Jürgen Ecker

Functions On Finite Groups. Compatibility vs. Polynomiality

Kompatible und Polynomfunktionen auf endlichen Gruppen

Dissertation zur Erlangung des akademischen Grades
eines Doktors der Technischen Wissenschaften

vorgelegt von
Dipl. Ing. Jürgen Ecker

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

bei
O. Univ.–Prof. Dr. Günter Pilz

Linz, den 16. 1. 2001

Contents

List of Figures

List of Tables

Vorwort

Mit der ganzen Algebra ist man oftmals nur ein Narr,
wenn man nicht noch etwas anderes weiß.

Friedrich, der Große

Friedrich der Große war offensichtlich kein leidenschaftlicher Anhänger der Algebra. Nachdem Sie bereits das Inhaltsverzeichnis dieser Arbeit überstanden haben, dürften Sie sich wesentlich von diesem Herrn unterscheiden. Und da Sie bestimmt noch vieles andere wissen, können Sie sich jetzt gleich noch tiefer in die Algebra stürzen, ohne fürchten zu müssen, als Narr zu gelten.

Ende der sechziger Jahre begann man, das überaus erfolgreiche Konzept der Polynome und Polynomfunktionen, welches bis dahin vorwiegend im Bereich der Körper und Ringe verwendet wurde, auf universelle Algebren zu übertragen. 1973 publizierten Hans Lausch und Winfried Nöbauer ein umfangreiches Werk zu diesem Themenkreis. Seitdem gelang es, die Polynomfunktionen auf den meisten bekannten Klassen von Gruppen zu beschreiben, eine einheitliche Methode für alle Gruppen scheint jedoch weniger denn je in Sicht.

Gleichfalls 1973 erschien ein Artikel von Stuart D. Scott, der von der sogenannten Länge einer Gruppe handelt. Diese Zahl stellt sich als die wesentliche Größe bei der Bestimmung der Polynomfunktionen auf Gruppen der Nilpotenzklasse 2 heraus.

Mitte der siebziger Jahre begannen Lausch und Nöbauer die sogenannten kompatiblen Funktionen auf Gruppen zu untersuchen. Insbesondere erweisen sich Polynomfunktionen stets als kompatibel. 1976 erschien eine Beschreibung der kompatiblen Funktionen auf endlichen abelschen Gruppen. Dieser Aufsatz enthält auch eine Charakterisierung derjenigen abelschen Gruppen, auf denen es außer den Polynomfunktionen keine kompatiblen Funktionen gibt, die sogenannten 1-affinvollständigen abelschen Gruppen.

Für Gruppen der Nilpotenzklasse 2 wurde die 1-Affinvollstängigkeit von Marianne Dorda in ihrer Dissertation aus dem Jahr 1977 weitgehend untersucht. Sie zeigte, dass 1-affinvollständige p-Gruppen der Nilpotenzklasse 2 zumindest von der Ordnung p^6 sein müssen, falls $p > 2$ ist.Schließlich konstruierte sie ein Beispiel einer 1-affinvollstädigen Gruppe der Ordnung p^6 und Nilpotenzklasse 2.

Scott's Arbeit über die Länge einer Gruppe zielt nicht primär auf eine algorithmische Lösung ab. Im Kapitel 1 entwickeln wir einen Algorithmus zur Bestimmung der Länge einer Gruppe der Nilpotenzklasse 2, und damit zur Bestimmung aller Polynomfunktionen auf einer derartigen Gruppe.

Mit den von Lausch, Nöbauer und Dorda entwickelten Methoden ist es u.a. möglich, die kompatiblen Funktionen auf Gruppen zu bestimmen, die einen einzigen nichttrivialen minimalen Normalteiler besitzen. Im Kapitel 2 werden diese Methoden verallgemeinert für den Fall, dass die Gruppe zumindest einen distributiven minimalen nichttrivialen Normalteiler besitzt. Darüberhinaus studieren wir in diesem Kapitel gewisse direkte Produkte von Gruppen.

Im Kapitel 3 werden die Resultate, die seit 1970 über Polynomfunktionen auf Gruppen erschienen sind, mit den Ergebnissen aus Kapitel 2 verknüpft. Dabei tauchen neue Klassen 1-affinvollständiger Gruppen auf. Schließlich wird in diesem Kapitel der Zusammenhang zwischen 1-Affinvollstädigkeit und direkten Produkten bzw. der Bildung von Quotienten untersucht.

Viele der Ergebnisse dieser Kapitel haben Konsequenzen im Bereich der rechnerischen Gruppen- und Fastringtheorie. Algorithmen zur Bestimmung von kompatiblen und Polynomfunktionen auf endlichen Gruppen wurden mit Hilfe des Computeralgebrasystems GAP[1] und des Pakets SONATA[2] implementiert. In Kapitel 5 finden sich Vergleiche zwischen verschiedenen Algorithmen, insbesondere auch Vergleiche mit früher angewandten Methoden.

Nähere Informationen zur verwendeten Software finden sich in GAP [1999]; Aichinger *et al.* [1997a,b, 1998].

[1] GAP, **G**roups, **A**lgorithms, **P**rograming, GAP [1999].

[2] SONATA, a **S**ystem **O**f **N**earrings **A**nd **T**heir **A**pplications, ist ein Paket zu GAP4 für Fastringe, entwickelt an der Abteilung für Algebra and der Johannes Kepler Universität Linz.

Preface

In the late sixties the concept of polynomials and polynomial functions – mainly used in the context of fields up to then – has been transfered to arbitrary algebras. In 1973, Hans Lausch and Winfried Nöbauer published an extensive work on such polynomials. Since then, most of the well-known classes of groups have been treated, but a theory for all groups still seems to be out of reach if not impossible.

Also in 1973 Stuart D. Scott published a paper on what he called the length of a group. It turns out that for nilpotent groups of class 2 the length contains the information needed to describe, enumerate and count polynomial functions on such groups.

In the mid-seventies, Lausch and Nöbauer began investigating so called compatible functions on groups. Compatibility is a property, which polynomial functions always have. In 1976, a description of the compatible functions on finite abelian groups was published, including a characterization of those finite abelian groups forcing compatible functions to be polynomial, so called 1-affine complete finite abelian groups.

In her thesis in 1977, Marianne Dorda treated 1-affine complete class 2 nilpotent p-groups, and showed that such groups have to have order at least p^6, if $p > 2$, and gave an example of such a group.

Since then, not much has been published in the field of 1-affine complete groups.

Scott's work on the length of a group was not really intended to lead to an algorithmic computation of the length. In Chapter 1, an algorithm for the computation of the length of a given nilpotent group of class 2 is developed.

With the methods found by Lausch, Nöbauer, and Dorda, it is possible to determine the compatible functions on groups, which have a unique minimal normal subgroup. In Chapter 2 we generalize this result to the case, where the group possesses a distributive minimal normal subgroup. Moreover, certain direct products of groups are treated.

In Chapter 3, the results on polynomial functions published since 1970 are combined with the results of Chapter 2, and new classes of 1-affine complete groups turn up. The connection between 1-affine completeness and building quotients and direct products of groups is studied.

Many of the results of these three chapters have consequences in the area of computational group and near ring theory. Algorithms for the computation of polynomial and compatible functions on arbitrary finite groups have been implemented using the computer algebra system GAP[3] together with the package SONATA[4]. Chapter 5 lists a few benchmarks of these algorithms and compares them to previously used algorithms.

Descriptions of the software used for the computational part of this thesis can be found in GAP [1999]; Aichinger *et al.* [1997a,b, 1998].

[3]GAP, **G**roups, **A**lgorithms, **P**rograming, GAP [1999].

[4]SONATA, a **S**ystem **O**f **N**earrings **A**nd **T**heir **A**pplications, is a GAP4 package for near rings, developed at the Algebra Department of the Johannes Kepler University, Linz.

Credits

I am indebted to Prof. Günter Pilz for his support, supervision and encouragement of the work on this thesis, and Prof. J.D.P. Meldrum for his ideas for Chapter 1. Many stimulating ideas for Chapter 2 are due to Prof. W. Kaiser.

I am much obliged to my colleagues at the department of algebra, Peter Mayr for his help with fixed point free automorphisms, which appear in Chapter 2, Franz Binder, who came up with the idea for Chapter 4, for being a never dwindling source of inspiration, and Erhard Aichinger, who helped with polynomial functions in Chapter 1 and whose programs for the computation of compatible functions were the toughest to compete with. Thanks to all of them for studiously preparing the foundations of our work, coffee and tea.

The authors of the computer algebra system GAP have produced a wonderful basis for the implementation of my results. Thomas Breuer, Alexander Hulpke, and Andrew Solomon – among others – have been very forthcoming, whenever technical help or even little changes of GAP were necessary.

Parts of this work were financed by the Austrian "Fond zur Förderung wissenschaftlicher Forschung" in the form of the projects "Computing with Near-Rings – Algorithms and Implementation" (P11486-TEC) and "Berechnungen mit Fastringen" (P12911-INF). The results have appeared in Ecker [1998]; Aichinger *et al.* [2000a,b,c].

CHAPTER 0

Preliminaries

Convention: *All the groups we are treating in this dissertation are finite. All groups are written additively, even if they are not abelian. Groups are displayed in bold face, their underlying sets are represented by uppercase roman letters. If* $\mathbf{G}$ *denotes a group,* G *denotes its underlying set, and vice versa.*

0.1. NOTATION. The set of integers will be indicated by $\mathbb{Z}$, the set of positive integers by $\mathbb{N}$, and the set of prime numbers by $\mathbb{P}$.

0.2. NOTATION. For the cyclic group of order n we write $\mathbb{Z}_n$. Moreover, $\mathbb{Z}_q^*$ denotes the multiplicative group of the finite field $\mathrm{GF}(q)$ (,where q is a prime power).

0.3. NOTATION. A description of all groups of order at most 32 (up to isomorphism) can be found in Thomas and Wood [1980]. The authors identify groups with pairs of integers, one being the size of the group. When talking about small groups we will occasionally use the notation in this book.

0.4. DEFINITION. Let $\mathbf{G}$ be a group. For elements $a, b \in G$ we call $[a, b] := -a - b + a + b$ the **commutator** of a and b. For two subgroups $\mathbf{H}_1$ and $\mathbf{H}_2$ of $\mathbf{G}$, we write $[\mathbf{H}_1, \mathbf{H}_2]$ for the subgroup generated by all $[h_1, h_2]$, where $h_1 \in H_1$ and $h_2 \in H_2$.

0.5. DEFINITION. Let $\mathrm{K}_i(\mathbf{G})$ be defined recursively in the following way: $\mathrm{K}_1(\mathbf{G}) := \mathbf{G}$ and $\mathrm{K}_i(\mathbf{G}) := [\mathrm{K}_{i-1}(\mathbf{G}), \mathbf{G}]$ for $i \geq 2$. If there is a natural number r, s.t. $\mathrm{K}_r(\mathbf{G}) = \{0\}$ then $\mathbf{G}$ is called **nilpotent** . If r is the smallest such number then $r - 1$ is called the **nilpotency class** of $\mathbf{G}$. Usually we write $\mathbf{G}'$ for $\mathrm{K}_2(\mathbf{G})$. The subgroup $\mathbf{G}'$ is often called the **derived subgroup** (or **commutator subgroup**) of $\mathbf{G}$.

0.6. NOTATION. Let $\mathbf{G}$ be a group, $g \in G$, $S \subseteq G$. Throughout this section, we write $\langle g \rangle$ for the subgroup of $\mathbf{G}$ generated by g and $\langle S \rangle$ for the subgroup of $\mathbf{G}$ generated by S. We write $[g]$ for the normal subgroup of $\mathbf{G}$ generated by g and $[S]$ for the normal subgroup of $\mathbf{G}$ generated by S.

0.7. NOTATION. We write group presentations in the following way:

$$\langle x_1, \dots, x_n; s_1, \dots, s_m \rangle,$$

where $x_1, \dots, x_n$ are generators, $s_1, \dots, s_m$ are words in $\{x_1, \dots, x_n\} \cup \{-x_1, \dots, -x_n\}$, and s_i stands for the generating relation $s_i = 0$.

0.8. NOTATION. Let $\mathbf{N}$ and $\mathbf{H}$ be two groups, and let α be a homomorphism from $\mathbf{H}$ into the group of automorphisms of $\mathbf{N}$. Defining

$$(n_1, h_1) +_\alpha (n_2, h_2) := (\alpha(h_2)(n_1) + n_2, h_1 + h_2),$$

for $n_1, n_2 \in N$ and $h_1, h_2 \in H$, $(N \times H, +_\alpha)$ turns out to be a group, the **semi-direct product** of $\mathbf{N}$ by $\mathbf{H}$ w.r.t. α, denoted by $\mathbf{N} \rtimes_\alpha \mathbf{H}$. For subsets $R \subseteq N$ and $S \subseteq H$, let (R, h) denote the set $\{(r, h) \mid r \in R\}$. Analogously we use the notations (n, S) and (R, S).

0.9. NOTATION. Let $\mathbf{G}$ be a group. Then $\mathrm{Z}(\mathbf{G})$ denotes the **center** of $\mathbf{G}$.

0.10. DEFINITION. For a group $\mathbf{G}$, let G^G denote the set of all functions from G to G. On G^G we define

$$(\varphi + \psi)(x) := \varphi(x) + \psi(x)$$

and

$$(\varphi \circ \psi)(x) := \varphi(\psi(x))$$

and note that $\mathbf{M}(\mathbf{G}) = (G^G, +, \circ)$ is a near ring[1]. All near rings we will consider are sub-near rings of such a near ring $\mathbf{M}(\mathbf{G})$.

0.11. REMARK. By the third isomorphism theorem [Robinson, 1996, 1.4.4], for a group $\mathbf{G}$ and $\mathbf{N} \trianglelefteq \mathbf{G}$, the natural epimorphism $\eta : \mathbf{G} \to \mathbf{G}/\mathbf{N}$, $g \mapsto g + \mathbf{N}$ induces a 1-to-1-correspondence between the normal subgroups of $\mathbf{G}$ containing $\mathbf{N}$ and the normal subgroups of $\mathbf{G}/\mathbf{N}$. Moreover η preserves inclusion in the lattices and for all $\mathbf{N} \leq \mathbf{I} \leq \mathbf{J} \leq \mathbf{G}$, $\mathbf{J}/\mathbf{I} \cong (\mathbf{J}/\mathbf{N})/(\mathbf{I}/\mathbf{N})$. The lattice of normal subgroups of a quotient $\mathbf{G}/\mathbf{N}$ can be derived from the lattice of normal subgroups of $\mathbf{G}$ simply by throwing away all normal subgroups not containing $\mathbf{N}$.

When studying compatible and polynomial functions on direct products of groups in the following chapters, we will ask, under which circumstances every pair of polynomial/compatible functions on two groups can be combined to a polynomial/compatible function on their direct product. In both cases we will prove that the necessary and sufficient condition is that every normal subgroup of the direct

[1] c.f. Pilz [1983]

product $\mathbf{G} \times \mathbf{H}$ is **G-H–decomposable**[2], i.e., it is a direct product of a normal subgroup of $\mathbf{G}$ and a normal subgroup of $\mathbf{H}$. The following theorem characterizes such direct products.

0.12. DEFINITION. We call a group $\mathbf{G}$ **super-perfect** iff

$$\forall \mathbf{N} \trianglelefteq \mathbf{G} \ : \ [\mathbf{G}, \mathbf{N}] = \mathbf{N}.$$

0.13. THEOREM ([Miller, 1975, Theorem 1]). *Every normal subgroup of the direct product of the groups* $\mathbf{G}$ *and* $\mathbf{H}$ *is* $\mathbf{G}$-$\mathbf{H}$*–decomposable* $\iff$

1. *at least one of* $\mathbf{G}$ *and* $\mathbf{H}$ *is super-perfect, or*
2. *for all* $\mathbf{M} \trianglelefteq \mathbf{G}$, $\mathbf{N} \trianglelefteq \mathbf{H}$, *the elements of* $\mathbf{M}/[\mathbf{G}, \mathbf{M}]$ *have order relatively prime to those of* $\mathbf{N}/[\mathbf{H}, \mathbf{N}]$.

0.14. NOTATION. For $\mathbf{I}, \mathbf{J} \trianglelefteq \mathbf{G}$, we write $\mathbf{I} \prec \mathbf{J}$ iff $\mathbf{I} < \mathbf{J}$, and for all $\mathbf{K} \trianglelefteq \mathbf{G}$, if $\mathbf{K} < \mathbf{J}$, then $\mathbf{I} \not\leq \mathbf{K}$.

[2] In Pilz [1980] and Nöbauer [1976] direct products of groups satisfying this condition are called **free of skew congruences**.

CHAPTER 1

Polynomial functions on groups

1. Introduction

1.1. Definition. Let $\mathbf{G}$ be a group. The **near ring of polynomial functions on $\mathbf{G}$**, $\mathbf{P}(\mathbf{G})$, is the sub-near ring of $\mathbf{M}(\mathbf{G})$ generated by the inner automorphisms and the constant functions on $\mathbf{G}$.

1.2. Lemma. *The near ring $\mathbf{P}(\mathbf{G})$ is also generated additively by the identity function and the constant functions on G.*

Proof. For every $g \in G$, the inner automorphism $x \mapsto -g + x + g$ is the sum of the constant function $x \mapsto -g$, the identity function, and the constant function $x \mapsto g$. Conversely, the identity function is the inner automorphism induced by $0 \in G$. □

Following Scott [1969], we make the following definition.

1.3. Definition. By a **polynomial** p over a group $\mathbf{G}$ we mean an element of the free product of $\mathbf{G}$ and the free group generated by $\{x\}$.[1] Every polynomial p over $\mathbf{G}$ **induces** a function $\bar{p}$ from G to G, mapping g to $p(g)$, where $p(g)$ is the element of $\mathbf{G}$ obtained when replacing every x in p by g. We call p a **term representation** of $\bar{p}$.

1.4. Remark. If $c \in \mathbf{G}$, the polynomial c induces the constant function $x \mapsto c$. The polynomial x induces the identity function on $\mathbf{G}$.

1.5. Remark. If $\mathbf{A}$ is an abelian group, then every polynomial function on $\mathbf{A}$ is induced by a polynomial of the form $kx+d$, where $k \in \{1, \dots, \exp \mathbf{A}\}$ and $d \in A$. Hence there are precisely

$$|\mathbf{P}(\mathbf{A})| = |\mathbf{A}| \cdot \exp \mathbf{A}$$

different polynomial functions on $\mathbf{A}$.

[1] The general definitions of a polynomial and a polynomial function over an algebra can be found in Lausch and Nöbauer [1973].

2. Nilpotent groups of class 2

In the case of a nilpotent group of class 2 a certain invariant of the group, the length defined by S. D. Scott, can be used to determine the number of polynomial functions on the group. We will determine sharp upper and lower bounds for this invariant. It is shown how the length of a group can be determined from a set of generating elements and the length of all p-groups up to order p^4 is determined as an application.

2.1. Introduction.

1.6. Lemma (Huppert [1967]). *For a nilpotent group* $\mathbf{G}$ *of class 2, the commutator operation is "bilinear" and "alternating", precisely, for all* $a, b, c \in G$, $k \in \mathbb{Z}$

$$\begin{aligned} [a, b + c] &= [a, b] + [a, c] \\ [a + b, c] &= [a, c] + [b, c] \\ [ka, b] &= [a, kb] = k[a, b] \\ [a, b] &= -[b, a] \end{aligned}$$

We deal with polynomial functions on nilpotent groups of class 2, which will be described in the next theorem.

1.7. Proposition. *If* $\mathbf{G}$ *is nilpotent of class 2, then every polynomial function* $\bar{p}$ *on* $\mathbf{G}$ *can be written in the form*

$$x \to g + kx + [x, h] \tag{1.1}$$

for some $g, h \in G$, $k \in \mathbb{N}$.

Proof. Say $\bar{p}$ is induced by a polynomial p of the form

$$p = g_0 + x + g_1 + x + \cdots + x + g_l.$$

Now swapping the g_i to the left using the rule $a + b = b + a + [a, b]$ and transferring the appearing commutators to the right (they are all in the center of $\mathbf{G}$) we get

$$p = \sum_{i=0}^{l} g_i + lx + \sum_{i=1}^{l} [x, \sum_{j=i}^{l} g_j],$$

which we can simplify to

$$p = \sum_{i=0}^{l} g_i + lx + [x, \sum_{i=1}^{l} i g_i].$$

□

This gives rise to a formula for the number of polynomial functions on a nilpotent group of class 2. We ask, when a polynomial $z = g + kx + [x, h]$ induces the zero function. Clearly, if $g \neq 0$ then $\bar{z}(0) = g \neq 0$, so g has to be equal to zero. Of course, $\exp \mathbf{G} \cdot x = [x, 0]$ for all $x \in G$. So there exists a smallest positive integer k such that there exists an element $\pi \in G$ with

$$kx = [x, \pi] \quad \forall x \in G. \tag{1.2}$$

This number k is known as the length of $\mathbf{G}$, which we define in the next section, before we write down the formula for the size of $\mathbf{P}(\mathbf{G})$.

2.2. Scott's lambda.

1.8. Definition (c.f. Scott [1969]). The **length** of the polynomial

$$p = g_0 + z_1 x + g_1 + z_2 x + \cdots + z_r x + g_r,$$

where $z_i \in \mathbb{Z}$, $g_i \in G$ and $\mathbf{G}$ is a group, is defined as $l(p) := \sum_{i=1}^{r} z_i$. The polynomial p is an **annihilating polynomial** of $\mathbf{G}$, iff the polynomial function induced by p is the zero function. A polynomial of minimal positive length among the annihilating polynomials is called a **minimum polynomial**, $\lambda(\mathbf{G})$ denotes its length which we call the **length** of $\mathbf{G}$. Furthermore, we define the **length** of a polynomial function as the minimal positive length of a polynomial inducing this function.

The smallest positive integer k satisfying (1.2) for some $\pi \in G$ is obviously the length of the group. Using λ we can write the formula

$$|\mathbf{P}(\mathbf{G})| = |\mathbf{G}| \cdot \lambda(\mathbf{G}) \cdot [\mathbf{G} : \mathrm{Z}(\mathbf{G})]. \tag{1.3}$$

The following results for the length of a group are taken from Scott [1969]:

1.9. Proposition ([Scott, 1969, Proposition 1.1]). *Let* $\mathbf{G}$ *be a nilpotent group of class 2. Then*

$$\lambda(\mathbf{G}) | \exp \mathbf{G}$$

Proof. In Proposition 1.1 of Scott [1969], we choose $R(x) = (\exp \mathbf{G})x$. □

1.10. Theorem ([Scott, 1969, Theorem 2.1]). *Let* $\mathbf{G}$ *and* $\mathbf{H}$ *be groups. Then*

$$\lambda(\mathbf{G} \times \mathbf{H}) = \mathrm{lcm}(\lambda(\mathbf{G}), \lambda(\mathbf{H})) \tag{1.4}$$

As every nilpotent group is the direct product of its p-Sylow subgroups, its length is the product of the lengths of its p-Sylow subgroups, and its center is the direct product of the centers of its p-Sylow subgroups, we can restrict ourselves to the case of a nilpotent p-group of class ≤ 2.

2.3. Bounds for $\lambda(\mathbf{G})$.

1.11. Lemma ([Huppert, 1967, III,2.13]). *Let* $\mathbf{G}$ *be a p-group of nilpotency class 2. Then* $\exp(\mathbf{G}/\operatorname{Z}(\mathbf{G})) \leq \exp \operatorname{Z}(\mathbf{G})$ *and* $\exp \mathbf{G}' \leq \exp(\mathbf{G}/\mathbf{G}')$.

A stronger version of [Scott, 1969, Proposition 2.3], which says that for all $\mathbf{N} \trianglelefteq \mathbf{G}$,

$$\lambda(\mathbf{G}/\mathbf{N}) \mid \lambda(\mathbf{G})$$

and

$$\lambda(\mathbf{G}) \mid \lambda(\mathbf{G}/\mathbf{N}) \cdot \lambda(\mathbf{N}),$$

for p-groups of nilpotency class 2 is the following. Observe, that for an abelian group $\mathbf{A}$, $\lambda(\mathbf{A}) = \exp \mathbf{A}$.

1.12. Proposition. *Let* $\mathbf{G}$ *be a p-group of nilpotency class 2. Then*

(a) $$\frac{\exp \mathbf{G}}{\exp(\mathbf{G}/\operatorname{Z}(\mathbf{G}))} \mid \lambda(\mathbf{G})$$

(b) $$\exp(\mathbf{G}/\mathbf{G}') \mid \lambda(\mathbf{G})$$

Proof. Let $\lambda = \lambda(\mathbf{G})$.

(a) First we observe that in a non-abelian p-group $\mathbf{G}$ there exists a non-central element of order $\exp \mathbf{G}$: of course, there exists an element e of order $\exp \mathbf{G}$. Suppose $e \in \operatorname{Z}(\mathbf{G})$. The group G is not abelian, take an arbitrary $a \notin \operatorname{Z}(\mathbf{G})$. Now $a + e$ is non-central and its order is $\exp \mathbf{G}$.

By the definition of $\lambda(\mathbf{G})$, there exists an element π such that $\lambda x = [x, \pi]$ for all $x \in G$. Abbreviate $q = \frac{\exp G}{\lambda}$. Then for all $x \in G$,

$$0 = q\lambda x = q[x, \pi] = [x, q\pi].$$

So $q\pi \in \operatorname{Z}(\mathbf{G})$. In particular this equation must hold if x is a non-central element of order $\exp \mathbf{G}$, so q is the smallest such number. Hence the order of $\pi + \operatorname{Z}(\mathbf{G})$ in $\mathbf{G}/\operatorname{Z}(\mathbf{G})$ is q. So q divides the exponent of $\mathbf{G}/\operatorname{Z}(\mathbf{G})$. The result follows from the fact that $\exp(\mathbf{G}/\operatorname{Z}(\mathbf{G}))$ divides $\exp \mathbf{G}$ (Lemma 1.11).

(b) Clearly, $\lambda\mathbf{G} \subseteq \mathbf{G}'$, so $\lambda \cdot (\mathbf{G}/\mathbf{G}') = \{0\}$.

□

1.13. Proposition. *Let* $\mathbf{G}$ *be a p-group of nilpotency class 2 with* $\exp \mathbf{G} = p^n$ *and* $\lambda(\mathbf{G}) = p^m$. *Then*

- $m \leq n$.
- *If p is equal to 2 then* $m \geq \frac{n+1}{2}$.
- *If p is odd then* $m \geq \frac{n}{2}$.

PROOF. Let $\lambda = \lambda(\mathbf{G})$. By the definition of λ, $m \leq n$. Suppose that $\pi \in G$ is such that $\lambda x = [x, \pi]$, for all $x \in G$. For $x = \pi$ it follows that $\lambda\pi = 0$. For $x = x + \pi$, we get

$$\lambda(x + \pi) = [x + \pi, \pi]$$
$$\lambda x + \lambda\pi - \binom{\lambda}{2}[x, \pi] = [x, \pi] \text{ (by [Huppert, 1967, III,1.3])}$$
$$\lambda x - \binom{\lambda}{2}(\lambda x) = \lambda x$$
$$\frac{\lambda^2(\lambda - 1)}{2}x = 0$$

So $p^n = \exp \mathbf{G} \mid \frac{\lambda^2(\lambda-1)}{2} = \frac{p^{2m}(p^m-1)}{2}$. If $p = 2$ then $2^m - 1$ is odd, hence $2^n | 2^{2m-1}$ and $n \leq 2m - 1$. If $p > 2$ then $p^m - 1$ is even, but p^n is odd, hence $p^n | p^{2m}$ and $n \leq 2m$. □

1.14. COROLLARY. *If* $\mathbf{G}$ *is nilpotent of class 2 and* $\exp \mathbf{G}$ *is equal to 4 then* $\lambda(\mathbf{G}) = \exp \mathbf{G} = 4$.

1.15. EXAMPLE. Let $\mathbf{G}$ be a Hamiltonian group (i.e., a non-abelian group where every subgroup is a normal subgroup) of order n and exponent e. If $e = 2^\lambda q$, where q is odd, then

$$|\mathbf{P}(\mathbf{G})| = 16nq.$$

PROOF. By Dedekind's theorem ([Huppert, 1967, III,7.12]), $\mathbf{G}$ is the direct product

$$\mathbf{G} = \mathbf{A} \times \mathrm{Q}_8 \times \mathbf{B}$$

of the group of quaternions Q_8 of order 8, an abelian group $\mathbf{A}$ of odd order and an abelian group $\mathbf{B}$, where $\exp \mathbf{B}$ is equal to either 1 or 2. Clearly, the exponent of $\mathbf{A}$ must be equal to q. The center of Q_8 has index 4 in Q_8, so the center of $\mathbf{G}$ has index 4 in $\mathbf{G}$. By Corollary 1.14, $\lambda(\mathrm{Q}_8 \times \mathbf{B}) = \exp(\mathrm{Q}_8 \times \mathbf{B}) = 4$, and by (1.4), $\lambda(\mathbf{G}) = \lambda(\mathrm{Q}_8 \times \mathbf{B}) \cdot \lambda(\mathbf{A}) = 4q$. As a consequence of (1.3),

$$|\mathbf{P}(\mathbf{G})| = n \cdot 4q \cdot 4 = 16nq.$$

□

Let $\mathbf{G}$ be a nilpotent group of class 2 and $p \in \mathbf{P}(\mathbf{G})$. Then of course, the function $p_0 := p - p \circ 0$ is a zero-symmetric polynomial function. It induces a zero-symmetric polynomial function $p_0^{\mathbf{G}'}$ on $\mathbf{G}/\mathbf{G}'$, where $p_0^{\mathbf{G}'}(g + \mathbf{G}') := p_0(g) + \mathbf{G}'$. Since $\mathbf{G}/\mathbf{G}'$ is abelian, $p_0^{\mathbf{G}'}$ is induced by a polynomial of the form kx, where $0 \leq k < \exp(\mathbf{G}/\mathbf{G}')$. The function q defined by $q(g) := p_0(g) - kg$ is polynomial and maps G into G'. It is induced by a polynomial of the form $lx + [x, h]$, where

$0 \leq l < \lambda(\mathbf{G})$ and $h \in G$. Since q maps G into G', the exponent of $\mathbf{G}/\mathbf{G}'$ must divide l.

Immediately, we find

$$q(g+c) = l(g+c) + [g+c, h] = lg + [g, h] = q(g),$$

for all $g \in G, c \in G'$, since by Lemma 1.11, the exponent of $\mathbf{G}'$ divides the exponent of $\mathbf{G}/\mathbf{G}'$. So q is constant on the cosets of $\mathbf{G}'$ in $\mathbf{G}$. This gives an upper bound for $|\mathbf{P}(\mathbf{G})|$, namely $|\mathbf{G}| \cdot \exp(\mathbf{G}/\mathbf{G}') \cdot |\mathbf{G}'|^{[\mathbf{G}:\mathbf{G}']}$. As a consequence,

$$\lambda(\mathbf{G}) \leq \frac{\exp(\mathbf{G}/\mathbf{G}')}{[\mathbf{G} : \mathrm{Z}(\mathbf{G})]} \cdot |\mathbf{G}'|^{[\mathbf{G}:\mathbf{G}']}. \tag{1.5}$$

Assume that $p > 2$ or $\exp \mathbf{G}' < \exp \mathbf{G}/\mathbf{G}'$. Then we observe that by Lemma 1.11,

$$\begin{aligned} q(x+y) &= l(x+y) + [x+y, h] \\ &= lx + [x, h] + ly + [y, h] - \binom{l}{2}[x, y] = q(x) + q(y). \end{aligned}$$

So q is a homomorphism from $\mathbf{G}$ into $\mathbf{G}'$. Again we get an upper bound from this observation: $|\mathbf{P}(\mathbf{G})| \leq |\mathbf{G}| \cdot \exp(\mathbf{G}/\mathbf{G}') \cdot |\hom(\mathbf{G}, \mathbf{G}')|$. And for the length of $\mathbf{G}$,

$$\lambda(\mathbf{G}) \leq \frac{\exp(\mathbf{G}/\mathbf{G}')}{[\mathbf{G} : \mathrm{Z}(\mathbf{G})]} \cdot |\hom(\mathbf{G}, \mathbf{G}')|. \tag{1.6}$$

2.4. Bounds for the order of π.

So far, we have tried to find bounds for $\lambda(\mathbf{G})$. If we want to check if a certain number k is the length of a group, we have to check, whether $kx = [x, \pi]$, for some $\pi \in G$, and that there is no smaller such number. Of course, elements in the same coset modulo the center of the group behave identically. The following proposition gives bounds for the order of such an element π.

1.16. Proposition. *Let $\mathbf{G}$ be a p-group of nilpotency class 2, $\exp \mathbf{G} = p^n$ and $m \in \mathbb{N}$, $\pi \in G$ such that $p^m x = [x, \pi]$ for all $x \in G$. Then the order of π is bounded by*

$$p^{n-m} \leq \mathit{ord}\ \pi \leq p^m.$$

Proof. We see immediately that $p^m \pi = [\pi, \pi] = 0$.
The second inequality can be seen as follows: In a p-group of exponent p^n there exists an element e of order p^n. Linearity of the commutator operation gives $[e, p^{n-m-1}\pi] = p^{n-m-1}[e, \pi] = p^{n-1}e \neq 0$, so in particular $p^{n-m-1}\pi \neq 0$. □

2.5. Presentations and generators.

Suppose that we have a presentation of a nilpotent group of class 2. Is it possible to determine the length of the group from this presentation? Or alternatively, given a set of generators of a nilpotent group of class 2. Is it possible to determine the length? We show that we have to consider the equation $kx = [x, \pi]$ only for the generators of the group.

1.17. PROPOSITION. *Let* $\mathbf{G}$ *be a nilpotent group of class 2 and generated by* a *and* b*. Then for any fixed* k *and* π *the following are equivalent:*

1. $\binom{k}{2}[a, b] = 0$ *and* $kx = [x, \pi]$ *holds for* $x \in \{a, b\}$.
2. $kx = [x, \pi]$ *holds for all* $x \in G$.

PROOF. Let $\mathbf{G}$ be generated by a and b.

- $1 \implies 2$: From the elementary properties of the commutator in nilpotent groups of class 2 it follows that if
  $y = \alpha_1 a + \beta_1 b + \cdots + \alpha_s a + \beta_s b$, then

$$\begin{aligned}[a, y] &= [a, (\sum_{i=1}^{s} \alpha_i)a + (\sum_{i=1}^{s} \beta_i)b] \\ &= [a, (\sum_{i=1}^{s} \beta_i)b] \\ &= \gamma[a, b],\end{aligned}$$

  for a suitable number γ. In particular, the assumptions imply $\binom{k}{2}[a, y] = 0$. Let x be a word over $\{a, b\}$. Now we use induction on the length of x. If $x = a + y$, then

$$\begin{aligned}kx = k(a + y) &= ka + ky - \binom{k}{2}[a, y] \\ &= [a, \pi] + [y, \pi] = [a + y, \pi] = [x, \pi].\end{aligned}$$

  For $x = b + y$ the proof is analogous.
- $2 \implies 1$: If $kx = [x, \pi]$ does not hold for $x \in \{a, b\}$ then 2 clearly does not hold. So suppose that $kx = [x, \pi]$ holds for $x \in \{a, b\}$, but $\binom{k}{2}[a, b] \neq 0$. Since $k(a + b) = ka + kb \iff \binom{k}{2}[a, b] = 0$ (use [Huppert, 1967, III,1.3)]) it follows that $k(a+b) \neq ka+kb$. But $[a+b, \pi] = [a, \pi]+[b, \pi]$, a contradiction.

□

The condition $\binom{k}{2}[a, b] = 0$ is inconvenient. We show now that we can drop it easily.

Let $\mathbf{G}$ be a p-group, $p^a = \exp \mathbf{G}'$, $p^b = \exp(\mathbf{G}/\mathbf{G}')$ and $p^e = \exp \mathbf{G}$. By Lemma 1.11, $a \leq b \leq e$. As a consequence, $\frac{e}{2} \geq a$.

So for $p > 2$, taking k a power of p and at least $p^{\frac{e}{2}}$ (as Proposition 1.13 suggests), we get $\binom{k}{2}[a,b] = \frac{k-1}{2}(k[a,b]) = 0$ for all $a, b \in G$, and hence need not check it.

For $p = 2$ and odd e, we have to choose k a power of 2 and (by Proposition 1.13) at least $2^{\frac{e+1}{2}}$, whence $\binom{k}{2}[a,b] = (k-1)q(2^{\frac{e-1}{2}}[a,b])$ (for some $q \in \mathbb{N}$). Since $2^{\frac{e-1}{2}}[a,b] = 0 \iff 2^{\frac{e}{2}}[a,b] = 0$, we are happy.

For $p = 2$ and even e, we have to choose k a power of 2 and at least $2^{\frac{e+1}{2}}$, which in this case is at least $2^{\frac{e}{2}+1}$. So, $\binom{k}{2}[a,b] = (k-1)q(2^{\frac{e}{2}}[a,b])$ (for some $q \in \mathbb{N}$), and $2^{\frac{e}{2}}[a,b] = 0$.

We formulate these results as a theorem:

1.18. Theorem. *Let $\mathbf{G}$ be a nilpotent group of class 2 and generated by a and b. If k fulfills the conditions for $\lambda(\mathbf{G})$ in Proposition 1.13, then for any π the following are equivalent:*

1. *$kx = [x, \pi]$ holds for $x \in \{a, b\}$.*
2. *$kx = [x, \pi]$ holds for all $x \in G$.*

Proposition 1.17 and Theorem 1.18 can be generalized to finitely many generators:

1.19. Corollary. *Let $\mathbf{G} = \langle g_1, \ldots, g_r \rangle$ be a p-group of nilpotency class 2. If k fulfills the conditions for $\lambda(\mathbf{G})$ in Proposition 1.13, then for fixed $\pi \in G$ the following are equivalent:*

1. *$kx = [x, \pi]$ holds for $x \in \{g_1, \ldots, g_r\}$.*
2. *$kx = [x, \pi]$ holds for all $x \in G$.*

2.6. Minimal examples of class 2 nilpotent p-groups.

In a p-group $\mathbf{G}$ of exponent p^n, the length $\lambda(\mathbf{G})$ is always a power of p between $p^{\frac{n(+1)}{2}}$ and p^n. We will now give examples of p-groups for which the lower bound is sharp. More precisely, for every prime power q, which is not equal to a prime, the square of a prime or a power of 8, we will give an example of such a group of order q, for which the lower bound is sharp.

1.20. Proposition. *For every prime p and every $l \geq 1$, the group*

$$\mathbf{G} = \langle a, b; p^{2l+1}a, p^l b, [a,b] = p^{l+1}a \rangle$$

is a semi-direct product of $\mathbb{Z}_{p^{2l+1}}$ with $\mathbb{Z}_{p^l}$ of order p^{3l+1} and exponent p^{2l+1}. This group is nilpotent of class 2 and $\lambda(\mathbf{G}) = p^{l+1}$.

Proof. Groups of this kind are described in [Huppert, 1967, Chapter III]. So size and exponent of $\mathbf{G}$ are well-known. The nilpotency class of $\mathbf{G}$ is 2. This can be demonstrated as follows: the commutator $[a,b] = p^{l+1}a$ has to commute with

both a and b; of course it commutes with a. Furthermore $[a,b]+b = p^{l+1}a + b = b + p^{l+1}(1+p^{l+1})a$, so we have to show that $p^{l+1}a = p^{l+1}(1+p^{l+1})a$, or equivalently $p^{l+1}(1+p^{l+1}) \equiv p^{l+1} \mod p^{2l+1}$, which can be verified immediately expanding the expression on the left. By Proposition 1.13, the length $\lambda(\mathbf{G})$ is greater or equal to p^{l+1}. In fact it is equal to p^{l+1}, which can be verified setting $\pi := b$ in Proposition 1.17. □

The following examples of size p^{3l+2} and p^{3l} look quite similar just as the proofs of the corresponding propositions, which are omitted for this reason.

1.21. Proposition. *For every prime p and every $l \geq 1$, the group*

$$\mathbf{G} = \langle a, b; p^{2l+2}a, p^l b, [a,b] = p^{l+2}a \rangle$$

is a semi-direct product of $\mathbb{Z}_{p^{2l+2}}$ with $\mathbb{Z}_{p^l}$ of order p^{3l+2} and exponent p^{2l+2}. This group is nilpotent of class 2 and $\lambda(\mathbf{G}) = p^{l+2}$.

1.22. Proposition. *For every odd prime p and every $l \geq 1$, the group*

$$\mathbf{G} = \langle a, b; p^{2l}a, p^l b, [a,b] = p^l a \rangle$$

is a semi-direct product of $\mathbb{Z}_{p^{2l}}$ with $\mathbb{Z}_{p^l}$ of order p^{3l} and exponent p^{2l}. This group is nilpotent of class 2 and $\lambda(\mathbf{G}) = p^l$.

2.7. Class 2 nilpotent p-groups of order at most p^4.

For all nilpotent groups $\mathbf{G}$ of class 2 and order p^n $(1 \leq n \leq 4)$ we list the numbers $\lambda(\mathbf{G})$ and the resulting sizes of $\mathbf{P}(\mathbf{G})$. From the discussion after (1.3) it is clear that the number $\lambda(\mathbf{G})$ contains the information needed to compute the number of polynomial functions.

2.7.1. p and p^2. All these groups are abelian.

2.7.2. p^3. The center must be of order p in this case, since it has to be nontrivial in a p-group and the quotient $\mathbf{G}/\operatorname{Z}(\mathbf{G})$ must be noncyclic in a non-abelian group.

$p = 2$: The non-abelian groups of order 8 are the dihedral group D_8 and the quaternion group Q_8. Both are nilpotent of class 2 and have exponent 4 (groups of exponent 2 are abelian, p-groups of exponent equal to their order are cyclic), thus by Corollary 1.14, $\lambda(\mathbf{G}) = \exp \mathbf{G} = 4$.

$$|\mathbf{P}(\mathrm{D}_8)| = |\mathbf{P}(\mathrm{Q}_8)| = 2^7$$

$p > 2$: For $p > 2$, there are two non-abelian non-isomorphic groups of order p^3 (see [Huppert, 1967, Chapter III]). One, P_1^3, has exponent p and hence

$\lambda(P_1^3) = p$. The other one is the group $P_2^3 = \langle a, b; p^2a, pb, [a, b] = pa\rangle$. Taking $\pi = b$, we find $\lambda(P_2^3) = p$.

$$|\mathbf{P}(P_1^3)| = |\mathbf{P}(P_2^3)| = p^6$$

2.7.3. p^4**.**

The center of each of these groups is nontrivial and has order at most p^2, since the quotient by the center has to be noncyclic, whence of order greater or equal to p^2. We shall show that the center of each has order at least p^2.

$p = 2$**:** There are 6 class 2 nilpotent groups of order 16, namely the groups 16/6, 16/7, 16/8, 16/9, 16/10, and 16/11 in Thomas and Wood [1980]. The group $16/11 = \langle a, b; 8a, 2b, [a, b] = 4a\rangle$ has exponent 8, so by Proposition 1.13, $\lambda(16/11) \geq 4$. Taking $\pi = b$, we find that $\lambda(16/11) = 4$, using Proposition 1.17. Each of the other five groups has exponent 4, so $\lambda(\mathbf{G}) = \exp \mathbf{G} = 4$, by Corollary 1.14.

$$\begin{aligned} |\mathbf{P}(16/6)| = |\mathbf{P}(16/7)| = |\mathbf{P}(16/8)| = |\mathbf{P}(16/9)| = \\ = |\mathbf{P}(16/10)| = |\mathbf{P}(16/11)| = 2^8 \end{aligned} \tag{1.7}$$

$p > 3$**:** For $p > 3$ there are 10 non-isomorphic non-abelian groups of order p^4 (see [Huppert, 1967, 12.6]). The remarks before [Huppert, 1967, III,14.3] say that the groups (9), (10), (12), and (13) are nilpotent of (maximal) class 3. So the six groups (6), (7), (8), (11), (14), and (15) in the list are nilpotent of class 2.

(6) The group $P_6^4 = \langle a, b; p^3a, pb, [a, b] = p^2a\rangle$ has exponent p^3. By Proposition 1.13, $\lambda(P_6^4) \geq p^2$. Choosing $\pi = b$, we find that $\lambda(P_6^4) = p^2$. Furthermore, $pa \in \mathrm{Z}(P_6^4)$, so $|\mathrm{Z}(P_6^4)| \geq p^2$.

$$|\mathbf{P}(P_6^4)| = p^8$$

(7) For the group $P_7^4 = \langle a, b; p^2a, p^2b, [a, b] = pa\rangle$, we have $p \leq \lambda(P_7^4) \leq \exp P_7^4 = p^2$. That $\lambda(P_7^4) \neq p$ can be seen as follows: Suppose that there is a $\pi \in G$, such that $px = [x, \pi]$ for all $x \in P_7^4$. Every a occurring in π produces a power of a in $[b, \pi]$, so the number of a's in π must be divisible by p^2. So $[b, \pi] = 0 \neq pb$. Furthermore, pa and pb generate a subgroup of $\mathrm{Z}(P_7^4)$ of order p^2.

$$|\mathbf{P}(P_7^4)| = p^8$$

(8) For the group
$P_8^4 = \langle a, b, c; pa, pb, p^2c, [a, b] = -pc, [a, c], [b, c]\rangle$, we have $p \leq \lambda(P_8^4) \leq \exp G = p^2$. Obviously, c is in the center of the group (it commutes

with every generator), so $[c, \pi] = 0$ for all $\pi \in P_8^4$, but $pc \neq 0$. So $\lambda(P_8^4) = p^2$. Since $c \in \mathrm{Z}(P_8^4)$, the center of P_8^4 has order p^2.

$$|\mathbf{P}(P_8^4)| = p^8$$

(11) The direct product of $\mathbb{Z}_p$ with the non-abelian group of order p^3 and exponent p has exponent p, so $\lambda(P_{11}^4) = p$. Its center is isomorphic to $(\mathbb{Z}_p)^2$.

$$|\mathbf{P}(P_{11}^4)| = p^7$$

(14) This is the group $P_{14}^4 = \mathbf{G} \times \mathbb{Z}_p$, where $\mathbf{G}$ is the only group of order p^3, where $\lambda(\mathbf{G}) = p < \exp \mathbf{G}$. So $\lambda(P_{14}^4) = \mathrm{lcm}(p, p) = p$, by (1.4). The center of P_{14}^4 is isomorphic to $(\mathbb{Z}_p)^2$.

$$|\mathbf{P}(P_{14}^4)| = p^7$$

(15) The group $P_{15}^4 = \langle a, b, c; p^2a, pb, pc, [a, b] = -c, [a, c], [b, c] \rangle$ has $\lambda(P_{15}^4) = \exp P_{15}^4 = p^2$. $\lambda(P_{15}^4) = p$ is not possible: Since a commutes with a and c, we would have $pa = [a, \pi] = [a, ib] = -ic$. But $-ic \neq pa$, because both c and pa have order p and so $-ic = pa$ would imply $|P_{15}^4| < p^4$. The center has size p^2, since pa and c generate a subgroup of $\mathrm{Z}(P_{15}^4)$ of order p^2.

$$|\mathbf{P}(P_{15}^4)| = p^8$$

$p = 3$: For $p = 3$, a complete list of all groups can be found in [Huppert, 1967, Chapter III, remarks before Definition 14.3]. This list differs from the one for $p > 3$ only in the group (13), which we did not have to consider. This group is replaced by another group of nilpotency class 3. Thus, the above results also hold for $p = 3$.

3. A possible generalization: nilpotent groups of class 3

For nilpotent groups of class 1 or 2, nice term representations for polynomial functions on these groups are known. For a class of nilpotent groups of class 3 fulfilling a specific property, a generalization of this presentation can be obtained.

3.1. Some elementary results.

From now on, $[[A, B], C]$ is abbreviated by $[A, B, C]$. The following results are presented in Huppert [1967], and in more detail in Hall [1969].

1.23. LEMMA. *For all elements of an arbitrary group* $\mathbf{G}$ *the following holds:*

i. $[a,b] = -[b,a]$
ii. $[a,b+c] = [a,b] + [a,c] + [a,b,c]$
iii. $[a+b,c] = [a,c] + [a,c,b] + [b,c]$
iv. $[a+b,c+d] = [a,c] + [a,c,b] + [b,c] + [a,d] + [a,d,b] + [b,d] + [a+b,c,d]$
v. $-[a,b] = [a,-b] + [a,b,-b]$ *and* $-[a,b] = [a,b,-a] + [-a,b]$

PROOF. i. - iii. see Huppert [1967]
iv. and v. are consequences of ii. and iii. □

3.2. Polynomial functions on nilpotent groups of class 3.

1.24. LEMMA. *If* $\mathbf{G}$ *is nilpotent of class 3, then for all* $x,a,b,c \in G$

$$[x,a,c] + [x,b,c] = [x,a+b,c]$$

PROOF. By Lemma 1.23

$$\begin{aligned}
[x,a,c] + [x,b,c] &= [[x,a],c] + [[x,b],c] \\
&= [[x,a] + [x,b],c] - [[x,a],c,[x,b]] \\
&= [[x,a+b] - [x,a,b],c] \\
&= [[x,a+b] + [a,x,b],c] \\
&= [x,a+b,c] + [[a,x,b],c] \\
&= [x,a+b,c]
\end{aligned}$$

□

1.25. PROPOSITION. *If* $\mathbf{G}$ *is nilpotent of class 3 and satisfies*

(CL) $\quad \forall\, a,b,c,d \in G\ \exists\, e,f \in G\ \forall x \in G \quad [x,a,b] + [x,c,d] = [x,e,f],$

then every polynomial function has a term representation of the form

$$p = a + kx + [x,b] + [x,c,d] + [x,e,x]$$

for some $a,b,c,d,e \in G$, $k \in \mathbb{N}$.

PROOF. The idea is to transform a polynomial

$$p = g_0 + x + g_1 + x + \cdots + x + g_l$$

into a polynomial of the form

$$a + x + [x,b] + [x,c,d] + [x,e,x].$$

We will proceed towards the desired form in 4 steps.

1. x can change place with any group element producing a commutator. So we can transform p into

$$p = g + [x, a_0] + x + [x, a_1] + x + \cdots + x + [x, a_k]$$

for some $g, a_0, \ldots, a_k \in G$ and a suitable $k \in \mathbb{N}$.

2. Now we start the same thing again:

$$[x, a] + x = x + [x, a] + \underbrace{[x, a, x]}_{*}$$

Now $*$ commutes with everything and can be brought to the right hand side. As a consequence of the fact that $\mathbf{G}$ is nilpotent of class 3 it holds $[x, a] + [x, b] = [x, a + b] + \underbrace{[x, a, b]}_{**}$, and $**$ can again be brought to the right hand side.

3. The result we get is of the form

$$p = g + kx + [x, h] + [x, c_0, d_0] + \cdots + [x, c_r, d_r] + \\ + [x, e_0, x] + \cdots + [x, e_s, x]$$

where $g, c_0, \ldots, c_r, d_0, \ldots, d_r, e_0, \ldots, e_s$ are from G and $k, r, s \in \mathbb{N}$.

4. What remains to show is, that sums of expressions of the form $*$ and $**$ are again of one of these forms.

   $*$. By Lemma 1.24, $[x, a, x] + [x, b, x] = [x, a + b, x]$.

   $**$. $\mathbf{G}$ satisfies (CL).

□

3.3. A sufficient condition for (CL)**.**

Lemma 1.24 shows that in a class 3 nilpotent group with (CL) the operator $[.,.,.]$ is "linear" in all three places.

1.26. Proposition. *Let again* $\mathbf{G}$ *be a nilpotent group of class 3 and let* $\sim$ *be the relation* $a \sim b :\iff \forall c \in G'\ [c, a] = [c, b]$*. Then* $\sim$ *is a congruence relation. If* $\mathbf{G}/_\sim$ *is cyclic then* $\mathbf{G}$ *satisfies* (CL)*.*

Proof. That $\sim$ is a congruence follows again from the fact that $[.,.,.]$ is linear in all three places. Let a, b, c, d be arbitrary, but fixed elements of $\mathbf{G}$. We have to show that there exist elements e and f of $\mathbf{G}$, s.t. for all $x \in G$:

$$[x, a, b] + [x, c, d] = [x, e, f].$$

- If $b \sim 0$ then $[x, a, b] = [x, a, 0] = 0$ and we can choose $e = c$ and $f = d$, analogously we get $e = a$ and $f = b$ for $c \sim 0$.
- If $b \sim d$ then $[x, a, b] = [x, a, d]$, since $[x, a] \in G'$. So $[x, a, b] + [x, c, d] = [x, a, d] + [x, c, d] = [x, a + c, d]$, by Lemma 1.24.

- Suppose $b \not\sim d$. Let g be the preimage of a generator of $\mathbf{G}/_\sim$ with respect to the natural epimorphism from $\mathbf{G}$ to $\mathbf{G}/_\sim$. Then there exist natural numbers k_b and k_d, such that $b \sim k_b g$ and $d \sim k_d g$. Now $[x, a, b] = [x, a, k_b g] = k_b[x, a, g] = [x, k_b a, g]$ and similarly $[x, c, d] = [x, k_d c, g]$. So $[x, a, b] + [x, c, d] = [x, k_b a + k_d c, g]$.

□

1.27. Remark.

- If $\mathbf{G}$ is not nilpotent of class ≤ 3, $\sim$ need not be a congruence.
- The kernel of this congruence is the centralizer of $\mathbf{G}'$ in $\mathbf{G}$.
- By [Huppert, 1967, III,2.11] it holds $[\mathbf{G}', \mathbf{G}'] \leq \mathrm{K}_4(\mathbf{G}) = \{0\}$. Hence $\mathbf{G}' \leq \ker \sim$. So $\mathbf{G}/_\sim$ is abelian.

3.4. Generalization.

Every abelian group is the direct product of cyclic groups. Let $\Delta(\mathbf{G})$ be the smallest natural number d, such that $\mathbf{G}/_\sim$ is a direct product of d cyclic groups. With this notation we get the following simple corollary.

1.28. Corollary. *If $\mathbf{G}$ is a class 3 nilpotent group then every polynomial function over $\mathbf{G}$ has a term representation of the form*

$$p = g_0 + kx + [x, g_1] + [x, g_2, x] + [x, c_1, d_1] + \dots [x, c_{\Delta(\mathbf{G})}, d_{\Delta(\mathbf{G})}], \tag{1.8}$$

where $k \in \mathbf{N}$, $g_0, g_1, g_2, c_1, \dots, c_{\Delta(\mathbf{G})}, d_1, \dots, d_{\Delta(\mathbf{G})} \in G$.

3.5. Examples (p-groups).

order	cl. 3 nilp. groups	$\Delta(\mathbf{G}) = 1$	$\Delta(\mathbf{G}) = 2$	$\Delta(\mathbf{G}) = 3$
2^4	3	3	-	-
2^5	15	15	-	-
2^6	114	98	16	-
2^7	1137	803	290	44
3^4	4	4	-	-
3^5	26	19	7	-
3^6	148	134	-	-

1.29. Corollary. *Let $\mathbf{G}$ be a nilpotent group of class 3. Then*

$$|\mathbf{P}(\mathbf{G})| \leq |\mathbf{G}| \cdot \lambda(\mathbf{G}) \cdot \Big([\mathbf{G} : \mathrm{Z}(\mathbf{G})] \cdot [\mathbf{G} : \mathbf{G}']\Big)^{2+\Delta(\mathbf{G})}$$

4. Direct products

In this section we prove that every polynomial function on a direct product of groups can be decomposed into polynomial functions on the direct factors. Furthermore we characterize the direct products where the converse holds.

1.30. PROPOSITION. *Let* $\mathbf{G}$ *and* $\mathbf{H}$ *be two arbitrary groups. For every zero-symmetric polynomial function* p *on* $\mathbf{G} \times \mathbf{H}$ *and for all* $g \in G$ *and* $h \in H$*, the following holds:*

$$p((g,h)) = p((g,0)) + p((0,h)) \tag{1.9}$$

The function $p_G : \mathbf{G} \to \mathbf{G}$*,* $g \mapsto g'$*, where* $p((g,0)) = (g',0)$*, is a polynomial function on* $\mathbf{G}$*. The function* $p_H : \mathbf{H} \to \mathbf{H}$*,* $h \mapsto h'$*, where* $p((0,h)) = (0,h')$*, is a polynomial function on* $\mathbf{H}$*.*

PROOF. We can write p in the form $(x,y) \mapsto (a_0,b_0) + (x,y) + \cdots + (x,y) + (a_m,b_m)$ for suitable elements $a_i \in G, b_i \in H$, $0 \leq i \leq m \in \mathbb{N}_0$. We start with

$$\begin{aligned} p((g,h)) &= (a_0,b_0) + (g,h) + \cdots + (g,h) + (a_m,b_m) \\ &= (a_0 + g + \cdots + g + a_m, b_0 + h + \cdots + h + b_m). \end{aligned}$$

p is zero-symmetric, which gives us

$$(0,0) = p((0,0)) = (a_0 + a_1 \cdots + a_m, b_0 + b_1 + \cdots + b_m),$$

which allows us to write

$$\begin{aligned} p((g,0)) &= (a_0 + g + \cdots + g + a_m, 0) \quad \text{and} \\ p((0,h)) &= (0, b_0 + h + \cdots + h + b_m) \end{aligned}$$

Consequently,

$$p((g,h)) = p((g,0)) + p((0,h)).$$

□

1.31. COROLLARY. *Let* $\mathbf{G}$ *and* $\mathbf{H}$ *be two arbitrary groups. For every polynomial function* p *on* $\mathbf{G} \times \mathbf{H}$ *there exist polynomial functions* p_G *on* $\mathbf{G}$ *and* p_H *on* $\mathbf{H}$ *such that for all* $g \in G$ *and* $h \in H$*, the following holds:*

$$p((g,h)) = (p_G(g), p_H(h)) \tag{1.10}$$

The converse holds if and only if the lengths of $\mathbf{G}$ and $\mathbf{H}$ are coprime. I.e., in this case for every pair of functions $p_G \in \mathbf{P}(\mathbf{G})$ and $p_H \in \mathbf{P}(\mathbf{H})$ the function $(g,h) \mapsto (p_G(g), p_H(h))$ is a polynomial function. We show that this is the case, if and only if every normal subgroup of $\mathbf{G} \times \mathbf{H}$ is $\mathbf{G}$-$\mathbf{H}$-decomposable. This proves Conjecture 2.10 in Pilz [1980]. We make use of the following theorem which characterizes the prime factors of $\lambda(\mathbf{G})$.

1.32. THEOREM ([Scott, 1969, Theorem 3.4]). *If* $\mathbf{G}$ *is a group and* $\mathbf{N}_0 \lhd \mathbf{N}_1 \lhd \cdots \lhd \mathbf{N}_r = \mathbf{G}$ *is a chief series of* $\mathbf{G}$*, then*

$$q \mid \lambda(\mathbf{G}) \iff q \mid \prod_{i=0}^{r-1} \sigma(\mathbf{N}_{i+1}/\mathbf{N}_i),$$

where $\sigma(\mathbf{N}_{i+1}/\mathbf{N}_i) = \begin{cases} [\mathbf{N}_{i+1} : \mathbf{N}_i] & \text{if } \mathbf{N}_{i+1}/\mathbf{N}_i \subseteq \mathrm{Z}(\mathbf{G}/\mathbf{N}_i), \\ 1 & \text{otherwise} \end{cases}$.

1.33. THEOREM. *Let* $\mathbf{G}$ *and* $\mathbf{H}$ *be two groups. Then the following are equivalent:*

1. $\mathbf{P}(\mathbf{G} \times \mathbf{H}) \cong \mathbf{P}(\mathbf{G}) \times \mathbf{P}(\mathbf{H})$
2. $(\lambda(\mathbf{G}), \lambda(\mathbf{H})) = 1$
3. *every normal subgroup of* $\mathbf{G} \times \mathbf{H}$ *is* $\mathbf{G}$-$\mathbf{H}$*-decomposable.*

PROOF.

$1 \Leftrightarrow 2$: This is a consequence of [Scott, 1969, Theorem 2.3].

$2 \Leftrightarrow 3$: By Theorem 0.13 and Theorem 1.32, it suffices to show that for every prime number p

$$\exists \mathbf{I}, \mathbf{J} \trianglelefteq \mathbf{G}, \mathbf{I} \prec \mathbf{J} \ : \ p \mid [\mathbf{J} : \mathbf{I}] \ \& \ \mathbf{J}/\mathbf{I} \leq \mathrm{Z}(\mathbf{G}/\mathbf{I})$$
$$\iff$$
$$\exists \mathbf{J} \trianglelefteq \mathbf{G} \ : \ p \mid [\mathbf{J} : [\mathbf{G}, \mathbf{J}]].$$

$\Rightarrow$: By our assumptions, there exist $\mathbf{I}, \mathbf{J} \trianglelefteq \mathbf{G}, \mathbf{I} \prec \mathbf{J}$, such that $p \mid [\mathbf{J} : \mathbf{I}]$ and $\mathbf{J}/\mathbf{I} \leq \mathrm{Z}(\mathbf{G}/\mathbf{I})$. Hence $[\mathbf{G}, \mathbf{J}] \leq \mathbf{I}$ and consequently, $p \mid [\mathbf{J} : \mathbf{I}] \mid [\mathbf{J} : [\mathbf{G}, \mathbf{J}]]$.

$\Leftarrow$: Let us assume that there is a normal subgroup $\mathbf{J} \trianglelefteq \mathbf{G}$, such that $p \mid [\mathbf{J} : [\mathbf{G}, \mathbf{J}]]$. Clearly, $[\mathbf{G}, \mathbf{K}] \leq [\mathbf{G}, \mathbf{J}]$ for every $\mathbf{K} \leq \mathbf{J}$. Let $\mathbf{K}_0, \ldots, \mathbf{K}_s$ be such that $[\mathbf{G}, \mathbf{J}] = \mathbf{K}_0 \prec \mathbf{K}_1 \prec \cdots \prec \mathbf{K}_s = \mathbf{J}$. Since $p \mid [\mathbf{J} : [\mathbf{G}, \mathbf{J}]]$, there exists an $1 \leq i \leq s$, such that $p \mid [\mathbf{K}_i, \mathbf{K}_{i-1}]$. We have $[\mathbf{G}, \mathbf{K}_i] \leq [\mathbf{G}, \mathbf{J}] \leq \mathbf{K}_{i-1}$, so $\mathbf{K}_i/\mathbf{K}_{i-1} \leq \mathrm{Z}(\mathbf{G}/\mathbf{K}_{i-1})$.

□

5. Other classes of groups

We gather some of the results on polynomial near rings.

1.34. THEOREM.

a. **Abelian groups ((1.3)):** *For an arbitrary finite abelian group* $\mathbf{A}$*,*

$$|\mathbf{P}(\mathbf{A})| = |\mathbf{A}| \cdot \exp \mathbf{A}.$$

b. **Non abelian simple groups (Fröhlich [1958]):** *If* $\mathbf{G}$ *is a non abelian simple group, then*

$$|\mathbf{P}(\mathbf{G})| = |\mathbf{G}|^{|\mathbf{G}|}.$$

c. **Dihedral groups (Malone and Lyons [1972, 1973]):** *For* $n \in \mathbb{N}$*,*

$$|\mathbf{P}(\mathrm{D}_{2n})| = \begin{cases} 4n^4 & \text{if } n \text{ is odd,} \\ \frac{1}{2}n^4 & \text{if } n \text{ is even.} \end{cases}$$

d. **Generalized quaternion groups (Malone [1973]):** *For every* $n \in \mathbb{N}$*,*

$$|\mathbf{P}(\mathrm{Q}_{2^n})| = 2^{4n-5}.$$

e. **Symmetric groups: (Lausch and Nöbauer [1976]; Fong and Meldrum [1981b])]**
For $n > 4$*,*

$$|\mathbf{P}(\mathrm{S}_n)| = 4\left(\frac{n!}{2}\right)^{n!}.$$

f. S_3 **and** S_4 **(Fong [1979]; Fong and Meldrum [1981a]):**

$$|\mathbf{P}(\mathrm{S}_3)| = 2^2 3^4 \quad \text{and}$$
$$|\mathbf{P}(\mathrm{S}_4)| = 2^{38} 3^4.$$

g. **Dicyclic groups (Lyons and Mason [1991]):** *Let* $n \in \mathbb{N}$*. Then*

$$|\mathbf{P}(\mathrm{Q}_{4n})| = \begin{cases} 16n^4 & \text{if } n \text{ is odd,} \\ 8n^4 & \text{if } n \text{ is even.} \end{cases}$$

h. **Generalized dihedral groups (Lyons and Mason [1991]):**
Let $\mathbf{A}$ *be an abelian group. Assume that* $\mathbf{A}$ *is a direct product of* d *cyclic groups of even order and some groups of odd order. Then* d *is well-defined and*

$$|\mathbf{P}(\mathrm{Dih}(\mathbf{A}))| = \begin{cases} 4|\mathbf{P}(\mathbf{A})|^2 & \text{if } |\mathbf{A}| \text{ is odd,} \\ \frac{1}{2^d}|\mathbf{P}(\mathbf{A})|^2 & \text{if } |\mathbf{A}| \text{ is even.} \end{cases}$$

i. **Fong and Kaarli [1995]:** *Let* $\mathbf{G}$ *be a finite group with a unique minimal normal subgroup* $\mathbf{H}$*, and* $\mathbf{H}$ *the only nonzero normal subgroup with nonzero centralizer in* $\mathbf{G}$*. Then*

$$|\mathbf{P}(\mathbf{G})| = |\mathbf{P}(\mathbf{G}/\mathbf{H})| \cdot |\mathbf{H}|^{m(n+1)},$$

where $m = |\mathbf{G}/\mathbf{H}|$ *and* n *is the dimension of* $\mathbf{H}$ *over End* $\mathbf{H}_{I(\mathbf{G})}$. *In particular, if* $\mathbf{G}$ *is a non-abelian group of order* pq, *where* $p < q$ *are two prime numbers, then the following holds:*

$$|\mathbf{P}(\mathbf{G})| = (pq^p)^2$$

1.35. Remark. The result in Lyons and Mason [1991] for abelian groups $\mathbf{A}$ of odd order was already proved in Clay and Grainger [1989].

1.36. Proposition. *Let* $\mathbf{G}$ *be a group,* $\mathbf{I}, \mathbf{J} \trianglelefteq \mathbf{G}$, *and* $\mathbf{N} \leq \mathbf{M}(\mathbf{G})$. *We define the Noetherian quotient*

$$(\mathbf{I}, \mathbf{J})_{\mathbf{N}} := \{n \in N \mid n(J) \subseteq I\}$$

With this notation

$$|\mathbf{P}(\mathbf{G})| = |\mathbf{P}(\mathbf{G}/\mathbf{N})| \cdot |(\mathbf{N} : \mathbf{G})_{\mathbf{P}(\mathbf{G})}| \tag{1.11}$$

Proof. Define

$$\begin{aligned} \Phi : \mathrm{P}(\mathbf{G}) &\to \mathrm{P}(\mathbf{G}/\mathbf{N}) \\ p &\mapsto p^{\mathbf{N}} : G/N \to G/N, \end{aligned}$$

where $p^{\mathbf{N}}$ maps $g + \mathbf{N}$ to $p(g) + \mathbf{N}$. The mapping Φ is well-defined and a homomorphism. Its kernel is $(\mathbf{N} : \mathbf{G})_{\mathbf{P}(\mathbf{G})}$, so this is an ideal of $\mathbf{P}(\mathbf{G})$. It is surjective, since for an arbitrary polynomial function $q \in \mathrm{P}(\mathbf{G}/\mathbf{N})$, q is of the form $x \mapsto a_0 + \mathbf{N} + x + \cdots + a_{n-1} + \mathbf{N} + x + a_n + \mathbf{N}$. The function p which maps x to $a_0 + x + \cdots + a_{n-1} + x + a_n$ fulfills $p^{\mathbf{N}} = q$. The equation follows from the homomorphism theorem $\mathbf{P}(\mathbf{G})/\ker(\Phi) \cong \mathrm{Im}(\Phi)$. □

6. Generating polynomial near rings additively

A set of generating elements of a near ring uniquely determines the near ring. In practice it is very difficult even to decide membership in a near ring which is given by a set of generators.[2] If the elements generate the near ring purely additively, the problem is by far easier. A group given by a set of generators is "almost known". Efficient algorithms are described e.g. in Sims [1970] for permutation groups and in Sims [1994] for finitely presented, in particular for polycyclic groups.

Let $E_{\mathbf{G}}$ be a set of additive generators of $\mathbf{G}$. The near ring $\mathbf{P}(\mathbf{G})$ of polynomial functions on $\mathbf{G}$ is generated additively by the constant functions $f : x \mapsto e$, for $e \in E_{\mathbf{G}}$ and $id : x \mapsto x$.

A list of numbers of zero-symmetric polynomial functions on all groups of order at most 100 – composed by a computer program – has been published in Saad *et al.* [1997].

[2] For more details see e.g. Scott [1979]; Meldrum [1985]; Clay [1992].

7. Storing polynomial functions

Let p be a polynomial function on the group $\mathbf{G}$. If $p(0) = a \neq 0$, then $p_0 : x \mapsto p(x) - a$ is also a polynomial function and $p_0(0) = 0$. From now on let p be zero-symmetric, i.e. $p(0) = 0$.

If $\mathbf{G}$ is abelian, it contains an element e of order $\exp \mathbf{G}$. Let k be the least natural number such that $p(e) = ke$. Then k is the length of p. It suffices to store the length k.

If $\mathbf{G}$ is nilpotent of class 2, p is induced by a polynomial of the form $kx + [x, \pi]$. Clearly, if k and π are known, it is sufficient to store these. It is rather difficult to find out k and π in practice. If $p > 2$ or $\exp \mathbf{G}' < \exp(\mathbf{G}/\mathbf{G}')$, we can choose another representation, which is easier to determine: the quotient $\mathbf{G}/\mathbf{G}'$ is abelian, so it is possible to find the length of the polynomial function $p' : x + \mathbf{G}' \mapsto p(x) + \mathbf{G}'$ on $\mathbf{G}/\mathbf{G}'$. In this way we find the length of p modulo the exponent of $\mathbf{G}/\mathbf{G}'$. The zero-symmetric polynomial function p behaves almost like a homomorphism:

$$p(x + y) = p(x) + p(y) - \binom{k}{2}[x, y]$$

Since $\exp \mathbf{G}' \leq \exp(\mathbf{G}/\mathbf{G}')$ and equality may only hold if $p > 2$, it suffices to store k modulo $\exp \mathbf{G}'$ and the values of p for a set of generators of $\mathbf{G}$.

8. Is the function polynomial?

A general method to test algorithmically, if f is a polynomial function is to generate $\mathrm{P}(\mathbf{G})$ and test if $f \in \mathrm{P}(\mathbf{G})$ (see Section 6).

The method used for storing a polynomial function can also be used to test whether a given function f on a class 2 nilpotent group $\mathbf{G}$ is polynomial: first we check whether it is compatible with $\mathbf{G}'$. If so, we check whether the induced function on the abelian quotient $\mathbf{G}/\mathbf{G}'$ is polynomial. As a side-result we get the length of f modulo $\exp \mathbf{G}$. Now we can test if f is polynomial. This test is analogous to the test if f is a homomorphism.

CHAPTER 2

Compatible functions on groups

Polynomial functions have the nice property that they can be written down nicely, by a polynomial. Especially nice are groups, where every function is a polynomial function. These are called polynomially complete. It turns out that only very "few" groups are polynomially complete (c.f. Chapter 3). One reason is, that polynomial functions are compatible, i.e., for every normal subgroup $\mathbf{N}$, if x and y are elements of the same coset modulo $\mathbf{N}$, then their images under any polynomial function will be in the same coset. Functions fulfilling this property are called compatible. So, if the group we consider is not simple, it is not polynomially complete. Or, with James I,

No Bishop, no King.

We might weaken our concept of completeness to so called affine completeness. We demand that every compatible function is polynomial.

We shall only consider the case of unary functions on groups.

1. Definitions and basic results

2.1. Definition. Let $\mathbf{G}$ be a group and φ a function from G to G. Let $\mathbf{N}$ be a normal subgroup of $\mathbf{G}$. The function φ is called **compatible with N**, iff the following implication holds for all $x, y \in G$:

$$x - y \in N \implies \varphi(x) - \varphi(y) \in N.$$

The function φ is called **compatible**, iff it is compatible with every normal subgroup of $\mathbf{G}$.

The following proposition shows that the set of compatible functions on a group is closed under composition and point-wise addition. Like polynomial functions, also compatible functions form a sub-near ring of the near ring of all self-maps on a group.

2.2. Proposition. *Let φ and ψ be compatible functions on a group $\mathbf{G}$. Then $\varphi + \psi$ and $\varphi \circ \psi$ are compatible functions on $\mathbf{G}$, too.*

PROOF. Take an arbitrary normal subgroup $\mathbf{N}$ of $\mathbf{G}$ and two elements $x, y \in G$, such that $x - y \in N$. Then for a suitable $n \in N$,

$$\begin{aligned}(\varphi+\psi)(x) - (\varphi+\psi)(y) &= \varphi(x) + \underbrace{\psi(x) - \psi(y)}_{\in N} - \varphi(y) \\ &= \underbrace{\varphi(x) - \varphi(y)}_{\in N} + \underbrace{\psi(x) - \psi(y)}_{\in N} + n\end{aligned}$$

and

$$\begin{aligned}x - y \in N &\implies \psi(x) - \psi(y) \in N \\ &\implies \varphi(\psi(x)) - \varphi(\psi(y)) \in N.\end{aligned}$$

□

2.3. NOTATION. Let $\mathbf{C}(\mathbf{G})$ denote the near ring of all compatible functions on a group $\mathbf{G}$ with point-wise addition and composition.

Polynomial functions are compatible: the near ring of polynomial functions is generated by the identity function and all constant functions on a group. Clearly, each of these are compatible. The converse is not true in general, as the group $\mathbb{Z}_3$ shows: every function on $\mathbb{Z}_3$ is compatible, since $\mathbb{Z}_3$ is simple, but only 9 of these 27 functions are polynomial functions. Groups, where every compatible function is polynomial, are called **1-affine complete**. Such groups will be considered in Chapter 3.

For the following proofs we will be happy to have a few equivalent characterizations of compatibility at hand.

2.4. PROPOSITION. *Let $\mathbf{G}$ be a group and $\varphi : G \to G$. Then the following are equivalent:*

1. $\forall \mathbf{N} \trianglelefteq \mathbf{G}\ \forall x, y \in G \quad x - y \in N \implies \varphi(x) - \varphi(y) \in N$ *(i.e., φ is compatible).*
2. $\forall x, y \in G \quad \varphi(x) - \varphi(y) \in [x - y]$.
3. $\forall \mathbf{N} \trianglelefteq \mathbf{G}\ \forall x \in G\ \forall n \in N \quad \varphi(x + n) - \varphi(x) \in N$.

PROOF. We will prove $1 \implies 2 \implies 3 \implies 1$.

$1 \Rightarrow 2$**:** Let $x, y \in G$. Then $x - y \in [x - y]$, so also $\varphi(x) - \varphi(y) \in [x - y]$.

$2 \Rightarrow 3$**:** Let $\mathbf{N} \trianglelefteq \mathbf{G}$, $x \in G$ and $n \in N$. Then $\varphi(x + n) - \varphi(x) \in [x + n - x] = [n] \subseteq N$.

$3 \Rightarrow 1$**:** Let $\mathbf{N} \trianglelefteq \mathbf{G}$. Suppose that $x, y \in G$ and $y - x \in N$. Then there is an element $n \in N$, such that $y = x + n$. Hence $\varphi(y) - \varphi(x) = \varphi(x + n) - \varphi(x) \in N$.

□

Sometimes we want to express that a function respects a certain normal subgroup, especially when it comes to generating near rings of compatible functions.

2.5. Notation. Let $\mathbf{N}$ be a fixed normal subgroup of $\mathbf{G}$. Then $\mathrm{Comp}_{\mathbf{N}}(\mathbf{G})$ denotes the near ring of all functions on $\mathbf{G}$ compatible with $\mathbf{N}$.

With this notation,

$$\mathbf{C}(\mathbf{G}) = \bigcap_{\mathbf{N} \trianglelefteq \mathbf{G}} \mathrm{Comp}_{\mathbf{N}}(\mathbf{G}). \tag{2.1}$$

The key to a more efficient computation of compatible functions on a group is the following lemma, which allows us to select a (small) subset of normal subgroups for the intersection. Moreover, one may understand it as a technical lemma, very helpful in some of the following proofs.

2.6. Lemma. *Let* $\mathbf{G}$ *be a group,* $\mathbf{I}$ *and* $\mathbf{J}$ *two normal subgroups of* $\mathbf{G}$. *Then the following inclusions hold*

$$\mathrm{Comp}_{\mathbf{I}}(\mathbf{G}) \cap \mathrm{Comp}_{\mathbf{J}}(\mathbf{G}) \subseteq \mathrm{Comp}_{\mathbf{I}\cap\mathbf{J}}(\mathbf{G})$$
$$\mathrm{Comp}_{\mathbf{I}}(\mathbf{G}) \cap \mathrm{Comp}_{\mathbf{J}}(\mathbf{G}) \subseteq \mathrm{Comp}_{\mathbf{I}+\mathbf{J}}(\mathbf{G})$$

Proof. Let $\varphi \in \mathrm{Comp}_{\mathbf{I}}(\mathbf{G}) \cap \mathrm{Comp}_{\mathbf{J}}(\mathbf{G})$.
Take $x, y \in G$ such that $x - y \in I \cap J$. Then $\varphi(x) - \varphi(y) \in I$ and analogously $\varphi(x) - \varphi(y) \in J$, wherefore $\varphi(x) - \varphi(y) \in I \cap J$. So $\varphi \in \mathrm{Comp}_{\mathbf{I}\cap\mathbf{J}}(G)$.
For the "+" part, we notice that

$$\varphi \in \mathrm{Comp}_{\mathbf{N}}(\mathbf{G}) \iff \forall x \in G\ \forall n \in N\ \varphi(x+n) - \varphi(x) \in N.$$

Consequently, for $i \in I$ and $j \in J$,
$\varphi(x + (i + j)) - \varphi(x) = \underbrace{\varphi((x + i) + j) - \varphi(x + i)}_{\in J} + \underbrace{\varphi(x + i) - \varphi(x)}_{\in I} \in I + J.$ □

A nice characterisation of compatibility in terms of interpolation with polynomial functions is the following.

2.7. Definition. Let $\mathbf{N} \leq \mathbf{M}(\mathbf{G})$. The near ring $\mathrm{L}_n\mathbf{N}$ is the near ring of all functions $f : G \to G$ for which for arbitrary $g_1, \ldots, g_n \in G$ there exists a function $p \in N$ such that $p(g_i) = f(g_i)$ for all $1 \leq i \leq n$.

2.8. Theorem ([Pilz, 1983, Proposition 7.131]).

$$\mathbf{C}(\mathbf{G}) = \mathrm{L}_2\mathrm{P}(\mathbf{G})$$

2. Quotients of a group

If $\mathbf{G}$ is a simple group, every function on $\mathbf{G}$ is polynomial.

2.9. PROPOSITION. *Let* $\mathbf{G}$ *be a group, then*

$$\mathbf{G} \text{ is simple } \iff \mathbf{C}(\mathbf{G}) = \mathbf{M}(\mathbf{G})$$

PROOF. By definition, every function is compatible with the normal subgroups $\{0\}$ and $\mathbf{G}$. □

There is a natural way to "project" a polynomial function to a quotient of a group (c.f. the proof of Proposition1.36), simply project the coefficients. Compatible functions share this property.

2.10. DEFINITION. Let $\mathbf{G}$ be a group and $\mathbf{N}$ a normal subgroup of $\mathbf{G}$. Every right inverse of the natural epimorphism from $\mathbf{G}$ onto $\mathbf{G}/\mathbf{N}$ is called a **lifting** of $\mathbf{G}/\mathbf{N}$. For a fixed complete set R of coset representatives of $\mathbf{N}$ in $\mathbf{G}$, we call the unique lifting of $\mathbf{G}/\mathbf{N}$ with range R the **R-lifting of $\mathbf{G}/\mathbf{N}$** .

2.11. LEMMA. *For* $\varphi \in \mathrm{C}(\mathbf{G})$ *and* $\mathbf{N} \trianglelefteq \mathbf{G}$ *we define*

$$\begin{aligned} \varphi^{\mathbf{N}} : G/N &\to G/N \\ g + \mathbf{N} &\mapsto \varphi(g) + \mathbf{N} \end{aligned}$$

This function is compatible on $\mathbf{G}/\mathbf{N}$. *The mapping* $\varphi \mapsto \varphi^{\mathbf{N}}$ *is a near ring homomorphism from* $\mathbf{C}(\mathbf{G})$ *to* $\mathbf{C}(\mathbf{G}/\mathbf{N})$, *its kernel is the Noetherian quotient*[1] $(\mathbf{N} : \mathbf{G})_{\mathbf{C}(\mathbf{G})}$ *and*

$$|\mathbf{C}(\mathbf{G})| \leq |\mathbf{C}(\mathbf{G}/\mathbf{N})| \cdot |(\mathbf{N} : \mathbf{G})_{\mathbf{C}(\mathbf{G})}|$$

PROOF. The function $\varphi^{\mathbf{N}}$ is well-defined, since for $a - b \in N$, $\varphi(a) - \varphi(b) \in N$, so $\varphi^{\mathbf{N}}(a) = \varphi(a) + \mathbf{N} = \varphi(b) + \mathbf{N} = \varphi^{\mathbf{N}}(b)$. Let h be the natural epimorphism from $\mathbf{G}$ onto $\mathbf{G}/\mathbf{N}$ and $\mathbf{I}$ be a normal subgroup of $\mathbf{G}/\mathbf{N}$. By the diamond lemma, there is a normal subgroup $\bar{\mathbf{I}}$ of $\mathbf{G}$, such that $h(\bar{I}) = I$. Suppose that for $a, b \in G$, $(a+\mathbf{N}) - (b+\mathbf{N}) \in I$. Then $a - b \in \bar{I}$, whence $\varphi(a) - \varphi(b) \in \bar{I}$ and $\varphi^{\mathbf{N}}(a + \mathbf{N}) - \varphi^{\mathbf{N}}(b + \mathbf{N}) = \varphi(a) - \varphi(b) + \mathbf{N} \in I$. The mapping $\varphi \mapsto \varphi^{\mathbf{N}}$ is a homomorphism:

$$\begin{aligned} (\varphi + \psi)^{\mathbf{N}}(g + \mathbf{N}) &= (\varphi + \psi)(g) + \mathbf{N} \\ &= \varphi^{\mathbf{N}}(g + \mathbf{N}) + \psi^{\mathbf{N}}(g + \mathbf{N}) \end{aligned}$$

[1] c.f. Pilz [1983]

and

$$\begin{aligned}\varphi^{\mathbf{N}} \circ \psi^{\mathbf{N}}(g + \mathbf{N}) &= \varphi^{\mathbf{N}}(\psi(g) + \mathbf{N}) \\ &= \varphi \circ \psi(g) + \mathbf{N} \\ &= (\varphi \circ \psi)^{\mathbf{N}}(g + \mathbf{N}).\end{aligned}$$

Its kernel consists of all functions in $\mathbf{C}(\mathbf{G})$ with range contained in $\mathbf{N}$. □

In Section 4, we will discuss, when this homomorphism $\varphi \mapsto \varphi^{\mathbf{N}}$ is surjective.

We find a different point of view in Theorem 2.12. Given $\mathbf{N} \trianglelefteq \mathbf{G}$, every compatible function on $\mathbf{G}$ can be built from a compatible function on the quotient $\mathbf{G}/\mathbf{N}$ and a function mapping G into N.

2.12. Theorem (Lausch and Nöbauer [1976]). *Let $\mathbf{G}$ be a finite group, $\mathbf{N}$ a normal subgroup of index s in $\mathbf{G}$. Let $R = \{r_1, \dots, r_s\}$ be a complete set of coset representatives of $\mathbf{N}$ in $\mathbf{G}$ and λ the R-lifting of $\mathbf{G}/\mathbf{N}$. Then for each $\varphi \in \mathrm{C}(\mathbf{G})$ and $i \in \{1, \dots, s\}$ there exist $\psi \in C(\mathbf{G}/\mathbf{N})$ and $\pi_i \in \mathrm{M}(\mathbf{N})$, such that for all $n \in N$*

$$\varphi(r_i + n) = \lambda \circ \psi(r_i + \mathbf{N}) + \pi_i(n).$$

Proof. Let $\varphi \in \mathrm{C}(\mathbf{G})$ and $\psi = \varphi^{\mathbf{N}}$. We fix an arbitrary $1 \leq i \leq s$. There exists an $n_i \in N$ such that $\varphi(r_i) = \lambda \circ \psi(r_i + \mathbf{N}) + n_i$. Since φ maps cosets of $\mathbf{N}$ into cosets of $\mathbf{N}$, there is a function $\rho_i \in \mathrm{M}(\mathbf{N})$ such that $\varphi(r_i + n) = \varphi(r_i) + \rho_i(n)$. So we have $\varphi(r_i + n) = \lambda \circ \psi(r_i + \mathbf{N}) + n_i + \rho_i(n)$. We choose $\pi_i : n \mapsto n_i + \rho_i(n) \in \mathrm{M}(\mathbf{N})$. □

If the normal subgroup $\mathbf{N}$ has the very special property, that every other normal subgroup of $\mathbf{G}$ is either contained in $\mathbf{N}$ or contains $\mathbf{N}$, it is possible to characterize the function mapping $\mathbf{G}$ into $\mathbf{N}$, and even to say a little bit more.

2.13. Theorem ([Dorda, 1977, Satz 2]). *Let $\mathbf{G}$ be a group, $\mathbf{N}$ a normal subgroup of index s which is a member of every chief series of $\mathbf{G}$. With the notation of Theorem 2.12, we state: For each $\varphi \in \mathrm{C}(\mathbf{G})$ and $i \in \{1, \dots, s\}$, there exist $\pi_i \in \mathrm{M}(\mathbf{N})$, compatible with all normal subgroups of $\mathbf{G}$ contained in $\mathbf{N}$, and $\psi \in \mathrm{C}(\mathbf{G}/\mathbf{N})$, such that*

$$\varphi(r_i + n) = \lambda \circ \psi(r_i + \mathbf{N}) + \pi_i(n).$$

Conversely, any such function is a compatible function on $\mathbf{G}$.

Proof. By Theorem 2.12, φ can be written in the form

$$\varphi(r_i + n) = \lambda \circ \psi(r_i + \mathbf{N}) + \pi_i(n).$$

It remains to show that each π_i is compatible with all normal subgroups of $\mathbf{G}$ contained in $\mathbf{N}$. Let $\mathbf{M}$ be a normal subgroup contained in $\mathbf{N}$. Fix an arbitrary $i \in \{1, \dots, s\}$ and $n_1, n_2 \in N$ with $n_1 - n_2 \in M$. Then $(r_i + n_1) - (r_i + n_2) \in M$

and $\varphi(r_i + n_1) - \varphi(r_i + n_2) \in M$, since φ is compatible. From $\varphi(r_i + n_1) = \lambda \circ \psi(r_i + \mathbf{N}) + \pi_i(n_1)$ and $\varphi(r_i + n_2) = \lambda \circ \psi(r_i + \mathbf{N}) + \pi_i(n_2)$, we see that also $\pi_i(n_1) - \pi_i(n_2) \in M$.
To show the converse, let φ be a function of the above form, $\mathbf{M}$ a nontrivial normal subgroup of $\mathbf{G}$ and $g, h \in G$ two elements, such that $g - h \in M$. We distinguish two cases.

1. $M \supseteq N$: We can find coset representatives r_{i_g} and r_{i_h} and $n_g, n_h \in N$, such that $g = r_{i_g} + n_g$ and $h = r_{i_h} + n_h$. Since $N \subseteq M$, $\mathbf{M}/\mathbf{N} \trianglelefteq \mathbf{G}/\mathbf{N}$, and (modulo $\mathbf{M}$)

$$\begin{aligned}
\varphi(g) &= \varphi(r_{i_g} + n_g) \\
&= \lambda \circ \psi(r_{i_g} + \mathbf{N}) + \pi_{i_g}(n_g) \\
&\equiv \lambda \circ \psi(g + \mathbf{N}) \quad (\pi_{i_g}(n_g) \in N \subseteq M) \\
&\equiv \lambda \circ \psi(h + \mathbf{N}) \quad (g \equiv h \text{ and } \psi \text{ is compatible}) \\
&\equiv \lambda \circ \psi(r_{i_h} + \mathbf{N}) + \pi_{i_h}(n_h) \\
&= \varphi(h)
\end{aligned}$$

2. $M \subseteq N$: We can find a coset representative r_i and elements $n \in N$ and $m \in M$ such that $g = r_i + n$ and $h = r_i + n + m$. Then (modulo $\mathbf{M}$)

$$\begin{aligned}
\varphi(g) &= \varphi(r_i + n) \\
&= \lambda \circ \psi(r_i + \mathbf{N}) + \pi_i(n) \\
&\equiv \lambda \circ \psi(r_i + \mathbf{N}) + \pi_i(n + m) \\
&= \varphi(h),
\end{aligned}$$

   because π_i is compatible with $\mathbf{M}$.

So finally, φ is compatible on $\mathbf{G}$. □

We will often refer to the last theorem in the special case where all normal subgroups of $\mathbf{N}$ are normal in $\mathbf{G}$.

2.14. Corollary. *Let $\mathbf{G}$ be a group, $\mathbf{N}$ a normal subgroup of index s that is a member of every chief series of $\mathbf{G}$. Suppose that every normal subgroup of $\mathbf{N}$ is normal in $\mathbf{G}$. Then with the notation from Theorem 2.12, we state: For each $\varphi \in \mathrm{C}(\mathbf{G})$ and $i \in \{1, \dots, s\}$, there exist $\psi \in \mathrm{C}(\mathbf{G}/\mathbf{N})$ and $\pi_i \in \mathrm{C}(\mathbf{N})$, such that*

$$\varphi(r_i + n) = \lambda \circ \psi(r_i + \mathbf{N}) + \pi_i(n).$$

Conversely, any such function is a compatible function on $\mathbf{G}$, whence

$$|\mathbf{C}(\mathbf{G})| = |\mathbf{C}(\mathbf{G}/\mathbf{N})| \cdot |\mathbf{C}(\mathbf{N})|^{[\mathbf{G}:\mathbf{N}]}$$

The following result is older than the previous two, which in fact are a later generalization. I find it convenient to present it as a corollary.

2.15. Corollary (Lausch and Nöbauer [1976]). *Let* $\mathbf{G}$ *be a finite group with unique minimal normal subgroup* $\mathbf{N}$. *Then every function of the form given in Theorem 2.12 is compatible.*

Proof. The normal subgroup $\mathbf{N}$ is part of every composition series of $\mathbf{G}$ and no nontrivial normal subgroup of $\mathbf{G}$ is properly contained in $\mathbf{N}$. □

The following corollary is useful in following proofs. It says that functions constructed in the Lausch–Nöbauer-Dorda way are "by construction compatible with the old normal subgroups".

2.16. Corollary. *Let* $\mathbf{N} \trianglelefteq \mathbf{G}$ *and* ψ *be a compatible function on* $\mathbf{G}/\mathbf{N}$. *For* $1 \leq i \leq n$ *let* π_i *be an arbitrary function from* N *to* N. *Then the function*

$$\varphi(r_i + n) := \lambda \circ \psi(r_i + \mathbf{N}) + \pi_i(n)$$

is compatible with all normal subgroups of $\mathbf{G}$ *containing* $\mathbf{N}$.

Proof. Follows from the first part of the proof of Theorem 2.13. □

The strong relation between the functions φ and ψ in the last theorems and lemmata can be expressed as simple as

$$\psi = \varphi^{\mathbf{N}}$$

To see this, suppose that for $i \in \{1, \dots, s\}$, $\varphi^{\mathbf{N}}(r_i + \mathbf{N}) = r_j + \mathbf{N}$. Since $\pi_i \in \mathrm{M}(\mathbf{N})$, φ maps r_i into the coset $r_j + \mathbf{N}$. Hence $\psi(r_i + \mathbf{N}) = r_j + \mathbf{N}$, so $\psi = \varphi^{\mathbf{N}}$.

We conclude this section with a small lemma, which will be needed later.

2.17. Lemma. *Let* $\mathbf{M} \leq \mathbf{N}$ *be two normal subgroups of the group* $\mathbf{G}$, *and* φ *a function on* $\mathbf{G}$ *compatible with* $\mathbf{M}$ *and* $\mathbf{N}$. *Then*

$$(\varphi^{\mathbf{M}})^{\mathbf{N}/\mathbf{M}} = \varphi^{\mathbf{N}}$$

Proof. The function $\varphi^{\mathbf{M}}$ maps $x + \mathbf{M}$ to $\varphi(x) + \mathbf{M}$, so $(\varphi^{\mathbf{M}})^{\mathbf{N}/\mathbf{M}}$ maps $(x + \mathbf{M}) + \mathbf{N}/\mathbf{M}$ to $\varphi(x) + \mathbf{M} + \mathbf{N}/\mathbf{M}$, or equivalently, it maps $x + \mathbf{N}$ to $\varphi(x) + \mathbf{N}$. So does $\varphi^{\mathbf{N}}$. □

These few results will suffice to characterize compatible functions on generalized quaternion groups, symmetric groups, holomorphs of simple abelian groups, certain dihedral and quaternion groups. Before we have a look at these examples, we are going to gather a few more results. The existence of a normal subgroup which is a member of every chief series is a rather restrictive condition. We are now going to look in which direction we can expand. First we will study direct products. Afterwards, distributivity will be our main point of interest.

3. Direct Products of groups

Among the first discoveries in the area of compatible functions has been the following: every compatible function on a direct product of two groups decomposes into two compatible functions.

2.18. LEMMA (Lausch and Nöbauer [1976]). *Let* $\mathbf{G}$ *and* $\mathbf{H}$ *be two groups. For every compatible function* φ *on* $\mathbf{G} \times \mathbf{H}$*, there exist functions* $\varphi_G \in \mathrm{C}(\mathbf{G})$ *and* $\varphi_H \in \mathrm{C}(\mathbf{H})$ *such that for all* $g \in G$ *and* $h \in H$*, the following holds:*

$$\varphi((g,h)) = (\varphi_G(g), \varphi_H(h)) \tag{2.2}$$

PROOF. Choose $\varphi_G := \pi_G \circ \varphi \circ e_G$, where π_G is the projection of $\mathbf{G} \times \mathbf{H}$ onto $\mathbf{G}$ and e_G is the embedding of $\mathbf{G}$ into $\mathbf{G} \times \mathbf{H}$, and choose φ_H analogously. □

Like zero-symmetric polynomial functions, also zero-symmetric compatible functions on direct products can be decomposed.

2.19. LEMMA. *Let* $\mathbf{G}$ *and* $\mathbf{H}$ *be two arbitrary groups. For every zero-symmetric, compatible function* φ *on* $\mathbf{G} \times \mathbf{H}$ *and for all* $g \in G$ *and* $h \in H$*, the following holds:*

$$\varphi((g,h)) = \varphi((g,0)) + \varphi((0,h)) \tag{2.3}$$

PROOF. Let (g,h) be an arbitrary, but fixed element of $G \times H$. Then there exists a zero-symmetric polynomial function $p_{g,h}$ (depending on g and h) s. t.

$$\varphi((g,h)) = p_{g,h}((g,h))$$

and by (1.9),

$$= p_{g,h}((g,0)) + p_{g,h}((0,h))$$

In the same way, we get a zero-symmetric polynomial function $p_{g,0}$ s. t.

$$\varphi((g,0)) = p_{g,0}((g,0))$$

Now,

$$\varphi((g,h)) - \varphi((g,0)) = p_{g,h}((g,0)) + p_{g,h}((0,h)) - p_{g,0}((g,0))$$

By Proposition 2.4, $\varphi((g,h)) - \varphi((g,0)) \in [(0,h)]$. Therefore

$$p_{g,h}((g,0)) = p_{g,0}((g,0)) = \varphi((g,0)).$$

Interchanging the roles of g and h, we get $p_{g,h}((0,h)) = \varphi((0,h))$ and finally the desired equation (2.3). □

It is natural to ask, under which conditions the converse of Lemma 2.18 holds. In Pilz [1980], a direct product $\mathbf{G}\times\mathbf{H}$ of two groups is called **nice**, iff every function φ obtained from two compatible functions on $\mathbf{G}$ and $\mathbf{H}$ like in (2.2) is compatible. Nice direct products can be nicely characterized.

2.20. Proposition. *Let* $\mathbf{G}$ *and* $\mathbf{H}$ *be two groups. Then the following are equivalent:*

1. *Every normal subgroup of* $\mathbf{G}\times\mathbf{H}$ *is* $\mathbf{G}$-$\mathbf{H}$*–decomposable.*
2. *The direct product* $\mathbf{G}\times\mathbf{H}$ *is nice.*
3. *The near rings* $\mathbf{C}(\mathbf{G}\times\mathbf{H})$ *and* $\mathbf{C}(\mathbf{G})\times\mathbf{C}(\mathbf{H})$ *are isomorphic.*

Proof. The equivalence $2\Leftrightarrow 3$ is clear from the definitions. A proof for $1\Rightarrow 2$ can be found in [Pilz, 1980, Proposition 2.8]. It remains to show $2\Rightarrow 1$.

Let $\mathbf{N}\trianglelefteq\mathbf{G}\times\mathbf{H}$.

Firstly, $I := \{g \mid (g,0)\in N\}$ is a normal subgroup of $\mathbf{G}$ and $J := \{h \mid (0,h)\in N\}$ is a normal subgroup of $\mathbf{H}$, since they are the images of $\mathbf{N}$ under the projections of $\mathbf{G}\times\mathbf{H}$ onto $\mathbf{G}$ and $\mathbf{H}$ respectively.

Secondly, for every $\mathbf{N}\trianglelefteq\mathbf{G}\times\mathbf{H}$, if for some $g\in G$, $h\in H$, $(g,h)\in N$, then also $(g,0)\in N$: suppose $(g,h)\in N$. Let φ be the identity function on $\mathbf{G}$, ψ be the 0-function on $\mathbf{H}$. Both functions are polynomial whence compatible. Since $\mathbf{G}\times\mathbf{H}$ is nice, the composed function $\xi : (g,h)\mapsto(\varphi(g),\psi(h))$ is compatible on $\mathbf{G}\times\mathbf{H}$. Now $(g,0)-(0,-h)=(g,h)\in N$, thus $\xi((g,0))-\xi((0,-h))\in N$. But $\xi((g,0))-\xi((0,-h))=(g,0)-(0,0)=(g,0)$. So $\mathbf{N}=\mathbf{I}\times\mathbf{J}$. □

Recall, that by Theorem 1.33, also the near rings $\mathbf{P}(\mathbf{G}\times\mathbf{H})$ and $\mathbf{P}(\mathbf{G})\times\mathbf{P}(\mathbf{H})$ are isomorphic, if and only if every normal subgroup of $\mathbf{G}\times\mathbf{H}$ is $\mathbf{G}$-$\mathbf{H}$–decomposable.

Now, we ask, what direct products of groups are nice, or with other words, where do skew congruences come from. If $\mathbf{G}$ and $\mathbf{H}$ have coprime order, everything is behaving nice.

2.21. Theorem (Lausch and Nöbauer [1976]). *For any two groups* $\mathbf{G}$ *and* $\mathbf{H}$ *with* $(|\mathbf{G}|,|\mathbf{H}|)=1$*, the direct product* $\mathbf{G}\times\mathbf{H}$ *is nice.*

Proof. By Lemma 2.18, every compatible function φ on $\mathbf{G}\times\mathbf{H}$ can be written as $\varphi((g,h))=(\varphi_G(g),\varphi_H(h))$, where $\varphi_G\in\mathrm{C}(\mathbf{G})$ and $\varphi_H\in\mathrm{C}(\mathbf{H})$. Every normal subgroup of $\mathbf{G}\times\mathbf{H}$ is the direct product of normal subgroups of $\mathbf{G}$ and $\mathbf{H}$ (since $(|\mathbf{G}|,|\mathbf{H}|)=1$), hence $\mathbf{G}$-$\mathbf{H}$–decomposable. Now Proposition 2.20 applies. □

For quasi-nilpotent groups, the condition in Theorem 2.21 is necessary for niceness:

2.22. Definition. We call a torsion group **G quasi-nilpotent**, iff

$$\forall p \in \mathbb{P}\ [(\exists g \in G\ \operatorname{ord}(g) = p) \implies (\exists \mathbf{N} \trianglelefteq \mathbf{G}\ \exists h \in N/[G,N]\ \operatorname{ord}(h) = p)]$$

In English: Whenever **G** has an element of prime order p, then there is a normal subgroup $\mathbf{N} \trianglelefteq \mathbf{G}$ such that $\mathbf{N}/[\mathbf{G},\mathbf{N}]$ has an element of order p.

Nilpotent torsion groups are quasi-nilpotent. The group $S_3 \times \mathbb{Z}_3$ is quasi-nilpotent, yet not nilpotent.

2.23. Corollary ([Miller, 1975, Corollary 3]). *If* **G** *and* **H** *are quasi-nilpotent groups, then* $\mathbf{G} \times \mathbf{H}$ *is nice, if and only if* $(|\mathbf{G}|, |\mathbf{H}|) = 1$.

The next step is to consider direct products, which are "almost nice", which means that they only have very few **G**-**H**-indecomposable normal subgroups.

2.24. Remark. For $d \geq 2$, every compatible function on the group $(\mathbb{Z}_p)^d$ is polynomial (see Corollary 3.3 in Chapter 3). For every polynomial function q on $(\mathbb{Z}_p)^d$, there is a unique integer $k \in \{0, \dots, p-1\}$ and an element $(c_1, \dots, c_d) \in (\mathbb{Z}_p)^d$, such that q is of the form

$$\begin{aligned} q : (x_1, \dots, x_d) &\mapsto k(x_1, \dots, x_d) + (c_1, \dots, c_d) \\ &= (kx_1 + c_1, \dots, kx_d + c_d) \\ &=: (q_1(x_1), \dots, q_d(x_d)). \end{aligned}$$

Recall, that k is the length of q as defined in Definition 1.8. We observe that the lengths of $q_1, \dots, q_d$ and q are equal.

2.25. Lemma. *Let* $\mathbf{G}_1$ *and* $\mathbf{G}_2$ *be two groups,* $\mathbf{N}_1 \trianglelefteq \mathbf{G}_1$ *and* $\mathbf{N}_2 \trianglelefteq \mathbf{G}_2$. *Let* $\mathbf{G} := \mathbf{G}_1 \times \mathbf{G}_2$ *and* $\mathbf{N} := \mathbf{N}_1 \times \mathbf{N}_2$. *Let* φ *be a compatible function on* **G**, *and let* φ_1 *and* φ_2 *be such that* $\forall (g_1, g_2) \in \mathbf{G}\ \varphi((g_1, g_2)) = (\varphi_1(g_1), \varphi_2(g_2))$. *Then*

$$\varphi^{\mathbf{N}}((g_1, g_2) + \mathbf{N}) = (\varphi_1^{\mathbf{N}_1}(g_1 + \mathbf{N}_1), \varphi_2^{\mathbf{N}_2}(g_2 + \mathbf{N}_2))$$

Proof.

$$\begin{aligned} \varphi^{\mathbf{N}}((g_1, g_2) + \mathbf{N}) &= \varphi((g_1, g_2)) + \mathbf{N} \\ &= (\varphi_1(g_1), \varphi_2(g_2)) + \mathbf{N} \\ &= (\varphi_1(g_1) + \mathbf{N}_1, \varphi_2(g_2) + \mathbf{N}_2) \\ &= (\varphi_1^{\mathbf{N}_1}(g_1 + \mathbf{N}_1), \varphi_2^{\mathbf{N}_2}(g_2 + \mathbf{N}_2)) \end{aligned}$$

□

As we already know from Theorem 2.21, $|\mathbf{C}(\mathbf{G} \times \mathbb{Z}_p)| = p^p \cdot |\mathbf{C}(\mathbf{G})|$, if p does not divide $|\mathbf{G}|$. Here is more:

2.26. Lemma. *Let* $\mathbf{G}$ *be a group with a unique normal subgroup* $\mathbf{N}$ *of index 2. If for every proper normal subgroup* $\mathbf{I}$ *of* $\mathbf{G}$, $|\mathbf{I}/[\mathbf{G},\mathbf{I}]|$ *is odd, then for* $d \geq 1$,

$$|\mathbf{C}(\mathbf{G} \times (\mathbb{Z}_2)^d)| = 2^d \cdot |\mathbf{C}(\mathbf{G})| = \frac{1}{2} \cdot |\mathbf{C}(\mathbf{G})| \cdot |\mathbf{C}(\mathbb{Z}_2)^d)|.$$

Proof. Let $\mathbf{N}$ be the normal subgroup of index 2 in $\mathbf{G}$ and $\varphi \in \mathrm{C}(\mathbf{G} \times (\mathbb{Z}_2)^d)$. Define $\mathbf{N}_0 := \mathbf{N} \times \{0\}^d \trianglelefteq \mathbf{G} \times (\mathbb{Z}_2)^d$. There exist functions $\varphi_1 \in \mathrm{C}(\mathbf{G})$ and $\varphi_2 \in \mathrm{C}((\mathbb{Z}_2)^d)$ (by Theorem 2.36 or later by Corollary 3.3, $\mathbf{C}((\mathbb{Z}_2)^d) = \mathbf{P}((\mathbb{Z}_2)^d)$), such that for all $(g,z) \in G \times (\mathbb{Z}_2)^d$, $\varphi((g,z)) = (\varphi_1(g), \varphi_2(z))$. The quotient $\mathbf{G}/\mathbf{N}$ is abelian of order 2, hence the quotient $\mathbf{H} := (\mathbf{G} \times (\mathbb{Z}_2)^d)/\mathbf{N}_0$ is isomorphic to the elementary abelian group $(\mathbb{Z}_2)^{d+1}$. By Lemma 2.25, the function $\varphi^{\mathbf{N}_0}$ fulfills

$$\varphi^{\mathbf{N}_0}((g,z) + \mathbf{N}_0) = (\varphi_1^{\mathbf{N}}(g + \mathbf{N}), \varphi_2^{\{0\}^d}(z + \{0\}^d)).$$

Since $(\mathbb{Z}_2)^d$ is 1-affine complete, $\varphi_2^{\{0\}^d}$ is polynomial. The function $\varphi_1^{\mathbf{N}}$ is also polynomial: combining Lemmata 2.17 and 2.25, we may understand this function as the first coordinate of the function $\varphi^{\mathbf{N}_0}$, which is polynomial, because $(\mathbf{G} \times (\mathbb{Z}_2)^d)/\mathbf{N}_0 \cong (\mathbb{Z}_2)^{d+1}$ is 1-affine complete. Hence, its first coordinate function must also be polynomial. So by Remark 2.24, $\varphi_1^{\mathbf{N}}$ and $\varphi_2^{\{0\}^d}$ have the same length, and $\varphi_1^{\mathbf{N}}$ determines $\varphi_2^{\{0\}^d} = \varphi_2$ up to a constant. Hence there are at most $2^d \cdot |\mathbf{C}(\mathbf{G})|$ compatible functions on $\mathbf{G} \times (\mathbb{Z}_2)^d$.

The quotient $\mathbf{G}/\mathbf{N}$ is 1-affine complete. It remains to show that every function of the form (φ_1, φ_2), where φ_2 and $\varphi_1^{\mathbf{N}}$ have the same length, is compatible. By Theorem 0.13, the normal subgroups of $\mathbf{G} \times (\mathbb{Z}_2)^d$ are exactly the direct products of normal subgroups of $\mathbf{G}$ with normal subgroups of $(\mathbb{Z}_2)^d$, and the normal subgroups between $\mathbf{G} \times (\mathbb{Z}_2)^d$ and $\mathbf{N}_0$. (Remember that $\mathbf{G} \times (\mathbb{Z}_2)^d/\mathbf{N}_0 \cong (\mathbb{Z}_2)^{d+1}$.) Let $\mathbf{M}$ be a normal subgroup of $\mathbf{G} \times (\mathbb{Z}_2)^d$.

- If $\mathbf{M}$ is one of the normal subgroups between $\mathbf{G} \times (\mathbb{Z}_2)^d$ and $\mathbf{N}_0$, then by our construction, Corollary 2.16 applies and φ is compatible with $\mathbf{M}$.
- $\mathbf{M} = \mathbf{M}_1 \times \mathbf{M}_2$ for a normal subgroup $\mathbf{M}_1$ of $\mathbf{G}$ and a normal subgroup $\mathbf{M}_2$ of $(\mathbb{Z}_2)^d$: Let $(g,z) - (g',z') \in M$, i.e., $g - g' \in M_1$ and $z - z' \in M_2$. Then

  $$\varphi((g,z)) - \varphi((g',z')) = (\varphi_1(g) - \varphi_1(g'), \varphi_2(z) - \varphi_2(z'))$$

  Since φ_1 is compatible on $\mathbf{G}$ and φ_2 is compatible on $(\mathbb{Z}_2)^d$, this difference is in M.

□

4. Liftings

In this section, we discuss, under which circumstances every compatible function ψ on a quotient $\mathbf{G}/\mathbf{N}$ can be lifted to $\mathbf{G}$, i.e., when there is a compatible

function φ on $\mathbf{G}$, such that $\varphi^{\mathbf{N}} = \psi$. In this case the number of compatible functions on $\mathbf{G}$ can be computed as

$$|\mathbf{C}(\mathbf{G})| = |\mathbf{C}(\mathbf{G}/\mathbf{N})| \cdot |(\mathbf{N} : \mathbf{G})_{\mathbf{C}(\mathbf{G})}|.$$

2.27. Definition. Let $\mathbf{G}$ be a group. A normal subgroup $\mathbf{N}$ of $\mathbf{G}$ **admits lifting of compatible functions**, iff every compatible function ψ on the quotient $\mathbf{G}/\mathbf{N}$ can be lifted to $\mathbf{G}$, i.e.,

$$\forall \psi \in \mathrm{C}(\mathbf{G}/\mathbf{N})\ \exists \varphi \in \mathrm{C}(\mathbf{G}) \quad \varphi^{\mathbf{N}} = \psi.$$

4.1. N is the unique minimal normal subgroup of G.

If $\mathbf{N}$ is the unique minimal normal subgroup of $\mathbf{G}$, then, by Corollary 2.15, it admits lifting of compatible functions: let π be the natural epimorphism from $\mathbf{G}$ to $\mathbf{G}/\mathbf{N}$ and λ a lifting of $\mathbf{G}/\mathbf{N}$. Then for $\psi \in \mathrm{C}(\mathbf{G}/\mathbf{N})$, we may choose $\varphi := \lambda \circ \psi \circ \pi \in \mathrm{C}(\mathbf{G})$ to get $\varphi^{\mathbf{N}} = \psi$.

4.2. 1-affine complete quotients.

2.28. Lemma. *If $\mathbf{G}/\mathbf{N}$ is 1-affine complete, then $\mathbf{N}$ admits lifting of compatible functions.*

Proof. Every compatible function on the 1-affine complete group $\mathbf{G}/\mathbf{N}$ is polynomial, so by Lemma 1.36, it can can be lifted to a polynomial function on $\mathbf{G}$. □

4.3. Noetherian quotients.

If every compatible function on a quotient $\mathbf{G}/\mathbf{A}$ can be lifted, we can assemble every compatible function on $\mathbf{G}$ from a compatible function on the quotient and a compatible function on $\mathbf{G}$ mapping G into A. We study now the Noetherian quotients $(\mathbf{A} : \mathbf{G})_{\mathbf{C}(\mathbf{G})}$. The sum $\mathbf{K}$ of all normal subgroups not containing the minimal normal subgroup $\mathbf{A}$ turns out to play an important role.

2.29. Theorem. *Let $\mathbf{G}$ be a group, $\mathbf{A}$ a minimal normal subgroup of $\mathbf{G}$. Define $\mathbf{K}$ to be the sum of all normal subgroups having trivial intersection with $\mathbf{A}$. Then the functions in $(\mathbf{A} : \mathbf{G})_{\mathbf{C}(\mathbf{G})}$ are precisely the functions which are constant on the cosets of $\mathbf{K}$ in $\mathbf{G}$.*

If $\mathbf{A}$ is a minimal normal subgroup, then $\mathbf{A}$ admits lifting of compatible functions, if and only if

$$|\mathbf{C}(\mathbf{G})| = |\mathbf{C}(\mathbf{G}/\mathbf{A})| \cdot |\mathbf{A}|^{[\mathbf{G}:\mathbf{K}]}.$$

Proof. Let φ be a compatible function with $\varphi(G) \subseteq A$. Let us consider a normal subgroup $\mathbf{N}$ of $\mathbf{G}$, with $A \cap N = \{0\}$. For $g, h \in G$ and $g - h \in N$, we have $\varphi(g) - \varphi(h) \in N \cap A = \{0\}$, forcing $\varphi(g) = \varphi(h)$. So φ is constant on the

cosets of every $\mathbf{N} \trianglelefteq \mathbf{G}$ with $N \cap A = \{0\}$. Let $\mathbf{N}_1$ and $\mathbf{N}_2$ be two such normal subgroups. Consider $\mathbf{S} := \mathbf{N}_1 + \mathbf{N}_2$. If $g - h \in S$, then $g = n_1 + n_2 + h$, and $\varphi(h) = \varphi(n_2 + h) = \varphi(n_1 + n_2 + h) = \varphi(g)$. Consequently, φ is constant on the cosets of $\mathbf{K}$.

Conversely, let φ be a function mapping G into A and let φ be constant on the cosets of $\mathbf{K}$. Then φ is compatible on $\mathbf{G}$: let $\mathbf{I} \trianglelefteq \mathbf{G}$. If $\mathbf{I} \geq \mathbf{A}$, then φ is compatible with $\mathbf{I}$, because $\varphi(G) \subseteq A \subseteq I$. If $\mathbf{I} \not\geq \mathbf{A}$, then by the definition of $\mathbf{K}$, $\mathbf{I} \leq \mathbf{K}$. So φ is compatible with $\mathbf{I}$, because it is constant on the cosets of $\mathbf{I}$.

There are precisely $|\mathbf{A}|^{[\mathbf{G}:\mathbf{K}]}$ functions mapping G into A, which are constant on the cosets of $\mathbf{K}$. The mapping $\Phi : \mathbf{C}(\mathbf{G}) \to \mathbf{C}(\mathbf{G}/\mathbf{A})$, $\varphi \mapsto \varphi^{\mathbf{A}}$ is a homomorphism with kernel $(\mathbf{A} : \mathbf{G})_{\mathbf{C}(\mathbf{G})}$. The normal subgroup $\mathbf{A}$ admits lifting of compatible functions, if and only if Φ is surjective, which holds, if and only if $|\mathbf{C}(\mathbf{G})| = |\mathbf{C}(\mathbf{G}/\mathbf{A})| \cdot |\mathbf{A}|^{[\mathbf{G}:\mathbf{K}]}$. □

4.4. The A-K-Theorem.

The **A**-**K**-Theorem is stated here with a bunch of technical premises, which are quite helpful in the proof. After a short outing to the realm of lattice theory, we will be able to reformulate the theorem. The **A**-**K**-Theorem may be understood as another generalization of Lausch and Nöbauer's Corollary 2.15.

2.30. Theorem (**A**-**K**-Theorem). *Let* $\mathbf{A}$ *be a minimal normal subgroup of* $\mathbf{G}$. *Suppose that* $\mathbf{G}$ *has a normal subgroup* $\mathbf{K}$, *such that* $A \cap K = \{0\}$ *and the lattice of normal subgroups of* $\mathbf{G}$ *is generated (w.r.t.* $\cap$ *and* $+$*) by* $\mathbf{K}$ *and the normal subgroups of* $\mathbf{G}$ *containing* $\mathbf{A}$. *Then*

$$|\mathbf{C}(\mathbf{G})| = |\mathbf{C}(\mathbf{G}/\mathbf{A})| \cdot |\mathbf{A}|^{[\mathbf{G}:\mathbf{K}]}.$$

Proof. For the following, we fix a complete set $R = \{r_1, \ldots, r_n\}$ of coset representatives of $\mathbf{A}$ in $\mathbf{G}$ ($n = [\mathbf{G} : \mathbf{A}]$) and λ, the R-lifting of $\mathbf{G}/\mathbf{A}$. Let φ be a compatible function on $\mathbf{G}$. For $g \in G$, we define $i(g)$ such that $\lambda(g + \mathbf{A}) = r_{i(g)}$, and define $a(g) = -\lambda(g + \mathbf{A}) + g$. Finally, let us write $\psi(g)$ for $\pi_{i(g)}(a(g))$. We may regard ψ as a function from G into A.

Let S be a complete set of coset representatives of $\mathbf{K}$ in $\mathbf{G}$. Let $x \in G$, and $s \in S$ be the coset representative of the coset of $\mathbf{K}$ containing x. Then $x - s \in K$ and by Theorem 2.12,

$$K \ni \varphi(x) - \varphi(s) = \lambda \circ \varphi^{\mathbf{A}}(x + \mathbf{A}) + \psi(x) - \psi(s) - \lambda \circ \varphi^{\mathbf{A}}(s + \mathbf{A}).$$

Conjugating with $\lambda \circ \varphi^{\mathbf{A}}(s + \mathbf{A})$ gives

$$\underbrace{-\lambda \circ \varphi^{\mathbf{A}}(s + \mathbf{A}) + \lambda \circ \varphi^{\mathbf{A}}(x + \mathbf{A})}_{=:d_x} + \psi(x) - \psi(s) \in K.$$

Since $\varphi^{\mathbf{A}}$ is compatible on $\mathbf{G}/\mathbf{A}$, $\lambda \circ \varphi^{\mathbf{A}}(x+\mathbf{A}) - \lambda \circ \varphi^{\mathbf{A}}(s+\mathbf{A}) \in A+K$, and conjugating with $\lambda \circ \varphi^{\mathbf{A}}(s+\mathbf{A})$ once more gives $d_x \in A+K$. $A \cap K = \{0\}$ implies that there exists exactly one $c_x \in A$, such that $d_x + c_x \in K$. The equation

$$\psi(x) - \psi(s) = c_x$$

uniquely determines $\psi(x)$, once that $\psi(s)$ is fixed. For fixed coset representatives and a fixed s, there are exactly $|\mathbf{A}|$ possibilities to send $a(s)$ to an element of A. Once $\psi(s)$ is fixed for all $s \in S$, it is determined for all $x \in G$. Since there are $[\mathbf{G} : \mathbf{K}]$ cosets of $\mathbf{K}$ in $\mathbf{G}$, there can be at most $|\mathbf{A}|^{[\mathbf{G}:\mathbf{K}]} \cdot |\mathbf{C}(\mathbf{G}/\mathbf{A})|$ distinct compatible functions.

It remains to be shown that for an arbitrary compatible function F on $\mathbf{G}/\mathbf{A}$ and arbitrary but fixed values for $\psi(s)$ ($s \in S$), every function φ of the form

$$\varphi(x) = \lambda \circ F(x+\mathbf{A}) + \psi(x),$$

where the values of ψ are chosen as described, is compatible. By Corollary 2.16 and Lemma 2.6, it suffices to check that φ is compatible with $\mathbf{K}$. Let $x, y \in s+\mathbf{K}$ for some $s \in S$. Then

$$\begin{aligned}
\varphi(x) - \varphi(y) &= \varphi(x) - \varphi(s) + \varphi(s) - \varphi(y) \\
&= \lambda \circ \varphi^{\mathbf{A}}(x+\mathbf{A}) + \psi(x) - \psi(s) - \lambda \circ \varphi^{\mathbf{A}}(s+\mathbf{A}) \\
&\quad + \lambda \circ \varphi^{\mathbf{A}}(s+\mathbf{A}) + \psi(s) - \psi(y) - \lambda \circ \varphi^{\mathbf{A}}(y+\mathbf{A}) \\
&= \underbrace{\lambda \circ \varphi^{A}(x+\mathbf{A}) + c_x - \lambda \circ \varphi^{\mathbf{A}}(s+\mathbf{A})}_{\in K} \\
&\quad + \underbrace{\lambda \circ \varphi^{\mathbf{A}}(s+\mathbf{A}) + c_y - \lambda \circ \varphi^{\mathbf{A}}(y+\mathbf{A})}_{\in K} \in K
\end{aligned}$$

□

4.5. Local distributivity.

We may reformulate Theorem 2.30 as follows:

2.31. THEOREM. *Let* $\mathbf{A}$ *be a minimal normal subgroup of* $\mathbf{G}$. *Suppose that* $\mathbf{G}$ *has a normal subgroup* $\mathbf{K}$, *such that* $A \cap K = \{0\}$ *and the lattice of normal subgroups of* $\mathbf{G}$ *is generated (w.r.t.* $\cap$ *and* $+$*) by* $\mathbf{K}$ *and the normal subgroups of* $\mathbf{G}$ *containing* $\mathbf{A}$. *Then every compatible function on* $\mathbf{G}/\mathbf{A}$ *can be lifted to* $\mathbf{G}$ *in precisely* $|\mathbf{A}|^{[\mathbf{G}:\mathbf{K}]}$ *ways.*

It is time now for a jaunt to lattice theory. The assumptions for $\mathbf{A}$ look very technical. The next theorem shows that they are equivalent to $\mathbf{A}$ being a distributive normal subgroup of $\mathbf{G}$, and that $\mathbf{K}$ is simply the sum of all normal subgroups of $\mathbf{G}$ not containing $\mathbf{A}$. But first of all, may I offer you a definition?

2.32. DEFINITION (Grätzer [1978]). An element a of a lattice is called **distributive**, iff for all elements x and y of the lattice

$$a \vee (x \wedge y) = (a \vee x) \wedge (a \vee y)$$

and **dually distributive**, iff the dual of this equality holds. The element a is **standard**, iff for all elements x and y of the lattice

$$x \wedge (a \vee y) = (x \wedge a) \vee (x \wedge y).$$

We call a normal subgroup **N** of a group **G** distributive, dually distributive or standard, if it has this property as an element of the lattice of normal subgroups of **G**.

The lattices of normal subgroups of a group is always modular. In this case there is no difference between all these notions, which I (we?) would certainly confuse anyway.

2.33. REMARK. [2] In a modular lattice $\mathcal{L}$, the following are equivalent for $a \in \mathcal{L}$:

1. a is distributive.
2. a is standard.
3. $\forall x, y \in \mathcal{L}$, the sub-lattice generated by a, x and y is distributive.
4. a is dually distributive.
5. for every $x \in \mathcal{L}$, a has at most 1 complement in the interval $\{y \in \mathcal{L} \mid x \wedge a \leq y \leq x \vee a\}$.

The distributive elements of a modular lattice $\mathcal{L}$ form a sub-lattice of $\mathcal{L}$.

Distributivity of an atom can be expressed in a very nice way.

2.34. LEMMA. *Let a be an in the lattice $\mathcal{L}$. Then the following are equivalent:*

(i) a is distributive.

(ii) For all $x, y \in \mathcal{L}$,

$$[a \wedge x = 0 \ \& \ a \wedge y = 0] \implies a \wedge (x \vee y) = 0$$

(iii) There exists an element $k \in \mathcal{L}$, such that $a \wedge k = 0$ and $\mathcal{L}$ is generated (w.r.t. $\wedge$ and $\vee$) by k and the elements of $\mathcal{L}$ containing a.

PROOF. We are going to show $(iii) \Rightarrow (ii) \Rightarrow (i)$ and $(i) \Rightarrow (ii) \Rightarrow (iii)$.

$(iii) \Rightarrow (ii)$ We assume that there is a $k \in \mathcal{L}$ not containing a which together with all the elements of $\mathcal{L}$ containing a generates the whole lattice $\mathcal{L}$. We show that every element of the sub-lattice of $\mathcal{L}$ generated by k and all elements containing a, is either contained in k or contains a. This will imply (ii) immediately.

[2] c.f. [Grätzer, 1978, p. 138-144], Grätzer and Schmidt [1961]

Joins and meets of elements containing a contain a. The only way to generate an element not containing a is to intersect elements containing a with k and add and intersect the results. What comes out is contained in k in this case.

$(ii) \Rightarrow (i)$ By Grätzer and Schmidt [1961], a is standard, if and only if

$$\forall\, x, y \in \mathcal{L} \quad x \leq a \vee y \implies x = (x \wedge a) \vee (x \wedge y). \tag{2.4}$$

If a is not distributive, this implication has to be false. The implication in (2.4) is always true, if any of the three elements is contained in any other of the three. So we may assume that (2.4) is false for some fixed pairwise incomparable a, x and y. So, $x \wedge a = 0$, and (2.4) says

$$x \leq a \vee y \implies x = x \wedge y,$$

or equivalently,

$$x \not\leq y \implies x \not\leq a \vee y.$$

So far, we have found out that a is not distributive, if and only if there are pairwise incomparable elements x, $y \not\geq a$, with $x \leq a \vee y$. It remains to show that $x \vee y \geq a$. We see that $y < x \vee y \leq a \vee y$, because $x \leq a \vee y$. Since a is an atom, there are no elements in $\mathcal{L}$ between 0 and a, hence there are no elements between y and $a \vee y$. So $x \vee y = a \vee y \geq a$.

$(i) \Rightarrow (ii)$ If a is distributive, then $a \wedge (x \vee y) = a \wedge x \vee a \wedge y = 0$.

$(ii) \Rightarrow (iii)$ We assume that a is distributive. Let k be the join of all $x \in \mathcal{L}$ with $x \wedge a = 0$. Then by (ii), $k \wedge a = 0$ and for any $a \not\leq x \in \mathcal{L}$, $(a \vee x) \wedge k = a \wedge k \vee x \wedge k = x$, because a is standard.

□

On the one hand, the previous lemma suggests a good algorithm for deciding distributivity. On the other hand it shows, that the technical premises of the **A**-**K**-Theorem are equivalent to the distributivity of **A**, and that **K** is simply the sum of the normal subgroups of **G** not containing **A**.

In particular, if the lattice of normal subgroups of a group **G** is distributive, every minimal normal subgroup **A** is distributive, whence every compatible function on $\mathbf{G}/\mathbf{A}$ can be lifted to **G**. As a consequence, this holds for every normal subgroup, and the lifting process of a function can be iterated.

There are groups having non-distributive minimal normal subgroups with non 1-affine-complete factor group admitting lifting of compatible functions. An example is the group $(\mathbb{Z}_2)^2 \times \mathbb{Z}_3$ with minimal normal subgroup $\mathbb{Z}_2 \times \{0\} \times \{0\}$, which can easily be checked using Theorem 2.29 and Corollary 2.39 (which is to follow).

4.6. Global distributivity.

2.35. THEOREM. *Let $s \in \mathbb{N}$ and $\mathbf{G}$ be a group having s minimal normal subgroups $\mathbf{M}_1, \dots, \mathbf{M}_s$, such that the normal subgroups of $\mathbf{G}$ contained in $\mathbf{M} := \sum_{i=1}^{s} \mathbf{M}_i$ form a distributive lattice. If all compatible functions on $\mathbf{G}/\mathbf{M}_i$ ($i \in \{1, \dots, s\}$) and $\mathbf{G}/\mathbf{M}$ can be lifted to compatible functions on $\mathbf{G}$, then*

$$|\mathbf{C}(\mathbf{G})| = \sqrt[s-1]{\frac{\prod_{i=1}^{s} |\mathbf{C}(\mathbf{G}/\mathbf{M}_i)|}{|\mathbf{C}(\mathbf{G}/(\sum_{i=1}^{s} \mathbf{M}_i))|}}$$

PROOF. We will show that

$$\times_{i=1}^{s} (\mathbf{M}_i : \mathbf{G})_{\mathbf{C}(\mathbf{G})} \cong (\mathbf{M} : \mathbf{G})_{\mathbf{C}(\mathbf{G})}. \tag{2.5}$$

Then by Lemma 2.11 and our liftability assumptions,

$$|\mathbf{C}(\mathbf{G})| = |\mathbf{C}(\mathbf{G}/\mathbf{M}_j)| \cdot |(\mathbf{M}_j : \mathbf{G})_{\mathbf{C}(\mathbf{G})}| = |\mathbf{C}(\mathbf{G}/\mathbf{M})| \cdot |(\mathbf{M} : \mathbf{G})_{\mathbf{C}(\mathbf{G})}|,$$

for each $j \in \{1, \dots, s\}$. Hence

$$\prod_{i=1}^{s} \frac{|\mathbf{C}(\mathbf{G})|}{|\mathbf{C}(\mathbf{G}/\mathbf{M}_i)|} = \frac{|\mathbf{C}(\mathbf{G})|}{\mathbf{C}(\mathbf{G}/\mathbf{M})}$$

and

$$|\mathbf{C}(\mathbf{G})|^{s-1} = \frac{\prod_{i=1}^{s} |\mathbf{C}(\mathbf{G}/\mathbf{M}_i)|}{|\mathbf{C}(\mathbf{G}/\mathbf{M})|}.$$

In order to verify equation (2.5), we show that the mapping

$$b : \times_{i=1}^{s} (\mathbf{M}_i : \mathbf{G})_{\mathbf{C}(\mathbf{G})} \to (\mathbf{M} : \mathbf{G})_{\mathbf{C}(\mathbf{G})}$$

$$(\varphi_1, \dots, \varphi_s) \mapsto \sum_{i=1}^{s} \varphi_i$$

is a (group) isomorphism.

We observe that for distinct $k, l \in \{1, \dots, s\}$, the functions from $(\mathbf{M}_k : \mathbf{G})_{\mathbf{C}(\mathbf{G})}$ and $(\mathbf{M}_l : \mathbf{G})_{\mathbf{C}(\mathbf{G})}$ commute (w.r.t. addition), i.e., for φ_k in $(\mathbf{M}_k : \mathbf{G})_{\mathbf{C}(\mathbf{G})}$ and φ_l in $(\mathbf{M}_l : \mathbf{G})_{\mathbf{C}(\mathbf{G})}$, we have $[\varphi_k, \varphi_l] = 0$, because this function maps G into $[M_k, M_l] \leq M_k \cap M_l = \{0\}$.

The mapping b is a homomorphism, since

$$\begin{aligned} b((\varphi_1, \dots, \varphi_s) + (\varphi'_1, \dots, \varphi'_s)) &= b((\varphi_1 + \varphi'_1, \dots, \varphi_s + \varphi'_s)) \\ &= \varphi_1 + \varphi'_1 + \cdots + \varphi_s + \varphi'_s \\ &= \sum_{i=1}^{s} \varphi_i + \sum_{i=1}^{s} \varphi'_i \\ &= b((\varphi_1, \dots, \varphi_s)) + b((\varphi'_1, \dots, \varphi'_s)). \end{aligned}$$

The mapping b is injective: suppose $(\varphi_1, \dots, \varphi_s) \in \ker b$, then $b((\varphi_1, \dots, \varphi_s)) = \sum_{i=1}^{s} \varphi_i = 0$, and consequently $\varphi_i = 0$ for each $i \in \{1, \dots, s\}$.
The mapping b is surjective: for $j \in \{1, \dots, s\}$, let π_j be the projection from M onto M_j, and for $\psi \in (\mathbf{M} : \mathbf{G})_{\mathbf{C}(\mathbf{G})}$, we define $\varphi_j := \pi_j \circ \psi$. It remains to show that $\varphi_j \in (\mathbf{M}_j : \mathbf{G})_{\mathbf{C}(\mathbf{G})}$.
By definition, $\varphi_j(G) \subseteq M_j$. We show that it is compatible. Let $\mathbf{N} \trianglelefteq \mathbf{G}$ be arbitrary and define $I_{\mathbf{N}} := \{i \in \{1, \dots, s\} \mid \mathbf{M}_i \leq \mathbf{N}\}$. For $g, h \in G$ and $g - h \in N$, $\psi(g) - \psi(h) \in N \cap M = \sum_{i \in I_{\mathbf{N}}} (M_i \cap N) = \sum_{i \in I_{\mathbf{N}}} M_i$. Finally,

$$\begin{aligned} \varphi_j(g) - \varphi_j(h) &= \pi_j \circ \psi(g) - \pi_j \circ \psi(h) \\ &= \pi_j \circ \underbrace{(\psi(g) - \psi(h))}_{\in \sum_{i \in I_{\mathbf{N}}} M_i} \in \begin{cases} M_j \leq N & \text{if } j \in I_{\mathbf{N}}, \\ \{0\} \leq N & \text{if } j \notin I_{\mathbf{N}} \end{cases}. \end{aligned}$$

□

This theorem allows to recursively compute the size of $\mathbf{C}(\mathbf{G})$ for a group $\mathbf{G}$ with distributive lattice of normal subgroups, but it does not show, what the compatible functions look like.

5. Examples

We continue this chapter with a small assemblage of examples. We start with abelian groups. The compatible functions on finite abelian groups have been characterized by Hans Lausch and Wilfried Nöbauer in Lausch and Nöbauer [1976]. A few examples then show, where the results in Dorda [1977] can be applied. Finally, we will mention some classes of groups, where the newer results can help. As a reward for our work, we will happen to find new 1-affine complete groups among the examples.

5.1. Abelian groups.

We give recursive formulae for the numbers of compatible functions on abelian p-groups.

5.1.1. Cyclic p-groups.

2.36. Theorem ([Lausch and Nöbauer, 1976, Folgerung 1]). *For all $n \geq 0$ the following equation holds.*

$$|\mathbf{C}(\mathbb{Z}_{p^n})| = \prod_{i=1}^{n} p^{p^i} = p^{p\frac{p^n-1}{p-1}} \tag{2.6}$$

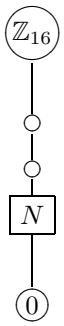

FIGURE 2.1. The lattice of normal subgroups of a cyclic p-group

PROOF. Let $\mathbf{G} = \mathbb{Z}_{p^n}$. The (normal) subgroup $\mathbf{N} = p^{n-1}\mathbf{G}$ is the unique minimal normal subgroup of $\mathbf{G}$. We see that $|\mathbf{N}| = p$ and $\mathbf{G}/\mathbf{N} \cong \mathbb{Z}_{p^{n-1}}$. Applying Corollary 2.15, we get

$$|\mathbf{C}(\mathbb{Z}_{p^n})| = |\mathbf{C}(\mathbb{Z}_{p^{n-1}})| \cdot p^{p^n}$$

From this recursion and $|\mathbf{C}(\mathbb{Z}_p)| = p^p$ we get the desired formula. □

5.1.2. Abelian p-groups.

2.37. THEOREM (Lausch and Nöbauer [1976]).
For all $s \in \mathbb{N}$, $m_1 \geq \cdots \geq m_s \in \mathbb{N}$ and $\mathbf{G} = \mathbb{Z}_{p^{m_1}} \times \cdots \times \mathbb{Z}_{p^{m_s}}$ the following holds:

$$|\mathbf{C}(\mathbf{G})| = |\mathbf{G}| \cdot p^{2m_2 - m_1} \cdot |\mathbf{C}(\mathbb{Z}_{p^{m_1 - m_2}})| \tag{2.7}$$

Moreover, with $\mathbf{N} = p^{m_2}\mathbf{G}$, e the natural epimorphism from $\mathbf{G}$ to $\mathbf{G}/\mathbf{N}$ and λ a lifting of $\mathbf{G}/\mathbf{N}$, the near ring $\mathbf{C}(\mathbf{G})$ consists exactly of the functions

$$x \mapsto p(x) + p^{m_2} \cdot \lambda(c(e(x))),$$

where $p \in \mathrm{P}(\mathbf{G})$ and $c \in \mathrm{C}(\mathbf{G}/\mathbf{N})$.

Together with Theorem 2.21, this theorem enables us to describe the compatible functions on every finite abelian group.

5.1.3. Cyclic groups.

2.38. COROLLARY. *Let $n = p_1^{\alpha_1} \dots p_s^{\alpha_s} \in \mathbb{N}$ ($i \neq j \implies p_i \neq p_j$). Then*

$$|\mathbf{C}(\mathbb{Z}_n)| = \prod_{i=1}^{s} p_i^{p_i \frac{p_i^{\alpha_i} - 1}{p_i - 1}}$$

PROOF. $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \ldots \times \mathbb{Z}_{p_s^{\alpha_s}}$. The result follows from Theorem 2.21 and Theorem 2.36. □

5.1.4. Abelian groups.

2.39. Corollary. *Let* $\mathbf{A} = \bigotimes_{i=1}^{s} \mathbf{G}_i$, *where* $\mathbf{G}_i \cong \bigotimes_{j=1}^{s_i} \mathbb{Z}_{p_i^{m_{i,j}}}$ *and* $m_{i,1} \geq m_{i,2} \geq \cdots \geq m_{i,s_i}$ *for all* $1 \leq i \leq s$. *Then*

$$|\mathbf{C}(\mathbf{A})| = \prod_{i=1}^{s} |\mathbf{C}(\mathbf{G}_i)| = |\mathbf{A}| \cdot \prod_{i=1}^{s} p_i^{2m_{i,2}-m_{i,1}} \cdot |\mathbf{C}(\mathbb{Z}_{p_i^{m_{i,1}-m_{i,2}}})|$$

5.1.5. Liftings.

Which of the minimal normal subgroups of an abelian p-group admit lifting of compatible functions?

2.40. Theorem. *Let* $\alpha \geq \beta$ *be two natural numbers and* $\mathbf{G} = \mathbb{Z}_{p^\alpha} \times \mathbb{Z}_{p^\beta}$. *Then the minimal normal subgroup* $\mathbf{N}$ *admits lifting of compatible functions, if*

- $\mathbf{N}$ *is a subgroup of* $\mathbb{Z}_{p^\alpha} \times \{0\}$ *or*
- $\alpha = \beta$ *and* $p = 2$.

Proof. In Vogt [1995], it is shown that the lattice of subgroups of the finite abelian p-group $\mathbf{G}$ with two cyclic factors can be obtained from the lattice of subgroups of the group $p\mathbf{G}$ by replacing each subgroup in the subgroup lattice of $p\mathbf{G}$ ([Vogt, 1995, Theorem 3.4]) by a block isomorphic to the subgroup lattice of the group $(\mathbb{Z}_p)^2$ ([Vogt, 1995, Theorem 3.5]). If for two blocks B_1 and B_2, the interval (B_1, B_2) has length l, then these two blocks intersect in a block isomorphic to $(\mathbb{Z}_p)^{2-l}$ ([Vogt, 1995, Proposition 3.4]). Figure 2.2 illustrates the transition from $p\mathbf{G}$ to $\mathbf{G}$.

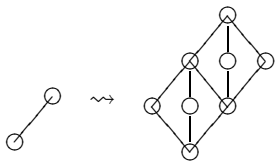

Figure 2.2. The transition from $\mathbb{Z}_2$ to $\mathbb{Z}_2 \times \mathbb{Z}_4$

By Theorem 2.37,

$$|\mathbf{C}(\mathbf{G})| = |\mathbf{G}| \cdot p^{2\beta-\alpha} \cdot |\mathbf{C}(\mathbb{Z}_{p^{\alpha-\beta}})|.$$

$\mathbf{N} \leq \mathbb{Z}_{p^\alpha} \times \{0\}$**:**

$$|\mathbf{C}(\mathbf{G}/\mathbf{N})| = \frac{|\mathbf{G}|}{|\mathbf{N}|} \cdot p^{2\beta-\alpha+1} \cdot |\mathbf{C}(\mathbb{Z}_{p^{\alpha-\beta-1}})|.$$

Hence $\frac{|\mathbf{C}(\mathbf{G})|}{|\mathbf{C}(\mathbf{G}/\mathbf{N})|} = p^{p^{\alpha-\beta}}$. We show that $[\mathbf{G} : \mathbf{K}] = p^{\alpha-\beta}$, whence $\mathbf{N}$ admits lifting of compatible functions.

If $\beta = 1$, then clearly $[\mathbf{G} : \mathbf{K}] = p^{\alpha-1}$. Suppose $\beta \geq 2$. There exists precisely one minimal normal subgroup of $\mathbf{G}_1 := \mathbb{Z}_{p^{\alpha-1}} \times \mathbb{Z}_{p^{\beta-1}} \cong p\mathbf{G}$, which is contained in $\langle(1,0)\rangle \leq p\mathbf{G}$. Let $\mathbf{N}_1$ denote this normal subgroup and let $\mathbf{K}_1$ be the sum of all normal subgroups of $\mathbf{G}_1$ not containing $\mathbf{N}_1$. We show that $[\mathbf{G} : \mathbf{K}] = [\mathbf{G}_1 : \mathbf{K}_1]$: By Vogt [1995], if the vertices in the lattice of normal subgroups of $\mathbf{G}_1$ are replaced by the subgroup lattice of $\mathbb{Z}_{p^2}$ in the correct manner, we get the lattice of normal sugroups of $\mathbf{G}$. Therefore, $|\mathbf{K}| = p^2 \cdot |\mathbf{K}_1|$. Since $|\mathbf{G}| = p^2 \cdot |\mathbf{G}_1|$, the index is the same in both cases.

We conclude that $[\mathbf{G} : \mathbf{K}] = p^{\alpha-\beta}$.

$\mathbf{N} \not\leq \mathbb{Z}_{p^\alpha} \times \{0\}$: Each automorphism $(x, y) \mapsto (x + kp^{\alpha-1}, y)$ $(0 < k < p)$ permutes the minimal normal subgroups of $\mathbf{G}$ not contained in $\mathbb{Z}_{p^\alpha} \times \{0\}$. Therefore it suffices to consider the case where the minimal normal subgroup $\mathbf{N}$ is contained in $\{0\} \times \mathbb{Z}_{p^\beta}$.

$$|\mathbf{C}(\mathbf{G}/\mathbf{N})| = \frac{|\mathbf{G}|}{|\mathbf{N}|} \cdot p^{2\beta-\alpha-2} \cdot |\mathbf{C}(\mathbb{Z}_{p^{\alpha-\beta+1}})|.$$

Hence $\frac{|\mathbf{C}(\mathbf{G})|}{|\mathbf{C}(\mathbf{G}/\mathbf{N})|} = p^{3-p^{\alpha-\beta+1}}$. Since $\alpha \geq \beta$ and $p \geq 2$, the exponent $3 - p^{\alpha-\beta+1}$ is positive only if $p = 2$ and $\alpha = \beta$. We are back in the first case.

□

5.2. Small p-groups.

Groups of order p or p^2 are abelian.

2.41. Proposition. *If $\mathbf{G}$ is a non-abelian group of size p^3, then*

$$|\mathbf{C}(\mathbf{G})| = p^{p^3+3}$$

Proof. These groups are of maximal class, so by [Huppert, 1967, III,14.2], $\mathbf{G}'$ is the unique minimal subgroup of $\mathbf{G}$ and $\mathbf{G}/\mathbf{G}' \cong (\mathbb{Z}_p)^2$. By Corollary 2.15, $|\mathbf{C}(\mathbf{G})| = p^{p^3+3}$. □

5.3. Alternating groups.

2.42. Theorem. *Let A_n $(n \geq 3)$ be the* **alternating group** *on n elements. Then*

$$|\mathbf{C}(\mathrm{A}_n)| = \left(\frac{n!}{2}\right)^{\frac{n!}{2}} \quad \text{, if } n \neq 4 \text{ and}$$
$$|\mathbf{C}(\mathrm{A}_4)| = 2^{24}3^3.$$

Proof. For $n \neq 4$, A_n is simple, so every function on A_n is compatible. The group A_4 has one normal subgroup of index 3. So by Corollary 2.15, $|\mathbf{C}(\mathrm{A}_4)| = 4^{12}3^3$. □

5.4. Symmetric groups.

2.43. THEOREM. *Let* S_n *(*$n \geq 3$*) be the* **symmetric group** *on* n *elements. Then*

$$|\mathbf{C}(\mathrm{S}_n)| = 4|\mathbf{C}(\mathrm{A}_n)|^2$$

PROOF. The normal subgroups of S_n are precisely the normal subgroup A_n of index 2 and its normal subgroups. Now we use Corollary 2.14. □

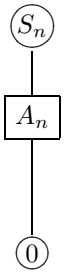

FIGURE 2.3. The lattice of normal subgroups of S_n ($n \geq 5$)

5.5. Dihedral groups.

The finite **dihedral group**, D_{2n}, of order $2n$ is the group $\langle a, b; na, 2b, 2(a+b)\rangle$. These groups will appear as quotients of some of the groups in the following examples.

We will distinguish the following three cases:

1. $n \equiv 1$ or $3 \pmod 4$,
2. $n \equiv 2 \pmod 4$ and
3. $n \equiv 0 \pmod 4$

In the first case we find a unique maximal normal subgroup and will be able to apply Theorem 2.13. In the second case our group is the direct product of $\mathbb{Z}_2$ with a group of the first type. Lemma 2.26 can be applied. In the third case we find a distributive minimal normal subgroup and use Theorem 2.30.

5.5.1. $n \equiv 1$ or $3 \pmod 4$.

2.44. LEMMA ([Malone and Lyons, 1972, Lemma 1.1]). *The proper normal subgroups of* D_{2n} *(*n *odd) are precisely the (cyclic) subgroup* $\mathbf{A} := \langle a\rangle$ *and its subgroups.*

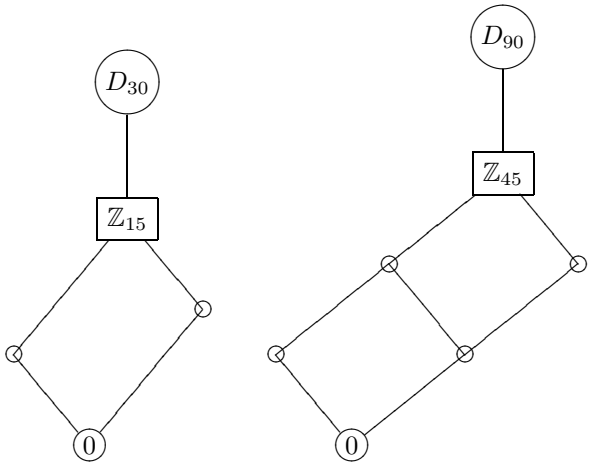

FIGURE 2.4. The lattices of normal subgroups of D_{30} and D_{90}

2.45. THEOREM. *The compatible functions on* D_{2n} *(n odd) are precisely the functions of the form*

$$\varphi(ib+ja) = \lambda \circ \psi(ib+\mathbf{A}) + \pi_i(ja) \quad , 0 \le i \le 1, 0 \le j < n$$

where ψ *is a function on* $\mathrm{D}_{2n}/\mathbf{A} \cong \mathbb{Z}_2$, λ *is the* $\{0,b\}$*-lifting of* $\mathrm{D}_{2n}/\mathbf{A}$ *and* π_i *is a compatible function on* $\mathbf{A}$*. In particular,*

$$|\mathbf{C}(\mathrm{D}_{2n})| = 4|\mathbf{C}(\mathbb{Z}_n)|^2$$

PROOF. The normal subgroup $\mathbf{A}$ fulfills the requirements of Theorem 2.13. All normal subgroups of $\mathbf{A}$ are normal in D_{2n}. The index $[\mathrm{D}_{2n} : \mathbf{A}]$ is equal to 2. Now Corollary 2.14 and Corollary 2.38 give the formula for $|\mathbf{C}(\mathrm{D}_{2n})|$. □

5.5.2. $n \equiv 2 \pmod 4$**.**

2.46. LEMMA. *The proper normal subgroups of* D_{2n} *(n even) are precisely*

1. *the subgroup* $\mathbf{A} = \langle a \rangle$ *and its subgroups,*
2. *the normal subgroup* $[b]$ *of index 2 and*
3. *the normal subgroup* $[a+b]$ *of index 2.*

PROOF (also in Malone and Lyons [1973]).

1. The subgroups of $\mathbf{A}$ are clearly normal in D_{2n}.
2. $-a+b+a = -2a+b \in [b]$ and $b-2a+b = 2a \in [b]$. Hence $[b] = \{2ka+lb \mid 0 \le k < \frac{n}{2} \wedge 0 \le l \le 1\}$. Moreover $[2ka+b] = [b]$ for all $0 \le k < \frac{n}{2}$.
3. $-a+(a+b)+a = b+a \in [a+b]$ and $a+b+b+a = 2a \in [a+b]$. Hence $[a+b] = \{2ka \mid 0 \le k < \frac{n}{2}\} \cup \{(2k+1)a+b \mid 0 \le k < \frac{n}{2}\}$.

□

2.47. Lemma. *For even n and $G = \mathrm{D}_{2n}$, the following holds:*

1. *The center* $\mathbf{Z}$ *of* $\mathbf{G}$ *is* $\{0, \frac{n}{2}a\}$.
2. $\mathbf{G}/\mathbf{Z} \cong \mathrm{D}_{2\frac{n}{2}}$.
3. *The subgroups* $[b]$ *and* $[a+b]$ *are isomorphic to* $\mathrm{D}_{2\frac{n}{2}}$.

Proof.

1. Suppose that $xb + ya \in Z$. Then the equation $(xb + ya) + (kb + la) = (kb + la) + (xb + ya)$ must hold for all $k \in \{0, 1\}$ and $l \in \{0, \dots, n-1\}$.

   Assuming that $x = 1$, we get $b+ya+kb+la = kb+la+b+ya$. Choosing $k = 0$, this equation becomes $b + (y + l)a = b + (y - l)a$, which can only be fulfilled for $2l \equiv 0 \pmod{n}$. Since this restricts our choice of l, x cannot be 1.

   Assume now that $x = 0$. Choosing $k = 1$, we get the equation $b + (l - y)a = b + (l + y)a$, which forces y to fulfill the equation $2y \equiv 0 \pmod{n}$.

   Finally, we observe that both 0 and $\frac{n}{2}a$ commute with every element of D_{2n}.
2. In $\mathbf{G}/\mathbf{Z}$, the element $2a + \mathbf{Z}$ has order $\frac{n}{2}$ and the element $b + \mathbf{Z}$ has order 2. Moreover, $2(2a + b) + \mathbf{Z} = \mathbf{Z}$. So, $\mathbf{G}/\mathbf{Z}$ is a group of order n satisfying the same relations as $\mathrm{D}_{2\frac{n}{2}}$.
3. The normal subgroups $[b]$ and $\mathbf{Z}$ intersect trivially. By 2., $\mathbf{G}/\mathbf{Z} \cong \mathrm{D}_{2\frac{n}{2}}$, and by the isomorphism theorem $\mathbf{G}/\mathbf{Z} \cong [b]/\{0\} \cong [b]$. The same holds for the normal subgroup $[a + b]$.

□

The following is a well known result which can be found e.g. in Coxeter and Moser [1965]. Later we will prove a generalization of this result for generalized dihedral groups.

2.48. Lemma. *Let $k \in \mathbb{N}$ be odd, $n = 2k$. Then*

$$\mathrm{D}_{2n} \cong \mathrm{D}_{2k} \times \mathbb{Z}_2$$

2.49. Theorem. *Let $k \in \mathbb{N}$ be odd, $n = 2k$. Then*

$$|\mathbf{C}(\mathrm{D}_{2n})| = 2 \cdot |\mathbf{C}(\mathrm{D}_{2k})|$$

Proof. By Lemma 2.48, $\mathrm{D}_{2n} \cong \mathrm{D}_{2k} \times \mathbb{Z}_2$. By Lemma 2.44, D_{2k} has a (cyclic) unique normal subgroup of index 2, so Lemma 2.26 applies and gives the desired result. □

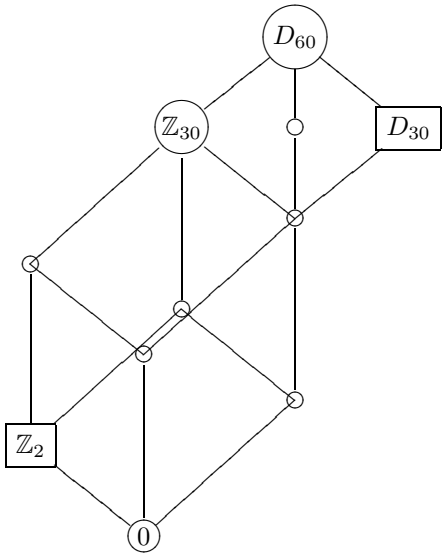

FIGURE 2.5. The lattice of normal subgroups of D_{60}

5.5.3. $n \equiv 0 \pmod 4$**.**

2.50. LEMMA. *For* $n \equiv 0 \pmod 4$*, precisely the normal subgroups of even order contain the center of* D_{2n}*.*

PROOF. Follows directly from Lemma 2.46 and Lemma 2.47. □

2.51. THEOREM. *Let* $n = 2^e k$*, where* k *is odd and* $e \geq 2$*. Then*

$$|\mathbf{C}(\mathrm{D}_{2n})| = 2^{2^{e+1}} \cdot |\mathbf{C}(\mathrm{D}_{2\frac{n}{2}})|$$

PROOF. Let $\mathbf{G} = \mathrm{D}_{2n}$, $\mathbf{A} = \mathrm{Z}(\mathbf{G})$ and $\mathbf{K}$ be the unique normal subgroup of order k. Then $A \cap K = \{0\}$. By Lemma 2.50, every normal subgroup of even order contains A and every normal subgroup of odd order m is the intersection of the unique normal subgroup of (even) order $2m$ (containing A) with $\mathbf{K}$. So Theorem 2.30 applies and gives the desired result. □

2.52. REMARK. The case, where $n = 2^e$ is a special case for the last theorem, which can also be proved directly, using Corollary 2.15.

When playing with generalized dihedral groups later, we will obtain a generalization of these results, without distinction of cases, in only a few lines, but with a very special technique. This is why I like the above proofs, as a demonstration of the applicability of all these general results.

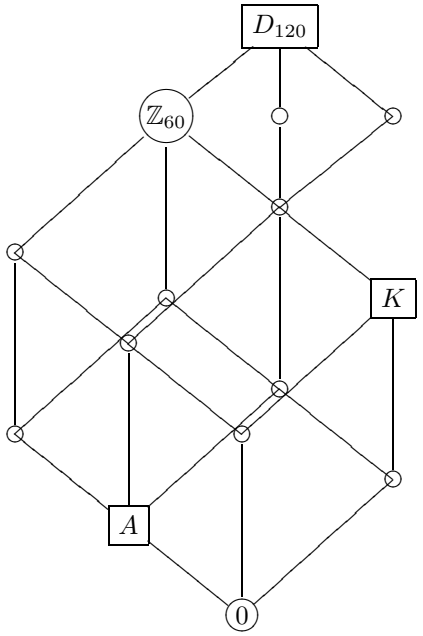

FIGURE 2.6. The lattice of normal subgroups of D_{120}

5.6. Semi-dihedral groups.

The **semi-dihedral group**, SD_{2^n}, of order 2^n, $n \geq 3$, is the group $\langle a, b; 2^{n-1}a, 2b, a+b = b + (2^{n-2}-1)a\rangle$.

2.53. LEMMA. *For $n > 3$, the normal subgroups of SD_{2^n} are precisely*

- *the subgroup $\mathbf{A} := \langle a\rangle$ and its subgroups,*
- *the normal subgroup $[b]$ of index 2 and*
- *the normal subgroup $[a+b]$ of index 2.*

2.54. THEOREM. *For $n > 3$,*

$$|\mathbf{C}(\mathrm{SD}_{2^n})| = 2^{2^n}|\mathbf{C}(\mathrm{D}_{2^{n-1}})|$$

and

$$\mathrm{SD}_8 \cong \mathbb{Z}_2 \times \mathbb{Z}_4$$

PROOF. First, we notice that $\langle 2^{n-2}a\rangle \trianglelefteq \mathrm{SD}_{2^n}$ and the quotient $\mathrm{SD}_{2^n}/\langle 2^{n-2}a\rangle$ is isomorphic to $\mathrm{D}_{2\cdot 2^{n-2}}$, simply by adding $2^{n-2}a = 0$ to the set of defining relations and simplifying the other relations, and checking that the order of the quotient is 2^{n-1}. The result follows from Corollary 2.15. From its presentation it is clear that the semi-dihedral group of order 8 is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$. □

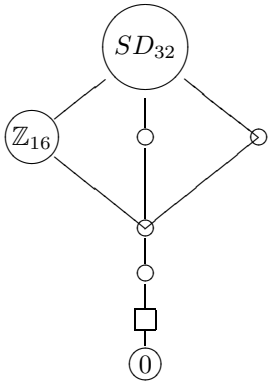

FIGURE 2.7. The lattice of normal subgroups of SD_{32}

5.7. Generalized quaternion groups.

The **generalized quaternion group** Q_{2^n}, of order 2^n, $n \geq 3$, is the group $\langle a, b; 2^{n-1}a, b + a - b + a, 2^{n-2}a + 2b \rangle$.

2.55. LEMMA ([Malone, 1973, Lemma 1]). *The normal subgroups of* Q_{2^n} *are precisely*

- *the subgroup* $\mathbf{A} := \langle a \rangle$ *and its subgroups,*
- *the normal subgroup* $[b]$ *of index 2 and*
- *the normal subgroup* $[a + b]$ *of index 2.*

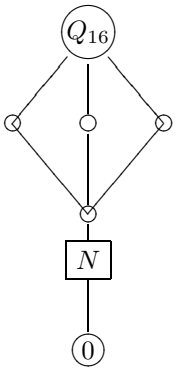

FIGURE 2.8. The lattice of normal subgroups of Q_{16}

2.56. THEOREM. *For* $n \geq 3$,

$$|\mathbf{C}(\mathrm{Q}_{2^n})| = 2^{2^n} |\mathbf{C}(\mathrm{D}_{2^{n-1}})|$$

PROOF. Let $n \geq 3$ and $\mathbf{N} = \langle 2^{n-2}a \rangle \trianglelefteq \mathrm{Q}_{2^n}$. Then $\mathbf{N}$ is the unique minimal normal subgroup of Q_{2^n}. The quotient $\mathrm{Q}_{2^n}/\mathbf{N}$ is isomorphic to $\mathrm{D}_{2^{n-1}}$. Corollary 2.15 yields the formula. □

5.8. An extension of a cyclic by an abelian group.

A group of order p^n has a cyclic maximal subgroup if and only if it is cyclic, a direct product of a cyclic group with a group of order p, a dihedral group of order a power of two, a generalized quaternion group, a semi-dihedral group, or a group of the form $\mathrm{CM}_{p^n} := \langle p^{n-1}a, pb, a^b = (1+p^{n-2})a \rangle$ ([Robinson, 1996, Theorem 5.3.4]). The only class of groups among these that we have not studied, yet, are next.

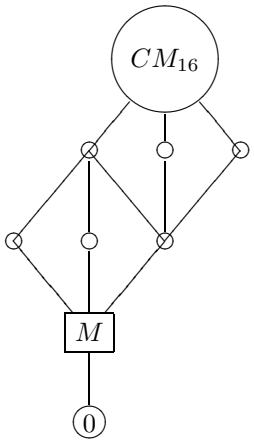

FIGURE 2.9. The lattice of normal subgroups of CM_{16}

2.57. THEOREM. *For $n \geq 3$,*

$$|\mathbf{C}(\mathrm{CM}_{p^n})| = p^{p^n} \cdot |\mathbf{C}(\mathbb{Z}_p \times \mathbb{Z}_{p^{n-2}})|$$

PROOF. Factoring CM_{p^n} by the unique minimal normal subgroup $\mathbf{M} = \langle p^{n-2}a \rangle$, we get the group $\mathbb{Z}_p \times \mathbb{Z}_{p^{n-2}}$. Corollary 2.15 yields the formula. □

5.9. Generalized dihedral groups.

For an abelian group $\mathbf{A}$, the **dihedral group of A**, $\mathrm{Dih}(\mathbf{A})$, is the semi-direct product of $\mathbf{A}$ with $\mathbb{Z}_2$, where the non-zero element of $\mathbb{Z}_2$ takes a to $-a$, for $a \in A$. This is a generalization of dihedral groups, as $\mathrm{Dih}(\mathbb{Z}_n) \cong \mathrm{D}_{2n}$.

2.58. LEMMA. *For every abelian group $\mathbf{A}$ and every $d \geq 0$, the following holds.*

$$\mathrm{Dih}(\mathbf{A}) \times \mathbb{Z}_2^d \cong \mathrm{Dih}(\mathbf{A} \times \mathbb{Z}_2^d)$$

PROOF. In $\mathbb{Z}_2^d$, the function $x \mapsto -x$ is the identity function. □

2.59. Lemma. *The proper normal subgroups of* $\mathrm{Dih}(\mathbf{A})$ *are precisely*

1. *the subgroups of* $\mathbf{A}$ *(embedded via* $a \mapsto (a,0)$*)*
2. *the sums of the normal subgroups* $[(r,1)] = (r + 2\mathbf{A}, 1) \cup (2\mathbf{A}, 0)$*, where* r *runs through a complete set of coset representatives of* $2\mathbf{A}$ *in* $\mathbf{A}$*.*

Proof.

1. $[(a,0)] = \langle (a,0) \rangle = (\langle a \rangle, 0)$, since
$$(a,0)^{(b,z)} = \begin{cases} (a,0) & \text{if } z = 0, \\ (-a,0) & \text{if } z = 1 \end{cases}.$$
2.
$$(a,1)^{(b,z)} = \begin{cases} (a+2b,1) & \text{if } z = 0, \\ (-a-2b,1) & \text{if } z = 1 \end{cases},$$
and $(a+2b,1) + (a,1) = (-2b,0)$. Hence $[(a,1)] = (a + 2\mathbf{A}, 1) \cup (2\mathbf{A}, 0)$.

□

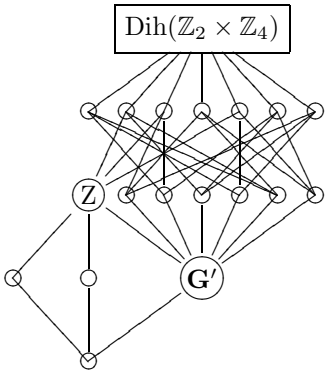

Figure 2.10. The lattice of normal subgroups of $\mathrm{Dih}(\mathbb{Z}_2 \times \mathbb{Z}_4)$

2.60. Lemma. *Let* $\mathbf{G} = \mathrm{Dih}(\mathbf{A})$*, where* $\mathbf{A}$ *is the direct product of* d *cyclic groups of even order and some cyclic groups of odd order. Then the derived subgroup of* $\mathrm{Dih}(\mathbf{A})$ *is* $(2A, 0)$ *and for every* $a \in A$*,* $[(a,1)] \supseteq (2A, 0)$*. Moreover,*

$$\mathrm{Z}(\mathbf{G}) \cong (\mathbb{Z}_2)^d$$
$$\mathbf{G}' \cong 2 \cdot \mathbf{A}$$
$$\mathbf{G}/\mathbf{G}' \cong (\mathbb{Z}_2)^{d+1},$$

Proof. As in the proof of the previous lemma, we can find $\mathbf{G}' = (2A, 0) \cong 2 \cdot \mathbf{A}$ by straightforward computation of commutators. The center of $\mathbf{G}$ is found in the same way. The quotient $\mathbf{G}/\mathbf{G}'$ is isomorphic to $\mathbb{Z}_2 \times \mathbf{A}/2\mathbf{A} \cong (\mathbb{Z}_2)^{d+1}$. □

Now we come to the point, where this method becomes a little bit specific, elegant, but not generally applicable.

2.61. LEMMA. *Let* $\mathbf{G} = \mathrm{Dih}(\mathbf{A})$*, where* $\mathbf{A}$ *is an abelian group. Then*

$$|(\mathbf{G}' : \mathbf{G})_{\mathbf{C}(\mathbf{G})}| = |(\mathbf{G}' : \mathbf{A})_{\mathbf{C}(\mathbf{A})}|^2.$$

PROOF. Let $c_1, c_2 \in (G' : A)_{\mathbf{C}(\mathbf{A})}$. We show that the function $c : G \to G$, which maps (a, i) to $c_i(a)$, for $a \in A$ and $i \in \{0, 1\}$, is an element of $(\mathbf{G}' : \mathbf{G})_{\mathbf{C}(\mathbf{G})}$. By definition, $c(G) \subseteq G'$, so it remains to show that c is compatible, i.e., for arbitrary $g, h \in G$, $c(g) - c(h) \in [g - h]$. We distinguish 3 cases:

- If there are $a, b \in A$ such that $g = (a, 0)$ and $h = (b, 0)$, then

$$\begin{aligned} c(g) - c(h) = c_0(a) - c_0(b) &\in [(a - b, 0)] \\ &= [(a, 0) - (b, 0)] = [g - h]. \end{aligned}$$

- If there are $a, b \in A$ such that $g = (a, 1)$ and $h = (b, 1)$, then

$$\begin{aligned} c(g) - c(h) = c_1(a) - c_1(b) &\in [(a - b, 0)] = [(a, 1) + (b, 1)] \\ &= [(a, 1) - (b, 1)] = [g - h]. \end{aligned}$$

- If there are $a, b \in A$ such that $g = (a, 1)$ and $h = (b, 0)$, then $[g - h] \geq \mathbf{G}'$, but trivially, $c(g) - c(h) \in G'$. The same holds, if $g = (a, 0)$ and $h = (b, 1)$.

Conversely, we show that for every function $c \in (\mathbf{G}' : \mathbf{G})_{\mathbf{C}(\mathbf{G})}$, the functions $c_i : A \to G'$, $a \mapsto c(a, i)$ $(i \in \{0, 1\})$, are compatible on $\mathbf{A}$.

- Let $a, b \in A$, then

$$\begin{aligned} c_0(a) - c_0(b) = c(a, 0) - c(b, 0) &\in [(a, 0) - (b, 0)] = [(a - b, 0)] \\ &= ([a - b], 0). \end{aligned}$$

- Let $a, b \in A$, then

$$\begin{aligned} c_1(a) - c_1(b) = c(a, 1) - c(b, 1) &\in [(a, 1) - (b, 1)] = [(a, 1) + (b, 1)] \\ &= [(b - a, 0)] = ([a - b], 0). \end{aligned}$$

□

2.62. THEOREM. *Let* $\mathbf{G} = \mathrm{Dih}(\mathbf{A})$*, where* $\mathbf{A}$ *is the direct product of* d *cyclic groups of even order and some cyclic groups of odd order. Then*

$$|\mathbf{C}(\mathbf{G})| = 2^{d+2} \cdot \left[\frac{|\mathbf{C}(\mathbf{A})|}{|\mathbf{C}(\mathbf{A}/2\mathbf{A})|}\right]^2$$

PROOF. In this proof we use a result from Chapter 3. As an immediate consequence of Theorem 2.37, Corollary 3.3 will tell us that elementary abelian groups

are 1-affine complete. We know that $2\mathbf{A}$ is normal in $\mathbf{A}$ and $\mathbf{A}/2\mathbf{A} \cong (\mathbb{Z}_2)^d$. By Lemma 2.28,

$$|\mathbf{C}(\mathbf{A})| = |\mathbf{C}(\mathbf{A}/2\mathbf{A})| \cdot |(2\mathbf{A} : \mathbf{A})_{\mathbf{C}(\mathbf{A})}|,$$

or equivalently,

$$|(2\mathbf{A} : \mathbf{A})_{\mathbf{C}(\mathbf{A})}| = \frac{|\mathbf{C}(\mathbf{A})|}{|\mathbf{C}(\mathbf{A}/2\mathbf{A})|} \tag{2.8}$$

Recall that $\mathbf{G}/\mathbf{G}'$ is elementary abelian and $\mathbf{G}' = (2A, 0) \cong 2\mathbf{A}$. Using Lemma 2.28 once more, for $\mathbf{G}$ instead of $\mathbf{A}$, we get

$$\begin{aligned} |\mathbf{C}(\mathbf{G})| &= |\mathbf{C}(\mathbf{G}/\mathbf{G}')| \cdot |(\mathbf{G}' : \mathbf{G})_{\mathbf{C}(\mathbf{G})}| \\ &= |\mathbf{C}(\mathbf{G}/\mathbf{G}')| \cdot |(2A : A)_{\mathbf{C}(\mathbf{A})}|^2 \quad \text{by Lemma 2.61} \\ &= 2^{d+2} \cdot \left[\frac{|\mathbf{C}(\mathbf{A})|}{|\mathbf{C}(\mathbf{A}/2\mathbf{A})|}\right]^2 \quad \text{by (2.8)} \end{aligned}$$

This completes the proof. □

Yes, dear reader, you are right. Here we have found a large class of 1-affine complete non-abelian groups. I will prove this in the next chapter. But first, let me present the rest of my examples.

5.10. Dicyclic groups.

The finite dicyclic group of order $4n$ is the group

$$\mathrm{Q}_{4n} := \langle a, b; 2na, na - 2b, a + b + a - b\rangle.$$

This generalizes generalized quaternion groups. From the presentation above we can see that $\mathrm{Q}_{4\cdot 2^{m-2}} \cong \mathrm{Q}_{2^m}$, as this notation suggests.

2.63. Lemma ([Lyons and Mason, 1991, Lemma 2.1]). *The normal subgroups of* Q_{4n} *are precisely*

- *the subgroup* $\mathbf{A} := \langle a\rangle$ *and all its subgroups*

and in addition, if n *is even,*

- *the normal subgroups* $[b]$ *and* $[a + b]$.

2.64. Lemma. *For* $n \equiv 0 \pmod 2$*, the following holds:*

1. *The center* $\mathbf{Z}$ *of* Q_{4n} *is* $\{0, na\}$.
2. $\mathrm{Q}_{4n}/\mathbf{Z} \cong \mathrm{D}_{2n}$.

Proof. The first part is proved in [Lyons and Mason, 1991, Lemma 2.1]. For the second part, we simply add na to the set of defining relations of the group and reduce this set obtaining $\langle a, b; na, 2b, 2(a+b)\rangle$, which is a presentation of the group D_{2n}. Finally, we compare the orders. □

2.65. THEOREM. *Let n be odd. Then*

$$|\mathbf{C}(\mathrm{Q}_{4n})| = 4 \cdot |\mathbf{C}(\mathbb{Z}_{2n})|^2$$

PROOF. This is a consequence of Lemma 2.63 and Corollary 2.14 (with $\mathbf{N} = \mathbf{A}$). □

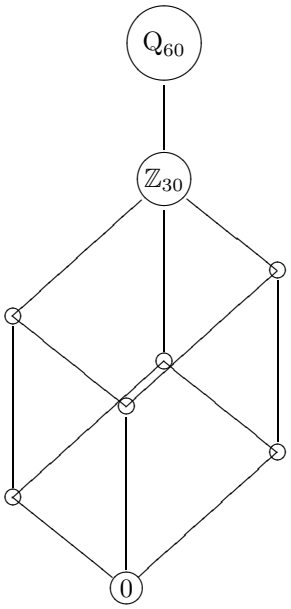

FIGURE 2.11. The lattice of normal subgroups of Q_{60}

2.66. LEMMA. *For even n and $\mathbf{G} = \mathrm{Q}_{2n}$, precisely the normal subgroups of even order contain the center of $\mathbf{G}$.*

PROOF. Follows directly from Lemma 2.63 and Lemma 2.64. □

2.67. THEOREM. *Let $n = 2^e k$, where k is odd and $e \geq 1$. Then*

$$|\mathbf{C}(\mathrm{Q}_{4n})| = 2^{2^e} \cdot |\mathbf{C}(\mathrm{D}_{2n})|$$

PROOF. Let $\mathbf{G} = \mathrm{Q}_{4n}$, $\mathbf{A} = \mathrm{Z}(\mathbf{G})$ and $\mathbf{K}$ be the unique normal subgroup of order k generated by $2^{e+1}a$. Then $A \cap K = \{0\}$. By Lemma 2.66, every normal subgroup of even order contains $\mathbf{A}$ and every normal subgroup of odd order m is the intersection of the unique normal subgroup of (even) order $2m$ (containing $\mathbf{A}$) with $\mathbf{K}$. So Theorem 2.30 applies and together with Lemma 2.63 gives the desired result. □

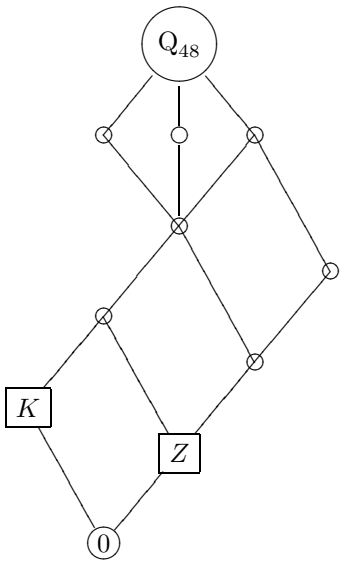

FIGURE 2.12. The lattice of normal subgroups of Q_{48}

5.11. Special Linear Groups.

2.68. THEOREM. *Let $m \geq 3$ or $m = 2$ and $q > 3$. Then with $d = (m, q-1)$,*

$$|\mathbf{C}(\mathrm{SL}(m,q))| = \Big(|\,\mathrm{PSL}(m,q)| \cdot |\mathbf{C}(\mathbb{Z}_d)|\Big)^{|\,\mathrm{PSL}(m,q)|}.$$

In addition,

$$|\mathbf{C}(\mathrm{SL}(2,2))| = 2^2 3^6 \text{ and } |\mathbf{C}(\mathrm{SL}(2,3))| = 2^{48} 3^3.$$

PROOF. Let $m \geq 3$ or $m = 2$ and $q > 3$. Any standard proof of the Jordan-Dickson theorem (e.g. in [Huppert, 1967, II,6.13]), shows that the proper normal subgroups of $\mathrm{SL}(m,q)$ are precisely the subgroups of its center, which is a cyclic group of order d. Now we apply Corollary 2.14.

The group $\mathrm{SL}(2,2) \cong S_3$ has been dealt with in Theorem 2.43. The center of $\mathrm{SL}(2,3)$ has 2 elements. The quotient of $\mathrm{SL}(2,3)$ by its center is $\mathrm{PSL}(2,3) \cong \mathrm{A}_4$. Now we use Corollary 2.15 and Theorem 2.42. □

5.12. General Linear Groups.

In this section we treat a class of general linear groups with a very nice structure.

2.69. THEOREM. *Suppose that $m \in \mathbb{N}$ and q is a prime power, such that $(m, q-1) = 1$. Then*

$$|\mathbf{C}(\mathrm{GL}(m,q))| = |\mathbf{C}(\mathbb{Z}_q^*)| \cdot |\mathbf{C}(\mathrm{SL}(m,q))|$$

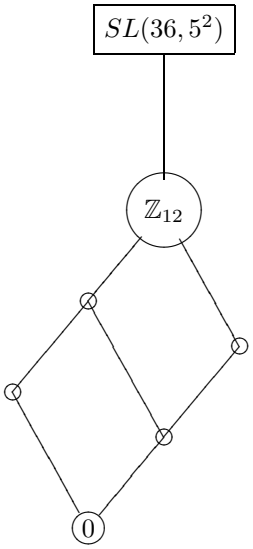

FIGURE 2.13. The lattice of normal subgroups of SL(36, 25)

PROOF. By [Meldrum, 1979, Lemma 1.13], $\mathrm{Z}(\mathrm{GL}(m,q)) \cap \mathrm{SL}(m,q) = \{0\}$ and $\mathrm{GL}(m,q) = \mathrm{Z}(\mathrm{GL}(m,q)) \times \mathrm{SL}(m,q)$. If $(m,q) \neq (2,2)$, then $\mathrm{SL}(m,q)$ is a non-abelian simple group, hence super-perfect. The center $\mathrm{Z}(\mathrm{GL}(m,q))$ is isomorphic to the cyclic group $\mathbb{Z}_q^*$. The result follows from Theorem 0.13. For $(m,q) = (2,2)$, we observe that $\mathrm{GL}(2,2) \cong \mathrm{SL}(2,2)$ and $|\mathbb{Z}_2^*| = 1$. The formula is also valid in this case. □

5.13. The holomorph of a cyclic p-group.

In this section we develop a recursive formula for the number of compatible functions on the groups $\mathrm{Hol}(\mathbb{Z}_{p^n})$. The main part is to proof that the lattices of normal subgroups of these groups are distributive. We begin with the case $n = 1$.

2.70. LEMMA. *Let p be a prime and $\mathbf{G} = \mathrm{Hol}(\mathbb{Z}_p)$. Then $\mathbf{G}$ has a unique minimal normal subgroup $\mathbf{M}$ isomorphic to $\mathbb{Z}_p$ and $\mathbf{G}/\mathbf{M} \cong \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$.*

PROOF. Notice that $\mathrm{Hol}(\mathbb{Z}_2) \cong \mathbb{Z}_2$, in this case the result follows trivially. From now on we assume $p > 2$.

We work with $\mathbf{G}$ as the semi-direct product of $\mathbf{P} = \mathbb{Z}_p$ with its automorphism group $\mathbf{A}$, where the automorphisms act on $\mathbf{P}$ in the natural way. Of course, $\mathbf{G}/\mathbf{P} \cong \mathbf{A} \cong \mathbb{Z}_{p-1}$. The subgroup $(\mathbf{P}, id)$ is normal in $\mathbf{G}$. We show that if a normal subgroup $\mathbf{N}$ contains a nonzero element (x, α), then it contains every element (z, id), and conclude that $(\mathbf{P}, id)$ is the unique minimal normal subgroup of G.

First, assume that $x \neq 0$. There exists an automorphism $\beta \in A$, such that $\beta(x) \neq \alpha(x)$. If $(x,\alpha) \in N$, then $(x,\alpha)^{(0,\beta)} = (\beta(x),\alpha) \in N$, and $(x,\alpha)^{(0,\alpha)} =$

$(\alpha(x),\alpha) \in N$, since $\mathbf{N}$ is normal. Consequently, $(\beta(x),\alpha)-(\alpha(x),\alpha) = (\underbrace{x+\alpha^{-1}\circ\beta(-x)}_{=:y}, id) \in N$. Since $\beta(x) \neq \alpha(x)$, $y \neq 0$, and (y, id) generates $(\mathbf{P}, id)$.

If $x = 0$, we choose an element $x' \in P$, such that $\alpha(x') \neq x'$. Such an x' exists, since $\alpha \neq id$. Then $(0,\alpha)^{(x',id)} = (x'-\alpha(x'),\alpha) \in N$ and $x'-\alpha(x') \neq 0$. □

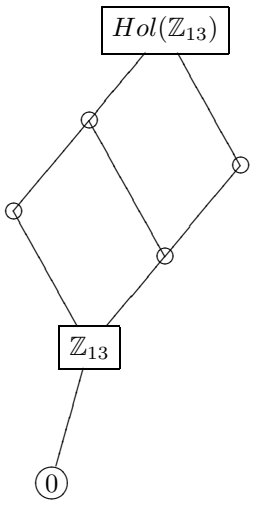

FIGURE 2.14. The lattice of normal subgroups of $\mathrm{Hol}(\mathbb{Z}_{13})$

2.71. THEOREM. *Let* $\mathbf{G} = \mathrm{Hol}(\mathbb{Z}_p)$. *Then*

$$|\mathbf{C}(\mathbf{G})| = p^{p(p-1)} \cdot |\mathbf{C}(\mathbb{Z}_{p-1})|$$

PROOF. By Corollary 2.15 and Lemma 2.70,

$$|\mathbf{C}(\mathbf{G})| = |\mathbf{C}(\mathbb{Z}_{p-1})| \cdot |\mathbb{Z}_p|^{|\mathbf{G}|}.$$

□

2.72. PROPOSITION. *Let* $n \geq 2$, $p > 2$, *and* $\mathbf{G} = \mathrm{Hol}(\mathbb{Z}_{p^n})$. *Then*

1. $\mathbf{G}$ *has a distributive lattice of normal subgroups.*
2. $\mathbf{G}$ *has a unique minimal normal subgroup* $\mathbf{M}$ *and* $|\mathbf{M}| = p$.
3. $\mathbf{G}/\mathbf{M}$ *has a minimal normal subgroup* $\mathbf{N}/\mathbf{M}$, *such that* $\mathbf{G}/\mathbf{N} \cong \mathrm{Hol}(\mathbb{Z}_{p^{n-1}})$, *and the sum* $\mathbf{K}/\mathbf{M}$ *of all normal subgroups of* $\mathbf{G}/\mathbf{M}$ *having trivial intersection with* $\mathbf{N}/\mathbf{M}$ *has index* p^{n-1} *in* $\mathbf{G}/\mathbf{M}$.

PROOF.

1. Let $\mathbf{N}$ be a normal subgroup of $\mathbf{G}$ and $(x,\alpha) \in N$. Let ξ be the automorphism $x \mapsto -x$ on $\mathbb{Z}_{p^n}$. Then $[(x,\alpha),(0,\xi)] = (-2x, id) \in N$. Since -2

is invertible modulo p^n, also $(x, id) \in N$ and as consequence $(0, \alpha) \in N$. So every normal subgroup can be written as a semidirect sum $\mathbf{I} \rtimes \mathbf{J}$, where $\mathbf{I} \trianglelefteq \mathbb{Z}_{p^n}$ and $\mathbf{J} \trianglelefteq \mathrm{Aut}(\mathbb{Z}_{p^n})$. The lattice of normal subgroups is therefore a sublattice of the direct product of the lattices of the cyclic groups $\mathbb{Z}_{p^n}$ and $\mathbb{Z}_{(p-1)p^{n-1}}$.

The normal subgroups containing $(\mathbb{Z}_{p^n}, id)$ are known to form a distributive lattice (isomorphic to the lattice of subgroups of the cyclic group $\mathbb{Z}_{(p-1)p^{n-1}}$).

Let β be a fixed point free automorphism on $\mathbb{Z}_{p^n}$ (i.e., $x \in \mathbb{Z}_{p^n} \setminus \{0\} \implies \beta(x) \neq x$). Then the mapping $\sigma : x \mapsto x - \beta(x)$ is an isomorphism on $\mathbb{Z}_{p^n}$ (it is clearly a homomorphism on the abelian group and its kernel is equal to $\{0\}$). If $\mathbf{N}$ contains an element (y, β) (β fixed point free), then it contains $(0, \beta)$ also. As a consequence, it contains $(0, \beta)^{(x,id)} = (x - \beta(x), \beta)$ and $(x - \beta(x), id)$, where x is an arbitrary generator of $\mathbb{Z}_{p^n}$. Since σ is an automorphism, $\sigma(x)$ is also a generator of $\mathbb{Z}_{p^n}$, whence $\mathbf{N}$ contains $(\mathbb{Z}_{p^n}, id)$. Since the fixed point free automorphisms on $\mathbb{Z}_{p^n}$ are precisely the automorphisms, the order of which is not a power of p, the lattice of normal subgroups of $\mathbf{G}$ is a sublattice of the direct product of two chains. Therefore the normal subgroups not containing $(\mathbb{Z}_{p^n}, id)$ form a distributive lattice.

2. The proof is the same as in Lemma 2.70.
3. Since there is only one minimal normal subgroup, $\mathbf{G}$ has at most two normal subgroups of order p^2. The subgroups $p^{n-2}\mathbb{Z}_{p^n} \rtimes \{0\}$ and $\mathbf{N} := p^{n-1}\mathbb{Z}_{p^n} \rtimes (p-1)p^{n-2}\mathbb{Z}_{(p-1)p^{n-1}}$ are normal in $\mathbf{G}$. Clearly, $\mathbf{G}/\mathbf{N} \cong \mathrm{Hol}(\mathbb{Z}_{p^{n-1}})$. The normal subgroup $\mathbf{K}$ is $\mathbb{Z}_{p^n} \rtimes (p-1)\mathbb{Z}_{(p-1)p^{n-1}}$.

□

2.73. Corollary. *Let $p > 2$ be prime, $n \geq 2$. Then*

$$|\operatorname{Hol}(\mathbb{Z}_{p^n})| = (p-1)p^{2n-1}$$

and

$$|\mathbf{C}(\operatorname{Hol}(\mathbb{Z}_{p^n}))| = p^{p^{2n}-p^{2n-1}+p^{n-1}} \cdot |\mathbf{C}(\operatorname{Hol}(\mathbb{Z}_{p^{n-1}}))|$$

Proof. The automorphism group of $\mathbb{Z}_{p^n}$ is cyclic of order $(p-1)p^{n-1}$, whence $|\operatorname{Hol}(\mathbb{Z}_{p^n})| = (p-1)p^{2n-1}$. With the notation from the last proposition, $|\mathbf{C}(\mathbf{G}/\mathbf{N})| = |\mathbf{C}(\operatorname{Hol}(\mathbb{Z}_{p^{n-1}}))|$. By Theorem 2.31, $|\mathbf{C}(\mathbf{G}/\mathbf{M})| = |\mathbf{C}(\mathbf{G}/\mathbf{N})| \cdot p^{p^{n-1}}$. Now by Corollary 2.15, $|\mathbf{C}(\mathbf{G})| = |\mathbf{C}(\mathbf{G}/\mathbf{M})| \cdot p^{(p-1)p^{2n-1}}$. □

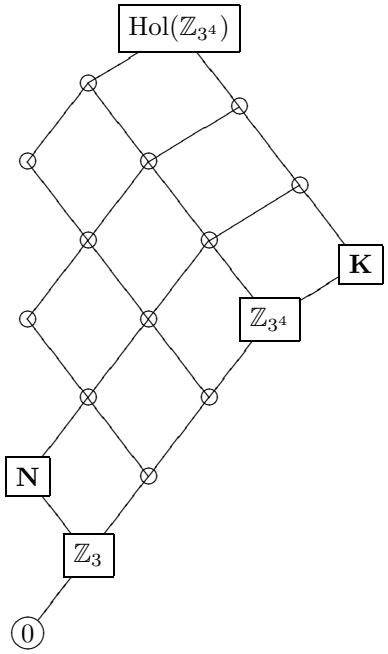

FIGURE 2.15. The lattice of normal subgroups of Hol($\mathbb{Z}_{3^4}$)

5.14. The groups 16/9 **and** 16/10**.**

With the results so far, it is possible to determine the near rings of compatible functions for almost every group with less than 32 elements. Apart from our examples there are some more groups, which can also be handled easily.

The smallest examples have order 16. The groups 16/8, 16/11, 16/13 are all subdirectly irreducible, therefore are treated in Corollary 2.15. The group $\mathbb{Z}_2 \times \mathrm{Q}_8$ will be dealt with in Section 11 of the next chapter.

We are not going to work through the groups of order 17 to 31, each of which can be treated with the methods demonstrated, as soon as its lattice of normal subgroups is known. The groups of order 32 pose problems because of their complex lattices of normal subgroups.

As a last application let us use the results obtained to compute the number of compatible functions on the groups 16/9 and 16/10.

Let $\mathbf{G}$ be any of these groups. The quotient $\mathbf{G}/\mathbf{G}'$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$, which is 1-affine complete, so $\mathbf{G}'$ admits lifting of compatible functions. The sum of the normal subgroups not containing the minimal normal subgroup $\mathbf{G}'$ is $\mathrm{Z}(\mathbf{G})$, which has index 4 in $\mathbf{G}$. By Theorem 2.29, there are $|\mathbf{C}(\mathbf{G}/\mathbf{G}')| \cdot |\mathbf{G}'|^{[\mathbf{G}:\mathbf{K}]} = 2^5 \cdot 2^4 = 2^9$ compatible functions on $\mathbf{G}$.

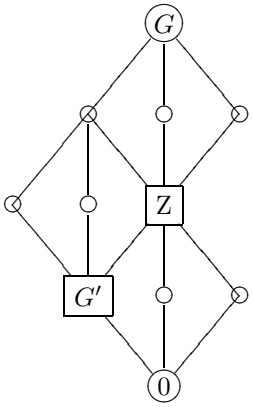

FIGURE 2.16. The lattice of normal subgroups of 16/9 and 16/10

6. Compatible endomorphisms

- Let h be an endomorphism on the group G, N a normal subgroup of G. Then h is compatible w. r. t. N, iff

$$x - y \in N \implies h(x) - h(y) = h(x - y) \in N \quad \text{for all } x, y \in N \tag{2.9}$$

or equivalently

$$h(N) \subseteq N \tag{2.10}$$

- For any group G the following holds

$$C(G) \cap End(G) \geq Inn(G) \tag{2.11}$$

For which groups does equality hold? (It does not hold for 8/4, 8/5 and 12/4.) When is every nonzero compatible endomorphism an inner automorphism?

7. Generating compatible function near rings additively

Since we have seen Lemma 2.6, we are interested in a set of generators of the lattice of normal subgroups of $\mathbf{G}$, which can be computed easily. There are of course very fast algorithms for computing the lattice of normal subgroups (e.g. Hulpke [1998]), nevertheless it seems to be more suitable to generate only the generators, which are really needed.

7.1. Generators of the lattice of normal subgroups.

Let $C_1, \ldots, C_s$ be the conjugacy classes of G, $r_1, \ldots, r_s$ a set of representatives of the conjugacy classes. The lattice of normal subgroups is generated by the normal subgroups that are generated by single elements. These are the subgroups generated by conjugacy classes of elements. If for two such normal subgroups $\mathbf{N}_i = [r_i]$ and

$\mathbf{N}_j$ there exists a number k, such that $kr_i \in C_j$, then $\mathbf{N}_i \leq \mathbf{N}_j$. We consider the following cases.

1. If $(k, \operatorname{ord} r_i) = 1$, then k is invertible modulo r_i, and as a consequence, $k^{-1}(kr_i) = r_i$ is a multiple of $kr_i \in C_j$. So $\mathbf{N}_j \leq \mathbf{N}_i$, whence $\mathbf{N}_j = \mathbf{N}_i$.
2. If $(k, \operatorname{ord} r_i) \neq 1$, then $\mathbf{N}_i < \mathbf{N}_j$.

We summarize these observations in Algorithm 1.

Algorithm 1 Additive generators of the normal subgroup lattice

Require: $r_1, \ldots, r_s$ representatives for the s different conjugacy classes $C_1, \ldots, C_s$ of the group G

Ensure: *generatingClasses* is a subset of $\{1, \ldots, s\}$, s.t. the lattice of normal subgroups of G is generated additively by $\{[r_i] \mid i \in \mathit{generatingClasses}\}$

```
generatingClasses := {1, ..., s};
for i ∈ generatingClasses do
  for k ∈ {q ∈ ℕ | q < ord c_i & (q, ord c_i) = 1} do
    for j ∈ generatingClasses, s.t. j > i do
      if kr_i and r_j are conjugate then
        Delete j from generatingClasses;
      end if
    end for
  end for
end for
```

In the case of the elementary abelian group of order 2^n, the set of generators for the lattice of normal subgroups is as big as $|\mathbf{G}| - 1$.

7.2. Additive generators for $\mathbf{C}(\mathbf{G})$.

7.2.1. The generic solution.

For a set $\mathcal{N}$ of normal subgroups of $\mathbf{G}$, let

$$\operatorname{Comp}_{\mathcal{N}}(\mathbf{G}) := \bigcap_{\mathbf{N} \in \mathcal{N}} \operatorname{Comp}_{\mathbf{N}}(\mathbf{G}).$$

Let $\mathcal{E}$ be a set of generators of the normal subgroup lattice of $\mathbf{G}$ as computed with Algorithm 1. Then, by Lemma 2.6, $\mathbf{C}(\mathbf{G})$ can be computed as

$$\mathbf{C}(\mathbf{G}) = \operatorname{Comp}_{\mathcal{E}}(\mathbf{G}).$$

We can describe a set of additive generators for $\operatorname{Comp}_{\mathcal{N}}(\mathbf{G})$, if $\mathcal{N}$ is a chain of normal subgroups of $\mathbf{G}$.

2.74. THEOREM. *Let $\mathcal{N} = (\mathbf{G} = \mathbf{N}_0, \mathbf{N}_1, \dots, \mathbf{N}_s = \{0\})$ be a descending chain of normal subgroups of $\mathbf{G}$, and let E_i be a set of additive generators of $\mathbf{N}_i$ and R_i a complete set of coset representatives of $\mathbf{N}_i$ in $\mathbf{G}$, for all $0 \leq i \leq s$. Then the following functions generate* $\mathrm{Comp}_{\mathcal{N}}(\mathbf{G})$ *additively:*

$$c^i_{r\to e} : x \mapsto \begin{cases} e & \text{if } x - r \in N_i, \\ 0 & \text{otherwise} \end{cases}$$

where $r \in R_i, e \in E_{i-1}, 1 \leq i \leq s$.

PROOF. The functions of type $c^i_{r\to e}$ are constant on the cosets of $\mathbf{N}_i$ in G. They are compatible with N_j for $j < i$, since their range is contained in N_i. They are compatible with N_j for $j \geq i$, because they are constant on the cosets of $\mathbf{N}_j$ in G.

We show, that every function f from $\mathrm{Comp}_{\mathcal{N}}(\mathbf{G})$ can be written as a sum of certain ones of these:
For $i \in \{1, \dots, s\}$ set $n_i = [G : \mathbf{N}_i]$ and suppose that for $1 \leq i \leq s$, the set R_i of coset representatives of $\mathbf{N}_i$ in $\mathbf{G}$ is $\{r^i_1, \dots, r^i_{n_i}\}$.

In s steps we will decompose f into a sum of type $c^i_{r\to e}$. Starting with $f_1 := f$, let us describe the i-th step:
Assume that f_i maps the coset $r^i_j + \mathbf{N}_i$ into the coset $r^i_{\varphi_i(j)} + \mathbf{N}_i$ of $\mathbf{N}_{i-1}$. Now define f_{i+1} as follows:

$$f_{i+1} := f_i - \sum_{j=1}^{n_i} c^i_{r^i_j \to r^i_{\varphi_i(j)}}$$

Note, that for different j_1, j_2 the functions $c^i_{r^i_{j_1}\to x}$ and $c^i_{r^i_{j_2}\to y}$ commute (additively) for all $x, y \in G$. The function f_{i+1} maps G into N_i and cosets of $\mathbf{N}_{i+1}$ in G into cosets of $\mathbf{N}_{i+1}$ in $\mathbf{N}_i$(!).

Continuing with this process, we get a function f_{s+1}, which maps G into $N_s = \{0\}$, so f_{s+1} is the zero-function on G. We finally get that

$$f = \sum_{i=1}^{s} \sum_{j=1}^{n_i} c_{r^i_j \to r^i_{\varphi_i(j)}}$$

(where i runs from s to 1). Factoring $r^i_{\varphi_i(j)}$ in $\mathbf{G}$, we find how the summand $c^i_{r^i_j \to r^i_{\varphi_i(j)}}$ can be written as a sum of functions of the form $c^i_{r^i_j \to e}$. □

The following example illustrates, how this procedure of decomposition into a sum works.

2.75. EXAMPLE. Let $\mathbf{G} = \mathbb{Z}_8$, we denote the elements of $\mathbf{G}$ $0, 1, \dots, 7$. The group $\mathbf{G}$ is generated by 1. For the sake of simplicity, let us write the function mapping $i \in \mathbb{Z}_8$ to f_i as the vector $(f_0, f_1, \dots, f_7)$. We will now decompose the

(compatible) function $f : x \mapsto 3x^3 + 1$ on $\mathbb{Z}_8$. Using our notation, this function is $(1, 4, 1, 2, 1, 0, 1, 6)$.

Let $\mathbf{N}_0 = \mathbf{G} = \mathbb{Z}_8$, $\mathbf{N}_1 = 2\mathbb{Z}_8$, $\mathbf{N}_2 = 4\mathbb{Z}_8$, and $\mathbf{N}_3 = \{0\}$. Let $R_1 = \{0, 1\}$, $R_2 = \{0, 1, 2, 3\}$, and $R_3 = \{0, 1, \ldots, 7\}$ be the corresponding sets of representatives.

We start with $f_1 = f = (1, 4, 1, 2, 1, 0, 1, 6)$. The coset $0 + \mathbf{N}_1$ is mapped into the coset $1 + \mathbf{N}_1$, the coset $1 + \mathbf{N}_1$ is mapped into the coset $0 + \mathbf{N}_1$. So we have to subtract the functions $c^1_{0\to1} = (1, 0, 1, 0, 1, 0, 1, 0)$ and $c^1_{1\to0} = (0, 0, 0, 0, 0, 0, 0, 0)$.

Subtracting, we find $f_2 = (0, 4, 0, 2, 0, 0, 0, 6)$. This function maps G into N_1, and it is compatible, because it is the difference of compatible functions.

The function f_2 maps the coset $3 + \mathbf{N}_2$ into the coset $2 + \mathbf{N}_2$, and all other cosets of $\mathbf{N}_2$ into the coset $0 + \mathbf{N}_2$. We have to subtract the functions $c^2_{0\to0} = c^2_{1\to0} = c^2_{2\to0} = (0, 0, 0, 0, 0, 0, 0, 0)$ and $c^2_{3\to2} = (0, 0, 0, 2, 0, 0, 0, 2)$.

We subtract and get $f_3 = (0, 4, 0, 0, 0, 0, 0, 4)$. This function maps G into N_2.

The function f_3 maps the cosets $1 + \mathbf{N}_3$ and $7 + \mathbf{N}_3$ into the coset $4 + \mathbf{N}_3$, and all other cosets of $\mathbf{N}_3$ into the coset $0 + \mathbf{N}_3$. We have to subtract the functions $c^3_{1\to4} = (0, 4, 0, 0, 0, 0, 0, 0)$, $c^3_{7\to4} = (0, 0, 0, 0, 0, 0, 0, 4)$ and $c^3_{0\to0} = c^3_{2\to0} = c^3_{3\to0} = c^3_{4\to0} = c^3_{5\to0} = c^3_{6\to0} = (0, 0, 0, 0, 0, 0, 0, 0)$.

Finally, the result is $f_4 = (0, 0, 0, 0, 0, 0, 0, 0)$. So, f can be written as the sum $f = c^3_{7\to4} + c^3_{1\to4} + c^2_{3\to2} + c^1_{0\to1} = 4c^3_{7\to1} + 4c^3_{1\to1} + 2c^2_{3\to1} + c^1_{0\to1}$.

Summarizing, if the set of generators of the normal subgroup lattice of G as computed in section 7.1 is the union of the chains $(\mathcal{N}_j)_{j\in J}$, then $\mathbf{C}(\mathbf{G})$ can be computed as the intersection of near rings with known additive generators:

$$\mathbf{C}(\mathbf{G}) = \bigcap_{j\in J} \mathrm{Comp}_{\mathcal{N}_j}(\mathbf{G})$$

It is useful to avoid disjoint unions of chains and prefer longer chains. In this way, smaller near rings will have to be intersected.

The near ring of zero-symmetric compatible functions is generated additively by the zero-symmetric functions in the last theorem. In practice, it is useful to generate only the zero symmetric parts, intersect the near rings, and finally add a constant function $x \mapsto e$ for every generator e of the group.

7.2.2. Congruence lattice is a chain.

If the normal subgroup lattice of a group $\mathbf{G}$ is a chain, Theorem 2.74 gives a set of additive generators for $\mathbf{C}(\mathbf{G})$ explicitly.

7.2.3. Finite abelian groups.

Congruence lattices of cyclic p-groups are chains, so Theorem 2.74 applies.

Following Theorem 2.37, we can explicitly give a set of additive generators of $\mathbf{C}(\mathbf{G})$ for every finite abelian p-group $\mathbf{G} = \mathbb{Z}_{p^{m_1}} \times \cdots \times \mathbb{Z}_{p^{m_s}}$, where $m_1 > m_2 \geq \ldots \geq m_s$ (in the case that $m_1 = m_2$, the group is known to be 1-affine complete by Corollary 3.3), in the following way: For the generation of $\mathbf{P}(\mathbf{G})$ we need the identity function on G and the constant functions $f_i(x) = g_i$, where g_i is a generating element of the cyclic subgroup $\{0\} \times \ldots \{0\} \times \mathbb{Z}_{p^{m_i}} \times \{0\} \times \cdots \times \{0\}$ of $\mathbf{G}$. Furthermore, we find generators for the cyclic group $\mathbf{G}/p^{m_2}\mathbf{G}$ and use Theorem 2.37 to transform them into the corresponding generators for $\mathbf{C}(\mathbf{G})$.

Direct products of groups of coprime order are nice, so with Theorem 2.21 we get generators explicitly in the case of abelian groups.

7.2.4. A distributive minimal normal subgroup.

Let $\mathbf{M}$ be a distributive minimal normal subgroup of $\mathbf{G}$, and let $\mathbf{G}$ be generated by E. Then the proof of Theorem 2.30 shows how to construct a set of additive generators of $\mathbf{C}(\mathbf{G})$ from a set of additive generators of $\mathbf{C}(\mathbf{G}/\mathbf{M})$: For every additive generator F of $\mathbf{C}(\mathbf{G}/\mathbf{M})$, we may fix arbitrary values for ψ at every point in S. The function ψ can then be extended to a function from G to M in a unique way, as described in the proof of Theorem 2.30. We choose

$$\psi(s_i) = \begin{cases} 0 & \text{if } i \neq j \\ e & \text{if } i = j \end{cases},$$

for each $j \in \{1, \ldots, [\mathbf{G} : \mathbf{M}]\}$ and each $e \in E$. In this way we obtain $[\mathbf{G} : \mathbf{M}] \cdot |E|$ generators for $\mathbf{C}(\mathbf{G})$ for each generator of $\mathbf{C}(\mathbf{G}/\mathbf{M})$.

8. Testing compatibility of a function

What do we have to test to find out, whether a given function φ is compatible with a certain normal subgroup $\mathbf{N}$ of $\mathbf{G}$?

2.76. Lemma. *Let $\mathbf{G}$ be a group, $\mathbf{N} \trianglelefteq \mathbf{G}$ and E a set of (subgroup) generators of $\mathbf{N}$. Then for every $\varphi \in \mathrm{M}(\mathbf{G})$,*

$$\varphi \in \mathrm{Comp}_{\mathbf{N}}(\mathbf{G}) \iff \forall g \in G\ \forall e \in E\ \varphi(g+e) - \varphi(g) \in N$$

Proof. The "only-if-part" is clear by Proposition 2.4. For the "if-part", it suffices to show that $\varphi(x+n) - \varphi(x) \in N$ for all $n \in N$ and $x \in G$. For an arbitrary but fixed $n \in N$, there exist $s \in \mathbb{N}$ and $e_1, \ldots, e_s \in E$, such that $n = \sum_{i=1}^{s} e_i$.

Then for arbitrary $x \in G$

$$\begin{aligned}\varphi(x+n) - \varphi(x) &= \varphi(x + e_1 + \cdots + e_s) - \varphi(x) \\ &= \varphi((x + e_1 + \cdots + e_{s-1}) + e_s) - \varphi(x + e_1 + \cdots + e_{s-1}) \\ &\quad + \varphi((x + e_1 + \cdots + e_{s-2}) + e_{s-1}) - \varphi(x + e_1 + \cdots + e_{s-2}) \\ &\quad + \ldots \\ &\quad + \varphi(x + e_1) - \varphi(x)\end{aligned}$$

By our assumption, this is a sum of elements of $\mathbf{N}$. □

This gives a time complexity of $|\mathbf{G}| \cdot |E|$. In order to decide compatibility we have to do this for more than one normal subgroup, precisely for up to every normal subgroup in a generating set of the lattice of normal subgroups. In many cases we can then speed up some of the tests.

If we know that φ is compatible with $\mathbf{I}$ and we want to test compatibility of φ with a normal subgroup $\mathbf{J}$ containing $\mathbf{I}$, we should somehow be able to use our knowledge. The following lemma says, that we are allowed to project everything down to the quotient $\mathbf{G}/\mathbf{I}$. Of course, this cheapens the test by the factor $|\mathbf{I}|$: if $\mathbf{J}$ is generated by j elements, the test costs $|\mathbf{G}/\mathbf{I}| \cdot j$ instead of $|\mathbf{G}| \cdot j$.

2.77. Lemma. *Let $\mathbf{G}$ be a group and $\mathbf{I} < \mathbf{J}$ be two normal subgroups of $\mathbf{G}$. Let $\varphi \in \mathrm{M}(\mathbf{G})$ be compatible with $\mathbf{I}$. Then*

$$\varphi \in \mathrm{Comp}_{\mathbf{J}}(\mathbf{G}) \iff \varphi^{\mathbf{I}} \in \mathrm{Comp}_{\mathbf{J}/\mathbf{I}}(\mathbf{G}/\mathbf{I})$$

Proof. First, let us remark that the assumption that φ is compatible with $\mathbf{I}$ is necessary and sufficient for $\varphi^{\mathbf{I}}$ to be well-defined. Let λ be an arbitrary lifting of $\mathbf{G}/\mathbf{I}$.

Assume that $\varphi \in \mathrm{Comp}_{\mathbf{J}}(\mathbf{G})$. If $x + \mathbf{I}, y + \mathbf{I} \in G/I$, such that $x + \mathbf{I} - y + \mathbf{I} \in J/I$, then $\lambda(x+\mathbf{I}) - \lambda(y+\mathbf{I}) \in J$, so $\varphi(\lambda(x+\mathbf{I})) - \varphi(\lambda(y+\mathbf{I})) \in J$. Thus $\varphi^{\mathbf{I}}(x+\mathbf{I}) - \varphi^{\mathbf{I}}(y+\mathbf{I}) \in J/I$.

Conversely, if $\varphi \notin \mathrm{Comp}_{\mathbf{J}}(\mathbf{G})$, then there are $x, y \in G$, such that $x - y \in J$, but $\varphi(x) - \varphi(y) \notin J$. As a consequence, $x + \mathbf{I} - y + \mathbf{I} \in J/I$, but $\varphi^{\mathbf{I}}(x+\mathbf{I}) - \varphi^{\mathbf{I}}(y+\mathbf{I}) \notin J/I$. □

On a computer, it does not make sense to generate the whole near ring of compatible functions on a group in order to decide compatibility for a single function (by simply testing membership). These near rings use to be extraordinarily large, so that even storing them can be difficult. Even in the case that many functions have to be tested, it is wise to test them this way.

Algorithm 2 Testing compatibility

Require: $\varphi \in \mathrm{M}(G)$; $\mathcal{N}$ a list of generators of the lattice of normal subgroups of G, s.t. $\mathcal{N}_i \not\geq \mathcal{N}_j$ for $i < j$.
Ensure: $answer \iff \varphi \in \mathrm{C}(G)$
  $answer :=$ TRUE;
  for $N \in \mathcal{N}$ **do**
    $I := \sum_{N \geq J \in \mathcal{N}} J$;
    for $g \in G/I$, $e \in$ Generators(N/I) **do**
      if $\varphi^I(g+e) - \varphi^I(e) \notin N/I$ **then**
        $answer :=$ FALSE;
        return ;
      end if
    end for
  end for

9. Results

Table 2.1 shows the number of compatible functions on all non-abelian groups up to order 32. They have been computed using the near ring package SONATA for GAP (Aichinger *et al.* [1997b]; GAP [1999]). These results have lead to good guesses for the results in this chapter. A (valid) conjecture for the formula for the number of compatible functions on dihedral groups and holomorphs of cyclic p-groups existed long before the proofs.

G	$\lvert\mathbf{C}(\mathbf{G})\rvert$	**G**	$\lvert\mathbf{C}(\mathbf{G})\rvert$	**G**	$\lvert\mathbf{C}(\mathbf{G})\rvert$	**G**	$\lvert\mathbf{C}(\mathbf{G})\rvert$
6/2	$2^2 \cdot 3^6$	21/2	$3^3 \cdot 7^{21}$	32/8	2^9	32/30	2^{17}
8/4	2^{11}	22/2	$2^2 \cdot 11^{22}$	32/9	2^9	32/31	2^{41}
8/5	2^{11}	24/4	$2^4 \cdot 3^6$	32/10	2^{13}	32/32	2^{41}
10/2	$2^2 \cdot 5^{10}$	24/5	$2^{26} \cdot 3^3$	32/11	2^{10}	32/33	2^{10}
12/3	$2^3 \cdot 3^6$	24/6	$2^5 \cdot 3^6$	32/12	2^{10}	32/34	2^{10}
12/4	$2^{24} \cdot 3^3$	24/7	$2^{11} \cdot 3^3$	32/13	2^{14}	32/35	2^{10}
12/5	$2^6 \cdot 3^6$	24/8	$2^{11} \cdot 3^3$	32/14	2^{10}	32/36	2^{12}
14/2	$2^2 \cdot 7^{14}$	24/9	$2^5 \cdot 3^6$	32/15	2^{10}	32/37	2^{12}
16/6	2^8	24/10	$2^{11} \cdot 3^6$	32/16	2^{14}	32/38	2^{16}
16/7	2^8	24/11	$2^{11} \cdot 3^6$	32/17	2^{38}	32/39	2^{16}
16/8	2^{20}	24/12	$2^{50} \cdot 3^6$	32/18	2^{10}	32/40	2^{16}
16/9	2^9	24/13	$2^{48} \cdot 3^3$	32/19	2^{14}	32/41	2^{28}
16/10	2^9	24/14	$2^{14} \cdot 3^6$	32/20	2^{13}	32/42	2^{37}
16/11	2^{21}	24/15	$2^{11} \cdot 3^6$	32/21	2^{13}	32/43	2^{37}
16/12	2^{27}	26/2	$2^2 \cdot 13^{26}$	32/22	2^{41}	32/44	2^{40}
16/13	2^{27}	27/4	3^{30}	32/23	2^{16}	32/45	2^{40}
16/14	2^{27}	27/5	3^{30}	32/24	2^{16}	32/46	2^{41}
18/3	$2^2 \cdot 3^9$	28/3	$2^3 \cdot 7^{14}$	32/25	2^{16}	32/47	2^{41}
18/4	$2^2 \cdot 3^{24}$	28/4	$2^6 \cdot 7^{14}$	32/26	2^{40}	32/48	2^{41}
18/5	$2^2 \cdot 3^6$	30/2	$2^2 \cdot 3^3 \cdot 5^{10}$	32/27	2^{17}	32/49	2^{59}
20/3	$2^3 \cdot 5^{10}$	30/3	$2^2 \cdot 3^6 \cdot 5^5$	32/28	2^{17}	32/50	2^{59}
20/4	$2^6 \cdot 5^{10}$	30/4	$2^2 \cdot 3^6 \cdot 5^{10}$	32/29	2^{17}	32/51	2^{59}
20/5	$2^6 \cdot 5^{20}$						

TABLE 2.1. The numbers of compatible functions on small non-abelian groups

CHAPTER 3

1-affine complete groups

1. Polynomially complete groups

Polynomial completeness is the best that can happen, every function can be written down as a polynomial.

3.1. Definition. A group $\mathbf{G}$ is called **polynomially complete**, iff $\mathbf{P}(\mathbf{G}) = \mathbf{M}(\mathbf{G})$. It is called **1-affine complete**, iff $\mathbf{P}(\mathbf{G}) = \mathbf{C}(\mathbf{G})$.[1]

Obviously, polynomially complete groups are 1-affine complete. They can be characterized in a nice way, but turn out to be a very particular class of groups.

3.2. Theorem (Lausch and Nöbauer [1973]). *The polynomially complete groups are exactly $\mathbb{Z}_2$ and all finite non-abelian simple groups.*

2. Abelian groups

A characterization of abelian 1-affine complete groups has been given by Lausch and Nöbauer (Lausch and Nöbauer [1976]). We will only consider the finite case, which has been solved completely in Lausch and Nöbauer [1976]. In Nöbauer [1978] and Kaarli [1982] the infinite case is treated. The result follows almost immediately from the results in the previous chapters, we only need to compare the numbers of polynomial and compatible functions.

3.3. Corollary. (to Remark 1.2 and Theorem 2.37, Lausch and Nöbauer [1976]) *Precisely the following finite abelian p-groups are 1-affine complete.*

1. $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p^{\alpha_r}}$, *where* $\alpha_1 = \alpha_2 \geq \cdots \geq \alpha_r$ *and*
2. $\mathbb{Z}_{2^{\alpha_1}} \times \mathbb{Z}_{2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{2^{\alpha_r}}$, *where* $\alpha_1 - 1 = \alpha_2 \geq \cdots \geq \alpha_r$,

for all $r \geq 2$ *and* $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$.

Proof. Every abelian group $\mathbf{A}$ can be written as $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p^{\alpha_r}}$, for suitable $r \in \mathbb{N}$ and $\alpha_1 \geq \ldots \geq \alpha_r \in \mathbb{N}_0$. The number of polynomial functions on such a group is

$$|\mathbf{A}| \cdot \exp \mathbf{A} = |\mathbf{A}| \cdot p^{\alpha_1}.$$

[1] More generally, algebras, where every compatible n-ary function is polynomial, are called n-affine complete. For details see . . . .

By Theorem 2.37, the number of compatible functions is

$$|\mathbf{A}| \cdot p^{2\alpha_2-\alpha_1} \cdot |\mathbf{C}(\mathbb{Z}_{p^{\alpha_1-\alpha_2}})|.$$

Plugging in Theorem 2.36, a simple computation shows that these numbers are equal, if and only if $\alpha_1 = \alpha_2$, or $p = 2$ and $\alpha_1 = \alpha_2 + 1$. □

3. Nilpotent groups

We may see nilpotent groups as a generalization of abelian groups. The following results are from Dorda [1977] and express that 1-affine complete p-groups are usually rather big. We will later see Dorda's example of a 1-affine complete p-group of order p^6.

3.4. Theorem (Dorda [1977]). *Let* $\mathbf{G}$ *be a 1-affine complete, non-abelian* p*-group, where* $p > 2$*. Then*

1. $\mathbf{G}' \cap \mathrm{Z}(\mathbf{G})$ *is not cyclic. (Satz 1)*
2. $\mathbf{G}'$ *is 1-affine complete. (Satz 2, Satz 2a)*

Furthermore, if $\mathbf{G}$ *is nilpotent of class 2, then*

3. *Neither* $\mathbf{G}'$ *nor* $\mathrm{Z}(\mathbf{G})$ *are cyclic.*
4. $\mathbf{G}/\mathrm{Z}(\mathbf{G})$ *is 1-affine complete. (Satz 3)*
5. $\mathbf{G}/\mathrm{Z}(\mathbf{G})$ *is the direct product of at least 3 cyclic groups or isomorphic to* $\mathbb{Z}_2 \times \mathbb{Z}_2$*. (Satz4, Satz 4a)*
6. *For no* $a \in \mathbb{N}$*, the set* $\{ag \mid g \in G\}$ *forms a cyclic subgroup of* $\mathbf{G}$ *with more than 2 elements.*
7. $|\mathrm{Z}(\mathbf{G})| \geq |\mathbf{G}'| > p^2$*. (Satz 9)*
8. *The order of* $\mathbf{G}$ *is at least* p^6*.*

4. and 5. also hold, if $p = 2$*.*

Among the examples of 1-affine complete groups later in this chapter one can find a lot of 2-groups for which the above statements are not true. In particular, there are examples of 1-affine complete groups of order 2^4, 2^5 and 2^6.

4. Symmetric groups

3.5. Theorem (Kaiser [1977]). *Let* $\mathbf{G}$ *be a finite group having precisely one minimal normal subgroup* $\mathbf{N}$ *of order not equal to 2. Then* $\mathbf{G}$ *is 1-affine complete, if and only if* $\mathbf{N}$ *is a non abelian simple group and* $\mathbf{G}/\mathbf{N}$ *is 1-affine complete.*

3.6. Corollary (Kaiser [1977]). *The symmetric group* S_n *of degree* n *is 1-affine complete precisely for* $n \notin \{3, 4\}$*.*

5. Generalized dihedral groups

Combining the results about compatible functions on generalized dihedral groups from the last chapter with the results on polynomial functions on these groups in Lyons and Mason [1991], we can easily describe the 1-affine complete generalized dihedral groups. This gives another infinite class of 1-affine complete groups.

3.7. Corollary (to Theorem 1.34.h and Theorem 2.62). *Let* $\mathbf{A}$ *be an abelian group. Then*

$$\mathrm{Dih}(\mathbf{A}) \text{ is 1-affine complete} \iff \mathbf{A} \text{ is 1-affine complete.}$$

Proof. Assume that $\mathbf{A}$ is a direct product of d cyclic groups of even order and some groups of odd order. By Theorem 1.34.h,

$$|\mathbf{P}(\mathrm{Dih}(\mathbf{A}))| = \begin{cases} 4|\mathbf{P}(\mathbf{A})|^2 & \text{if } |\mathbf{A}| \text{ is odd,} \\ \frac{1}{2^d}|\mathbf{P}(\mathbf{A})|^2 & \text{if } |\mathbf{A}| \text{ is even.} \end{cases}$$

If $|\mathbf{A}|$ is odd, then $2\mathbf{A} = \mathbf{A}$, so by Theorem 2.62,

$$|\mathbf{C}(\mathrm{Dih}(\mathbf{A}))| = 4|\mathbf{C}(\mathbf{A})|^2.$$

If $|\mathbf{A}|$ is even, then $\mathbf{A}/2\mathbf{A} \cong (\mathbb{Z}_2)^d$. By Corollary 3.3, $|\,\mathrm{C}((\mathbb{Z}_2)^d)| = 2^{d+1}$, and by Theorem 2.62,

$$\begin{aligned} |\mathbf{C}(\mathrm{Dih}(\mathbf{A}))| &= 2^{d+2} \cdot \left[\frac{|\mathbf{C}(\mathbf{A})|}{2^{d+1}}\right]^2 \\ &= \frac{1}{2^d} \cdot |\mathbf{C}(\mathbf{A})|^2 \end{aligned}$$

In both cases, the numbers $|\mathbf{P}(\mathrm{Dih}(\mathbf{A}))|$ and $|\mathbf{C}(\mathrm{Dih}(\mathbf{A}))|$ coincide, if and only if $|\mathbf{P}(\mathbf{A})| = |\mathbf{C}(\mathbf{A})|$. □

6. Quotients

Is 1-affine completeness hereditary? Are quotients of 1-affine complete groups 1-affine complete? Good ones are, others may be.

3.8. Theorem. *Let* $\mathbf{G}$ *be a 1-affine complete group,* $\mathbf{N} \trianglelefteq \mathbf{G}$ *such that* $\mathbf{N}$ *admits lifting of compatible functions. Then* $\mathbf{G}/\mathbf{N}$ *is 1-affine complete.*

Proof. Let $\psi \in \mathrm{C}(\mathbf{G}/\mathbf{N})$. Then ψ can be lifted to some $\varphi \in \mathrm{C}(\mathbf{G}) = \mathrm{P}(\mathbf{G})$. Thus $\psi = \varphi^{\mathbf{N}}$ is polynomial. □

It is interesting to read this theorem in the following way: If $\mathbf{G}$ has a normal subgroup $\mathbf{N}$, which admits lifting of compatible functions, but $\mathbf{G}/\mathbf{N}$ is not 1-affine complete, then $\mathbf{G}$ is not 1-affine complete.

If there are compatible functions on the quotient, which can not be lifted, then the quotient may be 1-affine incomplete. The 1-affine complete group $\mathbb{Z}_4 \times \mathbb{Z}_2$ has two normal subgroups with quotient isomorphic to the 1-affine incomplete group $\mathbb{Z}_4$.

The converse of Theorem 3.8 is not true in general. The group $\mathbb{Z}_4$ has a quotient isomorphic to $\mathbb{Z}_2$, which is 1-affine complete. So every compatible function on the quotient can be lifted, by Lemma 2.28. After all, $\mathbb{Z}_4$ is not 1-affine complete.

7. Direct products

By Corollary 3.3, the direct product of an abelian group $\mathbf{G}$ with itself is 1-affine complete and the direct product of abelian 1-affine complete groups is 1-affine complete. In the non-abelian case nothing of this kind is true anymore in general, as the following examples show.

7.1. The direct product of a group by itself.

The direct product of the symmetric group S_3 with itself is not 1-affine complete: Let $\mathbf{N}$ be the unique nontrivial normal subgroup of S_3. Factoring $S_3 \times S_3$ by the normal subgroup $\mathbf{N} \times \{0\}$, we get a quotient isomorphic to $\mathbb{Z}_2 \times S_3 \cong D_{12}$. By Corollary 3.7, this quotient is not 1-affine complete. Since $\mathbf{N} \times \{0\}$ is minimal and distributive as an element of the lattice of normal subgroups of $S_3 \times S_3$, every compatible function on the quotient can be lifted to a compatible function on $S_3 \times S_3$, so the group $S_3 \times S_3$ is not 1-affine complete, by Theorem 3.8.

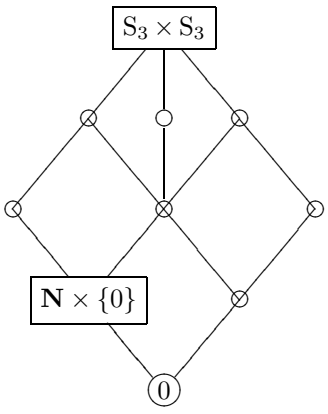

FIGURE 3.1. The lattice of normal subgroups of $S_3 \times S_3$

7.2. The direct product of 1-affine complete groups.

The direct product of 1-affine complete groups is 1-affine complete, if their lengths are coprime, because in this case

$$\mathbf{C}(\mathbf{G}\times\mathbf{H})\cong\mathbf{C}(\mathbf{G})\times\mathbf{C}(\mathbf{H})=\mathbf{P}(\mathbf{G})\times\mathbf{P}(\mathbf{H})\cong\mathbf{P}(\mathbf{G}\times\mathbf{H}).$$

But not even the direct product of a 1-affine complete group with itself is always 1-affine complete. An example is the direct product $\mathbf{G}$ of $\mathbf{D}:=\mathrm{Dih}(\mathbb{Z}_2\times\mathbb{Z}_4)\cong\mathbb{Z}_2\times\mathrm{D}_8$ (by Lemma2.58) with itself. The normal subgroup $\mathbf{A}:=\{0\}\times\mathbf{D}'$ is of order 2, the quotient $\mathbf{G}/\mathbf{A}$ is isomorphic to $\mathbf{D}\times(\mathbb{Z}_2)^2\cong\mathrm{Dih}((\mathbb{Z}_2)^4\times\mathbb{Z}_4)$, which is 1-affine complete. So $\mathbf{A}$ admits lifting of compatible functions. Every normal subgroup not containing $\mathbf{A}$ is contained in $\mathbf{D}\times\mathbb{Z}_2\times\mathrm{D}'_8$, which is a normal subgroup of index 4. Hence the sum of all normal subgroups not containing $\mathbf{A}$ has at least index 4 in $\mathbf{G}$. Therefore, $|\mathbf{C}(\mathbf{G})|\geq|\mathbf{C}(\mathrm{Dih}((\mathbb{Z}_2)^4\times\mathbb{Z}_4))|\cdot 2^4=2^{15}$. The number of polynomial functions can be computed as $|\mathbf{G}|\cdot\lambda(\mathbf{G})\cdot[\mathbf{G}:\mathrm{Z}(\mathbf{G})]=2^8\cdot 2^2\cdot 2^4=2^{14}$, by (1.3). Hence $\mathbf{G}$ is not 1-affine complete. Alternatively, we could show that the function $\varphi:D\times D\to D\times D$, $(x,y)\mapsto(0,2y)$ is compatible on $\mathbf{G}$. It is not polynomial, by [Scott, 1969, Theorem 2.3].

8. Conditions on the normal subgroups

In this section we try to gather restrictions to the lattice of normal subgroups or particular normal subgroups of a group, which ensure its 1-affine completeness.

3.9. Theorem ([Dorda, 1977, Lemma 8]). *Let $\mathbf{G}$ be a group, such that $\mathbf{G}'$ is non-abelian, $\mathbf{G}'$ is the only minimal normal subgroup of $\mathbf{G}$, and $\mathbf{G}/\mathbf{G}'\cong(\mathbb{Z}_2)^n$, for some $n\in\mathbb{N}$. Then $\mathbf{G}$ is 1-affine complete and*

$$|\mathbf{C}(\mathbf{G})|=|\mathbf{P}(\mathbf{G})|=2^{n+1}|\mathbf{G}'|^{2^n|\mathbf{G}'|}.$$

Examples of such groups are the symmetric groups S_n, for $n>4$.

3.10. Corollary (to Theorem 2.29). *Let $\mathbf{G}$ be a group having a normal subgroup $\mathbf{M}$, such that $\mathbf{G}/\mathbf{M}$ is 1-affine complete. Let $\mathbf{K}$ be the sum of all normal subgroups having trivial intersection with $\mathbf{M}$. Then every compatible function φ, with $\varphi(G)\subseteq M$ is constant on the cosets of $\mathbf{K}$ in $\mathbf{G}$.*

In particular, if $\mathbf{K}=\mathbf{G}$, then $\mathbf{G}$ is 1-affine complete.

Proof. Every compatible function on $\mathbf{G}/\mathbf{M}$ is polynomial. By Theorem 2.29, every compatible function from G into M is constant on the cosets of $\mathbf{K}$ in $\mathbf{G}$.

If $\mathbf{K}=\mathbf{G}$, then every compatible function φ, with $\varphi(G)\subseteq M$ is constant, hence it is polynomial. As a consequence, every compatible function on $\mathbf{G}$ is polynomial. □

As an application of Corollary 3.10, we show, how it can be used to find some more 1-affine complete groups. In the following examples, the normal subgroup $\mathbf{K}$

constructed as in Corollary 3.10, is a proper normal subgroup. Nevertheless we will be able to prove 1-affine completeness. The only additional work is to show that every compatible function, that is constant on the cosets of $\mathbf{K}$, is polynomial.

8.1. The groups $Q_8 \times(\mathbb{Z}_2)^d$.

We have seen, that the group $D_8 \times(\mathbb{Z}_2)^d$ ($d \in \mathbb{N}$) is isomorphic to $\mathrm{Dih}(\mathbb{Z}_4 \times (\mathbb{Z}_2)^d)$, which is 1-affine complete. The groups Q_8 and D_8 are so similar, let us prove that the groups $Q_8 \times(\mathbb{Z}_2)^d$ are also 1-affine complete.

In this example we use a counting argument to guarantee that every compatible function, that is constant on the cosets of $\mathbf{K}$, is polynomial.

Let $\mathbf{G}$ be the group $Q_8 \times(\mathbb{Z}_2)^d$. Then $\mathbf{M} = \mathbf{G}'$ is a minimal normal subgroup and the quotient $\mathbf{G}/\mathbf{M} \cong (\mathbb{Z}_2)^{d+2}$ is 1-affine complete. The sum of the minimal normal subgroups not equal to $\mathbf{M}$ is the center of $\mathbf{G}$, which has index 4 in $\mathbf{G}$. Hence there are 4 cosets and as a consequence 2^4 functions from $\mathbf{G}$ to $\mathbf{M}$, which are constant on these cosets. It remains to show that each of these is polynomial. By equation (1.11),

$$|\mathbf{P}(\mathbf{G})| = |\mathbf{P}(\mathbf{G}/\mathbf{M})| \cdot |(\mathbf{M} : \mathbf{G})_{\mathbf{P}(\mathbf{G})}|.$$

By (1.3), $|\mathbf{P}(\mathbf{G})| = |\mathbf{G}| \cdot \lambda(\mathbf{G}) \cdot [\mathbf{G} : \mathrm{Z}(\mathbf{G})] = 2^{d+3} \cdot 2^2 \cdot 2^2 = 2^{d+7}$ and $|\mathbf{P}(\mathbf{G}/\mathbf{M})| = 2^{d+3}$, whence $|(\mathbf{M} : \mathbf{G})_{\mathbf{P}(\mathbf{G})}| = 2^4$. So all of these functions are polynomial.

8.2. The group 32/33.

This example is a semidirect product, which can be easily described. This time we simply list all zerosymmetric compatible functions, which are constant on the cosets of $\mathbf{K}$, and check that each of them is polynomial. This makes sense, because the index of $\mathbf{K}$ is only 2.

Let $\mathbf{G}$ be the semi-direct product of $\mathbf{A} = (\mathbb{Z}_2)^4$ with $\mathbb{Z}_2$, where $\mathbb{Z}_2$ acts on $\mathbf{A}$ via the automorphism $\alpha : A \to A$, $(x_1, x_2, x_3, x_4) \mapsto (x_1 + x_3, x_2 + x_4, x_3, x_4)$. We show that this group is 1-affine complete. We write elements of $\mathbf{G}$ as pairs of such vectors and elements from $\{0, 1\}$.

We choose the minimal normal subgroup on

$$M := \{((0,0,0,0),0), ((1,0,0,0),0)\}.$$

The quotient $\mathbf{G}/\mathbf{M}$ is isomorphic to $\mathrm{Dih}(\mathbb{Z}_2 \times \mathbb{Z}_4)$, which is 1-affine complete, by Corollary 3.7. We can see this easily in the following way: A presentation for $\mathbf{G}$ is: $\langle a, b, c, d, e; 2a, 2b, 2c, 2d, 2e, c^e = a + c, d^e = b + d,$ all other generators commute $\rangle$. Now we factor by the normal subgroup $\{0, a\}$, and get the following presentation for $\mathbf{G}/\mathbf{M}$: $\langle b, c, d, e; 2b, 2c, 2d, 2e, d^e = b + d,$ all other generators commute $\rangle$. A presentation for $\mathrm{Dih}(\mathbb{Z}_2 \times \mathbb{Z}_4)$ is $\langle A, B, C; 4A, 2B, 2C, A^C = 3A,$ all other generators commute $\rangle$. It is now easy to check that the homomorphism defined by $A \mapsto d + e$,

$B \mapsto c$ and $C \mapsto e$ (and as a consequence $2A \mapsto b$), is an isomorphism between $\mathrm{Dih}(\mathbb{Z}_2 \times \mathbb{Z}_4)$ and $\mathbf{G}/\mathbf{M}$.

The subgroups $\mathbf{I}_1$ generated by $((1,1,0,0),0)$ and $((0,0,1,1),0)$ and $\mathbf{I}_2$ generated by $((1,0,0,1),0)$ and $((0,1,0,0),0)$ are two normal subgroups, they are both 2-dimensional subspaces of the 4-dimensional vector space $(\mathbf{A},0)$. Their intersection is trivial, whence their sum is $(\mathbf{A},0)$. Both $\mathbf{I}_1 \cap \mathbf{M}$ and $\mathbf{I}_2 \cap \mathbf{M}$ are trivial, so the sum of all normal subgroups having trivial intersection with $\mathbf{M}$ is at least $\mathbf{I}_1 + \mathbf{I}_2 = (\mathbf{A},0)$.

By Corollary 3.10, it remains to show that every compatible zero-symmetric function, which is constant on the cosets of $(\mathbf{A},0)$, is polynomial. The polynomial function $x \mapsto [x,((0,0,1,0),0)]$ maps every $g \in (A,0)$ to $((0,0,0,0),0)$ and every $g \in (A,1)$ to $((1,0,0,0),0)$. This is the only nonzero compatible zero-symmetric function, which is constant on the cosets of $(\mathbf{A},0)$.

Center and derived subgroup of this group coincide with the subgroup of $\mathbf{G}$ generated by $((1,0,0,0),0)$ and $((0,1,0,0),0)$. So $\mathbf{G}$ is nilpotent of class 2. From Chapter 1, we know that

$$|\mathbf{C}(\mathbf{G})| = |\mathbf{P}(\mathbf{G})| = |\mathbf{G}| \cdot \lambda(\mathbf{G}) \cdot [\mathbf{G} : \mathrm{Z}(\mathbf{G})] = 2^5 \cdot 2^2 \cdot 2^3 = 2^{10}$$

and every compatible function is of the form

$$x \mapsto a + kx + [x,b],$$

where $a, b \in G$ and $k \in \{0,1,2,3\}$.

8.3. The group 32/35.

Computer investigations have shown that the small non-abelian 1-affine groups we have seen so far are $\mathrm{Dih}(\mathbb{Z}_2 \times \mathbb{Z}_4)$, $\mathrm{Dih}((\mathbb{Z}_2)^2 \times \mathbb{Z}_4)$, $\mathrm{Dih}((\mathbb{Z}_4)^2)$, $\mathrm{Dih}((\mathbb{Z}_3)^2)$, $\mathrm{Q}_8 \times \mathbb{Z}_2$, $\mathrm{Q}_8 \times (\mathbb{Z}_2)^2$, 32/33 and 32/35. In order to fill the last gap, we conclude this section showing that 32/35 is 1-affine complete. We omit the details of the proof.

Let $\mathbf{G}$ be the group $\langle a,b,c; 4a, 4b, 2c = 2a, [a,b], a^c = -a, b^c = -b\rangle$.

The subgroup $\mathbf{M} := \langle 2a\rangle$ is normal. The quotient $\mathbf{G}/\mathbf{M}$ is isomorphic to $\mathrm{Q}_8 \times \mathbb{Z}_2$, which is 1-affine complete. The sum of all normal subgroups having trivial intersection with $\mathbf{M}$ is $\mathbf{K} = \langle a,b\rangle$ and has index 2 in $\mathbf{G}$. The polynomial function $x \mapsto [3a,x]$ maps K to 0 and the second coset of $\mathbf{K}$ in $\mathbf{G}$ to $2a$. This group is 1-affine complete.

9. Hamiltonian groups

Hamiltonian groups are groups of the type $\mathbf{A} \times \mathrm{Q}_8 \times \mathbf{B}$, where Q_8 is the eight element quaternion group, $\mathbf{A}$ is an abelian group of odd order, and $\mathbf{B}$ is a group of exponent at most 2.

Since $(|\mathbf{A}|, |\,\mathrm{Q}_8 \times\mathbf{B}|) = 1$,

$$|\mathbf{P}(\mathbf{A} \times \mathrm{Q}_8 \times\mathbf{B})| = |\mathbf{P}(\mathbf{A})| \cdot |\mathbf{P}(\mathrm{Q}_8 \times\mathbf{B})|$$

and

$$|\mathbf{C}(\mathbf{A} \times \mathrm{Q}_8 \times\mathbf{B})| = |\mathbf{C}(\mathbf{A})| \cdot |\mathbf{C}(\mathrm{Q}_8 \times\mathbf{B})|.$$

Moreover the sizes of the near rings over $\mathbf{A}$ are odd, the sizes of the near rings over $\mathrm{Q}_8 \times\mathbf{B}$ are a power of 2. Therefore such a group is 1-affine complete, if and only if $\mathrm{Q}_8 \times\mathbf{B}$ is 1-affine complete and $\mathbf{A}$ is 1-affine complete.

We know, that $|\mathbf{C}(\mathrm{Q}_8)| = 2^{11}$ and $|\mathbf{P}(\mathrm{Q}_8)| = 2^7$, so $\mathrm{Q}_8 \times\mathbf{B}$ is not 1-affine complete, if $|\mathbf{B}| = 1$. Otherwise $\mathbf{B}$ is elementary abelian of exponent 2, and we know $\mathrm{Q}_8 \times\mathbf{B}$ is 1-affine complete.

10. Dorda's example

In Dorda [1977], Dorda shows that a 1-affine complete p-group of nilpotency class 2 ($p \neq 2$) has at least p^6 elements (recall Theorem 3.4) and constructs such a group of order p^6. The example shown is the group

$$\langle a, b, c, d, e, f \ ; \ pa, pb, pc, pd, pe, pf,$$
$$[a, b] = d, [a, c] = e, [b, c] = f, \text{ all other generators commute}\rangle.$$

The exponent of this group is p and the index of the center is p^3, whence there are p^{10} polynomial (compatible) functions on this group (c.f. Chapter 1).

11. The groups 16/9 and 16/10

In Section 5.14 of Chapter 3 we computed the number of compatible functions on these groups as 2^9. From the results in Chapter 1 we know that there are 2^8 polynomial functions on each of these groups. So these groups are not 1-affine complete. An alternative way would be to show that the function

$$\varphi : G \to G$$
$$g \mapsto \begin{cases} e & \text{if } g \in \mathrm{Z}(G), \\ 0 & \text{otherwise} \end{cases}$$

where e denotes the non-zero element of the 2-element derived subgroup of $\mathbf{G}$, is polynomial. (The function is compatible: it is compatible with every normal subgroup of $\mathbf{G}$ containing $\mathbf{G}'$, because its range is G', and it is constant on the cosets of the sum of all other normal subgroups, whence compatible with these).

12. Results

3.11. Conjecture. *I believe that the only non abelian 1-affine complete groups of order at most 63 are the generalized dihedral groups of abelian 1-affine complete groups, the groups* $\mathrm{Q}_8 \times (\mathbb{Z}_2)^n$ *(*$n \geq 1$*) and the groups* 32/33 *and* 32/35.

13. Other coincidences

Question: Is it possible to have

$$\mathbf{P}(\mathbf{G}) \leq \mathrm{LP}(\mathbf{G}) < \mathrm{L_2P}(\mathbf{G}) = \mathbf{C}(\mathbf{G}) = \mathbf{M}(\mathbf{G}) = \mathrm{L_1P}(\mathbf{G}) \tag{3.1}$$

for a group $\mathbf{G}$?

Answer: For any finite group $\mathbf{G}$, $|\mathbf{G}| > 2$,

$$\mathbf{G} \text{ is cyclic of prime order} \iff \mathbf{G} \text{ fulfills (3.1).}$$

Proof. Clearly,

$$\mathbf{C}(\mathbf{G}) = \mathbf{M}(\mathbf{G}) \iff \mathbf{G} \text{ is simple.}$$

By [Aichinger, 1994, Corollary 4.17], a group fulfilling (3.1) must be abelian. □

Question: Is there happening anything of interest in the series

$$\mathbf{C}(\mathbf{G}) \leq \mathrm{LC}(\mathbf{G}) \leq \ldots \leq \mathrm{L_2C}(\mathbf{G}) \leq \mathrm{L_2C}(\mathbf{G})?$$

Answer: No, from $\mathrm{L}_m(\mathrm{L}_n\mathrm{P}(\mathbf{G})) = \mathrm{L}_{min(m,n)}\mathrm{P}(\mathbf{G})$ (see Aichinger [1994]) and $\mathrm{L_2P}(\mathbf{G}) = \mathbf{C}(\mathbf{G})$, the following is obvious.

$$\mathbf{C}(\mathbf{G}) = \mathrm{L_2C}(\mathbf{G}) \leq \mathrm{L_1C}(\mathbf{G}) = \mathbf{M}(\mathbf{G})$$

So "locally compatible" functions are compatible functions.

CHAPTER 4

Sundries

1. Finding the identity in a near ring of transformations

Let Γ be an arbitrary group and $\mathbf{N} \leq \mathbf{M}(\Gamma)$. Clearly, if the identity transformation id is an element of $\mathbf{N}$, the near ring has an identity and it is id. The converse, in general, is not true, as the following example demonstrates:

4.1. Example. Let $\Gamma = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbf{N} = (\{\bar{0}, \pi_1\}, +, \circ)$, where π_1 is the projection onto the first component of Γ. Then $\mathbf{N}$ is a near ring with identity π_1 (in fact, $\mathbf{N} \cong (\mathbb{Z}_2, +, \cdot)$).

Nevertheless, the identity in $\mathbf{N}$ (if it exists) is not too far from the identity transformation. In the sequel we give some necessary conditions for a transformation i to be the identity of $\mathbf{N}$.

For all $n \in N$ and all $x \in \Gamma$ we have $i(n(x)) = (in)(x) = n(x)$. Hence

$$i|_{\mathbf{N}(\Gamma)} = id|_{\mathbf{N}(\Gamma)} \tag{4.1}$$

is a necessary condition for i to be the near ring's identity. On $\mathbf{N}(\Gamma)$ it has to behave like the identity mapping. (Remark: $\mathbf{N}(\Gamma)$ can be computed from a set of generators of $\mathbf{N}$ (c.f. Aichinger *et al.* [2000a]).)

Furthermore for all $n \in N$ and all $x \in \Gamma$ we have $n(i(x)) = (ni)(x) = n(x)$, or equivalently $i(x) \in n^{-1}(n(x))$. So $i(x) \in I_x := N(\Gamma) \cap \bigcap_{n \in N} n^{-1}(n(x))$. If for some $x \in \Gamma$ the set I_x is empty, $\mathbf{N}$ clearly has no identity. On the other hand, if I_x contains more than one element for some $x \in \Gamma$, also $\mathbf{N}$ has no identity. This can be seen as follows: Suppose, $a, b \in I_x$ and $a \neq b$. Then $a, b \in N(\Gamma)$ and $\forall\, n \in N\ : n(a) = n(x) = n(b)$. In particular $i(a) = i(b)$, but a and b are from $N(\Gamma)$ (whereupon i acts as identity transformation by (4.1)). So $i(a) = a \neq b = i(b)$, a contradiction. Fortunately, the condition $n(i(x)) = n(x)$ only has to be tested for a set of generators of $\mathbf{N}$, because from $n(i(x)) = n(x)$ and $m(i(x)) = m(x)$, we get immediately that $m(n(i(x))) = m(n(x))$ and $(m + n)(i(x)) = (m + n)(x)$. Summarizing, if $\mathbf{N}$ is generated by E,

$$\forall\, x \in \Gamma\ :\ |\mathbf{N}(\Gamma) \cap \bigcap_{n \in E} n^{-1}(n(x))| = 1. \tag{4.2}$$

Conditions (4.1) and (4.2) uniquely determine i (or contradict the existence of an identity). If in addition $i \in N$, then i is the identity of $\mathbf{N}$. So, the problem of

deciding whether a near ring of transformations on a group has an identity can be reduced to the problem of deciding membership of a single transformation.

Algorithm 3 constructs the element i, if it exists.

Algorithm 3 Identity

Let $\mathbf{N}$ be a near ring of transformations on the group Γ.

Require: E a set of generators of $\mathbf{N}$.
Ensure: Find an identity, if there is one.
  for $x \in \Gamma$ **do**
    $I_x := \bigcap_{n \in E}(N(\Gamma) \cap n^{-1}nx)$;
    if $|I_x| \neq 1$ **then**
      return ($\mathbf{N}$ has no identity);
    end if
    Define $i(x)$ to be the unique element in I_x.
  end for
  if $i \in N$ or $\mathbf{N}$ contains an identity **then**
    return (i is the identity of $\mathbf{N}$);
  else
    return ($\mathbf{N}$ has no identity);
  end if

CHAPTER 5

Benchmarks

In this chapter we compare several methods for computing compatible functions on groups.

Method A enumerates all compatible functions on a group. Given a partial function on the group all possible extensions to a total function are computed.

Method B computes $L_2P(\mathbf{G})$, the 2-local near ring of the polynomial near ring on the group $\mathbf{G}$ (Theorem 2.8).

Method C uses chains of lattice generators of the lattice of normal subgroups of the group (Theorem 2.74).

Method D uses the lifting process from a cyclic factor in the abelian case (Theorem 2.38, Theorem 2.39).

Method E uses the liftability and distributivity related results in the previous chapters and assumes that all 1-affine complete nontrivial quotients are known (Theorem 2.13, Theorem 2.30, Lemma 2.28).

Listed is the time needed to compute a strong generating set of the additive group of the near ring of compatible functions. In case of method A, the time needed to enumerate all compatible functions is listed, instead.

These benchmarks were computed on a Pentium II/333 with 512MB RAM running under a Linux operating system. We have computed 45000 GAP-stones[1] for this machine.

[1] A certain program running under GAP computes a number – the GAP-stones of the computer – reflecting its speed. See GAP [1999] for more details

group	A	B	C	D
$\mathbb{Z}_2$	< 1 sec.			
$\mathbb{Z}_3$				
$\mathbb{Z}_4$				
$(\mathbb{Z}_2)^2$				
$\mathbb{Z}_5$				
$\mathbb{Z}_6$	1 sec.	1.2 sec.	< 1 sec.	
$\mathbb{Z}_7$	35.7 sec.	< 1 sec.		
$\mathbb{Z}_8$	1.1 min.	2.9 sec.	< 1 sec.	
$\mathbb{Z}_2 \times \mathbb{Z}_4$	2.2 sec.	5.7 sec.		
$(\mathbb{Z}_2)^3$	< 1 sec.	9.0 sec.		
$\mathbb{Z}_9$	11.5 min.	4.2 sec.		
$(\mathbb{Z}_3)^2$	1.6 sec.	8.0 sec.		
$\mathbb{Z}_{10}$	5.5 min.	8.7 sec.		
$\mathbb{Z}_{11}$	-	25.8 sec.		
$\mathbb{Z}_{12}$	1.5 min.	1.7 min.	1.5 sec.	< 1 sec.
$\mathbb{Z}_2 \times \mathbb{Z}_6$	31.5 sec.	34.7 sec.	< 1 sec.	
$\mathbb{Z}_{13}$	-	1.5 min.		
$\mathbb{Z}_{14}$	-	3.5 min.	2.2 sec.	0.7 sec.
$\mathbb{Z}_{15}$	-	5.4 min.	2.4 sec.	1.2 sec.
$\mathbb{Z}_{16}$	-	13.9 min.	1.5 sec.	0.8 sec.
$\mathbb{Z}_2 \times \mathbb{Z}_8$	16.6 min.	13.7 min.	8.0 sec.	0.2 sec.
$\mathbb{Z}_4 \times \mathbb{Z}_4$	20.0 sec.	9.2 min.	6.0 sec.	0.02 sec.
$(\mathbb{Z}_2)^2 \times \mathbb{Z}_4$	21.8 sec.	15.0 min.	18.0 sec.	0.02 sec.
$(\mathbb{Z}_2)^4$	10.3 sec.	24.5 min.	44.0 sec.	0.03 sec.
$\mathbb{Z}_{17}$	-	9.0 min.	< 1 sec.	
$\mathbb{Z}_{18}$	-	22.5 min.	4.9 sec.	1.6 sec.
$\mathbb{Z}_3 \times \mathbb{Z}_6$	44.0 sec.	19.2 min.	7.3 sec.	0.1 sec.

TABLE 5.1. Running times for the computation of $\mathbf{C}(\mathbf{G})$. Abelian groups of orders 2–18

group	C	D	E
$\mathbb{Z}_{19}$	< 1 sec.		1.4 sec.
$\mathbb{Z}_{20}$	6.6 sec.	2.6 sec.	2.1 sec.
$\mathbb{Z}_2 \times \mathbb{Z}_{10}$	8.1 sec.	0.2 sec.	1.5 sec.
$\mathbb{Z}_{21}$	8.6 sec.	3.4 sec.	0.5 sec.
$\mathbb{Z}_{22}$	10.5 sec.	4.7 sec.	0.4 sec.
$\mathbb{Z}_{23}$	< 1 sec.		
$\mathbb{Z}_{24}$	14.0 sec.	6.1 sec.	1.3 sec.
$\mathbb{Z}_2 \times \mathbb{Z}_{12}$	26.0 sec.	0.3 sec.	1.8 sec.
$(\mathbb{Z}_2)^3 \times \mathbb{Z}_3$	35.0 sec.	0.3 sec.	2.0 sec.
$\mathbb{Z}_{25}$	3.2 sec.	5.4 sec.	0.4 sec.
$(\mathbb{Z}_5)^2$	4.7 min.	0.05 sec.	12.3 sec.
$\mathbb{Z}_{26}$	22.0 sec.	9.5 sec.	0.6 sec.
$\mathbb{Z}_{27}$	6.0 sec.	7.3 sec.	0.7 sec.
$\mathbb{Z}_3 \times \mathbb{Z}_9$	42 sec.	0.3 sec.	0.8 sec.
$(\mathbb{Z}_3)^3$	1.5 min.	0.06 sec.	1.0 sec.
$\mathbb{Z}_{28}$	27.0 sec.	11.0 sec.	0.8 sec.
$\mathbb{Z}_2 \times \mathbb{Z}_{14}$	27.0 sec.	0.5 sec.	1.3 sec.
$\mathbb{Z}_{29}$	< 1 sec.		
$\mathbb{Z}_{30}$	53.0 sec.	19.5 sec.	0.9 sec.
$\mathbb{Z}_{31}$	< 1 sec.		
$\mathbb{Z}_{32}$	10.0 sec.	11.7 sec.	1.6 sec.
$\mathbb{Z}_2 \times \mathbb{Z}_{16}$	2.8 min.	1.0 sec.	2.2 min.
$\mathbb{Z}_4 \times \mathbb{Z}_8$	2.5 min.	0.07 sec.	3.2 sec.
$(\mathbb{Z}_2)^2 \times \mathbb{Z}_8$	6.4 min.	0.5 sec.	4.2 sec.
$\mathbb{Z}_2 \times (\mathbb{Z}_4)^2$	5.5 min.	0.1 sec.	4.4 sec.
$(\mathbb{Z}_2)^3 \times \mathbb{Z}_4$	11.0 min.	0.5 sec.	6.2 sec.
$(\mathbb{Z}_2)^5$	21.3 min.	0.08 sec.	8.3 sec.

TABLE 5.2. Running times for the computation of $\mathbf{C}(\mathbf{G})$. Abelian groups of orders 19–32

group	B	C	E
6/2	1.0 sec.	1.3 sec.	0.7 sec.
8/4	5.6 sec.	0.9 sec.	0.8 sec.
8/5	5.0 sec.	0.6 sec.	0.4 sec.
10/2	10.4 sec.	0.1 sec.	0.1 sec.
12/3	35.0 sec.	1.3 sec.	0.4 sec.
12/4	22.8 sec.	0.4 sec.	0.9 sec.
12/5	1.9 min.	1.3 sec.	0.6 sec.
14/2	55.3 sec.	0.2 sec.	0.2 sec.
16/6	4.1 min.	5.3 sec.	1.7 sec.
16/7	15.8 min.	12.5 sec.	1.0 sec.
16/8	16.6 min.	14.0 sec.	1.4 sec.
16/9	16.6 min.	7.5 sec.	1.3 sec.
16/10	15.0 min.	6.9 sec.	1.0 sec.
16/11	13.4 min.	9.5 sec.	1.0 sec.
16/12	10.5 min.	5.7 sec.	1.7 sec.
16/13	13.7 min.	8.4 sec.	1.1 sec.
16/14	15.1 min.	7.7 sec.	1.0 sec.
18/3	13.9 min.	2.6 sec.	0.6 sec.
18/4	22.1 min.	1.4 sec.	0.4 sec.
18/5	30.8 min.	9.5 sec.	7.9 sec.
20/3	43.3 min.	7.7 sec.	1.2 sec.
20/4	48.6 min.	7.4 sec.	0.6 sec.
20/5	47.3 min.	1.5 sec.	0.5 sec.

TABLE 5.3. Running times for the computation of $\mathbf{C}(\mathbf{G})$. Non abelian groups of orders 2–20

group	B	C	E
21/2	50.6 min.	1.9 sec.	0.3 sec.
22/2	1.0 hrs	1.9 sec.	0.2 sec.
24/4	3.2 hrs	33.4 sec.	1.5 sec.
24/5	2.2 hrs	9.4 sec.	0.9 sec.
24/6	3.4 hrs	19.0 sec.	1.6 sec.
24/7	2.7 hrs	16.7 sec.	2.4 sec.
24/8	3.1 hrs	14.8 sec.	1.7 sec.
24/9	-	18.9 sec.	1.0 sec.
24/10	-	17.8 sec.	1.2 sec.
24/11	-	28.3 sec.	1.1 sec.
24/12	-	1.0 sec.	0.9 sec.
24/13	-	3.4 sec.	0.8 sec.
24/14	-	14.8 sec.	1.3 sec.
24/15	-	33.2 sec.	1.9 sec.
26/2	-	2.9 sec.	0.3 sec.
27/4	-	77.3 sec.	1.1 sec.
27/5	-	69.3 sec.	0.7 sec.
28/3	-	31.3 sec.	0.7 sec.
28/4	-	29.0 sec.	0.6 sec.
30/2	-	10.8 sec.	0.6 sec.
30/3	-	11.9 sec.	0.7 sec.
30/4	-	22.1 sec.	0.6 sec.

TABLE 5.4. Running times for the computation of $\mathbf{C}(\mathbf{G})$. Non abelian groups of orders 21–30

group	C	E	group	C	E
32/8	8.3 min.	7.4 sec.	32/30	2.1 min.	1.8 min.
32/9	7.7 min.	6.1 sec.	32/31	3.0 min.	2.5 sec.
32/10	7.0 min.	6.1 sec.	32/32	2.8 min.	2.2 sec.
32/11	6.1 min.	4.2 sec.	32/33	4.2 min.	3.8 min.
32/12	4.8 min.	3.2 sec.	32/34	4.1 min.	3.7 min.
32/13	4.5 min.	4.3 sec.	32/35	3.6 min.	3.6 sec.
32/14	4.2 min.	3.6 sec.	32/36	4.8 min.	3.5 min.
32/15	3.9 min.	3.6 sec.	32/37	3.6 min.	3.6 sec.
32/16	4.1 min.	3.9 sec.	32/38	3.8 min.	3.4 min.
32/17	6.6 min.	5.3 sec.	32/39	3.8 min.	3.4 min.
32/18	2.5 min.	3.4 sec.	32/40	3.5 min.	4.1 sec.
32/19	2.1 min.	3.1 sec.	32/41	3.5 min.	3.2 min.
32/20	1.9 min.	1.7 min.	32/42	6.6 min.	6.5 sec.
32/21	1.7 min.	1.4 min.	32/43	8.9 min.	6.4 sec.
32/22	4.1 min.	2.3 sec.	32/44	6.2 min.	3.5 sec.
32/23	4.4 min.	3.9 min.	32/45	6.2 min.	4.4 sec.
32/24	4.1 min.	3.7 min.	32/46	3.3 min.	2.7 sec.
32/25	4.0 min.	3.6 min.	32/47	3.2 min.	2.5 sec.
32/26	8.5 min.	3.2 sec.	32/48	3.1 min.	2.4 sec.
32/27	2.3 min.	2.0 min.	32/49	2.7 min.	2.1 sec.
32/28	2.1 min.	1.9 min.	32/50	2.7 min.	2.1 sec.
32/29	2.1 min.	1.8 min.	32/51	2.5 min.	2.1 sec.

TABLE 5.5. Running times for the computation of $\mathbf{C}(\mathbf{G})$. Non abelian groups of order 32

APPENDIX A

Small Groups

A complete list of the small groups of order at most 32 has been published by Thomas and Wood in Thomas and Wood [1980]. We use their notation, whenever we name a small group, which has no general-known name, in particular, if the group is a semidirect product, which we do not want to describe explicitely. Below, we list some of the most commonly used names for the small groups in Thomas and Wood [1980].

2/1	$\mathbb{Z}_2$
3/1	$\mathbb{Z}_3$
4/1	$\mathbb{Z}_4$
4/2	$(\mathbb{Z}_2)^2$, V_4
5/1	$\mathbb{Z}_5$
6/1	$\mathbb{Z}_6$
6/2	S_3, $\mathrm{Hol}(\mathbb{Z}_3)$
7/1	$\mathbb{Z}_7$
8_1	$\mathbb{Z}_8$
8/2	$\mathbb{Z}_2 \times \mathbb{Z}_4$
8/3	$(\mathbb{Z}_2)^3$
8/4	D_8, $\mathrm{Hol}(\mathbb{Z}_4)$
8/5	Q_8
9/1	$\mathbb{Z}_9$
9/2	$(\mathbb{Z}_3)^2$
10/1	$\mathbb{Z}_{10}$
10/2	D_{10}
11/1	$\mathbb{Z}_{11}$
12/1	$\mathbb{Z}_{12}$
12/2	$(\mathbb{Z}_2)^2 \times \mathbb{Z}_3$
12/3	D_{12}, $\mathbb{Z}_2 \times S_3$, $\mathrm{Hol}(\mathbb{Z}_6)$, $\mathrm{Aut}((\mathbb{Z}_2)^2 \times \mathbb{Z}_3)$, $\mathrm{Aut}(Q_{12})$
12/4	A_4
12/5	Q_{12}
13/1	$\mathbb{Z}_{13}$
14/1	$\mathbb{Z}_{14}$
14/2	D_{14}

15/1	$\mathbb{Z}_{15}$
16/1	$\mathbb{Z}_{16}$
16/2	$\mathbb{Z}_2 \times \mathbb{Z}_8$
16/3	$(\mathbb{Z}_4)^2$
16/4	$(\mathbb{Z}_2)^2 \times \mathbb{Z}_4$
16/5	$(\mathbb{Z}_2)^5$
16/6	$\mathbb{Z}_2 \times D_8$, $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_8)$
16/7	$\mathbb{Z}_2 \times Q_8$
16/8	$(\mathbb{Z}_2 \times \mathbb{Z}_4) \rtimes \mathbb{Z}_2$
16/9	$(\mathbb{Z}_2 \times \mathbb{Z}_4) \rtimes \mathbb{Z}_2$
16/10	$\mathbb{Z}_4 \rtimes \mathbb{Z}_4$
16/11	$\mathbb{Z}_8 \rtimes \mathbb{Z}_2$
16/12	D_{16}
16/13	$\mathbb{Z}_8 \rtimes \mathbb{Z}_2$
16/14	Q_{16}
17/1	$\mathbb{Z}_{17}$
18/1	$\mathbb{Z}_{18}$
18/2	$\mathbb{Z}_2 \times (\mathbb{Z}_3)^2$
18/3	$\mathbb{Z}_3 \times S_3$
18/4	D_{18}
18/5	$\mathrm{Dih}((\mathbb{Z}_3)^2)$
19/1	$\mathbb{Z}_{19}$
20/1	$\mathbb{Z}_{20}$
20/2	$(\mathbb{Z}_2)^2 \times \mathbb{Z}_5$
20/3	D_{20}
20/4	Q_{20}
20/5	$\mathrm{Hol}(\mathbb{Z}_5)$, $\mathrm{Aut}(D_{10})$
21/1	$\mathbb{Z}_{21}$
21/2	$\mathbb{Z}_7 \rtimes \mathbb{Z}_3$
22/1	$\mathbb{Z}_{22}$
22/2	D_{22}
23/1	$\mathbb{Z}_{23}$

24/1	$\mathbb{Z}_{24}$
24/2	$(\mathbb{Z}_2 \times \mathbb{Z}_4) \times \mathbb{Z}_3$
24/3	$(\mathbb{Z}_2)^3 \times \mathbb{Z}_3$
24/4	$\mathbb{Z}_2 \times \mathrm{D}_{12}$, $(\mathbb{Z}_2)^2 \times \mathrm{S}_3$, $\mathrm{Dih}((\mathbb{Z}_2)^2 \times \mathbb{Z}_3)$, $\mathrm{Aut}(\mathbb{Z}_4 \times \mathrm{S}_3)$
24/5	$\mathbb{Z}_2 \times \mathrm{A}_4$
24/6	$\mathbb{Z}_2 \times \mathrm{Q}_{12}$
24/7	$\mathbb{Z}_3 \times \mathrm{D}_8$
24/8	$\mathbb{Z}_3 \times \mathrm{Q}_8$
24/9	$\mathbb{Z}_4 \times \mathrm{S}_3$
24/10	D_{24}
24/11	Q_{24}
24/12	S_4, $\mathrm{Aut}(\mathrm{A}_4)$, $\mathrm{Hol}((\mathbb{Z}_2)^2)$
24/13	$\mathrm{SL}(2,3)$
24/14	$\mathbb{Z}_3 \rtimes \mathbb{Z}_8$
24/15	$\mathrm{Q}_{12} \rtimes \mathbb{Z}_2$, $\mathbb{Z}_3 \rtimes \mathrm{D}_8$
25/1	$\mathbb{Z}_{25}$
25/2	$(\mathbb{Z}_5)^2$
26/1	$\mathbb{Z}_{26}$
26/2	D_{26}
27/1	$\mathbb{Z}_{27}$
27/2	$\mathbb{Z}_3 \times \mathbb{Z}_9$
27/3	$(\mathbb{Z}_3)^3$
27/4	$(\mathbb{Z}_3)^2 \rtimes \mathbb{Z}_3$
27/5	$\mathbb{Z}_9 \rtimes \mathbb{Z}_3$
28/1	$\mathbb{Z}_{28}$
28/2	$(\mathbb{Z}_2)^2 \times \mathbb{Z}_7$
28/3	D_{28}
28/4	Q_{28}
29/1	$\mathbb{Z}_{29}$
30/1	$\mathbb{Z}_{30}$
30/2	$\mathbb{Z}_3 \times \mathrm{D}_{10}$
30/3	$\mathbb{Z}_5 \times \mathrm{S}_3$
30/4	D_{30}
31/1	$\mathbb{Z}_{31}$

32/1	$\mathbb{Z}_{32}$
32/2	$\mathbb{Z}_2 \times \mathbb{Z}_{16}$
32/3	$\mathbb{Z}_4 \times \mathbb{Z}_8$
32/4	$(\mathbb{Z}_2)^2 \times \mathbb{Z}_8$
32/5	$\mathbb{Z}_2 \times (\mathbb{Z}_4)^2$
32/6	$(\mathbb{Z}2)^3 \times \mathbb{Z}_4$
32/7	$(\mathbb{Z}_2)^5$
32/8	$(\mathbb{Z}_2)^2 \times \mathrm{D}_8$
32/9	$(\mathbb{Z}_2)^2 \times \mathrm{Q}_8$
32/10	$\mathbb{Z}_2 \times 16/8$
32/11	$\mathbb{Z}_2 \times 16/9$
32/12	$\mathbb{Z}_2 \times 16/10$
32/13	$\mathbb{Z}_2 \times 16/11$
32/14	$\mathbb{Z}_4 \times \mathrm{D}_8$
32/15	$\mathbb{Z}_4 \times \mathrm{Q}_8$
32/16	$(\mathbb{Z}_4)^2 \rtimes \mathbb{Z}_2$
32/17	$(\mathbb{Z}_2 \times \mathbb{Z}_8) \rtimes \mathbb{Z}_2$
32/18	$(\mathbb{Z}_2 \times \mathbb{Z}_4) \rtimes \mathbb{Z}_4$
32/19	$\mathbb{Z}_8 \rtimes \mathbb{Z}_4$
32/20	$(\mathbb{Z}_2 \times \mathbb{Z}_8) \rtimes \mathbb{Z}_2$
32/21	$\mathbb{Z}_4 \rtimes \mathbb{Z}_8$
32/22	$\mathbb{Z}_{16} \rtimes \mathbb{Z}_2$
32/23	$\mathbb{Z}_2 \times \mathrm{D}_{16}$
32/24	$\mathbb{Z}_2 \times 16/13$
32/25	$\mathbb{Z}_2 \times \mathrm{Q}_{16}$
32/26	$(\mathbb{Z}_2 \times \mathbb{Z}_8) \rtimes \mathbb{Z}_2$
32/27	$(\mathbb{Z}_2 \times \mathbb{Z}_8) \rtimes \mathbb{Z}_2$
32/29	$\mathbb{Z}_8 \rtimes \mathbb{Z}_4$
32/30	$\mathbb{Z}_8 \rtimes \mathbb{Z}_4$
32/31	$(\mathbb{Z}_4)^2 \rtimes \mathbb{Z}_2$
32/33	$\mathrm{Aut}(16/9)$, $(\mathbb{Z}_2)^4 \rtimes \mathbb{Z}_2$
32/34	$\mathrm{Dih}((\mathbb{Z}_4)^2)$
32/39	$(\mathbb{Z}_4)^2 \rtimes \mathbb{Z}_2$
32/44	$\mathrm{Hol}(\mathbb{Z}_8)$, $\mathrm{Aut}(\mathrm{Q}_{16})$
32/47	$16/11 \rtimes \mathbb{Z}_2$
32/49	D_{32}
32/50	$\mathbb{Z}_{16} \rtimes \mathbb{Z}_2$
32/51	Q_{32}

Bibliography

Aichinger, E. (1994). *Interpolation with Near-rings of Polynomial Functions*. Master's thesis, Johannes Kepler Universität Linz.

Aichinger, E., Binder, F., Ecker, J., Eggetsberger, R., Mayr, P., and Nöbauer, C. (1997a). *9 easy pieces for "SONATA" – Tutorial*. Linz, Austria.

Aichinger, E., Binder, F., Ecker, J., Eggetsberger, R., Mayr, P., and Nöbauer, C. (1997b). *The Share Package "SONATA" – Reference Manual*. Linz, Austria. `(http://www.algebra.uni-linz.ac.at/Sonata2/)`.

Aichinger, E., Binder, F., Ecker, J., Eggetsberger, R., Mayr, P., and Nöbauer, C. (1998). Sonata - a system of near-rings and their applications. In *Near Ring Newsletter*, volume 17, Linz, Austria.

Aichinger, E., Binder, F., Ecker, J., Mayr, P., and Nöbauer, C. (2000a). Algorithms for near rings of non-linear transformations. In *Proceedings of the ISSAC 2000*, pages 23–29, St. Andrews, Scotland.

Aichinger, E., Binder, F., Ecker, J., Mayr, P., and Nöbauer, C. (2000b). Constructing near-rings. Submitted.

Aichinger, E., Ecker, J., and Nöbauer, C. (2000c). The use of computers in near-ring theory. In *Nearrings And Nearfields (Stellenbosch, 1997)*, pages 35–41. Kluwer Academic Publishing, Dordrecht, the Netherlands.

Clay, J. R. (1992). *Nearrings: Geneses and Applications*. Oxford University Press, Oxford, New York, Tokyo.

Clay, J. R. and Grainger, G. R. (1989). Endomorphism nearrings of odd generalized dihedral groups. *J. Algebra*, **127**(2), 320–339.

Coxeter, H. S. M. and Moser, W. O. J. (1965). *Generators and relations for discrete groups*. Springer-Verlag, Berlin. Second edition. Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Band 14.

Dorda, A. (1977). *Über Vollständigkeit bei endlichen Gruppen*. Ph.D. dissertation, Techn. Universität Wien, Vienna. (German).

Ecker, J. (1998). On the number of polynomial functions on nilpotent groups of class 2. In *Contributions to general algebra, 10 (Klagenfurt, 1997)*, pages 133–137. Heyn, Klagenfurt.

Fong, Y. (1979). *The Endomorphism Near-rings of the Symmetric Groups*. Ph.D. dissertation, Univ. of Edinb., Edinburgh.

Fong, Y. and Kaarli, K. (1995). Unary polynomials on a class of groups. *Acta Sci. Math. (Szeged)*, **61**(1-4), 139–154.

Fong, Y. and Meldrum, J. D. P. (1981a). The endomorphism near-ring of the symmetric group of degree four. *Tamkang J. Math.*, **12**(2), 193–203.

Fong, Y. and Meldrum, J. D. P. (1981b). The endomorphism near-rings of the symmetric groups of degree at least five. *J. Austral. Math. Soc. Ser. A*, **30**(1), 37–49.

Fröhlich, A. (1958). The near-ring generated by the inner automorphisms of a finite simple group. *J. London Math. Soc.*, **33**, 95–107.

GAP (1999). *GAP – Groups, Algorithms, and Programming, Version 4.1*. The GAP Group, Aachen, St Andrews. `(http://www-gap.dcs.st-and.ac.uk/~gap)`.

Grätzer, G. (1978). *General lattice theory*. Birkhäuser Verlag, Basel. Lehrbücher und Monographien aus dem Gebiete der Exakten Wissenschaften, Mathematische Reihe, Band 52.

Grätzer, G. and Schmidt, E. T. (1961). Standard ideals in lattices. *Acta Math. Acad. Sci. Hungar.*, **12**, 17–86.

Hall, P. (1969). *The Edmonton notes on nilpotent groups*. Mathematics Department, Queen Mary College, London. Queen Mary College Mathematics Notes.

Hulpke, A. (1998). Computing normal subgroups. In *Proceedings of the 1998 international symposium on symbolic and algebraic computation, ISSAC '98, Rostock, Germany*, pages 194–198, New York. ACM Press.

Huppert, B. (1967). *Endliche Gruppen. I*. Springer-Verlag, Berlin. Die Grundlehren der Mathematischen Wissenschaften, Band 134.

Kaarli, K. (1982). Affine complete abelian groups. *Math. Nachr.*, **107**, 235–239.

Kaiser, H. K. (1977). Über kompatible Funktionen in universalen Algebren. *Acta Math. Acad. Sci. Hungar.*, **30**(1-2), 105–111.

Lausch, H. and Nöbauer, W. (1973). *Algebra of polynomials*. North-Holland Publishing Co., Amsterdam. North-Holland Mathematical Library, Vol. 5.

Lausch, H. and Nöbauer, W. (1976). Funktionen auf endlichen Gruppen. *Publ. Math. Debrecen*, **23**(1-2), 53–61.

Lyons, C. G. and Mason, G. (1991). Endomorphism near-rings of dicyclic and generalised dihedral groups. *Proc. Roy. Irish Acad. Sect. A*, **91**(1), 99–111.

Malone, J. J. (1973). Generalised quaternion groups and distributively generated near-rings. *Proc. Edinburgh Math. Soc. (2)*, **18**, 235–238.

Malone, J. J. and Lyons, C. G. (1972). Finite dihedral groups and d.g. near rings. I. *Compositio Math.*, **24**, 305–312.

Malone, J. J. and Lyons, C. G. (1973). Finite dihedral groups and d.g. near rings. II. *Compositio Math.*, **26**, 249–259.

Meldrum, J. D. P. (1979). The endomorphism near-ring of finite general linear groups. *Proc. Roy. Irish Acad. Sect. A*, **79**(10), 87–96.

Meldrum, J. D. P. (1985). *Near-rings and their links with groups*. Pitman (Advanced Publishing Program), Boston, Mass.

Miller, M. D. (1975). On the lattice of normal subgroups of a direct product. *Pacific J. Math.*, **60**(2), 153–158.

Nöbauer, W. (1976). Über die affin vollständigen, endlich erzeugbaren Moduln. *Monatsh. Math.*, **82**(3), 187–198.

Nöbauer, W. (1978). Affinvollständige Moduln. *Math. Nachr.*, **86**, 85–96.

Pilz, G. (1980). Near-rings of compatible functions. *Proc. Edinburgh Math. Soc. (2)*, **23**(1), 87–95.

Pilz, G. (1983). *Near-rings. The theory and its applications*. North-Holland Publishing Co., Amsterdam, second edition.

Robinson, D. J. S. (1996). *A course in the theory of groups*. Springer-Verlag, New York, second edition.

Saad, G., Syskin, S. A., and Thomsen, M. J. (1997). The inner automorphism nearrings $I(G)$ on all nonabelian groups G of order $|G| \leq 100$. In *Nearrings, nearfields and K-loops (Hamburg, 1995)*, pages 377–402. Kluwer Acad. Publ., Dordrecht.

Scott, S. D. (1969). The arithmetic of polynomial maps over a group and the structure of certain permutational polynomial groups. I. *Monatsh. Math.*, **73**, 250–267.

Scott, S. D. (1979). Involution near-rings. *Proc. Edinburgh Math. Soc. (2)*, **22**(3), 241–245.

Sims, C. C. (1970). Computational methods in the study of permutation groups. In *Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967)*, pages 169–183. Pergamon, Oxford.

Sims, C. C. (1994). *Computation with finitely presented groups*. Cambridge University Press, Cambridge.

Thomas, A. D. and Wood, G. V. (1980). *Group tables*. Shiva Publishing Ltd., Nantwich.

Vogt, F. (1995). Subgroup lattices of finite abelian groups: Structure and cardinality. *Lattice Theory and its Applications*, pages 214–259.

Index