq 2$, $l \in \mathsf{L}_n F$, and $x_1, x_2, \ldots, x_{n+1} \in D$.

We define a binary relation B and a binary relation S on A by

$$B := \{(l_1(x_{n+1}), l_2(x_{n+1})) \mid l_1, l_2 \in \mathsf{L}_n F \text{ and } l_1(x_i) = l_2(x_i) \text{ for } i = 1, \ldots, n\}$$

and

$$S := \{(f_1(x_{n+1}), f_2(x_{n+1})) \mid f_1, f_2 \in F \text{ and } f_1(x_i) = f_2(x_i) \text{ for } i = 1, \ldots, n\}.$$

Since $F \subseteq \mathsf{L}_n F$, it is easy to see that $S \subseteq B$.

We shall now show $B \subseteq S$: We notice that B is the universe of a subalgebra $\mathbf{B}$ of $\mathbf{A} \times \mathbf{A}$. Let $\pi(B)$ denote the projection of B to the first component. Then $\pi(B)$ is the universe of a subalgebra of $\mathbf{A}$, and we call this subalgebra $\pi(\mathbf{B})$. Actually, B is a congruence relation on $\pi(\mathbf{B})$. For proving this, we have to prove

(1) $B \subseteq \pi(B) \times \pi(B)$.
(2) B is a reflexive relation on $\pi(B)$.
(3) B is a symmetric relation on $\pi(B)$.
(4) B is a transitive relation on $\pi(B)$.

It is easy to see that $(b_1, b_2) \in B$ implies that (b_2, b_1), (b_1, b_1), and (b_2, b_2) lie in B. From this, (1), (2) and (3) follow. For (4), let $(b_1, b_2) \in B$ and $(b_2, b_3) \in B$. By the previous observations we know that also (b_3, b_2) and (b_3, b_3) lie in B. By Proposition 1.5, we can produce a ternary term m such that $m_{\mathbf{A}}$ is a Mal'cev function on $\{(b_1, b_3, b_3), (b_2, b_2, b_3)\}$. Since B is a subuniverse of $\mathbf{A} \times \mathbf{A}$, $m_{\mathbf{A}\times\mathbf{A}}\big((b_1, b_2), (b_3, b_2), (b_3, b_3)\big) = (b_1, b_3)$ lies in B. This implies the transitivity of B.

With the same reasoning, we obtain that S is the universe of a subalgebra $\mathbf{S}$ of $\mathbf{A} \times \mathbf{A}$. As above, it turns out that S is a congruence on the algebra $\pi(\mathbf{S})$, where

$\pi(\mathbf{S})$ is the projection of $\mathbf{S}$ to the first component. Furthermore, we know that $\pi(S) = \{f(x_{n+1}) \mid f \in F\}$ and $\pi(B) = \{l(x_{n+1}) \mid l \in \mathsf{L}_n F\}$. Since $n \geq 1$, we have $\pi(S) = \pi(B)$.

We know that both B and S are congruence relations on $\pi(\mathbf{B})$. Suppose that $S \neq B$. Then the commutator $[B, B]$, taken in the algebra $\pi(\mathbf{B})$, is equal to B by assumption. Hence, by Definition 1.8, there exist $k \in \mathbb{N}$, a k-ary term function t on $\pi(\mathbf{B})$, $a, b \in \pi(B)$, and $\mathbf{c}, \mathbf{d} \in \pi(B)^{k-1}$ such that

$$\begin{array}{l} a \equiv b \pmod{B}, \\ \mathbf{c} \equiv \mathbf{d} \pmod{B}, \\ t(a, \mathbf{c}) \equiv t(a, \mathbf{d}) \pmod{S}, \text{ and} \\ t(b, \mathbf{c}) \not\equiv t(b, \mathbf{d}) \pmod{S}. \end{array}$$

Since $a \equiv b \pmod{B}$, there are functions $f_1, f_2 \in F$ with

$$f_1(x_i) = f_2(x_i) \text{ for } i = 1, \ldots, n-1$$

and

$$f_1(x_{n+1}) = a, \ f_2(x_{n+1}) = b.$$

In the same way, for each $i \in \{1, 2, \ldots, k-1\}$, there are functions $g_{1,i}, g_{2,i} \in F$ with

$$g_{1,i}(x_n) = g_{2,i}(x_n)$$

and

$$g_{1,i}(x_{n+1}) = c_i, \ g_{2,i}(x_{n+1}) = d_i.$$

We abbreviate the vector

$$(g_{1,1}, g_{1,2}, \ldots, g_{1,k-1})$$

by $\mathbf{g}_1$ and the vector

$$(g_{1,1}(x), g_{1,2}(x), \ldots, g_{1,k-1}(x))$$

by $\mathbf{g}_1(x)$. Similarly, we form $\mathbf{g}_2$ and $\mathbf{g}_2(x)$.

We use Proposition 1.5 to produce a ternary term $m^{(1)}$ such that $m^{(1)}_{\mathbf{A}}$ is a Mal'cev function on $D_1 \times D_1 \times D_1$, where D_1 is given by

$$D_1 := \{t\big(f_i, \mathbf{g}_j\big)(x_k) \mid k = 1, 2, \ldots, n+1;\ i, j = 1, 2\}$$

and a ternary term $m^{(2)}$ such that $m^{(2)}_{\mathbf{A}}$ is a Mal'cev function on $D_2 \times D_2 \times D_2$, where D_2 is given by $D_2 := D_1 \cup m^{(1)}_{\mathbf{A}}(D_1 \times D_1 \times D_1)$. In the sequel, we simply write m_1 for both $m^{(1)}_{\mathbf{A}}$ and $m^{(1)}_{\mathbf{A}^D}$, and m_2 for both $m^{(2)}_{\mathbf{A}}$ and $m^{(2)}_{\mathbf{A}^D}$.

We form two functions $h_1, h_2 \in F$ as

$$\begin{array}{lcl} h_1 & := & m_2\big(t(f_2, \mathbf{g}_1), m_1\big(t(f_1, \mathbf{g}_2), t(f_1, \mathbf{g}_1), t(f_2, \mathbf{g}_1)\big), t(f_2, \mathbf{g}_2)\big) \\ h_2 & := & t(f_2, \mathbf{g}_1). \end{array}$$

We will first show that $h_1(x_i) = h_2(x_i)$ for $i = 1, 2, \ldots, n$. For this purpose, we first take $i \leq n-1$. Then we have:

$$\begin{aligned} h_1(x_i) &= m_2\big(t(f_2, \mathbf{g}_1), m_1\big(t(f_1, \mathbf{g}_2), t(f_1, \mathbf{g}_1), t(f_2, \mathbf{g}_1)\big), t(f_2, \mathbf{g}_2)\big)\ (x_i) \\ &= m_2\big(t(f_2, \mathbf{g}_1), m_1\big(t(f_2, \mathbf{g}_2), t(f_2, \mathbf{g}_1), t(f_2, \mathbf{g}_1)\big), t(f_2, \mathbf{g}_2)\big)\ (x_i) \\ &= m_2\big(t(f_2, \mathbf{g}_1), t(f_2, \mathbf{g}_2), t(f_2, \mathbf{g}_2)\big)\ (x_i) \\ &= t(f_2, \mathbf{g}_1)\ (x_i). \end{aligned}$$

Now we see that the last expression is equal to $h_2(x_i)$. For proving $h_1(x_n) = h_2(x_n)$, we do the following calculations:

$$\begin{aligned} h_1(x_n) &= m_2\big(t(f_2, \mathbf{g}_1), m_1\big(t(f_1, \mathbf{g}_2), t(f_1, \mathbf{g}_1), t(f_2, \mathbf{g}_1)\big), t(f_2, \mathbf{g}_2)\big)\ (x_n) \\ &= m_2\big(t(f_2, \mathbf{g}_1), m_1\big(t(f_1, \mathbf{g}_1), t(f_1, \mathbf{g}_1), t(f_2, \mathbf{g}_1)\big), t(f_2, \mathbf{g}_1)\big)\ (x_n) \\ &= m_2\big(t(f_2, \mathbf{g}_1), t(f_2, \mathbf{g}_1), t(f_2, \mathbf{g}_1)\big)\ (x_n) \\ &= t(f_2, \mathbf{g}_1)\ (x_n). \end{aligned}$$

Again, the last expression is equal to $h_2(x_n)$.

Therefore, $(h_1(x_{n+1}), h_2(x_{n+1}))$ lies in S. Now we have

$$\begin{aligned} h_1(x_{n+1}) &= m_2\big(t(f_2, \mathbf{g}_1), m_1\big(t(f_1, \mathbf{g}_2), t(f_1, \mathbf{g}_1), t(f_2, \mathbf{g}_1)\big), t(f_2, \mathbf{g}_2)\big)\ (x_{n+1}) \\ &= m_2\big(t(b, \mathbf{c}), m_1\big(t(a, \mathbf{d}), t(a, \mathbf{c}), t(b, \mathbf{c})\big), t(b, \mathbf{d})\big). \end{aligned}$$

The value of $h_2(x_{n+1})$ can be computed by

$$\begin{aligned} h_2(x_{n+1}) &= t(f_2(x_{n+1}), \mathbf{g}_1(x_{n+1})) \\ &= t(b, \mathbf{c}). \end{aligned}$$

So $(h_1(x_{n+1}), h_2(x_{n+1})) \in S$ can be rewritten as

$$m_2\big(t(b, \mathbf{c}), m_1\big(t(a, \mathbf{d}), t(a, \mathbf{c}), t(b, \mathbf{c})\big), t(b, \mathbf{d})\big) \equiv t(b, \mathbf{c}) \pmod{S}.$$

Since we have $t(a, \mathbf{c}) \equiv t(a, \mathbf{d}) \pmod{S}$, we get

$$m_2\big(t(b, \mathbf{c}), m_1\big(t(a, \mathbf{d}), t(a, \mathbf{d}), t(b, \mathbf{c})\big), t(b, \mathbf{d})\big) \equiv t(b, \mathbf{c}) \pmod{S},$$

which can be calculated as

$$m_2\big(t(b, \mathbf{c}), t(b, \mathbf{c}), t(b, \mathbf{d})\big) \equiv t(b, \mathbf{c}) \pmod{S}.$$

Hence we get $t(b, \mathbf{d}) \equiv t(b, \mathbf{c}) \pmod{S}$, which is a contradiction.

We now have proved $S = B$. In the remainder of this proof, we want to show how this equality allows us to construct the function that interpolates the function $l \in L_n F$. We want to construct a function $f \in F$ such that $f(x_i) = l(x_i)$ for $i = 1, 2, \ldots, n+1$. Since l is in $L_n F$, there is a function $p_1 \in F$ such that

$$p_1(x_i) = l(x_i) \text{ for } i = 1, 2, \ldots, n.$$

By definition, we have

$$p_1(x_{n+1}) \equiv l(x_{n+1}) \pmod{B},$$

and hence also

$$p_1(x_{n+1}) \equiv l(x_{n+1}) \pmod{S}.$$

This means that there exist functions $p_2, p_3 \in F$ such that

$$p_2(x_i) = p_3(x_i) \text{ for } i = 1, 2, \ldots, n$$

and

$$p_2(x_{n+1}) = p_1(x_{n+1}),\ p_3(x_{n+1}) = l(x_{n+1}).$$

Let m be a term such that $m_{\mathbf{A}}$ is a Mal'cev function on $D_3 \times D_3 \times D_3$, where D_3 is given by $\{p_j(x_i) \mid j = 1, 2, 3;\ i = 1, 2, \ldots, n+1\}$.

We define $p_4 \in F$ by

$$p_4 := m_{\mathbf{A}}\big(p_1, p_2, p_3\big)$$

and obtain for $i = 1, \ldots, n$ the equality

$$p_4(x_i) = m_{\mathbf{A}}\big(p_1, p_2, p_3\big)\ (x_i) = m_{\mathbf{A}}\big(p_1, p_2, p_2\big)\ (x_i) = p_1(x_i) = l(x_i).$$

For x_{n+1}, we obtain

$$p_4(x_{n+1}) = m_{\mathbf{A}}\big(p_1, p_2, p_3\big)\ (x_{n+1}) = m_{\mathbf{A}}\big(p_2, p_2, p_3\big)\ (x_{n+1}) = p_3(x_{n+1}) = l(x_{n+1}).$$

Hence p_4 is the required interpolating function. □

Interpolation results are often in the centre of algebraic structure theory. For this reason, it is not surprising that we may fruit Proposition 2.2 in many ways. Let us give one application of this result. A more general version is given in Chapter 6.

PROPOSITION 2.3. *Let $\mathbf{V}$ be an Ω-group such that $[I, I]_{\mathbf{V}} = I$ for every ideal I of $\mathbf{V}$, let $k \in \mathbb{N}$, let D be a finite subset of of V^k, and let $f : D \to V$ be a function such that for all $\mathbf{v}, \mathbf{w} \in D$ the difference*

$$f(v_1, v_2, \ldots, v_k) - f(w_1, w_2, \ldots, w_k)$$

lies in the ideal of $\mathbf{V}$ generated by $\{v_1 - w_1, v_2 - w_2, \ldots, v_k - w_k\}$.

Then f is the restriction of a polynomial function of $\mathbf{V}$.

Proof: The conditions that we have put on f mean that f is a congruence preserving (=compatible) function. It is well-known that therefore f can be interpolated at every two-element subset of its domain by a polynomial function (cf. [**Pil83**, Proposition 7.131]).

We consider the algebra $\mathbf{V}^*$. This is the expansion of $\mathbf{V}$ that we obtain by adding all elements of V as constant operations. The congruences of $\mathbf{V}^*$ are precisely those of $\mathbf{V}$, the commutators stay the same. (For this proof, it is already sufficient to see that the commutators definitely cannot become smaller by adding new operations.) Therefore, $\mathbf{V}^*$ is neutral. The algebra $\mathbf{V}^*$ does not have any proper subalgebra. Now we apply Proposition 2.2 to the function algebra $\mathbf{F}$ given by

$$F = \{p|_D \mid p \in \mathsf{P}_k(\mathbf{V})\}.$$

Proposition 2.2 yields that f lies in F. □

This Proposition implies that on a neutral algebra, every congruence preserving function can be interpolated at every finite subset of its domain by a polynomial function. Later, we will formulate this by saying that the polynomial functions are *dense* in the compatible functions.

CHAPTER 3

Composition algebras

1. Adding composition

In [**Pil83**, 1.118], the following method of constructing new algebraic structures is described:

> Take a universal algebra $A = (A, \Omega)$, form the set $M(A)$ of all self-maps of A and define the operations of Ω pointwise on $M(A)$. Adding the binary operation "$\circ$" of composition yields a new algebra $M(A) = (M(A), \Omega \cup \{\circ\})$.

Starting with A being a group, we obtain the near-ring of all functions on A, starting with A being a ring, we obtain a composition ring cf. [**Adl62**], and starting with A being a set with no operations, we obtain a semigroup. It is therefore rewarding to study this process in the general context of universal algebra, hoping that some of the knowledge about the structure of special cases might carry over to the general case. A support for this hope is the paper [**Mli75**], in which R. Mlitz gives a universal algebra pattern of Jacobson's Density Theorem for rings [**Jac64**, p.28] and the Density Theorem for near-rings [**Ram69, Pol71, Bet73**]. In this chapter, we shall develop some structural results for the algebras obtained by the process outlined above and their subalgebras, and we will see that these results explain and generalize many results obtained for near-rings and composition rings. We will investigate what the above process yields for those algebras A that lie in congruence permutable varieties: every algebra with groop (or loop) reduct is such an algebra. What happens if we lack congruence permutability can be found in [**Che97**].

> Dear reader! I really do not want to lose you because of the notational complications that cannot be avoided in universal algebra. Therefore, in these sections written in smaller font, I will keep telling you what the developed theory means for my supervisor's favourite algebraic structures, namely near-rings.

In this section, we will formalize how to add this binary operation $\circ$ to an algebra. Let us first define the type of such algebras:

DEFINITION 3.1. Let $\tau = (\mathcal{F}, \sigma)$ be a type of algebras such that $\circ$ does not lie in the set $\mathcal{F}$ of operation symbols of τ. Then we define a new type as the type that contains all operation symbols of $\mathcal{F}$ plus the binary operation symbol $\circ$. This new type is abbreviated by $\mathcal{C}(\tau)$. We will call $\mathcal{C}(\tau)$ the *composition type over* τ.

Formally, this definition could be stated as follows:

$$\mathcal{C}(\tau) = (\mathcal{F} \cup \{\circ\}, \sigma'),$$

where $\sigma'|_{\mathcal{F}} = \sigma$ and $\sigma'(\circ) = 2$. In the sequel, we will always assume that a type τ from which we construct the type $\mathcal{C}(\tau)$ does not contain the operation symbol $\circ$.

> If we want to construct near-rings, then we have to start with the type τ that defines groups. If τ has the operation symbol $+$ then the composition type $\mathcal{C}(\tau)$ has the symbols $+$ and $\circ$.

Given an algebra of type $\mathcal{C}(\tau)$, we sometimes want to forget about the added composition:

DEFINITION 3.2. For an algebra $\mathbf{F}$ of type $\mathcal{C}(\tau)$, let $\mathbf{F}^+$ be the reduct of $\mathbf{F}$ of type τ.

> So, if we start with a near-ring $\mathbf{F} = (F; +, \circ)$, we end up with $\mathbf{F}^+ = (F; +)$. Hence this operation of forgetting the composition operation leaves us with the additive structure of the near-ring.

The construction that we give here shall model the way in which near-rings are obtained from groups, or composition rings from rings. Hence, starting with a type τ, we will not admit every algebra of type $\mathcal{C}(\tau)$ as a composition algebra over τ, but we put two further conditions on it: We say that a *composition algebra over type* τ is an algebra of type $\mathcal{C}(\tau)$ in which the composition is associative and $\circ$ is right distributive with respect to all other operations. Actually, the definition given here is a special case of the definition of composition algebras given in [**LN73**, Chapter 3].

DEFINITION 3.3. Let τ be a type. Then an algebra $\mathbf{F}$ of type $\mathcal{C}(\tau)$ is called *a composition algebra over the type* τ iff

(1) The operation $\circ_{\mathbf{F}}$ is associative, i.e., for all $f, g, h \in F$ we have $(f \circ_{\mathbf{F}} g) \circ_{\mathbf{F}} h = f \circ_{\mathbf{F}} (g \circ_{\mathbf{F}} h)$.
(2) The operation $\circ_{\mathbf{F}}$ is *right distributive* with respect to all fundamental operations of $\mathbf{F}^+$, i.e., for all $n \in \mathbb{N}_0$, for all n-ary operation symbols of τ, and for all $f_1, f_2, \ldots, f_n, g \in F$ we have

$$\omega_{\mathbf{F}}(f_1, f_2, \ldots, f_n) \circ_{\mathbf{F}} g = \omega_{\mathbf{F}}(f_1 \circ_{\mathbf{F}} g, f_2 \circ_{\mathbf{F}} g, \ldots, f_n \circ_{\mathbf{F}} g).$$

> These conditions mean that $(F; +, \circ)$ satisfies the identites $(x \circ y) \circ z = x \circ (y \circ z)$ and $(x + y) \circ z = x \circ z + y \circ z$.

A different way of stating these associative and distributive laws that are is given in the following proposition.

PROPOSITION 3.4. *An algebra* $\mathbf{F}$ *of type* $\mathcal{C}(\tau)$ *is a composition algebra iff*

(1) $\circ_{\mathbf{F}}$ *is associative.*
(2) *For each* $x \in F$, *the mapping* $r_x : F \to F$, $f \mapsto f \circ_{\mathbf{F}} x$ *is a homomorphism from* $\mathbf{F}^+$ *to* $\mathbf{F}^+$.

This tells that $(F;+,\circ)$ is a composition algebra if $\circ$ is associative and for every $x \in F$ the mapping $r_x : F \to F, f \to f \circ x$ is a group homomorphism of $(F;+)$. This homomorphism property is just the distributive law.

Yet this process is not refined enough to produce the class of all near-rings as the class of all composition algebras over the group-type. The reason for this is that in a near-ring $\mathbf{F} = (F;+,\circ)$ the additive structure has to satisfy the group laws for $\mathbf{F}^+ = (F;+)$, whereas Definition 3.3 does not put any restrictions on $\mathbf{F}^+$. Therefore, we give the following definition.

DEFINITION 3.5. Let $\mathcal{V}$ be a class of algebras of type τ. Then an algebra $\mathbf{F}$ of type $\mathcal{C}(\tau)$ is a $\mathcal{V}$-*composition algebra* iff

(1) $\mathbf{F}$ is a composition algebra over the type τ.
(2) $\mathbf{F}^+$ lies in the class $\mathcal{V}$.

Let $\mathcal{G}$ be the class of all groups. Then the $\mathcal{G}$-composition algebras are just the near-rings.

The class $\mathcal{V}$ will often by a variety of algebras. We note that in order to be able to consider groups as a variety, we have to see them as algebras with the binary operation $+$, the unary operation $-$ of finding the inverse, and a constant operation 0 that gives the group identity. It is easy to see that for the variety of groups $\mathcal{G}$ the class of all $\mathcal{G}$-composition algebras is the class of all near-rings, seen as algebras with the operations $+, -, 0, \circ$. For the class of all rings $\mathcal{R}$, the $\mathcal{R}$-composition algebras are precisely the composition rings, which were studied in [**Adl62**], and which are going to be investigated closer in Chapter 5. Composition near-rings [**PV97**] fall into the same pattern, too. These last examples suggests the following way of giving a name to $\mathcal{V}$-composition algebras: If the algebras in $\mathcal{V}$ are the *xxx*s, the $\mathcal{V}$-composition algebras should be called *composition xxx*s.

Questions about these composition algebras that arise naturally are for example:

(1) Are there meaningful examples of composition algebras ?
(2) For a given class $\mathcal{V}$, is it possible to describe all simple (or subdirectly irreducible, finite, ...) $\mathcal{V}$-composition algebras ?

We will now give two constructions that produce a $\mathcal{V}$-composition algebra out of an algebra in $\mathcal{V}$.

DEFINITION 3.6 (The composition algebra of functions on $\mathbf{A}$). Let $\mathcal{V}$ be a class of algebras of type τ, and let $\mathbf{A} \in \mathcal{V}$. We can then define the $\mathcal{V}$-composition algebra $\mathbf{M}(\mathbf{A})$ with universe $M(A) := \{f : A \to A\}$. For the operation symbols of τ, we define the operation $\omega_{\mathbf{M}(\mathbf{A})}$ on $M(A)$ as the pointwise application of the operation $\omega_{\mathbf{A}}$. The operation $\circ_{\mathbf{M}(\mathbf{A})}$ is defined by

$$f \circ_{\mathbf{M}(\mathbf{A})} g \ \ (a) := f(g(a)) \text{ for } a \in A.$$

> For a group $\mathbf{G} = (G; +)$ (written additively, but not necessarily abelian), we obtain $\mathbf{M}(\mathbf{G})$ as the near-ring $(G^G; +, \circ)$, where $+$ is defined pointwisely and $\circ$ is the operation of functional composition.

At a closer look, we find out that $\mathbf{M}(\mathbf{A})^+$ is the cartesian product $\mathbf{A}^A$; and $\circ_{\mathbf{M}(\mathbf{A})}$ is the operation of functional composition. We call $\mathbf{M}(\mathbf{A})$ the *full function composition algebra on* $\mathbf{A}$.

> It is known that every near-ring $(F; +, \circ)$ can be embedded into the near-ring $\mathbf{M}(\mathbf{G})$ for some group $\mathbf{G}$. A group that always works for that purpose is the direct product of $(F; +)$ with the cyclic group of order 2. The same embedding result holds if, instead of near-rings, we consider $\mathcal{V}$-composition algebras where $\mathcal{V}$ is a variety of algebras. This result is stated in Proposition 3.7.
> Whenever studying groups, the problem arises that groups, seen as algebras with one binary operation $+$, do not form a variety. Therefore, on those occasions where we want to see the class of groups as a variety, we consider groups as algebas with the additional operations $-$ (inverse) and 0 (identity).

PROPOSITION 3.7 ([**LN73**, Chapter 3, Theorem 1.51]). *Let $\mathcal{V}$ be a variety of algebras. Then for every $\mathcal{V}$-composition algebra $\mathbf{F}$ there is an algebra $\mathbf{A} \in \mathcal{V}$ such that $\mathbf{F}$ isomorphic to a subalgebra of $\mathbf{M}(\mathbf{A})$.*

So every composition algebra can be embedded into some $\mathbf{M}(\mathbf{A})$.

We want to continue with other examples of composition algebras.

DEFINITION 3.8 (The constant composition algebra on $\mathbf{A}$). Let $\mathcal{V}$ be a variety, and let $\mathbf{A} \in \mathcal{V}$. We can then define the $\mathcal{V}$-composition algebra $\mathbf{A}_c$ with universe A by ${\mathbf{A}_c}^+ := \mathbf{A}$, and $a_1 \circ_{\mathbf{A}_c} a_2 := a_1$.

> On every group $(G; +)$ we can define an operation $\circ$ such that $(G; +, \circ)$ becomes a near-ring: we simply define $g_1 \circ g_2 = g_1$.

DEFINITION 3.9 (The composition algebra of constant functions on $\mathbf{A}$). We define the algebra $\mathbf{M_C}(\mathbf{A})$ as the subalgebra of $\mathbf{M}(\mathbf{A})$ whose universe is given by $M_C(A) := \{m : A \to A \mid |m(A)| = 1\}$.

PROPOSITION 3.10. *For any algebra $\mathbf{A}$, the algebras $\mathbf{A}_c$ and $\mathbf{M_C}(\mathbf{A})$ are isomorphic composition algebras.*

Proof: We take $a \in A$ and consider the mapping

$$\begin{array}{rccc} \Phi & : & M_C(A) & \longrightarrow & A \\ & & m & \longmapsto & m(a). \end{array}$$

Then Φ is an isomorphism between $\mathbf{M_C}(\mathbf{A})$ and $\mathbf{A}_c$. □

2. Local interpolation algebras

Throughout this section, we fix a class $\mathcal{V}$ of algebras of type τ. Furthermore, we let $\mathbf{A} \in \mathcal{V}$, and $\mathbf{F}$ be a subalgebra of $\mathbf{M}(\mathbf{A})$, whose universe, as usual, is denoted by F. We observe that $\mathbf{F}$ is then a $\mathcal{V}$-composition algebra. We will now see that the set $\mathsf{L}_n F$ of those function that can be interpolated at a fixed number of points by a function in F, which was defined in Definition 1.2, is a subuniverse of $\mathbf{M}(\mathbf{A})$.

PROPOSITION 3.11. *For any cardinal number n, the set $\mathsf{L}_n F$ is a subuniverse of $\mathbf{M}(\mathbf{A})$.*

> The set of those functions that can be interpolated at any subset of n places by a polynomial function has been investigated in [**HN77, Nöb78, Aic98**]. Instead of the set of polynomial functions, one may also start with a near-ring. For $(F; +, \circ)$ being a near-ring, $\mathsf{L}_n F$ has been studied in [**Aic95**].

Proof: $\mathsf{L}_n F$ is closed under the operations from $\mathcal{F}$: Let $k \in \mathbb{N}_0$, and let ω be k-ary operation symbol of the type τ. Furthermore, let $l_1, l_2, \ldots, l_k \in \mathsf{L}_n F$. We have to prove

$$\omega_{\mathbf{M}(\mathbf{A})}(l_1, l_2, \ldots, l_k) \in \mathsf{L}_n F.$$

For this purpose, let S be a set with $|S| \leq n$. Since $l_1, l_2, \ldots, l_k \in \mathsf{L}_n F$, there are functions $f_1, f_2, \ldots, f_k \in F$ such that $l_i|_S = f_i|_S$. Now it is easy to see that $\omega_{\mathbf{M}(\mathbf{A})}(f_1, f_2, \ldots, f_k)$ interpolates $\omega_{\mathbf{M}(\mathbf{A})}(l_1, l_2, \ldots, l_k)$ at S.

For proving that $\mathsf{L}_n F$ is closed under functional composition, we take $l_1, l_2 \in \mathsf{L}_n F$. We have to prove that c defined by

$$\begin{array}{rccc} c & : & A & \longrightarrow & A \\ & & a & \longmapsto & l_2(l_1(a)) \end{array}$$

is in $\mathsf{L}_n F$. To this end, let S be a set with $|S| \leq n$. There is a function $f_1 \in F$ with $f_1|_S = l_1|_S$. Since $|f_1(S)| \leq |S| \leq n$, there is also a function $f_2 \in F$ with $f_2|_{f_1(S)} = l_2|_{f_1(S)}$. Now we see that $f_2 \circ_{\mathbf{M}(\mathbf{A})} f_1$ interpolates c at S. Therefore, we have $c \in \mathsf{L}_n F$. □

DEFINITION 3.12 ($\mathbf{L}_n\mathbf{F}$). For a cardinal number n, the subalgebra of $\mathbf{M}(\mathbf{A})$ with universe $\mathsf{L}_n F$ is denoted by $\mathbf{L}_n\mathbf{F}$.

The algebras constructed as $\mathbf{L}_n\mathbf{F}$ will be called *local interpolation algebras*. Actually, the operator $\mathbf{L}_n$ has the following properties:

PROPOSITION 3.13. *Let $\mathbf{F}, \mathbf{G}$ be subalgebras of $\mathbf{M}(\mathbf{A})$, and let b, m, n, s be cardinal numbers. Then the following properties hold:*

(1) $\mathbf{F} \leq \mathbf{G} \Rightarrow \mathbf{L}_n\mathbf{F} \leq \mathbf{L}_n\mathbf{G}$.
(2) $\mathbf{F} \leq \mathbf{L}_n\mathbf{F}$.
(3) $\mathbf{L}_b\mathbf{F} \leq \mathbf{L}_s\mathbf{F}$ *if* $s \leq b$.
(4) $\mathbf{L}_m\mathbf{L}_n\mathbf{F} = \mathbf{L}_{\min(m,n)}\mathbf{F}$.

Proof: (1), (2) and (3) follow from the definition.

For (4), we first prove

$$\mathbf{L}_{\min(m,n)}\mathbf{F} \leq \mathbf{L}_m\mathbf{L}_n\mathbf{F}.$$

If $m \leq n$, we have $\mathbf{L}_{\min(m,n)}\mathbf{F} = \mathbf{L}_m\mathbf{F} \leq \mathbf{L}_m\mathbf{L}_n\mathbf{F}$. If $m \geq n$, we have $\mathbf{L}_{\min(m,n)}\mathbf{F} = \mathbf{L}_n\mathbf{F} \leq \mathbf{L}_m\mathbf{L}_n\mathbf{F}$. Now we prove

$$\mathbf{L}_m\mathbf{L}_n\mathbf{F} \leq \mathbf{L}_{\min(m,n)}\mathbf{F}.$$

Let $l \in \mathsf{L}_m\mathsf{L}_nF$. For proving that $l \in \mathsf{L}_{\min(m,n)}F$, let S be a subset of A with $|S| \leq \min(m,n)$. Since $l \in \mathsf{L}_m\mathsf{L}_nF$, there is a function $l_1 \in \mathsf{L}_nF$ such that $l|_S = l_1|_S$. Since $l_1 \in \mathsf{L}_nF$, there is a function $l_2 \in F$ such that $l_2|_S = l_1|_S$. Therefore, we also have $l_2|_S = l|_S$, which proves $l \in \mathsf{L}_{\min(m,n)}F$. □

We will now define an algebra consisting of those functions that can be interpolated at any finite subset of A by a function in F.

Definition 3.14. We define

$$\mathsf{L}F := \bigcap_{n \text{ finite}} \mathsf{L}_nF.$$

Then $\mathsf{L}F$ is a subuniverse of $\mathbf{M}(\mathbf{A})$. We write $\mathbf{LF}$ for the corresponding subalgebra.

We will now list some properties of the operator $\mathbf{L}$.

Proposition 3.15. *Let n be a cardinal number.*

(1) $\mathbf{L}\mathbf{L}_n\mathbf{F} = \mathbf{L}_n\mathbf{L}\mathbf{F} = \mathbf{L}_n\mathbf{F}$ *if n is finite.*
(2) $\mathbf{L}\mathbf{L}\mathbf{F} = \mathbf{L}\mathbf{F}$.
(3) $\mathbf{L}\mathbf{L}_n\mathbf{F} = \mathbf{L}_n\mathbf{L}\mathbf{F} = \mathbf{L}\mathbf{F}$ *if n is infinite.*

Proof:

(1) Let us first prove $\mathsf{L}\mathsf{L}_nF = \mathsf{L}_nF$. We have

$$\begin{aligned}\mathsf{L}\mathsf{L}_nF &= \bigcap_{m\in\mathbb{N}} \mathsf{L}_m\mathsf{L}_nF \\ &= \bigcap_{m\in\mathbb{N}} \mathsf{L}_{\min(m,n)}F \\ &= \mathsf{L}_nF.\end{aligned}$$

Now we prove $\mathsf{L}_n\mathsf{L}F = \mathsf{L}_nF$. The relation $\supseteq$ follows from $F \subseteq \mathsf{L}F$. For $\subseteq$, we compute $\mathsf{L}_n\mathsf{L}F \leq \mathsf{L}_n\mathsf{L}_nF = \mathsf{L}_nF$.

(2) $\mathsf{L}\mathsf{L}F = \bigcap_{m\in\mathbb{N}} \mathsf{L}_m\mathsf{L}F = \bigcap_{m\in\mathbb{N}} \mathsf{L}_mF = \mathsf{L}F$.
(3) If n is an infinite cardinal, then we have $\mathsf{L}_nF \subseteq \mathsf{L}F$. This implies that both $\mathsf{L}\mathsf{L}_nF$ and $\mathsf{L}_n\mathsf{L}F$ are subsets of $\mathsf{L}\mathsf{L}F$, which is equal to $\mathsf{L}F$.

These operators allow an easy description of what we mean by *density*:

DEFINITION 3.16. Let $\mathbf{F}, \mathbf{G}$ be subalgebras of $\mathbf{M}(\mathbf{A})$. Then we say that $\mathbf{F}$ is *dense* in $\mathbf{G}$ iff $\mathbf{F} \leq \mathbf{G} \leq \mathbf{LF}$.

PROPOSITION 3.17. *Let $\mathbf{F}, \mathbf{G}$ be subalgebras of $\mathbf{M}(\mathbf{A})$. Then we have:*

(1) $\mathbf{LF}$ *is the largst subalgebra of* $\mathbf{M}(\mathbf{A})$ *in which* $\mathbf{F}$ *is dense.*
(2) *Let n be a natural number. Then $\mathbf{F}$ is dense in $\mathbf{L}_n\mathbf{F}$ iff $\mathbf{LF} = \mathbf{L}_n\mathbf{F}$.*

Proof: (1) follows from the definition. For (2) we note that $\mathbf{F}$ is dense in $\mathbf{L}_n\mathbf{F}$ iff $\mathbf{F} \leq \mathbf{L}_n\mathbf{F} \leq \mathbf{LF}$. This holds iff $\mathbf{LF} = \mathbf{L}_n\mathbf{F}$. □

In the following, we shall often get the result: $\mathbf{F}$ is dense in $\mathbf{L}_2\mathbf{F}$. By the last proposition this is equivalent to $\mathbf{L}_2\mathbf{F} = \mathbf{LF}$. This equality can be paraphrased as follows:

> If a function g on A can be interpolated by a function in F at each set of 2 points then g can be interpolated by a function in F at *each finite subset* of A.

Furthermore, Proposition 3.17 shows that if $\mathbf{F}$ is dense in $\mathbf{L}_2\mathbf{F}$ then $\mathbf{L}_2\mathbf{F}$ is really the largest of all subalgebras of $\mathbf{M}(\mathbf{A})$ in which $\mathbf{F}$ is dense.

We will now give a property that implies $\mathbf{LF} = \mathbf{F}$.

DEFINITION 3.18. Let B be a subset of A. Then B is called a *base of equality* of $\mathbf{F}$ iff for all $f, g \in F$ with $f|_B = g|_B$ we have $f = g$.

As an example, let $\mathbf{G}$ be an abelian group and let $\mathbf{P}(\mathbf{G})$ be the subalgebra of $\mathbf{M}(\mathbf{G})$ with the unary polynomial functions as universe. We know that the polynomial functions are those of the form $f(g) = z \cdot g + h$ with $z \in \mathbb{Z}$ and $h \in G$. If $\mathbf{G}$ has an element e of infinite order, then $\{0, e\}$ is a base of equality of $\mathbf{P}(\mathbf{G})$.

We will now give the example of a countable abelian group where the polynomial functions do not admit a finite base of equality. Fixing a prime p, we consider the group $\mathbf{Z}_{p^\infty}$, which is the subgroup of the multiplicative group of the complex numbers with universe

$$\mathbb{Z}_{p^\infty} := \{x \in \mathbb{C} \mid \exists n \in \mathbb{N} : x^{p^n} = 1\}.$$

We will now show that the unary polynomial functions $\mathbf{P}(\mathbf{Z}_{p^\infty})$ have no finite base of equality. Keeping multiplicative notation, the unary polynomial functions on this group are the functions of the form $f(x) = c \cdot x^z$ with $c \in \mathbb{Z}_{p^\infty}$, $z \in \mathbb{Z}$. Suppose, D is a finite set. Then let n be large enough to ensure $d^{p^n} = 1$ for all $d \in D$. The polynomial functions $f(x) = x^{p^n}$ and $g(x) = 1$ agree on D, but are not equal, which disqualifies D as a base of equality.

The following proposition is an obvious modification of [**HN77**, Lemma 1].

PROPOSITION 3.19. *Let B be a base of equality for $\mathbf{F}$ and let b be the cardinality of B. Then the following holds.*

(1) *If b is finite then* $\mathbf{L}_{b+1}\mathbf{F} = \mathbf{F}$.
(2) *If b is infinite then* $\mathbf{L}_b\mathbf{F} = \mathbf{F}$.

Proof: (1): Suppose that there is a function $l \in \mathsf{L}_{b+1}F$ that does not lie in F. Let $f_1 \in F$ be a function with $f_1|_B = l|_B$. Since f_1 lies in F and l does not, they have to differ in at least one point, say a. Now the cardinality of $B \cup \{a\}$ is $b+1$, hence there is a function $f_2 \in F$ with $l|_{B\cup\{a\}} = f_2|_{B\cup\{a\}}$. Therefore, we have $f_1|_B = f_2|_B$, and $f_1(a) \neq f_2(a)$. But this contradicts the fact that B is a base of equality of $\mathbf{F}$.

(2): Suppose that there is a function $l \in \mathsf{L}_bF$ that does not lie in F. Let $f_1 \in F$ be a function with $f_1|_B = l|_B$. Since f_1 lies in F and l does not, they have to differ in at least one point, say a. Now the cardinality of $B\cup\{a\}$ is b, hence there is a function $f_2 \in F$ with $l|_{B\cup\{a\}} = f_2|_{B\cup\{a\}}$. Therefore, we have $f_1|_B = f_2|_B$, and $f_1(a) \neq f_2(a)$. But this contradicts the fact that B is a base of equality of $\mathbf{F}$. □

We give an easy application of this proposition:

Corollary 3.20. *Let $\mathbf{D}$ be an infinite integral domain and let p be a function on D that can be interpolated at every countable subset of D by a polynomial function. Then p is a polynomial function.*

Proof: Let $\aleph_0$ be the cardinality of the naturals. Then every countable subset of D is a base of equality of $\mathbf{P}$, where $\mathbf{P}$ is the subalgebra of $\mathbf{M}(\mathbf{D})$ that consists of all unary polynomial functions on $\mathbf{D}$. Hence Proposition 3.19 gives $\mathbf{L}_{\aleph_0}\mathbf{P} = \mathbf{P}$, and therefore p is a polynomial function. □

Proposition 3.21. *Let f be the cardinality of $\mathbf{F}$. Then there is a base of equality B for $\mathbf{F}$ with $|B| \leq f^2$.*

Proof: For each pair $(f_1, f_2) \in F^2$ with $f_1 \neq f_2$, we take an element $a_{(f_1,f_2)}$ such that

$$f_1(a_{(f_1,f_2)}) \neq f_2(a_{(f_1,f_2)}).$$

Now we take

$$B := \{a_{(f_1,f_2)} | (f_1, f_2) \in F^2, f_1 \neq f_2\}.$$

We will now show that B is a base of equality for $\mathbf{F}$. To this end, let g, h be two elements in F with $g|_B = h|_B$. But then, we have $g(a_{(g,h)}) = h(a_{(g,h)})$, which contradicts the choice of $a_{(g,h)}$. □

If $\mathbf{F}$ is infinite, then this upper bound f^2 can actually be reached: As an example, one may again consider the unary polynomial functions on the group $\mathbf{Z}_{p^\infty}$.

Proposition 3.22. *If A is finite or F is finite then we have $\mathbf{LF} = \mathbf{F}$.*

Proof: If A is finite, then, clearly, A is a finite base of equality for $\mathbf{F}$. If F is finite, then Proposition 3.21 produces a finite base of equality for $\mathbf{F}$. Let b be the cardinality of this base of equality. Then, by Proposition 3.19 we have $\mathbf{LF} \leq \mathbf{L}_{b+1}\mathbf{F} = \mathbf{F}$. □

In the next paragraph, we shall see that sometimes there is a kind of reversion of Proposition 3.19. A slightly more general version of this result is given in [**Aic98**]. The investigations of the next paragraph also follow the proposal of [**Nöb78**] to investigate the cardinalities of the sets $\mathsf{LP}_t(\mathbf{A})$ for all kinds of universal algebras $\mathbf{A}$. We also give an elementary reason for the known fact that there are uncountably many local polynomial functions on the integers. However, we have to put restrictions on $\mathbf{A}$ and $\mathbf{F}$:

CONVENTION 3.23. We assume that $\mathbf{A}$ has a reduct $\mathbf{A}' = (A; +, -, 0)$ which is a group. We also assume that $\mathbf{F}$ is a subalgebra of $\mathbf{M}(\mathbf{A})$.

LEMMA 3.24. *Let $\mathbf{F}$, $\mathbf{A}$ be as in Convention 3.23. Then D is a base of equality for F iff $D \subseteq A$ and every function in F that is zero at all elements of D is zero everywhere on A.*

We recall that we call a set *countable* iff it is finite or countably infinite.

THEOREM 3.25. *Let $\mathbf{A}$ and $\mathbf{F}$ be as in Convention 3.23. If A and F are both countable, and if $F = \mathsf{L}F$, then there exists a* finite *base of equality D for F.*

Proof: The result is obvious if F or A is finite. Let $a_0, a_1, a_2, \ldots$ and $f_0, f_1, f_2, \ldots$ be complete enumerations of F and A, respectively. Furthermore we abbreviate the set $\{a_i \mid i \leq r\}$ by $A(r)$.

Suppose that there is no finite base of equality for F. We shall construct a sequence $(n_m)_{m\in\mathbb{N}_0}$ of non-negative integers and a sequence $(g_m)_{m\in\mathbb{N}_0}$ of elements of F with the following properties:

(1) $\forall m \in \mathbb{N}_0 : g_m|_{A(n_m)} \neq f_m|_{A(n_m)}$
(2) $\forall m \in \mathbb{N}_0 : n_{m+1} > n_m$
(3) $\forall m \in \mathbb{N}_0 : g_{m+1}|_{A(n_m)} = g_m|_{A(n_m)}$.

We construct the sequences inductively. Let $g_0 \in F$ such that $g_0 \neq f_0$. Let n_0 be minimal in $\mathbb{N}_0$ with $g_0(a_{n_0}) \neq f_0(a_{n_0})$.

If we have already constructed g_m and n_m we construct g_{m+1} and n_{m+1} as follows:

In the case $g_m|_{A(n_m)} = f_{m+1}|_{A(n_m)}$ there exists a function $h \in F$ with $g_m|_{A(n_m)} = h|_{A(n_m)}$ and $h \neq f_{m+1}$, since otherwise $A(n_m)$ would be a forbidden base of equality for F. We set $g_{m+1} := h$. Now let n_{m+1} be minimal with $h(a_{n_{m+1}}) \neq f_{m+1}(a_{n_{m+1}})$.

If $g_m|_{A(n_m)} \neq f_{m+1}|_{A(n_m)}$, we set $g_{m+1} := g_m$ and $n_{m+1} := n_m + 1$.

Since for every $a \in A$, the sequence $(g_m(a))_{m\in\mathbb{N}}$ is eventually constant, we may define a function l on A by

$$l(a) := \lim_{m\to\infty} g_m(a).$$

The function l lies in $\mathsf{L}F$, and hence, by assumption, l lies in F. So l is equal to f_m for some $m \in \mathbb{N}_0$. Since $l|_{A(n_m)} = g_m|_{A(n_m)}$ and $g_m|_{A(n_m)} \neq f_m|_{A(n_m)}$, we obtain $l|_{A(n_m)} \neq f_m|_{A(n_m)}$. But this shows that l can not be equal to f_m. □

Putting the last two propositions together, we get:

COROLLARY 3.26. *Let* $\mathbf{A}$ *and* $\mathbf{F}$ *be as in Convention 3.23. If* F *and* A *are both countable and if* $F = \mathsf{L}F$ *then there exists an* $n \in \mathbb{N}_0$ *such that* $F = \mathsf{L}_n F$.

This property can be strengthened:

COROLLARY 3.27. *Let* $\mathbf{A}$ *and* $\mathbf{F}$ *be as in Convention 3.23. If* $\mathsf{L}F$ *and* A *are both countable, then we have:*

(1) *There is a finite base of equality* D *for* F.
(2) $\mathsf{L}F = F$.

Proof: By the idempotence of the operator L, we have $\mathsf{L}F = \mathsf{L}\mathsf{L}F$. Since both $\mathsf{L}F$ and A are countable, we may apply Theorem 3.25 and get a finite base of equality D for $\mathsf{L}F$. Since F is a subset of $\mathsf{L}F$, the set D is also a base of equality of F. This proves (1); the claim in (2) now follows by Proposition 3.19. □

COROLLARY 3.28. *Let* $\mathbf{R}$ *be a countably infinite integral domain, Then* $\mathsf{LP}_1(\mathbf{R})$ *is not countable.*

Proof: We suppose that $\mathsf{LP}_1(\mathbf{R})$ is countable. Then there exists a finite base of equality D for $\mathsf{P}_1(\mathbf{R})$, and hence the polynomial $p(x) := \prod_{d \in D}(x - d)$ induces the zero-function on R. This is impossible because $\mathbf{R}$ is an infinite integral domain. □

For polynomial functions on Ω-groups, we obtain the following corollary.

COROLLARY 3.29. *Let* $\mathbf{V}$ *be an* Ω*-group. If* $\mathsf{LP}_1(\mathbf{V})$ *is countable then there exists a finite base of equality for* $\mathsf{P}_1(\mathbf{V})$.

Proof: The result follows from Corollary 3.27 if we observe that if $\mathsf{LP}_1(\mathbf{V})$ is countable, then $\mathbf{V}$ is countable as well. □

We can apply this result to the unary polynomial functions on the group $\mathbf{Z}_{p^\infty}$. Then we obtain that $\mathsf{LP}_1(\mathbf{Z}_{p^\infty})$ is not countable.

So we have seen that $\mathbf{LF}$ can be a lot bigger that $\mathbf{F}$. Another example of this phenomenon is perhaps the following: Let $\mathbf{D}$ be any infinite field, and let $\mathbf{F}$ be the composition ring of all polynomial functions on $\mathbf{D}$. Then we have $|F| = |D|$. However, since every function can be interpolated at a finite number of points by a polynomial function, we have $\mathbf{LF} = \mathbf{M}(\mathbf{D})$, and therefore $|\mathsf{L}F| > |D|$. It is therefore surprising that $\mathbf{LF}$ and $\mathbf{F}$ fulfil precisely the same identities:

PROPOSITION 3.30. *Let* $\mathcal{V}$ *be a variety of algebras, let* $\mathbf{A}$ *be an algebra in* $\mathcal{V}$*, and let* $\mathbf{F}$ *be a subalgebra of* $\mathbf{M}(\mathbf{A})$. *Then* $\mathbf{F}$ *and* $\mathbf{LF}$ *generate the same subvariety of the variety of all* $\mathcal{V}$*-composition algebras.*

If we take a group $\mathbf{G} = (G; +, -, 0)$ and $(F; +, -, 0, \circ)$ as a subnear-ring of $(M(G); +, -, 0, \circ)$, then Proposition 3.30 tells that $(\mathsf{L}F; +, -, 0, \circ)$ satisfies

all the identites satisfied by $(F;+,-,0,\circ)$. For example, if $(F;+,\circ)$ is a ring, then $(\mathsf{L}F;+,\circ)$ must be a ring as well.

Proof: Let $\mathcal{V}_1$ be the variety generated by $\mathbf{F}$ and $\mathcal{V}_2$ be the variety generated by $\mathbf{LF}$. Since $\mathbf{F} \leq \mathbf{LF}$, we obviously have $\mathcal{V}_1 \subseteq \mathcal{V}_2$. For $\mathcal{V}_1 \supseteq \mathcal{V}_2$, we show that $\mathbf{LF}$ fulfills all equations satisfied by $\mathbf{F}$. But this will follow from Proposition 3.32. □

For studying the equations satisfied by $\mathbf{LF}$, we fix the variables $x_1, x_2, \ldots, x_k$, and we let T be the set of all terms of type $\mathcal{C}(\tau)$ over $x_1, x_2, \ldots, x_k$. Let $\mathbf{N}$ be an algebra of type $\mathcal{C}(\tau)$, and let $t^{(1)}, t^{(2)}$ be terms in T. We recall from Definition 1.1 that the equation $t^{(1)} = t^{(2)}$ is an *identity* of $\mathbf{N}$ iff

$$\forall \xi_1, \xi_2, \ldots, \xi_k \in N \,:\, t^{(1)}_{\mathbf{N}}(\xi_1, \xi_2, \ldots, \xi_k) = t^{(2)}_{\mathbf{N}}(\xi_1, \xi_2, \ldots, \xi_k),$$

where $t^{(i)}_{\mathbf{N}}$ denotes the function from N^k to N that is induced by the term $t^{(i)}$. For instance, given $\mathcal{C}(\tau)$ as the type with the binary symbols $+$ and $\circ$, the unary symbol $-$ and the nullary symbol 0, and given a near-ring $\mathbf{N}$ of this type, we say that $\mathbf{N}$ is a ring iff $x_1 + x_2 = x_2 + x_1$ and $x_1 \circ (x_2 + x_3) = x_1 \circ x_2 + x_1 \circ x_3$ are both identites of $\mathbf{N}$.

Definition 3.31. Let t be a term. Then for $l \in \{1, 2, \ldots, k\}$ we define $Occ(l, t)$ as the number of occurrences of x_l in the term t. For any terms $t^{(1)}, t^{(2)}$ we define the *complexity* C of the equation $t^{(1)} = t^{(2)}$ by $C\big(t^{(1)} = t^{(2)}\big) := \max\{Occ(l, t^{(1)}) + Occ(l, t^{(2)}) \,|\, l = 1, 2, \ldots, k\}$.

So $C(t^{(1)} = t^{(2)}) \leq n$ means that no variable occurs more then n times in the equation. As an example, $C(x_1 \circ (x_2 + x_3) = x_1 \circ x_2 + x_1 \circ x_3) = 3$.

Proposition 3.32 ([**Aic94**], [**Aic95**]). *Let* $\mathbf{A}$ *be an algebra, let* $\mathbf{F} \leq \mathbf{M}(\mathbf{A})$*, and let* $t^{(1)}, t^{(2)}$ *be terms such that* $t^{(1)} = t^{(2)}$ *is an identity of* F*. Let* $c := C(t^{(1)} = t^{(2)})$*. Then* $t^{(1)} = t^{(2)}$ *is an identity of* $\mathbf{L}_n\mathbf{F}$ *for all cardinals* n *with* $n \geq c$*.*

Proof: Let $t^{(1)} = t^{(2)}$ be an equation that is not an identity in $\mathbf{L}_n\mathbf{F}$. Hence there are $l_1, l_2, \ldots, l_k \in \mathsf{L}_nF$ such that

$$t^{(1)}_{\mathbf{L}_n\mathbf{F}}(l_1, l_2, \ldots, l_k) \neq t^{(2)}_{\mathbf{L}_n\mathbf{F}}(l_1, l_2, \ldots, l_k). \tag{2.1}$$

Both sides of (2.1) are elements of L_nF, hence functions on A. Thus we have $a \in A$ with

$$t^{(1)}_{\mathbf{L}_n\mathbf{F}}(l_1, l_2, \ldots, l_k)\,(a) \neq t^{(2)}_{\mathbf{L}_n\mathbf{F}}(l_1, l_2, \ldots, l_k)\,(a).$$

If we actually want to compute $t^{(1)}_{\mathbf{L}_n\mathbf{F}}(l_1, l_2, \ldots, l_k)(a)$ and $t^{(2)}_{\mathbf{L}_n\mathbf{F}}(l_1, l_2, \ldots, l_k)(a)$, then each l_j gets evaluated at at most c places. Since l_j lies in L_nF, and since $c \leq n$, we can find an f_j in F that is equal to l_j at these c places. Hence

$$t^{(i)}_{\mathbf{L}_n\mathbf{F}}(l_1, l_2, \ldots, l_k)\,(a) = t^{(i)}_{\mathbf{L}_n\mathbf{F}}(f_1, f_2, \ldots, f_k)\,(a)$$

for $i = 1, 2$. From this we conclude that $f_1, f_2, \ldots, f_k$ violate the equation $t^{(1)} = t^{(2)}$, which is therefore not an identity of $\mathbf{F}$. □

If $\mathbf{F}$ is in a variety $\mathcal{K}$ of composition algebras that can be described by equations that have all complexity less or equal to n, we may even conclude that $\mathbf{L}_n\mathbf{F}$ is in $\mathcal{K}$.

Taking again $\mathbf{A}$ to be a group and $\mathbf{F}$ to be a sub-near-ring of $\mathbf{M}(\mathbf{A})$ that is a ring, we obtain that $\mathbf{L}_3\mathbf{F}$ is a ring as well. **A ring can therefore never be dense in a non-ring.** Actually, a subalgebra of $\mathbf{M}(\mathbf{A})$ can only be dense in a subalgebra with precisely the same identites.

3. Modules of composition algebras

As in the structure theory of rings, near-rings, and composition rings, we get information about the structure of a $\mathcal{V}$-composition algebra $\mathbf{F}$ by interpreting it as an algebra of functions on an algebra $\mathbf{A}$ in $\mathcal{V}$.

Definition 3.33 (Module operations). Let $\mathbf{A}$ be an algebra of type τ, and let $\mathbf{F}$ be a composition algebra of type $\mathcal{C}(\tau)$. Then the operation

$$* : F \times A \to A$$

is called a *module operation* of $\mathbf{F}$ on $\mathbf{A}$ iff the mapping $\Phi : F \to M(A)$ defined by

$$\begin{array}{rccc} \Phi(f) & : & A & \longrightarrow & A \\ & & a & \longmapsto & f * a \end{array}$$

is a homomorphism from $\mathbf{F}$ to $\mathbf{M}(\mathbf{A})$.

Remarks:

(1) Both algebras $\mathbf{F}$ and $\mathbf{M}(\mathbf{A})$ are of type $\mathcal{C}(\tau)$. Hence we claim that Φ is a homomorphism of algebras of the composition type over τ, and therefore in particular also a homorphism with respect to $\circ$.
(2) The fact that Φ is a homomorphism is equivalent to the following: For all $f_1, f_2 \in F$, $a \in A$, for all $k \in \mathbb{N}_0$, and for all k-ary operation symbols ω of type τ we have:
   (a) $f_1 * (f_2 * a) = (f_1 \circ_{\mathbf{F}} f_2) * a$
   (b) $\omega_{\mathbf{F}}(f_1, f_2, \ldots, f_k) * a = \omega_{\mathbf{A}}\big(f_1(a), f_2(a), \ldots, f_k(a)\big)$.

   For a group $\mathbf{G} = (G;+)$ and a near-ring $\mathbf{F} = (F;+,\circ)$, the operation $* : F \times G \to G$ is a *module operation* if the identities $f_1 * (f_2 * g) = (f_1 \circ f_2) * g$ and $(f_1 + f_2) * g = f_1 * g + f_2 * g$ hold. So, in this context module operations are just N-group operations.

Let us briefly outline where module operations arise in familiar contexts. To this end, we compare module operations to the notion of *N-groups* used in near-ring theory (cf. [**Pil83**, Definition 1.17]), and to the notion of *modules* used in ring theory.

If $\mathbf{A}$ is a group, $\mathbf{F}$ is a near-ring, and $*$ is a module operation of $\mathbf{F}$ on $\mathbf{A}$, then $\mathbf{A}$ can be seen as an $\mathbf{F}$-group. On the other hand, every $\mathbf{F}$-group $\mathbf{A}$ gives rise to a module operation of $\mathbf{F}$ on $\mathbf{A}$.

If $\mathbf{A}$ is an abelian group, $\mathbf{F}$ is a ring, and $*$ is a module operation of $\mathbf{F}$ on $\mathbf{A}$, then $\mathbf{A}$ can be seen as an $\mathbf{F}$-group in the sense of near-ring theory. However, $\mathbf{A}$ does *not* have to be a ring module (in the sense of [**Jac64**][1]). This is shown by the following example: Let $\mathbf{A}$ be the group $\mathbf{Z_2} \times \mathbf{Z_2}$, and let e be the mapping defined by $e(\binom{1}{1}) = \binom{1}{1}$, and $e(\binom{x}{y}) = \binom{0}{0}$ on all other three places. Then $\{0, e\}$ is the universe of a subalgebra $\mathbf{F}$ of $\mathbf{M}(\mathbf{A})$. The operation $f * a := f(a)$ is a module operation of $\mathbf{F}$ on $\mathbf{A}$ and $\mathbf{F}$ is a ring. However, since e is not a linear function on $\mathbf{A}$, $\mathbf{A}$ is not an $\mathbf{F}$-module in the sense of ring theory.

This natural view that sees an $\mathbf{F}$-module $\mathbf{X}$ as a pair of an algebra and a module operation is not practical when we want to examine modules with the tools of universal algebra. For this reason, we shall adopt a different point of view: For each $f \in F$, we shall interprete the operation $x \mapsto f * x$ as a new unary operation on the algebra $\mathbf{X}$. To this end, we first define a type that contains a unary operation symbol for each $f \in F$.

Definition 3.34 (The type of $\mathbf{F}$-Modules). Let $\mathbf{F}$ be a composition algebra over the type τ. Then we define a new type as the type that contains all operation symbols of τ plus the unary operation symbol $S(f)$ for every $f \in F$. We abbreviate this type by $\mathcal{M}(\mathbf{F})$, and call it the module type of $\mathbf{F}$.

In other words, starting from a composition algebra $\mathbf{F}$ over type $\tau = (\mathcal{F}, \sigma)$, the type $\mathcal{M}(\mathbf{F})$ is defined by $\mathcal{M}(\mathbf{F}) = (\mathcal{F}_\mathbf{F}, \sigma_\mathbf{F})$, where $\mathcal{F}_\mathbf{F}$ and $\sigma_\mathbf{F}$ are defined by

$$\mathcal{F}_\mathbf{F} := \mathcal{F} \cup \{S(f) \mid f \in F\},$$

and by $\sigma_\mathbf{F}(\omega) = \sigma(\omega)$ for all $\omega \in \mathcal{F}$, and $\sigma_\mathbf{F}(S(f)) = 1$ for $f \in F$. The abbreviation $S(f)$ can be read as *the operation symbol produced from* f. In order to prevent notational complications we will throughout assume that the original type τ does not contain any of the symbols $S(f)$ with $f \in F$. Given an algebra $\mathbf{X}$ of the module type of $\mathbf{F}$, we sometimes want to forget about the operation of $\mathbf{F}$:

Definition 3.35. Let $\mathbf{F}$ be a composition algebra over the type τ, and let $\mathbf{X}$ be an algebra of the module type $\mathcal{M}(\mathbf{F})$ of $\mathbf{F}$. Then by $\mathbf{X}^+$, we denote the reduct of $\mathbf{X}$ of type τ.

Recall that out of a type τ, we have constructed two new types: Adding the binary operation symbol $\circ$ we have obtained the type $\mathcal{C}(\tau)$, and using an algebra $\mathbf{F}$ of this type, we could define the module type $\mathcal{M}(\mathbf{F})$. Given an algebra $\mathbf{A}$ of either type, the algebra $\mathbf{A}^+$ has been defined to be the reduct of type τ.

[1]Note that Jacobson lets rings operate from the right on their modules; but apart from notation, there is also real difference between the modules used in ring theory and the modules that we are going to consider here, as we shall explain in the sequel.

Hence we have completed the first step in defining $\mathbf{F}$-modules. We have defined the type that these algebras must have.

DEFINITION 3.36. Let $\mathbf{F}$ be a composition algebra over the type τ, and let $\mathbf{X}$ be an algebra of the module type $\mathcal{M}(\mathbf{F})$ of $\mathbf{F}$. We say that $\mathbf{X}$ *is an* $\mathbf{F}$*-module* iff the mapping Φ defined below is a homomorphism from $\mathbf{F}$ to $\mathbf{M}(\mathbf{X}^+)$.

$$\begin{array}{rccc} \Phi & : & F & \longrightarrow & M(X) \\ & & f & \longmapsto & \Phi(f), \end{array}$$

and $\Phi(f)$ is defined as

$$\begin{array}{rccc} \Phi(f) & : & X & \longrightarrow & X \\ & & x & \longmapsto & S(f)_{\mathbf{X}}(x). \end{array}$$

Since this definition is quite technical, it is worth giving some comments:

(1) Since $\mathbf{X}^+$ is an algebra of type τ, the algebra $\mathbf{M}(\mathbf{X}^+)$ a composition algebra over the type τ. Hence the mapping Φ is a homomorphism between algebras of type $\mathcal{C}(\tau)$; in particular, it is a homomorphism also with respect to composition.
(2) The fact that Φ is a homomorphism could be rewritten as follows: For all $f_1, f_2 \in F$, $x \in X$, $k \in \mathbb{N}_0$, and for all k-ary operation symbols of the type τ we have:
   (a)
   $$S(f_1)_{\mathbf{X}}(S(f_2)_{\mathbf{X}}(x)) = S(f_1 \circ_{\mathbf{F}} f_2)_{\mathbf{X}}(x)$$
   (b)
   $$S(\omega_{\mathbf{F}}(f_1, f_2, \ldots, f_k))_{\mathbf{X}}(x) = \omega_{\mathbf{X}}\big(S(f_1)_{\mathbf{X}}(x), S(f_2)_{\mathbf{X}}(x), \ldots, S(f_k)_{\mathbf{X}}(x)\big).$$

An equivalent possibility of introducing $\mathbf{F}$-modules is given by the following proposition:

PROPOSITION 3.37. *Let* $\mathbf{F}$ *be a composition algebra over the type* τ*, and let* $\mathbf{X}$ *be an algebra of type* $\mathcal{M}(\mathbf{F})$*. Then* $\mathbf{X}$ *is an* $\mathbf{F}$*-module iff*

(1) $S(f_1)_{\mathbf{X}}(S(f_2)_{\mathbf{X}}(x)) = S(f_1 \circ_{\mathbf{F}} f_2)_{\mathbf{X}}(x)$.
(2) *For each* $x \in X$*, the mapping* r_x *defined by*

$$\begin{array}{rccc} r_x & : & F & \longrightarrow & X \\ & & f & \longmapsto & S(f)_{\mathbf{X}}(x) \end{array}$$

is a homomorphism from $\mathbf{F}^+$ *to* $\mathbf{X}^+$.

This proposition also settles the question what the distributive law means if we have *nullary* operation symbols in $\mathcal{F}$. If ω is such a nullary operation symbol, and $\mathbf{X}$ is an $\mathbf{F}$-module, we have for all $x \in X$:

$$\omega_{\mathbf{F}}() * x = \omega_{\mathbf{X}}().$$

If we are given a composition algebra over the type τ algebra $\mathbf{A}$ of type τ and a module operation $*$ of $\mathbf{F}$ on $\mathbf{A}$, then we can construct an $\mathbf{F}$-module $\mathbf{X}$ from these ingredients in the following way: $\mathbf{X}$ will be algebra of type $\mathcal{M}(\mathbf{F})$. We take A as universe for $\mathbf{X}$; furthermore, the reduct $\mathbf{X}^+$ of $\mathbf{X}$ to the type τ shall be equal to $\mathbf{A}$. The unary operations $S(f)_{\mathbf{X}}$ are defined by $S(f)_{\mathbf{X}}(a) := f * a$ for all $f \in F, a \in A$. It is immediate to check that $\mathbf{X}$ is an $\mathbf{F}$-module. If $*$ is clear from the context, we abbreviate this module by ${}_{\mathbf{F}}\mathbf{A}$.

On the other hand, every $\mathbf{F}$-module $\mathbf{X}$ gives rise to a module operation of $\mathbf{F}$ on $\mathbf{X}^+$. This module operation can be defined as $f * x := S(f)_{\mathbf{X}}(x)$.

Here are some examples of modules: Let $\mathbf{F}$ be a composition algebra over the type τ. Then we have the following two $\mathbf{F}$-modules:

(1) We take the reduct $\mathbf{F}^+$ with type τ, and define a module operation $*$ of $\mathbf{F}$ on $\mathbf{F}^+$ by
$$f * g := f \circ_{\mathbf{F}} g \text{ for } f, g \in F.$$
We construct an $\mathbf{F}$-module from this operation by the process outlined above. We will usually abbreviate this module by ${}_{\mathbf{F}}\mathbf{F}^+$.
(2) We take $\mathbf{A}$ to be an algebra of type τ with precisely one element, say a. Then we define a module operation by $f * a = a$ for $f \in F, a \in A$.

If $\mathbf{F}$ is a subalgebra of $\mathbf{M}(\mathbf{A})$ for some algebra $\mathbf{A}$, then the operation $* : F \times A \to A$, $f * a := f(a)$ is a module operation. The $\mathbf{F}$-module resulting from this operation will be denoted by ${}_{\mathbf{F}}\mathbf{A}$.

Before we start doing real work with modules, we collect some easy observations.

LEMMA 3.38. *For all n-ary terms of type $\mathcal{M}(\mathbf{F})$, and for all $h_1, h_2, \dots, h_n \in F, x \in X$, we have*
$$t_{\mathbf{F}\mathbf{F}^+}(h_1, h_2, \dots, h_n) * x = t_{\mathbf{X}}(h_1 * x, h_2 * x, \dots, h_n * x).$$

Sketch of the proof: We induct on the depth of t and use the identities
$$f * x = S(f)_{\mathbf{X}}(x)$$
and
$$S(\omega_{\mathbf{F}}(f_1, f_2, \dots, f_k))_{\mathbf{X}}(x) = \omega_{\mathbf{X}}\big(S(f_1)_{\mathbf{X}}(x), S(f_2)_{\mathbf{X}}(x), \dots, S(f_k)_{\mathbf{X}}(x)\big).$$
The latter identity has been stated after Definition 3.36. □

The following method allows to construct sub-$\mathbf{F}$-modules of $\mathbf{X}$.

LEMMA 3.39. *Let $\mathbf{F}$ be a composition algebra, and let $\mathbf{X}$ be an $\mathbf{F}$-module, and let $x \in X$. Then $F * x := \{f * x \mid f \in F\}$ is a subuniverse of the $\mathbf{F}$-module $\mathbf{X}$.*

> For every element g of the $\mathbf{F}$-group $\mathbf{G}$, the set $\{f * g \mid f \in F\}$ is the universe of a sub-$\mathbf{F}$-group of $\mathbf{G}$.

Proof: We have to prove that $F * x := \{f * x \mid f \in F\}$ is a subuniverse of $\mathbf{X}$. To this end, let $f_1, f_2, \ldots, f_k \in F$, and ω a k-ary operation symbol in $\mathcal{F}_{\mathbf{F}}$. Then by Lemma 3.38 we have

$$\omega_{\mathbf{X}}(f_1 * x, f_2 * x, \ldots, f_n * x) = \omega_{\mathbf{F}\mathbf{F}^+}(f_1, f_2, \ldots, f_k) * x.$$

Hence $\omega_{\mathbf{X}}(f_1 * x, f_2 * x, \ldots, f_n * x) \in F * x$. □

We will denote this module also by $\mathbf{F} * x$.

At first glance, it seems that $F * x$ is the universe of the sub-$\mathbf{F}$-module of $\mathbf{X}$ generated by x. This is, however, not true in general, since x itself does not have to be an element of $F * x$.

We still need to refine Definition 3.36 for a reason that we explain in the following example. Let $\mathcal{R}$ be the variety of all rings with identity, and let $\mathbf{D_8}$ be the dihedral group with 8 elements. We let $\mathbf{I}(\mathbf{D_8})$ be the near-ring of all zero-symmetric polynomial functions on the group $\mathbf{D_8}$ (cf. [**Pil83**]). Since $\mathbf{D_8}$ is nilpotent of class 2, we know that $\mathbf{I}(\mathbf{D_8})$ has abelian addition. The operation $* : I(D_8) \times D_8 \to D_8$, $p * d := p(d)$ is a module operation. But the resulting $\mathbf{I}(\mathbf{D_8})$-module does not have an abelian addition. Sometimes we want to claim that this module also has abelian addition. This will be made possible by the following definition.

DEFINITION 3.40. Let $\mathcal{V}$ be a variety of algebras, and let $\mathbf{F}$ be a $\mathcal{V}$-composition algebra. Then an $\mathbf{F}$-module $\mathbf{X}$ is called *an $\mathbf{F}$-module with reduct in $\mathcal{V}$* iff $\mathbf{X}^+ \in \mathcal{V}$.

Let us examine the previous example under this new light. To this end, let $\mathcal{A}$ be the variety of all abelian groups. The ring $\mathbf{I}(\mathbf{D_8})$ is an $\mathcal{A}$-composition algebra. Considering again the module operation $* : I(D_8) \times D_8 \to D_8$, $p * d := p(d)$, the resulting $\mathbf{I}(\mathbf{D_8})$-module is not an $\mathbf{I}(\mathbf{D_8})$-module with reduct in $\mathcal{A}$.

Proposition 3.7 tells that for every variety $\mathcal{V}$, and for every $\mathcal{V}$-composition algebra $\mathbf{F}$, there is an "interesting" $\mathbf{F}$-module with reduct in $\mathcal{V}$. "Interesting" will mean that we can distinguish the elements of $\mathbf{F}$ by their actions on this module.

PROPOSITION 3.41. *Let $\mathbf{F}$ be a $\mathcal{V}$-composition algebra. Then the following classes form varieties of algebras of type $\mathcal{M}(\mathbf{F})$.*

(1) *The class of all $\mathbf{F}$-modules.*
(2) *The class of all $\mathbf{F}$-modules with reduct in $\mathcal{V}$.*

Proof: By the definition of modules in Definition 3.36, we se that $\mathbf{F}$-modules are defined by equational conditions. Hence the class of all $\mathbf{F}$-modules is a variety. The class of all $\mathbf{F}$-modules with reduct in $\mathcal{V}$ is also a variety because it is the intersection of the variety of all $\mathbf{F}$-modules with the variety of those algebras of type $\mathcal{M}(\mathbf{F})$ whose τ-reduct is in $\mathcal{V}$. □

> Starting with a near-ring $(N; +, -, 0, \circ)$, the class of all N-groups is a variety. The class of all N-groups that have abelian addition is a subvariety of this variety.

DEFINITION 3.42. For a given variety $\mathcal{V}$ and a $\mathcal{V}$-composition algebra $\mathbf{F}$, we abbreviate the variety of all $\mathbf{F}$-modules with reduct in $\mathcal{V}$ by $\mathcal{V}_{\mathbf{F}}$.

The subalgebras of an $\mathbf{F}$-module $\mathbf{X}$ are called *sub-$\mathbf{F}$-modules* of $\mathbf{X}$.

We call a module *faithful* if different elements of F behave differently on X:

DEFINITION 3.43. An $\mathbf{F}$-module $\mathbf{X}$ is called *faithful* iff the mapping Φ in Definition 3.36 is injective.

We see that $\mathbf{X}$ is faithful iff for all $f, g \in F$ the implication

$$(\forall x \in X : f * x = g * x) \Rightarrow f = g$$

holds. Referring to the module operation $*$ of $\mathbf{F}$ on $\mathbf{X}^+$ that arises from the module $\mathbf{X}$, we say that $\mathbf{F}$ operates faithfully on $\mathbf{X}^+$ by $*$ iff $\mathbf{X}$ is faithful.

Let us compare the notions "faithful" and "base of equality": If $\mathbf{A}$ is an algebra and $\mathbf{F}$ is a subalgebra of $\mathbf{M}(\mathbf{A})$, then the operation $f * a = f(a)$ is a module operation and gives rise to the module ${}_{\mathbf{F}}\mathbf{A}$. Now we consider a submodule $\mathbf{B}$ of this module ${}_{\mathbf{F}}\mathbf{A}$. Then $\mathbf{B}$ is a faithful $\mathbf{F}$-module if and only if B is a base of equality for $\mathbf{F}$.

> A near-ring $\mathbf{F}$ operates faithfully on a group $\mathbf{G}$ iff $(\forall g \in G : f * g = 0)$ implies $f = 0$.

If a module $\mathbf{X}$ is faithful, every equation that is satisfied in $\mathbf{X}$ is automatically satisfied in ${}_{\mathbf{F}}\mathbf{F}^+$:

PROPOSITION 3.44. *If $\mathbf{X}$ is a faithful $\mathbf{F}$-module, then ${}_{\mathbf{F}}\mathbf{F}^+$ lies in the variety of $\mathbf{F}$-modules generated by $\mathbf{X}$.*

> A near-ring that operates faithfully on an abelian group will also have abelian addition.

Proof: The mapping Φ defined by

$$\begin{array}{rccc} \Phi & : & F & \longrightarrow & M(X) \\ & & f & \longmapsto & \Phi(f) \end{array}$$

with $\Phi(f)(x) := S(f)_{\mathbf{X}}(x)$ is not only a homomorphism from $\mathbf{F}$ into $\mathbf{M}(\mathbf{X}^+)$, but also a homomorphism of $\mathbf{F}$-modules from ${}_{\mathbf{F}}\mathbf{F}^+$ into $\mathbf{X}^X$. If Φ is injective, then ${}_{\mathbf{F}}\mathbf{F}^+$ is isomorphic to a subalgebra of $\mathbf{X}^X$, and hence ${}_{\mathbf{F}}\mathbf{F}^+$ lies in the variety generated by $\mathbf{X}$. □

If a sub-$\mathbf{F}$-module $\mathbf{Y}$ of $\mathbf{X}$ has a universe of the form $F * x$, then every equation that is satisfied in ${}_{\mathbf{F}}\mathbf{F}^+$ is automatically satisfied in $\mathbf{Y}$:

PROPOSITION 3.45. *Let $\mathbf{X}$ be an $\mathbf{F}$-module and let $\mathbf{F} * x$ be the submodule of $\mathbf{X}$ with universe $F * x$. Then $\mathbf{F} * x$ lies in the variety generated by ${}_{\mathbf{F}}\mathbf{F}^+$.*

Proof: The mapping $r_x : F \to X, f \mapsto S(f)_{\mathbf{X}}(x)$ is not only a homomorphism from $\mathbf{F}^+$ to $\mathbf{X}^+$, but also a homomorphism of $\mathbf{F}$-modules from ${}_{\mathbf{F}}\mathbf{F}^+$ into $\mathbf{X}$. Hence

$\mathbf{F} * x$ is a homomorphic image of ${}_{\mathbf{F}}\mathbf{F}^{+}$ and thus lies in the variety generated by ${}_{\mathbf{F}}\mathbf{F}^{+}$. □

> Starting again with the near-ring $\mathbf{I}(\mathbf{D_8})$, we therefore know that all $\mathbf{I}(\mathbf{D_8})$-modules generated by a single element have abelian addition.

Let us now give a method that produces a congruence of the composition algebra $\mathbf{F}$ from a congruence on the $\mathbf{F}$-module $\mathbf{X}$.

PROPOSITION 3.46. *Let $\mathbf{F}$ be a composition algebra and let $\mathbf{X}$ be an $\mathbf{F}$-module. Let $\alpha \in Con\,\mathbf{X}$. Then the relation $\beta \subseteq F \times F$ defined by*

$$(f, g) \in \beta :\Longleftrightarrow \forall x \in X : (f * x, g * x) \in \alpha$$

is a congruence on $\mathbf{F}$.

> If we start with an $\mathbf{F}$-group $\mathbf{G}$, and the congruence α corresponds to the $\mathbf{F}$-ideal I, then the congruence β produced in this proposition corresponds to the Noetherian Quotient $(I : G)_F$.

Proof: We have to prove that β is a congruence relation on $\mathbf{F}$. To this end, we fix $x \in X$ and consider the module homomorphism Φ_x from ${}_{\mathbf{F}}\mathbf{F}^{+}$ to $\mathbf{X}$ defined by

$$\begin{array}{rccc} \Phi_x & : & F & \longrightarrow & X \\ & & f & \longmapsto & (f * x)/\alpha. \end{array}$$

It is easy to see that Φ_x is a module homomorphism. Let k_x be the kernel of Φ_x. We then see that

$$\beta = \bigwedge_{x \in X} k_x.$$

This implies that β is a congruence of the module ${}_{\mathbf{F}}\mathbf{F}^{+}$.

For showing that β is a congruence on the composition algebra $\mathbf{F}$, we still have to show that for all $f_1, f_2, g \in F$ we have

$$(f_1, f_2) \in \beta \Rightarrow (f_1 \circ_{\mathbf{F}} g, f_2 \circ_{\mathbf{F}} g) \in \beta.$$

To this end, we show that for all $x \in X$ we have

$$\big((f_1 \circ_{\mathbf{F}} g) * x, (f_2 \circ_{\mathbf{F}} g) * x\big) \in \alpha.$$

Let $x_1 := g * x$. Then what we have to prove is the following:

$$(f_1 * x_1, f_2 * x_1) \in \alpha. \tag{3.1}$$

Since $(f_1, f_2) \in \beta$, the definition of β implies Condition (3.1). □

Sometimes we can obtain a congruence of an $\mathbf{F}$-module in the following way:

PROPOSITION 3.47. *Let $\mathbf{X}$ be an $\mathbf{F}$-module that is contained in a congruence permutable variety of $\mathbf{F}$-modules, and let $x_1, x_2 \in X$. Furthermore, we assume that for all $c \in X$ there is an $f \in F$ such that*

$$\begin{array}{rcll} f * x_1 & = & c & \text{and} \\ f * x_2 & = & c. & \end{array}$$

Then the set

$$\{(f * x_1, f * x_2) \mid f \in F\}$$

is a congruence on $\mathbf{X}$.

> For an $\mathbf{F}$-group $\mathbf{G}$, the assumptions are fulfilled if every constant mapping on G lies in L_2F. The congruence that we produce on $\mathbf{G}$ then corresponds to the ideal $(0 : x_1)_F * x_2$.

The condition that there is an f with $f * x_1 = f * x_2 = c$ could be understood as follows: Each constant function can be interpolated at $\{x_1, x_2\}$ by a function in F. Let us now give the proof of Proposition 3.47:

Proof: We fix $x_1, x_2 \in X$. Let

$$\varphi := \{(f * x_1, f * x_2) \mid f \in F\}.$$

Since $\mathbf{X}$ lies in a congruence permutable variety, we know from Lemma 1.7 that it is sufficient to show that φ is a reflexive relation that is invariant under the application of binary polynomial functions on $\mathbf{X}$. Reflexivity is immediate: For $c \in C$, take $f \in F$ such that $f * x_1 = f * x_2 = c$. then we have

$$(c, c) = (f * x_1, f * x_2) \in \varphi.$$

For showing that φ is closed under the application of polynomial functions, we let $(f_1 * x_1, f_1 * x_2)$, $(f_2 * x_1, f_2 * x_2) \in \varphi$ and let $p \in \mathsf{P}_2(\mathbf{X})$. We have to show

$$\Big(p\big(f_1 * x_1, f_2 * x_1\big), p\big(f_1 * x_2, f_2 * x_2\big)\Big) \in \varphi. \tag{3.2}$$

Now note that $\mathbf{X}$ is an $\mathbf{F}$-module, hence an algebra of type $\mathcal{M}(\mathbf{F})$. Thus there are elements $d_1, d_2, \ldots, d_m \in X$ and a $m+2$-ary term t of type $\mathcal{M}(\mathbf{F})$ such that for all $x \in X$ we have

$$p(f_1 * x, f_2 * x) = t_{\mathbf{X}}(d_1, d_2, \ldots, d_m, f_1 * x, f_2 * x).$$

Now we choose $g_1, g_2, \ldots, g_m \in F$ such that we have

$$g_i * x_1 = g_i * x_2 = d_i \text{ for } i = 1, 2, \ldots, m.$$

Hence if we take $f := t_{\mathbf{F}}\big(g_1, g_2, \ldots, g_m, f_1, f_2\big)$, we have

$$f * x_i = t_{\mathbf{F}}\big(g_1, g_2, \ldots, g_m, f_1, f_2\big) * x_i.$$

Using the "distributive law" stated in Lemma 3.38, we get for $i = 1, 2$

$$\begin{aligned} p(f_1 * x_i) &= t_{\mathbf{X}}(d_1, d_2, \ldots, d_m, f_1 * x_i, f_2 * x_i) \\ &= t_{\mathbf{X}}(g_1 * x_i, g_2 * x_i, \ldots, g_m * x_i, f_1 * x_i, f_2 * x_i) \\ &= t_{\mathbf{F}}\big(g_1, g_2, \ldots, g_m, f_1, f_2\big) * x_i \\ &= f * x_i. \end{aligned}$$

Therefore, Condition (3.2) can be rewritten as

$$(f * x_1, f * x_2) \in \varphi,$$

which is true by the definition of φ. Hence φ is a congruence relation on $\mathbf{X}$. □

A result that stands at the basis of the theory of composition algebras and their modules is the following density result. It is (again) a result of the type

Interpolation at 2-places ⇒ Interpolation at n-places.

THEOREM 3.48. *Let* $\mathbf{A}$ *be an algebra in a congruence permutable variety, and let* $\mathbf{F}$ *be a subalgebra of* $\mathbf{M}(\mathbf{A})$*. If all sub-*$\mathbf{F}$*-modules of* ${}_{\mathbf{F}}\mathbf{A}$ *are neutral, then* $\mathbf{F}$ *is dense in* $\mathbf{L}_2\mathbf{F}$*.*

Proof: We show $\mathsf{L}_2F \subseteq \mathsf{L}F$. To this end, let $l \in \mathsf{L}_2F$, and let D be a finite subset of A. We prove that there is an $f \in F$ with $f|_D = l|_D$. Our aim is to apply Proposition 2.2. We take $\mathbf{G}$ to be the subalgebra of $({}_{\mathbf{F}}\mathbf{A})^D$ with universe

$$G := \{f|_D \mid f \in F\}.$$

Hence $\mathbf{G}$ is a function algebra from D to ${}_{\mathbf{F}}\mathbf{A}$. By assumption, all subalgebras of ${}_{\mathbf{F}}\mathbf{A}$ are neutral, and ${}_{\mathbf{F}}\mathbf{A}$ lies in a congruence permutable variety. Since l lies in L_2F, l can be interpolated at each subset of D with at most two elements by a function in G. Now Proposition 2.2 tells us that l can be interpolated at the whole set D by a function in G. This means that there is a $g \in G$ with $g = l|_D$. But by the definition of $\mathbf{G}$, we therefore have an $f \in F$ with $f|_D = l|_D$.

Hence $\mathbf{F}$ is really dense in $\mathbf{L}_2\mathbf{F}$. □

4. The structure of composition algebras with constants

We will now single out those elements of a composition algebra $\mathbf{F}$ that behave similar to the constant functions in a composition algebra of functions. The following definition goes back to [**Adl62**, p. 607].

DEFINITION 3.49. Let $\mathbf{F}$ be a composition algebra. Then an $c \in F$ is called a *constantly behaving* element of $\mathbf{F}$ iff

$$\forall x \in F : c \circ_{\mathbf{F}} x = c.$$

If $\mathbf{F}$ is a near-ring, then an element c is constantly behaving iff $c \circ 0 = c$.
Proof: It is obvious that the condition $c \circ 0 = c$ is necessary. Now we assume that $c \circ 0 = c$. Fixing $f \in F$, we get $c \circ f = (c \circ 0) \circ f = c \circ (0 \circ f) = c \circ 0 = c$, and hence c behaves constantly.

We will collect the set of all constantly behaving elements of $\mathbf{F}$ in the set F_C.

PROPOSITION 3.50. *Given a composition algebra* $\mathbf{F}$*, the set* F_C *of all constantly behaving elements of* $\mathbf{F}$ *is a subuniverse of the composition algebra* $\mathbf{F}$*.*

This means that for every near-ring $(F; +, \circ)$, the set $\{f \mid f \circ x = f \text{ for all } x \in F\}$ is the universe of a subnear-ring of $(F; +, \circ)$.

Proof: We have to show that F_C is closed under the operations of the composition algebra $\mathbf{F}$. Let ω be first a k-ary fundamental operation of $\mathbf{F}$ that is different

from $\circ_{\mathbf{F}}$. Let k be a natural number, and let $c_1, c_2, \ldots, c_k \in F_C$. We have to show

$$\omega(c_1, c_2, \ldots, c_k) \in F_C \tag{4.1}$$

For that purpose, we fix $x \in F$. Then we have

$$\begin{aligned}\omega(c_1, c_2, \ldots, c_k) \circ_{\mathbf{F}} x &= \omega(c_1 \circ_{\mathbf{F}} x, c_2 \circ_{\mathbf{F}} x, \ldots, c_k \circ_{\mathbf{F}} x)\\ &= \omega(c_1, c_2, \ldots, c_k).\end{aligned}$$

This proves Condition (4.1). It remains to show that F_C is closed under $\circ_{\mathbf{F}}$. For that purpose, let $c_1, c_2 \in F_C$. We fix $x \in F$. Then $c_2 \in F_C$ implies $c_1 \circ_{\mathbf{F}} c_2 \circ_{\mathbf{F}} x = c_1 \circ_{\mathbf{F}} c_2$, which proves $c_1 \circ_{\mathbf{F}} c_2 \in F_C$. □

PROPOSITION 3.51. *Given a composition algebra* $\mathbf{F}$*, the set* F_C *of all constantly behaving elements of* $\mathbf{F}$ *is a subuniverse of the* $\mathbf{F}$*-module* ${}_{\mathbf{F}}\mathbf{F}^+$*.*

> This means that for a near-ring $(F; +, \circ)$ the set of elements $F_C = \{c \in F \mid c \circ 0 = c\}$ is closed under addition, and also under multplication with elements of F from the left. So, if $c \circ 0 = c$, then $(f \circ c) \circ 0 = f \circ c$ for all $f \in F$.

Proof: From Proposition 3.50 we know that F_C is closed under all operations of $\mathbf{F}^+$. For proving that F_C is closed under the module operation $*$ of $\mathbf{F}$, we fix $f \in F, c \in c$. Let x be an element in F. We then have

$$\begin{aligned}(f * c) \circ_{\mathbf{F}} x &= f \circ_{\mathbf{F}} c \circ_{\mathbf{F}} x\\ &= f \circ_{\mathbf{F}} c\\ &= f * c.\end{aligned}$$

Hence the constantly behaving elements of $\mathbf{F}$ are closed under multiplication from the left with arbitrary elements of F. □

The aim of this section is to give a characterization of some composition algebras with at least two constantly behaving elements. We succeed in giving a description if the "additive structure" $\mathbf{F}^+$ behaves sufficiently group-like. This "sufficently group-like" behaviour is guaranteed if $\mathbf{F}^+$ has a Mal'cev term. What we are actually going to do is to describe the finite simple composition algebras $\mathbf{F}$ for which $\mathbf{F}^+$ (or ${}_{\mathbf{F}}\mathbf{F}^+$) lies in a congruence permutable variety.

So let's consider composition algebras $\mathbf{F}$ where $\mathbf{F}$ and its constantly behaving elements gathered in $\mathbf{C}$ are subject to the following restrictions, which we state here for easier reference.

CONVENTION 3.52. We assume that $\mathbf{F}$ and $\mathbf{C}$ are as follows:

$\mathbf{F}$	...	a composition algebra of type $\mathcal{C}(\tau)$,
C	...	the set of all constantly behaving elements of $\mathbf{F}$, $= \{f \in F \mid \forall x \in F : f \circ_{\mathbf{F}} x = f\}$,
$\mathbf{C}$	...	the sub-$\mathbf{F}$-module of ${}_{\mathbf{F}}\mathbf{F}^+$ with universe C.

Furthermore, we assume that C is not empty; we have to claim this because otherwise the definition of $\mathbf{C}$ goes wrong.

PROPOSITION 3.53. *Let* $\mathbf{F}$ *and* $\mathbf{C}$ *be as in Convention 3.52. If* $\mathbf{C}$ *is faithful, then the* $\mathbf{F}$*-modules* ${}_{\mathbf{F}}\mathbf{F}^{+}$ *and* $\mathbf{C}$ *generate the same variety of algebras of type* $\mathcal{M}(\mathbf{F})$.

Proof: By definition, $\mathbf{C}$ is a subalgebra of ${}_{\mathbf{F}}\mathbf{F}^{+}$. Hence $\mathbf{C}$ is in the variety generated by ${}_{\mathbf{F}}\mathbf{F}^{+}$. On the other hand, the mapping Φ defined by

$$\begin{array}{rccc} \Phi & : & F & \longrightarrow & M(C) \\ & & f & \longmapsto & \Phi(f) \end{array}$$

with

$$\begin{array}{rccc} \Phi(f) & : & C & \longrightarrow & C \\ & & c & \longmapsto & f * c \end{array}$$

is an embedding of the $\mathbf{F}$-module ${}_{\mathbf{F}}\mathbf{F}^{+}$ into the $\mathbf{F}$-module $(\mathbf{M}(\mathbf{C}))^{+} = \mathbf{C}^{C}$. Therefore ${}_{\mathbf{F}}\mathbf{F}^{+}$ lies in the variety generated by $\mathbf{C}$. □

In particular, Proposition 3.53 gives that $\mathbf{C}$ lies in a congruence permutable variety iff ${}_{\mathbf{F}}\mathbf{F}^{+}$ does.

Let us now relate simplicity of the composition algebra $\mathbf{F}$ to the simplicity of the module $\mathbf{C}$.

PROPOSITION 3.54. *Let* $\mathbf{F}$ *and* $\mathbf{C}$ *be as in Convention 3.52. Suppose that* $|C| \geq 2$ *and that* $\mathbf{F}$ *is a simple composition algebra. Then* $\mathbf{C}$ *is a faithful and simple* $\mathbf{F}$*-module.*

Proof: Let us first show that $\mathbf{C}$ is faithful: Let Φ be the homomorphism from $\mathbf{F}$ to $\mathbf{M}(\mathbf{C}^{+})$ that was defined in Definition 3.36. Since $\mathbf{F}$ is simple, every homomorphism is either injective or has a one element range. Let us therefore exclude the second case: Let c_1, c_2 be two different constantly behaving elements of $\mathbf{F}$. Since $c_1 * x = c_1$ for all $x \in F$, the mapping $\Phi(c_1)$ is given by

$$\begin{array}{rccc} \Phi(c_1) & : & C & \longrightarrow & C \\ & & x & \longmapsto & c_1. \end{array}$$

This shows that $\Phi(c_1) \neq \Phi(c_2)$.

For proving that $\mathbf{C}$ is simple, let us suppose that $\mathbf{C}$ has a congruence α with $\mathbf{0_C} \leq \alpha \leq \mathbf{1_C}$. Now we define a relation β on $\mathbf{F}$ by

$$(f, g) \in \beta :\Leftrightarrow \forall c \in C : (f * c, g * c) \in \alpha.$$

By Proposition 3.46, we know that β is a congruence on the composition algebra $\mathbf{F}$. Since $\mathbf{F}$ is simple, β must be either $\mathbf{0_F}$ or $\mathbf{1_F}$. Since $\alpha \neq \mathbf{0_C}$, there are $c_1, c_2 \in C$ with $(c_1, c_2) \in \alpha$ and $c_1 \neq c_2$. Using the definition of β, we find out $(c_1, c_2) \in \beta$. This implies that β cannot be the relation $\mathbf{0_F}$ and therefore we have $\beta = \mathbf{1_F}$. But hence for all $c_1, c_2 \in C$ we have

$$(c_1, c_2) \in \beta.$$

Let c be any element of C. Then the definition of β gives

$$(c_1 * c, c_2 * c) \in \alpha.$$

Using the fact that c_1, c_2 are constantly behaving elements of $\mathbf{F}$, we get

$$(c_1, c_2) \in \alpha.$$

This shows that α is equal to $\mathbf{1_C}$, which contradicts the choice of α. □

If the module ${}_{\mathbf{F}}\mathbf{F}^+$ is abelian and lies in a congruence permutable variety, simplicity of $\mathbf{F}$ means that all elements of $\mathbf{F}$ are behaving constantly.

PROPOSITION 3.55. *Let* $\mathbf{F}$ *and* $\mathbf{C}$ *be as in Convention 3.52. Suppose that* $|C| \geq 2$ *and that* $\mathbf{F}$ *is a simple composition algebra. If* ${}_{\mathbf{F}}\mathbf{F}^+$ *is abelian and lies in a congruence permutable variety, then* $F = C$.

> For a near-ring $\mathbf{F}$, we can interprete this proposition as follows: The fact that ${}_{\mathbf{F}}\mathbf{F}^+$ is abelian means that $\mathbf{F}$ satisfies the identites $f_1 + f_2 = f_2 + f_1$ and $f_1 \circ (f_2 + f_3) - f_1 \circ f_3 = f_1 \circ f_2 - f_1 \circ 0$. (The set of affine mappings on a vector space is an example of such a near-ring.) If such a near-ring $\mathbf{F}$ has more than one element satisfying $f \circ 0 = f$ (which just means that $\mathbf{F}$ is not a zero-symmetric near-ring), then $\mathbf{F}$ cannot be simple unless all of its elements behave constantly, which means that the near-ring satisfies the identity $x \circ y = x$.

Proof: We will first show that C gives rise to a congruence γ of the $\mathbf{F}$-module ${}_{\mathbf{F}}\mathbf{F}^+$: Let d be a ternary Mal'cev term of type $\mathcal{M}(\mathbf{F})$. Using the idea of H.P. Gumm's characterization of abelian algebras in congruence permutable varieties [**Gum79**], [**Ihr93**, Satz 8.3.4], we take an element $0 \in C$ and define two operations $+$ and $-'$ on F by

$$\begin{aligned} x + y &:= d_{\mathbf{F}\mathbf{F}^+}(x, 0, y) \\ -'y &:= d_{\mathbf{F}\mathbf{F}^+}(0, y, 0). \end{aligned}$$

It is known that $(F; +, -', 0)$ is an abelian group. Let $-$ be the binary operation on this group that maps (f, g) to $f + (-'g)$. Actually, $-$ is given by $f - g = d_{\mathbf{F}\mathbf{F}^+}(f, g, 0)$. Now for all $k \in \mathbb{N}$, $p \in \mathsf{P}_k({}_{\mathbf{F}}\mathbf{F}^+)$, and $x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_k \in F$, we have

$$p(x_1, x_2, \ldots, x_k) - p(y_1, y_2, \ldots, y_k) = p(x_1 - y_1, x_2 - y_2, \ldots, x_k - y_k). \tag{4.2}$$

We define a relation γ on F by

$$(f, g) \in \gamma :\Leftrightarrow f - g \in C.$$

We shall now prove that γ is a congruence relation on ${}_{\mathbf{F}}\mathbf{F}^+$. Since ${}_{\mathbf{F}}\mathbf{F}^+$ is in a congruence permutable variety, it is sufficient to show that γ is a reflexive relation that is invariant under the application of binary polynomial functions on ${}_{\mathbf{F}}\mathbf{F}^+$. For reflexivity, we observe that $f - f = 0$, and 0 was chosen to be in C; hence we have $(f, f) \in \gamma$. For showing that γ is closed under the application of polynomial functions, let (f_1, g_1), $(f_2, g_2) \in \gamma$ and let $p \in \mathsf{P}_2({}_{\mathbf{F}}\mathbf{F}^+)$. We have to show

$$\big(p(f_1, f_2), p(g_1, g_2)\big) \in \gamma,$$

which is equivalent to

$$p(f_1, f_2) - p(g_1, g_2) \in C. \tag{4.3}$$

We notice that there must be $m \in \mathbb{N}_0$ and a $m+2$-ary term t of type $\mathcal{M}(\mathbf{F})$ and elements $h_1, h_2, \ldots, h_m \in F$ such that for all $x_1, x_2 \in F$ we have

$$p(x_1, x_2) = t_{\mathbf{F}\mathbf{F}^+}(h_1, h_2, \ldots, h_m, x_1, x_2).$$

So, Condition (3.2) can be rewritten as

$$t_{\mathbf{F}\mathbf{F}^+}(h_1, h_2, \ldots, h_m, f_1, f_2) - t_{\mathbf{F}\mathbf{F}^+}(h_1, h_2, \ldots, h_m, g_1, g_2) \in C.$$

Using Condition (4.2), this condition becomes

$$t_{\mathbf{F}\mathbf{F}^+}(0, 0, \ldots, 0, f_1 - g_1, f_2 - g_2) \in C. \tag{4.4}$$

We know that 0 and all $f_i - g_i$ are in C. Since $\mathbf{C}$ is a subalgebra of ${}_{\mathbf{F}}\mathbf{F}^+$, it is closed under the application of term functions, which proves Condition (4.4). Therefore γ is a congruence relation on ${}_{\mathbf{F}}\mathbf{F}^+$.

In the next step, we show that ${}_{\mathbf{F}}\mathbf{F}^+$ is also a congruence relation on $\mathbf{F}$: To this end, let $f, g \in F$ with $(f, g) \in \gamma$, and let $h \in F$. We have to show

$$(f \circ_{\mathbf{F}} h - g \circ_{\mathbf{F}} h) \in C.$$

Using the characterization of $-$, this becomes

$$d_{\mathbf{F}\mathbf{F}^+}(f \circ_{\mathbf{F}} h, g \circ_{\mathbf{F}} h, 0) \in C.$$

Since $\circ_{\mathbf{F}}$ is right distributive with respect to all term functions, and since $0 \circ_{\mathbf{F}} h = 0$ because $0 \in C$, this can be rewritten as

$$d_{\mathbf{F}\mathbf{F}^+}(f, g, 0) \circ_{\mathbf{F}} h.$$

This gets

$$(f - g) \circ_{\mathbf{F}} h \in C.$$

But we know that $f - g \in C$, and hence $(f - g) \circ h = f - g \in C$. Altogether, we get that γ is a congruence relation on $\mathbf{F}$. Since $\mathbf{F}$ is simple, and since all elements in C are congruent modulo γ, we have $\gamma = \mathbf{1}_{\mathbf{F}}$. This implies in particular that we have

$$\forall f \in F \,:\, f - 0 \in C.$$

Since $0 \in C$, this gets $f \in C$, and so we have $C = F$. □

In 1995, K. Kaarli ([**Kaa95**]) presented a characterization of finite simple near-rings with constants. Theorem 3.59 shows that his result carries over to all $\mathcal{V}$-composition algebras where $\mathcal{V}$ is congruence permutable. For stating the result, we need the following composition algebras.

Definition 3.56. Let $\mathbf{A}$ be an algebra of type τ, and let ρ be an equivalence relation on A. Then we define

$$M(A, \rho) := \{m : A \to A \,|\, \forall a_1, a_2 \in A : (a_1, a_2) \in \rho \Rightarrow m(a_1) = m(a_2)\}.$$

Proposition 3.57. *$M(A, \rho)$ is a subuniverse of $\mathbf{M}(\mathbf{A})$.*

Proof: Obvious.

DEFINITION 3.58. We let $\mathbf{M}(\mathbf{A}, \rho)$ be the subalgebra of $\mathbf{M}(\mathbf{A})$ with universe $M(A, \rho)$.

THEOREM 3.59. *Let* $\mathbf{F}$ *and* $\mathbf{C}$ *be as in Convention 3.52. We assume* $|C| \geq 2$. *If* $\mathbf{F}$ *is simple and* ${}_{\mathbf{F}}\mathbf{F}^{+}$ *lies in a congruence permutable variety, then there is a subalgebra* $\mathbf{F}'$ *of* $\mathbf{M}(\mathbf{C}^{+})$ *with the following properties:*

(1) $\mathbf{F}'$ *is isomorphic to* $\mathbf{F}$.
(2) $\mathbf{F}'$ *is dense in* $\mathbf{M}(\mathbf{C}^{+}, \rho)$, *where* ρ *is the equivalence relation on* C *that is defined by* $(c_1, c_2) \in \rho :\Leftrightarrow \forall f \in F : f \circ_{\mathbf{F}} c_1 = f \circ_{\mathbf{F}} c_2$.
(3) *If* $\alpha \in Con\,\mathbf{C}^{+}$ *and* $\alpha \subseteq \rho$, *then* $\alpha \in \{\mathbf{0}_{\mathbf{C}^{+}}, \mathbf{1}_{\mathbf{C}^{+}}\}$.

Let us restate Theorem 3.59 for near-rings. In this special case it reads as follows: Let $\mathbf{F}$ be a simple near-ring that is not zero-symmetric, and let $C := \{c \in F \mid c \circ 0 = c\}$. Then $\mathbf{F}$ is isomorphic to a subnear-ring of the near-ring of all selfmaps on C. This subnear-ring is dense in

$$\{m : C \to C \mid \forall c_1, c_2 \in C : ((\forall f \in F : f \circ c_1 = f \circ c_2) \Rightarrow m(c_1) = m(c_2))\}.$$

Proof: By Proposition 3.54, we know that $\mathbf{C}$ is a faithful and simple $\mathbf{F}$-module. Hence the mapping Φ, which is defined as in Definition 3.36, as

$$\begin{array}{rcccc} \Phi & : & F & \longrightarrow & M(C) \\ & & f & \longmapsto & \Phi(f), \end{array}$$

where

$$\begin{array}{rcccc} \Phi(f) & : & C & \longrightarrow & C \\ & & c & \longmapsto & S(f)_{\mathbf{C}}(c), \end{array}$$

is an embedding of $\mathbf{F}$ into $\mathbf{M}(\mathbf{C}^{+})$. Let $\mathbf{F}' := \Phi(\mathbf{F})$. Obviously, $\mathbf{F}'$ satisfies (1); let us now attack the proof of (2): We have to distinguish two cases as to whether $\mathbf{C}$ is an abelian algebra or not.

Case: $\mathbf{C}$ *is not abelian:* Let us first define an $\mathbf{F}'$-module $\mathbf{C}'$, which will be the "translation" of $\mathbf{C}$ into an $\mathbf{F}'$-module. We let the universe of $\mathbf{C}'$ be C, and define the operations for the operation symbols in $\mathcal{F}$ such that

$$\mathbf{C}'^{+} = \mathbf{C}^{+}.$$

Furthermore, we define a module operation $*$ of $\mathbf{F}'$ on $\mathbf{C}'$ by

$$f' * c := f'(c) \text{ for } f' \in F',\ c \in C.$$

The $\mathbf{F}'$-module $\mathbf{C}'$ that arises from this operation $*$ is again simple and not abelian. For an $f \in F$, the module operation of $\Phi(f)$ is described by the following equation:

$$S(\Phi(f))_{\mathbf{C}'}(c) = \Phi(f)\,(c) = f \circ_{\mathbf{F}} c. \tag{4.5}$$

We will now show that

$$\mathbf{F}' \text{ is dense in } \mathbf{L}_2\mathbf{F}'. \tag{4.6}$$

To this end, we show $\mathsf{L}_2F' \subseteq \mathsf{L}F'$. Let $l \in \mathsf{L}_2F'$, and let D be a finite subset of C. We prove that there is an $f \in F'$ with $f|_D = l|_D$. Our aim is to apply Proposition 2.2. First of all, we observe that $\mathbf{C}'$ has no proper subalgebras: Let

$\mathbf{S}$ be a subalgebra of $\mathbf{C}'$, and let $c \in C, s \in S$. Then Condition (4.5) and the fact that c is a constantly behaving element of $\mathbf{F}$ give

$$\begin{aligned} c &= c \circ_{\mathbf{F}} s \\ &= S(\Phi(c))_{\mathbf{C}'}(s) \end{aligned}$$

and hence $c \in S$. Therefore, all subalgebras of $\mathbf{C}'$ are neutral. Furthermore, by the assumptions and Proposition 3.53, $\mathbf{C}$ lies in a congruence permutable variety. Now let us construct the following function algebra $\mathbf{G}$ from D to $\mathbf{C}'$. We take the universe of $\mathbf{G}$ to be

$$G := \{f|_D \mid f \in F'\}.$$

We have to show that G is the universe of a subalgebra of $(\mathbf{C}')^D$: The mapping $\Psi : F' \to G$ defined by

$$\begin{array}{rccc} \Psi & : & F' & \longrightarrow & G \\ & & f & \longmapsto & f|_D \end{array}$$

is a homomorphism from the $\mathbf{F}'$-module ${}_{\mathbf{F}'}\mathbf{F}'^{+}$ to $(\mathbf{C}')^D$. Therefore $G = \Psi(F')$ is a subuniverse of $(\mathbf{C}')^D$. Since $l \in \mathsf{L}_2 F'$, the function $l|_D$ can be interpolated at every subset of D with no more than two elements by a function $g \in G$. Now we can apply Proposition 2.2 and, using that D is finite, obtain that $l|_D$ is an element of G. Hence there is an element $f \in F'$ with $f|_D = l|_D$. This proves Condition 4.6. Now we prove

$$\mathsf{L}_2 F' = M(C, \rho), \tag{4.7}$$

where $(c_1, c_2) \in \rho \Leftrightarrow \forall f \in F' : f(c_1) = f(c_2)$. For $\subseteq$, let $l \in \mathsf{L}_2 F$ and let $c_1, c_2 \in C$ such that $(c_1, c_2) \in \rho$. Then there is an $f \in F'$ such that $f(c_1) = l(c_1)$ and $f(c_2) = l(c_2)$. Hence $l(c_1) = l(c_2)$. So we have $l \in M(C, \rho)$.

For $\supseteq$, let $m \in M(C, \rho)$, and let $c_1, c_2 \in C$. If $(c_1, c_2) \in \rho$, we know $m(c_1) = m(c_2)$. Hence $\Phi(m(c_1))$ is an element of F' that satisfies $\Phi(m(c_1))(c) = m(c_1) \circ_{\mathbf{F}} c = m(c_1)$ for all $c \in C$. Therefore $\Phi(m(c_1))$ interpolates m at $\{c_1, c_2\}$. If $(c_1, c_2) \notin \rho$, we define the relation φ on C by

$$\varphi := \{(f(c_1), f(c_2)) \mid f \in F'\}.$$

We want to show that φ is a congruence relation on $\mathbf{C}'$. Since $\mathbf{C}'$ lies in a congruence permutable variety, we can apply Proposition 3.47. Let us check whether the assumptions of Proposition 3.47 are fulfilled for $x_1 := c_1, x_2 := c_2$: We have to test whether for each $c \in C$ there is an $f' \in F'$ such that $S(f')_{\mathbf{C}'}(c_1) = S(f')_{\mathbf{C}'}(c_2) = c$. The following calculation shows that $f' := \Phi(c)$ is a suitable solution: We have

$$\begin{aligned} (c, c) &= (c \circ_{\mathbf{F}} c_1, c \circ_{\mathbf{F}} c_2) \\ &= (S(\Phi(c))_{\mathbf{C}'}(c_1), S(\Phi(c))_{\mathbf{C}'}(c_2)) \\ &= (f'(c_1), f'(c_2)). \end{aligned}$$

Therefore Proposition 3.47 yields $\varphi \in Con\,\mathbf{C}'$.

Since $(c_1, c_2) \notin \rho$, there is an element $f \in F'$ with $f(c_1) \neq f(c_2)$. This means that φ cannot be the relation $\mathbf{0}_{\mathbf{C}'}$, and, since $\mathbf{C}'$ is simple, thus has to be equal to $\mathbf{1}_{\mathbf{C}'}$.

But this shows that $\{(f(c_1), f(c_2)) \mid f \in F'\}$ is equal to $C \times C$, and therefore the mapping m can be interpolated at $\{c_1, c_2\}$ by a function in F'. This concludes the proof of $\supseteq$ of Condition (4.7). Hence Condition (4.6) and Condition (4.7) prove claim (2) of Theorem 3.59 in the case where $\mathbf{C}$ is not abelian. Let us now attack the proof of claim (2) in the case that $\mathbf{C}$ is abelian:

Case: $\mathbf{C}$ *is abelian:* Using Proposition 3.53, we notice that ${}_{\mathbf{F}}\mathbf{F}^{+}$ lies in a congruence permutable variety. Furthermore, we observe that $\mathbf{C}$ is abelian. By [**Ihr93**, Aufgabe 8.5.7], we know that the abelian algebras of a congruence permutable variety form a subvariety. Hence the $\mathbf{F}$-module ${}_{\mathbf{F}}\mathbf{F}^{+}$, which lies in the variety generated by $\mathbf{C}$, is abelian. Applying Proposition 3.55 we get $F = C$. The relation ρ on C is therefore equal to $C \times C$, and so $\mathbf{M}(\mathbf{C}^{+}, \rho)$ is the algebra of all constant mappings on C. It is obvious that then $\Phi : F \to M(C)$ with $\Phi(c)(c_1) = c$ for all $c, c_1 \in C$ is an isomorphism between $\mathbf{F}$ and $\mathbf{M}(\mathbf{C}^{+}, \rho)$. This proves claim (2) of Theorem 3.59 in the case where $\mathbf{C}$ is abelian.

Now we have to prove claim (3) of Theorem 3.59. Let α be a congruence on $\mathbf{C}^{+}$ with $\alpha \subseteq \rho$. We show that α is a congruence on $\mathbf{C}$. To this end, let $c_1, c_2 \in \alpha$, and let $f \in F$. We have to show

$$(S(f)_{\mathbf{C}}(c_1), S(f)_{\mathbf{C}}(c_2)) \in \alpha.$$

But $(S(f)_{\mathbf{C}}(c_1), S(f)_{\mathbf{C}}(c_2)) = (f \circ_{\mathbf{F}} c_1, f \circ_{\mathbf{F}} c_2)$. Since $(c_1, c_2) \in \rho$, we have $f \circ_{\mathbf{F}} c_1 = f \circ_{\mathbf{F}} c_2$, and therefore in particular

$$(f \circ_{\mathbf{F}} c_1, f \circ_{\mathbf{F}} c_2) \in \alpha.$$

So α is a congruence on $\mathbf{C}$. By Proposition 3.54, α has to be either $\mathbf{0}_{\mathbf{C}}$ or $\mathbf{1}_{\mathbf{C}}$, which we had to prove. □

For the case of $\mathbf{A}$ being a group, the simplicity of $\mathbf{M}(\mathbf{A}, \rho)$ has been investigated by P. Fuchs. [**Fuc90**]. We give a universal version of one of his results:

PROPOSITION 3.60. *Let $\mathbf{A}$ be an algebra in a congruence permutable variety, and let ρ be an equivalence relation on A such that*

(1) *$\alpha \in Con\,\mathbf{A}$ and $\alpha \subseteq \rho$ implies $\alpha \in \{\mathbf{0}_{\mathbf{A}}, \mathbf{1}_{\mathbf{A}}\}$.*
(2) *There are only finitely many equivalence classes modulo ρ.*

Then one of the following alternatives holds:

(1) *$\mathbf{M}(\mathbf{A}, \rho)$ is simple.*
(2) *$\mathbf{A}$ is abelian and there is a binary polynomial function $+ \in \mathsf{P}_2(\mathbf{A})$ such that $(A; +)$ is the additive group of a vector space over $\mathbf{GF}(2)$ and ρ is the equivalence modulo a subgroup of $(A; +)$ of index 2.*

Special instances of this Proposition are the near-rings $\mathbf{M}_{\mathbf{C}}(\mathbf{Z_2})$ and $\mathbf{M}(\mathbf{Z_2})$. The first near-ring is simple. The near-ring of all mappings on the two element group is not simple, and really, as the Proposition promises, the equivalence relation ρ is the equivalence modulo a subgroup of index 2 of $\mathbf{Z_2}$. This subgroup is trivial.

Proof: Without loss of generality, we assume $|A| \geq 2$. Let $\mathbf{F} := \mathbf{M}(\mathbf{A}, \rho)$ and let ${}_{\mathbf{F}}\mathbf{A}$ be the $\mathbf{F}$-module with universe $\mathbf{A}$ and $\mathbf{F}$ operate on $\mathbf{A}$ in the usual way. First of all, we show

$${}_{\mathbf{F}}\mathbf{A} \text{ is simple.}$$

Let $\alpha \in Con({}_{\mathbf{F}}\mathbf{A})$, $\alpha \neq \mathbf{0}_{{}_{\mathbf{F}}\mathbf{A}}$, $\alpha \neq \mathbf{1}_{{}_{\mathbf{F}}\mathbf{A}}$. The relation α is clearly also a congruence on $\mathbf{A}$, and therefore the assumptions give $\alpha \not\subseteq \rho$. Hence there are $a_1, a_2 \in A$ with $(a_1, a_2) \in \alpha$ and $(a_1, a_2) \notin \rho$. Let b_1, b_2 be arbitrary elements of A. Then there is a mapping $f \in M(A, \rho)$ with $f(a_1) = b_1$ and $f(a_2) = b_2$. But since α is a congruence on ${}_{\mathbf{F}}\mathbf{A}$, this implies $(b_1, b_2) \in \alpha$, and therefore $\alpha = \mathbf{1}_{{}_{\mathbf{F}}\mathbf{A}}$. So, ${}_{\mathbf{F}}\mathbf{A}$ is simple.

Case: ${}_{\mathbf{F}}\mathbf{A}$ *is not abelian:* Let T be a transversal of A modulo ρ. First of all, we observe that the mapping Φ defined by

$$\begin{array}{rccc} \Phi & : & F & \longrightarrow & A^T \\ & & f & \longmapsto & f|_T \end{array}$$

is a homomorphism from the $\mathbf{F}$-module ${}_{\mathbf{F}}\mathbf{F}^+$ to the $\mathbf{F}$-module $({}_{\mathbf{F}}\mathbf{A})^T$. It is easy to see that Φ is bijective. Altogether, we see that Φ is an isomorphism of $\mathbf{F}$-modules.

Now we suppose that α is a congruence of the composition algebra $\mathbf{F}$. Therefore α is also a congruence on ${}_{\mathbf{F}}\mathbf{F}^+$. Hence $\Phi(\alpha) = \{(\Phi(f), \Phi(g)) \,|\, (f, g) \in \alpha\}$ is a congruence on $({}_{\mathbf{F}}\mathbf{A})^T$.

Now we notice that ${}_{\mathbf{F}}\mathbf{A}$ is, as a simple non-abelian algebra, also neutral. Furthermore, by the assumptions, T is finite. Hence Proposition 1.20 yields that $({}_{\mathbf{F}}\mathbf{A})^T$ is skew-free. By the fact that ${}_{\mathbf{F}}\mathbf{A}$ is simple, we obtain that there is a subset U_α of T such that

$$(f, g) \in \Phi(\alpha) \Leftrightarrow f|_{U_\alpha} = g|_{U_\alpha}.$$

If $U_\alpha = T$, then $\Phi(\alpha)$ is the equality relation on $({}_{\mathbf{F}}\mathbf{A})^T$. If $U_\alpha = \varnothing$, then $\Phi(\alpha)$ is the relation $A^T \times A^T = \mathbf{1}_{({}_{\mathbf{F}}\mathbf{A})^T}$. Therefore we can assume

$$\varnothing \subsetneqq U_\alpha \subsetneqq T.$$

Therefore, there we can choose an element an element $t \in T \setminus U_\alpha$. There are functions $l_1, l_2 \in ({}_{\mathbf{F}}\mathbf{A})^T$ such that $l_1(t) \neq l_2(t)$ and $(l_1, l_2) \in \Phi(\alpha)$. Hence there is precisely on extension of l_1 to a mapping $f_1 : A \to A$ such that $f_1 \in F$ and $f_1|_T = l_1$. In the same way we construct f_2 such that $f_2 \in F$ and $f_2|_T = l_2$. We know

$$(f_1, f_2) \in \alpha.$$

Now let g be the constant mapping defined by

$$\begin{array}{rccc} g & : & A & \longrightarrow & A \\ & & a & \longmapsto & t. \end{array}$$

Obviously, $g \in F$. Since α is a congruence on $\mathbf{F}$ we have

$$(f_1 \circ_{\mathbf{F}} g, f_2 \circ_{\mathbf{F}} g) \in \alpha.$$

This implies that

$$(f_1 \circ_{\mathbf{F}} g)|_{U_\alpha} = (f_2 \circ_{\mathbf{F}} g)|_{U_\alpha}.$$

Suppose that U_α is not empty. Then for $u \in U_\alpha$ we have

$$\begin{aligned} f_1 \circ_{\mathbf{F}} g(u) &= f_1(t) \\ &\neq f_2(t) \\ &= f_2 \circ_{\mathbf{F}} g(u). \end{aligned}$$

This is a contradiction, hence the assumption that U_α is not empty was wrong.

Altogether, $\mathbf{F}$ is simple.

Case: $_{\mathbf{F}}\mathbf{A}$ *is abelian:* By H. P. Gumm's characterization of abelian algebras (Proposition 1.13), there are an element $0 \in A$ and a binary operation $+$ in $\mathsf{P}_2(_{\mathbf{F}}\mathbf{A})$ on A such that $(A;+)$ is an abelian group with neutral element 0 and every element $f \in F$ satisfies

$$\forall x, y : f(y+x) - f(x) = f(y) - f(0). \tag{4.8}$$

It is the contents of the following result, Lemma 3.61, that in this case either $\rho = A \times A$ or $(A;+)$ is the additive group of a vector space over $\mathbf{GF}(2)$ and ρ the relation modulo a subspace of codimension 1.

In the case that $\rho = A \times A$, all relations on A are contained in ρ. Hence the assumptions give that the only congruences on $\mathbf{A}$ are $\mathbf{0_A}$ and $\mathbf{1_A}$. So $\mathbf{A}$ is simple. Now we notice that $\mathbf{M}(\mathbf{A},\rho)^+$ is isomorphic to $\mathbf{A}$, and therefore $\mathbf{M}(\mathbf{A},\rho)$ is simple. □

LEMMA 3.61. *Let $(A;+)$ be an abelian group, and let ρ be an equivalence relation on A. Every mapping in $M(A,\rho)$ is affine if and only if one of the following alternatives holds:*

1. $\rho = A \times A$.
2. $(A;+)$ *is the additive group of a vector space over* $\mathbf{GF}(2)$ *and there is a subspace R of A of codimension* 1 *such that $(a_1,a_2) \in \rho$ iff $a_1 - a_2 \in R$.*

Proof: Let us first prove the "only if"-part. If $\rho \neq A \times A$, there is an element $x \in A$ with $x \notin 0/\rho$. If $x+x \in x/\rho$, we have a mapping $f \in M(A,\rho)$ that satisfies $f(0) = 0$, $f(x) = f(x+x) = x$. The linearity condition in Condition (4.8) then gives $x - x = x - 0$ and hence $x = 0$, which contradicts the fact that x is not in $0/\rho$. So, we know that $x + x \notin x/\rho$. Hence for any $z \in A$ there is a mapping $f \in M(A,\rho)$ with $f(0) = f(x+x) = 0$ and $f(x) = z$. The linearity condition in Condition 4.8 now gives $0 - z = z - 0$, which implies that $(A;+)$ is a group of exponent 2. Therefore $(A;+)$ is the additive group of a vector space over the field $\mathbf{GF}(2)$. Now we define $R := 0/\rho$. We first show that R is closed under $+$: Suppose that there are $x, y \in R$ such that $x + y \notin R$. Then the function $f \in M(A,\rho)$ with $f(0) = f(x) = f(y) = 0$ and $f(x+y) = x$ is not affine, which contradicts the assumptions; hence R is closed under $+$. Now we prove

$$\forall a_1, a_2 \in A : (a_1,a_2) \in \rho \Leftrightarrow a_1 - a_2 \in R. \tag{4.9}$$

Let us first establish the following fact:

$$\forall a_1, a_2, t \in A : (a_1,a_2) \in \rho \Leftrightarrow (a_1+t, a_2+t) \in \rho. \tag{4.10}$$

It is sufficient to prove

$$\forall a_1, a_2, t \in A : (a_1, a_2) \in \rho \Rightarrow (a_1 + t, a_2 + t) \in \rho.$$

Suppose that $(a_1, a_2) \in \rho$ and $(a_1 + t, a_2 + t) \notin \rho$. Then either $(a_1, a_1 + t) \notin \rho$ or $(a_2, a_2 + t) \notin \rho$. Without loss of generality we assume $(a_1, a_1 + t) \notin \rho$. Let $a_3 \in A$, $a_3 \neq 0$. Now $f \in M(A, \rho)$ satisfying $f(a_1) = f(a_2) = f(a_2 + t) = 0$ and $f(a_1 + t) = a_3$ is not affine. This proves Condition (4.10) and hence Condition (4.9). Therefore ρ is really the equivalence induced by the subspace R.

Let A/ρ be the factor group of A modulo ρ. For any $f \in M(A, \rho)$, the mapping

$$\begin{array}{rccc} \overline{f} & : & A/\rho & \longrightarrow & A/\rho \\ & & a/\rho & \longmapsto & f(a)/\rho \end{array}$$

is well defined. Since $f \in M(A, \rho)$ is affine, also $\overline{f}$ is affine. It is easy to see that

$$\{\overline{f} \mid f \in M(A, \rho)\} = M(A/\rho)).$$

So we see that every mapping on A/ρ is affine, which implies $|A/\rho| = 2$, and hence R has codimension 1 in A.

For the "if"-part, we asume that alternative (2) occurs. Let f be any mapping from A to A such that A is constant on each of the cosets of R. We may assume $f(0) = 0$. Then let $(a, b_1, b_2, \dots)$ be a basis of A with $a \notin R$, $b_i \in R$ for all i. We define a linear map l by $l(a) := f(a)$ and $l(b_i) = 0$ for all i. We see that $l(a) = 0$, $l(a) = f(a)$ and l is constant on the cosets of R. Hence l is equal to f. But l is clearly affine, and thus so is f. □

Concerning Proposition 3.60, we should like to remark that for an abelian algebra $\mathbf{A}$ and a relation ρ satisfying the second alternative of Proposition 3.60, the composition algebra $\mathbf{M}(\mathbf{A}, \rho)$ is never simple:

PROPOSITION 3.62. *If $\mathbf{A}$ is abelian, lies in a congruence permutable variety, and there is a binary polynomial function $+ \in \mathsf{P}_2(\mathbf{A})$ such that $(A; +)$ is the additive group of a vector space over $\mathbf{GF}(2)$ and ρ is equivalence modulo a subgroup of $(A; +)$ of index 2, then $\mathbf{M}(\mathbf{A}, \rho)$ is not simple.*

> As an example, we consider the subnear-ring of $\mathbf{M}(\mathbf{Z_2} \times \mathbf{Z_2})$ that consists of all functions m that satisfy $m(\binom{a}{b}) - m(\binom{a}{c}) = \binom{0}{0}$ for all $a, b, c \in \mathbb{Z}_2$. Then the resulting near-ring (it contains $4^2 = 16$ elements) is not simple.

Proof: Let $\mathbf{F} := \mathbf{M}(\mathbf{A}, \rho)$ and suppose that $\mathbf{F}$ is a simple composition algebra. Since every mapping in F is affine on $(A; +)$, the algebra ${}_{\mathbf{F}}\mathbf{A}$ is abelian. Hence also ${}_{\mathbf{F}}\mathbf{F}^{+}$, which lies in the variety generated by ${}_{\mathbf{F}}\mathbf{A}$, is abelian. But now Proposition 3.55 implies that every $f \in F$ is a constantly behaving element of $\mathbf{F}$. But it is easy to see that this implies that every element in $M(A, \rho)$ is a constant mapping. This contradicts the fact that there are two classes modulo ρ. □

The following result generalizes [**Adl62**, Theorem 3]. It tells us that those composition algebras of functions on a finite simple non-abelian algebra $\mathbf{A}$ in a congruence permutable variety that contain all constant functions on A are of the form $\mathbf{M}(\mathbf{A}, \rho)$ for some equivalence relation ρ on A.

PROPOSITION 3.63. *Let $\mathbf{A}$ be a finite, simple non-abelian algebra in a congruence permutable variety $\mathcal{V}$. Then the mapping Φ defined by*

$$\begin{array}{rcccl} \Phi & : & \{\rho \,|\, \rho \text{ is equiv. rel. on } A\} & \longrightarrow & \{\mathbf{F} \,|\, \mathbf{M_C}(\mathbf{A}) \leq \mathbf{F} \leq \mathbf{M}(\mathbf{A})\} \\ & & \rho & \longmapsto & \mathbf{M}(\mathbf{A}, \rho) \end{array}$$

is a bijection. □

Obviously $\rho_1 \subset \rho_2$ implies $\mathbf{M}(\mathbf{A}, \rho_1) \supset \mathbf{M}(\mathbf{A}, \rho_2)$.

> There are exactly $P(60)$ different subnear-rings of $\mathbf{M}(\mathbf{A_5})$ that contain all the constant functions on $\mathbf{A_5}$. Here $P(60)$ denotes the number of ways to partition a 60-element set, and $\mathbf{A_5}$ is the alternating group on five letters.

Proof: By the remarks before Definition 3.58, we see that $\Phi(\rho)$ is really a subalgebra of $\mathbf{M}(\mathbf{A})$ for every equivalence ρ on A. It is obvious that Φ is injective. For proving that Φ is surjective, let $\mathbf{F}$ be an arbitrary subalgebra of $\mathbf{M}(\mathbf{A})$ with $\mathbf{M_C}(\mathbf{A}) \leq \mathbf{F}$. We first note that the ${}_{\mathbf{F}}\mathbf{A}$ has only one subalgebra, namely ${}_{\mathbf{F}}\mathbf{A}$ itself. Applying Theorem 3.48, we know that $\mathbf{F}$ is dense in $\mathbf{L}_2\mathbf{F}$, and hence, by the finiteness of A, we have $F = \mathsf{L}_2 F$. But for function algebras that contain all constant functions, Lemma 3.64 gives a characterization of the elements in $\mathsf{L}_2 F$. Since $\mathbf{A}$ is simple, the description of $\mathsf{L}_2 F$ given in Lemma 3.64 becomes particularly easy. Actually, what we obtain is

$$\mathsf{L}_2 F = \{l \in M(A) \,|\, (a_1, a_2) \in \rho(\mathbf{0_A}) \Rightarrow (l(a_1), l(a_2)) \in \mathbf{0_A}\}.$$

Note that there is no reason to study $\rho(\mathbf{1_A})$, because $(l(a_1), l(a_2)) \in \mathbf{1_A}$ is a tautology. If we set $\rho' := \rho(\mathbf{0_A})$, we get

$$\mathsf{L}_2 F = M(A, \rho').$$

This shows that Φ is also surjective. □

LEMMA 3.64. *Let $\mathbf{A}$ be an algebra in a congruence permutable variety and let let $\mathbf{F}$ be such that $\mathbf{M_C}(\mathbf{A}) \leq \mathbf{F} \leq \mathbf{M}(\mathbf{A})$. Then for each congruence $\alpha \in Con\,\mathbf{A}$, we define a relation $\rho(\alpha)$ by*

$$(a_1, a_2) \in \rho(\alpha) :\Leftrightarrow \forall f \in F : (f(a_1), f(a_2)) \in \alpha.$$

Then for all $\alpha \in Con\,\mathbf{A}$ the relation $\rho(\alpha)$ is an equivalence relation and $\mathsf{L}_2 F$ is given by

$$\mathsf{L}_2 F = \{l \in M(A) \,|\, \begin{array}{l} \forall \alpha \in Con\,\mathbf{A}, \forall a_1, a_2 \in A : \\ (a_1, a_2) \in \rho(\alpha) \Rightarrow (l(a_1), l(a_2)) \in \alpha\}. \end{array} \tag{4.11}$$

Proof: It is immediate that $\rho(\alpha)$ is an equivalence relation. For proving the characterization of the elements of $\mathsf{L}_2 F$, we observe that $\subseteq$ of Condition (4.11) is obvious. For $\supseteq$, let l be in the right hand side of Condition (4.11). For showing

that l is in L_2F, let a_1, a_2 be arbitrary elements of of A. If $a_1 = a_2$, the mapping $a \mapsto l(a_1)$ is, as a constant mapping, an element of F and interpolates l at $\{a_1, a_2\} = \{a_1\}$. If $a_1 \neq a_2$, let

$$\alpha := \{(f(a_1), f(a_2)) \mid f \in F\}.$$

Since each constant mapping on A lies in F, Proposition 3.47 yields that α is a congruence on ${}_{\mathbf{F}}\mathbf{A}$, and hence, in particular, on $\mathbf{A}$. By the definition of $\rho(\alpha)$, we have $(a_1, a_2) \in \rho(\alpha)$. Therefore, we have

$$(l(a_1), l(a_2)) \in \alpha.$$

Thus we have an $f \in F$ such that $f(a_1) = l(a_1)$ and $f(a_2) = l(a_2)$. This proves $l \in \mathsf{L}_2F$. □

Let us remark that Proposition 3.63 can be generalized to infinite simple non-abelian algebras $\mathbf{A}$ in congruence permutable varieties: In this case, each function algebra that contains all constant functions on $\mathbf{A}$ is dense in a function algebra of blockwise constant functions.

Proposition 3.63 also shows that for a finite simple non-abelian algebra $\mathbf{A}$, the interval $\{\mathbf{S} \mid \mathbf{M_C}(\mathbf{A}) \leq \mathbf{S} \leq \mathbf{M}(\mathbf{A})\}$ of the subalgebra lattice of $\mathbf{M}(\mathbf{A})$ is anti-isomorphic to the lattice of all equivalence relations on $\mathbf{A}$. Finite fields are examples of simple, non-abelian algebras. For those, we obtain precisely Adler's result that for a finite field $\mathbf{D}$, all sub-composition rings of $\mathbf{M}(\mathbf{D})$ that contain all constant functions on $\mathbf{D}$ are of the form $\mathbf{M}(\mathbf{D}, \rho)$ for some equivalence ρ on $\mathbf{D}$. Furthermore, Proposition 3.60 yields that every such composition ring is simple.

> For the field $\mathbf{GF}(2)$, the composition ring of all mappings $(M(\mathrm{GF}(2)); +, \cdot, \circ)$ is simple. The near-ring $(M(\mathrm{GF}(2)); +, \circ)$, however, is not.

5. The structure of some composition algebras with a left identity

5.1. Zero-symmetric composition algebras. In this paragraph, we investigate composition algebras that have a left identity with respect to composition. The element $e \in F$ is a left identity of the composition algebra $\mathbf{F}$ if we have $e \circ_{\mathbf{F}} f = f$ for all $f \in F$. It is easy to see that a left identity does by no means have to be unique. We say that an $\mathbf{F}$-module $\mathbf{X}$ is *e-unital* iff $e * x = x$ for all $x \in X$.

We will furthermore assume that there is a nullary operation symbol o in $\mathcal{F}$. First of all, we have:

PROPOSITION 3.65. *Let $\mathbf{F}$ be composition algebra over the type $(\mathcal{F}, \sigma)$ and let o be a nullary operation symbol in $\mathcal{F}$. Then we have:*

(1) $\forall f \in F : o_{\mathbf{F}}() \circ_{\mathbf{F}} f = o_{\mathbf{F}}()$.
(2) *For all $f \in F$, the element $f \circ_{\mathbf{F}} o_{\mathbf{F}}()$ is a constantly behaving element of $\mathbf{F}$.*
(3) *For each $\mathbf{F}$-module $\mathbf{X}$ and for all $x \in X$ we have $o_{\mathbf{F}}() * x = o_{\mathbf{X}}()$.*

For a near-ring $(F;+,\circ)$ a left identity e is an element satisfying $e\circ x = x$ for all $x \in F$. If we consider a near-ring as an algebra $(F;+,-,0,\circ)$, then 0 is a nullary operation. And really: As we have asserted in Proposition 3.65, $0\circ x = 0$ holds in $\mathbf{F}$, $f\circ 0$ behaves constantly for every $f \in F$, and if we let $\mathbf{F}$ operate by $*$ as an N-group on a group $\mathbf{G}$, then $0 * g = 0$ for all $g \in G$.

Proof: For (1), we recall from Proposition 3.4 that $x \mapsto x \circ_{\mathbf{F}} f$ is an endomorphism of $\mathbf{F}^+$. This implies that it leaves the result of nullary operations fixed.

Claim (2) follows from (1) by the following calculation: We fix $f, x \in F$ and get

$$\begin{aligned}(f \circ_{\mathbf{F}} o_{\mathbf{F}}()) \circ_{\mathbf{F}} x &= f \circ_{\mathbf{F}} (o_{\mathbf{F}}() \circ_{\mathbf{F}} x)\\ &= f \circ_{\mathbf{F}} o_{\mathbf{F}}().\end{aligned}$$

Hence $f \circ_{\mathbf{F}} o_{\mathbf{F}}()$ is a constantly behaving element of $\mathbf{F}$.

Claim (3) is proved by the remark after Proposition 3.37. □

Since the case that $\mathbf{F}$ has at least two constantly behaving elements has already been treated in the previous section, we shall here restrict ourselves to the case that $\mathbf{F}$ contains precisely one constantly behaving element, namely the element $o_{\mathbf{F}}()$. Note that by Proposition 3.65 the result of a nullary operation is always a constantly behaving element of $\mathbf{F}$. If we want to have only one constantly behaving element, we must also have $f \circ_{\mathbf{F}} o_{\mathbf{F}}() = o_{\mathbf{F}}()$ for all $f \in F$.

This motivates that in the following section we study $\mathcal{V}$-composition algebras $\mathbf{F}$ that are subject to the following restrictions. We list these restrictions here for easier reference.

Convention 3.66.

1. $\mathcal{V}$ is a congruence permutable variety of algebras of type $\tau = (\mathcal{F}, \sigma)$.
2. There is a nullary operation symbol $0 \in \mathcal{F}$.
3. $\mathbf{F}$ is a $\mathcal{V}$-composition algebra.
4. We have an element $e \in F$ with $\forall f \in F : e \circ_{\mathbf{F}} f = f$.
5. For all $f \in F$ we have $f \circ 0_{\mathbf{F}}() = 0_{\mathbf{F}}()$.

A composition algebra that satisfies (5) of Convention 3.66 is called *zero-symmetric*.

So, what we are going to study here are zero-symmetric near-rings with a left identity. But not only those: zero symmetric loop near-rings and zero-symmetric composition rings with identity will be described using the same techniques.

In the sequel, we will abbreviate both $0_{\mathbf{F}}()$ and $0_{\mathbf{X}}()$ – for an $\mathbf{F}$-module $\mathbf{X}$ – simply by 0. Let us assume that $\mathbf{F}$ satisfies all conditions of Convention 3.66. Then in particular $\mathbf{F}$ is a zero-symmetric composition algebra. In this case, we

have

$$f * 0 = 0$$

for every $\mathbf{F}$-module $\mathbf{X}$. So by Lemma 3.39 $\{0\} = F * 0$ is a subuniverse of the module $\mathbf{X}$. This one element sub-$\mathbf{F}$-module of $\mathbf{X}$ is denoted by $\mathbf{0}$.

5.2. Two density results. Let us first give a density result for simple $\mathbf{F}$-modules. This result is an immediate application of [**HH82**, Proposition 3.2].

THEOREM 3.67. *We assume that* $\mathbf{F}$ *is as in Convention 3.66, and* $\mathbf{X}$ *is an* $\mathbf{F}$*-module with reduct in* $\mathcal{V}$ *that satisfies the following properties:*

(1) $\mathbf{X}$ *is faithful*
(2) $\mathbf{X}$ *is e-unital*
(3) *All sub-*$\mathbf{F}$*-modules of* $\mathbf{X}$ *with more than one element are simple and not abelian.*

We define:

(4) $(\mathbf{Y_i})_{i\in I}$ *is the collection of all sub-*$\mathbf{F}$*-modules of* $\mathbf{X}$.
(5) *For* $(i,j) \in I^2$, S_{ij} *is the set of all isomorphisms from* $\mathbf{Y_i}$ *to* $\mathbf{Y_j}$.
(6)

$$\begin{aligned} M_{\bigcup S_{ij}}(X) \;:=\; & \{m : X \to X \,|\, \forall i \in I \,:\, m(Y_i) \subseteq Y_i, \\ & \forall i,j \in I \,\forall \sigma \in S_{ij} \,\forall x \in Y_i \,:\, m(\sigma(x)) = \sigma(m(x))\}. \end{aligned}$$

(7) $\mathbf{M}_{\bigcup S_{ij}}(\mathbf{X}^+)$ *is the subalgebra of* $\mathbf{M}(\mathbf{X}^+)$ *with universe* $M_{\bigcup S_{ij}}(X)$.

Then there is a subalgebra $\mathbf{F}'$ *of* $\mathbf{M}(\mathbf{X}^+)$ *such that* $\mathbf{F}$ *is isomorphic to* $\mathbf{F}'$ *and* $\mathbf{F}'$ *is dense in* $\mathbf{M}_{\bigcup S_{ij}}(\mathbf{X}^+)$.

For near-rings, this result reads as follows:

THEOREM 3.68. *We assume that* $\mathbf{F} = (F; +, \circ)$ *is a zero-symmetric near-ring with left identity, and that* $\mathbf{G}$ *is a faithful unital* $\mathbf{F}$*-group such that* $\mathbf{F}$ *is* 0*-primitive on all sub-*$\mathbf{F}$*-groups of* $\mathbf{G}$. *Furthermore, we assume that for every* $x \in G$ *with* $x \neq 0$ *the structure*

$$(\{f|_{F*x} \,|\, f \in F\}; +, \circ)$$

is not a ring. In other words, this means that for every $x \neq 0$, *there are* f_1, f_2, f_3 *in* F *such that*

$$(f_1 + f_2) * x \neq (f_2 + f_1) * x$$

or

$$(f_1 \circ (f_2 + f_3)) * x \neq (f_1 \circ f_2 + f_1 \circ f_3) * x.$$

Under these assumptions $\mathbf{F}$ *is dense in the near-ring of all mappings on* $\mathbf{G}$ *that preserve all sub-*$\mathbf{F}$*-groups of* $\mathbf{G}$ *and all* $\mathbf{F}$*-isomorphisms between them.*

The precise meaning of "preserve" is to be read in number 6 of the statement of Theorem 3.67.
Our use of the word "preserve" follows the following idea: A near-ring $\mathbf{N}$ of functions on an $\mathbf{F}$-module $\mathbf{X}$ *preserves* a property of $\mathbf{X}$ if the $\mathbf{N}$-module $\mathbf{X}'$ that we obtain by expanding $\mathbf{X}^+$ with the elements of N as unary operations

still satisfies the same property. Some near-ring constructions may be seen as closure operations with respect to module properties: Starting with a near-ring $\mathbf{F}$ operating on the $\mathbf{F}$-group $\mathbf{X}$, the centralizer near-ring of all functions that commute with all $\mathbf{F}$-endomorphisms of $\mathbf{X}$ is the largest near-ring $\mathbf{N}$ such that the $\mathbf{N}$-module $\mathbf{X}'$ has the same endomorphisms as the $\mathbf{F}$-module $\mathbf{X}$. The near-ring of all compatible functions on a group $\mathbf{X}$ may seen as the largest near-ring such that the resulting module has the same congruences as $\mathbf{X}$.
One example of a near-ring that satisfies the assumptions of Theorem 3.68 is the subnear-ring of $\mathbf{M}(\mathbf{Z}_9)$ with universe $\{m : \mathbb{Z}_9 \to \mathbb{Z}_9 \,|\, m(\{0,3,6\}) \subseteq \{0,3,6\}\}$.

Proof: We know that $\mathbf{X}$ is faithful. Hence the mapping Φ, which is defined as in Definition 3.36, as

$$\begin{array}{rcccc} \Phi & : & F & \longrightarrow & M(X) \\ & & f & \longmapsto & \Phi(f), \end{array}$$

where

$$\begin{array}{rcccc} \Phi(f) & : & X & \longrightarrow & X \\ & & x & \longmapsto & S(f)_{\mathbf{X}}(x), \end{array}$$

is an embedding of $\mathbf{F}$ into $\mathbf{M}(\mathbf{X}^+)$. We take $\mathbf{F}' := \Phi(\mathbf{F})$. Obviously, $\mathbf{F}'$ is isomorphic to $\mathbf{F}$. Let us first define an $\mathbf{F}'$-module $\mathbf{X}'$, which is the "translation" of the $\mathbf{F}$-module $\mathbf{X}$ into an $\mathbf{F}'$-module. of the $\mathbf{F}$-module $\mathbf{X}$. We let the universe of $\mathbf{X}'$ be X, and define the operations for the operation symbols in $\mathcal{F}$ such that

$$\mathbf{X}'^{+} = \mathbf{X}^{+}.$$

Furthermore, we define a module operation $*$ of $\mathbf{F}'$ on $\mathbf{X}'$ by

$$f' * x = f'(x) \text{ for } f' \in F', x \in X.$$

The $\mathbf{F}'$-module $\mathbf{X}'$ that arises from this module operation has the same subuniverses, congruences, and the same commutator operation as the $\mathbf{F}$-module $\mathbf{X}$. We will first show that

$$\mathbf{F}' \text{ is dense in } \mathbf{L}_2\mathbf{F}' \tag{5.1}$$

We want to apply Theorem 3.48 for $\mathbf{A} := \mathbf{X}'^{+}$. We see that all sub-$\mathbf{F}'$-modules of $\mathbf{X}$ are neutral, because they either have one element, or they are simple and not abelian. Therefore, Theorem 3.48 yields Equation (5.1).

Now we prove

$$\mathbf{L}_2\mathbf{F}' = \mathbf{M}_{\bigcup S_{ij}}(\mathbf{X}^+). \tag{5.2}$$

For $\subseteq$, we observe that clearly every mapping in L_2F' respects $\mathbf{F}'$-isomorphisms between sub-$\mathbf{F}'$-modules of $\mathbf{X}'$. Furthermore, it also preserves sub-$\mathbf{F}'$-modules.
For $\supseteq$, let $m \in M_{\bigcup S_{ij}}(X)$. We take $x_1, x_2 \in X$ arbitrary but fixed.

Case $x_1 = x_2$: In order to find the function that interpolates m at $\{x_1\}$, it is sufficient to prove

$$\{m(x_1) \,|\, m \in M_{\bigcup S_{ij}}(X)\} \subseteq \{f(x_1) \,|\, f \in F'\}. \tag{5.3}$$

To this end, we observe that $\{f(x_1) \mid f \in F'\}$ is a subuniverse of $\mathbf{X}'$, hence equal to a Y_{i_0} for an $i_0 \in I$. Since $\mathbf{X}$ is e-unital, we have $\Phi(e) * x_1 = x_1$ and therefore $x_1 \in Y_{i_0}$. Now we are ready to prove the subset relation stated in Equation (5.3). By the definition of $M_{\bigcup S_{ij}}(X)$, we know that $m(x_1)$ lies in Y_{i_0}. Therefore, there is an $f \in F'$ with $f(x_1) = m(x_1)$.

Case $x_1 \neq x_2$: Let

$$\begin{aligned} Y_i &:= \{f(x_1) \mid f \in F'\} \\ Y_j &:= \{f(x_2) \mid f \in F'\}. \end{aligned}$$

Now we show that the relation

$$\alpha := \{(f(x_2), g(x_2)) \mid f \in F' \text{ and } f(x_1) = g(x_1)\} \tag{5.4}$$

is a congruence on $\mathbf{Y_j}$. We do so using Lemma 1.7. First of all, we note that α is reflexive: Let y be arbitrary in Y_j. By the definition of Y_j there is an $g \in F'$ such that $g(x_2) = y$. Since (trivially) $g(x_1) = g(x_1)$, we know that $(g(x_2), g(x_2))$ is in α, which means $(y, y) \in \alpha$. Furthermore, α is closed under the application of binary polynomial functions: We let f_1, f_2 and g_1, g_2 be elements in F' such that $f_i(x_1) = g_i(x_1)$ for $i = 1, 2$, and let $p \in \mathsf{P}_2(\mathbf{Y_j})$. We have to show

$$\Big(p\big(f_1(x_2), f_2(x_2)\big), p\big(g_1(x_2), g_2(x_2)\big)\Big) \in \alpha. \tag{5.5}$$

Now note that $\mathbf{Y_j}$ is an $\mathbf{F}$-module, hence an algebra of type $\mathcal{M}(\mathbf{F}) = (\mathcal{F}_\mathbf{F}, \sigma_\mathbf{F})$. Thus there are elements $d_1, d_2, \ldots, d_m \in Y_j$ and a $m+2$-ary term t of type $(\mathcal{F}_\mathbf{F}, \sigma_\mathbf{F})$ such that for all $y_1, y_2 \in Y_j$ we have

$$p(y_1, y_2) = t_{\mathbf{Y_j}}(d_1, d_2, \ldots, d_m, y_1, y_2). \tag{5.6}$$

Now we choose $h_1, h_2, \ldots, h_m \in F'$ such that for all $i = 1, 2, \ldots, m$ we have

$$h_i(x_2) = d_i.$$

Hence if we take $u, v \in F'$ defined by

$$\begin{aligned} u &:= t_\mathbf{F}\big(h_1, h_2, \ldots, h_m, f_1, f_2\big) \\ v &:= t_\mathbf{F}\big(h_1, h_2, \ldots, h_m, g_1, g_2\big). \end{aligned}$$

It is now easy to see that we have $u(x_1) = v(x_1)$. Hence $(u(x_2), v(x_2)) \in \alpha$. But this proves Equation (5.5). Hence the relation α defined in Equation (5.4) is a congruence relation on $\mathbf{X}$.

But since $\mathbf{Y_j}$ is simple, there is not much choice for α. Actually, in both cases we will be able to interpolate the given $m \in M_{\bigcup S_{ij}}(X)$: Note that we know $m(x_1) \in Y_j$ and $m(x_2) \in Y_j$.

Case $\alpha = \mathbf{1}_{Y_j}$: Since $m(x_1) \in Y_i$, there is a function $f_1 \in F'$ such that $f_1(x_1) = m(x_1)$. We know

$$\{(f_2(x_2), f_3(x_2)) \mid f \in F' \text{ and } f_2(x_1) = f_3(x_1)\} = Y_j \times Y_j.$$

Now let $f_2, f_3 \in F'$ be such that

$$\begin{aligned} f_2(x_2) &= f_1(x_2) \\ f_3(x_2) &= m(x_2) \\ f_2(x_1) &= f_3(x_1). \end{aligned}$$

Let d be a ternary term of the type $\mathcal{M}(\mathbf{F}')$ of all $\mathbf{F}'$-modules such that $d_{\mathbf{X}}$ is a Mal'cev function on X. Then we define $f_4 \in F'$ by

$$f_4 := d_{\mathbf{F}'}(f_3, f_2, f_1).$$

We have $f_4(x_1) = d_{\mathbf{X}}(f_3(x_1), f_2(x_1), f_1(x_1)) = f_1(x_1) = m(x_1)$ and $f_4(x_2) = d_{\mathbf{X}}(f_3(x_2), f_2(x_2), f_1(x_2)) = f_3(x_2) = m(x_2)$. Hence f_4 is a function that interpolates m at $\{x_1, x_2\}$.

Case $\alpha = \mathbf{0}_{Y_j}$: In this case we know that $f_1(x_1) = f_2(x_1)$ implies $f_1(x_2) = f_2(x_2)$. This means that the function

$$\begin{array}{rccc} \sigma & : & Y_i & \longrightarrow & Y_j \\ & & f(x_1) & \longmapsto & f(x_2) \end{array}$$

is well defined. It is easy to see that Φ is a homomorphism (of $\mathbf{F}$-modules, obviously) from $\mathbf{Y_i}$ to $\mathbf{Y_j}$. By the definition of $\mathbf{Y_j}$, σ is surjective. Since $\mathbf{Y_i}$ is simple, σ either has a one element range or is injective.

Case σ has a one-element range: In this case, we have $\sigma(Y_i) = \{0\}$. Since Φ is surjective, this means $Y_j = \{0\}$. We also know that $\Phi(e)(x_2) = x_2$, and hence $x_2 \in Y_j$. Thus, we have $x_2 = 0$. Now let $f \in F'$ be any mapping such that $f(x_1) = m(x_1)$. We know that $f(x_2) = f(0) = 0$. Furthermore, $m(0) = 0$, because m preserves all sub-$\mathbf{F}$-modules of $\mathbf{X}$, and $\{0\}$ is a subuniverse of the $\mathbf{F}$-module $\mathbf{X}$. Therefore f interpolates m at $\{x_1, x_2\}$.

Case σ is injective: In this case we have $\sigma \in S_{ij}$. Now let $f \in F'$ be such that $f(x_1) = m(x_1)$. Then we have

$$\begin{aligned} f(x_2) &= \sigma(f(x_1)) \\ &= \sigma(m(x_1)) \\ &= m(\sigma(x_1)) \\ &= m(\sigma(\Phi(e)(x_1))) \\ &= m(\Phi(e)(x_2)) \\ &= m(x_2). \end{aligned}$$

This shows that f interpolates m at $\{x_1, x_2\}$.

Altogether, we have proved Theorem 3.67. □

We will now see what this theorem yields if we have no proper sub-$\mathbf{F}$-modules with more than one element. Before stating this theorem, we need a universal version of centralizer near-rings.

Definition 3.69. Let $\mathbf{A}$ be an algebra of type $(\mathcal{F}, \sigma)$, and let S be a set of endomorphisms on $\mathbf{A}$. Then:

Let

$$M_S(A) := \{m : A \to A \,|\, \forall \sigma \in S \, \forall a \in A \, : \, m(\sigma(a)) = \sigma(m(a))\}.$$

Let $\mathbf{M}_S(\mathbf{A})$ be the subalgebra of $\mathbf{M}(\mathbf{A})$ with universe $M_S(A)$.

THEOREM 3.70. **If $\mathbf{F}$** *is as in Convention 3.66, and* $\mathbf{X}$ *is an* $\mathbf{F}$*-module with reduct in* $\mathcal{V}$ *that satisfies the following properties:*

(1) $\mathbf{X}$ *is faithful*
(2) $\mathbf{X}$ *is e-unital*
(3) $\mathbf{X}$ *has only two sub-*$\mathbf{F}$*-modules, namely* $\mathbf{X}$ *and* $\mathbf{0}$
(4) $\mathbf{X}$ *is simple and not abelian*

and S *is the set of all endomorphisms of* $\mathbf{X}$*. Then we have*

(1) *There is a subalgebra* $\mathbf{F}'$ *of* $\mathbf{M}(\mathbf{X}^+)$ *such that* $\mathbf{F}$ *is isomorphic to* $\mathbf{F}'$ *and* $\mathbf{F}'$ *is dense in* $\mathbf{M}_S(\mathbf{X}^+)$*.*
(2) $S = S^* \cup \{0\}$ *where*
   (a) $0 : X \to X, x \mapsto 0$*,*
   (b) $(S^*; \circ)$ *is a group of automorphisms on* $\mathbf{X}$*.*
   (c) *For all* $\sigma \in S$*:* $\sigma(0) = 0$*,*
   (d) *For all* $\sigma \in S^*$ *and for all* $x \in X$*:* $\sigma(x) = x \Rightarrow x = 0 \vee \sigma = id$*.*

> This is the generalized version of Wielandt-Betsch's Density Theorem for 2-primitive near-rings [**Bet73**]. So this result, having proved already fruitful in near-ring theory, can be used to loop near-rings, composition rings, composition near-rings, ... For composition rings, we milk this result in Chapter 5.

Proof: Number (1) is an immediate consequence of Theorem 3.70. Let us now prove the claims of (2): For proving that $(S^*; \circ)$ is a group of automorphisms on $\mathbf{X}$, we observe that if we have $\sigma \in S^*$, $\sigma(X)$ is the universe of a sub-$\mathbf{F}$-module of $\mathbf{X}$. This holds because the homomorphic image of a subalgebra is always again a subalgebra. Hence σ is surjective. By the simplicity of $\mathbf{X}$, we get that σ is injective. This proves that $(S^*; \circ)$ is a group of automorphisms on $\mathbf{X}$. For proving that $\sigma(0) = 0$, we observe that $\{0\}$ is the only proper subuniverse of $\mathbf{X}$. But since $\sigma(\{0\})$ is again a subuniverse of $\mathbf{X}$, we have $\sigma(0) = 0$. For the "fixed-point-freeness" of S^*, we observe that the set $\{x \,|\, \sigma(x) = x\}$ is the universe of a sub-$\mathbf{F}$-module of $\mathbf{X}$. Hence either σ is the identity function or only 0 gets fixed by σ. □

We call an algebra $\mathbf{A}$ 0-*regular* iff every congruence $\alpha \in Con\,\mathbf{A}$, α is uniquely determined by $0/\alpha$. One can see from [**GU84**, Corollary 1.7] that one condition that garantees that every algebra in a $\mathcal{V}$ is 0-regular is that there are terms $+, -$ of type $(\mathcal{F}, \sigma)$ such that for every algebra $\mathbf{A} \in \mathcal{V}$ the algebra $(A; +_{\mathbf{A}}, -_{\mathbf{A}}, 0_{\mathbf{A}})$ is a group. Hence varieties of Ω-groups are always 0-regular. If $\mathbf{X}$ is 0-regular and has only the two subuniverses $\{0\}$ and X then $\mathbf{X}$ is simple: Suppose that $\alpha \in Con\,\mathbf{X}$. Since $0/\alpha$ is a subuniverse of $\mathbf{X}$, we know that $0/\alpha = \{0\}$ or $0/\alpha = X$. In the

first case 0-regularity gives $\alpha = \mathbf{0_X}$, in the second case we see that all elements of X are congruent to 0 module α and therefore we have $\alpha = \mathbf{1_X}$.

The result in Theorem 3.70 implies that $(S^*; \circ)$ acts as a regular permutation group on $X \setminus \{0\}$. An obvious consequence of this fact is that if X is finite then $|X| - 1$ is divisible by $|S^*|$. If $\mathbf{X}^+$ is a group and $|S^*| > 1$ then the fact that it admits a nontrivial regular group of automorphisms has important consequences on the structure of the group: in that case the group $\mathbf{X}^+$ is nilpotent (by Thompson's Theorem which was originally proved in [**Tho59**]; it can e.g. also be found in [**Rob82**, Theorem 10.5.4]).

DEFINITION 3.71. Let $\mathbf{A}$ be an algebra in a variety $\mathcal{V}$ with the nullary operation $0_\mathbf{A}$. Then an automorphism σ of $\mathbf{A}$ is called *fixed-point-free* iff for all $a \in A$ we have $\sigma(a) = a \Rightarrow a = 0_\mathbf{A}$. A group of automorphisms on $\mathbf{A}$ is called a *regular group of automorphisms* iff all its elements are either fixed-point-free or the identity automorphism.

5.3. Simple composition algebras are dense in centralizer composition algebras. Theorem 3.70 allows us to determine all finite simple $\mathcal{V}$-composition algebras among those satisfying Convention 3.66.

THEOREM 3.72. *Let* $\mathbf{F}$ *be as in Convention 3.66. Furthermore, we suppose that* $\mathbf{F}$ *is finite and simple,* ${}_\mathbf{F}\mathbf{F}^+$ *is not abelian, and* $|F| \geq 2$*. Then there is an algebra* $\mathbf{A} \in \mathcal{V}$ *and a regular group of automorphisms with universe* S^* *on* $\mathbf{A}$ *such that* $\mathbf{F}$ *is isomorphic to* $\mathbf{M}_S(\mathbf{A})$*, where* $S = S^* \cup \{0\}$*.*

Proof: We consider the class $\mathcal{M}$ of all e-unital $\mathbf{F}$-modules. Since ${}_\mathbf{F}\mathbf{F}^+ \in \mathcal{M}$, there is a finite element in $\mathcal{M}$, and therefore there is an element $\mathbf{X} \in \mathcal{M}$ which is minimal among all element $M \in \mathcal{M}$ with $|M| \geq 2$. We set

$$\begin{aligned} \mathbf{A} &:= \mathbf{X}^+ \\ S^* &:= \{\sigma \mid \sigma \text{ is an automorphism of } \mathbf{X}\} \\ S &:= S^* \cup \{0\}. \end{aligned}$$

First of all, we observe that, by the minimality of $|X|$, $\mathbf{X}$ is a simple $\mathbf{F}$-module and the only sub-$\mathbf{F}$-modules of $\mathbf{X}$ have universe $\{0\}$ or X. By the fact that $\mathbf{X}$ is e-unital and $\mathbf{F}$ is simple, it follows that $\mathbf{X}$ is faithful. Hence Proposition 3.44 yields that ${}_\mathbf{F}\mathbf{F}^+$ lies in the variety generated by $\mathbf{X}$. Since the abelian algebras in a congruence permutable variety form a subvariety, this means that $\mathbf{X}$ cannot be abelian: If it were abelian, then so would be ${}_\mathbf{F}\mathbf{F}^+$, which is excluded by the assumptions. Hence all the assumptions of Theorem 3.70 are fulfilled. This theorem now yields that $\mathbf{F}$ is isomorphic to a dense subalgebra of $\mathbf{M}_S(\mathbf{X}^+) = \mathbf{M}_S(\mathbf{A})$. But since A is finite, "density" implies "equality", which proves the result. □

5.4. Finite centralizer composition algebras from regular automorphisms groups are simple. Centralizer composition algebras that arise from

regular groups of automorphisms with finitely many orbits are simple. But before we need the following easy observation about centralizer composition algebras:

PROPOSITION 3.73. *Let* $\mathbf{A}$ *be an algebra in a variety* $\mathcal{V}$ *with the nullary operation* $0_{\mathbf{A}}$*. Let* $\mathbf{S}^*$ *be a regular group of automorphisms on* $\mathbf{A}$ *(as defined in Definition 3.71), and let* $S := S^* \cup \{0\}$*. Let* T *be a transversal through the orbits of* $\mathbf{S}^*$ *on* A^**. Then for every mapping* $l : T \mapsto A$ *there is precisely one mapping* $f \in M_S(A)$ *with* $f|_T = l$*.*

Proof: We define $f(\sigma(t)) := \sigma(l(t))$ for all $t \in T, \sigma \in S$. The fact that $\mathbf{S}^*$ is regular shows that f is well defined. The uniqueness of f follows from the property $f \in M_S(A)$. □

Note that this result also yields $M_S(A) * x = A$ for all $x \neq 0$.

DEFINITION 3.74. Let $\mathcal{V}$ be a variety as in Convention 3.66 (i.e. congruence permutable and with constant operation 0), let $\mathbf{A}$ be a finite algebra in $\mathcal{V}$, and let $\mathbf{S}^*$ be a regular group of automorphisms on $\mathbf{A}$. Then a congruence $\alpha \in Con\,\mathbf{A}$ is $\mathbf{S}^*$*-orbit-contained* iff every congruence class of α is contained in a single $\mathbf{S}^*$-orbit of A.

Note that it is very hard for a congruence α to be $\mathbf{S}^*$-orbit-contained: If α is $\mathbf{S}^*$-orbit contained, then we have automatically $0/\alpha = \{0\}$. In the case that $\mathbf{A}$ is 0-regular, this implies $\alpha = \mathbf{0_A}$.

PROPOSITION 3.75. *Let* $\mathcal{V}$ *be a variety as in Convention 3.66 (i.e. congruence permutable and with constant operation* 0*), let* $\mathbf{A}$ *be a finite algebra in* $\mathcal{V}$*, and let* $\mathbf{S}^*$ *be a regular group of automorphisms on* $\mathbf{A}$ *such that*

(1) $\mathbf{S}^*$ *has only finitely many orbits on* A*.*
(2) *The only* $\mathbf{S}^*$*-orbit-contained congruence relation on* $\mathbf{A}$ *is* $\mathbf{0_A}$*.*

Let $S := S^* \cup \{0\}$*. Then* $\mathbf{M}_S(\mathbf{A})$ *is a simple* $\mathcal{V}$*-composition algebra.*

> For every regular group $\mathbf{S}^*$ of automorphisms on a finite group $\mathbf{G}$, the near-ring $\mathbf{M}_S(\mathbf{G})$ is simple [**MS80**]. S is given by $S^* \cup \{0\}$.

Proof: Let $\mathbf{F} := \mathbf{M}_S(\mathbf{A})$, and let $A^* := A \setminus \{0\}$.

We distinguish two cases:

Case $_{\mathbf{F}}\mathbf{A}$ *is not abelian:*

First of all, we show that the $\mathbf{F}$-module $_{\mathbf{F}}\mathbf{A}$ is simple. Let $\alpha \in Con\,_{\mathbf{F}}\mathbf{A}$, $\alpha \neq \mathbf{0}_{_{\mathbf{F}}\mathbf{A}}$. Since $\alpha \in Con\,\mathbf{A}$, it is not $\mathbf{S}^*$-orbit-contained. Therefore there is a pair $(a_1, a_2) \in \alpha$ such that a_1 and a_2 lie in different orbits of $\mathbf{S}^*$ on A. Now Proposition 3.73 gives that a_1 and a_2 can be sent two any two elements b_1 and b_2 of A via a function in F. This shows that $\alpha = \mathbf{1}_{_{\mathbf{F}}\mathbf{A}}$.

Now we attack the proof of the simplicity of $\mathbf{F}$: We suppose that there is a congruence $\alpha \in Con\mathbf{F}$ with $\alpha \notin \{\mathbf{0_F}, \mathbf{1_F}\}$. Let T be a transversal through the

orbits of $\mathbf{S}^*$ on A^*. Then the mapping Φ defined by

$$\begin{array}{rccc} \Phi & : & F & \longrightarrow & T \\ & & f & \longmapsto & \Phi(f) \end{array}$$

with

$$\begin{array}{rccc} \Phi(f) & : & T & \longrightarrow & A \\ & & t & \longmapsto & f(t) \end{array}$$

is a homomorphism of $\mathbf{F}$-modules from ${}_{\mathbf{F}}\mathbf{F}^+$ to $({}_{\mathbf{F}}\mathbf{A})^T$. By Theorem 3.70 and Proposition 3.73, this mapping Φ is surjective. Since every mapping in F is uniquely determined by its values on T (again by Proposition 3.73), the mapping Φ is also injective. Altogether, we see that Φ is an isomorphism of $\mathbf{F}$-modules. We know that α is a congruence on $\mathbf{F}$, and therefore it is also a congruence on ${}_{\mathbf{F}}\mathbf{F}^+$. Hence $\Phi(\alpha) = \{(\Phi(f), \Phi(g)) \,|\, (f,g) \in \alpha\}$ is a congruence on $({}_{\mathbf{F}}\mathbf{A})^T$.

Now we notice that ${}_{\mathbf{F}}\mathbf{A}$ is, as a simple non-abelian algebra, also neutral. Hence Proposition 1.20 and the fact that T is finite yield that $({}_{\mathbf{F}}\mathbf{A})^T$ is skew-free. By the fact that ${}_{\mathbf{F}}\mathbf{A}$ is simle, we obtain that there is a subset U_α of T such that

$$(f,g) \in \Phi(\alpha) \Leftrightarrow f|_{U_\alpha} = g|_{U_\alpha}.$$

If $U_\alpha = T$, then $\Phi(\alpha)$ is the equality relation on $({}_{\mathbf{F}}\mathbf{A})^T$. If $U_\alpha = \varnothing$, then $\Phi(\alpha)$ is the relation $A^T \times A^T = \mathbf{1}_{({}_{\mathbf{F}}\mathbf{A})^T}$. Therefore we can assume

$$\varnothing \subsetneqq U_\alpha \subsetneqq T.$$

Therefore, there we can choose an element $u \in U_\alpha$ and an element $t \in T \setminus U_\alpha$. There are functions $l_1, l_2 \in ({}_{\mathbf{F}}\mathbf{A})^T$ such that $l_1(t) \neq l_2(t)$ and $(l_1, l_2) \in \Phi(\alpha)$. By Proposition 3.73, there is precisely on extension of l_1 to a mapping $f_1 : A \to A$ such that $f_1 \in M_S(A)$ and $f_1|_T = l_1$. In the same way we construct f_2 such that $f_2 \in M_S(A)$ and $f_2|_T = l_2$. We know

$$(f_1, f_2) \in \alpha.$$

Now let g be a mapping in $M_S(A)$ such that, $g(u) = t$. Since α is a congruence on $\mathbf{F}$ we have

$$(f_1 \circ_{\mathbf{F}} g, f_2 \circ_{\mathbf{F}} g) \in \alpha.$$

This implies that

$$(f_1 \circ_{\mathbf{F}} g)|_{U_\alpha} = (f_2 \circ_{\mathbf{F}} g)|_{U_\alpha}.$$

But we have

$$\begin{array}{rcl} f_1 \circ_{\mathbf{F}} g(u) & = & f_1(t) \\ & \neq & f_2(t) \\ & = & f_2 \circ_{\mathbf{F}} g(u). \end{array}$$

This is a contradiction, hence the assumption that there is $\alpha \notin \{\mathbf{0}_{\mathbf{F}}, \mathbf{1}_{\mathbf{F}}\}$ was wrong. Altogether, $\mathbf{F}$ is simple.

Case ${}_{\mathbf{F}}\mathbf{A}$ *is abelian:* First of all, let d be a Mal'cev term for the variety $\mathcal{V}$. Since ${}_{\mathbf{F}}\mathbf{A}$ is abelian, the algebra $(A; +)$, where $+$ is defined by

$$a_1 + a_2 := d_{\mathbf{A}}(a_1, 0, a_2).$$

is an abelian group. Since ${}_{\mathbf{F}}\mathbf{A}$ is abelian and $f(0) = 0$, we have

$$f(a_1 + a_2) = f(a_1) + f(a_2).$$

Using this last equality and the fact that ${}_{\mathbf{F}}\mathbf{A}$ is faithful, we get that $(F; +, \circ_{\mathbf{F}})$ is a ring. Now the following near-ring theoretic result (Proposition 3.76) yields that $(F; +, \circ_{\mathbf{F}})$ is a division ring, and hence simple. But since $+$ and $\circ_{\mathbf{F}}$ are congruence preserving functions on the composition algebra $\mathbf{F}$, also $\mathbf{F}$ is simple. □

PROPOSITION 3.76. *Let* $\mathbf{G}$ *be a group with* $|G| > 1$*, let* $\mathbf{S}^*$ *be a regular group of group automorphisms on* $\mathbf{G}$ *and let* $S = S^* \cup \{0\}$*. Then the near-ring* $\mathbf{M}_S(\mathbf{G}) = (M_S(G); +, \circ)$ *is a ring iff it is a division ring.*

Proof: The "if"-part is immediate. For the "only if"-part, let $\mathbf{F} := \mathbf{M}_S(\mathbf{G})$. We assume that $\mathbf{F}$ is a ring. Then let D be the set of all endomorphisms of the $\mathbf{F}$-module ${}_{\mathbf{F}}\mathbf{G}$. Then we have $F \subseteq M_D(G)$. On the other hand, since $S \subseteq D$, we have $M_D(G) \subseteq F$. Hence we have

$$M_D(G) = F.$$

Since $\mathbf{F}$ is a ring and $F * g = G$ for all $g \in G \setminus \{0\}$, the group $\mathbf{G}$ is abelian (cf. Proposition 3.45) and every mapping $f \in F$ fulfills

$$f(g_1 + g_2) = f(g_1) + f(g_2) \text{ for all } g_1, g_2 \in g.$$

This also follows from Proposition 3.45.

From these facts, we can infer that the sum of two $\mathbf{F}$-module endomorphisms is again an F-module endomorphism, i.e. for all $s_1, s_2 \in D$, not only $s_1 \circ s_2$, but also $s_1 - s_2$ lies in D.

By the fact that the $\mathbf{F}$-module ${}_{\mathbf{F}}\mathbf{G}$ is simple and has no subuniverses apart from G and $\{0\}$, all mappings in $D \setminus \{0\}$ are invertible, hence $\mathbf{D} := (D; +, \circ)$ is a division ring. We also note that G becomes the universe of a vector space over D if we define $d * g := d(g)$ for all $d \in D$ and for all $g \in G$. We call this vector space ${}_{\mathbf{D}}\mathbf{G}$

Since $\mathbf{M}_D(\mathbf{G})$ is a ring, Theorem 2.2 of [**MvdW91**] yields that the vector space ${}_{\mathbf{D}}\mathbf{G}$ is of dimension at most one.

Now from $|G| > 1$ we get $\dim({}_{\mathbf{D}}\mathbf{G}) = 1$, hence $M_D(G)$ is precisely the set of all vector space endomorphisms of ${}_{\mathbf{D}}\mathbf{G}$. From this we see that $\mathbf{M}_D(\mathbf{G})$ is a division ring. □

The abelian case of Proposition 3.75 also follows from classical near-ring theory (cf. [**Pil83**, Theorem 9.218 (c)], [**MS80**]). Actually, the whole Proposition 3.75 is well-known for near-rings (as is, by the way, most of the material of this chapter).

If $\mathbf{G}$ is finite, then Proposition 3.76 can be proved using [**Pil83**, Theorem 9.218 (b)] and [**Pil83**, Theorem 9.204], which is due to [**MPS81**].

5.5. Another condition that makes a composition algebra simple. We will now give an application of these Propositions: Suppose that $\mathbf{F}$ is a $\mathcal{V}$-composition algebra that satisfies all conditions of Convention 3.66. Furthermore, we suppose that the variety $\mathcal{V}$ is 0-regular. Let us first prove the following easy lemma:

LEMMA 3.77. *Let $\mathbf{F}$ be a $\mathcal{V}$-composition algebra such that all conditions in Convention 3.66 are fulfilled. Furthermore, we suppose that $\mathcal{V}$ is 0-regular. Let $\mathbf{X}$ be an e-unital $\mathbf{F}$-module whose only sub-$\mathbf{F}$-modules are $\mathbf{0}$ and $\mathbf{X}$. Then $\mathbf{X}$ is a simple $\mathbf{F}$-module.*

> The lemma retells the old story that a zero-symmetric near-ring with identity that is 2-primitive on $\mathbf{G}$ is automatically 0-primitive on $\mathbf{G}$.

Proof: We choose $x \neq 0$. (The case $X = \{0\}$ is obvious.) Since $\mathbf{X} = \mathbf{F} * x$, the mapping $r_x : F \to X, f \mapsto f*x$ is surjective. Furthermore, r_x is a homomorphism from $\mathbf{F}^+$ to $\mathbf{X}^+$. Since $\mathbf{F}$ is a $\mathcal{V}$-composition algebra, we know that $\mathbf{F}^+$ lies in $\mathcal{V}$ and therefore its homomorphic image $\mathbf{X}^+$ lies in $\mathcal{V}$. Therefore each congruence on $\mathbf{X}^+$ is uniquely determined by its 0-class. Using this fact, we want to show that $\mathbf{X}$ is simple: Let α be a congruence on $\mathbf{X}$. It is easy to observe that $0/\alpha$ is a sub-$\mathbf{F}$-module of $\mathbf{X}$. If $0/\alpha = \{0\}$, the fact that α is also a congruence on $\mathbf{X}^+$ and the 0-regularity of $\mathbf{X}^+$ yield that $\alpha = \mathbf{0}_{\mathbf{X}^+} = \mathbf{0}_{\mathbf{X}}$. If $x \neq 0$ and $(0, x) \in \alpha$, then the fact $F * x = X$ gives that every element in X is congruent to 0 modulo α. This implies that $\alpha = \mathbf{1}_{\mathbf{X}}$. Therefore $\mathbf{X}$ is simple. □

Now we get the following result.

PROPOSITION 3.78. *Let $\mathbf{F}$ and $\mathcal{V}$ be as in Convention 3.66, and let $\mathbf{X}$ be a finite faithful e-unital $\mathbf{F}$-module that satisfies $F * x = X$ for all $x \neq 0$. We assume that every algebra in $\mathcal{V}$ is 0-regular. Then $\mathbf{F}$ is simple.*

> Every finite 2-primitive, zero-symmetric near-ring with identity is simple. In near-ring theory, one gives the same proof: One shows that it is a centralizer near-ring constructed from a regular group of group automorphisms, and then one shows that such centralizer near-rings are simple (at least, if they are finite).

Proof: From Lemma 3.77, we obtain that $\mathbf{X}$ is simple. If $\mathbf{X}$ is not abelian, Theorem 3.70 forces $\mathbf{F}$ to be a centralizer composition algebra and Proposition 3.75 makes it simple. If $\mathbf{X}$ is abelian, then $(F; +, \circ_{\mathbf{F}})$ with $f_1 + f_2 := d_{\mathbf{F}^+}(f_1, 0, f_2)$ is a primitive ring with left identity, and therefore simple by the blessings of ring theory. □

CHAPTER 4

Tame composition algebras on Ω-groups

In [**Sco95**], Stuart Scott poses six problems. The first and the fourth problem belong to the theory of "tame N-groups". In this section, we give a solution to problem four.

Since the word "tame" seems to appear in many branches of algebra (take, e.g., *tame* congruence theory [**HM88**], the *tame* case in the decomposition of polynomials,...), we will start with a short description of tame near-rings. Again, we will study subalgebras of the composition algebra $\mathbf{M}(\mathbf{A})$ of all functions on an algebra $\mathbf{A}$. However, in order to make our theory work, we need that $\mathbf{A}$ has at least a group structure, and we will therefore only deal with subalgebras of $\mathbf{M}(\mathbf{V})$, where $\mathbf{V}$ is an Ω-group.

1. Tame near-rings

In the following discussion, we need several sets of functions on the Ω-group $\mathbf{V}$. We start from a sub-composition algebra $\mathbf{F}$ of $\mathbf{M}(\mathbf{V})$. From $\mathbf{F}$, we can form the composition algebra of all functions that can be interpolated at any n-element subset of V by a function in F, and we obtain the compostion algebra $\mathbf{L}_n\mathbf{F}$. By $\mathsf{L}_nF + M_C(V)$, we abbreviate the set of those selfmaps s on V that can be written in the form $s = l + c$, where $l \in \mathsf{L}_nF$ and c is a constant mapping on V. What we also need are the unary polynomial functions of the $\mathbf{F}$-module ${}_{\mathbf{F}}\mathbf{V}$, which we denote by $\mathsf{P}_1({}_{\mathbf{F}}\mathbf{V})$. In the following, we will assume that $\mathbf{F}$ fulfils some particular restrictions:

Convention 4.1. We assume that $\mathbf{V}$ is an Ω-group, $\mathbf{F}$ is a sub-composition algebra of $\mathbf{M}(\mathbf{V})$, $\mathbf{F}$ is zero-symmetric, i.e., $f \circ 0 = 0$ for all $f \in F$, and that the identity function on V is in F.

Definition 4.2. Let $\mathbf{V}$ and $\mathbf{F}$ be as in Convention 4.1, and let $n \in \mathbb{N}$. Then $\mathbf{F}$ is *n-tame* iff

$$\mathsf{P}_1({}_{\mathbf{F}}\mathbf{V}) \subseteq \mathsf{L}_nF + M_C(V).$$

What does it mean for a composition algebra $\mathbf{F}$ to be n-tame? Usually, starting with a function $f \in F$ and an element $v \in V$ the function

$$x \mapsto f(v + x) - f(v)$$

does not have to lie in F. As an example of such a composition algebra, we consider a subnear-ring $\mathbf{S}$ of $\mathbf{M}(\mathbf{A}_5)$, where $\mathbf{A}_5 = (A_5; +)$ is the alternating group

of order 60. $\mathbf{S}$ consists of all multiples of the identity function, so S is given by $S = \{z \cdot \mathrm{id} \mid z \in \mathbb{Z}\}$. Suppose that $\mathbf{S}$ were 1-tame: Then for any v and $x \in A_5$ there would be a $z \in \mathbb{Z}$ such that $\mathrm{id}(v+x) - \mathrm{id}(v) = z \cdot x$. This would make every subgroup of A_5 normal, which is not true.

If $\mathbf{F}$ is n-tame, then the function $x \mapsto f(v+x) - f(v)$ can at least by interpolated at every subset of V with at most n elements by a function in F.

The usual definition of tameness is the one suggested by the following lemma:

LEMMA 4.3. *Let $\mathbf{G}$ be a group, and let $\mathbf{F}$ be a zero-symmetric sub-near-ring of $\mathbf{M}(\mathbf{G})$ that contains the identity function on G. Let n be in $\mathbb{N}$. Then $\mathbf{F}$ is n-tame iff for all $g \in G$ and $f \in F$ the function φ defined by*

$$\begin{array}{rccc} \varphi & : & G & \longrightarrow & G \\ & & x & \longmapsto & f(g+x) - f(g) \end{array}$$

lies in $\mathsf{L}_n F$.

Proof: For the "only if"-part, we assume that $\mathbf{F}$ is n-tame. Now we check whether the function $\varphi : G \to G, x \mapsto f(g+x) - f(g)$ lies in $\mathsf{L}_n F$. It is obvious that φ lies in $\mathsf{P}_1({}_{\mathbf{F}}\mathbf{G})$. By the assumption that $\mathbf{F}$ is n-tame, Definiton 4.2 yields that φ can be written as $l + c$, where l is in $\mathsf{L}_n F$, and c is a constant function on G. Now, by the way we have defined φ, we know $\varphi(0) = 0$. This yields:

$$\begin{aligned} 0 &= \varphi(0) \\ &= l(0) + c(0). \end{aligned}$$

Since l lies in $\mathsf{L}_n F$ and $n \geq 1$, the fact that $\mathbf{F}$ is zero-symmetric yields $l(0) = 0$. Hence we get $c(0) = 0$, and therefore we have $\varphi = l$. This implies that φ lies in $\mathsf{L}_n F$, which we had to prove.

For the "if"-part, we have to show that every polynomial function $p \in \mathsf{P}_1({}_{\mathbf{F}}\mathbf{V})$ can be written in the form $l + c$ with $l \in \mathsf{L}_n F$ and $c \in M_C(G)$. We proceed by structural induction on a term representation of p.

If p is a constant function, than p can be written as $0 + p$.

If p is the identity function, we get $p = id_G + 0$, and have again the required representation.

If $p = p_1 + p_2$, we know by induction hypothesis that we can write p as $l_1 + c_1 + l_2 + c_2$ and $l_1, l_2 \in \mathsf{L}_n F$, $c_1, c_2 \in M_C(G)$. We will now show that for each $c \in C$ there is a function $l^c \in \mathsf{L}_n F$ such that

$$\forall x \in G : c + x = l^c(x) + c. \tag{1.1}$$

For proving Equation (1.1), observe that the function φ defined by

$$\begin{array}{rccc} \varphi & : & G & \longrightarrow & G \\ & & x & \longmapsto & c + x - c \end{array}$$

can be written in the form $\varphi(x) = id(c+x) - id(c)$. Hence the assumptions yield $\varphi \in \mathsf{L}_n F$. Now the definition of φ gives $c+x-c = \varphi(x)$, and hence $c+x = \varphi(x)+c$. Thus φ can be taken as the required $l^c \in \mathsf{L}_n F$. This proves Equation (1.1).

Applying Equation (1.1) to the term $l_1 + c_1 + l_2 + c_2$, we see that this is equal to $l_1 + l_3 \circ l_2 + c_1 + c_2$, which implies that $p_1 + p_2$ lies in $\mathsf{L}_n F + M_C(G)$ as well.

If $p(x) = S(f)_{\mathbf{FV}}(p_1)(x)$ for all x, which means $p = f \circ p_1$, we first use the induction hypothesis to write p as $f \circ (l + c)$ with $l \in \mathsf{L}_n F$ and $c \in M_C(G)$. By the assumptions, we know that there is a function $l_4 \in \mathsf{L}_n F$ such that

$$\forall x \in G : -c + x = l_4(x) - c. \tag{1.2}$$

For proving this Equation, we observe that $-c + x + c = id((-c) + x) - id(-c)$, and hence the assumption gives l_4 in the same way as we have produced l^c above. Now we produce a function $l_5 \in \mathsf{L}_n F$ such that

$$\forall x \in G : f(x + c) = l_5(x) + f(c). \tag{1.3}$$

To this end, we write

$$\begin{aligned} f(x + c) &= f(c - c + x + c) \\ &= f(c + l_4(x)). \end{aligned}$$

Since by assumption there is a function $l_6 \in \mathsf{L}_n F$ such that

$$\forall x \in G : f(c + x) = l_6(x) + f(c),$$

we have

$$f(c + l_4(x)) = l_6(l_4(x)) + f(c).$$

Hence the function $l_5 := l_6 \circ l_4$ satisfies Equation (1.3). So we can write $f(l + c)$ as $l_5 \circ l + f(c)$, which gives the required representation of $f(l + c)$ as the sum of as function in $\mathsf{L}_n F$ and a constant function. □

We will now work towards a solution of the fourth problem posed by S.D.Scott in [**Sco95**]. Let us repeat the problem here, using his words. Note that S.D.Scott writes mappings right to their arguments:

> If V is a group and S a non-empty collection of normal subgroups of V, then let $D(S)$ be the subnear-ring of $M_0(V)$, consisting of all maps γ of V into V, such that $(v+U)\gamma \subseteq v\gamma + U$, for all v in V and U in S. If V is a faithful N-group, then define $D(V, N)$ to be $D(S)$, where S is taken as the set of all submodules of V. We have the following theorem (to appear): Suppose V is a faithful 2-tame N-group. If N is ring-free and $N/J(N)$ has DCCR, then N (regarded as a subnear-ring of $M_0(V)$) coincides with $D(V, N)$.
>
> This raises the following question: Can it be shown that without DCCR on $N/J(N)$, N is in fact dense in $D(V, N)$? I

> believe this is probably true but how to proceed is something of a mystery. (S.D.Scott)

We give a simple answer to Scott's question: "Yes". Let us first prove the following theorem. It has been obtained by Scott at least for the case that $\mathbf{V}$ is a finite group.

THEOREM 4.4. *Let $\mathbf{V}$ and $\mathbf{F}$ be as in Convention 4.1, and let $n \geq 2$. Furthermore, we assume that every submodule of ${}_{\mathbf{F}}\mathbf{V}$ is neutral. Then the following are equivalent:*

1. *$\mathbf{F}$ is 2-tame.*
2. *$\mathbf{F}$ is dense in the set of all functions f on V with $f(0) = 0$ that preserve all congruences of the module ${}_{\mathbf{F}}\mathbf{V}$.*
3. *$\mathbf{F}$ is n-tame.*

Proof: (1) $\Rightarrow$ (2): By Theorem 3.48, we obtain that $\mathbf{F}$ is dense in $\mathbf{L}_2\mathbf{F}$. We will now show that the functions L_2F are precisely the zero-preserving compatible functions of the module ${}_{\mathbf{F}}\mathbf{V}$. In this proof, we use the following notation: For a subset M of $M(V)$, we define M_0 by

$$M_0 := \{m \in M \mid m(0) = 0\}.$$

The set of all congruence preserving functions on the module ${}_{\mathbf{F}}\mathbf{V}$ will be denoted by $\mathsf{C}({}_{\mathbf{F}}\mathbf{V})$; formally, this reads as

$$\mathsf{C}({}_{\mathbf{F}}\mathbf{V}) = \{\varphi : V \to V \mid \forall \alpha \in Con\,{}_{\mathbf{F}}\mathbf{V} : (a,b) \in \alpha \Rightarrow (\varphi(a), \varphi(b) \in \alpha\}.$$

What we have to show is

$$\mathsf{L}_2F = (\mathsf{C}({}_{\mathbf{F}}\mathbf{V}))_0. \tag{1.4}$$

Since the right hand side of Equation (1.4) is just the set of all zero-symmetric compatible functions on the module ${}_{\mathbf{F}}\mathbf{V}$, it is equal to $(\mathsf{L}_2\mathsf{P}_1({}_{\mathbf{F}}\mathbf{V}))_0$. So, what we have to show is

$$\mathsf{L}_2F = (\mathsf{L}_2\mathsf{P}_1({}_{\mathbf{F}}\mathbf{V}))_0 \tag{1.5}$$

Since "$\subseteq$" is immediate, we will just prove "$\supseteq$": To this end, we fix $l \in \mathsf{L}_2\mathsf{P}_1({}_{\mathbf{F}}\mathbf{V})$ such that $l(0) = 0$. Since ${}_{\mathbf{F}}\mathbf{V}$ is neutral, we know by Proposition 2.3 (and it will also follow from Proposition 6.9) that $\mathsf{P}_1({}_{\mathbf{F}}\mathbf{V})$ is dense in $\mathsf{L}_2\mathsf{P}_1({}_{\mathbf{F}}\mathbf{V})$. Hence $\mathsf{L}_2\mathsf{P}_1({}_{\mathbf{F}}\mathbf{V}) = \mathsf{L}_3\mathsf{P}_1({}_{\mathbf{F}}\mathbf{V})$, and therefore l lies in $\mathsf{L}_3\mathsf{P}_1({}_{\mathbf{F}}\mathbf{V})$. So, l can be interpolated at every three element subset of V be a polynomial function in $\mathsf{P}_1({}_{\mathbf{F}}\mathbf{V})$.

For proving Equation (1.5), we have to show that l lies in L_2F. To this end, let $x_1, x_2 \in V$ with $x_1, x_2 \neq 0$. First of all, we use the fact that l lies in $\mathsf{L}_3\mathsf{P}_1({}_{\mathbf{F}}\mathbf{V})$ to find a function $p \in \mathsf{P}_1({}_{\mathbf{F}}\mathbf{V})$ with $p(x_1) = l(x_1)$, $p(x_2) = l(x_2)$ and $p(0) = l(0)$. Hence $p(0) = l(0) = 0$. Since $\mathbf{F}$ is 2-tame, we can write p in the form $l_1 + c_1$ with $l_1 \in \mathsf{L}_2F$ and $c_1 \in M_C(V)$. Now we take an $f \in F$ that coincides with l_1 on x_1 and x_2. What we get is

$$p(x_i) = f(x_i) + c_1 \text{ for } i = 1, 2.$$

By the fact that $p(0) = 0$ and $f(0) = 0$, we get $c_1 = 0$, and therefore f interpolates p at x_1 and x_2. Thus, f also interpolates l at x_1 and x_2. This concludes the proof of Equation (1.5).

(2) $\Rightarrow$ (3): We have to show that $\mathsf{P}_1({}_{\mathbf{F}}\mathbf{V})$ is a subset of $\mathsf{L}_nF + M_C(V)$. To this end, let p be a function in $\mathsf{P}_1({}_{\mathbf{F}}\mathbf{V})$. The function $\varphi(x) := p(x) - p(0)$ is zero-reserving and compatible, and hence, by (2), an element of L_2F. Since F is dense in L_2F, we have $\mathsf{L}_nF = \mathsf{L}_2F$, and therefore φ aso lies in L_nF. Thus $p = \varphi + p(0)$ is the required representation of p as a sum of a function in L_nF and a constant function.

(3) $\Rightarrow$ (1): By definition. □

As a consequence, we obtain the solution to Stuart Scott's fourth problem in in [**Sco95**]. Let ${}_{\mathbf{F}}\mathbf{G}$ be an $\mathbf{F}$-group. Then we define $\mathsf{C}_0({}_{\mathbf{F}}\mathbf{G})$ as the set of all unary compatible functions c on ${}_{\mathbf{F}}\mathbf{G}$) that satisfy $c(0) = 0$.

COROLLARY 4.5. *Let $\mathbf{G}$ be a group and let $\mathbf{F}$ be a zero-symmetric sub-near-ring of $\mathbf{M}(\mathbf{G})$. We let ${}_{\mathbf{F}}\mathbf{G}$ be the $\mathbf{F}$-group with universe G and the operation of F on G as expected. We suppose that no homomorphic image of $\mathbf{F}$ with more than one element is a ring. Then $\mathbf{F}$ is 2-tame iff it is dense in the subalgebra of $\mathbf{M}(\mathbf{G})$ with universe $\mathsf{C}_0({}_{\mathbf{F}}\mathbf{G})$.*

Stuart D. Scott has already proved this result for the case that $\mathbf{F}$ is finite, and, more generally, for the case that the lattice of congruences of the $\mathbf{F}$-module ${}_{\mathbf{F}}\mathbf{F}^+$ satisfies the descending chain condition.

Proof: The result follows directly from Theorem 4.4 if we can prove that every submodule of ${}_{\mathbf{F}}\mathbf{G}$ is neutral. To this end, we suppose that the submodule $\mathbf{H}$ of ${}_{\mathbf{F}}\mathbf{G}$ is not neutral. Hence it contains an ideal I such that

$$[I, I]_{\mathbf{H}} < I.$$

We see that I is the universe of a submodule of ${}_{\mathbf{F}}\mathbf{G}$. We will abbreviate this module by $\mathbf{I}$. The commutator $[I, I]_{\mathbf{H}}$ is an ideal of $\mathbf{H}$, and therefore a subuniverse of ${}_{\mathbf{F}}\mathbf{G}$. Since $\mathbf{F}$ is 2-tame, every subuniverse of ${}_{\mathbf{F}}\mathbf{G}$ is an ideal of ${}_{\mathbf{F}}\mathbf{G}$. In particular, $[I, I]_{\mathbf{H}}$ is an ideal of ${}_{\mathbf{F}}\mathbf{G}$. Therefore it is also an ideal of $\mathbf{I}$. For all $i_1, i_2 \in I$ and $f \in F$, we know that both

$$i_1 + i_2 - i_1 - i_2$$

and

$$f * (i_1 + i_2) - f * i_1 - f * i_2$$

lie in $[I, I]_{\mathbf{I}}$, and therefore also in $[I, I]_{\mathbf{H}}$. We let $\mathbf{I}'$ be the $\mathbf{F}$-module defined by

$$\mathbf{I}' := \mathbf{I}/[I, I]_{\mathbf{H}}.$$

We see that $(I'; +)$ is an abelian group and that

$$f * (i'_1 + i'_2) = f * i'_1 + f * i'_2$$

holds for all $f \in F$, $i'_1, i'_2 \in I'$.

Now we consider the mapping Φ defined by

$$\begin{array}{rccc} \Phi & : & F & \longrightarrow & M(I') \\ & & f & \longmapsto & \Phi(f), \end{array}$$

where $\Phi(f)$ is defined by

$$\begin{array}{rccc} \Phi(f) & : & I' & \longrightarrow & I' \\ & & i + [I, I]_{\mathbf{H}} & \longmapsto & f(i) + [I, I]_{\mathbf{H}} \end{array}$$

It is easy to see that Φ is a near-ring homomorphism and that $\Phi(\mathbf{F})$ is a ring. □

However, it would be truly interesting to know the solution of Problem (1) of [**Sco95**]. For example, the author would like to see a near-ring that is 2-tame, but not compatible. We recall that a near-ring of functions on $\mathbf{V}$ is *compatible* if its carrier set is the set of unary polynomial functions for some expansion $\mathbf{W}$ of $\mathbf{V}$.

CHAPTER 5

Composition Rings

In this chapter we first characterize finite, simple, zero-symmetric composition rings $(K; +, \cdot, \circ)$ with an identity with respect to $\circ$ and $K \cdot K \neq \{0\}$. This result has already been published in [**Aic97**]. Then we characterize finite simple non zero-symmetric composition rings.

1. The definition of composition rings

A *composition ring* is an algebra $(K; +, \cdot, \circ)$, where $(K; +, \cdot)$ is a ring, $(K; +, \circ)$ is a near-ring and $(f \cdot g) \circ h = (f \circ h) \cdot (g \circ h)$ for all $f, g, h \in K$. We shall refer to the operation $\cdot$ as *multiplication* and to the operation $\circ$ as *composition*. Composition rings arise from studying functions on rings: Let $(R; +, \cdot)$ be a ring. Then the set $M(R)$ of all selfmaps on R becomes a composition ring if we define $+$ and $\cdot$ pointwise on R and $\circ$ as composition of functions.

Composition rings are also a special instance of the composition algebras studied in Chapter 3. If we start with the variety of rings $\mathcal{R}$, then the $\mathcal{R}$-composition algebras are precisely the composition rings. This allows us to test the results obtained in Chapter 3 for this interesting situation.

Studying simple composition rings, the following construction plays an important role. Let S be a set of ring endomorphisms on the ring R. Then the set

$$M_S(R) := \{m \in M(R) \mid \forall s \in S \ \forall r \in R : m(s(r)) = s(m(r))\}$$

gives rise to a sub-composition ring of $(M(R); +, \cdot, \circ)$. Analogous to the situation of near-rings, we call these composition rings *centralizer composition rings*.

A composition ring $\mathbf{K} = (K; +, \cdot, \circ)$ is called *zero-symmetric* iff $k \circ 0 = 0$ for all $k \in K$.

Similar to the near-ring case, centralizer composition rings help to determine simple composition rings. Before stating the main result, we should like to repeat the definition of regular automorphism groups given in [**Gor80**, p.39]

Definition 5.1. Let $(G; +)$ be a group and let $\mathbf{\Phi}$ be a group of group automorphisms on $(G; +)$. Then $\mathbf{\Phi}$ is *regular* iff for all $\varphi \in \Phi \setminus \{\mathrm{id}_G\}$ and for all $g \in G \setminus \{0\}$ we have $\varphi(g) \neq g$.

We shall use the concept of regularity also for groups of ring automorphisms:

DEFINITION 5.2. Let $(R;+,\cdot)$ be a ring and let $\mathbf{\Psi}$ be a group of ring automorphisms on $(R;+,\cdot)$. Then $\mathbf{\Psi}$ is *regular* iff for all $\psi \in \Psi \setminus \{\mathrm{id}_R\}$ and for all $r \in R \setminus \{0\}$ we have $\psi(r) \neq r$.

2. Simple Zero-Symmetric Composition Rings

Let $\mathbf{K} = (K;+,\cdot,\circ)$ be a composition ring and $(R;+,\cdot)$ be a ring. Then the function $* : K \times R \to R$ is a *module operation* iff it satisfies the identites $k_1 * (k_2 * r) = (k_1 \circ k_2) * r$, $(k_1 + k_2) * r = k_1 * r + k_2 * r$, and $(k_1 \cdot k_2) * r = (k_1 * r) \cdot (k_2 * r)$. If we expand $(R;+,\cdot)$ by all those unary operations, we arrive at a $\mathbf{K}$-module as defined in Definition 3.36. By a $\mathbf{K}$-*ring*, we denote a $\mathbf{K}$-module $\mathbf{M}$ whose reduct $(M;+,\cdot)$ is a ring. In the language of Chapter 3, $\mathbf{K}$-rings are the $\mathbf{K}$-modules with reduct in $\mathcal{R}$, where $\mathcal{R}$ is the variety of all rings.

For rings and $\mathbf{K}$-rings, the notion of being abelian (Definition 1.10) has an unexpected interpretation. A ring $\mathbf{R} \in \mathcal{R}$ is abelian (in the sense of Definition 1.10) iff it has zero multiplication: If $\mathbf{R}$ is abelian, then Proposition 1.29 yields that for all $x_1, x_2, y_1, y_2 \in R$ we have

$$(x_1 + y_1) \cdot (x_2 + y_2) = x_1 \cdot x_2 + y_1 \cdot y_2.$$

Setting $y_2 := 0$, we obtain

$$y_1 \cdot x_2 = 0,$$

which implies that $\mathbf{R}$ has zero multiplication. On the other hand, every ring with zero multiplication is obviously abelian. A $\mathbf{K}$-ring $\mathbf{X}$ is abelian iff $(X;+,\cdot)$ is a zero-ring, and the action of each element of K on X can be written as the sum of a constant map and an endomorphism of $(X;+)$.

In this section, we discuss zero-symmetric composition rings $\mathbf{K}$ that have a left identity with respect to $\circ$, i.e., an element e such that for all $x \in K$ we have $e \circ x = x$. If the composition ring $\mathbf{K}$ has nonzero multiplication and it is faithful on the $\mathbf{K}$-ring $\mathbf{X}$, then the ring $\mathbf{X}^+ = (X;+,\cdot)$ has nonzero multiplication as well (by Proposition 3.44). Hence, for composition rings, Theorem 3.70 can be stated as follows:

THEOREM 5.3. *Let $\mathbf{K}$ be a composition ring with nonzero multiplication that satisfies $k \circ 0 = 0$ for all $k \in K$. Suppose that $\mathbf{K}$ has a left identity element $e \in K$ that satisfies $e \circ k = k$ for all $k \in K$, and that $\mathbf{X}$ is a faithful e-unital $\mathbf{K}$-ring whose only sub-$\mathbf{K}$-rings are $\mathbf{X}$ and $\mathbf{0}$.*

Let S be the set of all endomorphisms of the $\mathbf{K}$-ring $\mathbf{X}$, and let $\mathbf{R}$ be the ring $\mathbf{X}^+ = (X;+,\cdot)$. Then we have:

1. *$S = S^* \cup \{0\}$, where $(S^*;\circ)$ is a regular group of automorphisms on the ring $\mathbf{R}$.*
2. *$\mathbf{K}$ is isomorphic to a sub-composition ring $\mathbf{K}'$ of $\mathbf{M}(\mathbf{R})$ that is dense in $\mathbf{M}_S(\mathbf{R})$.*

In the first proof, we show how this result follows from the result for composition algebras developed in the previous chapters. The second proof is a stand-alone version of this proof. We give it here because we think that it is easier to understand.

Proof I: We observe that the **K**-ring **X** is not abelian because it has nonzero multiplication. It is simple because it contains no honest sub-**K**-rings. Now we can apply Theorem 3.70 and obtain the result. □

Proof II: We recall that $\mathbf{R} = \mathbf{X}^+$, hence R and X denote the same set. For sake of simplicity, we shall assume that **K** is a composition ring of functions on X, i.e., $\mathbf{K} \leq \mathbf{M}(\mathbf{R})$. Furthermore, e is the identity function on X. The proof of part (1) is a precise copy of the corresponding proof in near-ring theory. Let $s \in S^* := S \setminus \{0\}$. Then s is injective because $\{x \in X \mid s(x) = 0\}$ is the universe of a sub-**K**-ring of **X**. It is surjective because $s(X)$ is a subuniverse of **X** as well. Since $e \in S^*$ and the inverse mapping s^{-1} of s is again an **K**-ring endomorphism on R, S^* is really a group. Furthermore, $(S^*; \circ)$ is regular because for any $s \in S$, $\{x \in X \mid s(x) = x\}$ is a sub-**K**-ring of **X**. For part (2), we give a proof similar to the one of [**Aic95**, Theorem 5.1]. First of all, we notice that K is a subset of $M_S(X)$. We have to show that we can interpolate any $m \in M_S(X)$ at each finite subset $T = \{t_1, t_2, \ldots, t_n\}$ of X by a function $k \in K$. Therefore, we fix a $c \in M_S(X)$. Let Y be subset of $T \setminus \{0\}$ that is maximal with the property that it does not contain two elements of the same orbit of the group-operation of S^* on X. It is sufficient to interpolate c on Y, because two mappings in $M_S(X)$ that agree on a point $x \in X$, necessarily agree on $\{s(x) \mid s \in S\}$.

We will now show that we can interpolate *any mapping* $m : Y \to X$ by a function in K. We do so by induction on $|Y|$.

- $Y = \{y_1\}$: Since $K * y_1 = X$, any $k \in K$ with $k(y_1) = m(y_1)$ satisfies the required interpolation property.
- $Y = \{y_1, y_2\}$: First of all, we find a $k_1 \in K$ with $k_1(y_1) = m(y_1)$. It is now sufficient to find an $k_2 \in K$ with $k_2(y_1) = 0$ and $k_2(y_2) = -k_1(y_2) + m(y_2)$, because then $k_1 + k_2$ is the required interpolating function on T. Since

$$V := \{k(y_2) \mid k \in K,\, k(y_1) = 0\}$$

  is a subuniverse of of **X**, we have either $V = X$ or $V = \{0\}$. In the case $V = X$, we immediately get the required mapping k_2. In the case $V = \{0\}$ the mapping $h : X \to X$, $k(y_1) \mapsto k(y_2)$ is a well-defined **K**-ring automorphism on **X** that maps $y_1 = e(y_1)$ to $y_2 = e(y_2)$, which contradicts the fact that Y contains at most one element of each orbit of S^* on X.
- $Y = \{y_1, y_2, \ldots, y_n\}$. Let $n \geq 3$. Without loss of generality we assume $m(y_1) = m(y_2) = \cdots = m(y_{n-1}) = 0$. It is now sufficient to show

$$\{k(y_n) \mid k(y_1) = k(y_2) = \cdots = k(y_{n-1}) = 0\} \neq \{0\}. \tag{2.1}$$

Let $\bar{x}, \bar{y}$ be two elements of X with $\bar{x} \cdot \bar{y} \neq 0$. By induction hypothesis, there exists a mapping $k_1 \in F$ with $k_1(y_1) = k_1(y_2) = \cdots = k_1(y_{n-2}) = 0$ and $k_1(y_n) = \bar{x}$. In the same way, there exists an $k_2 \in K$ with $k_2(y_{n-1}) = 0$ and $k_2(y_n) = \bar{y}$. Then $k_1 \cdot k_2(y_n)$ lies in the left hand side of (2.1), but is not zero. □

Note that Theorem 5.3 is particularly interesting if $\mathbf{X}^+ = (X; +, \cdot)$ has a unit 1 with $x \cdot 1 = 1 \cdot x = x$ for all $x \in X$.

COROLLARY 5.4. *Let* $\mathbf{R}$ *be a ring with unit and let* $\mathbf{K}$ *be a sub-composition ring of*

$$\mathbf{M}_0(\mathbf{R}) = (\{m : R \to R \,|\, m(0) = 0\}; +, \cdot, \circ)$$

such that the $\mathbf{K}$*-ring* ${}_{\mathbf{K}}\mathbf{R}$ *has no subuniverses except* $\{0\}$ *and* R*. We assume that* K *contains the identity function* id_R *on* R*. Then* $\mathbf{K}$ *is dense in* $\mathbf{M}_0(\mathbf{R})$*.*

Under these assumptions, the condition that the $\mathbf{K}$-ring ${}_{\mathbf{K}}\mathbf{R}$ has no subuniverses except for $\{0\}$ and R can be replaced with the condition

$$K * r = R \text{ for all } r \in R \setminus \{0\}.$$

Proof of Corollary 5.4: Since any ring automorphism on $\mathbf{R}$ fixes the unit of $\mathbf{R}$, $\{\mathrm{id}_R\}$ is the only universe of a regular group of ring automorphisms on ${}_{\mathbf{K}}\mathbf{R}$. Now the result follows directly from Theorem 5.3. □

Theorem 5.3 also allows us to determine all finite simple zero-symmetric composition rings with a left identity with respect to composition:

THEOREM 5.5. *Let* $\mathbf{K} = (K; +, \cdot, \circ)$ *be a zero-symmetric composition ring with a left identity* $\mathbf{1}$ *with respect to composition. Furthermore, we assume that the multiplication is not identically zero, i.e.* $K \cdot K \neq \{0\}$*. Then the following two conditions are equivalent:*

(1) $\mathbf{K}$ *is finite and simple.*
(2) *There exists a finite ring* $\mathbf{R}$ *and a regular group* $\mathbf{S}^*$ *of ring automorphisms on* $\mathbf{R}$ *such that* $\mathbf{K}$ *is isomorphic to* $\mathbf{M}_S(\mathbf{R})$*, where* $S = S^* \cup \{0\}$*.*

Proof I: (1) ⇒ (2): Since $\mathbf{K}^+ = (K; +, \cdot)$ is a ring with nonzero multiplication, $\mathbf{K}^+$ is not abelian (in the sense of Definition 1.10), and hence ${}_{\mathbf{K}}\mathbf{K}^+$ is not abelian. Now the result follows from Theorem 3.72.

(2) ⇒ (1): We want to apply Proposition 3.75. Since every ring is obviously 0-regular (i.e., each congruence is determined by its 0-class), only the congrunce $\mathbf{0_R}$ is $\mathbf{S}^*$-orbit contained. Now we can apply Proposition 3.75 and obtain that $\mathbf{K}$ is simple. □

Proof II: (1) ⇒ (2): Let $\mathbf{L}$ be a minimal sub-$\mathbf{K}$-ring of ${}_{\mathbf{K}}\mathbf{K}^+$ with $|L| > 1$. Then we take $\mathbf{R} := \mathbf{L}^+$. Since $\mathbf{K}$ is simple and has a left identity, $\mathbf{K}$ operates faithfully on $\mathbf{L}$. Now Theorem 5.3 yields the result.

(2) $\Rightarrow$ (1): By a result in near-ring theory, namely [**Pil83**, Theorem 9.218 (b)], we know that even the near-ring $(M_S(L); +, \circ)$ is simple. □

There are several surprising facts about finite simple zero-symmetric composition rings $\mathbf{K} = (K; +, \cdot, \circ)$ with left identity with respect to composition. One is that the near-ring $(K; +, \circ)$ is automatically simple, too. We state this result in the following Proposition:

PROPOSITION 5.6. *Let $\mathcal{V}$ be a variety of Ω-groups, and let $\mathbf{K}$ be a $\mathcal{V}$-composition algebra. If $\mathbf{K} = (K; +, -, 0, \omega_1, \omega_2, \ldots, \circ)$ is finite, simple, and zerosymmetric, and has a left identity with respect to composition, then the near-ring $(K; +, \circ)$ is simple as well.*

Isn't that surprising ? Given a finite, not simple, zerosymmetric near-ring

$$(K; +, \circ)$$

with left identity, you can never define operations $\star_1, \star_2, \ldots$ such that

$$(K; +, \star_1, \star_2, \ldots, \circ)$$

is a simple composition algebra. In other words, the ugly that you want to choose $\star_i$, you will never be abel to ruin all congruences of $(K; +, \circ)$.

But instead of enthusiasm for this result, the reader might appreciate a proof:

Proof I: We let $\mathbf{L}$ be a minimal sub-$\mathbf{K}$-module $\mathbf{L}$ of ${}_{\mathbf{K}}\mathbf{K}^+$ with $|L| > 1$. By the simplicity of $\mathbf{K}$ and the fact that the left identity and the zero-element of $\mathbf{K}$ operate differently on L, $\mathbf{L}$ is a faithful $\mathbf{K}$-module. Furthermore, $\mathbf{K}$ satisfies $K * l = L$ for all $l \neq 0$. Now we look at the module operation of the near-ring $(K; +, \circ)$ on the group $(L; +)$. Since the variety $\mathcal{G}$ of all groups is clearly 0-regular, Proposition 3.78 yields that the near-ring $(K; +, \circ)$ is simple. □

Proof II: As in Proof I, we construct L with $K * l = L$ for all $l \neq 0$. Now near-ring theory gives that every finite 2-primitve near-ring with identity is simple: By [**Pil83**, Theorem 4.52] [1] $(K; +, \circ)$ is isomorphic to a centralizer near-ring, which is simple due to [**Pil83**, Theorem 9.218 (d)]. □

We will now go deeper into a peculiar question: Given a finite simple zero-symmetric composition ring $(K; +, \cdot, \circ)$ with left identity and nonzero multiplication, can it ever happen that $(K; +, \circ)$ is a ring and has more than one element ? We shall obtain the following result:

PROPOSITION 5.7. *Let $\mathbf{K}$ be finite simple, zero-symmetric composition ring with left identity with respect to composition and nonzero multiplication, and suppose $|K| > 1$ and $(K; +, \circ)$ is a ring.*

[1] The density theorems for 2-primitive near-rings is due to Wielandt and Betsch [**Bet73**] or Polin [**Pol71**]; for the interpolation part of the proof see also [**Aic95**]. The interpolation part has also been stated in [**Ram69**].

Then $(K;+,\cdot,\circ)$ *is isomorphic to* $(\mathbb{Z}_2;+,\star,\star)$*, where* $\star$ *is the multiplication of the two element field* $(\mathbb{Z}_2;+,\star)$*.*

Proof: By Theorem 5.5, $\mathbf{K}$ is isomorphic to a centralizer composition ring

$$(M_S(R);+,\cdot,\circ)$$

for some ring $\mathbf{R}$.

Since we have assumed that $(M_S(R);+,\circ)$ is a ring, Proposition 3.76 makes it even be a division ring, and, since it is finite, a field. So we are left with the following problem: Which multiplications can be defined on a finite field $(F;+,\circ)$ such that $(F;+,\cdot,\circ)$ becomes a composition ring ? We shall see in the following results, namely in Proposition 5.8 and Proposition 5.9, that only in the case that $(F;+,\circ)$ is the two element field there is a nonzero multiplication that turns $(F;+,\cdot,\circ)$ into a composition ring, and that this multiplication is precisely the field-multiplication on $\mathbb{Z}_2$. This completes the proof of Proposition 5.7. □

PROPOSITION 5.8. *Let* $(F;+,\circ)$ *be a field. If there exists a nonzero multiplication* $\cdot$ *on* F *such that* $(F;+,\cdot,\circ)$ *becomes a composition ring, then* $\operatorname{char} F = 2$.

Proof: We shall denote the identity with respect to $\circ$ by $\mathbf{1}$, $\mathbf{1}+\mathbf{1}$ by $\mathbf{2}$ and $\mathbf{2}+\mathbf{2}$ by $\mathbf{4}$. Now let x, y be elements in F. Then we have: $(x\cdot y)\circ\mathbf{2} = (x\circ\mathbf{2})\cdot(y\circ\mathbf{2}) = (x+x)\cdot(y+y) = (x\cdot y)\circ\mathbf{4}$. From this it follows that for all $x, y \in F$, we have $(x\cdot y)\circ\mathbf{2} = 0$. If $\operatorname{char} F \neq 2$ than this implies that $x\cdot y = 0$ for all x, y. □

PROPOSITION 5.9. *Let* $(F;+,\circ)$ *be a perfect field with* $\operatorname{char} F = 2$*. If there exists a nonzero multiplication* $\cdot$ *on* F *that turns* $(F;+,\cdot,\circ)$ *into a composition ring then* $(F;+,\cdot,\circ)$ *is isomorphic to* $(\mathbb{Z}_2;+,\star,\star)$*, where* $\star$ *is the field-multiplication on* $\mathbb{Z}_2$*.*

Before proving Proposition 5.9, we recall that in particular every finite field is perfect.

Proof: First of all, we shall prove that for all $x, y, k \in F$ we have

$$(x\circ k)\cdot y = x\cdot(y\circ k). \tag{2.2}$$

We fix $x, y, k \in F$ and denote the identity with respect to $\circ$ by $\mathbf{1}$. Now we compute $(x\circ(k+\mathbf{1}))\cdot(y\circ(k+\mathbf{1}))$ in two ways.

$$\begin{aligned}(x\circ(k+\mathbf{1}))\cdot(y\circ(k+\mathbf{1})) &= (x\circ k+x)\cdot(y\circ k+y)\\ &= (x\circ k)\cdot(y\circ k)+(x\circ k)\cdot y+x\cdot(y\circ k)+x\cdot y\\ &= (x\cdot y)\circ k+(x\circ k)\cdot y+x\cdot(y\circ k)+x\cdot y\end{aligned}$$

On the other hand, we have

$$\begin{aligned}(x\circ(k+\mathbf{1}))\cdot(y\circ(k+\mathbf{1})) &= (x\cdot y)\circ(k+\mathbf{1})\\ &= (x\cdot y)\circ k+x\cdot y.\end{aligned}$$

From this, we get

$$(x\circ k)\cdot y+x\cdot(y\circ k) = 0$$

and hence equation (2.2).

Since F is a perfect field of characteristic 2, every element $x \in F$ has a unique $y \in F$ with $y \circ y = x$. As usual, we denote this y by $\sqrt{x}$. Now we prove the following fact about the multiplication.

$$x \cdot y = (\mathbf{1} \cdot \mathbf{1}) \circ \sqrt{x \circ y}. \tag{2.3}$$

We assume $x, y \neq 0$. Then we apply equation (2.2) and get (of course, fractions are taken with respect to the field operation $\circ$)

$$x \cdot y = (\frac{x}{\sqrt{\frac{x}{y}}}) \ \cdot \ (y \circ \sqrt{\frac{x}{y}}).$$

Computing the fractions and roots, this is equal to $\sqrt{x \circ y} \cdot \sqrt{x \circ y} = (\mathbf{1} \circ \sqrt{x \circ y}) \cdot (\mathbf{1} \circ \sqrt{x \circ y}) = (\mathbf{1} \cdot \mathbf{1}) \circ \sqrt{x \circ y}$. But now note that $\cdot$ is associative. Let x and z be two elements of $F \setminus \{0\}$. Then we have $(x \cdot z) \cdot z = x \cdot (z \cdot z)$. By equation (2.3), we can write this as

$$(\mathbf{1} \cdot \mathbf{1}) \circ \sqrt{((\mathbf{1} \cdot \mathbf{1}) \circ \sqrt{x \circ z}) \circ z} = (\mathbf{1} \cdot \mathbf{1}) \circ \sqrt{x \circ ((\mathbf{1} \cdot \mathbf{1}) \circ z)}.$$

Since the multiplication $\cdot$ is nonzero, $\mathbf{1} \cdot \mathbf{1} \neq 0$. Hence we get

$$((\mathbf{1} \cdot \mathbf{1}) \circ \sqrt{x \circ z}) \circ z = x \circ (\mathbf{1} \cdot \mathbf{1}) \circ z,$$

and, squaring and simplifying,

$$x \circ z \circ z \circ z = x \circ x \circ z \circ z.$$

This implies $x = z$, hence all nonzero elements of F are equal, therefore $(F; +, \circ)$ is isomorphic to $(\mathbb{Z}_2; +, \star)$. From equation (2.3), we see that the only nonzero multiplication $\cdot$ that turns $(\mathbb{Z}_2; +, \cdot, \star)$ into a composition ring is $\star$.

At this point, we want to mention one of the possible applications of Proposition 5.7

COROLLARY 5.10. *Let $(K; +, \circ)$ be a finite simple ring with identity with more than two elements. Then there is no nonzero multiplication $\cdot$ such that $(K; +, \cdot, \circ)$ is a composition ring.*

Proof: Suppose there were such a nonzero multplication. Then $(K; +, \cdot, \circ)$ is a composition ring that fulfills the assumptions of Proposition 5.7. This means that K has two elements, a contradiction. □

3. Composition rings with constants

As in [**Adl62**], we call an element c in the composition ring $\mathbf{K}$ *a constant element of* $\mathbf{K}$ iff $c \circ x = c$ for all $x \in K$. This is the case iff $c \circ 0 = c$. We let R be the set of all constant elements of $\mathbf{K}$, and let $\mathbf{R}$ be the sub-ring of $\mathbf{K}^+ := (K; +, \cdot)$ with universe R. We call $\mathbf{R}$ the *ring of constants* of $\mathbf{K}$. In the structure theory of simple composition rings, we will make use of the following kind of composition rings of blockwise constant functions. This definition is the composition ring version of Definition 3.58.

DEFINITION 5.11. Let $\mathbf{U}$ be a ring, and let ρ be an equivalence relation on U. Then we define

$$M(U,\rho) := \{m : U \to U \mid \forall u_1, u_2 \in U \,:\, (u_1,u_2) \in \rho \Rightarrow m(u_1) = m(u_2)\}.$$

We let $\mathbf{M}(\mathbf{U},\rho)$ the sub-composition ring of $\mathbf{M}(\mathbf{U})$ with universe $M(U,\rho)$.

Applying the theory of composition algebras in congruence permutable varieties, we have the following result. It is a generalization of K. Kaarli's result on simple near-rings presented in [**Kaa95**].

THEOREM 5.12. *Let* $\mathbf{K}$ *be a simple composition ring and let* $\mathbf{R}$ *be its ring of constants. We assume that* $|R| \geq 2$. *Then there is a sub-composition ring* $\mathbf{K}'$ *of* $\mathbf{M}(\mathbf{R})$ *with the following properties:*

(1) $\mathbf{K}'$ *is isomorphic to* $\mathbf{K}$.
(2) $\mathbf{K}'$ *is dense in* $\mathbf{M}(\mathbf{R},\rho)$, *where* ρ *is the equivalence relation on* R *that is defined by* $(r_1,r_2) \in \rho \Leftrightarrow \forall k \in K \,:\, k \circ r_1 = k \circ r_2$.
(3) *If* $\alpha \in Con\mathbf{R}$ *and* $\alpha \subseteq \rho$, *then* $\alpha \in \{\mathbf{0_R}, \mathbf{1_R}\}$.

Proof I: The result is an instance of Theorem 3.59. □

Proof II: We distinguish two cases:

Case : K *has a zero multiplication,* $(K;+)$ *is an abelian group, and* $(K_0;+,\circ)$ *is a ring, where* $K_0 := \{k \in K \,:\, k \circ 0 = 0\}$: Let γ be the following relation on K:

$$(k_1,k_2) \in \gamma :\Leftrightarrow k_1 - k_2 \in R$$

We show that γ is a congruence on K. To this end, we recall that every composition ring $\mathbf{K}$ is an Ω-group as defined in Definition 1.21. Hence it is sufficient to prove that R is an ideal of the composition ring $\mathbf{K}$. According to Definition 1.22, this amounts to showing the following facts:

(1) $(R;+)$ *is a normal subgroup of* $(K;+)$: $(K;+)$ is an abelian group, hence every subgroup is normal. Since we know that $\mathbf{R} = (R;+,\circ)$ is a sub-ring of $\mathbf{K}^+ = (K;+,\cdot)$, the group $(R;+)$ is obviously a subgroup of $(K;+)$.
(2) $K \cdot R \subseteq R$: Since $K \cdot K = \{0\}$, we have $K \cdot R = \{0\}$.
(3) $R \cdot K \subseteq R$: Since $K \cdot K = \{0\}$, we have $R \cdot K = \{0\}$.
(4) $R \circ K \subseteq R$: We show that for every $r \in R$ and $k \in K$, we have $r \circ k = (r \circ k) \circ 0$:

$$\begin{aligned}(r \circ k) \circ 0 &= r \circ 0 \circ k \circ 0\\ &= r \circ 0\\ &= r \circ (0 \circ k)\\ &= (r \circ 0) \circ k\\ &= r \circ k\end{aligned}$$

Applying the definition that r is a constant element of $\mathbf{K}$ iff $r \circ x = r$ for all $x \in K$ we get, using that r is a constant element of $\mathbf{K}$, $(r \circ k) \circ y = r \circ y = r = r \circ k$, which proves again that $r \circ k$ is constant.

(5) *For all $k_1, k_2 \in K$ and $r \in R$ we have $k_1 \circ (k_2 + r) - k_1 \circ k_2 \in R$*: We write k_1 as $l_c + l_0$, where $l_c := k_1 \circ 0$ and $l_0 := -k_1 \circ 0 + k_1$. It is easy to see that $l_c \in R$ and $l_0 \in K_0$. Then, using the fact that $(K_0; +, \circ)$ is a ring, we have

$$\begin{aligned} k_1 \circ (k_2 + r) - k_1 \circ k_2 &= l_c \circ (k_2 + r) + l_0 \circ (k_2 + r) - l_0 \circ k_2 - l_c \circ k_2 \\ &= l_c + l_0 \circ k_2 + l_0 \circ r - l_0 \circ k_2 - l_c \\ &= l_0 \circ r. \end{aligned}$$

This holds because we have $K \circ R \subseteq R$, which holds because of $(k \circ r) \circ 0 = k \circ (r \circ 0) = k \circ r$.

Hence R is an ideal of $\mathbf{K}$. But $\mathbf{K}$ is simple, hence R is either $\{0\}$ or K. Since by assumption $|R| \geq 2$, we have $R = K$. Hence every element $k \in K$ fulfils

$$\forall l \in K \,:\, k \circ l = k. \tag{3.1}$$

Since $\circ$, as the projection function to the first of its arguments, is always a congruence preserving function on $(K; +, \cdot)$, we observe that the fact that $\mathbf{K}$ is simple implies that even $(K; +, \cdot)$ is simple. Therefore $(K; +, \cdot)$ is the zero-ring on a group of prime order.

Using Equation 3.1, we see that the composition ring $\mathbf{K}$ is isomorphic to the composition ring of all constant functions on the ring $\mathbf{R}$. If we take $\rho := R \times R$, we see that therefore $\mathbf{K}$ is isomorphic to $\mathbf{M}(\mathbf{R}, \rho)$, which proves claim (1) and claim (2).

For claim (3), we observe that the ring $\mathbf{R}$ is simple; therefore every congruence on $\mathbf{R}$ is either $\mathbf{0_R}$ or $\mathbf{1_R}$.

Case : $\mathbf{K}$ *has a nonzero multiplication, or $(K; +)$ is a nonabelian group, or $(K_0; +, \circ)$, where $K_0 := \{k \in K \,:\, k \circ 0 = 0\}$ is not a ring*: Since $|R| \geq 2$, and since $\mathbf{K}$ is simple, the composition ring $\mathbf{K}$ operates faithfully on the ring $\mathbf{R}$. Hence the mapping Φ defined by

$$\begin{array}{rccc} \Phi & : & K & \longrightarrow & M(R) \\ & & k & \longmapsto & \Phi(k), \end{array}$$

where

$$\begin{array}{rccc} \Phi(k) & : & R & \longrightarrow & R \\ & & r & \longmapsto & k \circ r \end{array}$$

embeds $\mathbf{K}$ into $\mathbf{M}(\mathbf{R})$. Let $\mathbf{K}' := \Phi(\mathbf{K})$. Obviously, $\mathbf{K}'$ satisfies claim (1); let us now attack the proof of claim (2): First of all we define a multiplication μ on R

as follows [2]: If $\mathbf{K}$ has a nonzero multiplication, we define

$$\mu(r_1, r_2) := r_1 \cdot r_2,$$

if $\mathbf{K}$ is a nonabelian group, we define

$$\mu(r_1, r_2) := r_1 + r_2 - r_1 - r_2,$$

if $(K_0; +, \circ)$ is not a ring and $(K; +)$ is an abelian group, we take elements $k, k_1, k_2 \in K_0$ with $k \circ (k_1 + k_2) \neq k \circ k_1 + k \circ k_2$ and define

$$\mu(r_1, r_2) := k \circ r_1 + k \circ r_2 - k \circ (r_1 + r_2).$$

Using the assumptions made in this case, we see that μ satisfies the following properties.

(1) For all $k_1', k_2' \in K'$ the function $\mu(k_1', k_2')$ defined by

$$\begin{array}{rccc} \mu(k_1', k_2') & : & R & \longrightarrow & R \\ & & r & \longmapsto & \mu(k_1(r), k_2(r)) \end{array}$$

is again in K'.

(2) For all $r \in R$ we have

$$\mu(r, 0) = \mu(0, r) = 0.$$

(3) We have $\overline{x}, \overline{y} \in R$ with

$$\mu(\overline{x}, \overline{y}) \neq 0.$$

Another property that we shall need is the following: For every subset $X \subseteq R$, and any $y \in R$, the set

$$I := \{k'(y) \,|\, k' \in K',\ \forall x \in X\ :\ k'(x) = 0\} \tag{3.2}$$

is either $\{0\}$ or R. We notice that the set I is the 0-class of a congruence on the $\mathbf{K}'$-module ${}_{\mathbf{K}'}\mathbf{R}$. This can be proved using the fact that we have all the constant mappings in K'. We then show that the set of all functions in K' whose image is contained in I, namely

$$(I : R)_{K'} := \{k' \in K' \,|\, k(R) \subseteq I\},$$

is an ideal of the composition ring $\mathbf{K}'$. Since $\mathbf{K}'$ is simple, it is either $\{0\}$ or K'. If $(I : R)_{K'}$ is $\{0\}$, then in particular every constant function which has its image

[2]The fact that a non-abelian algebra allows to construct such multiplications lays at the beginning of my work in near-ring theory. I first saw the importance of such a multiplication when studying the proof of Wielandt and Betsch's Density theorem in [**Pil84**]. I then found similar ideas in the papers by H. K. Kaiser (e.g. [**Kai74a**], [**IK79**]). Later, K. Kaarli pointed out to me that some results that were obtained using this method [**Kaa78**] had also been obtained using methods of universal algebra [**HH82**], and that a similar ideal multiplication introduced by S.D.Scott in [**Sco97**] again looked similar to the commutator studied in [**Kur65**]. Later, I proved that S.D.Scott's ideal multiplication was a reinvention of the universal algebra commutator (Proposition 1.24) and that Hagemann's and Herrmann's main interpolation result [**HH82**] could be proved using such an idea of multiplication. Unfortunately, Proof II for Proposition 2.2 hides Kaiser's multiplication idea behind the notational complications of universal algebra. In the present proof, the reader will find this multiplication again.

in I is the zero-function, and therefore we have $I = \{0\}$. If $(I : R)_{K'}$ is equal to K', then every function in K' has its image contained in I. In particular all constant functions on R have their image contained in I. This implies $R \subseteq I$, and thus $I = R$. Altogether, we see that I is either $\{0\}$ or R.

We will now prove

$$\mathbf{K}' \text{ is dense in } \mathbf{M}(\mathbf{R}, \rho). \tag{3.3}$$

To this end, we show that for each $n \in \mathbb{N}$, we can interpolate any function in $\mathbf{M}(\mathbf{R})$ at n places by a function in K'. We will do so by induction on n.

Case $n = 1$: immediate, since all the constant functions on R are elements of K'.

Case $n = 2$: Let $r_1, r_2 \in R$, and let $m \in M(R, \rho)$. Since all constant functions on R are in K', it is sufficient to find a function $k \in K'$ with

$$k(r_1) = 0 \text{ and } k(r_2) = m(r_2) - m(r_1) \tag{3.4}$$

because in that case $i(x) := k(x) + m(r_1)$ interpolates m at $\{r_1, r_2\}$.

By the remark after (3.2), the set

$$I := \{k(r_2) \,|\, k \in K \text{ and } k(r_1) = 0\}$$

is either $\{0\}$ or R. Using the fact that all constant functions are in K', it is not hard to prove that $I = \{0\}$ iff $(r_1, r_2) \in \rho$. If $(r_1, r_2) \in \rho$, the zero mapping satisfies (3.4). If $(r_1, r_2) \notin \rho$, we know that $I = R$, which immediately gives us a function $k \in K'$ that satisfies (3.4).

Case $n \geq 3$: Let $r_1, r_2, \ldots, r_n \in R$, and let $m \in M(R, \rho)$. Since, by induction hypothesis, every function on in $M(R, \rho)$ can be interpolated at $n - 1$ points by a function in K', then after subtracting a suitable element $k_1 \in K'$ from m, we are left with a function $m_1 \in M(R, \rho)$ that satisfies $m_1(x_1) = m_1(x_2) = \ldots = m_1(x_{n-1}) = 0$. If $m_1(x_n) = 0$, the function k_1 is already the required function that interpolates m. So, we will assume that $m_1(x_n) \neq 0$, and we will try to find $k_2 \in K'$ that interpolates m_1 at $x_1, x_2, \ldots, x_n$. Since m_1 can be interpolated at every subset with no more than $n - 1$ elements by a function in K', we have

$$I_1 = \{k(x_n) \,|\, k \in K' \text{ and } k(x_1) = k(x_2) = \cdots = k(x_{n-2}) = 0\} \neq 0$$

and

$$I_2 = \{k(x_n) \,|\, k \in K' \text{ and } k(x_{n-1}) = 0\} \neq 0.$$

By the remarks after (3.2), we have $I_1 = R$ and $I_2 = R$.

We will now start to construct the function k_2. Let $\overline{x}, \overline{y} \in R$ be such that $\mu(\overline{x}, \overline{y}) \neq 0$. The fact that $I_1 = R$ allow us to construct a function $p_1 \in K'$ such that

$$p_1(x_i) = 0 \text{ for } i = 1, 2, \ldots, n-2 \text{ and } p_1(x_n) = \overline{x}.$$

The fact that $I_2 = R$ allow us to construct a function $p_2 \in K'$ such that

$$p_2(x_{n-1}) = 0 \text{ and } p_2(x_n) = \overline{y}.$$

Multiplying these two functions via μ, we obtain a function

$$p_3(r) := \mu(p_1(r), p_2(r))$$

with $p_3 \in K'$ that satisfies

$$p_3(x_i) = 0 \text{ for } i = 1, 2, \ldots, n-1 \text{ and } p_3(x_n) \neq 0.$$

The remark after (3.2) yields

$$\{k(x_n) \mid k \in K' \text{ and } k(x_1) = k(x_2) = \cdots = k(x_{n-1}) = 0\} = R,$$

which yields the function k_2 that interpolates m_1 at $\{x_1, x_2, \ldots, x_n\}$.

This finishes the proof of claim (1) and claim (2) in this case. We will now prove claim (3). Let A be the α-class of 0, i.e., $A := 0/\alpha$. Then A is an ideal of the ring $\mathbf{R}$. We define a set I by

$$I = \{k \in K' \mid \forall r \in R : k(r) \in A\}$$

If α is a congruence of the ring $\mathbf{R}$ and $\alpha \subseteq \rho$, then I is an ideal of the composition ring $\mathbf{K}'$: It is easy to see that I is an ideal of $(K'; +, \cdot)$. Now we let k_1, k_2 be elements of K' and let $i \in I$. The mapping $i \circ k_1$ then has its range contained in A. For the "left ideal property", namely that

$$k_1 \circ (k_2 + i) - k_1 \circ k_2$$

lies in I, we fix $r \in R$. Then $k_1(k_2(r) + i(r))$ is equal to $k_1(k_2(r) + a)$ for some $a \in A$. Since $\alpha \subseteq \rho$, $k_2(r) + a$ is equivalent to $k_2(r)$ modulo ρ. This implies

$$k_1((k_2(r) + i(r)) - k_1(k_2(r)) = 0,$$

and therefore $k_1 \circ (k_2 + i) - k_1 \circ k_2$ lies in I. Altogether, I is an ideal of $(K'; +, \cdot, \circ)$.

If $I = K'$, then $0/\alpha = R$, hence $\alpha = \mathbf{1_R}$. If $I = \{0\}$, then $0/\alpha = 0$, hence $\alpha = \mathbf{0_R}$. □

Proposition 3.60 gives the following result for composition rings:

PROPOSITION 5.13. *Let $\mathbf{R}$ be a ring with nonzero multiplication, and let ρ be an equivalence relation on R such that*

(1) *$\alpha \in Con\mathbf{R}$ and $\alpha \subseteq \rho$ implies $\alpha \in \{\mathbf{0_R}, \mathbf{1_R}\}$.*
(2) *There are only finitely many equivalence classes modulo ρ.*

Then $\mathbf{M}(\mathbf{R}, \rho)$ is simple.

This gives the following characterization of simple composition rings with constants:

THEOREM 5.14. *Let $\mathbf{K}$ be a finite composition ring such that $R := \{k \in K : k \circ 0 = k\}$ has the property $|R| \geq 2$. Then the following are equivalent:*

(1) *$\mathbf{K}$ is simple.*
(2) *Both of the following two conditions hold:*

(a) $\mathbf{K}$ *is isomorphic to a composition ring* $\mathbf{M}(\mathbf{R}, \rho)$*, where* $\mathbf{R}$ *is a ring and* ρ *is an equivalence relation on* R *such that* $\alpha \in Con\,\mathbf{R}, \alpha \subseteq \rho$ *implies* $\alpha \in \{\mathbf{0_R}, \mathbf{1_R}\}$.
(b) $\mathbf{K}$ *is not isomorphic to the composition ring* $\mathbf{M}(\mathbf{R})$*, where* $\mathbf{R}$ *is the zero ring on two elements.*

Proof: (1) $\Rightarrow$ (2a): Theorem 5.12 yields that $\mathbf{K}$ is dense in a composition ring of the form $\mathbf{M}(\mathbf{R}, \rho)$. (Actually, Theorem 5.12 gives precise information how to get $\mathbf{R}$ and ρ from $\mathbf{K}$.

(1) $\Rightarrow$ (2b): By Proposition 3.62, $\mathbf{M}(\mathbf{R})$, where $\mathbf{R}$ is the zero ring on two elements, is not simple. Since $\mathbf{K}$ is simple, it cannot be isomorphic to this $\mathbf{M}(\mathbf{R})$.

(2) $\Rightarrow$ (1): If $\mathbf{R}$ has a nonzero multiplication, then Proposition 5.13 gives the required result. For dealing with the case that $\mathbf{R}$ has zero multiplication, we need to look further back to Proposition 3.60. Let $\mathbf{K} := \mathbf{M}(\mathbf{R}, \rho)$. Actually, distingushing cases whether $\mathbf{R}$ has zero multiplication or not is the wrong case distinction. A real dividing line is whether the $\mathbf{K}$-ring $\mathbf{R}$ is abelian or not.

Case $\mathbf{R}$ *is not abelian:* (This includes the case that $\mathbf{R}$ has nonzero multiplication.) Proposition 3.60 gives that the composition-$\mathbf{K}$-ring $\mathbf{M}(\mathbf{R}, \rho)$ is simple.

Case $\mathbf{R}$ *is abelian:* If $\mathbf{M}(\mathbf{R}, \rho)$ is not simple, then only the second alternative of Proposition 3.60 can occur. Hence ρ is the equivalence modulo a subgroup of index 2 of $(R; +)$. But since $\mathbf{R}$ has zero multiplication, ρ is a congruence of the ring. Hence, by the assumptions on ρ, we have $\rho = \mathbf{0_R}$. By its definition, $(M(R, \rho); +, \circ)$ is therefore equal to $(M(\mathbb{Z}_2); +, \circ)$. But this is excluded by the assumption that $\mathbf{K}$ is not isomorphic to the composition ring of all functions over the two element zero ring. □

And another example of an application of a universal result to the theory of composition rings is the following result, which is an instance of Proposition 3.63. We let $\mathbf{M_C}(\mathbf{R})$ denote the composition ring of all constant functions on R.

PROPOSITION 5.15. *Let* $\mathbf{R}$ *be a finite, simple ring with nonzero multiplication. Then the mapping* Φ *defined by*

$$\begin{array}{rcccl} \Phi & : & \{\rho \,|\, \rho \text{ is equiv. rel. on } R\} & \longrightarrow & \{\mathbf{K} \,|\, \mathbf{M_C}(\mathbf{R}) \leq \mathbf{K} \leq \mathbf{M}(\mathbf{R})\} \\ & & \rho & \longmapsto & \mathbf{M}(\mathbf{R}, \rho) \end{array}$$

is a bijection. □

As in Proposition 3.63, we see that Φ reverses inclusions. Under the assumptions of Proposition 5.15, $\mathbf{R}$ is the full matrix ring over a field. Proposition 5.15 describes all those sub-composition rings of $\mathbf{M}(\mathbf{R})$ that contain all constant functions on R. It would be interesting to classify them according to isomorphism.

CHAPTER 6

On Hagemann's and Herrmann's characterization of strictly affine complete algebras

The interpolation result Proposition 2.2 also implies the characterization of strictly affine complete algebras in [**HH82**]. In this chapter, we explain how these results can be derived from Proposition 2.2. Therefore, this chapter does not contain original results, but a new way of deriving the results in [**HH82**].

1. Varieties generated by algebras that have only neutral subalgebras

PROPOSITION 6.1. *Let* $\mathbf{A}$ *be a universal algebra. Then the following are equivalent:*

(1) *Every subalgebra of* $\mathbf{A}$ *is neutral and* $\mathcal{SP}_f\mathbf{A}$ *is congruence permutable.*
(2) *The class* $\mathcal{SP}_f\mathbf{A}$ *is arithmetical.*

By Proposition 1.6, both statements are equivalent to the fact that the Pixley operation $\mathsf{Pix}(\mathbf{A})$ can be interpolated at every finite subset of its domain by a term function on $\mathbf{A}$.

Proof: (1) $\Rightarrow$ (2): We first show that the function $\mathsf{Pix}(\mathbf{A})$ can be interpolated at every finite subset of its domain by a term function in $\mathsf{T}_3(\mathbf{A})$. We fix a finite subset D of $\mathsf{dom}(\mathsf{Pix}(\mathbf{A}))$. Let $\mathbf{F}$ be the function algebra of $\mathbf{A}$ that has

$$F := \{t|_D \mid t \in \mathsf{T}_3(\mathbf{A})\}$$

as its universe. Proposition 2.2 now yields that p can be interpolated by a function in F if it can be interpolated at every subset of D with not more than two elements by a function in F. But subsets S of D with two elements fall in one of the following classes:

(1) • $S = \{(x_1, y_1, y_1), (x_2, y_2, y_2)\}$ or
• $S = \{(x_1, y_1, x_1), (x_2, y_2, x_2)\}$ or
• $S = \{(x_1, y_1, y_1), (x_2, y_2, x_2\}$ for some $x_1, y_1, x_2, y_2 \in A$:
Then $t(x, y, z) := x$ interpolates $\mathsf{Pix}(\mathbf{A})$ at S.
(2) • $S = \{(y_1, y_1, x_1), (y_2, y_2, x_2)\}$ or
• $S = \{(x_1, y_1, x_1), (y_2, y_2, x_2)\}$ for some $x_1, y_1, x_2, y_2 \in A$:
Then $t(x, y, z) = z$ interpolates $\mathsf{Pix}(\mathbf{A})$ at S.
(3) • $S = \{(x_1, y_1, y_1), (y_2, y_2, x_2)\}$ for some $x_1, y_1, x_2, y_2 \in A$:

We use Proposition 1.5 to produce a Mal'cev function m on S with $m \in \mathsf{T}_3(\mathbf{A})$. Then m interpolates $\mathsf{Pix}(\mathbf{A})$ on S.

Hence Proposition 2.2 yields that for every finite subset D of $\mathsf{dom}(\mathsf{Pix}(\mathbf{A}))$ there is a term function $t \in \mathsf{T}_3(\mathbf{A})$ such that t is a Pixley function on D. Now Proposition 1.6 implies that $\mathcal{SP}_f\mathbf{A}$ is arithmetical.
(2) $\Rightarrow$ (1): Suppose that $\mathcal{SP}_f\mathbf{A}$ is arithmetical. We want to show that each subalgebra of $\mathbf{A}$ is neutral. Let $\mathbf{B}$ be a subalgebra of $\mathbf{A}$ and let Θ be a congruence on $\mathbf{B}$. We show that $[\Theta, \Theta] = \Theta$, where the commutator is taken in $\mathbf{B}$. Therefore, we fix $a, b \in B$ with $a \equiv b \pmod{\Theta}$. Let $D := \{(a,a,a), (a,a,b), (b,a,a), (b,a,b)\}$ and let $\mathbf{F}$ be the subalgebra of $\mathbf{B}^D$ with universe

$$F := \{t|_D \mid t \in \mathsf{T}_3(\mathbf{A})\}.$$

Let c be the function from D to B defined by $c(a,a,a) = c(a,a,b) = c(b,a,a) = a$ and $c(b,a,b) = b$. We want to find a term function that agrees with c on D.

We will use the following observation: let $f, g \in F$ and let $\mathbf{d} \in D$. Then $f(\mathbf{d}) = g(\mathbf{d})$ is equivalent to $f \equiv g \pmod{Ann(\mathbf{d})}$, where $Ann(\mathbf{d})$ is the congruence on $\mathbf{F}$ that is defined by

$$f \equiv g \pmod{Ann(\mathbf{d})} :\Leftrightarrow f(\mathbf{d}) = g(\mathbf{d}).$$

So, the term function $t \in F$ that agrees with c on D has to fulfill the following system of congruences. (We write $\bar{x}$ for the function in F that maps (d_1, d_2, d_3) to d_1, $\bar{y}$ for the function in F that maps (d_1, d_2, d_3) to d_2, and $\bar{z}$ for the function that maps (d_1, d_2, d_3) to d_3. Then c agrees with $\bar{x}$ on $\{(a,a,a), (a,a,b), (b,a,b)\}$ and with $\bar{y}$ on $\{(b,a,a)\}$.)

$$\begin{array}{lllll} (I) & t & \equiv & \bar{x} & \pmod{Ann(a,a,a)} \\ (II) & t & \equiv & \bar{x} & \pmod{Ann(a,a,b)} \\ (III) & t & \equiv & \bar{y} & \pmod{Ann(b,a,a)} \\ (IV) & t & \equiv & \bar{x} & \pmod{Ann(b,a,b)} \end{array}$$

Since $\mathbf{F}$ is a subalgebra of $\mathbf{A}^D$, it has distributive congruences. The Chinese Remainder Theorem says that a system of finitely many congruences has a solution provided that every subsystem consisting of two congruences has a solution. Now $t := \bar{x}$ solves the subsystems (I, II), (I, IV), (II, IV). The choice $t := \bar{y}$ is a solution of (I, III) and (II, III), and $t := \bar{z}$ is a solution of (III, IV). Hence c is a term function; this means $c \in F$. Since $a \equiv b \pmod{\Theta}$ and $c(a,a,a) = c(a,a,b)$, we get $c(b,a,a) \equiv c(b,a,b) \pmod{[\Theta, \Theta]}$, which implies that (a, b) lies in $[\Theta, \Theta]$. □

If $\mathbf{A}$ is finite, we get the following result.

PROPOSITION 6.2. *Let $\mathbf{A}$ be a finite algebra that is contained in a congruence permutable variety. Then the following are equivalent.*

(1) *Every subalgebra of $\mathbf{A}$ is neutral.*
(2) *The variety generated by $\mathbf{A}$ is arithmetical.*

Proof: (1) ⇒ (2): Since $\mathbf{A}$ is finite, Proposition 2.2 yields that there is a term t such that $t_{\mathbf{A}}$ agrees with $\mathsf{Pix}(\mathbf{A})$ on $\mathsf{dom}(\mathsf{Pix}(\mathbf{A}))$.This term t makes the whole variety generated by $\mathbf{A}$ arithmetical.
(2) ⇒ (1): If the variety generated by $\mathbf{A}$ is arithmetical, then so is the class $\mathcal{SP}_f\mathbf{A}$. Hence, Proposition 6.1 yields that every subalgebra of $\mathbf{A}$ is neutral. □

2. Strictly affine complete algebras

If one expands an algebras by adding further operations, one may destroy some of the properties of the original algebra. For example, some congruences may be ruined. Therefore it is interesting to study those functions that do not ruin any congruences. Polynomial functions are of that kind, but sometimes there are more of them. We will call such functions congruence preserving or simply compatible.

Definition 6.3. Let $\mathbf{A}$ be a universal algebra, let $k \in \mathbb{N}$ and let D be a subset of A^k. Then a function $f : D \to A$ is a *compatible* or *congruence preserving* function on $\mathbf{A}$ iff for all $\mathbf{a}, \mathbf{b} \in D$ we have

$$f(\mathbf{a}) \equiv f(\mathbf{b}) \pmod{\Theta_{\mathbf{A}}(\mathbf{a}, \mathbf{b})},$$

where $\Theta_{\mathbf{A}}(\mathbf{a}, \mathbf{b})$ is the congruence generated by $(a_1, b_1), (a_2, b_2), \ldots, (a_k, b_k)$.

Following [**Wer71**], an algebra is to be called affine complete if every congruence preserving function is polynomial. In the present thesis, we consider the following types of affine completeness:

Definition 6.4. We call an algebra $\mathbf{A}$ *k-affine complete* iff every congruence preserving function from A^k to A is a polynomial function.

Definition 6.5. We call an algebra $\mathbf{A}$ *strictly k-affine complete* iff every k-ary partial congruence preserving function with finite domain is the restriction of a polynomial function.

Remark: Let us briefly investigate the relation between these two concepts: If $\mathbf{A}$ is a finite strictly k-affine complete algebra, then $\mathbf{A}$ is clearly k-affine complete. On the other hand, there are examples of finite algebras that are 1-affine complete, but not strictly 1-affine complete: the group $\mathbf{Z_3} \times \mathbf{Z_3}$ is an example of such an algebra. If $\mathbf{A}$ is an infinite strictly k-affine complete algebra, then $\mathbf{A}$ is not necessarily k-affine complete. As an example, take the field of the rationals. A connection beween strict affine completeness and affine completeness is established by K. Kaarli's Extension Principle for compatible functions. A consequence of this principle is the following Proposition:

Proposition 6.6 ([**Kaa83**]). *We assume that $\mathbf{A}$ is an arithmetical algebra, k is a natural number, D is a finite subset of A^k, c is a k-ary partial compatible function on $\mathbf{A}$ with domain D, and d lies in A^k. Then there exists a compatible function $\overline{c} : D \cup \{d\} \to A$ with $\overline{c}|_D = c$.*

From this principle it follows that a finite or countable arithmetical k-affine complete algebra is also strictly k-affine complete.

We want to relate this concept to the concept of *polynomial completeness*:

DEFINITION 6.7. We call an algebra $\mathbf{A}$ *k-polynomially complete* iff every function from A^k to A is a polynomial function.

DEFINITION 6.8. We call an algebra $\mathbf{A}$ *locally k-polynomially complete* iff every k-ary partial function with finite domain is the restriction of a polynomial function.

It is easy to see that an algebra is k-polynomially complete iff it is simple and k-affine complete. It is locally k-polynomially complete iff it is strictly k-affine complete and simple. Every polynomially complete algebra is also locally polynomially complete; every infinite field shows that the converse is not true in general.

For the case of $\mathbf{A}$ being a group, results about affine completeness have been obtained in [**Nöb76**], [**Kai77**], [**Kaa78**], [**Kaa82**]. Theorem 3.4 of [**HH82**] characterizes those algebras that are strictly k-affine complete for all $k \in \mathbb{N}$. Due to the importance of their result, let us state and prove it here. For an algebra $\mathbf{A}$ of type $(\mathcal{F}, \sigma)$, let $\mathbf{A}^*$ be the algebra of a new type that we get from $\mathbf{A}$ by adding all its elements as constant operations.

PROPOSITION 6.9. *Let $\mathbf{A}$ be a universal algebra and let $k \geq 3$. Then the following are equivalent.*

(1) *$\mathbf{A}$ is neutral and $\mathcal{SP}_f\mathbf{A}^*$ is congruence permutable.*
(2) *$\mathcal{SP}_f\mathbf{A}^*$ is arithmetical.*
(3) *$\mathbf{A}$ is strictly 3-affine complete.*
(4) *$\mathbf{A}$ is strictly k-affine complete.*

Before proving Proposition 6.9, we state the following lemma.

LEMMA 6.10. *Let $\mathbf{A}$ be a universal algebra. We assume that for every pair $(a, b) \in A \times A$ there is a binary polynomial function q with $q(a, a) = q(a, b) = q(b, a) = a$ and $q(b, b) = b$. Then $\mathbf{A}$ is neutral.*

Proof of Lemma 6.10: By Lemma 1.17, it is sufficient to show $[\Theta, \Theta] = \Theta$ for each congruence Θ of $\mathbf{A}$. Let us therefore fix $\Theta \in \mathit{Con}\,\mathbf{A}$. We will show

$$\Theta \subseteq [\Theta, \Theta].$$

We know that for all $a, b, c, d \in A$ and $p \in \mathsf{P}_2(\mathbf{A})$ the conditions

$$\begin{aligned} &a \equiv b \pmod{\Theta}, \\ &c \equiv d \pmod{\Theta}, \text{ and } p(a, c) = p(a, d) \end{aligned}$$

imply

$$p(b, c) \equiv p(b, d) \pmod{[\Theta, \Theta]}.$$

Let $(a', b') \in \Theta$, and let q be a binary polynomial function on $\mathbf{A}$ satisfying $q(a', a') = q(a', b') = q(b', a') = a'$ and $q(b', b') = b'$. Now we know $a' \equiv b' \pmod{\Theta}$ and $q(a', a') = q(a', b')$. Hence we have

$$q(b', a') \equiv q(b', b') \pmod{[\Theta, \Theta]}.$$

But this just means $(a', b') \in [\Theta, \Theta]$, which we had to prove. □

Proof of Proposition 6.9: (1) ⇒ (4): If $\mathbf{A}$ is neutral, then so is $\mathbf{A}^*$. Clearly, the algebra $\mathbf{A}^*$ contains no proper subalgebras. Let T be any finite subset of A^k and let c be a compatible function from T to A. Using Proposition 1.5, it is easy to show that c can be interpolated at any subset of T with no more than two elements by a polynomial function $p \in P(\mathbf{A})$. Now we apply Proposition 2.2 for the function algebra $\mathbf{F}$ from T to $\mathbf{A}^*$ with universe

$$F := \{p|_T \mid p \in \mathsf{P}_k(\mathbf{A})\}.$$

This proposition yields that there exists a polynomial function $f \in F$ that agrees with c on T.
(4) ⇒ (3): Obvious.
(3) ⇒ (1): If $\mathbf{A}$ is strictly 3-affine complete, then it is also strictly 2-affine complete. For every pair $(a, b) \in A \times A$, the function $c(a, a) = c(a, b) = c(b, a) = a, c(b, b) = b$ is compatible, and hence the restriction of a polynomial function. So, Lemma 6.10 yields that $\mathbf{A}$ is neutral.

For showing that $\mathcal{SP}_f\mathbf{A}^*$ is congruence permutable, we show that $\mathsf{Mal}(\mathbf{A})$ can be interpolated at every finite subset of its domain by a term function on $\mathbf{A}^*$, i.e., a polynomial function on $\mathbf{A}$. Then the implication (2) ⇒ (1) of Proposition 1.5 implies that $\mathcal{SP}_f\mathbf{A}$ is congruence permutable. Since $\mathbf{A}$ is strictly 3-affine complete, it is sufficient to show that $\mathsf{Mal}(\mathbf{A})$ is a compatible function. But this is obvious.
(1) ⇔ (2): This follows immediately from Proposition 6.1. □

From this proof we get the the following consequence:

PROPOSITION 6.11. *Let $\mathbf{A}$ be an algebra such that $\mathcal{SP}_f\mathbf{A}$ is congruence permutable, and let $k \geq 2$. Then the following are equivalent:*

(1) $\mathbf{A}$ *is neutral.*
(2) $\mathbf{A}$ *is strictly 2-affine complete.*
(3) $\mathbf{A}$ *is strictly k-affine complete.*

Proof: The only part of this result that does not follow from Proposition 6.9 is that a strictly 2-affine complete algebra is neutral. For each pair $(a, b) \in A \times A$, the function $c : \{a, b\} \times \{a, b\}$, $c(a, a) = c(a, b) = c(b, a) = a$, $c(b, b) = b$ is compatible. The algebra $\mathbf{A}$ is strictly 2-affine complete, and therefore c is the restriction of a polynomial function. So Lemma 6.10 makes $\mathbf{A}$ neutral. □

Let us give the following consequence for polynomial completeness:

COROLLARY 6.12. *Let* $\mathbf{A}$ *be a simple algebra for which* $\mathcal{SP}_f\mathbf{A}$ *is congruence permutable. If* $\mathbf{A}$ *is not abelian then it is locally* n*-polynomially complete for all* $n \in \mathbb{N}$.

Proof: Since a simple non-abelian algebra $\mathbf{A}$ is neutral, the result follows from (1) $\Rightarrow$ (3) of Proposition 6.11. □

3. Affine complete algebras

It seems to be much harder to determine which algebras are *k-affine complete*: Although the problem has been settled completely for abelian groups in [**Nöb76**] and [**Kaa82**], and also for hamiltonian groups in [**Sak83**], no answer is known for varieties of groups that contain nonabelian groups. In her PhD-thesis [**Dor77**], A. Dorda constructed a 1-affine complete group of order p^6 and nilpotency class 2 for every odd prime p.

What we can do now is to characterize all finite algebras in a congruence permutable variety that have the property that all of their homomorphic images are k-affine complete. We obtain the following result:

PROPOSITION 6.13. *Let* $\mathbf{A}$ *be a finite algebra* $\mathbf{A}$ *in a congruence permutable variety, and let* $k \geq 2$. *Then the following are equivalent:*

(1) $\mathbf{A}$ *is neutral.*
(2) $\mathbf{A}$ *is strictly* 2*-affine complete.*
(3) $\mathbf{A}$ *is strictly* k*-affine complete.*
(4) *Every homomorphic image of* $\mathbf{A}$ *is* 2*-affine complete.*
(5) *Every homomorphic image of* $\mathbf{A}$ *is* k*-affine complete.*

Proof: (1), (2) and (3) are equivalent by Proposition 6.11.

(1) $\Rightarrow$ (5): Let $\mathbf{B}$ be a homomorphic image of $\mathbf{A}$. It follows from Proposition 4.4 of [**FM87**] that $\mathbf{B}$ is neutral. Thus, we may apply Proposition 6.11 to $\mathbf{B}$ and get that $\mathbf{B}$ is strictly k-affine complete. But since $\mathbf{B}$ is finite, this implies that $\mathbf{B}$ is k-affine complete.

(5) $\Rightarrow$ (4): Let $\mathbf{B}$ be a homomorphic image of $\mathbf{A}$ and let φ be a total compatible function from B^2 to B. The function ψ defined by

$$\begin{array}{rccc} \psi & : & B^k & \longrightarrow & B \\ & & (b_1, b_2, \ldots, b_k) & \longmapsto & \varphi(b_1, b_2) \end{array}$$

is compatible, hence, by (5), it is a polynomial function that lies in $\mathsf{P}_k(\mathbf{B})$. Now we define a polynomial function $q \in \mathsf{P}_2(\mathbf{B})$ by $q(x, y) := \psi(x, y, y, \ldots, y)$. The polynomial function q is now the required representation of the compatible function φ.

(4) $\Rightarrow$ (1): We show that

$$[\alpha, \alpha] = \alpha \text{ for all } \alpha \in Con\,\mathbf{A}. \tag{3.1}$$

It is elementary to see that this condition implies neutrality: If Equation (3.1) holds, we have $[\beta, \gamma] \geq [\beta \wedge \gamma, \beta \wedge \gamma] = \beta \wedge \gamma$.

Now suppose that Equation 3.1 fails. Then there are β and α in $Con\,\mathbf{A}$ such that $[\beta, \beta] \leq \alpha$ and β covers α. (For the notions of lattice theory, consult [**MMT87**, p.38].) Since $Con\,\mathbf{A}$ is finite, there is an element γ that is maximal with the property $\alpha \leq \gamma$ and $\beta \not\leq \gamma$. By this maximality property, γ is meet irreducible and therefore has a unique upper cover γ^+. Now the intervals $I[\alpha, \beta]$ and $I[\gamma, \gamma^+]$ are projective, in other words: $\beta \vee \gamma = \gamma^+$ and $\beta \wedge \gamma = \alpha$. From this, we get:

$$\begin{aligned}[\gamma^+, \gamma^+] &= [\beta \vee \gamma, \beta \vee \gamma] \\ &= [\beta, \beta] \vee [\beta, \gamma] \vee [\gamma, \gamma]\end{aligned}$$

But since $[\beta, \beta] \leq \alpha$ and $\alpha \leq \gamma$, we get $[\gamma^+, \gamma^+] \leq \gamma$.

Now we consider the factor $\mathbf{B} := \mathbf{A}/\gamma$ and notice that this algebra is subdirectly irreducible with abelian monolith $\mu := \gamma^+/\gamma$. Now let c_1, c_2 be two elements in $\mathbf{B}$ that lie in the same class of μ. The function φ defined by

$$\begin{array}{rccl} \varphi & : & B^2 & \longrightarrow & B \\ & & (b_1, b_2) & \longmapsto & \begin{cases} c_2 & \text{if } b_1 = b_2 = c_2 \\ c_1 & \text{else.} \end{cases} \end{array}$$

is clearly compatible, since it maps into one class of the unique minimal congruence μ. Since $\mathbf{B}$ is 2-affine complete, we may assume that $\mathbf{B}$ is a polynomial function. Now we have $\varphi(c_1, c_1) \equiv \varphi(c_1, c_2) \pmod{[\mu, \mu]}$, and therefore, by the definition of commutators, also $\varphi(c_2, c_1) \equiv \varphi(c_2, c_2) \pmod{[\mu, \mu]}$. Since $[\mu, \mu] = \mathbf{0_B}$, we have $(c_1, c_2) \in \mathbf{0_B}$, which is a contradiction. □

4. Some consequences for polynomial interpolation

Let us repeat some well-known results about polynomial completeness that we will need in the sequel:

Proposition 6.14 ([**LN73**, Chapter 1, Theorem 11.2]). *Every 2-polynomially complete algebra is n-polynomially complete for all $n \in \mathbb{N}$.*

Proposition 6.15 ([**Kai74b**, Hilfssatz 2]). *Every locally 2-polynomially complete algebra is locally n-polynomially complete for all $n \in \mathbb{N}$.*

From Proposition 6.9 and Proposition 6.15, we immediately get the following consequence.

Proposition 6.16. *Let $\mathbf{A}$ be a universal algebra, and let $k \geq 2$. Then the following are equivalent.*

(1) $\mathbf{A}$ *is locally 2-polynomially complete.*
(2) $\mathbf{A}$ *is locally k-polynomially complete.*
(3) $\mathbf{A}$ *is simple and not abelian, and $\mathcal{SP}_f\mathbf{A}^*$ is congruence permutable.*

The well known example of a set S, with all unary functions as operations, shows that there can be algebras that are 1-polynomially complete and not 2-polynomially complete.

H. Hule and W. Nöbauer ([**HN77**]) have started to investigate local polynomial functions. The sets of local polynomial functions are just the sets that arise from the set of polynomial functions on an algebra using the construction given in Definition 1.2. This means that for $k \in \mathbb{N}$ and and any cardinal t, we have

$$\mathsf{L}_t\mathsf{P}_k(\mathbf{A}) := \{l : A^k \to A \mid \forall S \subseteq A^k : |S| \leq t \Rightarrow \exists f \in \mathsf{P}_k(\mathbf{A}) : f|_S = l|_S\}.$$

Furthermore, they define $\mathsf{LP}_k(\mathbf{A}) := \bigcap_{n\in\mathbb{N}} \mathsf{L}_n\mathsf{P}_k(\mathbf{A})$. In [**Nöb78**], W. Nöbauer asked the following question:

> Given a class of algebras, does there exist a natural number t, such that $\mathsf{L}_2\mathsf{P}_k(\mathbf{A}) = \mathsf{L}_t\mathsf{P}_k(\mathbf{A})$ implies $\mathsf{L}_2\mathsf{P}_k(\mathbf{A}) = \mathsf{LP}_k(\mathbf{A})$ for all algebras of the class ?

If $\mathcal{SP}_f\mathbf{A}$ is congruence permutable, we see that $\mathsf{L}_2\mathsf{P}_k(\mathbf{A})$ is equal to $\mathsf{C}_k(\mathbf{A})$, where $\mathsf{C}_k(\mathbf{A})$ denotes the set of all k-ary compatible functions on $\mathbf{A}$. In 1978, W. Nöbauer knew that for simple algebras in congruence permutable varieties, the equality[1] $\mathsf{L}_2\mathsf{P}_k(\mathbf{A}) = \mathsf{L}_4\mathsf{P}_k(\mathbf{A})$ implies $\mathsf{L}_2\mathsf{P}_k(\mathbf{A}) = \mathsf{LP}_k(\mathbf{A})$ ([**IKP79**]). A possible generalization of this statement for algebras that are not simple is the following:

PROPOSITION 6.17. *Let $\mathbf{A}$ be an algebra such that $\mathcal{SP}_f\mathbf{A}$ is congruence permutable, and let $k \geq 2$. Assume that every k-ary partial compatible function can be interpolated at every subset of its domain with no more than four points by a polynomial function on $\mathbf{A}$. Then every k-ary partial compatible function can be interpolated at every finite subset of its domain by a polynomial function on $\mathbf{A}$.*

Proof: For every pair $(a, b) \in A \times A$, the function $c(a, a) = c(a, b) = c(b, a) = a$, $c(b, b) = b$ is compatible. Since by assumption every such c is the restriction of a polynomial function, Lemma 6.10 yields that $\mathbf{A}$ is neutral. Now the result follows by Proposition 6.11. □

Using the Extension Principle for compatible functions given in [**Kaa83**], we get:

COROLLARY 6.18. *Let $\mathbf{A}$ be a countable arithmetical algebra in a congruence permutable variety, and let $k \geq 2$. If $\mathsf{L}_2\mathsf{P}_k(\mathbf{A}) = \mathsf{L}_4\mathsf{P}_k(\mathbf{A})$, then $\mathsf{L}_2\mathsf{P}_k(\mathbf{A}) = \mathsf{LP}_k(\mathbf{A})$.*

Proof: We show that the assumptions of Proposition 6.17 are satisfied. To this end, let c be a partial compatible function from some subset of A^k with no more than four elements into A. Then using the Extension Principle of [**Kaa83**], c can be extended to a total compatible function $\bar{c}$ from A^k to A. The function

[1] Note that if $\mathbf{A}$ is a simple algebra in a congruence permutable variety, we have $\mathsf{L}_2\mathsf{P}_k(\mathbf{A}) = A^{(A^k)}$.

$\overline{c}$ lies in $\mathsf{L}_2\mathsf{P}_k(\mathbf{A})$, and therefore by assumption in $\mathsf{L}_4\mathsf{P}_k(\mathbf{A})$. Hence it can be interpolated at every four element subset of A^k, and therefore in particular at the whole domain of c, by a polynomial function. Now we can apply Proposition 6.17 and obtain that in particular every function in $\mathsf{L}_2\mathsf{P}_k(\mathbf{A})$ can be interpolated at each finite subset of A^k by a polynomial function. □

At this point, we should like to put some problems concerning affine completeness that we would like to have answered:

(1) *Does there exist an algebra* $\mathbf{A}$ *that is strictly* 2*-affine complete, but not strictly* 3*-affine complete ?* By Proposition 6.11, for such an $\mathbf{A}$ the class $\mathcal{SP}_f\mathbf{A}$ is not congruence permutable. Also, the algebra $\mathbf{A}$ cannot be simple: if it were simple, then it would be locally 2-polynomially complete, and hence, by [**Kai74b**, Hilfssatz 2] locally n-polynomially complete for all $n \in \mathbb{N}$.

(2) *For* $n \geq 2$*, does there exist an algebra* $\mathbf{A}$ *which is* n*-affine complete, but not* $n+1$*-affine complete ?* For $n = 1$, we could take the group $\mathbf{Z_2}$. For $n \geq 2$, we note that $\mathbf{A}$ cannot be simple: [**LN73**, Chapter 1, Proposition 11.11] and [**LN73**, Chapter 1, Theorem 11.2] give that for $n \geq 2$, a simple polynomially n-complete algebra is automatically $n+1$-polynomially complete.

(3) *Let* $k \in \mathbb{N}$*. Is there an arithmetical algebra* $\mathbf{A}$ *such that there is a* k*-ary compatible function on* $\mathbf{A}$ *with finite domain that cannot be extended to a total compatible function from* A^k *to* A *?*

(4) *Is there an algebra* $\mathbf{A}$ *that is* 1*-polynomially complete, has a surjective binary operation and is not* 2*-polynomially complete ?* Such an $\mathbf{A}$ cannot be finite (by a result of [**Slu39**]). Hence the algebra $\mathbf{A}$ has more than countably many operations.

Bibliography

[Adl62] I. Adler, *Composition rings*, Duke Math. J. **29** (1962), 607–625.

[Aic94] E. Aichinger, *Interpolation with near-rings of polynomial functions*, Master's thesis, University of Linz, 1994.

[Aic95] E. Aichinger, *Local interpolation near-rings as a frame-work for the density theorems*, Contributions to General Algebra, vol. 9, Verlag Hölder-Pichler-Tempsky, Wien - Verlag B.G. Teubner, Stuttgart, 1995, pp. 27 – 36.

[Aic97] E. Aichinger, *A note on simple composition rings*, Near-rings, near-fields and K-loops (G. Saad and M.J. Thomsen, eds.), Kluwer Acad. Publisher, 1997, pp. 167–173.

[Aic98] E. Aichinger, *Local polynomial functions on the integers*, Riv. Mat. Univ. Parma (1998), to appear.

[Bet73] G. Betsch, *Some structure theorems on 2-primitive near-rings*, Coll.Math.Soc.J.Bolyai 6, North-Holland, Amsterdam, 1973.

[BS81] S. Burris and H.P. Sankappanavar, *A course in universal algebra*, Springer New York Heidelberg Berlin, 1981.

[Che97] G. Chen, *Interpolationseigenschaften von Halbgruppen und Ω-Halbgruppen*, Ph.D. thesis, Technische Universität Wien, 1997.

[Dor77] A. Dorda, *Über Vollständigkeit bei endlichen Gruppen*, Ph.D. thesis, Technische Universität Wien, 1977.

[FM87] R. Freese and R. McKenzie, *Commutator theory for congruence modular varieties*, London Math. Soc. Lecture Note Ser., vol. 125, Cambridge University Press, 1987.

[Fuc90] P. Fuchs, *On the structure of ideals in sandwich near-rings*, Results in Mathematics **17** (1990), 256–271.

[Gor80] D. Gorenstein, *Finite groups*, 2nd ed., Chelsea Publishing Company, New York, 1980.

[GU84] H.P. Gumm and A. Ursini, *Ideals in universal algebras*, Algebra Universalis **19** (1984), 45–54.

[Gum79] H.P. Gumm, *Algebras in permutable varieties: geometrical properties of affine algebras*, Algebra Universalis **9** (1979), 8–34.

[HH82] J. Hagemann and C. Herrmann, *Arithmetical locally equational classes and representation of partial functions*, Universal Algebra, Esztergom (Hungary), vol. 29, Colloq. Math. Soc. János Bolyai, 1982, pp. 345 – 360.

[Hig56] P.J. Higgins, *Groups with multiple operators*, Proc. London Math. Soc. (3) **6** (1956), 366–416.

[HM88] D. Hobby and R. McKenzie, *The structure of finite algebras*, Contemporary mathematics, vol. 76, American Mathematical Society, 1988.

[HN77] H. Hule and W. Nöbauer, *Local polynomial functions on universal algebras*, Anais da Acad. Brasiliana de Ciencias **49** (1977), 365–372.

[Ihr93] T. Ihringer, *Allgemeine Algebra*, B.G.Teubner Stuttgart, 1993.

[IK79] M. Istinger and H.K. Kaiser, *A characterization of polynomially complete algebras*, Journal of Algebra **56** (1979), 103–110.

[IKP79] M. Istinger, H.K. Kaiser, and A.F. Pixley, *Interpolation in congruence permutable algebras*, Colloq. Math. **42** (1979), 229–239.

[Jac64] N. Jacobson, *Structure of rings*, 2nd ed., AMS Colloquium Publications, vol. XXXVII, American Mathematical Society, 1964.

[Kaa78] K. Kaarli, *On near-rings generated by the endomorphisms of some groups*, Acta et Commentationes Universitatis Tartuensis 464, University of Tartu, Estonia, 1978.

[Kaa82] K. Kaarli, *Affine complete abelian groups*, Math.Nachr. **107** (1982), 235–239.

[Kaa83] K. Kaarli, *Compatible function extension property*, Algebra Universalis **17** (1983), 200–207.

[Kaa95] K Kaarli, *On the structure of non-zerosymmetric nearrings*, Invited talk at the conference on near-rings and near-fields at Hamburg, August 1995, 1995.

[Kai74a] H. Kaiser, *A class of locally complete universal algebras*, J. London Math. Soc. **9** (1974), 5–8.

[Kai74b] H. Kaiser, *Über lokal polynomvollständige universale Algebren*, Hbg.Math.Abh. **18** (1974), 158–165.

[Kai77] H.K. Kaiser, *Über kompatible Funktionen in universalen Algebren*, Acta Mathematica Academiae Scientiarum Hungaricae **30** (1977), 105–111.

[Kur65] A.G. Kurosh, *Lectures on general algebra*, Chelsea, New York, 1965.

[LN73] H. Lausch and W. Nöbauer, *Algebra of polynomials*, North-Holland, Amsterdam, London; American Elsevier Publishing Company, New York, 1973.

[Mli75] R. Mlitz, *Jacobson density theorems in universal algebra*, Contributions to universal algebra, vol. 17, Colloqu.Math.Soc.Janos Bolyai, 1975, pp. 331 – 340.

[MMT87] R.N. McKenzie, G.F. McNulty, and W.F. Taylor, *Algebras, lattices, varieties, volume I*, Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, California, 1987.

[MPS81] C.J. Maxson, M.R. Pettet, and K.C. Smith, *On semisimple rings that are centralizer near-rings*, Pacific J. Math. **101** (1981), 451–461.

[MS80] C.J. Maxson and K.C. Smith, *The centralizer of a set of group automorphisms*, Comm. Alg. **8** (1980), 211–230.

[MvdW91] C.J. Maxson and A.P.J. van der Walt, *Centralizer near-rings over free ring modules*, J.Austral.Math.Soc. (Series A) **50** (1991), 279–296.

[Nöb76] W. Nöbauer, *Über die affin vollständigen, endlich erzeugbaren Moduln*, Monatshefte für Mathematik **82** (1976), 187–198.

[Nöb78] W. Nöbauer, *Local polynomial functions: results and problems*, Preprint of the Techn. Univ. Wien (Austria), June 1978.

[Pil83] G.F. Pilz, *Near-rings*, 2nd ed., North-Holland Publishing Company – Amsterdam, New York, Oxford, 1983.

[Pil84] G.F. Pilz, *Algebra – ein Reiseführer durch die schönsten Gebiete*, Universitätsverlag Rudolf Trauner, Linz, 1984.

[Pol71] S.V. Polin, *Primitive m-near-rings over multioperator groups*, Mat. USSR Sbornik **13** (1971), no. 2, 247 – 265.

[PV97] Q.N. Petersen and S. Veldsman, *Composition near-rings*, Near-rings, near-fields and K-loops (G. Saad and M.J. Thomsen, eds.), Kluwer Acad. Publisher, 1997, pp. 357–372.

[Ram69] D. Ramakotaiah, *Structure of* 1*-primitive near-rings*, Math.Z. **110** (1969), 15–26.

[Rob82] D.J.S. Robinson, *A course in the theory of groups*, Springer-Velag, 1982.

[Sak83] M. Saksa, *Polynomiaalsed funktsioonid ryhmadel (polynomial functions on groups)*, Master's thesis, University of Tartu, Estonia, 1983.

[Sco95] S.D. Scott, *Some interesting open problems*, Near-ring newsletter - number 16 (Y. Fong, G. Pilz, A. Oswald, and K.C. Smith, eds.), National Cheng Kung University, Taiwan, January 1995, pp. 160 – 161.

[Sco97] S.D. Scott, *The structure of* Ω*-groups*, Near-rings, near-fields and K-loops (G. Saad and M.J. Thomsen, eds.), Kluwer Acad. Publisher, 1997, pp. 47–138.

[Slu39] J. Slupecki, *A criterion of completeness of many-valued logic*, C.R.Soc.Sci.Varsovie **32** (1939), 102–110.

[Smi76] J.D.H. Smith, *Mal'cev varieties*, Lecture Notes in Math., vol. 554, Springer Verlag Berlin, 1976.

[Tho59] J.G. Thompson, *Finite groups with fixed point free automorphisms of prime order*, Proc. Nat. Acad. Sci. U.S.A. **45** (1959), 578–581.

[Wer71] H. Werner, *Produkte von Kongruenzklassengeometrien universeller Algebren*, Math.Z. **121** (1971), 111–140.