Interpolation with Near-rings of Polynomial Functions

(Interpolation mit Fastringen von Polynomfunktionen)

Diplomarbeit
zur Erlangung des akademischen Grades eines Diplom-Ingenieurs
in der Studienrichtung Technische Mathematik

verfaßt von
Erhard Aichinger

Angefertigt am Institut für Mathematik
der Technisch-Naturwissenschaftlichen Fakultät
der Johannes Kepler Universität Linz

bei
A.Univ.-Prof.Dr.Günter Pilz

Linz, im März 1994

Vorwort

> "De todos es conocido que los polinomios constituyen el núcleo del álgebra" (Jaime Gutierrez)

Polynome und Polynomfunktionen erfreuen sich von jeher großer Beliebtheit. Sie verdanken ihre Popularität der Tatsache, daß Polynomfunktionen durch einen (endlichen) Term darstellbar sind. So ein Term gibt außerdem an, wie die Funktion aus grundlegenden Funktionen (im einfachsten (=univariaten) Fall aus den konstanten Funktionen und der Identität) aufgebaut sind. Die Termdarstellung einer Funktion sollte man nicht nur als Datenkompression sehen, das heißt, als Möglichkeit, Funktionen auf eventuell unendlichen Mengen durch endliche Terme darzustellen, sondern auch als übersichtliche und aussagekräftige Weise, eine Funktion anzugeben. Der Begriff der Polynomfunktion läßt sich recht einfach von Ringen auf universale Algebren verallgemeinern. Man bezeichnet dann all jene Funktionen als Polynomfunktionen, die sich aus konstanten Funktionen und der Identität mithilfe der in der Algebra zur Verfügung stehenden Operationen aufbauen lassen. Es kann passieren, daß sich zwei auf verschiedene Weise aus den grundlegenden Funktionen aufgebaute Funktionen als gleich erweisen, das heißt, daß verschiedene Terme dieselbe Funktion induzieren. So induzieren zum Beispiel die Terme $(x + 2) \cdot x$ und $x^2 + 2x$ dieselbe Funktion auf den rationalen Zahlen. In unserem Fall folgt das aus dem (rechten) Distributivgesetz. Wir werden Methoden zur Früherkennung solcher Gleichheiten studieren. Ein Polynom wird dann eine Äquivalenzklasse von Termen sein, die aufgrund von Gleichheiten wie zum Beispiel dem Assoziativ- oder Distributivgesetz zur selben Funktion führen. Das wird der Inhalt des ersten Kapitels sein.

Im zweiten Kapitel werden wir uns damit beschäftigen, ob die Früherkennung solcher Gleichheiten auch effektiv, das heißt algorithmisch, möglich ist. Wir zeigen zunächst für wichtige Spezialfälle (d.h.: für Gruppen, abelsche Gruppen, Ringe), wie die Polynome über diesen Algebren aussehen. Sodann erwähnen wir eine Methode, wie man das Problem der "Gleichheit modulo gegebenen Identitäten" (wie z.B. dem Distributivgesetz) algorithmisch behandeln kann. Der Anhang enthält einfache Versuche mit einer spannenden Methode, einem Vervollständigungsalgorithmus, der die Idee der kritischen Paare verwendet und 1967 von D.Knuth und P.Bendix entwickelt wurde.

Hierauf wenden wir uns von den Polynomen ab und widmen uns wieder voll den Polynomfunktionen. Diese erlauben eine wichtige Charakterisierung der Ideale von Ω-Gruppen (das sind Gruppen mit weiteren Operationen, z.B. Multiplikationen).

Leider ist nicht jede Funktion im Leben eine Polynomfunktion. Daher werden wir danach trachten, möglichst viele Funktionen durch Polynomfunktionen zu interpolieren. Auf den Polynomfunktionen kann man, durch punktweises Anwenden, die gleichen Operationen wie auf den zugrundeliegenden Algebren ausführen. Dies wird jedoch dem Wesen der Funktionsalgebren nicht voll gerecht, behandeln wir doch auf diese Weise Funktionsalgebren so, als wären sie lediglich direkte Produkte der zugrundeliegenden Algebren (oder Unteralgebren des direkten Produkts). Um die Funktionen nicht nur punktweise betrachten zu können, bilden wir ihre Hintereinanderausführung. Eine Menge von Funktionen auf einer Gruppe, die unter punktweiser Addition und unter der Hintereinanderausführung abgeschlossen ist, bezeichnen wir als (Funktionen-)Fastring. Wir führen den Fastring der an n Stellen durch einen (kleinen, übersichtlichen) Funktionsfastring (wie etwa den Polynomfunktionen) interpolierbaren Funktionen ($L_n P$) ein, der uns erlauben wird, viele Resultate aus der Interpolationstheorie übersichtlich darzustellen. Ein typisches Resultat aus diesem Dunstkreis ist etwa der folgende Satz:

> Kann man mit einem Fastring von Funktionen auf einer Gruppe schon an vier Stellen interpolieren, so auch an beliebig (aber endlich) vielen Stellen.

Wir wissen, daß die Polynomfunktionen auf den reellen Zahlen die Interpolationseigenschaft besitzen, das heißt, wir können stets durch n Punkte in der Ebene mit verschieden x-Koordinaten den Graphen einer Polynomfunktion legen. Obiger Satz zeigt uns, daß es reicht, dieses Resultat für vier Punkte zu beweisen und enthebt uns beim Beweis dieser reellen Interpolationseigenschaft der Berechnung der Vandermonde-Determinante für $n > 4$, die wir üblicherweise zu Hilfe nehmen, um diesen Satz zu zeigen. Weiters charakterisieren wir alle Gruppen, Ringe und Fastringe, auf denen jede Funktion eine Polynomfunktion ist oder auf denen sich zumindest jede Funktion an beliebig aber endlich vielen Stellen durch eine Polynomfunktion interpolieren läßt. Solche Algebren bezeichnet man als polynomvollständig bzw. lokal polynomvollständig. Die Polynomvollständigkeit von Algebren wurde bisher besonders mit zwei Methoden erfolgreich untersucht: Der Interpolationstheorie, wie sie z.B. H.K.Kaiser und A.F.Pixley betreiben und (für Ω-Gruppen) mit den Dichtesätzen der Fastringtheorie, die auf H.Wielandt und G.Betsch zurückgehen. Wir beweisen im vierten Kapitel den Dichtesatz für nullsymmetrische, 2-primitive Fastringe mit 1 und den Interpolationssatz für nullsymmetrische, 0-primitive Fastringe mithilfe eines übergeordneten Interpolationssatzes für Fastringe, dessen Beweis die Ideen der Interpolationstheorie verwendet. Dieser übergeordnete Interpolationssatz verhilft uns zu den bekannten Resultaten über polynomvollständige Ω-Gruppen, die wir bereits als Konsequenz der Fastring-Dichtesätze kennen. Ebenso möchte ich die Ideen vorstellen, mit denen es R.Mlitz gelungen ist, einen Dichtesatz für universelle Algebren zu formulieren, der sowohl den Dichtesatz für Ringe als auch den für Fastringe impliziert.

Wir werden außerdem sehen, daß der Interpolation mithilfe von Polynomfunktionen Grenzen gesetzt sind: Im wesentlichen gibt es zwei Hindernisse für die Polynomvollständigkeit: Manchmal sind alle Polynomfunktionen von der Form “lineare Funktion + konstante Funktion”. Der tiefere Grund, daß in diesem Fall die Polynome oft nicht ausreichen, beliebige, das heißt auch nichtlineare Funktionen zu interpolieren, ist, daß der Fastring der Polynomfunktionen dann Gleichungen (wie etwa die Linearität) erfüllt, die im Fastring der zu interpolierenden Funktionen nicht gelten. Falls alle Polynomfunktionen “linear + konstant” sind, kann man aber zumindest noch die Funktionen der Form “linear + konstant” hinreichend gut interpolieren. Um dies zu zeigen, verwendet man den Dichtesatz von Jacobson aus der Ringtheorie. Polynome haben aber noch die zweite ihrer Interpolationsfähigkeit abträgliche Eigenschaft, Kongruenzrelationen auf Algebren zu respektieren. Wir können also bestenfalls die Funktionen interpolieren, die die Kongruenzrelationen ebenfalls respektieren. Solche Funktionen bezeichnet man als kompatibel. Algebren, bei denen jede kompatible Funktion bereits eine Polynomfunktion ist, bezeichnet man als affin vollständig. Wir beweisen eine Version des Interpolationssatzes für Fastringe, die manchmal die affine Vollständigkeit garantiert. Dann betrachten wir kurz, wie man die Sätze über einstellige Funktionen auf Sätze über mehrstellige Funktionen erweitern kann.

Im fünften Kapitel behandeln wir ein konkretes Problem: Sei n eine vorgegebene natürliche Zahl. Welche Funktionen auf den ganzen Zahlen können an n beliebig ausgewählten Punkten durch eine Polynomfunktion (die von einem Polynom mit ganzzahligen Koeffizienten induziert wird) interpoliert werden ? Wir erhalten eine vollständige Charakterisierung dieser Funktionen. Oder, um es in der Sprache des Fastringbuches von G.Pilz auszudrücken, wir bestimmen $L_n P(\mathbf{Z})$ explizit.

Dem Betreuer dieser Diplomarbeit, Herrn Prof.Dr.Günter Pilz, möchte ich ganz herzlich für seine Förderung und Unterstützung danken.Den zahllosen Gesprächen mit ihm über Mathematik verdanke ich nicht nur die Entstehung dieser Arbeit, sondern auch den Antrieb und das Selbstvertrauen, die für das Betreiben von Mathematik unersetzbar sind.

Meine wichtigsten Förderer aber waren meine Eltern und meine Brüder, die mir schon seit frühester Kindheit Freude am Denken zu vermitteln versuchten.

Preface

> "De todos es conocido que los polinomios constituyen el núcleo del álgebra" (Jaime Gutierrez)

Polynomials and polynomial functions have always been among the most important and most stimulating topics of algebra. They owe their popularity to the fact that polynomial functions can be represented by a (finite) term. Such a term shows how the function is built up of some basic functions (in the simplest (=univariate) case, these basic functions are the constant functions and the identity.). The term-representation of a function should not be regarded only as data-compression, i.e as possibility to represent functions on possibly infinite sets by finite terms, but also as a way of representing functions that gives us immediately some insight into the nature of the function. The notion of polynomial functions can easily be generalized from the well known concept of polynomial functions over rings to polynomial functions over universal algebras. The polynomial functions shall be those that can be constructed out of the constant functions and the identity by the operations available in the algebra. It can happen that two functions that have been built up in different ways turn out to be the same, or, in other words, that two terms induce the same functions. As an example, consider the terms $(x + 2) \cdot x$ and $x^2 + 2x$ that induce the same function on the rationals. In this case, this is a consequence of the (right) distributive law. We will study methods of detecting such equalities. A *polynomial* will be an equivalence class of terms that can be seen to induce the same function by a method of early diagnosis. Unfortunately, the early diagnosis does not always work: Two terms that induce the same function might escape us, or the diagnosis can not be effectively computed. This will be the contents of the first chapter.

In the second chapter we will try to show how one can detect such equalities effectively in some special cases. We give normal forms for the polynomials over groups, abelian groups and rings. We then mention a method of treating the problem of the "equality modulo given identities"(such as the distributiv law) in an algorithmic, non ad-hoc way. The appendix contains some experiments with a very intersesting method, a critical pair completion procedure that has been invented by D.E.Knuth and P.Bendix in 1967.

We will then leave the polynomials and devote our attention entirely to polynomial functions. As morning gift, they yield an important characterization of the ideals in Ω-groups (these are groups, possibly with further operations, such as multiplications).

Unfortunately, not every function is a polynomial function. Hence we try to interpolate as many functions as possible by polynomial functions. We can perform the same operations on polynomial functions on an algebra A as on the algebra A itself if we regard algebras of functions as direct products of the underlying algebra. This approach gives us only "pointwise" information and does not take account of the fact that we are not treating just any cartesian product (or subalgebra of the product), but that we are concerned with functions. Hence we concatenate functions. A set of functions on a group that is closed under pointwise addition and under functional composition, will be called a function-near-ring. We will introduce the near-ring of those functions that can be interpolated at at most n places by the functions in a (small and beautiful) function-near-ring. (The polynomial functions are such are beautiful near-ring). This near-ring, we shall call it L_nP, will allow us to state many of the results of interpolation theory. A typical result in this area is:

> If one can interpolate with a near-ring of functions at four places, then one can interpolate at arbitrary (finitely) many places.

We know that the polynomial functions on the reals have the interpolation property. This means that we can always find a polynomial function whose graph passes through n given points (with pairwise different x-coordinates). The above theorem shows that it is actually sufficient to show this result for four points. Furthermore we shall characterize all groups, rings and near-rings on which each function is a polynomial function or on which each function can at least be interpolated by a polynomial function at arbitrarily but finitely many places. Such algebras will be called polynomially complete and locally polynomially complete, resp. The polynomial completeness of algebras has been studied with success by two approaches: By interpolation theory, as it has been done e.g. by H.K.Kaiser and A.F.Pixley and (for Ω-groups) by the density theorems of near-ring theory that go back to H.Wielandt and G.Betsch. In the fourth chapter, we are going to prove the density theorem for zerosymmetric, 2-primitive near-rings with 1 and the interpolation theorem for zerosymmetric 0-primitive near-rings using an interpolation theorem for near-rings that can be proved with the ideas of interpolation theory. This interpolation theorem will allow us to show the results about (locally) polynomially complete Ω-groups that we have already known as consequences of the density theorems of near-rings. I also want to explain R.Mlitz's ideas that lead to a density theorem in universal algebra which implies both density theorems, the one for rings and the one for near-rings.

There are limitations for the interpolation by polynomial functions: There are two main obstacles for an algebra to be polynomially complete: Sometimes, all polynomial functions are of the form "linear + constant" or (perhaps this idea is slightly more general) the near-ring of the polynomial functions satisfies equations that are not satisfied in the near-ring of the functions to be interpolated. If all polynomial functions are "linear + constant " then one can at least interpolate those functions that are also of the form "linear + constant" sufficiently well. This is a consequence of Jacobson's density theorem for rings. But polynomial functions also have another property that has a bad effect on their interpolation potency: they respect congruences. Hence we can at most interpolate those functions that respect all congruences on a given algebra. Such a function is called *compatible*. Algebras in which every compatible function is a is a polynomial function are called *affine complete*. We prove a version of the interpolation-theorem for near-rings which guarantees affine completeness in some cases. Then we will see how we can generalize the results from unary to n-ary functions.

In the fifth chapter we treat a concrete problem: Let n be a natural number. Which functions on the integers can be interpolated by a polynomial function (induced by a polynomial with integer coefficients) on n arbitrarily selected points ? We get a complete characterization of these functions. Or, in order to put it in the language of G. Pilz's near-ring-book, we determine $L_n P(\mathbf{Z})$ explicitly.

My special thanks go to the advisor of this thesis, Prof.Dr.Günter Pilz for his support. A great number of discussions with him were not only the basis for this thesis, but they have also meant the encouragement for me that is indispensable for doing mathematics.

Most of all I am grateful to my parents and my brothers, who have tried to stimulate my creativity since my early childhood.

Contents

Chapter 1

Polynomials and polynomial functions over universal algebras

1.1 Basic notions of universal algebra

1.1.1 Algebras

Motivation

Anybody who has studied classical algebra will have observed that there are theorems in different fields of algebra, such as ring theory and group theory, that have striking simililarities and sometimes even very similar proofs. As an example we should like to mention the diamond lemma, which holds in the theory of groups, rings, near-rings, lattices, ... Thus it its natural to investigate whether there is a common explanation for these properties that seem to be shared by all "reasonable" algebraic structures. The resulting theory has been called *Universal algebra* .

Thus let us define a notion of an *algebra* which shall comprise the examples of groups, rings, near-rings, ... The definitions of all of these structures start with "A group (ring, near-ring, ...) is a set G together with an operation (two operations, ...) such that ...". You will agree that this is a strong reason for starting the general theory in the same way.

Definition 1.1 *An* algebra *is a set A together with a set Op of operations, where each $\omega \in \Omega$ is a function from A^{n_ω} to A for some $n_\omega \in \mathbf{N}_0$.*

There are however two points in which I will make this definition more concise.

- *together with* has no defined meaning in mathematics.
- It would be difficult to investigate the properties shared by the two algebras A and B, where A has two unary operations but B has 5 ternary operations.

The first problem is a purely notational one, but in order to settle the second problem we will divide the class of all algebras into subclasses. The *signature* of an algebra will tell us how many nullary, unary,... operations the algebra has.

Signatures

Definition 1.2 *$\Omega = (Op, Ar)$ is a* signature *:* $\Longleftrightarrow$

1. *Op is a set*
2. *Ar is a function with $Ar : Op \longrightarrow \mathbf{N}_0$*

Given $\Omega = (Op, Ar)$, we denote Op by Op_Ω and Ar by Ar_Ω

For a signature Ω, an $\omega \in Op_\Omega$ can be understood as an operation symbol and $Ar_\Omega(\omega)$ as its arity.

Definition 1.3 *Let Ω be a signature. Then (B, φ_B) is an* Ω-algebra *:* $\Longleftrightarrow$

1. *B is a set*
2. *$\varphi_B : Op_\Omega \longrightarrow \bigcup_{n \in \mathbf{N}_0} \{f | f : B^n \to B\}$*
3. *$\forall \omega \in \Omega : \varphi_B(\omega) : B^{Ar_\Omega(\omega)} \longrightarrow B$*

We will also write ω^B for $\varphi_B(\omega)$ and Op_Ω^B for the set $\varphi_B(Op_\Omega)$.

We will now give some examples for these definitions.

- Let Ω be a signature such that

$$Op_\Omega = \{\omega_1, \omega_2\}$$

$$Ar_\Omega(\omega_1) = Ar_\Omega(\omega_2) = 2$$

  Let $(L, \cup, \cap)$ be an arbitrary lattice. Then (L, φ_L) is an Ω-algebra setting

$$\omega_1^L := \cup, \omega_2^L := \cap$$

  We then have

$$Op_\Omega^L = \{f, g\}$$

  where

$$\begin{array}{rcrcl} f & : & L \times L & \longrightarrow & L \\ & & (x, y) & \longmapsto & x \cup y \end{array}$$

  and

$$\begin{array}{rcrcl} g & : & L \times L & \longrightarrow & L \\ & & (x, y) & \longmapsto & x \cap y \end{array}$$

- Let Ω be a signature such that

$$Op_\Omega = \{\omega_1, \omega_2, w_3\}$$
$$Ar_\Omega(\omega_1) = 2, Ar_\Omega(\omega_2) = 1, Ar_\Omega(\omega_3) = 0$$

Let $(G, +)$ be a group with neutral element 0. Then (G, φ_G) is an Ω-algebra if we define ω_1^G, ω_2^G, ω_3^G as follows:

$$\begin{array}{rcccc} w_1^G & : & G \times G & \longrightarrow & G \\ & & (x,y) & \longmapsto & x+y \end{array}$$
$$\begin{array}{rcccc} w_2^G & : & G & \longrightarrow & G \\ & & x & \longmapsto & -x \end{array}$$
$$\begin{array}{rcccc} w_3^G & : & \{()\} & \longrightarrow & G \\ & & () & \longmapsto & 0 \end{array}$$

From now on, we will denote an algebra (B, φ_B) simply by B because otherwise a lot of confusion would arise from the concise notations.

We will now collect all algebras with the same signature in one class.

Definition 1.4 *Let τ be a signature. Then $\mathbf{K}(\tau)$ denotes the class of all τ-algebras.*

Signatures for special classes of algebras

We will now give names to some important signatures that describe the algebraic structures studied in classical algebra, such as groups and rings.

- **Groups**

τ_{group} is defined by

$$Op_{\tau_{\text{group}}} := \{+, -, 0\}$$
$$Ar_{\tau_{\text{group}}}(+) = 2, Ar_{\tau_{\text{group}}}(-) = 1, Ar_{\tau_{\text{group}}}(0) = 0$$

- **Rings**

τ_{ring} is defined by

$$Op_{\tau_{\text{ring}}} := \{+, -, 0, \cdot\}$$
$$Ar_{\tau_{\text{ring}}}(+) = 2, Ar_{\tau_{\text{ring}}}(-) = 1, Ar_{\tau_{\text{ring}}}(0) = 0, Ar_{\tau_{\text{ring}}}(\cdot) = 2$$

- **Rings with identity**

τ_{ring1} is defined by

$$Op_{\tau_{\text{ring1}}} := \{+, -, 0, \cdot, 1\}$$
$$Ar_{\tau_{\text{ring1}}}(+) = 2, Ar_{\tau_{\text{ring1}}}(-) = 1, Ar_{\tau_{\text{ring1}}}(0) = 0$$
$$Ar_{\tau_{\text{ring1}}}(\cdot) = 2, Ar_{\tau_{\text{ring1}}}(1) = 0$$

Note that an algebra $A \in \mathbf{K}(\tau_{\text{ring}})$ is not necessarily a ring in the classical sense. The only thing we can say about A is that it has operations of the right arity to make it a candidate for being a ring.

1.1.2 Subalgebras and direct products

In this section, we will show to methods of getting new Ω-algebras out of old ones.

Definition 1.5 (Subalgebras) *Let $A, B \in \mathbf{K}(\Omega)$. Then A is a* sub-Ω-algebra *of B:* $\Longleftrightarrow$

1. $A \subseteq B$
2. *For all $\omega \in Op_\Omega$: $\omega^A = \omega^B|_{A^{Ar(\omega)}}$, where $f|_{A^{Ar(\omega)}}$ denotes the restriction of f to $A^{Ar(\omega)}$.*

If A is a subalgebra of B then B is called an *extension* of A.

Examples:

- We consider the ring $(\mathbf{Z}, +, \cdot)$ as an element of $\mathbf{K}(\tau_{\text{ring}})$. Then $2\mathbf{Z}$ is a sub-τ_{ring}-algebra of $\mathbf{Z}$.
- We consider the ring $(\mathbf{Z}, +, \cdot)$ as an element of $\mathbf{K}(\tau_{\text{ring1}})$. Then $2\mathbf{Z}$ is *not* a sub-τ_{ring1}-algebra of $\mathbf{Z}$.

Definition 1.6 (Direct products) *Let I be a set and let A_i be Ω-algebras for $i \in I$. Then $\times_{i \in I} A_i$ becomes an Ω-algebra if we define the operations on $\times_{i \in I} A_i$ componentwise.*

Example: Let A be an Ω-algebra. Then A^A is an Ω-algebra as well.

1.1.3 Moore-systems and generated algebras

Moore-systems are the right context to describe e.g.

- generated topologies
- generated subalgebras
- generated congruences

Definition 1.7 (Moore-system) *Let A be a set. $\mathcal{M} \subseteq \mathcal{P}(A)$ (where $\mathcal{P}(A)$ denotes the powerset of A) is a* Moore-system *on A:* $\Longleftrightarrow$

1. $A \in \mathcal{M}$
2. *For any set I we have:*

$$(\forall i \in I : M_i \in \mathcal{M}) \Rightarrow \bigcap_{i \in I} M_i \in \mathcal{M}$$

Definition 1.8 (Generated objects) *Let $\mathcal{M}$ be a Moore-system on A. Let $S \subseteq A$. Then we define*

$$\langle S \rangle_{\mathcal{M}} := \bigcap_{B \in \mathcal{M}, S \subseteq B} B$$

$\langle S \rangle_{\mathcal{M}}$ is called the object generated by M.

Note that we have $\langle S \rangle_{\mathcal{M}} \in \mathcal{M}$

The following two "generalized finiteness" conditions are closely related (cf.[Pil84]):

- Each $M \in \mathcal{M}$ is finitely generated.
- $\mathcal{M}$ has the ACC.

These two conditions are equivalent, e.g. for:

- The set of all subalgebras of a given algebra A. Note that this set is a Moore-system on A.
- The set of all congruence relations on a given algebra A. Note that this set is a Moore-system on $A \times A$.

By the way, if a collection of subsets is not a Moore-system, don't worry. Consider the generated Moore-system.

Definition 1.9 (Generated subalgebra) *Let $Sub(A)$ denote the set of all subalgebras of a given algebra A. Then the* subalgebra generated by S *is defined by*

$$\langle S \rangle_{Sub(A)}$$

1.1.4 Homomorphisms and free algebras

Definition 1.10 (Homomorphisms) *Let $B, C \in \mathbf{K}(\Omega)$. A mapping h is an* Ω-homomorphism *:* $\iff$

$$\forall \omega \in Op_\Omega \, \forall b_1, b_2, \ldots, b_{Ar_\Omega(\omega)} :$$

$$h\left(\omega^B\left(b_1, b_2, \ldots, b_{Ar_\Omega(\omega)}\right)\right) = \omega^C\left(h(b_1), h(b_2), \ldots, h(b_{Ar_\Omega(\omega)})\right)$$

As usual, injective (*surjective, bijective*) homomorphisms will be called monomorphisms (*epimorphisms, isomorphisms*). If $Ar_\Omega(\omega) = 0$, then for each homomorphism $h : B \to C$ we have :

$$h(\omega^B) = \omega^C$$

Later, we will try to explain when it is possible to extend a given partial function f from B to C (B, C of the same signature) to a homomorphism. *Free algebras* are algebras for which this extension is "very often" possible.

Definition 1.11 *Let* $\mathbf{K} \subseteq \mathbf{K}(\tau)$, $F \in \mathbf{K}$ *and* $B \subseteq F$. *Then* F is free over B in $\mathbf{K}$ $:\Longleftrightarrow$

$$\forall A \in \mathbf{K}, \forall f : B \longrightarrow A$$

$$\exists!\ \tau - \ \textit{homomorphism}\ h : F \longrightarrow A$$

such that the following diagram commutes.

$$\begin{tikzcd} B \arrow[r, "\iota"] \arrow[dr, "f"'] & F \arrow[d, "h"] \\ & A \end{tikzcd}$$

(ι denotes the natural injection from B to F.) We then call B a basis *for F.*

We want to stress that we claim two properties:

- $F \in \mathbf{K}$
- Any mapping from B to any $A \in \mathbf{K}$ can be uniquely extended to a homomorphism $h : F \to A$.

We give the following example of a vector space over the reals, where we represent the scalar multiplication of V (which we denote by $\odot_V$) by a lot of unary operations. Let τ be such that $Op_\tau := \{+\} \cup \{m_r | r \in \mathbf{R}\}$, $Ar_\tau(+) = 2$, $Ar_\tau(m_r) = 1$ for all $r \in \mathbf{R}$. Each vector space $(V, +_V, \odot_V)$ then becomes a τ-algebra if we set:

$$\varphi_V(+) := +_V$$

and

$$\begin{array}{rcccc} \varphi_V(m_r) & : & V & \longrightarrow & V \\ & & x & \longmapsto & r \odot_V x \end{array}$$

Let $\mathcal{V} \subseteq \mathbf{K}(\tau)$ the class of all vector spaces over $\mathbf{R}$ and let $V \in \mathcal{V}$. Then V is free over B in $\mathcal{V}$ iff B is a vector-space basis of V.

In the next sections we shall construct some free structures and explain the word free. But before, we prove the following lemma.

Theorem 1.12 *Let τ be a signature and $\mathbf{K} \subseteq \mathbf{K}(\tau)$ Let F, F' be free over B in $\mathbf{K}$. Then F is isomorphic to F'.*

Proof: Let $\iota_{B,F}$ be the natural injection from B to F and let $\iota_{B,F'}$ be the canonical injection from B to F'.

In the first step we use the property that F is free over B. Hence, $\iota_{B,F'}$ can uniquely be extended to a homomorphism $h_1 : F \longrightarrow F'$.

In the second step, we construct $h_2 : F' \longrightarrow F$ such that h_2 extends $\iota_{B,F}$.

We observe that $h_2 \circ h_1$ is a homomorphism from F to F that extends $\iota_{B,F}$. Since the identity function id_F is already a homomorphism from F to F extending $\iota_{B,F}$ and since (by the definition of free algebras) this homomorphism is *unique*, we get

$$h_2 \circ h_1 = id_F \tag{1.1}$$

A very similar argument shows that

$$h_1 \circ h_2 = id_{F'} \tag{1.2}$$

From (1.1) it follows that h_1 is injective, from (1.2) it follows that h_1 is surjective. Thus h_1 is an isomorphism. □

1.2 Terms

1.2.1 Term-algebras

Terms will be expressions like $x + x \cdot y$. Of course, we need a clean definition which should basically supply the following information:

- Which strings are "well-formed" expressions? "$+ + x + +$" e.g. does not look like a reasonable expression[1].
- Is x a variable ? A symbol[2] ?

We recall that a *word* over an *alphabet* is a string of elements of the alphabet, or more precisely, a function from $\{1, 2, \ldots, n\}$ to the alphabet (for some $n \in \mathbf{N}$). The set of all words over the alphabet A will be denoted by $Words(A)$. In this section, Ω will always be a signature.

Definition 1.13 (Terms) *Let X be a set, such that Ω, X and the singletons $\{[\}$ $\{]\}$,$\{,\}$ are all pairwise disjoint. Then we define a sequence $(T_i)_{i\in\mathbf{N}_0}$ with $T_i \subseteq Words(Op_\Omega \cup X \cup \{[\} \cup \{]\} \cup \{,\})$ recursively as follows.*

- **Base case** $i = 0$*:*
$$T_0 := X$$
- **Induction step** $i \in \mathbf{N}$*:*
$$T_i := \{\omega[t_1, t_2, \ldots, t_{Ar(\omega)}] \,|\, \omega \in Op_\Omega,\ t_1, t_2, \ldots, t_{Ar(\omega)} \in \bigcup_{j=0}^{i-1} T_j\}$$

[1]unless you like the frightening features of a widely used programming language
[2]whatever that means

Then $T_\Omega(X)$ is defined by

$$T_\Omega(X) := \bigcup_{j \in \mathbf{N}_0} T_j$$

$T_\Omega(X)$ is called the set of all Ω-terms over X.

Note:

- If $\omega \in Op_\Omega$ and $Ar_\Omega(\omega) = 0$ then we have: $\omega \in T_\Omega(X)$ for any X.

The so-defined terms look different from usual mathematical expressions such as $x \cdot (y + z)$. There are mainly two differences:

- We use prefix instead of infix notation.
- We use special parentheses ([,]) for constructing terms.

The first difference is purely notational. It is sometimes more convenient to write terms in infix notation instead of prefix notation. Without defining it cleanly, we shall write e.g. $[x_1 + x_2] + x_3$ for the term $+[+[x_1, x_2], x_3]$.

We made the second distinction in order to make the reader keep in mind that a term is only a word. This means that you cannot compute a thing like the sum of two terms [3].

Therefore we will define some operations on the terms.

Definition 1.14 *For each $\omega \in Op_\Omega$, we define*

$$\begin{array}{cccc} \omega^{T_\Omega(X)} & : & T_\Omega(X)^{Ar_\Omega(\omega)} & \longrightarrow & T_\Omega(X) \\ & & (t_1, t_2, \ldots, t_{Ar_\Omega(\omega)}) & \longmapsto & \omega[t_1, t_2, \ldots, t_{Ar_\Omega(\omega)}] \end{array}$$

Note that this definition makes $T_\Omega(X)$ an Ω-algebra. This algebra is called the *term algebra* over X.

Actually, we have constructed another example for free algebras.

Theorem 1.15 *$T_\Omega(X)$ is free over X in $\mathbf{K}(\tau)$*

Sketch of the proof: Let A be any algebra in $\mathbf{K}(\tau)$ and let f be a function with $f : X \longrightarrow A$. We have to construct an extension $\bar{f}$ of f such that

$$\bar{f} : T_\Omega(X) \longrightarrow A$$

We define $\bar{f}$ on all terms t by induction on the length of t. If $t \in X$ then $\bar{f}(t) := f(t)$. If

$$t = \omega[t_1, t_2, \ldots, t_{Ar_\Omega(\omega)}]$$

then we define

$$\bar{f}(t) := \omega^A \left(\bar{f}(t_1), \bar{f}(t_2), \ldots, \bar{f}(t_{Ar_\Omega(\omega)})\right)$$

We check that

[3] The only operations that you can perform on terms at this stage is the word-theoretic concatenation. A term concatenated with another term, however, is *never* a term.

- $\bar{f}$ is well-defined, that means we have defined one and only one value for each $t \in T_\Omega(X)$.
- $\bar{f}$ is a homomorphism.
- $\bar{f}$ is the only homomorphism extending f.

1.2.2 Term functions

The term

$$+[\cdot[x,y],y] \in T_{\tau_{\text{ring}}}(\{x,y\})$$

induces the function f on the integers, where

$$\begin{array}{rcrcl} f & : & \mathbf{Z}\times\mathbf{Z} & \longrightarrow & \mathbf{Z} \\ & & (x,y) & \longmapsto & x\cdot y+y \end{array}$$

We will now formalize this definition. However, we have to fix objects such as x, y to play the role of "variables".

Definition 1.16 *Let A be an Ω-algebra and let $z_1, z_2, \ldots, z_n$ such that $z_i \notin A$, $z_i \notin Op_\Omega$ (which means that they are* new *symbols).*

A tuple $(z_1, z_2, \ldots, z_n)$ that satisfies these conditions is called a tuple of variables.

Then we define the mapping

$$I_{A,n} \quad : \quad T_\Omega(A \cup \{z_1, z_2, \ldots, z_n\}) \quad \longrightarrow \quad \{f | f : A^n \longrightarrow A\}$$

by induction on the length of t. We will denote $I_{A,n}(t)$ by $t^{A,n}$.

- **Base case**

  1. $t = a \in A$: Then

$$\begin{array}{rcccl} a^{A,n} & : & A^n & \longrightarrow & A \\ & & (x_1, x_2, \ldots, x_n) & \longmapsto & a \end{array}$$

  2. $t = z_i$: Then

$$\begin{array}{rcccl} {z_i}^{A,n} & : & A^n & \longrightarrow & A \\ & & (x_1, x_2, \ldots, x_n) & \longmapsto & x_i \end{array}$$

- **Induction step**

$$\omega[s_1, s_2, \ldots, s_n]^{A,n} \quad : \quad A^n \quad \longrightarrow \quad A$$

$$(x_1, x_2, \ldots, x_n) \longmapsto$$

$$\omega^A\left({s_1}^{A,n}(x_1, x_2, \ldots, x_n), {s_2}^{A,n}(x_1, x_2, \ldots, x_n), \ldots, {s_n}^{A,n}(x_1, x_2, \ldots, x_n)\right)$$

Note:

- If we use the notation $\lambda xy.t(x,y)$ for the function that maps (x,y) to $t(x,y)$ then we can write this definition shorter as:
  - **Base case**
$$a^{A,n} := \lambda y_1 y_2 \dots y_n.a$$
$$z_i{}^{A,n} := \lambda y_1 y_2 \dots y_n.y_i$$
  - **Induction step**
$$\omega[s_1, s_2, \dots, s_n]^{A,n} :=$$
$$\lambda y_1 y_2 \dots y_n.\omega^A \left(s_1{}^{A,n}(y_1, y_2, \dots, y_n), \dots, s_n{}^{A,n}(y_1, y_2, \dots, y_n) \right)$$
- If $Ar_\Omega(\omega) = 0$ then $\omega^{A,n} = \lambda y_1 y_2 \dots y_n.\omega^A$.

We give one example of an induced function: Let τ and $\mathcal{V}$ be like in the example on vectorspaces in (section 1.1.4). Take $V := \mathbf{R}^3$. Let (x_1) be the tuple of variables. Then the term $m_5[+[x_1, \begin{pmatrix} 0 \\ 1 \\ 5 \end{pmatrix}]]$ induces the function $\lambda x.5 \cdot (x + \begin{pmatrix} 0 \\ 1 \\ 5 \end{pmatrix})$.

We will distinguish between term-functions and polynomial functions.

Definition 1.17 (Term functions) *A* term function *is a function induced by a term in*
$$T_\Omega(\{x_1, x_2, \dots, x_k\})$$

Definition 1.18 (Polynomial functions) *A* polynomial function *is a function induced by a term in*
$$T_\Omega(\mathbf{A} \cup \{x_1, x_2, \dots, x_k\})$$

When it is clear from the context which objects are variables we will omit statements like "$x_1, x_2, \dots, x_n$ is a tuple of variables" (as we have already done with statements like " Let Ω be a signature ").

1.2.3 Term functions and congruences

Term functions commute with homomorphisms. We will state this in the following theorem:

Theorem 1.19 *Let $B, C \in \mathbf{K}(\Omega)$, let $z_1, z_2, \dots, z_n$ be the tuple of variables and let $t \in T_\Omega(z_1, z_2, \dots, z_n)$. Let $\varphi : B \longrightarrow C$ be a homomorphism. Then we have:*
$$\forall x_1, x_2, \dots, x_n \in B$$
$$\varphi(t^{B,n}(x_1, x_2, \dots, x_n)) = t^{C,n}\left(\varphi(x_1), \varphi(x_2), \dots, \varphi(x_n)\right)$$

Congruence relations on an algebra A are equivalence relations that are respected by each operation.

Definition 1.20 (Congruence relations) *Let A be an Ω-algebra. Then a relation $R \subseteq A \times A$ is a congruence on A: $\Longleftrightarrow$*

1. *R is an equivalence relation on A*
2. *For all $\omega \in Op_\Omega$ and for all $x_1, x_2, \ldots, x_{Ar_\Omega(\omega)}$, $y_1, y_2, \ldots, y_{Ar_\Omega(\omega)} \in A$ we have:* **If** *for all $i \in \{1, 2, \ldots, Ar_\Omega(\omega)\}$:*

$$x_i \equiv_R y_i$$

then

$$\omega^A(x_1, x_2, \ldots, x_{Ar(\omega)}) \equiv_R \omega^A(y_1, y_2, \ldots, y_{Ar(\omega)})$$

Each algebra has at least the following ("trival") congruence relations:

- the identity $(\{(x,x)|x \in A\})$
- $A \times A$, i.e. $x \equiv_R y$ for all $x, y \in A$

An algebra that admits only the trivial congruence relations is called *simple*.

We will now fill all elements of A into bags such that two elements are in the same bag iff they are equivalent. We then calculate only with the bags[4].

Definition 1.21 (Factor algebras) *Let A be an Ω-algebra and R be a congruence relation on A. Then let $[a]$ denote the equivalence class of an $a \in A$ and let $A/_R := \{[a]|a \in A\}$. For all $\omega \in Op_\Omega$ we define*

$$\omega^{A/_R}([a_1], [a_2], \ldots, [a_n]) := [\omega^A(a_1, a_2, \ldots, a_n)]$$

The resulting Ω-algebra is called the factor-*algebra of A modulo R.*

Note that the operations defined on $A/_R$ are in fact well-defined.

Homomorphic images correspond to factor algebras

Theorem 1.22 *Each factor algebra of A is a homomorphic image of A.*

Proof: Let R be a congruence relation on A and let π_R be the *canonical projection* defined by

$$\begin{array}{rcrcl} \pi_R & : & A & \longrightarrow & A/_R \\ & & a & \longmapsto & [a] \end{array}$$

Then π_R is a homomorphism.

[4]This very intuitive illustration of factor structures is taken from [Pil83], p.135

Theorem 1.23 *For each homomorphic image (that means : the image of a homomorphism) of A there is a congruence relation R in A such that A is isomorphic to $A/_R$.*

Sketch of the proof: Let B be the homomorphic image of A under the homomorphism h. Then define R such that $a_1 \equiv_R a_2$ iff $h(a_1) = h(a_2)$ (cf. (definition 1.24)). Note however that there is not really a bijection between the congruence relations and the isomorphism classes of the homomorphic images. There are are examples of algebras in which different congruence relations might give rise to isomorphic factor algebras.

The first homomorphism theorem and the diamond lemma

From each homomorphism h, we get one important congruence relation.

Definition 1.24 *Let h be an homomorphism from A to B. Then we define the relation $Ker(h)$ by:*

$$a_1 \equiv_{Ker(h)} a_2 \textit{ iff } h(a_1) = h(a_2)$$

$Ker(h)$ is actually a congruence relation. Hence we can rewrite (theorem 1.23) as follows.

Theorem 1.25 (First homomorphism theorem) *Let h be a homomorphism from A to B. (In this case, $h(A)$ is a subalgebra of B.) Then we have:*

$$A/_{Ker(h)} \textit{ is isomorphic to } h(A)$$

Sketch of the proof:

$$\begin{array}{rcccc} i & : & A/_{Ker(h)} & \longrightarrow & h(A) \\ & & [a] & \longmapsto & h(a) \end{array}$$

is well-defined and turns out to be an isomorphism. The next theorem is a bit deeper.

Theorem 1.26 (Diamond lemma) *Let G, H be Ω-algebras and let h be an epimorphism from G to H. Then there is a bijective correspondence between the congruences of H and those congruences of G that contain $Ker(h)$.*

Sketch of the proof: We define a bijection

$$\Phi : \{R | R \text{ congruence on } H\} \longrightarrow$$

$$\{S | S \text{ congruence on } G \text{ and } Ker(h) \subseteq S\}$$

by

$$g_1 \equiv_{\Phi(R)} g_2 \text{ iff } h(g_1) \equiv_R h(g_2) \text{ for } g_1, g_2 \in G$$

Compatible functions

Functions that respect congruences allow useful tricks such as modular computation. Thus, let us give a special name to the functions that have this nice property of respecting congruences.

Definition 1.27 (Compatible functions) *Let A be an algebra and let f be a function from A to A. Then f is* compatible *:* $\iff$ *For all congruences R of A and for all $x, y \in A$ we have:*

$$x \equiv_R y \Rightarrow f(x) \equiv_R f(y)$$

Term functions are of that kind:

Theorem 1.28 *Let t be in $T_\Omega(\{x_1\})$ and let A be an algebra. Then $t^{A,1}$ is compatible.*

Sketch of one proof and presentation of another one: Term functions are built up only by the operations of the algebra A. These operations respect congruences. However, the fact that homomorphisms and term functions commute allow another proof. Let R be an arbitrary congruence on A and let B be a an homomorphic image of A under the epimorphism h such that

$$a_1 \equiv_R a_2 \text{ iff } h(a_1) \equiv_R h(a_2)$$

Now let $x, y \in A$ be fixed with $x \equiv_R y$. We have to show

$$h(t^{A,1}(x)) = h(t^{A,1}(y)) \tag{1.3}$$

By (theorem 1.19) we have

$$\forall z : h(t^{A,1}(z)) = t^{B,1}(h(z))$$

Since $h(x)$ is equal to $h(y)$ we can conclude 1.3. $\square$

This theorem can easily be generalized to polynomial functions:

Theorem 1.29 *Let A be an Ω-algebra and let t be in $T_\Omega(\mathbf{A} \cup \{x_1\})$. Then $t^{A,1}$ is compatible.*

There are two nice things about term functions:

- They are easy to write down. A finite word suffices to express a function on a possibly infinite algebra A.
- The term gives more intellegible information about a function than the representation of the function by a set of pairs.

1.3 Polynomial functions

1.3.1 Polynomial functions and related concepts

We will study the relations between some classes of functions. For the following definitions, let A be an Ω-algebra and $k \in \mathbf{N}$.

Definition 1.30

$$F_k(A) := \{f| \; f \;\; : \;\; A^k \;\; \longrightarrow \;\; A \;\} = A^{(A^k)}$$

Definition 1.31 (Polynomial functions)

$$P_k(A) :=$$

$$\{t^{A,k}|t \in T_\Omega(A \cup \{x_1, x_2, \ldots, x_k\})\}$$

Note that if $R \in \mathbf{K}(\tau_{\text{ring1}})$ is a ring then the polynomial functions defined here are precisely the polynomial functions in the classical sense.

Definition 1.32 (Term functions)

$$G_k(A) := \{t^{A,k}|t \in T_\Omega(\{x_1, x_2, \ldots, x_n\})\}$$

We have called the term functions G_k because they are called like that in [LN73]. They were considered in [Gra68] and called polynomial functions there. The concept of a polynomial as it is presented in [LN73] and as we shall define it in this thesis goes back to [Hul69]. Hule's definition is a real generalization of the notion of polynomials as they are known in ring theory.

Example: Consider $\mathbf{Z} \times \mathbf{Z}$.

- $\mathbf{Z} \times \mathbf{Z}$ can be considered an element of $\mathbf{K}(\tau_{\text{ring}})$ in a fairly obvious way. Then we have:
$$P_1(\mathbf{Z} \times \mathbf{Z}) = \{x \mapsto \sum_{i=0}^{n} v_i x^i | n \in \mathbf{N}, v_i \in \mathbf{Z} \times \mathbf{Z}\}$$
$$G_1(\mathbf{Z} \times \mathbf{Z}) = \{x \mapsto \sum_{i=\mathbf{1}}^{n} z_i x^i | n \in \mathbf{N}, z_i \in \mathbf{Z}\}$$
- $\mathbf{Z} \times \mathbf{Z}$ can also be considered as an element of $\mathbf{K}(\tau_{\text{ring1}})$. Then we get for $P_1(\mathbf{Z} \times \mathbf{Z})$ the same as before, but for $G_1(\mathbf{Z} \times \mathbf{Z})$ we get
$$G_1(\mathbf{Z} \times \mathbf{Z}) = \{x \mapsto \sum_{i=\mathbf{0}}^{n} z_i x^i | n \in \mathbf{N}, z_i \in \mathbf{Z}\}$$

The unary functions will be the most important ones for our purposes.

Definition 1.33 (Polynomial functions)

$$P(A) := P_1(A)$$

Definition 1.34 (Compatible functions)

$$C(A) := \{\ f \ :\ A \longrightarrow A \ | f \textit{ is compatible } \}$$

Definition 1.35 (All functions)

$$M(A) := F_1(A) = A^A$$

1.3.2 Function algebras

Function algebras as homomorphic images of term algebras

For an Ω-algebra A, $F_k(A)$, $P_k(A)$ and $G_k(A)$ become Ω-algebras if we define the operations pointwisely. It turns out that

$$\begin{array}{cccc} I_{A,k} & : & T_\Omega(A \cup \{x_1, x_2, \dots, x_k\}) & \longrightarrow & F_k(A) \\ & & t & \longmapsto & t^{A,k} \end{array}$$

is a homomorphism. Then we get:
Theorem 1.36

$$P_k(A) = I_{A,k}(T_\Omega(A \cup \{x_1, x_2, \dots, x_k\}))$$

$$G_k(A) = I_{A,k}(T_\Omega(\{x_1, x_2, \dots, x_k\}))$$

Generators for the function algebras

Let $Sub(A)$ be the class of all subalgebras of A. Then we have the following relations:
Theorem 1.37

$$P_k(A) = \langle \{\lambda x_1 x_2 \dots x_k.a | a \in A\} \cup \{\lambda x_1 x_2 \dots x_k.x_i | i \in \{1, \dots, n\}\}\rangle_{Sub(F_k(A))}$$

and

$$G_k(A) = \langle \{\lambda x_1 x_2 \dots x_k.x_i | i \in \{1, \dots, n\}\}\rangle_{Sub(F_k(A))}$$

1.3.3 Composition in function algebras

It will be very useful to observe that on the function algebras, we always have one operation apart from those in Op_Ω, namely functional composition.

An example for this approach is near-ring theory: Take a group $(G, +)$ and define on

$$M(G) = \{\ f \ :\ G \longrightarrow G\ \}$$

addition pointwisely and let $\circ$ denote functional composition. The resulting structure is a *near-ring*.

The fact that some sets of functions are closed not only under the pointwise defined operations but also under functional composition will allow us to derive interesting results e.g. in interpolation theory.

It is clear how to compose two unary term functions. For other dimensions we have to introduce a concept similar to matrices.

In this section Ω will always denote a signature, A an Ω-algebra and $x_1, x_2, \ldots, x_n$ a tuple of variables.

Definition 1.38 (Term matrices) *Let $i, k \in \mathbf{N}$ and let $t_1, t_2, \ldots, t_i$ be elements of $T_\Omega(A \cup \{x_1, x_2, \ldots, x_k\})$. Then $(t_1, t_2, \ldots, t_i)$ is called a* term-matrix *of dimension $i \times k$ over A. The set of all term matrices of this dimension will be abbreviated by $T_k^i(A)$.*

Definition 1.39 (Functions induced by term matrices) *Let i, k be natural numbers and let $(t_1, t_2, \ldots, t_i) \in T_k^i(A)$ Then we define:*

$$\begin{array}{rcccc} (t_1, t_2, \ldots, t_i)^{A,k\to i} & : & A^k & \longrightarrow & A^i \\ & & (y_1, y_2, \ldots, y_k) & \longmapsto & \begin{pmatrix} {t_1}^{A,k}(y_1, y_2, \ldots, y_k) \\ {t_2}^{A,k}(y_1, y_2, \ldots, y_k) \\ \vdots \\ {t_i}^{A,k}(y_1, y_2, \ldots, y_k) \end{pmatrix} \end{array}$$

This function is called a polynomial-function-matrix *of dimension $i \times k$ over A. The set of all polynomial function matrices of this dimension will be called $P_k^i(A)$*

Example: We consider the integers $\mathbf{Z}$ as an algebra in $\mathbf{K}(\tau_{\text{ring1}})$ in the usual way. Then

$$S = \begin{pmatrix} {x_1}^2 + 6 \\ x_1 - x_2 + 8 \\ {x_2}^3 \\ x_1 x_2 \end{pmatrix}$$

is an element of $T_2^4(\mathbf{Z})$. The induced function

$$\begin{array}{rcccc} f & : & \mathbf{Z}^2 & \longrightarrow & \mathbf{Z}^4 \\ & & (y_1, y_2) & \longmapsto & \begin{pmatrix} {y_1}^2 + 6 \\ y_1 - y_2 + 8 \\ {y_2}^3 \\ y_1 y_2 \end{pmatrix} \end{array}$$

is an element of $P_2^4(\mathbf{Z})$.

Theorem 1.40 *Let A be an Ω-algebra, $n \in \mathbf{N}$. The following sets of functions are closed under functional composition:*

- $P(A)$
- $C(A)$

- $G_1(A)$
- $P_n^n(A)$

For the compatible functions, the proof is immediate. For the other structures the statement follows from the connection between

- substitution in terms and
- composition of functions

We will investigate this connection now.

1.3.4 Substitution in term algebras

Definition 1.41 (Substitution of term matrices) *Let*

$$M = (m_1, m_2, \ldots, m_i) \in T_k^i(A)$$

Each m_r is an element of $T_\Omega(A \cup (x_1, x_2, \ldots, x_k)$. Let

$$N = (n_1, n_2, \ldots, n_k) \in T_j^k(A)$$

Each n_r is an element of $T_\Omega(A \cup (x_1, x_2, \ldots, x_j)$ Then $M \Box N$ is defined by:

$$M \Box N \in T_j^i(A)$$

and

$$M \Box N := M^{T_\Omega(A \cup \{x_1, x_2, \ldots, x_j\}), k \to i}(n_1, n_2, \ldots, n_k)$$

After this definition we give a completely informal description of what we are doing.

$$\begin{pmatrix} m_1(x_1, x_2, \ldots, x_k) \\ \vdots \\ m_i(x_1, x_2, \ldots, x_k) \end{pmatrix} \Box \begin{pmatrix} n_1(x_1, x_2, \ldots, x_j) \\ \vdots \\ n_k(x_1, x_2, \ldots, x_j) \end{pmatrix} =$$

$$\begin{pmatrix} m_1(n_1(x_1, x_2, \ldots, x_j), \ldots, n_k(x_1, x_2, \ldots, x_j)) \\ \vdots \\ m_i(n_1(x_1, x_2, \ldots, x_j), \ldots, n_k(x_1, x_2, \ldots, x_j)) \end{pmatrix}$$

Example: Let $S_1 \in T_2^4$ and $S_2 \in T_3^2$ be defined by

$$S_1 = \begin{pmatrix} {x_1}^2 + 6 \\ x_1 - x_2 + 8 \\ {x_2}^3 \\ x_1 x_2 \end{pmatrix}$$

$$S_2 = \begin{pmatrix} x_1x_2x_3 \\ {x_1}^2 + {x_2}^2 + {x_3}^2 \end{pmatrix}$$

Then $S_1 \Box S_2 \in T_3^4$ is given by

$$S_1 \Box S_2 = \begin{pmatrix} (x_1x_2x_3)^2 + 6 \\ (x_1x_2x_3) - ({x_1}^2 + {x_2}^2 + {x_3}^2) + 8 \\ ({x_1}^2 + {x_2}^2 + {x_3}^2)^3 \\ (x_1x_2x_3)({x_1}^2 + {x_2}^2 + {x_3}^2) \end{pmatrix}$$

Now we have seen how we can "substitute" term matrices. In the same way, we can multiply polynomial function matrices.

Definition 1.42 (Composition of polynomial function matrices) *Let $M \in P_k^i(A)$, $N \in P_j^k(A)$. Then let*

$$M \circ N$$

be the functional composition of M and N. Note that $M \circ N$ is a function from A_j to A_i.

The relation between these two concepts is given by the following theorem.

Theorem 1.43 *Let $M \in T_k^i(A)$ and $N \in T_j^k(A)$. Then we have:*

$$(M \Box N)^{A,j \to i} = M^{A,k \to i} \circ N^{A,j \to k}$$

This theorem guarantees us that under the conditions of (theorem 1.42) we have: $M \circ N \in P_j^i$.

1.3.5 Describing generated subalgebras by term functions

Let A be an Ω-algebra and let $S \subseteq A$. Then

$$\langle S \rangle_{Sub(A)} = \bigcup_{i \in \mathbf{N}_0} \{t^{A,i}(s_1, s_2, \ldots, s_i) | t \in T_\Omega(\{x_1, x_2, \ldots, x_i\}), s_1, s_2, \ldots, s_i \in S\}$$

For an important class of algebras, namely Ω-groups, we will get a similar characterization of the ideals. We have talked a lot about polynomial functions now. Thus we have to answer one important question: *What is a polynomial ?*

1.4 Polynomials

1.4.1 When do two terms induce the same function ?

We consider the field $\mathbf{Z}_5 = GF(5)$ as an element of $\mathbf{K}(\tau_{\text{ring1}})$. Then we note that the following pairs of terms in $T_{\tau_{\text{ring1}}}(\mathbf{Z}_5 \cup \{x\})$ induce the same functions on $\mathbf{Z}_5$. We will write terms in infix notation and with the usual parentheses.

1.
   - $(x+x^2)\cdot x$ and x^2+x^3
   - $x\cdot(3x+x^2)$ and $3x^2+x^{45}+x^3-x^{45}$
2.
   - $3x+2x$ and 0
   - $(x+1)^5$ and x^5+1
3.
   - $x(x-1)(x-2)(x-3)(x-4)$ and 0

Why do these pairs induce the same functions ?

1. Both terms of the first pair in (1.) induce the same function because $\mathbf{Z}_5$ is distributive. The terms of the second pair in (1.) induce the same function because addition in $\mathbf{Z}_5$ is commutative. Note that these two pairs would induce the same functions on *any ring with 1*[5].
2. The terms of the first pair in (2.) induce the same function because of distributivity and the fact that $3+2=0$ in $\mathbf{Z}_5$. They would not induce the same function on the integers but they induce the same function on *any ring with 1 that contains* $\mathbf{Z}_5$.
3. $x(x-1)(x-2)(x-3)(x-4)$ and 0 will usually not induce the same functions on a ring, even if the ring contains $\mathbf{Z}_5$. For example they induce different functions on $GF(25)$. So we can only state: The terms induce the same function *on* $\mathbf{Z}_5$.

Hence we can say that the pairs of terms were "equivalent" on three different levels, namely

1. Both terms are elements of $T_\Omega(\{x_1,x_2,\ldots,x_n\})$ and they induce the same function on any algebra that satisfies some axioms such as distributivity. This equivalence will be dealt with in (section 1.4.3).
2. Both terms are elements of $T_\Omega(A\cup\{x_1,x_2,\ldots,x_n\})$ and they induce the same function on any algebra that contains A. This equivalence will be dealt with in (section 1.4.4).
3. Both terms induce the same function on A but for detecting this equality we have to look at the inner structure of A. This equivalence will be dealt with in (section 1.4.5).

We will study these three types of equivalence now. First, however, we have to define what it means that an algebra satisfies axioms such as distributivity.

[5] 3 has to be interpreted as $1+1+1$, which makes 3 an element of $T_{\tau_{\mathrm{ring1}}}(\{x\})$ and thus perfectly suitable for inducing functions in any ring with 1 you like.

1.4.2 Identities and varieties

Equations and Identities

Let Ω denote a signature and let $(x_1, x_2, \ldots)$ be a tuple of variables.

Definition 1.44 (Equations) *Let X be a set of new symbols (i.e. a set that is disjoint from Op_ω). A pair*

$$(t_1, t_2)$$

with

$$t_1, t_2 \in T_\Omega(X)$$

is called an equation *over Ω.*

Definition 1.45 (Validity of an equation) *Let A be an Ω-algebra and let (t_1, t_2) be an equation over Ω. Let $x_1, x_2, \ldots, x_n \in X$ be such that*

- $t_1, t_2 \in T_\Omega(\{x_1, x_2, \ldots, x_n\})$.
- $(x_1, x_2, \ldots, x_n)$ *is a tuple of variables (as defined in (definition 1.16)).*

Then

$$(t_1, t_2) \text{ holds in } A :\Longleftrightarrow$$
$$t_1{}^{A,n} = t_2{}^{A,n} \tag{1.4}$$

Note that (1.4) is independent of the choice of $x_1, x_2, \ldots, x_n$. Having to show things like this independence is one of the unpleasant features of universal algebra (or logic). In my view, [EM85] is unequalled in syntactical precision.

Definition 1.46 (Identities) *An* identity *of A is an equation that holds in A.*

Examples:

- $(+[x_1, x_2], +[x_2, x_1])$ is an identity of the group G iff the group is abelian.
- $(\cdot[x_1, x_1], x_1)$ is an identity of the rings $(\mathbf{Z}_2, +, \cdot)$ and $(\mathcal{P}(M), \Delta, \cap)$. (It is clear how to consider these rings as elements of $\mathbf{K}(\tau_{\text{ring}})$.)
- (x_1, x_1) is an identity of any algebra.
- (x_1, x_2) is an identity of an algebra A iff A has 0 or 1 elements.

Specifications and Varieties

Definition 1.47 (Specifications) *A* specification *is a set of equations over Ω.*

Definition 1.48 *If Σ is a specification then*

$$\mathbf{K}(\Omega, \Sigma)$$

is the class of all Ω-algebras in which all equations in Σ hold.

We will now give specifications for some classical algebraic structures.

- **Groups**

  Let Σ_{group} be the specification over τ_{group} defined by:

$$\begin{array}{rclrcl} \Sigma_{\text{group}} & := & \{ & ([x_1 + x_2] + x_3 & , & x_1 + [x_2 + x_3]), \\ & & & (0 + x_1 & , & x_1), \\ & & & (-[x_1] + x_1] & , & 0) \qquad\qquad \} \end{array}$$

- **Rings**

  Let Σ_{ring} be the specification over τ_{ring} defined by

$$\begin{array}{rclrcl} \Sigma_{\text{ring}} & := \Sigma_{\text{group}} \cup & \{ & (x_1 + x_2 & , & x_2 + x_1), \\ & & & [x_1 \cdot x_2] \cdot x_3 & , & x_1 \cdot [x_2 \cdot x_3]), \\ & & & (x_1 \cdot [x_2 + x_3] & , & [x_1 \cdot x_2] + [x_1 \cdot x_3]), \\ & & & ([x_1 + x_2] \cdot x_3 & , & [x_1 \cdot x_3] + [x_2 \cdot x_3]), \quad \} \end{array}$$

- **Commutative rings with 1**

  Let $\Sigma_{\text{c ring 1}}$ be the specification over τ_{ring1} defined by:

$$\begin{array}{rclrcl} \Sigma_{\text{c ring 1}} & := \Sigma_{\text{ring}} \cup & \{ & (x_1 \cdot x_2 & , & x_2 \cdot x_1), \\ & & & (1 \cdot x_1 & , & x_1) \qquad \} \end{array}$$

These examples are well known from classical algebra.

- $\mathbf{K}(\tau_{\text{group}}, \Sigma_{\text{group}})$ is the class of all groups.
- $\mathbf{K}(\tau_{\text{ring}}, \Sigma_{\text{ring}})$ is the class of all rings.
- $\mathbf{K}(\tau_{\text{ring1}}, \Sigma_{\text{c ring 1}})$ is the class of all commutative rings with 1.

Many interesting algebraic structures S are of the form: $(S, +)$ is a group and $(S, \cdot)$ fulfills the axioms .... We will call groups with some more operations Ω-*groups*.(cf. [Pil84])

Definition 1.49 (Ω-groups) *Let Ω be a signature such that $\{+, -, 0\} \subseteq Op_\Omega$. Then A is an Ω-group: $\Longleftrightarrow$*

1. $(A; +^A, -^A, 0^A) \in \mathbf{K}(\tau_{\text{group}}, \Sigma_{\text{group}})$
2. *For all $\omega \in Op_\Omega$ with positive arity :* $\omega^A(0^A, 0^A, \ldots, 0^A) = 0^A$

Note that we have exluded the constant operations from condition (2.). Hence, e.g. also a commutative ring with 1 is a τ_{ring1}-group.

However it is not possible to describe all classes of algebras that have been dealt with in classical algebra by a signature and a specification.

Theorem 1.50 ($\mathbf{K}(\Omega, \Sigma)$ and direct products) *Let I be a set and let A_i be in $\mathbf{K}(\Omega, \Sigma)$ for all $i \in I$. Then we have:*

$$\times_{i \in I} A_i \in \mathbf{K}(\Omega, \Sigma)$$

Corollary 1.51 *Let τ_{field} be a signature that contains τ_{ring}. Then for any Σ one of the following two statements is true:*

- *$\mathbf{K}(\tau_{\text{field}}, \Sigma)$ contains only the isomorphism classes of the τ_{field}-algebras with less than 2 elements.*
- *$\mathbf{K}(\tau_{\text{field}}, \Sigma)$ contains an algebra A with $|A| \geq 2$ (perhaps infinite) such that A is not a field.*

Proof: Suppose that $\mathbf{K}(\tau_{\text{field}}, \Sigma)$ contains an algebra A with $|A| \geq 2$. If A is not a field, we are done, otherwise $A \times A$ is not a field (zero-divisers). $\square$

Theorem 1.52 ($\mathbf{K}(\Omega, \Sigma)$ and subalgebras) *Let $A \in \mathbf{K}(\Omega, \Sigma)$ and let $B \in \mathbf{K}(\Omega)$ be a subalgebra of A. Then we have:*

$$B \in \mathbf{K}(\Omega, \Sigma)$$

Theorem 1.53 ($\mathbf{K}(\Omega, \Sigma)$ and homomorphic images) *Let $A \in \mathbf{K}(\Omega, \Sigma)$, $B \in \mathbf{K}(\Omega)$. Let $h : A \longrightarrow B$ be an Ω-epimorphism. Then we have:*

$$B \in \mathbf{K}(\Omega, \Sigma)$$

Proof: By (theorem 1.19).

Definition 1.54 (Varieties) *A subclass $\mathbf{K}$ of $\mathbf{K}(\Omega)$ is a* variety*: $\Longleftrightarrow$ the following conditions (1.), (2.) and (3.) hold.*

1. **If**
   - $A \in \mathbf{K}$
   - $B \in \mathbf{K}(\Omega)$
   - *B is a sub-Ω-algebra of A*

   then $B \in \mathbf{K}$
2. **If**
   - *I is a set*
   - *$A_i \in \mathbf{K}$ for all $i \in I$*

   then $\times_{i \in I} A_i \in \mathbf{K}$
3. **If**

- $A \in \mathbf{K}$
- $B \in \mathbf{K}(\Omega)$
- *B is a homomorphic image of A*

then $B \in \mathbf{K}$

Theorem 1.55 (Characterization of varieties) $\mathbf{K} \subseteq \mathbf{K}(\Omega)$ *is a variety* $\Longleftrightarrow$ *There is a specification Σ with $\mathbf{K} = \mathbf{K}(\Omega, \Sigma)$.*

We have proved "$\Leftarrow$". "$\Rightarrow$" is harder. The proof can be found e.g. in [Pil84].

1.4.3 Free algebras in varieties

Identities of free algebras

We will see that free algebras (if they exist) are very cautious not to have too many identities. The reason for this is the following theorem:

Theorem 1.56 (Extension of partial functions to homomorphisms) *Let $B, C \in \mathbf{K}(\Omega)$ and let I be a set and let $(b_i)_{i\in I}$ a family of elements of B and $(c_i)_{i\in I}$ a family of elements of C . Then*

$$\begin{array}{rcrcl} h & : & \{b_i | i \in I\} & \longrightarrow & \{c_i | i \in I\} \\ & & b_i & \longmapsto & c_i \end{array}$$

can be extended to a homomorphism

$$\bar{h} \ : \ \langle \{b_i | i \in I\} \rangle_{Sub(B)} \ \longrightarrow \ C$$

$\Longleftrightarrow$

$$\forall n \in \mathbf{N}$$

$$\forall t_1, t_2 \in T_\Omega(\{x_1, x_2, \ldots, x_n\})$$

$$\forall \ \varphi \ : \ \{1, 2, \ldots, n\} \ \longrightarrow \ I$$

$$t_1{}^{B,n}(b_{\varphi(1)}, b_{\varphi(2)}, \ldots, b_{\varphi(n)}) = t_2{}^{B,n}(b_{\varphi(1)}, b_{\varphi(2)}, \ldots, b_{\varphi(n)}) \Rightarrow$$
$$t_1{}^{C,n}(c_{\varphi(1)}, c_{\varphi(2)}, \ldots, c_{\varphi(n)}) = t_2{}^{C,n}(c_{\varphi(1)}, c_{\varphi(2)}, \ldots, c_{\varphi(n)})$$

Theorem 1.57 (The theory of a class of algebras) *Let X be a set of variables and let $\mathbf{K} \subseteq \mathbf{K}(\Omega)$. Then*

$$Th(\mathbf{K}) := \{(t_1, t_2) | t_1, t_2 \in T_\Omega(X) \text{ and } (t_1, t_2) \text{ is an identity of all } A \in \mathbf{K}\}$$

Theorem 1.58 *Suppose that there exists the free algebra F (as defined in (definition 1.11)) in $\mathbf{K} \subseteq \mathbf{K}(\Omega)$ over B. Let $n \in \mathbf{N}$, $t_1, t_2 \in T_\Omega(\{x_1, x_2, \ldots, x_n\})$ and let $b_1, b_2, \ldots, b_n$ be pairwise different elements of B. Then we have:*

$$t_1{}^{F,n}(b_1, b_2, \ldots, b_n) = t_2{}^{F,n}(b_1, b_2, \ldots, b_n) \Longleftrightarrow (t_1, t_2) \in Th(\mathbf{K})$$

Proof: "$\Longleftarrow$": F is in $\mathbf{K}$, thus any equation in $Th(\mathbf{K})$ holds in F. In particular, it holds for $b_1, b_2, \ldots, b_n$.

"$\Longrightarrow$": Suppose there exist $n \in \mathbf{N}$, $A \in \mathbf{K}$, $a_1, a_2, \ldots, a_n \in A$, $b_1, b_2, \ldots, b_n \in B$ with

$$t_1{}^{F,n}(b_1, b_2, \ldots, b_n) = t_2{}^{F,n}(b_1, b_2, \ldots, b_n)$$

and

$$t_1{}^{A,n}(a_1, a_2, \ldots, a_n) \neq t_2{}^{A,n}(a_1, a_2, \ldots, a_n)$$

Then, by (theorem 1.56), $b_i \mapsto a_i$ can not be extended to a homorphism, which is a contradiction to the fact that F is free.

Corollary 1.59 *Let (t_1, t_2) be an equation with $t_1, t_2 \in T_\Omega(\{x_1, x_2, \ldots, x_n\})$. Let F be free over B in $\mathbf{K}$ with $|B| \geq n$. Then we have:*

$$(t_1, t_2) \in Th(\mathbf{K}) \Leftrightarrow (t_1, t_2) \in Th(\{F\})$$

Construction of the free algebra in $\mathbf{K}(\Omega, \Sigma)$

A good candidate for the free algebra in $\mathbf{K}(\Omega, \Sigma)$ should

- satisfy all equations in Σ.
- avoid further identities.

We will construct the free algebra over X as a factor algebra of $T_\Omega(X)$. From (theorem 1.58) we get an idea which terms we should identify.

Definition 1.60 (Semantic equivalence) *Let $t_1, t_2 \in T_\Omega(X)$. Then we define:*

$$t_1 \equiv_{\text{sem}} t_2 :\Longleftrightarrow (t_1, t_2) \in Th(\mathbf{K}(\Omega, \Sigma))$$

(We can consider (t_1, t_2) as an equation if we take X as a set of variables)

This means, roughly speaking, that $t_1 \equiv_{\text{sem}} t_2$ iff for all $A \in \mathbf{K}(\Omega, \Sigma)$ and for all $a_1, a_2, \ldots, a_n \in A$:

$$t_1{}^{A,n}(a_1, a_2, \ldots, a_n) = t_2{}^{A,n}(a_1, a_2, \ldots, a_n)$$

So, two terms are *semantically equivalent* iff they "denote" the same element in any algebra A and for any substitution of the variables by elements of A.

We will call two elements $t_1, t_2 \in T_\Omega(X)$ *syntactically equivalent* if it can be proved using only using a certain *equational calculus* that in each algebra A in $\mathbf{K}(\Omega, \Sigma)$ they will denote the same element for each substitution.

Definition 1.61 (The equational calculus) *Let $\equiv_{\text{synt}}$ be the intersection of all relations S on $T_\Omega(X)$ with the following properties: (Let t, t_i range over $T_\Omega(X)$.)*

- S **contains** Σ

  $(t_1, t_2) \in \Sigma \Rightarrow (t_1, t_2) \in S$

- S **is an equivalence relation**

  - $(t, t) \in S$
  - $(t_1, t_2) \in S \Rightarrow (t_2, t_1) \in S$
  - $(t_1, t_2) \in S, (t_2, t_3) \in S \Rightarrow (t_1, t_3) \in S$

- **Substitution**

  If

  - (t_1, t_2) *in* S
  - $x_1, x_2, \ldots, x_n \in X$ *such that*
    - $t_1, t_2 \in T_\Omega(\{x_1, x_2, \ldots, x_n\})$
    - $(x_1, x_2, \ldots, x_n)$ *is a tuple of variables*
  - $r_1, r_2, \ldots, r_n \in T_\Omega(X)$

  then
  $$\left(t_1{}^{T_\Omega(X),n}\left(r_1, r_2, \ldots, r_n\right); t_2{}^{T_\Omega(X),n}\left(r_1, r_2, \ldots, r_n\right)\right)\right) \in S$$

- **Replacement**

  If

  - r *in* $T_\Omega(X)$
  - $x_1, x_2, \ldots, x_n \in X$ *such that*
    - $r \in T_\Omega(\{x_1, x_2, \ldots, x_n\})$
    - $(x_1, x_2, \ldots, x_n)$ *is a tuple of variables*
  - $s_1, s_2, \ldots, s_n, s'_1, s'_2, \ldots, s'_n \in T_\Omega(X)$
  - $\forall i : (s_i, s'_i) \in S$

  then

  $$\left(r^{T_\Omega(X),n}\left(s_1, s_2, \ldots, s_n\right); r^{T_\Omega(X),n}\left(s'_1, s'_2, \ldots, s'_n\right)\right) \in S$$

If $t_1 \equiv_{\text{synt}} t_2$ *then we call* (t_1, t_2) *a* syntactical consequence *of* Σ.

We note some nice properties of $\equiv_{\text{synt}}$:

Theorem 1.62 $\equiv_{\text{synt}}$ *is a congruence on* $T_\Omega(X)$.

Sketch of the proof: Use the property "replacement".□

Thus let's have a look at the factor-structure $T_\Omega(X)/_{\equiv_{\text{synt}}}$.

Theorem 1.63 $T_\Omega(X)/_{\equiv_{\text{synt}}} \in \mathbf{K}(\Omega, \Sigma)$

Sketch of the Proof: Use the properties: "$\Sigma \subseteq \equiv_{\text{synt}}$" and "substitution".$\Box$

We will also need the following (fairly obvious) lemma:

Theorem 1.64 *Let Θ be a congruence on $T_\Omega(X)$ and let $[t]$ denote the congruence class of t modulo Θ. Let $t \in T_\Omega(\{x_1, x_2, \ldots, x_n\})$, such that $x_1, x_2, \ldots, x_n$ qualify as a tuple of variables (definition 1.16). Then we have:*

$$t^{T_\Omega(X)/_\Theta, n}([x_1], [x_2], \ldots, [x_n]) = [t]$$

We shall now show that semantical and syntactical equivalence are the same congruence on $T_\Omega(X)$. This means that the equational calculus as introduced in (definition 1.61) is

- correct

and

- complete

The correctness part is purely technical. The fact that the equational calculus is complete means that for each equation (t_1, t_2) that holds in all $A \in \mathbf{K}(\Omega, \Sigma)$ we have $t_1 \equiv_{\text{synt}} t_2$. If we put it the other way round we can state this property as: If $t_1 \not\equiv_{\text{synt}} t_2$ then there is an algebra in $\mathbf{K}(\Omega, \Sigma)$ on which t_1 and t_2 induce different functions.

Theorem 1.65 (Correctness and completeness) *Let $t_1, t_2 \in T_\Omega(X)$. Then we have:*

$$t_1 \equiv_{\text{sem}} t_2 \Longleftrightarrow t_1 \equiv_{\text{synt}} t_2$$

We only prove the completeness, that means ("$\Rightarrow$").

Let $x_1, x_2, \ldots, x_n$ be a tuple of of variables such that t_1, t_2 are elements of $T_\Omega(\{x_1, x_2, \ldots, x_n\})$. We assume $t_1 \equiv_{\text{sem}} t_2$.

such that $x_1, x_2, \ldots, x_n$ qualify as a tuple of variables. We recall that $T_\Omega(X)/_{\equiv_{\text{synt}}} \in \mathbf{K}(\Omega, \Sigma)$. Then, by the definition of $\equiv_{\text{sem}}$ we have:

$${t_1}^{T_\Omega(X)/_{\equiv_{\text{synt}}}, n} = {t_2}^{T_\Omega(X)/_{\equiv_{\text{synt}}}, n}$$

Using (theorem 1.64) we get

$$[t_1] = {t_1}^{T_\Omega(X)/_{\equiv_{\text{synt}}}, n}([x_1], [x_2], \ldots, [x_n]) =$$

$${t_2}^{T_\Omega(X)/_{\equiv_{\text{synt}}}, n}([x_1], [x_2], \ldots, [x_n]) = [t_2]$$

Hence $[t_1] = [t_2]$. $\Box$

(Theorem 1.65) implies that $\equiv_{\text{synt}}$ is actually independent of the equations we use for defining the variety.

Corollary 1.66 *If* $\mathbf{K}(\Omega, \Sigma) = \mathbf{K}(\Omega, \Sigma')$ *then we get the same* $\equiv_{\text{synt}}$ *from* Σ *and* Σ'.

The structure $T_\Omega(X)/_{\equiv_{\text{synt}}}$ is so important that we shall give it a name.

Definition 1.67

$$\mathit{Free}(X, \Omega, \Sigma) := T_\Omega(X)/_{\equiv_{\text{synt}}}$$

Let's investigate when two elements of the basis can be equivalent.

Theorem 1.68 *There are* $x_1, x_2 \in X$, $x_1 \neq x_2$ *and* $[x_1] = [x_2] \Leftrightarrow \mathbf{K}(\Omega, \Sigma)$ *contains only algebras* A *with* $|A| \leq 1$.

"$\Rightarrow$":$x_1 \equiv_{\text{sem}} x_2$ means that in any algebra $A \in \mathbf{K}(\Omega, \Sigma)$ we have $a_1 = a_2$ for all $a_1, a_2 \in A$. Hence A contains at most one element.

"$\Leftarrow$": (x_1, x_2) holds in all algebras with less than two elements, hence we have $x_1 \equiv_{\text{sem}} x_2$. $\square$

Definition 1.69 (Degenerate varieties) *A variety* $\mathbf{K}$ *which contains only algebras with less than two elements is called* degenerate.

We justify the name "free" with the following proposition.

Theorem 1.70 $\mathit{Free}(X, \Omega, \Sigma)$ *is free over* X *in* $\mathbf{K}(\Omega, \Sigma)$.

Sketch of the proof: For degenerate varieties, the property is clear, so assume that $\mathbf{K}(\Omega, \Sigma)$ is not degenerate. We have $\text{Free}(X, \Omega, \Sigma) \in \mathbf{K}(\Omega, \Sigma)$ by (theorem 1.63). Let $A \in \mathbf{K}(\Omega, \Sigma)$ and let

$$\begin{array}{rclcl} h & : & \{[x_1], [x_2], \ldots, [x_n]\} & \longrightarrow & A \\ & & [x_i] & \longmapsto & a_i \end{array}$$

We recall that by (theorem 1.56) and (theorem 1.65) we can extend h to a homomorphism

$$\bar{h} \;:\; \text{Free}(X, \Omega, \Sigma) \;\longrightarrow\; A$$

The extension is unique due to an argument very similar to (theorem 1.19).

The congruence $\equiv_{\text{synt}}$ was precisely the equivalence mentioned in (1.) of the enumeration in (section 1.4.1). In the next section, we shall deal with (2.)

1.4.4 Polynomials

Polynomials as free algebras

In this section we shall define the algebra of polynomials over an algebra A with variables X in a variety $\mathcal{V} = \mathbf{K}(\Omega, \Sigma)$. We will call it $A[X, \mathcal{V}]$. We will construct it as a factor structure of $T_\Omega(A \cup X)$. According to (2.) of the enumeration in (section cleverEnum), two terms shall be equivalent iff they denote the same element in any $\mathcal{V}$-extension of A. However, we do not have to make a new term construction of the polynomial algebra, as we did it for the free algebra, but we will just use the work we have already done. In order to do this, we will define a new variety that contains the extensions of A. We will omit obvious conditions such as $A \cap X = \emptyset$.

Definition 1.71 *Let Ω be a signature, Σ be a specification and let $A \in \mathbf{K}(\Omega, \Sigma)$. Then we define a new signature Ω^A by:*

$$Op_{\Omega^A} := \Omega \cup \{\bar{a} | a \in A\}$$

$$Ar_{\Omega^A} := \begin{cases} Ar_\Omega(\omega) & \text{for } \omega \in Op_\Omega \\ 0 & \text{for } \bar{a} \text{ with } a \in A \end{cases}$$

We define a new specification Σ^A by:

$$\begin{aligned} \Sigma^A := \Sigma \cup \\ & \{\left(\omega[\bar{a}_1, \bar{a}_2, \ldots \overline{a_{Ar_\Omega(\omega)}}]\, ,\ \bar{a}\right) | \\ & \omega \in Op_\Omega; a, a_1, a_2, \ldots, a_{Ar_\Omega(\omega)} \in A; \omega^A(a_1, a_2, \ldots, a_{Ar_\Omega(\omega)}) = a\} \end{aligned}$$

We shall call the resulting variety $\mathbf{K}(\Omega^A, \Sigma^A) =: \mathcal{V}^A$.

Theorem 1.72 *Let $B \in \mathcal{V}$ such that A is a subalgebra of B. Then*

$$B \in \mathcal{V}^A$$

if we define

$$\bar{a}() := a$$

for all $a \in A$.

Definition 1.73 (Polynomials)

$$A[X, \mathcal{V}] := \mathit{Free}(X, \Omega^A, \Sigma^A)$$

$A[X, \mathcal{V}]$ is called the algebra of polynomials over A with variables X.

If $X = \{x_1, x_2, \ldots, x_n\}$ (with x_i pairwise different) then we will write $A[x_1, x_2, \ldots, x_n; \mathcal{V}]$ for $A[X, \mathcal{V}]$.

By (definition 1.73), every polynomial is an equivalence class of terms in $T_{\Omega^A}(X)$ $= T_\Omega(\{\bar{a}|a \in A\} \cup X)$. It is clear how $T_\Omega(\{\bar{a}|a \in A\} \cup X)$ can be identified with $T_\Omega(A \cup X)$. In the (section 1.4.5) we will consider a polynomial as an equivalence class of terms in $T_\Omega(A \cup X)$.

Next, we shall see when it can happen that two different elements in $\{\bar{a}|a \in A\} \cup X$ are in the same equivalence class. This can only happen for special algebras in special varieties.

Degeneracies of the polynomial algebra

Definition 1.74 (Semi-degenerate varieties) *A variety $\mathcal{V}$ is* semi-degenerate*: $\iff$ There is an algebra $A \in \mathcal{V}$ such that $\mathcal{V}^A$ is degenerate.*

In this case we get: $|A| \in \{0, 1\}$ since $A \in \mathcal{V}^A$. If $A = \emptyset$ then $\mathcal{V} = \mathcal{V}^A$. Hence in the interesting examples of semi-degenerate varieties, $|A|$ will always be 1.

Theorem 1.75 *$\mathcal{V}^A$ is degenerate $\Longleftrightarrow$ $\mathcal{V}$ is degenerate* or *both of the following two conditions are true:*

1. $|A| = 1$
2. *for all $B \in \mathcal{V}$ with A sub-Ω-algebra of B:* $|B| = 1$

Actually, the most popular variety for constructing polynomials (the commutative rings with 1) is semi-degenerate.

Theorem 1.76 $\mathbf{K}(\tau_{\text{ring1}}, \Sigma_{\text{c ring 1}})$ *is semi-degenerate.*

Proof: We use (theorem 1.75). We observe that $N = \{n\}$ becomes an element of $\mathbf{K}(\tau_{\text{ring1}}, \Sigma_{\text{c ring 1}})$ if we define $n +^N n = n -^N n = n \cdot^N n = 0^N = 1^N := n$. Let S be an element of $\mathbf{K}(\tau_{\text{ring1}}, \Sigma_{\text{c ring 1}})$ such that N is a sub-τ_{ring1}-algebra of S. First, we observe that $s \cdot^S 0^S = 0^S$ holds for any $s \in S$, because the equation $([x \cdot 0], 0)$ is a syntactical consequence of $\Sigma_{\text{c ring 1}}$. Since N is a subalgebra of S, we furthermore have $s = s \cdot 1^S = s \cdot 1^N = s \cdot n = s \cdot 0^N = s \cdot 0^S = 0^S$ for any $s \in S$. Hence $|S| = 1$, which we wanted to prove. □

Theorem 1.77 *Let $\mathcal{V}$ be a non-degenerate variety. Then if there are two elements $z_1, z_2 \in A \cup X$ with $z_1 \neq z_2$ and $[z_1] = [z_2]$ in $A[X, \mathcal{V}]$, then $\mathcal{V}$ is semi-degenerate and $|A| = 1$.*

Proof: By (theorem 1.68) we know that $\mathcal{V}^A$ contains only algebras with less than 2 elements, that means it is degenerate. Hence $\mathcal{V}$ is semi-degenerate by (definition 1.74). We get $|A| = 1$ from (theorem 1.75).

Theorem 1.78 *$\mathcal{V}$ is semi-degenerate and $|A| = 1 \Rightarrow$ For all elements z_1, z_2 in $A \cup X$ we have: $[z_1] = [z_2]$ in $A[X, \mathcal{V}]$*

Proof: Since A has only one element, the mapping

$$\begin{array}{cccc} h : & A & \longrightarrow & A[X, \mathcal{V}] \\ & a & \longmapsto & [a] \end{array}$$

is an embedding. Hence

$$A[X, \mathcal{V}] \in \mathcal{V}^A$$

which implies $|A[X, \mathcal{V}]| = 1$.

[LN73] remarks that

> in all examples for semi-degenerate varieties we know, semi-degeneracy is due to 0-ary operations. We do not know whether or not the existence of 0-ary operations is a necessary condition for semi-degeneracy.

If universal algebras give you a hard time, go over to lovely Ω-groups.

Theorem 1.79 *Let $\mathcal{V} = \mathbf{K}(\Omega, \Sigma)$ be a non-degenerate variety of Ω-groups such that 0 is the only $\omega \in Op_\Omega$ with $Ar_\Omega(\omega) = 0$. Then $\mathcal{V}$ is not semi-degenerate.*

Proof: Let $A \in \mathcal{V}$, $|A| = 1$. By (theorem 1.72) it is sufficient to show that there is an algebra B with $|B| \geq 2$ such that A can be embedded into B. Let B be any algebra in $\mathcal{V}$ with two or more elements. We show that

$$\begin{array}{rcccc} h & : & A & \longrightarrow & B \\ & & 0^A & \longmapsto & 0^B \end{array}$$

is an embedding. From the definition of Ω-groups (definition 1.49) we get that h fulfills the homomorphism-property for operations with positive arity. Since there is only one nullary operation, namely 0 and since for this operation we have $h(0^A) = 0^B$, h is actually a homomorphism.

Diagram properties of the algebra of polynomials

In this section, we will characterize the algebra of polynomials $A[X, \mathcal{V}]$ by diagram properties which are very similar to those of (definition 1.11). Throughout this section let $\mathcal{V} = \mathbf{K}(\Omega, \Sigma)$,

$$\begin{array}{rcccc} i_{A \to A[X,\mathcal{V}]} & : & A & \longrightarrow & A[X, \mathcal{V}] \\ & & a & \longmapsto & [a] \end{array}$$

and let

$$\begin{array}{rcccc} i_{X \to A[X,\mathcal{V}]} & : & X & \longrightarrow & A[X, \mathcal{V}] \\ & & x & \longmapsto & [x] \end{array}$$

Note that $i_{A \to A[X,\mathcal{V}]}$ is always injective. If A is a subalgebra of B, then let $\iota_{A \to B}$ be the canonical injection of A into B.

Theorem 1.80 *If*

- $A, B \in \mathcal{V}$, *B is an extension of A*
- *φ is an arbitrary mapping from X to B*

then there exists one and only one Ω-homomorphism

$$h \; : \; A[X, \mathcal{V}] \longrightarrow B$$

such that the following diagram commutes.

$$\begin{tikzcd}
A \arrow[d, "i_{A\to A[X,\mathcal{V}]}"] \arrow[dr, "\iota_{A\to B}"] & \\
A[X;\mathcal{V}] \arrow[r, "h"] & B \\
X \arrow[u, "i_{X\to A[X,\mathcal{V}]}"] \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

This property actually characterizes $A[X,\mathcal{V}]$ (up to isomorphism).

Theorem 1.81 *Let $P \in \mathcal{V}$, $h_{A\to P}$ and $h_{X\to P}$ be such that*

- *$h_{A\to P}$ is an Ω-homomomorphism from A to P*
- *$h_{X\to P}$ is an arbitrary mapping from X to P*

If for any extension $B \in \mathcal{V}$ of A and for any function $\varphi : X \longrightarrow B$ there is one and only one Ω-homomorphism $h : P \longrightarrow B$ such that the following diagram commutes, then P is Ω-isomorphic to $A[X,\mathcal{V}]$.

$$\begin{tikzcd}
A \arrow[d, "h_{A\to P}"] \arrow[dr, "\iota_{A\to B}"] & \\
P \arrow[r, "h"] & B \\
X \arrow[u, "h_{X\to P}"] \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

The next proposition shows that the polynomial algebra is really what we looked for in (2.) of (section 1.4.1).

Theorem 1.82 *Let $A \in \mathcal{V}$, $t_1, t_2 \in T_\Omega(A \cup \{x_1, x_2, \ldots, x_n\})$. Then we have: $[t_1] = [t_2] \iff$ For each $\mathcal{V}$-extension B of A we have ${t_1}^{B,n} = {t_2}^{B,n}$.*

1.4.5 Polynomials and polynomial functions

Definition 1.83 (Function induced by a polynomial) *Let $p \in A[x_1, x_2, \ldots, x_n; \mathcal{V}]$. Then we define*

$$\begin{array}{rcccl} I^{pol}_{A,n} & : & A[x_1, x_2, \ldots, x_n; \mathcal{V}] & \longrightarrow & F_n(A) \\ & & p = [t] & \longmapsto & t^{A,n} \end{array}$$

We will abbreviate $I^{pol}_{A,n}(p)$ by $\bar{p}$.

From "$\Rightarrow$" of (theorem 1.82) we see that $I^{pol}_{A,n}$ is well-defined. It is obvious that

$$I^{pol}_{A,n}(A[x_1, x_2, \ldots, x_n; \mathcal{V}]) = P_n(A)$$

Polynomially n-complete algebras

We will call an algebra n-polynomially complete iff every function from A^n to A is a polynomial function.

Definition 1.84 *A is n-polynomially complete: $\Longleftrightarrow P_n(A) = F_n(A)$*

If A is 1-polynomially complete we shall simply say that A is polynomially complete. The proofs of the next two theorems can be found in [LN73].

Theorem 1.85 *If A is n-polynomially complete and $m \leq n$ then A is m-polynomially complete.*

Theorem 1.86 *If A is 2-polynomially complete then A is n-polynomially complete for all $n \in \mathbf{N}$.*

So, any algebra A has to fall into precisely one of the following cases.

1. A is not 1-polynomially complete
2. A is 1-polynomially complete, but not 2-polynomially complete
3. A is n-polynomially complete for all $n \in \mathbf{N}$.

We will see in (section 4.5.1) that for Ω-groups case (2.) almost never occurs.

From the fact that polynomial functions respect congruences on A, (cf. (theorem 1.29)) we get

Theorem 1.87 *If A is polynomially complete then A is simple.*

In (section 4.3.7) we will get characterizations of polynomially complete rings, near-rings and groups.

An algebra A is n-polynomially complete iff $I^{pol}_{A,n}$ is surjective. We will now investigate when $I^{pol}_{A,n}$ is injective.

Functionally distinguishable polynomials

We will call an algebra A k-functionally distinguishable iff A has the property: p and q induce the same k-place function $\Rightarrow$ p and q are equal as polynomials.

Definition 1.88 *A is k-functionally distinguishable:* $\Longleftrightarrow$

$$I^{pol}_{A,k} \quad : \quad A[x_1, x_2, \ldots, x_k; \mathcal{V}] \quad \longrightarrow \quad F_k(A)$$

is injective.

Theorem 1.89 *If A is n-functionally distinguishable and $m \leq n$ then A is m-functionally distinguishable.*

Sketch of the proof: $A[x_1, x_2, \ldots, x_m; \mathcal{V}]$ can be embedded into $A[x_1, x_2, \ldots, x_n; \mathcal{V}]$ in the natural way. Let $i_{m \to n}$ be the embedding function. Since

$$I^{pol}_{A,m} = I^{pol}_{A,n} \circ i_{m \to n},$$

$I^{pol}_{A,m}$ is injective.

1.4.6 Substitution of polynomials

We will define an operation $\triangle$ on $A[x; \mathcal{V}]$ which corresponds to (definition 1.41). We restrict ourselves to univariate polynomials.

Definition 1.90 (Substitution of polynomials) *Let $[t_1], [t_2] \in A[x; \mathcal{V}]$. Then we define $[t_1] \triangle [t_2]$ by*

$$[t_1] \triangle [t_2] := [{t_1}^{T_\Omega(A \cup \{x\}),1}(t_2)](= [t_1 \Box t_2])$$

This definition is ok because of the theorems (theorem 1.82) and (theorem 1.29).

The result that corresponds to (theorem 1.43) is the following proposition.

Definition 1.91 *Let $p, q \in A[x, \mathcal{V}]$.*

$$I^{pol}_{A,1}(p \triangle q) = I^{pol}_{A,1}(p) \circ I^{pol}_{A,1}(q)$$

Hence $I^{pol}_{A,n}$ is not only an Ω-homomorphism, but also a composition homomorphism. The proof can be done using (theorem 1.43) or directly, using induction on the length of the shortest word representing p.

1.5 Literature and Sources

[Pil84] provides an introduction to universal algebra. He presents the term-construction of free algebras, the complete proof of the characterization of varieties by their closure properties and the proof of the completeness of the equational calculus which is due to [Bir35]. [EM85] give the following idea of implementing abstract data-types: The *programmer* provides only a signature and a specification defining the data-type. They then line out how one can actually compute with the thereby defined data-type. Hence, instead of implementing a function by a procedure the function is implemented by its mathematical properties. There are already programming languages (algebraic specification languages) that use this approach, as for example OBJ3 (see [GW88]).[EM85] also give an introduction to universal algebra, e.g. they give the term construction of the free algebra in a variety and the proof of the completeness of the equational calculus. I like their presentation because everything is presented in full detail. They bother about all syntactical problems arising from the presentation of universal algebra, which is indispensible for using the material in computer implementations. The approach presented in [EM85] is also more general than the approach of [Bir35], because they use "types" for terms similar to data-types in programming languages. In the language of algebra, this means that they use *many-sorted algebras* as introduced in [BL70]. [LN73] is the standard reference on polynomials over universal algebras. Pratically the whole material presented in this chapter can be found in the sections 1–4 of chapter 1 and the sections 1–3 of chapter 3 of this book.

Chapter 2

The word problem

2.1 The problem

In the construction of the free algebras and the polynomial algebras in a variety, the relation $\equiv_{\text{synt}}$ played an important role (cf. (definition 1.61)). We recall that given a specification Σ and an equation (t_1, t_2) we have:

$$t_1 \equiv_{\text{sem}} t_2 \iff$$

> in each algebra in which all equations in Σ hold the equation (t_1, t_2) holds as well.

We shall also write

$$\Sigma \models (t_1, t_2)$$

for $t_1 \equiv_{\text{sem}} t_2$. In this case we know that there is a proof in the equational calculus which shows that (t_1, t_2) is a consequence of Σ. However, in general we can not find this proof algorithmically. The following problem is called the *word problem* for a variety $\mathbf{K}(\Omega, \Sigma)$.

- **Given** An equation (t_1, t_2)
- **Asked** Is $\Sigma \models (t_1, t_2)$ true or false ?

2.2 Normal forms

2.2.1 Deciding equivalence by computing normal forms

Definition 2.1 (Normal forms) *Let T be a set and let $\equiv$ be an equivalence relation on T. Then N is a set of normal forms of T for the relation $\equiv$: $\iff$ N contains precisely one element of each equivalence class.*

So for each equivalence relation on T there exists a set of normal forms. Now suppose that N is a set of normal forms of T for the relation $\equiv$. Then for each $t \in T$, let $NF(t)$ denote the $n \in N$ such that $t \equiv n$. If we find a set of normal forms such that the function NF can be computed by an algorithm then we can decide by an algorithm whether two elements of T are equivalent[1] .

2.2.2 Normal forms for polynomials

We will give normal forms for polynomials over groups and rings (cf.[LN73]).

Abelian groups

Let $\Omega := \tau_{\text{group}}$ and let $\Sigma := \Sigma_{\text{group}} \cup \{(+[x_1, x_2], +[x_2, x_1])\}$. We will write the terms in a more readable form by

- using normal parentheses and commas
- writing $x_1 + x_2 + x_3$ for $+(x_1, +(x_2, x_3))$
- writing zx_1 with $z \in \mathbf{Z}$ with the following meaning:

$$zx_1 := \begin{cases} \underbrace{x_1 + x_1 + \cdots + x_1}_{z \text{ times}} & \text{for} \quad z \geq 0 \\ \underbrace{(-x_1) + (-x_1) + \cdots + (-x_1)}_{-z \text{ times}} & \text{for} \quad z < 0 \end{cases}$$

Let G be an abelian group. Then the following set N_{Ab} is a set of normal forms for $G[x_1, x_2, \ldots, x_n; \mathbf{K}(\Omega, \Sigma)]$.

$$N_{Ab} := \{g + z_1x_1 + z_2x_2 + \cdots + z_nx_n \,|\, g \in G,\, z_1, z_2, \ldots, z_n \in \mathbf{Z}\}$$

Groups

We will keep the comfortable way of writing terms. Let G be a group. Then the following set N is a set of normal forms for $G[x; \mathbf{K}(\tau_{\text{group}}, \Sigma_{\text{group}})]$.

$$N := \{a_0 + z_1x + a_1 + z_2x + \cdots + a_{r-1} + z_rx + a_r |$$
$$r \geq 0; z_1, z_2, \ldots, z_r \in \mathbf{Z} \setminus \{0\};$$
$$a_0, a_1, \ldots, a_r \in G; a_t \neq 0 \text{ for } t \in \{1, 2, \ldots, r-1\}\}$$

From this set of normal forms we also get a set of normal forms for

$$G[x_1, x_2, \ldots, x_k; \mathbf{K}(\tau_{\text{group}}, \Sigma_{\text{group}})].$$

This is because $A[X \cup Y, \mathcal{V}]$ is isomorphic in a natural way to $(A[X, \mathcal{V}])[Y, \mathcal{V}]$[2].

[1] [LN73] claim already in the definition of normal forms that for each $t \in T$, "it is possible to find" $NF(t)$ "in finitely many steps".

[2] Theorem (4.6.) of the first chapter of [LN73]

Commutative rings with 1

Let R be a commutative ring with 1. Then we obtain the following normal forms for $R[x; \mathbf{K}(\tau_{\text{ring1}}, \Sigma_{\text{c ring 1}})]$:

$$N := \{\sum_{i=0}^{n} r_i \cdot x^i \mid n \in \mathbf{N}_0,\ r_1, r_2, \ldots, r_n \in R, r_n \neq 0\} \cup \{0\}$$

2.3 An informal introduction to rewriting

I will not explain the concepts of rewriting and algebraic simplification in this section. I warmly recommend [Buc82] as a survey on these topics. Furthermore, [Jou87] is entirely devoted to rewriting.

However, I will try to give some ideas of rewriting in a very informal way.

Let's consider an example. Let Ω consist only of the binary symbol * and let

$$\Sigma := \{(x_1 * x_2) * x_3; x_1 * (x_2 * x_3)\}$$

Then we see immediately that

$$((a * b) * c) * d \equiv (a * (b * c)) * d$$

in $\text{Free}(\{a, b, c, d\}, \Omega, \Sigma)$. An algorithm for deciding the word problem of $\mathbf{K}(\Omega, \Sigma)$ would be the following:

- **Input** $t_1, t_2 \in T_\Omega(X)$
- **Output** *True* iff $t_1 \equiv t_2$ in $\text{Free}(X, \Omega, \Sigma)$
- **Algorithm**
  1. Move all parentheses of t_1 to the right. Let $S(t_1)$ be the result of this operation.
  2. Move all parentheses of t_2 to the right. Let $S(t_2)$ be the result of this operation.
  3. Return *True* iff $S(t_1) = S(t_2)$

In the language of rewriting, step (1.) of the algorithm can be stated as: Simplify t_1 applying the rule

$$(x_1 * x_2) * x_3 \rightarrow x_1 * (x_2 * x_3)$$

The following strategy

1. Transform all equations of Σ (t_1, t_2) into rewrite rules $t_1 \rightarrow t_2$

2. Use the resulting rewrite system as a decision algorithm for the word problem

does obviously not work for many reasons:

1. The rewrite system that arises from transforming the equations into rewrite rules might be non-terminating, that means that there might be terms for which the simplification process never stops. (Termination)
2. Let $S(t)$ be the simplified form of t. Then we want to have $S(t_1) = S(t_2) \Leftrightarrow t_1 \equiv t_2$. We always have $\Rightarrow$, but $\Leftarrow$ is a serious problem. (Completeness)

We could try to settle these problems in the following way:

1. Use rules $l \to r$, such that r is simpler (e.g. shorter, ...) than l.
2. In [KB67] a procedure is given which tries to change a rewrite system R into a rewrite system R' such that $\Leftarrow$ is also fulfilled. This procedure is called the Knuth-Bendix procedure. It is successful in many cases (cf. [Geh92]).

   Actually, [KB67] says that for a given rewrite system $\forall t_1, t_2 \in T : t_1 \equiv t_2 \Rightarrow S(t_1) = S(t_2)$ holds if it holds for some interesting choices of (t_1, t_2). These choices are called the critical pairs.

The first condition seems to guarantee that the rewrite system is terminating. This approach has the following drawbacks.

- It needs to be defined what it means for a rule $l \to r$ that r is "simpler" than l.
- There is no algorithm that tells for each rewrite system whether it is terminating or not[3].

Actually, it might be quite hard even for a human to prove that a given rewrite system is terminating.

The Knuth-Bendix procedure has many limitations as well:

- The Knuth-Bendix procedure might keep producing new rewrite rules forever.
- Even if the Knuth-Bendix procedure stops with a finite number of rewrite rules, the resulting rewrite system might be non-terminating.

Rewrite systems in the sense of [KB67] cannot deal with axioms such as commutativity, because a rule like $x_1 + x_2 \to x_2 + x_1$ causes a rewrite system to be non terminating. $(a + b \to b + a \to a + b \to b + a \to \cdots)$ See [Fag87] if you want to know how such problems can be treated by rewriting techniques.

Despite of all these problems, in the theory of near-rings the Knuth-Bendix procedure yields a rewrite system R with the nice property that R decides the word problem for near-rings.

[3] Termination of rewrite systems is an undecidable problem.

2.4 A canonical system for near-rings

2.4.1 Introduction

After giving the definition of a near-ring, we will give a rewrite system deciding the word-problem for near-rings. It has been obtained using the critical pair algorithm by Knuth and Bendix[KB67]. I have implemented this algorithm in Modula 2. The implementation follows the presentation in [Buc82]. My implementation does not take account of improvements and generalizations of the Knuth-Bendix method that have been done since 1967. In the appendix, I show how the program completes the group axioms and the near-ring-axioms. It has always fascinated me how the program derives *automatically* from the group axioms

1. $(x + y) + z = x + (y + z)$
2. $0 + x = x$
3. $(-x) + x = 0$

the identities

$$x + 0 = x$$

and

$$x + (-x) = 0.$$

The termination of the resulting rewrite system for near-rings was proved extending the termination proof of a canonical rewrite systems for groups given in [HO80]. This extension has been done by my colleague Wolfgang Stöcher.

2.4.2 Near-rings

Definition 2.2 (Near-rings) *A set N together with two binary operations $+$ and $\circ$ is a* near-ring*:* $\iff$

1. *$(N, +)$ is a group*
2. *$(x \circ y) \circ z = x \circ (y \circ z)$ for all $x, y, z \in N$*
3. *$(x + y) \circ z = x \circ z + y \circ z$ for all $x, y, z \in N$*

So, in contrast to rings, the additive group does not have to be abelian and we claim only one distributive law.

2.4.3 Completion of the near-ring axioms

The problem

The following set of equations is a specification for the variety of nearrings. Note that we use three operations: $\circ$ (binary), $-$ (unary), 0 (nullary).

1. $0 + x_1 = x_1$
2. $-(x_1) + x_1 = 0$
3. $(x_1 + x_2) + x_3 = x_1 + (x_2 + x_3)$
4. $(x_1 \circ x_2) \circ x_3 = x_1 \circ (x_2 \circ x_3)$
5. $(x_1 + x_2) \circ x_3 = x_1 \circ x_3 + x_2 \circ x_3$

Interpreting these axioms as rewrite rules we obtain a rewrite system which is not canonical. (For example, $0 \circ x$ and 0 are both irreducible. However, $0 \circ x = 0$ holds in the theory of near-rings.) Thus we try to complete it using the Knuth-Bendix procedure.

The solution

We are lucky. The programm stops with success (i.e. all critical pairs have a common successor), giving the following candidate for a complete rewrite system:

1. $0 + x_1 \to x_1$
2. $-(x_1) + x_1 \to 0$
3. $(x_1 + x_2) + x_3 \to x_1 + (x_2 + x_3)$
4. $(x_1 \circ x_2) \circ x_3 \to x_1 \circ (x_2 \circ x_3)$
5. $(x_1 + x_2) \circ x_3 \to x_1 \circ x_3 + x_2 \circ x_3$
6. $(-x_1) + (x_1 + x_2) \to x_2$
7. $-0 \to 0$
8. $x_1 + 0 \to x_1$
9. $-(-x_1) \to x_1$
10. $x_1 + (-x_1) \to 0$
11. $x_1 + (-(x_1) + x_2) \to x_2$
12. $0 \circ x_1 \to 0$
13. $-(x_1 + x_2) \to (-x_2) + (-x_1)$
14. $(-x_1) \circ x_2 \to -(x_1 \circ x_2)$

The strategy

We have implemented the critical pair completion algorithm mainly the way it is presented in [Buc82].In addition, we always keep the rules reduced with respect to each other. Critical pairs are reduced as much as possible when they are computed. However, we have to explain how we coped with the two "non-deterministic" parts of the algorithm, namely

1. Choice of the critical pair to be added as a rule
2. Ordering of the new rule to guarantee termination

Choice of the critical pair

Already Knuth and Bendix [KB67] remark that it is vital for the effectiveness and efficiency of the algorithm to choose "small" critical pairs first. Whenever we compute a new critical pair, after reducing it we compute a measure of the size of the critical pair as follows:

$$\mathrm{Size}((p,q)) := \max(\mathrm{Size}(p), \mathrm{Size}(q)),$$

where Size is defined recursively:

- $\mathrm{Size}(v) := 3$ if v is a variable
- $\mathrm{Size}(0) := 1$
- $\mathrm{Size}(-t) := \mathrm{Size}(t) + 3$
- $\mathrm{Size}(t_1 + t_2) = \mathrm{Size}(t_1 \circ t_2) := \mathrm{Size}(t_1)+\mathrm{Size}(t_2) + 4$

Ordering of a rule

Given p, q, we have to decide whether $p \to q$ or $q \to p$ should be added as a rule. Often, only one direction is possible, e.g. if p contains a variable not contained in q.

Our program requires as input an ordering of the operation symbols. The intuition is that a symbol with lower order should drop inside a symbol with higher order during simplification. For instance $p = (-x_1) \circ x_2$, $q = -(x_1 \circ x_2)$ gets ordered $p \to q$ if $\circ < -$ because $\circ$ should drop inside $-$.In the program, this is realized as follows: Let t be a term.Let s_1, s_2 be two operation symbols. (s_1, s_2 is a pair of misplaced symbols if s_1 is contained in the subterm rooted as s_2, but $s_1 > s_2$. We add the rule $p \to q$ if p contains more misplaced symbols than q, else we add $q \to p$.

We admit that these strategies are ad-hoc heuristics for dealing with the "non-deterministic" parts of the Knuth-Bendix procedure. That is why we did not explain them too rigorously. Surprisingly enough, the resulting rewrite system is actually terminating. We prove this in the following section.

Termination

We use the *increasing interpretation method* described in [HO80] or [Der87]. We define a function V from the set of all near-ring–terms to $\{3, 4, 5, \ldots\}$ in the following way:

- $V(0) := V_0$
- $V(-t_1) := V_-(V(t_1))$
- $V(t_1 + t_2) := V_+(V(t_1), V(t_2))$
- $V(t_1 \circ t_2) := V_\circ(V(t_1), V(t_2))$
- $V(v) := V_0$ if v is a constant,

where

- $V_-(x) := x^2$
- $V_+(x, y) := x(1 + 2y)$

So far, everything is as in [HO80].

- $V_\circ(x, y) := y^x$
- $V_0 := 3$

Now we prove:

1. $V_0, V_-, V_+, V_\circ$ are strictly monotonous in each argument. A function
$$f \quad : \quad \mathbf{Z}^n \quad \longrightarrow \quad \mathbf{Z}$$
with $n \in \mathbf{N}_0$ is strictly monotonous iff for all $z_1, z_2, \ldots, z_n$, for all $i \in \mathbf{N}$ and for all $a, b \in \mathbf{Z}$ with $a < b$ we have:
$$f(z_1, z_2, \ldots, z_{i-1}, a, z_{i+1}, \ldots) < f(z_1, z_2, \ldots, z_{i-1}, b, z_{i+1}, \ldots)$$
2. $V(t) \geq 3$ for all terms t
3. For all substitutions σ and for each rule $l \to r$ we have $V(\sigma(l)) > V(\sigma(r))$.

(1.) and (2.) can easily be verified. Proof of (3.): Let σ be arbitrary but fixed and let $x := V(\sigma(x_1))$, $y := V(\sigma(x_2))$, $z := V(\sigma(x_3))$. Thus we only investigate the rules containing 0 or $\circ$.

- $0 + x_1 \to x_1$: We have to prove $3(1 + 2x) > x$. This is obvious.

- $(-x_1) + x_1 \to 0$: We have to prove $x^2(1+2x) > 3$. This is obvious.
- $(x_1 \circ x_2) \circ x_3 \to x_1 \circ (x_2 \circ x_3)$: We have to prove: $z^{(y^x)} > (z^y)^x$. Since $z > 1$ and $(z^y)^x = z^{yx}$, it is sufficient to prove that $y^x > yx$, or, equivalently, $y^{x-1} > x$. This holds because $y^{x-1} \geq 3^{x-1} = (1+2)^{x-1} \geq 1 + 2(x-1) = 2x - 1 \geq x$.
- $(x_1 + x_2) \circ x_3 \to x_1 \circ x_3 + x_2 \circ x_3$: We have to prove $z^{x(1+2y)} > z^x(1+2z^y)$, i.e. $z^{x+2xy} > z^x(1+2z^y)$. Dividing by z^x we get $z^{2xy} > 1 + 2z^y$ This holds because $z^{2xy} \geq z^{6y} = z^{5y}z^y > 3z^y \geq 1 + 2z^y$.
- $-0 \to 0$: We have to prove $3^2 > 3$. Rather easy.
- $x_1 + 0 \to x_1$: We have to prove $x(1 + 2 \cdot 3) > x$.Trivial.
- $x_1 + (-x_1) \to 0$: We have to prove $x(1 + 2x^2) > 3$.Trivial.
- $0 \circ x_1 \to 0$: We have to prove: $x^3 > 3$.Trivial.
- $(-x_1) \circ x_2 \to -(x_1 \circ x_2)$: We have to prove $y^{(x^2)} > (y^x)^2$. Since $x^2 > 2x$, this holds.

Why you should be happy about this result

The given rewriting-system for near-rings *decides* the word problem for near-rings. So, if you want to check whether $t_1 \equiv t_2$ in the free near-ring over X, then simplify both terms until you can no longer simplify them. Since the rewriting-system is terminating, this simplification will end after some time. If at some stage you could apply more than one rule, apply the one you like most. Your choice does not affect the result. (Canonical rewrite systems are that nice !) If the results of your simplification, say $S(t_1)$ and $S(t_2)$ are (syntactically) the same, then $t_1 \equiv t_2$ in the free near-ring. If $S(t_1) \neq S(t_2)$ then $t_1 \not\equiv t_2$ in the free near-ring.

2.5 Literature and sources

The literature used for this chapter has already been referred to in the exposition of the material. Furthermore, [Geh92] gives several examples how the Knuth-Bendix procedure works. (cf. Appendix A)

Chapter 3

Ω-groups, composition-Ω-groups and near-rings

3.1 Ω-groups and their ideals

We recall from (definition 1.49) that an Ω-*group* is a group Γ with further operations such that for all $\omega^\Gamma \in Op_\Omega^\Gamma$ with positive arity n we have

$$\omega^\Gamma(0, 0, \ldots, 0) = 0$$

Ω-groups allow a nice description of their congruences.

Definition 3.1 *Let G be an Ω-group. Then I is an Ω-ideal of G $:\Longleftrightarrow$*

- *I is a subgroup of G.*
- *For all $n \in \mathbf{N}$, for all $\omega \in Op_\Omega$ with $Ar_\Omega(\omega) = n$, for all $j \in \{1, 2, \ldots, n\}$ we have:*
$$\forall g_1, g_2, \ldots, g_n \in G, \forall i \in I$$
$$\omega(g_1, \ldots, g_{j-1}, g_j + i, g_{j+1}, \ldots, g_n) - \omega(g_1, \ldots, g_{j-1}, g_j, g_{j+1}, \ldots, g_n) \in I$$

Remarks:

- Note that an Ω-ideal I is also a normal subgroup of G because of $g + i - g = +(g, i) - +(g, 0)$, which is an element of I by the definition of Ω-ideals.
- An Ω-ideal I need not be an Ω-algebra. It will be always closed under $+$ and $-$, but it need not be closed under some other $\omega^G \in Op_\Omega^G$. We have already seen that in classical algebra. $2\mathbf{Z}$ is a τ_{ring1}-ideal of $\mathbf{Z}$, but not a ring with 1.

Theorem 3.2 *Let G be an Ω-group. The mapping Φ is a bijection between the ideals of G and the congruences on G.*

$$\begin{array}{rcccc} \Phi & : & \{I \mid I \ \Omega\text{-ideal of } G\} & \longrightarrow & \{R \mid R \text{ congruence on } G\} \\ & & I & \longmapsto & \equiv_I \end{array}$$

where

$$g_1 \equiv_I g_2 \text{ iff } g_1 - g_2 \in I$$

Proof: [Pil84]

The set $\mathcal{I}$ of all Ω-ideals of an Ω-group forms a Moore-system on G. Hence we can speak about the generated ideal.

Theorem 3.3 *Let G be an Ω-group and let $B \subseteq G$. Then we have:*

$$\langle B \rangle_{\Omega-\text{ideal}} =$$

$$\{\sum_{i=1}^{n} p_i(b_i) \mid n \in \mathbf{N},\, p_1(0) = \cdots = p_n(0) = 0,\, \forall i : p_i \in P(G), b_i \in B\} \tag{3.1}$$

Sketch of the proof (cf.[Pil83]):

1. Case $B = \{b\}$:
$$\{p(b) \mid p \in P(G) \text{ and } p(0) = 0\} \tag{3.2}$$
is an Ω-ideal. Since it contains B ($id \in P(G)$) we only have to show that any ideal containing B has to contain (3.2). This can be seen by the fact that polynomial functions respect all congruences (cf. (theorem 1.29)).

2. If B is not a singleton, we use the following proposition:
$$\langle B \rangle_{\Omega-\text{ideal}} = \{\sum_{i=1}^{n} c_i \mid n \in N; \forall i \, \exists b \in B : c_i \in \langle \{b\} \rangle_{\Omega-\text{ideal}} \}$$
"$\subseteq$" holds, because an ideal is always closed under $+$. Hence it is sufficient to show that the right hand side is actually an ideal. This can be done by (definition 3.1) and some telescoping.

3.2 Composition-Ω-algebras

We will introduce one additional operation on Ω-algebras. Let $\Omega_\circ$ be defined by $Op_{\Omega_\circ} = Op_\Omega \cup \{\circ\}$ and $Ar_{\Omega_\circ}(\omega) = Ar_\Omega(\omega)$ for $\omega \in Op_\Omega$, $Ar_{\Omega_\circ}(\circ) = 2$.

Definition 3.4 *An $\Omega_\circ$-algebra A is called a* composition-Ω-algebra:$\Longleftrightarrow$

1. *$(A, \circ)$ is a semi-group, i.e. the equation*
$$([x_1 \circ x_2] \circ x_3; x_1 \circ [x_2 \circ x_3])$$
holds in A.

2. *$\circ$ is right-distributive with respect to all other operations, i.e. for all $\omega \in Op_\Omega$ with $Ar_\Omega(\omega) = n \in \mathbf{N}_0$ the following equation holds in A.*

$$(\omega[x_1, x_2, \ldots, x_n] \circ x_{n+1}; \omega[x_1 \circ x_{n+1}, x_2 \circ x_{n+1}, \ldots, x_n \circ x_{n+1}])$$

Since it is quite complicated to carry the signatures wherever we go we will allow ourselves to write statements like " Let $(A, \circ)$ be a composition-Ω-algebra. ". A composition algebra $(A, \circ)$ where A is an Ω-group will be called *composition-Ω-group*.

Examples of composition-Ω-algebras (cf. (theorem 1.40)):

1. Those sub-Ω-algebras of $M(A) = \{ f : A \longrightarrow A \}$ that are closed under functional composition are composition-Ω-algebras.
2. $(T_n^n, \Box)$ is a composition-Ω-algebra.
3. For $\mathcal{V} = \mathbf{K}(\Omega, \Sigma)$, $(A[x; \mathcal{V}], \triangle)$ is a compostion Ω-algebra.
4. Near-rings (cf. (definition 2.2)) are exactly the composition-groups.

Many of the well-known algebraic structures are created by (1.). We give the following examples:

- **Rings:** Let A be an abelian group and let $End(A)$ be the set of all endomorphisms (mappings with $h(a + b) = h(a) + h(b)$) of A. $End(A)$ is closed under composition. $End(A)$ is a classical example of a ring.
- **Near-rings:** Let G be a group and let $M(G) = G^G$ (as above). Then $M(G)$ is a classical example of a near-ring.

These rings and near-rings will be called function-rings and function-near-rings resp. in the sequel.

Remarks:

- Of course the concepts of near-rings or rings seem to be something much more general than just a set of functions closed under composition because we are familiar with a lot of rings that are not function-rings. However, the characterization theory of rings and near-rings basically uses the following three-step approach:
  1. Try to consider the ring as a subdirect product of "nice" rings.
  2. If step (1.) does not work, find an ideal I of R, such that for $R/_I$ step (1.) works.
  3. Characterize "nice" rings.

The nice rings or near-rings are always special function-rings or function-near-rings, resp. Step (3.) is crucial for the whole process because it tells us which ideals we should consider in (2.). These ideals are usually called "radicals". Hence we see that function-rings are the building blocks of all rings.

In group theory, function-groups play an important role, too. However, they are usually called permutation groups there. Each permutation group $G \leq S(X)$ is a subalgebra of $(M(X) = X^X, \circ)$ where X is an algebra without any operations[1]. Most of the finite simple groups can be best described as permutation groups.

- If A is an Ω-group, it is natural to consider the sub-composition-Ω-algebras F of $M(A)$. For many results about F, we will not need the fact that F is closed under all operations in Op_Ω. Actually the most important thing is that F is a subgroup of $M(A)$ (that means that F is closed under $+$,$-$,0) and that F is closed under composition. The subalgebras F of $M(A)$ that are closed under the group operations and composition, i.e. the sub-composition-groups, are exactly the sub-near-rings of the near-ring $(M(A), +, \circ)$.

We have taken a very one-directional view to composition algebras by now. We have started from A and then talked about subalgebras of $M(A)$.

Thus, let's see it the other way round: Start with a near-ring and consider it as a near-ring of functions on some group G.

3.3 Near-rings and N-groups

Definition 3.5 *Let Γ be a group and let N be a nearring. Let*

$$* \ : \ N \times \Gamma \ \longrightarrow \ \Gamma$$

Then Γ is an N-group: $\Longleftrightarrow$

1. *$n_1 * (n_2 * \gamma) = (n_1 \circ n_2) * \gamma$ for all $n_1, n_2 \in N$, $\gamma \in \Gamma$.*
2. *$(n_1 + n_2) * \gamma = n_1 * \gamma + n_2 * \gamma$ for all $n_1, n_2 \in N$, $\gamma \in \Gamma$.*

We will also write ${}_N\Gamma$ for the N-group Γ.

Examples of N-groups:

1. Let A be an Ω-group and let $(F, +, \circ)$ be a sub-near-ring of $(M(A), +, \circ)$. Then A becomes an F-group by setting

$$f * a := f(a)$$

for $f \in F, a \in A$. Hence A can be considered as a

[1] i.e. X is a (naked) set (modulo syntactical sugar)

(a) $P(A)$-group.

(b) $C(A)$-group.

(c) $M(A)$-group.

Note that $P(A)$ depends on Ω: The more operations you allow the more functions you can build with terms. Adding operations has also a positive effect on $C(A)$: It will never transform a compatible function into a non-compatible one. Actually adding operations might give you less congruences and hence more compatible functions.

2. Let $\mathcal{V}$ be a variety of Ω-groups and let $A \in \mathcal{V}$. Then A becomes an $A[x;\mathcal{V}]$-group if we set
$$p * a := \bar{p}(a)$$
for all $p \in A[x;\mathcal{V}]$, where $\bar{p}$ denotes the induced function $I^{pol}_{A,n}(p)$.

We could also have defined N-groups in the following equivalent ways:

1. $(N, +, \circ)$ be a near-ring. Let Ω_N be given by:
$$Op_{\Omega_N} := \{+, -, 0\} \cup \{\overline{n} | n \in N\} \tag{3.3}$$
$$Ar_{\Omega_N}(+) := 2, Ar_{\Omega_N}(-) := 1, Ar_{\Omega_N}(0) := 0$$
and
$$Ar_{\Omega_N}(\overline{n}) := 1 \text{ for all } n \in N$$
We also give a specification Σ_N:
$$\Sigma_N := \Sigma_{\text{group}} \cup \{(+[\overline{n_1}[x_1], \overline{n_2}[x_1]]; \overline{n_1 + n_2}[x_1]) \,| n_1, n_2 \in N\} \cup$$
$$\{(\overline{n_1 \circ n_2}[x_1]; \overline{n_1}[\overline{n_2}[x_1]]) \,| n_1, n_2 \in N\}$$
Then G is an N-group: $\Longleftrightarrow$
$$G \in \mathbf{K}(\Omega_N, \Sigma_N)$$

2. G is an N-group: $\Longleftrightarrow$ there is a near-ring-homomorphism h with
$$h \;:\; N \longrightarrow M(G) \tag{3.4}$$
In this way, each $n \in N$ is represented by a function in $M(G)$.

Please convince yourself that you know how to translate an N-group in one sense into an N-group in another sense.

Note that an N-group as an element of $\mathbf{K}(\Omega_N, \Sigma_N)$ is by definition an Ω_N-algebra, but not necessarily an Ω_N-group. It could well be that $\overline{n}(0) \neq 0$ for some $n \in N$.

Definition 3.6 (Constants) *Let N be a near-ring. An element $n \in N$ is called a* constant*:* $\Longleftrightarrow$

$$n \circ 0^N = n$$

The set of all constants of a near-ring form a sub-near-ring of N. This nearring is called N_c.

Definition 3.7 (Zero-symmetric elements) *Let N be a near-ring. An element $n \in N$ is* zero-symmetric*:* $\Longleftrightarrow$

$$n \circ 0^N = 0^N$$

The set of all zero-symmetric elements of a near-ring form a sub-near-ring of N. This near-ring is called N_0.

Theorem 3.8 *Let N be a nearring. Then for each element $n \in N$ there is one and only one pair $(n_0, n_c) \in N_0 \times N_c$ such that*

$$n = n_0 + n_c$$

Proof: $n_0 := n - n \circ 0^N$ and $n_c := n \circ 0^N$ do the job. Uniqueness follows from the fact that $N_0 \cap N_c = \{0^N\}$.

Theorem 3.9 *Let Γ be an N-group. Then for all $n_0 \in N_0$ we have*

$$n_0 * 0^\Gamma = 0$$

For all $n_c \in N_c$ we have

$$n_c * \gamma = n_c * 0^\Gamma \text{ for all } \gamma \in \Gamma$$

Proof: We have: $0^N * \gamma = 0^\Gamma$ for all $\gamma \in \Gamma$. Therefore, we have $n_0 * 0^\Gamma = n_0 * (0^N * 0^\Gamma) = (n_0 \circ 0^N) * 0^\Gamma = 0^N * 0^\Gamma = 0^\Gamma$ and $n_c * \gamma = (n_c \circ 0^N) * \gamma = n_c * (0^N * \gamma) = n_c * 0^\Gamma$.□

Note that $n * 0^\Gamma = 0^\Gamma$ does not imply $n \in N_0$.

3.4 Ideals in near-rings and N-groups

Since a near-ring is an Ω-group (note that $0^N \circ 0^N = 0^N$), we get the following characterization of ideals of N as an application of (theorem 3.2):

Theorem 3.10 *$I \subseteq N$ is a* near-ring-ideal *of N:* $\Longleftrightarrow$

1. *$(I, +)$ is a normal subgroup of $(N, +)$.*
2. *For all $n_1, n_2 \in N$, $i \in I$ we have:*
   (a) $n_1 \circ (n_2 + i) - n_1 \circ n_2 \in I$
   (b) $i \circ n_1 \in I$

Next, we will take a look at the congruences of an N-group $_NG$. It is not quite clear what "congruence" means if we define N-groups as in (definition 3.5) or (3.4) . It is clear if we give the definition of N-groups as in (3.3). Hence, (3.3) allows us to speak about

1. N-congruences ($= \Omega_N$-congruences)
2. N-homomorphisms ($= \Omega_N$-homomorphisms)
3. sub-N-groups ($=$ sub-Ω_N-algebras)

We characterize these concepts in the language of (definition 3.5).

Theorem 3.11 *1. Let G be an N-group. Then R is an N-congruence on $_NG$ $\Longleftrightarrow$*

(a) R is a congruence on the group $(G, +)$

(b) For all $n \in N$ and $x, y \in G$ we have:

$$x \equiv_R y \Rightarrow n * x \equiv_R n * y$$

2. Let G_1, G_2 be N-groups. Then

$$h \ : \ G_1 \ \longrightarrow \ G_2$$

is an N-homomorphism $\Longleftrightarrow$

(a) h is a group-homomorphism

(b) For all $n \in N$, $g_1 \in G_1$ we have:

$$h(n *_1 g_1) = n *_2 h(g_1)$$

3. Let G be an N-group. Then H is a sub-N-group of G $\Longleftrightarrow$

(a) H is a subgroup of G

(b) For all $n \in N$, $h \in H$ we have: $n * h \in H$.

As in the case of Ω-groups we can describe N-congruences by ideals. This is possible because of the following theorem.

Theorem 3.12 *Let G be an N-group. Then G is also an N_0-group in the natural way. We then have: Each N_0-congruence R_0 of the N_0-group G is also an N-congruence of the N-group G. Of course, each N-congruence is also an N_0-congruence.*

Proof: Let R_0 be a N_0-congruence on ${}_{N_0}G$. Let $x, y \in G$ with $x \equiv_{R_0} y$ and let $n \in N$. We have to show that $n * x \equiv_{R_0} n * y$. Decompose n into $n_0 + n_c$ as in (theorem 3.8). Since R_0 is a congruence with respect to $+$, it is sufficient to show $n_0 * x \equiv_{R_0} n_0 * y$ and $n_c * x \equiv_{R_0} n_c * y$. The first statement holds because R_0 is an N_0-congruence, the second one because $n_c * x = n_c * y$ (by (theorem 3.9)). Hence R_0 is also an N-congruence. □

This is surprising because an N_0-homomorphism

$$h \;:\; {}_{N_0}G_1 \longrightarrow {}_{N_0}G_2$$

is not necessarily an N-homomorphism $h \;:\; {}_N G_1 \longrightarrow {}_N G_2$ As an example, consider

$$\begin{array}{rccc} h \;: & {}_{P(Z)_0}\mathbf{Z} & \longrightarrow & {}_{P(Z)_0}\mathbf{Z} \\ & z & \longmapsto & 0 \end{array}$$

Theorem 3.13 *The congruences of an N-group ${}_N G$ are given as the relation modulo the N-ideals I, where I is an N-ideal iff*

1. *I is a normal subgroup of G.*
2. *For all $n \in N$, $\gamma \in G$, $i \in I$ we have:*

$$n * (\gamma + i) - n * \gamma \in I$$

3.5 Types of N-groups

As a service to the reader, we repeat some of the definitions given in ([Pil83]) that will be needed in the next chapter. N will be a near-ring and ${}_N G$ an N-group in the sequel.

Definition 3.14 *${}_N G$ is* monogenic*:* $\Longleftrightarrow$

$$\exists g \in G : N * g = G$$

Definition 3.15 *${}_N G$ is* strongly monogenic *:* $\Longleftrightarrow$ *${}_N G$ is monogenic and for all $g \in G$:*

$$N * g = \{0\} \text{ or } N * g = G$$

Definition 3.16 (N-groups of type 0) *Let ${}_N G$ be monogenic, $G \neq \{0\}$. Then ${}_N G$ is of type 0:* $\Longleftrightarrow$

$${}_N G \textit{ has no non-trivial } N-\textit{ideals.}$$

As usually, the *trivial* ideals of G are $\{ 0 \}$ and G.

One would be tempted to say "${}_N G$ is N-simple." instead of "${}_N G$ has no non-trivial N-ideals.". [Pil83] however uses the notion "N-simple" for something different and calls an N-group that has no non-trivial N-ideals "simple". We avoid conflicts with the literature or inconstencies by avoiding both notions: "N-simple" and "simple".

Definition 3.17 (N-groups of type 1) *Let $_NG$ be monogenic, $G \neq \{0\}$. Then $_NG$ is of type 1:* $\Longleftrightarrow$

$$_NG \textit{ has no non-trivial } N - \textit{ideals and is strongly monogenic.}$$

Definition 3.18 (N-groups of type 2) *Let $_NG$ be monogenic, $G \neq \{0\}$. Then $_NG$ is of type 2:* $\Longleftrightarrow$

$$_{N_0}G \textit{ has no non-trivial } sub - N_0 - groups.$$

As usually, the *trivial* sub-N_0-groups of G are $\{\ 0\ \}$ and G.

Theorem 3.19 *$_NG$ of type 2 $\Longrightarrow$ $_NG$ of type 1 $\Longrightarrow$ $_NG$ of type 0*

Proof: “type 2 $\Rightarrow$ type 1” holds because

- Each ideal of $_NG$ is a sub-N_0-group of $_{N_0}G$.
- For each $g \in G :\ N * g$ is a sub-N_0-group of $_{N_0}G$.

“type 1 $\Rightarrow$ type 0” is trivial.

3.6 Literature and sources

The whole material presented in this chapter can be found in [Pil83].

Chapter 4

Density theorems and interpolation

4.1 Generalizing polynomial completeness

In this chapter, we will characterize all 1-polynomially complete algebras for some varieties of Ω-groups such as rings, commutative rings with 1, groups and near-rings. It is quite hard for an algebra A to be 1-polynomially complete, because if A is 1-polynomially complete then we know:

- A is simple.
- If Op_Ω is finite (and it is finite for rings, groups, near-rings, ...) then A is finite.

A is simple because we know that $P(A) \subseteq C(A)$ (cf. (theorem 1.29)). For non-simple algebras A, we will try to investigate when $P(A)$ actually reaches its upper bound $C(A)$.

A 1-polynomially complete algebra A is finite, provided that it has finitely (or at most countably) many operations because of a cardinality argument: If A were infinite then there would be more functions than terms. So instead of asking whether every function *is* a polynomial function, we ask whether every function *can be interpolated at finitely many places* by a polynomial. More generally we can ask whether every function of a (big) function-near-ring G can be interpolated by a function in a (small and beautiful) function-near-ring F.

If a simple Ω-group A is 1-polynomially complete then it is natural to ask whether it is also n-polynomially complete. The answer is surprisingly easy: Yes, if $|A| \geq 3$.

4.2 Interpolation and the near-rings L_nF

Definition 4.1 (n-interpolation property) *Let Γ be a group and let $(F, +, \circ)$ be a sub-near-ring of $(M(\Gamma), +, \circ)$. Then F has the n-*interpolation-property *:* $\Longleftrightarrow$

$$\textit{For all } m \in M(\Gamma) \textit{ and for all } x_1, x_2, \ldots, x_n \in \Gamma$$

$$\textit{there exists } f \in F \textit{ such that for all } i \in 1, 2, \ldots, n:$$
$$f(x_i) = m(x_i)$$

Remarks:

1. The affine functions on the reals (i.e. the functions $x \mapsto kx + d$) have the 2-interpolation property. They do not have the 3-interpolation property.
2. Let F be a sub-near-ring of $M(\Gamma)$, $\Gamma \neq \{0\}$. If F has the 2-interpolation-property, then ${}_F\Gamma$ is of type 2.

The next definition sees the problem the other way round: We start with a small near-ring F and collect all the functions that can be interpolated by F at at most n places.

Definition 4.2 *Let F be a sub-near-ring of $M(\Gamma)$ and $n \in \mathbf{N}$. Then*

$$L_nF := \{l \in M(\Gamma) \mid \forall x_1, x_2, \ldots, x_n \in \Gamma : \ \exists f \in F :$$

$$f(x_i) = l(x_i) \textit{ for } i = 1, 2, \ldots, n\}$$

L_nF is actually a near-ring:

Theorem 4.3 *Let F be as above. Then $(L_nF, +, \circ)$ is a sub-near-ring of $(M(\Gamma), +, \circ)$.*

Proof: Let $l_1, l_2 \in L_nF$. Then $l_1 + l_2$ is in L_nF. For proving this, let $x_1, x_2, \ldots, x_n$ be arbitrary but fixed and let $f_1 \in F$ be such that it agrees with l_1 on $x_1, x_2, \ldots, x_n$. In the same way, we get f_2 for l_2. $f_1 + f_2$ does the interpolation-job for $l_1 + l_2$. In the same way we see that F is closed under $-$.

It remains to show that $l_1 \circ l_2 \in L_nF$. Take f_2 such that it agrees with l_2 on $x_1, x_2, \ldots, x_n$ and f_1 such that it agrees with l_1 on $l_2(x_1), l_2(x_2), \ldots, l_2(x_n)$. $f_2 \circ f_1$ does the job.$\square$

This construction of L_nF out of F is not limited to near-rings. The general process would be the following: Let A be an Ω-algebra. Take a sub-Ω-algebra F of $M(A)$ and define L_nF as in (definition 4.2). L_nF will not only be an Ω-algebra: If F is contained in a variety $\mathcal{V} = \mathbf{K}(\Omega, \Sigma)$ of Ω-algebras then so is L_nF (for $n \in \mathbf{N}$) and if F is closed under concatenation then L_nF is closed under concatenation as well. We will restrict ourselves to near-rings in the sequel.

L_nF inherits a lot of properties from F. If $(F, +, \circ)$ is a ring then $(L_3F, +, \circ)$ will be a ring as well.

We will explain this now:

Definition 4.4 *Let τ be an arbitrary signature. Let $t \in T_\tau(\{x_1, x_2, \ldots, x_k\})$. 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. Let (t_1, t_2) be an equation over τ, $t_1, t_2 \in T_\tau(\{x_1, x_2, \ldots, x_k\})$. Then we define the complexity C *of the equation by*

$$C((t_1, t_2)) := max\{Occ(l, t_1) + Occ(l, t_2) | l \in \{1, 2, \ldots, k\}\}.$$

So $C((t_1, t_2)) \leq n$ means that no variable occurs more then n times in the equation. Example: $C((\circ[x_1, +[x_2, x_3]]; +[\circ[x_1, x_2], \circ[x_1, x_3]])) = 3$.

Theorem 4.5 *Let Γ be a group and let F be a sub-near-ring of $M(\Gamma)$. Let (t_1, t_2) be an equation over $\Omega_\circ$ with $Op_{\Omega_\circ} = \{+, -, 0, \circ\}$. Let $c := C((t_1, t_2))$. Then we have:*

$$(t_1, t_2) \text{ holds in } F \Rightarrow \forall n \geq c : (t_1, t_2) \text{ holds in } L_nF$$

Proof: Let (t_1, t_2) be an equation that does not hold in L_nF, $t_1, t_2 \in T_{\Omega_\circ}(\{x_1, x_2, \ldots, x_k\})$. Hence there are $l_1, l_2, \ldots, l_k \in L_nF$ such that

$$t_1{}^{L_nF,k}(l_1, l_2, \ldots, l_k) \neq t_2{}^{L_nF,k}(l_1, l_2, \ldots, l_k). \tag{4.1}$$

Both sides of (4.1) are functions. Hence we have $\gamma \in \Gamma$ with

$$t_1{}^{L_nF,k}(l_1, l_2, \ldots, l_k)(\gamma) \neq t_2{}^{L_nF,k}(l_1, l_2, \ldots, l_k)(\gamma).$$

If we actually want to calculate $t_1{}^{L_nF,k}(l_1, l_2, \ldots, l_k)(\gamma)$ and $t_2{}^{L_nF,k}(l_1, l_2, \ldots, l_k)(\gamma)$ then each l_j gets evaluated at at most c places. Hence we can find an f_j that is equal to l_j at these c places. Hence

$$t_1{}^{L_nF,k}(l_1, l_2, \ldots, l_k)(\gamma) = t_1{}^{L_nF,k}(f_1, f_2, \ldots, f_k)(\gamma).$$

From this we conclude that $f_1, f_2, \ldots, f_k$ violate the equation (t_1, t_2), which therefore does not hold in $(F, +, \circ)$.$\square$

Note that any equation that holds in some L_nF with $n \in \mathbf{N}$ obviously also holds in F because of $F \subseteq L_nF$ (cf. (theorem 4.8)).

Especially interesting will be those functions that can "locally", i.e. considering only a finite number of points, not be distinguished from functions in F.

Definition 4.6 (Local F-functions) *Let Γ be a group and F a sub-near-ring of $M(\Gamma)$.*

$$L_\infty F := \bigcap_{n \in \mathbf{N}} L_nF$$

An l in $L_\infty F$ is called a local F-function.

If Γ is finite then $L_\infty F = F$. And if Γ is infinite then $L_\infty F$ keeps the traditions of its origin F. From (theorem 4.5) we get:

Corollary 4.7 *Let Γ be a group, F a sub-near-ring of $M(\Gamma)$. Let $\mathcal{V}$ be a variety over $\Omega_\circ$, where $Op_{\Omega_{circ}} = \{+, -, 0, \circ\}$. Then we have:*

$$F \in \mathcal{V} \Rightarrow L_\infty F \in \mathcal{V}$$

We will list some properties of L_n as an operator on the set of all sub-near-rings of $M(\Gamma)$.

Theorem 4.8 *Let F, G be sub-near-rings of $M(\Gamma)$.*

1. *The near-rings $L_i F$ form a chain. For all $k \in \mathbf{N}$, $k \geq 2$, we have:*

$$F \subseteq L_\infty F \subseteq \cdots \subseteq L_{k+1} F \subseteq L_k F \subseteq \cdots \subseteq L_2 F \subseteq L_1 F \subseteq M(\Gamma)$$

2. *For all $n \in \mathbf{N}$: $F \subseteq G \Longrightarrow L_n F \subseteq L_n G$*
3. *For all $m, n \in \mathbf{N}$: $L_n(L_m F) = L_{min(m,n)} F$*
4. *For all $n \in \mathbf{N}$: $L_n(L_n F) = L_n F$*
5. *For all $n, m \in \mathbf{N}$: $L_n(L_m F) = L_m(L_n F)$*

(1.) and (2.) are obvious, (4.) and (5.) follows from (3.). Hence we only need to prove property (3.):

- **Case** $n \leq m$: We have to show: $L_n(L_m F) = L_n F$.
  - "$\supseteq$" follows from $F \subseteq L_m F$ and (2.).
  - "$\subseteq$": Let f be in $L_n(L_m F)$ be arbitrary but fixed. We have to show $f \in L_n F$. We fix $x_1, x_2, \ldots, x_n \in \Gamma$. There is a function $g \in L_m F$ such that $g(x_i) = f(x_i)$ for $i = 1, \ldots, n$. Since $g \in L_m F$ and since $m \geq n$ there is $h \in F$ such that $h(x_i) = g(x_i)$ for $i = 1, \ldots, n$. h is the required function of F.
- **Case** $n \geq m$: We have to show: $L_n(L_m F) = L_m F$
  - "$\supseteq$" follows from $G \subseteq L_n G$.
  - "$\subseteq$" can be proved as in the case $n \leq m$.

The following proposition connects $L_n F$ and the interpolation property.

Theorem 4.9 *Γ, F as in (definition 4.6). Then $L_n F = M(\Gamma)$ iff F has the n-interpolation property.*

If every function of the (big) near-ring G is a local F-function for the (small) near-ring F, we say that F is *dense* in G.

Definition 4.10 (Density) *Let Γ be a group, F,G sub-near-rings of $M(\Gamma)$. Then F is* dense *in G: $\Longleftrightarrow$*

1. $F \subseteq G$
2. $G \subseteq L_\infty F$

Note that for a given F, (theorem 4.5) puts bounds on the G's in which F can be dense. For example, a ring can never be dense in a non-ring. I think this is worth observing.

Corollary 4.11 *Let Γ be a group and F, G be sub-near-rings of $M(\Gamma)$. Suppose that F is a ring and that F is dense in G. Then G is also a ring.*

Proof: By (corollary 4.7), $L_\infty F$ is a ring. Since G is a sub-near-ring of $L_\infty F$, G is also a ring. □

We will now look at these concepts for $F := P(\Gamma)$. We get a surprising description of the compatible functions.

Theorem 4.12 *Let Γ be an Ω-group. We have:*

$$L_2P(\Gamma) = C(\Gamma)$$

For the proof use (theorem 1.29) for "$\subseteq$" and (theorem 3.3) for "$\supseteq$" or look into [Pil83].□

The functions in $L_\infty P(\Gamma)$ are called *local polynomial functions.* It is interesting when some $L_nP(\Gamma)$ coincide. As in [Pil83] we define:

Definition 4.13 *An Ω-group Γ is*

1. affine complete *iff* $P(\Gamma) = C(\Gamma)$
2. locally polynomially complete *iff* $L_\infty P(\Gamma) = M(\Gamma)$
3. locally affine complete *iff* $L_\infty P(\Gamma) = C(\Gamma)$

It is a corollary to (theorem 4.12) that a locally polynomially complete Ω-group Γ has to be simple.

An Ω-group is locally polynomially complete iff any function

$$f \;:\; X \longrightarrow \Gamma$$

with finite domain $X \subseteq \Gamma$ can be extended to a polynomial function

$$\bar{f} \;:\; \Gamma \longrightarrow \Gamma\ .$$

Therefore one could be tempted to believe that Γ is locally affine complete iff any *compatible* function with finite domain can be extended to a polynomial function. (A function $f \;:\; X \subseteq \Gamma \longrightarrow \Gamma$ is compatible iff

$$\forall \text{ ideals } I \text{ of } \Gamma\, \forall x_1, x_2 \in \mathbf{X} :$$

$$x_1 \equiv_I x_2 \Rightarrow f(x_1) \equiv_I f(x_2).\ )$$

We will clarify the difference now:

Definition 4.14 *An Ω-group Γ has the FCEPP (finite compatibles extend to polynomials - property):*$\Longleftrightarrow$

$$\begin{gathered}\textit{For all } X \subseteq \Gamma \textit{ with } X \textit{ finite}\\ \textit{for all compatible functions } f : X \longrightarrow \Gamma\\ \textit{there exists } \bar{f} \in P(\Gamma) \textit{ such that}\\ \forall x \in X : \bar{f}(x) = f(x)\end{gathered}$$

.

If an Ω-group satisfies the FCEPP then it is locally affine complete. Fulfilling the FCEPP may be harder than being locally affine complete because there might be compatible functions $f : X \longrightarrow \Gamma$ which cannot even be extended to a *compatible* function $\bar{f} : \Gamma \longrightarrow \Gamma$.

Obviously, local affine completeness implies the FCEPP if every compatible function on a finite domain can be extended to a compatible function on Γ. This, however, is not the case. In arithmetical algebras (that means that the congruences are permutable and that the congruence-lattice is distributive) the extension of a compatible function $c : X \longrightarrow \Gamma$ to a compatible function $c : Y \longrightarrow \Gamma$ with X,Y finite, $X \subseteq Y$ is always possible, but this extension property actually characterizes the arithmetical algebras (cf. [Kaa83]).

We will take a closer look at $L_n P(\mathbf{Z})$ later on.

Now we will come to one of the absolute highlights of near-ring-theory.

4.3 Density theorems for near-rings

4.3.1 What is a density theorem ?

A density theorem is a theorem that gives conditions on two function-near-rings F and G that guarantee that F is dense (cf. (definition 4.10)) in G. As an example I want to give the following proposition that will be a corollary of (theorem 4.16).

Theorem 4.15 *Let F be a sub-near-ring of $M(\Gamma)$. Then we have:*

$$L_4 F = M(\Gamma) \Longrightarrow L_\infty F = M(\Gamma)$$

If a near-ring has the 4-interpolation property, it has the n-interpolation property for all $n \in \mathbf{N}$.

4.3.2 An interpolation theorem for near-rings

Theorem 4.16 *Let F be a sub-near-ring of $M(\Gamma)$. Let $n \in \mathbf{N}$, and let $x_1, x_2, \ldots, x_n \in \Gamma$ such that (1.), (2.) and (3.) are satisfied.*

1. *$\forall i \in \{1,2,\ldots,n\} : F * x_i = \Gamma$ and*
   $\forall i,j \in \{1,2,\ldots,n\}$ with $i \neq j$ $\forall \gamma_1, \gamma_2 \in \Gamma\, \exists f \in F$ such that

$$f(x_i) = \gamma_1 \text{ and } f(x_j) = \gamma_2$$

2. *Γ has no non-trivial F-ideals*

3. *We have a function $k : \Gamma \times \Gamma \longrightarrow \Gamma$ that satisfies the properties (a), (b) and (c):*

   (a) $\forall f, g \in F$: The mapping $h_{f,g}$

$$\begin{array}{rcccc} h_{f,g} & : & \Gamma & \longrightarrow & \Gamma \\ & & x & \longmapsto & k(f(x), g(x)) \end{array}$$

   is an element of F.

   (b) $\forall x, y \in \Gamma : k(x,0) = 0$ and $k(0,y) = 0$

   (c) $\exists x, y \in \Gamma : k(x,y) \neq 0$

Then we have:

$$\begin{gathered} \forall y_1, y_2, \ldots, y_n \in \Gamma \\ \exists f \in F : \\ f(x_i) = y_i \text{ for } i = 1,\ldots,n \end{gathered} \tag{4.2}$$

Before proving the theorem I want to underline that for condition (2.) it is sufficient that Γ has no non-trivial sub-F_0-group, because every F-ideal is a sub-F_0-group.
Proof: We proceed by induction on n.

- **Base case** $n \leq 2$: (4.2) is assumption (1.).
- **Induction step** $n \to n+1$:
  - Let $x_1, x_2, \ldots, x_{n+1}$ be arbitrary but fixed elements of Γ that satisfy (1.), (2.) and (3.) . Let $y_1, y_2, \ldots, y_{n+1} \in \Gamma$.
  - By induction hypothesis, we find $s_1 \in F$ with

$$s_1(x_i) = y_i \text{ for } i = 1,2,\ldots,n$$

  - It is now sufficient to find $s_2 \in F$ with

$$\begin{gathered} s_2(x_i) = 0 \text{ for } i = 1,2,\ldots,n \\ \text{and} \\ s_2(x_{n+1}) = y_{n+1} - s_1(x_{n+1}). \end{gathered} \tag{4.3}$$

  This is sufficient, because then $s := s_1 + s_2$ does the required interpolation job.

- We will now start to construct such an s_2. Let $\bar{x}, \bar{y}$ be such that

$$k(\bar{x}, \bar{y}) \neq 0.$$

Then we construct $p_1 \in F$ by induction hypothesis such that

$$p_1(x_i) = 0 \text{ for } i = 1, 2, \ldots, n-1$$

$$p_1(x_{n+1}) = \bar{x}.$$

This is possible, because we construct p_1 by interpolation on n places: $1, 2, \ldots, n-1, n+1$. We construct $p_2 \in F$ such that

$$p_2(x_n) = 0$$

$$p_2(x_{n+1}) = \bar{y}.$$

- The mapping

$$h : x \mapsto k(p_1(x), p_2(x)) \tag{4.4}$$

is an element of F (by (3.a)) and has the properties:

$$h(x_i) = 0 \text{ for } i = 1, 2, \ldots, n$$

$$h(x_{n+1}) \neq 0$$

Hence the set I defined by

$$I = \{f(x_{n+1}) | f \in F \text{ and } f(x_i) = 0 \text{ for } i = 1, 2, \ldots n\}$$

has the property: $I \neq \{0\}$.

- I will show:

$$I = \Gamma$$

For this, it is sufficient to show that I is an F-ideal of Γ. We see immediately that I is a subgroup of Γ. I is normal. For this, we have to show:

$$\forall \gamma \in \Gamma \, \forall \iota \in I : \gamma + \iota - \gamma \in I \tag{4.5}$$

Let $\gamma \in \Gamma$ and $\iota \in I$ be arbitrary but fixed. Since $F * x_{n+1} = \Gamma$ we have $f_2 \in F$ such that $f_2(x_{n+1}) = \gamma$. Using the definition of I we can write ι as $g(x_{n+1})$ with $g \in F$, $g(x_i) = 0$ for $i \in \{1, 2, \ldots, n\}$. Then (4.5) becomes

$$f_2(x_{n+1}) + g(x_{n+1}) - f_2(x_{n+1}) \in I$$

We observe that $f_3 := f_2 + g - f_2$ has the property $f_3(x_i) = 0$ for $i = 1, 2, \ldots, n$ and $f_3(x_{n+1}) = \gamma + \iota - \gamma$. Hence I is actually normal in Γ. Now we have to show

$$\forall f_1 \in F \, \forall \gamma \in \Gamma \, \forall \iota \in I : f_1(\gamma + \iota) - f_1(\gamma) \in I \tag{4.6}$$

Let again $f_1 \in F$, $\gamma \in \Gamma$ and $\iota \in I$ be arbitrary but fixed. Since $\iota \in I$, we can write ι as $g(x_{n+1})$ with $g(x_1) = \cdots g(x_n) = 0$ and $g \in F$. Since $F * x_{n+1} = \Gamma$ there is an $f_2 \in F$ such that $f_2(x_{n+1}) = \gamma$. Now, (4.6) becomes:

$$f_1\left(f_2(x_{n+1}) + g(x_{n+1})\right) - f_1\left(f_2(x_{n+1})\right) \in I$$

The function f_3 defined by

$$f_3 := f_1 \circ (f_2 + g) - f_1 \circ f_2$$

has the properties:

1. $f_3(x_i) = 0$ for $i = 1, 2 \ldots n$
2. $f_3(x_{n+1}) = f_1(\gamma + \iota) - f_1(\gamma)$

Hence, $f_3(x_{n+1}) \in I$ and therefore we have shown (4.6). This means that I is an ideal, hence (by the assumption that ${}_F\Gamma$ is F-simple) either $\{0\}$ or Γ. In our case (because of h constructed in (4.4)) we know that $I = \Gamma$.

– Since $I = \Gamma$ there is a mapping s_2 that satisfies the conditions put on it in (4.3). $\Box$

We will give many applications of this theorem, but before we want to underline that in some cases the proof is constructive.

4.3.3 An interpolation algorithm for near-rings

If $M(\Gamma) \subseteq L_2F$ and if the $f \in F$ interpolating an arbitrary mapping on Γ at *two* places can be found algorithmically then we can compute the functions interpolating at n places by the following algorithm. We will suppose: $|\Gamma| \geq 2$.

The algorithm

Let us suppose that we have algorithms for the following functions available that satisfy the following specifications:

1. **InterpolateAtTwo**
   - **Input** $(x_1, y_1), (x_2, y_2)$ with $x_1, y_1, x_2, y_2 \in \Gamma$ such that $x_1 \neq x_2$.
   - **Output** $f \in F$ such that $f(x_1) = y_1$ and $f(x_2) = y_2$.
2. **kForGamma**
   - **Input** $x, y \in \Gamma$
   - **Output** z with $z = 0$ if ($x = 0$ or $y = 0$).
3. **kForF**

- **Input** $f, g \in F$
- **Output** $h \in F$ such that $h(x) = \textbf{kForGamma}[f(x), g(x)]$ for all $x \in \Gamma$.

4. **xForK**

   - **Input** none
   - **Output** $\gamma \in \Gamma$

5. **yForK**

   - **Input** none
   - **Output** $\gamma \in \Gamma$ such that $\textbf{kForGamma}[\textbf{xForK}, \gamma] \neq 0$

6. **Compose**

   - **Input** $f, g \in F$
   - **Output** $c \in F$ such that $c = f \circ g$.

Then we can have an algorithm **InterpolateAtN** that satisfies the following specification

- **InterpolateAtN**
  - **Input** $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$ with $\forall i : x_i, y_i \in \Gamma$ and $\forall i, j : x_i = x_j \Rightarrow i = j$.
  - **Output** $f \in F$ such that $f(x_i) = y_i$ for $i = 1, 2, \ldots, n$.
  - **Algorithm**

if $n = 1$ **then**
  $x_2 :=$ arbitrary in $\Gamma \setminus \{x_1\}$
  return InterpolateAtTwo $[(x_1, y_1), (x_2, 0)]$
elsif $n = 2$ **then**
  return InterpolateAtTwo $[(x_1, y_1), (x_2, y_2)]$
else
  $s_1 :=$ **InterpolateAtN** $[(x_1, y_1), (x_2, y_2), \ldots, (x_{n-1}, y_{n-1})]$
  $p_1 :=$ **InterpolateAtN** $[(x_1, 0), (x_2, 0), \ldots, (x_{n-2}, 0), (x_n, \textbf{xForK})]$
  $p_2 :=$ **InterpolateAtTwo**$[(x_{n-1}, 0), (x_n, \textbf{yForK})]$
  $h :=$ **kForF**$[p_1, p_2]$
  $g :=$**InterpolateAtTwo** $[(0, 0), (h(x_n), y_n - s_1(x_n))]$
  $s_2 :=$ **Compose** $[g, h]$
  return $s_1 + s_2$
endif

Remarks:

- The input conditions for our algorithms are stronger than the assumptions of (theorem 4.16):

1. Instead of claiming that there are no F-ideals, we claim the stronger $M(\Gamma) \subseteq L_2F$.
2. In the case $F = P(\Gamma)$, we know that if Γ is a simple Ω-group then $M(\Gamma) = L_2P(\Gamma)$. This follows immediately from (theorem 4.12). Usually, one cannot determine the polynomial interpolating at two places algorithmically.

- The algorithm is slow. Two recursive calls make the algorithm be of $O(2^n)$.

4.3.4 Applications to interpolation theory

Γ will always denote a group and F will always be a sub-near-ring of $M(\Gamma)$.

Corollary 4.17 *If $(\Gamma, +)$ is not commutative or there is a function $f \in F_0$ such that f is not linear (i.e. we have $f(x+y) \neq f(x) + f(y)$ for some $x, y \in \Gamma$) then we have:*

$$L_2F = M(\Gamma) \Longrightarrow L_\infty F = M(\Gamma)$$

Proof: We take $x_1, x_2, \ldots, x_n$ arbitrary but fixed in Γ. Condition (1.) of the assumptions in (theorem 4.16) is clearly fulfilled. Furthermore, Γ cannot have a non-trivial sub-F_0-group: Let S be a sub-F_0-group and $\sigma \neq 0$, $\sigma \in S$. Then any $\gamma \in \Gamma$ is also in S. Take $f \in F$ with $f(0) = 0$ and $f(\sigma) = \gamma$. Hence, condition (2.) is satisfied. For condition (3.) we distinguish two cases.

- **Case** $(\Gamma, +)$ not commutative: Then we define k by

$$\begin{array}{cccc} k & : & \Gamma \times \Gamma & \longrightarrow & \Gamma \\ & & (x, y) & \longmapsto & x + y - x - y \end{array}$$

- **Case** $f_1 \in F_0$ is not linear. We define k by

$$\begin{array}{cccc} k & : & \Gamma \times \Gamma & \longrightarrow & \Gamma \\ & & (x, y) & \longmapsto & f_1(x) + f_1(y) - f_1(x+y) \end{array}$$

From this corollary it follows that if F_0 is not a ring then the 2-interpolation property implies the n-interpolation property for all n.

Corollary 4.18 *Let Γ be such that there is $\gamma \in \Gamma$ with $\gamma + \gamma \neq 0$. Then we have:*

$$L_3F = M(\Gamma) \Longrightarrow L_\infty F = M(\Gamma)$$

Proof: Let $\gamma \in \Gamma$ have the property $\gamma + \gamma \neq 0$. Then we have $f \in F$ with $f(0) = f(\gamma) = 0$, $f(\gamma + \gamma) \neq 0$.[1] Since f is not linear, we get the result applying (corollary 4.17).□

[1]The reader will have checked that 0, γ and $\gamma + \gamma$ are pairwise different.

Corollary 4.19

$$L_4 F = M(\Gamma) \Longrightarrow L_\infty F = M(\Gamma)$$

Proof: If $|\Gamma| \leq 4$ the result is trivial. If $|\Gamma| > 4$, let $x \in \Gamma$ such that $x \neq 0$ and let $y \in \Gamma$ such that $y \neq 0$, $y \neq -x$. Then we have $f \in F$ with $f(0) = f(x) = f(y) = 0$ and $f(x+y) \neq 0$. We get the result applying (corollary 4.17).□

We give an example of a near-ring F with $L_3 F = M(\Gamma)$, but F is *not* dense in $M(\Gamma)$. Let $\Gamma := \mathbf{Z}_2 \times \mathbf{Z}_2$ and let

$$F := \{\vec{x} \mapsto Q \cdot \vec{x} + \vec{b} \mid Q \text{ a matrix } in (\mathbf{Z}_2)_2^2,$$

$$\vec{b} \text{ a vector in } (\mathbf{Z}_2)^2\}$$

Then any two distinct vectors $\vec{x}_1, \vec{x}_2 \in \Gamma \setminus \{0\}$ are linearly independent. From this we derive that F has the 3-interpolation property. $|F|$ can be at most $2^4 \cdot 2^2 = 2^6$. $|M(\Gamma)| = 4^4 = 2^8$. Since for a finite Γ *density* means *equality* we have: F is not dense in $M(\Gamma)$.

4.3.5 0-primitive near-rings

(Theorem 4.16) also implies two well-known theorems of near-ring theory.

Definition 4.20 *Let Γ be a group and F be a sub-near-ring of $M(\Gamma)$. Then F is* 0-primitive*: $\Longleftrightarrow$ ${}_F\Gamma$ is of type 0.*

The fact that we have restricted ourselves to function-near-rings has allowed us to simplify the definition compared to [Pil83].

Theorem 4.21 (0-primitive near-rings) *Let Γ be a group and F be a sub-near-ring of $M(\Gamma)$.*
If

1. *F is zero-symmetric, i.e. $F = F_0$.*
2. *F is not a ring.*
3. *F is 0-primitive.*
4. $x_1, x_2, \ldots, x_n \in \Gamma \setminus \{0\}$
5. $\forall i, j : i \neq j \Rightarrow \{f \in F | f(x_i) = 0\} \neq \{f \in F | f(x_j) = 0\}$
6. $\forall i : F * x_i = \Gamma$
7. $y_1, y_2, \ldots, y_n \in \Gamma$

then

$$\exists f \in F : f(x_i) = y_i \textit{ for } i = 1, 2, \ldots, n$$

Proof: Let $x_1, x_2, \ldots, x_n \in \Gamma$ be arbitrary but fixed and assume that F and $x_1, x_2, \ldots, x_n$ satisfy the assumptions of this theorem. Let $y_1, y_2, \ldots, y_n \in \Gamma$ be arbitrary but fixed. We want to construct the required $f \in F$ by (theorem 4.16). Hence we have to see how we can guarantee the conditions (1.),(2.) and (3.) of the assumptions of (theorem 4.16) for $x_1, x_2, \ldots, x_n$ and F.

- **Condition (1.) of (theorem 4.16)**: Let $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$. It is sufficient to show that for all $\gamma \in \Gamma$ there exists $f \in F$ with

  $$f(x_i) = \gamma \text{ and } f(x_j) = 0.$$

  Since

  $$I := \{f(x_i) | f(x_j) = 0\}$$

  is an F-ideal of Γ (cf. the corresponding step in the proof of (theorem 4.16)), it is sufficient to show that $I \neq \{0\}$. Suppose that $I = \{0\}$. We then have:

  $$\forall f \in F : f(x_j) = 0 \Rightarrow f(x_i) = 0$$

  or, in other words

  $$\{f | f(x_j) = 0\} \subseteq \{f | f(x_i) = 0\}. \tag{4.7}$$

  The mapping

  $$\begin{array}{cccc} h & : & {}_F F & \longrightarrow & {}_F \Gamma \\ & & f & \longmapsto & f(x_j) \end{array}$$

  is a homomorphism of F-groups. By our assumptions, we know that h is surjective. Since $\Gamma = Im(h)$ is F-simple and since $Im(h)$ is F-isomorphic to $F/_{ker(h)}$, where $ker(h) = \{f | f(x_j) = 0\}$, we know that $\{f | f(x_j) = 0\}$ is a maximal F-ideal of F. The right hand side of (4.7) is an F-ideal as well. By the maximality of the left hand side, we get equality in (4.7). This is a contradiction to our assumptions.

- **Condition (2.) of (theorem 4.16)**: This condition is part of our assumptions.

- **Condition (3.) of (theorem 4.16)**: If $(F, +, \circ)$ does not satisfy the left distributive law then there is an $f \in F$ such that there are x, y with $f(x+y) \neq f(x) + f(y)$. Then

  $$k : (x, y) \mapsto f(x + y) - f(x) - f(y)$$

  does the job in (3.). If F is not commutative then the group Γ is not commutative either and we define

  $$k : (x, y) \mapsto x + y - x - y$$

Therefore (theorem 4.16) gives us the required function $f \in F$.□

4.3.6 2-primitive near-rings

Definition 4.22 *Let F be a sub-near-ring of $M(\Gamma)$. Then F is* 2-primitive*:* $\Longleftrightarrow$ ${}_F\Gamma$ *is of type 2.*

We will state the density theorem only for zero-symmetric 2-primitive near-rings with identity.(See [Pil83] how to deal with the not zero-symmetric case.) We will obtain a real density theorem for these near-rings. F is however not necessarily dense in $M(\Gamma)$. This can be motivated in the following way.

Definition 4.23 (Bicentralizer near-rings)
Let S be a set of group-endomorphisms of Γ. Then $M_S(\Gamma)$ defined by

$$M_S(\Gamma) := \{f \in M(\Gamma) | \forall x \in \Gamma \, \forall s \in S : f(s(x)) = s(f(x))\}$$

turns out to be a near-ring.

Theorem 4.24 *Let F be a sub-near-ring of $M(\Gamma)$. Then $End_F(\Gamma)$ is the set of all F-endomorphisms of ${}_F\Gamma$. We then have:*

1. $F \subseteq M_{End_F(\Gamma)}(\Gamma)$
2. *for all $n \in \mathbf{N}$ with $n \geq 2$:* $L_n F \subseteq M_{End_F(\Gamma)}(\Gamma)$

Proof: (1.): Let $f \in F$ and $h \in End_F(\Gamma)$. We then have $f(h(\gamma)) = f * h(\gamma) = h(f * \gamma) = h(f(\gamma))$.

(2.): Suppose that we have an l in $L_n F$ such that there is $\gamma \in \Gamma$, $s \in M_{End_F(\Gamma)}(\Gamma)$ such that

$$l(s(\gamma)) \neq s(l(\gamma)) \tag{4.8}$$

Since $l \in L_2 F$ there is $f \in F$ with $f(\gamma) = l(\gamma)$ and $f(s(\gamma)) = l(s(\gamma))$. Putting this into (4.8) we get

$$f(s(\gamma)) \neq s(f(\gamma))$$

which disqualifies s as F-homomorphism.□

Hence, $M_{End_F(\Gamma)}(\Gamma)$ is an upper bound for $L_\infty F$. The method of getting this upper bound is similar to (theorem 4.5). We sometimes reach the bound. Before proving the density theorem, we need some information about $End_F(\Gamma)$.

Theorem 4.25 *Let $F = F_0$ be a sub-near-ring of $M(\Gamma)$ and ${}_F\Gamma$ be of type 2. Let ${}_F\Gamma$ be F-simple. Then each F-endomorphism $h \in End_F(\Gamma)$ is either the zero-mapping or bijective.*

Proof: Let $h \in End_F(\Gamma)$, $h \neq 0$. Then h is injective because $ker(h)$ is an F-ideal of Γ. It is surjective because $h(\Gamma)$ is a sub-F-group of Γ.

Corollary 4.26 *Let F, Γ be as in (theorem 4.25). Then*

$$End_F(\Gamma) \setminus \{0^{End(\Gamma)}\}$$

is a group.

Corollary 4.27 *Let* F, Γ *be as in (theorem 4.25).* $End_F(\Gamma) \setminus \{0^{End(\Gamma)}\}$ *operates* fix-point free *on* $\Gamma \setminus \{0\}$*, i.e.*

$$\forall g, h \in End_F(\Gamma) \setminus \{0^{End(\Gamma)}\}\, \forall \gamma \in \Gamma \setminus \{0\}$$

$$h(\gamma) = g(\gamma) \Rightarrow h = g$$

Proof: $\{\gamma \in \Gamma | h(\gamma) = g(\gamma)\}$ is always a sub-F-group of Γ. □

Theorem 4.28 (2-primitive near-rings) *Let* F *be a sub-near-ring of* $M(\Gamma)$*.*
If

1. $F = F_0$
2. F *is not a ring*
3. F *is 2-primitive*
4. $id \in F$

then

$$L_\infty F = M_{End_F(\Gamma)}(\Gamma) \tag{4.9}$$

Proof: We have to show "$\supseteq$" of (4.9). Let $m \in M_{End_F(\Gamma)}(\Gamma)$ be arbitrary but fixed. Let $n \in \mathbf{N}$ and $x_1, x_2, \ldots, x_n$ be arbitrary but fixed .

We will interpolate m by (theorem 4.16), but not at $x_1, x_2, \ldots, x_n$, but at some other places. Let $T \subseteq \Gamma \setminus \{0\}$ be a set of representatives for the orbits of the group action of $End_F(\Gamma) \setminus \{0^{End(\Gamma)}\}$ on $\Gamma \setminus \{0\}$. Let $T_1 \subseteq T$ be such that

$$t \in T_1 :\Longleftrightarrow \exists i \in \{1, \ldots, n\} : t \text{ and } x_i \text{ are in the same orbits.}$$

We now show that the assumptions of (theorem 4.16) are actually fulfilled for $t_1, t_2, \ldots, t_k$ with t_i pairwise different and $\{t_1, t_2, \ldots, t_k\} = T_1$.

- **Condition (1.)**: Let $i, j \in \{1, 2, \ldots, k\}$. Let $\gamma \in \Gamma$ be arbitrary. It is sufficient to show that there exists $f \in F$ with

  $$f(t_i) = \gamma \text{ and } f(t_j) = 0.$$

  Since

  $$I := \{f(t_i) | f(t_j) = 0\}$$

  is a sub-F-group of Γ, it is sufficient to show that $I \neq \{0\}$. Suppose that $I = \{0\}$. We then have:

  $$\forall f \in F : f(t_j) = 0 \Rightarrow f(t_i) = 0. \tag{4.10}$$

Note that $F * t_j = \Gamma$. This is because $id \in F$ and the fact that $F * t_j$ is a sub-F-group of Γ. We define the following mapping h by

$$\begin{array}{rccc} h & : & \Gamma & \longrightarrow & \Gamma \\ & & n * t_j & \longmapsto & n * t_i \end{array}$$

h is well-defined because of (4.10). h turns out to be a F-homomorphism that maps t_j to t_i (because of id). Therefore t_j and t_i are in the same orbit, which is a contradiction.

- **Condition (2.)**: From the assumptions.
- **Condition (3.)**: We construct k as in the proof of (theorem 4.21).

Applying (theorem 4.16) we get a function $f \in F$ with

$$f(t_i) = m(t_i) \text{ for } i = 1, 2, \ldots, k$$

We have to show that this property implies

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

Let $j \in \{1, 2, \ldots, n\}$ and let $t \in T_1$ be such that x_j is in the orbit of t. Let σ be the F-endomorphism with $\sigma(t) = x_j$ Then we have $f(x_j) = f(\sigma(t)) = \sigma(f(t)) = \sigma(m(t)) = m(\sigma(t)) = m(x_j)$. $\square$

4.3.7 Polynomially complete Ω-groups

If A is a simple Ω-group then (theorem 4.12) implies

$$M(A) \subseteq L_2P(A)$$

Hence we can apply (corollary 4.17) and get

Theorem 4.29 *Let A be a simple Ω-group.*
If *$P(A)_0$ contains a function p_0 such that*

$$\exists x, y \in A : p_0(x + y) \neq p_0(x) + p_0(y)$$

or

$$(A, +) \textit{ is not abelian}$$

then *A is* locally polynomially complete.

Sometimes we want to apply directly (theorem 4.16). We note that for simple Ω-groups A and for $F := P(A)$ conditions (1.) and (2.) are satisfied for all $a_1, a_2, \ldots, a_n \in A$ because of the 2-interpolation property of the polynomial functions. (Recall that $L_2P(A) = C(A) = M(A)$ for simple A.)

Note:

- $P(A)$ depends on Ω. If we talk e.g. about the polynomial functions of a *ring* R , we mean the polynomial functions of R as element of $\mathbf{K}(\tau_{\text{ring}})$.
- For finite A, *locally polynomially complete* implies *polynomially complete.*

Locally polynomially complete groups

Theorem 4.30 *The following is a complete list of the locally polynomially complete groups:*

1. $(\{0\}, +)$
2. $(\mathbf{Z}_2, +)$
3. *The simple, non-abelian groups.*

We check immediately that (1.) and (2.) are in fact polynomially complete. For simple, non-abelian groups the result follows from (theorem 4.29). So suppose that there is a locally polynomially complete group not contained in the list: it has to be simple and abelian, hence finite. For $G = (\mathbf{Z}_p, +)$, we get

$$P(G) := \{x \mapsto ax + g | a \in \{0, 1, \ldots, p-1\}, g \in G\}$$

and since $|P(G)| = p^2$ it is impossible for Z_p to be polynomially complete unless $p = 2$.

Locally polynomially complete rings

We now look at $\mathbf{K}(\tau_{\text{ring}}, \Sigma_{\text{ring}})$.

Theorem 4.31 *Each simple non-zero ring is locally polynomially complete.*

We have already seen that we only have to guarantee condition (3.) of (theorem 4.16). Setting

$$k(x, y) := x \cdot y$$

we are done.

Locally polynomially complete commutative rings with 1

We consider $\mathbf{K}(\tau_{\text{ring1}}, \Sigma_{\text{c ring 1}})$. The simple algebras in this variety are precisely the fields and the ring $(\{0\}, +, \cdot)$.

Theorem 4.32
A commutative ring with 1 R is locally polynomially complete $\Longleftrightarrow$ $|R| = 1$ *or* R *is a field.*

"$\Rightarrow$" follows from our knowledge of the simple commutative rings with 1, "$\Leftarrow$" from (theorem 4.31).

Locally polynomially complete near-rings

The operations we use for constructing the polynomial functions are $+, -, 0, *$. (We use $*$ in in order to avoid confusions with the functional composition $\circ$).

Theorem 4.33 *The following is a complete list of the locally polynomially complete near-rings (see [IK79]).*

1. $(\{0\}, +, *)$
2. $(\mathbf{Z}_2, +, *)$ *for any* $*$ *such that* $(\mathbf{Z}_2, +, *)$ *is a near-ring*[2].
3. $(N, +, *)$ *is simple and* $(N, +)$ *is not abelian.*
4. $(N, +, *)$ *is simple and abelian and* $\exists x, y : x * y \neq x * 0$.

We have to construct k of the condition (3.) of (theorem 4.16). If the addition is not abelian, take $k(x, y) := x + y - x - y$. For case (4.), take

$$k(x, y) := x * y - x * 0.$$

So suppose there is a locally polynomially complete near-ring N not contained in the list: It has to be simple and abelian with $x * y = x * 0$ for all $x, y \in N$. Hence there is a mapping $v : N \longrightarrow N$ such that $x * y = v(x)$ for all $x \in N$. Since $v(x + y) = (x + y) * 0 = x * 0 + y * 0 = v(x) + v(y)$, v is a group-homomorphism of $(N, +)$. v is also idempotent because $v(v(x)) = v(x) * 0 = (x * 0) * 0 = x * 0 = v(x)$ for all $x \in N$. Thus we get for $P(N)$:

$$P(N) = \{x \mapsto z_1 v(x) + z_2 x + g_3 | z_1, z_2 \in \mathbf{Z}, g_3 \in N\} \tag{4.11}$$

Note that the set given here contains the identity and the constants. It is closed under $+, -, 0$ and $*$. From the explicit calculation of $P(N)$ we get that $(P_N, +, \circ)$ satisfies the equation[3]

$$(x_1 \circ [x_2 + x_3] - x_1 \circ x_2 - x_1 \circ x_3 + x_1 \circ 0\,;\, 0). \tag{4.12}$$

Since N is locally polynomially complete, we use (theorem 4.5) and the fact that $P(N)$ is dense in $M(N)$ to derive that the equation (4.12) also holds in $M(N)$. Hence $|N| \leq 3$. For $N = \mathbf{Z}_3$ we get $v = 0$ or $v = id$. From (4.11) we know that in both cases $P(N) \neq M(N)$.□

4.4 Density in near-rings such as $C(A)$

4.4.1 A density theorem suitable for the compatibles

The next theorem will teach a small near-ring F how to be dense in a big G.

[2] There are three different multiplications that turn $(\mathbf{Z}_2, +)$ into a near-ring.
[3] We use an informal way of writing down equation (4.12)

Theorem 4.34 *Let Γ be a group and let F, G be sub-near-rings of $M(\Gamma)$.*
If

1. $F \subseteq G$ *and* $G \subseteq L_2 F$
2. $\forall \gamma \in \Gamma : F * \gamma = \Gamma$
3. *For all G-ideals S, B of $_G\Gamma$ with $S \subseteq B$, $S \neq B$ there is a mapping $k_{S,B}$ with the following properties*[4]*:*
   (a) $\forall x \in \Gamma : k_{S,B}(0, x) = k_{S,B}(x, 0) = 0$
   (b) $\exists x, y \in B : k_{S,B}(x, y) \notin S$
   (c) $\forall f, g \in F$: *The mapping* $h_{f,g}$

$$h_{f,g} \; : \; \begin{array}{ccc} \Gamma & \longrightarrow & \Gamma \\ x & \longmapsto & k_{S,B}(f(x), g(x)) \end{array}$$

   is an element of F.

then

$$\forall n \in \mathbf{N} : G \subseteq L_n F \tag{4.13}$$

that means F is dense in G.

Proof: We proceed by induction on n.

- **Base case** $n \leq 2$: (4.13) follows from assumption (1.).
- **Induction step** $n \to n+1$: Let $g \in G$ be arbitrary but fixed.
  - Let $x_1, x_2, \ldots, x_{n+1}$ be arbitrary but fixed elements of Γ. By induction hypothesis, we find $s_1 \in F$ with

$$s_1(x_i) = g(x_i) \text{ for } i = 1, 2, \ldots, n$$

  - It is now sufficient to find $s_2 \in F$ with

$$\begin{array}{c} s_2(x_i) = 0 \text{ for } i = 1, 2, \ldots, n \\ \text{and} \\ s_2(x_{n+1}) = g(x_{n+1}) - s_1(x_{n+1}). \end{array} \tag{4.14}$$

  This is sufficient, because then $s := s_1 + s_2$ does the required interpolation job.

[4]Think of "S"mall and "B"ig

– We will now start to construct such an s_2. Let

$$B := \{g(x_{n+1}) | g \in G \text{ and } g(x_i) = 0 \text{ for } i = 1, 2, \dots, n\}$$

$$S := \{f(x_{n+1}) | f \in F \text{ and } f(x_i) = 0 \text{ for } i = 1, 2, \dots, n\}$$

I will now show that B and S are G-ideals of of ${}_G\Gamma$.

– S is a G-ideal: Observing that $F * x_{n+1} = \Gamma$ we conclude as in the proof of (theorem 4.16) that S is normal in Γ. For showing that for all $\sigma \in S$, $g \in G$, $\gamma \in \Gamma$ we have

$$g(\gamma + \sigma) - g(\gamma) \in S,$$

we interpolate g at the places $\gamma + \sigma$ and γ by $f \in F$ and continue as in the proof of (theorem 4.16).

– B is a G-ideal: As in the proof of (theorem 4.16)

– Clearly, we have $S \subseteq B$. I will now show

$$S = B.$$

Suppose that $S \neq B$. Then let $b_1, b_2 \in B$ such that $k(b_1, b_2) \notin S$. By the definition of B there are functions $g_1, g_2 \in G$ with $g_1(x_i) = g_2(x_i) = 0$ for $i = 1, 2, \dots, n$ and $g_1(x_{n+1}) = b_1$, $g_2(x_{n+1}) = b_2$. We use the induction hypothesis to interpolate g_1 at $x_1, x_2, \dots, x_{n-1}, x_{n+1}$ by $f_1 \in F$. In the same way, we interpolate g_2 at x_n, x_{n+1} by $f_2 \in F$. We now construct the function h by

$$h : x \mapsto k_{S,B}(f_1(x), f_2(x)).$$

We get:

* $h \in F$ by (3.a)
* $h(x_i) = 0$ for $i = 1, 2, \dots, n$
* $h(x_{n+1}) \notin S$

This is clearly a contradiction to the definition of S, hence $S = B$.

– From $g(x_{n+1}) - s_1(x_{n+1}) \in B$ and $B \subseteq S$, we know (by the definition of S) that there is an $s_2 \in F$ with the properties required in (4.14).

4.4.2 Some locally affine complete Ω-groups

This theorem helps us to determine some locally affine complete Ω-groups. Before, we need some information about the $C(\Gamma)$-ideals of ${}_{C(\Gamma)}\Gamma$.

Theorem 4.35 *Let Γ be an Ω-group, $I \subseteq \Gamma$. Then the following three statements are equivalent.*

1. *I is an Ω-ideal of Γ.*

2. *I is a $P(\Gamma)$-ideal of ${}_{P(\Gamma)}\Gamma$.*

3. *I is a $C(\Gamma)$-ideal of ${}_{C(\Gamma)}\Gamma$.*

We prove (1.) $\Rightarrow$ (3.) $\Rightarrow$ (2.) $\Rightarrow$ (1.).
(1.) $\Rightarrow$ (3.): We take I arbitrary but fixed and assume that I is an Ω-ideal. We have to show:

$$\forall c \in C(\Gamma)\, \forall \gamma \in \Gamma, i \in I :$$
$$c(\gamma + i) - c(\gamma) \in I \tag{4.15}$$

We fix c, γ, i. Since $\gamma + i \equiv_I \gamma$ and since c is compatible, we get (4.15).
(3.) $\Rightarrow$ (2.): $P(\Gamma)$ is a sub-near-ring of $C(\Gamma)$.
(2.) $\Rightarrow$ (1.): We fix $\omega \in Op_\Omega$ with $Ar_\Omega(\omega) = n$ and fix $\gamma_1, \gamma_2, \ldots, \gamma_n \in \Gamma$, $i \in I$ and an index $j \in \{1, 2, \ldots, n\}$. We have to show

$$\omega(\gamma_1, \gamma_2, \ldots, \gamma_{j-1}, \gamma_j + i, \gamma_{j+1}, \ldots, \gamma_n) - \omega(\gamma_1, \gamma_2, \ldots, \gamma_n) \in I \tag{4.16}$$

We know that I is a $P(\Gamma)$-ideal and hence a sub-$P(\Gamma)_0$-group of ${}_{P(\Gamma)_0}\Gamma$. Therefore the function $p \in P(\Gamma)_0$ with

$$p : x \mapsto \omega(\gamma_1, \gamma_2, \ldots, \gamma_{j-1}, \gamma_j + x, \gamma_{j+1}, \ldots, \gamma_n) - \omega(\gamma_1, \gamma_2, \ldots, \gamma_n)$$

maps elements of I to elements of I, hence we get the required $p(i) \in I$. □

For $F = P(\Gamma)$ and $G = C(\Gamma)$, assumptions (1.) and (2.) of (theorem 4.34) are always fulfilled. Hence the existence of a suitable $k_{S,B}$ for all Ω-ideals S, B of Γ with $S \subseteq B, S \neq B$ is sufficient for local affine completeness.

Theorem 4.36 *Let G be a group such that for all normal subgroups N_1, N_2 of G with $N_1 \subseteq N_2$, $N_1 \neq N_2$ we have:*

$$N_2/_{N_1} \textit{ is not abelian.}$$

Then G is locally affine complete.

Proof: Define $k_{S,B}(x, y) := x + y - x - y$ for all S, B. Then apply (theorem 4.34).□

If the normal subgroups of G form a chain then (theorem 4.36) is a special case of a corollary in [Kai77].

Theorem 4.37 *Let R be a ring such that for all ideals I_1, I_2 with $I_1 \subseteq I_2$, $I_1 \neq I_2$ we have:*

$$I_2/_{I_1} \textit{ is not a zero-ring.}$$

Then R is locally affine complete.

Sketch of the proof: $k_{S,B}(x, y) := x \cdot y$.

4.5 Density in more dimensions

4.5.1 Matrix near-rings

Almost every (locally) 1-polynomially complete Ω-group is also (locally) 2-polynomially complete. This is a consequence of a result of [Slu39]. We will prove this result introducing matrix near-rings, which we shall define adapting the ideas of [MVdW86] to the case of function near-rings.

Definition 4.38 *Let Γ be a group and let $m \in \mathbf{N}$. For all $f \in M(\Gamma)$ and $i, j \in \{1, 2, \ldots, m\}$ we define $\varphi(f, i, j)$ by:*

$$\begin{array}{rccc} \varphi(f,i,j) & : & \Gamma^m & \longrightarrow & \Gamma^m \\ & & \vec{x} & \longmapsto & \iota_i \circ f \circ \pi_j(\vec{x}) \end{array},$$

where ι_i is defined as the i-th canonical injection

$$\begin{array}{rcccc} \iota_i & : & \Gamma & \longrightarrow & \Gamma^m \\ & & \gamma & \longmapsto & (0, \ldots, 0, \gamma, 0, \ldots, 0) \end{array}, \gamma \textit{ on the } i - th \textit{ place}$$

and π_j as the j-th canonical projection

$$\begin{array}{rcccc} \pi_j & : & \Gamma^m & \longrightarrow & \Gamma \\ & & (x_1, x_2, \ldots, x_m) & \longmapsto & x_j \end{array}.$$

Definition 4.39 (Matrix near-rings) *Let F be a sub-near-ring of $M(\Gamma)$. Then we define $Mat_m F$ as the sub-near-ring of $M(\Gamma^m)$ generated by*

$$\{\varphi(f, i, j) | f \in F, i, j \in \{1, 2, \ldots, m\}\}.$$

Theorem 4.40 *Let F,G be sub-near-rings of $M(\Gamma)$ and $m \in \mathbf{N}$. Then we have:*

$$F \subseteq G \Rightarrow Mat_m F \subseteq Mat_m G$$

Theorem 4.41 *Let $m, n \in \mathbf{N}$ and let F, G be sub-near-rings of $M(\Gamma)$ with $G \subseteq L_n F$. Then we have:*

$$Mat_m G \subseteq L_n(Mat_m F)$$

Proof: Since $L_n(Mat_m F)$ is a near-ring, it is sufficient to show that the generators of $Mat_m G$ are elements of $L_n(Mat_m F)$. We fix $g \in G$ and $i, j \in \{1, 2, \ldots, m\}$. Now let $x^{(1)}, x^{(2)}, \ldots, x^{(n)} \in \Gamma^m$ be arbitrary but fixed. Let $f \in F$ be such that $f({x^{(k)}}_j) = g({x^{(k)}}_j)$ for $k = 1, 2, \ldots, n$. Then for $k \in \{1, 2, \ldots, n\}$ we have:

$$\varphi(f, i, j)(x^{(k)}) = \varphi(g, i, j)(x^{(k)}).$$

Since $\varphi(f, i, j) \in Mat_m F$, the proof is complete. $\Box$

Corollary 4.42 *Let F, G be sub-near-rings of $M(\Gamma)$. If F is dense in G, then $Mat_m F$ is dense in $Mat_m G$.*

4.5.2 Matrix near-rings, polynomial function matrices and n-polynomial completeness

Theorem 4.43 *Let m be a natural number and let Γ be an Ω-group. Then we have:*

$$Mat_m(P(\Gamma)) \subseteq P_m^m(\Gamma),$$

For the definition of $P_m^m(\Gamma)$, see (definition 1.39).
Proof:$P_m^m(\Gamma)$ is a near-ring that contains the the generators of $Mat_m(P(\Gamma))$.□

We give examples for $P(\Gamma), P_m(\Gamma), P_m^m(\Gamma), Mat_m(P(\Gamma)), Mat_m(M(\Gamma))$ and $M(\Gamma^m)$ right now.

1. $\Gamma = (\mathbf{Z}_2, +, \cdot)$ is an Ω-group for $\Omega = \tau_{\text{ring1}}$. We get:
   (a) $P(\Gamma) =$

   $$\left\{ \begin{array}{cccc} f & : & \mathbf{Z}_2 & \longrightarrow & \mathbf{Z}_2 \\ & & x & \longmapsto & \bar{p}(x) \end{array} \mid p \in \mathbf{Z}_2[x_1; \mathbf{K}(\tau_{\text{ring1}}, \Sigma_{\text{c ring 1}})] \right\},$$

   which means that $P(\Gamma)$ is just the set of the "usual" polynomial functions.

   (b) $P_2(\Gamma) =$

   $$\left\{ \begin{array}{cccc} f & : & {\mathbf{Z}_2}^2 & \longrightarrow & \mathbf{Z}_2 \\ & & (x, y) & \longmapsto & \bar{p}(x, y) \end{array} \mid p \in \mathbf{Z}_2[x_1, x_2\,;\, \mathbf{K}(\tau_{\text{ring1}}, \Sigma_{\text{c ring 1}})] \right\},$$

   which means that $P_2(\Gamma)$ is the set of the "usual" binary polynomial functions.

   (c) $P_2^2(\Gamma) =$

   $$\left\{ \begin{array}{cccc} f & : & {\mathbf{Z}_2}^2 & \longrightarrow & {\mathbf{Z}_2}^2 \\ & & (x, y) & \longmapsto & \begin{pmatrix} \bar{p}(x, y) \\ \bar{q}(x, y) \end{pmatrix} \end{array} \mid p, q \in \mathbf{Z}_2[x_1, x_2\,;\, \mathbf{K}(\tau_{\text{ring1}}, \Sigma_{\text{c ring 1}})] \right\}$$

   (d) $Mat_2(P(\Gamma)) =$

   $$\left\{ \begin{array}{cccc} f & : & {\mathbf{Z}_2}^2 & \longrightarrow & {\mathbf{Z}_2}^2 \\ & & (x, y) & \longmapsto & \begin{pmatrix} \bar{p}_1(x) + \bar{p}_2(y) \\ \bar{q}_1(x) + \bar{q}_2(y) \end{pmatrix} \end{array} \mid p_1, p_2, q_1, q_2 \in \mathbf{Z}_2[x_1\,;\, \mathbf{K}(\tau_{\text{ring1}}, \Sigma_{\text{c ring 1}})] \right\}$$

   This needs a proof:
   "$\supseteq$": Let M be an arbitrary but fixed element of the right hand side. Then it is clear how M can be built up from the generators of $Mat_2(P(\Gamma))$. Hence M is contained in $Mat_2(P(\Gamma))$.
   "$\subseteq$": We observe immediately that the right-hand side contains the generators of $Mat_2(P(\Gamma))$. Hence it is sufficient to show that it is a near-ring.

It is obvious that it is closed under $+$, hence let us compose two functions. We will write $\lambda xy.f(x,y)$ for the function that maps (x,y) to $(f(x),f(y))$.

$$\lambda xy.\begin{pmatrix} \bar{p}_1(x)+\bar{p}_2(y) \\ \bar{q}_1(x)+\bar{q}_2(y) \end{pmatrix} \circ \lambda xy.\begin{pmatrix} \bar{p}'_1(x)+\bar{p}'_2(y) \\ \bar{q}'_1(x)+\bar{q}'_2(y) \end{pmatrix} =$$

$$\lambda xy.\begin{pmatrix} \bar{p}_1(\bar{p}'_1(x)+\bar{p}'_2(y))+\bar{p}_2(\bar{q}'_1(x)+\bar{q}'_2(y)) \\ \bar{q}_1(\bar{p}'_1(x)+\bar{p}'_2(y))+\bar{q}_2(\bar{q}'_1(x)+\bar{q}'_2(y)) \end{pmatrix} =$$

$$\lambda xy.\begin{pmatrix} \bar{p}_1(\bar{p}'_1(x))+\bar{p}_1(\bar{p}'_2(y))-\bar{p}_1(0)+\bar{p}_2(\bar{q}'_1(x))+\bar{p}_2(\bar{q}'_2(y))-\bar{p}_2(0) \\ \bar{q}_1(\bar{p}'_1(x))+\bar{q}_1(\bar{p}'_2(y))-\bar{q}_1(0)+\bar{q}_2(\bar{q}'_1(x))+\bar{q}_2(\bar{q}'_2(y))-\bar{q}_2(0) \end{pmatrix}$$

The last equality holds because $f(x+y)=f(x)+f(y)-f(0)$ holds for all functions in $M(\mathbf{Z}_2)$. In the last expression, each component is the sum of two univariate polynomial functions, as required.

(e) $Mat_2(M(\Gamma)) = Mat_2(P(\Gamma))$ because of $M(\Gamma)=P(\Gamma)$.

(f) $M(\Gamma^m)$ is the set of all functions from Γ^m to Γ^m.

This example is interesting because $\lambda xy.\begin{pmatrix} x\cdot y \\ 0 \end{pmatrix}$ is in $P_2^2(\Gamma)$, but not in $Mat_2(P(\Gamma))$.

2. Let $\Gamma \in \mathbf{K}(\tau_{\text{ring1}}, \Sigma_{\text{c ring 1}})$ be a field with $char(\Gamma) \neq 2$. Then we have

$$Mat_2(P(\Gamma)) = P_2^2(\Gamma)$$

We leave the proof to the reader. (Hint: The equality $(x+y)^2-(x-y)^2=4xy$ helps to build the product of two functions.)

For studying whether an algebra is (locally) m-polynomially complete, we have to study $P_m(A)$. It is clear how one can define the n-interpolation property for $P_m(A)$:

Definition 4.44 *Let A be an Ω-algebra. Then $F \subseteq F_m(A)$ has the n-interpolation property:* $\Longleftrightarrow$

$$\forall \vec{x}_1, \vec{x}_2, \ldots, \vec{x}_n \in A^m$$
$$\forall y_1, y_2, \ldots, y_n \in A$$
$$\exists f \in F :$$
$$f(\vec{x}_j) = y_i \textit{ for } i = 1,2,\ldots,n$$

We recall that Γ is locally m-polynomially complete iff $P_m(\Gamma)$ has the n-interpolation property for all $n \in \mathbf{N}$. Now we give the relation between the n-interpolation property for $P_m(\Gamma)$ and $P_m^m(\Gamma)$.

Theorem 4.45 *Let Γ be an Ω-group. Then the following are equivalent.*

1. *$P_m(\Gamma)$ has the n-interpolation property.*

2. *$P^m_m(\Gamma)$ has the n-interpolation property.*

Proof:
(1.) $\Rightarrow$ (2.): Find the interpolating polynomial function matrix coordinate-wise.
(2.) $\Rightarrow$ (1.): For finding the interpolating functions whose graph passes through all points in

$$\{(\vec{x}_i, y_i),\ i = 1, 2, \dots n\}$$

use (2.) to construct a function through

$$\{(\vec{x}_i, (y_i, 0, 0 \dots, 0))\, i = 1, 2, \dots n\}$$

and take the polynomial function in the first coordinate of the thereby obtained polynomial function matrix. □

Let us now combine the result and see what is still missing for the proof of: locally 1-polynomially complete $\Rightarrow$ locally m-polynomially complete.

We assume that Γ is locally 1-polynomially complete. For proving that Γ is locally n-polynomially complete (theorem 4.45) indicates that it is sufficient to show:

$$P^m_m(\Gamma) \text{ is dense in } M(\Gamma^m)$$

We will actually show something even stronger:

$$Mat_m(P(\Gamma)) \text{ is dense in } M(\Gamma^m)$$

We prove this using the transitivity of the relation of being dense. This transitivity is a consequence of the idempotence of the operator L_∞. We are going to prove the following chain:

$$Mat_m(P(\Gamma)) \text{ dense in } Mat_m(M(\Gamma)) \text{ dense in } M(\Gamma^m). \tag{4.17}$$

For the second "dense in"-relation we will need:

$$|\Gamma| \geq 3.$$

The first "dense in"-relation is guaranteed by the assumption that Γ is locally 1-polynomially complete and (corollary 4.42). Hence what remains to show is:

Theorem 4.46 *Let Γ be an Ω-group with $|\Gamma| \geq 3$. Then we have:*

$$Mat_m(M(\Gamma)) \textit{ dense in } M(\Gamma^m).$$

Proof: We proceed by induction on m.

- **Base case** $m = 1$: $Mat_1(M(\Gamma)) = M(\Gamma) = M(\Gamma^1)$.

- **Induction step** $m-1 \to m$:
Let $a, b \in \Gamma$ with $a \neq 0, b \neq 0, a \neq b$. Let $n \in \mathbf{N}$ and $x^{(1)}, x^{(2)}, \ldots, x^{(n)} \in \Gamma^m$ be arbitrary but fixed. It is sufficient to show that for $j \in \{1, 2, \ldots, n\}$ there exists a function $f \in Mat_m(M(\Gamma))$ with
$$f(x^{(i)}) = \begin{cases} (a, 0, \ldots, 0) & \text{for } i = j \\ (0, 0, \ldots, 0) & \text{for } i \neq j \end{cases} \tag{4.18}$$
W.l.o.g. let $j := 1$. By induction hypothesis there is $f_1 \in Mat_{m-1}\Gamma$ with
$$f_1(\left(x^{(1)}{}_1, x^{(1)}{}_2, \ldots, x^{(1)}{}_{m-1}\right)) = (a, 0, \ldots, 0)$$
and
$$f_1(\left(x^{(i)}{}_1, x^{(i)}{}_2, \ldots, x^{(i)}{}_{m-1}\right)) = (0, 0, \ldots, 0)$$
$$\text{for all i} \in \{2, 3, \ldots, n\} \text{ with}$$
$$\left(x^{(i)}{}_1, x^{(i)}{}_2, \ldots, x^{(i)}{}_{m-1}\right) \neq \left(x^{(1)}{}_1, x^{(1)}{}_2, \ldots, x^{(1)}{}_{m-1}\right).$$
We can also find an $f_2 \in M(\Gamma)$ with
$$f_2(x^{(1)}{}_m) = b$$
and
$$f_2(x^{(i)}{}_m) = 0 \text{ for all i} \in \{2, 3, \ldots, n\} \text{ with } x^{(i)}_m \neq x^{(1)}{}_m.$$
Let $f_3 \in M(\Gamma)$ be such that:
$$f_3(a-b) = a$$
and
$$f_3(a) = f_3(-b) = f_3(0) = 0.$$
Note that it can happen that $a = -b$, but this does not matter because f_3 assigns the same value to a and to $-b$. The assumptions guarantee that $a - b$ is different from a, $-b$ and 0.
Then $f_4 \in Mat_m(\Gamma)$ defined by
$$\begin{array}{cccc} f_4 : & \Gamma^m & \longrightarrow & \Gamma^m \\ & (y_1, y_2, \ldots, y_m) & \longmapsto & (f_3(f_1(y_1, y_2, \ldots, y_{m-1}) - f_2(y_m)), 0, \ldots, 0) \end{array}$$
is the f required in (4.18).

Hence we get the desired

Theorem 4.47 *Let Γ be an Ω-group with $|\Gamma| \geq 3$. If Γ is locally 1-polynomially complete then Γ is locally m-polynomially complete for all $m \in \mathbf{N}$.*

4.6 Jacobson's density theorem for rings

In this section we will prove a common ancestor to the density theorem for rings and the density theorem for near-rings. These two theorems say:

Let F be a sub-near-ring of $M(\Gamma)$, where Γ is a group, $F = F_0$ and F contains the identity function. If F is 2-primitive on Γ and if F is not a ring, then F is dense in the near-ring $M_{End_F(\Gamma)}(\Gamma)$. If F is a ring with identity and primitive on Γ, then by Jacobson's theorem (cf. [Pil84]) F is dense in the ring of all vector-space homomorphisms of the vector-space ${}_{End_F(\Gamma)}\Gamma$. (Note that $End_F(\Gamma)$ is a division ring in this case.)

[Mli75] has extracted the ideas of the proof of Jacobson's density theorem for investigating density in universal algebras. We will present his ideas in the context of near-rings. For me, proof of the near-ring density theorem given in this section and the proof following H.K.Kaiser's ideas have a completely different flavour: H.K.Kaiser constructs a "Lagrange interpolation function" by an algorithm. In this section, an indirect proof is given: If the "Lagrange interpolation function" did not exist then there would be a forbidden F - homomorphism from Γ^n to Γ for some n.

We will first define a class of near-rings that comprises both matrix rings and bicentralizer near-rings. Then we will show that each 2-primitive near-ring with identity is actually dense in a near-ring of that class.

4.6.1 Another version of bicentralizer near-rings

Definition 4.48 *Let Γ be a group and let S be a set that satisfies the following properties.*

1. $S = \bigcup_{i=1}^{\infty} S_i$
2. $\forall i \in \mathbf{N} : S_i \subseteq Hom(\Gamma^i, \Gamma)$, *where $Hom(\Gamma^i, \Gamma)$ denotes the set of all group-homomorphisms from Γ^i to Γ.*

Then we define the set $M^S(\Gamma)$ by:

$$\begin{aligned} M^S(\Gamma) \ := \ & \{m \in M(\Gamma) | \forall n \in \mathbf{N}\, \forall s \in S_n\, \forall x_1, x_2, \ldots, x_n \in \Gamma : \\ & m(s(x_1, x_2, \ldots, x_n)) = s(m(x_1), m(x_2), \ldots, m(x_n))\} \end{aligned}$$

Theorem 4.49 *Let Γ and S be as in (definition 4.48). Then we have:*

$$M^S(\Gamma) \text{ is a near-ring.}$$

Proof: Straightforward.

A 2-primitive, zero-symmetric near-ring with identity which is not a ring is dense in the near-ring of all those functions that commute with F-homomorphisms from Γ to Γ. We can include the ring-case if we take the near-ring of all those functions that commute with the F-homomorphisms from Γ^i to Γ for all $i \in \mathbf{N}$.

4.6.2 A common ancestor of Jacobson's and Wielandt-Betsch's density theorems

Theorem 4.50 *Let Γ be a group and F be a sub-near-ring of $M(\Gamma)$ with the following properties.*

1. $F = F_0$
2. F *is 2-primitive*
3. $id \in F$

Let $MEnd_F(\Gamma)$ be defined by[5]

$$MEnd_F(\Gamma) := \bigcup_{i=1}^{\infty} Hom_F(\Gamma^i, \Gamma)$$

(Note that Γ^i is an F-group with $f * (\gamma_1, \gamma_2, \dots, \gamma_i) := (f(\gamma_1), f(\gamma_2), \dots, f(\gamma_i))$.) Then we have:

$$F \text{ is dense in } M^{MEnd_F(\Gamma)}(\Gamma)$$

For proving this theorem we will need a concept similar to linear independence.

Definition 4.51 *A vector $\gamma_1, \gamma_2, \dots, \gamma_n$ is $MEnd_F(\Gamma)$ - independent:$\Longleftrightarrow$*

1. $\forall i : \gamma_i \neq 0$
2. *There is no $i \in \{2, 3, \dots, n\}$ such that*

$$\exists h \in Hom_F(\Gamma^{i-1}, \Gamma) : h(\gamma_1, \gamma_2, \dots, \gamma_{i-1}) = \gamma_i$$

We will now prove the following interpolation lemma:

Lemma 4.52 *Let Γ be a group and F be a sub-near-ring of $M(\Gamma)$ with the following properties.*

1. $F = F_0$
2. F *is 2-primitive*
3. $id \in F$

Let $x_1, x_2, \dots, x_n \in \Gamma$ such that $x_1, x_2, \dots, x_n$ are $MEnd_F(\Gamma)$-independent. Then we have:

$$\forall y_1, y_2, \dots, y_n \in \Gamma \, \exists f \in F$$
$$\forall i \in \{1, 2, \dots, n\} : f(x_i) = y_i$$

[5] $MEnd_F(\Gamma)$ stands for "M"ulti-ary F-"End"omorphisms

Proof: We proceed by induction on n:

- **Base case** $n = 1$: $Fx_1 = \Gamma$ by the 2-primitivity of F
- **Induction step** $n-1 \to n$: Let $x_1, x_2, \ldots, x_n$ be arbitrary but fixed $MEnd_F(\Gamma)$-independent elements of Γ First we use the induction hypothesis to construct $s_1 \in F$ such that

$$s_1(x_i) = y_i \text{ for } i \in \{1, 2, \ldots, n-1\}.$$

(Note that $(x_1, x_2, \ldots, x_{n-1})$ is $MEnd_F(\Gamma)$-independent.) Now it is sufficient to construct an $s_2 \in F$ with

$$s_2(x_i) = 0 \text{ for } i \in \{1, 2, \ldots, n-1\}$$

and

$$s_2(x_n) := y_n - s_1(x_n).$$

Since

$$R := \{f(x_n) | f \in F \text{ and } f(x_1) = f(x_2) = \cdots = f(x_{n-1}) = 0\}$$

is a sub-F-group of ${}_F\Gamma$, it is sufficient to show

$$R \neq \{0\}.$$

Suppose that $R = \{0\}$. Then the mapping h defined by

$$h \ : \ \Gamma^{n-1} \ \longrightarrow \ \Gamma$$

and the property

$$\forall f \in F : h\left((f(x_1), f(x_2), \ldots, f(x_{n-1}))\right) := f(x_n)$$

is a well-defined mapping from Γ^{n-1} to Γ. It can easily be checked that $h \in Hom_F(\Gamma^{n-1}, \Gamma)$. Since $id \in F$, we have

$$h\left((x_1, x_2, \ldots, x_{n-1})\right) := x_n,$$

which is a contradiction to the $MEnd_F(\Gamma)$-independence of $(x_1, x_2, \ldots, x_n)$. $\square$

We are now ready to prove (theorem 4.50). Let $m \in M^{MEnd_F(\Gamma)}(\Gamma)$ be arbitrary but fixed. Let $x_1, x_2, \ldots, x_n$ be arbitrary but fixed elements of Γ. We will construct $f \in F$ such that

$$f(x_k) = m(x_k) \text{ for } k \in \{1, 2, \ldots, n\}. \tag{4.19}$$

We will now extract a "maximal independent" vector out of $x_1, x_2, \ldots, x_n$ in the following way. Let d be maximal such that there exists a vector $(x_{i_1}, x_{i_2}, \ldots, x_{i_d})$ with the property that $(x_{i_1}, x_{i_2}, \ldots, x_{i_d})$ is $MEnd_F(\Gamma)$-independent. By the interpolation lemma (lemma 4.52) we get a function $f \in F$ with

$$f(x_{i_j}) = m(x_{i_j}) \text{ for } j \in \{1, 2, \ldots, d\}. \tag{4.20}$$

We will now show that f satisfies (4.19). Let $k \in \{1, 2, \ldots, n\}$ be arbitrary but fixed. If $k \in \{i_1, i_2, \ldots, i_d\}$, then (4.19) is immediate. If $k \notin \{1, 2, \ldots, n\}$ then by the maximality of d, $(x_{i_1}, x_{i_2}, \ldots, x_{i_d}, x_k)$ is $MEnd_F(\Gamma)$-dependent. In this case there is $h \in Hom_F(\Gamma^d, \Gamma)$ with

$$h(x_{i_1}, x_{i_2}, \ldots, x_{i_d}) = x_k.$$

Hence we get

$$f(x_k) = f(h(x_{i_1}, x_{i_2}, \ldots, x_{i_d}))$$

Since h is an F-endomorphism, this is equal to

$$h(f(x_{i_1}), f(x_{i_2}), \ldots, f(x_{i_d}))$$

By (4.20) this is equal to

$$h(m(x_{i_1}), m(x_{i_2}), \ldots, m(x_{i_d})) =$$

$$= m(h(x_{i_1}, x_{i_2}, \ldots, x_{i_d})) = m(x_k).$$

□

4.6.3 Deriving Jacobson's and Wielandt-Betsch's results

We will now try to characterize $End_F(\Gamma^i, \Gamma)$. Note:

$$h\,(x_1, x_2, \ldots, x_i) = h(x_1, 0, 0, 0, \ldots) + h(0, x_2, 0, 0, \ldots) + h(0, 0, x_3, 0, \ldots) + \cdots + h(0, 0, \ldots, x_i).$$

This means that any F-homomorphism h from Γ^i to Γ can be written in the form:

$$h(x_1, x_2, \ldots, x_i) = h_1(x_1) + h_2(x_2) + \cdots + h_i(x_i), \tag{4.21}$$

where $h_j \in End_F(\Gamma)$ for $j = 1, 2, \ldots, i$. We will formalize this in the following definition.

Definition 4.53 *Let Γ be a group and F be a sub-near-ring of $M(\Gamma)$. Then we define Φ by:*

$$\begin{array}{rccc} \Phi & : & Hom_F(\Gamma^i, \Gamma) & \longrightarrow & End_F(\Gamma)^i \\ & & h & \longmapsto & (h_1, h_2, \ldots, h_i) \end{array}.$$

h_j is defined by:

$$\begin{array}{rcccc} h_j & : & \Gamma & \longrightarrow & \Gamma \\ & & \gamma & \longmapsto & h(0, 0, \ldots, 0, \gamma, 0, \ldots, 0) \end{array}$$

where γ stands at the j-th place.

With this definition, (4.21) holds. Actually, for each permutation π of $\{1, 2, \ldots, i\}$ we have:

$$h(x_1, x_2, \ldots, x_i) = h_{\pi(1)}(x_{\pi(1)}) + h_{\pi(2)}(x_{\pi(2)}) + \cdots + h_{\pi(i)}(x_{\pi(i)})$$

Now we shall see the difference between the ring and the non-ring case.

Theorem 4.54 *Let $i \in N$ and let F be a sub-near-ring of $M(\Gamma)$.*
If

1. $F = F_0$
2. *F is 2-primitive*
3. $id \in F$
4. *F is a ring*

then
Φ is surjective.

Sketch of the proof: For each $(h_1, h_2, \ldots, h_i) \in End_F(\Gamma)^i$,

$$\begin{array}{cccc} h & : & \Gamma^i & \longrightarrow & \Gamma \\ & & x_1, x_2, \ldots, x_i & \longmapsto & h_1(x_1) + h_2(x_2) + \cdots + h_i(x_i) \end{array}$$

turns out to be an element of $Hom_F(\Gamma^i, \Gamma)$.

Theorem 4.55 *Let $i \in N$ and let F be a sub-near-ring of $M(\Gamma)$.*
If

1. $F = F_0$
2. *F is 2-primitive*
3. $id \in F$
4. *F is not a ring*

then

$$\Phi(Hom_F(\Gamma^i, \Gamma)) =$$
$$\{(h, 0, 0, \ldots, 0) | h \in End_F(\Gamma)\} \cup \{(0, h, 0, \ldots, 0) | h \in End_F(\Gamma)\} \cup \ldots$$
$$\ldots \cup \{(0, 0, \ldots, 0, h, 0) | h \in End_F(\Gamma)\} \cup \{(0, 0, 0, \ldots, h) | h \in End_F(\Gamma)\}$$

Proof: Suppose there exists an $h \in Hom_F(\Gamma^i, \Gamma)$ such that $\Phi(h) = (h_1, h_2, \ldots, h_i)$ has the property that there are $k, l \in \{1, 2, \ldots, i\}$ with $k \neq l$, $h_k \neq 0$ and $h_l \neq 0$.

- **Case** $(F,+)$ is not abelian: In this case, Γ is not abelian, hence there are $a, b \in \Gamma$ such that $a+b \neq b+a$. Since h_k is bijective, we find $x_1 \in \Gamma$ such that $h_k(x_1) = a$. In the same way, let $x_2 \in \Gamma$ be such that $h_l(x_2) = b$. Now let $(z_1, z_2, \ldots, z_i) \in \Gamma^i$ be defined by:

$$z_m := \begin{cases} x_1 & \text{for} \quad m = k \\ x_2 & \text{for} \quad m = l \\ 0 & \text{else} \end{cases}$$

  Then we have:
$$h(\vec{z}) = h_k(x_1) + h_l(x_2)$$
  and also
$$h(\vec{z}) = h_l(x_2) + h_k(x_1).$$
  From this, it follows that $a+b = b+a$, which is a contradiction.

- **Case** There is a function $f \in F$ such that there are $a, b \in \Gamma$ with $f(a+b) \neq f(a)+f(b)$. We define x_1, x_2 and $\vec{z}$ as in the case above. Then we have: $f(a+b) = f(h_k(x_1)+h_l(x_2)) = f(h(\vec{z})) = h(f(z_1), f(z_2), \ldots, f(z_i)) = h_k(f(z_k)) + h_l(f(z_l)) = f(h_k(z_k)) + f(h_l(z_l)) = f(h_k(x_1)) + f(h_l(x_2)) = f(a)+f(b)$, which is a contradiction. $\square$

Now we get:

Theorem 4.56 *Let Γ be a group, F a sub-near-ring of $M(\Gamma)$. Suppose that $F = F_0$, $id \in F$ and F is 2-primitive. If F is a ring then we have:*

1. *$End_F(\Gamma)$ is a division ring.*
2. *$M^{MEnd_F(\Gamma)}(\Gamma)$ is the set of all linear mappings from the vector space ${}_{End_F(\Gamma)}\Gamma$ into itself.*

The proof of (1.) can be found in [Pil84]. Now we show (2.). Let h be in $M^{MEnd_F(\Gamma)}(\Gamma)$. We show that h is linear. For doing so, let $x, y \in \Gamma$ and $\lambda, \mu \in End_F(\Gamma)$. The mapping r defined by

$$\begin{array}{rcccc} r & : & \Gamma^2 & \longrightarrow & \Gamma \\ & & (\gamma_1, \gamma_2) & \longmapsto & \lambda(\gamma_1) + \mu(\gamma_2) \end{array}$$

is in $MEnd_F(\Gamma)$, therfore we have: $h(\lambda x + \mu y) = h(r(x,y)) = r(h(x), h(y)) = \lambda h(x) + \mu h(y)$. On the other hand, it is easy to show that each linear mapping is in $M^{MEnd_F(\Gamma)}(\Gamma)$. $\square$

Jacobson's theorem now follows immediately.

For the density theorem for 2-primitive near-rings, we have to show one thing:

Theorem 4.57 *Let Γ be a group, F a sub-near-ring of $M(\Gamma)$. Suppose that $F = F_0$, $id \in F$ and F is 2-primitive. If F is not a ring then $M^{MEnd_F(\Gamma)}(\Gamma) = M_{End_F(\Gamma)}(\Gamma)$.*

Proof: "$\subseteq$" is trivial, because $End_F(\Gamma) \subseteq MEnd_F(\Gamma)$.
"$\supseteq$": Let $f \in M_{End_F(\Gamma)}(\Gamma)$, let $i \in \mathbf{N}$ and let h be an element of $Hom_F(\Gamma^i, \Gamma)$. By the characterization of $Hom_F(\Gamma^i, \Gamma)$ we have a j such that $f(h(x_1, x_2, \ldots, x_i)) = f(h_j(x_j)) = h_j(f(x_j)) = h(f(x_1), f(x_2), \ldots, f(x_i))$.

I think that this way of proving the density theorems is interesting because:

- It reveals common aspects of Jacobson's and Wielandt-Betsch's theorems.
- For (theorem 4.50 it is not necessary that Γ is a group. This theorem remains true for algebras $(A, +, -, 0)$, where $+$ and $-$ are binary and the 0 is a nullary function and the following laws are fulfilled:

  1. $x + 0 = x$
  2. $x + (z - x) = z$
  3. $0 - 0 = 0$

  The approach presented here leads the way to the definition of primitivity for a large class of composition-algebras. Note that the characterization of primitive composition-groups, i.e. the characterization of primitive rings and 2-primitive near-rings has been very fruitful in many respects, as for example in determining simple rings and near-rings, resp.

4.7 Literature and sources

[Pil80] introduces the near-rings $L_nP(\Gamma)$. The properties of $L_nP(\Gamma)$, as for example $L_2P(\Gamma) = C(\Gamma)$, can be found in [Pil83]. The study of the near-ring L_nF for arbitrary near-rings F is motivated by a concept of completeness which contains polynomial completeness as a special case that is explained, e.g., in the *remarks and comments*-section of [LN73], chapter 1, section 11. I think that the results on L_nF, such as (theorem 4.5) and (corollary 4.7) have not yet appeared in the literature. (Theorem 4.16) is very similar to the interpolation theorem for 0-primitive near-rings due to [Bet73a]. The proof given in this thesis is new in the context of near-rings. It has the advantage that it yields an interpolation algorithm in some cases. The ideas of the proof of (theorem 4.16), such as e.g. the introduction of a function k, can be found in [IK79]. (Theorem 4.29) is actually a common instance of (theorem 2) in [IK79] and (theorem 4.16). Although these two results are the same for polynomials over Ω-groups, they generalize (theorem 4.29) into two different directions:

- (Theorem 2) of [IK79] can also be applied to polynomial algebras $P(A)$ where A is not an Ω-group, but just any universal algebra.
- (Theorem 4.16) can be also applied to other near-rings than $P(A)$. A, however, has to be an Ω-group.

The density theorem for 2-primitive near-rings can be found in [Bet73b] and in [Pil83]. The well-known corollaries about polynomially complete Ω-groups somehow follow more smoothly from (theorem 4.29) than from the density theorems for near-rings because using (theorem 4.29) we do not have to bother about the F-endomorphisms of ${}_F\Gamma$. (Theorem 4.34) is new. The definition of matrix near-rings (definition 4.39) and also the results follow the ideas of [MVdW86]. (Theorem 4.47) has already been proved in [Slu39].

[Mli75] has generalized Jacobson's density theorem and the corresponding radical theory to universal algebras.

Chapter 5

Local polynomials on the integers

5.1 Characterization of $L_nP(\mathbf{Z})$

5.1.1 Statement of the result

In this chapter, we consider $\mathbf{Z}$ as a commutative ring with 1. We will keep the classical notations and shall therefore write $\mathbf{Z}[x]$ for $\mathbf{Z}[x;\Sigma_{\text{c ring 1}}]$. We shall use $\circ$ for both the composition of functions and the substitution of polynomials (as defined in (definition 1.90)).

For the characterization of $L_nP(\mathbf{Z})$, we need some definitions.

Definition 5.1 *Let $n, i \in \mathbf{N}$ Then*

$$PS(n,i) := \{k_1k_2\cdots k_n | k_1, k_2, \ldots, k_n \in \{1,2,\ldots,i\} \text{ and}$$

$$\forall j_1, j_2 \in \{1,2,\ldots,n\} : k_{j_1} = k_{j_2} \Rightarrow (j_1 = j_2 \vee k_{j_1} = k_{j_2} = 1)\}$$

For $n = 0$ or $i = 0$ we define

$$PS(n,0) = PS(0,i) := \emptyset$$

$PS(n,i)$ is the set of all products of at most n different numbers lying in $\{1,2,\ldots,n\}$. We give two examples.

1. The set $PS(3,7)$ is given by $PS(3,7) = \{1\cdot1\cdot1,\ 1\cdot1\cdot2,\ 1\cdot1\cdot3,\ 1\cdot1\cdot4,\ 1\cdot1\cdot5,\ 1\cdot1\cdot6,\ 1\cdot1\cdot7,\ 1\cdot2\cdot3, 1\cdot2\cdot4, 1\cdot2\cdot5, 1\cdot2\cdot6, 1\cdot2\cdot7, 1\cdot3\cdot4,\ 1\cdot3\cdot5,\ 1\cdot3\cdot6,\ 1\cdot3\cdot7,\ 1\cdot4\cdot5,\ 1\cdot4\cdot6,\ 1\cdot4\cdot7,\ 1\cdot5\cdot6,\ 1\cdot5\cdot7,\ 1\cdot6\cdot7,\ 2\cdot3\cdot4,\ 2\cdot3\cdot5,\ 2\cdot3\cdot6,\ 2\cdot3\cdot7,\ 2\cdot4\cdot5,\ 2\cdot4\cdot6,\ 2\cdot4\cdot7,\ 2\cdot5\cdot6,\ 2\cdot5\cdot7,\ 2\cdot6\cdot7,\ 3\cdot4\cdot5,\ 3\cdot4\cdot6,\ 3\cdot4\cdot7,\ 3\cdot5\cdot6,\ 3\cdot5\cdot7,\ 3\cdot6\cdot7,\ 4\cdot5\cdot6,\ 4\cdot5\cdot7,\ 4\cdot6\cdot7,\ 5\cdot6\cdot7\}$

2. The set $PS(7,3)$ is given by $PS(7,3) = \{1\cdot1\cdot1\cdot1\cdot1\cdot1\cdot1,\ 1\cdot1\cdot1\cdot1\cdot1\cdot1\cdot2,\ 1\cdot1\cdot1\cdot1\cdot1\cdot1\cdot3,\ 1\cdot1\cdot1\cdot1\cdot1\cdot2\cdot3\}$

Definition 5.2 *We define $A(n,i)$ by*

$$A(n,i) = lcm(PS(n,i)),$$

where $lcm(S)$ denotes the least common multiple of a set S of numbers and $lcm(\emptyset) = 1$.

Examples:

1. $A(1,i)$ is the least common multiple of $1, 2, \ldots, n$.
2. $A(i,i) = A(i+1,i) = A(i+2,i) = \cdots = i\,!$.
3. The following table shows the values of $A(n,i)$ for small n, i.

$A(n,i)$	$i=0$	$i=1$	$i=2$	$i=3$	$i=4$	$i=5$	$i=6$	$i=7$	$i=8$
$n=0$	1	1	1	1	1	1	1	1	1
$n=1$	1	1	2	6	12	60	60	420	840
$n=2$	1	1	2	6	24	120	360	2520	10080
$n=3$	1	1	2	6	24	120	720	5040	20160
$n=4$	1	1	2	6	24	120	720	5040	40320
$n=5$	1	1	2	6	24	120	720	5040	40320

Theorem 5.3 (Local polynomials on the naturals) *Let $n \in \mathbf{N}$. Then all functions*

$$f \;:\; \mathbf{N} \longrightarrow \mathbf{Z}$$

with the property:

$$\forall x_1, x_2, \ldots, x_n \in \mathbf{N}\, \exists p \in \mathbf{Z}[x] :$$
$$f(x_i) = \bar{p}(x_i) \text{ for } i = 1, 2, \ldots, n$$

are given by:

$$f(x) = \sum_{i=0}^{\infty} c_i \cdot A(n-1,i) \binom{x-1}{i}$$

with

$$(c_i)_{i \in \mathbf{N}_0} \in \mathbf{Z}^{\mathbf{N}_0}$$

For $n = 2$, this is a result of [Hal71]. And now, we give the desired characterization of $L_nP(\mathbf{Z})$.

Theorem 5.4 *The mapping Φ maps $\mathbf{Z}^{\mathbf{Z}}$ bijectively to $L_nP(\mathbf{Z})$, where*

$$\Phi\left((c_i)_{i \in \mathbf{Z}}\right)(x) =$$

$$\sum_{j=1}^{\infty} c_j A(n-1, 2j-1) \binom{x+j-1}{2j-1} + \sum_{j=0}^{\infty} c_{-j} A(n-1, 2j) \binom{x+j-1}{2j}$$

Note that the above sums are finite for any $x \in \mathbf{Z}$, because $j > |x|$ implies $\binom{x+j-1}{2j-1} = \binom{x+j-1}{2j} = 0$.

5.1.2 The proof

Local polynomials on finite domains

For the proof of (theorem 5.4), let the sequence $(z_i)_{i\in\mathbf{Z}} \in \mathbf{Z}^{\mathbf{N}_0}$ be defined by

$$z_k := \begin{cases} \frac{1}{2}(k+1) & \text{for} \quad k \text{ odd} \\ -\frac{1}{2}k & \text{for} \quad k \text{ even} \end{cases}$$

where $k \in \mathbf{N}_0$. $(z_i)_{i\in\mathbf{Z}}$ is an enumeration of the integers with

$$z_0 = 0,\ z_1 = 1,\ z_2 = -1,\ z_3 = 2\, z_4 = -2\ \ldots.$$

We will now look at those functions that can be interpolated by a polynomial at any n places taken from $\{z_1, z_2, \ldots, z_m\}$.
Definition 5.5

$$L(n,m) := \{\ f \ :\ \mathbf{Z} \ \longrightarrow\ \mathbf{Z} \mid \forall i_1, i_2, \ldots, i_n \in \{0,1,2,\ldots,m\}\, \exists p \in \mathbf{Z}[x] :$$

$$\bar{p}(z_{i_j}) = f(z_{i_j}) \textit{ for } j = 1, 2, \ldots n\}$$

Lemma 5.6 *We have the following inclusions:*

1. $L_nP(\mathbf{Z}) \subseteq L(n,m)$ *for all* $m \in \mathbf{N}_0$
2. $\bigcap_{m\in\mathbf{N}_0} L(n,m) = L_nP(\mathbf{Z})$

Definition 5.7 *For each* $n \in \mathbf{N}, m \in \mathbf{N}_0$*, we define an ideal* $I(n,m)$ *of* $\mathbf{Z}$ *by:*

$$I(n,m) := \{f(z_m) | f(z_0) = f(z_1) = \cdots = f(z_{m-1}) = 0 \textit{ and } f \in L(n,m)\}$$

One immediately checks that $I(n,m)$ is an ideal for all n, m. $I(n,m)$ always contains 0. Furthermore, it always contains at least one more element. For checking this, consider the polynomial $q \in \mathbf{Q}[x]$ with $\bar{q}(z_0) = \bar{q}(z_1) = \cdots = \bar{q}(z_{m-1}) = 0$ and $\bar{q}(z_m) = 1$. By multiplying the polynomial q with all denominators appearing in its coefficients, we get a polynomial q' with the properties $\bar{q}'(z_0) = \bar{q}'(z_1) = \cdots = \bar{q}'(z_{m-1}) = 0$ and $\bar{q}'(z_m) \neq 0$. Since q' is an element of $L(n,m)$, we get: $\bar{q}'(z_m) \in I(n,m)$.

We will give a name to the generators of these ideals:
Definition 5.8 *For each* $n \in \mathbf{N}, m \in \mathbf{N}_0$*, let*

$$g(n,m) := \textit{ the non-negative generator of } I(n,m)$$

Lemma 5.9
If *there exists a sequence* $(b_i)_{i\in\mathbf{N}_0}$ *with*

1. $b_i \in L_nP(\mathbf{Z})$

2. $b_i(z_0) = b_i(z_1) = b_i(z_2) = \cdots = b_i(z_{i-1}) = 0$
3. $b_i(z_i) = g(n, i)$

then *every $f \in L_nP(\mathbf{Z})$ can be written as:*

$$f(x) = \sum_{i=0}^{\infty} a_i \cdot b_i(x) \textit{ for all } x \in \mathbf{Z},$$

where $(a_i)_{i\in\mathbf{N}_0}$ is a sequence of integers. The a_i are furthermore unique.

Note:

- The above sum is finite for any $x \in \mathbf{Z}$, because for $x = z_i$ we get $b_{i+1}(z_i) = b_{i+2}(z_i) = \cdots = 0$.
- At this stage of the proof, we do not know whether such a sequence (b_i) actually exists. We just hope.

We now give the proof of (lemma 5.9):
Each $f : \mathbf{Z} \longrightarrow \mathbf{Z}$ can be written as

$$f = \sum_{i=0}^{\infty} q_i b_i,$$

where the $q_i \in \mathbf{Q}$ are unique. We get the q_i's as follows. Suppose, we have already computed $q_0, q_1, \ldots, q_{i-1}$. Then q_i has to be chosen such that

$$f(z_i) = \sum_{j=0}^{\infty} q_j b_j(z_i)$$

Since $b_j(z_i) = 0$ for $j > i$, this means

$$f(i) = \sum_{j=0}^{i} q_j b_j(z_i).$$

So, we compute q_i by

$$\frac{f(i) - \sum_{j=0}^{i-1} q_j b_j(z_i)}{b_i(z_i)} = q_i$$

(Note that not every sequence $(q_i)_{i\in\mathbf{N}_0}$ gives actually rise to a function $f : \mathbf{Z} \longrightarrow \mathbf{Z}$.)
Let $l \in L_nP(\mathbf{Z})$ be arbitrary but fixed. We find $a_i \in \mathbf{Q}$ such that

$$l = \sum_{i=0}^{\infty} a_i b_i.$$

Suppose that we have an $m \in \mathbf{N}_0$ with $a_m \notin \mathbf{Z}$. We take m_0 to be the smallest such m. Since $l \in L_n(P(\mathbf{Z}))$, we also have:

$$l = \sum_{i=0}^{\infty} a_i b_i \in L(n, m_0).$$

Since the summands $a_i b_i$ for $i > m_0$ make no contribution to $l(z_j)$ for $j \leq m_0$, we get:

$$l' = \sum_{i=0}^{m_0} a_i b_i \in L(n, m_0).$$

Now we notice that by the minimality of m_0 and by the assumption that b_i is in $L_n(P(\mathbf{Z}))$ we have

$$\sum_{i=0}^{m_0 - 1} a_i b_i \in L(n, m_0).$$

From this we get:

$$a_{m_0} b_{m_0} \in L(n, m_0).$$

Since $b_{m_0}(z_0) = b_{m_0}(z_1) = \cdots = b_{m_0}(z_{m_0-1}) = 0$ and $b_{m_0}(z_{m_0}) = g(n, m_0)$, we get:

$$a_{m_0} g(n, m_0) \in I(n, m_0).$$

All elements in $I(n, m_0)$ are divisible by $g(n, m_0)$, hence $a_{m_0} \in \mathbf{Z}$, which is a contradiction. □

We shall now give a lower bound (with respect to the divisibility relation) for $g(n, i)$.

Lemma 5.10

$$A(n-1, i) \text{ divides } g(n, i)$$

Proof: We show that each $p \in PS(n-1, i)$ divides $g(n, i)$. Let $p \in PS(n-1, i)$ be arbitrary but fixed. For showing that p divides $g(n, i)$ we prove that for each $l \in L(n, i)$ with $l(z_0) = l(z_1) = l(z_2) = \cdots = l(z_{i-1}) = 0$ we have:

$$p \text{ divides } l(z_i)$$

Let $l \in L(n, i)$ be arbitrary but fixed and assume that $l(z_0) = l(z_1) = l(z_2) = \cdots = l(z_{i-1}) = 0$. Let $n_0 \leq n$ and $d_1, d_2, \ldots, d_{n_0-1} \in \{1, 2, \ldots, i\}$ be such that

$$p = d_1 \cdot d_2 \cdots d_{n_0-1}$$

with d_i pairwise different.

- **Case** i is odd: Let l be an element of $L(n, i)$. Note that $z_i - j \in \{z_0, z_1, z_2, \ldots, z_{i-1}\}$ for $j \in \{1, 2, \ldots, i\}$. Hence we can find a polynomial $q \in \mathbf{Z}[x]$ such that $\bar{q}$ interpolates l at the places

$$z_i - d_1, z_i - d_2, z_i - d_3, \ldots, z_i - d_{n_0-1} \text{ and } z_i.$$

This q has the following properties:

$$\bar{q}(z_i - d_j) = 0 \text{ for } j = 1, 2, \ldots, n_0 - 1$$

and

$$\bar{q}(z_i) = l(z_i).$$

From our knowledge of polynomials over the field $\mathbf{Q}$ we know that

$$q = q_1 \prod_{j=1}^{n_0-1} \left(x - (z_i - d_j)\right), \tag{5.1}$$

where q_1 is a polynomial in $\mathbf{Q}[x]$. Since we can find q_1 by dividing the integer polynomial q by an integer polynomial with leading coefficient 1, we get:

$$q_1 \in \mathbf{Z}[x]$$

From (5.1) we get:

$$l(z_i) = \bar{q}(z_i) = \bar{q}_1(z_i) \prod_{i=1}^{n_0-1} d_j.$$

Therfore we have:

$$p = d_1 \cdot d_2 \cdot d_{n_0-1} \text{ divides } l(z_i),$$

which we wanted to prove.

- **Case** i even: Analogous.□

The next theorem does two jobs:

- It shows: $A(n-1, i) = g(n, i)$.
- It allows to produce an example of the b_i required in (lemma 5.9)

A "basis" for $L_nP(\mathbf{Z})$

Theorem 5.11 *Let $\beta_i^{(n)}$ be defined by:*

$$\begin{array}{rcccc} \beta_i^{(n)} & : & \mathbf{Z} & \longrightarrow & \mathbf{Z} \\ & & x & \longmapsto & \binom{x}{i} \cdot A(n-1, i) \end{array}$$

Then we have:

$$\beta_i^{(n)} \in L_nP(\mathbf{Z}).$$

Before we go on, I give a list of $\beta_i^{(n)}$ for small n, i.

$$
\begin{aligned}
&\beta_0^{(1)}(x) = 1\\
&\beta_1^{(1)}(x) = x\\
&\beta_2^{(1)}(x) = \tfrac{(-1+x)\,x}{2}\\
&\beta_3^{(1)}(x) = \tfrac{(-2+x)\,(-1+x)\,x}{6}\\
&\beta_4^{(1)}(x) = \tfrac{(-3+x)\,(-2+x)\,(-1+x)\,x}{24}\\
&\beta_5^{(1)}(x) = \tfrac{(-4+x)\,(-3+x)\,(-2+x)\,(-1+x)\,x}{120}\\
&\beta_0^{(2)}(x) = 1\\
&\beta_1^{(2)}(x) = x\\
&\beta_2^{(2)}(x) = (-1+x)\;x\\
&\beta_3^{(2)}(x) = (-2+x)\;(-1+x)\;x\\
&\beta_4^{(2)}(x) = \tfrac{(-3+x)\,(-2+x)\,(-1+x)\,x}{2}\\
&\beta_5^{(2)}(x) = \tfrac{(-4+x)\,(-3+x)\,(-2+\ x)\,(-1+x)\,x}{2}\\
&\beta_0^{(3)}(x) = 1\\
&\beta_1^{(3)}(x) = x\\
&\beta_2^{(3)}(x) = (-1+x)\;x\\
&\beta_3^{(3)}(x) = (-2+x)\;(-1+x)\;x\\
&\beta_4^{(3)}(x) = (-3+x)\;(-2+x)\;(-1+x)\;x\\
&\beta_5^{(3)}(x) = (-4+x)\;(-3+x)\;(-2+x)\;(-1+x)\;x\\
&\beta_6^{(3)}(x) = \tfrac{(-5+x)\,(-4+x)\,(-3+x)\,(-2+x)\,(-1+x)\,x}{2}
\end{aligned}
$$

Our proof will consist of three steps.

1. $\beta_i^{(n)}$ can be interpolated by a polynomial function at at most n places in $\{0, 1, 2, \ldots, m\}$ for all $m \in \mathbf{N}_0$.

2. $\beta_i^{(n)}$ can be interpolated by a polynomial function at at most n places in $\mathbf{N}_0$.

3. $\beta_i^{(n)} \in L_nP(\mathbf{Z})$

Step (1.)

Definition 5.12 *For $n \in \mathbf{N}$ and $m \in \mathbf{N}_0$ we define a set $LP(n, m)$ as follows:*

$$LP(n,m) := \{\ f\ :\ \mathbf{Z}\ \longrightarrow\ \mathbf{Z}\ |\forall x_1, x_2, \ldots, x_n \in \{0,1,2,\ldots,m\}\ \exists p \in \mathbf{Z}[x] :$$

$$\bar{p}(x_i) = f(x_i) \text{ for } i = 1, 2, \ldots n\ \}$$

Note that this definition also makes sense for $n > m$.

The following lemma is crucial. It says that we can compute the sets $LP(n, m)$ recursively:

Lemma 5.13 *Let $f\ :\ \mathbf{Z}\ \longrightarrow\ \mathbf{Z}$. Then we have:*

$$f \in LP(n, m)$$

$$\Longleftrightarrow$$

1. $f \circ \overline{x+1} \in LP(n, m-1)$ and
2. $x \mapsto \begin{cases} \frac{f(x+1)-f(0)}{x+1} & \textit{for} \quad x \neq -1 \\ 0 & \textit{for} \quad x = -1 \end{cases} \in LP(n-1, m-1)$

Proof: "$\Longrightarrow$":

- $f \circ \overline{x+1} \in LP(n, m-1)$ is immediate.
- Let g be defined by

$$g(x) := \begin{cases} \frac{f(x+1)-f(0)}{x+1} & \text{for} \quad x \neq -1 \\ 0 & \text{for} \quad x = -1 \end{cases}.$$

  Let $x_1, x_2, \ldots, x_{n-1} \in \{0, 1, 2, \ldots m-1\}$ be arbitrary but fixed. Since $f \in LP(n, m)$ there exists $p \in \mathbf{Z}[x]$ with

$$\bar{p}(x_i + 1) = f(x_i + 1) - f(0),\ i = 1, 2, \ldots, n-1$$

$$\bar{p}(0) = 0.$$

  (This p can be obtained by interpolating $x \mapsto f(x) - f(0)$.) Since $\bar{p}(0) = 0$, the polynomial p is divisible by x. Let $p_1 := \frac{p}{x}$. Then we have:

$$\bar{p}_1(x_i + 1) = \frac{f(x_i + 1) - f(0)}{x_i + 1},\ i = 1, 2, \ldots, n-1$$

  Since

$$\frac{f(x_i + 1) - f(0)}{x_i + 1} = g(x_i),\ i = 1, 2, \ldots, n-1$$

  p_1 is the required interpolation polynomial.

"$\Longleftarrow$" Let $x_1, x_2, \ldots, x_n$ be arbitrary but fixed.

- **Case** $x_1 \cdot x_2 \cdots x_n \neq 0$: By the assumptions we know:

$$f \circ \overline{x+1} \in LP(n, m-1).$$

  Hence there exists a polynomial $p \in \mathbf{Z}[x]$ such that

$$\bar{p}(x_i - 1) = f \circ \overline{x+1}\,(x_i - 1) \text{ for } i = 1, 2, \ldots, n$$

  Note that $x_i \neq 0$ guarantees us that all x_i are in $\{0, 1, 2, \ldots, m-1\}$. Take p_1 such that

$$\bar{p}_1 = \bar{p} \circ \overline{x-1}.$$

  Then we have:

$$\bar{p}_1(x_i) = \bar{p}(x_i - 1) = f \circ \overline{x+1}(x_i - 1) = f(x_i)$$

  Therefore p_1 is the required interpolation polynomial.

- Case $\exists i : x_i = 0$. W.l.o.g we take $i = 1$. By the assumptions we find a polynomial p with

$$\bar{p}(x_i - 1) = \frac{f(x_i) - f(0)}{x_i} \text{ for } i = 2, 3, \dots, n$$

(This p is found as follows: Since for $i \geq 2$ the x_i are in $\{1, 2, \dots, m\}$, all $x_i - 1$ are in $\{0, 1, \dots, m-1\}$. We then construct $\bar{p}$ by interpolating $x \mapsto \begin{cases} \frac{f(x+1)-f(0)}{x+1} & \text{for} \quad x \neq -1 \\ 0 & \text{for} \quad x = -1 \end{cases}$ at $x_i - 1$, $i = 2, 3, \dots, n$.)

Now let the polynomial p_1 be such that

$$\bar{p}_1(x) = \bar{p}(x-1) \cdot x + f(0) \text{ for all } x \in \mathbf{Z}$$

Then we have $\bar{p}_1(x_1) = 0 + f(0)$ and $\bar{p}_1(x_i) = \bar{p}(x_i - 1) \cdot x_i + f(0) = f(x_i)$. □

Lemma 5.14 *For all $m \in \mathbf{N}_0$ the proposition $P(m)$ holds, where $P(m)$ is defined by*

$$P(m) :\Leftrightarrow \forall n \in \mathbf{N}\, \forall i \in \mathbf{N}_0 : \ \beta_i^{(n)} \in LP(n, m)$$

Proof: We prove $P(m)$ by induction on m.

- **Base case** $m = 0$: $\beta_i^{(n)}(0)$ is an integer.

- **Induction step** $m - 1 \to m$: We fix $m \in \mathbf{N}$, $n \in \mathbf{N}$, $i \in \mathbf{N}_0$. We have to show:

$$\beta_i^{(n)} : x \mapsto \binom{x}{i} \cdot A(n-1, i) \text{ is an element of } LP(n, m).$$

For $i = 0$, one sees immediately that $\beta_i^{(n)} \in LP(n, m)$. Hence we assume $i \geq 1$. For $n = 1$, $\beta_i^{(n)} \in LP(n, m)$ is also obvious. Hence we assume $n \geq 2$. By "$\Leftarrow$" of (lemma 5.13), it is sufficient to show the following two propositions:

1. $x \mapsto \beta_i^{(n)} \circ \overline{x+1} \in LP(n, m-1)$
2. $x \mapsto \begin{cases} \frac{\beta_i^{(n)}(x+1) - \beta_i^{(n)}(0)}{x+1} \text{ for } x \neq -1 \\ 0 \text{ for } x = -1 \end{cases} \in LP(n-1, m-1)$.

We show (1.): We know that

$$\beta_i^{(n)}(x+1) = \binom{x+1}{i} \cdot A(n-1, i) = \left(\binom{x}{i-1} + \binom{x}{i}\right) \cdot A(n-1, i).$$

By the induction hypothesis $P(m-1)$ we know that

$$(x \mapsto \binom{x}{i-1} \cdot A(n-1, i-1)) \in LP(n, m-1).$$

Since $PS(n-1,i-1) \subseteq PS(n-1,i)$, we get:

$$A(n-1,i-1) \text{ divides } A(n-1,i),$$

hence it follows that

$$(x \mapsto \binom{x}{i-1} \cdot A(n-1,i)) \in LP(n,m-1).$$

By induction hypothesis we know:

$$(x \mapsto \binom{x}{i} \cdot A(n-1,i)) \in LP(n,m-1).$$

Now we show (2.): For $x \in \mathbf{N}_0$ we have:

$$\frac{\beta_i^{(n)}(x+1) - \beta_i^{(n)}(0)}{x+1} = \frac{\binom{x+1}{i} \cdot A(n-1,i)}{x+1} = \binom{x}{i-1} \cdot \frac{A(n-1,i)}{i}$$

Therefore it is sufficient to show:

$$(x \mapsto \binom{x}{i-1} \cdot \frac{A(n-1,i)}{i}) \in LP(n-1,m-1).$$

By induction hypothesis we know:

$$(x \mapsto \binom{x}{i-1} \cdot A(n-2,i-1)) \in LP(n-1,m-1).$$

Hence we are done if we show:

$$A(n-2,i-1) \text{ divides } \frac{A(n-1,i)}{i}.$$

This is true, because:

$$\{i \cdot p : p \in PS(n-2,i-1)\} \subseteq PS(n-1,i)$$

Hence we get: $A(n-2,i-1) \cdot i = lcm(PS(n-2,i-1)) \cdot i = lcm(\{i \cdot p : p \in PS(n-2,i-1)\})$ divides $lcm(PS(n-1,i)) = A(n-1,i)$. □

(Lemma 5.14) has completed the first step of our plan of proving (theorem 5.11).

In step(2.) we want to prove that the functions $\beta_i^{(n)}$ can be interpolated by a polynomial function at any $x_1, x_2, \ldots x_n \in \mathbf{N}_0$. This follows from (lemma 5.14).

(Theorem 5.3) can now be derived from the results obtained up to now. We leave the puzzle of putting the lemmas together in a suitable way and filling in some glue to the reader. But we have not yet proved (theorem 5.11). A terrible suspicion tortures us: and if $x \mapsto \binom{x}{i} \cdot A(n-1,i)$ behaves badly on the negatives? We have to get certainty immediately and give the proof of (theorem 5.11): We proceed by induction on i.

- **Base case** $i = 0$: $\beta_0^{(n)}$ is constant, hence in $L_nP(\mathbf{Z})$.

- **Induction step** $i-1 \to i$: We take $x_1, x_2, \ldots, x_n \in \mathbf{Z}$ arbitrary but fixed. Let r be any positive number with $x_k > -r$ for $k = 1, 2, \ldots, n$. We recall the following formula for the binomial coefficients: Let $r \geq 1$.

$$\binom{x}{i} = \binom{x+r}{i} - \sum_{s=0}^{r-1} \binom{x+s}{i-1}$$

This formula arises from a repeated application of the identity $\binom{x}{i} = \binom{x+1}{i} - \binom{x}{i-1}$. Hence we have:

$$\beta_i^{(n)}(x) = \binom{x}{i} \cdot A(n-1, i) =$$

$$= \binom{x+r}{i} \cdot A(n-1, i) - \sum_{s=0}^{r-1} (\binom{x+s}{i-1} \cdot A(n-1, i))$$

By induction hypothesis we know that $x \mapsto \binom{x}{i-1} \cdot A(n-1, i-1)$ is in $L_nP(\mathbf{Z})$. Since $L_nP(\mathbf{Z})$ is closed under functional composition and since $A(n-1, i-1)$ divides $A(n-1, i)$, the function

$$x \mapsto \binom{x+s}{i-1} \cdot A(n-1, i)$$

is in $L_nP(\mathbf{Z})$ for all $s \in \mathbf{N}$. So it is sufficient to find $p \in \mathbf{Z}[x]$ with

$$\bar{p}(x_k) = \binom{x_k + r}{i-1} \cdot A(n-1, i) \text{ for } k = 1, 2, \ldots, n \tag{5.2}$$

Since $x_k + r \geq 0$ for $k = 1, 2, \ldots, n$, we can use (lemma 5.14) (for a sufficiently large m) to construct a polynomial $p_1 \in \mathbf{Z}[x]$ with

$$\bar{p}_1(x_k + r) = \binom{x_k + r}{i-1} \cdot A(n-1, i) \text{ for } k = 1, 2, \ldots, n.$$

Now set

$$p := p_1 \circ (x + r).$$

Now p satisfies (5.2). This completes the induction step. □

Combining the lemmas

In order to prove (theorem 5.4), we fix $n \in \mathbf{N}$. We will now construct functions b_i that satisfy the assumptions of (lemma 5.9). We define sequences of functions $(t_j)_{j \in \mathbf{N}_0}$ and $(s_j)_{j \in \mathbf{N}}$ as follows:

$$\begin{array}{rcccc} s_j & : & \mathbf{Z} & \longrightarrow & \mathbf{Z} \\ & & x & \longmapsto & \binom{x+j-1}{2j-1} \cdot A(n-1, 2j-1) \end{array}$$

or, stated differently,

$$s_j := \beta^{(n)}_{2j-1} \circ \overline{x+j-1}$$

$$\begin{array}{rcrcl} t_j & : & \mathbf{Z} & \longrightarrow & \mathbf{Z} \\ & & x & \longmapsto & \binom{x+j-1}{2j} \cdot A(n-1,2j) \end{array}$$

or, stated differently,

$$t_j := \beta^{(n)}_{2j} \circ \overline{x+j-1}$$

Now let $(b_0, b_1, b_2, b_3, \ldots) := (t_0, s_1, t_1, s_2, t_2, s_3, \ldots)$. This sequence satisfies the assumptions of (lemma 5.9) and yields the characterization of $L_n P(\mathbf{Z})$ given in (theorem 5.4).

5.2 The compatibles on $\mathbf{Z}_n$

We want to characterize those n for which the ring Z_n is affine complete. We will use the following corollary of a theorem in [Kaa83].

Theorem 5.15 (Extension principle) *Let R be a finite or countable arithmetical[1] ring. Let $f : X \longrightarrow R$ be a function such that for all ideals I and for all $x_1, x_2 \in X$ with $x_1 \equiv_I x_2$ we have $f(x_1) \equiv_I f(x_2)$. Then f can be extended to a compatible function $\tilde{f} : R \longrightarrow R$.*

We give the following proposition:

Lemma 5.16 *Let R be an arithmetical and commutative ring with 1, R finite or countable. Then we have:*

$$R \text{ affine complete } \Rightarrow \forall a \in R : \langle 2a \rangle_{ideal} = \left\langle 2a^2 \right\rangle_{ideal}$$

Proof: Let $a \in R$ be arbitrary but fixed. If $2a = 0$ then the result is immediate. So we assume that $2a \neq 0$. "$\supseteq$" is clear, hence we have to prove "$\subseteq$". Suppose that there exists $s \in R$ with $s \in \langle 2a \rangle_{ideal}$ and $s \notin \langle 2a^2 \rangle_{ideal}$. The function $f : \{0, a, 2a\} \longrightarrow R$ with $f(a) = f(2a) = 0$ and $f(0) = s$ respects all ideals. Therefore it can be extended to a function $\tilde{f} \in C(R)$. Since R is affine complete, there exists a polynomial $q \in R[x]$ with

$$\bar{q} = \tilde{f}.$$

We write the polynomial q in the following way:

$$q = r_0 + r_1(x-a) + (x-a)(x-2a)q_1,$$

where $r_0, r_1 \in R$ and $q_1 \in R[x]$. From $\bar{q}(a) = 0$ we get $r_0 = 0$. From $\bar{q}(2a) = 0$ we get $r_1 \cdot a = 0$. Now we compute $q(0)$.

$$\bar{q}(0) = r_0 + r_1 \cdot (-a) + (-a)(-2a)\bar{q}_1(0)$$

[1] A ring is *arithmetical* iff its congruence lattice $(\mathcal{K}, \diamond, \cap)$ is distributive, where $\diamond$ denotes the relation product and $\cap$ the intersection of relations.

Since $r_0 = r_1 \cdot a = 0$ we get:

$$\bar{q}(0) = 2a^2 \cdot \bar{q}_1(0).$$

Hence $s = f(0) = \bar{q}(0) \in \langle 2a^2 \rangle_{ideal}$, which is a contradiction. □

Corollary 5.17 *Let $(p_1, p_2, p_3, \ldots) = (2, 3, 5, \ldots)$ be an enumeration of the primes. Let $n = \prod_{i=0}^{\infty} p_i^{\alpha(i)}$. Then $\mathbf{Z}_n$ is affine complete $\Longleftrightarrow$ $\alpha(1) \in \{0, 1, 2\}$ and $\alpha(i) \in \{0, 1\}$ for $i \geq 2$.*

Sketch of the proof: $\Leftarrow$: $\mathbf{Z}_p$ is affine complete for each prime p. Furthermore, we have to check that $\mathbf{Z}_4$ is affine complete. Then the result follows from the fact that both compatible and polynomial functions on direct products can be studied component-wise. $\Rightarrow$:

- **Case** There exists a prime $p \neq 2$ such that p^2 divides n: In this case we take $a := p$. We suppose:

  $$\langle 2p \rangle_{ideal} = \left\langle 2p^2 \right\rangle_{ideal}$$

  Hence we have:

  $$\exists k \in \mathbf{N} : 2p^2 \cdot k \equiv 2p \pmod{n}$$

  Let $\bar{k}$ be such a k. Then we have:

  $$n \text{ divides } 2p^2\bar{k} - 2p$$

  Since p^2 divides n we get:

  $$p^2 \text{ divides } 2p,$$

  which is a contradiction.

- **Case** 8 divides n. Take $a := 2$ and proceed as in the first case. □

I want to close with some problems.

1. Determine $L_n P(Z_m)$.
2. Why does the extension principle (cf.(theorem 5.15)) also hold for the functions in $L_n P(\mathbf{Z})$? Is there an explanation using the properties of the ideal lattice, as for $n = 2$? Does it hold for all arithmetical rings ?
3. What can be said about $L_m P(A \times B)$? What about $P(A \times B)$?

5.3 Literature and sources

The characterization of $L_n P(\mathbf{Z})$ seems to be new. The compatible functions from the naturals into the integers have been characterized in [Hal71].

The characterization of those n for which $\mathbf{Z}_n$ is affine complete is known. The cardinality of $P(\mathbf{Z}_n)$ has been computed in [KO68]. Their result can also be found in [Pil83]. The cardinality of $C(\mathbf{Z}_n)$ is easy to compute, hence by comparing the two numbers the result follows. (Lemma 5.16) and the proof given here are considered to provide a new solution to this exercise.

[Pil80] gives information about $P(A \times B)$.

Appendix A

Using the Knuth-Bendix procedure

A.1 What can you find in this appendix ?

We run our program (cf. chapter 2) on three examples. The completion of the first two axiom-systems is as in [KB67]. [Geh92] provides 15 examples for the completion of various axiom-systems using more advanced techniques such as AC-completion. He gives rewriting systems deciding the word problems of

1. Groupoids
2. Quasigroups
3. Semigroups and Monoids
4. Groups
5. (l,r)-systems
6. Commutative Semigroups and Monoids
7. Abelian Groups
8. Rings
9. A-modules
10. A-bimodules
11. A-rings
12. A-algebras
13. Distributive Lattices

I show the input-files and the trace of my program. The input file contains the following information:

1. A numerical value for each operation symbol. If the value of the symbol s_1 is lower than the value of s_2 then s_1 should rather drop inside s_2 during simplification.
2. The axioms system that has to be completed.

The Modula 2-program can be obtained from me. However, my program has the following main disadvantages:

- It uses "plain" completion as it was presented in [KB67]. The invention of AC-completion has considerably enlarged the number of axiom systems that can be treated by the Knuth-Bendix-method.
- The program does not prove termination of the resulting rewrite-system. If the program answers `All c.p.s converge !` then the resulting rewrite-system is canonical iff it is terminating.

[Geh92] gives a pointer to a professional implementation.

A.2 Completion of the group-axioms

A.2.1 Input file

```
A (+, 10)
A (*, 5)
A (-, 1)
A (0, 0)
 Rules :
+(0,x_1)
  x_1
+(-(x_1),x_1)
  0
+(+(x_1,x_2),x_3)
  +(x_1,+(x_2,x_3))
```

A.2.2 Completion

```
Original set of rules :

------------------------------------------------------------
```

```
Operators :
0:  0
-:  1
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
------------------------------------------------------------

Reduced set of rules
------------------------------------------------------------
Operators :
0:  0
-:  1
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
------------------------------------------------------------

-(x_1) + (x_1 + x_3) = x_3 from   3 and   2.
------------------------------------------------------------
Operators :
0:  0
-:  1
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: -(x_1) + (x_1 + x_3) ==> x_3
------------------------------------------------------------

-(0) + x_1 = x_1 from   4 and   1.
------------------------------------------------------------
Operators :
0:  0
```

```
-:  1
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: -(x_1) + (x_1 + x_3) ==> x_3
  5: -(0) + x_1 ==> x_1
------------------------------------------------------------

-(-(0)) + x_1 = x_1 from   4 and   5.
------------------------------------------------------------
Operators :
0:  0
-:  1
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: -(x_1) + (x_1 + x_3) ==> x_3
  5: -(0) + x_1 ==> x_1
  6: -(-(0)) + x_1 ==> x_1
------------------------------------------------------------

-(0) = 0 from   2 and   6.
------------------------------------------------------------
Operators :
0:  0
-:  1
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: -(x_1) + (x_1 + x_3) ==> x_3
  7: -(0) ==> 0
------------------------------------------------------------
```

```
-(-(x_1)) + 0 = x_1 from   4 and   2.
------------------------------------------------------------
Operators :
0:  0
-:  1
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: -(x_1) + (x_1 + x_3) ==> x_3
  7: -(0) ==> 0
  8: -(-(x_1)) + 0 ==> x_1
------------------------------------------------------------

-(-(x_1)) + x_3 = x_1 + x_3 from   3 and   8.
------------------------------------------------------------
Operators :
0:  0
-:  1
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: -(x_1) + (x_1 + x_3) ==> x_3
  7: -(0) ==> 0
108: x_1 + 0 ==> x_1
  9: -(-(x_1)) + x_3 ==> x_1 + x_3
------------------------------------------------------------

-(-(x_1)) = x_1 from 108 and   9.
------------------------------------------------------------
Operators :
0:  0
-:  1
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
```

```
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: -(x_1) + (x_1 + x_3) ==> x_3
  7: -(0) ==> 0
108: x_1 + 0 ==> x_1
 10: -(-(x_1)) ==> x_1
------------------------------------------------------------

x_1 + -(x_1) = 0 from   2 and  10.
------------------------------------------------------------
Operators :
0:  0
-:  1
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: -(x_1) + (x_1 + x_3) ==> x_3
  7: -(0) ==> 0
108: x_1 + 0 ==> x_1
 10: -(-(x_1)) ==> x_1
 11: x_1 + -(x_1) ==> 0
------------------------------------------------------------

x_1 + (-(x_1) + x_3) = x_3 from   3 and  11.
------------------------------------------------------------
Operators :
0:  0
-:  1
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: -(x_1) + (x_1 + x_3) ==> x_3
  7: -(0) ==> 0
108: x_1 + 0 ==> x_1
 10: -(-(x_1)) ==> x_1
 11: x_1 + -(x_1) ==> 0
 12: x_1 + (-(x_1) + x_3) ==> x_3
```

```
-----------------------------------------------------------

x_1 + (x_2 + -(x_1 + x_2)) = 0 from   3 and  11.
-----------------------------------------------------------
Operators :
0:  0
-:  1
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: -(x_1) + (x_1 + x_3) ==> x_3
  7: -(0) ==> 0
108: x_1 + 0 ==> x_1
 10: -(-(x_1)) ==> x_1
 11: x_1 + -(x_1) ==> 0
 12: x_1 + (-(x_1) + x_3) ==> x_3
 13: x_1 + (x_2 + -(x_1 + x_2)) ==> 0
-----------------------------------------------------------

x_2 + -(x_1 + x_2) = -(x_1) from   4 and  13.
-----------------------------------------------------------
Operators :
0:  0
-:  1
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: -(x_1) + (x_1 + x_3) ==> x_3
  7: -(0) ==> 0
108: x_1 + 0 ==> x_1
 10: -(-(x_1)) ==> x_1
 11: x_1 + -(x_1) ==> 0
 12: x_1 + (-(x_1) + x_3) ==> x_3
 14: x_2 + -(x_1 + x_2) ==> -(x_1)
-----------------------------------------------------------

-(x_1 + x_2) = -(x_2) + -(x_1) from   4 and  14.
```

```
-----------------------------------------------------------
Operators :
0:  0
-:  1
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: -(x_1) + (x_1 + x_3) ==> x_3
  7: -(0) ==> 0
108: x_1 + 0 ==> x_1
 10: -(-(x_1)) ==> x_1
 11: x_1 + -(x_1) ==> 0
 12: x_1 + (-(x_1) + x_3) ==> x_3
 15: -(x_1 + x_2) ==> -(x_2) + -(x_1)
-----------------------------------------------------------

All c.p.s converge !
```

A.3 A system of one rule

A.3.1 Input file

```
R
+(-(x_1),+(x_1,x_2))
  x_2
```

A.3.2 Completion

```
Original set of rules :

-----------------------------------------------------------
Operators :

Rewrite - rules :
  1: -(x_1) + (x_1 + x_2) ==> x_2
-----------------------------------------------------------

Reduced set of rules
-----------------------------------------------------------
```

```
Operators :

Rewrite - rules :
  1: -(x_1) + (x_1 + x_2) ==> x_2
------------------------------------------------------------

-(-(x_1)) + x_2 = x_1 + x_2 from   1 and   1.
------------------------------------------------------------
Operators :

Rewrite - rules :
  1: -(x_1) + (x_1 + x_2) ==> x_2
  2: -(-(x_1)) + x_2 ==> x_1 + x_2
------------------------------------------------------------

x_1 + (-(x_1) + x_2) = x_2 from   1 and   2.
------------------------------------------------------------
Operators :

Rewrite - rules :
  1: -(x_1) + (x_1 + x_2) ==> x_2
  2: -(-(x_1)) + x_2 ==> x_1 + x_2
  3: x_1 + (-(x_1) + x_2) ==> x_2
------------------------------------------------------------

All c.p.s converge !
```

A.4 Completion of the near-ring axioms

A.4.1 Input file

```
A (+, 10)
A (*, 5)
A (-, 7)
A (0, 0)
 Rules :
+(0,x_1)
  x_1
+(-(x_1),x_1)
  0
+(+(x_1,x_2),x_3)
  +(x_1,+(x_2,x_3))
*(*(x_1,x_2),x_3)
```

```
  *(x_1,*(x_2,x_3))
*(+(x_1,x_2),x_3)
  +(*(x_1,x_3),*(x_2,x_3))
```

A.4.2 Completion

```
Original set of rules :

------------------------------------------------------------
Operators :
0:  0
-:  7
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
------------------------------------------------------------

Reduced set of rules
------------------------------------------------------------
Operators :
0:  0
-:  7
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
------------------------------------------------------------

-(x_1) + (x_1 + x_3) = x_3 from   3 and   2.
------------------------------------------------------------
Operators :
0:  0
```

```
-:  7
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
  6: -(x_1) + (x_1 + x_3) ==> x_3
------------------------------------------------------------

-(0) + x_1 = x_1 from   6 and   1.
------------------------------------------------------------
Operators :
0:  0
-:  7
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
  6: -(x_1) + (x_1 + x_3) ==> x_3
  7: -(0) + x_1 ==> x_1
------------------------------------------------------------

-(-(0)) + x_1 = x_1 from   6 and   7.
------------------------------------------------------------
Operators :
0:  0
-:  7
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
```

```
  6: -(x_1) + (x_1 + x_3) ==> x_3
  7: -(0) + x_1 ==> x_1
  8: -(-(0)) + x_1 ==> x_1
------------------------------------------------------------

-(0) = 0 from   2 and   8.
------------------------------------------------------------
Operators :
0:  0
-:  7
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
  6: -(x_1) + (x_1 + x_3) ==> x_3
  9: -(0) ==> 0
------------------------------------------------------------

-(-(x_1)) + 0 = x_1 from   6 and   2.
------------------------------------------------------------
Operators :
0:  0
-:  7
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
  6: -(x_1) + (x_1 + x_3) ==> x_3
  9: -(0) ==> 0
 10: -(-(x_1)) + 0 ==> x_1
------------------------------------------------------------

-(-(x_1)) + x_3 = x_1 + x_3 from   3 and  10.
------------------------------------------------------------
Operators :
```

```
0:  0
-:  7
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
  6: -(x_1) + (x_1 + x_3) ==> x_3
  9: -(0) ==> 0
110: x_1 + 0 ==> x_1
 11: -(-(x_1)) + x_3 ==> x_1 + x_3
------------------------------------------------------------

-(-(x_1)) = x_1 from 110 and  11.
------------------------------------------------------------
Operators :
0:  0
-:  7
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
  6: -(x_1) + (x_1 + x_3) ==> x_3
  9: -(0) ==> 0
110: x_1 + 0 ==> x_1
 12: -(-(x_1)) ==> x_1
------------------------------------------------------------

x_1 + -(x_1) = 0 from   2 and  12.
------------------------------------------------------------
Operators :
0:  0
-:  7
*:  5
+: 10
```

```
Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
  6: -(x_1) + (x_1 + x_3) ==> x_3
  9: -(0) ==> 0
110: x_1 + 0 ==> x_1
 12: -(-(x_1)) ==> x_1
 13: x_1 + -(x_1) ==> 0
------------------------------------------------------------

x_1 + (-(x_1) + x_3) = x_3 from   3 and  13.
------------------------------------------------------------
Operators :
0:  0
-:  7
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
  6: -(x_1) + (x_1 + x_3) ==> x_3
  9: -(0) ==> 0
110: x_1 + 0 ==> x_1
 12: -(-(x_1)) ==> x_1
 13: x_1 + -(x_1) ==> 0
 14: x_1 + (-(x_1) + x_3) ==> x_3
------------------------------------------------------------

(x_1 * x_3) + (0 * x_3) = x_1 * x_3 from   5 and 110.
------------------------------------------------------------
Operators :
0:  0
-:  7
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
```

```
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
  6: -(x_1) + (x_1 + x_3) ==> x_3
  9: -(0) ==> 0
110: x_1 + 0 ==> x_1
 12: -(-(x_1)) ==> x_1
 13: x_1 + -(x_1) ==> 0
 14: x_1 + (-(x_1) + x_3) ==> x_3
 15: (x_1 * x_3) + (0 * x_3) ==> x_1 * x_3
------------------------------------------------------------

0 * x_3 = 0 from   6 and  15.
------------------------------------------------------------
Operators :
0:  0
-:  7
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
  6: -(x_1) + (x_1 + x_3) ==> x_3
  9: -(0) ==> 0
110: x_1 + 0 ==> x_1
 12: -(-(x_1)) ==> x_1
 13: x_1 + -(x_1) ==> 0
 14: x_1 + (-(x_1) + x_3) ==> x_3
 16: 0 * x_3 ==> 0
------------------------------------------------------------

x_1 + (x_2 + -(x_1 + x_2)) = 0 from   3 and  13.
------------------------------------------------------------
Operators :
0:  0
-:  7
*:  5
+: 10

Rewrite - rules :
```

```
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
  6: -(x_1) + (x_1 + x_3) ==> x_3
  9: -(0) ==> 0
110: x_1 + 0 ==> x_1
 12: -(-(x_1)) ==> x_1
 13: x_1 + -(x_1) ==> 0
 14: x_1 + (-(x_1) + x_3) ==> x_3
 16: 0 * x_3 ==> 0
 17: x_1 + (x_2 + -(x_1 + x_2)) ==> 0
------------------------------------------------------------

x_2 + -(x_1 + x_2) = -(x_1) from   6 and  17.
------------------------------------------------------------
Operators :
0:  0
-:  7
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
  6: -(x_1) + (x_1 + x_3) ==> x_3
  9: -(0) ==> 0
110: x_1 + 0 ==> x_1
 12: -(-(x_1)) ==> x_1
 13: x_1 + -(x_1) ==> 0
 14: x_1 + (-(x_1) + x_3) ==> x_3
 16: 0 * x_3 ==> 0
 18: x_2 + -(x_1 + x_2) ==> -(x_1)
------------------------------------------------------------

-(x_1 + x_2) = -(x_2) + -(x_1) from   6 and  18.
------------------------------------------------------------
Operators :
0:  0
-:  7
*:  5
```

```
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
  6: -(x_1) + (x_1 + x_3) ==> x_3
  9: -(0) ==> 0
110: x_1 + 0 ==> x_1
 12: -(-(x_1)) ==> x_1
 13: x_1 + -(x_1) ==> 0
 14: x_1 + (-(x_1) + x_3) ==> x_3
 16: 0 * x_3 ==> 0
 19: -(x_1 + x_2) ==> -(x_2) + -(x_1)
------------------------------------------------------------

(x_1 * x_3) + (-(x_1) * x_3) = 0 from   5 and  13.
------------------------------------------------------------
Operators :
0:  0
-:  7
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
  6: -(x_1) + (x_1 + x_3) ==> x_3
  9: -(0) ==> 0
110: x_1 + 0 ==> x_1
 12: -(-(x_1)) ==> x_1
 13: x_1 + -(x_1) ==> 0
 14: x_1 + (-(x_1) + x_3) ==> x_3
 16: 0 * x_3 ==> 0
 19: -(x_1 + x_2) ==> -(x_2) + -(x_1)
 20: (x_1 * x_3) + (-(x_1) * x_3) ==> 0
------------------------------------------------------------

-(x_1) * x_3 = -(x_1 * x_3) from   6 and  20.
------------------------------------------------------------
```

```
Operators :
0:  0
-:  7
*:  5
+: 10

Rewrite - rules :
  1: 0 + x_1 ==> x_1
  2: -(x_1) + x_1 ==> 0
  3: (x_1 + x_2) + x_3 ==> x_1 + (x_2 + x_3)
  4: (x_1 * x_2) * x_3 ==> x_1 * (x_2 * x_3)
  5: (x_1 + x_2) * x_3 ==> (x_1 * x_3) + (x_2 * x_3)
  6: -(x_1) + (x_1 + x_3) ==> x_3
  9: -(0) ==> 0
110: x_1 + 0 ==> x_1
 12: -(-(x_1)) ==> x_1
 13: x_1 + -(x_1) ==> 0
 14: x_1 + (-(x_1) + x_3) ==> x_3
 16: 0 * x_3 ==> 0
 19: -(x_1 + x_2) ==> -(x_2) + -(x_1)
 21: -(x_1) * x_3 ==> -(x_1 * x_3)
------------------------------------------------------------

All c.p.s converge !
```

Lebenslauf

Am 8.April 1970 wurde ich in Linz als Sohn der kaufmännischen Angestellten Gertraud und Bruno Aichinger geboren. Ich habe zwei Brüder, Bruno und Wolfram, die 1962 bzw. 1963 auf die Welt gekommen sind. Ich besuchte die Übungsvolksschule der Pädagogischen Akademie der Diözese Linz und dann den neusprachlichen Zweig des Akademischen Gymnasiums Linz, an dem ich im Juni 1988 die Reifeprüfung mit ausgezeichnetem Erfolg ablegte.

Seit Oktober 1988 studiere ich an der Johannes Kepler Universität Linz Technische Mathematik im Studienzweig Informations- und Datenverarbeitung. Den ersten Studienabschnitt habe ich im Jänner 1991 mit ausgezeichnetem Erfolg abgeschlossen.

Während des Studiums besuchte ich Sprachkurse an der Universität (Italienisch, Französisch, Spanisch) und erweiterte meine Englischkenntnisse durch den dauernden Gebrauch der englischen Sprache als Arbeitssprache am RISC-Linz und in der Arbeitsgruppe Algebra des Mathematikinstituts der Universität Linz. Im Sommer 1990 arbeitete ich als freier Mitarbeiter der oberösterreichischen Kulturredaktion der Tageszeitung "Der Standard".

Ich interessiere mich sehr für Informatik und habe Erfahrung mit den Programmiersprachen Modula 2, C, Lisp, Prolog und Fortran.

Im November und Dezember 1991 arbeitete ich als teilzeitbeschäftigter Studienassistent bei Prof.Dr.Günter Pilz (Algebra). Weiters betreute ich Tutorien zu den Lehrveranstaltungen "Mathematik für Mechatroniker", "Algorithmen und Datenstrukturen" und "Mathematik für Sozial- und Wirtschaftswissenschafter".

Das Studienjahr 92/93 verbrachte ich in Florenz, wo ich an der "Università Degli Studi" im Rahmen des Erasmus-Programms besonders bei Prof.Adriano Barlotti Geometrie studierte.

Bibliography

[Bet73a] G. Betsch. Primitive near-rings. *Math.Z.*, 130:351–361, 1973.

[Bet73b] G. Betsch. Some structure theorems on 2-primitive near-rings. In *Coll.Math.Soc.J.Bolyai 6*. North-Holland, Amsterdam, 1973.

[Bir35] G. Birkhoff. On the structure of abstract algebras. *Proc.Cambridge Phil.Soc.*, 31:433–454, 1935.

[BL70] G. Birkhoff and J.D. Lipson. Heterogeneous algebras. *J.Comb:Theory*, 8:115–133, 1970.

[Buc82] B. Buchberger. Algebraic simplification. In B. Buchberger, G.E. Collins, and R. Loos, editors, *Computer algebra – symbolic and algebraic computation*, pages 11–43. Springer-Verlag Wien, 1982.

[Der87] N. Dershowitz. Termination of rewriting. *Journal of symbolic computation*, 3:69–116, 1987.

[EM85] H. Ehrig and B. Mahr. *Fundamentals of algebraic specification 1 – Equations and initial semantics*, volume 6 of *EATCS : Monographs on theoretical computer science*. Springer Berlin-Heidelberg-New York, 1985.

[Fag87] F. Fages. Associative-commutative unification. *Journal of symbolic computation*, 3:257–275, 1987.

[Geh92] W. Gehrke. Detailed catalogue of canonical term rewriting systems generated automatically. Technical Report 92-64, RISC-Linz, Johannes Kepler University, A-4040 Linz,Austria,Europe, November 1992.

[Gra68] Graetzer, G. *Universal algebra*. Van Nostrand, 1968.

[GW88] J.A. Goguen and T. Winkler. Introducing OBJ3. Technical Report SRI-CSL-88-9, Computer Science Laboratory, SRI International, 333 Ravenswood Ave., Menlo Park, August 1988.

[Hal71] R.R. Hall. On pseudo-polynomials. *Mathematika*, 18:71–77, 1971.

[HO80] G. Huet and D.C. Oppen. Equations and rewrite-rules: a survey. Technical Report CSL-111, Computer Science Laboratory, SRI International, 333 Ravenswood Ave., Menlo Park, January 1980.

[Hul69] H. Hule. Polynome über universalen Algebren. *Monatshefte für Mathematik*, 73:329–340, 1969. German.

[IK79] M. Istinger and H.K. Kaiser. A characterization of polynomially complete algebras. *Journal of Algebra*, 56:103–110, 1979.

[Jou87] J.P. Jouannaud, editor. *Rewriting Techniques and Applications*. Academic Press, 1987.

[Kaa83] K. Kaarli. Compatible function extension property. *Algebra universalis*, 17:200–207, 1983.

[Kai77] H.K. Kaiser. Über kompatible Funktionen in universalen Algebren. *Acta Mathematica Academiae Scientiarum Hungaricae*, 30(1-2):105–111, 1977.

[KB67] D.E. Knuth and P.B. Bendix. Simple word problems in universal algebras. In *OXFORD 67*, pages 263–298, 1967.

[KO68] G. Keller and F.R. Olson. Counting polynomial functions (mod p^n). *Duke Math. J.*, 35:835–838, 1968.

[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. In *Contributions to universal algebra*, volume 17, pages 331 – 340. Colloqu.Math.Soc.Janos Bolyai, 1975.

[MVdW86] J.D.P. Meldrum and A.P. Van der Walt. Matrix near-rings. *Arch.Math*, 47:312–319, 1986.

[Pil80] G.F. Pilz. Near-rings of compatible functions. *Proceedings of the Edinburgh Mathematical Society*, 23:87–95, 1980.

[Pil83] G.F. Pilz. *Near-rings*. North-Holland Publishing Company – Amsterdam, New York, Oxford, 2nd edition, 1983.

[Pil84] G.F. Pilz. *Algebra – Ein Reiseführer durch die schönsten Gebiete*. Universitätsverlag Rudolf Trauner, Linz, 1984.

[Slu39] J. Slupecki. A criterion of completeness of many-valued logic. *C.R.Soc.Sci.Varsovie*, 32:102–110, 1939.