# Polynome über Gruppen

## Polynomials over Groups

**Diplomarbeit zur Erlangung des akademischen Grades eines Magisters in der Studienrichtung Mathematik an der formal- und naturwissenschaftlichen Fakultät**


verfaßt von

**Peter Balazs**



Angefertigt am Institut für Mathematik der Universität Wien bei

**Univ. Prof. G. Kowol**



Wien, November 2001

# Vorwort

## Einleitung

*"'Polynome haben wir in der Schule gemacht, und von Gruppen habe ich schon gehört! Aber was sind* 'Polynome über Gruppen'*?"*

Polynome sind „klassische" Objekte der Mathematik. Es gibt wohl keinen Mathematikstudenten, ja sogar keinen Schüler, der noch nie etwas mit Polynomen zu tun hatte. Bereits in der Mittelschule kommt man damit sehr oft in Kontakt.

Dort kennt man Polynome, genauer Polynomfunktionen, als Funktionen, deren Werte (an einer bestimmten Stelle) durch „einfache" Rechnungen, d.h Addition, Subtraktion und Multiplikation, bestimmt werden kann. Als Term bezeichnet man die Beschreibung dieser Rechnungen mit Unbestimmten („$x$"). So ist die Funktion (über den reellen Zahlen $\mathbb{R}$ )

$$f(x) = x^2 + 1$$

eine Polynomfunktion. Der Term $x^2 + 1$ beschreibt sehr anschaulich, wie man von einem Ausgangswert $x$ auf den Funktionswert $f(x)$ kommt. Man muß gerade den Ausgangswert $x$ mit sich selbst multiplizieren und dann 1 addieren.

Polynome haben (hier) die folgende allgemeine Gestalt:

$$f(x) = a_k \cdot x^k + a_{k-1} \cdot x^{k-1} + \ldots + a_2 \cdot x^2 + a_1 \cdot x + a_0$$

Die $a_i$ nennt man *Koeffizienten*, das höchste $k$ für das $a_k \neq 0$ den *Grad* des Polynoms. Dem Nullpolynom ($a_i = 0 \forall i$) ordnet man keinen Grad zu.

In der Mittelschule werden Polynomfunktionen als Beispielsfunktionen für verschiedenste analytische Methoden wie das Differenzieren und Integrieren sowie das Auffinden von Nullstellen herangezogen, da sie durch ihre Terme leicht beschreibbar sind und diese Operationen bei Polynomfunktionen recht leicht durchführbar sind.

Man denke nur an die endlosen Kurvendiskussionen, wo nur die schwierigeren Beispiele *nicht* Polynomfunktionen waren.

In der Mittelschule wird sowohl für die Koeffizienten als auch für den Wertebereich meist der Körper der rationalen Zahlen $\mathbb{Q}$ oder der reellen Zahlen $\mathbb{R}$ herangezogen.

Doch sind Körper bereits in der Mittelschule nicht die einzigen interessanten Mengen, so sind ist z.B. die Menge der ganzen Zahlen, $\mathbb{Z}$, kein Körper mehr (sondern ein kommutativer Ring mit Eins), da es im allgemeinen kein multiplikatives Inverses gibt.

Behandelt man zum Beispiel Matrizen über $\mathbb{R}$ , so geht man mit einer Menge um, wo die Multiplikation im allgemeinen nicht mehr kommutativ ist (d.h. für zwei Matrizen $A$ und $B$ ist im allgemeinen $A \cdot B \neq B \cdot A$).

Aber auch auf diesen beiden Mengen kann man Polynome betrachten und auswerten. So kann die obige Polynomfunktion $f(x) = x^2 + 1$ als Funktion auf diesen beiden Mengen aufgefaßt werden. D.h. wir sind nicht auf Körper beschränkt!

Diese genauere Untersuchung von Polynomen über anderen algebraischen Strukturen bleibt der Hochschule vorbehalten. In der Analysis werden Polynomfunktionen untersucht, diese werden wiederum als Beispiele herangezogen, aber sie dienen auch zur Approximation und man lernt Schemate, um Werte schnell zu berechnen.

In der Algebra werden Polynome über beliebigen (meist kommutativen) Ringen betrachtet. Sei $R$ ein kommutativer Ring mit Einslement, dann sind Polynome Wörter, d.h„sinnvolle“ Aneinanderreihung von Symbolen (Elemente und Operationen von $R$ und eine „Unbestimmte“ $x$ sind), die man ebenso in symbolischer Art und Weise addieren, subtrahieren und muliplizieren kann. Als „sinnvoll“ läßt man Ausdrücke zu, die, wenn man für die Unbestimmte ein Element aus $R$ einsetzt, wieder ein Element von $R$ ergeben. D.h. man läßt nur jene Ausdrücke zu,wo die Unbestimmte so wie ein Element des Rings verwendet wird. So sind z.B. die Ausdrücke $3 \cdot x$, $x + x + x$ und $-x + 2 \cdot x^2 - x$ sinnvolle Ausdrücke über den ganzen Zahlen, im Gegensatz zu $+ + x + +$ oder $xxx\cdot^{-1}$

Jedes Polynom kann auf die folgende Form gebracht werden:

$$p = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

wobei die Koeffizienten $a_i$ in $R$ liegen. Die Potenzschreibweise verwendet man (wie üblich) als Abkürzung des mehrmaligen Produkts mit sich selbst, so ist $x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n}$.

Wenn wir dies als Abbildung $x \mapsto p(x), x \in R$ auffassen, gelangen wir zu Polynomfunktionen. Ein Kernproblem dieser Arbeit wird hier aufgeworfen: Repräsentieren verschiedene Polynome verschiedene Funktionen? Welche Polynome repräsentieren die selbe Funktion? Wann sind Polynome überhaupt verschieden?

**Beispiel:** Betrachten wir den Körper $\mathbb{Z}_2 = \{0, 1\}$ dessen Operationen $\cdot$ und $+$ wir folgt festgelegt sind:

| $+$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

| $\cdot$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

Dann induzieren z.B. die Polynome $x^2 - x$ und 0, oder $1 \cdot x$ und $x$, $x - 1$ und $x^4 - x^3 + x^2 - x - 1$ jeweils dieselbe Polynomfunktion.

Wir wollen in dieser Arbeit einen Schritt weiter als in der klassischen Algebra gehen. Im ersten Kapitel werden wir untersuchen, wie man sich Polynome und Polynomfunktionen über allgemeinen Klassen von algebraischen Strukturen vorstellen kann, sogenannten *Varietäten*, d.h. Klassen von Mengen mit bestimmten Operation und bestimmten Gesetzen. Die meisten bekannten Strukturen wie Ringe, Gruppen oder Verbände sind Varietäten. Wir werden feststellen, welche Ausagen dort getroffen werden können und welche Begriffe dort bereits sinnvoll sind. Wir werden in diesem Kapitel auch die Frage untersuchen, für welche Mengen alle Funktionen Polynomfunktionen sind.

Im zweiten Kapitel studieren wir die Funktionenkomposition (das Hintereinanderausführen von Funktionen) und eine analoge Operation für Polynome. Weiters definieren wir mehrstellige Polynome. Wir werden sehen, daß jeder Strukturhomomorphismus (das ist eine Abbildung $\varphi$, die die Operationen „respektiert“, d.h. z.B. für die Multiplikation in Gruppen gilt: $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$) einen Homorphismus auf der Menge der Polynomen bzw. Polynomfunktionen induziert. Wir werden definieren, was wir uns unter einer Polynommatrix verstehen, und Polynomfunktionen betrachten, die Permutationen (d.h. „1 zu 1“ Abbildungen) sind.

Im dritten und letzten Kapitel spezialisieren wir die erlangten Erkenntnisse und Begriffe auf Gruppen. Wir werden untersuchen in welchen Formen wir die Polynome und Polynomfunktionen darstellen können, wie sich spezielle Eigenschaften von Gruppen (Nilpotenz, Auflösbarkeit und Permutationseigenschaften) der Gruppe auf die Gruppe der Polynome und Polynomfunktionen sowie umgekehrt auswirken. Wir werden uns dort auch der Frage stellen,

welche Polynome bijektive Abbildungen oder Homomorphismen induzieren!

Stellt man sich unbeeinflußt, ohne (größere) Vorkenntnisse die Frage, was Polynome über Gruppen sind, dann denkt man darüber nach, was mit den obigen Formen der Polynome (über Ringen) „passiert“ wenn es keine Multiplikation gibt und die Addition nicht kommutativ ist. Man würde wohl vermuten (zumindest hat das der Autor beim ersten Kontakt mit diesem Thema getan), daß (einstellige) Polynome über Gruppen in der folgenden Art und Weise dargestellt werden können:

$$p = a_0 + \sum_{i=1}^{n} (k_i \cdot x + a_i) \text{ für } k_i \in \mathbf{Z}$$

wobei die $k_i$ ganzen Zahlen sind, sodaß $k_i \cdot x = \underbrace{x + x + \ldots + x}_{k_i}$. Zu beachten ist auch, daß in Gruppen die Operation (hier die Addition $+$) im allgemeinen eben nicht kommutativ ist. Die hier präsentierte Theorie der Polynome leistet genau das, angewandt auf Ringe liefert sie die bekannten Polynome, auf Gruppen angewandt liefert sie Ausdrücke der obigen Form. Sie ist somit eine recht „natürliche“ Theorie.

Warum wendet man sich überhaupt so ausgiebig dieser Klasse von Funktionen zu? Polynomfunktionen sind weit verbreitet in der Mathematik. Ihre Bedeutung kommt daher, dass sie mit einem einfachen, nur Grundrechnungsarten enthaltenden Term darstellbar und dadurch leicht beschreib- und berechenbar sind. Dadurch kann man nicht nur eine Funktion, die eventuell auf einer unendlichen Menge wirkt, mit einem endlichen Term beschreiben, man kann auch durch diese Beschreibung bereits einige Eigenschaften „sehen“ ohne viel berechnen zu müssen. Analytische Eigenschaften von Polynomfunktionen sind leicht berechenbar, wodurch sie sich eben auch in vielen (Schul-) Aufgaben wiederfinden.

In der numerischen Mathematik verwendet man Polynomfunktionen, um andere Funktionen zu approximieren. Man versucht nach Möglichkeit immer zu Polynomfunktionen zu gelangen, da diese eben leicht berechenbar und darstellbar sind. Anwendungen für Polynomfunktion gibt es sehr viele:

So kann man zum Beispiel jede stetige reelle Funktion beliebig genau durch eine Polynomfunktion approximiert werden, und somit der Wert einer solche Funktion an jeder Stelle beliebig genau durch den einer Polynomfunktion bestimmt werden.

In der numerischen Akustik kombiniert man mit der „Chaospolynom“-

methode verschiedene Lösungsmethoden (BEM, FEM und andere) um Schallfelder zu berechnen.

In der Physik wird ein Ausgleichspolynom durch Werte der Experimentmessungen gelegt, um damit Modelle zu bilden. Auch haben viele physikalischen Aussagen polynomialen Charakter (z.B. die Gleichung für die gleichmäßig beschleunigte Bewegung $s = \frac{at^2}{2}$)

Das wohl wichtigste Buch für diese Arbeit war *„Algebra of Polynomials“* [18]. Neben den zahlreichen anderen Artikeln und Arbeiten möchte ich *„Interpolation with Near-rings of Polynomial Functions“* [1] hervorheben, das mir einen anderen, „frischeren “ Zugang zu dem Thema bot.

# Ziel

Ziel dieser Arbeit ist es eine möglichst verständliche Erarbeitung und Einführung der Grundlagen, einen möglichst ausführlichen Überblick über die existierenden Ergebnisse und einen exemplarischer Einblick in die Methoden der Beweisführung zu geben.

Zudem wurde versucht, einen etwas anderen Zugang als in [18] (und dadurch dem Großteil der Literatur) mit etwas (zumindest für den Autor) intuitiverer Symbolik zu erreichen. Einige Aussagen konnten verallgemeinert werden. Der Großteil davon wird in der Literatur erwähnt, jedoch nicht ausformuliert. Darüber hinaus konnten auch z.B. einige Aussagen von *Scott* [29] für den nicht unbedingt endlichen und den mehrstelligen Fall, $k > 1$, untersucht und teilweise verallgemeinert werden.

Beweise wurden dann aufgenommen,

- wenn sie guten Einblick in die Materie bieten
- wenn sie einer genaueren Ausformulierung bedurften, um das Verständnis zu erleichtern, bzw. wenn „Trivialitäten“ es verdienten, genauer durchdacht und ausformuliert zu werden
- wenn sie durch Umformulierung leichter verständlich wurden
- wenn sie Beweise für Aussagen sind, die nicht oder nicht so in der Literatur erwähnt werden

Da aber ein Überblick angestrebt ist und der Rahmen dieser Arbeit nicht all zu sehr gesprengt werden sollte, kann nur ein Bruchteil der Aussagen bewiesen werden. Nur ausformulierte Beweise enden mit □, bei anderen ist ein Zitat angegeben. Sollte beides fehlen, so ist die Beweisführung durch die vorangegangenen Überlegungen und Sätze klar.

# Danksagung

Ich bin *Prof. F. Punz* für seinen Mathematikunterricht dankbar, der neben den „Rechnereien“ doch noch immer wieder genug Platz für Logik und Nachdenken fand. Ich bin ihm auch dankbar, daß er mich mit den Worten "Versuch das nicht, das ist Dir zu schwer!“ erst recht motiviert hat, mich dem Studium der Mathematik zuzuwenden.

Neben vielen anderen Professoren möchte ich Herrn *Univ. Prof. S. Grosser* danken, der in mir das Interesse an Algebra und Topologie geweckt und gefördert hat. In diesem Zusammenhang möchte ich *Dr. G. Landsmann* für die zahllosen Gespräche nach den Proseminaren danken. Hr. *Mag. Alexej Tajmel* danke ich für die vielen gemeinsamen Stunden, in denen wir doch auch manchmal etwas für unser Studium gemacht haben.

Ausdrücklich möchte ich noch *Univ. Prof. H. Schoißengeier* danken, der nicht nur mein Interesse an der Algebra und der Topologie weiter verstärkte, sondern mir auch beim Abschluß (gemeinsam mit *Univ. Prof . F. Haslinger*) geholfen hat, einige bürokratische Hürden zu überwinden.

Ich bin der *Akademie der Wissenschaften*, insbesondere dem *Insitut für Schallforschung* unter der Leitung von *Univ. Doz. W.A. Deutsch* zu Dank verpflichtet, da ich nicht nur durch den Posten als Programmierer dort nun finanziell abgesichert bin, Freiheiten in der Arbeitseinteilung habe, um das Studium voranzutreiben, und zur Fertigstellung der Diplomarbeit Sonderurlaub bekommen habe, sondern v.a., da ich dort auch wissenschaftlich tätig sein darf.

Zu großem Dank bin ich verpflichtet:

- Meiner ganzen Familie, besonders meiner *Mutter* , die mich nun 30 Jahre lang unterstützt hat und nur ein bissschen die Geduld verloren hat.

- *Dr. Robert Baumgartner* , der nicht nur im gemeinsamen Studium half, Motivationslöcher zu überwinden (aber auch andere zu öffnen),

sondern der sich auch die Aufgabe auferlegt hat, sich in diese Arbeit einzulesen und sie auch inhaltlich Korrektur zu lesen.

- Meinem Betreuer, *Univ. Prof. G. Kowol* , der mich für dieses Thema interessieren konnte, der mir auch beim bürokratischen Abschluß des zweiten Studienabschnitts sehr half und der immer für Fragen offen war.

- Und ganz besonderen Dank gilt meiner Frau, *Claudia* , die mich all die Jahre mit Geduld und Liebe unterstützt hat. Sie macht mich vollständig!

# Inhaltsverzeichnis

# Kapitel 1

# Polynome über universalen Algebren

## 1.1 Universale Algebra

In der klassischen Algebra studiert man verschiedenste Klassen von algebraischen Strukturen. Damit meint man Mengen mit bestimmten Operationen, die bestimmte Eigenschaften haben. Klassische algebraische Strukturen sind zum Beispiel Halbgruppen, Gruppen, Ringe, Körper und Verbände. Wir können nun eine „allgemeine algebraische Struktur“ definieren, die eine Verallgemeinerung dieser Begriffe im obigen Sinne , d.h. eine Menge mit Operationen und Bedingungen, ist. (Körper entziehen sich uns bei dieser Verallgemeinerung, wie wir in 1.1.5 sehen werden. )

Untersucht man die oben genannten klassischen Beispiele von algebraischen Strukturen bemerkt man Parallelen und Analogien in bestimmten Aussagen, aber auch in den Beweisführungen dazu. Z.B. gibt es in alle diesen Strukturen (mehr oder weniger) analoge Homomorphie- und Isomorphiesätze . Das läßt uns vermuten (und hoffen), daß wir solche Aussagen auch über diese „allgemeine algebraischen Strukturen“ , den *universalen Algebren* , treffen können.

**Definition 1.1.1** *Sei $A$ eine nicht-leere Menge und $n$ eine natürliche Zahl. Eine* **n-äre Operation** *$\omega^A$ auf der Menge $A$ ist eine Funktion vom kartesischen Produkt $A^n$ nach $A$. Wir bezeichnen $n$ als die Arität der Operation $\omega$.*

$$\omega^A : A^n \to A$$

*Sind Verwechslungen auszuschließen, so schreiben wir einfach $\omega$ statt $\omega^A$.*

Für $n = 2$ kann das Symbol für die Operation $\omega$ in Anlehnung an die Multiplikation (z.B. in $\mathbb{R}$) zwischen die beiden Argumente geschrieben werden, also $\omega(a, b) = a\omega b$. Ist $n = 1$ schreiben wir $\omega$ manchmal als Exponent, also $\omega(a) = a^{\omega}$.

Eine 0-äre Operation ($\omega : \emptyset \to A$) bedeutet, dass man aus der Menge $M$ ein festes Element auswählt. Dieses Element bezeichnet man auch mit dem selben Symbol $\omega$ der Operation.

**Definition 1.1.2** *Eine* **universale Algebra**, *oder $\Omega$-Algebra, ist ein Paar $[A; \Omega]$, wobei $A$ eine nicht-leere Menge und $\Omega = \{\omega_i | i \in I\}$ eine Familie von Operationen auf $A$ ist, mit der Indexmenge $I$.*
*Die Klasse aller $\Omega$-Algebren bezeichnen wir mit $\mathfrak{V}(\Omega)$.*

Wenn es keine Möglichkeit für Verwechselungen gibt, schreiben wir für die Algebra $[A; \Omega]$ einfach nur $A$.

Wir werden manchmal für das Paar $[A; \Omega \cup \{\omega_1\} \cup \ldots \{\omega_n\}]$ einfach

$$[A; \Omega, \omega_1, \ldots, \omega_n]$$

schreiben, wenn die Bedeutung klar bleibt. Daher verwenden wir die Notation „[ ; ] “ und nicht „( , )“, da dies dann kein „echtes“ Paar mehr ist.

Da es verschiedene Begriffe von „Algebra“ gibt, nennen wir $A$ zur Klarheit in der Definition oben „universale“ Algebra. Wenn es keine Möglichkeit zur Verwechslung gibt, bezeichnen wir universale Algebren aber nur als Algebren.

Ab nun sei ein für alle mal vorausgesetzt, dass eine Indexmenge $I$ eine Menge aller Ordinalzahlen $i < o$ sei, wobei $o$ eine beliebige Ordinalzahl sei. Diese Beschränktheit fordern wir, um einerseits die Indexmenge logisch einwandfrei bilden zu können, andererseits eine wohlgeordnete Indexmenge vorauszusetzen. Weiters werden wir die Erwähnung der Indexmenge manchmal einfach weglassen, wenn diese Menge aus dem Umfeld ersichtlich ist und es dadurch nicht zu Unklarheiten kommen kann.

Die folgende Definition stellt eine abstrakte Verallgemeinerung des Begriffs der Operationen dar:

**Definition 1.1.3** *Das Paar $(\Omega, Ar)$ ist eine* **Signatur**, *wenn*
*(1) $\Omega$ eine Menge ist*
*(2) $Ar : \Omega \to \boldsymbol{N}_0$ eine Funktion ist.*

Wenn es keine Verwechslungen geben kann, bezeichen wir einfach die Menge $\Omega$ als Signatur.

Jede Menge von Operationen mit den Zuweisungen der Arität als Abbildungen ist eine Signatur .

**Definition 1.1.4** *Die Familie $T$ der Paare $(n_a, a)$, wobei $a$ die Aritäten von $\Omega$ durchläuft und $n_a = |\{\omega \in \Omega : Ar(\omega) = a\}|$ ist, nennen wir den* **Typ** *von $\Omega$ oder $[A; \Omega]$ .*

Der Typ einer $\Omega$-Algebra ist somit

$$T(\Omega) = \{(n(\omega), Ar(\omega)) : \omega \in \Omega,\ n(\omega) = |\{\omega' \in \Omega : Ar(\omega') = Ar(\omega)\}|\}$$

Im Falle eines abzählbaren $\Omega$ können wir eine andere, kürzere Schreibweise für den Typ einer Algebra angeben. Der Typ von $\Omega$ ist dann das Tupel

$$T(\Omega) = (Ar(\omega_1), Ar(\omega_2), \ldots)$$

wobei $\omega_i$ $\Omega$ durchläuft. Diese Schreibweise ist allerdings nicht mehr eindeutig, da z.B. der Typ $(2, 1) = (1, 2)$.

**Definition 1.1.5** *Zwei Algebren $A$, $B$ heißen* **ähnlich**, *wenn sie vom selben Typ sind.*

Klarerweise sind Algebren mit dem selben $\Omega$ ähnlich.

Für ähnliche Algebren A, B können wir die gleichen Operationssymbole verwenden. Somit ist für $A, B$ ähnlich, $A \in \mathfrak{V}(\Omega)$, $B \in \mathfrak{V}(\Omega)$.

**Definition 1.1.6** *Wenn $A$ eine Algebra ist, dann nennt man die Kardinalität $|A|$ die* **Ordnung** *von $A$. Eine Algebra $A$ mit endlicher Ordnung nennt man endliche Algebra.*

**Beispiel:** Die klassische Algebra liefert uns viele Beispiele von Algebren, so liefert zum Beispiel ein Verband $V$ mit den Operationen $\cap$, $\cup$ liefert die (ähnlichen, aber nicht identischen) Algebren $[V; \cap, \cup]$ und $[V; \cup, \cap]$ des Typs $(2, 2)$ .

Wir werden aber als immer wieder verwendetes Beispiel für die universale Algebren die Gruppen heranziehen:

Eine *Gruppe* ist eine Algebra des Typs $(2, 1, 0)$, d.h. es gibt eine 2-stellige Operation („$\cdot$“, die „Multiplikation“), eine unäre Operation (die Zuweisung des inversen Elements, „$^{-1}$“) und eine 0-wertige Operation (das neutrale Element, die „Eins“ „1“). Eine andere verbreitete Bezeichnung ist „$+$“, die Addition, für die 2-wertige Operation, „$-$“ für die unäre Operation und “Null“ „0“ für die 0-wertige Operation.

### 1.1.1 Teilalgebren und Homomorphismen

**Definition 1.1.7** *Sei $|A;\Omega]$ eine universale Algebra und $U$ eine nicht-leere Teilmenge von $A$, so dass für alle $i \in I, \omega_i(a_1, a_2, ..., a_{n_i}) \in U$ für alle $a_1, a_2, ..., a_{n_i} \in U$, für alle $\omega_i \in \Omega$ und alle $n_i = Ar(\omega_i) > 0$. Für $n_i = Ar(\omega_i) = 0$ soll gelten: $\omega_i \in U$. Bezeichnen wir die Einschränkung der Operationen $\omega_i$, die ja dann Operationen auf $U$ sind, wieder mit $\omega_i$, ($\omega_i^U = \omega_i^A|_U$) so ist $[U;\Omega]$ wieder eine Algebra, wir bezeichnen sie als* **Unteralgebra** *bzw.* **Teilalgebra** *von $A$. $A$ nennen wir eine* **Erweiterung** *von $U$.*

$$Symbolisch: \ U \preceq_\Omega A$$

$U$ ist somit Teilalgebra von $A$ genau dann, wenn es bezüglich allen Operationen $\omega_i$ abgeschlossen ist.

Ist die Operationenmenge, auf die Bezug genommen wird, klar, so schreiben wir $U \preceq A$.

Jeder nicht-leere Schnitt von Unteralgebren von $A$ bildet klarerweise wieder eine Unteralgebra:

$$\forall i \in I : U_i \preceq A \Longrightarrow \cap U_i \preceq A$$

**Definition 1.1.8** *Ist $S$ eine nicht-leere Teilmenge von $A$, dann nennt man den Schnitt aller Unteralgebren, die $S$ enthalten, die* **von $S$ erzeugte Unteralgebra**, *symbolisch $\langle S\rangle$. Wenn gilt $\langle S\rangle = A$, dann nennt man $S$ eine* **Erzeugermenge** *bzw.* **Erzeugendensystem** *von $A$. Ist die Unterscheidung der Erweiterung wichtig, so schreiben wir: $\langle S\rangle_A$*
*Ist weiters $B \preceq A$, $S$ eine nicht leere Teilalgebra von $A$ so bezeichnen wir mit $B(S) = \langle B \cup S\rangle$ die* **Erweiterung von B um S**.

**Lemma 1.1.9** *Es seien A,B $\Omega$-Algebren mit $A \preceq B$, $U,V \subseteq B$. Dann ist: $A(U \cup V) = (A(U))(V)$.*

**Beweis:** $A(U \cup V)$ ist eine Algebra, die sowohl A und U, also auch $A(U)$, sowie V enthält, also gilt: $A(U \cup V) \supseteq (A(U))(V)$.
$(A(U))(V)$ ist eine Algebra, die A und $U \cup V$ enthält also gilt: $A(U \cup V) \subseteq (A(U))(V)$ □

Ebenso kann man zeigen

**Lemma 1.1.10** *Es sei $B$ eine $\Omega$-Algebra, es sei $A \preceq B$ und $S,U \subseteq B$. Sei $A = \langle S\rangle$. Dann ist $A(U) = \langle S \cup U\rangle$.*

**Beweis:** Da $S \subseteq A$ ist $S \cup U \subseteq A \cup U$. Also $\langle S \cup U\rangle \subseteq \langle A \cup U\rangle$.

Andererseits gilt $A \subseteq \langle S\rangle \subseteq \langle S \cup U\rangle$ und $U \subseteq S \cup U \subseteq \langle S \cup U\rangle$. Also ist $A \cup U \subseteq \langle S \cup U\rangle$ und somit auch $\langle A \cup U\rangle \subseteq \langle S \cup U\rangle$ □

**Definition 1.1.11** *Es seien A,B $\Omega$-Algebren. Eine Funktion $\varphi : A \to B$ heißt* **Homomorphismus** *(von universalen Algebren), wenn für alle $\omega_i \in \Omega$ und $n_i = Ar(\omega_i)$ gilt:*

$$\varphi(\omega_i^A(a_1, a_2, ..., a_{n_i})) = \omega_i^B(\varphi(a_1), \varphi(a_2)..., \varphi(a_{n_i}))) \quad für\ n_i > 0$$

$$\varphi(\omega_i^A) = \omega_i^B \quad für\ n_i = 0$$

*Ist $\varphi$ injektiv (surjektiv resp. bijektiv) so nennen wir sie einen* ***Monomorphismus*** *(einen* ***Epimorphismus*** *resp. einen* ***Isomorphismus****).*

*Symbolisch schreiben wir $\varphi \in Hom(A, B)$ $(Epi(A, B), Iso(A, B))$.*

*Ist die Unterscheidung der Menge der Operationen wichtig, so schreiben wir $\varphi \in Hom_\Omega(A, B)$.*

*Die Homomorphismen von A in sich selbst nennen wir* **Endomorphismen***, $End(A) = Hom(A, A)$. Die Isomorphismen von A nach A nennen wir* **Automorphismen** *: $Aut(A) = Iso(A, A)$.*

**Beispiel:** Für die Gruppen heißt das: Eine Funktion $\varphi : [G; \cdot_G, ^{-1^{(G)}}, 1_G] \to [H; \cdot_H, ^{-1^{(H)}}, 1_H]$ ist Homomorphismus, wenn gilt

- $\varphi(a \cdot_G b) = \varphi(a) \cdot_H \varphi(b)$
- $\varphi(a^{-1^{(G)}}) = \varphi(a)^{-1^{(H)}}$
- $\varphi(1_G) = 1_H$

Da für Gruppen aus der ersten Eigenschaft bereits die beiden anderen folgen, wird nur diese für die Definition von Homomorphismen für Gruppen herangezogen.

Für diesen Homomorphie-Begriff lassen sich für universale Algebren viele bekannte Tatsachen aus der klassischen Algebra übertragen. Z.B.:

**Proposition 1.1.12** *Es seien A,B $\Omega$-Algebren, $A' \preceq A, B' \preceq B$, $C \subseteq A$, $\varphi \in Hom(A, B)$. Dann gilt:*
*(1) $\varphi(A') \preceq B$*
*(2) $\varphi^{-1}(B') \preceq A$*
*(3) $\varphi\left(\langle C\rangle_A\right) = \langle\varphi(C)\rangle_B$*

**Beweis:** ad (1): Es gilt sicher $\varphi(A') \subseteq B$, d.h. es ist noch die Abgeschlossenheit zu zeigen.
Für $n_i > 0$ seien $b_j \in \varphi(A')$ für $j = 1, 2, ...., n_i$. Dann gibt es $a_i$ mit $\varphi(a_i) = b_i$. Damit ist

$$\omega_i^B(b_1, b_2, ..., b_{n_i}) = \omega_i^B(\varphi(a_1), \varphi(a_2), ..., \varphi(a_{n_i})) = \varphi(\omega_i^A(a_1, a_2, ..., a_{n_i}))$$

Damit ist $\omega_i(b_1, b_2, ..., b_{n_i}) \in \varphi(A)$. Für $n_i = 0$ ist $\omega_i^B = \varphi(\omega_i^A) \in \varphi(A)$.
ad (2): Durchrechnen wie ad (1)
ad (3):

$$C \subseteq \langle C \rangle \Longrightarrow \varphi(C) \subseteq \varphi\left(\langle C \rangle\right) \Longrightarrow \langle \varphi(C) \rangle \subseteq \varphi\left(\langle C \rangle\right)$$

Andererseits gilt

$$C \subseteq \varphi^{-1}\left(\varphi(C)\right) \subseteq \varphi^{-1}\left(\langle \varphi(C) \rangle\right)$$

Nach (2) ist das eine Unteralgebra

$$\Longrightarrow \langle C \rangle \subseteq \varphi^{-1}\left(\langle \varphi(C) \rangle\right) \Longrightarrow \varphi\left(\langle C \rangle\right) \subseteq \langle \varphi(C) \rangle$$

□

Die Komposition von Homomorphismen, das Hintereinanderausführen zweier Homomorphismen ist wieder ein Homomorphismus, was man einfach durch direktes Rechnen zeigen kann.

**Proposition 1.1.13** *Ist $\varphi \in Hom(A, B)$, $\psi \in Hom(B, C)$, dann ist $\psi \circ \varphi \in Hom(A, C)$.*

**Bemerkung:** Da für alle Algebren $A$ $id_A : a \mapsto a$ offensichtlich ein Homomorphismus ist, folgt daß die universalen Algebren eines bestimmten Typs mit den Homomorphismen eine Kategorie (siehe A.5) bilden.

**Definition 1.1.14** *Gibt es ein $\varphi \in Epi(A, B)$ so nennen wir $B$ ein* **homomorphes Bild** *von $A$.*
*$B$ heißt* **isomorph** *zu $A$, wenn es einen Isomorphismus von $B$ nach $A$ gibt, symbolisch: $A \simeq B$*
*Gibt es einen Monomorphismus von $A$ nach $B$, so können wir die Elemente von $A$ mit jenen von $\varphi(A)$ identifizieren, $\varphi : A \to \varphi(A)$ ist somit ein Isomorphismus. Dies nennen wir eine* **Einbettung**.

**Definition 1.1.15** *Es sei $I$ eine Indexmenge. Es seien $A_i$ für $i \in I$ $\Omega$-Algebren. Dann seien die Operationen auf $\prod_{i \in I} A_i$, dem kartesische Produkt, komponentenweise definiert.*

D.h. für abzählbares $I$ ist mit $\mathfrak{a}^{(i)} = (a_1^{(i)}, a_2^{(i)}, \ldots) \in \prod_{i \in I} A_i$ für $Ar(\omega_i) = 0$

$$\omega_i = (\omega_i^{A_1}, \omega_i^{A_2}, \ldots)$$

Für $Ar(\omega_i) > 0$ gilt:

$$\omega_i(\mathfrak{a}^{(1)}, \mathfrak{a}^{(2)}, \ldots, (\mathfrak{a}^{(Ar(\omega_i)}) =$$

$$= (\omega_i^{A_1}(a_1^{(1)}, a_1^{(2)}, \ldots, a_1^{Ar(\omega_i)}), \omega_i^{A_2}(a_2^{(1)}, a_2^{(2)}, \ldots, a_2^{Ar(\omega_i)}), \ldots)$$

Daraus folgt direkt

**Lemma 1.1.16** $[\prod_{i\in I} A_i; \Omega]$ *ist eine* $\Omega$*-Algebra.*

**Definition 1.1.17** *Die Abbildungen* $\xi_i : [\prod_{i\in I} A_i; \Omega] \to A_i$*, mit* $\xi_i(a_1, \ldots, a_k) = a_i$ *nennen wir die* **Projektionen.**

Sind die $A_i$ $\Omega$-Algebren, so sind die Projektionen klarerweise Epimorphismen.

**Definition 1.1.18** *Seien* $A_i$ $\Omega$*-Algebren. Ist* $S \preceq [\prod_{i\in I} A_i; \Omega]$ *und* $\xi_i(S) = A_i$ *so nennen wir* $S$ **subdirektes Produkt**.

### 1.1.2 Kongruenzen

Betrachten wir auf der Menge A eine Äquivalenzrelation $R \subseteq A \times A$, so sei

$$a \sim_R a' \Longleftrightarrow (a, a') \in R$$

**Definition 1.1.19** *Es sei A eine* $\Omega$*-Algebra. Eine Äquivalenzrelation K in* $A \times A$ *heißt* **Kongruenz**, *wenn* $\forall \omega \in \Omega$ *mit* $Ar(\omega) > 0$ *gilt:*
$a_i \sim_K b_i, \forall i = 1, ..., Ar(\omega) \Longrightarrow \omega(a_1, a_2, ..., a_{Ar(\omega)}) \sim_K \omega(b_1, b_2, ..., b_{Ar(\omega)})$
*Mit* $C(a) = \{b | b \sim_K a\}$ *bezeichnen wir die Äquivalenzklasse von a.*
*Die Menge aller Kongruenzen auf A bezeichnen wir mit* $\mathfrak{K}(A)$.

Da die Kongruenz $K$ eine Äquivalenzrelation ist, gilt wegen der Reflexivität, daß für alle 0-ären Operationen $\omega$ $\omega \sim_K \omega$ gilt.

**Beispiel:** Betrachten wir die Menge der ganzen Zahlen $\mathbb{Z}$ als Ring, also $[\mathbb{Z}; +, -, 0, \cdot]$. Dann definiere die Relation $a \sim_R b \Longleftrightarrow a \equiv b \bmod 2$, d.h. zwei Zahlen stehen in Relation, wenn Ihr Rest bei der Division durch 2 gleich ist. Diese Relation ist reflexiv, symmetrisch und transitiv. Sie ist damit eine Äquivalenzrelation, die Einteilung in gerade und ungerade Zahlen. Ist sie auch eine Kongruenz? Zu zeigen ist, daß für $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ mit $x_1 \sim_R y_1$ und $y_2 \sim_R x_2$ gilt:

- $x_1 + x_2 \sim_R y_1 + y_2$
- $x_1 \cdot x_2 \sim_R y_1 \cdot y_2$

- $-x_1 \sim_R -y_1$ und $-x_2 \sim_R -y_2$

Das kann man leicht durch Fallunterscheidungen zeigen, es gibt ja nur zwei mögliche Klassen. Also ist $R$ eine Kongruenz.

**Definition 1.1.20** *Eine Teilmenge $U \subseteq A$ heißt* **repräsentativ** *bzgl. $K$, wenn in jeder Äquivalenzklasse genau ein Element von $U$ liegt.* $(\forall C(a) : \exists!\ u \in U : u \in C(a))$

Im obigen Beispiel ist die Menge $\{0, 1\}$ eine repräsentative Menge.

Klarerweise sind die trivialen Äquivalenzrelation

- $K = \{(a, a)|a \in A\}$ mit $a \sim b \Leftrightarrow a = b$, genannt die *Identität*
- $K = A \times A$ mit $a \sim b : \forall a, b \in A)$, genannt die *Allrelation*

auch Kongruenzen.

**Definition 1.1.21** *Eine Algebra, die nur die trivialen Kongruenzen hat, nennen wir* ***einfach****.*

**Definition 1.1.22** *Sei $M \subseteq A \times A$. Die* **von $M$ erzeugte Kongruenz** *ist $\langle M \rangle_A = \bigcap_{K \in \mathfrak{K}(A), M \subseteq K} K$, i.e der Durchschnitt aller Kongruenzen, die $M$ enthalten.*

Da die Allrelation $A \times A$ immer eine Kongruenz ist, ist der obige Durchschnitt nie leer.

Sind $M$ und $N \subseteq A \times A$, so ist $\langle M \cup N \rangle = \langle \langle M \rangle \cup \langle N \rangle \rangle$, da einerseits $M \cup N \subseteq \langle M \rangle \cup \langle N \rangle$ gilt, andererseits ist $M \subseteq M \cup N \Longrightarrow \langle M \rangle \subseteq \langle M \cup N \rangle$, ebenso natürlich $\langle N \rangle \subseteq \langle M \cup N \rangle$, damit gilt also $\langle M \rangle \cup \langle N \rangle \subseteq \langle M \cup N \rangle$ und daraus folgt $\langle M \cup N \rangle \supseteq \langle \langle M \rangle \cup \langle N \rangle \rangle$.

Wir können nun die Äquivalenzklassen betrachten und darauf Operationen definieren:

**Definition 1.1.23** *Sei $A$ eine $\Omega$-Algebra, $K$ eine Kongruenz. Auf der Menge der Äquivalenzklassen $A/K = \{C(a_i)|a_i \in A\}$ definieren wir die Operationen $\omega_i^{A/K}$ mittels den Operationen $\omega_i^A$:*
*Für $Ar(\omega_i^A) > 0$ :*

$$\omega_i^{A/K}\left(C(a_1), C(a_2), ..., C(a_{Ar(\omega_i^A)})\right) = C\left(\omega_i^A(a_1, a_2, ..., a_{Ar(\omega_i^A)})\right)$$

*Ist $Ar(\omega_i^A) = 0 : \omega_i^{A/K} = C(\omega_i^A)$*

**Proposition 1.1.24** *Es seien $[A;\Omega]$ eine Algebra, $K$ eine Kongruenz von $A$. Dann ist $[A/K;\Omega]$ eine $\Omega$-Algebra. $\pi_K : A \to A/K$ mit $\pi_K(a) = C(a)$ ist ein surjektiver Homomorphismus, der sogenannte kanonische Epimorphismus.*

**Beweis:** Aufgrund der Definition einer Kongruenz sieht man, daß die Operationen wohldefiniert ist. Zwischen den Operationen auf $A$ und jenen auf $A/K$ gibt es eine eineindeutige Beziehung, somit ist $A/K$ eine $\Omega$-Algebra. Aus der Definition der Operationen aus $A/K$ sieht man, daß $\pi_K$ ein Homomorphismus ist. □

Wir können nun den Homomorphiesatz formulieren, dazu benötigen wir die folgende Definition:

**Definition 1.1.25** *Es seien $A$,$B$ $\Omega$-Algebren und $\varphi \in Hom(A,B)$. Die Relation $Ker(\varphi) \subseteq A \times A$ ist definiert durch:*

$$a_1 \sim_{Ker(\varphi)} a_2 :\Longleftrightarrow \varphi(a_1) = \varphi(a_2)$$

**Proposition 1.1.26** *$Ker(\varphi)$ ist eine Kongruenz.*

**Beweis:** Reflexivität, Symmetrie und Transitivität sind klar, also ist $Ker(\varphi)$ eine Äquivalenzrelation.
Sei $a_i \sim_{Ker(\varphi)} a_i'$ für $i = 1, \ldots, Ar(\omega)$. Dann ist

$$\varphi\left(\omega\left(a_1, a_2, \ldots, a_{Ar(\omega)}\right)\right) = \omega\left(\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_{Ar(\omega)})\right) =$$

$$= \omega\left(\varphi(a_1'), \varphi(a_2'), \ldots, \varphi(a'_{Ar(\omega)})\right) = \varphi\left(\omega\left(a_1', a_2', \ldots, a'_{Ar(\omega)}\right)\right)$$

□

**Satz 1.1.27** ( Homomorphiesatz) *Es seien $A$,$B$ $\Omega$-Algebren. Sei $\varphi \in Hom(A,B)$. Dann ist $A/Ker(\varphi)$ isomorph zum Bild $\varphi(A)$.*

$$A/Ker(\varphi) \simeq \varphi(A)$$

**Beweis:** Betrachte die Abbildung $\psi : A/Ker(\varphi) \to \varphi(A)$ mit $\psi(C(a)) = \varphi(a)$. Aus der Definition von $Ker(\varphi)$ folgt, daß diese Abbildung wohldefiniert ist. Aus der Definition der Operationen auf $A/K$ und aus der Eigenschaft, daß $\varphi$ ein Homomorphismus ist, folgt, daß $\psi$ ein Homomorphismus ist. $\psi$ ist klarerweise surjektiv, und wegen der Definition von $Ker(\varphi)$ injektiv. □

Wir können den Homorphiesatz umformulieren zu:

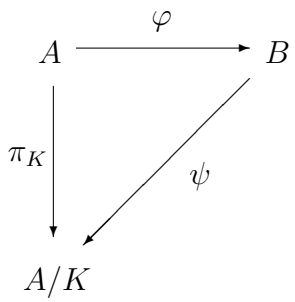


Abbildung 1.1: Homomorphiesatz

**Lemma 1.1.28** *Es seien $A$ und $B$ $\Omega$-Algebren. Sei $\varphi \in Epi(A,B)$. Dann gibt es eine Kongruenz $K \subseteq A \times A$ und $\psi \in Iso(B, A/K)$, sodass: $\psi \circ \varphi = \pi_K$. D.h. das Diagramm in Abbildung 1.1. ist kommutativ.*

**Beispiel:** Es sei $GL_n(\mathbb{R})$ die Menge aller invertierbaren $n \times n$-Matrizen über $\mathbb{R}$, $GL_n(\mathbb{R}) = \{A \in M_{n,n}(\mathbb{R}) | det(A) \neq 0\}$. Bezüglich der Multiplikation von Matrizen bildet $[GL_n(\mathbb{R}, \cdot, ^{-1}, \mathbb{1}]$ eine Gruppe, wobei

$$\mathbb{1} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

die *Einheitsmatrix* ist.

Es sei $\mathbb{R}^* = \mathbb{R} \backslash 0$. Sei $\varphi : [GL_n(\mathbb{R}), \cdot, ^{-1}, \mathbb{1}] \to [\mathbb{R}^*, \cdot, ^1/., 1]$ mit $\varphi(A) = det(A)$. Dann ist $\varphi$ ein Homomorphismus, denn

$$\varphi(A \cdot B) = \det(A \cdot B) = \det(A) \cdot \det(B) = \varphi(A) \cdot \varphi(B)$$

wie wir aus der linearen Algebra wissen. Die Abbildung $\varphi$ ist klarerweise surjektiv, denn für $r \in \mathbb{R}^*$ beliebig ist $\varphi(A) = r$ falls

$$A = \begin{pmatrix} r & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

Der Kern $Ker(\varphi) = \{A \in GL_n : det(A) = 1\} = SL_n(\mathbb{R})$. $SL_n(\mathbb{R})$ ist die *spezielle lineare Gruppe*. Nach obigem Satz gilt $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*$.

**Lemma 1.1.29** *Eine Algebra A ist einfach genau dann, wenn für jede Algebra B jeder Homomorphismus $\varphi : A \to B$ entweder ein Monomorphismus ist oder $Ker(\varphi)$ die Allrelation ist, d.h. $\varphi(A) \preceq B$ mit $|\varphi(A)| = 1$.*

**Beweis:** $\Longleftarrow$ Sei K eine Kongruenz auf A, dann ist der kanonische Epimorphismus $\pi_k : A \to A/K$ entweder ein Isomorphismus oder $|A/K| = 1$, also ist im ersten Fall $C(a) = \{b \,|\varphi(b) = \varphi(a)\} = \{a\}$ oder im zweiten Fall $C(a) = A$. Damit ist $K$ eine der trivialen Kongruenzen, also ist A einfach.
$\Longrightarrow$ Ist $\varphi$ ein Homomorphismus, so ist $Ker(\varphi)$ eine Kongruenz. Da A einfach ist, ist entweder $C(a) = \{a\}\ \forall a \in A$, dann ist $\varphi$ injektiv, oder $C(a) = A\ \forall a \in A$, also ist $|\varphi(A)| = 1$. □

**Lemma 1.1.30** *Seien A,B $\Omega$-Algebren und sei $\varphi \in Epi(A, B)$. Dann gibt es eine bijektive Beziehung zwischen den Kongruenzen auf B und jenen auf A, die $Ker(\varphi)$ enthalten.*

**Beweis:** Es sei $\mathfrak{M} = \{K \in \mathfrak{K}(A) : K \supseteq Ker(\varphi)\}$. Für jede Kongruenz $K \in \mathfrak{M}$ sei die Relation $\Phi(K)$ definiert durch: $g_1 \simeq_{\Phi(K)} g_2 \Longleftrightarrow \varphi(g_1) \simeq_K \varphi(g_2)$. Daraus folgt, daß $\Phi(K)$ eine Kongruenz ist und die Abbildung $\Phi : \mathfrak{M} \to \mathfrak{K}(B)$ bijektiv ist. □

Auf der Menge aller Kongruenzen $\mathfrak{K}(A)$ können wir eine Ordnung definieren:

**Definition 1.1.31** *Sei $K_1$, $K_2 \in \mathfrak{K}(A)$, dann ist:*

$$K_1 \leq K_2 :\Longleftrightarrow K_1 \subseteq K_2 \ (als\ Teilmengen\ von\ A \times A)$$

Man kann zeigen, daß dies eine Ordnung ist und daß bezüglich dieser Ordnung für jede nicht-leere Teilmenge $\mathfrak{M} \subseteq \mathfrak{K}(A)$ stets das Supremum und das Infinum von $\mathfrak{M}$ existieren, d.h. daß $\mathfrak{K}(A)$ ein vollständiger Verband (siehe A.4) ist:

**Lemma 1.1.32** $[\mathfrak{K}(A); \leq]$ *ist ein vollständiger Verband.*
*Die kleinste obere Schranke, das Supremum, einer Teilmenge M von Kongruenzen, $M \subseteq \mathfrak{K}(A)$, ist die folgende Kongruenz S:*

$$a \sim_S b :\Longleftrightarrow \exists K_i \in M, c_j \in A,\ soda\ss\ gilt$$

$$a \sim_{K_1} c_1, c_1 \sim_{K_2} c_2, \ldots, c_{r-2} \sim_{K_{r-1}} c_{r-1}, c_{r-1} \sim_{K_r} c_r = b$$

**Beweis:** [18] Kapitel 1, Satz 1.61.

**Definition 1.1.33** *Wir nennen eine Konstruktion wie in 1.1.32* **Kette der Länge r** *von $a$ nach $b$ in den $K_i$.*

Damit können wir die erzeugte Kongruenz genauer beschreiben. Sind $R$,$S$ Kongruenzen auf einer Algebra $A$, so ist $T = \langle R \cup S \rangle$ klarerweise gleich dem Supremum von $R$ und $S$. Für $a, b \in A$ gilt somit $a \sim_T b$ genau dann, wenn es eine Kette von $a$ nach $b$ in $R$ und $S$ gibt.

**Satz 1.1.34** (Isomorphiesatz) *Sei $A$ eine $\Omega$-Algebra, $K$ eine Kongruenz auf $A$. Sei $\mathfrak{M} \subseteq \mathfrak{K}(A)$ mit $\mathfrak{M} = \{L \in \mathfrak{K}(A) \,|L \geq K\}$. Dann gilt*

1. *Sei $L \in \mathfrak{M} \Longrightarrow \exists (L/K) \in \mathfrak{K}(A/K)$ : $C(a) \sim_{L/K} C(b) \Longleftrightarrow a \sim_L b$.*
2. *Sei $L' \in \mathfrak{K}(A/K) \Longrightarrow \exists \overline{L'} \in \mathfrak{M}$ : $a \sim_{\overline{L'}} b \Longleftrightarrow C(a) \sim_{L'} C(b)$.*
3. *Die Abbildung $\varphi : \mathfrak{M} \to \mathfrak{K}(A)$ mit $\varphi(L) = L/K$ ist ein Verbandsisomorphismus und $\varphi^{-1}(L') = \overline{L'}$.*
4. *$A/L \simeq (A/K)/(L/K)$*

**Beweis:** [18] Kapitel 1, Satz 1.71.

**Bemerkung:**

- Die Abbildung $\varphi : \mathfrak{M} \to \mathfrak{K}(A)$ im obigen Satz ist gerade die Abbildung $\phi \times \phi : A \times A \to A/K \times A/K$, wo $\phi : A \to A/K$ der kanonische Epimorphismus und wir unter $\phi \times \phi$ die komponentenweise Anwendung verstehen (siehe A.3.9). Dann ist

  $$C(a) \sim_{\varphi(L)} C(b) \Longleftrightarrow a \sim_L b \Longleftrightarrow (a,b) \in L \Longrightarrow (\phi(a), \phi(b)) \in (\phi \times \phi)(L)$$

  $$\Longleftrightarrow (C(a), C(b)) \in (\phi \times \phi)(L)$$

  Andererseits sei $(C(a), C(b)) \in (\phi \times \phi)(L)$

  $$\Longrightarrow \exists (a', b') \in L : (\phi \times \phi)(a', b') = (\phi(a'), \phi(b')) = (C(a), C(b))$$

  $$\Longrightarrow C(a) = C(a') \sim_{\varphi(L)} C(b') = C(b)$$

- Betrachten wir nun zwei Teilmengen $M$ und $N$ von $A \times A$ und die davon erzeugte Kongruenz $\langle M \cup N \rangle$, so ist also

  $$A/\langle M \cup N \rangle = (A/\langle M \rangle) / (\langle M \cup N \rangle / \langle M \rangle) = (A/\langle M \rangle) / \langle N \rangle_{A/<M>}$$

  wenn wir unter $\langle N \rangle_{A/<M>} = \langle (\phi \times \phi)(N) \rangle_{A/<M>}$ verstehen.

Die Menge der Funktionen von $A^k$ nach $A$ wird nach A.3.1 mit $F_k(A)$ bezeichnet.

**Definition 1.1.35** *Eine Funktion $f \in F_k(A)$, für die bzgl einer Kongruenz $K$ von $A$ gilt:*

$$x_i \sim_K y_i \ \forall i \Longrightarrow f(x_1, x_2, \ldots, x_k) \sim_K f(y_1, y_2, \ldots, y_k)$$

*nennen wir* **kompatibel mit K** *oder* **verträglich mit K**.
*Ist $f$ kompatibel für alle $K \in \mathfrak{K}(A)$ so nennen wir $f$* **kompatibel**.

### 1.1.3 Freie Algebra, freie Vereinigung, freies Produkt

In diesem Abschnitt bezeichne $\Omega$ stets eine Menge von Operationen. Weiters sei $\mathfrak{U}$ eine beliebige Unterklasse aller $\Omega$-Algebren.

**Definition 1.1.36** *Eine Algebra $[A;\Omega] \in \mathfrak{U}$ heißt* **frei über $X$ in $\mathfrak{U}$** *, wobei $X \subseteq A$, wenn $\forall B \in \mathfrak{U}$ jede Funktion $f : X \to B$ eindeutig zu einem Homomorphismus $\varphi : A \to B$ erweitert werden kann. Es sei $\iota : X \to A$ die Inklusion, dann gilt also:*

$$\forall B \in \mathfrak{U}, \forall f : X \to B \ : \ \exists!\ \varphi \in Hom(A,B) \text{ mit } \varphi|_X = \varphi \circ \iota = f$$

Damit ist das Diagramm in Abbildung 1.2. kommutativ.

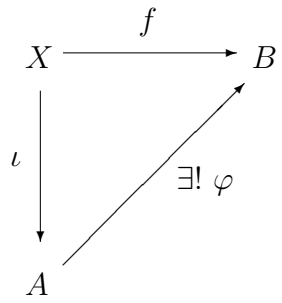


Abbildung 1.2: $A$ frei über $X$

**Bemerkung:**

1. Wenn $\mathfrak{U} \subseteq \mathfrak{U}'$ und $A$ frei in $\mathfrak{U}'$ ist, dann ist klarerweise $A$ auch frei in $\mathfrak{U}$.

2. Es gilt, daß $\varphi$ ein Epimorphismus ist, wenn $f$ surjektiv ist.

3. Andererseits gilt, daß $\varphi$ i.a. nicht injektiv ist, wenn $f$ injektiv ist, denn angenommen diese Eigenschaft gelte, dann betrachte $B = X$, dann wäre $\varphi$ ein Isomorphismus von $A$ nach $X$, also ist $X = A$. Es gibt jedoch Beispiele für freie Algebren, wo $X \neq A$ ist, z.B. ist $\mathbb{Z}$ als abelsche additive Gruppe frei über $\{1\}$, wie man sich leicht überlegen kann.

**Satz 1.1.37** *Ist $A$ frei über $X$ in $\mathfrak{U}$ und $B$ frei über $Y$ in $\mathfrak{U}$ und gilt $|X| = |Y|$, so gilt $A \simeq B$.*

**Beweis:** Da $|X| = |Y|$, gibt es also eine Bijektion $f : X \to Y$. Da $A$ frei über $X$ ist und $Y \subseteq B$, gibt es also einen eindeutigen Homomorphismus $\varphi$ , der $f : X \to B$ auf $A$ erweitert. Umgekehrt gibt es einen Homomorphismus $\psi$, der $f^{-1} : Y \to A$ auf $B$ erweitert. $\varphi \circ \psi$ ist somit ein Homomorphismus von $B$ nach $B$, der $id_B$ erweitert. Wegen der Eindeutigkeit der Erweiterung gilt also $\varphi \circ \psi = id_B$, ebenso ist auch $\psi \circ \varphi$ eine Erweiterung von $id_A$ als gleich $id_A$. Somit sind $\varphi$ und $\psi$ bijektiv. □

Daraus folgt unmittelbar

**Lemma 1.1.38** *Sind $A$ und $A'$ frei über $X$ in $\mathfrak{U}$, so gilt: $A \simeq A'$.*

**Definition 1.1.39** *Sei $\mathfrak{W} \subseteq \mathfrak{V}(\Omega)$. Sei $\{A_i \,|i \in I\} \subseteq \mathfrak{W}$. Eine Algebra $A$ mit den Abbildungen $\varphi_i \in Hom(A_i, A)$ heißt* **freie Vereinigung** *der Algebren $A_i$ in $\mathfrak{W}$, symbolisch: $A = \bigcup_{\varphi_i} A_i$., wenn es für jede Algebra $B$ aus $\mathfrak{W}$ und alle Homomorphismen $\psi_i \in Hom(A_i, B)$ einen eindeutigen Homomorphismus $\rho \in Hom(A, B)$ gibt, sodaß $\psi_i = \rho \circ \varphi_i$.*

Ist $A = \bigcup_{\varphi_i} A_i$ so ist das Diagramm in Abb. 1.3 für jedes $B \in \mathfrak{W}$ kommutativ.

Die freie Vereinigung der Algebren $A_i$ sind bis auf Isomorphie eindeutig:

**Proposition 1.1.40** *Seien $A = \bigcup_{\varphi_i} A_i$ und $A' = \bigcup_{\varphi'_i} A_i$ freie Vereinigungen der $A_i$ in $\mathfrak{W}$. Dann gibt es einen Isomorphismus $\rho \in Iso(A, A')$ mit $\varphi'_i = \rho \circ \varphi_i$.*

**Beweis:** [18] Kapitel 1, Proposition 3.31

**Definition 1.1.41** *Eine freie Vereinigung $A = \bigcup_{\varphi_i} A_i$ heißt* **freies Produkt**, *wenn alle $\varphi_i$ Monomorphismen sind und $\bigcup_{i \in I} \varphi_i(A_i)$ ein Erzeugendensystem von $A$ ist, i.e. $A = \left\langle \bigcup_{i \in I} \varphi_i(A_i) \right\rangle$. Symbolisch: $A = \bigotimes_{\varphi_i} A_i$*

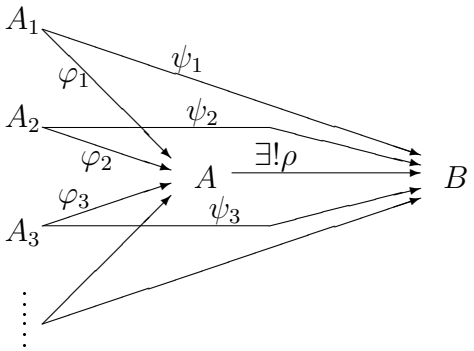


Abbildung 1.3: $A$ ist freie Vereinigung der $A_i$

### 1.1.4 Wörter

**Definition 1.1.42** *Es sei $\Omega$ eine Signatur. Sei weiters $M$ eine Menge, die disjunkt zu $\Omega$ ist. Wir definieren nun die* **Wörter in $M$ über $\Omega$** *, $W(M)_\Omega$ und deren Stufen induktiv:*

1. *Jedes $m \in M$ und jedes $\omega \in \Omega$ mit $Ar(\omega) = 0$ ist Wort 0-ter Stufe.*
2. *Für $k \geq 1$ sind die Wörter k-ter Stufe:*
   (a) *die Wörter der Stufe k-1.*
   (b) *die Ausdrücke der Form $\omega(w_1, w_2, ..., w_n)$, wobei $\omega \in \Omega$, $n = Ar(\omega) > 0$ und die $w_i$ Wörter $k-1$-ter Stufe sind.*

*Die minimale Stufe eines Wortes bezeichnen wir als den* **Rang** *des Wortes, symbolisch $r(w)$.*

*Ist $w$ ein Wort, so bezeichen wir als* **Unterwörter** *von $w$*

- *$w$ selbst*
- *die Unterwörter von den $w_i$, wenn $w = \omega(w_1, w_2, ..., w_n)$ ist.*

Durch Induktion nach dem Rang $r(w)$ eines Wortes $w$ sind also Unterwörter eindeutig definiert. Für $r = 0$ ist nur $w$ selbst ein Unterwort, für $r = 1$ und $w = \omega(w_1, w_2, ..., w_n)$ mit $r(w_i) = 0$ sind $w$ und diese $w_i$ Unterwörter. Für $r = m$ und $w = \omega(w_1, w_2, ..., w_n)$ mit $r(w_i) \leq m - 1$ sind also die Unterwörter der $w_i$ definiert, alle diese sind nun Unterwörter von $w$.

**Beispiel:** Seien $\odot$, $^*$ und $\Upsilon$ die Elemente von $\Omega$ mit $Ar(\odot) = 2$, $Ar(^*) = 1$ und $Ar(\Upsilon) = 0$. Sei $M = \{a, b\}$.
Dann sind die Wörter 0-ter Stufe: $\Upsilon, a, b$
Die Wörter 1-ter Stufe: $\odot(\Upsilon, a), \odot(\Upsilon, b), \odot(a, \Upsilon), \odot(b, \Upsilon), \odot(a, b), \odot(b, a)$, $^*(a), ^*(b), ^*(\Upsilon), a, b, \Upsilon$
bzw. in anderer Schreibweise: $\Upsilon \odot a, \Upsilon \odot b, a \odot \Upsilon, b \odot \Upsilon, a \odot b, b \odot a, a^*, b^*, \Upsilon^*, a$, $b$, $\Upsilon$
Ein Wort 4-ter Stufe ist zum Beispiel $a \odot (\Upsilon^* \odot (a \odot b))^*$.

Dieses (seltsam anmutende) Beispiel soll uns zeigen, daß Wörter nichts anders als Aneinanderreihung von „Symbolen“, von „Buchstaben“ aus $A$ und $\Omega$ sind, wobei die Aritäten der Elemente von $\Omega$ berücksichtigt werden, die ansonsten jedoch „sinnleer“, „formal“ sind.

Gehen wir nun zu dem für uns besonders interessanten Fall einer Algebra über:

**Definition 1.1.43** *Sei nun $A$ eine $\Omega$-Algebra, dann definiere auf $W(A)_\Omega$ die Operationen: $\omega$ angewandt auf die Wörter $w_1, w_2, ..., w_{Ar(\omega)}$ ist das Wort $\omega(w_1, w_2, ..., w_n)$ für $n = Ar(\omega) > 0$. Die 0-äre Operationen sind die Wörter, die den Operationssymbole entsprechen.*

*Wir bezeichnen das Wort $\omega(w_1, w_2, ..., w_n) \in W(A)_\Omega$ für $n = Ar(\omega) > 0$ oder das Wort $\omega \in W(A)_\Omega$ für $Ar(\omega) = 0$ als* **formale** *Operationen.*

Daraus folgt direkt:

**Lemma 1.1.44** $[W(A)_\Omega, \Omega]$ *ist eine $\Omega$-Algebra, die* **Wortalgebra** .

Die Bezeichnung „formal“ soll den Unterschied zwischen dem Wort in $W(A)_\Omega$ und der entsprechenden Operation in $G$ aufzeigen.

Zum besseren Verständnis betrachten wir ein Beispiel:

**Beispiel:** Sei $[G, \cdot, ^{-1}, 1]$ eine beliebige Gruppe $G = \{g_i | i \in I\}$. Dann können wir die Wörter auf $G$ induktiv bestimmen:

Die Wörter der Stufe 0 sind alle $g_i$ und 1. Nehmen wir an, daß das Einslement in $G$ ein anderes Symbol als die formale Eins ist, z.B. $e$ oder 0, so sind diese als Buchstaben in den Wörtern unterschiedlich! Die Wörter der 1-ten Stufe sind die formalen Produkte $g_i \cdot g_j$,$1 \cdot g_j$ und $g_i \cdot 1$ , die formalen Inversen $g_i^{-1}$ und $1^{-1}$ sowie die Wörter 0-ter Stufe. Die Wörter der 2-ten Stufe sind die Wörter $g_i \cdot g_j \cdot g_k$, die formalen Produkte $h_i \cdot h_j$, wobei die $h_i, h_j$ gleich $g_i, 1, g_i^{-1}$ oder $1^{-1}$ sein können (also Wörter 1-ter Stufe sind),

die formalen Inversen $h_i^{-1}$ mit $h_i$ ein Wort 1-ter Stufe, sowie alle Wörter der 1-ten Stufe.

Ingesamt sind also in $W(A)_\Omega$ alle endlichen formalen Produkte von den Elementen aus $G$ und 1, deren formalen Inversen und 1 enthalten.

Wir bereits erwähnt, bezeichnen wir ein Wort als *formales* Produkt oder formales Inverses, um zwischen dem Element in $W(A)_\Omega$ und der entsprechenden Operation in $G$ zu unterscheiden. So sind z.B. die Wörter $g_i \cdot g_i^{-1}$, $g_i^{-1} \cdot g_i$ und 1 in $W(A)_\Omega$ unterschiedlich, die entsprechenden Elemente in $G$ jedoch nicht!

Nehmen wir als konkretes Beispiel die Menge der ganzen Zahlen mit der Addition, $[\mathbb{Z}; +, -, 0]$, so sind die folgenden Wörter alle unterschiedlich:

$$1 + (1 + (1 + 1)), (1 + 1) + (1 + 1), 1 + 3, 4, (1 + 4) - 1, -(-1 + (-3))$$

Diese Beispiel läßt uns bemerken, daß man in der Wortalgebra einige „natürliche“ Äquivalenzen angeben kann (alle obigen Wörter sind in $\mathbb{Z}$ ausgewertet $= 4$). Das werden wir tun und dann die Quotientenalgebra betrachten ( siehe 1.1.62 ).

**Definition 1.1.45** *Mit $w(m_1, m_2, ...., m_k)$ bezeichnen wir ein Wort aus $W(M)$, in dem ausser den Elementen $\omega$ der Signatur $\Omega$ höchstens die Elemente $m_i \in M$ vorkommen.*

Beachte in dieser Definition das Wort „höchstens“. So sind z.B. in $W(\mathbb{Z})_{\{+,-,0\}}$

$$3 + 4, 1 + (2 + 4), -1 + (-2 + 3) \text{ und } (-4 + 3) - 1$$

alle Wörter in $1, 2, 3$ und $4$ also $w(1, 2, 3, 4)$. Wir lassen diese „Ungenauigkeit“ zu, da wir oft ein Wort nicht eindeutig bestimmen können, z.B. beim Übergang zu einer Quotientenalgebra, wir aber dennoch Aussagen über das Wort machen können, es bei verschiedenen Worten „angenehmer“ ist *oBdA* davon ausgehen zu können, daß sie Wörter in denselben Buchstaben sind.

**Definition 1.1.46** *Es seien $M$, $A$ Mengen, $k \geq 1$ eine ganze Zahl und $m_i \in M$ und $a_i \in A$ für $i = 1, \ldots, k$ Ist $w(m_1, m_2, ...., m_k) \in W(M)_\Omega$, dann bezeichnen wir mit $w(a_1, a_2, ...., a_k)$ das Wort aus $W(A)_\Omega$, wo jedes $m_i$ durch das $a_i$ ersetzt wird.*

Diese Zuordnung ist eindeutig, denn ist $w(m_1, \ldots, m_k) = w(m_1, \ldots, m_n)$ (obdA $k \leq n$ und die Unterwörter $m_i$ sind für $i = 1, \ldots, k$ gleich) dann

gibt es die Elemente $m_{i_1}, \ldots, m_{i_l}$ sodaß $w(m_1, \ldots, m_k) = w(m_1, \ldots, m_n) = w(m_{i_1}, \ldots, m_{i_l})$, sodaß genau die $m_{i_j}$ im Wort vorkommen. Dann ist aber

$$w(a_1, \ldots, a_k) = w(a_1, \ldots, a_n) = w(a_{i_1}, \ldots, a_{i_l})$$

Auch für jede Umordnung der $m_i$ bleibt diese Zuordnung eindeutig.

**Beispiel:** Ist $w(g_1, g_2, g_3) = g_1 \cdot g_2^{-1}$, so ist $w(1, 2, 3) = 1 \cdot 2^{-1}$.

Wir werden manchmal $w(a_i; x_j)$ als Abkürzung für

$$w(a_1, a_2, \ldots, a_n, x_1, x_2, \ldots, x_m)$$

verwenden, wenn die Bedeutung klar ist.

**Bemerkung** ( über das Auswerten ): Sei $A$ eine Algebra. Die Elemente von W(A) sind (bis jetzt) eine Aneinanderreihung von Symbolen aus $(A \cup \Omega \cup \{(,)\})$. Eine Beziehung zu der Algebra $A$ kann durch "'Auswerten"' erlangt werden. Wir können jedem Wort $w = w(a_1, a_2, ..., a_n) \in W(A)$ ein Element $\varphi(w)$ aus $A$ zuweisen, indem wir den Unterwörtern, beginnend mit dem niedrigsten Rang das Ergebnis der entsprechenden Operation zuordnen. Indem wir also den formalen Operationen jene in $A$ zuordnen:

Ist der Rang $r = 0$, dann ist entweder $w = a$ mit $a \in A$ oder $w = \omega_i$ mit $Ar(\omega_i) = 0$. Im ersten Fall sei $\varphi(w) = a$, im zweiten Fall ordnen wir $\varphi(w)$ jenes feste Element aus A zu, daß die 0-äre Operation $\omega_i$ auswählt.

Ist der Rang r $> 0$, dann nehmen wir an, wir haben allen Wörtern niedrigerer Ränge bereits ein Element aus A zugeordnet. $w = \omega(w_1, ..., w_{Ar(\omega)}) \Longrightarrow \varphi(w) = \omega(a_1, ..., a_{Ar(\omega)}) \in A$ mit $\varphi(w_i) = a_i$.

Diese Abbildung ist klarerweise ein Epimorphismus.

**Definition 1.1.47** *Diesen Epimorphismus $\varphi : W(A) \to A$ bezeichnen wir als den* **„Auswerteepimorphismus"**, *symbolisch $|.|_A$.*

**Definition 1.1.48** *Sei $[A; \Omega]$ eine Algebra, dann nennen wir die Elemente von $X = \{x_1, x_2, ..., x_k\}$* **Unbestimmte** *, wenn diese Menge disjunkt zu $A$ ist.*

**Bemerkung:** Sei $X = \{x_1, ..., x_k\}$ eine Menge von Unbestimmten. Sei $w = w(x_1, x_2, ..., x_n) \in W(X)$. Ersetzen wir nun jedes $x_i$ durch ein $a_i \in A$, so erhalten wir ein Wort aus $W(A)$. Mit $|.|_A$ ergibt sich ein Element aus A. D.h. wir können jedem $w \in W(X)$ eine Funktion $f_w : A^k \to A$ zuordnen. D.h. $\sigma_k[A] : W(X) \to F_k(A)$ mit $\sigma_k[A] : w \mapsto f_w$ ist eine Funktion. Es ist leicht zu sehen, daß das ein Homomorphismus ist.

**Definition 1.1.49** $T_k(A) = \sigma_k[A](W(X)) = \{f \in F_k(A) : \exists w \in W(X) : f(a_1, \ldots, a_k) = w(a_1, \ldots, a_k)\}$ *ist die Menge der k-wertigen* **Termfunktionen**.

Ist $w \in W(X)$, so bezeichnen wir $\sigma_k[A](w)$ oft mit demselben Symbol $w$, wenn es klar ist, daß damit die Funktion $A^k \to A$ gemeint ist. Wir lassen oft, so wie hier, ambivalente Bezeichnungen zu, aber es zeigt sich, daß wir keine Klarheit verlieren, aber viele eigentlich redundante Symbole weglassen können.

Die Kenntnis des Auswerteepimorphismus wäre sehr interessant. Welche Wörter induzieren dieselbe Funktion? Dieses Problem ist als Wortproblem bekannt, wir werden uns diesem Problem in 1.2.1 zuwenden.

**Proposition 1.1.50** *Es seien $A, B$ $\Omega$-Algebren, $X$ eine Menge von Unbestimmten. Sei $\varphi \in Hom(A, B)$, dann ist für $w \in W(X)$ mit $w = w(x_1, \ldots, x_n)$*

$$\varphi(w(a_1, a_2, ..., a_n) = w(\varphi(a_1), \varphi(a_2), ..., \varphi(a_n)).$$

*D.h.*

$$\varphi \circ \sigma_k[A](w) = \sigma_k[B](w) \circ \varphi^n$$

**Beweis:** Induktion nach dem Rang $r$ des Wortes $w(a_1, a_2, ..., a_k)$:
Für $r = 0$ gilt die Aussage, denn für $w = \omega$ mit $Ar(\omega) = 0$ ist $\varphi(w) = \varphi(\omega) = \omega = w$ und ist $w = w(a_i) = a_i$ so ist $\varphi(w) = \varphi(a_i) = w(\varphi(a_i))$.
Sei nun die Aussage für Wörter der Ränge 0,1,..., $r-1$ gezeigt. Sei $w(a_1, a_2, ..., a_k)$ ein Wort des Rangs $r$. Dann ist

$$w(a_1, a_2, ..., a_k) = \omega\left(w_1(a_1, a_2, ..., a_k), w_2(a_1, a_2, ..., a_k), ..., w_n(a_1, a_2, ..., a_k)\right)$$

wobei $w_i$ Wörter von Rängen $\leq$ r sind und $n = Ar(\omega) > 0$. Dann ist

$$\varphi\left(w(a_1, a_2, ..., a_k)\right) =$$

$$= \varphi\left(\omega\left(w_1(a_1, a_2, ..., a_k), w_2(a_1, a_2, ..., a_k), ..., w_n(a_1, a_2, ..., a_k)\right)\right) =$$

$$\overset{\varphi \overset{Hom}{=}}{=} \omega\left(\varphi\left(w_1(a_1, a_2, ..., a_k)\right), \varphi\left(w_2(a_1, a_2, ..., a_k)\right), ..., \varphi\left(w_n(a_1, a_2, ..., a_k)\right)\right) =$$

$$\overset{Ind.vorr.}{=} \omega\left(w_1\left(\varphi(a_1), \varphi(a_2), ..., \varphi(a_k)\right), w_2\left(\varphi(a_1), \varphi(a_2), ..., \varphi(a_k)\right)\right), ...$$

$$..., w_n\left(\varphi(a_1), \varphi(a_2), ..., \varphi(a_k)\right)$$

□

**Proposition 1.1.51** *Es sei $A$ eine $\Omega$-Algebra. $W(A)_\Omega$ ist frei über $A$ in $\mathfrak{V}(\Omega)$.*

**Beweis:** D.h. zu zeigen ist, daß jede Funktion $f : A \to B$, in der B eine $\Omega$-Algebra ist, eindeutig zu einem Homomorphismus $\varphi : W(A) \to B$ erweitert werden kann. Wir definieren:

$$\varphi(w(a_1, a_2, ..., a_n)) = w(f(a_1), f(a_2), ..., f(a_n)) \quad für\ a_i \in A\ \forall\ i = 1, ..., n$$

Diese Zuordnung ist nach 1.1.46 eindeutig. Sie ist klarerweise ein Homomorphismus. Jeder Homomorphismus muß aber nach der vorherigen Behauptung diese Definition erfüllen. □

**Proposition 1.1.52** *Es sei $A$ eine $\omega$-Algebra. $M \subseteq A$. Dann gilt: $\langle M \rangle_A = |W(M)_\Omega|_A$*

**Beweis:** $|.|_A$ ist klarerweise ein Epimorphismus. Damit ist $|W(M)_\Omega|_A \prec A, M \subseteq |W(M)_\Omega|_A \Longrightarrow \langle M \rangle_A \subseteq |W(M)_\Omega|_A$
Andererseits muß in jeder Algebra, die M enthält, jedes Wort $w(m_1, .., m_n)$ aus M enthalten sein, wie man leicht mit Induktion nach dem Rang des Wortes w zeigen kann. $\Longrightarrow |W(M)_\Omega|_A \subseteq \langle M \rangle_A$ □

Eine alternative Formulierung von (1.1.52) ist unter Verwendung von Termfunktionen:

**Proposition 1.1.53** *$A$ $\Omega$-Algebra, $M \subseteq A$. Dann ist:*

$$\langle M \rangle_A = \bigcup_{k \in \mathbb{N}} \{t(m_1, m_2, \ldots, m_i) \,|t \in T_k(A), m_1, m_2, \ldots, m_i \in M\}$$

**Proposition 1.1.54** *$A$ sei eine $\Omega$-Algebra, $M \subseteq A$, sodaß $A = \langle M \rangle_A$ dann gilt:*

$$A \simeq W(M)_\Omega / Ker|.|_A$$

*Insbesondere ist also jede Algebra Quotient einer freien Algebra.*

**Beweis:** Das folgt sofort aus dem Homomorphiesatz (1.1.27). □

Ist $M \subseteq A$, so ist für $m_1, \ldots, m_l \in M$ $|w(m_1, \ldots, m_l)|_A \in A$. Zur Vereinfachung werden wir oft die $|.|_A$ weglassen, da es klar ist, wenn ein Wort $w \in A$ ist, daß damit nur die Auswertung gemeint sein kann. Also ist $w = w(m_1, \ldots, m_l) \in A$, so meinen wir damit $w = |w(m_1, \ldots, m_l)|_A$.

Aus 1.1.50 folgt daß für einen Homomorphismus $\varphi : A \to B$ und $a = |w(m_1, \ldots, m_l)|_A = w(m_1, \ldots, m_l)$ gilt:

$$\varphi(a) = \varphi(w(m_1, \ldots, m_l)) = w(\varphi(m_1), \ldots, \varphi(m_l))$$

**Bemerkung:** Satz 1.1.54 ermöglicht die Darstellung von Algebren mit Erzeugenden und Relationen. Der Kern von $|.|_A$ besteht aus allen Elementen $(w(m_i), w'(m_j))$ von $W(M) \times W(M)$ für die in A gilt $w(m_i) = w'(m_j)$. Solche Relationen nennen wir *Identitäten*, siehe Kapitel 1.1.5. Wir können nach oben jede Algebra als $A = W(S)/\langle R\rangle$ darstellen, wobei $A = \langle S\rangle$ ist und $R$ eine Untermenge von $W(S) \times W(S)$ sowie $\langle R\rangle$ die davon erzeugte Kongruenz ist. Man schreibt dann auch kurz $A = \langle S; R\rangle$.

Umgekehrt können wir auch die Algebra $A$ suchen, wenn wir die Mengen $S$ und $R$ kennen. In Kapitel 1.1.5 werden wir ein Beispiel zu dieser Darstellung angebenn.

Aus den vorherigen Sätzen und jenen über freie Algebren folgt

**Proposition 1.1.55** *Es sei $A$ eine $\Omega$-Algebra, $\mathfrak{W} \subseteq \mathfrak{V}(\Omega)$. Ist $A$ frei über $X$ in $\mathfrak{W}$, so ist $A \simeq W(X)$, der Isomorphismus ist der Auswerteepimorphismus, $|.|_A : W(X) \to A$. Damit gilt $A = \langle X\rangle$. Gibt es ein weiteres Erzeugendensystem $Y$ von $A$, dann ist $|Y| \geq |X|$.*

**Beweis:** Sowohl $A$ als auch $W(X)$ sind frei über $X$, damit wissen wir daß also $A \simeq W(X)$. Wie sieht dieser Isomorphismus aus? Es kann $\iota_1 : X \to A$ eindeutig zu einem $f : W(X) \to A$ erweitert werden. Da $f$ eindeutig ist, ist $f = |.|_A$. Ebenso kann $\iota_2 : X \to W(X)$ zu einem $g : A \to W(X)$ erweitert werden. Somit sind aber wegen der Eindeutigkeit $f \circ g = id_A$ und $g \circ f = id_{W(X)}$, d.h. $|.|_A$ ist der gesuchte Isomorphismus. Sei $Y$ ein weiteres Erzeugendensystem von $A$, mit $|Y| < |X|$, also gibt es eine surjektive Abbildung von $f : X \to Y$, die nicht injektiv ist. Also kann die Abbildung zu einem Epimorphismus $f' : W(X) \to W(Y)$ erweitert werden, es gilt jedoch $W(Y) = W(X)$. Seien $x, x'$ zwei verschiedene Elemente aus $X$ mit $f(x) = f(x') = y$, dann ist aber $y = w(x_j)$ und diese Darstellung ist nach oben eindeutig, also ist $x = x'$. Widerspruch □

Beachten sollte man, daß aus dieser Proposition folgt, daß bei einer freien Algebra $A$ über $X$ die Darstellung eines Elements durch Worte in $X$ eindeutig ist.

**Proposition 1.1.56** *Seien $A, B$ $\Omega$-Algebren, $S \subseteq A$. Sei $A = \langle S\rangle$. Ist $f : S \to B$ eine Abbildung, so gibt es höchstens einen Homomorphismus*

*$\varphi : A \to B$, der $f$ erweitert, d.h. $\varphi|_S = f$.*
*Ist $B = \langle T \rangle$ und ist $f : S \to T$ surjektiv, so ist dieser Homomorphsimus $\varphi$ surjektiv, falls er existiert.*

**Beweis:** Seien $\varphi_1, \varphi_2$ zwei solche Homomorphismen, dann ist für $a = |w(s_i)|_A = w(s_i)$ :

$$\varphi_1(a) = \varphi_1(w(s_i)) = w(\varphi_1(s_i)) = w(f(s_i)) = w(\varphi_2(s_i)) = \varphi_2(a)$$

Sei nun $B = \langle T \rangle$, dann kann jedes $b \in B$ ausgedrückt werden als $b = w(t_i)$ mit $t_i \in T$, seien $s_i \in S$ mit $f(s_i) = t_i$, dann ist $\varphi(w(s_i)) = w(\varphi(s_i)) = w(t_i)$, wenn dieser Homomorphismus $\varphi$ existiert. □

Insbesondere ist somit ein Homomorphismus bereits durch die Wirkung auf ein Erzeugendensystem eindeutig bestimmt.

### 1.1.5 Varietäten

**Definition 1.1.57** *Sei $A$ eine $\Omega-$Algebra, $X = \{x_1, ..., x_k\}$ Unbestimmte. Ein Wortpaar $\gamma \in W(X) \times W(X)$ nennen wir* **Gleichung**. *Eine Gleichung $(w_1, w_2)$* **gilt in A**, *wenn $w_1(a_1, ..., a_k) = w_2(a_1, ..., a_k)$ $\forall a_i \in A$. Wir nennen diese Gleichung dann* **Gesetz von A**. *D.h. $\sigma_k[A](w_1) = \sigma_k[A](w_2)$. Ist $\mathfrak{W} \subseteq \mathfrak{V}(\Omega)$ eine Unterklasse der Klasse aller $\Omega$-Algebren, so bezeichnen wir die Menge aller Gesetze, die in jeder Algebra $A \in \mathfrak{W}$ gelten, mit $\Gamma(\mathfrak{W})$, die* **Gesetze von $\mathfrak{W}$** .

*Ein Wortpaar $\iota = (w_1, w_2) \in W(A) \times W(A)$ nennen wir* **Identität für A** , *wenn in $A$ gilt $w_1 = w_2$.*

Jedes Gesetz angewandt auf Elemente von $A$ ist eine Identität. Der Kern der Abbildung $|.|_A$ besteht genau aus allen Identitäten.

**Beispiel** Auf der Menge der ganzen Zahlen ist $1 + 1 = 2$ eine Identität und $x + (-x) = 0$ ein Gesetz.

In der klassischen Algebra beschäftigt man sich mit bestimmten Klassen von Algebren, die nicht nur einen gewissen Typ von Operationen besitzt, sondern auch bestimmten Gesetzen wie zum Beispiel dem Assoziativitätsgesetz gehorchen. Das führt uns zu der folgenden Definition:

**Definition 1.1.58** *Sei $\Omega$ eine Menge von Operationen. $\Gamma$ eine Menge von Gleichungen. Dann nennen wir die Klasse aller $\Omega$-Algebren, in der alle Gleichungen aus $\Gamma$ gelten, eine* **Varietät** , $\mathfrak{V} = \mathfrak{V}(\Omega, \Gamma)$

**Definition 1.1.59** *Varietäten $\mathcal{V}$, die nur ein-elementige Algebren $A$ enthalten, nennen wir* **vollständig entartet**.

$$\mathfrak{V} \text{ vollständig entartet} \Longleftrightarrow \forall A \in \mathcal{V} : |A| = 1$$

*Gilt für alle Algebren $A \in \mathcal{V}$ mit $|A| > 1$, daß sie keine ein-elementigen Unteralgebren enthalten, so nennen wir die Varietäten $\mathfrak{V}$* **halb entartet**.

$$\mathfrak{V} \text{ halb entartet} \Longleftrightarrow \forall A \in \mathcal{V} : (|A| = 1 \vee (\forall U \prec A \Longrightarrow |U| \neq 1))$$

**Bemerkung:** Die Bedingung für „halb entartet“ ist für vollständig entartete Varietäten klarerweise erfüllt. Also folgt aus „vollständig entartet“ „halb entartet“.

Die Eigenschaften „vollständig entartet“ und „halb entartet“ übertragen sich klarerweise auf Untermengen, und somit auf alle enthaltenen Varietäten.

Es läßt sich eine interessante Tatsache über freie Algebren formulieren:

**Proposition 1.1.60** *Sei $\mathfrak{W} \subseteq \mathfrak{V}(\Omega)$, sei $A$ eine freie Algebra über $X$ in $\mathfrak{W}$. Sei $k \in \mathbb{N}$, und $w_1, w_2 \in W(X)$ und seien $x_1, \ldots, x_k \in X$ paarweise verschieden. Dann gilt*

$$w_1(x_1, \ldots, x_k) = w_2(x_1, \ldots, x_k) \Longleftrightarrow (w_1, w_2) \in \Gamma(\mathfrak{W})$$

**Beweis:** [1] Satz 1.58

D.h. gilt eine Gleichung in $X$ (mit paarweise verschiedenen $x_i$), so gilt sie bereits in allen Algebren in $\mathfrak{W}$.

**Beispiel:** Die meisten algebraischen Strukturen der klassischen Algebra sind Varietäten.

So ist die Klasse der *Gruppen* die Varietät $\mathfrak{V}(\Omega, \Gamma)$ mit

- $\Omega = \{\cdot, ^{-1}, 1\}$

des Typs {2,1,0} und den Gleichungen

- $x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$ $(Assoziativität)$
- $x_1 \cdot 1 = x_1$ $(Eins)$
- $x_1 \cdot x_1^{-1} = 1$ $(Inverses)$

also ist

$$\Gamma = \{(x_1 \cdot (x_2 \cdot x_3)\,, (x_1 \cdot x_2) \cdot x_3)\,; (x_1 \cdot 1, x_1)\,; \left(x_1 \cdot x_1^{-1}, 1\right)\}$$

Ebenso sind u.a. die Ringe, die kommutativen Ringe mit Eins und die Verbände Varietäten. Die Klasse der *Körper* ist keine Varietät bzgl. $\Omega = \{+, \cdot, -^{-1}, 0, 1\}$, da das Auffinden des multiplikativen Inversen keine Operation ist. (0 ist ausgenommen.) Würde man 0 dazu nehmen, es also $0^{-1}$ geben, so hätte man eine vollständig entartete Varietät:

$$1 = 0 \cdot 0^{-1} = 0 \implies a = a \cdot 1 = a \cdot 0 = 0 \quad \forall\, a \in K$$

Die Klasse der Ringe mit (linker) Eins ist halb entartet, denn angenommen die Algebra $A$ hat eine Unteralgebra $B$ mit $|B| = 1$, dann ist $1 = 0$, damit aber $x = 1 \cdot x = 0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x = 1 \cdot x + 1 \cdot x = x + x$ $\implies x = 0\ \forall x$. Jede Varietät, die in dieser Varietät enthalten ist, ist somit auch halb entartet. Es gibt eine größere Varietät für die das gilt, siehe 3.1.5.

**Satz 1.1.61** *Sei $\mathfrak{V}$ eine Varietät und $A \in \mathfrak{V}$. Dann ist jede Unteralgebra $(A' \preceq A) \in \mathfrak{V}$ und jedes homomorphe Bild $\varphi(A) \in \mathfrak{V}$. Ist $\{A_i\} \subset \mathfrak{V}$ dann ist auch das Produkt $\prod_i A_i \ \in \mathfrak{V}$.*

D.h. für Varietäten gilt die Abgeschlossenheit bzgl. Bildung von Unteralgebren, homomorphen Bildern und Produkten. Es gilt aber auch die Umkehrung: Jede Klasse von Algebren, die bezüglich dieser Operationen abgeschlossen ist und die zumindest eine Algebra mit nicht leerer Trägermenge enthält, ist eine Varietät (siehe [2] Satz IV.3.1).

Insbesondere folgt daraus, daß die Klasse der Körper auch bezüglich anderer Operationenmengen keine Varietät bilden, da das direkte Produkte von Körpern keine Körper sind. Denn es gibt nicht nur für $(0, \ldots, 0)$ sondern für alle $(a_1, \ldots, a_k)$, für die es ein $1 \leq i \leq k$ gibt, sodaß $a_i = 0$, kein multiplikatives Inverses.

Wir werden für Varietäten nun freie Algebren konstruieren. Wir werden die freie Algebra $W(X)$ betrachten und dort eine Relation definieren, sodaß wir eine Algebra der gegebenen Varietät erhalten.

**Satz 1.1.62** *Für jede beliebige Kardinalität der Menge $X$ gibt es in jeder nicht entarteten Varietät $\mathfrak{V}$ freie Algebren über der Menge $X$ in $\mathfrak{V}$.*

**Beweis:** Sei $\mathfrak{V} = \mathfrak{V}(\Gamma)$. Sei $X = \{x_i \,|i \in I\,\}$ eine Menge von Unbestimmten von beliebiger Kardinalität.

Wir konstruieren nun eine Relation $R$ auf der Wortalgebra $W(X)$. Die Menge $P \subseteq W(X) \times W(X)$ bestehe aus den folgenden Elementen:

1. $(w, w)$ wo $w \in W(X)$ (Die diagonalen Elemente sind enthalten).

2. $(w_1(u_1, \ldots, u_k), w_2(u_1, \ldots, u_k))$ und $(w_1(u_2, \ldots, u_k), w_1(u_1, \ldots, u_k))$, wo $((w_1(y_1, \ldots, y_k), w_2(y_1, \ldots, y_k)) \in \Gamma$ und $u_i \in W(X)$ für $1 \leq i \leq k$.

Dann gelte $w \sim_R w'$ genau dann, wenn eine endliche Kette von $w$ nach $w$ ' in $P$ existiert, d.h. $\exists r : \exists v_i,\ i = 1, \ldots, r$, sodaß $w = v_0, v_1, \ldots, v_r = w'$, wobei man von $v_i$ auf $v_{i+1}$ kommt, indem man ein Unterwort $v_i'$ von $v_i$ durch ein Wort $v_i''$ ersetzt, für das gilt: $(v_i', v_i'') \in P$. (D.h. entweder ist $v_i = v_{i+1}$ oder wir ersetzen ein Unterwort durch ein bezüglich der Gesetze von $\mathfrak{V}$ äquivalentes Wort.)

$R$ ist klarerweise reflexiv, symmetrisch. R ist transitiv, da wir zwei entsprechende Kette einfach hintereinanderhängen können, damit ist $R$ eine Äquivalenzrelation.

$R$ ist eine Kongruenz, denn angenommen es sei $\omega \in \Omega$ mit $Ar(\omega) > 0$. Es seien $w_i$ und $w_i'$ Wörter aus $W(X)$ für $i = 1, \ldots, Ar(\omega))$ mit $w_i \sim_R w_i'$. D.h. es gibt für jedes $i$ eine Kette der Länge $r_i$ von $w_i$ nach $w_i'$ : $w_i = v_0^i, v_1^i, \ldots, v_{r_i}^i = w_i'$ so können wir auch eine Kette von $\omega\left(w_1, \ldots, w_{Ar(\omega)}\right)$ nach $\omega\left(w_1', \ldots, w_{Ar(\omega)}'\right)$ konstruieren, indem wir in jedem Schritt ein Wort durch ein äquivalentes Wort aus den bekannten Ketten ersetzen:

$$\omega\left(w_1, w_2, \ldots, w_{Ar(\omega)}\right), \omega\left(v_1^1, w_2, \ldots, w_{Ar(\omega)}\right), \ldots, \omega\left(w_1', v_1^2 \ldots, w_{Ar(\omega)}\right), \ldots$$

$$\ldots\ldots\ldots$$

$$\ldots, \omega\left(w_1', \ldots, w_{Ar(\omega)-1}', w_{Ar(\omega)}\right), \omega\left(w_1', \ldots, w_{Ar(\omega)-1}', v_1^{Ar(\omega)}\right), \ldots$$

$$\ldots, \omega\left(w_1', \ldots, w_{Ar(\omega)-1}', v_{r-1}^{Ar(\omega)}\right), \omega\left(w_1', \ldots, w_{Ar(\omega)-1}', w_{Ar(\omega)}'\right)$$

Wir werden nun zeigen, daß $W(X)/R$ eine freie Algebra in $\mathfrak{V}$ über $\overline{X} = \{C(x_i) | i \in I\}$ ist, wobei $\left|\overline{X}\right| = |X| = |I|$. Wir zeigen zuerst die letzte Behauptung. Angenommen sie gilt nicht, so gibt es $n, m$, sodaß $C(x_n) = C(x_m)$, d.h. es gibt eine Kette von $x_n$ nach $x_m$. D.h. $x_n = x_m$ ist ein Gesetz aus $\Gamma$, somit ist $\mathfrak{V}$ vollständig entartet. Widerspruch.

Da $W(X) = \langle X \rangle$, ist $W(X)/R = \left\langle \overline{X} \right\rangle$. Sei $w_1(y_1, \ldots, y_k) = w_2(y_1, \ldots, y_k) \in \Gamma$ und $u_1, \ldots, u_k \in W(X)$. Dann ist

$$w_1(C(u_1), \ldots, C(u_k)) \overset{(1.1.50)}{=} C(w_1(u_1, \ldots, u_k)) = C(w_2(u_1, \ldots, u_k)) =$$

$$= w_2(C(u_1), \ldots, C(u_k))$$

Also ist $W(X)/R$ eine Algebra aus $\mathfrak{V}$. Sei nun $A \in \mathfrak{V}$ beliebig, und $\varphi : \overline{X} \to A$ eine beliebige Abbildung. Wir definieren nun eine Abbildung $\psi$ :

$W(X)/R \to A$ durch $\psi\left(C(w(x_{i_1},\ldots,x_{i_k})\right) := w\left(\varphi(C(x_{i_1},\ldots,x_{i_k})\right)$. $\psi$ ist wohldefiniert, denn angenommen $w_1(x_{i_1},\ldots,x_{i_k}) \sim_R w_1(x_{i_1},\ldots,x_{i_k})$. Dann ist
$w_1\left(\varphi(C(x_{i_1},\ldots,x_{i_k})\right) \sim_R w_2\left(\varphi(C(x_{i_1},\ldots,x_{i_k})\right)$, da wir eine Kette von $w_1$ nach $w_2$ finden, indem wir in der Kette von $w_1$ nach $w_2$ jedes $x_j$ durch ein $\varphi\left(C(x_j)\right)$ ersetzen. Klarerweise ist $\psi$ eine Erweiterung von $\varphi$, und

$$\psi\left(\omega_i\left(C(w_1),\ldots,C(w_{Ar(\omega_i)})\right)\right) \overset{R\in\mathfrak{K}(W(X))}{=} \psi\left(C\left(\omega_i\left(w_1,\ldots,w_{Ar(\omega_i)}\right)\right)\right) =$$

$$\overset{Def.\ +\ 1.1.50}{=} \omega_i\left(\psi\left(C(w_1),\ldots,C(w_{Ar(\omega_i)})\right)\right)$$

Also ist $\psi$ ein Homomorphismus. Jeder Homomorphismus, der $\varphi$ erweitert muß aber die Definition von $\psi$ erfüllen, also ist $\psi$ eindeutig bestimmt, also ist $W(X)/R$ frei. □

**Definition 1.1.63** *Die freie Algebra über $X = \{x_i \,|i \in I\}$ der Varietät $\mathfrak{V}$ bezeichnen wir mit $F(X,\mathfrak{V})$.*

Ist $\mathfrak{V}(\Gamma)$ vollständig entartet, so können wir $(x_1, x_2)$ ohne Änderung der Varietät zu $\Gamma$ hinzufügen, also ist $C(x_m) = C(x_n)\ \forall n, m$, vielmehr noch $C(w) = C(w')\ \forall w, w'$ und damit $|F(X,\mathfrak{V})| = |W(X)/R| = 1$. Also bezeichnen wir mit $F(X,\mathfrak{V})$ die (bis auf Isomorphie) einzige Algebra dieser Varietät.

Sei nun $A$ eine Algebra der Varietät $\mathfrak{V}$. Aus der Definition der Relation in 1.1.62 sieht man, daß der Epimorphismus $\sigma_k$ aus 1.1.49 mit dieser verträglich ist. D.h. wir können $\sigma_k$ auf $F(X,\mathfrak{V})$ anwenden, $\sigma'_k : F(X,\mathfrak{V}) \to F_k(A)$ mit $\sigma'_k\left(C(w(x_1,\ldots,x_k))\right) = \sigma_k(w(x_1,\ldots,x_k))$. Dies ist dann wieder ein Epimorphismus, den wir wieder mit $\sigma_k$ bezeichnen, und es gilt auch für die Menge der Termfunktionen $T_k(A) = \sigma_k(F(X,\mathfrak{V}))$.

Man kann zeigen, daß es für Varietäten $\mathfrak{V}$ für jede Menge von Algebren auch die freie Vereinigung gibt, siehe [2] Kapitel IV, Korollar 3.4.

**Beispiel:** Der Satz 1.1.54 ermöglicht wie bereits erwähnt die Darstellung von Algebren mit Erzeugenden und Relationen. Der Kern von $|.|_A$ besteht aus allen Elementen $(w(m_i), w'(m_j))$ von $W(M) \times W(M)$ für die in A gilt $w(m_i) = w'(m_j)$, d.h. aus allen Identitäten (vgl. 1.1.5).

Als Beispiel ziehen wir wieder die Gruppen heran.( Im Kern $|.|_A$ sind inbesondere die Gruppengesetze enthalten.) Betrachte $G = \langle\{x,y\};\{x^3, y^3, (xy)^3\}\rangle$, d.h. $G$ ist jene Gruppe für die neben den Gruppeneigenschaften, d.h. den Gesetzen der Gruppe, auch die Gleichungen $x^3 = 1, y^3 = 1$ und $(xy)^3 = 1$ für die Erzeugenden $x$ und $y$ gelten. (Für Gruppen können Gleichungen immer

auf die Form $w = 1$ umgeformt werden.) Geht man von abelschen oder einer anderen Varietät von Gruppen aus, so setzt man zusätzlich noch diese Gesetze voraus. Es sei $\Gamma(\mathfrak{Grp})$ die Menge der Gesetze der Varietät der Gruppen, dann ist

$$G = W(\{x, y\}) / \left\langle \Gamma(\mathfrak{Grp}) \cup \left\{ \left(x^3, 1\right), \left(y^3, 1\right), \left((xy)^3, 1\right) \right\} \right\rangle$$

Das ist aber nach 1.1.34 und den darauf folgenden Anmerkungen

$$G = F(\{x, y\}) / \left\langle \left\{ \left(x^3, 1\right), \left(y^3, 1\right), \left((xy)^3, 1\right) \right\} \right\rangle$$

Diese Darstellung ist nicht eindeutig, denn die obige Gruppe wird z.B. auch durch $G = \langle \{a, b, c\}; \{a^3, b^3, c^3, abc\} \rangle$ repräsentiert. Wieder stellt sich hier ein *Wortproblem* ! Repäsentieren zwei Darstellungen die selbe Gruppe, allgemeiner Algebra? Oder elementarer noch die Frage, wann stehen zwei Wörter aus $W(M)$ in Relation zueinande, sind also in der Quotientenalgebra gleich?

Für Gruppen kann man zeigen, daß dieses Problem insofern unentscheidbar ist, daß es keinen allgemeinen Algorithmus gibt, der nach endlich vielen Schritten zu einer Entscheidung führt. Dennoch bewährt sich diese Darstellungsweise in vielen Fällen.

## 1.2 Polynome

Wir kommen nun zu den Hauptobjekten dieser Arbeit: den Polynomen. Die Polynome über einer Algebra $A$ einer Varietät $\mathfrak{V}$ sollen insbesondere auch eine Algebra aus $\mathfrak{V}$ bilden, d.h. die Gesetze der Varietät erfüllen. Die Algebra $A$ soll Teilalgebra dieser Polynomalgebra sein. Dies erfüllt die folgende Konstruktion:

Sei A eine Algebra aus der Varietät $\mathfrak{V}$ mit den Gesetzen $\Gamma$. Sei $X = \{x_i\}_{i \in I}$ eine Menge von Unbestimmten, also disjunkt zu A. Wir bilden nun die Wortalgebra $W(A \cup X)$ und definieren darauf eine ähnliche Kongruenz wie in 1.1.62. Sei also $P \subseteq W(A \cup X) \times W(A \cup X)$ bestehend aus den folgenden Elementen:

1. $(w, w)$ wo $w \in W(A \cup X)$ (Die diagonalen Elemente sind enthalten).
2. $(w_1(u_1, \ldots, u_k), w_2(u_1, \ldots, u_k))$ wo $(w_1(y_1, \ldots, y_k), w_2(y_1, \ldots, y_k)) \in \Gamma$ und $u_i \in W(A \cup X)$
3. $\left(a, \omega(a_1, \ldots, a_{Ar(\omega)})\right)$ und $\left(\omega(a_1, \ldots, a_{Ar(\omega)}), a\right)$ für $Ar(\omega) > 0, a \in A$, $a_i \in A$ mit $\omega(a_1, \ldots, a_{Ar(\omega)}) = a$

4. $(a, \omega)$ und $(\omega, a)$ für $Ar(\omega) = 0, a \in A$ mit $\omega = a$

Wir definieren eine Relation $R$ nun wieder durch eine Kette: $w \sim_R w' :\Longleftrightarrow$ $\exists$ endliche Kette von $w$ nach $w'$ in $P$. Man kann wie in 1.1.62 zeigen, daß das wiederum eine Kongruenz ist.

Also können wir $A[X, \mathfrak{V}] := W(A \cup X)/R$ bilden. Angenommen: $a \sim_R a'$, dann sehen wir aus der Definition von $P$, daß eine Kette von $a$ nach $a'$ in eine Kette von Gleichungen übergeht, also $a = a'$. Also können wir A in $A[X, \mathfrak{V}]$ einbetten mittels $a \mapsto a$.

Wann sind jedoch Elemente aus $A \cup X$ kongruent? Angenommen: $x_i \sim_R x_j$ und sei $i \neq j$, dann existiert also eine Kette von $x_i$ nach $x_j$:

$$x_i, w_1, w_2, \ldots, w_n, x_j$$

Setzen wir in dieser Kette statt $x_i$ $a$ und für $x_j$ $a'$, sowie für etwaige sonstig vorkommende weitere Unbestimmte beliebige Elemente aus A, so erhalten wir eine Kette von $a$ nach $a'$, also wieder $a = a'$. Also gilt $|A| = 1$. Die selbe Argumentation zeigt, daß aus $a \sim_R x_i$ folgt, daß $|A| = 1$.

Sei nun $B$ eine Algebra derselben Varietät, die die einelementige Algebra $A = \{a\}$ als echte Unteralgebra hat. Es gibt also ein $b \in B, b \neq a$. In der obigen Kette ersetzen wir nun wiederum $x_i$ durch $a$, $x_j$ durch $b$ sowie andere Unbestimmte durch beliebige Elemente aus B. Also gilt entgegengesetzt der Annahme $b = a$. Also gibt es so ein $B$ nicht. In jedes $B$ mit einer einelementigen Teilalgebra können wir aber dieses $A$ einbetten, somit kann kein $B \in \mathfrak{V}$ mit $|B| > 1$ eine einelementige Unteralgebra besitzen, also ist $\mathfrak{V}$ halb entartet.

Ist also $|A| \neq 1$ oder $\mathfrak{V}$ nicht halb entartet, so ist $X \to A[X, \mathfrak{V}]$ injektiv. Wir identifizieren $a$ mit $C(a)$ und $x_i$ mit $C(x_i)$. Da $W(A \cup X)$ von $A$ und $X$ erzeugt wird, gilt das auch für $A[X, \mathfrak{V}]$.

$A[X, \mathfrak{V}]$ ist in $\mathfrak{V}$, denn angenommen $(w_1(y_1, \ldots, y_k), w_2(y_1, \ldots, y_k)) \in \Gamma$, dann ist $w_1(v_1, \ldots, v_k) \sim_R w_2(v_1, \ldots, v_k)$ $\forall v_i \in W(A \cup X)$. Also gilt

$$C(w_1(v_1, \ldots, v_k) = C(w_2(v_1, \ldots, v_k))$$

Da $R$ aber eine Kongruenz ist, gilt:

$$w_1(C(v_1), \ldots, C(v_k)) = w_2(C(v_1), \ldots, C(v_k))$$

**Definition 1.2.1** *Wir nennen $A[X, \mathfrak{V}]$ die* **Polynomalgebra** *über $A$ in $X$, die Elemente daraus* **Polynome**.

**Satz 1.2.2** *Sei $A$ eine Algebra der Varietät $\mathfrak{V}$. Dann liegt die Polynomalgebra $A[X, \mathfrak{V}]$ auch in $\mathfrak{V}$ und es gilt $A \prec A[X, \mathfrak{V}]$. $A[X, \mathfrak{V}] = \langle A \cup X \rangle$.*

*Ist* $|A| = 1$ *und ist* $\mathfrak{V}$ *halb entartet, so ist* $|A[X, \mathfrak{V}]| = 1$, *d.h. alle Elemente fallen zusammen. In jedem anderen Fall sind alle Elemente aus* $A \cup X$ *unterschiedlich.*

Die Elemente aus $A[X, \mathfrak{V}]$, die Polynome, sind Klassen von äquivalenten Wörtern (und nicht etwa Funktionen).

**Beispiel:** Betrachten wir einen kommutativen Ring $R$ mit Eins, d.h. eine Algebra vom Typ $(2, 1, 0, 2, 0)$. Was ist in diesem Fall $R[x]$?

Die Wörter $w$ in $A \cup \{x\}$ mit gegebenen $r(w)$ sind endliche Produkte, endliche Summen bzw. endliche Subtraktionen von Wörtern mit kleineren Rängen.

Sei $R$ die Kongruenz aus obigem Beweis, dann gilt für jedes Produkt der Form

$$a_0 x_1^l a_1 \ldots a_{n-1} x^{l_n} a_n \sim_R (a_0 \cdot \ldots a_n) x^{l_1 + \ldots + l_n} \sim_R a x^l$$

Für die Summe solcher Wörter gilt, wenn der Exponent der Unbestimmten gleich ist:

$$a x^l + b x^l \sim_R (a + b) x^l \sim_R c x^l$$

Durch Induktion nach dem Rang eines Wortes kann man somit zeigen, daß die Polynome über einem kommutativen Ring mit Eins die Form

$$p = a_0 + a_1 \cdot x + a_2 \cdot x^2 \ldots + a_{n-1} \cdot x^{n-1} + a_n \cdot x^n$$

haben.

Das entspricht dem Polynombegriff, den man aus der Analysis und klassischen Algebra kennt. Das größte $n$, für das $a_n \neq 0$ nennt man den *Grad* des Polynoms für $p \neq 0$.

Mit ähnlichen Überlegungen (siehe 3.1.1 ) kann man sich klar machen, daß Polynome über Gruppen $G$ die Form

$$p = a_0 \cdot x^{l_1} \cdot a_1 \ldots \cdot a_{n-1} x^{l_n} a_n, a_i \in G, l_i \in \mathbb{Z} \forall i = 1, \ldots, n$$

haben. Wir nennen die Summe aller $l_i$ die *Länge* des Polynoms, $l(p) = \sum_{i=1}^{n} l_i$, siehe 3.2.2

**Lemma 1.2.3** *Es sei* $A$ *eine Algebra der Varietät* $\mathfrak{V}$. *Ist* $A' \preceq A$, *so ist* $A'[X, \mathfrak{V}] \preceq A[X, \mathfrak{V}]$

**Beweis:** Da $A' \subseteq A$ ist $W(A' \cup X) \subseteq W(A \cup X)$. Für die (oben definierten) Relationen $R'$ und $R$ mit $A'[X, \mathfrak{V}] = W(A' \cup X)/R'$ und $A[X, \mathfrak{V}] = W(A \cup X)/R$ gilt $R' = R \cap (W(A' \cup X) \times W(A' \cup X))$. Daher ist aber

$$A'[X, \mathfrak{V}] = W(A' \cup X)/R' = W(A' \cup X)/R \subseteq W(A \cup X)/R = A[X, \mathfrak{V}] \ \square$$

**Proposition 1.2.4** *Es sei $A$ eine Algebra der Varietät $\mathfrak{V}$, $X$ eine Menge von Unbestimmten. Die Polynomalgebra über $A$ in $X$ ist die freie Vereinigung von $A$ mit $F(X, \mathfrak{V})$.*

$$A[X, \mathfrak{V}] = A \cup_{\varphi_i} F(X, \mathfrak{V})$$

**Beweis:** $\varphi_1 : A \to A[X, \mathfrak{V}]$, $\varphi_1(a) = a$ ist nach (1.2.2) ein Monomorphismus. Die Abbildung $f : X \to A[X, \mathfrak{V}]$ mit $x_i \mapsto x_i$ kann zu einem Homomorphismus $\varphi_2 : F(X, \mathfrak{V}) \to A[X, \mathfrak{V}]$ erweitert werden, da $F(X, \mathfrak{V})$ frei über X ist. (Ist $\mathfrak{V}$ entartet, so gilt das auch noch, denn $\varphi_2$ ist dann die einzige Abbildung, die es von der einelementigen Algebra $F(X, \mathfrak{V})$ in die einelementige Algebra $A[X, \mathfrak{V}]$ gibt!)

Seien nun also $\psi_1 : A \to B$ und $\psi_2 : F(X, \mathfrak{V}) \to B$ Homomorphismen, wobei $B \in \mathfrak{V}$, dann definieren wir:

$$\rho(C(w(a_i; x_j))) = C(w(\psi_1(a_i); \psi_2(x_j)))$$

Tatsächlich sieht man, daß die Definition ja so sein muß, um unsere Bedingungen aus 1.1.39 zu erfüllen. Da $A[X, \mathfrak{V}] = \langle A \cup X \rangle$, ist $\rho$ auf ganz $A[X, \mathfrak{V}]$ definiert. Zu zeigen bleibt, daß $\rho$ wohldefiniert ist.

Sei also $C(w_1(a_i; x_j)) = C(w_2(a_i; x_j))$ in $A[X, \mathfrak{V}]$, also $w_1(a_i; x_j) \sim_R w_2(a_i; x_j)$. Es gibt dann eine Kette von $w_1(a_i; x_j)$ nach $w_2(a_i; x_j)$. Ersetzen wir darin die $a_i$ durch $\psi_1(a_i)$ sowie die $x_j$ durch $\psi_2(x_j)$ so erhalten wir eine Kette von $\rho(w_1)$ nach $\rho(w_2)$, da $B \in \mathfrak{V}$, somit Punkt (2) in der Definition von P erfüllt bleibt, und $\psi_1$ ein Homomorphismus ist und somit Punkt (3) weiterhin gilt. $\square$

Wir wissen bereits, daß $A \to A[X, \mathfrak{V}]$ ein Monomorphismus ist. Weiters ist $A[X, \mathfrak{V}] = \langle A \cup X \rangle$, damit ist $A[X, \mathfrak{V}]$ genau dann direktes Produkt, wenn $\varphi_2$ injektiv ist. Das ist nicht immer der Fall, denn angenommen $\mathfrak{V}$ ist eine halb entartete, nicht vollständig entartete Varietät, z.B. jene der Ringe mit Einheit, dann ist $|F(X, \mathfrak{V})| > 1$, aber wenn $|A| = 1$ ist nach oben $|A[X, \mathfrak{V}]| = 1$.

Was ist, wenn verschiedene Gesetzesmengen die selbe Varietät bestimmen. Wie hängt die Polynomalgebra davon ab? Es gilt:

**Proposition 1.2.5** *Die Polynomalgebra $A[X, \mathfrak{V}]$ ist unabhängig von der Menge $\Gamma$, die $\mathfrak{V}(\Gamma)$ bestimmt.*

**Beweis:** [18] Kapitel 1, Korollar 4.32

D.h. ist $\mathfrak{V}(\Gamma) = \mathfrak{V}(\Gamma')$ so ist $A[X, \mathfrak{V}(\Gamma)] = A[X, \mathfrak{V}(\Gamma')]$ .

$A[X, \mathfrak{V}]$ ist eine Erweiterung von A, die bezüglich anderen Erweiterungen eine interessante Eigenschaft hat:

**Proposition 1.2.6** *Es sei $A$ eine Algebra der Varietät $\mathfrak{V}$. Sei $A(U)$ eine Erweiterung von $A$ und $X = \{x_u \,|u \in U\}$ mit $x_u \neq x_v$, wenn $u \neq v$. Dann gibt es einen Epimorphismus $\rho : A[X, \mathfrak{V}] \to A(U)$ mit $\rho(a) = a$ und $\rho(x_u) = u$.*

**Beweis:** [18] Kapitel 1, Lemma 4.43.

**Lemma 1.2.7** *Es sei $A$ eine Algebra der Varietät $\mathfrak{V}$. Sei $R$ jene Kongruenz, sodaß $A[X, \mathfrak{V}] = W(A \cup X)/R$ und bezeichne $C(.)$ die Konrguenzklasse bezüglich $R$. Seien $w(a_i; x_j)$ und $w'(a_i; x_j)$ Wörter in $A$ und $X$. Dann gilt:*

$$C(w(a_i; x_j)) = C(w'(a_i; x_j)) \Longleftrightarrow \forall B \succeq A : \forall b_j \in B : w(a_i; b_j) = w'(a_i; b_j)$$

**Beweis:** [1] Satz 1.82

**Satz 1.2.8** *Sei $A \in \mathfrak{V}$ und $\vartheta \in Hom(A, B)$. Dann gibt es eine eindeutige Erweiterung von $\vartheta$ zu einem Homomorphismus $\rho : A[X, \mathfrak{V}] \to B[X, \mathfrak{V}]$ mit $\rho(x_i) = x_i$. Ist $\vartheta$ ein Epimorphismus resp. ein Isomorphismus, so ist das auch $\rho$.*

**Beweis:** $B \preceq B[X, \mathfrak{V}]$, $B[X, \mathfrak{V}] \in \mathfrak{V}$, daher ist $\psi_1 : A \to B[X, \mathfrak{V}]$ mit $\psi_1 = \iota \circ \varphi$ ($\iota$ die Einbettung) ein Homomorphismus. Sei $\psi_2$ die eindeutige Erweiterung der Abbildung $x_i \mapsto x_i$ von X nach $B[X, \mathfrak{V}]$ zu einem Homomorphismus $F(X, \mathfrak{V})$ nach $B[X, \mathfrak{V}]$. Da $A[X, \mathfrak{V}] = A \cup_{\varphi_i} F(X, \mathfrak{V})$ gibt es einen Homomorphismus $\rho : A(X, \mathfrak{V}) \to B(X, \mathfrak{V})$, sodaß $\psi_i = \rho \circ \varphi_i$, also ist $\rho(a) = \vartheta(a)$ und $\rho(x_i) = x_i$. Da $A[X, \mathfrak{V}] = \langle A \cup X \rangle$ ist $\rho$ nach 1.1.56 eindeutig.

Ist $\vartheta$ surjektiv, so ist das $\rho$ auch, da $B[X, \mathfrak{V}] = \langle B \cup X \rangle$ und $B$ und $X$ im Bild von $\rho$ liegen.

Ist $\vartheta$ ein Isomorphismus, so ist $\vartheta^{-1}$ ein Epimorphismus, also gibt es einen Epimorphismus $\sigma : B(X, \mathfrak{V}) \to A(X, \mathfrak{V})$. Also sind $\rho \circ \sigma$ und $\sigma \circ \rho$ wegen der Eindeutigkeit die Identitätsabbildungen, also ist $\rho$ bijektiv. □

**Definition 1.2.9** *Den eindeutigen Homomorphismus $\rho$ aus Satz 1.2.8 bezeichnen wir mit $\vartheta[X]$, die kanonische Erweiterung.*

Für Monomorphismen ist die kanonische Erweiterung i.A. nicht mehr injektiv. So kann z.B. in der Varietät der nilpotenten Gruppen der Klasse $\leq 2$ (siehe 3.5.2 und A.8.4) ein Gegenbeispiel konstruiert werden, siehe [18] §4, *Remarks and comments* zu Kapitel1.

Aber in der Varietät der Gruppen (ebenso wie in jener der kommutativen Ringen mit Eins) gilt, daß die kanonische Erweiterung eines Monomorphismus injektiv ist, siehe 3.1.12.

Eine weitere interessante Eigenschaft ist, daß man die Polynomalgebra auch „stufenweise“ bilden kann, was bei manchen Beweisen Induktion zuläßt:

**Proposition 1.2.10** *Es seien $X_1, X_2, \ldots, X_n$ paarweise disjunkte Mengen von Unbestimmten und sei $X = \bigcup_{i=1}^{n} X_i$. Dann gibt es einen Isomorphismus $\psi : A(X, \mathfrak{V}) \to (\ldots((A(X_1, \mathfrak{V}))\,(X_2, \mathfrak{V}))\ldots)\,(X_n, \mathfrak{V})$, der jedes Element aus $A \cup X$ auf sich selbst abbildet.*

**Beweis:** [18] Kapitel 1, Korollar 4.61

Sei nun $X = \{x_1, \ldots, x_k\}$ eine Menge von Unbestimmten und sei $p \in A[X, \mathfrak{V}]$. Sei $B$ eine $\mathfrak{V}$-Erweiterung von $A$ und $(b_1, \ldots, b_k) \in B^k$. Sei $\varphi_1 : A \to B$ mit $\varphi_1(a) = a$ und $\varphi_2 : F(X, \mathfrak{V}) \to B$, die kanonische Erweiterung von $x_i \mapsto b_i$. Dann können wir nun jedem $p$ für dieses feste $\mathfrak{b} = (b_1, \ldots, b_k)$ ein $p(\mathfrak{b}) \in B$ zuordnen. Ist $p = w(a_i; x_j)$ eine Repräsentation von p, dann sieht man leicht, daß $p(\mathfrak{b}) = w(a_i; b_j)$. Durch die Definition und die Eigenschaft der freien Vereinigung ist das wohldefiniert. Betrachten wir nun $\mathfrak{b}$ als variabel, so können wir jedem $p \in A[X, \mathfrak{V}]$ ein $\sigma_k(p) \in F_k(B)$ zuordnen. Man kann zeigen:

**Proposition 1.2.11** ( Substitutionsprinzip ) *Die Abbildung*

$$p \mapsto p(\mathfrak{b}) \text{ mit } w(a_i; x_j) \mapsto w(a_i; b_j)$$

*ist wohldefiniert. Die Abbildung $\sigma_k : A[X, \mathfrak{V}] \to F_k(B)$ mit*

$$(\sigma_k(p))\,(\mathfrak{b}) = p(\mathfrak{b})$$

*ist ein Homomorphismus.*

**Beweis:** [18] Kapitel 1, Proposition 6.41.

### 1.2.1 Das Wortproblem

Welche Wörter induzieren nun die selben Polynome? Wann sind zwei Polynome gleich? Wir haben die Polynomalgebra als Quotient der Wortalgebra $W(A \cup X)$ gebildet, sodaß es im allgemeinen für ein Polynom verschiedene Wörter gibt, die dieses Polynom repräsentieren. So sind zum Beispiel $x \cdot (x \cdot x)$ und $(x \cdot x) \cdot x$ verschiedene Repräsentanten des Polynom $x^3$, wenn wir etwa die Varietät der Gruppen betrachten. Dieses Problem werden wir im nächsten Abschnitt 1.2.2 genauer betrachten. Man könnte es als *„erstes Wortproblem“* bezeichnen.

Wir können uns aber auch einem anderen Problem stellen: Wir haben in 1.2.11 gesehen, daß ein Polynom eine eindeutig bestimmte Funktion festlegt. Wann sind zwei solche Funktionen gleich? Wann repäsentieren zwei Wörter die selbe Funktion? Klarerweise gilt daß zwei Wörter, die das selbe Polynom repräsentieren, auch dieselbe Funktion induzieren. So gelangen wir zum *zweiten Wortproblem*: Wann repräsentieren zwei Polynome dieselbe Funktion? D.h. wann sind zwei Polynome im Kern $ker(\sigma_k)$, wobei $\sigma_k : A[X, \mathfrak{V}] \to F_k(A)$ die Abbildung aus 1.2.11 ist? Die Untersuchung dieser Abbildung wird ein zentraler Punkt dieser Arbeit bleiben.

**Beispiel:** Betrachten wir den Ring $\mathbb{Z}_3$, dort induzieren u.a. folgenden Wortpaare die selben Funktionen:

1. $(x_1 + 1) \cdot x_1$ und $x_1^2 + x_1$
2. $x_1 \cdot x_2$ und $x_2 x_1$
3. $1 \cdot x_1 + 2 \cdot x_1$ und $0$
4. $x \cdot (x + 1) \cdot (x + 2)$ und $0$

Wir sehen verschiedene Arten von Gleichheiten,

1. erklärt sich aus den Gesetzen der Varietät der Ringe mit Eins. Die beiden Wörter sind Elemente aus $W(X)$ und sind bereits in $F(X)$ gleich.
2. entspricht einer Gleichung. Diese Gleichung (Kommutitivität) gilt natürlich nicht in allen Algebren dieser Varietät (Ringe). Man kann jedoch die Klasse aller Algebren dieser Varietät betrachten, in der diese Gleichung Gesetz ist und erhält eine Varietät. Im diesem Falle die Klasse der kommutativen Ringe mit Eins.

3. ist eine Identität, die auch in jedem Ring gilt, der diesen Ring als Unterring enthält. In diesem Fall repräsentieren die beiden Wörter dasselbe Polynom, denn im Polynomring gilt $1 \cdot x_1 + 2 \cdot x_1 = (1+2) \cdot x_1 = 0$.

4. ist eine sehr spezifische Identität, die stark von der inneren Struktur des zugrundeliegenden Rings abhängt! Dieses Problem tritt z.B. im Abschnitt über Vollständigkeiten auf (1.4.4). Im Kapitel über Gruppen werden wir uns die Frage stellen, wie sich spezielle Eigenschaften der Gruppe $G$ auf die Polynome oder die von Polynomen induzierte Funktionen auswirken.

### 1.2.2 Normalformen

Wie können wir das „erste Wortproblem“ lösen? Was würden wir als „gute“ Lösung ansehen?

Die Menge der Polynome $A[X, \mathfrak{V}]$ wird aus der Menge der Wörter $W(A \cup X)$ durch eine Kongruenz gefunden. Finden wir also eine (bezüglich dieser Kongruenz) repräsentative Menge (siehe Definition 1.1.20, wissen wir mehr über die Polynome.

Wir wollen noch mehr fordern, für die gesuchte Menge soll es noch einen endlichen Algorithmus geben, um von einer gegebenen Repräsentation auf diese ausgezeichnete zu kommen. Dann kann man bei zwei gegebenen Wörtern den Algorithmus anwenden, kommt man auf dasselbe Ergebnis, so repräsentieren sie daselbe Polynom, anderenfalls nicht.

**Definition 1.2.12** *Eine Teilmenge $N \subseteq W(A \cup X)$ heißt* **Normalformsystem** *für die Polynome $A[X, \mathfrak{V}]$, wenn es die Polynome vollständig und eindeutig beschreibt, d.h. für die Kongruenz aus 1.2.2 repräsentativ ist, und man für jede Repräsentation eines Polynoms in endlichen Schritten eine aus $N$ finden kann. Wir bezeichnen ein Normalformsystem für $A[X]$ symbolisch mit $N(A, X)$.*

Eine alternative Formulierung, die klarerweise äquivalent ist:

**Korollar 1.2.13** *Eine Teilmenge $N \subseteq W(A \cup X)$ ist genau dann Normalformsystem für $A[X, \mathfrak{V}]$, wenn*

1. *Für jede Repräsentation $p = w(a_i; x_j)$ eines Elements $p \in A[X, \mathfrak{V}]$ als Element von $W(A \cup X)$ kann man in endlichen Schritten ein Element aus $N$ finden, das $p$ repräsentiert.*

2. *Je zwei verschiedene Wörter in N repräsentieren zwei verschiedene Polynome.*

**Bemerkung:** Solch einen Algorithmus von einem Wort auf das äquivalente Normalformwort zu kommen, nennt man auch „Umschreibalgorithmus". Bei diesem Algorithmus ist (wie bei jedem Algorithmus) wichtig, daß er terminiert, i.e. daß er abbricht. Es muß also eine Beurteilung geben, ob ein äquivalentes Wort „einfacher" ist oder nicht, d.h. „näher" bei unserem Normalformsystem ist. Das kann man zum Beispiel erreichen, indem man jedem Wort einen geeigneten Zahlenwert zuordnet, sodaß den Wörtern des Normalformsystems minimale Zahlen zugeordnet sind.

Eine Methode für ein Umschreibsystem für Gruppen liefert die sogenannte Knuth-Bendix Methode. (siehe z.B. [1]).

**Beispiel:**

- Wie schon angemerkt, kann gezeigt werden, daß in *Ringen mit Eins*, $\Omega = \{+, -, 0, \cdot, 1\}$, Polynome in $X = \{x\}$ durch ein Wort der Form

  $$a_0 + a_1 \cdot x + a_2 \cdot x^2 + \ldots + a_n x^n \text{ oder } 0$$

  dargestellt werden können. Diese Darstellung ist eindeutig, wenn man fordert, daß $a_n \neq 0$ ist (und klarerweise $n \geq 0$ und $a_i$ im Ring). Man kann einen Algorithmus angeben (siehe [18] Kapitel 1, Satz 8.11), in endlichen Schritten aus irgendeiner Darstellung eines Polynoms als Wort auf so eine Darstellung zu kommen. Also liegt ein Normalformsystem vor.

- Über *Gruppen*, $\Omega = \{\cdot, ^{-1}, 1\}$, kann jedes Polynom in $X = \{x\}$ in der Form

  $$a_0 \cdot x^{n_1} \cdot a_1 \cdot x^{n_2} \cdot a_2 \ldots a_{r-1} \cdot x^{n_r} \cdot a_r$$

  dargestellt werden. Auch hier kann man zeigen (siehe 3.1.4), daß ein Normalformsystem vorliegt, wenn man fordert $a_t \neq 1$ für $t = 1, 2, ..., r-1$ (und natürlich $r \in \mathbb{N}$, $n_i \in \mathbb{Z}, n_i \neq 0$ und $a_t \in G$ für $t = 0, 1, ..., r$).

Ein angenehme Eigenschaft der Normalformsysteme ist die folgende:

**Korollar 1.2.14** *Seien A,B Algebren der Varietät $\mathfrak{V}$. Sei $N(A, X) \subseteq W(A \cup X)$ Normalformsystem für $A[X, \mathfrak{V}]$. Gilt $\forall\, \eta \in Mon(A, B)$, daß mit $w(a_i; x_j)$ auch $w(\eta(a_i); x_j)$ Element aus $N(A, X)$ sind, so ist der kanonische Homomorphismus $\eta[X]$ ein Monomorphismus.*

**Beweis:** Durch die Voraussetzungen folgt aus $\eta[X]p = \eta[X]q$ für $p = w(a_i; x_j)$ und $q = w(b_i; x_j)$, daß $w(\eta(a_i); x_j) = w(\eta(b_i); x_j)$. Das sind jedoch Elemente des Normalformsystems, stellen also nicht nur dasselbe Polynom dar, sondern sind auch als Wörter gleich. Somit ist $\eta(a_i) = \eta(b_i)$, also $a_i = b_i$ □

Dieses Korollar kann leicht selbständig formuliert und gezeigt werden. Es kann aber auch als Folgerung einer anderen Aussage gesehen werden. Dazu benötigen wir zuerst die folgende Eigenschaft.

**Lemma 1.2.15** *Es sei $B$ eine Algebra der Varietät $\mathfrak{V}$, für jedes $A \preceq B$ sei $\iota_A : A \to B$ die Einbettung. Die Abbildung $\iota_A[X]$ ist Für jedes $A \preceq B$ genau dann eine Einbettung, wenn für jeden Monomorphismus $\vartheta : C \to B$ die Abbildung $\vartheta[X]$ ein Monomorphismus ist für alle $C$ Algebra aus $\mathfrak{V}$.*

**Beweis:** $\Longleftarrow$ ist klar

$\Longrightarrow$ Es sei $\vartheta : C \to B$ ein Monomorphismus, also ist $\vartheta : C \to \vartheta(C)$ ein Isomorphismus. Somit ist $\vartheta[X, \vartheta(C)] : C[X, \mathfrak{V}] \to \vartheta(C)[X]$ auch ein Isomorphismus. Da $\vartheta(C) \preceq B$ ist, ist nach Voraussetzung $\iota_{\vartheta(C)}[X] : \vartheta(C) \to B[X]$ ein Monomorphismus, also ist $\vartheta[X, B] = \iota_{\vartheta(C)}[X] \circ \vartheta[X, \vartheta(c)]$ ein Monomorphismus. □

**Definition 1.2.16** *Eine Varietät $\mathfrak{V}$ hat* **mit Unteralgebren kompatible Normalformsysteme**, *wenn es $\forall A \in \mathfrak{V}$ ein Normalformsystem $N(A, X)$ für $A[X, \mathfrak{V}]$ gibt, sodaß für alle $B$ mit $A \preceq B$ gilt $N(A, X) \subseteq N(B, X)$.*

Die Eigenschaft, daß es einen für das Normalformsystem terminierenden Algorithmus gibt, ist für diese Eigenschaft, insbesondere für den nächsten Satz nicht wichtig.

**Proposition 1.2.17** *Hat die Varietät $\mathfrak{V}$ ein Normalformsystem, das kompatibel mit Unteralgebren ist, so ist $\forall A \preceq B \in \mathfrak{V}$ mit $A \preceq B$ $\iota[X] : A[X, \mathfrak{V}] \to B[X, \mathfrak{V}]$ injektiv.*

**Beweis:** Das folgt direkt aus der Definition und 1.2.14 □

Mit dem vorherigen Lemma folgt also, daß in Varietäten $\mathfrak{V}$, die mit Unteralgebren kompatible Normalformsysteme haben, für jeden Monomorphismus $\vartheta : A \to B$ für $A, B \in \mathfrak{V}$ folgt, daß $\vartheta[X]$ ein Monomorphismus ist.

Nicht nur die Varietät der Gruppen und der abelschen Gruppen (siehe Kapitel3.1.1), sowie die Halbgruppen, Halbgruppen mit Eins, kommutative

Halbgruppen, kommutative Halbgruppen mit Eins (siehe Kapitel 3.4.1) haben diese Eigenschaft, auch für die kommutativen Ringe, die kommutativen Ringe mit Eins, die Verbände, die distributiven Verbände, die distributiven Verbände mit 0 und 1 sowie die Boolschen Algebren kann man solche Normalformsysteme finden.

**Bemerkung:** Ein weitere Eigenschaft einer Varietät ist die sogenannte *Amalgamierungs Eigenschaft*, die auch eine hinreichende Bedingung für die Injektivität von $\iota[X]$ liefert (siehe [7] Satz 1). Eine Varietät besitzt diese Eigenschaft, wenn es für alle Erweiterungen $B, C$ einer beliebigen Algebra $A \in \mathfrak{V}$ eine Erweiterung $D$ gibt, sodaß es Isomorphismen $\psi_1 : B \to D$ und $\psi_2 : C \to D$ gibt, die beide $A$ fest lassen, $\psi_i(a) = a$.

## 1.3 Funktionen und Polynomfunktionen

In diesem Abschnitt sei $A$ immer als $\Omega$-Algebra der Varietät $\mathfrak{V}$ angenommen.

Auf der Menge der $k$-wertigen Funktionen von $A$, $F_k(A)$, definieren wir für $f_i \in F_k(A)$ die Operationen $\omega_i$:
Für $Ar(\omega_i) > 0$ :

$$\left(\omega_i^{F_k(A)}\left(f_1, f_2, \ldots, f_{Ar(\omega_i)}\right)\right)(a_1, a_2, \ldots, a_k) :=$$

$$\omega_i^A\left(f_1(a_1, a_2, \ldots, a_k), f_2(a_1, a_2, \ldots, a_k), \ldots, f_{Ar(\omega_i)}(a_1, a_2, \ldots, a_k)\right)$$

Für $Ar(\omega_i) = 0$ :

$$\omega_i^{F_k(A)}(a_1, a_2, \ldots, a_k) := \omega_i^A$$

**Definition 1.3.1** *Mit $F_k(A)$ bezeichnen wir die* **volle k-stellige Funktionenalgebra**, *die Algebra alle $k$-stelligen Funktionen von $A$. $F_k(A) = \{f : A^k \to A\}$.*

Wir sehen, daß $F_k(A) \simeq \prod_{\nu \in A^k} A$, also folgt aus 1.1.61, daß $F_k(A) \in \mathfrak{V}$ ist. Also gilt:

**Lemma 1.3.2** *Sei $A$ eine $\Omega$-Algebra aus der Varietät $\mathfrak{V}$. Dann ist $F_k(A)$ eine $\Omega$-Algebra aus $\mathfrak{V}$.*

Wir können $A$ in $F_k(A)$ einbetten mittels $a \mapsto a$. Diese Zuordnung ist klarerweise injektiv und nach Definition der Operationen klarerweise ein Homomorphismus, d.h. tatsächlich eine Einbettung.

**Definition 1.3.3** *Die Bilder der Einbettung von $A$ in $F_k(A)$ nennen wir die* **konstanten Funktionen**.

Weitere ausgezeichnete Funktionen sind die Projektionen (nach 1.1.17): $\xi_i : A^k \to A$, mit $\xi_i(a_1, \ldots, a_k) = a_i$

Betrachten wir nun die durch diese beiden Arten von speziellen Funktionen bestimmte Untermenge von $F_k(A)$.

**Definition 1.3.4** *Wir bezeichnen mit $P_k(A) = \langle A \cup \{\xi_i, i = 1, \ldots, k\}\rangle_{F_k(A)}$ die Menge der* **Polynomfunktionen** .

Da $P_k(A) \preceq F_k(A)$ gilt klarerweise:

**Lemma 1.3.5** *$P_k(A)$ ist eine Algebra aus $\mathfrak{V}$. $A \preceq P_k(A)$.*

Betrachten wir die Termfunktionen, so folgt aus der Definition direkt

**Lemma 1.3.6** *Für die Menge$T_k(A)$ der Termfunktionen gilt:*

$$T_k(A) = \langle \{\xi_i, i = 1, \ldots, k\}\rangle_{F_k(A)} \preceq P_k(A)$$

Die Termfunktionen werden oft auch als *„Grätzerpolynomfunktionen “* bezeichnet.

**Lemma 1.3.7** *$A$ ist endlich $\Longleftrightarrow$ $P_k(A)$ ist endlich.*

**Beweis:** $A \preceq P_k(A)$, also ist $A$ endlich, wenn es nur $P_k(A)$ ist. Da $A$ endlich ist, ist auch $F_k(A)$ endlich und somit auch $P_k(A)$. □

Sei $X = \{x_1 \ldots, x_k\}$. Wir wissen, daß $A[X, \mathfrak{V}]$ freie Vereinigung von $A \cup X$ ist, damit ist mit $a \mapsto a$ und $x_i \mapsto \xi_i$ ein Homomorphismus von $A[X, \mathfrak{V}]$ nach $P_k(A)$ definiert. Aus $P_k(A) = \langle A \cup \{\xi_i\}\rangle$ und der Definition der Operationen auf $A\,[X, \mathfrak{V}]$ und $P_k(A)$ folgt, daß diese ein Epimorphismus ist. Dies entspricht genau unserem in 1.2.11 konstruierten Homomorphismus.

**Definition 1.3.8** *$\sigma_k : A[X, \mathfrak{V}] \to P_k(A)$ und $\sigma_k : F(X) \to T_k(A)$ nennen wir die kanonischen Epimorphismen.*

Wir können zeigen, daß jede Polynomfunktion für alle Kongruenzen kompatibel ist, d.h. wenn für eine Kongruenz $K \in \mathfrak{K}(A)$ gilt, daß $y_i \sim_K y_i'$ für alle $i = 1, \ldots, k$, dann gilt $p(y_1, \ldots, y_k) \sim_K p(y_1', \ldots, y_k')$.

**Satz 1.3.9** *Jedes $p(x_1, x_2, \ldots, x_k) \in P_k(A)$ ist kompatibel.*

**Beweis:** Induktion nach dem Rang $n$ von $p$ als Wort in $W(A \cup \{\xi_1, \xi_2, \ldots, \xi_k\})$. $n = 0$: Sei $\varphi(x_1, x_2, \ldots, x_k) = a$ eine konstante Funktion. $\varphi(a_i) = \varphi(b_i) \forall a_i, b_i \in A$. Also ist $\varphi$ kompatibel. Die Projektionen $\xi_i(x_1, x_2, \ldots, x_k) = x_i$ sind kompatibel, da wenn $\forall j : a_j \sim_K b_j$ gilt, ist $\xi_i(a_1, a_2, \ldots, a_k) = a_i \sim_K b_i = \xi_i(b_1, b_2, \ldots, b_k)$.

Angenommen, die Aussage stimmt für alle $m < n$, dann kann $p$ dargestellt werden als

$$p\left(x_1, \ldots, x_k\right) = \omega\left(w_1\left(x_1 \ldots, x_k\right), w_2\left(x_1, \ldots, x_k\right), \ldots, w_{Ar(\omega)}\left(x_1, \ldots, x_k\right)\right)$$

wobei $r(w_i) < n$. Sei $(a_1, \ldots, a_k) \sim_K (b_1, \ldots, b_k)$. Nach Induktionsvorrausetzung gilt $w_i(a_1, \ldots, a_k) \sim_K w_i(b_1, \ldots, b_k)$. Da $K$ aber eine Kongruenz ist, folgt

$$\omega(w_1\left(a_1, \ldots, a_k\right), w_2\left(a_1, \ldots, a_k\right), \ldots, w_{Ar(\omega)}\left(a_1, \ldots, a_k\right) =$$

$$= \omega(w_1\left(b_1, \ldots, b_k\right), w_2\left(b_1, \ldots, b_k\right), \ldots, w_{Ar(\omega)}\left(b_1, \ldots, b_k\right))$$

□

Wir können auch zeigen, daß die kompatiblen Funktionen eine $\Omega$-Algebra der Varietät $\mathfrak{V}$ bilden:

**Definition 1.3.10** *Sei $A$ eine Algebra der Varietät $\mathfrak{V}$, sei $\mathfrak{M} \subseteq \mathfrak{K}(A)$ eine Menge von Kongruenzen. Dann bezeichnen wir die Menge aller Funktionen von $A^k$ nach $A$, die bezüglich aller Kongruenzen aus $\mathfrak{M}$ kompatibel sind, mit $K_k(A, \mathfrak{M})$, d.h.*

$$K_k(A, \mathfrak{M}) = \{f \in F_k(A) \,|\, f \text{ kompatibel bzgl. } K\ \forall K \in \mathfrak{M}\}$$

*Ist $\mathfrak{M} = \mathfrak{K}(A)$, so bezeichnen wir $K_k(A, \mathfrak{M})$ als $K_k(A)$ die Menge der* **kompatiblen Funktionen** .

$$K_k(A) = \{f \in F_k(A) \,|\, f \text{ kompatibel bzgl. } K\ \forall K \in \mathfrak{K}(A)\}$$

**Proposition 1.3.11** *$\forall \mathfrak{M} \subseteq \mathfrak{K}(A)$ gilt: $K_k(A, \mathfrak{M}) \preceq F_k(A)$.*

**Beweis:** Sei $\omega_i \in \Omega$ mit $Ar(\omega_i) = 0$. Da jede Kongruenz $K$ auch Äquivalenzrelation und somit reflexiv ist, gilt $\omega_i \sim_K \omega_i$, also ist die Abbildung $(x_1, \ldots, x_k) \mapsto \omega_i$ kompatibel, und somit $\omega_i \in K_k(A, \mathfrak{M})$.

Sei $\omega_i \in \Omega$ mit $n = Ar(\omega_i) > 0$ und $K \in \mathfrak{M}$. Seien $a_i \sim_K b_i$ für $i = 1, \ldots, k$ und $f_j$ kompatibel bzgl. $K$ für $j = 1, \ldots, n$ , dann gilt

$$\left(\omega_i\left(f_1, \ldots, f_n\right)\right)\left(a_1, \ldots, a_k\right) = \left(\omega_i\left(f_1\left(a_1, \ldots, a_k\right), \ldots, f_n\left(a_1, \ldots, a_k\right)\right)\right)$$

$$\sim_K$$
$$(\omega_i (f_1 (b_1, \ldots, b_k), \ldots, f_n (b_1, \ldots, b_k)))$$

Das gilt $\forall K \in \mathfrak{M}$, somit ist $\omega_i (f_1, \ldots, f_n) \in K_k(A, \mathfrak{M})$ □

Somit gilt

$$P_k(A) \subseteq K_k(A) \subseteq K_k(A, \mathfrak{M}) \subseteq F_k(A)$$

Hier drängt sich die Frage auf, ob das echte Inklusionen sind? Wann sind diese Menge gleich? Diesen Fragen stellen wir uns im nächsten Kapitel.

## 1.4 Polynomvollständigkeit

Wie ist die Beziehung der Polynomfunktionenalgebra zu der vollen Funktionsalgebra? Können diese beiden Algebren zusammenfallen? Gibt es Funktionen, die keine Polynomfunktionen sind?

**Definition 1.4.1** *Eine Algebra $A$ heißt* **k-polynomvollständig** *, wenn gilt:* $F_k(A) = P_k(A)$.

D.h. jede $k$-stellige Funktion ist bereits eine Polynomfunktion.

**Beispiel:** Betrachte die Gruppe $[\mathbb{Z}_2; +, -, 0]$. Dann ist

$$F_1(\mathbb{Z}_2) = \left\{ \begin{pmatrix} 0 \mapsto 0 \\ 1 \mapsto 0 \end{pmatrix}, \begin{pmatrix} 0 \mapsto 1 \\ 1 \mapsto 1 \end{pmatrix}, \begin{pmatrix} 0 \mapsto 1 \\ 1 \mapsto 0 \end{pmatrix}, \begin{pmatrix} 0 \mapsto 0 \\ 1 \mapsto 1 \end{pmatrix} \right\} =$$
$$= \{x \mapsto 0, x \mapsto 1, x \mapsto x + 1, x \mapsto x\} = P_1(\mathbb{Z}_2)$$

Also ist $\mathbb{Z}_2$ 1-polynomvollständig.

**Bemerkung:** Eine Algebra $A$ mit $|A| = 1$, $A = \{a\}$ ist klarerweise $n$-polynomvollständig ($\forall\, n \in \mathbb{N}$), da $F_k(A) = \{a\}$.

**Proposition 1.4.2** *Ist $A$ k-polynomvollständig, so ist $A$ auch n-polynomvollständig für alle $n \leq k$.*

**Beweis:** [18] Kapitel 1, Proposition 11.11

**Proposition 1.4.3** *Ist $A$ 2-polynomvollständig, dann ist $A$ n-polynomvollständig $\forall n \in \mathbb{N}$.*

**Beweis:** [18] Kapitel 1, Satz 11.2

Also gibt es für eine Algebra $A$ nur die folgende Fälle:

**Definition 1.4.4** *1. A ist n-polynomvollständig $\forall n \in \mathbb{N}$. Dann nennen wir A* **polynomvollständig**.

*2. A ist 1-polynomvollständig, aber nicht n-polynomvollständig für $n > 1$. Dann nennen wir A* **halb polynomvollständig**.

*3. A ist nicht n-polynomvollständig $\forall n \in \mathbb{N}$. Dann nennen wir A* **polynomunvollständig**.

**Proposition 1.4.5** *Ist A n-polynomvollständig, so ist A einfach.*

**Beweis:** Indirekt angenommen, A ist nicht einfach. Dann gibt es eine nicht triviale Kongruenz $K$. Also gibt es eine Kongruenzklasse $C_1$, sodaß $|C_1| > 1$ und $\exists C_2 \neq C_1$. Sei $a, b \in C_1, a \neq b, c \in C_2$. Definiere die Funktion $\psi$ :

$$\psi(x_1, \ldots, x_k) = \begin{cases} (a_1, \ldots, a_k) & (x_1, \ldots, x_k) = (a_1, \ldots, a_k) \\ (c_1, \ldots, c_k) & sonst \end{cases}$$

Damit ist aber $\psi(a, \ldots, a) \not\sim_K \psi(b, \ldots, b)$, aber nach (1.3.9) muß $\forall p \in P_k(A)$ gelten: $p(a, \ldots, a) \sim_K p(b, \ldots, b)$. Also ist $\psi \notin P_k(A)$. □

Mit $\eta : A \to B$ haben wir $\eta^k : A^k \to B^k$ definiert mit $\eta^k (a_1, \ldots, a_k) = (\eta(a_1), \ldots, \eta(a_k))$.

**Proposition 1.4.6** *Jede n-polynomvollständige Algebra mit endlich oder abzählbar vielen Operationen ($|\Omega| \leq \aleph_0$) ist endlich.*

**Beweis:** [18] Kapitel 1, Proposition 11.31

**Bemerkung:** Unteralgebren von $k$-polynomvollständigen Algebren sind im allgemeinen nicht $k$-polynomvollständig sein. So sind die alternierenden Gruppen $\mathbb{A}_k$ für $k \geq 5$ $k$-polynomvollständig, diese haben aber nicht triviale Untergruppen, die für kein $k \in \mathbb{N}$ k-polynomvollständig sind, wie z.B. die $\mathbb{A}_3$, wie wir in 3.1.4 sehen werden.

Ist $A$ nicht n-polynomvollständig, würde man gerne beurteilen, wie weit $A$ von der Vollständigkeit abweicht. Man definiert eine Maßzahl für diese Abweichung, indem man die Kardinalität der kleinsten Menge heranzieht, die mit den Polynomfunktionen die vollen Funktionen erzeugen.

**Definition 1.4.7** *Unter dem k-Polynomvollständigkeitsdefekt von A, symbolisch k-def(A), verstehen wir die kleinste Kardinalzahl einer Menge $D \subseteq F_k(A)$ für die gilt $\langle P_k(A) \cup D \rangle = F_k(A)$.*

Klarerweise ist $A$ dann und nur dann $k$-polynomvollständig, wenn der $k$-Defekt 0 ist.

Der Zusammenhang der Kongruenzen zur Polynomvollständigkeit äußert sich nicht nur darin, daß $k$-polynomvollständige Algebren einfach sind, die Größe der Kongruenzklassen haben einen Einfluß auf den $k$-Defekt:

**Proposition 1.4.8** *Sei* $[A;\Omega]$ *endlich, sei* $K \neq A \times A \in \mathfrak{K}(A)$ *eine Kongruenz auf* $A$*, sei* $m_K = \max_{a \in A}\{|C(a)|\}$ *das Maximum der Anzahl der Elemente in den Kongruenzklassen. Dann gilt*

$$k - def(A) \geq \min_{i \in \mathbb{N}} \left\{ |A/K|^i \geq m_K^k \right\}$$

**Beweis:** [32] Satz

Will man also den $k$-Defekt möglichst gut abschätzen, sollte man nach Kongruenzen suchen, wo es wenige, aber große Klassen gibt.

Da man festgestellt hat, daß nur „wenige“ Algebren polynomvollständig sind (siehe für Gruppen 3.1.4 ), haben sich einerseits der Begriff des Vollständigkeitsdefekts andererseits einige andere Vollständigkeitsbegriffe entwickelt. Für eine genauere Einführung und Abhandlung dieser Begriffe, sei auf *Kaiser* [9] verwiesen. Hier wollen wir nur die grundlegenden Definitionen und Eigenschaften angeben.

Gewisse „innere“ Hindernisse für die Polynomvollständigkeit sind die Unendlichkeit der Trägermenge $A$ der Algebra $[A;\Omega]$(für abzählbares $\Omega$), sowie die Existenz von nichttrivialen Kongruenzen. Diese versucht man mit den beiden folgenden Vollständigkeitsbegriffen zu umgehen.

**Definition 1.4.9** $LP_k(A) = \{g \in F_k(A) \,|\forall B \subseteq A, B \text{ endlich } \exists p \in P_k(A) : p|_{B^k} = g|_{B^k}\}$ *die Menge der* **lokalen l-Polynomfunktionen**.

Das sind also die Funktionen, die auf jeder endlichen Teilmenge mit einer Polynomfunktion übereinstimmen. Klarerweise gilt $P_k(A) \subseteq LP_k(A) \subseteq F_k(A)$. Falls $A$ endlich ist, fallen $P_k(A)$ und $LP_k(A)$ klarerweise zusammen. $LP_k(A) \preceq F_k(A)$, die lokalen Polynomfunktionen bilden also wieder eine Unteralgebra der vollen Funktionen.

**Definition 1.4.10** $A$ *heißt* **lokal l-polynomvollständig** *, wenn* $LP_k(A) = F_k(A)$.

Es läßt sich wieder zeigen, daß es nur drei Möglichkeiten der lokalen Polynomvollständigkeit gibt, die selben wie für die Polynomvollständigkeit. Eine Algebra kann somit lokal polynomvollständig, lokal halb polynomvollständig oder lokal polynomunvollständig sein.

Da $P_k(A) \subseteq LP_k(A) \subseteq F_k(A)$ gilt, ist die lokale Polynomvollständigkeit eine Verallgemeinerung der Polynomvollständigkeit. Diese Inklusion ist echt, da z.B. in der Varietät der Ringe mit Einselement gezeigt werden kann, daß genau die endlichen Körper polynomvollständig sind, aber alle Körper lokal polynom vollständig sind. Die letzte Tatsache kann gezeigt werden, da es für jede Funktion $f$ in einem Körper für endlich viele „Stützstellen“ immer ein Polynom gibt, das dort mit der Funktion überein stimmt (*Lagrangepolynom*).

Es läßt sich auch hier wieder zeigen, daß lokalpolynomvollständige Algebren einfach sind.

Ein weiterer Vollständigkeitsbegriff tritt auf, wenn man die kompatiblen Funktionen betrachtet:

**Definition 1.4.11** *$A$ heißt* **l-kongruenzpolynomvollständig** *, wenn gilt: $K_k(A) = F_k(A)$. $A$ heißt* **kongruenzpolynomvollständig** *, wenn $\forall\ k \in \mathbb{N}$ gilt: $K_k(A) = F_k(A)$.*

Aus der Kongruenzpolynomvollständigkeit für $m$ folgt wieder jene für $l \leq m$.

Nach 1.3.9 gilt $P_k(A) \subseteq K_k(A)$, somit sind polynomvollständige Algebren kongruenzpolynomvollständig. Und auch diese Inklusion ist echt (siehe 3.1.4). Lokal polynomvollständige Algebren sind auch kongruenzpolynomvollständig.

Für einfache Algebren fällt dieser Begriff natürlich mit der Polynomvollständigkeit zusammen.

Man kann sich auch fragen, welche Funktionen zumindest auf $n$ Stellen mit einem Polynom übereinstimmen.

**Definition 1.4.12** $L_nP_k(A) = \{g \in F_k(A) : \forall B \subseteq A \text{ mit } |B| = n\ \exists p \in P_k(A) : p|_{B^k} = g|_{B^k}\}$

Klarerweise gilt

$$P_k(A) \subseteq LP_k(A) \subseteq \ldots \subseteq L_tP_k(A) \ldots \subseteq L_2P_k(A) \subseteq K_k(A) \subseteq F_k(A)$$

Hier kann man sich natürlich nach Gleichheiten in dieser Kette fragen, einige davon haben wir bereits kennen gelernt. Die *Polynomvollständigkeit* und die

*lokale Polynomvollständigkeit* kennen wir bereits. Weiter können wir noch definieren

**Definition 1.4.13** *Eine Algebra $A \in \mathfrak{V}$ heißt* **k-affin vollständig**, *wenn $K_k(A) = P_k(A)$. Sie heißt* **k lokal vollständig**, *wenn $K_k(A) = LP_k(A)$.*

Ein anderer Weg den Vollständigkeitsbegriff zu erweitern ist, die Polynome auf einer Oberalgebra zu betrachten.

**Definition 1.4.14** *Sei $[A;\Omega]$ eine Algebra. $\overline{E}_k(A)$ sei die Menge aller Funktionen $f$ aus $F_k(A)$, für die es eine Erweiterung $B \succeq A$ und eine Polynomfunktion $g \in P_k(B)$ gibt, sodaß gilt: $g|_{A^k} = f$.*

Klarerweise gilt: $P_k(A) \subseteq \overline{E}_k(A)$, da die Erweiterung dann $A$ selbst ist.

**Definition 1.4.15** *Die Algebra $A$ heißt* **k-erweiterungspolynomvollständig**, *wenn $\overline{E}_k(A) = F_k(A)$. Sie heißt* **erweiterungspolynomvollständig** , *wenn $\overline{E}_k(A) = F_k(A)\ \forall\ k \in \mathbb{N}$.*

Dieser Vollständigkeitsbegriff überträgt sich (als einziger) auf Unteralgebren. Erweiterungspolynomvollständige Algebren müssen jedoch nicht notwendigerweise einfach sein.

Jede l-polynomvollständige Algebra ist trivialerweise l-erweiterungspolynomvollständig.

Neben zahlreichen anderen Verallgemeinerungen der Polynomvollständigkeit gibt es auch noch eine Spezialisierungen, die wichtigste betrachtet die Vollständigkeit bzgl. der sogenannten „Grätzer-polynome“, den Termfunktionen $T_k(A) = \{w(\xi_i)\}$.

**Definition 1.4.16** *$A$ heißt* **k-primal**, *wenn $T_k(A) = F_k(A)$. Sie heißt primal, wenn sie n-primal ist $\forall n \in \mathbb{N}$.*

Das ist eine Spezialisierung, da $T_k(A) \subseteq P_k(A)$.

Primale Algebren haben keine nicht trivialen Untergruppen oder Automorphismen. Damit folgt, daß es polynomvollständige Algebren gibt, die nicht primal sind. (Siehe 3.1.4)

Für alle diese Vollständigkeitsbegriffe lassen sich analoge Defektbegriffe definieren.

Bei der Frage nach der Vollständigkeit, haben wir Algebren gesucht, für die Algebren $A$ $\sigma_k : A[X, \mathfrak{V}] \to F_k(A)$ surjektiv sind. (Denn dann ist $\sigma_k(A[X, \mathfrak{V}]) = P_k(A) = F_k(A)$, also ist diese Algebra $k$-polynomvollständig!) Wann ist diese Abbildung injektiv?

**Definition 1.4.17** *Eine Algebra $[A, \Omega]$ heißt k-funktional unterscheidbar, wenn $\sigma_k : A[X, \mathfrak{V}] \to P_k(A)$ injektiv ist.*

D.h. wenn zwei Polynome $p, q \in A[X, \mathfrak{V}]$ die selbe Polynomfunktion induzieren, sind sie bereits gleich.

In diesem Fall ist also das Wortproblem aus 1.2.1 für ein bestimmtes $k$ gelöst. Können wir also das Wortproblem lösen, können wir auch diese Frage entscheiden.

Man kann zeigen:

**Lemma 1.4.18** *Ist $A$ k-funktional unterscheidbar und $l \leq k$, dann ist $A$ l-funktional unterscheidbar.*

Da $A[\{x_1, x_2, \ldots, x_l\}, \mathfrak{V}]$ in $A[\{x_1, x_2, \ldots, x_k\}, \mathfrak{V}]$ eingebettet werden kann, ist der Beweis klar.

**Beispiel:** Betrachten wir $[\mathbb{Z}, +, -, 0]$ so ist $\mathbb{Z}$ $k$-funktional unterscheidbar für alle $k \in \mathbb{N}$. Denn nach 3.1.9 lassen sich für $X = \{x_1, \ldots, x_k\}$ alle Polynome in $\mathbb{Z}[X]$ eindeutig als $a_0 + \mathfrak{x} \cdot \mathfrak{m}$ mit $\mathfrak{m} \in \mathbb{Z}^k$ $a \in G$ darstellen. Dasselbe gilt nach 3.1.16 auch für die Polynomfunktionen in $P_k(\mathbb{Z})$.

# Kapitel 2

# Kompositionsalgebren

Wenn wir Funktionen bzw. Funktionsalgebren betrachten, drängt sich uns eine Operation auf, das „Einsetzen“, die Komposition zweier Funktionen. Die Komposition zweier einstelliger Funktionen ist recht klar $((f \circ g)(x) = f(g(x)))$, für höher stellige Funktionen werden wir ein Konzept definieren, das Ähnlichkeiten zu Matrizen aufweist.

## 2.1 Kompositionsabbildung

Welche Eigenschaften würden wir uns von einer Komposition erwarten? Betrachten wir die Funktionenkomposition $f \circ g$ von zwei einstellige Funktionen und ihre Eigenschaften: Es seien $A, B, C$ und $D$ Mengen, sowie $f : C \to D, g : B \to C$ und $h : A \to B$ Funktionen. Dann hat die Komposition folgende Eigenschaften:

- Es gilt die Assoziativität: $f \circ (g \circ h) = (f \circ g) \circ h$
- Es gibt Identitäten: $id_D \circ f = f \circ id_C = f$

Sind die Mengen nun Algebren mit den Operationen $\Omega = \{\omega_i : i \in I\}$, so gilt, wenn wir die Operationen auf den Funktionen punktweise definieren (siehe 1.3.2):

- Rechts - Distributivität:
  - $\omega_i \circ f = \omega_i$ für $Ar(\omega_i) = 0$ und
  - $\omega_i(f_1, \ldots, f_n) \circ g = \omega_i(f_1 \circ g, \ldots, f_n \circ g)$ für $Ar(\omega_i) = n > 0$

Diese Eigenschaften wollen wir nun auf den allgemeinen Fall übertragen:

**Definition 2.1.1** *Sei $M$ eine nicht leere Menge, $k \in \mathbb{N}$, $\chi$ eine (k+1)-wertige Operatio $\omega_i$ Operationen auf M. Seien $x_j, y_l$ Unbestimmte. (j,l = 0,1,...,k)*
*$\chi$ heißt* **superassoziativ** *, wenn gilt:*

$$\chi\left(\chi(x_0, x_1, x_2, ..., x_k), y_1, y_2, ..., y_k\right) =$$

$$= \chi\left(x_0, \chi(x_1, y_1, y_2, ..., y_k), \chi(x_2, y_1, y_2, ..., y_k), ..., \chi(x_k, y_1, y_2, ..., y_k)\right)$$

*$\chi$ heißt* **rechts-superdistributiv** *in bezug auf $\omega_i$, wenn gilt:*

$$\chi(\omega_i, y_1, y_2, ..., y_k) = \omega_i \quad f\ddot{u}r Ar(\omega_i) = 0$$

$$\chi\left(\omega_i(x_1, x_2, ..., x_{Ar(\omega_i)}), y_1, y_2, ..., y_k\right) = \omega_i\left(\chi(x_1, y_1, ..., y_k), \chi(x_2, y_1, ..., y_k), ...\right.$$
$$\left. ..., \chi(x_{Ar(\omega_i)}, y_1, y_2, ..., y_k)\right) \quad f\ddot{u}r Ar(\omega_i) > 0$$

*Eine Teilmenge $\{s_1, s_2, ..., s_k\} \subseteq M$ heißt* **Selektorsystem** *für $\chi$, wenn gilt:*

$$\chi(s_i, y_1, y_2, ..., y_k) = y_i \quad \forall i = 1, 2, ..., k$$

$$\chi(x_1, s_1, s_2, ..., s_k) = x_1$$

Warum verwenden wir hier ein anders Symbol als das für die Funktionskomposition $\circ$? Damit wollen wir zwischen beliebigen superassoziativen und superrechtsdistributiven und jenen Operationen unterscheiden, die wir als Komposition von Funktionen auffassen können. Wir werden später (2.1.15) sehen, daß diese Unterscheidung eine künstliche ist.

Die Namensgebung der Eigenschaften kommt daher, daß sich für $k = 1$ und $Ar(\omega_i) = 2$ die Superassoziviativität auf die Assoziativität, die Rechts-Superdistributivität auf die Rechts-distributivität und ein Selektorsystem auf eine Einheit ($\chi(s, x) = x = \chi(x, s)$) bzw. Identität reduziert.

Die Komposition von einstelligen ($k = 1$) Funktionen hat genau diese Eigenschaften (aus Def. 2.1.1), und wir werden sehen, daß die Komposition von $k$-stelligen Funktionen (Def. 2.1.3) recht natürlich definiert werden kann, sodaß diese Eigenschaften erfüllt werden.

Wir können einige Eigenschaften eines Selektorsystems angeben. Klarerweise folgt aus $|M| = 1$, daß die Elemente eines Selektorsystems gleich sind. Aber der 2. Teil des folgenden Satzes sagt uns, daß auch die Umkehrung gilt, d.h. gibt es zwei Elemente eines Selektorsystems, die gleich sind, so gilt bereits $|M| = 1$.

Der erste Teil besagt, daß ein Selektorsystem eindeutig bestimmt ist.

**Lemma 2.1.2** *1. Ein Selektorsystem ist, falls existent, eindeutig bestimmt.*

*2. Genau dann, wenn $|M| \neq 1$, sind die Elemente aus einem Selektorsystem paarweise verschieden.*

**Beweis:** ad (1): Sei $\{t_1, t_2, ..., t_k\}$ ein zweites Selektorsystem. Dann gilt einerseits $\chi(s_i, t_1, ..., t_k) = t_i$, da die $s_i$ ein Selektorsystem bilden, andererseits gilt $\chi(s_i, t_1, ..., t_k) = s_i$, da die $t_i$ ein Selektorsystem sind. $\Longrightarrow t_i = s_i$
ad (2) Denn wenn $s_i = s_j$ für $i \neq j$, dann ist $y_i = y_j \ \forall i, j = 1, \ldots, k$. □

### 2.1.1 Komposition von Funktionen

Wie kann man nun die Funktionenkomposition für $k > 1$ definieren?

**Definition 2.1.3** *Es seien $\varphi \in F_k(A), \psi_i \in F_l(A)$ und $(a_1, \ldots, a_l) \in A^l$ beliebig. Dann definiere $\varphi \circ (\psi_1, \ldots, \psi_k) \in F_l(A)$ durch*

$$(\varphi \circ (\psi_1, \ldots, \psi_k))(a_1, \ldots, a_l) = \varphi(\psi_1(a_1, \ldots, a_l), \ldots, \psi_k(a_1, \ldots, a_l))$$

Für $k = 1$ entspricht diese Definition der Komposition einstelliger Funktionen.

Mit dieser Definition ist $\circ$ eine Abbildung von $F_k(A) \times F_l(A)^k$ nach $F_l(A)$. Wir können sogar zeigen, daß diese Abbildung in der ersten Koordinate ein Homomorphismus ist:

**Lemma 2.1.4** *Für jedes $(\psi_1, \ldots, \psi_k) \in F_l(A)^k$ ist die Abbildung $\varphi \mapsto \varphi \circ (\psi_1, \ldots, \psi_k)$ ein Homomorphismus von $F_k(A)$ nach $F_l(A)$.*

**Beweis:** Wir müssen zeigen, daß

- $\omega_i \circ (\psi_1, \ldots, \psi_k) = \omega_i$ für $Ar(\omega_i) = 0$.
- $\omega_i\left(\varphi_1, \ldots, \varphi_{Ar(\omega_i)}\right) \circ (\psi_1, \ldots, \psi_k) = \omega_i(\varphi_1 \circ (\psi_1, \ldots, \psi_k), \ldots$
  $\ldots, \varphi_{Ar(\omega_i)} \circ (\psi_1, \ldots, \psi_k))$ für $Ar(\omega_i) > 0$.

Aufgrund der Definition ist das gleichbedeutend damit, daß diese Gleichungen punktweise gelten:
Sei $Ar(\omega_i) = 0$ :

$$\omega_i \circ (\psi_1, \ldots, \psi_k)(a_1, \ldots, a_l) = \omega_i(\psi_1(a_1, \ldots, a_l), \ldots, \psi_k(a_1, \ldots, a_l)) = \omega_i$$

Sei $Ar(\omega_i) > 0$ :

$$\omega_i\left(\varphi_1, \ldots, \varphi_{Ar(\omega_i)}\right) \circ (\psi_1, \ldots, \psi_k)(a_1, \ldots, a_l) =$$

$$= \omega_i \left(\varphi_1, \ldots, \varphi_{Ar(\omega_i)}\right) \left(\psi_1 \left(a_1, \ldots, a_l\right), \ldots, \psi_k \left(a_1, \ldots, a_l\right)\right) =$$
$$= \omega_i \left(\varphi_1 \left(\psi_1 \left(a_1, \ldots, a_l\right), \ldots, \psi_k \left(a_1, \ldots, a_l\right)\right), \ldots, \varphi_{Ar(\omega_i)} \left(\psi_1 \left(a_1, \ldots, a_l\right), \ldots\right.\right.$$
$$\left.\left. \ldots, \psi_k \left(a_1, \ldots, a_l\right)\right)\right) = \omega_i \left(\varphi_1 \circ \left(\psi_1, \ldots, \psi_k\right), \ldots, \varphi_{Ar(\omega_i)} \circ \left(\psi_1, \ldots, \psi_k\right)\right) \quad \square$$

Mit derselben Argumentation zeigt man, daß diese Komposition superassoziativ ist:

**Lemma 2.1.5** *Sei $\varphi \in F_k(A)$, $(\psi_1, \ldots, \psi_k) \in F_l(A)^k$, und $(\chi_1, \ldots, \chi_l) \in F_m(A)^l$. Dann ist*

$$(\varphi \circ (\psi_1, \ldots, \psi_k)) \circ (\chi_1, \ldots, \chi_l) = \varphi \circ (\psi_1 \circ (\chi_1, \ldots, \chi_l), \ldots, \psi_k \circ (\chi_1, \ldots, \chi_l))$$

**Proposition 2.1.6** *Sei $A$ eine Algebra aus der Varietät $\mathfrak{V}$, $\Omega$ ihre Operationsmenge und $k \geq 1$ eine ganze Zahl. Auf $[F_k(A); \Omega]$definieren wir eine $(k+1)$-wertige Operation $\chi$ durch $\chi(\varphi_0, \ldots, \varphi_k) = \varphi_0 \circ (\varphi_1, \ldots, \varphi_k)$. Dann ist $\chi$ superassoziativ und super-rechtsdistributiv . Ist $\Omega_1 = \{\Omega, \chi\}$, dann ist $[F_k(A); \Omega_1]$ eine $\Omega_1$-algebra mit Selektorsystem $\{\xi_1, \ldots, \xi_k\}$, den Projektionen.*

**Beweis:** Nach 1.3.2 ist $[F_k(A); \Omega]$ eine Algebra aus $\mathfrak{V}$. Für $l = m = k$ liefert 2.1.5 die Superassoziativität. 2.1.4 liefert die Rechts-superdistributivität. (Das sieht man besonders gut, wenn man die Beweisführung von 2.1.4 mit der Definition der Rechts-superdistributivität vergleicht.) Die Projektionen erfüllen die Definition eines Selektorsystems klarerweise. $\square$

Wir konnten somit aus der $\Omega$-Algebra $[F_k(A); \Omega]$ eine $\Omega_1$-algebra $[F_k(A); \Omega, \chi]$ bilden. Diesen Schritt wollen wir nun im nächsten Abschnitt verallgemeinern.

### 2.1.2 Kompositionsalgebren

Hat man ganz allgemein eine Algebra gegeben, so kann man das obige Verfahren generalisieren:

Sei $\Omega = \{\omega_i \mid i \in I\}$ eine Menge von Operationen, $\mathfrak{W}$ eine Klasse von $\Omega$-Algebren. Sei weiters $\chi$ eine Operation mit $Ar(\chi) = k + 1$ mit $k$ eine positive ganze Zahl und sei $\Omega_1 = \Omega \cup \{\chi\}$.

**Definition 2.1.7** *Die Algebra $[A; \Omega_1]$ heißt* **k-dimensionale $\mathfrak{W}$-Kompositionsalgebra**, *wenn $[A; \Omega]$ eine Algebra aus $\mathfrak{W}$ ist, $\chi$ superassoziativ ist und $\chi$ rechtsdistributiv bzgl. $\omega_i$ ist $\forall \omega_i \in \Omega$.*

Der wichtigste Fall liegt vor, wenn die Klasse $\mathfrak{W}$ eine Varietät $\mathfrak{V}$ ist. Wir werden uns ab nun auf diesen beschränken.

**Beispiel:** Nach dem Satz 2.1.6 ist für jede Varietät $\mathfrak{V}$, für jede Algebra $A \in \mathfrak{V}$ und für jedes $k \geq 1$ die Algebra $[F_k(A); \Omega, \circ]$ eine $k$-dimensionale $\mathfrak{V}$-Kompositionsalgebra.

Hat die k-dimensionale $\mathfrak{V}$-Kompositionsalgebra ein Selektorsystem

$$S = \{s_1, s_2, ..., s_k\}$$

so kann sie als Algebra mit den Operationen $\Omega_2 = \Omega \cup \{\chi\} \cup \{s_1, s_2, ..., s_k\}$ aufgefaßt werden, wobei die $s_i$ als Operationen mit $Ar(s_i) = 0$ gelten.

**Proposition 2.1.8** *Die Klasse der k-dimensionalen $\mathfrak{V}$-Kompositionsalgebren ist eine Varietät bzgl. $\Omega_1$, die Klasse der k-dimensionalen $\mathfrak{V}$-Kompositionsalgebren mit Selektorsystem eine bzgl. $\Omega_2$.*

**Beweis:** Die Definitionen der Superassoziativität, der Rechts-Distributivität und der Selektorsysteme bestehen aus Gleichungen. Somit kann die Varietät aller $\Omega$-Algebren betrachtet werden, in der diese Gleichungen Gesetze sind. □

**Definition 2.1.9** *Ist $[A; \Omega, \chi]$ eine k-dimensionale $\mathfrak{V}$-Kompositionsalgebra und $B$ eine Unteralgebra von $A$ bezüglich $\Omega_1 = \Omega \cup \{\chi\}$, d.h. $B \preceq_{\Omega_1} A$, so bezeichnen wir $B$ als* **Kompositionsunteralgebra** *von $A$, symbolisch: $B \preceq_\chi A$.*

Damit unterscheiden wir die Unteralgebren $B$ von $A$ bezüglich $\Omega$, $B \preceq A$, von jenen bezüglich $\Omega_1$, $B \preceq_\chi A$. Klarerweise gilt:

$$B \preceq_\chi A \Longrightarrow B \preceq A$$

**Definition 2.1.10** *Es seien $[C; \Omega, \chi]$ und $[D; \Omega, \chi]$ k-dimensionale $\mathfrak{V}$-Kompositionsalgebren. Ein Homomorphismus*

$$\varphi : [C; \Omega] \to [D; \Omega] \text{ mit } \varphi \in Hom_\Omega(C, D)$$

*heißt* **Kompositionshomomorphismus** *, wenn er auch ein Homomorphismus von $[C; \Omega, \chi]$ nach $[D; \Omega, \chi]$ ist, $\varphi \in Hom_{\Omega \cup \{\chi\}}(A, B)$.*
*Ist $\varphi$ ein Mono-, Epi- oder Isomorphismus, so nennen wir es einen Kompositionsmono-, -epi- oder -isomorphismus.*

**Definition 2.1.11** *Sei $[C;\Omega,\chi]$ eine k-dimensionale $\mathfrak{V}$-Kompositionsalgebra. Ein Element $c \in C$ heißt* **Konstante** *von C, wenn $\forall\ c_i \in C, I = 1,\ldots,k$ gilt*

$$\chi(c, c_1, \ldots, c_k) = c$$

Die Elemente von $A$ sind klarerweise Konstanten in den Algebren $[F_k(A);\Omega,\circ]$ und $[P_k(A);\Omega,\circ]$. Ebenso klar ist auch die folgende Eigenschaft für Konstanten:

**Lemma 2.1.12** *Sei $\vartheta : [C;\Omega,\chi] \to [D;\Omega,\chi]$ ein Kompositionsepimorphismus. Dann bildet $\vartheta$ jede Konstante von C auf eine Konstante von D ab.*

Für Selektorsysteme gilt

**Lemma 2.1.13** *Sei $\vartheta : [C;\Omega,\chi] \to [D;\Omega,\chi]$ ein Kompositionshomomorphismus. Sei $\{s_1,\ldots,s_k\}$ ein Selektorsystem von D und $\{s_1,\ldots,s_k\} \subseteq \vartheta(C)$. Dann bildet $\vartheta$ ein Selektorsystem von C auf eines von D ab.*

**Beweis:** Sei $\{t_1,\ldots,t_k\}$ ein Selektorsystem von C. Betrachte $\vartheta(C)$. Nach 1.1.12 ist $\vartheta(C) \preceq_\chi D$. Dann gilt für beliebige $y_i \in \vartheta(C), i = 1,\ldots,k, \vartheta(x_i) = y_i$ mit geeigneten $x_i \in C$, und weiters

$$\chi(\vartheta(t_i), y_1, \ldots, y_k) = \chi(\vartheta(t_i), \vartheta(x_1), \ldots, (x_k)) =$$

$$= \vartheta(\chi(t_i, x_1, \ldots, x_k)) = \vartheta(x_i) = y_i$$

Angenommen $\vartheta(t_i) = \vartheta(t_j) \Longrightarrow y_i = y_j\ \forall i,j = 1,\ldots,k$, also wäre $|\vartheta(C)| = 1$, und damit auch $|\{s_1,\ldots,s_k\}| = 1$.
D.h. die $\vartheta(t_i)$ bilden ein Selektorsystem von $\vartheta(C)$, die $s_i$ bilden klarerweise auch eines. Die beiden Systeme sind somit nach 2.1.2 gleich. □

Für einen Kompositionsepimorphismus ist die Bedingung für dieses Lemma klarerweise erfüllt.

Wir können nun für die neue Operatorenmenge $\Omega_1 = \Omega \cup \{\chi\}$ die Kongruenzen betrachten und definieren:

**Definition 2.1.14** *Sei $[A;\Omega,\chi]$ eine k-dimensionale $\mathfrak{V}$-Kompositionsalgebra. Eine Kongruenz K von $[A;\Omega]$ heißt* **Vollkongruenz** *, wenn sie auch eine Kongruenz von $[A;\Omega,\chi]$ ist.*

Die Vollkongruenzen sind die Kongruenzen bezüglich der k-dimensionalen $\mathfrak{V}$-Kompositionsalgebren, damit gelten alle Sätze aus Kapitel 1, wie z.B. der Homomorphiesatz.

Der interessanteste Fall sind auch hier wieder die Funktionsalgebren. Man kann zeigen, daß für alle $A$ $F_k(A)$ für $k > 1$ nur die trivialen Vollkongruenzen besitzt, für $k = 1$ gilt das nur mehr für eine große Klasse von Algebren, aber nicht mehr für alle Algebren. (Für Literatur zu diesen Aussagen siehe [18] Kapitel 3, *Remarks and comments*zu §4)

Wir werden im nächsten Abschnitt die Komposition von Polynomen definieren, und uns dort dann (kurz) den Vollkongruenzen der Polynome- und Polynomfunktionen widmen.

Wir können nun als wichtige Beispiele für Kompositionsalgebren betrachten:
**Beispiele:**

1. Sei $\mathfrak{V}$ die Varietät der Mengen, d.h. $\Omega = \emptyset$, dann bilden die $k$-dimensionalen $\mathfrak{V}$-Kompositionsalgebren eine Varietät, die Varietät der sogenannten *k-dimensionalen superassoziativen Systeme.*
   Insbesondere sind die 1-dimensionalen superassoziativen Systeme genau die Halbgruppen.
   Die Familie aller unären Funktionen bilden also über jeder Menge eine Halbgruppe.

2. Sei $\mathfrak{V}$ die Varietät der Gruppen. Dann nennt man die $k$-dimensionalen $\mathfrak{V}$-Kompositionsalgebren *k-dimensionale Kompositionsgruppen* .
   Insbesondere sind die 1-dimensionale Kompositionsgruppen unter dem Namen *Fastringe* (siehe 3.1.5) bekannt.
   Die Familie der Funktionen über einer Gruppe bilden also einen Fastring.

Wir wissen, daß jede volle Funktionenalgebra $F_k(A)$ über der Algebra $A$ aus der Varietät $\mathfrak{V}$ eine k-dimensionale $\mathfrak{V}$-Kompositionsalgebra bilden, wenn man die Funktionenkomposition dazunimmt. Da die Klasse der $k$-dimensionalen $\mathfrak{V}$-Kompositionsalgebren eine Varietät ist, sind Unteralgebren auch wiederum k-dimensionale $\mathfrak{V}$-Kompositionsalgebren.

Wir können nun zeigen, daß es bis auf Isomorphismus keine anderen k-dimensionale $\mathfrak{V}$-Kompositionsalgebren gibt.

**Satz 2.1.15** *Sei $A = [A; \Omega, \chi]$ eine k-dimensionale $\mathfrak{V}$-Kompositionsalgebra. Dann gibt es eine Algebra $D$ aus $\mathfrak{V}$, sodaß $A$ isomorph zu einer Unteralgebra der k-dimensionalen $\mathfrak{V}$-Kompositionsalgebra $[F_k(D); \Omega, \circ]$ ist.*

**Beweis:** Dieser Satz gilt klarerweise für $|A| = 1$, denn dann ist auch $|F_k(A)| = 1$ und wir können dann $D = [A; \Omega]$ setzen.
Sei nun $|A| \neq 1$. Dann sei $D$ eine echte $\mathfrak{V}$-Erweiterung von $[A; \Omega]$, d.h.

$D \neq A$, wie z.B. $D = F_1(A)$. $\vartheta : [A; \Omega, \chi] \to [F_k(D); \Omega, \circ]$ definieren wir nun durch

$$(\vartheta(a))\,(d_1, \ldots, d_k) = \begin{cases} \chi(a, d_1, \ldots, d_k) & f\ddot{u}r\ d_i \in A \\ a & sonst \end{cases}$$

$\vartheta$ ist injektiv, da ein $(d_1, \ldots, d_k) \in D^k \backslash A^k$ existiert, und somit aus

$$(\vartheta(a))\,(d_1, \ldots, d_k) = (\vartheta(b))\,(d_1, \ldots, d_k)$$

folgt $a = b$.
Wir müssen nur mehr zeigen, daß $\vartheta$ ein Kompositionshomomorphismus ist. D.h. zu zeigen sind

- $(\vartheta(\omega_i))\,(d_1, \ldots, d_k) = \omega_i$ für $Ar(\omega_i) = 0$.
- $\left(\vartheta\left(\omega_i\left(a_1, \ldots, a_{Ar(\omega_i)}\right)\right)\right)(d_1, \ldots, d_k) =$
  $= \left(\omega_i\left(\vartheta(a_1), \ldots, \vartheta(a_{Ar(\omega_i)})\right)\right)(d_1, \ldots, d_k)$ für $Ar(\omega_i) > 0$.
- $\left(\vartheta\left(\chi\left(a_0, a_1, \ldots, a_{Ar(\omega_i)}\right)\right)\right)(d_1, \ldots, d_k) =$
  $= \vartheta(a_0) \circ \left(\vartheta(a_1), \ldots, \vartheta(a_{Ar(\omega_i)})\right)(d_1, \ldots, d_k)$

Ist $(d_1, \ldots, d_k) \notin A$, so sind alle drei Eigenschaften klar. Sei nun also $(d_1, \ldots, d_k) \in A$.
Sei $Ar(\omega_i) = 0$: Dann folgt aus der Rechts-Superdistributivität

$$(\vartheta(\omega_i))\,(d_1, \ldots, d_k) = \chi\,(\omega_i, d_1, \ldots, d_k) = \omega_i$$

Auch für den Fall $Ar(\omega_i) > 0$ können wir die Rechts-Superdistributivität anwenden:

$$\left(\vartheta\left(\omega_i(a_1, \ldots, a_{Ar(\omega_i)})\right)\right)(d_1, \ldots, d_k) = \chi\left(\omega_i(a_1, \ldots, a_{Ar(\omega_i)}), d_1, \ldots, d_k\right) =$$

$$= \omega_i\left(\chi(a_1, d_1, \ldots, d_k), \ldots, \chi(a_{Ar(\omega_i)}, d_1, \ldots, d_k)\right) =$$

$$= \left(\omega_i\left(\vartheta(a_1), \ldots, \vartheta(a_{Ar(\omega_i)})\right)\right)(d_1, \ldots, d_k)$$

Betrachte nun $a = \chi(a_0, \ldots, a_k)$ und wende die Superassoziativität an. Einerseits gilt dann

$$(\vartheta\,(\chi(a_0, \ldots, a_k)))\,(d_1, \ldots, d_k) = \chi\,(\chi(a_0, \ldots, a_k), d_1, \ldots, d_k) =$$

$$= \chi\,(a_0, \chi(a_1, d_1, \ldots, d_k), \ldots, \chi(a_1, d_1, \ldots, d_k)) =$$

Andererseits ist

$$\vartheta(a_0) \circ (\vartheta(a_1), \ldots, \vartheta(a_k))\,(d_1, \ldots, d_k) =$$

$$= \chi\left(a_0, \vartheta\left(a_1\right)\left(d_1, \ldots, d_k\right), \ldots, \vartheta\left(a_k\right)\left(d_1, \ldots, d_k\right)\right)$$
$$= \chi\left(a_0, \chi\left(a_1, d_1, \ldots, d_k\right), \ldots, \chi\left(a_k, d_1, \ldots, d_k\right)\right).$$

□

Ab nun können wir für die superassoziative und rechts-superdistributive Operation von $k$-dimensionalen $\mathfrak{V}$-Kompositionsalgebren immer das Symbol $\circ$ verwenden, da die von uns eingeführte Unterscheidung nur isomorphe Strukturen liefert. So können wir ab nun für eine Kompositionsunteralgebra $B$ der Kompositionsalgebra $A$ immer die Symbolik $B \preceq_\circ A$ verwenden.

### 2.1.3 Komposition von Polynomen

Die Algebra der Polynomfunktionen $[P_k; \Omega]$ ist eine Unteralgebra der vollen Funktionsalgebra $[F_k; \Omega]$. Um den folgenden Sachverhalt zu beweisen, müssen wir also nur zeigen, daß $P_k(A)$ bzgl. der Komposition abgeschlossen ist.

**Proposition 2.1.16** *Sei $A$ eine Algebra aus der Varietät $\mathfrak{V}$. Die Untermenge $P_k(A)$ der Kompositionsalgebra $[F_k; \Omega, \circ]$ ist eine Unteralgebra, d.h. $[P_k; \Omega]$ ist selbst wieder eine $k$-dimensionale $\mathfrak{V}$-Kompositionsalgebra mit Selektorsystem $\xi_1, \ldots, \xi_k$.*

$$P_k(A) \preceq_\circ F_k(A)$$

**Beweis:** Für $j = 0, \ldots, k$ seien $\pi_j$ Elemente aus $P_k(A)$. Da $P_k(A) = A(\xi_1, \ldots, \xi_k)$ ist, können wir diese schreiben als

$$\pi_j = w\left(a_1^{(j)}, \ldots, a_n^{(j)}; \xi_1, \ldots, \xi_k\right) = w\left(a_i^{(j)}; \xi_1, \ldots, \xi_k\right)$$

Betrachten wir nun $\pi_0 \circ (\pi_1, \ldots, \pi_k)$, dann ist

$$\left(\pi_0 \circ (\pi_1, \ldots, \pi_k)\right)(d_1, \ldots, d_k) = \pi_0\left(\pi_1(d_1, \ldots, d_k), \ldots, \pi_k(d_1, \ldots, d_k)\right) =$$
$$= w_0\left(a_i^{(0)}; w_1\left(a_i^{(1)}; d_1, \ldots, d_k\right), \ldots, w_k\left(a_i^{(k)}; d_1, \ldots, d_k\right)\right)$$
$$= w_0\left(a_i^{(0)}; w_1\left(a_i^{(1)}; \xi_1, \ldots, \xi_k\right), \ldots, w_k\left(a_i^{(k)}; \xi_1, \ldots, \xi_k\right)\right)(d_1, \ldots, d_k)$$

Also ist $\pi_0 \circ (\pi_1, \ldots, \pi_k) \in |W(A \cup \{\xi_1, \ldots, \xi_k\})|_{F_k(A)} = P_k(A)$ □

Die Menge der kompatiblen Funktionen bzgl. $\mathfrak{M}$, $K_k(A, \mathfrak{M})$, ist $\forall\ \mathfrak{M} \subseteq \mathfrak{K}(A)$ bezüglich der Komposition abgeschlossen. Klarerweise ist auch hier das Selektorsystem $\{\xi_1, \ldots, \xi_k\}$ enthalten. Also gilt auch hier:

$$K_k(A, \mathfrak{M}) \preceq_\circ F_k(A)$$

Jede Polynomfunktion $\pi \in P_k(A)$ ist Bild eines Polynoms $p \in A(X, \mathfrak{V})$. Können wir auf $A(X, \mathfrak{V})$ eine „Komposition“ definieren? (Eine, für die der kanonische Epimorphismus ein Kompositionsepimorphismus wird?)

**Definition 2.1.17** *Sei $A$ eine Algebra der Varietät $\mathfrak{V}$ mit den Operationen $\Omega$. Es seien $X = \{x_1, \ldots, x_k\}$ und $Y = \{y_1, \ldots, y_l\}$ (nicht notwendigerweise disjunkte) Menge von Unbestimmten. Seien $p \in A(X, \mathfrak{V})$ und $q_1, \ldots, q_k \in A(Y, \mathfrak{V})$, dann definieren wir*

$$p \circ (q_1, \ldots, q_k) = p(q_1, \ldots, q_k)$$

Nach 1.2.11 ist diese Komposition wohldefiniert.

Diese Definition der Komposition von Polynome ist eine sehr natürliche, denn wenn $p = w_0(a_j; x_1, \ldots, x_k)$ ist und $q_i = w_i(a_j; x_1, \ldots, x_k)$ sind, so ist $p \circ (q_1, \ldots, q_k) = w_0\left(a_j; w_1\left(a_j; x_1, \ldots, x_k\right), \ldots, w_k\left(a_j; x_1, \ldots, x_k\right)\right)$, d.h. die Komposition der Polynome ist das Einsetzen der „nachfolgenden “ Polynome in die Unbestimmten.

Es lassen sich zu 2.1.4, 2.1.5 und 2.1.6 analoge Aussagen formulieren, die auch analog bewiesen werden können. Dazu seien $X = \{x_1, \ldots, x_k\}, Y = \{y_1, \ldots, y_l\}$ und $Z = \{z_1, \ldots, z_m\}$.

**Lemma 2.1.18** *Für jedes $(p_1, \ldots, p_k) \in A(Y, \mathfrak{V})^k$ ist die Abbildung $q \mapsto q \circ (p_1, \ldots, p_k)$ ein Homomorphismus von $A(X, \mathfrak{V})$ nach $A(Y, \mathfrak{V})$.*

**Lemma 2.1.19** *Sei $p \in A(X, \mathfrak{V})$, $(q_1, \ldots, q_k) \in A(Y, \mathfrak{V})^k$, und $(r_1, \ldots, r_l) \in A(Z, \mathfrak{V})^l$. Dann ist*

$$(p \circ (q_1, \ldots, q_k)) \circ (r_1, \ldots, r_l) = p \circ \left(q_1 \circ (r_1, \ldots, r_l), \ldots, q_k \circ (r_1, \ldots, r_l)\right)$$

**Proposition 2.1.20** *Sei $A$ eine Algebra aus der Varietät $\mathfrak{V}$, $\Omega$ ihre Operationenmenge und $k \geq 1$ eine ganze Zahl. Auf $[A(X, \mathfrak{V}); \Omega]$definieren wir eine $(k+1)$-wertige Operation $\circ$ mit $p_0 \circ (p_1, \ldots, p_k) = p_0\left(p_1, \ldots, p_k\right)$. Ist $\Omega_1 = \{\Omega, \circ\}$, dann ist $[A[X, \mathfrak{V}]; \Omega_1]$ eine $k$-dimensionale $\mathfrak{V}$-Kompositionsalgebra mit Selektorsystem $\{x_1, \ldots, x_k\}$. Die Elemente aus $A$ sind in $A[X, \mathfrak{V}]$ Konstante.*

Es bleibt zu zeigen, daß der kanonische Epimorphismus $\sigma_k$ ein Kompositionshomomorphismus ist. Das folgt aus dem folgenden Satz, der alle Kompositionsepimorphismen von $A[X, \mathfrak{V}]$ beschreibt.

**Satz 2.1.21** *Es sei $A(x_1, \ldots, x_k, \mathfrak{V}) = A(X, \mathfrak{V})$ eine $\mathfrak{V}$-Polynomalgebra und $[C; \Omega, \circ]$ eine k-dimensionale $\mathfrak{V}$-Kompositionsalgebra, so daß*

1. *$C$ ein Selektorsystem $s_1, s_2, \ldots, s_k$ hat.*
2. *$[C; \Omega]$ eine Unteralgebra $B$ hat, die aus Konstanten von $[C; \Omega, \circ]$ besteht und $[C; \Omega] = B(s_1, \ldots, s_k)$ gilt.*

*Dann kann jeder Homomorphismus $\varsigma : A \to B$ zu einem Kompositionshomomorphismus $\rho : A(X, \mathfrak{V}) \to [C; \Omega]$ erweitert werden, der die $x_i$ auf die $s_i$ abbildet, $\forall i = 1, \ldots, k$. D.h. $\rho\,(w\,(a_i; x_j)) = w\,(\varsigma\,(a_i)\,; x_j)$*
*Ist $\eta$ ein Epimorphismus $\eta : A \to B$ so kann dieser eindeutig zu einem Kompositionsepimorphismus $\rho : A(X, \mathfrak{V}) \to [C; \Omega]$ erweitert werden. $\rho$ bildet die $x_i$ auf die $s_i$ ab, $\forall i = 1, \ldots, k$. Jeder Kompositionsepimorphismus von $A(X, \mathfrak{V})$ kann auf diese Art und Weise erreicht werden.*

**Beweis:** [18] Kapitel 3, Satz 3.21.

**Definition 2.1.22** *Diese Erweiterung $\rho$ des Homomorphismus $\eta : A \to B$ aus Satz 2.1.21 bezeichnen wir als* **Kompositionserweiterung** *von $\eta$.*

**Bemerkung:** Es gibt zwei grundlegende Anwendungen für diesen Satz

- Es seien $A, B$ Algebren der Varietät $\mathfrak{V}$. Sei $\eta : A \to B$ ein Homomorphismus. 1.2.9 liefert einen eindeutigen Homomorphsimus $\eta[X] : A[X, \mathfrak{V}] \to B[X, \mathfrak{V}]$ mit $\eta[X]\,(w(a_i; x_j)) = w(\eta(a_i); x_j)$. Das ist aber genau die Erweiterung von $\eta$ zu einem Kompositionshomomorphismus im vorherigen Satz, wenn $C = B[X, \mathfrak{V}]$. (Wir wissen, daß die $x_i$ ein Selektorsystem bilden und die Elemente $b \in B$ Konstanten von $B[X, \mathfrak{V}]$ sind.) Daher ist $\eta[X]$ ein Kompositionshomomorphismus. Für einen Epimorphismus existiert ein eindeutiger Kompositionsepimorphismus, für einen Isomorphismus ein eindeutiger Kompositionsisomorphismus.

- Sei $A$ eine Algebra der Varietät $\mathfrak{V}$. Dann gibt es die eindeutige Erweiterung von $a \mapsto a$ zu einem Kompositionsepimorphismus von $A\,[x, \mathfrak{V}]$ nach $P_k(A)$, die die $x_i$ auf die $\xi_i$ abbildet. Das entspricht aber genau dem in 1.3.8 konstruierten kanonischen Epimorphismus $\sigma_k$. Dieser ist also ein Kompositionsepimorphismus.
  Wollen wir auch die Abhängigkeit von $G$ ausdrücken, so schreiben wir $\sigma_k[G]$.

Da wir nun eine Komposition von Polynomen definiert haben, können wir uns fragen, was für die Vollkongruenzen der Polynom- oder Polynomfunktionsalgebra gilt? Der kanonische Epimorphismus $\sigma_k[A]$ ist ein Kompositionsepimorphismus, liefert somit nach 1.1.30 einen Isomorphismus zwischen den

Vollkongruenzen auf $P_k(A)$ und jenen auf $A[X, \mathfrak{V}]$, die $Ker(\sigma_k[A])$ enthalten. Deswegen reicht es, die Vollkongruenzen von $A[X, \mathfrak{V}]$ zu kennen.

Dazu läßt sich bemerken

**Lemma 2.1.23** *Die Kongruenz $K$ auf $A[X, \mathfrak{V}]$ ist Vollkongruenz genau dann, wenn aus $p_0 \sim_K q_0$ stets folgt*

$$\chi(p_0, p_1, \ldots, p_k) \sim_K \chi(q_0, p_1, \ldots, p_k) \ \forall (p_1, \ldots, p_k) \in A[X, \mathfrak{V}]^k$$

**Beweis:** [18] Kapitel 3, Lemma 4.31.

Aus 2.1.20 wissen wir, daß $A[X, \mathfrak{V}]$ eine Kompositionsalgebra ist. Wir können uns natürlich die Frage stellen, wann diese Algebra einfach ist, wann es also nur die trivialen Vollkongruenzen in $A[X, \mathfrak{V}]$ gibt. Man kann zeigen, daß das nur in sehr speziellen Fällen eintritt:

**Proposition 2.1.24** *Sei $A$ eine $\Omega$-Algebra der Varietät $\mathfrak{V}$, $|A| > 1$, $X = \{x_1, \ldots, x_k\}$ eine Menge von Unbestimmten. Dann ist die Kompositionsalgebra $[A[X, \mathfrak{V}]; \Omega, \circ]$ genau dann einfach, wenn*

- *der kanonische Epimorphismus $\sigma_k : A[X, \mathfrak{V}] \to P_k(A)$ injektiv (A also funktional unterscheidbar) ist*
- *$A$ einfach ist, und*
- *$\mathfrak{V}$ halb entartet ist*

**Beweis:** [8] Satz 3

### 2.1.4 Kompositionserweiterung von Polynomfunktionen

Wenden wir uns nun den Polynomfunktionsalgebren zu. Für diese kann wiederum zu jedem Epimorphismus der zugrundeliegenden Algebren eine eindeutiger Kompositionsepimorphismus gefunden werden:

**Proposition 2.1.25** *Sei $k > 0, k \in \mathbb{N}$, $A, B$ Algebren der Varietät $\mathfrak{V}$, $\eta : A \to B$ ein Epimorphismus. Dann kann $\eta$ eindeutig zu einem Kompositionsepimorphismus $\rho : P_k(A) \to P_k(B)$ erweitert werden.*
*Ist $\eta$ ein Isomorphismus, so ist das auch $\rho$.*

**Beweis:** [18] Kapitel 3 Proposition 3.31.

**Definition 2.1.26** *Diesen Kompositionsepimorphismus $\rho : P_k(A) \to P_k(B)$ nennen wir die* **Kompositionserweiterung** *von $\eta$ und bezeichnen ihn mit $P_k(\eta)$:*

$$P_k(\eta)\left(w\left(a_i;\xi_j\right)\right) = w\left(\eta(a_i);\xi_j\right)$$

**Bemerkung:** Es läge auch hier nahe, für jeden Homomorphismus $\varphi$ die Erweiterung $P_k(\varphi)$ zu definieren. Anders als bei der kanonische Erweiterung $\varphi[X]$ gelingt das jedoch nicht. Die Zuordnung $w(a_i;\xi_j) \mapsto w(\varphi(a_i);\xi_j)$ ist im allgemeinen nicht wohldefiniert.

**Beispiel:** Betrachte die Gruppen $H = [\mathbb{Z};+,-,0]$ und $G = [\{0\};+,-,0]$, dann ist $\varphi : G \to H$ mit $\varphi(0) = 0$ klarerweise ein Homomorphismus. Betrachte nun die Darstellungen der einzigen Funktion $f : G \to G$ mit $f(0) = 0$ mittels Wörter: z.B. $0$, $\xi$ und $\xi + \xi$. Diese Wörter induzieren auf $\mathbb{Z}$ jedoch verschiedene Funktionen. Somit ist die Abbildung $w(a_i;\xi_j) \mapsto w(\varphi(a_i);\xi_j)$ auf $P_k(G)^k$ nicht eindeutig. Betrachten wir jedoch $\varphi[X]$ so ist diese Abbildung $\varphi \mapsto \varphi[X]$ wohldefiniert, da diese Wörter auch auf $G[X]$ verschiedene Polynome darstellen.

**Lemma 2.1.27** *Seien A,B Algebren der Varietät $\mathfrak{V}$, $X = \{x_1,\ldots,x_k\}$. Sei $\eta : A \to B$ ein Epimorphsimus. Dann ist*

$$P_k(\eta) \circ \sigma_k[A] = \sigma_k[B] \circ \eta[X]$$

*D.h. das Diagramm in Abbildung 2.1 ist kommutativ.*

**Beweis:** Sei $p = w(a_i;x_j) \in A(X,\mathfrak{V})$. Dann ist

$$\left(P_k(\eta) \circ \sigma_k[A]\right)(p) = P_k(\eta)\left(w(a_i;\xi_j) = w(\eta(a_i);\xi_j\right)$$

Andererseits ist

$$\left(\sigma_k[B] \circ \eta[X]\right)(p) = \sigma_k[B]\left(w\left(\eta(a_i);x_i\right)\right) = w(\eta(a_i);\xi_i)$$

□

**Bemerkung:** Wir können sowohl zu jedem $A$ aus der Varietät $\mathfrak{V}$ $P_k(A)$ bilden, als auch für jedes $\eta \in Epi(A,B)$ $P_k(\varphi)$ finden. Damit ist $P_k(.)$ in der Sprache der Kategorientheorie (siehe dazu Anhang A.5 ) ein kovarianter Funktor zwischen der Kategorie der $\Omega$-Algebren dieser Varietät $\mathfrak{V}$ mit Epimorphismen und sich selbst. Denn für ein beliebiges $p = w(a_i;\xi_j)$, $\varphi \in Epi(B,C), \psi \in Epi(A,B)$ ist

$$P_k\left(\varphi \circ \psi\right)(p) = w((\varphi\circ\psi)(a_i);\xi_j) = w((\varphi(\psi(a_i));\xi_j) = P_k(\varphi)(w(\psi(a_i);\xi_j)) =$$

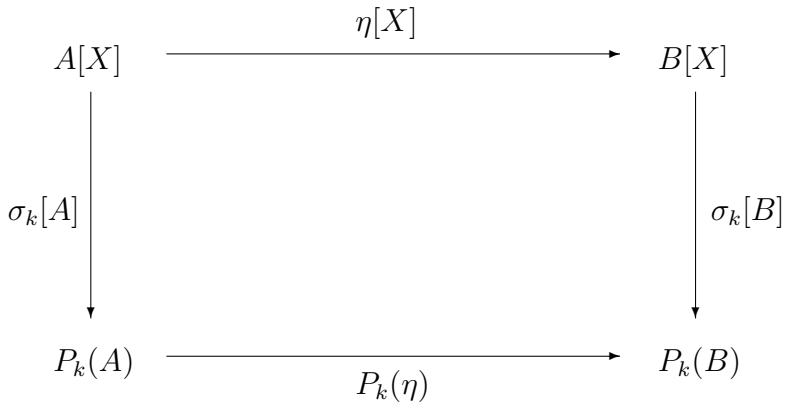


Abbildung 2.1: Die Beziehung zwischen den kanonischen Kompositionserweiterungen von Epimorphismen

$$= P_k(\varphi)\left(P_k(\psi)\left(w(a_i;\xi_j)\right)\right) = \left(P_k(\varphi)\circ P_k(\psi)\right)(p)$$

Somit ist $P_k(\varphi\circ\psi) = P_k(\varphi)\circ P_k(\psi)$. Ebenso zeigt man, dass $(\varphi\circ\psi)[X] = \varphi[X]\circ\psi[X]$. Weiters ist auch klarerweise $P_k(id_A) = id_{P_k(A)}$.

Für $A[X]$ respektive $\varphi[X]$ gilt dasselbe: $.[X]$ ist ein kovarianter Funktor zwischen der Kategorie der $\Omega$-Algebren dieser Varietät $\mathfrak{V}$ mit Epimorphismen und sich selbst. (Dies gilt ja sogar für Algebren mit Homomorphismen.)

Der kanonische Epimorphismus $\sigma_k[.]$ ist, wie aus der Abbildung 2.1 zu erkennen ist, eine natürliche Transformation zwischen diesen beiden Funktoren.

Für $f : A \to B$ bezeichne $f^k : A^k \to B^k$ jene Funktion mit $f^k(a_1,\ldots,a_k) = (f(a_1),\ldots,f(a_k))$. Damit können wir formulieren

**Lemma 2.1.28** *Sei $\eta : A \to B$ ein Epimorphismus, $p \in P_k(A)$ beliebig*

$$\left(P_k\left(\eta\right)\left(p\right)\right)\circ\eta^k = \eta\circ p$$

*D.h. das Diagramm in Abbildung 2.2 ist kommutativ.*

*Es sei $\varphi : A \to B$ ein Homomorphismus und $p \in A[X]$, dann ist*

$$\sigma_k[B]\left(\varphi[X]p\right)\circ\varphi^k = \varphi\circ\sigma_k[A]\left(p\right)$$

**Beweis:** Sei $p = w(a_i;\xi_j)$, dann ist

$$(\eta\circ p)(c_1,\ldots,c_k) = \eta\left(w(a_i;c_j)\right) = w(\eta(a_i);\eta(c_j))$$

Andererseits ist

$$\left(\left(P_k\left(\eta\right)\left(p\right)\right)\circ\eta^k\right)(c_1,\ldots,c_k) = \left(P_k\left(\eta\right)\left(p\right)\right)(\eta(c_1),\ldots,\eta(c_k)) =$$

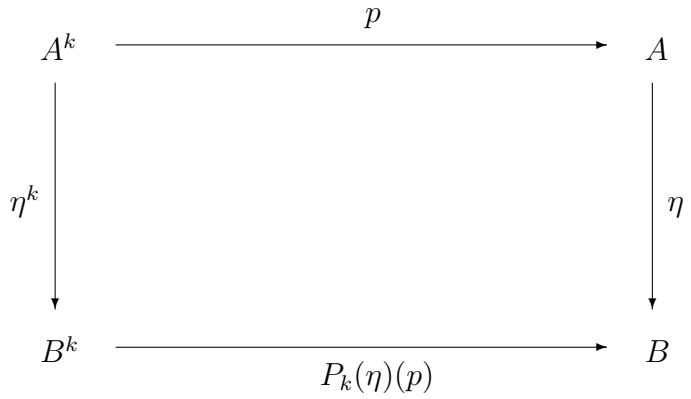


Abbildung 2.2: Die Vertauschung von Polynomen und Epimorphismen

$$= (w(\eta(a_j); \xi_j)\,(\eta(c_1), \ldots, \eta(c_k)) = w(\eta(a_i); \eta(c_j))$$

Der Beweis des zweiten Teils verläuft analog. □

Daraus folgt insbesondere, daß Termfunktionen direkt mit Epimorphismen vertauschen. D.h. sei $t \in T_k(A)$ und $\eta \in Epi(A, B)$ beliebig, dann ist $P_k(\eta)(t) = t$ und somit

$$t \circ \eta^k = \eta \circ t$$

**Lemma 2.1.29** *Durch die Eigenschaft in 2.1.28, d.h. daß* $\forall \eta \in Epi(A, B)$ *gilt*

$$(P_k\,(\eta)\,(p)) \circ \eta^k = \eta \circ p$$

*ist die Abbildung* $P_k : Epi(A, B) \to Hom(P_k(A), P_k(B))$ *eindeutig bestimmt.*

**Beweis:** Sei $\Xi : Epi(A, B) \to Hom(P_k(A), P_k(B))$, sodaß $\forall \eta \in Epi(A, B)$ gilt

$$(\Xi\,(\eta)\,(p)) \circ \eta^k = \eta \circ p$$

Sei $\Xi(p) = w'(b_i; x_j)$ für $p = w(a_i; x_j)$, dann ist für $(c_1, \ldots, c_k) \in A^k$ beliebig

$$\left((\Xi\,(\eta)\,(p)) \circ \eta^k\right)(c_1, \ldots, c_k) = (\eta \circ p)\,(c_1, \ldots, c_k)$$

$$(\Xi\,(\eta)\,(p))\,(\eta(c_1), \ldots, \eta(c_k)) = \eta\,(w(a_i; c_j))$$

$$w'(b_i; \eta(c_j)) = w(\eta(a_i); \eta(c_j))$$

Das gilt $\forall\ (c_1, \ldots, c_k)$. $\eta$ ist nach Voraussetzung surjektiv, also ist $\forall (d_1, \ldots, d_k) \in B^k$

$$w'(b_i; \eta(d_j)) = w(\eta(a_i); \eta(d_j))$$

und somit

$$\Xi(\eta) = w(\eta(a_i); x_j) = P_k(\eta) \ \square$$

Mit dieser Eigenschaft können wir für einen Epimorphismus $\vartheta : A \to B$ eine Abbildung $C_k(A) \to C_k(B)$ definieren:

**Definition 2.1.30** *Sei $\vartheta \in Epi(A, B)$. Dann ist für $f \in C_k(A)$*

$$\left(\left(C_k\left(\vartheta\right)\right)\left(f\right)\right)\left(\vartheta(a_1), \vartheta(a_2), \ldots, \vartheta(a_k)\right) = \vartheta\left(f\left(a_1, \ldots, a_k\right)\right)$$

Diese Abbildung ist wohldefiniert, denn, wenn $\vartheta(a_i) = \vartheta(a_i')$ für $i = 1, \ldots, k$, dann ist $a_i \sim_{Ker(\vartheta)} a_i'$. Da $f$ aber kompatibel ist, gilt somit

$$f(a_1, \ldots, a_k) \sim_{Ker(\vartheta)} f(a_1', \ldots, a_k')$$

also ist $\vartheta\left(f(a_1, \ldots, a_k)\right) = \vartheta\left(f(a_1', \ldots, a_k')\right)$.

Diese Abbildung ist auf $P_k(A)$ identisch mit $P_k(.)$ und somit dort surjektiv. Sie bildet auch $L_tP_k(A)$ nach $L_tP_k(B)$ und $LP_k(A)$ nach $LP_k(B)$ ab, ist dort aber im allgemeinen nicht mehr surjektiv(dazu siehe [3] Abschnitt 2).

### 2.1.5 Dekomposition

Da die $k$-dimensionalen $\mathfrak{V}$-Kompositionsalgebren eine Varietät bilden, ist mit $A, B$ auch $A \times B$ eine $k$-dimensionale $\mathfrak{V}$-Kompositionsalgebra. Insbesondere gilt das für $A[X, \mathfrak{V}] \times B[X, \mathfrak{V}]$ und $P_k(A) \times P_k(B)$, wenn $A, B$ Algebren der Varietät $\mathfrak{V}$ sind und $X = \{x_1, \ldots, x_k\}$.

**Proposition 2.1.31** *Seien $X = \{x_1, \ldots, x_k\}$, A,B Algebren der Varietät $\mathfrak{V}$. Dann gibt es einen eindeutigen Kompositionshomomorphismus $\tau_1$*

$$\tau_1 : \left(A \times B\right)[X, \mathfrak{V}] \to A[X, \mathfrak{V}] \times B[X, \mathfrak{V}]$$

*sodaß $\tau_1\left(\left(A \times B\right)[X, \mathfrak{V}]\right)$ ein subdirektes Produkt von $A[X, \mathfrak{V}]$ und $B[X, \mathfrak{V}]$ ist und $\tau_1$ $A \times B$ elementweise fest läßt, d.h. $\tau_1\left((a, b)\right) = (a, b)$. Für $p \in \left(A \times B\right)[X, \mathfrak{V}]$ gilt $\tau_1(p) = (\xi_1[X](p), \xi_2[X](p))$, wobei $\xi_1, \xi_2$ die Projektionen von $A \times B$ sind.*
*Ebenso existiert ein eindeutiger Kompositionshomomorphismus $\tau_2$*

$$\tau_1 : P_k\left(A \times B\right) \to P_k(A) \times P_k(B)$$

*sodaß $\tau_2\left(P_k\left(A \times B\right)\right)$ ein subdirektes Produkt von $P_k(A)$ und $P_k(B)$ ist und $\tau_2$ $A \times B$ elementweise fest läßt, d.h. $\tau_2\left((a, b)\right) = (a, b)$. Für $p \in P_k\left(A \times B\right)$ gilt $\tau_2(p) = (P_k(\xi_1)(p), P_k(\xi_2)(p))$, wobei $\xi_1, \xi_2$ die Projektionen von $A \times B$ sind.*

**Beweis:** Definieren wir nun also für $p \in (A \times B)[X, \mathfrak{V}]$

$$\tau_1(p) = (\xi_1[X](p), \xi_2[X](p))$$

wobei $\xi_1, \xi_2$ die Projektionen sind. Damit ist $\tau_1$ wohldefiniert,

$$\tau_1 : (A \times B)[X, \mathfrak{V}] \to A[X, \mathfrak{V}] \times B[X, \mathfrak{V}]$$

Es gilt auch, daß $\tau_1((a,b)) = (\xi_1[X]((a,b)), \xi_2[X]((a,b))) = (a,b)$. Sei $\pi_1 : A[X, \mathfrak{V}] \times B[X, \mathfrak{V}] \to A[X, \mathfrak{V}]$ die Projektion. Da $\pi_1 \circ \tau_1(p) = \xi_1[X](p)$ und wir für ein beliebiges $p_1 = w(a_i; x_j) \in A[X, \mathfrak{V}]$ $p = w((a_i, 1); x_j)$ wählen können, ist $\xi_1 \circ \tau_1(p) = p_1$. Also ist $\tau_1((A \times B)[X, \mathfrak{V}])$ ein subdirektes Produkt von $A[X, \mathfrak{V}]$ und $B[X, \mathfrak{V}]$.

Somit bleibt noch die Eindeutigkeit zu zeigen. Sei also $\sigma$ ein weiterer Kompositionshomomorphismus mit diesen Eigenschaften. D.h.

$$\pi_1(\sigma((A \times B)[X, \mathfrak{V}])) = A[X, \mathfrak{V}] \text{ und } \pi_2(\sigma((A \times B)[X, \mathfrak{V}])) = B[X, \mathfrak{V}]$$

und $\sigma$ läßt die Elemente von $A \times B$ fest. Dann ist $\pi_i \circ \sigma$ eine Kompositionserweiterung von $\xi_1 : A \times B \to A$ bzw. $\xi_2 : A \times B \to B$. Wegen der Eindeutigkeit der Kompositionserweiterung ist also $\pi_i \circ \sigma = \xi_i[X]$ . Da jedoch $\sigma(p) = (\pi_1(\sigma(p)), \pi_2(\sigma(p)))$ folgt: $\sigma = \tau_1$.
Für $\tau_2$ verläuft der Beweis analog. □

**Definition 2.1.32** *Wir nennen $\tau_1$ resp. $\tau_2$ den* **Dekompositionshomomorphismus** *von $(A \times B)[X, \mathfrak{V}]$ resp. $P_k(A \times B)$.*

Wie sieht dieser Kompositionshomomorphsimus aus? Wie bildet er ab? Zur besseren Verdeutlichung verwenden wir die Schreibweise $\begin{pmatrix} a \\ b \end{pmatrix}$ für ein Element aus $A \times B$.

Sei $p \in (A \times B)[X, \mathfrak{V}]$, dann ist $p = w(\begin{pmatrix} a_i \\ b_i \end{pmatrix}; x_j)$. Also ist

$$\tau_1(p) = \begin{pmatrix} \xi_1[X](p) \\ \xi_2[X](p) \end{pmatrix} = \begin{pmatrix} w(a_i; x_j) \\ w(b_i; x_j) \end{pmatrix}$$

Ebenso ist für $p = w(\begin{pmatrix} a_i \\ b_i \end{pmatrix}; \xi_j)$ :

$$\tau_2(p) = \begin{pmatrix} P_k(\xi_1)(p) \\ P_k(\xi_2)(p) \end{pmatrix} = \begin{pmatrix} w(a_i; \xi_j) \\ w(b_i; \xi_j) \end{pmatrix}$$

Ist $f : A \to A'$ und $g : B \to B'$, so sei $f \times g : A \times B \to A' \times B'$ die komponentenweise Anwendung von $f$ und $g$ mit $(f \times g)(a,b) = (f(a), g(b))$.

**Lemma 2.1.33** *Seien $A, B$ $\Omega$-algebren der Varietät $\mathfrak{V}$, $X = \{x_1, \ldots, x_k\}$. Sei $\sigma_K[.]$ der kanonische Epimorphismus, $\tau_1, \tau_2$ die Dekompositionshomomorphismen. Dann ist:*

$$\sigma_k[A] \times \sigma_k[B] \circ \tau_1 = \tau_2 \circ \sigma_k[A \times B]$$

*D.h das Diagramm in Abbildung 2.3 ist kommutativ.*

**Beweis:** Das folgt direkt aus Proposition 2.1.31 und der Kommutivität des Diagramms in Abbildung 2.1 □

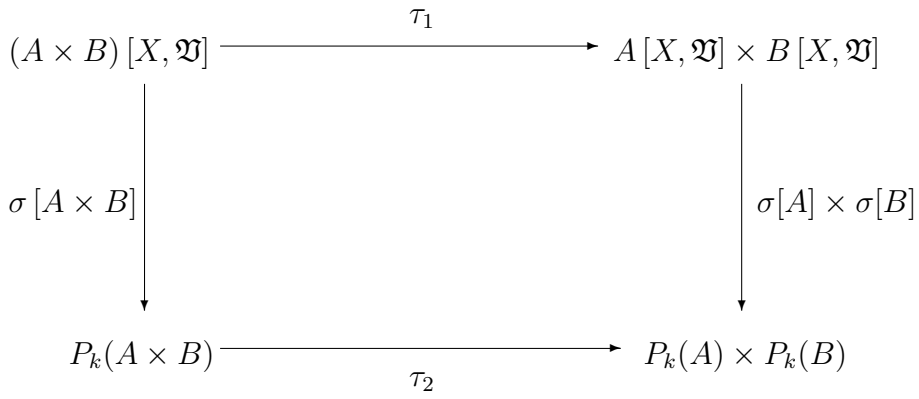


Abbildung 2.3: Dekomposition von Polynomen und Polynomfunktionen

**Lemma 2.1.34** *Sei $p \in P_k(A \times B)$. Dann ist $p = \tau_2(p) \circ (\xi_1^k \times \xi_2^k)$.*
*Sei $p \in (A \times B)[X, \mathfrak{V}]$. Dann ist $\sigma_k[A \times B](p) = (\sigma_k[A] \times \sigma_k[B](\tau_1(p))) \circ (\xi_1^k \times \xi_2^k)$.*

**Beweis:** Sei $p \in P_k(A \times B)[X, \mathfrak{V}]$, sei $w((a_i, b_i); \xi_j)$ eine Darstellung von $p$ als Wort. Dann ist für $((c_1, d_1), \ldots, (c_k, d_k)) \in (A \times B)^k$

$$p((c_1, d_1), \ldots, (c_k, d_k)) = w((a_i, b_i); (c_j, d_j)) \stackrel{*}{=} (w(a_i; c_j), w(b_i; d_j)) =$$

$$= (P_k(\xi_1)(p) \circ \xi_1^k, P_k(\xi_2)(p) \circ \xi_2^k) = \tau_2(p) \circ (\xi_1^k \times \xi_2^k)$$

Die Gleichheit $*$ gilt wegen der Definition der Operationen auf Produkten, sowie der Definition der Wörter.
Die zweite Aussage folgt direkt aus Abbildung 2.3. □

Wann sind die Dekompositionshomomorphismen nun Mono- oder Epimorphismen?

**Proposition 2.1.35** *Sei $X = \{x_1, \ldots, x_k\}$. Der Dekompositionshomomorphismus $\tau_1$ von $(A \times B)[X, \mathfrak{V}]$ ist ein Epimorphismus genau dann, wenn es für alle $(p, q) \in A[X, \mathfrak{V}] \times B[X, \mathfrak{V}]$ ein Wort*

$$w(y_1, \ldots, y_r, x_1, \ldots, x_k) \in W(Y \cup X)$$

*in den Unbestimmten $Y = \{y_1, \ldots, y_r\}$ und Elemente $(a_1, \ldots, a_r)$ und $(b_1, \ldots, b_r)$ gibt, sodaß*

$$w(a_1, \ldots, a_r, x_1, \ldots, x_k) = p, \;\; w(b_1, \ldots, b_r, x_1, \ldots, x_k) = q$$

*Repräsentationen von $p$ und $q$ sind.*
*Der Dekompositionshomomorphismus $\tau_2$ von $P_k(A \times B)$ ist ein Epimorphismus genau dann, wenn es für alle $(p, q) \in P_k(A) \times P_k(B)$ ein Wort*

$$w(y_1, \ldots, y_r, \xi_1, \ldots, \xi_k) \in W(Y \cup \{\xi_i, \ldots, \xi_k\})$$

*in den Unbestimmten $Y = \{y_1, \ldots, y_r\}$ und Elemente $(a_1, \ldots, a_r)$ und $(b_1, \ldots, b_r)$ gibt, sodaß*

$$w(a_1, \ldots, a_r, \xi_1, \ldots, \xi_k) = p, \;\; w(b_1, \ldots, b_r, \xi_1, \ldots, \xi_k) = q$$

*Darstellungen von $p$ und $q$ als Wörter sind.*

**Beweis:** [18] Kapitel 3, Proposition 3.51.

**Bemerkung:** Aus der Abbildung 2.3 folgt sofort, daß $\tau_2$ ein Epimorphismus ist, wenn $\tau_1$ einer ist.

**Proposition 2.1.36** *Der Dekompositionshomomorphismus $\tau_2$ ist immer ein Monomorphismus.*

**Beweis:** Sei $p, q \in P_k(A \times B)$. Sei $\tau_2(p) = \tau_2(q)$. Nach 2.1.34 ist

$$p = \tau_2(p) \circ (\xi_1^k \times \xi_2^k) = \tau_2(q) \circ (\xi_1^k \times \xi_2^k) = q$$

□

**Bemerkung:** In der Varietät der kommutativen Ringe mit Eins sind beide Dekompositionshomomorphismen Isomorphismen. In der Varietät der Gruppen leider nicht, als Ergebnis in dieser Richtung kann dort z.B. 3.2.15 formuliert werden.

Allgemeiner kann man für jede Funktion $f \in F_k(A \times B)$ so eine Dekompositionsabbildung $\mu : F_k(A \times B) \to F_k(A) \times F_k(B)$ definieren:

$$(\mu(f))((a_1, \ldots, a_k), (b_1, \ldots, b_k)) = f((a_1, b_1), \ldots, (a_k, b_k))$$

Die Abbildung $\mu$ ist immer ein Monomorphismus. Diese Abbildung eingeschränkt auf $P_k(A \times B)$ ist gerade $\tau_2$ wie wir aus 2.1.34 ersehen können. Aber sie bildet nicht nur Polynomfunktionen auf Polynomfunktionen ab, sondern auch die Menge der kompatiblen Funktionen $C_k(A \times B)$ in $C_k(A) \times C_k(B)$ ab. Ist sie auf $P_k(A \times B)$ bijektiv, so gilt für die lokalen Polynomfunktionen:

**Proposition 2.1.37** *Ist $\tau_2 = \mu|_{P_k(A \times B)}$ ein Isomorphismus, so bildet $\forall t$ $\mu|_{L_t P_k(A \times B)}$ $L_t P_k(A \times B)$ isomorph auf $L_t P_k(A) \times L_t P_k(B)$ ab. Ebenso bildet $\mu|_{LP_k(A \times B)}$ $LP_k(A \times B)$ isomorph auf $LP_k(A) \times LP_k(B)$ ab.*

**Beweis** [3] Satz 2

Nennen wir die Elemente $L_t P_k(A)$, $LP_k(A)$ und $P_k(A)$ aus der Kette

$$P_k(A) \subseteq LP_k(A) \subseteq \ldots \subseteq L_t P_k(A) \ldots \subseteq L_2 P_k(A) \subseteq K_k(A) \subseteq F_k(A)$$

*P-Elemente* so kann man aus dem vorherigen Satz folgern:

**Korollar 2.1.38** *Für $A \times B$ gilt: Zwei P-Elemente von $A \times B$ sind gleich, genau dann, wenn diese zwei P-Elemente von $A$ und von $B$ gleich sind.*

**Beweis:** [3] Korollar 1

Also gilt etwa

$$L_t P_k(A \times B) = LP_k(A \times B) \iff L_t P_k(A) = LP_k(A) \text{ und } L_t P_k(B) = LP_k(B)$$

## 2.2 Funktions- und Polynommatrizen

**Definition 2.2.1** *Sei $\mathfrak{V}$ eine Varietät, $\Omega$ die Menge von Operatoren, sei $k \geq 1$ fest. Sei $[A; \Omega, \chi]$ eine k-dimensionale $\mathfrak{V}$-Kompositionsalgebra, dann definieren wir eine Operation $\circ$ auf $A^k$*

$$(a_1, \ldots, a_k) \circ (b_1, \ldots, b_k) = (\chi(a_1, b_1, \ldots, b_k), \ldots, \chi(a_k, b_1, \ldots, b_k))$$

Damit wird mit $A$ auch $A^k$ eine Kompositionsalgebra mit den folgenden Eigenschaften, die alle sehr leicht bestätigt werden können:

**Satz 2.2.2** *Sei $A$ eine k-dimensionale $\mathfrak{V}$-Kompositionsalgebra, dann ist die Algebra $\left[A^k;\Omega,\circ\right]$ eine 1-dimensionale $\mathfrak{V}$-Kompositionsalgebra. $A^k$ hat ein Selektorsystem genau dann, wenn $A$ eines hat. Für jeden Homomorphismus $\rho \in Hom(A,B)$ ist die Abbildung $\rho^k : A^k \to B^k$ ein Homomorphismus. Weiters ist $id_A^k = id_{A^k}$. Ist $\sigma : B \to C$ ein Homomorphismus, so ist $(\sigma \circ \rho)^k = \sigma^k \circ \rho^k$. $\rho^k$ ist injektiv, surjektiv oder bijektiv genau dann, wenn das $\rho$ ist.*

$(.)^k$ ist somit ein kovarianter Funktor von der Kategorie der k-dimensionalen $\mathfrak{V}$-Kompositionsalgebren in jene der 1-dimensionalen $\mathfrak{V}$-Kompositionsalgebren.

Auch das nächste Lemma kann sehr leicht bewiesen werden. Die erste Aussage ist offensichtlich, die zweite kann direkt durchgerechnet werden.

**Lemma 2.2.3** *Sei $A$ eine k-dimensionalen $\mathfrak{V}$-Kompositionsalgebra, $B \preceq A$, dann ist $B^k \preceq A^k$. Ist weiters $C$ eine k-dimensionalen $\mathfrak{V}$-Kompositionsalgebra, dann ist die Abbildung $\psi : (A \times B)^k \to A^k \times B^k$ definiert durch*

$$\psi\left((a_1,b_1),\ldots,(a_k,b_k)\right) = \left((a_1,\ldots,a_k),(b_1,\ldots,b_k)\right)$$

*ein Isomorphismus.*

Betrachten wir nun die „natürlichsten“ $\mathfrak{V}$-Kompositionsalgebren, die Funktionsalgebra mit der Komposition.

**Definition 2.2.4** *Seien $i,k \in \mathbb{N}$ und $p_1,p_2,\ldots,p_k \in F(X)(T_k(A), A[X,\mathfrak{V}]$ resp. $P_k(A))$. Dann nennen wir das i-Tupel $(p_1,p_2,\ldots,p_i)$ die* **Termmatrix** *(* **Termfunktionsmatrix** *,* **Polynommatrix** *resp.* **Polynomfunktionsmatrix** *der Dimension $i \times k$ über $A$. Die Menge aller dieser Matrizen bezeichnen wir mit $F(X)$, $T_k^i(A)$ , $A[X,\mathfrak{V}]^i$ resp. $P_k^i(A)$ .*

Wir nennen diese Tupel Matrizen und nicht Vektoren (wie z.B. in [18]), da es für Gruppen einen Kompositionshomomorphismus zwischen $A[X,\mathfrak{V}]^i$ und $M_{i\times k}(\mathbb{Z})$ gibt, siehe 3.2.5 .

Wir können nun jeder Funktionsmatrix auf natürliche Weise eine Funktion $A^k \to A^i$ zuordnen:

**Definition 2.2.5** *Sei $\mathfrak{f} \in F_k(A)^i$. Damit ist $\mathfrak{f} = (f_1,f_2,\ldots,f_i)$ mit $f_j \in F_k(A)$ für $j = 1,\ldots,i$. Dann sei:*

$$\widehat{\mathfrak{f}}(a_1,a_2,\ldots,a_k) := \begin{pmatrix} f_1(a_1,a_2,\ldots,a_k) \\ f_2(a_1,a_2,\ldots,a_k) \\ \vdots \\ f_i(a_1,a_2,\ldots,a_k) \end{pmatrix}$$

*Es ist* $\widehat{\mathfrak{f}} : A^k \to A^i$. *Insbesondere ist mit* $\mathfrak{f} \in F_k(A)^k$ *ist* $\widehat{\mathfrak{f}} \in F_1(A^k)$. *Die Abbildung* $\pi_j : \mathfrak{f} \mapsto f_j$ *sei für* $j = 1, \ldots, i$ *die (kanonische) Projektion mit* $(\pi_j(\mathfrak{f}))(a_1, \ldots, a_i) = \xi_j(\mathfrak{f}(a_1, \ldots, a_i)) = f_j$, *wobei die* $\xi_j$ *die Projektionen von* $A^i$ *nach* $A$ *sind.*
*Wir nennen die* $f_j = \pi_j(\mathfrak{f})$ *die* **Koordinatenfunktionen** .

Die Abbildung $\widehat{\ }$ kann nun natürlich auf Teilmengen von $F_k(A)^i$ angewendet werden, wie z.B. $K_k(X)^i$ oder $P_k^i(A)$.

**Beispiel:** Betrachten wir den Ring mit Eins der ganzen Zahlen, $[\mathbb{Z}; +, -, 0, \cdot, 1]$, dann sei

$$\mathfrak{p} = \begin{pmatrix} x_1 \cdot x_2^2 \\ 1 \\ x_1 + 8 \end{pmatrix}$$

$\mathfrak{p}$ ist somit ein Element aus $P_2^3(\mathbb{Z})$, somit ist $\widehat{\mathfrak{p}} : \mathbb{Z}^2 \to \mathbb{Z}^3$:

$$\widehat{\mathfrak{p}}(y_1, y_2) = \begin{pmatrix} y_1 \cdot y_2^2 \\ 1 \\ y_1 + 8 \end{pmatrix}$$

Ist $i = k$ so geht die Abbildung $\widehat{\ }$ von $F_k(A)^k$ nach $F_1(A^k)$ und es gilt offensichtlich

**Proposition 2.2.6** *Die Abbildung* $\mathfrak{p} \mapsto \widehat{\mathfrak{p}}$ *mit* $\widehat{\ } : F_k(A)^k \to F_1(A^k)$ *ist ein Kompositionsisomorphismus.*

**Definition 2.2.7** *Die Umkehrung der Abbildung* $\widehat{\ }$ *stellen wir symbolisch mit* $\widetilde{\ }$ *dar.*

Es gilt sicher $P_1\left(A^k\right) \preceq \widehat{P_k(A)^k}$, da ja $\widehat{P_k(A)^k} \preceq F_1\left(A^k\right)$ und $\widehat{P_k(A)^k}$ alle konstanten Funktionen und die Projektionen enthält. Im allgemeinen sind das jedoch echte Inklusionen.
Ist $\eta \in Epi(A, B)$ so gilt für $P_1(\eta^k) : P_1(A^k) \to P_1(B^k)$, daß $P_1(\eta^k) = \left(\widehat{\ } \circ P_k(\eta)^k \circ \widetilde{\ }\right)\big|_{P_1(A^k)}$.

Wir können nun $\widehat{\ }$ auf die Funktionen und Mengen von Abbildung 2.1 anwenden und das Funktionsdiagramm bleibt kommutativ. D.h

$$P_k(\eta)^k \circ \sigma_k(A)^k = \sigma_k(B)^k \circ \eta[X, \mathfrak{V}]^k$$

Wir können nun die Dekompositionshomomorphsimen $\tau_1$ und $\tau_2$ betrachten, dann können wir $\tau_1^k$ und $\tau_2^k$ bilden. Nach 2.2.3 gibt es Isomorphismen $\psi_1 : (A[X, \mathfrak{V}] \times B[X, \mathfrak{V}])^k \to A[X, \mathfrak{V}]^k \times B[X, \mathfrak{V}]^k$ und $\psi_2 : (P_k(A) \times P_k(B))^k \to P_k(A)^k \times P_k(B)^k$.

**Proposition 2.2.8** *Der Homomorphismus* $\left(\psi_2 \circ \tau_2^k\right) : P_k\left(A \times B\right)^k \to P_k(A)^k \times P_k(B)^k$ *ist immer ein Monomorphismus.*
*Das Diagramm in Abbildung 2.4 ist kommutativ.*
*Sei* $\mathfrak{p} \in P_k^k(A \times B)$*, dann ist*

$$\mathfrak{p} = \tau_2^k(\mathfrak{p}) \circ (\xi_1^k \times \xi_2^k) = \left(P_k(\xi_1)^k(\mathfrak{p}) \circ \xi_1\right) \times \left(P_k(\xi_2)^k(\mathfrak{p}) \circ \xi_2\right)$$

$$\begin{array}{ccc}
((A \times B)[X, \mathfrak{V}])^k & \xrightarrow{\psi_1 \circ \tau_1^k} & (A[X, \mathfrak{V}])^k \times (B[X, \mathfrak{V}])^k \\
\Big\downarrow \sigma^k[A \times B] & & \Big\downarrow \sigma^k[A] \times \sigma^k[B] \\
P_k^k(A \times B) & \xrightarrow[\psi_2 \circ \tau_2^k]{} & P_k(A)^k \times P_k^k(B)
\end{array}$$

Abbildung 2.4: Dekomposition von Polynom- und Polynomfunktionsmatrizen

**Beweis:** [18] Kapitel 3, Bemerkung 11.22

**Bemerkung:** Für die Varietät der kommutativen Ringe mit Eins sind die beiden Abbildungen $\psi_2 \circ \tau_2^k$ und $\psi_1 \circ \tau_1^k$ Isomorphismen.

## 2.3 Permutationspolynome und Polynompermutationen

Ist $A \in \mathfrak{V}$ und $X = \{x_1, x_2, \ldots, x_k\}$. Dann sind die Algebren $\left[A[X, \mathfrak{V}]^k, \circ\right]$, $\left[F_k(A)^k, \circ\right]$, $\left[K_k(A, \mathfrak{M})^k, \circ\right]$ und $\left[P_k(A)^k, \circ\right]$ Halbgruppen. All diese Mengen besitzen ein Selektorsystem, haben also Einheiten. Die Einheiten einer Menge $M$ bezeichen wir mit $\mathcal{E}(M)$, die Menge der kürzbaren Elemente mit $\mathcal{C}(M)$ ( siehe A.8.1 für Definitionen und Eigenschaften).

Sei für beliebiges $A$ $\mathbb{S}_A = \{f : A \to A, f \textit{ bijektiv}\}$, dann gilt

**Lemma 2.3.1** *Es gilt*

$$\mathcal{E}(\widehat{F_k(A)^k}) = \mathcal{C}(\widehat{F_k(A)^k}) = \mathbb{S}_{A^k}$$

*Daraus folgt*

$$\mathcal{E}(F_k(A)^k) = \mathcal{C}(F_k(A)^k) = \widetilde{\mathbb{S}_{A^k}}$$

**Beweis:** Da $\widehat{\ }$ ein Kompositionsisomorphismus ist, ist es insbesondere ein Isomorphismus von Halbgruppen, also ist

$$\mathcal{E}(\widehat{F_k(A)}^k) = \mathcal{E}(F_1(A^k)) \text{ und } \mathcal{C}(\widehat{F_k(A)}^k) = \mathcal{C}(F_1(A^k))$$

Jedes Element aus $\mathbb{S}_{A^k}$ hat ein Inverses in $F_1(A^k)$ ist also Element aus $\mathcal{E}(F_1(A^k)$, also $\mathbb{S}_{A^k} \subseteq \mathcal{E}(F_1(A^k))$. Jedes kürzbare Element $f$ von $F_1(A^k)$ ist eine Permutation, also $\mathcal{C}(F_1(A^k)) \subseteq \mathbb{S}_{A^k}$. Denn aus den Bedingungen für die Kürzbarkeit folgt einerseits die Injektivität: Sei $f(\mathfrak{a}_1) = f(\mathfrak{a}_2)$, d.h. $f \circ \mathfrak{a}_1 = f \circ \mathfrak{a}_2 \Longrightarrow \mathfrak{a}_1 = \mathfrak{a}_2$ als Funktionen, somit jedoch auch als Elemente.

Andererseits gilt auch die Surjektivität, denn wähle ein $\mathfrak{a}_0 \in A^k$ beliebig, dann sei $id_{A^k}$ die Identität und $g : A^k \to A^k$ mit $g(x) = \begin{cases} x & x \in f(A^k) \\ \mathfrak{a}_0 & sonst \end{cases}$. Dann ist $id_{A^k} \circ f = g \circ f$, somit $id_{A^k} = g$ und nach Definition von $g$ ist $f$ surjektiv.

Ingesamt gilt also

$$\mathbb{S}_{A^k} \subseteq \mathcal{E}(\widehat{F_k(A)}^k \subseteq \mathcal{C}(\widehat{F_k(A)}^k \subseteq \mathbb{S}_{A^k}$$

□

**Definition 2.3.2** *Eine Polynommatrix ($\in M \subseteq A[X]^k$) resp. eine Funktionsmatrix ($\in M \subseteq F_k(A)^k$) heißt* **invertierbar in** *$M$ , wenn es Element von $\mathcal{E}(M)$ ist.*

**Definition 2.3.3** *Die Menge der* **Polynompermutationen** *ist $U_k(A) = P_k(A)^k \cap \widehat{\mathbb{S}_{A^k}}$. Letztere sind also jene Polynomfunktionsmatrizen, die als Funktionen von $A^k$ nach $A^k$ Permutationen sind.*
*Die Menge der* **Permutationspolynome** *ist $U_{[X]}(A) = \sigma_k[A]^{-1}(U_k(A))$.*

**Lemma 2.3.4** *Es gilt $\mathcal{E}(P_k(A)) \subseteq U_k(A) \subseteq \mathcal{C}(P_k(A))$*
*Ist $A$ endlich, so gilt hier die Gleichheit. Damit ist $U_k$ eine Gruppe.*

**Beweis:** Da $P_k(A)^k \subseteq F_k(A)^k$ folgt aus A.8.5

$$\mathcal{E}(P_k(A)^k) \subseteq \mathcal{E}(F_k(A)^k) \cap P_k(A)^k = \widetilde{\mathbb{S}_{A^k}} \cap P_k(A)^k =$$

$$= \mathcal{C}(F_k(A)^k) \cap P_k(A)^k \subseteq \mathcal{C}(P_k(A)^k)$$

Die Gleichheit bei Endlichkeit folgt aus A.8.5 und aus der Tatsache, daß mit $A$ auch $P_k(A)^k$ endlich ist. □

Die Inklusionen hier sind im allgemeinen echt! Sei $k = 1$ dann betrachten wir die Menge der reellen Zahlen $\mathbb{R}$ aufgefaßt als kommutativen Ring mit Eins. Dann ist das Element $\xi_1^3 \in P_1(A)$ sicher nicht in $\mathcal{E}(P_1(A))$, aber in $U_1(A)$. Andererseits sei wieder $k = 1$, $A = \mathbb{Z} = F(\{a\})$ die unendliche zyklische Gruppe, dann ist $\xi_1^2 \notin U_1(A)$ aber $\xi_1^2 \in \mathcal{C}(P_1(A))$.

Betrachten wir den kanonischen Epimorphismus $\sigma_k[A] : A[X, \mathfrak{V}] \to P_k(A)$, so gilt klarerweise $\mathcal{E}(A[X, \mathfrak{V}]) \subseteq \sigma_k[A]^{-1}(\mathcal{E}(P_k(A))) \subseteq \sigma_k[A]^{-1}(U_k(A)) \subseteq \sigma_k[A]^{-1}(\mathcal{C}(P_k(A)))$. Bei Endlichkeit gilt Gleichheit der letzen drei Inklusionen.

Seien $A$,$B$ Algebren aus $\mathfrak{V}$ und $\eta : A \to B$ ein Epimorphismus. Dann ist $P_k(\eta)^k : P_k(A)^k \to P_k(B)^k$ wieder ein Epimorphismus. Wir können uns nun fragen, wie er $\mathcal{E}(P_k(A)^k)$, $\mathcal{C}(P_k(A)^k)$ bzw. $U_k(A)$ abbildet. Es gilt

**Proposition 2.3.5** *Seien $A$,$B$ Algebren der Varietät $\mathfrak{V}$. Sei $\eta \in Epi(A, B)$. Dann ist*

1. $P_k(\eta)^k(\mathcal{E}(P_k(A)) \subseteq \mathcal{E}(P_k(B))$
2. *Ist $\eta$ ein Isomorphismus, so bildet $P_k(\eta)^k$ die Halbgruppen $\mathcal{E}(P_k(A))$, $\mathcal{C}(P_k(A))$ respektive $U_k(A)$ isomorph auf $\mathcal{E}(P_k(B))$, $\mathcal{C}(P_k(B))$ respektive $U_k(B)$ ab.*
3. *Ist $B$ endlich, so ist $P_k(\eta)^k(U_k(A)) \subseteq U_k(B)$.*

**Beweis:** Seien $\mathfrak{p}, \mathfrak{q} \in \mathcal{E}(P_k(A))$, sodaß

$$\mathfrak{p} \circ \mathfrak{q} = \mathfrak{q} \circ \mathfrak{p} = \mathfrak{x}$$

Da $P_k(\eta)$ und somit auch $P_k(\eta)^k$ ein Kompositionsepimorphismus ist, gilt

$$P_k(\eta)^k(\mathfrak{p} \circ \mathfrak{q}) = P_k(\eta)^k(\mathfrak{q} \circ \mathfrak{p}) = P_k(\eta)^k(\mathfrak{x})$$

$$P_k(\eta)^k(\mathfrak{p}) \circ P_k(\eta)^k(\mathfrak{q}) = P_k(\eta)^k(\mathfrak{q}) \circ P_k(\eta)^k(\mathfrak{p}) = \mathfrak{x}$$

Also gilt Punkt 1.

Sei nun $\mathfrak{p} \in U_k(A)$. Es gibt für alle $(b_1, \ldots, b_k)$ Elemente $(a_1, \ldots, a_k)$ sodaß $(b_1, \ldots, b_k) = (\eta(a_1), \ldots, \eta(a_k))$. Es folgt

$$P_k(\eta)^k(\mathfrak{p})(b_1, \ldots, b_k) = P_k(\eta)^k(\mathfrak{p})(\eta(a_1), \ldots, \eta(a_k)) \overset{2.1.28}{=} (\eta^k \circ p)(a_1, \ldots, a_k)$$

Ist nun $\eta$ ein Isomorphismus so ist

$$P_k(\eta)^k(\mathfrak{p})(b_1,\ldots,b_k) = (\eta^k \circ p \circ (\eta^{-1})^k)(b_1,\ldots,b_k)$$

Also ist mit $p$ und $\eta$ auch $P_k(\eta)^k(\mathfrak{p})$ bijektiv. Weiters ist $P_k(\eta)^k$ ein (Halbgruppen)Isomorphismus, also gilt

$$P_k(\eta)^k(\mathcal{E}(P_k(A)^k)) = \mathcal{E}(P_k(B)^k)$$

und

$$P_k(\eta)^k(\mathcal{C}(P_k(A)^k)) = \mathcal{C}(P_k(B)^k)$$

Damit ist Punkt 2 gezeigt!
Ist $B$ endlich, so ist klarerweise $P_k(\eta)^k(\mathfrak{p}) : B^k \to B^k$ surjektiv. Da $B$ und somit auch $B^k$ endlich sind, ist also $P_k(\eta)^k(\mathfrak{p})$ injektiv. Damit ist $P_k(\eta)^k(\mathfrak{p}) \in U_k(B)$. Also gilt Punkt 3. □

Wir können nun wieder das Produkt $A \times B$ betrachten und uns fragen wie der Monomorphismus $\psi_2 \circ \tau_2^k : P_k^k(A \times B) \to P_k(A)^k \times P_k^k(B)$ die Halbgruppen $\mathcal{E}(P_k(A \times B))$, $\mathcal{C}(P_k(A \times B))$ respektive $U_k(A \times B)$ abbildet.

**Proposition 2.3.6** *Seien A,B Algebren der Varietät $\mathfrak{V}$. Dann ist*

$$\left(\psi_2 \circ \tau_2^k\right)\left(\mathcal{E}\left(P_k^k(A \times B)\right)\right) \subseteq \mathcal{E}\left(P_k^k(A)\right) \times \mathcal{E}\left(P_k^k(B)\right)$$

$$\left(\psi_2 \circ \tau_2^k\right)\left(\mathcal{C}\left(P_k^k(A \times B)\right)\right) \subseteq \mathcal{C}\left(P_k^k(A)\right) \times \mathcal{C}\left(P_k^k(B)\right)$$

*Ist $\psi_2 \circ \tau_2^k$ ein Isomorphismus, so gilt in diesen beiden Fällen Gleichheit.*

*Für die Polynompermutationen gilt*

$$\left(\psi_2 \circ \tau_2^k\right)(U_k(A \times B))) = (U_k(A) \times U_k(B)) \cap \left(\psi_2 \circ \tau_2^k\right)(P_k^k(A \times B))$$

*Ist $\psi_2 \circ \tau_2^k$ ein Isomorphismus, so gilt*

$$\left(\psi_2 \circ \tau_2^k\right)(U_k(A \times B))) = (U_k(A) \times U_k(B))$$

**Beweis:** [18] Kapitel 3, Proposition 11.61. , Proposition 11.63 und Proposition 11.64

# Kapitel 3

# Polynome, Polynomfunktionen und deren Komposition über Gruppen

## 3.1 Spezialisierung auf Gruppen

Wir wollen noch einmal wiederholen

**Definition 3.1.1** *Eine Gruppe ist eine Algebra mit* $\Omega = \{\cdot, ^{-1}, 1\}$ *als Operationen vom Typ* $\{2, 1, 0\}$ *und den geltenden Gesetzen*

- $x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$
- $x_1 \cdot 1 = x_1$
- $x_1 \cdot {x_1}^{-1} = 1$

*Eine abel'sche Gruppe ist eine Gruppe, die auch dem Gesetz*

- $x_1 \cdot x_2 = x_2 \cdot x_1$

*genügt.*

Wollen wir das Einselement der Gruppe $G$ deutlich von jenem der ganzen Zahlen unterscheiden, so bezeichen wir es als $e$.

Die Operationen der Gruppe können auch additiv angeschrieben werden: $\Omega = \{+, -, 0\}$.

Die Klasse der Gruppen bildet eine nicht vollständig entartete, nicht halb entartete Varietät $\mathfrak{Grp}$, da es Gruppen gibt, die nicht nur die 1 enthalten (z.B.

$[\mathbb{Z}, +, -, 0]$), jedoch alle Gruppen $\{1\}$ als Untergruppe enthalten. Die Klasse der abelschen Gruppen bilden eine (nicht vollständig, nicht halb entartete) Varität, $\mathfrak{Grp}_{\mathfrak{ab}}$.

Damit sind nach Prop. 1.2.2 für Gruppen in $A[X, \mathfrak{V}]$ alle Elemente aus $A \cup X$ unterschiedlich. Wir werden die Polynomalgebra $G[X, \mathfrak{Grp}]$ über der Gruppe $G$ mit $G[X]$ bezeichnen.

**Proposition 3.1.2** *Die Kongruenzen der Varietät* $\mathfrak{Grp}$ *sind genau die durch Normalteiler induzierten Relationen.*

**Beweis:** Sei $K$ Kongruenz auf $G$: $a_i \sim_K b_i \Longrightarrow a_1 \cdot a_2 \sim_K b_1 \cdot b_2 \wedge a_1^{-1} \sim_K b_1^{-1}$. Sei $N$ die Kongruenzklasse von 1, also $N = C(1) \subseteq G$. Seien $a, b \in N \Longrightarrow a \sim_K 1, b \sim_K 1 \Longrightarrow a \cdot b \sim_k 1 \cdot 1 = 1$, $a^{-1} \sim_k 1^{-1} = 1$ also ist $N \preceq G$. Sei nun $c \in G \Longrightarrow c \cdot a \sim_K c \cdot 1 = c \Longrightarrow c \cdot a \cdot c^{-1} \sim_K c \cdot c^{-1} = 1$. Also ist $c \cdot N \cdot c^{-1} \subseteq N$ und damit $N \trianglelefteq G$.
Die Umkehrung gilt wegen A.8.12. □

Wie stehen die Untergruppen und Normalteiler von $G$ und $G[X]$ (bzw. $P_k(G)$) in Beziehung zueinander? Es läßt sich zumindest vermuten, daß es einen Zusammenhang gibt.

Ein einfacher Zusammenhang kann folgendermaßen formuliert werden. Dafür sei für $\mathfrak{A} \subseteq G[X]$ und für beliebiges $g \in G$ $\mathfrak{A} \circ g = \{\sigma_k[G](\mathfrak{p})(g) | \mathfrak{p} \in \mathfrak{A}\}$.

**Proposition 3.1.3** *Es sei $G$ eine Gruppe. Ist $\mathfrak{A} \preceq G[X]$ , so ist $\mathfrak{A} \circ g \preceq G$ $\forall g \in G$.*

*Ist $\mathfrak{A} \trianglelefteq G[X]$, so ist $\mathfrak{A} \circ g \trianglelefteq G$ $\forall g \in G$.*

**Beweis:** Sei $\mathfrak{A} \preceq G[X]$ und $g \in G$ beliebig. Seien $a, b \in \mathfrak{A} \circ g$, also gibt es $p_1, p_2 \in \mathfrak{A}$, sodaß $p_1(g) = a$ und $p_2(g) = b$, also ist

$$a \cdot b^{-1} = p_1(g) \cdot (p_2(g))^{-1} = (p_1 \cdot p_2^{-1})(g) \in \mathfrak{A} \circ g$$

Ist zusätzlich $\mathfrak{A} \trianglelefteq G[X]$, dann gilt für beliebiges $g_1$ in $G$, daß

$$g_1 \cdot a \cdot g_1^{-1} = g_1 \circ p_1(g) \circ g_1^{-1} = (g_1 \cdot p_1 \cdot g_1^{-1})(g) \in \mathfrak{A} \circ g$$

□

Aus diesem Beweis sieht man sofort, daß eine analoge Eigenschaft für $P_k(G)$ gilt.

Andererseits folgt durch 1.2.3 klarerweise aus $G' \preceq G$, daß $G'[X] \preceq G[X]$ ist.

### 3.1.1 Normalformen bezüglich $G[X]$

Können wir ein Normalformsystem (siehe Abschnitt 1.2.2) für $G[X]$ finden? D.h. ein System von Wörtern, das alle Polynome eindeutig beschreibt?

**Satz 3.1.4** *Sei $G \in \mathfrak{Grp}$. Die Wörter $a_0x^{n_1}a_1x^{n_2}...a_{r-1}x^{n_r}a_r$ mit $r \in \mathbb{N}$, $n_i \in \mathbb{Z}, n_i \neq 0$, $a_t \in G$ für $t = 0, 1, ..., r$, und $a_t \neq 1$ für $t = 1, 2, ..., r-1$ bilden ein Normalformsystem für $G[x]$.*

**Beweis:** 1.) Wir zeigen zuerst mittels Induktion nach dem Rang $r(w)$ des Wortes $w$, das das Polynom $p$ repräsentiert, daß jedes $p$ so dargestellt werden kann, d.h. $w$ zu einem Wort aus diesem System äquivalent ist.

Sei $r(w) = 0$, dann ist $p = a$ oder $p = x$, der erste Fall ist eine gesuchte Darstellung, im zweiten Fall können wir mit $p = 1 \cdot x \cdot 1$ eine finden.

Sei nun also $p = w_1 \cdot w_2$ oder $p = w_1^{-1}$ mit $r(w_i) < n$ und angenommen für diese Ränge ist die Behauptung gezeigt. Sei also $w_1 = a_0x^{n_1}a_1x^{n_2}...a_{r-1}x^{n_r}a_r$, $w_2 = b_0x^{m_1}b_1x^{m_2}...b_{r-1}x^{m_r}b_r$. Ist $p = w_1^{-1}$, so ist

$$p = a_r^{-1}x^{-n_r}a_{r-1}^{-1}x^{-n_{r-1}}...a_1^{-1}x^{-n_1}a_0^{-1}$$

und damit konnten wir eine Darstellung finden.

Ist $p = w_1 \cdot w_2$, dann können wir

$$p = (a_0x^{n_1}a_1x^{n_2}...a_{r-1}x^{n_r}a_r) \cdot (b_0x^{m_1}b_1x^{m_2}...b_{r-1}x^{m_r}b_r) =$$

$$= a_0x^{n_1}a_1x^{n_2}...a_{r-1}x^{n_r}\,(a_r \cdot b_0)\,x^{m_1}b_1x^{m_2}...b_{r-1}x^{m_r}b_r$$

durch Anwenden der Gesetze in die gewünschte Form bringen ("Kürzen"). Denn ist (1. Schritt) $a_r \cdot b_0 \neq 1$ so haben wir so eine Darstellung gefunden, ist $a_r \cdot b_0 = 1$, so ist $a_{r-1}x^{n_r}\,(a_r \cdot b_0)\,x^{m_1}b_1 = a_{r-1}x^{n_r+m_1}b_1$. Ist $n_r \neq -m_1$, so haben wir eine Darstellung gefunden, ansonsten ist $a_{r-1}x^{n_r+m_1}b_1 = a_{r-1} \cdot b_1$ und wir können hier wiederum den 1. Schritt anwenden. Diese Vorgehensweise ist endlich, da von $a_r$ auf $a_{r-1}$ und von $b_0$ auf $b_1$ übergegangen wird, d.h. das Kürzen kann maximal $r$ mal durchgeführt werden. Also gibt es für jedes $p$ eine angegebene Darstellung.

2.) Nun bleibt noch zu zeigen, daß diese Darstellung eindeutig ist. Wir suchen eine Menge in die $G[x]$ abgebildet werden kann, in der die Unterscheidung aber eindeutig ist. Betrachten wir $p = a_0x^{n_1}a_1x^{n_2}...a_{r-1}x^{n_r}a_r$, so bietet sich die Darstellung als Folge $(a_0, n_1, a_1, n_2, ..., a_{r-1}, n_r, a_r)$ an.
Wir betrachten nun also die Menge

$$S = \{(a_0, n_1, a_1, n_2, ..., a_{r-1}, n_r, a_r)|$$

$$r \in \mathbb{N}, a_i \in G, a_i \neq 1 \text{ für } i = 1, \ldots, r-1; n_i \in \mathbb{N}\}$$

und definieren darauf eine Operation $\cdot$. Das Ergebnis von

$$(a_0, n_1, a_1, n_2, ..., a_{r-1}, n_r, a_r) \cdot (b_0, m_1, b_1, m_2, ..., b_{s-1}, m_s, b_s)$$

ist jenes Element aus $S$, das wir durch „Kürzen“ des Elements

$$(a_0, n_1, a_1, n_2, ..., a_{r-1}, n_r, a_r \cdot b_0, m_1, b_1, m_2, ..., b_{s-1}, m_s, b_s)$$

erhalten.( Kürzen wie in Pkt.1 ). Ist also $a_r \cdot b_0 \neq 1$, so endet das Kürzen, ansonsten betrachten wir das Element

$$(a_0, n_1, a_1, n_2, ..., a_{r-1}, n_r + m_1, b_1, m_2, ..., b_{s-1}, m_s, b_s)$$

Ist $n_r + m_1 \neq 0$ so ist das Kürzen beendet, ansonsten betrachten wir

$$(a_0, n_1, a_1, n_2, ..., a_{r-1} \cdot b_1, m_2, ..., b_{s-1}, m_s, b_s)$$

Wir beginnen nun wieder „von vorne“, und sehen auch hier, daß dieser Prozeß endet.

Wir werden das Element, das wir durch Kürzen der Folge

$$(a_0, n_1, a_1, n_2, ..., a_{r-1}, n_r, a_r)$$

erhalten mit

$$\overline{(a_0, n_1, a_1, n_2, ..., a_{r-1}, n_r, a_r)}$$

bezeichnen.

Das Element (1) ist klarerweise die Eins, $(a_0, n_1, a_1, n_2, ..., a_{r-1}, n_r, a_r)^{-1} = (a_r^{-1}, -n_r, a_1^{-1}, -n_{r-1}, ..., a_1^{-1}, n_1, a_0)$. Können wir die Assoziativität von $\cdot$ zeigen, so ist $S$ eine Gruppe.

Wir können dann $G$ in $S$ einbetten mittels $a \mapsto (a)$, es sei dann $u = (e, 1, e)$, damit ist $(a_0, n_1, a_1, n_2, ..., a_{r-1}, n_r, a_r) = a_0 u^{n_1} a_1 u^{n_2} \dots a_{r-1} u^{n_r} a_r$, da $u^n = \underbrace{(e, 1, e) \cdot (e, 1, e) \cdot \ldots \cdot (e, 1, e)}_{n} = (e, \underbrace{1 + 1 + \ldots + 1}_{n}, e) = (e, n, e)$ und $(a) \cdot u^n = (a) \cdot (e, n, e) = (a, n, e)$. Somit ist $S \simeq G(\{u\})$. Nach Proposition 1.2.6 gibt es dann einen Epimorphismus $\rho : G[x] \to S$ mit $\rho(x) = u$ und $\rho(a) = a \forall a \in G$. Somit ist $\rho(a_0 x^{n_1} a_1 x^{n_2} ... a_{r-1} x^{n_r} a_r) = (a_0, n_1, a_1, n_2, ..., r - 1, n_r, a_r)$. Sind nun also zwei Elemente aus $G[x]$ gleich, so haben sie dasselbe Bild, damit haben sie aber auch dieselbe Darstellung.

Was noch zu zeigen bleibt ist, daß $\cdot$ auf $S$ assoziativ ist. D.h., daß $u_1 \cdot (u_2 \cdot u_3) = (u_1 \cdot u_2) \cdot u_3$ für alle $u_1 = (a_0, n_1, a_1, \ldots, a_{r-1}, n_r, a_r)$, $u_2 = (b_0, m_1, b_1, \ldots, b_{s-1}, m_s, b_s)$ und $u_3 = (c_0, l_1, c_1, \ldots, c_{t-1}, l_t, c_t)$. Nehmen wir an, daß die Behauptung sowohl für $u_2 = \alpha$ als auch $u_2 = \beta$ für alle $u_1, u_3$ gilt, so gilt sie wegen $(u_1 (\alpha\beta)) u_3 = ((u_1\alpha) \beta) u_3 = (u_1\alpha) (\beta u_3) = u_1 (\alpha (\beta u_3)) =$

$u_1\left((\alpha\beta)\,u_3\right)$ auch für $u_2 = \alpha\beta$. Angenommen die Behauptung gilt für $u_2 = (b_0)$ und $u_2 = (e, m_1, e)$, dann gilt die Behauptung für alle $u_1, u_2, u_3$. Denn sei also $u_2 = (b_0, m_1, b_1, \ldots, b_{s-1}, m_s, b_s)$, so gilt sie für $s = 0$ nach Voraussetzung und da $(b_0, m_1, b_1) = ((b_0)(e, m_1, e))\,(b_1)$ wegen der vorherigen Feststellung auch für $s = 1$. Angenommen die Behauptung gilt für $s-1$, so gilt sie wegen $(b_0, m_1, b_1, \ldots, b_{s-1}, m_s, b_s) = (b_0, m_1, b_1, \ldots, b_{s-1}) \cdot (e, m_s, b_s)$ auch für $s$.
Sei $u_2 = (b_0)$. Dann ist

$$\begin{aligned}(u_1u_2)\,u_3 &= ((a_0, n_1, a_1, \ldots, a_{r-1}, n_r, a_r) \cdot (b_0)) \cdot (c_0, l_1, c_1, \ldots, c_{t-1}, l_t, c_t) = \\ &= \overline{(a_0, n_1, a_1, \ldots, a_{r-1}, n_r, (a_r \cdot b_0))} \cdot (c_0, l_1, c_1, \ldots, c_{t-1}, l_t, c_t) = \\ &= \overline{(a_0, n_1, a_1, \ldots, a_{r-1}, n_r, (a_r \cdot b_0) \cdot c_0, l_1, c_1, \ldots, c_{t-1}, l_t, c_t)} = \\ &= \overline{(a_0, n_1, a_1, \ldots, a_{r-1}, n_r, a_r \cdot (b_0 \cdot c_0), l_1, c_1, \ldots, c_{t-1}, l_t, c_t)} = \\ &= (a_0, n_1, a_1, \ldots, a_{r-1}, n_r, a_r) \cdot ((b_0) \cdot (c_0, l_1, c_1, \ldots, c_{t-1}, l_t, c_t))\end{aligned}$$

Sei nun $u_2 = (e, m_1, e)$. Dann unterscheiden wir vier Fälle:

1. $a_r \neq e, c_0 \neq e$ : Dann ist

$$\begin{aligned}(u_1u_2)\,u_3 &= (a_0, n_1, a_1, \ldots, a_{r-1}, n_r, a_r, m_1, c_0, l_1, c_1, \ldots, c_{t-1}, l_t, c_t) = \\ &= u_1\,(u_2u_3)\end{aligned}$$

2. $a_r = e, c_0 \neq e$: Dann ist $(u_1u_2) = (a_0, n_1, a_1, \ldots, a_{r-1}, n_r + m_1, e)$, wenn $n_r \neq -m_1$ oder $(u_1u_2) = (a_0, n_1, a_1, \ldots, a_{r-1})$, wenn $n_r = -m_1$. Also ist im ersten Fall

$$(u_1u_2)\,u_3 = (a_0, n_1, a_1, \ldots, a_{r-1}, n_r + m_1, c_0, l_1, c_1, \ldots, c_{t-1}, l_t, c_t)$$

und im zweiten Fall

$$(u_1u_2)\,u_3 = \overline{(a_0, n_1, a_1, \ldots, a_{r-1} \cdot c_0, l_1, c_1, \ldots, c_{t-1}, l_t, c_t)}$$

Da $u_2u_3 = (e, m_1, c_0, l_1, c_1, \ldots, c_{t-1}, l_t, c_t)$ ist, ist dann in beiden Fällen $u_1\,(u_2u_3) = (u_1u_2)\,u_3$.

3. $a_r \neq e, c_0 = e$ : Verwende eine Argumentation wie in Fall 2.

4. $a_r = e, c_0 = e$: Dann ist $u_1u_2 = (a_0, n_1, a_1, \ldots, a_{r-1}, n_r + m_1, e)$, wenn $n_r \neq -m_1$ oder $(a_0, n_1, a_1, \ldots, a_{r-1})$, wenn $n_r = -m_1$. $u_2u_3$ ist $(e, m_1 + l_1, c_1, \ldots, c_{t-1}, l_t, c_t)$, wenn $m_1 \neq -l_1$ oder $(c_1, \ldots, c_{t-1}, l_t, c_t)$, wenn $m_1 = -l_1$ .
Also ist

$$(u_1u_2)\,u_3 = \overline{(a_0, n_1, a_1, \ldots, a_{r-1}, n_r + m_1 + l_1, c_1, \ldots, c_{t-1}, l_t, c_t)}$$

wenn $n_r \neq -m_1$, oder

$$(u_1u_2)\,u_3 = \overline{(a_0, n_1, a_1, \ldots, a_{r-1}, l_1, c_1, \ldots, c_{t-1}, l_t, c_t)}$$

sonst.

$$u_1\,(u_2u_3) = \overline{(a_0, n_1, a_1, \ldots, a_{r-1}, n_r + m_1 + l_1, c_1, \ldots, c_{t-1}, l_t, c_t)}$$

wenn $m_1 \neq -l_1$ oder

$$(a_0, n_1, a_1, \ldots, a_{r-1}, n_r, c_1, \ldots, c_{t-1}, l_t, c_t)$$

sonst.
Vergleicht man die Ergebnisse aller möglichen Fälle, so erhält man das gewünschte Ergebnis. □

Da wir jedes $a_{i-1}x^{n_i}a$ als $a_{i-1} \cdot x \cdot 1 \cdot x \cdot 1 \cdot \ldots \cdot 1 \cdot x \cdot 1 \cdot x \cdot a_i$ oder als $a_{i-1} \cdot x^{-1} \cdot 1 \cdot x^{-1} \cdot 1 \cdot \ldots \cdot 1 \cdot x^{-1} \cdot 1 \cdot x^{-1} \cdot a_i$ schreiben können, kann man auch ein anderes Normalformsystem angeben:

**Lemma 3.1.5** *Es sei $G$ eine Gruppe. Die Wörter $a_0x^{\epsilon_1}a_1x^{\epsilon_2}a_2...a_{m-1}x^{\epsilon_m}a_m$ mit $m \in \mathbb{N}$, $a_t \in G$, $\epsilon_t \in \{1, -1\}$ für $t = 0, 1, ..., m$ und $\epsilon_t = \epsilon_{t+1}$, wenn $a_t = 1$ für $t = 0, 1, ..., r-1$, bilden ein Normalformsystem für $G[x]$.*

Für abelsche Gruppen läßt sich das Normalformsystem klarerweise stark vereinfachen:

**Lemma 3.1.6** *Sei $H \in \mathfrak{Grp}_{\mathfrak{ab}}$. Die Wörter $ax^n$ bilden ein Normalformsystem ($a \in G, n \in \mathbb{Z}$).*

Betrachten wir nun den Fall $G[X]$ mit $X = \{x_1, x_2, \ldots, x_k\}$. Wie können die obigen Sätze verallgemeinert werden?

**Definition 3.1.7** *Betrachte $[\mathbb{Z}, +]$, dann ist $[\mathbb{Z}^k, +, -, \mathfrak{o}]$ eine Gruppe. Ein Paar $(\mathfrak{m}, \mathfrak{n})$ mit $\mathfrak{m} = (m_1, m_2, \ldots, m_k) \in \mathbb{Z}^k$, $\mathfrak{n} = (n_1, n_2, \ldots, n_k) \in \mathbb{Z}^k$ heißt* **reduzibel**, *wenn es ein $\nu$ gibt, sodaß $1 \leq \nu \leq k$ und $m_{\nu+1} = m_{\nu+2} = \ldots = m_k = n_1 = n_2 = \ldots = n_{\nu-1} = 0$.*
*Ist $\mathfrak{x} = (x_1, x_2, \ldots, x_k)$ so sei $\mathfrak{x}^{\mathfrak{m}} = x_1^{m_1} \cdot x_2^{m_2} \cdot \ldots \cdot x_k^{m_k}$.*

Die Definition „reduzibel“ ist von der Reihenfolge des Paares abhängig. Der Begriff wird klarer, wenn man beachtet, daß für $(\mathfrak{m}, \mathfrak{n})$ reduzibel folgt: $\mathfrak{x}^{\mathfrak{m}} \cdot \mathfrak{x}^{\mathfrak{n}} = \mathfrak{x}^{\mathfrak{m}+\mathfrak{n}}$.

**Satz 3.1.8** *$X = \{x_1, \ldots, x_k\}$. Sei $G \in \mathfrak{Grp}$. Die Wörter*

$$a_0\mathfrak{x}^{\mathfrak{m}_1}a_1\mathfrak{x}^{\mathfrak{m}_2}a_2 \ldots a_{r-1}\mathfrak{x}^{\mathfrak{m}_r}a_r$$

*bilden ein Normalformsystem für $G[X]$, wobei $r \in \mathbb{N}$, $\mathfrak{m}_\nu \in \mathbb{Z}^k$ $\mathfrak{m}_i \neq 0$ $\forall i = 1, 2, \ldots, r$, $a_j \in G$ und $\forall 0 < i < r$ gilt : $a_j = 1 \Longrightarrow (\mathfrak{m}_i, \mathfrak{m}_{i+1})$ ist nicht reduzibel.*

Dieser Satz beschreibt auch den Fall $k = 1$, denn in diesem Fall ist jedes Paar reduzibel, d.h. $\mathfrak{m}_i = (m_1) \neq 0$.

Aus dieser Aussage folgt unmittelbar:

**Lemma 3.1.9** *Sei $H \in \mathfrak{Grp}_{\mathfrak{ab}}$. Die Wörter $a_0\mathfrak{x}^{\mathfrak{m}}$ mit $\mathfrak{m} \in \mathbb{Z}^k$ $a \in G$ bilden ein Normalformsystem für $H[X]$.*

Wie sehen nun die Elemente aus $G[X]^k$ aus? Jedes einzelne Koordinatenpolynom hat die obige Gestalt. Durch Hinzufügen von Potenzen $x_\nu^0$ und Elementen $a_k = 1$ am Ende der einzelnen Polynome in erforderlicher Anzahl können wir erreichen, daß das $r$ von Satz 3.1.8 in allen Koordinatenpolynomen gleich groß, das Maximum aller $r$, ist. Diese Darstellung ist somit eindeutig.

Setzen wir nun $\mathfrak{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix}$, $\mathfrak{a}_s = \begin{pmatrix} a_{1s} \\ a_{2s} \\ \vdots \\ a_{ks} \end{pmatrix}$ für $1 \leq s \leq r+1$, $M_s = \left(m_{ij}^{(s)}\right)_{ij}$, $M_s \in M_k(\mathbb{Z})$ und $\mathfrak{x}^{M_s} = \begin{pmatrix} x_1^{m_{11}^{(s)}} \cdot & x_2^{m_{12}^{(s)}} \cdot & \dots & \cdot x_k^{m_{1k}^{(s)}} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ x_1^{m_{k1}^{(s)}} \cdot & x_2^{m_{k2}^{(s)}} \cdot & \dots & \cdot x_k^{m_{kk}^{(s)}} \end{pmatrix}$. Ist $\mathfrak{a} \in G^k$ und $\mathfrak{M} \in M_k\mathbb{Z}$ so seien zur Abkürzung $\mathfrak{a}^{(i)}$ die $i$-te Koordinate des Vektors und $\mathfrak{M}^{(i)}$ die $i$-te Zeile der Matrix.

**Lemma 3.1.10** *$G \in \mathfrak{Grp}$. Jedes $\mathfrak{p} \in G[X]^k$ läßt sich darstellen als $\mathfrak{p}(\mathfrak{x}) = \mathfrak{a}_1\mathfrak{x}^{M_1}\mathfrak{a}_2\mathfrak{x}^{M_2} \dots \mathfrak{a}_s\mathfrak{x}^{M_s}\mathfrak{a}_{s+1}$, sodaß für die Projektionen*

$$\xi_i(\mathfrak{p}) = \mathfrak{a}_1^{(i)}\mathfrak{x}^{M_1^{(i)}}\mathfrak{a}_2^{(i)}\mathfrak{x}^{M_2^{(i)}} \dots \mathfrak{a}_s^{(i)}\mathfrak{x}^{M_s^{(i)}}\mathfrak{a}_{s+1}^{(i)}$$

*gilt*

- $\forall i = 1, \dots, k : \mathfrak{a}_j^{(i)} = 1 \Longrightarrow \left(\left(M_j^{(i)}, M_{j+1}^{(i)}\right) \text{ ist nicht reduzibel}\right) \vee \left(M_l^{(i)} = \mathfrak{o} \ \forall \ l \geq j\right)$
- $\forall i = 1, \dots, k : M_j^{(i)} = \mathfrak{o} \Longrightarrow \mathfrak{a}_j^{(i)} = 1$
- $\exists i \in 1, \dots, k : M_j^{(i)} \neq \mathfrak{o}$

*Diese Darstellungsformen bilden ein Normalformsystem.*

*Sei $H \in \mathfrak{Grp}_{\mathfrak{ab}}$, dann läßt sich jedes $\mathfrak{p} \in H[X]$ darstellen als $\mathfrak{p}(\mathfrak{x}) = \mathfrak{a}\mathfrak{x}^M$.*

Man kann nun mit Hilfe des Normalformsystem zeigen, daß $G[X]$ das direkte Produkt von $G$ und $F(X)$ ist.

**Satz 3.1.11** *Es sei $G$ eine Gruppe. $G[X]$ ist das freie Produkt von $G$ und $F(X)$.*

**Beweis:** Wie wir aus 1.2 wissen, müssen wir nur zeigen, daß die Abbildung $\varphi_2 : F(X) \to G[X]$ ein Monomorphismus ist. Seien also $v_1, v_2$ in $F(X)$. Da $F(X) = \langle X \rangle$ gilt $v_1 = x_{i_1}^{n_1} \cdot x_{i_2}^{n_2} \cdot \ldots \cdot x_{i_r}^{n_r}$, also auch $v_1 = 1 \cdot \mathfrak{x}^{\lambda_1} \cdot 1 \cdot \mathfrak{x}^{\lambda_2} \cdot \ldots \cdot 1 \cdot \mathfrak{x}^{\lambda_s} \cdot 1$ mit $\lambda_\nu \in \mathbb{Z}^k$. Wir können die Darstellung obdA so wählen, daß kein Paar $\lambda_\nu, \lambda_{\nu+1}$ reduzibel ist. $v_2$ läßt sich natürlich ebenso darstellen. Da $\varphi_2$ ein Homomorphismus und die Erweiterung von $x \mapsto x$ ist folgt nun aus $\varphi_2(v_1) = \varphi_2(v_2)$ die Gleichheit $v_1 = v_2$. □

Mit einem Normalformsystem können wir auch direkt zeigen (vgl. Satz 1.2.2)

**Satz 3.1.12** *Seien G,H Gruppen und $\vartheta \in Mon(G, H)$. Dann ist die kanonische Erweiterung $\vartheta[X] : G[X, \mathfrak{V}] \to H[X, \mathfrak{V}]$ auch ein Monomorphismus.*

**Beweis:** Sei $p \in G[X]$, sei $a_0 \mathfrak{x}^{\mathfrak{m}_1} a_1 \ldots a_{r-1} \mathfrak{x}^{\mathfrak{m}_r} a_r$ Repräsentation von $p$ und Element des obigen Normalformsystem, dann ist

$$\eta[X](p) = \eta(a_0)\mathfrak{x}^{\mathfrak{m}_1}\eta(a_1)\ldots\eta(a_{r-1})\mathfrak{x}^{\mathfrak{m}_r}\eta(a_r)$$

Das ist wieder Teil des Normalformsystems, denn die $\mathfrak{m}_i$ bleiben natürlich $\neq 0$ und ist $\eta(a_i) = 1$, so ist auch $a_i = 1$. Damit ist aber $\eta[X](p)$ eindeutig und somit ist $\eta[X]$ injektiv. □

### 3.1.2 Normalformen bzgl. $P_k(G)$

Für $P_k(G)$ können wir im Falle eines endlichen Exponenten von $G$ die Form der $p \in P_k(G)$ einschränken. Setzen wir dazu $\mathfrak{x} = (\xi_1, \ldots, \xi_k)$ und sei für $\mathfrak{m} \in \mathbb{Z}^k$ $\mathfrak{x}^{\mathfrak{m}} = \xi_1^{\mathfrak{m}_1} \cdot \ldots \cdot \xi_k^{\mathfrak{m}_1}$.

**Lemma 3.1.13** *Ist $G$ eine Gruppe mit $exp(G)$ endlich. Dann ist*

$$P_k(G) = \{a_0\mathfrak{x}^{\mathfrak{m}_1}a_1\mathfrak{x}^{\mathfrak{m}_2}a_2\ldots a_{r-1}\mathfrak{x}^{\mathfrak{m}_r}a_r : r \in \mathbb{N}, \mathfrak{m}_\nu \in \mathbb{Z}^k_{exp(G)}, a_\nu \in G, \nu = 1, \ldots, r\}$$

**Beweis:** Für $\xi_j^m \in P_k(G)$ mit $j = 1, \ldots, k$ gilt klarerweise $\xi_j^m = \xi_j^{m'}$, wenn $m \equiv m' \bmod exp(G)$, also gibt es ein $l \in \mathbb{Z}_{exp(G)}$ sodaß $\xi_j^m = \xi_j^l$. Somit gibt es also für jedes $\mu \in \mathbb{Z}^k$ ein $\nu \in \mathbb{Z}^k_{exp(G)}$, sodaß $\mathfrak{x}^\mu = \mathfrak{x}^\nu$. Aus Satz 3.1.8 folgt die Aussage. □

**Korollar 3.1.14** *Ist $G$ eine Gruppe mit $exp(G)$ endlich. Dann ist*

$$P_k(G) = \{a_0\xi_{i_1}a_1\xi_{i_2}a_2 \dots a_{s-1}\xi_{i_s}a_s\}$$

$$\textit{mit } s \in \mathbb{N}; a_\nu \in G, \nu = 1, \dots, r; i_l = 1, \dots, k \textit{ für } l = 1, \dots, s$$

**Beweis:** Füge in die Darstellung aus 3.1.13 genügend Einsen ein. □

Daraus können wir nun leicht sehen, daß $\sigma_k[G]$ im allgemeinen natürlich nicht injektiv ist. Betrachte irgendeine Gruppe mit endlichem Exponenten, z.B. $\mathbb{Z}_k$, dann ist $\sigma_k[G](x_i^m) = \sigma_k[G](x_i^n)$, wenn $m = n \bmod exp(G)$. Insbesondere folgt also, daß Gruppen mit endlichem Exponenten nicht funktional unterscheidbar sein können.

Im Falle endlicher Gruppen bzw. Gruppen mit endlichem Exponenten können also die Elemente aus $P_k(G)$ stets mit positiven Exponenten dargestellt werden!

Eine Umkehrung des vorherigen Satzes gilt für abelsche Gruppen:

**Lemma 3.1.15** *Sei $G$ eine abelsche Gruppe. Gibt es ein $l \in \mathbb{Z}$ mit $l > 0$, sodaß $P_k(G) = \{a\mathfrak{x}^{\mathfrak{m}} : \mathfrak{m}_\nu \in \mathbb{Z}_l\}$, dann ist $exp(G)$ endlich und $exp(G) \leq l$.*

**Beweis:** Jedes $p \in P_k(G)$ läßt sich also in der obigen Form schreiben. Also auch $x_1^l = a\mathfrak{x}^{\mathfrak{m}}$. Setzt man $(1, \dots, 1)$ ein, folgt $a = 1$. Ist $|A| = 1$, so ist $exp(G) = 1$, also gilt der Satz klarerweise. Sei also $|A| > 1$, dann gibt es zumindest ein $y_1 \neq 1$. Setzen wir nun $\forall y_1 \neq 1$ $(y_1, 1, \dots, 1)$ in die Funktionengleichung ein, so folgt:

$$y_1^l = y_1^{m_1} \Longleftrightarrow y_1^{l-m_1} = e \ \forall y_1 \in G$$

Da $0 \leq m_1 < l$ ist somit $0 < exp(G) \leq l - m_1 \leq l$. □

Setzen wir $\mathbb{Z}_0 = \mathbb{Z}$ und für Gruppen, die keinen endlichen Exponenten besitzen, $exp(G) = 0$, so kann man sogar zeigen:

**Proposition 3.1.16** *Ist $G$ eine abelsche Gruppe, so ist die Darstellung für $p \in P_k(G)$*

$$p = a\mathfrak{x}^{\mathfrak{m}} \textit{ mit } \mathfrak{m}_\nu \in \mathbb{Z}^k_{exp(G)}$$

*eindeutig.*

*Damit gilt für endliche Gruppen*

$$|P_k(G)| = |G| \cdot exp(G)^k$$

**Beweis:** Angenommen $p = a\mathfrak{x}^{\mathfrak{m}}$, $q = b\mathfrak{x}^{\mathfrak{m}'} \in P_k(G)$ mit $p = q$. Setze $(1, \ldots, 1)$ ein, somit folgt $a = b$. Ist $y_i \neq 1$ so setze $(1, \ldots, 1, y_i, 1, \ldots, 1)$ ein, so ist $y_i^{m_i} = y_i^{m_i'} \Longleftrightarrow y_i^{m_i - m_i'} = 1$. Ist $exp(G) = 0$ folgt $m_i = m_i'$. Ist $exp(G) > 0$, so gilt $m_i = m_i' \bmod exp(G)$, da jedoch $m_i, m_i' \in \mathbb{Z}_{exp(G)}$ gilt $m_i = m_i'$. □

Auf die Polynomfunktionsmatrizen angewandt ergibt dieser Satz:

**Korollar 3.1.17** *Ist $G$ eine abelsche Gruppe, so ist die Darstellung für $\mathfrak{p} \in P_k(G)^k$*

$$\mathfrak{p} = \mathfrak{a}\mathfrak{x}^K \text{ mit } K \in M_k(\mathbb{Z}_{exp(G)})$$

*eindeutig.*

Weiters gilt:

**Lemma 3.1.18** *Sei $H$ eine abelsche Gruppe. $f, g \in P_k(H)^k$ mit $f = \mathfrak{x}^N$ und $g = \mathfrak{x}^L$, $N$ und $L \in M_k(\mathbb{Z})$. Dann ist*

$$f \circ g = \mathfrak{x}^{N \cdot L}$$

**Beweis:** Für die Matrix $N$ sei $N^{(i)}$ die $i$-te Zeile (siehe auch A.6.1):

$$f \circ g = f(\mathfrak{x}^{L^{(1)}}, \mathfrak{x}^{L^{(2)}}, \ldots, \mathfrak{x}^{L^{(k)}}) =$$

$$= ((\mathfrak{x}^{L^{(1)}}, \mathfrak{x}^{L^{(2)}}, \ldots, \mathfrak{x}^{L^{(k)}})^{N^{(1)}}, \ldots, (\mathfrak{x}^{L^{(1)}}, \mathfrak{x}^{L^{(2)}}, \ldots, \mathfrak{x}^{L^{(k)}})^{N^{(k)}})$$

Betrachten wir nun nur die $i$-te Koordinate für ein $i = 1, \ldots, k$:

$$\xi_i \circ (f \circ g) = (\mathfrak{x}^{N^{(1)}}, \mathfrak{x}^{N^{(2)}}, \ldots, \mathfrak{x}^{N^{(k)}})^{L^{(i)}} =$$

$$= (x_1^{n_{11}})^{l_{i1}} \cdot (x_2^{n_{12}})^{l_{i1}} \cdot \ldots \cdot (x_k^{n_{1k}})^{l_{i1}} \cdot (x_1^{n_{21}})^{l_{i2}} \cdot (x_2^{n_{22}})^{l_{i2}} \cdot \ldots \cdot (x_k^{n_{2k}})^{l_{i2}} \cdot \ldots$$

$$\ldots \cdot (x_1^{n_{k1}})^{l_{ik}} \cdot (x_2^{n_{k2}})^{l_{ik}} \cdot \ldots \cdot (x_k^{n_{kk}})^{l_{ik}} =$$

$$= x_1^{l_{i1} \cdot n_{11}} \cdot x_1^{l_{i1} \cdot n_{12}} \cdot \ldots \cdot x_1^{l_{i1} \cdot n_{k1}} \cdot \ldots \cdot x_k^{l_{ik} \cdot n_{k1}} \cdot \cdot x_k^{l_{ik} \cdot n_{2k}} \cdot \ldots \cdot x_k^{l_{ik} \cdot n_{kk}} =$$

$$= x_1^{\sum_{j=1}^{k} l_{ij} \cdot n_{j1}} \cdot \ldots \cdot x_k^{\sum_{j=1}^{k} l_{ij} \cdot n_{jk}} = \mathfrak{x}^{N \cdot L}$$

□

**Bemerkung:** Damit läßt sich zeigen (siehe Proposition 3.3.7), daß die Abbildung

$$\gamma : \left[P_k(G)^k; \cdot, ^{-1}, 1, \circ, \mathfrak{x}\right] \to \left[M_k(\mathbb{Z}_{exp(G)}); +, -, \mathfrak{o}, \cdot, \mathfrak{1}\right]$$

mit $\gamma(\mathfrak{a}\mathfrak{x}^K) = K$ ein Epimorphismus bezüglich dieser Operationen ist. (Sie ist ein *Fastringepimorphismus* , siehe Abschnitt 3.1.5). Daraus (und den obigen Feststellungen) folgt, daß $\gamma$ eingeschränkt auf die Termfunktionsmatrizen $T_k(G)^k$ sogar ein Isomorphismus ist. Somit ist für abelsche $G$ die Menge der Termfunktionsmatrizen $T_k(G)^k$ ein Ring bezüglich Multiplikation und Einsetzen!

Für nichtabelsche Gruppen kann man nur mehr zeigen

**Lemma 3.1.19** *Seien $p, q \in P_k(G)$ mit $p = a_0\mathfrak{x}^{\mathfrak{m}_1}a_1\mathfrak{x}^{\mathfrak{m}_2}a_2 \ldots a_{r-1}$ und $q = b_0\mathfrak{x}^{\mathfrak{m}'_1}b_1\mathfrak{x}^{\mathfrak{m}'_2}b_2 \ldots b_{l-1}$. Ist $p = q$, so ist*

$$a_0 \cdot a_1 \cdot \ldots a_{r-1} = b_0 \cdot b_1 \cdot \ldots b_{l-1}$$

**Beweis:** Setze $(1, \ldots, 1)$ in $p = q$ ein. □

### 3.1.3 Ω-Gruppen

Wenn wir z.B. Ringe betrachten, dann sind das Mengen mit zwei Operationen, wobei die Trägermenge mit einer davon eine Gruppe bildet. Betrachten wir andererseits die Komposition von Funktionen auf Gruppen, so haben wir wiederum eine Gruppe mit einer zusätzlichen Operation. Das motiviert uns eine neue Varietät zu untersuchen:

**Definition 3.1.20** *Es sei $G$ eine Menge mit den Operationen $\Omega_1 = \{+, -, 0\} \cup \Omega$. Dann nennen wir $G$ eine $\Omega$-Gruppe, wenn*

1. *$[G; +, -, 0]$ eine Gruppe ist*
2. *für Operationen $\omega \in \Omega$ mit $Ar(\omega) > 0$ gilt: $\omega(0, 0, \ldots, 0) = 0$.*

In Analogie zu den Ringen haben wir die Gruppe additiv angeschrieben. Natürlich kann die Gruppe auch hier multiplikativ geschrieben werden, d.h. $\Omega_1 = \{\cdot, ^{-1}, 1\} \cup \Omega$.

Die Definition der Ω-Gruppe beinhaltet neben den Gesetzen für eine Gruppe eine weitere Bedingung, die aber ebenso ein Gesetz ist, somit gilt

**Korollar 3.1.21** *Für jedes $\Omega$ bildet die Klasse der $\Omega$-Gruppen eine Varietät, $\mathfrak{Grp}_\Omega$.*

Wir wollen nun einige grundlegende Definitionen einführen:

**Definition 3.1.22** *Sei $G$ eine $\Omega$-Gruppe, $K$ eine Kongruenz auf $G$. Dann ist der* **Kern von K** *die Kongruenzklasse von* 0.

$$ker\ K = C(0)$$

Beachte die Kleinschreibung und damit die Unterscheidung zu dem Kern einer Abbildung $f$ : $Ker\ f$ (siehe Definition 1.1.25).

**Definition 3.1.23** *Sei $G$ eine $\Omega$-Gruppe. Eine Teilmenge $M \subseteq G$ heißt* **Ideal**, *wenn es eine Kongruenz $K$ gibt, sodaß*

$$M = ker\ K$$

*Die Menge aller Ideale von $G$ bezeichnen wir mit $\mathfrak{I}(G)$.*

**Definition 3.1.24** *Es seien $G$ und $H$ $\Omega$-Gruppen. Ist $\varphi \in Hom(G, H)$, dann ist der* **Idealkern von** $\varphi$

$$ker\ \varphi = ker\ Ker\ \varphi$$

**Korollar 3.1.25** *Sei $A$ ein Ideal der $\Omega$-Gruppe $G$, $A = ker\ K$. Dann ist $A$ normale Untergruppe der Gruppe $G$, $A \trianglelefteq G$, und $K$ ist genau die durch diesen Normalteiler induzierte Kongruenz.*

*Die Abbildung $ker : \mathfrak{K}(A) \to \mathfrak{I}(A)$ ist bijektiv. D.h. für jedes Ideal $I$ gibt es die Kongruenz $ker^{-1}(I)$.*

**Beweis:** Dies folgt direkt daraus, daß die Kongruenzen einer Gruppe genau die durch die Normalteiler bestimmten Äquivalenzrelationen sind, aus Proposition 3.1.2 und aus der Definition. □

Da das Ideal $A$ eine normale Untergruppe ist, gilt $0 \in A$ klarerweise.

Mit $A_i \trianglelefteq^{\Omega} G$, $i \in I$, sind offensichtlich auch $\bigcap\limits_{i \in I} A_i$ und $\sum\limits_{i \in I} A_i$ Ideale.

Ist $\Omega = \emptyset$, dann ist $G$ eine Gruppe. Die Ideale sind genau die normalen Untergruppen. In Anlehnung an die Notation $A \trianglelefteq G$, wenn $A$ eine normale Untergruppe von $G$ ist, werden wir also für „$I$ ist Ideal von $G$“ symbolisch schreiben: $I \trianglelefteq^{\Omega} G$.

**Proposition 3.1.26** *Es sei $G$ eien $\Omega$-Gruppe. Eine Untermenge $A \subseteq G$ ist ein Ideal von $G$ genau dann, wenn*

- $A \trianglelefteq G$, *d.h. A ist normale Untergruppe von G*
- *Für* $\omega_i \in \Omega$ *mit* $n = Ar(\omega_i) > 0$ *gilt* $\forall\ a \in A$, $\forall\ (g_1, \ldots, g_n) \in G^n$ *und* $\forall i$ *mit* $1 \leq i \leq n$*:*

$$\omega_i(g_1, \ldots, g_{i-1}, g_i + a, g_{i+1}, \ldots, g_n) - \omega_i(g_1, \ldots, g_n) \in A$$

**Beweis:** siehe [18] Anhang Lemma 3.4

Es gilt inbesondere, wenn die $\Omega$-Gruppe ein Ring ist, daß der Begriff des ($\Omega$-Gruppen-)Ideals mit jenem des (Ring-)Ideals zusammenfällt.

Die zweite Bedingung aus 3.1.26 kann umgeformt werden zu:

$$\omega_i(g_1, \ldots, g_{i-1}, g_i + a, g_{i+1}, \ldots, g_n) \in A + \omega_i(g_1, \ldots, g_n)$$

D.h. $\omega_i(g_1, \ldots, g_{i-1}, g_i + a, g_{i+1}, \ldots, g_n)$ ist in der selben Nebenklasse wie $\omega_i(g_1, \ldots, g_n)$ bezüglich $A$.

Multiplikativ angeschrieben heißt sie:

$$\omega_i(g_1, \ldots, g_{i-1}, g_i \cdot a, g_{i+1}, \ldots, g_n) \cdot \omega_i(g_1, \ldots, g_n)^{-1} \in A$$

Man kann eine äquivalente Formulierung zeigen

**Korollar 3.1.27** *Es sei G eine* $\Omega$*-Gruppe. Eine Untermenge* $A \subseteq G$ *ist ein Ideal von G genau dann, wenn*

- $A \trianglelefteq G$
- $\forall \omega_i \in \Omega$ *mit* $n = Ar(\omega_i)$ *gilt* $\forall\ (g_1, \ldots, g_n) \in G^n, \forall\ (a_1, \ldots, a_n) \in A^n$ :

$$\omega_i(g_1 + a_1, \ldots, g_i + a_i, \ldots, g_n + a_n) - \omega_i(g_1, \ldots, g_n) \in A$$

**Beweis:** Aus diesen Voraussetzungen folgen wegen $0 \in A$ jene von 3.1.26. Also gilt $\Longleftarrow$.

Für $\Longrightarrow$ zeigen wir, daß aus den Vorraussetzungen von 3.1.26 diese folgen. Betrachte $\omega_i \in \Omega$, sei zuerst $Ar(\omega_i) = 0$. Dann ist zu zeigen, daß $\omega_i - \omega_i \in A$ gilt. Dies gilt, da $0 \in A$.

Sei also $n = Ar(\omega_i) > 0$ . Nach 3.1.26 gilt

$$\omega(g_1 + a_1, g_2, \ldots, g_n) - \omega(g_1, g_2, \ldots, g_n) \in A$$

aber genauso

$$\omega(g_1 + a_1, g_2 + a_2, g_3, \ldots, g_n) - \omega(g_1 + a_1, g_2, \ldots, g_n) \in A$$

$$\vdots$$

$$\omega(g_1 + a_1, g_2 + a_2, \ldots, g_{n-1} + a_{n-1}, g_n + a_n) -$$
$$-\omega(g_1 + a_1, g_2 + a_2, \ldots, g_{n-1} + a_{n-1}, g_n) \in A$$

Da $A$ eine normale Untergruppe ist, ist damit die Summe all dieser Elemente in $A$, also

$$\omega(g_1 + a_1, \ldots, g_n + a_n) - \omega(g_1, \ldots, , g_n)$$

□

Ideale von $\Omega$-Gruppen müssen im allgemeinen keine $\Omega$-Untergruppen sein. Als Beispiel betrachte das Ideal $2 \cdot \mathbb{Z}$ der ganzen Zahlen $\mathbb{Z}$, als kommutativer Ring mit Eins aufgefaßt.

Aber sind alle 0-stelligen Operationen im Ideal, so ist es eine $\Omega$-Untergruppe.

**Proposition 3.1.28** *Sei $G$ eine $\Omega$-Gruppe, und $I \trianglelefteq^{\Omega} G$. Gilt für alle $\omega_i$ mit $Ar(\omega_i) = 0$, daß $\omega_i \in I$, so ist $I \preceq G$.*

**Beweis:** Es ist zu zeigen, daß für alle $\omega_i \in \Omega$ das Ideal $A$ abgeschlossen ist. Sei $Ar(\omega_i) = 0$, dann gilt das nach Vorraussetzung.

Sei nun $Ar(\omega_i) > 0$. Dann gilt nach Korollar 3.1.27

$$\omega_i(0 + a_1, \ldots, 0 + a_j, \ldots, 0 + a_n) - \omega_i(0, \ldots, 0) \in A$$

Somit ist mit $0 = \omega_i(0, \ldots, 0)$ auch

$$\omega_i(a_1, \ldots, a_n) \in A$$

□

Wir können nun auch leicht folgern:

**Korollar 3.1.29** *Seien $G$ und $H$ $\Omega$-Gruppen. Ist $A$ ein Ideal von $G$ und $\eta : G \to H$ ein Epimorphismus (bzgl. $\Omega$-Gruppen). Dann ist $\eta(A)$ ein Ideal in $H$.*

**Beweis:** Nach A.8.9 ist $\varphi(N) \trianglelefteq H$. Es bleibt zu zeigen, daß

$$\omega_i(h_1, \ldots, h_{i-1}, h_i + b, h_{i+1}, \ldots, h_n) - \omega_i(h_1, \ldots, h_n) \in \eta(A)$$

für alle $\omega_i \in \Omega$ mit $n = Ar(\omega_i) > 0$ und $\forall\ b \in A$, $\forall\ (h_1, \ldots, h_n) \in G^n$ und $\forall i$ mit $1 \leq i \leq n$ gilt.

Da $\eta$ ein Epimorphismus ist gibt es $a \in A$ und $g_i \in G$, sodaß $\eta(a) = b$ und $\eta(g_i) = h_i$ für $i = 1, \ldots, n$. Also ist

$$\omega_i(h_1, \ldots, h_{i-1}, h_i + b, h_{i+1}, \ldots, h_n) - \omega_i(h_1, \ldots, h_n) =$$

$$= \omega_i(\eta(g_1), \ldots, \eta(g_{i-1}), \eta(g_i)+\eta(a), \eta(g_{i+1}), \ldots, \eta(g_n))-\omega_i(\eta(g_1), \ldots, \eta(g_n)) =$$

$$= \eta(\omega_i(g_1, \ldots, g_{i-1}, g_i + a, g_{i+1}, \ldots, g_n) - \omega_i(g_1, \ldots, g_n) \in \eta(A)$$

□

Wir wissen, daß Ringe mit (linker) Eins eine halb entartete Varietät bilden. In der Ableitung 1.1.5 haben wir gesehen, daß von der Tatsache kommt, daß in einer einelementigen Algebra $1 = 0$ gilt. D.h. es gibt zumindest hier einen Zusammenhang zwischen den 0-ären Operationen und der Eigenschaft halb entartet zu sein.

Allgemein läßt sich zeigen:

**Lemma 3.1.30** *Sei $\mathfrak{V} \subseteq \mathfrak{Grp}_\Omega$ eine nicht vollständig entartete Varietät von $\Omega$-Gruppen, sodaß 0 die einzige 0-äre Operation ist. Dann ist $\mathfrak{V}$ nicht halb entartet.*

**Beweis:** siehe [1] Satz 1.79

Seien $G_i$ für $i \in I$ $\Omega$- Gruppen. Dann können wir das Produkt $\prod_{j \in J} G_j$ betrachten, das dann nach 1.1.61 wieder eine $\Omega$-Gruppe ist. Wir wissen die Projektionen $\xi_j : \prod_{j \in J} G_j \to G_j$ sind Epimorphismen. Wir können wie üblich auch eine Funktion in die Gegenrichtung betrachten.

**Definition 3.1.31** *Es seien $G_j$, $j \in J$, $\Omega$- Gruppen, dann definieren wir die* **kanonischen Einbettungen**

$$\iota_i : G_j \to \prod_{j \in J} G_j$$

*mit*

$$\xi_k\left(\iota_j(g)\right) = \begin{cases} g & k = j \\ 0 & sonst \end{cases}$$

Aus den Definitionen der Einbettung, der $\Omega$-Gruppen und den Operationen auf dem Produkt folgt direkt:

**Korollar 3.1.32** *Für alle $i \in I$ ist $\iota_i$ ein $\Omega$-Monomorphismus.*

Aus dieser Aussage, der Definition der Operationen auf dem Produkt und Proposition 3.1.26 folgt sofort, daß mit $A_i \trianglelefteq^\Omega G_i$, $i \in I$, auch $\prod A_i \trianglelefteq^\Omega \prod G_i$ gilt.

Wenden wir uns nun jenem Fall von $\Omega$-Gruppen zu, dem wir bereits begegnet sind, den Kompositionsgruppen. Wir verwenden in Analogie zu Kapitel 2 die muliplikative Schreibweise der Gruppe.

**Proposition 3.1.33** *Sei $[G; \cdot, ^{-1}, 1, \Omega, \circ]$ eine k-dimensionale $\mathfrak{Grp}_\Omega$-Kompositionsalgebra. Dann ist $G$ eine $\Omega_1$-Gruppe mit $\Omega_1 = \Omega \cup \{\circ\}$. 1 ist eine Konstante.*

**Beweis:** Zu zeigen bleibt nur, daß $1 \circ (1, \ldots, 1) = 1$ ist. Aber es gilt ja für beliebiges $(g_1, \ldots, g_k) \in G^k$ :

$$1 \circ (g_1, \ldots, g_k) = (1 \cdot 1) \circ (g_1, \ldots, g_k) = 1 \circ (g_1, \ldots, g_k) \cdot 1 \circ (g_1, \ldots, g_k)$$

da $\circ$ rechts-super-distributiv ist. Daraus folgt aber

$$1 = 1 \circ (g_1, \ldots, g_k) \; \forall g_i \in G \text{ mit } i = 1, \ldots, k$$

also insbesondere auch für $g_i = 1$ für alle $i = 1, \ldots, k$ □

Damit sind, wenn $G$ eine $\Omega$-Gruppe ist, $A[X, \mathfrak{V}]$, $P_k(A)$, $K_k(A)$ und $F_k(A)$ $\Omega \cup \{\circ\}$- Gruppen. Insbesondere sagt diese Proposition auch, daß $k$-dimensionale Kompositionsgruppen $\{\circ\}$-Gruppen sind.

**Definition 3.1.34** *Sei $[G; \cdot, ^{-1}, 1, \Omega, \circ]$ eine $\mathfrak{Grp}_\Omega$-Kompositionsalgebra. Ein Ideal $I$ von $[G; \cdot, ^{-1}, 1, \Omega]$, $I \trianglelefteq^\Omega G$, heißt* **Vollideal** *, wenn $I$ auch ein Ideal von $[G; \cdot, ^{-1}, 1, \Omega, \circ]$ ist, symbolisch $I \trianglelefteq_\circ^\Omega G$.*

**Proposition 3.1.35** *Sei $G$ eine $\Omega$-Gruppe. Sei $U \preceq_\circ F_k(G)$ oder $U = G[X]$, Sei $I \trianglelefteq U$. Dann gilt für alle $f \in U, \mathfrak{g} \in U^k$ und $u \in I, \mathfrak{v} \in I^k$*

$$f \circ (\mathfrak{g} + \mathfrak{v}) + u \circ (\mathfrak{g} + \mathfrak{v}) = f \circ \mathfrak{g} + I$$

**Beweis:** Da $\circ$ rechts-superdistributiv ist, gilt

$$f \circ (\mathfrak{g} + \mathfrak{v}) + u \circ (\mathfrak{g} + \mathfrak{v}) = (f + u) \circ (\mathfrak{g} + \mathfrak{v})$$

Es gilt für $\mathfrak{g} = (g_1, \ldots, g_k)$ und $\mathfrak{v} = (v_1, \ldots, v_k)$

$$f \circ (\mathfrak{g} + \mathfrak{v}) + u \circ (\mathfrak{g} + \mathfrak{v}) = \chi(f + u, g_1 + v_1, \ldots, g_k + v_k)$$

Da $I$ ein Vollideal ist gilt

$$\chi(f+u, g_1+v_1, \ldots, g_k+v_k) - \chi(f, g_1, \ldots, g_k) \in I$$

Also ist

$$f \circ (\mathfrak{g}+\mathfrak{v}) + u \circ (\mathfrak{g}+\mathfrak{v}) = f \circ \mathfrak{g} + I$$

□

Betrachten wir die Vollideale in Teil-Ω-Gruppen von $F_k(G)^k$ oder $G[X]^k$, dann können wir eine analoge Aussage zu Proposition 3.1.35 formulieren:

**Lemma 3.1.36** *Sei $G$ eine Ω-Gruppe. Sei $U \preceq_\circ F_k(G)^k$ und $I \trianglelefteq F_k(G)^k$. Dann gilt für alle $\mathfrak{f}, \mathfrak{g} \in U$ und $\mathfrak{u}, \mathfrak{v} \in I$*

$$\mathfrak{f} \circ (\mathfrak{g}+\mathfrak{v}) + \mathfrak{u} \circ (\mathfrak{g}+\mathfrak{v}) = \mathfrak{f} \circ \mathfrak{g} \bmod I$$

Dieser Satz kann klarerweise ebenso für Unter-Ω-Gruppen von $F_k(G)^i$ oder $G[X]^i$ für ein $i \geq 1$ formuliert werden.

Ist $I$ ein Vollideal, dann ist $ker^{-1}I$ eine Vollkongruenz. Damit lassen sich die Aussagen über Vollkongruenzen direkt auf Vollideale anwenden.

**Lemma 3.1.37** *Es sei $G$ eine Ω-Gruppe. Sei $U \preceq_\circ F_k(G)$ oder $U = G[X]$ für $i = 1, \ldots, k$. Ein Ideal $I$ von $U$ ist ein Vollideal genau dann, wenn $\forall\ (p_1, \ldots, p_k) \in U^k$ gilt*

$$f \in I \Longrightarrow f \circ (p_1, \ldots, p_k) \in I$$

**Beweis:** $\Longrightarrow$ folgt aus 3.1.35
$\Longleftarrow$ : Sei also $I$ eine Menge mit dieser Eigenschaft. Sei $K = ker^{-1}I$ die entsprechende Kongruenz. Seien $p_0 \sim_K q_0$, also ist $p_0 - q_0 \sim_K 0$. Also ist $(p_0 - q_0) \circ (p_1, \ldots, p_k) = (p_0, p_1, \ldots, p_k) - (q_0, p_1, \ldots, p_k) \in I$. Also gilt $(p_0, p_1, \ldots, p_k) \sim_K (q_0, p_1, \ldots, p_k)$. Damit ist $K$ aber nach 2.1.23 eineVollkongruenz, und somit ist $I$ ein Vollideal. □

Auch hier gilt klarerweise ein analoger Satz für $F_k(G)^i$ oder $G[X]^i$ für ein $i \geq 1$, insbesonderes für $i = k$.

### 3.1.4 Vollständigkeiten

Wir wollen in diesem Beispiel die Varietät der Gruppen in Hinblick auf Vollständigkeit untersuchen. Beginnen wollen wir mit der Polynomvollständigkeit:

**Beispiel:** In 1.4.4 haben wir gesehen, daß $\mathbb{Z}_2$ 1-polynomvollständig ist. Wir können zeigen, daß diese Menge jedoch nicht 2-polynomvollständig ist.

Ein Normalformsystem für $\mathbb{Z}_2[x_1, x_2]$ ist $\{k_1 \cdot x_1 + k_2 \cdot x_2 + a | k_1, k_2 \in \mathbb{Z}, a \in \mathbb{Z}_2\}$, also ist

$$P_2(\mathbb{Z}_2) = \{k_1 \cdot \xi_1 + k_2 \cdot \xi_2 + a | k_1 \in \mathbb{Z}, a \in \mathbb{Z}_2\}$$

Ist jedoch $k_1 = k_1'$ mod *2*, so ist $k_1\xi_1 + k_2\xi_2 + a = k_1'\xi_1 + k_2\xi_2 + a$ (siehe auch Lemma 3.1.13). Damit ist $P_2(\mathbb{Z}_2) = \{k_1 \cdot \xi_1 + k_2 \cdot \xi_2 + a | k_1, k_2 \in \mathbb{Z}_2, a \in \mathbb{Z}_2\}$, da alle diesen Funktionen nach Proposition 3.1.16 unterschiedlich sind, gilt $|P_2(\mathbb{Z}_2)| = 8$. Für die Anzahl aller zweiwertigen Funktionen gilt jedoch $|F_2(\mathbb{Z}_2)| = 2^4 = 16$. Also ist $P_2(G) \neq F_2(G)$.

Nach 1.4.4 gibt es für die Polynomvollständigkeit nur drei Fälle, die für Gruppen folgendermaßen verteilt sind:

**Satz 3.1.38** *In der Varietät der Gruppen sind die endlichen nicht abelschen einfachen Gruppen und die Gruppe mit* $|G| = 1$ *polynomvollständig, die Gruppe der Ordnung 2 ist polynomial halbvollständig, und alle anderen Gruppen sind polynomial unvollständig.*

**Beweis:** Aus 1.4.5 und 1.4.6 folgt, daß jede $n$-polynomvollständige Gruppe einfach und endlich ist.

Betrachten wir zunächst die endlichen *nicht abelschen* einfachen Gruppen. Setzen wir in A.8.29 (Anhang) $N = G$ und $A = G \times G$, dann ist $F(A, N) = F_2(G)$. Alle konstanten Funktionen gehören zu $P_2(G)$, und da alle inneren Automorphismen $\tau_g$ Polynome sind, gilt $\tau_g \circ p \in P_2(G)\ \forall p \in P_2(G)$. Seien $x \neq y \in A = G \times G$, dann ist entweder $\xi_1(x) \neq \xi_1(y)$ oder $\xi_2(x) \neq \xi_2(y)$. Somit erfüllt $P_2(G)$ die Bedingungen aus A.8.29, also gilt $P_2(G) = F_2(G)$. Also ist in diesem Fall $G$ 2-polynomvollständig, also polynomvollständig.

Betrachten wir nun die endlichen *abelschen* einfachen Gruppen. (Vergleiche mit dem vorherigen Beispiel). Nach A.8.28 gibt es eine Primzahl $p$, sodaß $|G| = p$. Nach 3.1.16 ist $P_1(G) = \{a\xi_1^r | a \in G,\ 0 \leq r < p\}$, wobei alle Elemente eindeutig dargestellt werden. Also ist $|P_1(G)| = |G| \cdot p = p^2$. Für die volle Funktionenalgebra gilt aber $|F_1(G)| = p^p$, somit gilt $F_1(G) = P_1(G)$ genau dann wenn $|G| = 2$.

Ist $|G| = 2$ so ist $G \simeq \mathbb{Z}_2$, also ist nach oben $G$ nicht 2-polynomvollständig. □

Unteralgebren von k-polynomvollständigen Algebren sind natürlich im allgemeinen nicht wieder $k$-polynomvollständig sein. Für Gruppen zeigen wir das anhand dem folgenden Beispiel:

**Beispiel:** Die alternierenden Gruppen $\mathbb{A}_k$ sind für $k \geq 5$ $k$-polynomvollständig, da sie nach A.8.42 nicht abelsch und einfach sind. Diese haben aber abelsche Untergruppen der Ordnung $> 2$, die somit für kein $k \in \mathbb{N}$ k-polynomvollständig sind, wie z.B. die $\mathbb{A}_3$.

Für bestimmte Gruppen läßt sich auch eine Aussage treffen, wie stark sie von der Polynomvollständigkeit abweicht!

**Proposition 3.1.39** *Jede zyklische Gruppe $G$ der Ordnung $m$ (d.h $G \simeq \mathbb{Z}_m$) hat k-Defekt*

$$k - def(G) = m^k - k - 1$$

**Beweis** siehe [9] Kapitel VII §2

Für die symmetrischen Gruppen läßt sich folgender Satz zeigen:

**Proposition 3.1.40** *Die symmetrische Gruppe $\mathbb{S}_n$ mit $n \geq 5$ hat höchstens den 1-Defekt $n! + 2$.*

$$1 - def(\mathbb{S}_n) \leq n! + 2$$

**Beweis:** siehe [9] Kapitel VII §3

Die anderen Vollständigkeitsbegriffe wurden (zumindest) für Gruppen noch nicht ausgiebig untersucht. Aussagen, die sich treffen lassen, sind z.B.:

**Proposition 3.1.41** *Sei $M$ eine Menge mit $|M| = \mathfrak{M} \geq \aleph_0$. Die alternierende Gruppe $\mathbb{A}_{\mathfrak{M}}$ ist lokal polynomvollständig.*

**Beweis:** siehe [9] Kapitel III §4
Für die Definition von $\mathbb{A}_{\mathfrak{M}}$ siehe A.8.45 . Nach Satz 3.1.38 ist $\mathbb{A}_{\mathfrak{M}}$ als nicht endliche Menge aber sicher polynomunvollständig. Damit haben wir auch für die Varietät der Gruppe gezeigt, daß es lokal polynomvollständige Gruppen gibt, die nicht polynomvollständig sind.

Für die Kongruenzpolynomvollständigkeit gilt:

**Proposition 3.1.42** *Die elementar abelsche Gruppe der Ordnung 4 ($\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$) ist 1-kongruenzenpolynomvollständig, aber nicht 1-polynomvollständig.*

**Beweis:** siehe [9] Kapitel IV §2

Für die Varietät der Gruppen läßt sich auch für den Begriff der Erweiterungspolynomvollständigkeit zeigen, daß dieser eine echte Erweiterung der Polynomvollständigkeit ist:

**Proposition 3.1.43** *Jede zyklische Gruppe ungerader Ordnung ist k-erweiterungspolynomvollständig* $\forall k \in \mathbb{N}$ *und somit erweiterungspolynomvollständig.*

**Beweis:** siehe [9] Kapitel V § 2

Die zyklischen Gruppen sind jedoch abelsch und somit für Ordnungen $\geq 3$ polynomunvollständig.

**Korollar 3.1.44** *Jede Gruppe ungerader Ordnung ist erweiterungspolynomvollständig.*

**Beweis:** siehe [9] Kapitel V § 2

Zum Begriff der Primalität kann man in der Varietät der Gruppen polynomvollständige Gruppen finden, die nicht primal sind. Die endlichen, nicht ableschen, einfachen Gruppen sind polynomvollständig, z.B. $\mathbb{A}_n$ mit $n \geq 5$, diese haben aber nicht triviale Untergruppen und können somit nicht primal sein.

### 3.1.5 Fastringe

**Definition 3.1.45** *Eine Menge M mit den Operationen* $+, -, 0$ *und* $\cdot$ *des Typs* $\{2, 1, 0, 2\}$ *heißt* **Fastring** *, wenn:*

1. $[M, +, -, 0]$ *eine Gruppe ist*
2. $(x \cdot y) \cdot z = x \cdot (y \cdot z)\ \forall\ x, y, z \in N$ *($\cdot$ ist assoziativ)*
3. $(x + y) \cdot z = x \cdot z + y \cdot z$ *($\cdot$ ist bzgl. $+$ rechtsdistributiv)*

   *Gilt ferner:*

4. $0 \cdot x = x \cdot 0 = 0$
   *so nennen wir den Fastring* **null-symmetrisch**.

   *Ein Element 1 heißt* **linke Eins** *wenn*

5. $1 \cdot x = x\ \forall x \in M$

Aus dieser Definition sieht man, daß die Fastringe eine Varietät des Typs $(2, 1, 0, 2)$ bilden. Im Vergleich zu Ringen muß die additive Gruppe nicht abelsch sein und die Distributivität gilt nur in eine Richtung. Die Menge der Fastringe mit linker Eins ist eine Varietät des Typs $(2, 1, 0, 2, 0)$.

Natürlich liefern Änderungen der Symbole, etwa auf $\{\cdot, ^{-1}, 1, \circ, id\}$, wiederum isomorphe Strukturen.

Die Gleichheit $0 \cdot x = 0$ gilt immer, denn $0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$. Daraus folgt durch Addition des additiven Inversen („Subtrahieren“) von $0 \cdot x$, daß $0 = 0 \cdot x$. Daraus folgt aber insbesondere, daß $0 \cdot 0 = 0$ ist und somit sind Fastringe bzw. Fastringe mit linker Eins $\Omega$-Gruppen mit $\Omega = \{\cdot\}$ bzw. $\Omega = \{\cdot, 1\}$.

Die Varietät der Fastringe mit linker Eins (1) ist halb entartet. Denn wenn es einen einelementigen Unterfastring des Fastrings $F$ gibt, so folgt $1 = 0$, damit aber für alle $x \in F$: $x = 1 \cdot x = 0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x = 1 \cdot x + 1 \cdot x = x + x \Longrightarrow 0 = x - x = (x + x) - x = x$.

Diese Varietät benötigen wir, da sich herausstellt, daß die von uns betrachteten Kompositionsgruppen $\left(G[X]^k, P_k(G)^k, F_k(G)^k\right)$ Fastringe sind. Denn für alle Produkte aus $k$ $k$-dimensionalen Kompositionsgruppen ist die Operation $\cdot$ zweiwertig, damit reduzieren sich (siehe Abschnitt 2.1) die Superassoziativität und Superrechtsdistributivität der Kompositionsabbildung auf die Assoziativität und Rechtsdistributivität. Also gilt:

**Lemma 3.1.46** *Ist $G$ eine $k$-dimensionale Kompositionsgruppe, so ist $G^k$ ein Fastring.*

Daraus folgt, daß $G^k[X]$ und alle $U^k$ mit $U \preceq_\circ F_k(G)$ Fastringe sind. Also insbesondere $P_k(G)^k$ und $K_k(G)^k$.

**Definition 3.1.47** *$G$ sei eine Gruppe. Für $k \in \mathbb{Z}$ mit $k \geq 1$ und $i = 1, \ldots, k$ sei $M \subseteq F_k^i(G)$. Dann bezeichnen wir mit $\overline{M} = \{f \in M : f(\underbrace{(0, \ldots, 0)}_{k}) = \underbrace{(0, \ldots, 0)}_{i}\}$.*

Das sind also jene Funktionen, die die Null wieder auf die Null abbilden.

**Lemma 3.1.48** *$\overline{F_k^k}(G)$ ist ein null-symmetrischer Fastring.*

**Beweis:** Zu zeigen ist nur, daß für $f \in \overline{M}$ gilt $f \circ (0, \ldots, 0) = (0, \ldots, 0)$. das gilt aber nach Definition. □

**Definition 3.1.49** *Sei $G = [G; +, -, 0, \Omega]$ eine $\Omega$-Gruppe. Ein Element $d \in G$ heißt* **links distributiv bzgl** *$\omega_i$ , mit $\omega_i \in \Omega$ und $Ar(\omega_i) > 0$ wenn gilt:*

$$\omega_i\,(d, a_1 + b_1, a_2 + b_2, \ldots, a_k + b_k) =$$

$$= \omega_i\,(d, a_1, a_2, \ldots, a_k) + \ \omega_i\,(d, b_1, b_2, \ldots, b_k) \quad \forall\ a_i, b_i \in G$$

*$G$ heißt* **links distributiv erzeugt** *wenn $\exists\{d_i | i \in I\}$, $d_i$ distributiv, sodaß $G = \langle\{d_i\}\rangle_{\{+,-,0\}}$ (D.h. die Elemente $d_i$ erzeugen $G$ als "'normale"' Gruppe.) Ist ein Element links distributiv und rechts- superdistributiv (im Sinne von 2.1.1) so nennen wir es* **distributiv** *.*

Aus dieser Definition folgt, daß für ein (links) distributives $d$ gilt:

$$\omega_i(d, 0, \ldots, 0) = 0,$$

da

$$\omega_i(d, 0, \ldots, 0) = \omega_i(d, 0+0, \ldots, 0+0) = \omega_i(d, 0, \ldots, 0) + \omega_i(d, 0, \ldots, 0)$$

Die für uns interessanten Beispiele sind

- Sei $G = [G; +, -, 0, \circ]$ eine Kompositionsgruppe. Dann können wir die distributiven Elemente von $G$ betrachten. (Klarerweise distributiv bzgl. $\circ$).
- Sei $F = [F; +, -, 0, \mu]$ ein Fastring. Dann können wir die distributiven Elemente von $F$ betrachten. (Klarerweise distributiv bzgl. $\mu$).

Es gibt eine Beziehung zwischen diesen beiden Beispielen

**Korollar 3.1.50** *Ist $G$ eine distributiv erzeugte $k$-dimensionale Kompositionsgruppe, so ist $G^k$ ein distributiv erzeugter Fastring.*

**Beweis:** [18] Kapitel 5, Proposition 2.11

Betrachten wir nun die Funktionen über Gruppen. Dort lassen sich natürliche Beispiele für distributive Elemente bezüglich der Komposition finden, denn es läßt sich der folgende Satz formulieren:

**Lemma 3.1.51** *Es sei $[G; +, -, 0]$ eine Gruppe, $k \in \mathbb{Z}$, $k \geq 1$. Dann sind die links distributiven Elemente von $\left[F_k(G)^k; +, -, 0, \circ\right]$ genau die Endomorphismen von $G^k$.*

**Beweis** Sei $f \in F_k(G)^k$, $f$ heißt distributiv, wenn $\forall\ g_i, h_i \in F_k(G)^k$

$$f\,(g_1 + h_1, g_2 + h_2, \ldots, g_k + h_k) = f\,(g_1, g_2, \ldots, g_k) + f\,(h_1, h_2, \ldots, h_k)$$

D.h. für $\mathfrak{g} = (g_1, \ldots, g_k)$ und $\mathfrak{h} = (h_1, \ldots, h_k)$ gilt somit

$$f(\mathfrak{g} + \mathfrak{h}) = f(\mathfrak{g}) + f(\mathfrak{h})$$

Das gilt inbesondere für die konstanten Funktionen $\mathfrak{a} = (a_1, \ldots, a_k)$ und $\mathfrak{b} = (b_1, \ldots, b_k)$ mit $a_i, b_i \in G$ für alle $i = 1, \ldots, k$. Also ist $f$ ein Homomorphismus.

Sei nun $\varphi$ ein Endomorphismus. Dann ist für $\forall\ \mathfrak{a},\ \mathfrak{b} \in G^k$

$$\varphi(\mathfrak{a} + \mathfrak{b}) = \varphi(\mathfrak{a}) + \varphi(\mathfrak{b})$$

Seien nun $\mathfrak{g} = (g_1, \ldots, g_k)$ und $\mathfrak{h} = (h_1, \ldots, h_k) \in F_k(G)^k$ und sei $\mathfrak{c} = (c_1, \ldots, c_k) \in G^k$ beliebig, dann ist

$$(\varphi \circ (\mathfrak{g} + \mathfrak{h}))\,(c_1, \ldots, c_k) =$$

$$= \varphi\left(g_1\left(c_1, \ldots, c_k\right) + h_1\left(c_1, \ldots, c_k\right), \ldots, g_k\left(c_1, \ldots, c_k\right) + h_k\left(c_1, \ldots, c_k\right)\right) =$$

$$= \varphi\left(\left(g_1\left(c_1, \ldots, c_k\right), \ldots, g_k\left(c_1, \ldots, c_k\right)\right) + \left(h_1\left(c_1, \ldots, c_k\right), \ldots, h_k\left(c_1, \ldots, c_k\right)\right)\right) =$$

$$= \varphi\left(g_1\left(c_1, \ldots, c_k\right), \ldots, g_k\left(c_1, \ldots, c_k\right)\right) + \varphi\left(h_1\left(c_1, \ldots, c_k\right), \ldots, h_k\left(c_1, \ldots, c_k\right)\right)$$

Also ist

$$\varphi \circ (\mathfrak{g} + \mathfrak{h}) = \varphi \circ \mathfrak{g} + \varphi \circ \mathfrak{h}$$

Also ist $\varphi$ distributiv. □

Daraus folgt, daß die Menge der Endomorphismen $End(G)$ und die der Automorphismen $Aut(G)$ aus distributiven Elementen bestehen. Ebenso sind die *inneren Automorphismen* $\tau_g \in Inn(G) = \{\tau_g \in F(G) | \exists g \in G : \tau_g(x) = g \cdot x \cdot g^{-1}\}$ distributiv. Also gilt:

**Lemma 3.1.52** *Sei $G$ eine Gruppe, $\Omega = \{+, -, 0\}$, $k \in \mathbb{Z}$ mit $k > 0$. Dann bilden $E(G) = \langle End(G)\rangle_\Omega$, $A(G) = \langle Aut(G)\rangle_\Omega$, und $I(G) = \langle Inn(G)\rangle_\Omega$ bezüglich $\{\cdot, ^{-1}, 1, \circ\}$ distributiv erzeugte Fastringe.*

**Bemerkung:** Klarerweise gilt

$$I(G^k) \preceq A(G^k) \preceq E(G^k) \preceq F(G^k)$$

Bezüglich dieser Kette kann man sich natürlich die Frage stellen, wann Gleichheiten gelten. Für $k = 1$ fällt die Frage, wann $I(G)$ gleich $A(G)$ oder $E(G)$ ist, mit der Frage zusammen, wann alle Automorphismen (respektive Endomorphismen) Polynomfunktionen sind. Denn es gilt:

$$I(G) = \overline{P_1(G)}$$

Denn einerseits gilt klarerweise $Inn(G) \subseteq \overline{P_1(G)}$ und somit $I(G) \subseteq \overline{P_1(G)}$. Andererseits sei $p \in \overline{P_1(G)}$ mit $p = a_0 x^{m_1} a_1 \cdot \ldots \cdot a_{r-1} x^{m_r} a_r$, dann ist

$e = p(e) = a_0 \cdot a_1 \cdot \ldots \cdot a_{r-1} \cdot a_r$. Wir können die Darstellungsform von $p$ umschreiben:

$$p = a_0 x^{m_1} a_0^{-1}(a_0 \cdot a_1) x^{m_2}(a_0 \cdot a_1)^{-1}(a_0 \cdot a_1 \cdot a_2) \cdot \ldots \cdot (a_0 \cdot a_1 \cdot \ldots a_{r-2})^{-1} \cdot$$

$$\cdot (a_0 \cdot a_1 \cdot \ldots \cdot a_{r-2}a_{r-1}) x^{m_r}(a_0 \cdot a_1 \cdot \ldots \cdot a_{r-2}a_{r-1})^{-1} \underbrace{(a_0 \cdot a_1 \cdot \ldots \cdot a_{r-1}a_r)}_{=e} =$$

$$= a_0 x^{m_1} a_0^{-1}(a_0 \cdot a_1) \cdot \ldots \cdot (a_0 \cdot a_1 \cdot \ldots \cdot a_{r-2}a_{r-1}) x^{m_r}(a_0 \cdot a_1 \cdot \ldots \cdot a_{r-2}a_{r-1})^{-1}$$

Also ist $p \in I(G)$, also gilt $\overline{P_1(G)} \subseteq I(G)$.

Wir werden uns dieser Frage noch einmal kurz im Kapitel 3.6 widmen. Jetzt wollen wir Eigenschaften von allgemeinen distributiv erzeugten Fastringen untersuchen.

Ist $G$ eine distributiv erzeugte Kompositionsgruppe, so können wir Vollideale auf folgende Weise charakterisieren:

**Lemma 3.1.53** *Ist $G$ eine distributiv erzeugte $k$-dimensionale Kompositionsgruppe und $A$ ein Normalteiler $A \trianglelefteq G$, so ist $A$ genau dann ein Vollideal in $G$, $A \trianglelefteq_\circ^\Omega G$, wenn*

- $a \circ (c_1, \ldots, c_k) \in A$
- $c \circ (0, \ldots, 0, a, 0, \ldots, 0) \in A$

*$\forall a \in A$ und $c_1, c_k, c \in G$.*

**Beweis:** Sei $A \trianglelefteq_\circ^\Omega G$ und $a \in A$ und $c_1, c_k, \in G.$, dann wissen wir nach 3.1.26, daß $a \circ (c_1, \ldots, c_k) - 0 \circ (c_1, \ldots, c_k) \in A$ und somit $a \circ (c_1, \ldots, c_k) \in A$. Sei nun $c \in G$, dann ist $c \circ (0, \ldots, a, \ldots, 0) - c \circ (0, \ldots, 0) \in A$. $G$ ist distributiv erzeugt, d.h. $c = w(d_i)$ für $d_i$ distributiv und $w(d_i) \in W(\{d_i\})_{+,-,0}$. Damit ist jedoch $c \circ (0, \ldots, 0) = w(d_i) \circ (0, \ldots 0) = w(d_i \circ (0, \ldots, 0))$ da $\circ$ rechts-superdistributiv ist. Da $d_i$ jedoch (links -) distributiv ist, ist $w(d_i \circ (0, \ldots, 0)) = w(0) = 0$.

Sei nun andererseits $A \trianglelefteq G$ mit den genannten Eigenschaften und seien $c_0, c_1, \ldots, c_k \in G$ und $a \in A$ beliebig. Dann ist

$$(c_0 + a) \circ (c_1, \ldots, c_k) - c_0 \circ (c_1, \ldots, c_k) =$$

$$= c_0 \circ (c_1, \ldots, c_k) + a \circ (c_1, \ldots, c_k) - c_0 \circ (c_1, \ldots, c_k)$$

$$= (c_0 + a - c_0) \circ (c_1, \ldots, c_k) \in A$$

da $\circ$ rechts - superdistributiv ist und $A \trianglelefteq G$ ist. Sei $d_i$ distributiv und $i = 1, \ldots, k$, dann ist $d_i \circ (c_1, \ldots, c_i + a, \ldots, c_k) = d_i \circ (c_1, \ldots, c_i, \ldots, c_k) + d_i \circ (0, \ldots, a, \ldots, 0)$, also ist $d_i \circ (c_1, \ldots, c_i + a, \ldots, c_k) - d_i \circ (c_1, \ldots, c_i, \ldots, c_k) = a_i \in A$. $G$ ist distributiv erzeugt, also ist $c_0 = w(d_i)$, also ist

$$c_0 \circ (c_1, \ldots, c_i + a, \ldots, c_k) - c_0 \circ (c_1, \ldots, c_i, \ldots, c_k) =$$

$$= w(d_i) \circ (c_1, \ldots, c_i + a, \ldots, c_k) - w(d_i) \circ (c_1, \ldots, c_i, \ldots, c_k) =$$

$$= w(d_i \circ (c_1, \ldots, c_i + a, \ldots, c_k)) - w(d_i \circ (c_1, \ldots, c_i, \ldots, c_k)) = (*)$$

Diese Wörter sind Summen von den distributiven Elementen und ihren Inversen, also $w(d_i) = \sum_{i=1}^{l} \pm d_i$. Also ist

$$(*) = \sum_{i=1}^{l} \pm d_i \circ (c_1, \ldots, c_i + a, \ldots, c_k) - \sum_{i=1}^{l} \pm d_i \circ (c_1, \ldots, c_i, \ldots, c_k) =$$

$$= \pm d_1 \circ (c_1, \ldots, c_i + a, \ldots, c_k) - \pm d_1 \circ (c_1, \ldots, c_i, \ldots, c_k) + \pm d_1 \circ (c_1, \ldots, c_i, \ldots, c_k) +$$

$$\pm d_2 \circ (c_1, \ldots, c_i + a, \ldots, c_k) - \pm d_2 \circ (c_1, \ldots, c_i, \ldots, c_k) + \pm d_2 \circ (c_1, \ldots, c_i, \ldots, c_k) +$$

$$\vdots$$

$$\pm d_l \circ (c_1, \ldots, c_i + a, \ldots, c_k) - \pm d_l \circ (c_1, \ldots, c_i, \ldots, c_k) + \pm d_l \circ (c_1, \ldots, c_i, \ldots, c_k) -$$

$$- \sum_{i=1}^{l} \pm d_i \circ (c_1, \ldots, c_i, \ldots, c_k) =$$

$$= \pm a_1 + \pm d_1 \circ (c_1, \ldots, c_i, \ldots, c_k) + \pm a_2 + \pm d_2 \circ (c_1, \ldots, c_i, \ldots, c_k) + \ldots$$

$$\ldots + \pm a_l + \pm d_l \circ (c_1, \ldots, c_i, \ldots, c_k) - \sum_{i=1}^{l} \pm d_i \circ (c_1, \ldots, c_i, \ldots, c_k) = **$$

$A$ ist normale Untergruppe, also gilt:

$$** = a_1' + a_2' + \ldots + a_l' + \pm d_1 \circ (c_1, \ldots, c_i, \ldots, c_k) + \pm d_2 \circ (c_1, \ldots, c_i, \ldots, c_k) + \ldots$$

$$\ldots + \pm d_l \circ (c_1, \ldots, c_i, \ldots, c_k) - \sum_{i=1}^{l} \pm d_i \circ (c_1, \ldots, c_i, \ldots, c_k) =$$

$$= a_1' + a_2' + \ldots + a_l' \in A$$

Also ist nach 3.1.26 $A$ ein Vollideal. $\square$

Es folgt insbesondere, daß $c \circ (a_1, \ldots, a_k) \in A$ ist, da wir nach 3.1.27 wissen, daß $c \circ (a_1, \ldots, a_k) - c \circ (0, \ldots, 0) \in A$ ist. Nach Beweis oben ist aber $c \circ (0, \ldots, 0) = 0$.

Auch die Einfachheit überträgt sich von Kompositionsgruppen auf Fastringe:

**Proposition 3.1.54** *Es sei $G$ eine distributiv erzeugte k-dimensionale Kompositionsgruppe mit Selektorsystem $\{s_1, \ldots, s_k\}$. Dann ist $G^k$ ein einfacher Fastring genau dann, wenn $G$ eine einfache k-dimensionale Kompositionsgruppe ist.*

**Beweis:** [18] Kapitel 5, Proposition 2.13.

**Beispiel:**

- $F(X) = \langle X \rangle$, also ist $F(X)$ distributiv erzeugt.
- $\underline{P_k(G)^k}$ ist im allgemeinen kein distributiv erzeugter Fastring. Aber $\overline{P_k(G)^k}$ ist distributiv erzeugt, da

  $$\overline{P_k(G)^k} = \langle \{\tau_a \circ \xi_i \,|a \in G, i = 1, \ldots, k\} \rangle = \left\langle \{a\xi_i a^{-1} \,|a \in G, i = 1, \ldots, k\} \right\rangle$$

  (Die Überlegung verläuft analog zu jener in der Bemerkung zu 3.1.52.)

  Dieses Beispiel können wir als Sonderfall des nächsten Beispiels erachten, da $G$ immer ein Normalteiler von sich selbst ist.
- Sei $N \trianglelefteq G$, dann können wir die Polynomfunktionen von $G^k$ auf $N^k$ einschränken und können sehen daß diese Menge $P_k(G, N)$ eine distributiv erzeugte k-dimensionale Kompositionsgruppe ist. Wir werden uns diesem Beispiel im nächsten Abschnitt widmen.

### 3.1.6 Einschränkung der Polynome auf Normalteiler

**Definition 3.1.55** *Es sei $G$ eine Gruppe und $N \trianglelefteq G$. Dann sei: $P_k(G, N) = \{\varphi|_{N^k}$ mit $\varphi \in P_k(G)\}$*

D.h. das sind dann Polynomfunktionen auf $N$ mit Koeffizienten aus $G$, deren Bildbereich $G$ ist.

Für $\mathfrak{M}(G) \subseteq F_k(G)$ haben wir $\overline{\mathfrak{M}(G)}$ als jene Funktionen definiert, die die Eins auf die Eins abbilden. Also ist

$$\overline{P}_k(G, N) = \{\varphi \in P_k(G, N) | \varphi(1, 1, \ldots, 1) = 1\}$$

**Lemma 3.1.56** *Es sei $G$ eine Gruppe und $N \trianglelefteq G$. Dann ist: $\overline{P}_k(G,N) \subseteq F_k(N)$.*

**Beweis:** $p(\mathfrak{x}) \in P_k(G)$ läßt sich schreiben als $a_0\mathfrak{x}^{m_1}a_1\mathfrak{x}^{m_2}a_2\ldots a_{r-1}\mathfrak{x}^{m_r}a_r$. Damit ist für $\mathfrak{n} \in N^k$ $p(\mathfrak{n}) = a_0\mathfrak{n}^{m_1}a_1\mathfrak{n}^{m_2}a_2\ldots a_{r-1}\mathfrak{n}^{m_r}a_r$. Da $N \trianglelefteq G$, ist das $= \mathfrak{n}' \cdot (a_0a_1\ldots a_r)$ für ein $\mathfrak{n}' \in N^k$.

Sei $p(\mathfrak{x}) \in \overline{P}_k(G,N) \Longrightarrow p(\mathfrak{e}) = a_0\mathfrak{e}^{m_1}a_1\mathfrak{e}^{m_2}a_2\ldots a_{r-1}\mathfrak{e}^{m_r}a_r = a_0a_1a_2\ldots a_{r-1}a_r = \mathfrak{e} \Longrightarrow p(\mathfrak{x}) = \mathfrak{n}' \cdot \mathfrak{e} = \mathfrak{n}' \in N$ □

$\overline{P}_k(G,G)$ ist klarerweise bezüglich Komposition $\circ$ abgeschlossen, also ist $\overline{P}_k(G,G) \preceq_\circ P_k(G)$. Die Abbildung $\varphi : P_k(G) \to P_k(G,N)$ mit $\varphi(p) = p|_{N^k}$ ist ein Kompositionsepimorphismus. $((p \circ q)|_{N^k} = p|_{N^k} \circ q|_{N^k})$. Also ist $\varphi\left(\overline{P}_k(G,G)\right) = \overline{P}_k(G,N)$ bezüglich $\circ$ abgeschlossen, und damit eine Kompositionsuntegruppe von $F_k(G)$. Daher ist $\overline{P}_k^k(G,G) \preceq_\circ F_k^k(N)$.

Betrachten wir $P_k(G,N)$ für die minimalen Normalteiler $N$ der endlichen Gruppe G, so gibt es nach A.8.28 zwei Fälle: $N$ ist entweder eine elementar abelsche $p$-Gruppe oder direktes Produkt nicht abelscher einfacher Gruppen.

**Proposition 3.1.57** *Sei $G$ eine endliche Gruppe und $N$ eine abelscher minimaler Normalteiler von $G$. Dann ist $\overline{P}_k^k(G,N)$ ein einfacher Ring.*

**Beweis:** siehe [18] Kapitel 5 Proposition 2.31

Diese beiden Fälle beinhalten wegen A.8.28 alle minimalen normalen abelschen Untergruppen von $G$. Also bleibt noch die nicht abelschen minimalen Untergruppen zu untersuchen:

**Proposition 3.1.58** *Sei $G$ eine endliche Gruppe. $N$ nicht abelscher, minimaler Normalteiler von $G$. Dann ist $\overline{P}_k(G,N) = \{\varphi \in F_k(N) | \varphi(\mathfrak{e}) = 1\}$.*

**Beweis:** siehe [18] Kapitel 5 Proposition 2.4

Die Menge $\overline{P}_k(G,N)$ ist in diesem Fall also die größtmögliche. Alle Abbildungen $\in F_k(N)$ , die $\mathfrak{e}$ auf 1 abbilden, sind bereits Polynome $\in \overline{P}_k(G,N)$.

Die obigen Sätze gelten für einfache Gruppen für $\overline{P}_k(G)$, denn ist $G$ einfach, so ist $G$ ein minimaler Normalteiler.

## 3.2 Länge

Wir können den kanonischen Epimorphismus $\sigma_k[G] : G[X] \to P_k(G)$ betrachten. Nach dem Homomorphiesatz gilt

$$G[X]/ker(\sigma_k[G]) \simeq P_k(G)$$

Da $\sigma_k[G]$ ein Kompositionshomomorphismus ist, gilt das auch wenn die beiden Mengen als Kompositionsgruppen betrachtet werden. Die Elemente aus $ker(\sigma_k[G])$ wollen wir bezeichnen:

**Definition 3.2.1** *Polynome* $\mathfrak{p} \in G[X]$*, für die gilt:* $\sigma_k(\mathfrak{p}) = 1$*, d.h.* $\mathfrak{p} \in ker(\sigma_k[G])$ *nennen wir* **annihilierend**.

Sei nun $\epsilon : G \to F(X)$ der Homomorphismus, der jedes Element von G auf die Eins in $F(X)$ abbildet: $\epsilon : g \mapsto 1$. Nach 3.1.11 gibt es also für $\epsilon$ und $id_{F(X)}$ einen eindeutigen Homomorphismus $\lambda_k[G] : G[X] \to F(X)$ mit $\lambda_k[G]|_{F(X)} = id_{F(X)}$ und $\lambda_k[G]|_G = \epsilon$. Insbesondere gilt also für $p \in G[X]$ mit $p = w(g_i; x_j)$ als Darstellung als Wort in geeigneten $g_i$ und $x_j$: $\lambda_k[G](p) = \lambda_k[G](w(g_i; x_j)) = w(1; x_j)$.

Das ist klarerweise ein Epimorphismus, da $id_{F(X)}$ bereits surjektiv ist.

**Definition 3.2.2** *Wir nennen* $\lambda_k[G]$ *den* **Längenepimorphismus** *von G,* $L_k[G] = \lambda_k[G]\left(ker\left(\sigma_k[G]\right)\right)$ *das* **Längenideal** *von G.*

Wir nennen $L_k[G]$ Längenideal und nicht *Länge von G* (wie z.B. in [18]), da es dem Autor „natürlicher“ erschien, dem Begriff Länge eine Zahl zuzuordnen. Daß $L_k[G]$ tatsächlich ein (Voll-)Ideal ist, werden wir noch zeigen!

**Bemerkung:** Worauf bildet nun $\lambda_k[G]$ ein Polynom ab? Sei zuerst $k = 1$, dann läßt sich $p \in G[x]$ darstellen als

$$p = a_0 x^{n_1} a_1 x^{n_2} ... a_{r-1} x^{n_r} a_r$$

Dann ist

$$\lambda_1[G](p) = 1 \cdot x^{n_1} \cdot x^{n_2} \cdot \ldots \cdot 1 \cdot x^{n_r} \cdot 1 = x^{\sum_{i=1}^{r} n_i}$$

Ist $k > 1$ , so ist $p = a_0 \mathfrak{x}^{\mathfrak{n}_1} a_1 \mathfrak{x}^{\mathfrak{n}_2} ... a_{r-1} \mathfrak{x}^{\mathfrak{n}_r} a_r$, also ist

$$\lambda_k[G](p) = \mathfrak{x}^{\mathfrak{n}_1} \mathfrak{x}^{\mathfrak{n}_2} \ldots \mathfrak{x}^{\mathfrak{n}_r}$$

Das ist jedoch i.A. $\neq \mathfrak{x}^{\sum_{i=1}^{r} \mathfrak{n}_i}$.
Betrachten wir $\mathfrak{p} \in G[X]^k$, so läßt sich $\mathfrak{p}$ darstellen als

$$\mathfrak{p} = \mathfrak{a}_1 \mathfrak{x}^{K_1} \mathfrak{a}_2 \mathfrak{x}^{K_2} \ldots \mathfrak{a}_s \mathfrak{x}^{K_s} \mathfrak{a}_{s+1}$$

Dann ist

$$\lambda_k^k[G](\mathfrak{p}) = 1 \cdot \mathfrak{x}^{K_1} \cdot 1 \cdot \mathfrak{x}^{K_2} \cdot \ldots \cdot 1 \cdot \mathfrak{x}^{K_s} \cdot 1 = \mathfrak{x}^{K_1} \cdot \mathfrak{x}^{K_2} \cdot \ldots \cdot \mathfrak{x}^{K_s} \overset{(i.a.)}{\neq} \mathfrak{x}^{\sum_{i=1}^{s} K_i}$$

**Bemerkung:** F(X) ist klarerweise bezüglich der Komposition

$$w_0 \circ (w_1, \ldots, w_k) = w_0(w_1, \ldots, x_k)$$

eine Kompositionsgruppe mit dem Selektorsystem $\{x_1, x_2, \ldots, x_k\}$. Weiters ist $F(X) \simeq \{1\}[X]$, da $\{1\}[X] = W(1 \cup X)/R = W(X)/R = F(X)$, da 1 eine unäre Operation ist.

**Lemma 3.2.3** *$\lambda_k[G]$ ist ein Kompositionshomomorphismus.*

**Beweis:** Wie bereits erwähnt ist $\lambda_k[G]$ ein Epimorphismus. Da $F(X) = \{1\}[X]$ ist, ist also $[F(X); \cdot, ^{-1}, 1, \circ]$ eine $k$-dimensionale Kompositionsgruppe mit Selektorsystem $\{x_1, \ldots, x_k\}$. Nach Definition ist $\lambda_k[G]$ die eindeutige Erweiterung des Epimorphismus $G \mapsto \{1\}$ und ist somit nach 2.1.21 ein Kompositionsepimorphismus. □

Aus diesem Satz erklärt sich die Bezeichnung von $L_k[G]$, denn $ker(\sigma_k[G])$ ist ein Vollideal, daher ist nach 3.1.29 $L_k[G] = \lambda_k[G]\,(ker(\sigma_k[G]))$ tatsächlich auch ein Vollideal. $L_k[G]$ ist auch Unterkompositionsgruppe, im allgemeinen jedoch ohne Selektorsystem.

**Bemerkung:** Für $X = \{x\}$ ist $F(X) = W(X)/R = W(\{x\})/R$, also ist $F(X)$ zyklisch und somit abelsch. Klarerweise ist $F(X)$ nicht endlich, und somit ist $F(X) \simeq \mathbb{Z}$, wobei der Isomorphismus $\varsigma : [F(x_1); \cdot, ^{-1}, e] \to [\mathbb{Z}, +, -, 0]$ gegeben ist durch $x^k \mapsto k$ abbildet. $\varsigma$ ist auch ein Fastringisomorphismus von $[F(x); \cdot, ^{-1}, e, \ , x]$ nach $[\mathbb{Z}; +, -, 0, \cdot, 1]$ da $\varsigma(x^{l_1} \circ x^{l_2}) = \varsigma(x^{l_1 \cdot l_2}) = l_1 \cdot l_2 = \varsigma(x^{l_1}) \cdot \varsigma(x^{l_2})$

Für $k = 1$ können wir also die Abbildung $l : G[x] \to \mathbb{Z}$ betrachten mit $l = \varsigma \circ \lambda_1[G]$, diese ist ein Fastringepimorphismus, die jedes Polynom $p = a_0 x^{n_1} a_1 x^{n_2} ... a_{r-1} x^{n_r} a_r$ auf $l(p) = \sum_{i=1}^{r} n_i$ abbildet. Dies wollen wir als *Länge* bezeichnen (vergleiche [29]), und soll uns unter anderem als Motivation für die Namensgebung dienen.

Insbesondere wird $\lambda_1[G](ker(\sigma_1[G]))$ durch $\varsigma$ auf ein Ideal von $\mathbb{Z}$ abgebildet. Es gibt also eine positive ganze Zahl $\lambda(G)$ sodaß $\varsigma(L_1[G]) \simeq \lambda(G) \cdot \mathbb{Z}$.

Somit ist $\lambda_1[G](p) \in L_1[G] \Longleftrightarrow \lambda(G)|l(p)$. Dieser Längebegriff für den einstelligen Fall wird in [29] untersucht.

Wir können diesen Längenbegriff für beliebige $k > 0$ definieren:

Sei $\eta_i : [F(X); \cdot, ^{-1}, 1, \circ] \to [\mathbb{Z}; +, -, 0, \cdot]$ die Erweiterung der Abbildung $x_j \mapsto \delta_{ij}$ zu einem Homomorphismus, wobei $\delta_{ij}$ das *Kronecker-Symbol*, d.h. $\delta_{ij} = \begin{cases} 1\ (\in \mathbb{Z}) & i = j \\ 0\ (\in \mathbb{Z}) & sonst \end{cases}$. Es gilt somit $\eta_i(x_i x_j) = \eta_i(x_i) + \eta_i(x_j)$.

Es sei $\pi_i : G[X]^k \to G[X]$ die $i$-te Projektion der Polynomgruppe (im Unterschied zu $\xi_i : G^k \to G$).

Wir können nun eine Funktion von den Polynommatrizen in die $k \times k$ - Matrizen ganzer Zahlen finden:

**Definition 3.2.4** *Es sei*

$$\zeta_k[G] : \left[G[X]^k; \cdot, ^{-1}, 1, \circ, id_G\right] \to [M_k(\mathbb{Z}); +, -, \mathfrak{o}, \cdot, \mathfrak{1}]$$

*jene Abbildung mit*

$$\zeta_k[G](\mathfrak{p}) = \left(\left(\eta_j \circ \lambda_k[G] \circ \pi_i\right)(\mathfrak{p})\right)_{ij}$$

*für* $\mathfrak{p} = (p_1, \ldots, p_k) \in G[X]^k$.

*Wir nennen* $\zeta_k[G](\mathfrak{p})$ *die* **Längenmatrix** *von* $\mathfrak{p}$.

Durch direktes Rechnen analog zu 3.1.18 kann man zeigen

**Lemma 3.2.5** $\zeta_k[G]$ *ist ein Fastringepimorphismus.*

**Definition 3.2.6** $l(\varphi) = det\left(\zeta_k[G](\varphi)\right)$ *heißt die* **Länge** *von* $\varphi$

**Bemerkung:** Wie bildet $l$ nun Polynome ab? Sei wieder zuerst $k = 1$. Dann ist $p = a_0 x^{n_1} a_1 x^{n_2} ... a_{r-1} x^{n_r} a_r$.

$\lambda_1[G](p) = x^{\sum_{i=1}^{r} n_i} \Longrightarrow \zeta_1[G](p) = \eta_j\left(x^{\sum_{i=1}^{r} n_i}\right) = \sum_{i=1}^{r} n_i.$

Sei nun $k > 1$. Dann ist für $\mathfrak{p} \in G[X]^k$, $\mathfrak{p} = \mathfrak{a}_1 \mathfrak{x}^{K_1} \mathfrak{a}_2 \mathfrak{x}^{K_2} \ldots \mathfrak{a}_s \mathfrak{x}^{K_s} \mathfrak{a}_{s+1}$. Also ist

$$\pi_i(\mathfrak{p}) = \mathfrak{a}_1^{(i)} \mathfrak{x}^{K_1^{(i)}} \mathfrak{a}_2^{(i)} \mathfrak{x}^{K_2^{(i)}} \ldots \mathfrak{a}_s^{(i)} \mathfrak{x}^{K_s^{(i)}} \mathfrak{a}_{s+1}^{(i)}$$

$$\Longrightarrow \zeta_k[G](\mathfrak{p}) = \left(\left(\eta_j \circ \lambda_k[G] \circ \pi_i\right)(\mathfrak{p})\right)_{ij} = \left(\sum_{l=1}^{s} (K_l)_{ij}\right)_{ij}$$

Also ist $\zeta_k[G](\mathfrak{p}) = \sum_{l=1}^{s} K_l$. Und somit $l(\mathfrak{p}) = det(\sum_{l=1}^{s} K_l)$

Für abelsche Gruppen gilt: $\zeta_k[G]\left(\mathfrak{a}_{\mathfrak{x}}{}^K\right) = K$ (vgl. Bemerkung nach 3.1.18).

Da $det(A \cdot B) = det(A) \cdot det(B)$ und $det(\mathfrak{1}) = 1$ gilt, ist $l : [G[X]; \circ, \mathfrak{x}] \to [\mathbb{Z}; \cdot, \mathfrak{1}]$ ein Halbgruppenhomomorphismus, der klarerweise surjektiv ist.

Untersuchen wir nun vorerst weitere Eigenschaften von $\lambda_k[G]$ und $L_k[G]$:
$L_k[G]$ ist nicht nur normale Untergruppe (weil Vollideal) von $F(X)$, sondern sogar voll invariant. D.h. dieses Ideal ist nicht nur bezüglich aller innerer Automorphismen, sondern aller Endomorphismen von $F(X)$ abgeschlossen. $L_k(G)$ ist eine Wortuntergruppe (siehe A.8.33).

**Proposition 3.2.7** *$L_k[G]$ ist eine Wortuntergruppe, also insbesondere voll invariant.*

**Beweis:** siehe [18] Kapitel 5, Proposition 1.12.

**Satz 3.2.8** *Ist* $\lambda_k(p) \notin \lambda_k(q) \cdot L_k[G] \Longrightarrow \sigma_k[G](p) \neq \sigma_k[G](q)$

**Beweis:** Denn sei angenommen $\sigma_k[G](p) = \sigma_k[G](q) \Longrightarrow \sigma_k[G](p) \cdot \sigma_k[G](q)^{-1} = 1 \Longrightarrow \sigma_k[G]\left(p \cdot q^{-1}\right) = 1 \Longrightarrow p \cdot q^{-1} \in ker\ \sigma_k[G] \Longrightarrow \lambda_k[G](p \cdot q^{-1}) \in L_k[G] \Longrightarrow \lambda_k[G](p) \cdot \lambda_k[G](q)^{-1} \in L_k[G]$ □

Das heißt, daß Polynome, die dieselbe Polynomfunktion repräsentieren, durch $\lambda_k[G]$ in dieselbe Nebenklasse bezüglich $L_k[G]$ in $F(X)$ abgebildet werden. D.h. $\alpha : P_k(G) \to F(X)/L_k(G)$ definiert durch $\alpha(\sigma_k[G](p)) := \lambda_k[G](p) \cdot L_k[G]$ ist ein wohldefinierter Epimorphismus und das Diagramm in Abb. 3.1 ist kommutativ. D.h. durch Kenntnisse der Längenideale können wir etwas über das Wortproblem aussagen.

Eine weitere Eigenschaft zeigt, daß das Längenideal von Gruppen eine „algebraische“ Eigenschaft insofern ist, daß isomorphe Gruppen dasselbe Längenideal zugeordnet haben.

**Lemma 3.2.9** *Ist $H \simeq G$, so ist $L_k[H] = L_k[G]$.*

**Beweis:** [18] Kapitel 5, Lemma 1.11.

Dieses Resultat kann sich in seiner Umkehrung als nützlich erweisen. Denn um Isomorphie zu zeigen muß man „nur“ einen Isomorphismus angeben, während der Nachweis, daß es keine Isomorphie gibt, manchmal nicht so klar ist. Isomorphe Gruppen müssen jedoch gleiche Längenideale haben, sodaß eine Untersuchung dieses Ideals in dieser Frage Sinn haben kann.

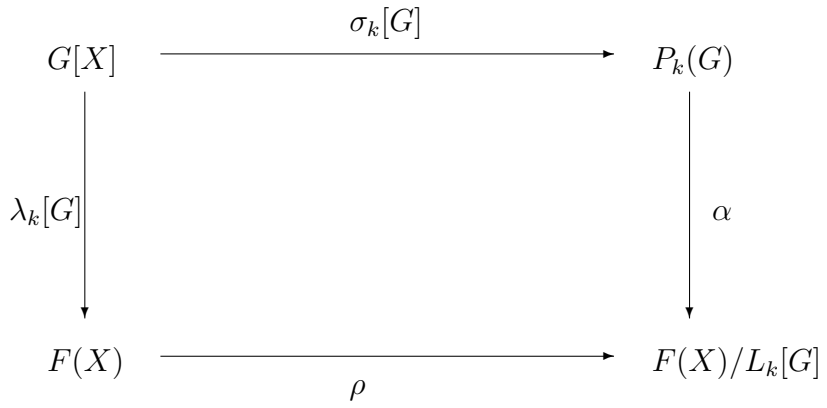


Abbildung 3.1: Länge und Polynomabbildungen

**Proposition 3.2.10** $G[X]/ker\sigma_k[G]ker\lambda_k[G] \simeq F(X)/L_k[G]$

**Beweis:**

$$F(X)/L_k(G) = \lambda_k[G](G[X])/\lambda_k[G]\left(ker\left(\sigma_k[G]\right)\right) \simeq$$

$$\simeq \left(G[X]/ker\left(\sigma_k[G]\right)\right)/ker\left(\lambda_k[G]\right) \simeq G[X]/\left(ker\left(\sigma_k[G]\right) \cdot ker\left(\lambda_k[G]\right)\right)$$

nach A.8.15 und A.8.19. □

**Satz 3.2.11** *Sei $G$ eine Gruppe. $k \in \mathbb{Z}$, $k \geq 1$. Es sei $X = \{x_1, \ldots, x_k\}$. Die folgenden Eigenschaften sind äquivalent*

1. $L_k[G] = F(X)$
2. $G[X] = ker(\sigma_k[G]) \cdot ker(\lambda_k[G])$
3. $\exists i, 1 \leq i \leq k : x_i \in L_k(G)$
4. $\forall i, 1 \leq i \leq k : x_i \in L_k[G]$
5. $\exists \mathfrak{p} \in \mathcal{E}(P_k(G)^k)$ *mit* $\lambda_k[G]^k(\mathfrak{p}) \in L_k[G]^k$
6. $\forall \mathfrak{p} \in \mathcal{E}(P_k(G)^k) : \lambda_k[G]^k(\mathfrak{p}) \in L_k[G]^k$

**Beweis:** $1 \Longrightarrow 3$, $1 \Longrightarrow 4$, $1 \Longrightarrow 5$ und $1 \Longrightarrow 6$ ist klar. Ebenso $4 \Longrightarrow 3$ und $6 \Longrightarrow 5$. $1 \Longleftrightarrow 2$ folgt aus Proposition 3.2.10

$3 \Longrightarrow 1$ folgt, da wir aus Lemma 3.1.37 wissen, daß mit $q \in A$, $A$ Vollideal von $F(X) = 1[X]$, auch $q \circ (p_1, \ldots, p_k) \in A$ für alle $p_i \in F(X)$, $i = 1, \ldots, k$.

Ist also $x_i \in L_k(G)$ so ist auch $x_i \circ (1, \ldots, 1, \lambda_k[G](p), 1, \ldots, 1) = \lambda_k[G](p) \in A$.

Es bleibt also noch zu zeigen $5 \Longrightarrow 4$. Seien nun also $\mathfrak{p}$ und $\mathfrak{q}$ in $\mathcal{E}(P_k(G)^k)$, mit

$$\sigma_k[G]^k(\mathfrak{p}) \circ \sigma_k[G]^k(\mathfrak{q}) = \sigma_k[G]^k(\mathfrak{p} \circ \mathfrak{q}) = id_{G^k}$$

also ist

$$(\mathfrak{p} \circ \mathfrak{q}) \cdot \mathfrak{x}^{-1} \in ker\sigma_k[G]^k$$

Und somit gilt

$$(\lambda_k[G]^k(\mathfrak{p} \circ \mathfrak{q})) \cdot \lambda_k[G]^k(\mathfrak{x}^{-1}) \in L_k[G]$$

also

$$\lambda_k[G]^k(\mathfrak{x}^1) \in (\lambda_k[G]^k(\mathfrak{p} \circ \mathfrak{q}))^{-1} L_k[G]$$

Sei nun $\lambda_k[G]^k(\mathfrak{p}) \in L_k[G]$. Da $L_k[G]$ ein Vollideal ist, gilt somit $\lambda_k[G]^k(\mathfrak{p}) \circ \lambda_k[G]^k(\mathfrak{q}) \in L_k[G]^k$, also $\lambda_k[G]^k(\mathfrak{p} \circ \mathfrak{q}) \in L_k[G]$. Damit ist also

$$(x_1, \ldots, x_k) = \lambda_k[G]^k(\mathfrak{x}^1) \in (\lambda_k[G]^k(\mathfrak{p} \circ \mathfrak{q}))^{-1} L_k[G] = L_k[G]$$

□

**Bemerkung:** Es gilt also

- Für Gruppen, wo das Längenideal nicht ganz $F(X)$ ist, wird kein invertierbares Polynom in $L_k[G]^k$ abgebildet.
- Für eine Gruppe, die eine der Bedingungen erfüllt, kann jedes Polynom $p$ als Produkt zweier Polynome $q_1, q_2$ dargestellt werden, wo eines durch den Längenepimorphismus auf 1 abgebildet wird und das andere als Polynomfunktion identisch 1 ist.
- Für einstellige Polynome, $k = 1$, betrachte $\lambda(G)$ aus der Bemerkung vor 3.2.4. Ist $\lambda(G) = 1$ so ist genau dann $L_k[G] = F(X)$, also sagt dieser Satz, daß für $\lambda(G) \neq 1$ , $\lambda(G)$ nicht $l(p)$ teilt!

Die folgende Eigenschaft folgt direkt aus der Definition des Längenepimorphismus:

**Lemma 3.2.12** *Es seien $G$ und $H$ Gruppen. Ist $\varphi : G \to H$ ein Homomorphismus, so ist für alle $k$*

$$\lambda_k[G] = \lambda_k[H] \circ \varphi[X]$$

*Ist $\eta$ ein Epimorphismus, so ist das Diagramm in Abbildung 3.2 kommutativ.*

*Insbesondere ist $L_k[G] \subseteq L_k(H)$, wenn es einen Epimorphismus $\eta : G \to H$ gibt.*

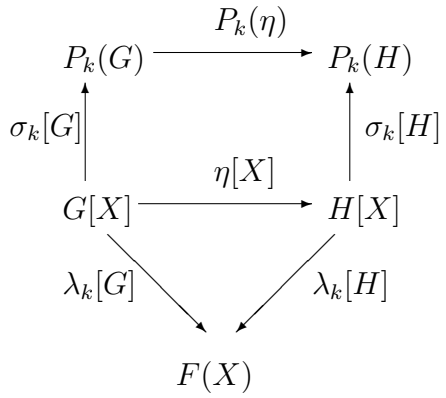


Abbildung 3.2: Beziehung der Längenepimorphismen

**Beweis:** Sei $\varphi : G \to H$ ein Homomorphismus, dann ist für $p = w(g_i; x_j)$

$$\varphi[X](p) = \varphi[X](w(g_i; x_j) = w(\varphi(g_i); x_j)$$

Somit ist aber

$$\lambda_k[G](p) = w(1; x_j) = \lambda_k[H](\varphi[X](p))$$

Sei $\eta \in Epi(G, H)$. Ist $\lambda_k[G](p) \in L_k(G)$, so ist obdA $p \in ker(\sigma_k[G])$, dann ist $\sigma_k[G](p) = 1$, also ist $P_k(\eta)(\sigma_k[G](p) = 1$. Damit ist jedoch $\sigma_k[H](\eta[X](p)) = 1$. Also ist $\eta[X](p) \in ker(\sigma_k[H]$. Daraus folgt:

$$\lambda_k[H](\eta[X](p)) \in L_k(H).$$

Nach oben gilt also: $\lambda_k[G](p) \in L_k(H)$. Somit gilt also: $L_k[G] \subseteq L_k[H]$. $\square$

**Proposition 3.2.13** *Ist $N \trianglelefteq G$, so ist $L_k[G] \subseteq L_k[G/N]$. Weiters gilt $L_k[G/N] \circ L_k[N]^k \subseteq L_k[G]$*

**Beweis:** Die Beziehung $L_k[G] \subseteq L_k[G/N]$ folgt mit $\pi : G \to G/N$ aus 3.2.12.

Sei nun $\lambda_k[N](p) \in L_k(N)$, wähle obdA $p$ so, daß $p \in ker(\sigma_k[N])$. Sei weiters für $l = 1, \ldots, k$ $\lambda_k(q_l) \in L_k(G/N)$ mit $q_l \in ker(\sigma_k[G/N])$. Es ist also $\sigma_k[G/N](q_l) = 1$, also ist $\forall g_i \in G, i = 1, \ldots, k : q_l(g_1N, \ldots, g_kN) = N$. Da $q_l \in G/N[X]$ existiert ein $q_l' \in G[X]$ mit $\pi[X](q_l') = q$, wobei $\pi : G \to G/N$ der kanonische Epimorphismus sei. Dann ist also

$$(\pi[X]\,(q_l'))\,(g_1N, \ldots, g_kN) = N$$

ausführlicher angeschrieben heißt das

$$(\sigma_k[G/N]\,(\pi[X]\,(q_l')))\,(g_1N, \ldots, g_kN) = N$$

$$\iff (P_k(\pi)\,(\sigma_k[G]\,(q_l')))\,(\pi(g_1), \ldots, \pi(g_k)) = \pi(1)$$

$$\overset{2.1.28}{\iff} \pi\left(\left(\sigma_k[G]\left(q_l'\right)\right)\left(g_1,\ldots,g_k\right)\right) = \pi(1)$$
$$\iff \left(\sigma_k[G]\left(q_l'\right)\right)\left(g_1,\ldots,g_k\right) \in ker(\pi) = N$$
$$\implies \sigma_k[N]\left(p\right)\left(\left(\sigma_k[G]\left(q_1'\right),\ldots,\sigma_k[G]\left(q_k'\right)\right)\left(g_1,\ldots,g_k\right)\right) = 1$$
$$\iff \sigma_k[G]\left(p\right)\left(\sigma_k[G]\left(q_1'\right),\ldots,\sigma_k[G]\left(q_k'\right)\right)\left(g_1,\ldots,g_k\right) = 1$$
$$\iff \sigma_k[G]\left(p \circ \left(q_1',\ldots,q_k'\right)\right)\left(g_1,\ldots,g_k\right) = 1$$
$$\iff \left(p \circ \left(q_1',\ldots,q_k'\right)\right) \in ker\sigma_k[G]$$
$$\implies \lambda_k[G](p) \circ \left(\lambda_k[G]\left(q_1'\right),\ldots,\lambda_k[G]\left(q_k'\right)\right) \in L_k[G]$$

□

**Proposition 3.2.14** *Es seien $G_1, G_2$ Gruppen.* $L_k[G_1 \times G_2] = L_k[G_1] \cap L_k[G_2]$

**Beweis:** siehe [18] Kapitel 5, Proposition 1.2

D.h., bei der Untersuchung des Längenideals von Produkten müssen wir nur den Durchschnitt der Faktoren betrachten.

### 3.2.1 Endliche Gruppen

In diesem Abschnitt werden kurz Aussagen für das Längenideal endlicher Gruppen zitiert.

**Proposition 3.2.15** *Sind $G_1$,$G_2$ endliche Gruppen und $G = G_1 \times G_2$. Dann ist der Dekompositionshomomorphismus $\tau_2 : P_k(G) \to P_k(G_1) \times P_k(G_2)$ (2.1.31) ein Isomorphismus genau dann wenn $L_k[G_1] \cdot L_k[G_2] = F(X)$.*

**Beweis:** [18] Kapitel 5, Korollar 1.22

**Lemma 3.2.16** *Ist $G$ eine endliche einfache nicht abelsche Gruppe, so ist $L_k[G] = F(X)$ $\forall k$.*

**Beweis:** [18] Kapitel 5, Korollar 2.43

In diesem Fall treffen also alle in 3.2.11 zitierten Bedingungen ein.

## 3.3 Polynompermutationen

Wir wollen nun die Halbgruppe $U_k(G) = P_k(G)^k \cap \widetilde{Sym(G)}$ untersuchen. Wir können für Gruppen einige grundlegende Resultate formulieren:

**Lemma 3.3.1** *Sei $G$ eine Gruppe. Die Abbildung $p_1(\mathfrak{x}) = \mathfrak{a}\mathfrak{x}^K \in U_k(G)$ $\Longleftrightarrow p_2(\mathfrak{x}) = \mathfrak{x}^K \in U_k(G)$*

**Beweis:** Klarerweise sind beides Polynome. Verwende A.3.8. Es gilt: $p_1 = (\mathfrak{a}\mathfrak{x}) \circ p_2$ und $p_2 = (\mathfrak{a}^{-1}\mathfrak{x}) \circ p_1$. D.h. $p_1$ injektiv $\Longleftrightarrow$ $p_2$ injektiv.

Sei $\mathfrak{b} = (b_1, b_2, \ldots, b_k)$ beliebig $\in G^k$, dann bildet $q(\mathfrak{x}) = \mathfrak{a}\mathfrak{x}$ das Element $\mathfrak{a}^{-1} \cdot \mathfrak{b}$ auf $\mathfrak{b}$ ab. Also ist $q(x)$ surjektiv. D.h. aber mit $p_1, q$ ist auch $p_2$ surjektiv, mit $p_2, q' = \mathfrak{a}^{-1}\mathfrak{x}$ auch $p_1$. □

Insbesondere folgt , daß $\mathfrak{a}\mathfrak{x}$ in $U_k(G)$ (das ist jedoch klar, weil die Linkstranslation immer bijektiv ist). Weiters ist auch klarerweise $Inn\left(G^k\right) \subseteq U_k(G)$.

Wir wissen, daß nach 2.3.4

$$\mathcal{E}(P_k(A)^k) \subseteq U_k(A) \subseteq \mathcal{C}(P_k(A)^k)$$

gilt, sowie, daß im endlichen Fall Gleichheit gilt. Im allgemeinen sind diese Inklusionen jedoch echt. Für den zweiten Teil konnten wir bereits eine Gruppe angeben, für die diese Inklusion echt ist. (In der unendlichen zyklischen Gruppe ist $\xi_1^2 \notin U_1(A)$ aber $\xi_1^2 \in \mathcal{C}(P_1(A))$.) Für die erste Inklusion konnten wir nur ein Gegenbeispiel aus der Varietät der Ringe angeben.

Wann gilt die erste Gleichheit in der Varietät der Gruppen? Wann ist sie echte Inklusion? Diese Frage fällt mit der Frage, wann $U_k(G)$ eine Gruppe ist, zusammen.

$$U_k(G) \text{ ist Gruppe } \Longleftrightarrow \mathcal{E}(P_k(G)^k) = U_k(G)$$

Wir werden uns diese Frage ab dem nächsten Abschnitt widmen, zuerst im Fall von abelschen Gruppen.

Doch zuvor sei noch kurz der Fall $k = 1$ betrachtet und der Exponent der Gruppe $exp(G)$ als endlich voausgesetzt. Es gehört dann die Polynomfunktion $\xi^n$ genau dann zu $U_1(G)$, wenn $ggT(n, exp(G)) = 1$.

Denn es gilt einerseits, wenn $exp(G)$ endlich ist, daß

$$ggT(n, exp(G)) = 1 \Longrightarrow \exists l, l' : l \cdot n + l' \cdot exp(G) = 1$$

$$\Longrightarrow \xi^{l\cdot n+l'\cdot exp(G)} = \xi \Longleftrightarrow \xi^{l\cdot n}\cdot\xi^{l'\cdot exp(G)} = \xi \Longleftrightarrow \xi^{l\cdot n} = \xi$$
$$\Longleftrightarrow \xi^l \circ \xi^n = \xi^n \circ \xi^l = \xi$$

Also ist $\xi^n$ invertierbar, i.e. $\xi^n \in \mathcal{E}(P_1(G)) \subseteq U_1(G)$.

Sei $\xi^n \in U_1(G)$ und sei angenommen $d = ggT(n, exp(G)) > 1$. Sei $p$ prim mit $p|d$. Da es zumindest $p$ Elemente $g \in G$ gibt mit $g^n = e$, ist $\xi^n$ nicht injektiv, Widerspruch.

Daraus folgt insbesondere, daß für $\xi^n \in U_1(G)$ gilt $\xi^n \in \mathcal{E}(P_1(G))$.

Also zusammengefaßt

**Lemma 3.3.2** *Es sei $G$ eine Gruppe mit endlichen Exponenten, dann gilt*

$$\xi^n \in U_1(G) \Longleftrightarrow ggT(n, exp(G)) = 1 \Longleftrightarrow \xi^n \in \mathcal{E}(P_1(G))$$

### 3.3.1 Abelsche Gruppen

Wir wollen zuerst beliebige abelsche Gruppen betrachten und einige Eigenschaften von $P_k(G)^k$ und $U_k(G)$ angeben.

Für den eindimensionalen Fall können wir die folgende Aussage treffen. Dazu sei $\varphi$ die Eulersche $\varphi$-Funktion (A.7.4).

**Proposition 3.3.3** *Ist $G$ abelsch, so ist $U_1(G)$ dann und nur dann eine Gruppe, wenn sie entweder*
*(i) nur durch Elemente der Form $p(x) = a \cdot x$ repräsentiert wird oder*
*(ii) $exp(G)$ endlich ist.*
*Gilt (i) so ist $U_1(G) \simeq G$, gilt (ii) so ist $U_1(G) = \{a \cdot \mathfrak{x}^k | a \in G, k \in \mathbb{Z}_{exp(G)} : ggT(k, exp(G)) = 1\}$, also ein halbdirektes Produkt von $G$ und $\mathcal{E}(\mathbb{Z}_{exp(G)})$. Für endliche $G$ gilt also $|U_1(G)| = |G| \cdot \varphi(exp(g))$*

**Beweis:** Wir wissen, daß $a \cdot \xi \in U_1(G)$ ist. Sei nun $U_1(G)$ eine Gruppe, in der auch ein Element $a \cdot \xi^k$ mit $k > 1$ enthalten ist. Nach 3.3.1 ist also auch $\xi^k \in U_1(G) = \mathcal{E}(P_1(G))$. Daher gibt es ein $p = b\xi^l \in P_1(G)$, sodaß $\left(b\xi^l\right) \circ \xi^k = \xi^k \circ \left(b\xi^l\right) = \xi$, insbesondere folgt durch das Einsetzen der Eins, daß $b = 1$ ist. Also ist

$$\xi^{l\cdot k} = \xi^{k\cdot l} = \xi \Longleftrightarrow$$
$$\xi^{l\cdot k-1} = 1 \Longrightarrow exp(G)|(l \cdot k - 1)$$

Der Exponent ist insbesondere endlich, da $l \cdot k - 1 \neq 0$.

Enthält umgekehrt $U_1(G)$ nur die Linkstranslationen, so ist klarerweise $U_1(G) \simeq G$ und somit eine Gruppe. Ist der Exponent der abelschen Gruppe $G$ endlich, so enthält $U_1(G)$ nach den Lemmas 3.1.6, 3.3.2 und 3.3.1 nur solche $a \cdot \xi^k$, für die gilt $ggT(k, exp(G)) = 1$. Wieder nach Lemma 3.3.1

folgt, daß $\xi^k \in \mathcal{E}(P_1(G))$. Da $a \cdot \xi$ für alle $a \in G$ klarerweise in dieser Gruppe liegt, folgt $U_1(G) \subseteq \mathcal{E}(P_1(G))$ und somit Gleichheit. Also ist $U_1(G)$ Gruppe.

Nach 3.1.13 können wir uns auf jene $\xi^k$ mit $0 \leq k < exp(G)$ beschränken. $\mathfrak{L} = \{a \cdot \xi | a \in G\}$ ist ein Normalteiler von $U_1(G)$, denn $\left(b \cdot x^k\right) \circ (a \cdot x) = \left(a^k \cdot x\right) \circ \left(b \cdot x^k\right)$. Für $\mathfrak{P} = \{\xi^k | ggT(k, exp(G)) = 1\}$ gilt klarerweise $\mathfrak{P} \simeq \mathfrak{P}_{exp(G)} = \mathcal{E}(\mathbb{Z}_{exp(G)})$ und $\mathfrak{P} \cap \mathfrak{L} = \{1\}$, also ist $U_1(G) \simeq G \times_s \mathfrak{P}_{exp(G)}$ □

Es folgt, daß die Inklusion $\mathcal{E}(P_1(G)) \subseteq U_1(G)$ im allgemeinen echt ist! Wir wissen, daß sie genau dann nicht echt ist, wenn $U_1(G)$ eine Gruppe ist. Denn sei z.B. $[\mathbb{Z}, +, -, 0]$, dann kann $x + x$ nicht durch $a + x$ dargestellt werden, also ist $U_1(G)$ nach oben keine Gruppe.

**Proposition 3.3.4** *Ist $G$ periodisch und abelsch. $U_1(G)$ ist genau dann eine Gruppe, wenn $G$ endlichen Exponenten hat oder unter den Ordnungen der Elemente von $G$ jede Primzahl vorkommt.*

**Beweis:** Ist $U_1(G)$ Gruppe und hat $G$ nicht endlichen Exponenten, so ist nach 3.1.18 $U_1(G) = \{g\xi | g \in G\}$. Alle Abbildungen der Form $x \mapsto x^k$ mit $k > 1$ sind somit keine Permutationen auf $G$. Da $G$ periodisch ist, ist es nach A.8.35 direktes Produkt von eindeutig bestimmten primär abelschen Gruppen $G_{p_i}$, d.h. es existiert ein $l$, sodaß $exp(G_{p_i}) = p_i^l$. Ist $(k, p_i) = 1$ für alle diese $p_i$, so ist $x \mapsto x^k$ nach 3.3.2 eine Permutation auf $G_{p_i}$ und somit auf ganz $G$.

D.h. für alle $k \in \mathbb{Z}$ muß es ein $p_\nu$ geben, sodaß $p_\nu | k$. Also müssen in den primären ableschen Gruppen $G_{p_\nu}$ alle Primzahlen vorkommen. □

Wir werden uns nun im nächsten Abschnitt den Polynompermutationen der endlichen, abelschen Gruppen zuwenden.

### 3.3.2 Endliche abelsche Gruppen

In diesem Abschnitt sei die abelsche Gruppe $G$ als endlich vorausgesetzt.

Wir wissen, daß die Polynommatrizen über abelsche Gruppen die Form $\mathfrak{a}\xi^K$ haben. Diese Behauptung ist für endliche Gruppen aber umkehrbar, sodaß diese Gestalt der Polynompermutationenmenge klassifizierend für die abelschen Gruppen ist:

**Satz 3.3.5** *Alle Elemente aus $U_k(G)$ haben die Gestalt $\varphi(\mathfrak{x}) = \mathfrak{a} \cdot \mathfrak{x}^K$ genau dann, wenn $G$ abelsch ist.*

**Beweis:** $\Longleftarrow$ Diese Richtung ist wegen 3.1.10 klar.
$\Longrightarrow$ Sei $k > 1$ und $p = c_0 x_1 c_1 x_1 c_2 ... c_{m-1} x_1 c_m \in P_1(G)$ ein beliebiges Polynom

in $x_1$. Nach Voraussetzung gilt

$$\begin{pmatrix} c_0x_1c_1x_1c_2...c_{m-1}x_1c_m \\ x_2 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} a_1\mathfrak{x}^{\mathfrak{m}_1} \\ a_2\mathfrak{x}^{\mathfrak{m}_2} \\ \vdots \\ a_k\mathfrak{x}^{\mathfrak{m}_k} \end{pmatrix}$$

D.h. die Voraussetzung ist auch für $k = 1$ erfüllt. Wir zeigen, daß daraus $G$ abelsch folgt.

Sei also $k = 1$. Alle $p \in U_1(G)$ lassen sich also als $x \mapsto ax^n$ darstellen. D.h. auch die Rechtstranslation $\rho_b = x \cdot b$ läßt sich so darstellen:

$$x \cdot b = ax^n$$

Setzen wir das Einselement ein, so sehen wir, daß $a = b$ ist. Das $n$ ist natürlich von $b$ abhängig, sodaß wir $n = n(b)$ schreiben. Es gilt dann

$$x \cdot b = b \cdot x^{n(b)}$$

und somit

$$b^{-1} \cdot x \cdot b = x^{n(b)}$$

Also kann man zu jedem inneren Automorphismus $\tau_b = b \cdot x \cdot b^{-1}$ ein $n \in \mathfrak{P}_{exp(G)} = \mathcal{E}(\mathbb{Z}_{expG})$ zuordnen, also

$$\tau_b \mapsto n(b^{-1})$$

Diese Abbildung ist nach oben injektiv und ein Homomorphismus $[Inn(G); \circ] \to [\mathfrak{P}_{expG}; \cdot]$. Insbesondere ist $Inn(G)$ also abelsch. Damit ist jedoch $G/Z(G) \simeq Inn(G)$ abelsch. Somit ist $G$ jedoch nilpotent (der Klasse $c(G) \leq 2$), somit also Produkt seiner $p$-Sylowgruppen $G_{p_\nu}$. Also gibt es ein $h \in G$ mit $o(h) = exp(G)$ (siehe A.8.23).

Setzen wir in die obere Gleichung $b$ ein, so folgt $b^{-1} \cdot b \cdot b = b^{n(b)}$, also $b^{n(b)-1} = 1$ für alle $b$. Also gilt für das gerade gefundene $h$, daß $expG | k(h) - 1$. Also gilt, wenn gilt $expG \cdot m = n(h) - 1$ für ein $m \in \mathbb{N}$

- $\xi^{n(h)-1} = \xi^{expG \cdot m} = 1 \Longleftrightarrow \xi^{n(h)} = \xi$
- $h^{-1}\xi h = \xi^{n(h)} = \xi \Longrightarrow h \in Z(G)$

Daraus folgt, daß $exp(Z(G)) = exp(G)$. Für $z \in Z(G)$, $b \in G$ gilt also $z^{k(b)} = b^{-1}zb = z$. Also $expG | n(b) - 1$ und $\xi^{n(b)} = \xi$. Somit ist also $\xi b = b\xi$ für alle $b \in G$, also ist $G$ abelsch. □

Eine analoge Aussage für einstellige Polynompermutationen kann für (beliebige) kommutative Halbgruppen mit Eins gemacht werden. Wir werden uns kurz diesem Thema in Abschnitt 3.4 widmen.

Es kann ein weiterer interessanter Sachverhalt bemerkt werden. Aus $G \simeq H$ folgt klarerweise, daß $U_k(G) \simeq U_k(H)$. Für abelsche Gruppen und einstellige Polynompermutationen gilt die Umkehrung:

**Proposition 3.3.6** *Es seien $G$, $H$ abelsche Gruppen mit $U_1(G) \simeq U_1(H)$, dann ist $G \simeq H$.*

**Beweis:** siehe [20] Satz 1

Für endliche Gruppen kann der zweite Teil von 3.3.3 auch für mehrstelligen Permutationen formuliert werden:

**Proposition 3.3.7** *Sei $G$ endlich, abelsch. Dann ist $U_k(G)$ isomorph zum semidirekten Produkt von $G^k$ mit den Einheiten von $M_k(\mathbb{Z}_{expG})$, den $k \times k$-Matrizen über den ganzen Zahlen modulo $expG$. $P_k(G)$ ist isomorph zum halbdirekten Produkt von $G^k$ mit $M_k(\mathbb{Z}_{expG})$.*

$$U_k(G) \simeq G^k \times_\mu \mathcal{E}\left(M_k\left(\mathbb{Z}_{exp(G)}\right)\right)$$

$$P_k(G)^k \simeq G^k \times_\mu M_k(\mathbb{Z}_{exp(G)})$$

*Also gilt insbesondere*

$$|U_k(G)| = |G|^k \, \varphi_n(exp(G))$$

$$\left|P_k(G)^k\right| = |G|^k \, exp(G)^{k^2},$$

*wobei $\varphi_n$ die verallgemeinerte Eulerfunktion (siehe A.7.6) ist.*

**Beweis:** Nach 3.1.10 läßt sich $\mathfrak{p} \in P_k^k(G)$ repräsentieren durch $\mathfrak{a}\mathfrak{x}^M$. Für $\mathfrak{q} \in \overline{P}_k(G)^k$ gilt somit $\mathfrak{q} = \mathfrak{x}^M$. Sei $\gamma : \overline{P}_k(G)^k \to M_k(\mathbb{Z}_{expG})$ mit $\mathfrak{q} \mapsto (m_{ij} \; mod \; exp(G))_{ij}$. Ist $\pi : \mathbb{Z} \to \mathbb{Z}_{expG}$ mit $z \mapsto z \; mod \; exp(G)$. Dann ist $\pi$ ein Fastringepimorphismus, denn klarerweise gilt $\pi(z_1 + z_2) = \pi(z_1) + \pi(z_2)$ und $\pi(z_1 \cdot z_2) = \pi(z_1) \cdot \pi(z_2)$. $\gamma(\mathfrak{p})$ läßt sich schreiben als $\pi^{k\times k} \circ \zeta_k[G](\mathfrak{p}')$, wobei $\zeta_k[G]$ die Längenmatrixabbildung aus 3.2.4 ist, $\pi^{k\times k}$ die Funktion sein soll, wo $\pi$ auf jeden einzelnen Eintrag angewendet wird und $\mathfrak{p}'$ ein Polynom in $G[X]^k$ mit $\sigma_k[G]^k(\mathfrak{p}') = \mathfrak{p}$.

$\pi^{k\times k}$ ist auch ein Epimorphismus, denn einerseits gilt für zwei $k \times k$ Matrizen $A, B$ klarerweise $\pi^{k\times k}(A+B) = \pi^{k\times k}(A) + \pi^{k\times k}(B)$, denn die Addition

von Matrizen entspricht der komponentenweisen Addition. Andererseits betrachte $C = A \cdot B$, dann ist der Eintrag von $C$ in der $i$ten Zeile und $j$ten Spalte

$$c_{ij} = \sum_{l=1}^{k} a_{il} \cdot b_{lj}$$

Somit gilt

$$\left(\pi^{k\times k}(A \cdot B)\right)_{ij} = \pi\left(\sum_{l=1}^{k} a_{il} \cdot b_{lj}\right) =$$

$$= \sum_{l=1}^{k} \pi(a_{il} \cdot b_{lj}) = \sum_{l=1}^{k} \pi(a_{il}) \cdot \pi(b_{lj}) =$$

$$= \left(\pi^{k\times k}(A) \cdot \pi^{k\times k}(B)\right)_{ij}$$

Ist $\gamma$ eine wohldefinierte Funktion, so ist sie daher ein Epimorphismus. Das ist sie, denn angenommen $\mathfrak{x}^M$ und $\mathfrak{x}^{M'}$ repräsentieren die selbe Funktion, dann gilt das in jeder Koordinate i: $\mathfrak{x}^{\mathfrak{m}_i} = \mathfrak{x}^{\mathfrak{m}'_i} \Longleftrightarrow x_1^{m_{i1}} \cdot x_2^{m_{i2}} \cdot \ldots \cdot x_k^{m_{ik}} = x_1^{m'_{i1}} \cdot x_2^{m'_{i2}} \cdot \ldots \cdot x_k^{m'_{ik}}$. Das gilt natürlich auch angewendet auf $(1, \ldots, 1, y_j, 1, \ldots, 1)$ für beliebige j $\Longrightarrow y_j^{m_{ij}} = y_j^{m'_{ij}}$. Also ist $y_j^{m_{ij}-m'_{ij}} = 1$, also teilt $expG\, m_{ij} - m'_{ij}$ $\Longrightarrow m_{ij} \equiv_{expG} m'_{ij}$. (Vergleiche 3.1.16 )

Hieraus sieht man auch, daß $\gamma$ injektiv ist. Also ist $\gamma$ ein Fastringisomorphismus von $\overline{P}_k(G)^k$ nach $M_k(\mathbb{Z}_{expG})$.

Jedes $\mathfrak{p} \in P_k(G)^k$ läßt sich schreiben als

$$\mathfrak{p} = \mathfrak{p}(e) \cdot \left((\mathfrak{p}(e))^{-1} \cdot \mathfrak{p}\right) = \mathfrak{p}(e) \cdot \mathfrak{q}$$

mit $\mathfrak{q} \in \overline{P}_k(G)^k$. Also ist $P_k(G)^k = G^k \cdot \overline{P}_k(G)^k$ für $G^k \subseteq P_k(G)^k$. Klarerweise ist $G^k \cap \overline{P}_k(G)^k = \{1\}$, also ist $P_k(G)^k$ das halbdirekte Produkt dieser Mengen.

Welche Polynome $\mathfrak{p}$ aus $\overline{P}_k(G)^k$ sind invertierbar? Da $\gamma$ ein Isomorphismus ist, sind das natürlich genau jene, für die $\gamma(\mathfrak{p}) \in \mathcal{E}(M_k(\mathbb{Z}_{expG}))$. Nach 3.3.1 ist $\mathfrak{p}$ genau dann Permutation, wenn $(\mathfrak{p}(e))^{-1} \cdot \mathfrak{p}$ das ist. Somit folgt die Behauptung. □

Für abelsche Gruppen ist, wie man hier leicht sieht, $\overline{P}_k(G)^k = T_k(G)^k$. Die Termfunktionen sind nach dem obigem Beweis ein Ring. Also gilt

**Korollar 3.3.8** *Es sei $G$ eine abelsche Gruppe, dann ist $\overline{P}_k(G)^k = T_k(G)^k$ ein Ring mit Eins.*

### 3.3.3 Endliche Gruppen

Betrachten wir in diesem Abschnitt beliebige endliche Gruppen. Wir können 2.3.5 Punkt 3 für endliche Gruppen formulieren und verschärfen:

**Lemma 3.3.9** *Sei $G$ endliche Gruppe, $\eta : G \to H$ ein Epimorphismus und $P_k(\eta) : P_k(G) \to P_k(H)$ die Erweiterung zu einem Kompositionsepimorphismus (2.1.26). Dann gilt: $P_k^k(\eta)\,(U_k(G)) = U_k(H)$.*

**Beweis:** siehe [18] Kapitel 5, Satz 3.3

Daraus folgt direkt:

**Korollar 3.3.10** *Ist $G$ nicht einfach, so ist der Fastring $[U_k(G); \cdot, ^{-1}, 1, \circ, \mathfrak{x}^1]$ nicht einfach. (Und damit ist weder die Gruppe $[U_k(G); \cdot, ^{-1}, 1]$ noch die Halbgruppe mit Eins $[U_k(G); \circ, \mathfrak{x}^1]$ einfach.)*

**Beweis:** Es sei $\varphi : G \to H$ ein Homomorphismus in eine Gruppe $H$, der kein Monomorphismus ist und nicht auf die einelementige Gruppe abbildet. D.h.:

$$\{1\} \subset Ker(\varphi) \subset G$$

Dieser Homomorphismus existiert, da $G$ nicht einfach ist. $\varphi$ ist klarerweise ein Epimorphismus $\varphi : A \to \varphi(A)$. Also können wir die Abbildung $P_k(\varphi)^k : P_k(A)^k \to P_k(\varphi(A))^k$ betrachten. Sei $\mathfrak{a} \in Ker(\varphi)^k$, dann ist $\mathfrak{p} = \mathfrak{a}$ in $Ker(P_k(\varphi)^k)$. Für $\mathfrak{b} \in (G \backslash Ker\,(\varphi))^k$ ist aber $\mathfrak{q} = \mathfrak{b}$ nicht in $Ker(P_k(\varphi)^k)$. Also gilt

$$\{1\} \subset Ker(P_k(\varphi)^k) \subset U_k(G)$$

Somit ist mit 1.1.29 der Fastring $U_k(G)$ nicht einfach. □

**Proposition 3.3.11** *Seien $G_1, G_2$ zwei endliche Gruppen und $G = G_1 \times G_2$. Dann bildet der Dekompositionshomomorphismus $\psi_2 \circ \tau_2^k$ (2.1.34) $U_k(G)$ genau dann isomorph auf $U_k(G_1) \times U_k(G_2)$ ab, wenn entweder*
*1.) $L_k(G_1) \cdot L_k(G_2) = F(X)$ oder*
*2.) $k = 1$ und $L_k(G_1) \cdot L_k(G_2) = \langle x^2 \rangle$*

**Beweis:** siehe [18] Kapitel 5, Satz 3.31

**Korollar 3.3.12** *Sind $G_1, G_2$ endliche Gruppen und $ggT(|G_1|, |G_2|) = 1$ , dann bildet $\psi_2 \circ \tau_2^k$ $U_k(G_1 \times G_2)$ isomorph auf $U_k(G_1) \times U_k(G_2)$ ab. Also*

$$U_k(G_1 \times G_2) \simeq U_k(G_1) \times U_k(G_2)$$

**Beweis:** $\forall g \in G_i$ gilt: $g^{|G_i|} = 1$. Sei $\mathfrak{p} = x_j^{|G_i|}$. $\Longrightarrow \mathfrak{p} \in ker\ \sigma_k[G_i] \Longrightarrow \lambda_k[G_i]\left(x_j^{|G_i|}\right) = x_j^{|G_i|} \in L_k[G_i]$
Da $|G_1|$ und $|G_2|$ teilerfremd sind, gibt es $n, n'$, sodaß $n \cdot |G_1| + n' \cdot |G_2| = 1$. Damit ist aber

$$x_i = x_i^1 = x_i^{n\cdot|G_1|+n'\cdot|G_2|} = x_i^{n\cdot|G_1|} \cdot x_i^{n'\cdot|G_2|} \in L_k[G_1] \cdot L_k[G_2]\ \forall i$$

$\Longrightarrow L_k[G_1]L_k[G_2] = F(X)$ Mit Proposition 3.3.11 folgt die Behauptung. □

Klarerweise sind die Fälle von einstelligen ($k = 1$) und mehrstelligen ($k > 1$) Polynompermutationen teilweise deutlich unterschiedlich. Einen deutlichen Unterschied können wir im nächsten Satz sehen:

**Proposition 3.3.13** *Für das Zentrum $Z([U_k(G); \circ])$ gilt*

- $Z(U_1(G)) = \{p(x) = c \cdot x, c \in Z(G), c^2 = 1\}$
- $Z(U_k(G)) = \{\mathfrak{e}\}$ *für* $k > 1$

**Beweis:** Erster Teil: siehe [25] Satz 5 . Zweiter Teil: siehe [26] Satz 6

**Korollar 3.3.14** *Für $k > 1$ und $|G| \neq 1$ kann $U_k(G)$ nicht nilpotent sein.*

**Beweis:** Das folgt direkt aus dem vorherigen Satz und der Definition von Nilpotenz. □

Ingesamt kann gezeigt werden:

**Proposition 3.3.15** *Ist $G$ endlich, dann und nur dann ist $U_k(G)$ nilpotent, wenn entweder*

- $|G| = 1$ *, oder*
- $k = 1$ *und $G$ ist eine 2-Gruppe.*

**Beweis:** [18] Kapitel 5, Korollar 4.44

Die in 3.2.6 definierte Länge hat für die Polynompermutationen Bedeutung und es kann eine Aussage ähnlich zu jener am Anfang dieses Abschnitts getroffen werden.

**Satz 3.3.16** *Ist $G \neq \{1\}$ eine endliche $p$-Gruppe, dann ist $\mathfrak{p} \in G^k[X]$ genau dann Polynompermutation, wenn $p$ nicht $l(\mathfrak{p})$ teilt. Also*

$$\mathfrak{p} \in U_k(G) \Longleftrightarrow ggT(p, l(\mathfrak{p})) = 1$$

**Beweis** siehe [18] Kapitel 5, Satz 4.41

Daraus folgt direkt

**Lemma 3.3.17** *Ist $G \neq \{1\}$ eine endliche nilpotente Gruppe, dann ist $\mathfrak{p} \in G^k[X]$ genau dann Permutationspolynommatrix, wenn $ggT(l(\mathfrak{p}), |G|) = 1$.*

**Beweis:** Die Gruppe $G$ ist nilpotent, damit nach A.8.75 das direkte Produkt ihrer Sylow $p_\nu$-Untergruppen $G_{p_\nu}$. Also ist nach 3.3.12 $U_k(G)$ direktes Produkt der $U_k(G_{p_\nu})$. Nach oben 3.3.16 folgt die Behauptung. □

Eine Richtung dieser Äquivalenz ist sogar charakeristisch für nilpotente Gruppen:

**Satz 3.3.18** *Es sei $G$ endlich. Wenn für alle $\mathfrak{p} \in G^k[X]$ aus der Bedingung $ggT(l(\mathfrak{p}), |G|) = 1$ folgt, daß $\sigma_k[G](\mathfrak{p}) \in U_k(G)$ ist (d.h. $\mathfrak{p}$ eine Permutationspolynommatrix), dann ist $G$ nilpotent.*

**Beweis:** siehe [18] Kapitel 5, Satz 5.2

Es gibt jedoch Gruppen, für die keine der Richtungen in 3.3.17 gilt.
**Beispiel:** Es sei

$$\mathbb{S}_3 = \{e, (123), (132), (12), (13), (23)\}$$

$\mathbb{S}_3$ ist überauflösbar, da

$$\{1\} \trianglelefteq \mathbb{A}_3 \trianglelefteq \mathbb{S}_3$$

eine Hauptreihe mit zyklischen Faktoren ist.

Es ist leicht zu erkennen, daß $\mathbb{S}_3 = \langle\{a, b\}; \{a^2, b^3, a^{-1}b^2ab^{-1}\}\rangle$ ist (z.B. mit $a = (12)$ und $b = (123)$). Dann ist $\mathbb{S}_3 = \{1, a, b, b^2, ab, ba\}$. (Die letzte Relation ist gleichbedeutend mit $ab = b^2a$.)

Für $p = xax^5bx^5$ gilt $p(1) = ab$ und $p(b^2) = b^2ab^{10}bb^{10} = b^2ab^{21} = b^2a = ab$, also ist $p \notin U_1(\mathbb{S}_3)$, aber $l(p) = 11$ und $ggT(l(p), |G|) = 1$.

Andererseits gilt für $p = xaxbx$, daß $l(p) = 3$ und somit $ggT(l(p), |G|) = 3 > 1$, aber $p(1) = ab$, $p(a) = a^3ba = aba = b^2a^2 = b^2$, $p(b) = bab^3 = ba$, $p(b^2) = b^2ab^5 = b^2ab^2 = ab^3 = a$, $p(ab) = aba^2b^2ab = ab^3ab = b$ und $p(ba) = ba^2bab^2a = b^2aab = b^3 = 1$. Also ist $p \in U_1(G)$.

Es lassen sich auch einige Aussagen über die Ordnung von $U_k(G)$ machen, in dem in 3.3.16 behandelten Fall gilt:

**Proposition 3.3.19** *Ist $G \neq \{1\}$ eine endliche p-Gruppe. Dann ist $|U_k(G)| = |GL(k,p)|\, p^t$, für eine ganze Zahl $t > 0$, und $U_k(G)$ ist eine Gruppenerweiterung einer p-Gruppe durch die Gruppe $GL_k(\mathbb{Z}_p)$. D.h. $U_k(G)/GL_k(\mathbb{Z}_p) \simeq H_p$, mit $H_p$ p-Gruppe*

**Beweis:** siehe [18] Kapitel 5, Satz 4.43

### 3.3.4 Einige spezielle Gruppen

Als Beispiel wie man bestimmte endliche Gruppen und deren (einstellige) Polynompermutationen genauer untersuchen kann, sei auf *Schuhmacher* [28] verwiesen.

Dort werden einige Gruppen untersucht, die durch Erzeugenden und Relationen (1.1.54) dargestellt werden. Durch die Relationen kann dann auch auf die Form der Polynomfunktionen und der Polynompermutationen geschlossen werden.

Wir werden hier nur einige Ergebnisse ohne Beweise zitieren, und zwar auch nur jene, die in kurzer Form dargestellt werden können. Für eine ausführlichere Abhandlung und für die Beweise sei dem Leser die Lektüre von [28] nahegelegt.

Bei den Beweisen wird wesentlich verwendet, daß jedes Element der betrachteten Gruppen als $x^a \cdot y^b$ geschrieben werden kann. Es werden viele zahlentheoretische Aussagen wie z.B. der Chinesische Restsatz benützt.

Es sei $G$ eine abelsche $p$-Gruppe mit $|G| = p^n$ mit einer zyklischen Untergruppe vom Index $p$, $p$ eine Primzahl. Dann kann $G$ dargestellt werden als

$$G = \left\langle x, y; x^{p^{n-1}}, y^p, x^{-1}y^{-1}x^{l+p^{n-2}}y \right\rangle$$

Wir beschränken uns auf die Fälle

- $p = 2$ und $n \leq 4$ und
- $p > 2$ und $n \leq 3$

Dann kann die folgende Aussage getroffen werden:

**Proposition 3.3.20**

- $P_1(G) = \{axbx^{s_2}c | a, b, c \in G, s_2 \in \mathbb{Z}\}$
- $|P_1(G)| = p^{2n}$
- $U_1(G) = \{ax^{s_1}b | a, b \in G, s_1 \in \mathbb{Z}, ggT(s_1, p) = 1\}$
- $|U_1(G)| = (p-1)p^{2n-1}$

Sei $G$ nun eine *Diedergruppe* der Ordnung $2^n$ (siehe A.8.32), d.h.

$$G = \langle \{x, y\}; \{x2^{n-1}, y^2, xyxy^{-1}\} \rangle$$

oder eine *verallgemeinerte Quaternionengruppe* der Ordnung $2^n$, d.h.

$$G = \left\langle \{x, y\}; \{x^{2^{n-1}}, y^{-2}x^{2^{n-2}}, xyxy^{-1}\} \right\rangle$$

Beide Gruppen haben Ordnung $2^n$.

Auch in diesem Fall können die möglichen Formen der Polynomfunktionen und Polynompermutationen noch angegeben werden. Eine Folgerung daraus ist, daß für beide Gruppen gilt:

**Proposition 3.3.21**

- $|P_1(G)| = 2^{4n-6}$
- $|U_1(G)| = 2^{4n-7}$

Für weitere Beispiele für Gruppen, die durch Erzeugende und Relationen gegeben sind, sowie Betrachtung der einstelligen Polynomfunktionen und Polynompermutationen über diesen sei hiermit endgültig auf [28] verwiesen.

### 3.3.5 Eigenschaften als Permutationsgruppe

Für diese letzte Betrachtung der Polynompermutationen sei $U_k(G)$ für ein endliches $G$ als Teilmenge der Menge der Permutationen von $G^k$, $\mathbb{S}_{G^k}$, betrachtet. Es geht also um die Eigenschaften als Permutationsgruppe; für die Begriffe siehe A.8.46:

**Satz 3.3.22** *Es sei $G$ eine endliche Gruppe. Dann gilt*

1. *$U_k(G)$ ist transitiv.*
2. *$U_k(G)$ ist zweifach transitiv genau dann, wenn $G$ einfach ist.*
3. *$U_k(G)$ ist primitiv genau dann, wenn $G$ einfach ist.*
4. *Genau dann ist $U_k(G) = \mathbb{S}_{G^k}$, wenn enweder $G$ eine nicht abelsche einfache Gruppe ist oder wenn gilt: $k = 1, |G| \leq 3$ resp. $k = 2, |G| = 2$*

**Beweis:** Da die reguläre Darstellung der Gruppe $G^k$ als Permutationsgruppe A.8.47, $\mathfrak{g} \mapsto \mathfrak{g} \cdot \mathfrak{x}$, eine Untergruppe von $U_k(G)$ ist, folgt sofort die Transitivität.

Ist $G$ nicht einfach, so gibt es ein nicht triviales $N \trianglelefteq G$. Die Nebenklassen von $N^k$ in $G^k$ stellen eine Zerlegung in Imprimitivitätsklassen bezüglich

$U_k(G)$ dar. Denn für $p \in P_k(G)$ folgt $p(\mathfrak{g}) \sim_N p(\mathfrak{g}')$ für $\mathfrak{g} \sim_{N^k} \mathfrak{g}'$. Ist nämlich $\mathfrak{g} = \mathfrak{g}' \cdot \mathfrak{n}$ für ein $\mathfrak{n} \in N^k$ und ist

$$p = a_0 \mathfrak{x}^{\mathfrak{k}_1} a_1 \mathfrak{x}^{\mathfrak{k}_2} a_2 \dots a_{r-1} \mathfrak{x}^{\mathfrak{k}_r} a_r$$

dann ist

$$p(\mathfrak{g}) = p(\mathfrak{g}'\mathfrak{n}) = a_0(\mathfrak{g}'\mathfrak{n})^{\mathfrak{k}_1} a_1(\mathfrak{g}'\mathfrak{n})^{\mathfrak{k}_2} a_2 \dots a_{r-1}(\mathfrak{g}'\mathfrak{n})^{\mathfrak{k}_r} a_r =$$

$$= n' \cdot \left(a_0(\mathfrak{g}')^{\mathfrak{k}_1} a_1(\mathfrak{g}')^{\mathfrak{k}_2} a_2 \dots a_{r-1}(\mathfrak{g}')^{\mathfrak{k}_r} a_r\right) = n' \cdot p(\mathfrak{g}')$$

Also folgt wirklich $\mathfrak{p}(\mathfrak{g}) \sim_{N^k} \mathfrak{p}(\mathfrak{g}')$. Daher ist $U_k(G)$ imprimitiv und kann somit nach A.8.49 nicht 2-fach transitiv sein.

Sei nun $G$ einfach. Betrachte zuerst den Fall, daß $G$ abelsch ist. Also hat $G$ nach A.8.28 Primzahlordnung, und ist somit zyklisch. Sei $z$ das erzeugende Element. Dann kann man jede Abbildung aus $U_k(G)$ nach 3.3.7 darstellen als

$$(z^{y_1}, z^{y_2}, \dots, z^{y_k}) \mapsto \left(z^{b_1 + \sum m_{1j} y_j}, z^{b_2 + \sum m_{2j} y_j}, \dots, z^{b_k + \sum m_{kj} y_j}\right)$$

mit $K = (k_{ij})_{ij}$ eine invertierbare Matrix aus $M_k(p)$. Die Gruppe der bijektiven $n$-dimensionalen inhomogenen Lineartransformationen

$$\mathfrak{y} \mapsto K\mathfrak{y} + \mathfrak{b} \bmod p$$

ist klarerweise zweifach transitiv. Somit ist $U_k(G)$ zweifach transitiv, also auch primitiv.

Sei nun $G$ einfach und nicht abelsch, dann ist $G$ polynomvollständig, also ist $U_k(G) = \mathbb{S}_{G^k}$. Damit ist $U_k(G)$ zweifach transitiv, also auch primitiv.

Sei nun $U_k(G) = \mathbb{S}_{G^k}$, dann ist $U_k(G)$ zweifach transitiv und somit muß $G$ einfach sein. Für die nicht abelschen, einfachen und endlichen Gruppen gilt diese Gleichheit immer, da $G$ polynomvollständig ist. Sei $G$ abelsch, also muß $G$ Primzahlordnung haben. Aus $\mathbb{S}_{G^k} = U_k(G)$ folgt

$$|\mathbb{S}_{G^k}| = |U_k(G)|$$

Also nach 3.3.7

$$p^k! = p^k \cdot \varphi_k(p)$$

$$\Longrightarrow \left(p^k - 1\right)! = \varphi_k(p)$$

$$\Longrightarrow \left(p^k - 1\right)! = (p^k - 1) \cdot (p^k - p) \cdot \ldots \cdot (p^k - p^{k-1})$$

Ist $k = 1$ so ist

$$(p-1)! = \varphi(p) = p \cdot \left(1 - \frac{1}{p}\right) = p - 1$$

Dies gilt also nur für $p = 2$ und $p = 3$.

Sei $k > 1$. Dann folgt

$$\big(p^k - 2\big)! = (p^k - p) \cdot (p^k - p^2) \ldots \cdot (p^k - p^{k-1})$$

Insbesondere kommt jeder Faktor auf der rechten Seite in der Fakultät auf der linken Seite vor. Also gilt diese Gleichheit nur bei $k = 2$ und $p = 2$. □

## 3.4 Abelsche Halbgruppen

Wir werden uns nun kurz Halbgruppen zu. Wir wollen nur zeigen, daß man (natürlich) auch Polynome über diese Varietät, die eine Oberklasse der Varietät der Gruppen ist, betrachten kann, und zu Ergebnissen kommt.

In [16] wurden Polynome über abelsche Halbgruppen untersucht. Ganz allgemein kann man kann ein Normalformsystem finden, indem man analog zu 3.1.4 zeigt:

**Lemma 3.4.1** *Es sei $H$ eine Halbgruppe. Die Wörter $a_0x^{n_1}a_1x^{n_2}...a_{r-1}x^{n_r}a_r$, $x^{n_1}a_1x^{n_2}...a_{r-1}x^{n_r}a_r$, $a_0x^{n_1}a_1x^{n_2}...a_{r-1}x^{n_r}$ und $x^{n_1}a_1x^{n_2}...a_{r-1}x^{n_r}$ mit $r \in \mathbb{N}$, $n_i \in \mathbb{N}, n_i \neq 0$ und $a_t \in H$ für $t = 0, 1, ..., r$ bilden ein Normalformsystem für $H[x]$.*

Betrachtet man die Halbgruppen mit Eins, so fallen die vier Wörter in 3.4.1 zusammen, sodaß gilt

**Korollar 3.4.2** *Es sei $H$ eine Halbgruppe mit Eins. Die Wörter*

$$a_0x^{n_1}a_1x^{n_2}...a_{r-1}x^{n_r}a_r \text{ mit } r \in \mathbb{N}, n_i \in \mathbb{N}, n_i \neq 0, a_t \in H \text{ für } t = 0, 1, ..., r$$

*und $a_t \neq 1$ für $t = 1, ..., r-1$ bilden ein Normalformsystem für $H[x]$.*

Wenden wir uns nun den Polynomfunktionen über abelsche Halbgruppen mit Eins zu, so kann eine zu 3.3.5 analoge Aussage gezeigt werden:

**Satz 3.4.3** *Es sei $S$ eine Halbgruppe, dann ist $P_1(S) = \{ax^n | n \in \mathbb{N}\}$ genau dann wenn $S$ eine kommutative Halbgruppe mit Eins ist.*

**Beweis:** siehe [16] Satz 1

Der Großteil von [16] beschäftigt sich mit der Regularität der Halbgruppe $[P_1(H); \circ, id_H]$ beziehungsweise einer Unterhalbgruppe davon. Für $P_1(H)$ kann die folgende Aussage getroffen werden:

**Satz 3.4.4** *Es sei $[H;\cdot,1]$ eine abelsche Halbgruppe mit Eins. Dann sind die folgenden Aussagen äquivalent:*

- *$[P_1(H);\circ,id_H]$ ist regulär.*
- *$[H;\cdot,1]$ und $[T_1(H);\circ,id_H]$ sind regulär.*
- *$exp(H)$ ist endlich und quadratfrei*

**Beweis:** siehe [16] Lemma 7, Korollar 11, Satz 15

# 3.5 Struktureigenschaften

## 3.5.1 Auflösbarkeit endlicher Gruppen

Für die Frage, wie sich die Auflösbarkeit einer endlichen Gruppe auf die Polynompermutationen auswirkt bzw. umgekehrt, werden wir uns auf jene Polynompermutationen beschränken, die die Eins auf Eins abbilden, also die Menge

$$\overline{U}_k(G) = \mathcal{E}\left(\overline{P}_k(G)^k\right) = U_k(G) \cap \overline{P}_k(G)^k$$

Es stellen sich Ergebnisse ein, die zeigen, wie prominent die Ordnung der Gruppe in ihre Struktur eingeht! In diesem Abschnitt seien die Gruppen immer als endlich vorausgesetzt.

**Satz 3.5.1** *Sei $|G| \neq 1$. Ist $\overline{U}_k(G)$ auflösbar, so ist das auch $G$ und es gilt entweder*

1. *k=1 und, für jeden Hauptfaktor $H/K$ von $G$ ist entweder*
   (a) *die Gruppe $Aut_G(H/K) = \{\varphi|_{H/K} \,|\varphi \in Inn(G)\}$ abelsch, oder*
   (b) *$|H/K| = 4$ oder 9*

   *oder*
2. *$k = 2$ und $G$ ist eine überauflösbare (2,3)-Gruppe*

**Beweis** siehe [18] Satz 4.11

Insbesondere heißt das, daß für $k > 2$ $\overline{U}_k(G)$ nicht auflösbar ist.

**Satz 3.5.2** *$U_k(G)$ ist auflösbar genau dann, wenn $G$ auflösbar ist und eine der beiden Bedingungen aus Satz 3.5.1 gilt oder $|G| = 1$ ist.*

**Beweis** $\Longrightarrow$: Ist $U_k(G)$ auflösbar, so auch $\overline{U_k(G)}$ als Untergruppe. Satz 3.5.1 liefert die Behauptung.

$\Longleftarrow$: Wir werden diese Aussage durch Induktion nach $|G|$ zeigen. Ist $|G| = 1$, so ist klarerweise $|U_k(G)| = 1$, also ist $U_k(G)$ auflösbar.

Sei nun $|G| > 1$, und sei $N$ ein minimaler normaler Normalteiler von $G$. Dann erfüllt $G/N$ auch die Bedingungen, sofern das nur $G$ tut. Denn sind $H' = H/N, K' = K/N$ Normalteiler von $G/N$, sodaß $H'/K'$ Hauptfaktor ist, so ist das auch $H/K \simeq (H/N)\,/\,(H/K) = H'/K'$. Ist $G$ eine überauflösbare $(2,3)$-Gruppe ist so auch $G/N$. Also ist $U_k(G/N)$ nach Induktion auflösbar. Es sei $\pi$ der kanonische Epimorphismus $G \to G/N$. Mit $P_k(\pi)^k : [U_k(G); \circ, ^{-1}, id_G] \to [U_k(G/N); \circ, ^{-1}, id_G]$ gilt wegen 3.3.9

$$U_k(G/N) \simeq U_k(G)/ker(P_k(\pi)^k)$$

Können wir zeigen, daß $ker(P_k(\pi)^k$ auflösbar ist, so folgt aus A.8.61, daß $U_k(G)$ auflösbar ist.

Wir betrachten den Kern dieses Epimorphismus bezüglich der Gruppenoperation $\circ$, so ist

$$ker(P_k(\pi)^k) = \{\mathfrak{p} \in U_k(G) : P_k(\pi)^k(\mathfrak{p}) = id_{G/N}\} =$$

$$= \{\mathfrak{p} \in U_k(G) : P_k(\pi)^k(\mathfrak{p})(\pi(g_1), \ldots, \pi(g_k)) = (\pi(g_1), \ldots, \pi(g_k))\, \forall g_1, \ldots, g_k \in G\}$$

Nach 2.1.28 ist also

$$ker(P_k(\pi)^k) =$$

$$= \{\mathfrak{p} \in U_k(G) : \pi^k(\mathfrak{p}(g_1, \ldots, g_k)) = (\pi(g_1), \ldots, \pi(g_k))\, \forall g_1, \ldots, g_k \in G\} =$$

$$= \{\mathfrak{p} \in U_k(G) : (\mathfrak{p}(g_1, \ldots, g_k)) \cdot N^k = (g_1, \ldots, g_k) \cdot N^k \forall g_1, \ldots, g_k \in G\} =$$

$$= \{\mathfrak{p} \in U_k(G) : \mathfrak{g}^{-1} \cdot (\mathfrak{p}(\mathfrak{g})) \in N^k \forall \mathfrak{g} \in G^k\}$$

Sei nun $\mathfrak{n}(\mathfrak{p}, \mathfrak{g}) \in N^k$ jenes von $\mathfrak{u}$ und $\mathfrak{p}$ abhängige Element aus $N^k$, für das gilt:

$$\mathfrak{p} \circ \mathfrak{g} = \mathfrak{g} \cdot \mathfrak{n}(\mathfrak{p}, \mathfrak{g})$$

Sei $\tau(\mathfrak{p}, \mathfrak{g}) : N^k \to N^k$ jene Abbildung, für die gilt

$$\tau(\mathfrak{p}, \mathfrak{g})(\mathfrak{n}) = (\mathfrak{p}(\mathfrak{g}))^{-1} \cdot \mathfrak{p}(\mathfrak{g} \cdot \mathfrak{n})$$

Diese Abbildung ist eine Abbildung nach $N^k$, da gilt

$$(\mathfrak{p}(\mathfrak{g}))^{-1} \cdot \mathfrak{p}(\mathfrak{g} \cdot \mathfrak{n}) = (\mathfrak{g} \cdot \mathfrak{n}(\mathfrak{p}, \mathfrak{g}))^{-1} \cdot (\mathfrak{g}\mathfrak{n} \cdot \mathfrak{n}(\mathfrak{p}, \mathfrak{g}\mathfrak{n})) = \mathfrak{n}(\mathfrak{p}, \mathfrak{g})^{-1} \cdot \mathfrak{n} \cdot \mathfrak{n}(\mathfrak{p}, \mathfrak{g}\mathfrak{n})$$

Ingesamt gilt also

$$\mathfrak{p}(\mathfrak{g} \cdot \mathfrak{n}) = \mathfrak{p}(\mathfrak{g}) \cdot \tau(\mathfrak{p}, \mathfrak{g})(\mathfrak{n})$$

Da $N$ minimaler Normalteiler der auflösbaren Gruppe $G$ ist, ist $N$ nach A.8.65 elementar abelsch. Betrachten wir die Abbildung $\tau_g(n) = g^{-1}ng$, so gilt $ng = g\tau_g(n)$. Klarerweise gilt $\tau_g(n_1 \cdot n_2) = \tau_g(n_1) \cdot \tau_g(n_2)$. Es sei $p \in P_k(G)$ mit $p = a_1\xi_{i_1}a_2\xi_{i_2}a_3 \ldots a_s\xi_{i_s}a_{s+1}$ (siehe 3.1.14), dann ist

$$p(g_1n_1, \ldots, g_kn_k) = (a_1g_{i_1}a_2g_{i_2}a_3 \ldots a_sg_{i_s}a_{s+1}) \cdot (a_2g_{i_2}a_3 \ldots a_sg_{i_s}a_{s+1})^{-1} \cdot n_{i_1} \cdot$$

$$\cdot (a_2g_{i_2}a_3 \ldots a_sg_{i_s}a_{s+1}) \cdot n_{i_2} (a_3 \ldots a_sg_{i_s}a_{s+1})^{-1} \cdot \ldots =$$

$$= p(g) \cdot \tau_{a_2g_{i_2}a_3 \ldots a_sg_{i_s}a_{s+1}}(n_{i_1}) \cdot \tau_{a_3 \ldots a_sg_{i_s}a_{s+1}}(n_{i_2}) \ldots$$

Also ist

$$\tau(\mathfrak{p}, \mathfrak{g})(\mathfrak{n}) = (\mathfrak{p}(\mathfrak{g}))^{-1} \cdot \mathfrak{p}(\mathfrak{g} \cdot \mathfrak{n})$$

ein Homomorphismus, da $N$ abelsch ist. Da $\mathfrak{p}$ bijektiv ist, ist $\tau(\mathfrak{p}, \mathfrak{g})$ auch bijektiv. Denn aus $\tau(\mathfrak{p}, \mathfrak{g})(n) = \tau(\mathfrak{p}, \mathfrak{g})(n')$ folgt $\mathfrak{p}(\mathfrak{g} \cdot \mathfrak{n}) = \mathfrak{p}(\mathfrak{g} \cdot \mathfrak{n}') \Longrightarrow \mathfrak{g} \cdot \mathfrak{n} = \mathfrak{g} \cdot \mathfrak{n}' \Longrightarrow \mathfrak{n} = \mathfrak{n}'$. Andererseits gibt es für ein $\mathfrak{n}'$ ein $\mathfrak{g}'$, sodaß $\mathfrak{p}(\mathfrak{g}') = \mathfrak{p}(\mathfrak{g}) \cdot \mathfrak{n}'$. Da somit $\mathfrak{p}(\mathfrak{g}') \sim_{N^k} \mathfrak{p}(\mathfrak{g})$ ist $\mathfrak{g}' \sim_{N^k} \mathfrak{g}$ und es existiert ein $\mathfrak{n}_0$ mit $\mathfrak{g}' = \mathfrak{g} \cdot \mathfrak{n}_0$ und es gilt

$$\tau(\mathfrak{p}, \mathfrak{g})(\mathfrak{n}_0) = (\mathfrak{p}(\mathfrak{g}))^{-1} \cdot \mathfrak{p}(\mathfrak{g} \cdot \mathfrak{n}_0) =$$

$$= (\mathfrak{p}(\mathfrak{g}))^{-1} \cdot \mathfrak{p}(\mathfrak{g}) \cdot \mathfrak{n}' = \mathfrak{n}'$$

Also ist $\mathfrak{p} \circ (\mathfrak{g}\mathfrak{n}) = \mathfrak{g} \cdot \mathfrak{n}(\mathfrak{p}, \mathfrak{g})\tau(\mathfrak{p}, \mathfrak{g})(\mathfrak{n})$ für $\mathfrak{p} \in ker(P_k(\pi)^k)$. Wir erhalten für jedes $\mathfrak{g} \in G^k$ eine Abbildung

$$\delta(\mathfrak{g}) : ker(P_k(\pi)^k) \to \mathbb{S}_{N^k}$$

definiert durch

$$(\delta(\mathfrak{g})(\mathfrak{p}))(\mathfrak{n}) = \mathfrak{n}(\mathfrak{p}, \mathfrak{g})\,\tau(\mathfrak{p}, \mathfrak{g})(\mathfrak{n})$$

$\delta(\mathfrak{g})(\mathfrak{p}) = (\mathfrak{n}(\mathfrak{p}, \mathfrak{g})\,\mathfrak{x}) \circ \tau(\mathfrak{p}, \mathfrak{g})(\mathfrak{n})$ ist also bijektiv. Es gilt

$$\mathfrak{g}(\delta(\mathfrak{g})(\mathfrak{p}))(\mathfrak{n}) = \mathfrak{g} \cdot (\mathfrak{n}(\mathfrak{p}, \mathfrak{g})\,\mathfrak{x}) \circ \tau(\mathfrak{p}, \mathfrak{g})(\mathfrak{n}) = \mathfrak{p}(\mathfrak{g}\mathfrak{n})$$

Weiters gilt

$$\mathfrak{g}(\delta(\mathfrak{g})(\mathfrak{p}_1 \circ \mathfrak{p}_2))(\mathfrak{n}) = \mathfrak{p}_1 \circ \mathfrak{p}_2(\mathfrak{g}) = \mathfrak{p}_1 \circ (\mathfrak{g}(\delta(\mathfrak{g})(\mathfrak{p}_2))(\mathfrak{n})) =$$

$$= \mathfrak{g}(\delta(\mathfrak{g})(\mathfrak{p}_1))((\delta(\mathfrak{g})(\mathfrak{p}_2))(\mathfrak{n})) = \mathfrak{g}(\delta(\mathfrak{g})(\mathfrak{p}_1) \circ \delta(\mathfrak{g})(\mathfrak{p}_2))(\mathfrak{n})$$

Also ist $\delta(g)(\mathfrak{p}_1 \circ \mathfrak{p}_2) = \delta(g)(\mathfrak{p}_1) \circ \delta(g)(\mathfrak{p}_2)$ und somit ist $\delta$ ein Homomorphismus. Der Kern der Abbildung $\delta(g)$ besteht aus jenen Polynompermutationen, für die gilt

$$\mathfrak{p}(\mathfrak{g}\mathfrak{n}) = \mathfrak{g}(\delta(\mathfrak{g})(\mathfrak{p}))(\mathfrak{n}) = \mathfrak{g}\mathfrak{n}$$

Insbesondere ist $\bigcap_{g\in G} ker\delta(g) = \{id_{N^k}\}$, betrachte die Abbildung

$$\delta : ker(P_k(\pi)^k) \to (Sym_{N^k})^G$$

mit

$$\delta(\mathfrak{p}) = (\delta(g)(\mathfrak{p}))_g$$

Dann ist

$$\delta(ker(P_k(\pi)^k) \simeq ker(P_k(\pi)^k)/ker\delta = ker(P_k(\pi)^k)$$

Somit ist

$$ker(P_k(\pi)^k) \simeq \prod_{g\in G} \delta(g)(ker(P_k(\pi)^k))$$

Also ist insbesondere $ker(P_k(\pi)^k)$ auflösbar, wenn das $\delta(g)(ker(P_k(\pi)^k))$ ist. Dies zeigen wir, indem wir eine Abbildung $\varphi$ definiere:

$$\varphi : \delta(g)\left(ker\left(P_k(\pi)^k\right)\right) \to Aut(N^k)$$

$$\varphi\left(\delta(g)\left(\mathfrak{p}\right)\right) = \tau(\mathfrak{p}, g)$$

Diese Abbildung ist wohldefiniert, denn wenn $\delta(g)(\mathfrak{p}) = \delta(g)(\mathfrak{q})$, so ist $\mathfrak{p}(\mathfrak{g}\cdot\mathfrak{n}) = \mathfrak{q}(\mathfrak{g}\cdot\mathfrak{n})\forall\mathfrak{n} \in N^k$, also insbesondere für $\mathfrak{n} = \mathfrak{e} = (1, 1, \ldots, 1)$, also ist $\mathfrak{g}\cdot\mathfrak{n}(\mathfrak{p}, \mathfrak{g}) = = \mathfrak{g}\cdot\mathfrak{n}(\mathfrak{q}, \mathfrak{g})$,also ist $\mathfrak{n}(\mathfrak{p}, \mathfrak{g}) = \mathfrak{n}(\mathfrak{q}, \mathfrak{g})$. Somit ist jedoch $\tau\left(\mathfrak{p}, \mathfrak{g}\right) = \tau\left(\mathfrak{q}, \mathfrak{g}\right)$. Es gilt weiters

$$\mathfrak{n}\left(\mathfrak{p}\circ\mathfrak{q}, \mathfrak{g}\right)\cdot\tau\left(\mathfrak{p}\circ\mathfrak{q}, \mathfrak{g}\right)\left(\mathfrak{n}\right) = \left(\delta(\mathfrak{g})(\mathfrak{p})\circ\delta(\mathfrak{g})(\mathfrak{q})\right)\left(\mathfrak{n}\right) =$$

$$= \delta(g)(\mathfrak{p})\left(\mathfrak{n}\left(\mathfrak{q}, \mathfrak{g}\right)\cdot\tau\left(\mathfrak{q}, \mathfrak{g}\right)\left(\mathfrak{n}\right)\right) = \mathfrak{n}\left(\mathfrak{p}, \mathfrak{g}\right)\cdot\tau\left(\mathfrak{p}, \mathfrak{g}\right)\left(\mathfrak{n}\left(\mathfrak{q}, \mathfrak{g}\right)\cdot\tau\left(\mathfrak{q}, \mathfrak{g}\right)\left(\mathfrak{n}\right)\right) =$$

$$= \mathfrak{n}\left(\mathfrak{p}, \mathfrak{g}\right)\cdot\tau\left(\mathfrak{p}, \mathfrak{g}\right)\left(\mathfrak{n}\left(\mathfrak{q}, \mathfrak{g}\right)\cdot\mathfrak{x}\circ\tau\left(\mathfrak{q}, \mathfrak{g}\right)\left(\mathfrak{n}\right)\right) =$$

$$= \mathfrak{n}\left(\mathfrak{p}, \mathfrak{g}\right)\cdot\tau\left(\mathfrak{p}, \mathfrak{g}\right)\left(\mathfrak{n}\left(\mathfrak{q}, \mathfrak{g}\right)\right)\cdot\mathfrak{n}\left(\mathfrak{p}, \mathfrak{g}\right)\cdot\tau\left(\mathfrak{p}, \mathfrak{g}\right)\circ\tau\left(\mathfrak{q}, \mathfrak{g}\right)\left(\mathfrak{n}\right)$$

Setzen wir $n = \mathfrak{e}$ ein, so erhalten wir die Gleichung

$$\mathfrak{n}\left(\mathfrak{p}\circ\mathfrak{q}, \mathfrak{g}\right) = \mathfrak{n}\left(\mathfrak{p}, \mathfrak{g}\right)\cdot\tau\left(\mathfrak{p}, \mathfrak{g}\right)\left(\mathfrak{n}\left(\mathfrak{q}, \mathfrak{g}\right)\right)\cdot\mathfrak{n}\left(\mathfrak{p}, \mathfrak{g}\right)$$

Also ist

$$\tau\left(\mathfrak{p}\circ\mathfrak{q}, \mathfrak{g}\right)\left(\mathfrak{n}\right) = \tau\left(\mathfrak{p}, \mathfrak{g}\right)\circ\tau\left(\mathfrak{q}, \mathfrak{g}\right)\left(\mathfrak{n}\right)$$

Damit ist $\varphi$ ein Homomorphismus. Ist $\delta(g)(\mathfrak{p}) \in ker\varphi$, so ist

$$\delta(\mathfrak{g})(\mathfrak{p})(\mathfrak{n}) = \mathfrak{n}(\mathfrak{p}, \mathfrak{g})\tau(\mathfrak{p}, \mathfrak{g})(\mathfrak{n}) = \mathfrak{n}(\mathfrak{p}, \mathfrak{g})\cdot\mathfrak{n}$$

Also ist $ker\varphi$ isomorph zu einer Untergruppe von $N^k$ und somit auflösbar . $\varphi(\delta(g)(ker(P_k(\pi)^k))$ ist eine Untergruppe von $Aut(N^k)$.

Ist $k = 2$ und $G$ eine überauflösbare $(2,3)$-Gruppe oder $k = 1$ und $|N| = 4$ oder 9, so ist $Aut(N^k)$ isomorph zu $GL(2,2)$ oder $GL(2,3)$, welche auflösbar sind. Ist jedoch $k = 1$ und $Aut_G(N)$ abelsch, dann kommutieren zwei Elemente $\tau(\mathfrak{p},\mathfrak{g})$ und $\tau(\mathfrak{q},\mathfrak{g})$, denn $\tau(\mathfrak{p})(\mathfrak{n}) = \mathfrak{p}(\mathfrak{g})^{-1}\mathfrak{p}(\mathfrak{g}\mathfrak{n})$, $U_k(G) \subseteq \overline{P}_k(G)^k$ und $\overline{P}_k(G)^k$ wird von $Inn(G^k)$ erzeugt (siehe Beispiel nach 3.1.54). Also ist auch hier $\varphi(\delta(g)(ker(P_k(\pi)^k))$ auflösbar. □

### 3.5.2 Nilpotenz

**Satz 3.5.3** *Ist $G$ eine endliche nilpotente Gruppe der Klasse $c(G) \leq 2$, dann ist $U_1(G) = \{\varphi = a\xi^l b\}$ mit $a, b \in G, ggT(l, |G|) = 1$*

**Beweis:** [20] Satz 4

Umgekehrt gilt

**Satz 3.5.4** *Ist $|G|$ ungerade und können alle $\varphi \in U_1(G)$ durch $\varphi(x) = ax^r b$ mit $a, b \in G$ dargestellt werden, so ist $G$ nilpotent der Klasse $c(G) \leq 3$. Gilt zusätzlich $3 \not| |G|$, so ist $c(G) \leq 2$.*

**Beweis:** Nach A.8.79 reicht es zu zeigen, daß $a$ und $b^{-1}ab$ für alle $a, b$ aus $G$ kommutieren. Da $ggT(|G|, 2) = 1$ ist, ist nach 3.3.2 $\xi^2$ und somit auch $\xi g^{-1}\xi g = \xi g^2 \circ \xi^2 \circ \xi g^{-1}$ ein Permutationspolynom für alle $g \in G$. Also gibt es eine ganze Zahl $l(g)$ und Elemente $a(g), b(g)$ sodaß

$$\xi g^{-1}\xi g = a(g)^{-1}\xi^{l(g)}b(g)$$

mit $ggT(l(g), |G|) = 1$. Setzen wir die Eins ein, so sehen wir, daß $b(g) = a(g)$. Es sei nun $\bar{l}(g)$ eine Lösung der Gleichung $\bar{l}(g) \cdot l(g) \equiv 1 \bmod |G|$, dann ist

$$\xi^{\bar{l}(g)} \cdot g^{-1}\xi^{\bar{l}(g)} \cdot g = a(g)^{-1} \cdot \xi^{\bar{l}(g)\cdot l(g)} \cdot a(g) = a(g)^{-1}\xi a(g)$$

Also ist diese Abbildung ein innerer Automorphismus $\tau_{a(g)}$. Insbesondere ist

$$\xi^{2\cdot\bar{l}(g)} \cdot g^{-1} \cdot \xi^{2\cdot\bar{l}(g)} \cdot g = a(g)^{-1}\xi^2 a(g) =$$

$$= \left(a(g)^{-1}\xi a(g)\right) \cdot \left(a(g)^{-1}\xi a(g)\right) = \xi^{\bar{l}(g)} \cdot g^{-1} \cdot \xi^{\bar{l}(g)} \cdot g \cdot \xi^{\bar{l}(g)} \cdot g^{-1} \cdot \xi^{\bar{l}(g)} \cdot g$$

Also ist

$$\xi^{\bar{l}(g)} \cdot g^{-1} \cdot \xi^{\bar{l}(g)} = g^{-1} \cdot \xi^{\bar{l}(g)} \cdot g \cdot \xi^{\bar{l}(g)} \cdot g^{-1}$$

und somit

$$\left(g \cdot \xi^{\bar{l}(g)} \cdot g^{-1}\right) \cdot \xi^{\bar{l}(g)} = \xi^{\bar{l}(g)} \cdot \left(g \cdot \xi^{\bar{l}(g)} \cdot g^{-1}\right)$$

Da $\bar{l}(g)$ teilerfremd zu $exp(G)$ ist, ist $\xi^{\bar{l}(g)}$ eine Polynompermutation. also ist

$$\left(g \cdot t \cdot g^{-1}\right) \cdot t = t \cdot \left(g \cdot t \cdot g^{-1}\right) \ \forall g, t \in G$$

Also sind die Vorrausetzung für den Satz von Levi A.8.79 erfüllt. Ist $ggT(3, |G|) = 1$ gibt es kein Element der Ordnung der Ordnung 3, also ist $c(G) \leq 2$. $\square$

Man kann den zweiten Teil dieses Satzes erweitern zu:

**Lemma 3.5.5** *Wenn $ggT\left(|G|, 6\right) = 1$, so sind folgende Bedingungen äquivalent:*

- *Alle $\varphi \in U_1(G)$ lassen sich darstellen durch $\varphi(x) = cx^r d$.*
- *$C_G(g) \trianglelefteq G \ \forall g \in G$*
- *Alle normalen Hüllen $N(g)$ sind abelsch.*
- *$C_G(g) = \prod A(g)$, wo $A(g)$ alle maximalen abelschen Normalteiler durchläuft, die $g$ enthalten.*
- *$c(\langle g, h \rangle) \leq 2 \ \forall g, h \in G$*
- *$G$ ist nilpotent der Klasse 2.*

**Beweis:** siehe [17] Lemma 5

Nach A.8.75 ist jede nilpotente Gruppe Produkt ihrer $p$-Sylow-gruppen. Ist $U_1(G) = \{c\xi^r d\}$ so folgt für $ggT\left(|G|, 6\right) = 1$, daß $G$ nilpotent der Klasse $c(G) \leq 2$ ist. Für $ggT(2, |G|) = 1$ ist nach 3.5.4 $G$ nilpotent der Klasse $c(G) \leq 3$. Also bleiben v.a. noch der Fall, $|G|$ ist gerade, offen und für den Fall, $G$ ist eine 3-Gruppe, ist zu klären ob eine schärfere Aussage als in A.8.75 möglich ist. Im allgemeinen kann nicht mehr auf die Nilpotenz geschlossen werden, wie das Beispiel $\mathbb{S}_3$ zeigt. Hier können alle Elemente von $U_1(G)$ auch in der obigen Form dargestellt werden (siehe [14]).

In [14] wird diese Frage des Zusammenhangs der Nilpotenz mit den Polynompermutationen durch die Anwendung des Begriffs der *fast-n-abelschen Gruppen* (siehe A.8.31) behandelt:

**Lemma 3.5.6** *Es sei $G$ endlich mit $ggT(|G|, 2) = 1$ und $U_1(G) = \{a\xi^r b | a, b \in G, r \in \mathfrak{P}_{exp(G)}\}$. Dann ist $G$ fast-$m$-abelsch für alle $m$ mit $ggT(m, exp(G)) = 1$. Inbesondere ist $G$ nilpotent und $c(G) \leq 2$ für $ggT(|G|, 6) = 1$.*

**Beweis:** siehe [14] Korollar 17

Im allgemeinen kann also aus der Eigenschaft, daß $U_1(G) = \{a\xi^r b | a, b \in G, r \in \mathbb{Z}_{exp(G)}\}$ ist, nicht mehr auf die Nilpotenz geschlossen werden. Die endliche Gruppe $G$ ist aber auflösbar, ja sogar überauflösbar:

**Satz 3.5.7** *Es sei $G$ endlich mit $U_1(G) = \{a\xi^r b | a, b \in G, r \in \mathfrak{P}_{exp(G)}\}$. Dann ist $G$ überauflösbar.*

**Beweis:** siehe [14] Satz 18

## 3.6 Polynome, die Homomorphismen sind

Als Abschluß wollen wir uns fragen, welche Polynomfunktionen Homomorphismen oder Isomorphismen sind!

Z.B. für die Varietät der Verbände kann ein interessanter Zusammenhang zwischen Polynomfunktionen und Automorphismen bemerkt werden. Dort sind alle invertierbaren Polynomfunktionen bereits Automorphismen (siehe [22] Lemma 1). Für die Varietät der Gruppen sind jedoch nur wenige Aussagen bekannt.

Klarerweise müssen polynomiale Homomorphismen Elemente von $\overline{P}_k(G)$ sein.

Wir beschränken uns auf den einstelligen Fall, $k = 1$. Betrachten wir $G \in \mathfrak{Grp}_{\mathfrak{ab}}$: Ist $a\xi^n$ ein Homomorphismus, so muß $a = ae^n = e$ gelten. Andererseits ist $\xi^n$ klarerweise ein Homomorphismus. Klarerweise sind somit Elemente aus $\mathcal{E}(\overline{P(G)})$ Automorphismen.

Ist $\xi^2$ ein Homomorphismus auf einer (beliebigen) Gruppe $G$, so folgt daraus, daß $G$ abelsch ist. $((a \cdot b)^2 = a^2 \cdot b^2 \Longrightarrow a \cdot b = b \cdot a)$. Diese Tatsache gilt auch für $\xi^{-1}$.

Die Untersuchung, ob die Abbildung $\xi^n$ auf der Gruppe $G$ ein Homomorphismus ist, fällt klarerweise mit der Frage zusammen, ob diese Gruppe $n$-abelsch (siehe A.8.30) ist.

Wir können einige Eigenschaften für polynomiale Homo- und Automorphismen aufstellen:

**Lemma 3.6.1** *Es sei $G$ eine Gruppe. Es seien $m$ und $n \in \mathbb{Z}$.*

- *Sind $\xi^m$ und $\xi^n \in End(G)$ so ist auch $\xi^{m \cdot n} \in End(G)$.*
- *Sind $\xi^m \in Aut(G)$ und $\xi^n \in End(G)$ und gilt $m$ teilt $n$, so ist auch $\xi^{\frac{n}{m}} \in End(G)$.*

- *Ist $\xi^n \in End(G)$, so ist auch $\xi^{1-n} \in End(G)$*
- *Ist $\xi^n \in Aut(G)$, so ist auch $\xi^{n-1} \in End(G)$*

**Beweis:** Die Komposition zweier Homomorphismen bleibt ein Homomorphismus, also ist $\xi^m \circ \xi^n = \xi^{m \cdot n} \in Hom(G, G)$.

Ist $\xi^m \in Aut(G)$, so ist $(\xi^m)^{-1}$ auch ein Automorphismus. Damit ist für beliebiges $l$

$$\xi^l = \xi^{m^{-1}} \circ \xi^m \circ \xi^l = \xi^{m^{-1}} \circ \xi^{(m \cdot l)}$$

Sei nun $n$ ein Vielfaches von $m$, $n = m \cdot l$, sodaß $\xi^n$ ein Homomorphismus ist, dann ist $\xi^l$ auch ein Homomorphismus.

Sei $\xi^n \in End(G)$, also ist $h^n \cdot g^n = (h \cdot g)^n$ für alle $h, g \in G$. Also auch für $h = x^{-1}$, $g = y^{-1}$ für alle $x, y \in G$, daraus folgt $x^{-n} \cdot y^{-n} = (y \cdot x)^{-n}$. Multiplizieren wir diese Gleichung links mit $x$ und rechts mit $y$, folgt

$$x^{1-n} \cdot y^{1-n} = x \cdot (y \cdot x)^{-n} \cdot y = x \cdot \underbrace{\left(x^{-1} \cdot y^{-1}\right) \ldots \left(x^{-1} \cdot y^{-1}\right)}_{n} y$$

$$= \underbrace{\left(y^{-1} \cdot x^{-1}\right) \ldots \left(y^{-1} \cdot x^{-1}\right)}_{n-1} = ((x \cdot y)^{-1})^{n-1} = (x \cdot y)^{1-n}$$

Sei $\xi^n \in Aut(G)$, also ist nach Punkt 2 $\xi^{1-n}$ Homomorphismus, also nach Punkt 1 auch $\xi^{(1-n)^2}$. Ebenso wieder nach Punkt 3 $\xi^{(1-(1-n)^2)} = \xi^{2n-n^2} = \xi^{n \cdot (2-n)}$, also ist nach Punkt 2 auch $\xi^{2-n}$ und damit auch $\xi^{1-(2-n)} = \xi^{n-1}$ ein Homomorphismus. □

Im Punkt 3 folgt daraus, daß $\xi^n$ ein Automorphismus ist, im allgemeinen nicht, daß $\xi^{1-n}$ auch einer ist. Denn gelte dies, so wäre $\xi^{(1-1)} = 1$ ein Isomorphismus, also wäre $|G| = 1$.

Gleiches gilt auch für Punkt 4. Wäre $\xi^{n-1}$ ein Automorphismus, wenn es nur $\xi^n$ ist, so wäre wiederum $\xi^{1-1}$ ein Isomorphismus.

Für die anderen beiden Punkte gilt jedoch, da die Komposition von bijektiven Funktionen wieder bijektiv ist:

**Korollar 3.6.2** *Es sei $G$ eine Gruppe. Es seien $m$ und $n \in \mathbb{Z}$, sodaß $\xi^m$ und $\xi^n \in Aut(G)$. Dann gilt:*

- *$\xi^{m \cdot n} \in Aut(G)$.*
- *Teilt $m$ $n$, so ist auch $\xi^{\frac{n}{m}} \in Aut(G)$.*

**Beweis:** Die Beweisführung in 3.6.1 für diese beiden Punkte gilt ebenso für Automorphismen. □

**Korollar 3.6.3** *Ist $p(x) = x^3$ ein Automorphismus, so ist $G$ abelsch!*

**Beweis:** Das folgt direkt aus dem obigen Lemma, denn ist $\xi^3$ ein Automorphismus, so ist nach Punkt 4 $\xi^2$ ein Homomorphismus. Daraus folgt, wie erwähnt, daß $G$ ablesch ist. □

Die folgende Aussage läßt sich auch recht direkt zeigen:

**Lemma 3.6.4** *Sind $\xi^n$ und $\xi^{n+1}$ Homomorphismen, so folgt aus $\xi^k \in End(G)$ stets $\xi^{k'} \in End(G)$ für $k' \equiv k \ mod \ n$.*

**Beweis:** [31]

Wir wollen uns nun noch kurz der Frage widmen, wann Automorphismen Polynomfunktionen sind!

### 3.6.1 Polynome, die Automorphismen sind

Die Frage, die wir uns nun stellen wollen, lautet: Welche Eigenschaften haben Automorphismen, die durch Polynome dargestellt werden können? Insbesondere wann sind alle Automorphismen Polynomfunktionen?

Wir wollen nur kurz die Frage umreissen und einige Aussagen ohne Beweis zitieren. Für eine genauerer Betrachtung sei auf [12] verweisen.

Wir definieren

**Definition 3.6.5** *Sei $G$ eine Gruppe, dann sei die Menge* **PAut(G)** *die Menge aller Funktionen, die Polynomfunktionen und Automorphismen sind*

Also ist

$$PAut(G) = Aut(G) \cap P_1(G) = Aut(G) \cap \overline{P_1}(G) = Aut(G) \cap U_1(G)$$

Es läßt sich zeigen, daß die Gruppe $PAut(G)$ genau dann auflösbar, überauflösbar bzw. nilpotent ist, wenn $G$ diese Eigenschaft hat.

Klarerweise gilt $Inn(G) \subseteq PAut(G)$. Es gilt offensichtlich

$$[Inn(G); \circ, ^{-1}, id_G] \trianglelefteq [PAut(G); \circ, ^{-1}, id_G] \trianglelefteq [Aut(G); \circ, ^{-1}, id_G]$$

Man kann also auch den Quotienten $PAut(G)/Inn(G)$ untersuchen.

Für diesen Quotienten läßt sich etwa zeigen:

**Lemma 3.6.6** *Sei* $G = \prod_{i=1,\ldots,m} A_i$ *eine direkte Zerlegung der endlichen Gruppe* $G$ *in direkt unzerlegbare Faktoren. Sind alle* $PAut(A_i)/Inn(A_i)$ *auflösbar, so ist auch* $PAut(G)/Inn(G)$ *auflösbar.*

**Beweis:** [12] Lemma 3

Wann gilt nun $PAut(G) = Aut(G)$? Klar ist, daß im Falle von endlichen, einfachen, nicht-abelschen Gruppen gilt: $PAut(G) = Aut(G)$, da diese Gruppen ja polynomvollständig sind.

Weitere (exemplarische) Ergebnisse:

**Satz 3.6.7** *Es sei* $G$ *eine Gruppe und* $N$ *ein charakteristischer, minimaler Normalteiler von* $G$ *mit* $C_G(N) = \{e\}$. *Gilt* $Aut(G/N) = PAut(G/N)$ *so gilt* $Aut(G) = PAut(G)$.

**Beweis:** [12] Satz 3

**Satz 3.6.8** *Eine vollständig reduzible Gruppe* $G$ *erfüllt* $Aut(G) = PAut(G)$ *genau dann, wenn* $G = \prod_{i=1,\ldots,m} A_i$ *mit einfachen Gruppen* $A_i (i = 1, \ldots, m)$, *die paarweise nicht isomorph sind.*

**Beweis:** [12] Satz 5

**Satz 3.6.9** *Für eine abelsche Gruppe* $G$ *gilt* $Aut(G) = PAut(G)$ *genau dann, wenn* $G$ *zyklisch ist.*

**Beweis:** [12] Lemma 4

Wir wissen aus 3.1.52, daß gilt:

$$I(G^k) \preceq A(G^k) \preceq E(G^k) \preceq F(G^k)$$

Aus der dort folgenden Bemerkung wissen wir, daß $I(G) = \overline{P_1(G)}$ ist. Gilt nun also $I(G) = A(G)$, dann folgt daraus klarerweise $PAut(G) = Aut(G)$. Gilt $PAut(G) = Aut(G)$, so folgt $A(G) \subseteq \overline{P_1(G)} = I(G)$, also $A(G) = I(G)$.

Die Frage, wann $I(G) = A(G)$ oder $I(G) = E(G)$ gilt, wird in [13] behandelt. Wir wollen nur exemplarisch eine Aussage herausgreifen und ansonsten für dieses Problem den Leser an [13] verweisen.

**Proposition 3.6.10** *Es sei* $G$ *eine Gruppe, die nur einen minimalen Normalteiler* $N$ *hat. Ist* $N$ *nicht abelsch und* $G/N$ *zyklisch, so gilt*

$$I(G) = A(G) = E(G)$$

**Beweis:** [13] Korollar 2

# Anhang A

# Grundlagen

## A.1 Mengen und Klassen

Da wir nicht in die (Un)tiefen der Mengen- und Klassentheorie eindringen wollen, seien nur einige Tatsachen und Definitionen kurz erwähnt. Die axiomatische Einführung dieser Begriffe kann man z.B. in [2] nachlesen.

**Definition A.1.1** *Eine* **Klasse** *ist eine (mitunter leere) Kollektion von Objekten. Eine* **Menge** *ist eine Klasse, die Element einer anderen Klasse ist. Ist ein Objekt $a$* **Element** *einer Menge $M$, so schreiben wir $a \in M$. Ist jedes Element von $A$ in $B$, so bezeichnen wir $A$* **Teilmenge** *von $B$, symbolisch $A \subseteq B$. Die Menge aller Teilmenge einer Menge $A$ ist die sogenannte* **Potenzmenge**, *symbolisch $\mathfrak{P}(A)$.*

Als bekannte Zahlenmengen setzen wir die natürlichen Zahlen, $\mathbb{N}$, die ganzen Zahlen $\mathbb{Z}$ und die reellen Zahlen $\mathbb{R}$ voraus.

## A.2 Relationen

**Definition A.2.1** *Eine* **Relation** *$R$ von $A$ nach $B$ ist eine Teilmenge von $A \times B$. Wir schreiben $a \sim_R b \iff (a, b) \in R$*

**Definition A.2.2** *Die* **Umkehrrelation** *ist $R^{-1} = \{(b, a) : (a, b) \in R\}$*

**Definition A.2.3** *Sei $R$ eine Relation von $A$ nach $B$, $S$ eine Relation von $B$ nach $C$. Dann ist die* **Komposition** *von $R$ und $S$*

$$R \circ S = \{(a, c) : \exists b \in B : (a, b) \in R \wedge (b, c) \in S\}$$

### A.2.1 Äquivalenzrelationen

**Definition A.2.4** *Eine Relation $R$ von $A$ nach $A$ heißt* **Äquivalenzrelation** *von $A$ , wenn sie die folgenden Eigenschaften erfüllt:*

- *sie ist* **reflexiv** *: $a \sim_R a \; \forall a \in A$*
- *sie ist* **symmetrisch** *: $\forall a, b \in A : (a \sim_R b \Longrightarrow b \sim_R a)$, und*
- *sie ist* **transitiv** *: $\forall a, a', a'' \in A : ((a \sim_R a' \wedge a' \sim_R a'') \Longrightarrow a \sim_R a'')$*

**Definition A.2.5** *Eine Familie von Teilmengen $K_i \subseteq A$, $i \in I$ heißt* **Klasseneinteilung** *, wenn*

- *$\forall a \exists i \in I$ mit $a \in K_i$*
- *$\forall i, j \in I : K_i \cap K_j = \emptyset$*

**Proposition A.2.6** *Die Äquivalenzrelationen entsprechen genau den Klasseneinteilungen.*

**Definition A.2.7** *Sei $R$ eine Äquivalenzrelation von $A$, dann ist $C(a) = \{b \in A | a \sim_R b\}$ die* **Klasse** *von $a$.*

### A.2.2 Ordnung

**Definition A.2.8** *Eine Relation $R$ von $A$ nach $A$ heißt* **partielle Ordnung**, *wenn sie*

- *reflexiv ist*
- *transitiv ist, und*
- **anti-symmetrisch** *ist: $\forall a, a' \in A : ((a \sim_R b \wedge b \sim_R a) \Longrightarrow a = b)$*

Ist $A$ eine beliebige Menge, so ist die Potenzmenge mit der Mengeninklusion, $[\mathfrak{P}(A); \subseteq]$, eine partiell geordnete Menge.

**Definition A.2.9** *Sei $[A; \leq]$ eine partiell geordnete Menge, $M \subseteq A$ , dann heißt ein Element $x \in A$*

- **größtes Element von M**, *wenn $x \in M$ und $\forall m \in M : m \leq x$*
- **kleinstes Element von M**, *wenn $x \in M$ und $\forall m \in M : m \geq x$*

- **Maximum von M** *bzw.* **maximales Element** *von $M$ , wenn $x \in M$ und $x \leq m \Longrightarrow x = m$*
- **Minimum von M** *bzw.* **minimales Element** *von $M$, wenn $x \in M$ und $m \leq x \Longrightarrow x = m$*
- **untere Schranke von M**, *wenn $\forall m \in M : x \leq m$*
- **obere Schranke von M**, *wenn $\forall m \in M : m \leq x$*
- **Supremum von M** *oder* **kleinste obere Schranke von M**, *wenn es minimale obere Schranke ist.*
- **Infinum von M** *oder* **größte untere Schranke von M**, *wenn es maximale untere Schranke ist.*

Also kann es höchstens ein größtes bzw. kleinstes Element einer Mengen geben, während es mehrere verschiedene maximale bzw. mininale Elemente geben kann.

**Definition A.2.10** *Sei $[A; \leq]$ eine partiell geordnete Menge. $A$ heißt* **vollständig geordnet** *(bzw. $\leq$ eine* **vollständige Ordnung**), wenn für jede Teilmenge $M \subseteq A$ das Supremum und das Infinum von M existiert.
$A$ heißt **wohl geordnet** *(bzw. $\leq$ eine* **Wohlordnung**), wenn jede Teilmenge $M \subseteq A$ ein kleinstes Element besitzt.
$A$ heißt **total geordnet** *(bzw. $\leq$ eine* **Totalordnung**), wenn für alle $a, b \in A$ gilt $a \leq b$ oder $b \leq a$.

## A.3 Funktionen

**Definition A.3.1** *Eine* **Funktion** *von $A$ nach $B$ ist eine Relation von $A$ nach $B$, für die es für jedes $a \in A$ genau ein $b \in B$ gibt, sodaß $(a, b) \in R$. Wir bezeichnen dieses Paar mit $(x, f(x))$ Die Menge aller Funktionen von $A$ nach $B$ bezeichnen wir mit $F(A, B)$. Die Funktionen von $A$ nach $A$ mit $F(A)$, die Funktionen von $A^k$ nach $A$ mit $F_k(A)$.*

**Definition A.3.2** *Ist $U \subseteq A$, dann bezeichnen wir die Abbildung $\iota : U \to A$ mit $u \mapsto u$ als* **Inklusion.**

**Definition A.3.3** *Ist $f : A \to B$ eine Funktion, $U \subseteq A$, dann sei $f|_U = f \circ \iota$, die* **Einschränkung von f auf** *$U$. Also gilt $f|_U : U \to B$ mit $u \mapsto f(u)$.*

**Definition A.3.4** *Ist $f : A \to B$ eine Funktion, dann ist für $b \in B$*

$$f^{-1}(b) = \{a \in A : f(a) = b\}$$

*Ist $U \subseteq B$, so ist*

$$f^{-1}(U) = \{a \in A : \exists u \in U : f(a) = u\}$$

**Lemma A.3.5** *Sei $U, U' \subseteq A$,$V, V' \subseteq B$, dann ist für $f : A \to B$*

- $U \subseteq U' \Longrightarrow f(U) \subseteq f(U')$
- $f(U \cup U') = f(U) \cup f(U')$
- $f(U \cap U') \subseteq f(U) \cap f(U')$
- $V \subseteq V' \Longrightarrow f^{-1}(V) \subseteq f^{-1}(V')$
- $f^{-1}(V \cup V') = f^{-1}(V) \cup f^{-1}(V')$
- $f^{-1}(V \cap V') = f^{-1}(V) \cap f^{-1}(V')$

**Definition A.3.6** *Sei $f$ eine Funktion von $A$ nach $B$. Dann heißt $f$*
**injektiv** $\Longleftrightarrow (\forall a, a' \in A : f(a) = f(a') \longrightarrow a = a')$
**surjektiv** $\Longleftrightarrow (\forall b \in B \exists a : f(a) = b)$
**bijektiv** $\Longleftrightarrow$ *$f$ injektiv und surjektiv. Ist $A = B$, so nennen wir bijektive Abildungen $f : A \to A$* **Permutationen**.

**Proposition A.3.7** *(i)* $A \subseteq f^{-1}(f(A))$;
*(ii)* $A = f^{-1}(f(A)) \Longleftrightarrow$ *$f$ injektiv*
*(iii)* $f(f^{-1}(A)) \subseteq A$
*(iv)* $f(f^{-1}(A)) = A \Longleftrightarrow$ *$f$ surjektiv*

**Lemma A.3.8** *$g : B \to C$, $h : A \to B$ und ist $f : A \to C$ mit $f = g \circ h$, dann gilt:*

1. *$f$ injektiv $\Longrightarrow$ $h$ injektiv*
2. *$f$ surjektiv $\Longrightarrow$ $g$ surjektiv*
3. *$h$,$g$ injektiv $\Longrightarrow$ $f$ injektiv*

*4. h,g surjektiv $\Longrightarrow$ f surjektiv*

**Definition A.3.9** *Sind $f : A \to B$ und $g : A' \to B'$ Funktionen so bezeichnen wir mit $f \times g : A \times A' \to B \times B'$ die (kanonische) Abbildung für die gilt: $(f \times g)(a, a') = (f(a), f(a'))$ die* **komponentenweise Anwendung**. *Ist $f : A \to B$, so sei $f^k : A^k \to B^k$ jene Abbildung für die gilt: $f^k(a_1, \ldots, a_k) = (f(a_1), \ldots, f(a_k))$, die* **Produktabbildung** .

**Definition A.3.10** *Zwei Menge $A, B$ heißen* **gleichmächtig**, *wenn es eine bijektive Abbildung $f : A \to B$ gibt.*

Das induziert eine Äquivalenzrelation.

**Definition A.3.11** *Die Klasse einer Menge A bezüglich dieser Relation wird* **Kardinalität** *oder Kardinalzahl genannt, symbolisch $|A|$.*

Für endliche Mengen kann die Kardinalität mit der Ordnung der Menge identifiziert werden. Die Kardinalität der Menge der natürlichen Zahlen wird mit $\aleph_0$ bezeichnet und als *abzählbare* Kardinaliät bezeichnet.

Wir können Operationen für Kardinalzahlen folgenderweise definieren:

**Definition A.3.12** *Es seien $\mathfrak{m}_i$ für $i \in I$ Kardinalzahlen mit $\mathfrak{m}_i = |A_i|$, weiters sei $A_i \cap A_j = \emptyset$ für alle $i \neq j \in I$, dann sei*

$$\sum_{i \in I} \mathfrak{m}_i = \left| \bigcup_{i \in I} A_i \right|$$

*und*

$$\prod_{i \in I} \mathfrak{m}_i = \left| \prod_{i \in I} A_i \right|$$

Wir können auch eine Ordnung von Kardinalzahlen einführen:

**Definition A.3.13** *Wir definieren $\mathfrak{m}_1 \leq \mathfrak{m}_2$ gilt genau dann, wenn es zwei Mengen A, B mit $\mathfrak{m}_1 = |A|$ und $\mathfrak{m}_2 = |B|$ und eine injektive Abbildung $f : A \to B$ gibt.*

Auf jeder Menge von Kardinalzahlen definiert das eine totale Ordnung.

Es gilt:

**Korollar A.3.14**

- *Ist $A \subseteq B$, so ist $|A| \leq |B|$.*
- *Für $n \in \mathbb{N}$ ist $n < \aleph_0$.*

- $\left|\bigcup_{i\in I} A_i\right| \leq \sum_{i\in I} |A_i|$.
- *Ist* $\mathfrak{m}_i \leq \mathfrak{n}_i$ *für alle* $i \in I$, *so ist* $\sum_{i\in I} \mathfrak{m}_i \leq \sum_{i\in I} \mathfrak{n}_i$ *und* $\prod_{i\in I} \mathfrak{m}_i \leq \prod_{i\in I} \mathfrak{n}_i$.
- *Ist* $\mathfrak{m}$ *oder* $\mathfrak{n}$ *eine unendliche Kardinalzahl so ist* $\mathfrak{m} + \mathfrak{n} = max(\mathfrak{m}, \mathfrak{n})$, *sind beide* $\neq 0$, *so ist auch* $\mathfrak{m} \cdot \mathfrak{n} = max(\mathfrak{m}, \mathfrak{n})$.
- *Ist* $\mathfrak{m}$ *eine unendliche Kardinalzahl und* $n \in \mathbb{N}$, *so ist* $\mathfrak{m}^n = \mathfrak{m}$.
- *Für jede Menge* $A$ *gilt* $|A| < 2^{|A|} = |\mathfrak{P}(A)|$.

## A.4 Verbände

**Definition A.4.1** *Eine Menge* $V$ *mit den binären Operation* $\cup$ *und* $\cap$ *heißt* **Verband**, *wenn für alle a,b in* $V$ *gilt*

$\cup$ *und* $\cap$ *sind assoziativ:*

1. $(a \cup b) \cup c = a \cup (b \cup c)$
2. $(a \cap b) \cap c = a \cap (b \cap c)$
   $\cup$ *und* $\cap$ *sind kommutativ:*
3. $a \cup b = b \cup a$
4. $a \cap b = b \cap a$
   $\cup$ *und* $\cap$ *erfüllen die sogenannten „Absorptionsgesetze“*
5. $a \cup (a \cap b) = a$
6. $a \cap (a \cup b) = a$

Es gibt einen engen Zusammenhang zwischen Verbänden und bestimmten partiell geordneten Mengen:

**Satz A.4.2** *Sei* $[V; \cup, \cap]$ *ein Verband. Dann sei* $a \leq b$ *genau dann, wenn* $a \cup b = b$. *Dann ist* $V_{\leq} = [V; \leq]$ *eine partiell geordnete Menge, wo für jede zweielementige Teilmenge* $\{a, b\}$ *stets das* $sup\{a, b\} = a \cup b$ *und das* $inf\{a, b\} = a \cap b$ *existieren.*

*Ist* $[P; \leq]$ *eine geordnete Menge, wo für jede zweielementige Teilmenge* $\{a, b\}$ *stets das* $sup\{a, b\}$ *und das* $inf\{a, b\}$ *existieren, so definieren* $a \cup b = sup\{a, b\}$ *und* $a \cap b = inf\{a, b\}$. *Dann ist* $\widetilde{P} = [P; \cup, \cap]$ *ein Verband. Für alle solchen* $P$ *gilt* $\left(\widetilde{P}\right)_{\leq} = P$ *und für jeden Verband* $V$ *gilt* $\widetilde{(V_{\leq})} = V$.

**Definition A.4.3** *Ein Verband heißt* **vollständig** *, wenn für alle $B \subseteq V$ in der zugehörigen partiellen Ordnung $sup(B)$ und $inf(B)$ existieren.*

**Lemma A.4.4** *Eine partiell geordnete Menge $[P; \leq]$ ist genau dann ein vollständiger Verband, wenn $P$ ein größtes Element hat und für jede nicht leere Teilmenge $B \subseteq A$ das $inf(B)$ existiert.*

## A.5 Kategorien

In vielen Bereichen der Mathematik können Parallelen in Aussagen und Konzepten beobachtet werden. So können wir in der Algebra aber auch der Topologie Mengen mit bestimmten Strukturen gemeinsam mit Abbildungen zwischen diesen Mengen, die diese Struktur erhalten, betrachten. Die untersuchten Mengen gemeinsam mit den Abbildungen bilden sogenannte *Kategorien*. In dieser Arbeit werden keine Resultate der Kategorientheorie verwendet, nur aufgezeigt, wenn bestimmte Klassen die folgenden grundlegenden Definition erfüllen:

**Definition A.5.1** *Eine* **Kategorie** $\mathfrak{K}$ *ist eine Klasse von* **$\mathfrak{K}$-Objekten** $\mathfrak{Ob}_{\mathfrak{K}}$ *gemeinsam mit* **$\mathfrak{K}$-Morphismen** $\mathfrak{Mor}_{\mathfrak{K}}$ *sodaß gilt:*

- *Für alle Objekte $A, B \in \mathfrak{Ob}_{\mathfrak{K}}$ gibt es eine Menge $Hom(A, B)$ von Morphismen, sodaß jeder Morphismus nur zu einer Menge $Hom(A, B)$ gehört*
- *Für alle Objekte $A, B, C \in \mathfrak{Ob}_{\mathfrak{K}}$ und alle $f \in Hom(A, B)$ und $g \in Hom(B, C)$, gibt es ein eindeutiges Element $h$ in $Hom(A, C)$, genannt die* **Komposition** *, symbolisch: $h = g \circ f$.*
- *Sind $A, B, C, D \in \mathfrak{Ob}_{\mathfrak{K}}$ und $f \in Hom(A, B), g \in Hom(B, C)$ und $h \in Hom(C, D)$, so gilt*

$$h \circ (g \circ f) = (h \circ g) \circ f$$

- *Für jedes Objekt $A \in \mathfrak{Ob}_{\mathfrak{K}}$ gibt es einen Morphismus $id_A \in Hom(A, A)$, genannt der* **Identitätsmorphismus** *, sodaß für alle $B \in \mathfrak{Ob}_{\mathfrak{K}}$ und für alle $g \in Hom(A, B)$ und $f \in Hom(B, A)$ gilt:*

$$f \circ id_A = f \text{ und } id_A \circ g = g$$

Diese Definition lassen bereits Beispiele für Kategorien vermuten:

**Beispiele:**

- Es sei $U$ eine Menge, das *Universum*. Dann bilden alle Teilmenge dieser Menge und die Funktionen dazwischen eine Kategorie.
- Die Kategorie der Gruppen mit Homomorphismen.
- Die Kategorie aller topologischen Räume und stetigen Funktionen.
- Die Kategorie aller geordneten Menge und Ordnungshomomorphismen.

**Definition A.5.2** *Ein* **kovarianter Funktor** *von der Kategorie $\mathfrak{K}$ in die Kategorie $\mathfrak{L}$ sind Abbildungen von $\mathfrak{Ob}_{\mathfrak{K}}$ nach $\mathfrak{Ob}_{\mathfrak{L}}$ und $\mathfrak{Mor}_{\mathfrak{K}}$ nach $\mathfrak{Mor}_{\mathfrak{K}}$, mit dem selben Symbol dargestellt, etwa $F$, sodaß gilt:*

1. $F(id_A) = id_{F(A)}$
2. *Wenn $f \circ g$ in $\mathfrak{K}$ definiert ist, so ist $F(f) \circ F(g)$ in $\mathfrak{L}$ definiert und es gilt $F(f \circ g) = F(f) \circ F(g)$.*

*$F$ heißt* **kontravarianter Funktor**, *wenn gilt:*

1. $F(id_A) = id_{F(A)}$
2. *Wenn $f \circ g$ in $\mathfrak{K}$ definiert ist, so ist $F(g) \circ F(f)$ in $\mathfrak{L}$ definiert und es gilt $F(f \circ g) = F(g) \circ F(f)$.*

**Definition A.5.3** *Es seien $\mathfrak{K}, \mathfrak{L}$ Kategorien und $F, G$ Funktoren zwischen diesen Kategorien. Eine Abbildung $\tau : F \to G$ heißt* **natürliche Transformation** *von Funktoren, wenn jedem Element $A \in \mathfrak{Ob}_{\mathfrak{K}}$ ein $\mathfrak{L}$-Morphismus $\tau(A) : F(A) \to G(A)$ zugeordnet wird, sodaß für alle $f : A \to B$ mit $B \in \mathfrak{Ob}_{\mathfrak{K}}$ gilt $\tau(B) \circ F(f) = G(f) \circ \tau(A)$, also das Diagramm in Abbildung A.1 kommutiert:*

## A.6 Matrizen

**Definition A.6.1** *Die Menge aller $k \times n$-Matrizen über einem Ring $R$ sei mit $M_{k \times n}(R)$ bezeichnet. $M^{(i)}$ bezeichne die $i$-te Zeile für $i = 1, \ldots, k$.*

*Ist $M = (m_{ij})$ eine Matrix, so sei $(M)_{ij}$ der Eintrag in der $i$-ten Zeile und $j$ten Spalte.*

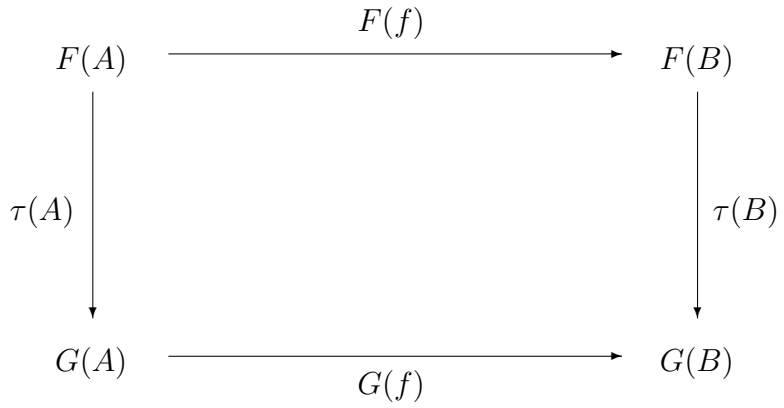


Abbildung A.1: Die natürliche Transformation von Funktoren

Also ist $M^{(i)} = (m_{i1}, m_{i2}, \ldots, m_{in})$.

Ist andererseits $a_{ij}$ eine Zahl für alle $i, j = 1, \ldots, k$, so sei $(a_{ij})_{i=1,\ldots,k;j=1,\ldots,k}$ jene Matrix mit $a_ij$ als Eintrag in der $i$-ten Zeile und $j$-ten Spalte. (Sind die Grenzen klar, so schreiben wir einfach $(a_{ij})_{ij}$

Wir können auf den Matrizen eine Addition und Muliplikation definieren, für $A = (a_{ij})$, $B = (b_{ij}) \in M_{k\times n}$ so ist für $C = A + B = (c_{ij}$ der Eintrag $c_{ij} = a_{ij} + b_{ij}$. Sind $A = (a_{ij})$, $B = (b_{ij}) \in M_{k\times k}$, dann ist für $D = A \cdot B = (d_{ij})$ $d_{ij} = \sum_{l=1}^{k} a_{il} \cdot b_{lj}$.

**Definition A.6.2** *Es sei $R$ ein Ring. Die Menge $M_{k\times k}(R)$ ist ein Ring, der* **volle** $k \times k$ **Matrizenring** *über $R$.*

Die Permutationen der Menge $\{1, 2, \ldots, n\}$ sei mit $\mathbb{S}_n$ bezeichnet. Das *Signum* einer Permutation $\sigma$ ist $sgn(\sigma) = (-1)^l$, wobei $l$ die Anzahl der Transpositionen ist, mit welchen $\sigma$ als Produkt darstellbar ist, dabei ist $l$ immer gerade oder ungerade (siehe A.8.39).

**Definition A.6.3** *Die* **Determinante** *einer $k \times k$ Matrix $A$ ist definiert durch:*

$$det(A) = \sum_{\sigma\in\mathbb{S}_k} (sgn(\sigma))\, a_{\sigma(1)1} \cdot a_{\sigma(2)2} \cdot \ldots a_{\sigma(k)k}$$

Es gilt:

**Korollar A.6.4** *Es seien $A, B$ $k \times k$ Matrizen, dann ist*

$$det(A \cdot B) = det(A) \cdot det(B)$$

*Ist $A$ eine invertierbare $k \times k$ Matrix, so ist*

$$det(A^{-1}) = det(A)^{-1}$$

*Es sei $A$ eine $k \times k$ Matrix, dann ist $A$ genau dann invertierbar, wenn $det(A) \neq 0$.*

**Definition A.6.5** *Es sei $GL(k, R) = \{M \in M_k(R) : det(M) \neq 0\}$ die invertierbaren $k \times k$ Matrizen.*

**Definition A.6.6** *Ist $K$ ein endlicher Körper der Ordnung $p^t$, so sei $GL(k, p^t) = GL(k, K)$.*

Es gilt $|GL(k, p^t)| = (p^{m \cdot t} - 1) \cdot (p^{m \cdot t} - p^t) \cdot (p^{m \cdot t} - p^{2 \cdot t}) \cdot \ldots \cdot (p^{m \cdot t} - p^{(m-1) \cdot t})$.

## A.7 Zahlentheorie

Wir benötigen nur einige wenige Definitionen und Aussagen der Zahlentheorie.

**Definition A.7.1** *Das* **kleinste gemeinsame Vielfache** *zweier Zahlen $n_1, n_2 \in \mathbb{Z}$ wird mit $kgV(n_1, n_2)$ oder $[n_1, n_2]$ bezeichnet.*

*Der* **größte gemeinsame Teiler** *zweier Zahlen $n_1, n_2 \in \mathbb{Z}$ wird mit $ggT(n_1, n_2)$ oder mit $(n_1, n_2)$ bezeichnet.*

*Ist für $n_1, n_2 \in \mathbb{Z}$ der größte gemeinsame Teiler $(n_1, n_2) = 1$, so nennt man $n_1, n_2$* **teilerfremd**.

Die folgende Aussage ist ganz klar

**Lemma A.7.2** *Es seien $n_1, n_2 \in \mathbb{Z}$ mit $ggT(n_1, n_2) = d$. Dann gibt es $x, y \in \mathbb{Z}$, sodaß $n_1 \cdot x + n_2 \cdot y = d$.*

Betrachten wir den Rest bei Division

**Definition A.7.3** *Es seien $a, b, c$ ganze Zahlen, dann ist $a \equiv_c b$, auch $a \equiv b \mod c$, wenn $l, l', r \in \mathbb{Z}$ existieren, sodaß $a = l \cdot c + r$ und $b = l' \cdot c + r$.*

D.h. bei der Division durch $c$ bleibt bei $a$ und $b$ der selbe Rest; bzw. $c$ teilt $a - b$

Eine für uns wichtige Funktion ist

**Definition A.7.4** *Die* **Euler Funktion** $\varphi : \mathbb{N} \to \mathbb{N}$ *ist definiert durch:*

- $\varphi(1) = 1$
- *$\varphi(h)$ ist die Anzahl der natürlichen Zahlen $k$ mit $1 \leq k < h$, für die gilt $ggT(k,h) = 1$*

**Proposition A.7.5** *Die Euler Funktion $\varphi$ hat folgende Eigenschaften*

- *Ist $p$ eine Primzahl, so ist $\varphi(p^t) = p^t \cdot \left(1 - \frac{1}{p}\right)$*
- *Ist $ggT(r,s) = 1$, so ist $\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$*
- *Es sei $h = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots p_l^{s_l}$ die eindeutige Primfaktorenzerlegung der Zahl $h$, dann ist $\varphi(h) = h \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_1}\right)$*

Die Euler Funktion an der Stelle $h$ entspricht der Anzahl der Einheiten des Restklassenrings modulo $h$ $\mathbb{Z}_h = \mathbb{Z}/h \cdot \mathbb{Z}$. Diese Menge $\mathcal{E}(\mathbb{Z}_h)$ ist eine Gruppe bzgl. der Multiplikation und wird die *Gruppe der primen Restklassen modulo $h$* genannt und mit $\mathfrak{P}_h$ bezeichnet.

$$\varphi(h) = |\mathcal{E}(\mathbb{Z}_h)| = |\mathfrak{P}_h|$$

Diese Definition können wir etwas verallgemeinern:

**Definition A.7.6** *Die verallgemeinerte Euler-Funktion*sei

$$\varphi_n(k) = |\mathfrak{P}_n(k)|$$

wobei $\mathfrak{P}_n(k)$ die Menge der invertierbaren $n \times n$-Matrizen über $\mathbb{Z}_k$ ist, also

$$\mathfrak{P}_n(k) = \mathcal{E}\left(M_n\left(\mathbb{Z}_k\right)\right)$$

Insbesondere gilt

$$\varphi_n(p) = (p^n - 1) \cdot (p^n - p) \cdot \ldots \cdot (p^n - p^{n-1})$$

# A.8 Gruppen und Halbgruppen

## A.8.1 Grundlagen

**Definition A.8.1** *Eine Menge $H$ mit einer binären Operation $\cdot : H \times H \to H$, $(h_1, h_2) \mapsto h_1 \cdot h_2$, heißt* **Halbgruppe** *, wenn diese Operation* **assoziativ** *ist, d.h. $\forall h_1, h_2, h_3 \in H$ gilt:*

$$h_1 \cdot (h_2 \cdot h_3) = (h_1 \cdot h_2) \cdot h_3$$

*Ein Element $e$ heißt* **linke Eins** *(resp. rechte Eins), wenn $\forall h_1 \in H$ gilt:*

$$e \cdot h_1 = h_1 \quad (resp.\ h_1 \cdot e = h_1)$$

*Ein Element $e$ heißt* **Eins**, *wenn es linke und rechte Eins ist.*

Ein Beispiel für Halbgruppen sind die Funktionen einer Menge in sich selbst mit der Komposition. Für alle $A$ ist $[F(A,A); \circ, id_A]$ eine Halbgruppe mit Eins.

**Definition A.8.2** *Eine Menge $G$ heißt* **Gruppe**, *wenn $G$ eine Halbgruppe mit Eins $e$ ist und es ein* **Inverses** *gibt, d.h. es gilt*

$$\forall x \in G\ \exists x^{-1} \in G : x^{-1} \cdot x = x \cdot x^{-1} = e$$

**Definition A.8.3** *Ist $H =< H; \circ >$ eine Halbgruppe mit Eins (1). Ein Element $a \in H$ heißt* **Einheit** *, wenn $\exists b \in H : a \circ b = b \circ a = 1$. Die Menge aller Einheiten bezeichnen wir mit $\mathcal{E}(H)$.*

**Bemerkung:** $\mathcal{E}(H)$ ist klarerweise eine Gruppe. Für $S_1 \subseteq S_2$ gilt: $\mathcal{E}(S_1) \subseteq \mathcal{E}(S_2)$.

**Definition A.8.4** *Ein Element $a$ einer Halbgruppe $H$ heißt* **regulär** *, wenn gilt:*

$$\exists x \in H : a \cdot x \cdot a = a$$

*Ein Element $a$ heißt* **linkskürzbar**

$$b, c \in H : a \circ b = a \circ c \Longrightarrow b = c$$

*es heißt* **rechtskürzbar** *, wenn gilt*

$$b, c \in H : b \circ a = c \circ a \Longrightarrow b = c$$

*Das Element $a$ heißt* **kürzbar** *, wenn es rechts- und linkskürzbar ist. Die Menge aller kürzbaren Elemente von $G$ bezeichnen wir mit $\mathcal{C}(G)$.*

**Lemma A.8.5** *1. $\mathcal{C}(H)$ ist eine Halbgruppe und $\mathcal{E}(H) \subseteq \mathcal{C}(H)$*

2. *Für $S_1 \subseteq S_2$ gilt: $\mathcal{C}(S_1) \supseteq \mathcal{C}(S_2) \cap S_1$. Insgesamt also $\mathcal{E}(S_1) \subseteq \mathcal{E}(S_2) \cap S_1 \subseteq \mathcal{C}(S_2) \cap S_1 \subseteq \mathcal{C}(S_1)$.*

3. *$\mathcal{E}(H) = \mathcal{C}(H) \Longleftrightarrow \mathcal{C}(H)$ ist eine Gruppe.*

4. *Ist $H$ endlich, gelten beide Bedingungen in (3).*

**Beweis:** (1), (2), (3) klar.
(4) Betrachte für $a \in \mathcal{C}(H)$ die Menge $M(a) = \{1, a, a^2, a^3, a^4, .....\}$. $M(a) \subseteq H$. Da $H$ endlich ist, ist auch diese Menge endlich, d.h. es existieren $m, n \in \mathbb{N}$, oBdA $m \geq n$, sodaß $a^m = a^n$. $a \in \mathcal{C}(H) \Longrightarrow a^{m-1} = a^{n-1} \Longrightarrow \ldots \Longrightarrow a^{m-n} = 1$. Damit gilt aber $a^{m-n-1} \circ a = a \circ a^{m-n-1} = 1$, d.h. $a \in \mathcal{E}(H)$. □

Der Vollständigkeit halber definieren wir analog zu 1.1.11:

**Definition A.8.6** *Es seien G,H Gruppen. Eine Abbildung* $\varphi : G \to H$ *heißt* **Homomorphismus**, *wenn gilt:* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(v)$. *Symb.:* $\varphi \in Hom(G, H)$
*Ist* $\varphi$ *injektiv so heißt es* **Monomorphismus**, *surjektiv* **Epimorphismus**, *bijektiv* **Isomorphismus**.
*Ist* $\varphi \in Hom(G, G)$ *so heißt es* **Endomorphismus**, *ist* $\varphi \in Hom(G, G)$ *so heißt es* **Automorphismus**.

**Definition A.8.7** *Die Abbildungen* $\tau_g : G \to G$ *mit* $\tau_g(x) = g \cdot x \cdot g^{-1}$, $g \in G$ *heißen* **innere Automorphismen** , *symb.* $\tau_g \in Inn(G)$.

Innere Automorphismen sind tatsächlich Automorphismen.

**Definition A.8.8** *Eine Untergruppe U von G heißt* **voll invariant, charakteristisch** *resp.* **normal** , *wenn sie bzgl. den Endomorphismen, Automorphismus resp. den inneren Automorphismen von G abgeschlossen ist. Eine normale Untergruppe nennen wir auch* **Normalteiler** *und schreiben symbolisch* $N \trianglelefteq G$.

*Eine Gruppe heißt* **einfach** *respektive* **charakteristisch einfach**, *wenn sie keine nicht trivialen normalen respektive charakteristischen Untergruppen enthält.*

Es ist leicht zu zeigen, daß gilt

**Lemma A.8.9** *Ist* $N \trianglelefteq G$, *und* $\varphi \in Epi(G, H)$ *so ist* $\varphi(N) \trianglelefteq \varphi(G)$.

**Definition A.8.10** *Eine Untergruppe U der Gruppe G heißt minimal* , wenn gilt:

$$\forall U' \preceq G \text{ mit } U' \subseteq U \Longrightarrow U' = \{1\} \vee U' = U$$

Die Begriffe einer maximalen Untergruppe, sowie eines minimalen oder maximalen Normalteilers sind auf ähnliche Weise definiert.

**Definition A.8.11** *Es sei* $[G;\cdot,^{-1},1]$ *eine Gruppe. Es sei* $N \trianglelefteq G$*, dann definiere* $\sim_N$ *als die durch den Normalteiler induzierte Relation:* $a \sim_N b \Longleftrightarrow a \cdot b^{-1} \in N$*. Das ist eine Äquivalenzrelation, die Klasseneinteilung der* **Nebenklassen** *. Auf den Klassen können die Operationen definiert werden, sodaß wieder eine Gruppe entsteht:* $[G/N;\cdot,^{-1},e]$ *mit* $C(g)\cdot C(g') = (g\cdot N)\cdot(g'\cdot N) = (g\cdot g')\cdot N = C(g\cdot g')$*,* $(g\cdot N)^{-1} = g^{-1}N$ *und* $e = 1\cdot N = N$*. Die Abbildung* $\pi : G \to G/N$ *mit* $\pi(g) = C(g)$ *nennen wir den* **kanonischen Epimorphismus**.

Diese Operationen sind wohldefiniert, denn es gilt:

**Lemma A.8.12** *Es sei* $G$ *eine Gruppe,* $N \trianglelefteq G$ *und* $a_1, a_2, b_1, b_2 \in G$ *mit* $a_1 \sim_N b_1, a_2 \sim_N b_2$*. Dann ist* $a_1 \cdot b_1 \sim_N a_2 \cdot b_2$ *und* $a_1^{-1} \sim_N b_1^{-1}$

**Beweis:** Sei $a_1 \sim_K b_1$ und $a_2 \sim_K b_2$. Dann ist $a_1 \in b_1 \cdot N$ und $a_2 \in b_2 \cdot N$ und $a_1 \cdot a_2 = b_1 \cdot n_1 \cdot b_2 \cdot n_2 = b_1 \cdot b_2 \cdot n_1' \cdot n_2 = (b_1 \cdot b_2) \cdot n'$.
Weiters ist $a_1^{-1} = (b_1 \cdot n_1)^{-1} = n_1^{-1} \cdot b_1^{-1} = b_1^{-1} \cdot n_1'$. □

**Definition A.8.13** *Es seien* $G$ *und* $H$ *Gruppen,* $\varphi : G \to H$ *ein Homomorphismus. Der* **Kern** *von* $\varphi$ *ist* $Ker(\varphi) = \{a \in G : \varphi(a) = 1\}$.

*Das* **Bild** *von* $\varphi$ *ist* $Im(\varphi) = \{b \in H : \exists a \in G : \varphi(a) = b\}$.

Es gilt: $Ker(\varphi) \trianglelefteq G$, $Im(\varphi) \preceq H$.

**Satz A.8.14** Homomorphiesatz *Es seien* $G, H$ *Gruppen.* $\varphi : G \to H$ *ein Homomorphismus. Dann ist*

$$G/Ker(\varphi) \simeq Im(\varphi)$$

*Der Isomorphismus ist gegeben durch* $g \cdot Ker(\varphi) \mapsto \varphi(g)$.

**Beweis:** [15] Kapitel 1, Satz 5.4.

Man kann diesen Homomorphiesatz verallgemeinern

**Proposition A.8.15** *Es sei* $G, H$ *Gruppen,* $N \trianglelefteq G$ *und es sei* $\varphi : G \to H$ *ein Homomorphismus. Dann existiert ein Epimorphismus* $\widetilde{\varphi} : G/N \to \varphi(G)/\varphi(N)$ *mit* $\widetilde{\varphi}(g\cdot N) = \varphi(g)\cdot\varphi(N)$*. Gilt* $N \subseteq Ker(\varphi)$ *so ist* $\widetilde{\varphi}(g\cdot N) = \varphi(g)$.

**Beweis:** Nach A.8.9 ist $\varphi(N) \trianglelefteq \varphi(G)$. Es ist leicht zu zeigen, daß die Abbildung $\widetilde{\varphi}$ ein wohldefinierter Epimoprhismus ist. Ist $H \subseteq Ker(\varphi)$, so ist $\varphi(H) = \{e\}$, so folgt die letze Behauptung. □

Ist in dieser Formulierung $N = Ker(\varphi)$, so ist $\widetilde{\varphi}$ injektiv und somit ein Isomorphismus und es folgt der Homomorphiesatz.

Es gilt ferner der sogenannte Korrespondenzsatz:

**Proposition A.8.16** *Es sei $N \trianglelefteq G$ und es sei $\pi : G \to G/N$ der kanonische Epimorphismus. Dann definiert $\pi$ eine bijektive Korrespondenz zwischen der Menge aller Untergruppen von $G$, die $N$ enthalten und den Untergruppen von $G/N$. Es gilt für $S, T \preceq G$*

- $\pi(S) \supset \pi(T) \Longleftrightarrow S \supset T$
- $\pi(S) \trianglelefteq \pi(T) \Longleftrightarrow S \trianglelefteq T$ *und dann gilt* $T/S \simeq \pi(T)/\pi(S)$

**Beweis:** [27] Satz 2.17.

Inbesondere entsprechen also Normalteiler von $G/N$ jenen von $G$, die $N$ enthalten. Aus der letzten Eigenschaft folgt direkt:

**Satz A.8.17** 1. Isomorphiemusatz *Es sei $G$ eine Gruppe, $N \trianglelefteq G$, $K \preceq G$. Dann gilt:*

$$K/(H \cap K) \simeq (K \cdot H)/H$$

**Beweis:** [15] Kapitel 1, Satz 5.6.

**Satz A.8.18** 2. Isomorphiesatz *Es sei $G$ eine Gruppe, $N \trianglelefteq G$, $K \trianglelefteq G$ und $K \subseteq N$. Dann gilt:*

$$G/N \simeq (G/K)/(N/K)$$

**Beweis:** [15] Kapitel 1, Satz 5.7.

**Lemma A.8.19** *Es sei $G$ eine Gruppe. Für $N \trianglelefteq G$ und $H \trianglelefteq G$ gilt: $G/(H \cdot N) \simeq (G/H)/(N/(N \cap H))$*

**Beweis:** Nach den Isomorphiesätzen gilt

$$G/(H \cdot N) \simeq (G(H) \,/\, ((H \cdot N) \,/H) \simeq (G(H) \,/\, (N/\,(H \cap N))$$

□

**Definition A.8.20** *Das* **Zentrum** *einer Gruppe $G$ ist definiert durch*

$$Z(G) = \{z \in G | g \cdot z = z \cdot g \ \forall g \in G\}$$

*Sei $S \subseteq G$. Dann ist der* **Normalisator** *von $S$ in $G$*

$$N_G(S) = \{n \in G | n \cdot S \cdot n^{-1} = S\}$$

*Der* **Zentralisator** *von $S$ in $G$ ist*

$$C_G(S) = \{c \in G | c \cdot x \cdot c^{-1} = x \ \forall x \in S\}$$

Für einelementige Mengen entspricht der Normalisator dem Zentralisator!

**Lemma A.8.21**

$$G/Z(G) \simeq Inn(G)$$

**Beweis:** Die Abbildung $g \mapsto \tau_g$ mit $\tau_g = g \cdot x \cdot g^{-1}$ ist ein Homomorphismus mit den Kern $Z(G)$. □

**Definition A.8.22** *Sei $g \in G$. Die* **Ordnung von** *$g$ , symb. $o(g)$, ist die Ordnung der von $g$ erzeugten Untergruppe: $o(g) = | < g >_G |$.*

Es gilt $g^{o(g)} = 1$. Mehr noch $o(g)$ ist die kleinste ganze Zahl $x$, für die gilt $g^x = 1$. Es gilt auch, wenn $G$ eine endliche Gruppe ist, daß $o(g) | |G|$.

**Definition A.8.23** *Eine Gruppe, die keine Elemente $g \neq 1$ mit endlicher Ordnung enthält ($\forall g \in G, g \neq 1 : o(g) \geq \aleph_0$) heißt* **torsionsfrei.**

*Eine Gruppe heißt* **periodisch**, *wenn jedes Element endliche Ordnung hat. Sind die Ordnungen aller Elemente in der Gruppe $G$ beschränkt, so gibt es ein kleinstes $x \in \mathbb{Z}$, sodaß $a^x = 1$ $\forall a \in G$, diese Zahl nennen wir den* **Exponenten von G** *, $exp(G) = x$. Ist die Ordnung der Elemente nicht beschränkt so setzen wir $exp(G) = 0$.*

*Es seien $p, q$ seien verschiedene Primzahlen. Wir nennen die Gruppe $G$ eine* **p-Gruppe**, *wenn die Ordnung jedes Elements von $G$ eine Potenz von $p$ ist. $G$ heißt* **(p,q)-Gruppe**, *wenn die Ordnung jedes Elements ein Produkt von Potenzen von $p$ und $q$ ist.*

*Eine Gruppe heißt* **zyklisch** *, wenn $\exists g \in G : G =< g >$*

Existiert der Exponent $exp(G) \neq 0$, so ist er das kleinste gemeinsame Vielfache der Ordnungen der Elemente. Also teilt insbesondere die Ordnung $o(g)$ jedes Elements $g \in G$ den Exponenten $exp(G)$. Klarerweise gilt für endliche Mengen auch $exp(G) | |G|$.

Ist $G$ eine $p$-Gruppe mit $|G| = p^m$, so gibt es ein Element $g$ in G, sodaß $o(g) = expG = p^n$ ist. Denn angenommen, das gilt nicht, also: $\forall g \in G$ : $o(g) < exp(G)$, also gilt $\forall g \in G \exists t_g \in \mathbb{N}$ mit $0 \leq t_g < n : o(g) = p^t$. Daraus folgt jedoch $g^{max(t_g)} = 1$, also ist $expG = max(t_g) < expG$. Widerspruch.

**Lemma A.8.24** *Jede Gruppe mit Primzahl - Ordnung ist zyklisch. In jeder endlichen, zyklischen Gruppe gibt es zu jedem Teiler der Gruppenordnung genau eine Untergruppe.*

**Beweis:** [11] (1.4.2)

**Lemma A.8.25** *Ist $G$ eine endliche Gruppe, so gibt es zu jeder Primzahlpotenz $p^t$, die $|G|$ teilt, eine Untergruppe $U$ mit $|U| = p^t$.*

**Beweis:** [11] (3.2.1)

**Definition A.8.26** *Es sei $G$ eine endliche Gruppe und $p$ eine Primzahl mit $p^t \mid |G|$ aber $p^{t+1} \not| |G|$. Dann nennen wir eine Untergruppe $S_1$ mit $|S_1| = p^t$* **p-Sylowgruppe** *von $G$.*

**Definition A.8.27** *Eine* **elementar abelsche** *Gruppe ist eine abelsche Gruppe mit exp(G) = p, p eine Primzahl. Eine* **primäre** *abelsche Gruppe ist eine abelsche p-Gruppe.*

**Lemma A.8.28** *Eine charakteristisch einfache Gruppe $G$ (also insbesondere jeder minimale Normalteiler) ist ein direktes Produkt von einfachen Gruppen $H_i$, $i \in I$, die zueinander isomorph sind. Dabei sind die die $H_i$'s zyklische Gruppen der Ordnung $p$, falls $G$ auflösbar, und nicht abelsche einfache Gruppen, falls $G$ nicht auflösbar ist.*

**Beweis:** [10] Satz 6.5

**Proposition A.8.29** *Sei $[G; \cdot, ^{-1}, 1]$ eine endliche Gruppe, $N$ eine nicht abelscher minimaler Normalteiler von $G$. Es seien $A \neq \emptyset$ endlich und $F = F(A, N)$ die Gruppe aller Funktionen von $A$ nach $N$. Sei $H \preceq F$ mit*

- *Jede konstante Funktion gehört zu $H$.*
- *$H$ trennt $A$, d.h. für jedes Paar $x, y \in A$, $x \neq y$ gibt es ein $f \in H$ : $f(x) \neq f(y)$.*
- *Für alle $f \in H$ und alle $r \in G$ gehört die Funktion $\tau_r \circ f$ zu $H$*

*Dann ist $H = F$.*

**Beweis:** [18] Kapitel 1, Proposition 12.5.

**Definition A.8.30** *Eine Gruppe $G$ heißt* **n-abelsch**, *wenn $\forall a, b \in G$ gilt $(a \cdot b)^n = a^n \cdot b^n$.*

**Definition A.8.31** *Eine Gruppe $G$ heißt* **fast n-abelsch**, *wenn gilt*

$$\forall a \in G \exists g(a) \in G \ : \ \forall b \in G \ : (a \cdot b)^n = \tau_{g(a)}(a^n \cdot b^n) = g(a) \cdot a^n \cdot b^n \cdot g(a)^{-1}$$

Man kann Gruppen durch Erzeugende und Relationen definieren (siehe auch 1.1.54), bekannte Beispiele sind:

**Definition A.8.32** *Eine Gruppe* $\mathbb{D}_n$ *heißt* **Diedergruppe it der Ordnung** $2n$**, wenn sie durch**

$$\mathbb{D}_n == \left\langle x, y; x^{2^{n-1}}, y^2, xyxy^{-1} \right\rangle$$

**gegeben ist.**

**Eine Gruppe** $\mathbb{Q}_n$ **heißt verallgemeinerte Quaternionen Gruppe**, *wenn sie durch*

$$\mathbb{Q}_n = \left\langle x, y; x^{2^{n-1}}, y^{-2}x^{2^{n-2}}, xyxy^{-1} \right\rangle$$

**Definition A.8.33** *Sei* $Y = \{y_1, y_2, \ldots, y_k\}$. *Ist* $W = \{w_j(y_{j_1}, y_{j_2}, \ldots, y_{j_{n_i}}) | i \in I\}$ *eine Menge von Wörtern in Y, G eine Gruppe,* $W(G) = \{w_j(g_1, ..., g_{n_j}) | i \in I, g_k \in G\}$. *Dann heißt die Untergruppe* $\langle W(G) \rangle$ *die von W erzeugte* **Wortuntergruppe** *von G.*

Für die Definition von freien Algebren und somit auch freien Gruppen siehe 1.1.36. Ist F eine freie Gruppe, dann sind die Wortuntergruppen von F genau die voll invarianten Untergruppen (siehe [18] 6.72.).

## A.8.2 Produkte

**Definition A.8.34** *Sei* $N \trianglelefteq G$, $H \preceq G$. *Dann heißt* $G$ **semidirektes Produkt** *von H und N, wenn gilt:* $NH = G$ *und* $N \cap H = \{1\}$. *Symbolisch:* $G = N \times_s H$

Damit folgt, daß die Darstellung $g = n \cdot h$ eindeutig ist. Denn angenommen $n_1 \cdot h_1 = n_2 \cdot h_2 \Longrightarrow n_2^{-1} n_1 = h_2 \cdot h_1^{-1}$ und somit $1 = n_2^{-1} n_1 = h_2 \cdot h_1^{-1}$.

Aus dem zweiten Isomorphismussatz folgt:

$$(N \times_s H) / N \simeq H$$

**Proposition A.8.35** *Jede periodische abelsche Gruppe ist die direkte Summe von eindeutig bestimmten primären Gruppen. Ist die Gruppe endlich, so ist sie direkte Summe ihrer Sylowgruppen.*

**Beweis:** [11] (5.1.1)

### A.8.3 Permutationsgruppen

**Proposition A.8.36** *Die Menge aller bijektiven Abbildungen einer Menge $M$ bildet bezüglich der Komposition $\circ$ eine Gruppe.*

**Beweis:** Klar.

**Definition A.8.37** *Diese Menge bezeichet man als die* **Permutationengruppe** *oder* **symmetrische Gruppe** *von $M$, $\mathbb{S}_M$ .*

Sind $X, Y$ Mengen mit $|X| = |Y|$, d.h. gibt es eine bijektive Abbildung $f : X \to Y$, so ist $\mathbb{S}_X \simeq \mathbb{S}_Y$, wobei der Isomorphismus $\sigma$ auf $f \circ \sigma \circ f^{-1}$ abbildet.

Insbesondere ist also für jede endliche Menge $\mathbb{S}_X \simeq \mathbb{S}_{\{1,2,\ldots,n\}}$, diese Menge $\mathbb{S}_{\{1,2\ldots,n\}}$ bezeichnen wir kürzer mit $\mathbb{S}_n$.

**Definition A.8.38** *Eine Permutation $\sigma$ heißt* **k-Zyklus** *, wenn es ein $k \in \mathbb{N}$ gibt, sodaß $\exists i \in X$ für das in der Menge $M = \{i, \sigma(i), \sigma^2(i), \ldots, \sigma^{k-1}(i)\}$ alle Elemente verschieden sind und für alle $s \notin M$ gilt $\sigma(s) = s$.*

*Einen 2-Zyklus nennt man* **Transposition**.

**Lemma A.8.39** *Jede Permutation $\sigma \in \mathbb{S}_n$ kann als Produkt von disjunkten Zyklen geschrieben werden. Diese kommutieren.*

*Jede Permutation $\sigma$ kann als Produkt von Transpositionen geschrieben werden. Die Anzahl dieser Transpositionen ist für festes $\sigma$ immer entweder gerade oder ungerade.*

**Beweis:** [27] Satz 3.3. , Satz 3.4.

**Definition A.8.40** *Eine Permutation $\sigma \in \mathbb{S}_n$ heißt* **gerade**, *wenn sie eine Zerlegung in eine gerade Anzahl von Transpositionen hat.*

**Definition A.8.41** *$\mathbb{A}_n$ ist die Menge aller geraden Permutationen $\subset \mathbb{S}_n$, genannt die* **alternierende Gruppe**.

**Lemma A.8.42** *Eigenschaften:*

- $\mathbb{A}_n \trianglelefteq \mathbb{S}_n$
- *$\mathbb{A}_n$ einfach und nicht abelsch für $n \geq 5$*

**Beweis:** [27] Satz 3.5., Satz 3.15

Als Verallgemeinerung können wir für beliebige Mengen $M$ $\mathbb{S}_{\mathfrak{M}}$ definieren. Zuerst bemerken wir:

**Lemma A.8.43** *Die Menge aller bijektiven Abbildungen der Menge $M$, mit $|M| = \mathfrak{M}$(eine beliebige Kardinalzahl), die fast alle Elemente von $M$ festlassen, bildet bezüglich der Komposition $\circ$ eine periodische Gruppe.*

**Beweis:** Klar.

**Definition A.8.44** *Diese Menge bezeichet man als die* **Permutationengruppe** *oder* **symmetrische Gruppe** *von $M$, $\mathbb{S}_{\mathfrak{M}}$.*

**Definition A.8.45** *$\mathbb{A}_{\mathfrak{M}}$ ist die Menge aller geraden Permutationen der Menge $M$, genannt die* **alternierende Gruppe**.

Betrachten wir nun Untergruppen $T$ der Permutationsgruppe einer Menge $X$. Dann kann man eine Äquivalenzrelation definieren: $a \sim_T b \Longleftrightarrow \exists \sigma \in \mathbb{S}_X : \sigma(a) = b$. Die zugehörige Klasseneinteilung nennt man die *Transitivitätsgebiete* von $T$. Gibt es nur eine Klasse, so nennt man $T$ transitiv:

**Definition A.8.46** *Eine Untergruppe $\mathbb{M}$ von $\mathbb{S}_X$ nennen wir* **transitiv**, *wenn es $\forall x, y \in X\ \exists \sigma \in \mathbb{M}$ mit $\sigma(x) = y$.*

*Eine Untergruppe $\mathbb{M}$ von $\mathbb{S}_X$ nennen wir* **n-fach transitiv**, *wenn es $\forall (x_1, x_2, \ldots, x_n)$ und $(y_1, y_s, \ldots, y_n) \in X^n\ \exists \sigma \in \mathbb{M}$ mit $\sigma(x_i) = y_i\ \forall i = 1, \ldots, n$. ( $x_i$ und $y_i$ sind paarweise verschieden)*

*Eine Untergruppe $\mathbb{M}$ von $\mathbb{S}_X$ nennen wir* **regulär**, *wenn sie transitiv ist und $\forall x \in X, \forall \sigma \in \mathbb{M}, \sigma \neq id_X : \sigma(x) \neq x$.*

Klarerweise ist für jede Menge $X$ die Menge aller Permutationen $\mathbb{S}_X$ $k$-fach transitiv für alle $k > 0$.

**Proposition A.8.47** Satz von Cayley *Jede Gruppe $G$ ist isomorph zu einer regulären Gruppen von Bijektionen der Menge $G$.*

**Beweis:** Die Abbildung des Elements $g \in G$ auf die Linkstranslation $\lambda_g(x) = g \cdot x$ ist klarerweise ein Isomorphismus von der Gruppe $G$ auf $\mathbb{S}_G$. □

**Definition A.8.48** *Eine transitive Untergruppe $\mathbb{M}$ von $\mathbb{S}_X$ nennen wir* **imprimitiv**, *wenn es eine Klasseneinteilung $\{K_i | i \in I\}$ gibt mit $|K_i| = |K_j|\ \forall i, j \in I$, sodaß*

$$\forall \sigma \in \mathbb{M}, \forall i \in I \exists j \in I : \sigma(K_i) = K_j$$

*Diese Klassen werden* **Imprimitivitätsgebiete** *genannt.*

*Gibt es eine solche Klasseneinteilung nicht, so nennen wir $\mathbb{M}$* **primitiv** .

D.h. ist $\mathbb{M}$ imprimitiv, so werden die Imprimitivitätsgebeite nicht „auseinander gerissen“. Daraus folgt:

**Korollar A.8.49** *Ist $\mathbb{M}$ k-fach transitiv für $k > 1$, so ist $\mathbb{M}$ primitiv.*

**Beweis:** Angenommen $\mathbb{M}$ ist imprimitiv, dann wähle $\alpha_1, \alpha_2$ in einem Imprimitivitätsgebiet, $\beta$ in einem anderen. Da $\mathbb{M}$ $k$-fach transitiv, also insbesondere 2-fach transitiv ist, gibt es ein $\sigma \in \mathbb{M}$ mit $\sigma(\alpha_1) = \alpha_1$ und $\sigma(\alpha_2) = \beta$. Widerspruch zur Definition der Imprimitivitätsgebiete. □

### A.8.4 Struktureigenschaften

**Definition A.8.50** *Eine endliche Folge*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_{r-1} \supseteq G_r$$

*heißt* **Subnormalreihe** *, wenn gilt*

- $G_{i+1} \trianglelefteq G_i$

*Die Zahl $r$ heißt die* **Länge** *der Subnormalreihe, die Faktorgruppen $G_i/G_{i+1}$ heißen* **Faktoren**. *Gilt $G_i \supset G_{i+1}$ für alle $i = 0, \ldots, r-1$, so spricht man von einer Subnormalreihe* **ohne Wiederholung**.

*Diese endliche Reihe heißt* **Normalreihe**, *wenn gilt*

- $G_i \trianglelefteq G$ *für alle* $i = 0, \ldots, r$

**Definition A.8.51** *Eine Subnormalreihe* (1) *heißt Verfeinerung einer anderen Subnormalreihe* (2), *wenn jede Gruppe in* (2) *auch in* (1) *auftritt.*

Subnormal- bzw.Normalreihen, die ohne Wiederholungen nicht verfeinert werden können, bekommen eigene Namen:

**Definition A.8.52** *Eine Subnormalreihe*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_{n-1} \supseteq G_n = \{e\}$$

*heißt* **Kompositionsreihe** *, wenn alle $G_{i+1}$ maximale normale Untergruppen von $G_r$ sind.*

*Sie heißt* **Hauptreihe**, *wenn die $G_i$ maximale, echt in $G_{i-1}$ enthaltene Normalteiler von $G$ sind. Die Faktoren werden* **Hauptfaktoren** *genannt.*

Jede Hauptreihe ist somit Normalreihe. Ist eine Kompositionsreihe Normalreihe, so ist sie klarerweise bereits Hauptreihe. Denn, angenommen es gibt ein $H \trianglelefteq G$ mit $G_i \supset H \supset G_{i+1}$, dann ist jedoch $H \trianglelefteq G_i$ Widerspruch, da $G_{i+1}$ maximaler Normalteiler von $G_i$.

Besitzt die Gruppe $G$ eine Kompositionsreihe, so besitzt sie eine Hauptreihe. (siehe [18] Anhang, Satz 6.51.)

**Lemma A.8.53** • *Eine Subnormalreihe mit $G_r = \{e\}$ ist genau dann eine Kompositionsreihe, wenn jeder nicht trivialer Faktor einfach ist.*

- *Eine Kompositionsreihe ist eine Subnormalreihe (ohne Wiederholungen) maximaler Länge.*
- *Jede endliche Gruppe hat eine Kompositionsreihe.*
- *Eine abelsche Gruppe hat genau dann eine Kompositionsreihe, wenn sie endlich ist.*
- *Besitzt eine Gruppe $G$ eine Kompositionsreihe, so läßt sich jede Subnormalreihe auf eine solche verfeinern.*

**Beweis:** [11] (2.7.4) , [27] Beispiel 6.17.

**Lemma A.8.54** • *Eine Normalreihe mit $G_r = \{e\}$ ist genau dann Hauptreihe, wenn jeder nicht trivialer Faktor charakteristisch einfach ist.*

- *Besitzt $G$ eine Hauptreihe, so läßt sich jede Normalreihe auf eine solche verfeinern. (Also gibt es für jeden Normalteiler $N \trianglelefteq G$ eine Hauptreihe von $G$, in der $N$ als Glied auftritt.)*
- *Besitzt $G$ eine Hauptreihe, so ist $Epi(G,G) = Aut(G)$, und für alle $N \lhd G$ gilt $N \not\cong G$.*
- *Eine Normalreihe mit $G_r = \{e\}$ ist genau dann eine Hauptreihe, wenn für alle $i$ der Faktor $G_{i-1}/G_i$ minimaler Normalteiler von $G/G_i$ ist.*

**Beweis:** [11] (2.7.6)

**Definition A.8.55** *Für zwei Normalteiler $H \supset K \trianglelefteq G$ nennt man den Faktor $H/K$ Hauptfaktor, wenn $H/K$ minimaler Normalteiler von $G/K$ ist.*

**Definition A.8.56** *Zwei Subnormalreihen heißen* **äquivalent**, *wenn es eine bijektive Abbildung zwischen den Faktoren gibt, sodaß die entsprechenden Faktorgruppen isomorph sind.*

Insbesondere haben äquivalente Subnormalreihen gleiche Länge.

**Proposition A.8.57** Jordan-Hölder *Je zwei Kompositionsreihen ohne Wiederholungen sind äquivalent.*

**Beweis:** [27] Satz 6.10.

Ebenso sind je zwei Hauptreihen ohne Wiederholungen äquivalent.

**Definition A.8.58** *Eine Gruppe heißt* **auflösbar** *, wenn sie eine Subnormalreihe mit abelschen Faktoren besitzt, für die ein $r$ existiert, sodaß $G_r = \{e\}$. Diese wird dann eine* **auflösbare Reihe** *genannt.*

**Beispiel:** $GL(k, p^t)$ ist genau dann auflösbar, wenn $k = 1$ oder $k = 2$ und $p^t = 2$ oder 3.

Jede endliche Gruppe hat eine Kompositionsreihe und es gilt

**Lemma A.8.59** *Eine endliche Gruppe ist genau dann auflösbar, wenn sie eine Kompositionsreihe mit zyklischen Faktoren von Primzahlordnung besitzt.*

**Beweis:** [11] (2.8.2)
Gibt es so eine Kompositionsreihe, die Normalreihe ist, so definieren wir:

**Definition A.8.60** *Eine Gruppe heißt* **überauflösbar**, *wenn sie eine Hauptreihe mit zyklischen Faktoren besitzt und ein $r$ existiert, sodaß $G_r = \{e\}$.*

Jede überauflösbare Gruppe ist klarerweise auflösbar.

**Proposition A.8.61** *Sei $G$ eine Gruppe. Ist $G$ (über-)auflösbar, so ist jede Untergruppe $H \preceq G$ (über-)auflösbar, ist $N \trianglelefteq G$, so ist $G/N$ (über-)auflösbar.*
*Gibt es einen Normalteiler $N \trianglelefteq G$ und sind sowohl $N$ als auch $G/N$ auflösbar, so ist $G$ auflösbar.*

**Beweis:** [11] (2.8.3) und (9.4.1) sowie [27] Satz 6.11 und Satz 6.12

**Satz A.8.62** (Feit und Thompson) *Jede endliche Gruppe ungerader Ordnung ist auflösbar.*

**Beweis:** [11] (2.8.1)
Weitere Zusammenhänge zwischen Auflösbarkeit und Gruppenordnung sind

**Lemma A.8.63**

- *Jede endliche $p$-Gruppe ist auflösbar, $p$ eine Primzahl*
- *Jede endliche $(p,q)$-Gruppe ist auflösbar, $p, q$ Primzahlen.*
- *Jede endliche Gruppe mit quadratfreier Ordnung ist auflösbar.*

**Beweis:** [27] Beispiele 6.26., Korollar 6.15 und [11] (3.4.4)

**Proposition A.8.64** *Sind $H$ und $K$ auflösbare Gruppen, so ist $H \times K$ auflösbar.*
*Sind $H, K \preceq G$ auflösbar, so ist $H \cdot K$ auflösbar.*

**Beweis:** [27] Korollar 6.14 und Beispiel 6.23

**Lemma A.8.65** *Jede minimaler Normalteiler $N$ einer endlichen auflösbaren Gruppe $G$ ist eine elementar abelsche Gruppe.*

**Beweis:** [27] Lemma 6.19
Die auflösbaren, einfachen Gruppen sind die $\mathbb{Z}_p$ für $p$ prim.

**Definition A.8.66** *Es sei $G$ eine Gruppe, die* **Kommutatoruntergruppe** *$G'$ ist definiert durch*

$$G' = \left\langle a \cdot b \cdot a^{-1} \cdot b^{-1} \,|a, b \in G \right\rangle$$

*Für zwei Untergruppen $H, K \preceq G$ sei*

$$[H, K] = \left\langle h \cdot k \cdot h^{-1} \cdot k^{-1} \,|h \in H, k \in K \right\rangle$$

Also ist $G' = [G, G]$.
Die Kommutatoruntergruppe hat die Eigenschaften

**Lemma A.8.67**

- $G' \trianglelefteq G$
- *Ist $N \trianglelefteq G$, so ist $G/N$ genau dann abelsch, wenn $G' \subseteq N$.*

**Beweis:** [15] Kapitel 1, Lemma 8.3.

**Definition A.8.68** *Es sei $G$ eine Gruppe. Die* **höheren Kommutatorgruppen** *werden induktiv definiert:*

$$G^{(0)} = G;\ G^{(i+1)} = G^{(i)'};$$

*Die Folge*

$$G = G^{(0)} \supseteq G^{(1)} \supset \ldots \supset G^{(i)} \supset \ldots$$

*nennen wir die* **derivierte Reihe** *von $G$.*

**Satz A.8.69** *Eine Gruppe $G$ ist genau dann auflösbar, wenn es ein $n \in \mathbb{N}$ gibt, sodaß $G^{(n)} = \{e\}$.*

**Beweis:** [15] Kapitel 1, Satz 8.4.

**Definition A.8.70** *Eine Gruppe $G$ heißt* **halbeinfach**, *wenn sie keinen nicht trivialen auflösbaren Normalteiler hat, i.e.*

$$\forall N \trianglelefteq G : N \neq \{e\} : N \text{ ist nicht auflösbar .}$$

*Eine Gruppe heißt* **vollständig reduzibel**, *wenn sie das direkte Produkt einfacher Gruppen ist.*

**Definition A.8.71** *Setzt man in einer beliebigen Gruppe $G$*

$$Z^0(G) = \{1\}$$

$$Z^1(G) = Z(G) \text{ das Zentrum von } G$$

*und definiert man allgemein $Z^i(G)$ durch*

$$Z^i(G)/Z^{i-1}(G) = Z(G/Z^{i-1}(G))$$

*so erhält man die* **aufsteigende Zentralfolge**

$$\{1\} = Z^0(G) \subseteq Z^1(G) \subseteq Z^2(G) \subseteq \ldots$$

**Definition A.8.72** *Eine Gruppe $G$ heißt* **nilpotent der Klasse c** *, wenn die aufsteigende Zentralfolge nach $c$ Schritten bis zur ganzen Gruppe $G$ aufsteigt, also*

$$\{1\} = Z^0(G) \subset Z^1(G) \subset Z^2(G) \subset \ldots \subset Z^{c-1}(G) \subset Z^c(G) = G$$

*Diese Reihe heißt dann die* **aufsteigende Zentralreihe** *von $G$. Ist $G$ nilpotent so bezeichne $c(G)$ die Klasse von $G$.*

**Definition A.8.73** *Eine endliche Reihe*

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_{n-1} \subseteq G_n = G$$

*heißt* **Zentralreihe** *, wenn*

- $G_i \trianglelefteq G$
- $G_i/G_{i-1} \subseteq Z(G/G_{i-1})$

Nilpotente Gruppen der Klasse $\leq c$ bestimmen eine Varietät, da die definierende Bedingung auch als Gesetz formuliert werden kann. Z.B. erfüllen nilpotente Gruppen der Klasse $\leq 2$ das Gesetz $aba^{-1}b^{-1}cbab^{-1}a^{-1}c^{-1} = e$.

**Proposition A.8.74** *$G$ ist genau dann nilpotent, wenn $G$ eine endliche Zentralreihe besitzt. Ist $G$ nilpotent der Klasse $c$, so hat jede Zentralreihe mindestens die Länge $c$.*

**Beweis:** [11] (9.2.1)

Damit ist klar, daß jede nilpotente Gruppe auflösbar ist. Es gibt aber Gruppen (z.B. $\mathbb{S}_3$) die auflösbar, aber nicht nilpotent sind.

**Proposition A.8.75** *Eine endliche Gruppe ist genau dann nilpotent, wenn sie direktes Produkt ihrer Sylowgruppen ist.*

**Beweis:** [11] (9.2.3)

**Definition A.8.76** *Setzt man in einer beliebigen Gruppe $G$*

$$Z_0(G) = G$$

$$Z_1(G) = [Z(G), G]$$

*und definiert man induktiv durch*

$$Z_i(G) = [Z_{i-1}(G), G]$$

*so erhält man die* **absteigende Zentralfolge**

$$G \supseteq Z_1(G) \supseteq Z_2(G) \supseteq \ldots$$

**Lemma A.8.77** *Es sei $G$ eine Gruppe. Bricht die absteigende Zentralreihe ab, so ist $G$ nilpotent.*

*Ist $G$ nilpotent, so haben die aufsteigende und die absteigende Zentralreihe die selbe Länge.*

**Beweis:** [11] (9.2.4)

**Lemma A.8.78** *Jede Untergruppe und jede Faktorgruppe einer nilpotenten Gruppe sind nilpotent der Klasse $c'$, wobei $c' \leq c(G)$*

**Beweis:** [11] (9.2.5)

**Satz A.8.79** Levi *Es sei $G$ eine Gruppe. Gilt*

$$ab^{-1}ab = b^{-1}aba \ \forall a, b \in G$$

*dann ist $G$ nilpotent der Klasse $\leq 3$. Hat $G$ kein Element der Ordnung 3, dann ist $G$ nilpotent der Klasse $\leq 2$.*

**Beweis:** siehe [18] Anhang, Satz 6.53

# Literaturverzeichnis


[1] E. Aichinger, *Interpolation with Near-Rings of Polynomial Functions*, Diplomarbeit Linz (1994)

[2] P.M. Cohn, *Universal Algebra*, Harper & Row, London (1965)

[3] D. Dorninger, W. Nöbauer, *Local polynomial functions on lattices and universal algebras*, Colloquium Mathematicum XLII (1979), 83-93

[4] A. Fröhlich, *The near - ring generated by the inner automorphisms of a finite simple group*, J. London Math. Soc. 33 (1958), 95-107

[5] S. Grosser, Vorlesungsskriptum *Algebra I*, Wien (1992)

[6] S. Grosser, Vorlesungsskriptum *Algebra II*, Wien (1993)

[7] H.Hule, *Polynomial normal forms and the embedding of polynomial algebras*, Colloquia Mathematica Societatis János Bolyai - 17. Contributions to Universal Algebra, North Holland, Amsterdam (1977), 179 - 187

[8] H. Hule, *Polynome über universalen Algebren*, Monatshefte für Mathematik 73 (1969), 329 - 340

[9] H. Kaiser, *Vollständigkeit in universalen Algebren*, Dissertation Wien (1972)

[10] H. Kurzweil, *Endliche Gruppen*, Springer, Berlin (1977)

[11] R. Kochendörfer, *Lehrbuch der Gruppentheorie unter besonderer Berücksichtigung der endlichen Gruppen*, Geest & Portig, Leipzig (1966)

[12] G.Kowol, *Polynomautomorphismen von Gruppen*, Arch. Math., Vol. 57 (1991), 114 - 121

[13] G.Kowol, *Near-Rings of Endomorphisms of Finite Groups*, Communications in Algebra, 25(7) (1997), 2333-2342

[14] G.Kowol, *Fast-n-abelsche Gruppen*, Arch. Math. Vol. XXIX (1977), 55 - 66

[15] G. Kowol, H. Mitsch, *Algebra I*, Prugg Verlag, Eisenstadt (1982)

[16] G.Kowol, H. Mitsch, *Polynomial Functions over Commutative Semi-Groups*, Semigroup Forum Vol. 12 (1976), 109-118

[17] H. Lausch, *Eine Charakterisierung nilpotenter Gruppen der Klasse 2*, Math. Zeitschr. 93 (1966), 206 - 209

[18] H. Lausch, W. Nöbauer, *Algebra of Polynomials*, North-Holland Publishing, London (1973)

[19] H. Lausch, W. Nöbauer, F. Schweiger, *Polynompermutationen auf Gruppen*, Monatshefte für Mathematik 69 (1965), 410 - 423

[20] H. Lausch, W. Nöbauer, F. Schweiger, *Polynompermutationen auf Gruppen II*, Monatshefte für Mathematik 70 (1966), 118 - 126

[21] J.D.P. Meldrum, *Near-Rings - A Non-Linear Tool For Groups*, General Algebra 1988, North - Holand, Amsterdam (1990), 199 - 212

[22] H. Mitsch, *Über Polynome und Polynomfunktionen auf Verbänden*, Monatshefte für Mathematik 74 (1970), 239 - 243

[23] H.Mitsch, *Lineare Algebra und Geometrie I*, Prugg Verlag Eisenstadt (1978)

[24] R. Mlitz, *Wilfried Nöbauer - A Life for Algebra of Polynomials*, General Algebra 1988, North - Holand, Amsterdam (1990) 13 - 22

[25] W. Nöbauer, *Die Operation des Einsetzens bei Polynomen in mehreren Unbestimmten*, J. Reine Angew. Math 201 (1959) , 207 - 220

[26] W. Nöbauer, *Mehrdimensionale Polynompermutationen auf endlichen Gruppen*, Monatsh. Math. 71 (1967), 148 - 155

[27] J.J. Rotman, *The Theory of Groups*, Allyn and Bacon, Boston (1965)

[28] F. Schuhmacher, *Über die Polynompermutationen der endlichen Gruppen*, Dissertation Wien (1970)

[29] S. D. Scott, *The Arithmetic of Polynomial Maps over a Group and the Structure of Certain Permutational Polynomial Groups. I*, Monatshefte für Mathematik 73 (1969), 250 - 267

[30] H. Schoißengeier, Vorlesungskriptum *Algebra II*, Wien (1998)

[31] H.F. Trotter,*Groups in which raising to a power is an automorphism*, Canadian Mathematical Bulletin 8 (1965), 825 - 827

[32] J.Wiesenbauer, *On the Polynomial Completeness Defect of Universal Algebras*, Colloquia Mathematica Societatis János Bolyai - 17. Contributions to Universal Algebra, North Holland, Amsterdam (1977), 577 - 579