North-Holland Mathematical Library

Board of Advisory Editors:

M. Artin, H. Bass, J. Eells, W. Feit, P. J. Freyd, F. W. Gehring, H. Halberstam, L. V. Hörmander, M. Kac, J. H. B. Kemperman, H. A. Lauwerier, W. A. J. Luxemburg, F. P. Peterson, I. M. Singer and A. C. Zaanen

VOLUME 5

NORTH-HOLLAND PUBLISHING COMPANY–AMSTERDAM • LONDON
AMERICAN ELSEVIER PUBLISHING COMPANY, INC. – NEW YORK

Algebra of Polynomials

HANS LAUSCH
Department of Mathematics
Monash University
Clayton, Australia

and

WILFRIED NÖBAUER
Technische Hochschule Wien
IV. Institut für Mathematik
Wien, Österreich

1973

NORTH-HOLLAND PUBLISHING COMPANY–AMSTERDAM • LONDON
AMERICAN ELSEVIER PUBLISHING COMPANY, INC. – NEW YORK

Library of Congress Catalog Card Number: 72—88283

North-Holland ISBN for the series: 0 7204 2450 x
North-Holland ISBN for this volume: 0 7204 24550

American Elsevier ISBN: 0 444 10441 0

Published by:

North-Holland Publishing Company — Amsterdam
North-Holland Publishing Company, Ltd. — London

Sole distributors for the U.S.A. and Canada:

American Elsevier Publishing Company, Inc.,
52 Vanderbilt Avenue
New York, N.Y. 10017

Printed in Hungary

TABLE OF CONTENTS

INTRODUCTION

Polynomials are a classical subject of mathematics. The first steps towards the abstract concept of a polynomial were the investigation of algebraic equations and the theory of real and complex functions f of the form $f(x) = a_n x^n + \ldots + a_1 x + a_0$. The introduction of the abstract notions of a field and ring at the beginning of this century subsequently brought about the development of the abstract concept of a polynomial over a commutative ring with identity. While polynomials over the fields of real or complex numbers play an important rôle in analysis and numerical mathematics, the algebraic properties of polynomials have also been a research object for a great number of papers and under various different points of view.

There are, however, features in the algebraic theory of classical polynomials that have been treated in several papers to some extent, but so far have not been given a coherent representation. Among all these aspects we think the most important ones to be the connection between polynomials and polynomial functions and the properties of polynomial functions. In particular, the so-called permutation polynomials over finite fields (i.e. polynomials which represent permutations) have suggested plenty of interesting algebraic and number-theoretical investigations. Moreover we think that an important and interesting part of the theory consists of the composition of polynomials. Questions concerning the decomposition of polynomials into indecomposable factors, permutable polynomials, or congruences which are compatible with the composition operation, have been tackled by various authors.

It may appear somewhat strange that polynomials over commutative rings with identity have been dealt with quite extensively while polynomials over other classes of algebraic structures, such as groups, semigroups, lattices etc. have been given little attention. Those papers on polynomials over classes other than rings, fields, and maybe Boolean algebras, are scarce and scattered, and so far not even a general agreement on basic definitions has been achieved. The first author who has endeavoured to

use some concept of polynomials over arbitrary algebraic structures, is G. GRÄTZER in his book on universal algebra, but these polynomials have turned out not to be a straightforward generalization of the classical polynomials.

With this state of the theory of polynomials in mind, this book will serve two different purposes. First we want to give a general approach to the notion of a polynomial via universal algebra in such a way that the classical concept of a polynomial becomes a special case within the general theory, hence we will endeavour to extend the classical theory to generalized polynomials. Secondly, our object is to give a representative sample of results on polynomials over special classes of algebraic structures, such as commutative rings or groups, which refer to the connection between polynomials and polynomial mappings or to the composition of polynomials.

This book consists of six chapters. Chapter 1 gives first of all a short exposition of those facts of universal algebra that are needed in this book, then the definitions and theorems on polynomial algebras and the algebra of polynomial functions that are fundamental for all the subsequent chapters. Finally these definitions and theorems are illustrated by special algebraic structures like rings, groups, lattices, and Boolean algebras. Chapter 2 deals with systems of algebraic equations and related topics such as algebraic extensions and algebraic dependence for arbitrary algebras, and finally specializes to systems of equations over groups. Chapter 3 is based merely on Chapter 1 and investigates the composition of polynomials and polynomial functions for universal algebras in general, then for multioperator groups in particular, and, again by specializing, for rings and groups. The last sections are devoted to polynomial vectors and polynomial function vectors over arbitrary universal algebras, and furthermore, to polynomial permutations, permutation polynomial vectors, and permutation polynomials. Chapter 4 is based just on Chapters 1 and 3 and deals with polynomial composition, polynomial vectors, permutation polynomials and polynomial permutations over rings and fields while Chapter 5 which again depends only on Chapters 1 and 3, does the same for groups. Each chapter concludes with a section "Remarks and Comments" which gives references to the sources being used for that chapter, mentions papers related to that chapter (which have been completed by summer 1971), and states some open problems (the number of which could be easily enlarged by a lot more problems, a task we leave to the reader).

We have tried to make this book comparatively "self-contained". This goal should be achieved by Chapter 6, Appendix. Here we have collected all those definitions and theorems (without proof) of classical algebra which are used in this book but can also be found in lots of textbooks in more detail. Furthermore concepts and results that cannot be found in textbooks but are necessary for understanding various proofs in the book are treated in detail.

We hope that this book will stimulate the interest in a field which still has lots of open problems that are often easily accessible and, in part, not too difficult. Moreover it was our goal to contribute to the development of a more "universal" approach to algebraic problems, i.e. considering the problems not only for a single class of algebraic structures but for a number (if not all) classes of structures simultaneously.

Finally the authors wish to express their deep gratitude to all those who have contributed to the completion of this book by their kind help and assistance. Our special thanks go to Mr. D. G. GREEN who did the proofreading, to Prof. C. WELLS and Dr. R. LIDL for helping us with compiling the bibliography, to Herr G. EIGENTHALER who also read the proofs and prepared the drawings, and to Frau A. CISKOVSKY who typed the manuscript with care and endurance. Moreover we owe our thanks to the North-Holland Publishing Company and its staff, in particular, to Drs. H. J. STOMPS and Mr. E. FREDRIKSSON whose invitation to publish this book, appointing a deadline for its completion, and kind advice on preparing the manuscript have substantially influenced our work. The book is partly based on our previous research work on this subject which, to a large extent, has been done at the Mathematisches Institut der Universität Wien, Vienna (Austria), and partly at the Department of Mathematics, Institute of Advanced Studies, Australian National University, Canberra (Australia). Consequently we express our gratitude to these institutions and their heads, Prof. E. HLAWKA, Prof. N. HOFREITER, and Prof. B. H. NEUMANN. Last not least we are grateful to those mathematicians and students who attended our lectures on subjects of this book and, by their interest, have given us encouragement and moreover frequently valuable suggestions.

Clayton, Vienna, April 1973

HANS LAUSCH

WILFRIED NÖBAUER

CHAPTER 1

POLYNOMIALS AND POLYNOMIAL FUNCTIONS

1. Basic concepts of universal algebra

1.1. Let M be a non-empty set and n a positive integer. An n-ary operation ω on the set M is a mapping from the Cartesian power M^n to M. That means that ω assigns a well-defined element $\omega a_1 a_2 \dots a_n$ of M to each ordered n-tuple $(a_1, a_2, \dots, a_n)$ of elements of M. For $n = 2$, which is a very important special case, we often use infix notation: The operation symbol ω stands between the two elements or may be omitted. A 0-ary operation on the set M means singling out a fixed element of M. This particular element is also denoted by the symbol ω of the 0-ary operation.

A universal algebra or, briefly, an algebra is a pair $\langle A; \Omega \rangle$ where A is a non-empty set and $\Omega = \{\omega_i \mid i \in I\}$ is a family of operations on A being indexed by the set I of all ordinals $\iota < o$, o being an arbitrary ordinal. If no confusion can arise, we will denote the algebra $\langle A; \Omega \rangle$ by A. The family $T = \{n_i \mid \omega_i \text{ is an } n_i\text{-ary operation}, i \in I\}$ is called the type of Ω or also the type of $\langle A; \Omega \rangle$. Any two algebras A, B of the same type are called similar. For similar algebras A, B we can use the same operation symbol for those operations of A and B respectively which are indexed by the same $i \in I$. If A is an algebra, the cardinal $|A|$ of the set A is called the order of A. An algebra A of finite order is called a finite algebra. Thus the order of a finite algebra A is the number of distinct elements of A.

Classical algebra gives us quite a lot of examples of algebras, e.g. a lattice V with the operations $\cup, \cap$ yields the (similar, but distinct) algebras $\langle V; \cup, \cap \rangle$ and $\langle V; \cap, \cup \rangle$ of type $\{2, 2\}$.

1.2. Let $\langle A; \Omega \rangle$ be a universal algebra, and U a non-empty subset of A such that, for all $i \in I$, $\omega_i a_1 a_2 \dots a_{n_i} \in U$ whenever $a_1, a_2, \dots, a_{n_i} \in U$ and $n_i > 0$, and $\omega_i \in U$ if $n_i = 0$. Then the restriction of any ω_i to U yields an operation on U which we will denote again by ω_i. The algebra $\langle U; \Omega \rangle$ is called a subalgebra of A, and A an extension of $\langle U; \Omega \rangle$.

Clearly, any non-empty intersection of subalgebras of A is again a subalgebra of A. If S is a non-empty subset of A, then the intersection of all subalgebras of A containing S as a subset is called the subalgebra of A

generated by S, and will be denoted by $[S]$. If $[S] = A$, then S is called a generating set for A.

1.3. Let A and B be similar algebras. A homomorphism from the algebra A to the algebra B is a mapping $\vartheta : A \to B$ such that $\vartheta\omega_i a_1 \dots a_{n_i} = \omega_i \vartheta a_1 \vartheta a_2 \dots \vartheta a_{n_i}$ for $n_i > 0$ and $\vartheta\omega_i = \omega_i$, for $n_i = 0$, for all $i \in I$. If ϑ is injective (surjective), ϑ is called a monomorphism (epimorphism), and if ϑ is bijective we call it an isomorphism. In case $B = A$, ϑ is an endomorphism of A; and if ϑ is an isomorphism, we call it an automorphism of A.

The algebra B is called a homomorphic image of A if there exists an epimorphism from A to B, and B is isomorphic to A if there is an isomorphism from A to B. In this case we write $B \cong A$.

As immediate consequences of the definitions we get: If ϑ is a homomorphism from A to B and η is a homomorphism from B to C, then $\eta\vartheta$ is a homomorphism from A to C; if ϑ is a homomorphism from A to B, then $\langle \vartheta A; \Omega \rangle$ is a subalgebra of B; if ϑ is an isomorphism from A to B, and η is an isomorphism from B to C, then $\eta\vartheta$ is an isomorphism from A to C; if ϑ is an isomorphism from A to B, then ϑ^{-1} is an isomorphism from B to A. Thus the relation "is isomorphic to", in any set of similar algebras, is an equivalence relation. If A is finite, then any monomorphism from A to A and any epimorphism from A to A is an automorphism of A.

Let ϑ be a monomorphism from A to B. Then there exists an algebra $\bar{B} \cong B$ such that A is a subalgebra of $\bar{B}$: WLOG, we may assume $A \cap B = \phi$. Then we get such an algebra $\bar{B}$ if we replace every element $\vartheta a \in B$ by the element $a \in A$, but do not change other elements in B. This procedure is called an embedding of A into B, and the isomorphism $\varepsilon : B \to \bar{B}$ defined by $\varepsilon\vartheta a = a$, for $a \in A$, $\varepsilon b = b$, for $b \in B - \vartheta A$, is called an embedding isomorphism from B to $\bar{B}$.

1.4. Let $\langle A; \Omega \rangle$ be an algebra. An equivalence relation Θ on A is called a congruence on the algebra A if, for any ω_i with $n_i > 0$, $a_1 \Theta b_1, \dots, a_{n_i} \Theta b_{n_i}$ implies $(\omega_i a_1 \dots a_{n_i}) \Theta (\omega_i b_1 \dots b_{n_i})$. Let F be the set of all equivalence classes under Θ, and $C(a)$ the class of $a \in A$. On F, we define, for any $i \in I$, an n_i-ary operation ω_i by

$$\begin{aligned} \omega_i C(a_1) \dots C(a_{n_i}) &= C(\omega_i a_1 \dots a_{n_i}), \quad \text{for} \quad n_i > 0, \\ \omega_i &= C(\omega_i), \quad \text{for} \quad n_i = 0. \end{aligned} \tag{1.4}$$

The operations ω_i on F are well-defined since the result of any operation does not depend on the particular choice of the representatives. The algebra $\langle F; \Omega \rangle$ is called the factor algebra of A with respect to the congruence Θ and will be denoted by $A|\Theta$. (1.4) implies that the mapping $\vartheta : A \to A|\Theta$ defined by $\vartheta a = C(a)$ is an epimorphism. ϑ is called the canonical epimorphism from A to $A|\Theta$. Thus $A|\Theta$ is a homomorphic image of A.

1.5. Up to isomorphism, the factor algebras are just all the homomorphic images of the algebra A. This is an immediate consequence of the following theorem:

1.51. Theorem (Homomorphism Theorem). *Let $\varphi : A \to B$ be an epimorphism of algebras. Then there exists a congruence K on A and an isomorphism $\psi : B \to A|K$ such that $\psi\varphi = \vartheta$, the canonical epimorphism from A to $A|K$.*

Proof. Let $b \in B$ and $\varphi^{-1}(b)$ be the set of inverse images of b under φ. Then $A = \bigcup(\varphi^{-1}(b) \mid b \in B)$ is a partition of A. Let K be the corresponding equivalence relation on A, then K is a congruence, for let $a_\nu K b_\nu$, $\nu = 1, 2, \dots, n_i$, then $\varphi a_\nu = \varphi b_\nu$, $\nu = 1, 2, \dots, n_i$, hence $\omega_i \varphi a_1 \dots \varphi a_{n_i} = \omega_i \varphi b_1 \dots \varphi b_{n_i}$, thus $(\omega_i a_1 \dots a_{n_i}) K (\omega_i b_1 \dots b_{n_i})$. Moreover $b \to \varphi^{-1}(b)$ is a bijective mapping ψ from B to $A|K$. It is also a homomorphism, for, let $b_\nu = \varphi a_\nu$, and $n_i > 0$, then

$$\begin{aligned} \psi\omega_i b_1 \dots b_{n_i} &= \varphi^{-1}(\omega_i b_1 \dots b_{n_i}) \\ &= \varphi^{-1}(\varphi\omega_i a_1 \dots a_{n_i}) \\ &= C(\omega_i a_1 \dots a_{n_i}) \\ &= \omega_i C(a_1) \dots C(a_{n_i}) \\ &= \omega_i \varphi^{-1}(b_1) \dots \varphi^{-1}(b_{n_i}) \\ &= \omega_i \psi b_1 \dots \psi b_{n_i}. \end{aligned}$$

If $n_i = 0$, then $\psi\omega_i = \varphi^{-1}(\omega_i) = C(\omega_i) = \omega_i$. Thus $\psi : B \to A|K$ is an isomorphism. Furthermore, if $a \in A$, then $\psi\varphi a = \varphi^{-1}(\varphi a) = C(a) = \vartheta a$ which completes the proof.

1.52. If $\varphi : A \to B$ is an algebra homomorphism then, by changing the range from B to φA, we obtain an epimorphism from A to φA which is

also denoted by φ. As in the proof of Th. 1.51, the set $\{\varphi^{-1}(b) \mid b \in \varphi A\}$ constitutes a partition of A which induces a congruence K on A. K is called the kernel of φ and we write $K = \operatorname{Ker} \varphi$.

Every algebra A has at least two congruences, the congruence where the classes consist of only one element, and the congruence whose only class is A itself. These are the trivial congruences. In case there are no further congruences we call A a simple algebra. The algebra A is simple if and only if every homomorphism of A is a monomorphism or maps A onto an algebra of order 1. Indeed, if A has only homomorphisms of this kind, and if Θ is a congruence on A, then the canonical epimorphism $\vartheta : A \to A|\Theta$ is an isomorphism or $|A|\Theta| = 1$, thus Θ is a trivial congruence. Conversely, if A has only the trivial congruences, φ is a homomorphism of A, and $\operatorname{Ker} \varphi = K$, then, by Th. 1.51, there is an isomorphism ψ such that $\psi\varphi = \vartheta$, the canonical epimorphism from A to $A|K$. Since K is a trivial congruence, ϑ is an isomorphism, or $|A|K| = 1$. Thus φ is a monomorphism, or $|\varphi A| = 1$.

1.6. Let $\mathfrak{L}(A)$ be the set of all congruences on A. On $\mathfrak{L}(A)$ we define a binary relation $\leqslant$ as follows: $\Theta_1 \leqslant \Theta_2$ if and only if the set-theoretical inclusion $\Theta_1 \subseteq \Theta_2$ holds; Θ_1, Θ_2 considered as subsets of the Cartesian product $A \times A$.

1.61. Theorem. *The set $\mathfrak{L}(A)$ is a complete lattice with respect to the relation $\leqslant$, the so-called congruence lattice of the algebra A.*

Proof. It is clear that $\leqslant$ is a partial order relation. It remains to show that every non-empty subset of $\mathfrak{L}(A)$ has a greatest lower bound, for $\mathfrak{L}(A)$ has a greatest element.

Let $M = \{\Theta_i \mid i \in I\}$ be a non-empty set of congruences on A, and $\Delta = \bigcap (\Theta_i \mid i \in I)$, the set-theoretical intersection of the subsets Θ_i of $A \times A$. Clearly, Δ is a congruence on A, and also the greatest lower bound of M. Hence $\mathfrak{L}(A)$ is a complete lattice.

1.62. In order to obtain a description of the least upper bound of M we proceed as follows: Let Φ be the binary relation on A defined by $a\Phi b$ if and only if there are congruences $\Theta_{i_1}, \ldots, \Theta_{i_r}$ in M and elements $c_1, \ldots, c_{r-1} \in A$ such that

$$a\Theta_{i_1}c_1,\ c_1\Theta_{i_2}c_2,\ \ldots,\ c_{r-2}\Theta_{i_{r-1}}c_{r-1},\ c_{r-1}\Theta_{i_r}b. \tag{1.6}$$

We call (1.6) a chain of length r from a to b. One can easily verify that Φ is an equivalence relation. Suppose now that $a_g \Phi b_g$, for some integer g, $1 \leqslant g \leqslant n_i$. Then there exists a chain of the form (1.6) from a_g to b_g which yields a chain from $\omega_i a_1 \ldots a_g \ldots a_{n_i}$ to $\omega_i a_1 \ldots b_g \ldots a_{n_i}$. Since Φ is transitive, $a_\nu \Phi b_\nu$, $\nu = 1, \ldots, n_i$ implies $\omega_i a_1 \ldots a_{n_i} \Phi \omega_i b_1 \ldots b_{n_i}$, hence Φ is a congruence, and, of course, the least upper bound of M.

Let P be a subset of $A \times A$, then the intersection of all congruences on A containing P as a subset is called the congruence on A generated by P.

1.7. We want to know the connections between the congruences on an algebra A and those on its factor algebra $A|\Theta$. These are given by

1.71. Theorem (Second Isomorphism Theorem). *Let A be an algebra, Θ a congruence on A, $C(a)$ the congruence class containing $a \in A$, and $\mathfrak{D}$ the sublattice of $\mathfrak{L}(A)$ consisting of all congruences $\Phi \geqslant \Theta$ on A. Then*

a) *If $\Phi \in \mathfrak{D}$, then there is a congruence $\Phi|\Theta \in \mathfrak{L}(A|\Theta)$ defined by: $C(a)\,(\Phi|\Theta)\,C(b)$ if and only if $a\Phi b$.*

b) *If $\Psi \in \mathfrak{L}(A|\Theta)$, then there is a congruence $\overline{\Psi} \in \mathfrak{D}$ defined by: $a\overline{\Psi}b$ if and only if $C(a)\,\Psi C(b)$.*

c) *The mapping $\alpha : \mathfrak{D} \to \mathfrak{L}(A|\Theta)$ defined by $\alpha\Phi = \Phi|\Theta$ is a lattice isomorphism, and $\alpha^{-1}\Psi = \overline{\Psi}$.*

d) *$A|\Phi \cong (A|\Theta)\big|(\Phi|\Theta)$, for any $\Phi \in \mathfrak{D}$.*

Proof. a) $\Phi|\Theta$ is well-defined since $a\Phi b$, $a_1\Theta a$, $b_1\Theta b$ imply $a_1\Phi a$, $b_1\Phi b$ and hence $a_1\Phi b_1$. $\Phi|\Theta$ is a congruence on $A|\Theta$ by definition of $A|\Theta$.

b) By definition of $A|\Theta$, $\overline{\Psi}$ is a congruence on A. Moreover $a\Theta b$ implies $C(a) = C(b)$, hence $\overline{\Psi} \geqslant \Theta$.

c) Let $\Phi \in \mathfrak{D}$, then $\overline{\Phi|\Theta} = \Phi$ since $a\,\overline{\Phi|\Theta}\,b$ is equivalent to $a\Phi b$. Similarly, for $\Psi \in \mathfrak{L}(A|\Theta)$, $\overline{\Psi}|\Theta = \Psi$. Thus α is bijective. Since $\Phi_1 \leqslant \Phi_2$ implies $\Phi_1|\Theta \leqslant \Phi_2|\Theta$ and vice versa, α is a lattice isomorphism. The last assertion follows from $\overline{\Phi|\Theta} = \Phi$.

d) Let Φ be a congruence of $\mathfrak{D}$, $C_1(a)$ the congruence class of Φ containing a, and $C_2(a)$ the congruence class of $\Phi|\Theta$ containing $C(a)$. Then $C_1(a) \to C_2(a)$ is an isomorphism from $A|\Phi$ to $(A|\Theta)\big|(\Phi|\Theta)$. For, by a), this is a well-defined mapping and is bijective since $\overline{\Phi|\Theta} = \Phi$. That this mapping is a homomorphism follows from straightforward calculation.

1.72. Remark. A straightforward argument shows: Let $\Phi \geqslant \Theta$ be congruences on A and $C(a)$, $\bar{C}(a)$ the congruence classes of Φ, Θ resp., con-

taining a. Then $\bar{C}(a) \to C(a)$ is an epimorphism from $A|\Theta$ to $A|\Phi$ which is called the canonical epimorphism.

1.8. Let $\{\langle G_\nu; \Omega\rangle | \nu \in I\}$ be a family of similar algebras, and D the Cartesian product of the sets G_ν. Its elements are families of the form $\{a(\nu)\}$, $\nu \in I$, where $a(\nu) \in G_\nu$, for every ν. We define the operations $\omega_i \in \Omega$ on D by $\omega_i\{a_1(\nu)\} \dots \{a_{n_i}(\nu)\} = \{\omega_i a_1(\nu) \dots a_{n_i}(\nu)\}$ if $n_i > 0$ and $\omega_i = \{\omega_i(\nu)\}$ if $n_i = 0$ and $\omega_i(\nu)$ is the ω_i of G_ν. The algebra $\langle D; \Omega\rangle$ is called the direct product of the algebras G_ν and is denoted by $\prod(G_\nu | \nu \in I)$, or, for $I = \{1, 2\}$ by $G_1 \times G_2$.

The definition of $\prod(G_\nu | \nu \in I) = D$ implies that, for fixed $\mu \in I$, the mapping $\{a(\nu)\} \to a(\mu)$ is an epimorphism π_μ from D to G_μ being called the projection of D onto G_μ. A subalgebra S of D is called a subdirect product of the algebras G_ν if $\pi_\mu S = G_\mu$ for all $\mu \in I$.

1.9. Let I be the set of all ordinals $\nu < \gamma$, γ being an arbitrary ordinal. A family of similar algebras $\langle G_\nu; \Omega\rangle$, $\nu \in I$ is called an ascending family of algebras, if G_α is a subalgebra of G_β, whenever $\alpha < \beta$. We set $G = \cup(G_\nu | \nu \in I)$ and define the operations $\omega_i \in \Omega$ on G by $\omega_i = \omega_i$ of G_0 if $n_i = 0$, while if $n_i > 0$ and μ is the least $\nu \in I$ such that $a_1, a_2, \dots, a_{n_i} \in G_\nu$ (which exists, since I is well ordered), we put $\omega_i a_1 \dots a_{n_i} = \omega_i a_1 \dots a_{n_i}$ of G_μ. The algebra $\langle G; \Omega\rangle$ is called the direct limit of the ascending family of the $\langle G_\nu; \Omega\rangle$.

It is easy to see that every G_ν is a subalgebra of G.

2. Varieties

2.1. Let $\Omega = \{\omega_i | i \in I\}$ be a set of elements ω_i, indexed by the set I of all ordinals $\iota < o$ where o is an arbitrary ordinal. Moreover, for all $i \in I$, let n_i be a non-negative integer, and $X = \{x_j | j \in J\}$ be a set which is disjoint from Ω. The elements of X will be called "indeterminates". We define "words in X over Ω" as follows: Words of rank 0 are the ω_i such that $n_i = 0$, and the $x_j \in X$. A word of rank $k+1$ is either a word of rank k or an expression of the form $\omega_i w_1 \dots w_{n_i}$, $n_i > 0$, and w_ν words of rank k, $\nu = 1, \dots, n_i$. The smallest rank of a word w is called the minimal rank of w. Induction on the minimal rank shows that every word is composed by means of a finite number of elements of $\Omega \cup X$. Let w be a word, then a "subword" of w is w if w is of rank 0, and if $w = \omega_i w_1 \dots w_{n_i}$ is a word of minimal rank $k+1$, then the subwords of w are w and the subwords of w_ν, $\nu = 1, \dots, n_i$. Induction on the minimal rank of w shows that every subword of a subword of w is again a subword of w.

Let W be the set of all words in X over Ω, and $i \in I$. Then we can define an n_i-ary operation ω_i on W by:

$$\begin{aligned} \omega_i w_1 \dots w_{n_i} &\text{ is the word } \omega_i w_1 \dots w_{n_i}, &&\text{for } n_i > 0, \\ \omega_i &\text{ is the word } \omega_i, &&\text{for } n_i = 0. \end{aligned} \tag{2.1}$$

The algebra $\langle W; \Omega\rangle = W(X)$ is called the word algebra in X over Ω.

2.2. Let $\langle A; \Omega\rangle$ be an algebra, $w = w(x_{j_1}, \dots, x_{j_n})$ a word of W containing no other indeterminates than $x_{j_1}, \dots, x_{j_n}$, and $a_{j_1}, \dots, a_{j_n}$ elements of A. By replacing each x_{j_ν} in w by a_{j_ν}, we obtain a well-defined element $w(a_{j_1}, \dots, a_{j_n}) \in A$ if we consider the ω_i occurring in w as operation symbols on A, as one readily finds by induction on the minimal rank of w. (2.1) shows that if $\{a_j | j \in J\}$ is any system of elements of A then the mapping $\vartheta : W(X) \to A$ defined by $w(x_{j_1}, \dots, x_{j_n}) \to w(a_{j_1}, \dots, a_{j_n})$ is a homomorphism of algebras.

2.3. Let $(w_1(x_{j_1}, \dots, x_{j_n}), w_2(x_{j_1}, \dots, x_{j_n}))$ be a pair of words in X over Ω. Such a pair is called a law over Ω. We say that the law $(w_1(x_{j_1}, \dots, x_{jn}), w_2(x_{j_1}, \dots, x_{j_n}))$ holds in the algebra $\langle A; \Omega\rangle$ if $w_1(a_{j_1}, \dots, a_{j_n}) = w_2(a_{j_1}, \dots, a_{j_n})$, for arbitrary elements $a_{j_1}, \dots, a_{j_n} \in A$. For the sake of convenience, we sometimes write $w_1(x_{j_1}, \dots, x_{j_n}) = w_2(x_{j_1}, \dots, x_{j_n})$ instead of $(w_1(x_{j_1}, \dots, x_{j_n}), w_2(x_{j_1}, \dots, x_{j_n}))$.

Let $\mathcal{G}$ be a set of laws over Ω. The class $\mathfrak{V}(\mathcal{G})$ of all algebras A of the same type as Ω, such that all laws of $\mathcal{G}$ hold in A, is called the variety defined by $\mathcal{G}$. One and the same variety can, however, be defined by different sets of laws: If $\mathfrak{V} = \mathfrak{V}(\mathcal{G})$ and we adjoin a law to $\mathcal{G}$ holding in all algebras of $\mathfrak{V}$, we get a new set of laws which also defines $\mathfrak{V}$. Every variety contains the algebra of order 1 of the type of Ω which is unique up to isomorphism. A variety which contains no other algebra is called a degenerate variety.

2.4. Most of the well-known classes of algebras are varieties. A few examples shall illustrate this:

a) The class of semigroups is a variety if we consider semigroups as algebras $\langle A; \omega_1 \rangle$ of type $\{2\}$.

b) The class of groups is a variety if we consider groups as algebras $\langle A; \omega_1, \omega_2, \omega_3 \rangle$ of type $\{2, 1, 0\}$ where ω_1 is the group operation, ω_2 the operation of forming the inverse, and ω_3 the identity. With the same operations, the class of abelian groups is a variety.

c) The class of rings is a variety if we consider rings as algebras $\langle A; \omega_1, \omega_2, \omega_3, \omega_4 \rangle$ of type $\{2, 1, 0, 2\}$ where ω_1 is the addition, ω_2 the operation of forming the additive inverse, ω_3 the zero, and ω_4 the multiplication.

d) The class of commutative rings with identity is a variety if we consider these rings as algebras $\langle A; \omega_1, \omega_2, \omega_3, \omega_4, \omega_5 \rangle$ of type $\{2, 1, 0, 2, 0\}$ where $\omega_1, \omega_2, \omega_3, \omega_4$ are defined as in c) and ω_5 is the identity.

e) The class of lattices is a variety if we consider lattices as algebras $\langle A; \omega_1, \omega_2 \rangle$ of type $\{2, 2\}$ where ω_1 is the union and ω_2 is the intersection.

f) The class of Boolean algebras is a variety if we consider Boolean algebras as algebras $\langle A; \omega_1, \omega_2, \omega_3, \omega_4, \omega_5 \rangle$ of type $\{2, 2, 0, 0, 1\}$ where ω_1, ω_2 are the operations of e), ω_3 is the zero, ω_4 the identity, and ω_5 the operation of forming complements.

From elementary algebra, it is well-known that for each of these classes there exists a set of laws defining just this class, and thus these classes are varieties.

2.5. An important result for varieties is provided by

2.51. Theorem. *Let $\mathfrak{V}$ be a variety and A an algebra in $\mathfrak{V}$. Then every subalgebra and every homomorphic image of A are also in $\mathfrak{V}$, and if $\{A_\nu\}$ is a family of algebras in $\mathfrak{V}$, then the direct product $\prod A_\nu$ is also in $\mathfrak{V}$.*

Proof. Suppose $\mathfrak{V} = \mathfrak{V}(\mathcal{G})$ and A is in $\mathfrak{V}$. If U is any subalgebra of A, the laws holding in A also hold in U, thus U is in $\mathfrak{V}$. Let B be a homomorphic image of A and $\varphi : A \to B$ an epimorphism. If $(w_1(x_{j_1}, \ldots, x_{j_n}), w_2(x_{j_1}, \ldots, x_{j_n}))$ is a law of $\mathcal{G}$ and $b_1, \ldots, b_n$ are arbitrary elements of B, then there exist elements $a_1, \ldots, a_n \in A$ such that $b_i = \varphi a_i$, $i = 1, \ldots, n$. Since $w_1(a_1, \ldots, a_n) = w_2(a_1, \ldots, a_n)$ and φ is a homomorphism, we get $w_1(b_1, \ldots, b_n) = w_2(b_1, \ldots, b_n)$ which means that B is in $\mathfrak{V}$. The last assertion is a consequence of the definition of $\prod A_\nu$.

2.52. We have just seen that every variety is closed with respect to forming subalgebras, homomorphic images and direct products. It is true that the converse also holds, i.e. a class of algebras closed with respect to these processes is a variety – which we are not going to prove since this result will not be required later on.

2.53. Proposition. *Let $\mathfrak{V}$ be a variety and $\{G_\nu \mid \nu \in I\}$ an ascending family of algebras in $\mathfrak{V}$. Then the direct limit of this family is also in $\mathfrak{V}$.*

Proof. This is a consequence of the fact that every G_ν is a subalgebra of the direct limit.

3. Free algebras, free unions, and free products

3.1. Let $\mathfrak{K}$ be a class of similar algebras, Ω its family of operations. An algebra F of $\mathfrak{K}$ is called a free algebra of $\mathfrak{K}$ with free generating set $X = \{x_i \mid i \in I\}$ if X is a subset of F generating F and if, for any algebra A of $\mathfrak{K}$, every mapping from X to A can uniquely be extended to a homomorphism from F to A.

A free algebra of $\mathfrak{K}$ with the free generating set X will be denoted by $F(X, \mathfrak{K})$. The structure of $F(X, \mathfrak{K})$ depends only on the cardinality of X, i.e.

3.11. Proposition. *Let $F(X, \mathfrak{K})$ and $F(Y, \mathfrak{K})$ be free algebras of $\mathfrak{K}$ and $|X| = |Y|$, then $F(X, \mathfrak{K}) \cong F(Y, \mathfrak{K})$.*

Proof. Let $X = \{x_i \mid i \in I\}$, then we may write Y as $Y = \{y_i \mid i \in I\}$. Let $\vartheta : F(X, \mathfrak{K}) \to F(Y, \mathfrak{K})$ be the unique extension of the mapping $x_i \to y_i$ to an algebra homomorphism, and $\eta : F(Y, \mathfrak{K}) \to F(X, \mathfrak{K})$ the unique extension of the mapping $y_i \to x_i$ to an algebra homomorphism. Then $\eta\vartheta : F(X, \mathfrak{K}) \to F(X, \mathfrak{K})$ extends $x_i \to x_i$ to an algebra homomorphism, and $\vartheta\eta : F(Y, \mathfrak{K}) \to F(Y, \mathfrak{K})$ extends $y_i \to y_i$ to an algebra homomorphism. By the uniqueness of extensions, $\eta\vartheta$ and $\vartheta\eta$ are the identity homomorphisms of $F(X, \mathfrak{K})$ and $F(Y, \mathfrak{K})$, resp. Thus ϑ is an isomorphism.

3.2. Not every class of algebras has free algebras. The following theorem, however, will ensure the existence of free algebras in varieties and thus is of great importance.

3.21. Theorem. *Any non-degenerate variety $\mathfrak{V}$ has free algebras with free generating sets of arbitrary cardinality.*

Proof. Let $\mathfrak{V} = \mathfrak{V}(\mathcal{G})$, $X = \{x_j | j \in J\}$ be a set of indeterminates of arbitrary cardinality, and $W(X)$ the word algebra. Let P be the subset of $W(X) \times W(X)$ consisting of all elements a) (w, w), $w \in W(X)$, b) $(w_1(u_1, \ldots, u_k), w_2(u_1, \ldots, u_k))$ and $(w_2(u_1, \ldots, u_k), w_1(u_1, \ldots, u_k))$, where $w_1(y_1, \ldots, y_k) = w_2(y_1, \ldots, y_k)$ is a law of $\mathcal{G}$ and $u_1, \ldots, u_k \in W(X)$. Let Θ be the binary relation on $W(X)$ defined by $v \Theta w$ if and only if there is a finite chain $v = z_0, z_1, \ldots, z_r = w$ of elements of $W(X)$ such that, for $t = 1, \ldots, r$, one can obtain z_t from z_{t-1} by replacing a subword of z_{t-1} which is the left-hand term of an element of P by the right-hand term of the same element—such a chain will be called, in short, a "chain from v to w". Θ is, of course, an equivalence relation on $W(X)$. Moreover, since any set of chains from v_ν to w_ν, $\nu = 1, 2, \ldots, n_i$, gives rise to a chain from $\omega_i v_1 \ldots v_{n_i}$ to $\omega_i w_1 \ldots w_{n_i}$, Θ is also a congruence. We claim that $W(X)|\Theta$ is a free algebra of $\mathfrak{V}$ with the free generating set $\{C(x_j) | j \in J\} = \bar{X}$ and $|\bar{X}| = |J|$. In order to prove the latter assertion we have to show that $C(x_m) \neq C(x_n)$, for any pair of distinct indices m, n in J. Suppose, by way of contradiction, that $x_m \Theta x_n$ for $m \neq n$. This means that there exists a chain from x_m to x_n. If B is an arbitrary algebra in $\mathfrak{V}$ and $\{b_j | j \in J\}$ a family of elements of B, then from this chain we get a chain of elements of B consisting of equal links by replacing each x_j by b_j, $j \in J$. Hence $b_m = b_n$, for all $b_m, b_n \in B$, i.e. $|B| = 1$, and $\mathfrak{V}$ would be degenerate, a contradiction. Since X generates $W(X)$, $\bar{X}$ is a generating set for $W(X)|\Theta$ of cardinality $|J|$. Let $w_1(y_1, \ldots, y_k) = w_2(y_1, \ldots, y_k)$ be a law of $\mathcal{G}$, and $u_1, \ldots, u_k \in W(X)$, then $w_1(C(u_1), \ldots, C(u_k)) = C(w_1(u_1, \ldots, u_k)) = C(w_2(u_1, \ldots, u_k)) = w_2(C(u_1), \ldots, C(u_k))$, hence $W(X)|\Theta$ is an algebra of $\mathfrak{V}$. Suppose now that A is an algebra of $\mathfrak{V}$, and $\psi: \bar{X} \to A$ an arbitrary mapping. We define a mapping φ: $W(X)|\Theta \to A$ by $\varphi C(w(x_{j_1}, \ldots, x_{j_n})) = w(\psi C(x_{j_1}), \ldots, \psi C(x_{j_n}))$. φ is well-defined since $w(x_{j_1}, \ldots, x_{j_n}) \Theta w_1(x_{j_1}, \ldots, x_{j_n})$ implies $w(\psi C(x_{j_1}), \ldots, \psi C(x_{j_n})) = w_1(\psi C(x_{j_1}), \ldots, \psi C(x_{j_n}))$, by replacing every x_j by $\psi C(x_j)$ in a chain from w to w_1. Clearly φ extends ψ, and $\varphi \omega_i C(w_1) \ldots C(w_{n_i}) = \varphi C(\omega_i w_1 \ldots w_{n_i}) = \omega_i \varphi C(w_1) \ldots \varphi C(w_{n_i})$. Therefore φ is a homomorphism and is clearly uniquely determined by being an extension of ψ.

3.3. Let $\mathfrak{K}$ again be a class of similar algebras, Ω its family of operations, and $\{A_l | l \in L\}$ a family of algebras of $\mathfrak{K}$. A pair $A, \{\varphi_l | l \in L\}$ (A being an algebra of $\mathfrak{K}$ and $\varphi_l : A_l \to A$, $l \in L$, an algebra homomorphism) is called a free union of the algebras A_l in $\mathfrak{K}$ if, for any algebra B of $\mathfrak{K}$ and any family of algebra homomorphisms $\psi_l : A_l \to B$, $l \in L$, there exists a unique homomorphism $\varrho: A \to B$ such that $\psi_l = \varrho \varphi_l$ for all $l \in L$.

The free union of the algebras A_l in $\mathfrak{K}$, so far as it exists at all, is unique up to isomorphism, which is a consequence of

3.31. Proposition. *Let $A, \{\varphi_l\}$ and $\bar{A}, \{\bar{\varphi}_l\}$ be free unions of the algebras A_l in $\mathfrak{K}$, then there is an isomorphism $\varrho : A \to \bar{A}$ such that $\bar{\varphi}_l = \varrho \varphi_l$, for all $l \in L$.*

Proof. By definition of free unions, there exist homomorphisms $\varrho : A \to \bar{A}$ and $\bar{\varrho} : \bar{A} \to A$ such that $\bar{\varphi}_l = \varrho \varphi_l$ and $\varphi_l = \bar{\varrho} \bar{\varphi}_l$, for all $l \in L$. By substituting these equations into one another, we get $\varphi_l = \bar{\varrho} \varrho \varphi_l$ and $\bar{\varphi}_l = \varrho \bar{\varrho} \bar{\varphi}_l$. But the uniqueness part of the definition of a free union forces $\bar{\varrho}\varrho$ and $\varrho\bar{\varrho}$ to be the identity mapping of A and $\bar{A}$, resp. Hence ϱ is an isomorphism.

3.32. Remark. A straightforward argument shows that if $A, \{\varphi_l\}$ is a free union of the algebras A_l in $\mathfrak{K}$ and $\sigma_l : \bar{A}_l \to A_l$ are isomorphisms, for all $l \in L$, then $A, \{\varphi_l \sigma_l\}$ is a free union of the algebras $\bar{A}_l$ in $\mathfrak{K}$.

3.33. If $\mathfrak{K}$ is a variety, then there exists a free union, for any family of algebras in $\mathfrak{K}$. A proof can be found in COHN [1].

3.4. Let $\{A_l | l \in L\}$ be a family of algebras of $\mathfrak{K}$. A free union A, $\{\varphi_l | l \in L\}$ of the algebras A_l in $\mathfrak{K}$ is called a free product of the A_l in $\mathfrak{K}$ if every φ_l is a monomorphism and $\cup(\varphi_l A_l | l \in L)$ is a generating set of A. This definition together with Prop. 3.31 implies that if the family $\{A_l | l \in L\}$ has a free product in $\mathfrak{K}$, then every free union of this family in $\mathfrak{K}$ is a free product. If there is no danger of confusion we will call the algebra A a free product of the A_l.

There exist varieties $\mathfrak{K}$ and families of algebras of $\mathfrak{K}$ such that the free union of these families in $\mathfrak{K}$ is not a free product. Conditions for the existence of the free product in $\mathfrak{K}$ of a family of algebras in $\mathfrak{K}$ are provided by GRÄTZER [3].

4. Polynomial algebras

4.1. Let A be an algebra of the variety $\mathfrak{V} = \mathfrak{V}(\mathcal{G})$ with Ω as its set of operations. To each element $a_j \in A$, we will assign a symbol $\bar{a}_j$ and $\bar{A}$ will denote the set of these symbols. Clearly, $\bar{A}$ and Ω are disjoint. Let $X = \{x_i | i \in I\}$ be a set of indeterminates disjoint from $\Omega \cup \bar{A}$, and $W(\bar{A} \cup X)$ the word algebra over Ω. Then $W(X)$ is a subalgebra of $W(\bar{A} \cup X)$. As in the proof of Th. 3.21, we consider a subset P of $W(\bar{A} \cup X) \times W(\bar{A} \cup X)$ which again will give rise to a congruence Θ. Let P be the set of all elements:

a) (w, w), $w \in W(\bar{A} \cup X)$,

b) $(w_1(u_1, \ldots, u_k), w_2(u_1, \ldots, u_k))$ and $(w_2(u_1, \ldots, u_k), w_1(u_1, \ldots, u_k))$ where $w_1(y_1, \ldots, y_k) = w_2(y_1, \ldots, y_k)$ is a law of $\mathcal{G}$, and $u_1 \ldots u_k \in W(\bar{A} \cup X)$

c) $(\omega_i, \bar{a})$ and $(\bar{a}, \omega_i)$ where ω_i is a 0-ary operation and $\omega_i = a$ in A, and $(\omega_i \bar{a}_1 \ldots \bar{a}_{n_i}, \bar{a})$ and $(\bar{a}, \omega_i \bar{a}_1 \ldots \bar{a}_{n_i})$ where ω_i is an n_i-ary operation, $n_i > 0$, and $\omega_i a_1 \ldots a_{n_i} = a$ in the algebra A.

The corresponding congruence Θ yields an algebra $W(\bar{A} \cup X)|\Theta$ of $\mathfrak{V}$, as in the proof of Th. 3.21. By c), the mapping $\varphi : A \to W(\bar{A} \cup X)|\Theta$ defined by $\varphi a = C(\bar{a})$ is a homomorphism. φ is even a monomorphism, for let $\bar{a}_m \Theta \bar{a}_n$, then there is a chain from $\bar{a}_m$ to $\bar{a}_n$. By replacing each x_i in this chain by some arbitrarily chosen $a_i \in A$ and each $\bar{a}_j$ by a_j, we get a chain of equal elements of A, hence $a_m = a_n$. By way of embedding we may thus identify A with φA, and if we write x_i instead of $C(x_i)$—and admit the possibility $x_i = x_j$ for $i \neq j$ (see the subsequent subsection)—we obtain an algebra $A(X, \mathfrak{V})$, with a generating set $A \cup \{x_i | i \in I\}$, isomorphic to $W(\bar{A} \cup X)|\Theta$ which we will call the $\mathfrak{V}$-polynomial algebra over A in the set of indeterminates X, and its elements will be called $\mathfrak{V}$-polynomials in X over A, or just "polynomials". In § 4.3 we will show that $A(X, \mathfrak{V})$ does not depend on the particular choice of $\mathcal{G}$. We summarize these considerations in

4.11. Proposition. *The polynomial algebra $A(X, \mathfrak{V})$ is an algebra of $\mathfrak{V}$, and A is a subalgebra of $A(X, \mathfrak{V})$. The set $A \cup \{x_i | i \in I\}$ is a generating set of $A(X, \mathfrak{V})$.*

4.2. The problem arises under what conditions it may happen that two elements of the generating set $A \cup \{x_i | i \in I\}$ are equal, i.e. $a_l = x_n$, or

$x_m = x_n$, for $m \neq n$. If this is the case, then in $W(\bar{A} \cup X)|\Theta$, we have $C(\bar{a}_l) = C(x_n)$ or $C(x_m) = C(x_n)$, whence $\bar{a}_l \Theta x_n$ or $x_m \Theta x_n$. In a chain $\mathfrak{C}$ from $\bar{a}_l$ to x_n or from x_m to x_n, we replace each x_i by an arbitrarily chosen $a_i \in A$ and each $\bar{a}_j$ by a_j, which shows that necessarily $|A| = 1$, so suppose $A = \{a\}$. If B is an algebra of $\mathfrak{V}$ containing a subalgebra of order 1, then we can embed A into B and thus obtain an algebra $B_1 \cong B$ having A as a subalgebra. By replacing each $\bar{a}_j$ by a_j, x_m by a and x_n by $b \in B_1$ in the chain $\mathfrak{C}$, and taking arbitrary elements of B, for all the other indeterminates, we obtain a chain of equal links. Thus $b = a$ and $|B_1| = |B| = 1$. This means that $\mathfrak{V}$ is a variety such that no algebra A of $\mathfrak{V}$ of order $|A| \neq 1$ contains a subalgebra of order 1. Such a variety will be called semidegenerate.

Conversely, let A be an algebra of order 1 of the semidegenerate variety $\mathfrak{V}$. Then, since A is a subalgebra of $A(X, \mathfrak{V})$, we have $|A(X, \mathfrak{V})| = 1$, and in particular all the elements of $A \cup \{x_i | i \in I\}$ coincide. We state this result as

4.21. Proposition. *If $|A| = 1$ and $\mathfrak{V}$ is a semidegenerate variety, then all the elements of $A \cup \{x_i | i \in I\} \subseteq A(X, \mathfrak{V})$ coincide. Otherwise all the elements of $A \cup \{x_i | i \in I\}$ are distinct, and in particular, we may identify X with $\{x_i | i \in I\}$.*

4.22. There do exist semidegenerate varieties which are not degenerate. We give two examples:

a) The variety of rings with left identity ε considered as algebras of type $\{2, 1, 0, 2, 0\}$ as in § 2.4. Indeed, if an algebra B of this variety has a subalgebra of order 1, then $\varepsilon = 0$ and hence $|B| = 1$.

b) The variety of lattices with zero and identity considered as algebras of type $\{2, 2, 0, 0\}$, by the same argument as in a).

4.3. Let $A(X, \mathfrak{V})$ be a polynomial algebra, then $A(X, \mathfrak{V})$ is in $\mathfrak{V}$, and A is a subalgebra of $A(X, \mathfrak{V})$. Hence $\varphi_1 : A \to A(X, \mathfrak{V})$ defined by $\varphi_1 a = a$ is a monomorphism. Let $F(X, \mathfrak{V})$ be the free algebra of $\mathfrak{V}$ with free generating set X, if $\mathfrak{V}$ is not degenerate, otherwise the algebra of order 1 of $\mathfrak{V}$. Let $\tilde{\varphi}_2 : X \to A(X, \mathfrak{V})$ be the mapping defined by $\tilde{\varphi}_2 x_i = x_i$, then $\tilde{\varphi}_2$ can be uniquely extended to a homomorphism $\varphi_2 : F(X, \mathfrak{V}) \to A(X, \mathfrak{V})$.

4.31. Theorem. *$A(X, \mathfrak{V})$, $\{\varphi_1, \varphi_2\}$ is a free union of the algebras A and $F(X, \mathfrak{V})$ in $\mathfrak{V}$.*

Proof. Let B be an algebra of $\mathfrak{V}$, and $\psi_1 : A \to B$, $\psi_2 : F(X, \mathfrak{V}) \to B$ algebra homomorphisms. Let $\varrho : A(X, \mathfrak{V}) \to B$ be the mapping defined by $\varrho w(a_{i_1}, \ldots, a_{i_k}, x_{j_1}, \ldots, x_{j_l}) = w(\psi_1 a_{i_1}, \ldots, \psi_1 a_{i_k}, \psi_2 x_{j_1}, \ldots, \psi_2 x_{j_l})$. Since $A \cup X$ is a generating set of $A(X, \mathfrak{V})$, ϱ is actually defined on the whole of $A(X, \mathfrak{V})$. ϱ is also well-defined, for let $w_1(a_{i_1}, \ldots, a_{i_k}, x_{j_1}, \ldots, x_{j_l}) = w_2(a_{i_1}, \ldots, a_{i_k}, x_{j_1}, \ldots, x_{j_l})$ in $A(X, \mathfrak{V})$. Then $w_1 \Theta w_2$ in $W(\bar{A} \cup X)$, by construction of $A(X, \mathfrak{V})$, hence there is a chain from w_1 to w_2. By replacing each $\bar{a}_j$ by $\psi_1 a_j$ and each x_j by $\psi_2 x_j$ in this chain, we get a chain of elements of B whose links coincide since B is in $\mathfrak{V}$ and ψ_1 is a homomorphism. Thus $\varrho w_1 = \varrho w_2$. ϱ is, of course, a homomorphism, by definition. Moreover, $\varrho \varphi_1 a_i = \psi_1 a_i$, for all $a_i \in A$, and, if $f \in F(X, \mathfrak{V})$, $f = w(x_{j_1}, \ldots, x_{j_k})$, then $\varrho \varphi_2 f = w(\psi_2 x_{j_1}, \ldots, \psi_2 x_{j_k}) = \psi_2 f$, i.e. $\varrho \varphi_l = \psi_l$. Finally, let $\sigma : A(X, \mathfrak{V}) \to B$ be any homomorphism such that $\psi_l = \sigma \varphi_l$, $l = 1, 2$. Since $\sigma \varphi_1 a_i = \psi_1 a_i = \varrho \varphi_1 a_i$, we have $\sigma a_i = \varrho a_i$, for all $a_i \in A$, and $\sigma \varphi_2 x_j = \psi_2 x_j = \varrho \varphi_2 x_j$ implies $\sigma x_j = \varrho x_j$, for all $x_j \in X$. Thus σ and ϱ coincide on the generating set $A \cup X$ of $A(X, \mathfrak{V})$, hence $\sigma = \varrho$.

4.32. Corollary. *The polynomial algebra $A(X, \mathfrak{V})$ is independent of the set $\mathcal{G}$ of laws defining $\mathfrak{V}$.*

Proof. Let $\mathcal{G}$, $\mathcal{G}^*$ be two sets of laws, each defining $\mathfrak{V}$, and $A(X, \mathfrak{V})$, $A(X, \mathfrak{V})^*$ the polynomial algebras constructed as in 4.1. Since both $A(X, \mathfrak{V})$, $\{\varphi_1, \varphi_2\}$ and $A(X, \mathfrak{V})^*$, $\{\varphi_1^*, \varphi_2^*\}$ are free unions of A and $F(X, \mathfrak{V})$ in $\mathfrak{V}$, there is an isomorphism $\varrho : A(X, \mathfrak{V}) \to A(X, \mathfrak{V})^*$ such that $\varphi_i^* = \varrho \varphi_i$, $i = 1, 2$ by Prop. 3.31. In particular, ϱ fixes $A \cup X$ elementwise, hence $A(X, \mathfrak{V}) = A(X, \mathfrak{V})^*$.

4.33. Remark. Since φ_1 is a monomorphism and $\varphi_1 A \cup \varphi_2 F(X, \mathfrak{V}) \supseteq A \cup \{x_i | i \in I\}$ which generates $A(X, \mathfrak{V})$, the free union $A(X, \mathfrak{V})$, $\{\varphi_1, \varphi_2\}$ is a free product if and only if φ_2 is a monomorphism. But, by no means, is this always the case: Let A be an algebra of order 1 in a semidegenerate, non-degenerate variety $\mathfrak{V}$, and let $|X| > 1$. Then $|A(X, \mathfrak{V})| = 1$, but $|F(X, \mathfrak{V})| > 1$.

4.4. Let B be an algebra, Ω the family of its operations, A a subalgebra and U a subset of B. We will write $A(U)$ for the subalgebra $[A \cup U]$ of B.

4.41. Lemma. *If A is a subalgebra and U, V are subsets of the algebra B, then $A(U \cup V) = A(U)(V)$.*

Proof. $A(U \cup V)$ is a subalgebra of B containing $A \cup U$ and V, hence $A(U \cup V) \supseteq A(U)(V)$. Also $A(U)(V)$ is a subalgebra of B containing A and $U \cup V$, hence $A(U)(V) \supseteq A(U \cup V)$.

4.42. Let A be an algebra of the variety $\mathfrak{V}$. An algebra B of $\mathfrak{V}$ containing A as a subalgebra is called a $\mathfrak{V}$-extension of A. In particular, every $\mathfrak{V}$-polynomial algebra over A is a $\mathfrak{V}$-extension of A. The role of $\mathfrak{V}$-polynomial algebras over A for $\mathfrak{V}$-extensions of A can be seen from

4.43. Lemma. *If $A(U)$ is a $\mathfrak{V}$-extension of A and $X = \{x_u | u \in U\}$ is a set of indeterminates, $x_u \neq x_v$ for $u \neq v$, then there is an epimorphism $\varrho : A(X, \mathfrak{V}) \to A(U)$ such that $\varrho a = a$, for all $a \in A$, and $\varrho x_u = u$, for all $x_u \in X$.*

Proof. The mapping $\psi_1 : A \to A(U)$, $\psi_1 a = a$, is a homomorphism. Moreover, the mapping $x_u \to u$ from X to $A(U)$ extends to a homomorphism $\psi_2 : F(X, \mathfrak{V}) \to A(U)$. By Th. 4.31, $A(X, \mathfrak{V})$, $\{\varphi_1, \varphi_2\}$ is a free union of the algebras A and $F(X, \mathfrak{V})$ in $\mathfrak{V}$, hence there is a homomorphism $\varrho : A(X, \mathfrak{V}) \to A(U)$ such that $\psi_1 = \varrho \varphi_1$, and $\psi_2 = \varrho \varphi_2$. By definition of φ_1, φ_2, we have $\varrho a = a$, for all $a \in A$, and $\varrho x_u = u$, for all $x_u \in X$. Since $A \cup U$ generates $A(U)$, and $A \cup U \subseteq \varrho A(X, \mathfrak{V})$, ϱ is an epimorphism.

4.5. Proposition. *Let A be an algebra of the variety $\mathfrak{V}$ and $\vartheta : A \to B$ an epimorphism. Then there exists exactly one extension of ϑ to an epimorphism $\varrho : A(X, \mathfrak{V}) \to B(X, \mathfrak{V})$ fixing X. If, in particular, ϑ is an isomorphism, then ϱ is an isomorphism.*

Proof. $B(X, \mathfrak{V})$ is an algebra of $\mathfrak{V}$, and B is a subalgebra of $B(X, \mathfrak{V})$, hence $\psi_1 = \vartheta : A \to B(X, \mathfrak{V})$ is a homomorphism. Let ψ_2 be the extension of the mapping $x_i \to x_i$ from X to $B(X, \mathfrak{V})$ to a homomorphism from $F(X, \mathfrak{V})$ to $B(X, \mathfrak{V})$. Since $A(X, \mathfrak{V})$, $\{\varphi_1, \varphi_2\}$ is a free union of A and $F(X, \mathfrak{V})$, there is a homomorphism $\varrho : A(X, \mathfrak{V}) \to B(X, \mathfrak{V})$ such that $\psi_\nu = \varrho \varphi_\nu$, $\nu = 1, 2$. Hence $\varrho a = \vartheta a$, for all $a \in A$, and $\varrho x_i = x_i$, for all $x_i \in X$. ϱ is an epimorphism since $B(X, \mathfrak{V}) = [B \cup X]$, $A(X, \mathfrak{V}) = [A \cup X]$ implies that ϱ is unique. If ϑ is an isomorphism, then $\vartheta^{-1} : B \to A$ is an epimorphism and thus extends to an epimorphism $\sigma : B(X, \mathfrak{V}) \to A(X, \mathfrak{V})$. Thus $\sigma \varrho$ and $\varrho \sigma$ are the identity mappings, implying that ϱ is an isomorphism.

4.51. Remark. The unique epimorphism ϱ so constructed will also be denoted by $\vartheta(X, \mathfrak{V})$, $\vartheta[X]$ or $\vartheta(X)$ if it is necessary to indicate the dependence of ϱ on ϑ.

4.6. Theorem. *Let Y, Z be disjoint sets of indeterminates and $X = Y \cup Z$. Then there exists an isomorphism $\varphi : A(X, \mathfrak{V}) \to A(Y, \mathfrak{V})(Z, \mathfrak{V})$ such that $\varphi u = u$, for all $u \in A \cup X$.*

Proof. Clearly $A(X, \mathfrak{V}) = A(X)$. By Lemma 4.41, $A(X, \mathfrak{V}) = A(Y)(Z)$. By Lemma 4.43, there is an epimorphism $\varrho : A(Y)(Z, \mathfrak{V}) \to A(Y)(Z)$ fixing $A(Y)$ and Z elementwise, and also an epimorphism $\tau : A(Y, \mathfrak{V}) \to A(Y)$ fixing A and Y elementwise. By Prop. 4.5, τ can be extended to an epimorphism $\sigma : A(Y, \mathfrak{V})(Z, \mathfrak{V}) \to A(Y)(Z, \mathfrak{V})$, fixing Z elementwise. Therefore $\chi = \varrho\sigma : A(Y, \mathfrak{V})(Z, \mathfrak{V}) \to A(Y)(Z)$ is an epimorphism fixing Z, Y, and A elementwise. Conversely, $A(Y, \mathfrak{V})(Z, \mathfrak{V}) = A(Y, \mathfrak{V})(Z) = A(Y)(Z) = A(X)$. By Lemma 4.43, there is an epimorphism $\varphi : A(X, \mathfrak{V}) \to A(Y, \mathfrak{V})(Z, \mathfrak{V})$ fixing A, Y, Z elementwise. Hence $\chi\varphi : A(X, \mathfrak{V}) \to A(X, \mathfrak{V})$ fixes $A \cup X$ elementwise, thus is the identity mapping. Similarly $\varphi\chi$ is the identity mapping of $A(Y, \mathfrak{V})(Z, \mathfrak{V})$. Hence φ is an isomorphism fixing $A \cup X$ elementwise.

4.61. Corollary. *Let $X_1, \ldots, X_n$ be pairwise disjoint sets of indeterminates and $X = X_1 \cup X_2 \cup \ldots \cup X_n$. Then there exists an isomorphism $\varphi : A(X, \mathfrak{V}) \to A(X_1, \mathfrak{V}) \ldots (X_n, \mathfrak{V})$ fixing $A \cup X$ elementwise.*

Proof. By induction on n, using Prop. 4.5.

4.62. Corollary. *If Y is a subset of a set X of indeterminates, then there is a monomorphism from $A(Y, \mathfrak{V})$ to $A(X, \mathfrak{V})$, fixing $A \cup Y$ elementwise.*

Proof. This is a consequence of Th. 4.6., putting $Z = X \smallsetminus Y$ and restricting φ^{-1} to $A(Y, \mathfrak{V})$.

5. The lattice of polynomial algebras over an algebra

5.1. Let A be an algebra, Ω the set of its operations, and X a set of indeterminates. The polynomial algebra $A(X, \mathfrak{V})$ depends, of course, on the variety $\mathfrak{V}$, and this dependence is now to be further investigated.

The $\mathfrak{V}$-polynomial algebra $A(X, \mathfrak{V})$ is defined for every variety $\mathfrak{V}$ containing A. Therefore let $\mathbf{M}$ be the set of all varieties containing A ($\mathbf{M}$ is a set, indeed, since every law over Ω involves just a finite number of indeterminates; thus taking a countable set Y of indeterminates, we can find every

law over Ω in $W(Y) \times W(Y)$, and thus every variety with the set Ω of operations is determined by a subset of $W(Y) \times W(Y)$). We define a partial order $\subseteq$ on $\mathbf{M}$ by: $\mathfrak{V}_1 \subseteq \mathfrak{V}_2$ if and only if every algebra of $\mathfrak{V}_1$ is an algebra of $\mathfrak{V}_2$.

5.11. Proposition. *The partially ordered set $\mathbf{M} = \langle \mathbf{M}; \subseteq \rangle$ of all varieties containing A is a complete lattice, the so-called lattice of A-varieties.*

Proof. Let $\{\mathfrak{V}_v \mid v \in I\}$ be a set of varieties of $\mathbf{M}$, and for each v, $\mathcal{G}_v$ the set of all laws which hold in every algebra of $\mathfrak{V}_v$. Then $\mathfrak{V}_v = \mathfrak{V}(\mathcal{G}_v)$. $\mathfrak{V}(\cup(\mathcal{G}_v \mid v \in I))$ and $\mathfrak{V}(\cap(\mathcal{G}_v \mid v \in I))$ are both varieties of $\mathbf{M}$, and these are the greatest lower bound and the least upper bound, resp., for the given set of varieties. As usual $\cap(\mathfrak{V}_v \mid v \in I)$ will denote the greatest lower bound and $\cup(\mathfrak{V}_v \mid v \in I)$ the least upper bound for $\{\mathfrak{V}_v \mid v \in I\}$.

5.2. Let $\mathbf{P} = \{A(X, \mathfrak{V}) \mid \mathfrak{V} \in \mathbf{M}\}$ be the set of all polynomial algebras in X over A, and $\preccurlyeq$ be the partial order on $\mathbf{P}$ defined by: $A(X, \mathfrak{V}_1) \preccurlyeq A(X, \mathfrak{V}_2)$ if and only if there is an epimorphism $\psi : A(X, \mathfrak{V}_2) \to A(X, \mathfrak{V}_1)$ fixing $A \cup X$ elementwise. Indeed, reflexivity and transitivity of $\preccurlyeq$ are immediate. The antisymmetry of $\preccurlyeq$ follows from

5.21. Lemma. *Let $A(X, \mathfrak{V}_1)$ and $A(X, \mathfrak{V}_2)$ be polynomial algebras in X over A, and Θ_1, Θ_2 those congruences on $W(\bar{A} \cup X)$ which are used for constructing $A(X, \mathfrak{V}_1)$ and $A(X, \mathfrak{V}_2)$, resp., according to 4.1. Then $A(X, \mathfrak{V}_1) \preccurlyeq A(X, \mathfrak{V}_2)$ if and only if $\Theta_1 \supseteq \Theta_2$.*

Proof. Let $A(X, \mathfrak{V}_1) \preccurlyeq A(X, \mathfrak{V}_2)$ and ψ: $A(X, \mathfrak{V}_2) \to A(X, \mathfrak{V}_1)$ an epimorphism fixing $A \cup X$ elementwise. Then $\psi w(a_i, x_j) = w(a_i, x_j)$. Hence $w(\bar{a}_i, x_j)\,\Theta_2\, v(\bar{a}_i, x_j)$ in $W(\bar{A} \cup X)$ implies $w(\bar{a}_i, x_j)\,\Theta_1\, v(\bar{a}_i, x_j)$, thus $\Theta_2 \subseteq \Theta_1$. Conversely, suppose that $\Theta_2 \subseteq \Theta_1$. Since $w(a_i, x_j) = v(a_i, x_j)$ in $A(X, \mathfrak{V}_2)$ implies $w(\bar{a}_i, x_j) \Theta_2 v(\bar{a}_i, x_j)$ in $W(\bar{A} \cup X)$ and hence $w(\bar{a}_i, x_j)\,\Theta_1\, v(\bar{a}_i, x_j)$, we conclude that $w(a_i, x_j) = v(a_i, x_j)$ in $A(X, \mathfrak{V}_1)$, and $\psi w(a_i, x_j) = w(a_i, x_j)$ is a well-defined epimorphism ψ: $A(X, \mathfrak{V}_2) \to A(X, \mathfrak{V}_1)$ fixing $A \cup X$ elementwise. Hence $A(X, \mathfrak{V}_1) \preccurlyeq A(X, \mathfrak{V}_2)$.

5.22. Theorem. *The mapping $\mathfrak{V} \to A(X, \mathfrak{V})$ is an order epimorphism $\varphi : \langle \mathbf{M}; \subseteq \rangle \to \langle \mathbf{P}; \preccurlyeq \rangle$.*

Proof. Let $\mathcal{G}_i$, $i = 1, 2$, be the set of all laws holding in $\mathfrak{V}_i$, thus $\mathfrak{V}_i = \mathfrak{V}(\mathcal{G}_i)$. Let $\mathfrak{V}_1 \subseteq \mathfrak{V}_2$, then $\mathcal{G}_1 \supseteq \mathcal{G}_2$. If $P_i \subseteq W(\bar{A} \cup X) \times W(\bar{A} \cup X)$, $i = 1, 2$, is the set of elements being used for defining Θ_i as in § 4.1, then $P_2 \subseteq P_1$, and hence $\Theta_2 \subseteq \Theta_1$. Lemma 5.21 implies $A(X, \mathfrak{V}_1) \leqslant A(X, \mathfrak{V}_2)$.

5.23. Remark. In general, φ is not an isomorphism. If, for example, $|A| = 1$ and $\mathfrak{V}_2$ is a semidegenerate variety, then $A(X, \mathfrak{V}_1) = A(X, \mathfrak{V}_2)$, for any $\mathfrak{V}_1 \subseteq \mathfrak{V}_2$. Another, not so trivial, example we will give in § 9.4. That φ is not, in general, an isomorphism is, to a large extent, due to

5.24. Lemma. *If $\mathfrak{V}_1 \subseteq \mathfrak{V}_2$, then $A(X, \mathfrak{V}_1) = A(X, \mathfrak{V}_2)$ if and only if $A(X, \mathfrak{V}_2)$ is an algebra of $\mathfrak{V}_1$.*

Proof. The "only if" part is obvious. Suppose now that $A(X, \mathfrak{V}_2)$ is in $\mathfrak{V}_1$. Since $A(X, \mathfrak{V}_2)$ is a $\mathfrak{V}_1$-extension of A, by Lemma 4.43 there is a unique epimorphism $\chi\colon A(X, \mathfrak{V}_1) \to A(X, \mathfrak{V}_2)$ fixing $A \cup X$ elementwise. By Th. 5.22, there is also an epimorphism $\psi\colon A(X, \mathfrak{V}_2) \to A(X, \mathfrak{V}_1)$ fixing $A \cup X$ elementwise. Then $\psi\chi\colon A(X, \mathfrak{V}_1) \to A(X, \mathfrak{V}_1)$ and $\chi\psi\colon A(X, \mathfrak{V}_2) \to A(X, \mathfrak{V}_2)$ are epimorphisms fixing $A \cup X$ elementwise, and hence are the identity mappings. Thus ψ is an isomorphism, and $A(X, \mathfrak{V}_1) = A(X, \mathfrak{V}_2)$.

5.3. Proposition. *In the partially ordered set $\langle \mathbf{P}; \leqslant \rangle$, every non-empty subset has a greatest lower bound. If $\bigcap(B_\nu \mid \nu \in I)$ denotes the greatest lower bound for the subset $\{B_\nu \mid \nu \in I\}$ of $\mathbf{P}$, and φ the order epimorphism of Th. 5.22, then*

$$\varphi(\bigcap(\mathfrak{V}_\nu \mid \nu \in I)) = \bigcap(\varphi\mathfrak{V}_\nu \mid \nu \in I). \tag{5.3}$$

This is the consequence of

5.31. Lemma. *Let $\{\mathfrak{V}_\nu \mid \nu \in I\}$ be a set of varieties of $\mathbf{M}$, and Θ_ν the congruence on $W(\bar{A} \cup X)$ corresponding to $\mathfrak{V}_\nu$, $\nu \in I$. If Θ is the congruence corresponding to $\bigcap(\mathfrak{V}_\nu \mid \nu \in I)$ on $W(\bar{A} \cup X)$, then $\Theta = \bigcup(\Theta_\nu \mid \nu \in I)$, the least upper bound in the lattice of congruences on $W(\bar{A} \cup X)$.*

Proof. Let $\mathcal{G}_\nu$ be the set of all laws in $\mathfrak{V}_\nu$, $\nu \in I$. By Prop. 5.11, $\bigcap(\mathfrak{V}_\nu \mid \nu \in I) = \mathfrak{V}(\bigcup(\mathcal{G}_\nu \mid \nu \in I))$. $v\Theta w$ holds if and only if there is a chain from v to w. If P_ν, P are the sets being used for defining Θ_ν, Θ as in 4.1,

then $P = \bigcup(P_\nu \mid \nu \in I)$. Hence $v\Theta w$ if and only if there are elements $w_1, \ldots, w_{r-1} \in W(\bar{A} \cup X)$ and congruences $\Theta_{i_1}, \ldots, \Theta_{i_r}$, $i_\nu \in I$, such that $v\Theta_{i_1}w_1$, $w_1\Theta_{i_2}w_2$, $\ldots$, $w_{r-1}\Theta_{i_r}w$. By § 1.62, this holds if and only if $v(\bigcup(\Theta_\nu \mid \nu \in I))w$. Hence $\Theta = \bigcup(\Theta_\nu \mid \nu \in I)$.

The proof of Prop. 5.3 can now be established. Let $\{A(X, \mathfrak{V}_\nu) \mid \nu \in I\}$ be a subset of $\langle \mathbf{P}; \leqslant \rangle$. Since $\bigcap(\mathfrak{V}_\nu \mid \nu \in I) \subseteq \mathfrak{V}_\nu$, by Th. 5.22, $A(X, \bigcap(\mathfrak{V}_\nu \mid \nu \in I)) \leqslant A(X, \mathfrak{V}_\nu)$, $\nu \in I$. Let $A(X, \mathfrak{V}) \in \mathbf{P}$ such that $A(X, \mathfrak{V}) \leqslant A(X, \mathfrak{V}_\nu)$, for all $\nu \in I$, and Θ be the congruence corresponding to $\mathfrak{V}$. Then, by Lemma 5.21, $\Theta \supseteq \Theta_\nu$, for all $\nu \in I$, thus $\Theta \supseteq \bigcup(\Theta_\nu \mid \nu \in I)$. Again, by Lemma 5.21, and Lemma 5.31, $A(X, \mathfrak{V}) \leqslant A(X, \bigcap(\mathfrak{V}_\nu \mid \nu \in I))$. Hence $A(X, \bigcap(\mathfrak{V}_\nu \mid \nu \in I)) = \bigcap(A(X, \mathfrak{V}_\nu) \mid \nu \in I)$.

5.32. Theorem. *The partially ordered set $\langle \mathbf{P}; \leqslant \rangle$ of all polynomial algebras in X over A is a complete lattice.*

Proof. By a well-known theorem of lattice theory, a partially ordered set is a complete lattice if it has a greatest element, and every non-empty subset has a greatest lower bound. By Prop. 5.3, the second condition holds for $\langle \mathbf{P}; \leqslant \rangle$. Moreover, if $\mathfrak{D} = \mathfrak{V}(\phi)$ is the variety defined by the empty set ϕ of laws $-A \in \mathfrak{D}$ obviously—then $A(X, \mathfrak{D})$ is a greatest element of $\langle \mathbf{P}; \leqslant \rangle$.

5.4. Remark. So far we have been interested in what happens to the polynomial algebra $A(X, \mathfrak{V})$ if the variety $\mathfrak{V}$ varies. But we may also vary the family Ω of operations and ask what happens to $A(X, \mathfrak{V})$. Let $D = \langle D; \Omega \rangle$ be an arbitrary algebra with Ω as its family of operations, and Φ a subfamily of Ω. We set $D_\Phi = \langle D; \Phi \rangle$, and if $\mathcal{G}$ is a set of laws over Ω, $\mathcal{G}_\Phi$ shall denote the subset of $\mathcal{G}$ consisting of the laws where only operations of Φ are involved. Then $\mathfrak{V}(\mathcal{G}_\Phi)$ is a variety over Φ, and if A is in $\mathfrak{V}(\mathcal{G})$, then A_Φ is in $\mathfrak{V}(\mathcal{G}_\Phi)$. $A(X, \mathfrak{V}(\mathcal{G}))_\Phi$ contains A_Φ as a subalgebra, hence $A_\Phi(X)$ is a subalgebra of $A(X, \mathfrak{V}(\mathcal{G}))_\Phi$ belonging to $\mathfrak{V}(\mathcal{G}_\Phi)$. By Lemma 4.43, there is an epimorphism from $A_\Phi(X, \mathfrak{V}(\mathcal{G}_\Phi))$ to $A_\Phi(X)$, or, as we may put it, a homomorphism from $A_\Phi(X, \mathfrak{V}(\mathcal{G}_\Phi))$ to $A(X, \mathfrak{V}(\mathcal{G}))_\Phi$ fixing $A \cup X$.

6. Functions and polynomial functions on algebras

6.1. Let A be an algebra, Ω its family of operations, and k a positive integer. By A^k we will denote the Cartesian product of k copies of A. A k-place function on A is a mapping from A^k to A. The set of all k-place functions on A will be denoted by $F_k(A)$. On $F_k(A)$ we now define the operations $\omega_i \in \Omega$ by

$$\omega_i\varphi_1 \dots \varphi_{n_i}(a_1, \dots, a_k) = \omega_i\varphi_1(a_1, \dots, a_k) \dots \varphi_{n_i}(a_1, \dots, a_k),$$

for every $(a_1, \dots, a_k) \in A^k$, if $n_i > 0$, and $\omega_i(a_1, \dots, a_k) = \omega_i$, for every $(a_1, \dots, a_k) \in A^k$, if $n_i = 0$. We call $\langle F_k(A); \Omega\rangle = F_k(A)$ the full k-place function algebra over A. Clearly, $F_k(A) \cong \prod(A \mid v \in A^k)$, the direct product of $|A^k|$ copies of A. Hence Th. 2.51 implies

6.11. Proposition. *If A is an algebra of the variety $\mathfrak{V}$, so is $F_k(A)$.*

6.12. The function $\varphi \in F_k(A)$ defined by $\varphi(a_1, \dots, a_k) = c$, for all $(a_1, \dots, a_k) \in A^k$, is called the constant function with value c, denoted by $\varkappa_c$. $c \to \varkappa_c$ is a monomorphism $\alpha: A \to F_k(A)$. Thus the set $C_k(A)$ of all constant functions of $F_k(A)$ is a subalgebra of $F_k(A)$, and A can be embedded into $F_k(A)$. Henceforth $F_k(A)$ will always be understood as the algebra obtained from this embedding.

6.2. Let $\xi_i \in F_k(A)$, $i = 1, 2, \dots, k$ be the functions defined by $\xi_i(a_1, \dots, a_k) = a_i$, for all $(a_1, \dots, a_k) \in A^k$. ξ_i is called the i-th projection of $F_k(A)$. $A(\xi_1, \dots, \xi_k)$ is a subalgebra of $F_k(A)$, called the algebra of k-place polynomial functions on A. We will write $P_k(A)$ for $A(\xi_1, \dots, \xi_k)$. By Prop. 6.11 and Th. 2.51, we get

6.21. Proposition. *If A is an algebra of the variety $\mathfrak{V}$, so is $P_k(A)$.*

6.22. Remark. It follows from the definition of $F_k(A)$ that $F_k(A_\Phi) = F_k(A)_\Phi$. Since $P_k(A_\Phi)$ is the subalgebra of $F_k(A_\Phi)$ which is generated by A_Φ and the projections and $P_k(A)_\Phi$ is a subalgebra of $F_k(A)_\Phi = F_k(A_\Phi)$ which contains A_Φ and the projections, $P_k(A_\Phi)$ is a subalgebra of $P_k(A)_\Phi$.

6.3. Let A be an algebra of the variety $\mathfrak{V}$, $X = \{x_1, \dots, x_k\}$ a set of indeterminates, and $A(X, \mathfrak{V}) = A(x_1, \dots, x_k, \mathfrak{V})$ the $\mathfrak{V}$-polynomial algebra

in X over A. Let B be a $\mathfrak{V}$-extension of A and $(b_1, \dots, b_k)$ a k-tuple of elements of B. Let $\psi_1: A \to B$, $\psi_1 a = a$, and $\psi_2: F(X, \mathfrak{V}) \to B$ be the extension of the mapping $x_u \to b_u$, from X to B, to a homomorphism. Using the same argument as in the proof of Lemma 4.43, we see that there is a homomorphism $\varrho: A(X, \mathfrak{V}) \to B$ such that $\varrho a = a$, $a \in A$, and $\varrho x_u = b_u$, $u = 1, \dots, k$. We summarize this in

6.31. Proposition (Substitution principle). *Let A be an algebra of the variety $\mathfrak{V}$, $\{x_1, \dots, x_k\}$ a set of indeterminates, and $(b_1, \dots, b_k)$ a fixed k-tuple of elements of the $\mathfrak{V}$-extension B of A. For every polynomial $p \in A(x_1, \dots, x_k, \mathfrak{V})$, define $\varrho p \in B$ as: $\varrho p = w(d_i, b_1, \dots, b_k)$ where $p = w(d_i, x_1, \dots, x_k)$ is any representation of p as a word in elements $d_i \in A$ and x_i. Then ϱp is well-defined and the mapping $p \to \varrho p$ is a homomorphism from $A(x_1, \dots, x_k, \mathfrak{V})$ to B.*

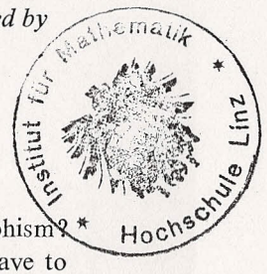
6.32. If $p \in A(x_1, \dots, x_k, \mathfrak{V})$, then $\varrho p \in B$ is called the value of the polynomial p at the place $(b_1, \dots, b_k)$, and is denoted by $p(b_1, \dots, b_k)$.

6.4. In Prop. 6.31, let $B = P_k(A)$ and $(b_1, \dots, b_k) = (\xi_1, \dots, \xi_k)$, then we obtain a homomorphism σ: $A(x_1, \dots, x_k, \mathfrak{V}) \to P_k(A)$ such that $\sigma a = a$, $a \in A$, and $\sigma x_i = \xi_i$, $i = 1, \dots, k$. Since $P_k(A)$ is generated by $A \cup \{\xi_1, \dots, \xi_k\}$, σ is an epimorphism. Let $p = w(d_i, x_1, \dots, x_k)$ be a representation of p as a word, then, by Prop. 6.31, and the definition of Ω on $F_k(A)$, we have $(\sigma p)(a_1, \dots, a_k) = w(d_i, \xi_1, \dots, \xi_k)(a_1, \dots, a_k) = w(d_i, a_1, \dots, a_k) = p(a_1, \dots, a_k)$. Hence we have proved

6.41. Proposition. *The mapping σ: $A(x_1, \dots, x_k, \mathfrak{V}) \to P_k(A)$ defined by*

$$(\sigma p)(a_1, \dots, a_k) = p(a_1, \dots, a_k), \qquad (a_1, \dots, a_k) \in A^k$$

is an epimorphism, the so-called canonical epimorphism.



6.42. One may raise the question: Can it happen that σ is an isomorphism? Since $A(X, \mathfrak{V})$ is defined for every variety $\mathfrak{V}$ containing A, we have to consider the lattice $\mathbf{M}$ of these varieties. Let $\mathcal{U}$ be the set of all laws in the countable set Y of indeterminates holding in A, then clearly $\mathfrak{V}(\mathcal{U})$ is the least element in $\mathbf{M}$.

6.43. Lemma. *If, for some* $\mathfrak{V} \in \mathbf{M}$, *the canonical epimorphism* $\sigma_1 : A(x_1, \ldots, x_k, \mathfrak{V}) \to P_k(A)$ *is an isomorphism, then the canonical epimorphism* $\sigma_2 : A(x_1, \ldots, x_k, \mathfrak{V}(\mathcal{U})) \to P_k(A)$ *is an isomorphism, too.*

Proof. By Th. 5.22, there exists an epimorphism $\psi : A(X, \mathfrak{V}) \to A(X, \mathfrak{V}(\mathcal{U}))$ which fixes $A \cup X$ elementwise. Then $\sigma_2 \psi \sigma_1^{-1} : P_k(A) \to P_k(A)$ is an epimorphism which fixes $A \cup \{\xi_1, \ldots, \xi_k\}$ elementwise. Hence $\sigma_2 \psi \sigma_1^{-1}$ is the identity mapping. Thus σ_2 is a monomorphism, hence an isomorphism.

6.44. Proposition. *If the set of* 0*-ary operations on* A *generates* A, *then the canonical epimorphism* $\sigma : A(x_1, \ldots, x_k, \mathfrak{V}(\mathcal{U})) \to P_k(A)$ *is an isomorphism.*

Proof. Let $p = w(a_i, x_1, \ldots, x_k)$ and $p_1 = w_1(a_i, x_1, \ldots, x_k)$ be polynomials of $A(X, \mathfrak{V}(\mathcal{U}))$ such that $\sigma p = \sigma p_1$. By definition of σ, $w(a_i, \xi_1, \ldots, \xi_k) = w_1(a_i, \xi_1, \ldots, \xi_k)$. By assumption, the elements a_i can be represented as words in the 0-ary operations of A. Performing this substitution, we obtain an equation $v(\xi_1, \ldots, \xi_k) = v_1(\xi_1, \ldots, \xi_k)$ where v, v_1 are words over Ω in $\xi_1, \ldots, \xi_k$. We evaluate this polynomial function for $(a_1, \ldots, a_k) \in A^k$. Then $v(a_1, \ldots, a_k) = v_1(a_1, \ldots, a_k)$, for all $(a_1, \ldots, a_k) \in A^k$, i.e. $v(y_1, \ldots, y_k) = v_1(y_1, \ldots, y_k)$ is a law of A and thus is in $\mathcal{U}$. Since $A(X, \mathfrak{V}(\mathcal{U}))$ is an algebra of $\mathfrak{V}(\mathcal{U})$, $v(x_1, \ldots, x_k) = v_1(x_1, \ldots, x_k)$ in $A(X, \mathfrak{V}(\mathcal{U}))$, and since A is a subalgebra of $A(X, \mathfrak{V}(\mathcal{U}))$, we have $w(a_i, x_1, \ldots, x_k) = w_1(a_i, x_1, \ldots, x_k)$. Hence σ is an isomorphism.

7. Normal forms of polynomials

7.1. Let A be an algebra of the variety $\mathfrak{V}$, and $A(X, \mathfrak{V})$ the $\mathfrak{V}$-polynomial algebra in X over A. By Prop. 4.11, $A(X, \mathfrak{V}) = [A \cup X]$, so every polynomial $p \in A(X, \mathfrak{V})$ has a representation $p = w(a_i, x_j)$ as a word in elements $a_i \in A$ and $x_j \in X$. In general, p will have various different representations of this kind. For practical reasons, in order to control the computations in $A(X, \mathfrak{V})$ completely, one wants a set $\mathfrak{N}$ of words $w(a_i, x_j)$ where each element of $A(X, \mathfrak{V})$ is represented exactly once. But this would still be too little for computations since one also wants to find, in a finite number of steps, the representation of the element

$\omega_i w_1 \ldots w_{n_i} \in A(X, \mathfrak{V})$ by a word in $\mathfrak{N}$, for all operations ω_i, and all words $w_1, \ldots, w_{n_i} \in \mathfrak{N}$. Thus we define:

A set $\mathfrak{N}$ of words in $W(A \cup X)$ is called a normal form system for $A(X, \mathfrak{V})$ if

a) every $p \in A(X, \mathfrak{V})$ is represented by exactly one word in $\mathfrak{N}$,

b) for any n_i-ary operation $\omega_i \in \Omega$ and every n_i-tuple of words $w_1, \ldots, w_{n_i} \in \mathfrak{N}$, it is possible to find the word in $\mathfrak{N}$ representing $\omega_i w_1 \ldots w_{n_i} \in A(X, \mathfrak{V})$, in finitely many steps.

If p is a polynomial of $A(X, \mathfrak{V})$, the word $w(a_i, x_j)$ in $\mathfrak{N}$ representing p is called the normal form of the polynomial p (with respect to $\mathfrak{N}$).

Having a normal form system of $A(X, \mathfrak{V})$ at hand, we can master the computation in $A(X, \mathfrak{V})$ completely. If we know even the normal forms of the polynomials a_i and x_j, we can find the normal form of $p \in A(X, \mathfrak{V})$ in a finite number of steps, for any presentation $p = w(a_i, x_j)$ as a word in a_i and x_j. Thus we can always decide in a finite number of steps whether or not two words of $W(A \cup X)$ represent the same element of $A(X, \mathfrak{V})$, and so have solved the "word problem" in $A(X, \mathfrak{V})$.

The subsequent sections will list some normal form systems for various important polynomial algebras $A(X, \mathfrak{V})$ by use of

7.11. Lemma. *A set* $\mathfrak{N}$ *of words in* $W(A \cup X)$ *is a normal form system of* $A(X, \mathfrak{V})$ *provided*

a) *for every representation* $p = w(a_i, x_j)$ *of an element* $p \in A(X, \mathfrak{V})$ *as a word in certain elements of* $A \cup X$, *one can find a word in* $\mathfrak{N}$ *representing* p, *in a finite number of steps;*

b) *any two different words of* $\mathfrak{N}$ *represent different elements of* $A(X, \mathfrak{V})$.

The proof of this lemma is clear, and follows straight from the definition of a normal form system.

8. Polynomials over commutative rings with identity

8.1. Let Ω be the family of operations $\{\omega_1, \omega_2, \omega_3, \omega_4, \omega_5\}$ of type $\{2, 1, 0, 2, 0\}$, and $\mathfrak{V}$ the variety of commutative rings with identity, these rings being considered as algebras $\langle A; \Omega \rangle$ as in § 2.4. Thus ω_1 is the addition, ω_2 the operation of forming the additive inverse, ω_3 the zero,

ω_4 the multiplication, and ω_5 the identity. As usual, we write $+$, $-$, 0, $\cdot$, and 1 for these operations, and use infix notation for $+$ and $\cdot$. Let R be an arbitrary commutative ring with identity, and $X = \{x\}$ a one-element set of indeterminates. The polynomial algebra $R(X, \mathfrak{V})$ will be denoted by $R[x]$, $\mathfrak{V}$ being kept fixed. Our objective is to obtain a normal form system for $R[x]$. For the sake of notational simplicity we define inductively: If (for any X) $w_1, w_2, \ldots, w_n$ are words in $W(R \cup X)$, then $w_1 + \ldots + w_n$ means $(w_1 + \ldots + w_{n-1}) + w_n$, and $w_1 \ldots w_n$ means $(w_1 \ldots w_{n-1})w_n$. If $w_1 = \ldots = w_n = w$, we write $w_1 \ldots w_n = w^n$, and set $w^0 = 1$. Then $(a_n x^n) + \ldots + (a_1 x) + a_0$, $a_\nu \in R$, $\nu = 0, \ldots, n$, is a well-defined word of $W(R \cup X)$ which we will write as $a_n x^n + \ldots + a_1 x + a_0$.

8.11. Theorem. *Let $\mathfrak{N}$ be the set of all words $a_n x^n + \ldots + a_1 x + a_0$ where $n \geqslant 0$, $a_t \in R$, for $t = 0, \ldots, n$, and $a_n \neq 0$. Then $\mathfrak{N} \cup \{0\}$ is a normal form system of $R[x]$.*

Proof. We will show that $\mathfrak{N}$ satisfies the conditions of Lemma 7.11.

a) We have to show that, for every representation $p = w(a_i, x)$ of an element $p \in R[x]$, we can find a word in $\mathfrak{N}$ representing p, in a finite number of steps. We proceed by induction on the minimal rank r of $w(a_i, x)$. The words of minimal rank 0 are 0, 1, a, and x, $a \in R$, and since $x = 1x + 0$ in $R[x]$, our assertion is true for $r = 0$. Suppose, that the assertion has been proved for words of minimal rank $r \leqslant m$. Every word of minimal rank $m+1$ is of one of the types $w_1 + w_2$, $-w_1$, $w_1 w_2$ where w_1, w_2 are words of minimal rank less or equal to m. By induction hypothesis, we can find, in a finite number of steps, words v_1, v_2 in $\mathfrak{N}$ representing the same elements of $R[x]$ as w_1, w_2, and applying the laws of $\mathfrak{V}$, we can find, in a finite number of steps, words in $\mathfrak{N}$ representing the same elements of $R[x]$ as $v_1 + v_2$, $-v_1$, and $v_1 v_2$.

b) We have to show that any two different words of $\mathfrak{N}$ represent different elements of $R[x]$. For this purpose, let S be the set of all infinite sequences $(a_0, a_1, \ldots)$ of elements in R where $a_\nu \neq 0$ just for finitely many indices ν. In S we define an operation $+$ by

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots).$$

$+$ is a binary operation on S. Furthermore, we define an operation $\cdot$ on S

by

$$(a_0, a_1, a_2, \ldots)(b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots)$$

where

$$c_\nu = a_0 b_\nu + a_1 b_{\nu-1} + a_2 b_{\nu-2} + \ldots + a_\nu b_0, \qquad \nu = 0, 1, 2, \ldots$$

$\cdot$ is really a binary operation on S since $c_\nu = 0$, for $\nu > r+s$, if $a_\nu = 0$, for $\nu > r$, and $b_\nu = 0$, for $\nu > s$. With respect to $+$, $\cdot$, S is a commutative ring with identity: Clearly $\langle S; + \rangle$ is an abelian group, and $\cdot$ is associative, commutative and distributive with respect to $+$; $(1, 0, 0, \ldots)$ is the identity. Thus S is an algebra $\langle S; \Omega \rangle$ of $\mathfrak{V}$.

The mapping $\vartheta : R \to S$, $\vartheta a = (a, 0, 0, \ldots)$ is a monomorphism of algebras, hence we can perform the embedding of R into S and obtain a ring $S_1 \cong S$ which contains R as a subalgebra. Let $\xi = (0, 1, 0, 0, \ldots) \in S_1$. Induction on n shows that $\xi^n = (0, 0, \ldots, 0, 1, 0, \ldots)$, the sequence with 1 at the place with index n and 0 elsewhere. Then

$$(a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots) = a_0 + a_1 \xi + a_2 \xi^2 + \ldots + a_n \xi^n,$$

i.e. $S_1 = R(\xi)$. By Lemma 4.43, there is an epimorphism $\varrho : R[x] \to S_1$ such that $\varrho x = \xi$ and $\varrho a = a$, $a \in R$. Hence

$$\varrho(a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0) = a_n \xi^n + a_{n-1} \xi^{n-1} + \ldots + a_1 \xi + a_0.$$

Let $\varepsilon : S \to S_1$ be the embedding isomorphism. Then

$$\varepsilon^{-1} \varrho(a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0) = (a_0, a_1, \ldots, a_n, 0, 0, \ldots).$$

We conclude that different words in $\mathfrak{N} \cup \{0\}$ represent different elements of $R[x]$.

8.2. Let R again be a commutative ring with identity, considered as an algebra of $\mathfrak{V}$ and suppose that $X = \{x_1, \ldots, x_k\}$. $R(X, \mathfrak{V})$ will be denoted by $R[x_1, \ldots, x_k]$. We want to find a normal form system for $R[x_1, \ldots, x_k]$, but first of all simplify our notation.

Let N be the additive semigroup of non-negative integers equipped with its natural total order $\leqslant$, and N^k the direct product of k copies of N, lexicographically ordered by $\leqslant$. Then it is well known that through $\leqslant$, N^k also becomes a totally ordered semigroup. If $\iota = (i_1, \ldots, i_k) \in N^k$, we will set $\sigma(\iota) = i_1 + i_2 + \ldots + i_k$, and if $(x_1, \ldots, x_k) = \mathfrak{x}$ is a k-tuple of arbitrary elements for which $x_1^{i_1} x_2^{i_2} \ldots x_k^{i_k}$ is well-defined, we will write $x_1^{i_1} x_2^{i_2} \ldots x_k^{i_k} = \mathfrak{x}^\iota$. Thus, if $x_1, \ldots, x_k$ are elements of a commutative semigroup with identity and $\iota, \lambda \in N^k$, then $\mathfrak{x}^\iota \mathfrak{x}^\lambda = \mathfrak{x}^{\iota + \lambda}$.

8.21. Theorem. *The set $\mathfrak{N}$ of all words $\sum(a_\lambda x^\lambda \mid \lambda \in P)$ where P is an arbitrary finite subset of N^k, $a_\lambda \in R$, $a_\lambda \neq 0$, for all $\lambda \in P$, the summands written with decreasing order of λ, is a normal form system for $R[x_1, x_2, \ldots, x_k]$ where $\sum(a_\lambda x^\lambda \mid \lambda \in \phi) = 0$ is additionally defined.*

8.22. Remark. For $k = 1$, this normal form system is different from the system of Th. 8.11 in so far as the words $a_v x^v$, where $a_v = 0$, of 8.11 do not appear in $\mathfrak{N}$ while a_0 of Th. 8.11 is replaced by $a_0 1$.

8.23. Proof of Th. 8.21. We are going to show that the conditions a), b) of 7.1 are satisfied for $\mathfrak{N}$. That b) holds is a consequence of the laws in $\mathfrak{V}$. We will prove by induction on k, that every $p \in R[x_1, \ldots, x_k]$ is represented by exactly one element of $\mathfrak{N}$. Th. 8.11 implies that our assertion holds for $k = 1$. Suppose the theorem is true for $k-1$. Since our theorem is true for one indeterminate, one can find a normal form system for $R[x_1, \ldots, x_{k-1}][x_k]$ of the form $\sum(a_{i_k} x_k^{i_k} \mid i_k \in Q)$ where Q is a finite subset of N, $a_{i_k} \in R[x_1, \ldots, x_{k-1}]$, $a_{i_k} \neq 0$, and the summands are written down with decreasing order of i_k. By induction, $R[x_1, \ldots, x_{k-1}]$ has a normal form system of the kind the theorem asserts. Hence if we replace each a_{i_k} by that word of this normal form system which represents the same element, we see that every element of $R[x_1, \ldots, x_{k-1}][x_k]$ can be represented by exactly one word of $\mathfrak{N}$. But, by Th. 4.6, $\mathfrak{N}$ is also a normal form system for $R[x_1, \ldots, x_k]$.

8.3. The normal form system of Th. 8.21 allows us to introduce some frequently-used concepts:

a) A polynomial $f \in R[x_1, \ldots, x_k]$ is called monic in x_1 if, in its normal form $\sum(a_\lambda x^\lambda \mid \lambda \in P)$, the first summand is $1 x_1^{l_1} x_2^0 \ldots x_k^0$.

b) A polynomial $f \in R[x_1, \ldots, x_k]$ is called a form of degree m if, in its normal form $\sum(a_\lambda x^\lambda \mid \lambda \in P)$, $\sigma(\lambda) = m$, for all $\lambda \in P$.

The polynomial 0 is a form of arbitrary degree. One can easily verify that the product of two forms of degree m and n resp. is a form of degree $m+n$. Forms of degree 1, 2, 3 resp. are called linear, quadratic and cubic forms.

Every polynomial $f \neq 0$ of $R[x_1, \ldots, x_k]$ can be represented uniquely as a sum of forms $q_i \neq 0$ of different degrees i. This is immediate from comparing the normal form for f and the forms q_i.

c) Let $f \in R[x_1, \ldots, x_k]$, and $\sum(a_\lambda x^\lambda \mid \lambda \in P)$ its normal form. We define the degree $[f]$ of f by $[f] = \max(\sigma(\lambda) \mid \lambda \in P)$. $[f]$ is a well-defined non-negative integer, for all $f \neq 0$. As a consequence of this definition when regarding the laws of $\mathfrak{V}$, we get that $f \neq 0$, $g \neq 0$, and $f+g \neq 0$, $fg \neq 0$ resp. implies $[f+g] \leqslant \max([f], [g])$, $[fg] \leqslant [f]+[g]$ resp. A polynomial of degree 1 is called linear.

8.31. Proposition. *If R is an integral domain, so is $R[x_1, \ldots, x_k]$, and then, for any two polynomials $f \neq 0, g \neq 0$, $[fg] = [f]+[g]$.*

Proof. Using Th. 8.21 and the laws of $\mathfrak{V}$, $R[x_1]$ is an integral domain, hence, by induction, $R[x_1, \ldots, x_{k-1}][x_k]$ is an integral domain, and so is $R[x_1, \ldots, x_k]$, by Th. 4.6. Let $[f] = m$, $[g] = n$, so that $f = q_m + q_{m-i_1} + \ldots$, $g = \bar{q}_n + \bar{q}_{n-j_1} + \ldots$ represent f and g as sums of forms $q_v \neq 0$ and $\bar{q}_v \neq 0$ of different degrees v. Since $q_m \neq 0$, $\bar{q}_n \neq 0$, and $q_m \bar{q}_n$ is a form of degree $m+n$, fg can be written as $fg = q_m \bar{q}_n + \bar{q}_{m+n-h_1} + \ldots$, i.e. as a sum of non-zero forms of different degrees, for $R[x_1, \ldots, x_k]$ is an integral domain. Hence $[fg] = [f]+[g]$.

9. Polynomials over groups

9.1. Let Ω be the family of operations $\{\omega_1, \omega_2, \omega_3\}$ of type $\{2, 1, 0\}$, and $\mathfrak{V}$ the variety defined by the laws for groups as in 2.4, the groups being regarded as algebras $\langle A; \Omega \rangle$. Thus ω_1 is the group multiplication, ω_2 the operation of forming the inverse, and ω_3 the identity. As usual, we will write $\cdot$, $^{-1}$, 1 for these operations and use infix notation for $\cdot$, and a^{-1} for $^{-1}(a)$. Let G be a group and $X = \{x\}$ a set of indeterminates consisting of one element x.

As in § 8 we will write $G[x]$ for $G(X, \mathfrak{V})$, and, for words $w_1, \ldots, w_n$ in any indeterminates, give $w_1 \ldots w_n$, and w^n, $n \geqslant 0$, the same meaning as in § 8. Moreover, if $n < 0$, then we will write $w^n = (w^{-1})^{-n}$.

9.11. Theorem. *The set $\mathfrak{N}$ of all words $a_0 x^{n_1} a_1 x^{n_2} \ldots a_{r-1} x^{n_r} a_r$ where r is a non-negative integer, each n_i a non-zero integer, $a_t \in G$, $t = 0, 1, \ldots, r$, and $a_t \neq 1$, $t = 1, 2, \ldots, r-1$, is a normal form system of $G[x]$.*

Proof. We will prove the theorem by means of Lemma 7.11.

a) We show by induction on the minimal rank of the word $w(a_i, x)$ that, for every representation $p = w(a_i, x)$ of an element $p \in G[x]$, we can find a word in $\mathfrak{N}$ representing p, in a finite number of steps. If $r = 0$, by $x = 1x1$ this is certainly true. Suppose the assertion holds for $r \leqslant m$. Every word of minimal rank $m+1$ has the form w_1w_2 or w_1^{-1} where w_1, w_2 are words of minimal rank $\leqslant m$. Using the induction hypothesis and the laws of $\mathfrak{V}$, we can find words in $\mathfrak{N}$ representing w_1w_2 and w_1^{-1}, in finitely many steps.

b) We have to show that no two different words in $\mathfrak{N}$ represent the same element of $G[x]$. For this purpose, let S be the set of all sequences $(a_0, n_1, a_1, n_2, \ldots, a_{r-1}, n_r, a_r)$ where $r \geqslant 0$, every n_i is a non-zero integer, $a_t \in G$, $t = 0, \ldots, r$, $a_t \neq 1$ for $t = 1, \ldots, r-1$. We define a binary operation on S: $(a_0, n_1, a_1, \ldots, a_{r-1}, n_r, a_r)(b_0, p_1, b_1, \ldots, b_{s-1}, p_s, b_s)$ is that element of S we get from "reducing" the sequence $(a_0, n_1, a_1, \ldots, a_{r-1}, n_r, a_r, b_0, p_1, b_1, \ldots, b_{s-1}, p_s, b_s)$. Here "reducing" means that we apply the following rewriting process: If $(a_0, n_1, \ldots, n_r, a_rb_0, p_1, \ldots, b_{s-1}, p_s, b_s)$ is an element of S, then this is the reduced sequence. Otherwise, $a_rb_0 = 1$ and we rewrite this sequence as $(a_0, n_1, \ldots, n_r+p_1, b_1, \ldots, b_s)$. Either this is an element of S, then this is the reduced sequence, or $n_r+p_1 = 0$. Then we rewrite the latter sequence as $(a_0, n_1, \ldots, a_{r-1}b_1, \ldots, b_s)$, and continue this process which has to terminate after a finite number of (rewriting) steps. We obtain then a well-defined element of S.

Clearly, the sequence (1) is the identity with respect to $\cdot$, and $(a_r^{-1}, -n_r, a_{r-1}^{-1}, \ldots, -n_1, a_0^{-1})$ is an inverse of $(a_0, n_1, \ldots, a_{r-1}, n_r, a_r)$. S will be a group as soon as the following lemma is established:

9.12. Lemma. *The operation $\cdot$ on S is associative.*

Proof. We have to show that $(u_1u_2)u_3 = u_1(u_2u_3)$, for arbitrary elements $u_1 = (a_0, n_1, a_1, n_2, \ldots, a_{r-1}, n_r, a_r)$, $u_2 = (b_0, p_1, b_1, p_2, \ldots, b_{s-1}, p_s, b_s)$, and $u_3 = (c_0, q_1, c_1, q_2, \ldots, c_{t-1}, q_t, c_t)$ of S. Suppose the lemma holds for $u_2 = \alpha$, $u_2 = \beta$, and all u_1, u_3. Then $[u_1(\alpha\beta)]u_3 = [(u_1\alpha)\beta]u_3 = (u_1\alpha)(\beta u_3) = u_1[\alpha(\beta u_3)] = u_1[(\alpha\beta)u_3]$, i.e. the lemma holds for $u_2 = \alpha\beta$ and all u_1, u_3. Suppose now that the lemma is true for all $u_2 = (b_0)$, all $u_2 = (1, p_1, 1)$, and all u_1, u_3. We claim that the lemma holds for all u_1, u_2, u_3. For $s = 0$, the lemma holds by hypothesis. Since $(b_0, p_1, b_1) = [(b_0)(1, p_1, 1)](b_1)$, the preceding argument proves the case $s = 1$.

Suppose the lemma is established for $s = \sigma-1$, then $(b_0, p_1, b_1, \ldots p_\sigma, b_\sigma) = (b_0, p_1, \ldots, p_{\sigma-1}, b_{\sigma-1})(1, p_\sigma, b_\sigma)$ and the preceding arguments prove the case $s = \sigma$.

Let $u_2 = (b_0)$, then $(u_1u_2)u_3 \to (a_0, n_1, a_1, \ldots, a_rb_0c_0, q_1, \ldots, c_t) \leftarrow u_1(u_2u_3)$ where the arrows denote the rewriting process. Hence $(u_1u_2)u_3 = u_1(u_2u_3)$. Let $u_2 = (1, p_1, 1)$. Four cases are to be distinguished:

a) $a_r \neq 1$, $c_0 \neq 1$. Then $(u_1u_2)u_3 = (a_0, n_1, \ldots, a_r, p_1, c_0, q_1, \ldots, c_t) = u_1(u_2u_3)$.

b) $a_r = 1$, $c_0 \neq 1$. Then $u_1u_2 = (a_0, n_1, \ldots, n_r+p_1, 1)$, for $n_r \neq -p_1$, and $u_1u_2 = (a_0, n_1, \ldots, n_{r-1}, a_{r-1})$, for $n_r = -p_1$. Thus $(u_1u_2)u_3 \to (a_0, n_1, \ldots, n_r, a_r, p_1, c_0, \ldots, c_t) \leftarrow u_1(u_2u_3)$ since $u_2u_3 = (1, p_1, c_0, \ldots, c_t)$.

c) $a_r \neq 1$, $c_0 = 1$. We apply a similar argument as in b).

d) $a_r = 1$, $c_0 = 1$. Then $u_1u_2 = (a_0, n_1, a_1, \ldots, n_r+p_1, 1)$, for $n_r \neq -p_1$, and $u_1u_2 = (a_0, n_1, a_1, \ldots, n_{r-1}, a_{r-1})$, for $n_r = -p_1$. Furthermore $u_2u_3 = (1, p_1+q_1, c_1, \ldots, q_t, c_t)$ if $q_1 \neq -p_1$, and $u_2u_3 = (c_1, q_2, c_2, \ldots, c_t)$ if $q_1 = -p_1$. Thus $(u_1u_2)u_3$ is obtained from $(a_0, n_1, \ldots, n_r+p_1, 1, q_1, \ldots, q_t, c_t)$ by reduction, for $n_r \neq -p_1$, and from $(a_0, n_1, \ldots, a_{r-1}, q_1, c_1, \ldots, q_t, c_t)$, for $n_r = -p_1$. $u_1(u_2u_3)$ is obtained from $(a_0, n_1, \ldots, n_r, 1, p_1+q_1, c_1, \ldots, q_t, c_t)$ by reduction, for $q_1 \neq -p_1$, and from $(a_0, n_1, \ldots, a_{r-1}, n_r, c_1, \ldots, q_t, c_t)$, for $q_1 = -p_1$.

Comparing $(u_1u_2)u_3$ with $u_1(u_2u_3)$ in all the four possible cases, our equation holds, and Lemma 9.12 is proved.

9.13. We complete the proof of Th. 9.11. Let us regard the group S as an algebra $\langle S; \Omega\rangle$ of $\mathfrak{V}$. $a \to (a)$ is a monomorphism from G to S, thus we can embed G into S, and obtain a group $S_1 \cong S$ containing G as a subalgebra. Let $(1, 1, 1) = \xi$. Then clearly $(a_0, n_1, a_1, n_2, \ldots, a_{r-1}, n_r, a_r) = a_0\xi^{n_1}a_1\xi^{n_2} \ldots \xi^{n_r}a_r$. Hence $S_1 = G(\xi)$. By Lemma 4.43, there is an epimorphism $\varrho: G[x] \to S_1$ such that $\varrho x = \xi$ and $\varrho a = a$, $a \in G$.

Then $\varrho(a_0x^{n_1} \ldots x^{n_r}a_r) = a_0\xi^{n_1} \ldots \xi^{n_r}a_r$ whence, if $\varepsilon: S \to S_1$ is the embedding isomorphism, $\varepsilon^{-1}\varrho(a_0x^{n_1} \ldots x^{n_r}a_r) = (a_0, n_1, \ldots, n_r, a_r)$. This establishes the theorem.

9.2. Let G be a group we will regard as an algebra of $\mathfrak{V}$ and suppose $X = \{x_1, \ldots, x_k\}$. We write $G(X, \mathfrak{V}) = G[x_1, \ldots, x_k]$ and want to find a normal form system for this algebra. Again we first simplify our nota-

tion. Let M be the additive group of integers and M^k the direct product of k copies of M. $(0, 0, \ldots, 0) \in M^k$ will be denoted by o. An ordered pair $(i_1, \ldots, i_k)$, $(l_1, \ldots, l_k)$ of elements of M^k is called reducible if, for some index v, $i_v \neq 0$, $i_{v+1} = i_{v+2} = \ldots = i_k = l_1 = l_2 = \ldots = l_{v-1} = 0$. If $\iota = (i_1, \ldots, i_k) \in M^k$ and $(x_1, x_2, \ldots, x_k) = \mathfrak{x}$ is a k-tuple of arbitrary elements such that $x_1^{i_1} \ldots x_k^{i_k}$ is well-defined, then we write $x_1^{i_1} \ldots x_k^{i_k} = \mathfrak{x}^\iota$.

9.21. Theorem. *Let $\mathfrak{N}$ be the set of all words $a_0\mathfrak{x}^{\lambda_1}a_1\mathfrak{x}^{\lambda_2} \ldots a_{r-1}\mathfrak{x}^{\lambda_r}a_r$ where r is a non-negative integer, $\lambda_v \in M^k$, $\lambda_v \neq o$, $v = 1, 2, \ldots, r$, $a_v \in G$, $v = 1, \ldots, r$, and $a_v = 1$, for $0 < v < r$ only if λ_v, λ_{v+1} is not reducible. Then $\mathfrak{N}$ is a normal form system for $G[x_1, \ldots, x_k]$.*

The proof is along the same lines as that of Th. 8.21.

Condition b) in the definition of a normal form system is satisfied for $\mathfrak{N}$ as a consequence of the laws of $\mathfrak{V}$. By induction on k, we prove that every $p \in G[x_1, \ldots, x_k]$ is represented by exactly one word of $\mathfrak{N}$. Th. 9.11 implies that the assertion holds for $k = 1$. Suppose this assertion is true for $k-1$. Then we can find a system $\mathfrak{N}_1$ of words representing each element of $G[x_1, \ldots, x_{k-1}][x_k]$ exactly once, namely $\mathfrak{N}_1$ is given by the set of all words $a_0x_k^{n_1}a_1x_k^{n_2} \ldots a_{r-1}x_k^{n_r}a_r$ where r is a non-negative integer, n_i are non-zero integers and every a_t runs over the normal form system for $G[x_1, \ldots, x_{k-1}]$ of our theorem which exists by induction, but $a_t \neq 1$ for $t = 1, \ldots r-1$. By inserting factors x_v^0 at suitable places in these words we obtain, for each element of $G[x_1, \ldots, x_{k-1}][x_k]$, a word in $\mathfrak{N}$ representing this element. Let us assume that different words w_1, w_2 in $\mathfrak{N}$ represent the same element of $G[x_1, \ldots, x_{k-1}][x_k]$. Omitting all factors x_k^0 and $x_1^0x_2^0 \ldots x_{k-1}^0$ and inserting a factor $a_t = 1$ in front of every factor x_k^v where $v \neq 0$ in these words, we get words v_1, v_2 of $\mathfrak{N}_1$ representing the same elements as w_1, w_2. Hence $v_1 = v_2$ which is a contradiction since $w_1 \neq w_2$ implies $v_1 \neq v_2$. $\mathfrak{N}$ is therefore a normal form system for $G[x_1, \ldots, x_{k-1}][x_k]$ and, by Th. 4.6, also one for $G[x_1, \ldots, x_k]$.

9.22. Corollary. *Let $X = \{x_1, \ldots, x_k\}$ and φ_1, φ_2 be the homomorphisms as defined in § 4.3. Then $G(X, \mathfrak{V})$, $\{\varphi_1, \varphi_2\}$ is a free product of the group G and the free group $F(X, \mathfrak{V})$ in the variety $\mathfrak{V}$ of groups.*

Proof. As stated in 4.33 we have just to prove that φ_2 is a monomorphism. Let $v_1, v_2 \in F(X, \mathfrak{V})$. Since $F(X, \mathfrak{V})$ is generated by X, we have $v_1 = x_{i_1}^{n_1}x_{i_2}^{n_2} \ldots x_{i_r}^{n_r}$. Thus we can write $v_1 = 1\mathfrak{x}^{\lambda_1}1\mathfrak{x}^{\lambda_2} \ldots \mathfrak{x}^{\lambda_s}1$ where $\lambda_v \in M^k$,

$\lambda_v \neq o$, $v = 1, \ldots, s$, and no pair λ_v, λ_{v+1} is reducible. Similarly, $v_2 = 1\mathfrak{x}^{\mu_1}1\mathfrak{x}^{\mu_2} \ldots \mathfrak{x}^{\mu_t}1$. By Th. 9.21, $\varphi_2v_1 = \varphi_2v_2$ implies $v_1 = v_2$.

9.3. Let Ω be the family of operations of § 9.1, $\mathfrak{W}$ the variety of abelian groups regarded as algebras $\langle A; \Omega\rangle$, and $X = \{x_1, \ldots, x_k\}$. The problem of finding a normal form system for $A(X, \mathfrak{W})$, $A \in \mathfrak{W}$, is solved by

9.31. Proposition. *The set $\mathfrak{N}$ of all words $a\mathfrak{x}^\lambda$, $\lambda \in M^k$, $a \in A$, is a normal form system for $A(X, \mathfrak{W})$.*

Proof. That, in a finite number of steps, every representation $p = w(a_i, x_j)$ of an element $p \in A(X, \mathfrak{W})$ leads to a word of $\mathfrak{N}$ representing p, is a consequence of the laws of $\mathfrak{W}$. That different words of $\mathfrak{N}$ represent different elements of $A(X, \mathfrak{W})$ follows from an argument similar to that in the proof of Th. 9.11 by considering the abelian group of all pairs (a, λ), $a \in A$, $\lambda \in M^k$, with respect to componentwise composition, i.e. the direct product $A \times M^k$.

9.4. We are now in the position to give another example—as announced in § 5.23—that the epimorphism of Th. 5.22 need not be an isomorphism. Let A be the group of order 1, then A belongs to $\mathfrak{W}$ and also to $\mathfrak{V}$, and $\mathfrak{W} \subset \mathfrak{V}$. A normal form system for $A(x, \mathfrak{V})$ is given by the set of all words $1x^{n_1}1$, by Th. 9.11, $n_1 \neq 0$ integral. Hence $A(x, \mathfrak{V})$ is also in $\mathfrak{W}$, and Lemma 5.24 implies $A(x, \mathfrak{V}) = A(x, \mathfrak{G})$.

10. Polynomials over lattices and Boolean algebras

10.1. Let Ω be the family of operations $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ of type $\{2, 2, 0, 0\}$, and $\mathfrak{V}$ the variety of distributive lattices with zero and identity considered as algebras $\langle A; \Omega\rangle$; here ω_1 is the union, ω_2 the intersection, ω_3 the zero, and ω_4 the identity. As usual, we use infix notation and write $\cup$, $\cap$, 0, 1 for these operations, while $\leqslant$ shall mean the partial order relation on these lattices resulting from these operations. Let D be a lattice of $\mathfrak{V}$, $X = \{x\}$, and set $D(X, \mathfrak{V}) = D[x]$.

10.11. Theorem. *The set $\mathfrak{N}$ of all words $(a \cap x) \cup b$, a, $b \in D$, $a \geqslant b$, is a normal form system for $D[x]$. If $w_1 = (a_1 \cap x) \cup b_1$ and $w_2 = (a_2 \cap x) \cup b_2$ are the representations of $w_1, w_2 \in D[x]$ in $\mathfrak{N}$, then $w_1 \leqslant w_2$ if and only if $a_1 \leqslant a_2$ and $b_1 \leqslant b_2$.*

Proof. We will use Lemma 7.11 to prove the theorem.

a) We show by induction on the minimal rank of $w(a_i, x)$ that, in a finite number of steps, for every representation $p = w(a_i, x)$ of an element $p \in D[x]$, we can find a word of $\mathfrak{N}$ representing p. Let $d \in D$, then $d = (d \cap x) \cup d$, and $x = (1 \cap x) \cup 0$, and thus the assertion holds for minimal rank 0. Suppose the assertion is true for words of minimal rank $\leqslant m$. Every word of minimal rank $m+1$ has the form $w_1 \cup w_2$ or $w_1 \cap w_2$ where w_1, w_2 are words of minimal rank $\leqslant m$. By induction, in a finite number of steps, we can find words $(a_1 \cap x) \cup b_1$ and $(a_2 \cap x) \cup b_2$ of $\mathfrak{N}$ representing the same elements as w_1 and w_2, resp. Using the laws of $\mathfrak{V}$, we have $[(a_1 \cap x) \cup b_1] \cup [(a_2 \cap x) \cup b_2] = [(a_1 \cup a_2) \cap x] \cup (b_1 \cup b_2)$ and $a_1 \cup a_2 \geqslant b_1 \cup b_2$ since $a_1 \geqslant b_1$, $a_2 \geqslant b_2$. Furthermore

$$\begin{aligned}[(a_1 \cap x) \cup b_1] \cap [(a_2 \cap x) \cup b_2] = \\ &= [[(a_1 \cap a_2) \cup (b_1 \cap a_2) \cup (a_1 \cap b_2)] \cap x] \cup (b_1 \cap b_2) \\ &= [[(a_1 \cup b_1) \cap (a_2 \cup b_2)] \cap x] \cup (b_1 \cap b_2) \\ &= [(a_1 \cap a_2) \cap x] \cup (b_1 \cap b_2)\end{aligned}$$

and

$$a_1 \cap a_2 \geqslant b_1 \cap b_2.$$

b) We have to show that no two different words of $\mathfrak{N}$ represent the same element of $D[x]$. Let $\sigma : D[x] \to P_1(D)$ be the canonical epimorphism. By § 6.4, $\sigma x = \xi$, the identity mapping of D and $\sigma d = d$, $d \in D$. Let $(a_1 \cap x) \cup b_1 = (a_2 \cap x) \cup b_2$ in $D[x]$. Then $(a_1 \cap \xi) \cup b_1 = (a_2 \cap \xi) \cup b_2$, for all $\xi \in D$. By substituting $\xi = 0$, we get $b_1 = b_2$, and, for $\xi = 1$, $a_1 \cup b_1 = a_2 \cup b_2$, but $b_i \leqslant a_i$, $i = 1, 2$, and hence $a_1 = a_2$.

c) Let $w_1 = (a_1 \cap x) \cup b_1$ and $w_2 = (a_2 \cap x) \cup b_2$ be two elements of $D[x]$ represented by words in $\mathfrak{N}$. Then $w_1 \cup w_2 = [(a_1 \cup a_2) \cap x] \cup (b_1 \cup b_2)$, by a), which is also the normal form for $w_1 \cup w_2$. Since $w_1 \leqslant w_2$ if and only if $w_1 \cup w_2 = w_2$, the second assertion of the theorem is true.

10.12. Remark. $\sigma : D[x] \to P_1(D)$ is, in fact, an isomorphism. This is an immediate consequence of Th. 10.11 and part b) of its proof. Since the 0-ary operations are, in general, far from being a generating set for D, we see that the condition of Prop. 6.44 is not necessary for σ being an isomorphism.

10.2. Let D again be a distributive lattice with zero and identity, regarded as an algebra of $\mathfrak{V}$, and let us write $D(x_1, \ldots, x_k, \mathfrak{V}) = D[x_1, \ldots, x_k]$.

We want to find a normal form system for $D[x_1, \ldots, x_k]$. For this purpose, we first introduce some new notations: As before, we define $w_1 \cup w_2 \cup \ldots \cup w_n$ and $w_1 \cap w_2 \cap \ldots \cap w_n$ inductively. Let P be the power set of the set $\{1, 2, \ldots, k\}$ and $\subseteq$ the set theoretical inclusion. Let $Q(r)$ be the subset of P consisting of all subsets of $\{1, 2, \ldots, k\}$ of cardinality r, $0 \leqslant r \leqslant k$. Each set of $Q(r)$ is ordered by the natural order of its numbers. This yields a total order $\leqslant$ on $Q(r)$ when injecting $Q(r)$ into the totally ordered direct product N^r of r copies of the semigroup of non-negative integers. Let $S_r = \{l_1, \ldots, l_r\} \in Q(r)$, and $\prod(S_r) = \bigcap (x_i \mid i \notin S_r)$, the x_i written down according to the natural order of the numbers i. Here $\bigcap (x_i \mid i \in \phi)$ means the element 1. With this notation we state

10.21. Theorem. *A normal form system of $D[x_1, \ldots, x_k]$ is given by the set $\mathfrak{N}$ of all words of the form $\bigcup_{r=0}^{k} \bigcup \left(a_{N_r} \cap \prod(N_r) \mid N_r \in Q(r)\right)$ where the $N_r \in Q(r)$ are written down according to the total order relation $\leqslant$ on $Q(r)$, and $a_{N_r} \geqslant a_{N_{r+1}}$, for $N_r \subseteq N_{r+1}$. If $v, w \in D[x_1, \ldots, x_k]$ are represented by the words of $\mathfrak{N}$ with coefficients a_{N_r} and b_{N_r}, resp., then $v \leqslant w$ if and only if $a_{N_r} \leqslant b_{N_r}$, for all $N_r \in P$.*

Proof. By induction on k. By Th. 10.11, all assertions are true for $k = 1$. Suppose that all the assertions are true for $k-1$.

a) Let $p = w(a_i, x_j)$ be any representation of $p \in D[x_1, \ldots, x_k]$. We have to find, in a finite number of steps, a word of $\mathfrak{N}$ representing p. By Th. 4.6, there is an isomorphism $\varphi : D[x_1, \ldots, x_k] \to D[x_1, \ldots, x_{k-1}][x_k]$ fixing $D \cup \{x_1, \ldots, x_k\}$ elementwise. By Th. 10.11, we can find a representation $p = (a_1 \cap x_k) \cup b_1$ where $a_1, b_1 \in D[x_1, \ldots, x_{k-1}]$, $a_1 \geqslant b_1$, in a finite number of steps. By induction, in a finite number of steps, we can find representations of a_1, b_1 in the $\mathfrak{N}$ belonging to $D[x_1, \ldots, x_{k-1}]$. By substituting these representations into $p = (a_1 \cap x_k) \cup b_1$ and applying the laws of $\mathfrak{V}$, we get a representation of p by a word of $\mathfrak{N}$.

b) No two different words of $\mathfrak{N}$ represent the same element of $D[x_1, \ldots, x_k]$, for let $p = \bigcup_{r=0}^{k} \bigcup \left(a_{N_r} \cap \prod(N_r) \mid N_r \in Q(r)\right)$ be the representation of p by a word in $\mathfrak{N}$ and let $b_i = 0$, for $i \notin N_r$, $b_i = 1$, for $i \notin N_r$, then $p(b_1, b_2, \ldots, b_k) = a_{N_r}$. Thus any two different words of $\mathfrak{N}$ represent different polynomials.

c) The proof of the second statement runs along the same lines as part c) of the proof of Th. 10.11.

10.3. Let $\Omega = \{\omega_1, \omega_2, \omega_3, \omega_4, \omega_5\}$ be the family of operations of type $\{2, 2, 0, 0, 1\}$, and $\mathfrak{V}$ the variety of Boolean algebras regarded as algebras $\langle A; \Omega\rangle$ as in § 2.4. Thus ω_1 is the union, ω_2 the intersection, ω_3 the zero, ω_4 the identity, and ω_5 the operation of forming the complement. We write $\cup$ for ω_1, and $\cap$ for ω_2, and use infix notation, 0 for ω_3, 1 for ω_4, and a^{-1} for $\omega_5 a$. Moreover, we set $a^1 = a$, thus $(a^i)^j = a^{ij}$, for every pair $i, j = \pm 1$. As before, we define $w_1 \cup w_2 \cup \ldots \cup w_n$ and $w_1 \cap w_2 \cap \ldots \cap w_n$ inductively. Let M be the set $\{-1, 1\}$ with total order $-1 \leqslant 1$, and M^k the lexicographically ordered Cartesian product of k copies of M. For $\lambda = (l_1, \ldots, l_k) \in M^k$, set $\mathfrak{x}^\lambda = x_1^{l_1} \cap \ldots \cap x_k^{l_k}$. Let $X = \{x_1, \ldots, x_k\}$ be a set of indeterminates and $B(X, \mathfrak{V}) = B[x_1, \ldots, x_k]$ the polynomial algebra in X over an arbitrary Boolean algebra B. Then

10.31. Theorem. *The set $\mathfrak{N}$ of all words $\cup(a_\lambda \cap \mathfrak{x}^\lambda \mid \lambda \in M^k)$, $a_\lambda \in B$, and the elements under the union symbol arranged according to the order relation on the index set M^k, is a normal form system for $B[x_1, \ldots, x_k]$.*

Proof. a) We first show for $k = 1$ that, in a finite number of steps, we can find a word of $\mathfrak{N}$ representing $p \in B[x_1, \ldots, x_k]$, for every representation $p = w(a_i, x_j)$. Since $a = (a \cap x^{-1}) \cup (a \cap x)$ and $x = (0 \cap x^{-1}) \cup (1 \cap x)$, we can use induction on the minimal rank of w. By the laws of $\mathfrak{V}$, we have

$$[(a \cap x^{-1}) \cup (b \cap x)] \cup [(c \cap x^{-1}) \cup (d \cap x)] = [(a \cup c) \cap x^{-1}] \cup [(b \cup d) \cap x],$$
$$[(a \cap x^{-1}) \cup (b \cap x)] \cap [(c \cap x^{-1}) \cup (d \cap x)] = [(a \cap c) \cap x^{-1}] \cup [(b \cap d) \cap x],$$
$$[(a \cap x^{-1}) \cup (b \cap x)]^{-1} = (a^{-1} \cup x) \cap (b^{-1} \cup x^{-1})$$
$$= (a^{-1} \cap b^{-1}) \cup (a^{-1} \cap x^{-1}) \cup (b^{-1} \cap x)$$
$$= (a^{-1} \cap b^{-1} \cap x^{-1}) \cup (b^{-1} \cap x) \cup (a^{-1} \cap b^{-1} \cap x)$$
$$= (a^{-1} \cap x^{-1}) \cup (b^{-1} \cap x). \quad \text{absorption}$$

As in the proof of Th. 10.21, we now proceed by induction on k.

b) Different words of $\mathfrak{N}$ represent different elements of $B[x_1, \ldots, x_k]$: For let $p = \cup(a_\lambda \cap \mathfrak{x}^\lambda \mid \lambda \in M^k)$ be a representation of p by a word of $\mathfrak{N}$, $\lambda = (l_1, \ldots, l_k)$, and $b_i = 1^{l_i}$, $i = 1, 2, \ldots, k$, then $p(b_1, \ldots, b_n) = a_\lambda$.

10.32. Remark. Th. 10.31 and part b) of its proof again show that the canonical epimorphism $\sigma : B[x_1, \ldots, x_k] \to P_k(B)$ is an isomorphism.

11. Polynomially complete algebras

11.1. Definition. An algebra A is called n-polynomially complete if $P_n(A) = F_n(A)$, i.e. every n-place function on A is a polynomial function.

11.11. Proposition. *If A is n-polynomially complete, then A is also m-polynomially complete for all $m \leqslant n$.*

Proof. Let $m \leqslant n$, and $\varphi \in F_m(A)$. Let $\psi \in F_n(A)$ such that $\psi(a_1, \ldots, a_n) = \varphi(a_1, \ldots, a_m)$, $(a_1, \ldots, a_n) \in A^n$. Since, by hypothesis, $\psi \in P_n(A)$, there exists a word $w(g_i, x_1, \ldots, x_n)$ such that $\psi = w(g_i, \xi_1, \ldots, \xi_n)$. Let $b_{m+1}, \ldots, b_n$ be arbitrary fixed elements of A, then $\varphi(a_1, \ldots, a_m) = \psi(a_1, \ldots, a_m, b_{m+1}, \ldots, b_n) = w(g_i, a_1, \ldots, a_m, b_{m+1}, \ldots, b_n) = w(g_i, \xi_1, \ldots, \xi_m, b_{m+1}, \ldots, b_n)(a_1, \ldots, a_m)$, for all $(a_1, \ldots, a_m) \in A^m$. Hence $\varphi = w(g_i, \xi_1, \ldots, \xi_m, b_{m+1}, \ldots, b_n)$, i.e. $\varphi \in P_m(A)$.

11.2. Theorem. *If an algebra A is 2-polynomially complete, then A is n-polynomially complete, for $n = 1, 2, 3, \ldots$.*

Proof. We have to show that A is n-polynomially complete for $n > 2$, by Prop. 11.11. We distinguish two cases:

a) $|A|$ is finite. Since $|A| = 1$ implies $|F_n(A)| = 1$, we may assume $|A| > 1$. To tackle this case, we need two lemmas, which hold under the hypothesis of Th. 11.2.

11.21. Lemma. *Let $n \geqslant 2$, $a \neq b \in A$, and $\varphi \in F_n(A)$ such that*

$$\varphi(g_1, \ldots, g_n) = \begin{cases} a, & \text{for } (g_1, \ldots, g_n) \neq (u_1, \ldots, u_n) \\ b, & \text{for } (g_1, \ldots, g_n) = (u_1, \ldots, u_n) \end{cases}$$

where $(u_1, \ldots, u_n) \in A^n$ arbitrary, then $\varphi \in P_n(A)$.

Proof. By induction on n. For $n = 2$, this is our hypothesis. Suppose the lemma holds for $n-1$ instead of n. Let $\psi \in F_{n-1}(A)$ be the function defined by

$$\psi(g_1, \ldots, g_{n-1}) = \begin{cases} a, & \text{for } (g_1, \ldots, g_{n-1}) \neq (u_1, \ldots, u_{n-1}) \\ b, & \text{for } (g_1, \ldots, g_{n-1}) = (u_1, \ldots, u_{n-1}). \end{cases}$$

Then, by induction, $\psi \in P_{n-1}(A)$, hence $\psi(g_1, \ldots, g_{n-1}) = w_1(a_i, g_1, \ldots, g_{n-1})$ where $w_1(a_i, x_1, \ldots, x_{n-1})$ is some word. Let $\chi \in F_2(A)$ be defined by

$$\chi(u, v) = \begin{cases} a, & \text{for } (u, v) \neq (b, u_n) \\ b, & \text{for } (u, v) = (b, u_n). \end{cases}$$

By hypothesis, $\chi \in P_2(A)$, hence $\chi(u, v) = w_2(b_j, u, v)$ where $w_2(b_j, x_1, x_2)$ is some word. Then

$$\varphi(g_1, \ldots, g_n) = \chi(\psi(g_1, \ldots, g_{n-1}), g_n), \quad \text{for all } (g_1, \ldots, g_n) \in A^n.$$

Hence

$$\begin{aligned}\varphi(g_1, \ldots, g_n) &= w_2(b_j, \psi(g_1, \ldots, g_{n-1}), g_n) \\ &= w_2(b_j, w_1(a_i, g_1, \ldots, g_{n-1}), g_n),\end{aligned}$$

i.e.

$$\varphi = w_2(b_j, w_1(a_i, \xi_1, \ldots, \xi_{n-1}), \xi_n) = w_3(a_i, b_j, \xi_1, \ldots, \xi_n),$$

for some word w_3. Thus $\varphi \in P_n(A)$.

11.22. Lemma. *Let $n \geqslant 2$, $\varrho \in P_n(A)$, and $\psi \in F_n(A)$ such that*

$$\psi(g_1, \ldots, g_n) = \varrho(g_1, \ldots, g_n), \quad \textit{for} \quad (g_1, \ldots, g_n) \neq (u_1, \ldots, u_n),$$

$$\psi(g_1, \ldots, g_n) \neq \varrho(g_1, \ldots, g_n), \quad \textit{for} \quad (g_1, \ldots, g_n) = (u_1, \ldots, u_n),$$

for some $(u_1, \ldots, u_n) \in A^n$, then $\psi \in P_n(A)$.

Proof. Suppose that $\psi(u_1, \ldots, u_n) = c$, and let $a \neq b \in A$. Let $\varphi \in F_n(A)$ be defined as in the hypothesis of Lemma 11.21. Then $\varphi \in P_n(A)$, thus $\varphi(g_1, \ldots, g_n) = v_1(a_i, g_1, \ldots, g_n)$, for some word v_1. Let $\chi \in F_2(A)$ be defined by

$$\chi(u, v) = \begin{cases} v, & \text{for } u \neq b \\ c, & \text{for } u = b. \end{cases}$$

Then, by hypothesis of Th. 11.2, $\chi \in P_2(A)$, i.e. $\chi(u, v) = v_2(b_j, u, v)$, for some word v_2. Then $\psi(g_1, \ldots, g_n) = \chi(\varphi(g_1, \ldots, g_n), \varrho(g_1, \ldots, g_n))$, for all $(g_1, \ldots, g_n) \in A^n$. Thus $\psi(g_1, \ldots, g_n) = v_2(b_j, v_1(a_i, g_1, \ldots, g_n), v_3(c_k, g_1, \ldots, g_n))$ if $\varrho(g_1, \ldots, g_n) = v_3(c_k, g_1, \ldots, g_n)$, for some word $v_3(c_k, x_1, \ldots, x_n)$. Hence ψ is a word in $\xi_1, \ldots, \xi_n$ and some elements of A.

11.23. We complete the proof of the theorem for case a). By definition of $P_n(A)$, every element of A is in $P_n(A)$. By Lemma 11.22, every function of $F_n(A)$ which differs from a constant function only for one $(g_1, \ldots, g_n) \in A^n$ is in $P_n(A)$. By repeating this argument, every function of $F_n(A)$ which differs from a constant function only for finitely many $(g_1, \ldots, g_n) \in A^n$ is in $P_n(A)$. Since A is finite, A^n is also finite, hence $F_n(A) = P_n(A)$.

11.24. b) Let $|A|$ be infinite. Then we use induction on n. For $n = 2$, the assertion holds by hypothesis. Suppose A is $(n-1)$-polynomially complete, for some $n > 2$, and $\varphi \in F_n(A)$. Since n is a finite cardinal, $|A^{n-1}| = |A|^{n-1} = |A|$, hence there is a bijective mapping $\psi : A^{n-1} \to A$, and $\psi^{-1} : A \to A^{n-1}$ is also a bijection. Let $\chi \in F_2(A)$ be defined by $\chi(u, v) = \varphi(\psi^{-1}u, v)$. Then $\varphi(g_1, \ldots, g_n) = \chi(\psi(g_1, \ldots, g_{n-1}), g_n)$, for all $(g_1, \ldots, g_n) \in A^n$. Since $\psi \in F_{n-1}(A)$, by induction, we have $\psi \in P_{n-1}(A)$, thus $\psi(g_1, \ldots, g_{n-1}) = w_1(a_i, g_1, \ldots, g_{n-1})$, for some word w_1. Also $\chi \in P_2(A)$ by hypothesis, thus $\chi(u, v) = w_2(b_j, u, v)$, for some word w_2. Hence $\varphi(g_1, \ldots, g_n) = w_2(b_j, w_1(a_i, g_1, \ldots, g_{n-1}), g_n)$, i.e. $\varphi = w_2(b_j, w_1(a_i, \xi_1, \ldots, \xi_{n-1}), \xi_n)$ is in $P_n(A)$. This completes the proof of the theorem.

11.3. Proposition. *Let A be 1-polynomially complete, then A is simple.*

Proof. By way of contradiction, suppose that A is not simple. Then there is a non-trivial congruence Θ on A. Thus Θ has a congruence class C_1 such that $|C_1| > 1$, moreover there is another congruence class $C_2 \neq C_1$. Let $a, b \in C_1$, $a \neq b$, $c \in C_2$, and $\psi \in F_1(A)$ such that $\psi(a) = a$, $\psi(b) = c$. Since $a \Theta b$ implies $\varphi(a) \Theta \varphi(b)$—by induction on the least minimal rank of the words representing φ—for all $\varphi \in P_1(A)$, we conclude that $\psi \notin P_1(A)$, i.e. A is not 1-polynomially complete.

11.31. Proposition. *Let the algebra $\langle A; \Omega \rangle$ be 1-polynomially complete, and Ω finite or countable. Then A is finite.*

Proof. This is an immediate consequence of

11.32. Lemma. *Any algebra $\langle A; \Omega \rangle$ such that $|A|$ is infinite and $|\Omega| \leqslant |A|$ is not 1-polynomially complete.*

Proof. We have $|F_1(A)| = |A|^{|A|} > |A|$. It suffices to show that $|P_1(A)| \leqslant |A|$. Let $W = W(A \cup \{x\})$ be the word algebra over Ω, and $w \in W$. The number of elements of $\Omega \cup A \cup \{x\}$ involved in w, each element counted with the multiplicity it appears in w, will be called the length of w. Being of the same length is an equivalence relation on W. Let C_n be the class consisting of all words of length n. C_n is a subset of $(\Omega \cup A \cup \{x\})^n$, hence $|C_n| \leqslant |(\Omega \cup A \cup \{x\})^n| = |\Omega \cup A \cup \{x\}|^n = |\Omega \cup A \cup \{x\}| = |\Omega| +$

$+|A|+1=|A|$. Since $W=\bigcup(C_n|n\geqslant 1)$, we have $|W|=\sum(|C_n||n\geqslant 1)$ $\leqslant\sum(|A||n\geqslant 1)=|A|$. As every element of $P_1(A)$ can be represented as a word of W, there is an injection from $P_1(A)$ to W, hence $|P_1(A)|$ $\leqslant|W|\leqslant|A|$.

12. Some examples of polynomially complete algebras

12.1. Let A be an arbitrary algebra. Then the results of § 11 show that the following three cases are possible:

a) A is n-polynomially complete for all n.

b) A is n-polynomially complete for $n=1$, but for no $n>1$.

c) A is n-polynomially complete for no n.

In case a) we say A is polynomially complete, in case b) A is polynomially semicomplete, and in case c) A is polynomially incomplete. For some important varieties, we are going to investigate now in what way the algebras of these varieties distribute over these three cases. We will consider just algebras A such that $|A|\neq 1$, for $|A|=1$ implies that A is polynomially complete for all varieties. These algebras will be called non-trivial algebras.

12.2. Let $\mathfrak{V}$ be the variety of commutative rings with identity as considered in § 2.4. By § 11.3, every 1-polynomially complete non-trivial algebra of $\mathfrak{V}$ is simple and finite, i.e., as we know, a finite field.

Conversely, let Q be a finite field of order q. Then the number of distinct polynomial functions of the form

$$a_{q-1}\xi_1^{q-1}+a_{q-2}\xi_1^{q-2}+\ldots+a_1\xi_1+a_0,\quad a_\nu\in Q,\quad \nu=0,\ldots,q-1,$$

is q^q. For, if any two such functions are equal, we get a polynomial function $u_{q-1}\xi_1^{q-1}+\ldots+u_1\xi_1+u_0$, by taking their difference which is the constant function with value 0. This is only possible if $u_0=u_1=\ldots=u_{q-1}=0$, else the polynomial $u_{q-1}x^{q-1}+\ldots+u_1x+u_0$ would have at most $q-1$ different roots, a contradiction. Hence $|P_1(Q)|\geqslant q^q=|F_1(Q)|$, i.e. Q is 1-polynomially complete.

The functions $p_{q-1}(\xi_1)\,\xi_2^{q-1}+p_{q-2}(\xi_1)\,\xi_2^{q-2}+\ldots+p_1(\xi_1)\,\xi_2+p_0(\xi_1)$, $p_\nu(\xi_1)\in P_1(Q)$, $\nu=0,\ldots,q-1$, are functions of $P_2(Q)$. These functions are pairwise distinct, for assume

$$\sum_{\nu=q-1}^{0}p_\nu(\xi_1)\,\xi_2^\nu=\sum_{\nu=q-1}^{0}r_\nu(\xi_1)\,\xi_2^\nu.$$

Let $a\in Q$ be arbitrary, then $\sum_{\nu=q-1}^{0}p_\nu(a)\,\xi_2^\nu=\sum_{\nu=q-1}^{0}r_\nu(a)\,\xi_2^\nu$, and by the argument from above we conclude $p_\nu(a)=r_\nu(a)$, $\nu=0,\ldots,q-1$, for all $a\in Q$, i.e. $p_\nu(\xi_1)=r_\nu(\xi_1)$, $\nu=0,\ldots,q-1$. Hence we have $|P_2(Q)|\geqslant q^{q^2}=|F_2(Q)|$, i.e. Q is 2-polynomially complete. Hence

12.21. Theorem. *The finite fields are the polynomially complete algebras in the variety of commutative rings with identity. All the other algebras of this variety are polynomially incomplete.*

12.3. Lemma. *Let L be a lattice and $\varphi\in P_1(L)$. Then φ is an order endomorphism of L, i.e. $a\leqslant b$ in L implies $\varphi(a)\leqslant\varphi(b)$.*

Proof. By induction on the least minimal rank k of the words representing φ. The lemma obviously holds for $k=0$. Suppose the lemma is proved for $k\leqslant m-1$, and let φ be a polynomial function of least minimal rank m. Then $\varphi=\psi_1\cup\psi_2$ or $\varphi=\psi_1\cap\psi_2$ where $\psi_1,\psi_2\in P_1(L)$ are of least minimal rank $\leqslant m-1$. By induction, for $a\leqslant b$ in L, $\varphi(a)=\psi_1(a)\cup$ $\cup\psi_2(a)\leqslant\psi_1(b)\cup\psi_2(b)=\varphi(b)$ or $\varphi(a)=\psi_1(a)\cap\psi_2(a)\leqslant\psi_1(b)\cap\psi_2(b)=$ $\varphi(b)$, respectively.

12.31. Let L be 1-polynomially complete, then, by § 11.31, L is finite, thus L has a least element 0 and a greatest element 1. If $\chi\in P_1(L)$ is a function such that $\chi(1)=0$ and $\chi(0)=1$, then, by Lemma 12.3, $1=\chi(0)\leqslant$ $\chi(1)=0$, i.e. $|L|=1$. Therefore we get

12.32. Theorem. *In the variety of lattices, every algebra is polynomially incomplete.*

12.4. Let $\mathfrak{V}$ be the variety of Boolean algebras as considered in § 2.4. If B is an n-polynomially complete algebra of $\mathfrak{V}$, then, by Prop. 11.11 and Prop. 11.31, B is finite. Let $|B|=r$. By 10.32 and Th. 10.31, $|P_n(B)|=|B[x_1,\ldots,x_n]|=r^{2^n}$. Since $|F_n(B)|=r^{r^n}$, we conclude $r\leqslant 2$. If, on the other hand, $r\leqslant 2$, then $F_n(B)=P_n(B)$. Thus we have proved

12.41. Theorem. *In the variety of Boolean algebras, the algebra of order 2 is polynomially complete, while all the other algebras are polynomially incomplete.*

12.5. Proposition. *Let G be a finite group, N a non-abelian minimal normal subgroup of G, A a non-empty finite set, and F the group of all functions from A to N where the multiplication in F is defined by $(\varphi\psi)(a) = \varphi(a)\psi(a)$, $a \in A$. Let H be a subgroup of F which satisfies*

a) *every constant function of F belongs to H;*

b) *for every pair $x, y \in A$, $x \neq y$, there exists $\varrho \in H$ such that $\varrho x \neq \varrho y$;*

c) *for all $\varphi \in H$ and all $r \in G$, the function $a \to r^{-1}\varphi(a)r$ from A to N belongs to H.*

Then $H = F$.

Proof. Let $j > 0$ be an integer such that $j \leqslant |A|$. A j-tuple $(g_1, \ldots, g_j)$, $g_i \in N$, $i = 1, \ldots, j$, shall be called accessible if, for every j-tuple $(a_1, \ldots, a_j)$ of pairwise distinct elements of A, there exists $\varphi \in H$ such that $\varphi(a_i) = g_i$, $i = 1, 2, \ldots, j$. By induction on j, we will show that every j-tuple is accessible. By a), this is true for $j = 1$. Suppose the assertion is true for k-tuples, $k < j$. It suffices to show that all j-tuples $(g, 1, 1, \ldots, 1)$, $g \in N$, are accessible. For, let $\varphi_i \in H$, $i = 1, \ldots, j$, such that $\varphi_i(a_i) = g_i$, $\varphi_i(a_h) = 1$, for $h \neq i$, $1 \leqslant h \leqslant j$, then $\varphi = \varphi_1\varphi_2 \ldots \varphi_j$ satisfies $\varphi(a_i) = g_i$, $i = 1, 2, \ldots, j$. Thus let $\mathfrak{a} = (a_1, \ldots, a_j)$ be a j-tuple of pairwise distinct elements of A, and $N_\mathfrak{a}$ the set of all $g \in N$ such that $\varphi(a_1) = g$, $\varphi(a_i) = 1$, $i = 2, 3, \ldots, j$, for some $\varphi \in H$. Since $1 \in N_\mathfrak{a}$, $N_\mathfrak{a}$ is not empty. Since H is a group, $N_\mathfrak{a}$ is a subgroup and by c), $N_\mathfrak{a}$ is a normal subgroup of G. Hence we have only to show that $N_\mathfrak{a} \neq \{1\}$, then the minimality of N implies $N_\mathfrak{a} = N$. First of all, let $j = 2$. By b), we can choose $\varrho \in H$ such that $\varrho(a_1) \neq \varrho(a_2)$. Let γ be the constant function with value $\varrho(a_2)^{-1}$ and set $\chi = \varrho\gamma$. Then $\chi \in H$ and $\chi(a_1) \neq 1$, $\chi(a_2) = 1$, hence $N_\mathfrak{a} \neq \{1\}$. Suppose now $j > 2$. Since N is non-abelian, we can find $g_1, g_2 \in N$ such that $g_1g_2 \neq g_2g_1$. By induction, every $(j-1)$-tuple is accessible, hence there exist $\psi_1, \psi_2 \in H$ such that $\psi_1(a_1) = g_1$, $\psi_1(a_2) = \psi_1(a_4) = \psi_1(a_5) = \ldots = \psi_1(a_j) = 1$, $\psi_2(a_1) = g_2$, $\psi_2(a_3) = \psi_2(a_4) = \psi_2(a_5) = \ldots = \psi_2(a_j) = 1$. Then $\psi_3 = \psi_1^{-1}\psi_2^{-1}\psi_1\psi_2 \in H$ and $\psi_3(a_1) = g_1^{-1}g_2^{-1}g_1g_2 \neq 1$, $\psi_3(a_i) = 1$, $i = 2, \ldots, j$. Hence $N_\mathfrak{a} \neq \{1\}$ and the proposition is proved.

12.51. Corollary. *Every finite non-abelian simple group G is 2-polynomially complete.*

Proof. We apply Prop. 12.5 to the case where $N = G$ and $A = G \times G$. Then $F = F_2(G)$. Conditions a) and c) are trivially satisfied for $H = P_2(G)$. Let $x, y \in A$, $x \neq y$, then $x = (g_1, g_2)$, $y = (h_1, h_2)$ where either $g_1 \neq h_1$ or $g_2 \neq h_2$. Thus $\varrho x \neq \varrho y$ is satisfied either by $\varrho = \xi_1$ or $\varrho = \xi_2$, and condition b) is satisfied. Hence $P_2(G) = F_2(G)$.

12.52. By Prop. 11.3 and Prop. 11.31, every 1-polynomially complete group must be a finite, simple group. Thus it remains to consider finite simple abelian groups G. Then $|G| = p$, a prime, and $|F_1(G)| = p^p$. The set $S = \{a\xi_1^r \mid a \in G, 0 \leqslant r < p\}$ is a subgroup of $P_1(G)$ containing ξ_1 and the constant functions. Hence $S = P_1(G)$, but every element of S is represented by exactly one $a\xi_1^r$, $a \in G$, $0 \leqslant r < p$, thus $|P_1(G)| = p^2$. We conclude that G is 1-polynomially complete if and only if $p = 2$. Conversely, if $|G| = 2$, then, as before, $P_2(G) = \{a\xi_1^{r_1}\xi_2^{r_2} \mid a \in G, 0 \leqslant r_i < 2, i = 1, 2\}$, $|P_2(G)| = 2^3$. But $|F_2(G)| = 2^4$, hence G is not 2-polynomially complete.

Summarizing these results we state

12.53. Theorem. *In the variety of groups, the finite non-abelian simple groups are polynomially complete, the group of order 2 is polynomially semicomplete, and all the other groups are polynomially incomplete.*

Remarks and comments

§§ 1–3. Universal algebra, the study of sets with arbitrary operations, was started off by G. BIRKHOFF about 1935 and since has advanced to an extensive theory. There are two excellent monographs on this subject, one by COHN [1] and one by GRÄTZER [3]. Moreover KUROŠ [2] also includes a transparent introduction into the fundamentals of universal algebra which, in particular, served us as model for some parts of Ch. 1.

§ 4. Up to 1950 the notion of a polynomial was used almost exclusively in connection with rings. Subsequently papers appeared sporadically which introduced polynomials over algebras other than rings, e.g. over groups, lattices, and Boolean algebras, especially being tied up with systems of algebraic equations (see, for example, SCHUFF [1], [2], SHAFAAT [1]). A few papers (e.g. SCHUFF [3], SŁOMINSKI [1]) consider polynomials even over arbitrary algebras. The first time, however, that the concept of a polynomial was used in universal algebra, was in GRÄTZER [3]. There the "polynomial symbols" are nothing else than the elements of

our word algebra $W(X)$ in § 2.1, and "k-ary polynomials over A" are, in our terminology, the elements of the subalgebra $G_k(A)$ of the algebra $F_k(A)$ in § 6 which is generated by the projections $\xi_1, \xi_2, \ldots, \xi_k$ and the 0-ary operations ω_i of A. Thus $G_k(A)$ is a subalgebra of $P_k(A)$, and we call the elements of $G_k(A)$ "Grätzer's polynomial functions" while our polynomial functions are called "algebraic functions" in GRÄTZER's book. The definition of polynomials as it is used in our book is due to HULE [1], [2], and is—as we show in § 8—a straightforward generalization of the classical concept of a polynomial over a commutative ring with identity. Our presentation of §§ 4–6 follows partly HULE's work.

In all examples for semidegenerate varieties we know, semidegeneracy is due to 0-ary operations. We do not know whether or not the existence of 0-ary operations is a necessary condition for semidegeneracy.

In some sense dual to our Prop. 4.5 is the following statement: Let A be an algebra of the variety $\mathfrak{V}$ and $\mu: B \to A$ a monomorphism. Then μ can uniquely be extended to a monomorphism from $B(X, \mathfrak{V})$ to $A(X, \mathfrak{V})$ that fixes X. In general, however, this is not true, as the following counterexample by L. G. KOVÁCS shows: Let $\mathfrak{V}$ be the variety of all nilpotent groups of class $\leqslant 2$, $A = F(y_1, y_2, \mathfrak{V})$ the free algebra of $\mathfrak{V}$ with free generating set $\{y_1, y_2\}$, $B = A'$ the commutator group of A. By H. NEUMANN [1], B is a free abelian group. Let g be any element of a free generating set of B and $g^{-1}x^{-1}gx \in B(x, \mathfrak{V})$. Since B is free abelian, there exists a homomorphism from B to the dihedral group D_4 that maps g onto some element $g_1 \in D_4$ where $D_4 = [g_1, g_2]$. Since D_4 belongs to $\mathfrak{V}$, there is a homomorphism from $B(x, \mathfrak{V})$ to D_4 that maps $\{g, x\}$ onto $\{g_1, g_2\}$ whence $g^{-1}x^{-1}gx \neq 1$ in $B(x, \mathfrak{V})$ as D_4 is non-abelian. In $A(x, \mathfrak{V})$, however, we have $g \in A(x, \mathfrak{V})'$, and since $A(x, \mathfrak{V})$ is nilpotent of class $\leqslant 2$, we have $g^{-1}x^{-1}gx = 1$.

If we replace "monomorphism" by "homomorphism", however, then the statement just considered is true. Moreover, there are varieties, e.g. the varieties of commutative rings with identity and groups, where this statement is true as it stands (the proof can be given by aid of the normal forms in §§ 8,9). Thus it would be interesting to characterize all these varieties.

The problem of determining all those homomorphisms (isomorphisms) from $A(X, \mathfrak{V})$ to $B(X, \mathfrak{V})$ which extend a given epimorphism (isomorphism) $\vartheta: A \to B$ without necessarily fixing X has been studied just for special cases (see e.g. GILMER [1]).

§ 5. The lattice of polynomial algebras over a given algebra was studied the first time by HULE [2]. Among the open questions concerning this lattice, there is the problem of characterising all those algebras for which the epimorphism φ of Th. 5.22 is an isomorphism and the question whether or not the equation (5.3) remains valid if $\cap$ is replaced by $\cup$.

§ 6. For rings and fields, polynomial functions have been investigated long before the concept of a polynomial was introduced. In connection with the canonical epimorphism σ of Prop. 6.41, one can raise the question—which is closely related to the problem referred to in § 6.42—how to characterize all those algebras of a variety $\mathfrak{V}$ for which the canonical epimorphism $\sigma: A(x_1, \ldots, x_k, \mathfrak{V}) \to P_k(A)$ is an isomorphism. For the variety of rings with identity there exist a few results (ACZÉL [1], HOSSZÚ [1]). Recently a characterization of those noetherian rings for which σ (in the case $k = 1$) is an isomorphism, could be achieved by CAHEN and CHABERT [1]. In § 10 we show that σ is always an isomorphism for the variety of distributive lattices with zero and identity and for the variety of Boolean algebras.

A central problem in the theory of polynomial functions is the "problem of interpolation" which can be stated as follows: How can one recognize a function $\varphi \in F_k(A)$ to be a polynomial function and if φ is a polynomial function, how can one construct a corresponding polynomial? A closely related problem is that of "local interpolation": Let B be any finite subset of A^k and $\psi: B \to A$ a function. Is there a way to see whether or not ψ can be extended to a polynomial function on A^k and if ψ is extensible, how can one construct a corresponding polynomial? Both problems have been attacked mainly for $k = 1$ where, as is well-known (see VAN DER WAERDEN [1]), for A being a field, a characterization of polynomial functions can be achieved by certain difference equations and the construction of the corresponding polynomials is possible by means of the interpolation formulae of NEWTON or LAGRANGE. For other algebras than fields, however, there are just scattered results (for rings see CARLITZ [8], DUEBALL [1], RÉDEI and SZELE [1], [2], SPIRA [1], for groups see SCHUMACHER [1], and for Boolean algebras SCOGNAMIGLIO [1]).

§ 8. Whereas polynomial functions over commutative rings with identity, and even more in the case of fields, have been considered in algebra and analysis from time immemorial, the concept of a polynomial has

not become relevant until the rise of modern algebra. In modern algebra texts, polynomials are usually defined by the procedure as in § 8.11, that means by using certain sequences. It should be mentioned that a similar construction performed with all sequences $(a_0, a_1, \ldots)$ of elements of a commutative ring R with identity, again leads to some extension ring of R being called the ring of formal power series in x over R which is frequently denoted by $R[[x]]$ (see e.g. KERTÉSZ [1]). Some of our definitions for polynomials over commutative rings with identity make sense also for formal power series, and also some of our results have their counterparts for formal power series. Since, however, a generalization of formal power series to arbitrary algebras seems to be almost impossible, we have abstained from including formal power series in our book. For the same reason, the elements of the total quotient ring of $R[x]$ (see ZARISKI and SAMUEL [1]), the so-called rational functions in x over R, have been used here only as a handy tool for some proofs. But there are possibilities of generalizing some definitions and results of this book about polynomials to rational functions (see NÖBAUER [15], [16], LIDL [3]).

§ 9. Polynomials over groups have so far been dealt with only implicitely in connection with systems of equations over groups (see the remarks and comments at the end of ch. 2.).

§ 10. For polynomial algebras over arbitrary lattices, a normal form system has been found by SCHUFF [2] which is defined recursively and looks rather complicated, but it seems hopeless at the moment to find a handy normal form system, and this makes the investigation of this polynomial algebra rather tedious (some results can be found in MITSCH [1], SCHWEIGERT [1], SHAFAAT [1]). For the varieties of distributive lattices and Boolean algebras, however, there are quite a few results (e.g. MITSCH [2], RUDEANU [4] and ANDREOLI [1], RUDEANU [2], resp.). Polynomials and polynomial functions over Boolean algebras have important applications to several branches of mathematics, we mention probability theory, propositional calculus, and the theory of switching circuits.

§ 11. Several authors have defined concepts that are related to our notion of polynomially complete algebras, for arbitrary algebras as well as for certain varieties (for a survey on these concepts, see KAISER [1]). The general idea behind all these concepts is:

Let $\mathfrak{K}$ be an arbitrary class of algebras and, for any integer $k \geqslant 1$ and any A in $\mathfrak{K}$, $S_k(A)$ and $T_k(A)$ a pair of subsets of $F_k(A)$ such that $S_k(A) \subseteq T_k(A)$. An algebra A of $\mathfrak{K}$ is called $k-(S, T)$-complete if $S_k(A) = T_k(A)$, and A is called (S, T)-complete if A is $k-(S, T)$-complete for any k. Moreover, A is called locally $k-(S, T)$-complete if, for any $\varphi \in T_k(A)$ and any finite subset B of A^k, there exists some $\psi \in S_k(A)$ such that $\psi(a_1, \ldots, a_k) = \varphi(a_1, \ldots, a_k)$, for all $(a_1, \ldots, a_k) \in B$, and consequently A is called locally (S, T)-complete if A is locally $k-(S, T)$-complete for any k. KAISER [1] has also introduced a measure for the degree of incompleteness of an algebra A: If $A \in \mathfrak{K}$, then the least amongst the cardinals of all subsets U of $T_k(A)$ such that $[S_k(A) \cup U] \supseteq T_k(A)$ is called the $k-(S, T)$-completeness defect of A. If $\mathfrak{K}$ is the class of all algebras, $S_k(A) = P_k(A)$ and $T_k(A) = F_k(A)$, then we obtain just our concept of polynomial completeness. Other concepts of completeness were studied by FOSTER and his school in a long series of papers (see FOSTER [1]–[9], FOSTER and PIXLEY [1], KNOEBEL [1], PIXLEY [1], QUACKENBUSH [1], WERNER [1]). There e.g. the following special cases of (S, T)-completeness were introduced:

a) $S_k(A) = G_k(A)$, the algebra of GRÄTZER's polynomial functions, $T_k(A) = F_k(A)$; the (S, T)-complete algebras are called primal.

b) $S_k(A) = G_k(A)$, $T_k(A)$ the set of all "conservative" functions of $F_k(A)$, i.e. the set of all those functions $\varphi \in F_k(A)$ such that, for any subalgebra U of A, $(a_1, \ldots, a_k) \in U^k$ implies $\varphi(a_1, \ldots, a_k) \in U$; the (S, T)-complete algebras are called semiprimal.

c) $S_k(A) = G_k(A)\,(P_k(A))$, $T_k(A)$ the set of all "compatible" functions of $F_k(A)$, i.e. the set of all those functions φ of $F_k(A)$ such that, for any congruence Θ on A, $a_i \Theta b_i$, $i = 1, \ldots, k$, implies $\varphi(a_1, \ldots, a_k)\, \Theta \varphi(b_1, \ldots, b_k)$; the (S, T)-complete algebras are called hemiprimal (polynomially hemicomplete).

Th. 11.2 and its proof are due to SIERPIŃSKI [1].

§ 12. Th. 12.21 has been proved by RÉDEI and SZELE [1]. In RÉDEI and SZELE [1], [2] and NÖBAUER [21], some more concepts of completeness are investigated for commutative rings with identity. HEISLER [1] generalizes Th. 12.21 to non-commutative rings. For the variety of lattices, SCHWEIGERT [1] has introduced the concept of 1-order-polynomial completeness which is a special case of $1-(S, T)$-completeness when setting $S_1 = P_1, T_1 = O_1$ where $O_1(A)$ is the set of all order endomorphisms of

A, and the same author has given examples for 1-order-polynomially complete lattices. GRÄTZER [1], [2] has studied polynomial hemicompleteness for the varieties of Boolean algebras and distributive lattices.

Our proof of Prop. 12.5 is due to MAURER and RHODES [1] who use this proposition to show that every finite simple nonabelian group is polynomially complete. By using different methods, FRÖHLICH [1] has proved earlier that these groups are 1-polynomially complete. These methods were also used by LAUSCH [4] to investigate 1-polynomially complete multioperator groups. ROUSSEAU [1] has studied polynomial completeness for algebras with a single operation.

CHAPTER 2

ALGEBRAIC EQUATIONS

1. Systems of algebraic equations

1.1. Let $\mathfrak{V}$ be any variety, A an algebra of $\mathfrak{V}$ and $X = \{x_1, \ldots, x_k\}$ a finite set of indeterminates. An algebraic equation over $(A, \mathfrak{V})$ in the indeterminates $x_1, \ldots, x_k$ is a formal expression of the form

$$p = q$$

where $p, q \in A(X, \mathfrak{V})$. A system of algebraic equations over $(A, \mathfrak{V})$—in short, an algebraic system—in the indeterminates $x_1, \ldots, x_k$ is a family of algebraic equations over $(A, \mathfrak{V})$ in $x_1, \ldots, x_k$, indexed by an arbitrary (possibly infinite) set I:

$$p_i = q_i, \quad i \in I. \tag{1.1}$$

In particular, we may regard a single algebraic equation as an algebraic system.

Let B be an arbitrary $\mathfrak{V}$-extension of A, then, by ch. 1, Prop. 6.31, $p(b_1, \ldots, b_k)$ is a well-defined element of B, for every $(b_1, \ldots, b_k) \in B^k$ and every $p \in A(X, \mathfrak{V})$. This allows us to make the following definition:

The element $(b_1, \ldots, b_k) \in B^k$ is called a solution of the algebraic system (1.1) if $p_i(b_1, \ldots, b_k) = q_i(b_1, \ldots, b_k)$, for all $i \in I$.

An algebraic system over $(A, \mathfrak{V})$ is called solvable if there exists a $\mathfrak{V}$-extension B of A such that the system has a solution in B.

1.2. We want to obtain a criterion for the solvability of an algebraic system. First we prove

1.21. Lemma. *Let X be an arbitrary set of indeterminates, $P = \{(p_i, q_i) \mid i \in I\}$ a subset of $A(X, \mathfrak{V}) \times A(X, \mathfrak{V})$, and Θ the congruence on $A(X, \mathfrak{V})$ generated by P. Then $f \Theta g$ holds if and only if there is a chain $f = z_0, z_1, \ldots, z_r = g$ of polynomials of $A(X, \mathfrak{V})$ such that any two polynomials z_j, z_{j+1} are either equal or z_{j+1} is obtained from z_j by replacing a subword equal to p_i of a representation of z_j as a word by the corresponding q_i or by replacing a subword equal to q_i of a representation of z_j as a word by the corresponding p_i.*

Proof. We set $f\Theta_1 g$ if and only if there is a chain from f to g as described in the lemma. Then Θ_1 is a congruence on $A(X, \mathfrak{V})$ as one can easily see. Certainly Θ_1 contains P. Also every congruence on $A(X, \mathfrak{V})$ containing P contains Θ_1. This proves the lemma.

1.22. We define: A congruence Θ on $A(X, \mathfrak{V})$ is called separating if, for any two elements $a, b \in A$, $a\Theta b$ implies $a = b$. With this definition we can now state

1.23. Theorem. *The algebraic system $p_i = q_i$, $i \in I$, over $(A, \mathfrak{V})$ in $X = \{x_1, \ldots, x_k\}$ is solvable if and only if the congruence Θ on $A(X, \mathfrak{V})$ generated by the subset $\{(p_i, q_i) | i \in I\}$ of $A(X, \mathfrak{V}) \times A(X, \mathfrak{V})$ is separating.*

Proof. Suppose the hypothesis of the theorem is satisfied. We can then perform the embedding of A into $A(X, \mathfrak{V})|\Theta$, this yields some $\mathfrak{V}$-extension B of A. Let $\bar{x}_i$, $i = 1, \ldots, k$, be the congruence class of x_i under Θ, then $p_i \Theta q_i$ implies $p_i(\bar{x}_1, \ldots, \bar{x}_k) = q_i(\bar{x}_1, \ldots, \bar{x}_k)$. Hence $(\bar{x}_1, \ldots, \bar{x}_k)$ is a solution of the algebraic system in B. Conversely, suppose that the system is solvable, and let $(b_1, \ldots, b_k)$ be a solution of the system in some $\mathfrak{V}$-extension B of A. Then $f\Theta g$ implies, by Lemma 1.21, that $f(b_1, \ldots, b_k) = g(b_1, \ldots, b_k)$, hence, for $a, b \in A$, $a\Theta b$ implies $a = b$. Thus Θ is separating.

1.3. Theorem. *Let $p_i = q_i$, $i \in I$, be any algebraic system over $(A, \mathfrak{V})$ in $X = \{x_1, \ldots, x_k\}$. Then one of the following statements is true:*

a) *The system has at most one solution in every $\mathfrak{V}$-extension of A.*

b) *For every cardinal* $\mathfrak{u}$, *there exists some $\mathfrak{V}$-extension C of A such that the set of all solutions of the system in C has cardinality greater than* $\mathfrak{u}$.

Proof. Suppose that alternative a) is not true. Then there exists some $\mathfrak{V}$-extension B of A such that the system has at least two different solutions in B, say $(b_1, \ldots, b_k)$ and $(c_1, \ldots, c_k)$. Let $\mathfrak{u}$ be an arbitrary cardinal, L any set of cardinality $2^{\mathfrak{u}}$, $Y = \{x_{lt} | l \in L, 1 \leqq t \leqq k\}$ a set of indeterminates, and Λ that congruence on $A(Y, \mathfrak{V})$ which is generated by $\{(p_i(x_{l1}, \ldots, x_{lk}), q_i(x_{l1}, \ldots, x_{lk})) | i \in I, l \in L\}$. Λ is separating since, for $a, b \in A$, $a\Lambda b$ yields a polynomial chain in $A(Y, \mathfrak{V})$ from a to b according to Lemma 1.21 which, by replacing each x_{lt} by x_t, yields a polynomial chain in $A(X, \mathfrak{V})$ from a to b showing that $a\Theta b$, again by

Lemma 1.21. But Θ is separating, by Th. 1.23, whence $a = b$. Hence A can be embedded into $C = A(Y, \mathfrak{V})|\Lambda$, a $\mathfrak{V}$-extension of A. If $\bar{x}_{lt}$ is the congruence class of x_{lt} under Λ, then $(\bar{x}_{l1}, \ldots, \bar{x}_{lk}) \in C^k$ is a solution of the given system, for all $l \in L$. We have to show that $m \neq n$ implies $(\bar{x}_{m1}, \ldots, \bar{x}_{mk}) \neq (\bar{x}_{n1}, \ldots, \bar{x}_{nk})$. Assume the contrary, then $x_{mt} \Lambda x_{nt}$, $t = 1, 2, \ldots, k$. Lemma 1.21 yields a polynomial chain in $A(Y, \mathfrak{V})$ from x_{mt} to x_{nt}. If we replace each x_{mt} by b_t and each x_{rt} by c_t, for $r \neq m$, in this chain, this chain turns into a sequence of equal elements of B whence $b_t = c_t$, $t = 1, \ldots, k$. This is a contradiction. Hence there are at least $|L| = 2^{\mathfrak{u}} > \mathfrak{u}$ solutions in C.

1.31. Remark. Unless $\mathfrak{V}$ is semidegenerate and $|A| = 1$, either alternative of Th. 1.3. can occur, for arbitrary k. Indeed, let $a_i \in A$, then the system $x_i = a_i$, $i = 1, 2, \ldots, k$ is an example for alternative a) while $a_i = a_i$, $i \in I$, represents alternative b).

1.4. Let (S) be any solvable algebraic system over $(A, \mathfrak{V})$ in $X = \{x_1, \ldots, x_k\}$, and $(b_1, \ldots, b_k)$ a solution of (S) in some $\mathfrak{V}$-extension B of A. The subalgebra $A(b_1, \ldots, b_k)$ of B is called an (S)-root extension of A. A pair $A(b_1, \ldots, b_k)$, $A(c_1, \ldots, c_k)$ of (S)-root extensions of A is called equivalent if there exists an isomorphism from $A(b_1, \ldots, b_k)$ to $A(c_1, \ldots, c_k)$ fixing A elementwise and mapping b_i to c_i, $i = 1, \ldots, k$. A greatest (S)-root extension of A is an (S)-root extension $A(c_1, \ldots, c_k)$ of A such that, for any (S)-root extension $A(b_1, \ldots, b_k)$ of A, there exists a homomorphism from $A(c_1, \ldots, c_k)$ to $A(b_1, \ldots, b_k)$ fixing A elementwise and mapping c_i to b_i, $i = 1, \ldots, k$. Clearly such a homomorphism is the only one with this property and is an epimorphism.

1.41. Lemma. *Every solvable algebraic system (S) over $(A, \mathfrak{V})$ in $X = \{x_1, \ldots, x_k\}$ has a greatest (S)-root extension, and any two greatest (S)-root extensions of A are equivalent.*

Proof. The second statement is an immediate consequence of the definition of a greatest (S)-root extension. We claim that, if Θ is the congruence on $A(X, \mathfrak{V})$ generated by the equations of (S), C the algebra resulting from embedding A into $A(X, \mathfrak{V})|\Theta$, and $\bar{x}_i$, $i = 1, \ldots, k$, the congruence class of x_i in C, then $C = A(\bar{x}_1, \ldots, \bar{x}_k)$ is a greatest (S)-root extension. For let $A(b_1, \ldots, b_k)$ be an arbitrary (S)-root extension of A. If $w(a_i, \bar{x}_1, \ldots, \bar{x}_k) =$

$v(a_i, \bar{x}_1, \ldots, \bar{x}_k)$, for two words w, v, then $w(a_i, x_1, \ldots, x_k) \Theta v(a_i, x_1, \ldots, x_k)$ whence, by Lemma 1.21, $w(a_i, b_1, \ldots, b_k) = v(a_i, b_1, \ldots, b_k)$. Let $f \in A(\bar{x}_1, \ldots, \bar{x}_k)$ and $f = w(a_i, \bar{x}_1, \ldots, \bar{x}_k)$ be any representation of f as a word, then $\varphi f = w(a_i, b_1, \ldots, b_k)$ yields a well-defined mapping φ from $A(\bar{x}_1, \ldots, \bar{x}_k)$ to $A(b_1, \ldots, b_k)$. Clearly φ fixes A elementwise, maps $\bar{x}_i$ onto b_i and is a homomorphism. Thus C is a greatest (S)-root extension.

1.5. Let A be any algebra of $\mathfrak{V}$, $X = \{x_1, \ldots, x_k\}$, and $\mathfrak{L}(A(X, \mathfrak{V}))$ the congruence lattice of $A(X, \mathfrak{V})$. One can easily verify that the subset $\mathfrak{T}$ of $\mathfrak{L}(A(X, \mathfrak{V}))$ consisting of all separating congruences is a subsemilattice with respect to $\cap$, i.e. the intersection of any two separating congruences is again separating.

Now let Λ be any congruence on $A(X, \mathfrak{V})$. A k-tuple $(u_1, \ldots, u_k)$ of elements of a $\mathfrak{V}$-extension U of A is called a general root of Λ whenever $p \Lambda q$ holds if and only if $p(u_1, \ldots, u_k) = q(u_1, \ldots, u_k)$.

1.51. Proposition. *A congruence Λ on $A(X, \mathfrak{V})$ has a general root if and only if $\Lambda \in \mathfrak{T}$. If U is an arbitrary $\mathfrak{V}$-extension of A and $(u_1, \ldots, u_k) \in U^k$, then there is one and only one congruence Λ on $A(X, \mathfrak{V})$ such that $(u_1, \ldots, u_k)$ is a general root of Λ.*

Proof. If $\Lambda \notin \mathfrak{T}$, then there exist $a, b \in A$ such that $a \neq b$ but $a \Lambda b$, thus Λ cannot have a general root in this case. If $\Lambda \in \mathfrak{T}$, let U be the $\mathfrak{V}$-extension of A obtained from embedding A into $A(X, \mathfrak{V})|\Lambda$. If $\bar{x}_i$ is the congruence class of x_i in U, then $(\bar{x}_1, \ldots, \bar{x}_k)$ is a general root of Λ. Let $(u_1, \ldots, u_k) \in U^k$ where U is now an arbitrary $\mathfrak{V}$-extension of A, and Λ be the binary relation on $A(X, \mathfrak{V})$ defined by: $p \Lambda q$ if and only if $p(u_1, \ldots, u_k) = q(u_1, \ldots, u_k)$. Clearly Λ is a congruence on $A(X, \mathfrak{V})$ with $(u_1, \ldots, u_k)$ as a general root. By definition of a general root, Λ is uniquely determined by $(u_1, \ldots, u_k)$.

1.6. Let (S_1), (S_2) be two solvable algebraic systems in $X = \{x_1, \ldots, x_k\}$ over $(A, \mathfrak{V})$. We define: $(S_1) \supseteq (S_2)$ means that every solution of (S_1) is a solution of (S_2). (S_1) and (S_2) will be called equivalent if $(S_1) \supseteq (S_2)$ and $(S_2) \supseteq (S_1)$.

1.61. Lemma. *Let (S_1), (S_2) be solvable algebraic systems in $x_1, \ldots, x_k$ over $(A, \mathfrak{V})$ and Θ_i, $i = 1, 2$, the congruences on $A(X, \mathfrak{V})$ generated by the equations of (S_i). Then $(S_1) \supseteq (S_2)$ if and only if $\Theta_1 \supseteq \Theta_2$.*

Proof. Suppose that $(S_1) \supseteq (S_2)$, and let B be the algebra we get from embedding A into $A(X, \mathfrak{V})|\Theta_1$. By the proof of Th. 1.23, the k-tuple $(\bar{x}_1, \ldots, \bar{x}_k)$ of congruence classes of the x_i under Θ_1 is a solution of (S_1) and therefore a solution of (S_2). Thus, for every equation $p_i = q_i$ of (S_2) we have $p_i(\bar{x}_1, \ldots, \bar{x}_k) = q_i(\bar{x}_1, \ldots, \bar{x}_k)$ whence $p_i \Theta_1 q_i$, thus $\Theta_1 \supseteq \Theta_2$. Conversely, if $\Theta_1 \supseteq \Theta_2$ and $p_i = q_i$ is an equation of (S_2), we have $p_i \Theta_1 q_i$. Hence, by Lemma 1.21, every solution of (S_1) is a solution of (S_2), thus $(S_1) \supseteq (S_2)$.

1.62. Corollary. *Two solvable algebraic systems (S_1) and (S_2) are equivalent if and only if $\Theta_1 = \Theta_2$ where Θ_i is the congruence on $A(X, \mathfrak{V})$ corresponding to (S_i), $i = 1, 2$.*

Proof. Obvious.

1.7. Let again $\mathfrak{V}$ be any variety, A an algebra of $\mathfrak{V}$, and $X = \{x_1, \ldots, x_k\}$ a finite set of indeterminates. An algebraic inequality over $(A, \mathfrak{V})$ in the indeterminates $x_1, \ldots, x_k$ is a formal expression of the form

$$f \neq g$$

where $f, g \in A(X, \mathfrak{V})$. A mixed algebraic system over $(A, \mathfrak{V})$ in the indeterminates $x_1, \ldots, x_k$ is a family consisting of algebraic equations and inequalities where the equations are indexed by some set I and the inequalities by some set J disjoint from I. Thus a mixed algebraic system has the form

$$p_i = q_i, \quad i \in I, \quad f_j \neq g_j, \quad j \in J. \tag{1.7}$$

In particular, we may regard any algebraic system as a mixed algebraic system.

Now let B be any $\mathfrak{V}$-extension of A. The element $(b_1, \ldots, b_k) \in B^k$ is called a solution of (1.7) if $p_i(b_1, \ldots, b_k) = q_i(b_1, \ldots, b_k)$, for all $i \in I$, and $f_j(b_1, \ldots, b_k) \neq g_j(b_1, \ldots, b_k)$, for all $j \in J$. The mixed algebraic system (1.7) is called solvable if it has a solution in some suitable $\mathfrak{V}$-extension of A.

Th. 1.23 can now be easily generalized to the case of mixed algebraic systems:

1.71. Theorem. *The mixed algebraic system* $p_i = q_i$, $i \in I$, $f_j \neq g_j$, $j \in J$, *over* $(A, \mathfrak{V})$ *in* $X = \{x_1, \ldots, x_k\}$ *is solvable if and only if the congruence* Θ *on* $A(X, \mathfrak{V})$ *generated by the subset* $\{(p_i, q_i) | i \in I\}$ *of* $A(X, \mathfrak{V}) \times A(X, \mathfrak{V})$ *is a separating congruence such that* $f_j \Theta g_j$ *holds for no index* $j \in J$.

Proof. Suppose the hypothesis of the theorem holds. Then we can embed A into $A(X, \mathfrak{V})|\Theta$ in order to obtain a $\mathfrak{V}$-extension B of A where the k-tuple $(\bar{x}_1, \ldots, \bar{x}_k)$ consisting of the congruence classes of the x_i under Θ is a solution of the given mixed algebraic system.

Conversely suppose the system is solvable, and let $(b_1, \ldots, b_k)$ be a solution of this system in some $\mathfrak{V}$-extension B of A. Since $f \Theta g$ implies $f(b_1, \ldots, b_k) = g(b_1, \ldots, b_k)$, by Lemma 1.21, we see that Θ is separating, but $f_j \Theta g_j$ never holds.

1.72. Again we will call two solvable mixed algebraic systems equivalent if they have the same solutions.

2. Maximal systems of algebraic equations

2.1. Let $\mathfrak{V}$ be any variety, A an algebra of $\mathfrak{V}$, and $X = \{x_1, \ldots, x_k\}$ a finite set of indeterminates. An algebraic system (S) over $(A, \mathfrak{V})$ in X is called maximal if the congruence Θ on $A(X, \mathfrak{V})$ generated by the equations of (S) is a maximal element of the partially ordered set $\langle \mathfrak{T}, \leqslant \rangle$ of separating congruences, where $\leqslant$ is the set-theoretical inclusion of congruences.

2.11. Theorem. *Let* (S) *be a solvable algebraic system. Then the following conditions are equivalent:*

a) (S) *is maximal.*

b) *If* $p = q$ *is any equation over* $(A, \mathfrak{V})$ *in* X *and* $(S_1) = (S) \cup \{p = q\}$, *then either* (S_1) *is equivalent to* (S) *or* (S_1) *is not solvable.*

c) *Any two* (S)*-root extensions of* A *are equivalent.*

d) *Every solution of* (S) *is a general root of one and the same congruence* Λ *on* $A(X, \mathfrak{V})$.

e) *Every* (S)*-root extension of* A *is a greatest* (S)*-root extension.*

f) *If* (S_1) *is any algebraic system over* $(A, \mathfrak{V})$ *in* X, *and* (S) *and* (S_1) *have one solution in common, then* $(S) \supseteq (S_1)$.

g) *Every solvable algebraic system* (S_1) *is either equivalent to* (S) *or* (S_1) *has a solution which is not a solution of* (S).

Proof. a) $\Rightarrow$ b). Let (S) be maximal, Θ be the congruence generated by the equations of (S), (S_1) as in the hypothesis of b), and Θ_1 the congruence generated by the equations of (S_1). Then $\Theta_1 \supseteq \Theta$ whence $\Theta_1 = \Theta$ or $\Theta_1 \notin \mathfrak{T}$. In the first case, (S_1) is equivalent to (S), by Cor. 1.62 while in the second case, (S_1) is not solvable, by Th. 1.23.

b) $\Rightarrow$ c). Suppose (S) satisfies b), but not c). Then Lemma 1.41 implies that A has a greatest (S)-root extension $A(c_1, \ldots, c_k)$ and some other inequivalent (S)-root extension $A(b_1, \ldots, b_k)$. The epimorphism from $A(c_1, \ldots, c_k)$ to $A(b_1, \ldots, b_k)$ fixing A elementwise and mapping c_i to b_i is therefore not an isomorphism whence, for some polynomials $p, q \in A(X, \mathfrak{V})$, we have $p(c_1, \ldots, c_k) \neq q(c_1, \ldots, c_k)$, but $p(b_1, \ldots, b_k) = q(b_1, \ldots, b_k)$. Let $(S_1) = (S) \cup \{p = q\}$. Then (S_1) is not equivalent to (S) and is solvable, contradicting b).

c) $\Rightarrow$ d). Let $(u_1, \ldots, u_k)$, $(v_1, \ldots, v_k)$ be solutions of (S) and Λ_1, Λ_2 the congruences according to Prop. 1.51 corresponding to these solutions, respectively. Then $p \Lambda_1 q$ holds if and only if $p(u_1, \ldots, u_k) = q(u_1, \ldots, u_k)$ which holds if and only if $p(v_1, \ldots, v_k) = q(v_1, \ldots, v_k)$ which is equivalent to $p \Lambda_2 q$. Thus $\Lambda_1 = \Lambda_2$.

d) $\Rightarrow$ e). Let $A(c_1, \ldots, c_k)$ and $A(b_1, \ldots, b_k)$ be two (S)-root extensions of A. Then $(c_1, \ldots, c_k)$ and $(b_1, \ldots, b_k)$ are both general roots of Λ. Let $\vartheta : A(c_1, \ldots, c_k) \to A(b_1, \ldots, b_k)$ be the mapping defined by: $\vartheta p(c_1, \ldots, c_k) = p(b_1, \ldots, b_k)$, for all $p \in A(X, \mathfrak{V})$. This is a well-defined mapping since $p(c_1, \ldots, c_k) = q(c_1, \ldots, c_k)$ implies $p \Lambda q$ whence $p(b_1, \ldots, b_k) = q(b_1, \ldots, b_k)$. Clearly ϑ is a homomorphism fixing A elementwise and mapping c_i to b_i. Thus $A(c_1, \ldots, c_k)$ is a greatest (S)-root extension.

e) $\Rightarrow$ f). Let $(c_1, \ldots, c_k)$ be a common solution of (S) and (S_1). Then $p_i(c_1, \ldots, c_k) = q_i(c_1, \ldots, c_k)$, for every equation $p_i = q_i$ of (S_1). Let $(b_1, \ldots, b_k)$ be any solution of (S). Then, by Lemma 1.41, there is an isomorphism $\vartheta : A(c_1, \ldots, c_k) \to A(b_1, \ldots, b_k)$ fixing A elementwise and mapping c_i to b_i, $i = 1, \ldots, k$. Hence $p_i(b_1, \ldots, b_k) = q_i(b_1, \ldots, b_k)$ and thus $(b_1, \ldots, b_k)$ is also a solution of (S_1).

f) $\Rightarrow$ g). Suppose every solution of (S_1) is also a solution of (S) i.e. (S) and (S_1) have some solution in common. Hence $(S) \supseteq (S_1) \supseteq (S)$, i.e. (S) and (S_1) are equivalent.

g) $\Rightarrow$ a). Let Θ be the congruence on $A(X, \mathfrak{V})$ generated by the equations of (S) and $\Theta_1 \in \mathfrak{T}$ such that $\Theta_1 \supseteq \Theta$. The algebraic system (S_1) consisting of all equations $p = q$ such that $p \Theta_1 q$ has Θ_1 as its correspond-

ing congruence. By Lemma 1.61, $(S_1) \supseteq (S)$, whence (S_1) has just solutions which are also solutions of (S). Thus (S_1) and (S) are equivalent. By Cor. 1.62, $\Theta_1 = \Theta$ showing that Θ is maximal in $\mathfrak{T}$. Therefore (S) is maximal.

2.2. Proposition. *An algebraic system in $X = \{x_1, \ldots, x_k\}$ over $(A, \mathfrak{V})$ which has a solution $(a_1, \ldots, a_k) \in A^k$ is maximal if and only if it is equivalent to the system $x_i = a_i$, $i = 1, \ldots, k$.*

Proof. Let (S) be a system equivalent to the system $x_i = a_i$, $i = 1, \ldots, k$, then (S) has the unique solution $(a_1, \ldots, a_k)$ in every $\mathfrak{V}$-extension of A. Thus every solvable algebraic system (S_1) has either a solution which is not a solution of (S) or is equivalent to (S). Hence, by Th. 2.11 g), (S) is maximal. Conversely, let (S) be a system with the solution $(a_1, \ldots, a_k) \in A^k$ which is maximal. Then, by Th. 2.11 d), every solution of (S) is a general root of the same congruence Λ on $A(X, \mathfrak{V})$. Hence $x_i \Lambda a_i$, $i = 1, \ldots, k$. Let $(b_1, \ldots, b_k)$ be an arbitrary solution of (S), then $b_i = a_i$, $i = 1, \ldots, k$. Thus (S) is equivalent to the system $x_i = a_i$, $i = 1, \ldots, k$.

2.21. Proposition. *Let (S) be any solvable algebraic system in X over $(A, \mathfrak{V})$. Then there exists at least one maximal algebraic system $(S_1) \supseteq (S)$.*

Proof. Let Θ be the congruence on $A(X, \mathfrak{V})$ generated by the equations of (S), $\mathfrak{S}$ the subset of $\mathfrak{T}$ consisting of all congruences of $\mathfrak{T}$ containing Θ, partially ordered by the partial order of $\mathfrak{T}$, and $\{\Theta_i \mid i \in I\}$ any chain of $\mathfrak{S}$. Then $Z = \bigcup \{\Theta_i \mid i \in I\}$ is a congruence on $A(X, \mathfrak{V})$ such that if aZb, then $a\Theta_i b$, for some $i \in I$, thus $a = b$. Hence $Z \in \mathfrak{T}$ and even more, $Z \in \mathfrak{S}$. By Zorn's Lemma, $\mathfrak{S}$ has a maximal element Λ which is, of course, maximal in $\mathfrak{T}$. If (S_1) is the algebraic system consisting of all equations $p = q$ such that $p \Lambda q$, then $(S_1) \supseteq (S)$ and (S_1) is maximal.

2.3. Lemma. *Let $\mathfrak{V}$ be a semidegenerate variety, A any simple algebra of $\mathfrak{V}$, $X = \{x_1, \ldots, x_k\}$, Θ any congruence on $A(X, \mathfrak{V})$ which is maximal in $\mathfrak{T}$ and P the congruence on $A(X, \mathfrak{V})$ which has only one congruence class. Then there is no congruence Z on $A(X, \mathfrak{V})$ such that $\Theta \subset Z \subset P$.*

Proof. Let Z be a congruence on $A(X, \mathfrak{V})$ such that $Z \supset \Theta$. Since $Z \notin \mathfrak{T}$, the congruence $Z \cap (A \times A)$ on A cannot be the congruence where every

congruence class contains only one element. Hence $Z \cap (A \times A) = A \times A$ since A is simple. Under the canonical epimorphism from $A(X, \mathfrak{V})$ to $A(X, \mathfrak{V}) \mid Z$, the subalgebra A of $A(X, \mathfrak{V})$ is therefore mapped onto an algebra of order 1. Since $\mathfrak{V}$ is semidegenerate, this means that $|A(X, \mathfrak{V}) \mid Z| = 1$, thus $Z = P$.

2.31. Proposition. *Let $\mathfrak{V}$ be semidegenerate and A any simple algebra of $\mathfrak{V}$. If $(u_1, \ldots, u_k)$ is a k-tuple of a $\mathfrak{V}$-extension of A which is a solution of a maximal algebraic system (S) over $(A, \mathfrak{V})$, then the algebra $A(u_1, \ldots, u_k)$ is simple.*

Proof. Let Θ be the congruence on $A(X, \mathfrak{V})$ generated by the equations of (S). By the proof of Th. 1.23, $A(X, \mathfrak{V}) \mid \Theta$ yields an (S)-root extension $A(\bar{x}_1, \ldots, \bar{x}_k)$ of A which, by Th. 2.11 c), is isomorphic to $A(u_1, \ldots, u_k)$. Hence $A(X, \mathfrak{V}) \mid \Theta \cong A(u_1, \ldots, u_k)$. Since Θ is maximal in $\mathfrak{T}$, there is no congruence on $A(X, \mathfrak{V})$ between Θ and P, by Lemma 2.3. Hence the algebra $A(X, \mathfrak{V}) \mid \Theta$ is simple, by ch. 1, Th. 1.71., which proves the proposition.

2.32. Proposition. *Let $\mathfrak{V}$ be an arbitrary variety, A an algebra of $\mathfrak{V}$ with $|A| > 1$, and $A(u_1, \ldots, u_k)$ any $\mathfrak{V}$-extension of A which is simple. Then there exists a maximal algebraic system (S) over $(A, \mathfrak{V})$ which has $(u_1, \ldots, u_k)$ as a solution.*

Proof. Let Λ be the congruence on $A(X, \mathfrak{V})$ which has $(u_1, \ldots, u_k)$ as a general root, thus $p \Lambda q$ if and only if $p(u_1, \ldots, u_k) = q(u_1, \ldots, u_k)$. Let (S) be the algebraic system consisting of all equations $p = q$ such that $p \Lambda q$. (S) has $(u_1, \ldots, u_k)$ as a solution. By the proof of Lemma 1.41, embedding of A into $A(X, \mathfrak{V}) \mid \Lambda$ yields a greatest (S)-root extension $A(\bar{x}_1, \ldots, \bar{x}_k)$ of A. Clearly, the homomorphism from $A(\bar{x}_1, \ldots, \bar{x}_k)$ to $A(u_1, \ldots, u_k)$ fixing A elementwise and mapping $\bar{x}_i$ to u_i, $i = 1, \ldots, k$, is an isomorphism, hence $A(u_1, \ldots, u_k)$ is a greatest (S)-root extension. If (S) were not maximal, then, by Th. 2.11 e), there would exist an (S)-root extension $A(b_1, \ldots, b_k)$ which is not a greatest (S)-root extension, and the epimorphism from $A(u_1, \ldots, u_k)$ to $A(b_1, \ldots, b_k)$ fixing A elementwise and mapping u_i to b_i would not be an isomorphism. Since $A(u_1, \ldots, u_k)$ is simple, we conclude that $|A(b_1, \ldots, b_k)| = 1$ whence $|A| = 1$, a contradiction. Hence (S) is maximal.

2.33. Theorem. *Let $\mathfrak{V}$ be a semidegenerate variety and A a simple algebra of $\mathfrak{V}$ with $|A| > 1$. Then the k-tuple $(u_1, \ldots, u_k)$ of a $\mathfrak{V}$-extension of A is a solution of a maximal algebraic system over $(A, \mathfrak{V})$ if and only if $A(u_1, \ldots, u_k)$ is a simple algebra.*

Proof. This is immediate from Prop. 2.31 and Prop. 2.32.

3. Algebraically closed algebras

3.1. An algebraic system (S) over $(A, \mathfrak{V})$ in $x_1, \ldots, x_k$ is called finite if it consists of a finite number of equations. Similarly a mixed algebraic system is called finite if it consists of a finite number of equations and inequalities.

Now let $\mathfrak{V}$ be any variety. An algebra A of $\mathfrak{V}$ is called (mixed) algebraically closed if, for every $k \geqslant 1$, every solvable (mixed) algebraic system over $(A, \mathfrak{V})$ in the indeterminates $x_1, \ldots, x_k$ has a solution in A. The algebra A of $\mathfrak{V}$ is called weakly (mixed) algebraically closed if, for every $k \geqslant 1$, every solvable finite (mixed) algebraic system over $(A, \mathfrak{V})$ in $x_1, \ldots, x_k$ has a solution in A. Thus every mixed algebraically closed algebra is algebraically closed and every weakly mixed algebraically closed algebra is weakly algebraically closed.

(Of course all these definitions depend on the variety $\mathfrak{V}$. Thus, in fact, we should call A "algebraically closed in $\mathfrak{V}$", but since $\mathfrak{V}$, throughout this section, is being kept fixed, there is no danger of confusion).

3.2. Theorem. *Let A be any algebra of $\mathfrak{V}$. Then there always exists some $\mathfrak{V}$-extension C of A which is weakly mixed algebraically closed and therefore weakly algebraically closed.*

The proof of this theorem will depend on

3.21. Lemma. *Let A be an algebra of $\mathfrak{V}$. Then there exists some $\mathfrak{V}$-extension $\mathscr{E}(A) = B$ of A such that, for every $k \geqslant 1$, every solvable mixed algebraic system over $(B, \mathfrak{V})$ in the indeterminates $x_1, \ldots, x_k$, where the polynomials occurring in the equations and inequalities can be represented by words over A, has a solution in B.*

Proof. We may regard every family of equations and inequalities in $x_1, \ldots, x_k$, $k = 1, 2, \ldots$, as a set by neglecting the index sets for the

equations and inequalities. Then any two systems, which regarded as sets are equal, have the same solutions. But there is an injective mapping from the class of sets of equations and inequalities to the Cartesian product of two copies of the power set of $A(X, \mathfrak{V}) \times A(X, \mathfrak{V})$, $X = \{x_1, x_2, x_3, \ldots\}$. Hence the class of sets of equations and inequalities over $(A, \mathfrak{V})$ in $x_1, \ldots, x_k$, $k = 1, 2, \ldots$, is a set M which can be well-ordered, say $M = \{(S_\alpha) | \alpha = 1, 2, \ldots\}$, α running through the ordinals $\varrho < o$, o being a fixed ordinal. We put $A_0 = A$. Suppose that $\alpha > 0$ is an ordinal such that, for every ordinal $\gamma < \alpha$, a $\mathfrak{V}$-extension A_γ of A has been defined such that A_μ is a subalgebra of A_ν, for $\mu < \nu$. Then we define A_α by $A_\alpha = \bigcup \{A_\gamma | \gamma < \alpha\}$—which is a $\mathfrak{V}$-extension of A—if (S_α), regarded as a mixed algebraic system over $\bigcup \{A_\gamma | \gamma < \alpha\}$, is not solvable, $A_\alpha = \left(\bigcup \{A_\gamma | \gamma < \alpha\}\right)(u_1, \ldots, u_k)$ where $(u_1, \ldots, u_k)$ is a solution of (S_α) in some $\mathfrak{V}$-extension of $\bigcup \{A_\gamma | \gamma < \alpha\}$ if (S_α) is solvable. Then, for every $\mu < \alpha$, A_μ is a subalgebra of A_α, thus A_α is a $\mathfrak{V}$-extension of A. By transfinite induction, A_α is then defined to be a $\mathfrak{V}$-extension of A, for all $\alpha < o$, and A_μ is a subalgebra of A_ν, for $\mu < \nu$. We put $B = \bigcup \{A_\alpha | \alpha < o\}$ which is again a $\mathfrak{V}$-extension of A. Now let (S) be any solvable mixed algebraic system over $(B, \mathfrak{V})$ which satisfies the hypothesis of the lemma. If we represent the equations and inequalities of (S) by words over A and take the mixed algebraic system over $(A, \mathfrak{V})$ represented by this representations and regarded as a set, we obtain some set $(S_\alpha) \in M$ which has the same solutions as (S). Since (S) is solvable in some $\mathfrak{V}$-extension of B, (S_α)—regarded as a system over $\bigcup (A_\gamma | \gamma < \alpha)$— is solvable and therefore has a solution in $A_\alpha \subseteq B$. Hence (S) has a solution in B.

We are now ready to prove the theorem.

3.22. Proof of Th. 3.2. Let $A^{(0)} = A$ and define $A^{(n)}$, $n \geqslant 1$, recursively by $A^{(n)} = \mathscr{E}(A^{(n-1)})$. This yields a chain $A^{(0)}, A^{(1)}, A^{(2)}, \ldots$ of algebras of $\mathfrak{V}$, every member of which is a subalgebra of the subsequent one. Hence every member is a $\mathfrak{V}$-extension of A. We set $C = \bigcup (A^{(n)} | n \geqslant 0)$, then C is also a $\mathfrak{V}$-extension of A. Let (T) be any solvable finite mixed algebraic system over $(C, \mathfrak{V})$ in the indeterminates $x_1, \ldots, x_k$. Then the polynomials of the equations and inequalities of (T) can be represented by words of $W(C \cup X)$ where just finitely many elements of C occur in this representation. Hence these words are words of $W(A^{(n)} \cup X)$, for some $n \geqslant 0$. We consider the system (T_1) over $(A^{(n+1)}, \mathfrak{V})$, represented by these words; it is solvable since it has a solution in some $\mathfrak{V}$-extension of C. But

$A^{(n+1)} = \mathcal{C}(A^{(n)})$, hence, by Lemma 3.21, (T_1) has a solution in $A^{(n+1)}$ which is also a solution in C. Thus (T) has a solution in C, and the theorem is proved.

3.3. Proposition. *Let C be any mixed algebraically closed algebra of the variety $\mathfrak{V}$ containing a subalgebra $\{e\}$ of order 1. Then every finite algebra of $\mathfrak{V}$ which contains a subalgebra of order 1 can be embedded into C. If C is just weakly mixed algebraically closed, $\mathfrak{V}$ has just a finite family of operations and C contains a subalgebra $\{e\}$ of order 1, then also every finite algebra of $\mathfrak{V}$ with a subalgebra of order 1 can be embedded into C.*

Proof. Let $E = \{u_1, \ldots, u_r\}$ be any finite algebra of $\mathfrak{V}$, $X = \{x_1, \ldots, x_r\}$ a set of indeterminates, and $\chi : E \to X$ a bijection. We construct a mixed algebraic system over $(C, \mathfrak{V})$ in X as follows: As equations we take $\omega_i = \chi\omega_i$ if ω_i is a 0-ary operation of $\mathfrak{V}$, $\omega_i \chi u_{j_1} \chi u_{j_2} \ldots \chi u_{j_{n_i}} = \chi\omega_i u_{j_1} u_{j_2} \ldots u_{j_{n_i}}$ if ω_i is an n_i-ary operation of $\mathfrak{V}$, $n_i > 0$, and u_{j_k} running independently over all elements of E; as inequalities we take $\chi u_s \neq \chi u_t$, for all pairs u_s, u_t of different elements of E. This mixed algebraic system has a solution in the $\mathfrak{V}$-extension of C obtained from embedding C into $C \times E$, namely $\chi u_s = (e, u_s)$, $s = 1, \ldots, r$. Both hypotheses of the proposition imply that this system has a solution in C, say $\chi u_i = v(u_i)$, $i = 1, \ldots, r$. Then

$$v(\omega_i) = \omega_i,$$

$$v(\omega_i u_{j_1} \ldots u_{j_{n_i}}) = \omega_i v(u_{j_1}) \ldots v(u_{j_{n_i}}),$$

$$v(u_s) \neq v(u_t).$$

Hence $v : E \to C$ is a monomorphism. This completes the proof.

4. Algebraic independence

4.1. Let A be any algebra, B an extension of A, and $U = \{u_1, \ldots, u_n\}$ a finite subset of B. If $\mathfrak{V}$ is a variety and $B \in \mathfrak{V}$, then U is called $\mathfrak{V}$-algebraically dependent over A if there exist polynomials $f, g \in A(x_1, \ldots, x_n, \mathfrak{V})$ such that $f \neq g$ and $f(u_1, \ldots, u_n) = g(u_1, \ldots, u_n)$ while U is called $\mathfrak{P}$-algebraically dependent over A if there exist polynomial functions φ, ψ in the subalgebra $A(\xi_1, \ldots, \xi_n)$ of $P_n(B)$ such that $\varphi \neq \psi$ and $\varphi(u_1, \ldots, u_n) = \psi(u_1, \ldots, u_n)$. Clearly this definition does not depend on the order in which the elements of U are written down but just on the set U.

Subsequently "dependent" shall always mean "algebraically dependent" and $\mathfrak{C}$ will mean either $\mathfrak{P}$ or a variety $\mathfrak{V}$ such that $B \in \mathfrak{V}$. An infinite subset U of B will be called $\mathfrak{C}$-dependent over A if U contains some finite subset, which is $\mathfrak{C}$-dependent over A. A subset which is not $\mathfrak{C}$-dependent over A is called $\mathfrak{C}$-independent over A. In particular, the empty subset of B is $\mathfrak{C}$-independent.

4.11. Lemma. *Let A be any algebra, B an extension of A, and $U = \{u_i \mid i \in I\}$ a subset of B. Then the following four conditions are equivalent:*

a) *U is $\mathfrak{C}$-independent.*

b) *Every finite subset of U is $\mathfrak{C}$-independent.*

c) *If $f, g \in A(x_1, \ldots, x_n, \mathfrak{V})$ $(\varphi, \psi \in A(\xi_1, \ldots, \xi_n))$ such that $f(u_1, \ldots, u_n) = g(u_1, \ldots, u_n)$ $(\varphi(u_1, \ldots, u_n) = \psi(u_1, \ldots, u_n))$, for a certain subset $\{u_1, \ldots, u_n\}$ of U, then $f = g$ $(\varphi = \psi)$.*

d) *If $\mathfrak{C} = \mathfrak{V}$, then, for all $\mathfrak{V}$-extensions C of A, every mapping $\alpha : U \to C$ can be extended to a homomorphism from $A(U)$ to C fixing every element of A. If $\mathfrak{C} = \mathfrak{P}$, then every mapping $\alpha : U \to B$ can be extended to a homomorphism from $A(U)$ to B fixing A elementwise.*

Proof. a) $\Rightarrow$ b). If some finite subset V of U were $\mathfrak{C}$-dependent, then U would be finite, say $U = \{u_1, \ldots, u_n\}$. Then $V = \{u_{i_1}, \ldots, u_{i_s}\}$, $1 \leqslant i_j \leqslant n$, and there would exist $f, g \in A(x_1, \ldots, x_s, \mathfrak{V})$ $(\varphi, \psi \in A(\xi_1, \ldots, \xi_s))$ such that $f \neq g$ $(\varphi \neq \psi)$ and $f(u_{i_1}, \ldots, u_{i_s}) = g(u_{i_1}, \ldots, u_{i_s})$ $(\varphi(u_{i_1}, \ldots, u_{i_s}) = \psi(u_{i_1}, \ldots, u_{i_s}))$. By ch. 1, Cor. 4.62 (by the fact that $A(\xi_1, \ldots, \xi_s)$ can be embedded into $A(\xi_1, \ldots, \xi_n)$ such that the embedding fixes $A \cup \{\xi_1, \ldots, \xi_s\}$ elementwise), U would be $\mathfrak{C}$-dependent, contradiction. Thus a) implies b).

b) $\Rightarrow$ c). Obvious.

c) $\Rightarrow$ d). Let $p \in A(U)$, and $p = w(a_i, u_j)$ a representation of p as a word. We set $\varrho p = w(a_i, \alpha u_j)$. Then ϱ is a well-defined mapping from $A(U)$ to C, or B, resp., because of the assumption of c). Clearly ϱ is then a homomorphism extending α and fixing A elementwise.

d) $\Rightarrow$ a). Suppose U is not $\mathfrak{C}$-independent. Then there exists a $\mathfrak{C}$-dependent finite subset $\{u_1, \ldots, u_n\}$ of U, i.e., there exist $f, g \in A(x_1, \ldots, x_n, \mathfrak{V})$ $(\varphi, \psi \in A(\xi_1, \ldots, \xi_n))$ such that $f \neq g$ $(\varphi \neq \psi)$, $f(u_1, \ldots, u_n) = g(u_1, \ldots, u_n)$ $(\varphi(u_1, \ldots, u_n) = \psi(u_1, \ldots, u_n))$.

If $\mathfrak{C} = \mathfrak{V}$, let $C = A(x_1, \ldots, x_n, \mathfrak{V})$ and $\alpha u_i = x_i$, $i = 1, \ldots, n$. Then α cannot be extended to a homomorphism fixing A elementwise,

contradiction. If $\mathfrak{C} = \mathfrak{P}$, then there exist $b_1, \ldots, b_n \in B$ such that $\varphi(b_1, \ldots, b_n) \neq \psi(b_1, \ldots, b_n)$. Let $\alpha: U \to B$ be the mapping taking u_i to b_i, $i = 1, \ldots, n$, then again α cannot be extended to a homomorphism fixing A elementwise, contradiction.

4.2. If B is an extension of A, then every variety $\mathfrak{V}$ such that B is an algebra of $\mathfrak{V}$ yields some notion of $\mathfrak{V}$-independence over A in B. Moreover there is also a notion of $\mathfrak{P}$-independence over A in B. The relationship between these different notions of independence is described by

4.21. Proposition. *Let B be any extension of A. If $\mathfrak{V}_2 \supseteq \mathfrak{V}_1$ and U is $\mathfrak{V}_2$-independent, then U is also $\mathfrak{V}_1$-independent, and if U is $\mathfrak{V}$-independent for some variety $\mathfrak{V}$, then U is $\mathfrak{P}$-independent.*

Proof. Let $\mathfrak{V}_1 \subseteq \mathfrak{V}_2$ and U be $\mathfrak{V}_1$-dependent. Then there exist polynomials $f, g \in A(x_1, \ldots, x_n, \mathfrak{V}_1)$ such that $f \neq g$ and $f(u_1, \ldots, u_n) = g(u_1, \ldots, u_n)$, for some finite subset $\{u_1, \ldots, u_n\}$ of U. Let $\psi: A(x_1, \ldots, x_n, \mathfrak{V}_2) \to A(x_1, \ldots, x_n, \mathfrak{V}_1)$ be the epimorphism fixing $A \cup \{x_1, \ldots, x_n\}$ elementwise, according to ch. 1, Th. 5.22., and $f_1, g_1 \in A(x_1, \ldots, x_n, \mathfrak{V}_2)$ such that $\psi f_1 = f, \psi g_1 = g$. Then $f_1 \neq g_1$, and $f_1(u_1, \ldots, u_n) = g_1(u_1, \ldots, u_n)$ whence U is $\mathfrak{V}_2$-dependent. Suppose now that U is $\mathfrak{P}$-dependent. Then there are $\varphi, \psi \in A(\xi_1, \ldots, \xi_n)$ such that $\varphi \neq \psi$ and $\varphi(u_1, \ldots, u_n) = \psi(u_1, \ldots, u_n)$, for some finite subset $\{u_1, \ldots, u_n\}$ of U. Let $\varphi = w(a_i, \xi_1, \ldots, \xi_n)$, $\psi = v(a_i, \xi_1, \ldots, \xi_n)$ be any representation of φ and ψ, resp., as words and $f_1, g_1 \in A(x_1, \ldots, x_n, \mathfrak{V})$ such that $f_1 = w(a_i, x_1, \ldots, x_n)$, $g_1 = v(a_i, x_1, \ldots, x_n)$. Then $f_1 \neq g_1$, and $f_1(u_1, \ldots, u_n) = g_1(u_1, \ldots, u_n)$, thus U is $\mathfrak{V}$-dependent.

4.3. Let B be any extension of the algebra A. A subset U of B such that $B = A(U)$ is called an A-generating set of B. An A-generating set U of B is called minimal if no proper subset of U is an A-generating set.

4.31. Lemma. *Let A be any algebra of the variety $\mathfrak{V}$ and $X = \{x_i | i \in I\}$ a set of indeterminates. Unless $\mathfrak{V}$ is semidegenerate and $|A| = 1$, then X is a minimal A-generating set of $A(X, \mathfrak{V})$.*

Proof. By ch. 1, Prop. 4.11, X is an A-generating set of $A(X, \mathfrak{V})$. Suppose there is a proper subset of X which is also A-generating. Then, for suitable,

pairwise different $j, i_1, \ldots, i_r$ we have $x_j = w(a_i, x_{i_1}, \ldots, x_{i_r})$. By hypothesis, there exists a $\mathfrak{V}$-extension B of A such that $|B| > 1$. Let $\chi: X \to B$ be a mapping such that $\chi x_{i_s} = b_{i_s}$, $s = 1, \ldots, r$, where $b_{i_1}, \ldots, b_{i_r}$ are arbitrary elements of B and $\chi x_j \neq w(a_i, b_{i_1}, \ldots, b_{i_r})$, and $\psi_2: F(X, \mathfrak{V}) \to B$ the extension of χ to a homomorphism.

By ch. 1, Th. 4.31, there exists a homomorphism $\varrho: A(X, \mathfrak{V}) \to B$ such that $\varrho x_i = \psi_2 x_i$, $i \in I$, and $\varrho a = a$, $a \in A$. Then $\varrho x_j = \varrho w(a_i, x_{i_1}, \ldots, x_{i_r})$ and hence $\chi x_j = w(a_i, b_{i_1}, \ldots, b_{i_r})$, contradiction.

4.32. Lemma. *Let B be any extension of A and $W = \{w_i | i \in I\}$ an infinite minimal A-generating set of B. Then all minimal A-generating sets of B are infinite and of one and the same cardinality.*

Proof. Let $V = \{v_j | j \in J\}$ be any minimal A-generating set of B. Then, for every v_j, there exists some finite subset V_j of W such that $v_j \in A(V_j)$. Hence $\overline{W} = \cup(V_j | j \in J)$ is an A-generating set of B. This implies $\overline{W} = W$ and finiteness of J would imply finiteness of W. Hence V is infinite. Moreover, $|W| = |\cup(V_j | j \in J)| \leqslant \sum(|V_j| \, | j \in J) \leqslant \sum(\aleph_0 | j \in J) = |J| \, \aleph_0 = |J| = |V|$. Similarly we get $|V| \leqslant |W|$, hence $|V| = |W|$.

4.4. Let B be any extension of the algebra A and $|B| > 1$. $\mathfrak{C}$ shall have the same meaning as before, i.e. $\mathfrak{C} = \mathfrak{P}$ or $\mathfrak{V}$, where B is an algebra of $\mathfrak{V}$. An A-generating set U of B is called a $\mathfrak{C}$-basis of B over A if U is $\mathfrak{C}$-independent over A.

4.41. Proposition. *Every $\mathfrak{C}$-basis of B over A is a minimal A-generating set of B.*

Proof. Let $U = \{u_i | i \in I\}$ be a $\mathfrak{C}$-basis of B over A which is not a minimal A-generating set of B. Then $u_j = w(a_i, u_{i_1}, \ldots, u_{i_r})$, for suitable, pairwise distinct indices $j, i_1, \ldots, i_r$. If $\mathfrak{C} = \mathfrak{V}$, then, by Lemma 4.11 c), $x_{r+1} = w(a_i, x_1, \ldots, x_r)$ in $A(x_1, \ldots, x_{r+1}, \mathfrak{V})$ which contradicts Lemma 4.31. If $\mathfrak{C} = \mathfrak{P}$, then again by Lemma 4.11 c), $\xi_{r+1} = w(a_i, \xi_1, \ldots, \xi_r)$ in $A(\xi_1, \ldots, \xi_{r+1})$. But, if $b_1, \ldots, b_r \in B$, there exists $b_{r+1} \in B$ such that $b_{r+1} \neq w(a_i, b_1, \ldots, b_r)$ since $|B| > 1$, contradiction.

4.42. Theorem. *If B has some infinite $\mathfrak{C}$-basis over A, then all $\mathfrak{C}$-bases of B over A are infinite and of one and the same cardinality.*

Proof. By Prop. 4.41 and Lemma 4.32.

4.43. Theorem. *Let A be any finite algebra and suppose that, for $\mathfrak{C} = \mathfrak{V}$, there is some finite $\mathfrak{V}$-extension C of A with $|C| > 1$ while, for $\mathfrak{C} = \mathfrak{P}$, there is some finite extension C of A with $|C| > 1$ being a subalgebra of B. Then all the $\mathfrak{C}$-bases of B over A are of one and the same cardinality.*

Proof. By Th. 4.42, we can assume that B has just finite $\mathfrak{C}$-bases over A. Let $U = \{u_1, \ldots, u_m\}$, $V = \{v_1, \ldots, v_n\}$ be such $\mathfrak{C}$-bases. If $\mathfrak{C} = \mathfrak{V}$, then $\mathfrak{V}$-independence of U over A implies that the epimorphism $\varrho : A(x_1, \ldots, x_m, \mathfrak{V}) \to A(U)$ as defined in ch. 1, Lemma 4.43, is an isomorphism. Hence, if φ_1, φ_2 are the homomorphisms from ch. 1, § 4.3, we see that B, $\{\varrho\varphi_1, \varrho\varphi_2\}$ is a free union of the algebras A and $F(x_1, \ldots, x_m, \mathfrak{V})$ in $\mathfrak{V}$. If $\psi_1 : A \to C$ is the inclusion map, i.e. $\psi_1 a = a$, for all $a \in A$, and $\psi_2 : F(x_1, \ldots, x_m, \mathfrak{V}) \to C$ the homomorphism defined uniquely by $\psi_2 x_i = c_i$, $i = 1, \ldots, m$, where $(c_1, \ldots, c_m)$ is an arbitrary m-tuple of elements of C, then there is a unique homomorphism $\tau : B \to C$ such that $\psi_1 = \tau\varrho\varphi_1$ and $\psi_2 = \tau\varrho\varphi_2$. Clearly $\tau a = a$, for all $a \in A$ while $\tau u_i = c_i$, $i = 1, \ldots, m$. Since $B = A(U)$, there is only one such homomorphism from B to C satisfying these conditions. Hence the number of all homomorphisms from B to C fixing A elementwise is $|C|^m$. Similarly we obtain $|C|^n$ for this number. Since $|C| > 1$, we conclude that $m = n$. Now let $\mathfrak{C} = \mathfrak{P}$. Let $u_i \to c_i$, $i = 1, \ldots, m$, be an arbitrary mapping from U to C. Since U is $\mathfrak{P}$-independent and C is a subalgebra of B, the mapping $w(a_j, u_i) \to w(a_j, c_i)$ is a well-defined mapping τ from B to C. Moreover τ is a homomorphism which extends $u_i \to c_i$ and fixes A elementwise, and there is just one homomorphism of this kind. Thus the number of all homomorphisms from B to C fixing A elementwise is again $|C|^m$. By the same argument, this number is also $|C|^n$. Hence again $m = n$.

4.5. Theorem. *Let B be any extension of A with $|B| > 1$ which has $\mathfrak{C}$-bases over A of different cardinalities. Then every $\mathfrak{C}$-basis of B is finite, and the numbers of elements of all $\mathfrak{C}$-bases constitute an arithmetic progression.*

Proof. Th. 4.42 implies that every $\mathfrak{C}$-basis of B is finite. Suppose we have already shown that, if $\{a_1, \ldots, a_p\}$, $\{b_1, \ldots, b_q\}$, $\{c_1, \ldots, c_{q+r}\}$ are $\mathfrak{C}$-bases, then there exists also a $\mathfrak{C}$-basis consisting of $p+r$ elements. Let m and $m+d$ be the smallest numbers of elements of $\mathfrak{C}$-bases, then there

exist $\mathfrak{C}$-bases with $m+2d$, $m+3d$, ... elements and if there were a $\mathfrak{C}$-basis with $m+kd+r$ elements, $0 < r < d$, then there would also be a basis with $m+r$ elements, contradiction. Let therefore $\{a_1, \ldots, a_p\}$, $\{b_1, \ldots, b_q\}$, $\{c_1, \ldots, c_{q+r}\}$ be $\mathfrak{C}$-bases. By Lemma 4.11 d), there exists a homomorphism $\varphi : B \to B$ such that φ fixes A elementwise and $\varphi b_i = c_i$, $i = 1, \ldots, q$, which is even a monomorphism, since, by Lemma 4.11 b), $\{c_1, \ldots, c_q\}$ is $\mathfrak{C}$-independent. Moreover $\varphi B = A(c_1, \ldots, c_q)$ implies that $\varphi a_i \neq c_{q+j}$, $1 \leqslant i \leqslant p$, $1 \leqslant j \leqslant r$. If we can show that $\{\varphi a_1, \ldots, \varphi a_p, c_{q+1}, \ldots, c_{q+r}\}$ is a $\mathfrak{C}$-basis of B, the proof will be completed. We have

$$
\begin{aligned}
&A(\varphi a_1, \ldots, \varphi a_p, c_{q+1}, \ldots, c_{q+r}) = A(\varphi a_1, \ldots, \varphi a_p)(c_{q+1}, \ldots, c_{q+r}) \\
&= [\varphi A(a_1, \ldots, a_p)](c_{q+1}, \ldots, c_{q+r}) = (\varphi B)(c_{q+1}, \ldots, c_{q+r}) \\
&= [\varphi A(b_1, \ldots, b_q)](c_{q+1}, \ldots, c_{q+r}) \\
&= A(\varphi b_1, \ldots, \varphi b_q)(c_{q+1}, \ldots, c_{q+r}) = A(c_1, \ldots, c_q)(c_{q+1}, \ldots, c_{q+r}) \\
&= A(c_1, \ldots, c_{q+r}) = B.
\end{aligned}
$$

Hence $\{\varphi a_1, \ldots, \varphi a_p, c_{q+1}, \ldots, c_{q+r}\}$ is an A-generating set of B. Let L be an arbitrary $\mathfrak{V}$-extension of A, for $\mathfrak{C} = \mathfrak{V}$, and $L = B$ if $\mathfrak{C} = \mathfrak{P}$, and α an arbitrary mapping from $\{\varphi a_1, \ldots, \varphi a_p, c_{q+1}, \ldots, c_{q+r}\}$ to L, e.g. $\alpha\varphi a_i = d_i$, $i = 1, \ldots, p$, $\alpha c_i = \bar{d}_i$, $i = q+1, \ldots, q+r$. The monomorphism φ induces an isomorphism $\bar{\varphi} : B \to \varphi B = A(c_1, \ldots, c_q)$. Also, by Lemma 4.11 d), there exists a homomorphism $\chi : B \to L$ fixing A elementwise such that $\chi a_i = d_i$, $i = 1, \ldots, p$. We put $\varrho = \chi\bar{\varphi}^{-1}$ which is a homomorphism from $A(c_1, \ldots, c_q)$ to L. Again by Lemma 4.11 d), there is a homomorphism $\delta : B \to L$ fixing A elementwise such that $\delta c_i = \varrho c_i$, $i = 1, \ldots, q$, $\delta c_i = \bar{d}_i$, $i = q+1, \ldots, q+r$. Since ϱ fixes A elementwise, we see that $\delta c = \varrho c$, for all $c \in A(c_1, \ldots, c_q)$; in particular, $\delta\varphi a_i = \varrho\varphi a_i = \chi a_i = d_i$, $i = 1, \ldots, p$. Hence δ is a homomorphism extending α whence, by Lemma 4.11 d), $\{\varphi a_1, \ldots, \varphi a_p, c_{q+1}, \ldots, c_{q+r}\}$ is $\mathfrak{C}$-independent.

4.51. Proposition. *Let B be any extension of A which has a $\mathfrak{C}$-basis over A of n elements. Then B has a $\mathfrak{C}$-basis over A of m elements if and only if there are words $g_1(a_j, x_1, \ldots, x_n), \ldots, g_m(a_j, x_1, \ldots, x_n)$; $h_1(a_j, x_1, \ldots, x_m), \ldots, h_n(a_j, x_1, \ldots, x_m)$ such that, for $\mathfrak{C} = \mathfrak{V}$,*

$$
g_i(a_j, h_1(a_j, x_1, \ldots, x_m), \ldots, h_n(a_j, x_1, \ldots, x_m)) = x_i, \qquad i = 1, \ldots, m, \tag{4.51}
$$

holds in $A(x_1, \ldots, x_m, \mathfrak{V})$ *and*

$$h_i(a_j, g_1(a_j, x_1, \ldots, x_n), \ldots, g_m(a_j, x_1, \ldots, x_n)) = x_i, \qquad i = 1, \ldots, n, \tag{4.52}$$

holds in $A(x_1, \ldots, x_n, \mathfrak{V})$ *while, for* $\mathfrak{C} = \mathfrak{P}$, *the same equations hold in* $A(\xi_1, \ldots, \xi_m)$ *and* $A(\xi_1, \ldots, \xi_n)$ *with* ξ_i *instead of* x_i.

Proof. Suppose $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_m\}$ are $\mathfrak{C}$-bases of A. Then $v_i = g_i(a_j, u_1, \ldots, u_n)$, $i = 1, \ldots, m$, and $u_i = h_i(a_j, v_1, \ldots, v_m)$, $i = 1, \ldots, n$, where $g_i(a_j, x_1, \ldots, x_n)$, $h_i(a_j, x_1, \ldots, x_m)$ are some words. Hence $v_i = g_i(a_j, h_1(a_j, v_1, \ldots, v_m), \ldots, h_n(a_j, v_1, \ldots, v_m))$. By Lemma 4.11, we obtain (4.51), similarly (4.52). Conversely, suppose that $\{u_1, \ldots, u_n\}$ is a $\mathfrak{C}$-basis of B over A and the conditions of the proposition are satisfied. We set $v_i = g_i(a_j, u_1, \ldots, u_n)$, $i = 1, \ldots, m$. Now let $c_i \in L$, $i = 1, \ldots, m$, where L is an arbitrary $\mathfrak{V}$-extension of A if $\mathfrak{C} = \mathfrak{V}$ and $L = B$ if $\mathfrak{C} = \mathfrak{P}$. Set $b_i = h_i(a_j, c_1, \ldots, c_m) \in L$, $i = 1, \ldots, n$, and let $\varphi : B \to L$ be the homomorphism fixing A elementwise such that $\varphi u_i = b_i$, $i = 1, \ldots, n$. Then $\varphi v_i = g_i(a_j, \varphi u_1, \ldots, \varphi u_n) = g_i(a_j, b_1, \ldots, b_n) = g_i(a_j, h_1(a_j, c_1, \ldots, c_m), \ldots, h_n(a_j, c_1, \ldots, c_m)) = c_i$, $i = 1, \ldots, m$. Hence $\{v_1, \ldots, v_m\}$ is $\mathfrak{C}$-independent. Moreover, $\{v_1, \ldots, v_m\}$ is A-generating by (4.52). $u_i = h_i(a_j, v_1, \ldots, v_m)$

4.52. Corollary. *If an extension* B *of* A *has a* $\mathfrak{C}$*-basis over* A *consisting of one element and a* $\mathfrak{C}$*-basis of* n *elements,* $n > 1$, *then* B *has an* A*-generating set consisting of one* $\mathfrak{C}$*-dependent element.*

Proof. Let $\{u_1, \ldots, u_n\}$ and $\{v\}$ be two $\mathfrak{C}$-bases of B, and $g(a_j, x_1, \ldots, x_n)$, $h_i(a_j, x_1)$, $i = 1, \ldots, n$, words satisfying (4.51) and (4.52). By (4.52), $h_i(a_j, g(a_j, v, \ldots, v)) = v$, $i = 1, \ldots, n$, hence $\{g(a_j, v, \ldots, v)\}$ is A-generating. But $h_i(a_j, x_1) = h_k(a_j, x_1)$ in $A(x_1, \mathfrak{V})$ would imply $x_i = x_k$ in $A(x_1, \ldots, x_n, \mathfrak{V})$, hence $g(a_j, v, \ldots, v)$ is $\mathfrak{C}$-dependent if $\mathfrak{C} = \mathfrak{V}$. A similar argument works for $\mathfrak{C} = \mathfrak{P}$.

5. Systems of algebraic equations over groups. Algebraically closed groups

5.1. In this section we will specialize some of the results of this chapter to the variety of groups. Throughout this section, $\mathfrak{V}$ will mean the variety of groups while G stands for a group. We will also write, as in ch. 1, $G[X]$ for $G(X, \mathfrak{V})$.

We easily see that every algebraic system over $(G, \mathfrak{V})$ is equivalent to an algebraic system

$$p_i = 1, \quad i \in I,$$

while every mixed algebraic system over $(G, \mathfrak{V})$ is equivalent to a mixed algebraic system of the form

$$p_i = 1, \quad i \in I, \qquad f_j \neq 1, \quad j \in J.$$

Thus it suffices to consider just systems of this special form.

We can now restate Th. 1.71 which will also comprise Th. 1.23:

5.11. Theorem. *The mixed algebraic system* $p_i = 1$, $i \in I$, $f_j \neq 1$, $j \in J$ *over* $(G, \mathfrak{V})$ *in* $X = \{x_1, \ldots, x_k\}$ *is solvable if and only if the normal subgroup* N *of* $G[X]$ *generated by the subset* $\{p_i \mid i \in I\}$ *of* $G[X]$ *is such that* $N \cap G = \{1\}$ *and contains no* f_j.

Proof. Let Θ be the congruence on $G[X]$ generated by the subset $\{(p_i, 1) \mid i \in I\}$ of $G[X] \times G[X]$. If Λ is any congruence on $G[X]$, then $(p_i, 1) \in \Lambda$ if and only if $p_i \in \ker \Lambda$, and, by ch. 6, Th. 3.24, we easily see that $\ker \Theta = N$. Thus Θ is separating if and only if $N \cap G = \{1\}$, and $f_j \Theta 1$ if and only if $f_j \in N$. Now the theorem follows from Th. 1.71.

5.12. Remark. One sees immediately that all the statements of this subsection are true for any arbitrary variety of Ω-multioperator groups if we replace 1 by 0 and "normal subgroup" by "ideal".

5.2. Not every algebraic system over $(G, \mathfrak{V})$, not even every system consisting of one equation is solvable, e.g. $x^{-1}ax = 1$ has no solution for $a \neq 1$. There is, however, a large class of solvable algebraic systems consisting of one equation over $(G, \mathfrak{V})$ as the next theorem will show.

5.21. Proposition. *Let* $p = xb_0xb_1 \ldots xb_{n-1} = 1$, $n \geqslant 1$, *be any equation over* $G[x]$, $b_i \in G$, $i = 0, \ldots, n-1$. *Then* $p = 1$ *is solvable.*

Proof. Let C be a cyclic group of order n, and G wr C the regular wreath product of G by C. By ch. 6, § 6.61, this is the set of all pairs (h, φ) such that $h \in C$ and $\varphi : C \to G$ is a mapping, together with the group operation $(h_1, \varphi_1)(h_2, \varphi_2) = (h_1h_2, \psi)$ where $\psi h = (\varphi_1 h)\, \varphi_2(hh_1)$. If $\varkappa(g)$ denotes the constant function with value g, then $g \to (1, \varkappa(g))$ is clearly a monomorphism from G to G wr C, thus embedding G along this monomorphism yields an extension group H of G. Let $C = [c]$ and $\varphi : C \to G$ be defined by $\varphi(c^i) = b_{n-1-i}^{-1}$, $i = 0, 1, \ldots, n-1$. We claim that $(c, \varphi) \in H$

is a solution of our equation. Indeed,

$$(c,\varphi)(1,\varkappa(b_0))(c,\varphi)(1,\varkappa(b_1))\ldots(c,\varphi)(1,\varkappa(b_{n-1}))=(c^n,\psi)$$

where, for $h\in C$, $\psi h=(\varphi h)\,b_0\varphi(hc)\,b_1\varphi(hc^2)\ldots\varphi(hc^{n-1})b_{n-1}$. Hence $\psi(c^i)=(b_{n-i-1}^{-1}b_0b_{n-i-2}^{-1}b_1\ldots b_0^{-1}b_{n-i-1})(b_{n-1}^{-1}b_{n-i}b_{n-2}^{-1}\ldots b_{n-i}^{-1}b_{n-1})=1$. This completes the proof.

5.22. Theorem. *Let $X=\{x_1,\ldots,x_k\}$ and $p\in G[X]$ be a polynomial such that, in the normal form $p=a_0\mathfrak{x}^{\lambda_1}a_1\mathfrak{x}^{\lambda_2}\ldots a_{r-1}\mathfrak{x}^{\lambda_r}a_r$ of p, we have $r>0$, and moreover, if $\lambda_j=(l_{1j},\ldots,l_{kj})$, there is t with $l_{tj}\geqslant 0$ for all j or $l_{tj}\leqslant 0$ for all j and $l_{tj}>0$ or $l_{tj}<0$, resp., for one j. Then the algebraic system $p=1$ is solvable.*

Proof. Since $p=1$ and $p^{-1}=1$ are equivalent equations, we may assume that $l_{tj}\geqslant 0$ and $l_{tj}>0$ for one j. Then $\bar{p}=a_0x_t^{l_{t1}}a_1x_t^{l_{t2}}\ldots a_{r-1}x_t^{l_{tr}}a_r=1$ is equivalent to some $\bar{\bar{p}}=x_tb_0x_tb_1\ldots x_tb_{n-1}=1$, and hence solvable by Prop. 5.21. But then, $x_1=1,\ldots,x_{t-1}=1$, $x_t=c$, $x_{t+1}=1,\ldots,x_k=1$, where c is a solution of $\bar{p}=1$, is a solution of $p=1$.

5.23. Corollary. *If G is finite, then every algebraic system of Th. 5.22 has a solution in some finite extension group of G.*

Proof. By Th. 5.22 and the proof of Prop. 5.21.

5.24. Corollary. *Every equation $x^n=g$ over $(G,\mathfrak{B})$, where $g\in G$ and $n\neq 0$, is solvable and, if G is finite, has a solution in some finite extension group of G.*

5.25. A very interesting result on the (S)-root extensions of G where (S) is any finite algebraic system over $(G,\mathfrak{B})$ has been obtained which, similarly to field theory, ensures the existence of a "primitive element":

Let (S) be any solvable finite algebraic system over $(G,\mathfrak{B})$ in $\{x_1,\ldots,x_k\}$ and $|G|\neq 1$. Then every (S)-root extension $G(a_1,\ldots,a_k)$ of G can be embedded into some extension group $G(a)$ of G.

5.3. As remarked in § 3.1, every weakly mixed algebraically closed algebra is weakly algebraically closed. For groups, we will show the converse.

5.31. Theorem. *Every weakly algebraically closed group G with $|G|\neq 1$ is weakly mixed algebraically closed.*

Proof. The proof of this theorem depends on two lemmas we are going to prove first.

5.32. Lemma. *Let G be any group and H an extension group of G such that the finite mixed algebraic system over $(G,\mathfrak{B})$ in $x_1,\ldots,x_k$,*

$$u_i=1,\quad i\in I,\qquad v_j\neq 1,\quad j\in J, \tag{5.31}$$

has a solution in H. Moreover, let $1\neq g\in G$. Then there exists some extension group K of H such that the finite mixed algebraic system over $(G,\mathfrak{B})$ in the indeterminates $x_1,\ldots,x_k,y,z,s_j,j\in J,t_j,j\in J$, which we obtain from (5.31) by adding the equations

$$y^2=1,\quad g^{-1}z^2=1,\quad (yz)^2=1, \tag{5.32}$$

$$s_j^2=1,\quad (s_jv_j)^3=1,\quad j\in J, \tag{5.33}$$

$$t_j^{-1}s_jt_jy^{-1}=1,\quad j\in J, \tag{5.34}$$

has a solution in K.

Proof. Let m be the order of g, and D the dihedral group of order $4m$, for $m>0$, and the infinite dihedral group, for m infinite. Then $D=[a,b]$, $a^2=b^{2m}=(ab)^2=1$. Let L be the free product of H and D with amalgamation $b^2=g$. Then, in L, the equations (5.32) have a solution $y=a$, $z=b$. Let $(h_1,\ldots,h_k)$ be a solution of (5.31) in H, and therefore in L, $v_j(h_1,\ldots,h_k)=f_j\in H$, $j\in J$, $m(j)$ the order of f_j, and C_j, $j\in J$, the group generated by $\{c_j,d_j\}$ defined by the relations $c_j^2=(c_jd_j)^3=d_j^{m(j)}=1$. We claim that c_j is of order 2 and d_j is of order $m(j)$. Indeed, if U is the group of unimodular 2×2-matrices over the integers mod $m(j)$, Z is the normal subgroup of U consisting of the matrices $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ and $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$, and V the subgroup of $U|Z$ generated by the elements $c_j=\begin{pmatrix}0&1\\-1&0\end{pmatrix}Z$ and $d_j=\begin{pmatrix}1&-1\\0&1\end{pmatrix}Z$, then an easy computation shows that c_j,d_j satisfy the relations above, c_j is of order 2, and d_j of order $m(j)$. Let M_1 be the free product of L and C_1 with amalgamation $d_1=f_1$, M_2 the free product of M_1 and C_2 with amalgamation $d_2=f_2$, etc., then we eventually get some extension group M of L. In M, the equations (5.33) have a solution $x_1=h_1,\ldots,x_k=h_k$, $s_j=c_j$, and a and c_j are elements of order 2. By ch. 6, Cor. 6.81, there is an ex-

tension group K of M where every c_j is conjugate to a whence there exist elements t_j in K solving (5.34). This completes the proof.

5.33. Lemma. *Let $g \neq 1$ be an element of G such that the algebraic system (T) consisting of the equations of* (5.31), (5.32), (5.33), (5.34) *is solvable. Then every solution of the algebraic system (T) is also a solution of the mixed algebraic system* (5.31).

Proof. Let $(h_1, \ldots, h_k, y, z, s_j, t_j)$ be a solution of the algebraic system (T) such that one of the inequalities of (5.31) fails to hold, i.e. $v_l(h_1, \ldots, h_k) = 1$, for some $l \in J$. Then (5.33) implies $s_l = 1$ whence, by (5.34), $y = 1$. Thus, by (5.32), $g = 1$, contradiction.

5.34. Proof of Th. 5.31. Let $|G| \neq 1$, with G weakly algebraically closed. Suppose (5.31) has a solution in some extension group H of G. For an arbitrary $1 \neq g \in G$, there exists, by Lemma 5.32, an extension group K of H such that the finite algebraic system (T) of Lemma 5.33 has a solution in K. Since G is algebraically closed, (T) has a solution in G which, by Lemma 5.33, is also a solution of (5.31). This completes the proof.

5.35. Proposition. *Every weakly algebraically closed group is simple.*

Proof. Since the group of order 1 is simple, we can assume that $|G| \neq 1$. Let N be any non-trivial normal subgroup of G and $1 \neq g_1 \in N$. Then the mixed system (5.31) consisting of $g_1 \neq 1$ is solvable, hence, if $1 \neq g \in G$, the corresponding system (T) of Lemma 5.33 is solvable and has therefore a solution in G. Hence with this solution

$$\begin{aligned} g = z^2 &= yz^{-1}yz = (t_1^{-1}s_1t_1)(z^{-1}t_1^{-1}s_1t_1z) \\ &= (t_1^{-1}(s_1g_1)^3 s_1t_1)(z^{-1}t_1^{-1}(s_1g_1)^3 s_1t_1z) \\ &= [(t_1^{-1}s_1^{-1}g_1s_1t_1)(t_1^{-1}g_1t_1)(t_1^{-1}s_1^{-1}g_1s_1t_1)] \\ &\quad \cdot [(z^{-1}t_1^{-1}s_1^{-1}g_1s_1t_1z)(z^{-1}t_1^{-1}g_1t_1z)(z^{-1}t_1^{-1}s_1^{-1}g_1s_1t_1z)]. \end{aligned}$$

Hence $g \in N$ and therefore $N = G$.

5.36. Corollary. *Every group can be embedded into a simple group.*

Proof. This is a consequence of Th. 3.2 and Prop. 5.35.

5.4. Remark. We have defined algebraic systems $p_i = q_i$ over $(A, \mathfrak{V})$ where p_i, q_i are polynomials of $A(X, \mathfrak{V})$ and X is a finite set of indeterminates. One could also drop the finiteness assumption on X, and it would still be possible to save a considerable part of the theory since the proof of ch. 1, Prop. 6.31 remains valid and thus the value of a polynomial on a place of a $\mathfrak{V}$-extension of A is well defined. Thus it makes sense to define solutions and solvability of such "unrestricted algebraic systems" as in § 1. An algebra A such that every solvable unrestricted algebraic system over $(A, \mathfrak{V})$ has a solution in A is called "absolutely algebraically closed".

Unrestricted algebraic systems have been considered by various authors and our results on algebraic systems are, to some extent, generalizable to unrestricted algebraic systems.

A remarkable result on the existence of absolutely algebraically closed algebras in the variety of groups is the following.

5.41. Theorem. *There is only one absolutely algebraically closed group, namely the group of order* 1.

Proof. The theorem will be a consequence of

5.42. Lemma. *Let G be a group and A any subgroup of G. Any unrestricted algebraic system over A which has some solution in G, has also a solution in A if and only if A is a semidirect factor (retract) of G.*

Proof. Let A be a semidirect factor of G. Then $G = AN$ where $N \lhd G$ and $A \cap N = \{1\}$. Let $f_i(x_l) = 1$, $i \in I$, be an arbitrary unrestricted system over A in the indeterminates $\{x_l | l \in J\}$ which has a solution $\{g_l | l \in J\}$ in G. Then $g_l = a_l d_l$, $a_l \in A$, $d_l \in N$, thus $g_l \Theta a_l$ where Θ is the congruence corresponding to N. Hence $f_i(a_l) \Theta 1$, thus $f_i(a_l) \in A \cap N = \{1\}$ whence $\{a_l | l \in J\}$ is a solution of the system in A.

Conversely suppose that the hypothesis of the lemma is satisfied for G and A. Let $M = \{g_l | l \in J\}$ be any set of elements of G with $G = A(M)$, and $\{f_i(x_l) | i \in I\}$ the set of all polynomials over A in the indeterminates $\{x_l | l \in J\}$ such that $f_i(g_l) = 1$. Then the unrestricted system $f_i = 1$, $i \in I$, has a solution in G whence it has also a solution $\{a_l | l \in J\}$ in A. Let $B = \{a_l^{-1} g_l | l \in J\}$ and N the least normal subgroup of G containing B. Then $AN = G$. Suppose that $a \in A \cap N$. Then $a = h_1^{-1}(a_{l_1}^{-1} g_{l_1})^{e_1} h_1 \ldots$

$\cdot h_k^{-1}(a_{l_k}^{-1}g_{l_k})^{e_k}h_k$ where $h_i \in G$, $e_i = \pm 1$. But since $G = A(M)$, we have $h_i = w_i(b_r, g_s)$, $b_r \in A$, thus $a^{-1}w_1(b_r, g_s)^{-1}(a_{l_1}^{-1}g_{l_1})^{e_1}w_1(b_r, g_s)\ldots = 1$. This is an equation over A of the form $f_i(g_l) = 1$. Hence we can replace every g_l by a_l and obtain a true relation. This shows that $a = 1$ whence A is a semidirect factor of G.

5.43. Proof of Th. 5.41. Let A be an absolutely algebraically closed group, and H any extension group of A such that $|H| > |A|$, e.g. $F_1(A)$ for $|A| \neq 1$. By Cor. 5.36, there exists a simple group G containing H as a subgroup. Every unrestricted algebraic system over A which has a solution in G, has also a solution in A, thus, by Lemma 5.42, A is a semidirect factor of G. Hence G has a normal subgroup N such that $G = AN$ and $A \cap N = \{1\}$. Since G is simple, $N = \{1\}$ or G. In the first case we would get $|G| = |A|$ whence $|H| \leqq |A|$, contradiction. Hence $A = \{1\}$.

Remarks and comments

§§ 1.2. Systems of algebraic equations have so far been studied mainly for special classes of algebras (see the comments on § 5). Algebraic inequalities in the sense of our definition have been introduced by W. R. SCOTT [1] for the class of groups. Systems of algebraic equations over arbitrary algebras have been considered by DÖRGE [1], [2], DÖRGE and SCHUFF [1], SŁOMINSKI [1], HULE [3], and under certain restrictions for the algebras, by SHODA [1], [2]. Our presentation partly follows HULE's paper, partly we have tried to generalize some fundamental concepts from the classical theory of algebraic manifolds (see e.g. VAN DER WAERDEN [2]) from fields to more general classes of algebras. Indeed, some of the results of § 2 seem to indicate that simple algebras in arbitrary semidegenerate varieties behave similarly as fields do in the variety of commutative rings with identity with respect to systems of algebraic equations.

Th. 1.23 is, we believe, due to DÖRGE who has proved the result for arbitrary algebras even for the case of infinitely many indeterminates and Th. 1.3 has been proved by HULE. Amongst the unsolved problems of this section, we mention:

a) Let (S) be a solvable algebraic system over $(A, \mathfrak{V})$, B a $\mathfrak{V}$-extension of A, $\vartheta: A(X, \mathfrak{V}) \to B(X, \mathfrak{V})$ that homomorphism which extends the inclusion monomorphism from A to B, and (ϑS) the algebraic system over $(B, \mathfrak{V})$ which is obtained from applying ϑ to each equation of (S). Is (ϑS) also solvable?

b) Has every solvable algebraic system over $(A, \mathfrak{V})$ which satisfies the first alternative of Th. 1.3 a solution in A?

§ 3. Various concepts of being algebraically closed have been used, and most of them are special cases of the general notion of being $(\mathfrak{m}, \mathfrak{n})$-algebraically closed which is defined as follows:

Let $\mathfrak{V}$ be any variety and $\mathfrak{m}$, $\mathfrak{n}$ arbitrary cardinals. An algebra A of $\mathfrak{V}$ is called $(\mathfrak{m}, \mathfrak{n})$-algebraically closed in $\mathfrak{V}$ if every (possibly unrestricted, see § 5.4) solvable algebraic system over $(A, \mathfrak{V})$ consisting of less than $\mathfrak{m}$ equations in less than $\mathfrak{n}$ indeterminates has a solution in A. For example, being weakly algebraically closed in our book means being $(\aleph_0, \aleph_0)$-algebraically closed. (By slightly modifying the definition of being $(\mathfrak{m}, \mathfrak{n})$-algebraically closed, one could also cover the classical concept of being algebraically closed for fields, this we leave to the reader). The relationship between the different concepts of being algebraically closed is far from being known completely.

Just occasionally there have been investigations on algebraic closedness in its general meaning (e.g. SHODA [3], FUJIWARA [1], BOKUT' [1]). Special results refer to the variety of groups or sometimes semigroups (see W. R. SCOTT [1], B. H. NEUMANN [1], [2], [3], ERDÉLYI [1]). Our proof of Th. 3.2 is a generalization of SCOTT's proof for groups, and Prop. 3.3 is due to B. H. NEUMANN for the special case of groups.

In this context we also refer to the concept of an equationally compact algebra which has recently been studied in several papers (see MYCIELSKY and RYLL-NARDZEWSKI [1], WEGLORZ [1], [2], WENZEL [1]). An algebra A of the variety $\mathfrak{V}$ is called equationally compact if every (unrestricted) algebraic system (S) over $(A, \mathfrak{V})$ has a solution in A provided that every finite subsystem of (S) has a solution in A (it is easy to see that this concept is independent of the variety $\mathfrak{V}$).

§ 4. There are several concepts of independence in classes of algebras (a general discussion of dependence relations in algebras can be found in COHN [1], for groups see LYNDON [1]). One of the most natural and, as we think, also most useful concepts has been introduced and thoroughly investigated by MARCZEWSKI and his school (there is an exposition of this work in GRÄTZER [3]). This is MARCZEWSKI's definition of independence:

Let B be an algebra and $S = \{u_i | i \in I\}$ a subset of B. Then S is called independent if and only if, for any $k \geqslant 1$, any two functions $p, q \in G_k(B)$ (the algebra of GRÄTZER's polynomial functions), and any subset $\{u_1, \ldots, u_k\}$ of S, $p(u_1, \ldots, u_k) = q(u_1, \ldots, u_k)$ implies $p = q$.

If B is an extension of A, then Lemma 4.11 shows that this definition of independence in B is closely related to our definition of $\mathfrak{P}$-independence over A. Indeed, if the subalgebra of A generated by the 0-ary operations coincides with A, then $\mathfrak{P}$-independence over A in our sense coincides with independence in B in the sense of MARCZEWSKI. Therefore all our results of § 4 correspond to results on MARCZEWSKI's independence. Hence the presentation of our § 4 resembles strongly that in GRÄTZER [3], § 31.

§ 5. As mentioned, there exists quite a large number of papers on systems of algebraic equations over certain special classes of algebras. Apart from systems of equations over commutative rings, and fields in particular (which are the subject of the classical theory of elimination, and fundamental in algebraic geometry, and have been treated in abundance), there exists also a remarkable literature on algebraic systems over Boolean algebras (e.g. ABIAN [1], ANDREOLI [2], RUDEANU [1], [3], [5]) and over groups (e.g. ALLENBY [1], ERDÉLYI [1], GERSTENHABER and ROTHAUS [1], HOANG KI [1], ISAACS [1], LEVIN [1], [2], SCHIEK [1], SCHUFF [1], SOLOMON [1]). For algebraic equations over other special classes of algebras, see GOODSTEIN [3], LEVIN [3], RUDEANU [4].

Th. 5.11 (for algebraic systems) is also contained in ERDÉLYI [1], Th. 5.22 and its proof is due to LEVIN [1], who has also proved (see [2]) the result which is mentioned in § 5.25. The results and proofs of § 5.3 are due to B. H. NEUMANN [1], Lemma 5.42 is a result of ERDÉLYI [1].

CHAPTER 3

COMPOSITION OF POLYNOMIALS AND POLYNOMIAL FUNCTIONS

1. Composition algebras

1.1. Let M be a non-empty set, k a positive integer, $\varkappa$ a $(k+1)$-ary operation on M, ω_i an n_i-ary operation on M, and $x_j, y_l, j, l = 0, 1, 2, \ldots$, indeterminates. We define:

a) The operation $\varkappa$ is called superassociative if $\varkappa$ satisfies the law

$$\varkappa\varkappa x_0 x_1 \ldots x_k y_1 y_2 \ldots y_k = \varkappa x_0 \varkappa x_1 y_1 \ldots y_k \varkappa x_2 y_1 \ldots y_k \ldots \varkappa x_k y_1 \ldots y_k.$$

b) The operation $\varkappa$ is called right-superdistributive with respect to ω_i if $\varkappa$ satisfies the law

$$\varkappa\omega_i y_1 \ldots y_k = \omega_i, \quad \text{for} \quad n_i = 0,$$

$$\varkappa\omega_i x_1 \ldots x_{n_i} y_1 \ldots y_k = \omega_i \varkappa x_1 y_1 \ldots y_k \varkappa x_2 y_1 \ldots y_k \ldots \varkappa x_{n_i} y_1 \ldots y_k, \quad \text{for} \quad n_i > 0.$$

c) The family $\{s_1, \ldots, s_k\}$ of elements of M is called a selector system for the operation $\varkappa$, if $s_1, \ldots, s_k$ regarded as 0-ary operations on M satisfy the laws

$$\varkappa s_i y_1 \ldots y_k = y_i, \qquad i = 1, 2, \ldots, k, \tag{1.1.a}$$

$$\varkappa x_1 s_1 \ldots s_k = x_1. \tag{1.1.b}$$

1.11. Lemma. *There exists at most one selector system for $\varkappa$.*

Proof. Let $\{t_1, \ldots, t_k\}$ be also a selector system for $\varkappa$. Then $t_i = \varkappa s_i t_1 \ldots t_k = s_i$, $i = 1, \ldots, k$, by (1.1.a) and (1.1.b).

1.12. Remark. Let $k = 1$ and $n_i = 2$. Then superassociativity reduces to ordinary associativity, right-superdistributivity to ordinary right-distributivity, and a selector system for $\varkappa$ to an identity for $\varkappa$.

1.2. Let $\mathfrak{V}$ be a class of algebras of type $T = \{n_\iota | \iota < o\}$ and $\Omega = \{\omega_\iota | \iota < o\}$ the family of operation symbols of the algebras in $\mathfrak{V}$ where o is a fixed

ordinal. Let A be any algebra of type T with Ω as its family of operations, and $\varkappa$ a $(k+1)$-ary operation on A, $k > 0$ an integer. If we put $\omega_o = \varkappa$, then $\Omega_1 = \{\omega_\iota | \iota < o+1\}$ is a family of operations on A.

The algebra $A = \langle A; \Omega_1 \rangle$ is called a k-dimensional $\mathfrak{V}$-composition algebra if

a) $\langle A; \Omega \rangle$ is an algebra of $\mathfrak{V}$,

b) $\varkappa$ is superassociative,

c) $\varkappa$ is right-superdistributive with respect to $\omega_\iota \in \Omega$, for all $\iota < o$.

The algebra $A = \langle A; \Omega_1 \rangle$ is called a k-dimensional $\mathfrak{V}$-composition algebra with selector system if there is a selector system for $\varkappa$ in A. Every k-dimensional $\mathfrak{V}$-composition algebra $\langle A; \Omega_1 \rangle$ with selector system can be regarded as an algebra with the family $\Omega_2 = \{\omega_\iota | \iota < o+k+1\}$ of operations where $\omega_{o+1}, \ldots, \omega_{o+k}$ is the selector system for $\varkappa$ regarded as a family of 0-ary operations.

1.21. Proposition. *If the class $\mathfrak{V}$ is a variety with respect to Ω, then, for any k, the class of k-dimensional $\mathfrak{V}$-composition algebras is a variety with respect to Ω_1, and the class of k-dimensional composition algebras with selector system is a variety with respect to Ω_2.*

This is a straightforward consequence of the definitions of superassociativity, right-superdistributivity, and selector systems since all these concepts are defined by laws.

1.3. A few examples will illustrate the concept of composition algebras:

Let $\mathfrak{V}$ be the variety of sets, i.e. $\Omega = \phi$, then the k-dimensional $\mathfrak{V}$-composition algebras are the so-called k-dimensional superassociative systems. In particular, the 1-dimensional superassociative systems are exactly the semigroups.

Let $\mathfrak{V}$ be the variety of groups as considered in ch. 1, § 2.4. Then the k-dimensional $\mathfrak{V}$-composition algebras are called k-dimensional composition groups. In particular, the 1-dimensional composition groups are better known under the name "near-rings".

If $\mathfrak{V}$ is the variety of rings as considered in ch. 1, § 2.4, then the k-dimensional $\mathfrak{V}$-composition algebras are called k-dimensional composition rings. 1-dimensional composition rings are also known as composition rings or tri-operational (TO-) algebras.

In case of $\mathfrak{V}$ being the variety of lattices as in ch. 1, § 2.4, the k-dimensional $\mathfrak{V}$-composition algebras are called k-dimensional composition lattices. For $k = 1$, we simply speak of composition lattices.

1.4. Let A be any algebra, Ω its family of operations, k, l, positive integers, $F_k(A)$ and $F_l(A)$ the full function algebras, $\varphi \in F_k(A)$, and $(\psi_1, \ldots, \psi_k) \in F_l(A)^k$. We define the "composition" $\varphi \circ (\psi_1, \ldots, \psi_k) \in F_l(A)$ by

$$(\varphi \circ (\psi_1, \ldots, \psi_k))(a_1, \ldots, a_l) = \varphi(\psi_1(a_1, \ldots, a_l), \ldots, \psi_k(a_1, \ldots, a_l)),$$
$$(a_1, \ldots, a_l) \in A^l.$$

1.41. Lemma. *For any $(\psi_1, \ldots, \psi_k) \in F_l(A)^k$, the mapping $\varphi \to \varphi \circ (\psi_1, \ldots, \psi_k)$ is a homomorphism from $F_k(A)$ to $F_l(A)$.*

Proof. We have to show that $\omega_i \circ (\psi_1, \ldots, \psi_k) = \omega_i$, for $n_i = 0$, and $(\omega_i \varphi_1 \ldots \varphi_{n_i}) \circ (\psi_1, \ldots, \psi_k) = \omega_i[\varphi_1 \circ (\psi_1, \ldots, \psi_k)] \ldots [\varphi_{n_i} \circ (\psi_1, \ldots, \psi_k)]$, for $n_i > 0$. This is done by showing that these equations hold "pointwise" for any $(a_1, \ldots, a_l) \in A^l$.

1.42. Lemma. *Let $\varphi \in F_k(A)$, $(\psi_1, \ldots, \psi_k) \in F_l(A)^k$, and $(\chi_1, \ldots, \chi_l) \in F_m(A)^l$. Then $[\varphi \circ (\psi_1, \ldots, \psi_k)] \circ (\chi_1, \ldots, \chi_l) = \varphi \circ (\psi_1 \circ (\chi_1, \ldots, \chi_l), \ldots, \psi_k \circ (\chi_1, \ldots, \chi_l))$.*

Proof. Again, by showing "pointwise" equality.

1.43. Proposition. *Let A be an algebra of the variety $\mathfrak{V}$, Ω its family of operations, and $k \geqslant 1$ an integer. On $\langle F_k(A); \Omega \rangle$, we define a $(k+1)$-ary operation $\varkappa$ by $\varkappa \varphi_0 \varphi_1 \ldots \varphi_k = \varphi_0 \circ (\varphi_1, \ldots, \varphi_k)$. If $\Omega_1 = \{\Omega, \varkappa\}$, then $\langle F_k(A); \Omega_1 \rangle$ is a k-dimensional $\mathfrak{V}$-composition algebra with selector system.*

Proof. By ch. 1, Prop. 6.11, $\langle F_k(A); \Omega \rangle$ is an algebra of $\mathfrak{V}$. For $l = m = k$, Lemma 1.42 yields superassociativity for $\varkappa$ while Lemma 1.41 shows the right-superdistributivity with respect to any $\omega_i \in \Omega$. Moreover, the family $\xi_1, \ldots, \xi_k$ of the projections of $F_k(A)$ is a selector system for $\varkappa$.

1.5. In the preceding proposition, we have shown that every full function algebra $F_k(A)$ over an algebra A of the variety $\mathfrak{V}$ is a k-dimensional $\mathfrak{V}$-composition algebra if the composition of functions is added to the operations on $F_k(A)$. Since the class of k-dimensional $\mathfrak{V}$-composition

algebras is a variety, every subalgebra of this composition algebra is also a k-dimensional $\mathfrak{V}$-composition algebra. The subsequent theorem will show that, up to isomorphism, there are no further k-dimensional $\mathfrak{V}$-composition algebras, this means that for every $\mathfrak{V}$-composition algebra there exists an isomorphic algebra consisting of functions on an algebra of $\mathfrak{V}$ where the composition operation is just the composition of functions or, as we say, that every $\mathfrak{V}$-composition algebra can be faithfully represented by such an algebra of functions.

1.51. Theorem. *Let $A = \langle A; \Omega, \varkappa\rangle$ be a k-dimensional $\mathfrak{V}$-composition algebra. Then there exists an algebra D of $\mathfrak{V}$ such that A is isomorphic to some subalgebra of the k-dimensional $\mathfrak{V}$-composition algebra $\langle F_k(D); \Omega, \varkappa\rangle$ where $\varkappa$ is the composition of functions.*

Proof. The theorem holds for $|A| = 1$ since then $|F_k(A)| = 1$ and we may take $D = \langle A; \Omega\rangle$. Assume now that $|A| \neq 1$. Let D be any $\mathfrak{V}$-extension of $\langle A; \Omega\rangle$ different from $\langle A; \Omega\rangle$ such as $\langle F_1(A); \Omega\rangle$. Let $\vartheta : A \to F_k(D)$ be defined by

$$(\vartheta a)(d_1, \ldots, d_k) = \begin{cases} \varkappa a d_1 \ldots d_k, & \text{for} \quad d_i \in A, \quad i = 1, \ldots, k \\ a, & \text{otherwise.} \end{cases}$$

ϑ is certainly injective since there exists $(d_1, \ldots, d_k) \in D^k \smallsetminus A^k$, hence $(\vartheta a)(d_1, \ldots, d_k) = a$, and $(\vartheta b)(d_1, \ldots, d_k) = b$, $a, b \in A$. We have to show that ϑ is a homomorphism, i.e.

$$\vartheta\omega_i = \omega_i, \quad \text{for} \quad n_i = 0,$$
$$\vartheta\omega_i a_1 \ldots a_{n_i} = \omega_i \vartheta a_1 \ldots \vartheta a_{n_i}, \quad \text{for} \quad n_i > 0$$
$$\vartheta\varkappa a_0 \ldots a_k = \varkappa \vartheta a_0 \ldots \vartheta a_k$$

That these equations hold, can be easily verified, by substituting any $(d_1, \ldots, d_k) \in D^k$ into either side of the equations, and using right superdistributivity and superassociativity of $\varkappa$ for $\langle A; \Omega, \varkappa\rangle$.

1.52. The examples of 1.3 yield some remarkable special cases of Th. 1.51:

a) Every k-dimensional superassociative system can be faithfully represented by some superassociative system of k-place functions on a set. Every semigroup can be faithfully represented by some semigroup of 1-place functions on a set.

b) Every k-dimensional composition group can be faithfully represented by a composition group of k-place functions on a group. Every near-ring can be faithfully represented by some near-ring of 1-place functions on a group.

c) Every k-dimensional composition ring can be faithfully represented by some composition ring of k-place functions on a ring.

d) Every k-dimensional composition lattice can be faithfully represented by some composition lattice of k-place functions on a lattice.

2. Composition algebras of polynomials and polynomial functions

2.1. $\langle P_k(A); \Omega\rangle$ is, by definition, a subalgebra of $\langle F_k(A); \Omega\rangle$. Let $\pi_0, \ldots, \pi_k \in P_k(A)$. Since $P_k(A) = A(\xi_1, \ldots, \xi_k)$, we have $\pi_i = w_i(a_j, \xi_1, \ldots, \xi_k)$, $i = 0, 1, \ldots, k$. If $\varkappa$ denotes the composition of functions, then $\varkappa\pi_0 \ldots \pi_k = \pi_0 \circ (\pi_1, \ldots, \pi_k) = w_0(a_j, w_1(a_j, \xi_1, \ldots, \xi_k), \ldots, w_k(a_j, \xi_1, \ldots, \xi_k))$ for this equations holds "pointwise" for all elements of A^k. Thus $\varkappa\pi_0 \ldots \pi_k \in P_k(A)$. Hence we obtain from Prop. 1.43 and Prop. 1.21

2.11. Proposition. *Let A be an algebra of the variety $\mathfrak{V}$. The subset $P_k(A)$ of the composition algebra $\langle F_\kappa(A); \Omega, \varkappa\rangle$ is a subalgebra, i.e. $\langle P_k(A); \Omega, \varkappa\rangle$ is a k-dimensional $\mathfrak{V}$-composition algebra with selector system $\xi_1, \xi_2, \ldots, \xi_k$.*

2.12. Remark. In ch. 1, § 6.2, we have shown that, for any subfamily Φ of Ω, the algebra $\langle P_k(A_\Phi); \Phi\rangle$ is a subalgebra of $\langle P_k(A); \Phi\rangle$. Since $P_k(A_\Phi)$ is, by Prop. 2.11, a subalgebra of $\langle F_k(A); \Phi, \varkappa\rangle$, we conclude that $P_k(A_\Phi)$ is closed with respect to the composition of functions, thus $\langle P_k(A_\Phi); \Phi, \varkappa\rangle$ is also a subalgebra of $\langle P_k(A); \Phi, \varkappa\rangle$.

2.2. Let A be an algebra of the variety $\mathfrak{V}$, Ω its family of operations, $X = \{x_1, \ldots, x_k\}$, $Y = \{y_1, \ldots, y_l\}$, $Z = \{z_1, \ldots, z_m\}$ (not necessarily disjoint) sets of indeterminates, and $p = p(x_1, \ldots, x_k) \in A(X, \mathfrak{V})$, $(q_1, \ldots, q_k) \in A(Y, \mathfrak{V})^k$. We define a "composition" $p \circ (q_1, \ldots, q_k)$ by $p \circ (q_1, \ldots, q_k) = p(q_1, \ldots, q_k)$ which is, by ch. 1, Prop. 6.31, a well-defined element of $A(Y, \mathfrak{V})$. Restating this proposition for this particular situation, we get

2.21. Lemma. *If $(q_1, \ldots, q_k)$ is aoy fixed element of $A(Y, \mathfrak{V})^k$, then the mapping $p \to p \circ (q_1, \ldots, q_k)$ is a homomorphism from $A(X, \mathfrak{V})$ to $A(Y, \mathfrak{V})$.*

2.22. By the definition of $p(q_1, \ldots, q_k)$ (see ch. 1, Prop. 6.31), a representation of $p \circ (q_1, \ldots, q_k)$ as a word can be obtained if we take any representation $p = w(a_j, x_1, \ldots, x_k)$ for p and representations $q_i = v_i(a_j, y_1, \ldots, y_l)$ for q_i, $i = 1, \ldots, k$, as words. Then $p \circ (q_1, \ldots, q_k) = w(a_j, v_1(a_j, y_1, \ldots, y_l), \ldots, v_k(a_j, y_1, \ldots, y_l))$. Hence

2.23. Lemma. *Let $p \in A(X, \mathfrak{V})$, $(q_1, \ldots, q_k) \in A(Y, \mathfrak{V})^k$, and $(r_1, \ldots, r_l) \in A(Z, \mathfrak{V})^l$. Then $[p \circ (q_1, \ldots, q_k)] \circ (r_1, \ldots, r_l) = p \circ (q_1 \circ (r_1, \ldots, r_l), \ldots, q_k \circ (r_1, \ldots, r_l))$.*

2.24. Proposition. *Let A be an algebra of the variety $\mathfrak{V}$ and Ω its family of operations. For any integer $k \geqslant 1$, define a $(k+1)$-ary operation $\varkappa$ on $\langle A(x_1, \ldots, x_k, \mathfrak{V}); \Omega \rangle$ by $\varkappa p_0 p_1 \ldots p_k = p_0 \circ (p_1, \ldots, p_k) = p_0(p_1, \ldots, p_k)$, and let $\Omega_1 = \{\Omega, \varkappa\}$. Then the algebra $\langle A(x_1, \ldots, x_k, \mathfrak{V}); \Omega_1 \rangle$ is a k-dimensional $\mathfrak{V}$-composition algebra with selector system.*

Proof. $\langle A(x_1, \ldots, x_k, \mathfrak{V}); \Omega \rangle$ is an algebra of $\mathfrak{V}$. Lemma 2.23 applied to $X = Y = Z$ shows the superassociativity of $\varkappa$, Lemma 2.21 the right-superdistributivity of $\varkappa$ with respect to any $\omega_i \in \Omega$. It is easy to see that the family $x_1, \ldots, x_k$ is a selector system for $\varkappa$.

3. Composition homomorphisms

3.1. Let $\langle C; \Omega, \varkappa \rangle$ and $\langle D; \Omega, \varkappa \rangle$ be k-dimensional $\mathfrak{V}$-composition algebras. A homomorphism from $\langle C; \Omega \rangle$ to $\langle D; \Omega \rangle$ is called a composition homomorphism if it is also a homomorphism from $\langle C; \Omega, \varkappa \rangle$ to $\langle D; \Omega, \varkappa \rangle$. If a composition homomorphism is a monomorphism (epimorphism, isomorphism), then it is called a composition monomorphism (epimorphism, isomorphism).

Let $C = \langle C; \Omega, \varkappa \rangle$ be a k-dimensional $\mathfrak{V}$-composition algebra. An element $c \in C$ is called a constant of C if $\varkappa c c_1 \ldots c_k = c$, for all $(c_1, \ldots, c_k) \in C^k$. Examples for constants are the elements of A in the $\mathfrak{V}$-composition algebras $\langle A(X, \mathfrak{V}); \Omega, \varkappa \rangle$, $\langle F_k(A); \Omega, \varkappa \rangle$, and $\langle P_k(A); \Omega, \varkappa \rangle$.

3.11. Lemma. *Let $\vartheta : \langle C; \Omega, \varkappa \rangle = C \to \langle D; \Omega, \varkappa \rangle = D$ be an epimorphism of composition algebras. Then ϑ maps any constant of C onto a constant of D, and a selector system of C onto a selector system of D.*

Proof. Straightforward.

3.2. We know from § 2 that, for any algebra A in $\mathfrak{V}$, the $\mathfrak{V}$-polynomial algebra $A(x_1, \ldots, x_k, \mathfrak{V})$ together with the composition $\varkappa$ of polynomials is a k-dimensional $\mathfrak{V}$-composition algebra. We are now going to determine all composition epimorphisms of $A(x_1, \ldots, x_k, \mathfrak{V})$.

3.21. Theorem. *Let $A(x_1, \ldots, x_k, \mathfrak{V}) = A(X, \mathfrak{V})$ be any $\mathfrak{V}$-polynomial algebra, and $\langle C; \Omega, \varkappa \rangle$ a k-dimensional $\mathfrak{V}$-composition algebra such that*

a) *C has a selector system $s_1, s_2, \ldots, s_k$,*

b) *$\langle C; \Omega \rangle$ has a subalgebra B consisting of constants of $\langle C; \Omega, \varkappa \rangle$ such that $\langle C; \Omega \rangle = B(s_1, \ldots, s_k)$.*

Then every epimorphism $\eta : A \to B$ can be uniquely extended to a composition epimorphism $\varrho : A(X, \mathfrak{V}) \to \langle C; \Omega \rangle$. ϱ maps x_i onto s_i, $i = 1, \ldots, k$, and is called the composition extension of η. Every composition epimorphism of $A(X, \mathfrak{V})$ can be obtained in this way.

Proof. Let $\eta : A \to B$ be an epimorphism, then η can be considered as a homomorphism from A to $\langle C; \Omega \rangle$. Let $\psi : F(X, \mathfrak{V}) \to \langle C; \Omega \rangle$ be the extension of the mapping $x_i \to s_i$ to a homomorphism of the free algebra $F(X, \mathfrak{V})$. Since $A(X, \mathfrak{V})$, $\{\varphi_1, \varphi_2\}$ is, by ch. 1, § 4.3, a free union of the algebras A and $F(X, \mathfrak{V})$ in $\mathfrak{V}$, there exists a homomorphism $\varrho : A(X, \mathfrak{V}) \to \langle C; \Omega \rangle$ such that $\eta = \varrho\varphi_1$ and $\psi = \varrho\varphi_2$. By definition of φ_1, φ_2, $\varrho a = \eta a$, $a \in A$, and $\varrho x_i = s_i$, $i = 1, \ldots, k$. Since $\langle C; \Omega \rangle = B(s_1, \ldots, s_k)$, ϱ is an epimorphism. Next we show that ϱ is even a composition epimorphism. Let $w_0, \ldots, w_k \in A(X, \mathfrak{V})$ and $w_0 = w_0(a_j, x_1, \ldots, x_k)$ be a representation of w_0 as a word. Then $\varkappa w_0 \ldots w_k = w_0(a_j, w_1, \ldots, w_k)$ and hence $\varrho\varkappa w_0 \ldots w_k = w_0(\eta a_j, \varrho w_1, \ldots, \varrho w_k)$. On the other hand, $\varrho w_0 = w_0(\eta a_j, s_1, \ldots, s_k)$. Since $\varkappa$ is right-superdistributive, $\eta a_j \in B$, i.e. ηa_j is a constant of $\langle C; \Omega, \varkappa \rangle$, and $s_1, \ldots, s_k$ is a selector system of $\langle C; \Omega, \varkappa \rangle$, we conclude

$$\varkappa\varrho w_0 \varrho w_1 \ldots \varrho w_k = w_0(\varkappa(\eta a_j)\varrho w_1 \ldots \varrho w_k, \varkappa s_1 \varrho w_1 \ldots \varrho w_k, \ldots, \varkappa s_k \varrho w_1 \ldots \varrho w_k)$$
$$= w_0(\eta a_j, \varrho w_1, \ldots, \varrho w_k).$$

Thus ϱ is a composition epimorphism.

Let σ be any composition epimorphism from $A(X, \mathfrak{V})$ to $\langle C; \Omega\rangle$ extending η. By Lemma 3.11, $\sigma x_1, \ldots, \sigma x_k$ is a selector system of $\langle C; \Omega, \varkappa\rangle$ and hence, by Lemma 1.11, $\sigma x_i = s_i$, $i = 1, \ldots, k$. Thus σ and ϱ coincide on $A \cup X$ which generates $A(X, \mathfrak{V})$. This implies $\sigma = \varrho$.

Finally let $\sigma : A(X, \mathfrak{V}) \to C$ be any composition epimorphism of $A(X, \mathfrak{V})$. By Lemma 3.11, the k-dimensional $\mathfrak{V}$-composition algebra $\langle C; \Omega, \varkappa\rangle$ has the selector system $\sigma x_1, \ldots, \sigma x_k$, and the algebra $\langle C; \Omega\rangle$ has σA as a subalgebra consisting of constants of $\langle C; \Omega, \varkappa\rangle$. Since $A(X, \mathfrak{V}) = [A \cup X]$, we conclude that $\langle C; \Omega\rangle = (\sigma A)(\sigma x_1, \ldots, \sigma x_k)$. If η is the restriction of σ to A, then σ is just the unique extension of η to a composition epimorphism from $A(X, \mathfrak{V})$ to $\langle C; \Omega\rangle$.

3.22. Three important special cases of Th. 3.21 deserve to be mentioned. Here $X = \{x_1, \ldots, x_k\}$.

a) Let A be an algebra of the variety $\mathfrak{V}$ and $\eta : A \to B$ an epimorphism. Then η can be uniquely extended to a composition epimorphism $\varrho : A(X, \mathfrak{V}) \to B(X, \mathfrak{V})$ which will be denoted by $\eta(X, \mathfrak{V})$, $\eta[X]$ or $\eta(X)$. We have $\varrho x_i = x_i$, and hence ϱ is just the homomorphism of ch. 1, Prop. 4.5. Thus the notation $\varrho = \eta(X, \mathfrak{V}) = \eta(X)$ is compatible with ch. 1, Remark 4.51.

b) Let $\mathfrak{V}_1 \subseteq \mathfrak{V}_2$ be two varieties and A an algebra of $\mathfrak{V}_1$. Then there is a unique composition epimorphism from $A(X, \mathfrak{V}_2)$ to $A(X, \mathfrak{V}_1)$ fixing $A \cup X$ elementwise (see also ch. 1, Th. 5.22).

c) Let A be an algebra of the variety $\mathfrak{V}$. Then there exists a unique composition epimorphism from $A(X, \mathfrak{V})$ to $P_k(A)$ fixing A elementwise and mapping x_i to ξ_i, $i = 1, \ldots, k$. This is, by ch. 1, Prop. 6.41, just the canonical epimorphism σ. The dependence of σ on A, k, and $\mathfrak{V}$ will, if necessary, be expressed by $\sigma = \sigma(A) = \sigma(A, k) = \sigma(A, k, \mathfrak{V}) = \sigma(X, \mathfrak{V}) = \sigma(A, X, \mathfrak{V})$.

3.3. We are now going to consider the algebras of k-place polynomial functions as k-dimensional composition algebras, in the sense of § 2. In particular, we shall obtain a result analogous to § 3.22, a).

3.31. Proposition. *Let $k > 0$ be an integer, A an algebra, and $\eta : A \to B$ an epimorphism. Then η can be uniquely extended to a composition epimorphism $\varrho : P_k(A) \to P_k(B)$. ϱ fixes every ξ_i and is called the composition extension of η. If η is an isomorphism, so is ϱ.*

Proof. Let $p \in P_k(A)$ and $p = w(a_j, \xi_1, \ldots, \xi_k)$ a representation of p as a word. We define $\varrho p = w(\eta a_j, \xi_1, \ldots, \xi_k)$ then ϱp is a well defined element of $P_k(B)$. For, if $p = v(a_j, \xi_1, \ldots, \xi_k)$ is another representation of p as a word, then $w(a_j, c_1, \ldots, c_k) = v(a_j, c_1, \ldots, c_k)$, for all $(c_1, \ldots, c_k) \in A^k$. Then $w(\eta a_j, \eta c_1, \ldots, \eta c_k) = v(\eta a_j, \eta c_1, \ldots, \eta c_k)$ whence $w(\eta a_j, \xi_1, \ldots, \xi_k) = v(\eta a_j, \xi_1, \ldots, \xi_k)$ as η is surjective. ϱ is obviously surjective and extends η. Straightforward computation exhibits ϱ as a composition homomorphism. In order to establish the uniqueness of ϱ, we take any composition epimorphism $\sigma : P_k(A) \to P_k(B)$ extending η. Under σ, the selector system $\xi_1, \ldots, \xi_k$ of $P_k(A)$ is mapped onto a selector system of $P_k(B)$ whence, by Lemma 1.11, $\sigma\xi_i = \xi_i$, $i = 1, \ldots, k$. Since $P_k(A) = [A \cup \{\xi_1, \ldots, \xi_k\}]$, σ coincides with ϱ. Suppose now that η is an isomorphism. Then $\eta^{-1} : B \to A$ is an isomorphism, in particular, η^{-1} is an epimorphism and thus can be extended to a composition epimorphism $\tau : P_k(B) \to P_k(A)$. Hence $\tau\varrho$ and $\varrho\tau$ are extensions of identity mappings and, by uniqueness, are identity mappings themselves.

3.32. Remark. Let $\eta : A \to B$ be an epimorphism and $X = \{x_1, \ldots, x_k\}$. The unique extension ϱ of η to a composition epimorphism from $P_k(A)$ to $P_k(B)$ will be denoted by $P_k(\eta)$. The diagram fig. 3.1 is commutative.

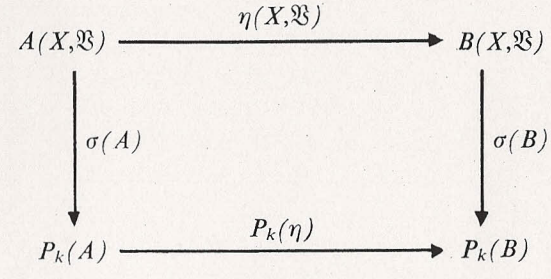


FIG. 3.1

3.4. Let R, S be algebras of the variety $\mathfrak{V}$ such that there is an additional operation $\varkappa$ on R, S making k-dimensional $\mathfrak{V}$-composition algebras of R, S. The direct product $R \times S$ by adding $\varkappa$ then also becomes a k-dimensional $\mathfrak{V}$-composition algebra, by Prop. 1.21 and ch. 1, Th. 2.51. In particular, if A, B are algebras of $\mathfrak{V}$ and $X = \{x_1, \ldots, x_k\}$, then $A(X, \mathfrak{V}) \times B(X, \mathfrak{V})$ and $P_k(A) \times P_k(B)$ are k-dimensional $\mathfrak{V}$-composition algebras.

3.41. Proposition. *Let $X = \{x_1, \ldots, x_k\}$, A, B algebras of $\mathfrak{V}$ and $U = A \times B$. Then there exists a unique composition homomorphism $\tau : U(X, \mathfrak{V}) \to A(X, \mathfrak{V}) \times B(X, \mathfrak{V})$ such that $\tau U(X, \mathfrak{V})$ is a subdirect product of $A(X, \mathfrak{V})$ and $B(X, \mathfrak{V})$ and τ fixes U elementwise. Similarly, there exists a unique composition homomorphism $\tau : P_k(U) \to P_k(A) \times P_k(B)$ such that $\tau P_k(U)$ is a subdirect product of $P_k(A)$ and $P_k(B)$ and τ fixes U elementwise. In either case, $\tau p = (\varrho_1 p, \varrho_2 p)$ where $\varrho_i = \pi_i(X)$ or $\varrho_i = P_k(\pi_i)$, respectively, $i = 1, 2$, and π_i are the projections of U.*

τ will be called the decomposition homomorphism of $U(X, \mathfrak{V})$ or $P_k(U)$, respectively.

Proof. We will prove just the first assertion, the second assertion can be shown by exactly the same argument. By straight forward calculation we see that τ as defined above has all the required properties. Therefore let σ be another composition homomorphism with these properties, and μ_i, $i = 1, 2$, the projections of the composition algebra $A(X, \mathfrak{V}) \times B(X, \mathfrak{V})$. Then $\mu_i \sigma$, $i = 1, 2$, is a composition extension of π_i, and hence, by Th. 3.21, $\mu_i \sigma = \pi_i(X)$, $i = 1, 2$. Since $\sigma p = (\mu_1 \sigma p, \mu_2 \sigma p)$, we conclude $\sigma = \tau$.

3.42. Remark. Let τ_1 be the decomposition homomorphism of $U(X, \mathfrak{V})$, τ_2 the decomposition homomorphism of $P_k(U)$, and $\sigma(A) \times \sigma(B) : A(X, \mathfrak{V}) \times B(X, \mathfrak{V}) \to P_k(A) \times P_k(B)$ the epimorphism defined by $(\sigma(A) \times \sigma(B))(p, q) = (\sigma(A)p, \sigma(B)q)$. Then diagram fig. 3.2 is commutative. This is an immediate consequence of the commutativity of diagram fig. 3.1.

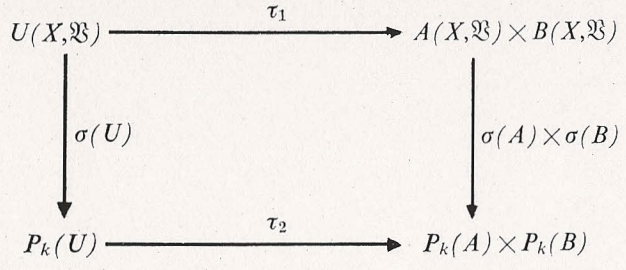


FIG. 3.2

3.5. We want to know under what circumstances the decomposition homomorphisms τ of $U(X, \mathfrak{V})$ and $P_k(U)$ are epimorphisms or monomorphisms. We start with the following

3.51. Proposition. *Let $X = \{x_1, \ldots, x_k\}$, and $U = A \times B$. The decomposition homomorphism τ of $U(X, \mathfrak{V})$ is an epimorphism if and only if, for any $(p, q) \in A(X, \mathfrak{V}) \times B(X, \mathfrak{V})$, there exists a word $w(y_1, \ldots, y_r, x_1, \ldots, x_k)$ in the indeterminates $y_1, \ldots, y_r$ and elements $a_1, \ldots, a_r \in A$, $b_1, \ldots, b_r \in B$ such that $w(a_1, \ldots, a_r, x_1, \ldots, x_k)$ is a representation of p and $w(b_1, \ldots, b_r, x_1, \ldots, x_k)$ is a representation of q. The decomposition homomorphism τ of $P_k(U)$ is an epimorphism if and only if, for any $(p, q) \in P_k(A) \times P_k(B)$, there exists a word $w(y_1, \ldots, y_r, \xi_1, \ldots, \xi_k)$ and elements $a_1, \ldots, a_r \in A$, $b_1, \ldots, b_r \in B$ with analogous properties.*

Proof. We prove the first assertion, the second one can be shown using exactly the same argument. Let τ be an epimorphism, then, for any $(p, q) \in A(X, \mathfrak{V}) \times B(X, \mathfrak{V})$, there exists an element $u \in U(X, \mathfrak{V})$ such that $\tau u = (p, q)$. Let $u = w(u_1, \ldots, u_r, x_1, \ldots, x_k)$ be any representation of u as a word. By Prop. 3.41, $\tau u = (\pi_1(X)u, \pi_2(X)u)$, π_i being the i-th projection of U, $i = 1, 2$. Hence $p = w(\pi_1 u_1, \ldots, \pi_1 u_r, x_1, \ldots, x_k)$ and $q = w(\pi_2 u_1, \ldots, \pi_2 u_r, x_1, \ldots, x_k)$, i.e. $w(y_1, \ldots, y_r, x_1, \ldots, x_k)$ is just a word we were looking for. Conversely, if $(p, q) \in A(X, \mathfrak{V}) \times B(X, \mathfrak{V})$ and $w(y_1, \ldots, y_r, x_1, \ldots, x_k)$ is a word such that $w(a_1, \ldots, a_r, x_1, \ldots, x_k) = p$ and $w(b_1, \ldots, b_r, x_1, \ldots, x_k) = q$, for some $a_1, \ldots, a_r \in A$, $b_1, \ldots, b_r \in B$, then $u = w((a_1, b_1), \ldots, (a_r, b_r), x_1, \ldots, x_k)$ is a polynomial in $U(X, \mathfrak{V})$ such that $\tau u = (p, q)$, thus τ is an epimorphism.

3.52. Remark. Diagram fig. 3.2 shows that the decomposition homomorphism τ_2 of $P_k(U)$ is an epimorphism if the decomposition homomorphism τ_1 of $U(X, \mathfrak{V})$ is an epimorphism.

3.53. Proposition. *For any algebra $U = A \times B$, the decomposition homomorphism τ of $P_k(U)$ is a monomorphism.*

Proof. Let $g \in P_k(U)$ and $((a_1, b_1), \ldots, (a_k, b_k)) \in U^k$. Then $g((a_1, b_1), \ldots, (a_k, b_k)) = ((P_k(\pi_1)g)(a_1, \ldots, a_k), (P_k(\pi_2)g)(b_1, \ldots, b_k))$. This is established by taking any representation of g as a word in elements of U and the projections ξ_i, $i = 1, \ldots, k$, or by applying τ. Suppose $\tau p = \tau q$, for some $p, q \in P_k(U)$. Then $P_k(\pi_i)p = P_k(\pi_i)q$, $i = 1, 2$, whence $p((a_1, b_1), \ldots, (a_k, b_k)) = q((a_1, b_1), \ldots, (a_k, b_k))$, for all $((a_1, b_1), \ldots, (a_k, b_k)) \in U^k$. Therefore $p = q$.

3.54. Remark. It is not known under what conditions the decomposition homomorphism τ of $U(X, \mathfrak{V})$ is a monomorphism.

3.6. As an application of the preceding results we prove:

3.61. Theorem. *Let $X = \{x_1, \ldots, x_k\}$, $\mathfrak{V}$ the variety of commutative rings with identity, and $U = A \times B$ an algebra of $\mathfrak{V}$. Then the decomposition homomorphisms $\tau_1 : U(X, \mathfrak{V}) \to A(X, \mathfrak{V}) \times B(X, \mathfrak{V})$ and $\tau_2 : P_k(U) \to P_k(A) \times P_k(B)$ are isomorphisms.*

Proof. Let $(p, q) \in A(X, \mathfrak{V}) \times B(X, \mathfrak{V})$. By ch. 1, Th. 8.21, there are representations of p, q as words of the form

$$p = \sum(a_\lambda \mathfrak{x}^\lambda \mid \lambda \in P_1), \quad q = \sum(b_\lambda \mathfrak{x}^\lambda \mid \lambda \in P_2)$$

Thus $\sum(y_\lambda \mathfrak{x}^\lambda \mid \lambda \in P_1 \cup P_2)$ is a word in the indeterminates y_λ satisfying the conditions of Prop. 3.51. Hence τ_1 is an epimorphism, and so is τ_2, by Remark 3.52. It remains to show that τ_1 is a monomorphism. Let $f, g \in U(X, \mathfrak{V})$ such that $\tau_1 f = \tau_1 g$. By ch. 1, Th. 8.21, there are representations of f, g as words of the form

$$f = \sum(u_\lambda \mathfrak{x}^\lambda \mid \lambda \in P), \quad g = \sum(v_\lambda \mathfrak{x}^\lambda \mid \lambda \in P)$$

We obtain normal forms for $\pi_i(X)f$ and $\pi_i(X)g$, $i = 1, 2$, if we remove those summands in the words $\sum((\pi_i u_\lambda)\mathfrak{x}^\lambda \mid \lambda \in P)$ and $\sum((\pi_i v_\lambda)\mathfrak{x}^\lambda \mid \lambda \in P)$ for which $\pi_i u_\lambda = 0$ and $\pi_i v_\lambda = 0$, respectively. Since $\tau f = \tau g$ implies $\pi_i(X)f = \pi_i(X)g$, $i = 1, 2$, we have $\pi_i u_\lambda = \pi_i v_\lambda$, for all $\lambda \in P$, hence $u_\lambda = v_\lambda$, for all $\lambda \in P$. Therefore $f = g$.

In ch. 5, we will show that, if $\mathfrak{V}$ is the variety of groups, the decomposition homomorphisms τ_1, τ_2 are, by no means, always isomorphisms.

4. Full congruences

4.1. Let $\langle A; \Omega, \varkappa \rangle$ be a k-dimensional $\mathfrak{V}$-composition algebra. The congruence Φ of $\langle A; \Omega \rangle$ is called a full congruence if Φ is also a congruence of $\langle A; \Omega, \varkappa \rangle$. Thus Φ is a full congruence if and only if $p_i \Phi q_i$, $i = 0, 1, \ldots, k$, implies $\varkappa p_0 p_1 \ldots p_k \Phi \varkappa q_0 q_1 \ldots q_k$.

Ch. 1, § 1.4 and Prop. 1.21 imply that, for any full congruence Φ on $\langle A; \Omega \rangle$, the factor algebra $\langle A; \Omega, \varkappa \rangle | \Phi$ is a k-dimensional $\mathfrak{V}$-composition algebra, and the canonical epimorphism from A to $A|\Phi$ is a composition epimorphism. Conversely, by ch. 1, Th. 1.51, for any composition epimorphism $\varphi : \langle A; \Omega \rangle \to \langle B; \Omega \rangle$, the kernel $\operatorname{Ker} \varphi = \Phi$ is a full congruence on $\langle A; \Omega \rangle$, and there is a composition isomorphism $\psi : B \to A|\Phi$ such that $\psi\varphi$ is the canonical epimorphism from A to $A|\Phi$. Thus we obtain, up to isomorphism, every homomorphic image of the composition algebra $\langle A; \Omega, \varkappa \rangle$ as a factor algebra of $\langle A; \Omega, \varkappa \rangle$ with respect to a suitable full congruence of $\langle A; \Omega \rangle$.

4.2. The definition of a full congruence applies, in particular, to the k-dimensional composition algebras $F_k(A)$, $P_k(A)$, and $A(X, \mathfrak{V})$ where $X = \{x_1, \ldots, x_k\}$. It has been shown that, for $k > 1$ and any A, the algebra $F_k(A)$ has just the trivial full congruences. This is also true for a large class of algebras if $k = 1$, but does not hold with full generality. By § 3.22 c), the canonical epimorphism $\sigma : A(X, \mathfrak{V}) \to P_k(A)$ is a composition epimorphism. The kernel $\Phi = \operatorname{Ker} \sigma$ is a full congruence on $A(X, \mathfrak{V})$. If $\psi : P_k(A) \to A(X, \mathfrak{V})|\Phi$ is the corresponding composition isomorphism, then ψ^{-1} yields a bijection from the set of full congruences on $A(X, \mathfrak{V})|\Phi$ to the set of those on $P_k(A)$. Thus the full congruences on $P_k(A)$ are completely determined by the full congruences on $A(X, \mathfrak{V})|\Phi$ which, in turn, are determined by the full congruences on $A(X, \mathfrak{V})$ containing Φ, by ch. 1, Th. 1.71. Therefore we restrict ourselves to the investigation of the full congruences on $A(X, \mathfrak{V})$.

4.3. Let $X = \{x_1, \ldots, x_k\}$ and A an algebra of $\mathfrak{V}$. First we give some characterization of the full congruences on $A(X, \mathfrak{V})$.

4.31. Lemma. *The congruence Φ on $A(X, \mathfrak{V})$ is a full congruence if and only if $p_0 \Phi q_0$ implies $(\varkappa p_0 p_1 \ldots p_k) \Phi (\varkappa q_0 p_1 \ldots p_k)$, for any $(p_1, \ldots, p_k) \in A(X, \mathfrak{V})^k$.*

Proof. The "only if" statement is obvious. Suppose now that Φ is a congruence satisfying the hypothesis, and $p_i \Phi q_i$, $i = 0, 1, \ldots, k$. By induction on the least minimal rank of the words representing p_0, $(\varkappa p_0 p_1 \ldots p_k) \Phi (\varkappa p_0 q_1 \ldots q_k)$, and by hypothesis, $(\varkappa p_0 q_1 \ldots q_k) \Phi (\varkappa q_0 q_1 \ldots q_k)$. Thus $(\varkappa p_0 p_1 \ldots p_k) \Phi (\varkappa q_0 q_1 \ldots q_k)$.

4.32. Now let Θ be a congruence on A and (Θ) the congruence on

$A(X, \mathfrak{V})$ generated by Θ, i.e. (Θ) is the set-theoretical intersection of all congruences on $A(X, \mathfrak{V})$ containing Θ.

4.33. Proposition. *For any congruence Θ on A, the congruence (Θ) is a full congruence on $A(X, \mathfrak{V})$.*

This proposition will be established if we prove the following

4.34. Lemma. *$p(\Theta)q$ holds if and only if there is a finite chain $p = r_0, r_1, \ldots, r_t = q$ of polynomials of $A(X, \mathfrak{V})$ such that, for any two adjacent polynomials r_i, r_{i+1}, we have $r_i = w_i(a_1, \ldots, a_m, x_1, \ldots, x_k)$, $r_{i+1} = w_i(b_1, \ldots, b_m, x_1, \ldots, x_k)$, where $w_i(y_1, \ldots, y_m, x_1, \ldots, x_k)$ is some word in indeterminates y_j, $j = 1, \ldots, m$, and where $a_j, b_j \in A$, $a_j \Theta b_j$, $j = 1, \ldots, m$.*

Proof. The existence of such chains between p and q is an equivalence relation Φ on $A(X, \mathfrak{V})$. Let ω be any n_i-ary operation and $p_k \Phi q_k$, $k = 1, \ldots, n_i$. For $k = 1, \ldots, n_i$, we take chains $p_k = r_{k0}, r_{k1}, \ldots, r_{kt_k} = q_k$ as described in the lemma. Then $\omega p_1 \ldots p_{n_i} = \omega r_{10} \ldots r_{n_i 0}$, $\omega r_{11} r_{20} \ldots r_{n_i 0}$, $\omega r_{12} r_{20} \ldots r_{n_i 0}$, $\ldots$, $\omega q_1 r_{20} \ldots r_{n_i 0}$, $\omega q_1 r_{21} \ldots r_{n_i 0}$, $\ldots$, $\omega q_1 q_2 \ldots q_{n_i}$ is again a chain of the type occurring in the lemma. Hence Φ is a congruence on $A(X, \mathfrak{V})$, and $a \Theta b$ implies $a \Phi b$, thus $\Phi \supseteq \Theta$ whence $\Phi \supseteq (\Theta)$. Conversely, if Ψ is a congruence on $A(X, \mathfrak{V})$ and $\Psi \supseteq \Theta$, then, for any two adjacent polynomials r_i, r_{i+1} of a chain as in the lemma, $r_i \Psi r_{i+1}$, thus $\Psi \supseteq \Phi$. Therefore $(\Theta) \supseteq \Phi$.

4.35. Proof of Proposition 4.33. We have to show that (Θ) satisfies the condition of Lemma 4.31. Let $p_0(\Theta)q_0$ and $(p_1, \ldots, p_k) \in A(X, \mathfrak{V})^k$. Then there exists a chain $p_0 = r_0, r_1, \ldots, r_t = q_0$ satisfying the conditions of Lemma 4.34. Moreover, $p_i = v_i(a_{i1}, \ldots, a_{in}, x_1, \ldots, x_k)$, $i = 1, \ldots, k$, for some words $v_i(y_{i1}, \ldots, y_{in}, x_1, \ldots, x_k)$ in the indeterminates y_{ij}, and $r_i = w_i(a_1, \ldots, a_m, x_1, \ldots, x_k)$, $i = 0, \ldots, t$, for some words w_i as in Lemma 4.34. Then $w_i(y_1, \ldots, y_m, v_1(y_{11}, \ldots, y_{1n}, x_1, \ldots, x_k), \ldots)$ is a word such that $r_i(p_1, \ldots, p_k) = w_i(a_1, \ldots, a_m, v_1(a_{11}, \ldots, a_{1n}, x_1, \ldots, x_k), \ldots)$ and $r_{i+1}(p_1, \ldots, p_k) = w_i(b_1, \ldots, b_m, v_1(a_{11}, \ldots, a_{1n}, x_1, \ldots, x_k), \ldots)$. Hence $p_0(p_1, \ldots, p_k) = r_0(p_1, \ldots, p_k), r_1(p_1, \ldots, p_k), \ldots, q_0(p_1, \ldots, p_k)$ is a chain satisfying the condition of Lemma 4.34, thus $p_0(p_1, \ldots, p_k)\,(\Theta)\,q_0(p_1, \ldots, p_k)$, i.e. (Θ) satisfies the condition of Lemma 4.31, and the proposition is proved.

4.36. Proposition. *Let Θ be a congruence on A. Then the binary relation $\{\Theta\}$ on $A(X, \mathfrak{V})$ defined by: $p\{\Theta\}q$ if and only if $p(a_1, \ldots, a_k)\,\Theta\, q(a_1, \ldots, a_k)$ for all $(a_1, \ldots, a_k) \in A^k$, is a full congruence on $A(X, \mathfrak{V})$.*

Proof. Let $\eta : A \to A|\Theta$ be the canonical epimorphism, and $\sigma(A|\Theta) : (A|\Theta)(X, \mathfrak{V}) \to P_k(A|\Theta)$ the canonical epimorphism. Then, by § 3.22 a) and c), $\sigma(A|\Theta)\,\eta(X)$ is a composition epimorphism. We have $\operatorname{Ker} \sigma(A|\Theta)\,\eta(X) = \{\Theta\}$, hence $\{\Theta\}$ is a full congruence.

4.37. Remark. If $\{\Theta_\nu \mid \nu \in I\}$ is a set of congruences on A and $\cap$ denotes the set-theoretical intersection, then

$$(\cap(\Theta_\nu \mid \nu \in I)) \subseteq \cap((\Theta_\nu) \mid \nu \in I) \quad \text{and} \quad \{\cap(\Theta_\nu \mid \nu \in I)\} = \cap(\{\Theta_\nu\} \mid \nu \in I).$$

Proof. Since $\cap(\Theta_\nu) \supseteq \cap\Theta_\nu$, the first formula holds. The second formula follows from the definition of $\{\cap\Theta_\nu\}$.

4.4. Theorem. *Let Φ be any full congruence on $A(X, \mathfrak{V})$. Then there exists exactly one congruence Θ on A such that $(\Theta) \subseteq \Phi \subseteq \{\Theta\}$.*

Θ will be called the enclosing congruence of Φ.

Proof. We put $\Theta = \Phi \cap (A \times A)$. Since A is a subalgebra of $A(X, \mathfrak{V})$, Θ is a congruence on A. $\Phi \supseteq \Theta$ implies $\Phi \supseteq (\Theta)$. If $p \Phi q$, then, for any $(a_1, \ldots, a_k) \in A^k$, $\varkappa p a_1 \ldots a_k \Phi \varkappa q a_1 \ldots a_k$ whence $p(a_1, \ldots, a_k)\,\Phi\, q(a_1, \ldots, a_k)$. Hence $p(a_1, \ldots, a_k)\,\Theta\, q(a_1, \ldots, a_k)$, for all $(a_1, \ldots, a_k) \in A^k$, thus $p\{\Theta\}q$. Therefore $\Phi \subseteq \{\Theta\}$.

Let Λ be an arbitrary congruence on A, then obviously $\{\Lambda\} \cap [A \times A] = \Lambda$. Since $\{\Lambda\} \supseteq \Lambda$, we conclude $\{\Lambda\} \supseteq (\Lambda)$ whence $\Lambda = \{\Lambda\} \cap [A \times A] \supseteq (\Lambda) \cap [A \times A] \supseteq \Lambda$. So we also have $(\Lambda) \cap [A \times A] = \Lambda$. If Θ_1 is a congruence on A such that $(\Theta_1) \subseteq \Phi \subseteq \{\Theta_1\}$, then $(\Theta_1) \cap [A \times A] \subseteq \Phi \cap [A \times A] \subseteq \{\Theta_1\} \cap [A \times A]$ which implies $\Theta_1 \subseteq \Theta \subseteq \Theta_1$, i.e. $\Theta = \Theta_1$, and the uniqueness assertion is proved.

4.5. Theorem. *The set $\mathfrak{F}$ of all full congruences on $A(X, \mathfrak{V})$ is a complete sublattice of the congruence lattice $\mathfrak{L}(A(X, \mathfrak{V}))$. If $\mathfrak{L}(A)$ is the congruence lattice of A, then $\sigma : \mathfrak{F} \to \mathfrak{L}(A)$ defined by $\sigma\Phi = \Phi \cap (A \times A)$ is a complete lattice epimorphism.*

Proof. The set $\mathfrak{F}$ of all full congruences on $A(X, \mathfrak{V})$ coincides with the set of all congruences on the algebra $\langle A(X, \mathfrak{V}); \Omega, \varkappa\rangle$. If M is any non-empty set of full congruences on $A(X, \mathfrak{V})$, then the greatest lower bound and the least upper bound of M in the congruence lattice of $\langle A(X, \mathfrak{V}); \Omega\rangle$ and of $\langle A(X, \mathfrak{V}); \Omega, \varkappa\rangle$ coincide, by construction (see ch. 1, § 1.6). Hence $\mathfrak{F}$ is a complete sublattice of $\mathfrak{L}(A(X, \mathfrak{V}))$.

Let $\Lambda \in \mathfrak{L}(A)$, then $\varrho(\Lambda) = (\Lambda) \cap (A \times A) = \Lambda$, hence σ is surjective. If $\{\Phi_i | i \in I\}$ is a subset of $\mathfrak{F}$ and Φ its greatest lower, Ψ its least upper bound, then

$$\sigma\Phi = \Phi \cap (A \times A) = \bigcap(\Phi_i | i \in I) \cap (A \times A)$$
$$= \bigcap(\Phi_i \cap (A \times A) | i \in I) = \bigcap(\sigma\Phi_i | i \in I).$$

Let Θ be the least upper bound of the set $\{\sigma\Phi_i | i \in I\}$ in $\mathfrak{L}(A)$, and $a(\sigma\Psi)b$. Since $\sigma\Psi \subseteq \Psi$, we have $a\Psi b$, therefore there are congruences $\Phi_{i_1}, \Phi_{i_2}, \ldots, \Phi_{i_r}$ and elements $a = p_0, p_1, \ldots, p_r = b$ of $A(X, \mathfrak{V})$ such that $p_{\nu-1}\Phi_{i_\nu}p_\nu$, $\nu = 1, 2, \ldots, r$. Let $(a_1, \ldots, a_k)$ be an arbitrary element of A^k, then

$$p_{\nu-1}(a_1, \ldots, a_k)\Phi_{i_\nu}p_\nu(a_1, \ldots, a_k).$$

Hence $p_{\nu-1}(a_1, \ldots, a_k)(\sigma\Phi_{i_\nu})p_\nu(a_1, \ldots, a_k)$, $\nu = 1, \ldots, r$, whence $a\Theta b$. Conversely, if $a\Theta b$, then there are congruences $\sigma\Phi_{i_1}, \ldots, \sigma\Phi_{i_r}$ and elements $a = c_0, c_1, \ldots, c_r = b$ of A such that $c_{\nu-1}(\sigma\Phi_{i_\nu})c_\nu$, $\nu = 1, \ldots, r$, hence $c_{\nu-1}\Phi_{i_\nu}c_\nu$, and thus $a\Psi b$. Therefore $a(\sigma\Psi)b$, and we conclude $\sigma\Psi = \Theta$.

4.6. Let Θ be any congruence on A. Then, by definition of the enclosing congruence, the set of all full congruences on $A(X, \mathfrak{V})$ with Θ as their enclosing congruence constitutes a complete sublattice $\mathfrak{F}(A(X, \mathfrak{V}), \Theta)$ of the lattice of all full congruences on $A(X, \mathfrak{V})$. We will now investigate this lattice more closely.

4.61. Proposition. *Let Θ be any congruence on A and $\vartheta: A \to A|\Theta$ the canonical epimorphism. Then $\vartheta(X)$ induces a lattice isomorphism from $\mathfrak{F}(A(X, \mathfrak{V}), \Theta)$ to $\mathfrak{F}((A|\Theta)(X, \mathfrak{V}), 0)$ where 0 denotes the congruence whose classes consist of a single element.*

Proof. By ch. 1, Th. 1.71, the canonical epimorphism $\zeta: \langle A(X, \mathfrak{V}); \Omega, \varkappa\rangle \to \langle A(X, \mathfrak{V}); \Omega, \varkappa\rangle|(\Theta)$ induces a lattice isomorphism from $\mathfrak{L}((\Theta))$—the lattice of all full congruences Φ on $A(X, \mathfrak{V})$ containing (Θ)—to the

congruence lattice of $\langle A(X, \mathfrak{V}); \Omega, \varkappa\rangle|(\Theta)$. For any $\Phi \in \mathfrak{L}((\Theta))$, we have $\zeta(\Phi \cap (A \times A)) \subseteq \zeta\Phi \cap (\zeta A \times \zeta A)$, and conversely let $c \in \zeta\Phi \cap (\zeta A \times \zeta A)$. Then $c = (\zeta a, \zeta b)$, $a, b \in A$, and there exist elements $p, q \in A(X, \mathfrak{V})$ such that $p\Phi q$ and $\zeta p = \zeta a$, $\zeta q = \zeta b$, whence $p(\Theta)a$ and $q(\Theta)b$. Let $(a_1, \ldots, a_k) \in A^k$, then, since both (Θ) and Φ are full congruences, we have $p(a_1, \ldots, a_k)(\Theta)a$, $q(a_1, \ldots, a_k)(\Theta)b$, and $p(a_1, \ldots, a_k)\Phi q(a_1, \ldots, a_k)$. Thus $\zeta a = \zeta p(a_1, \ldots, a_k)$, $\zeta b = \zeta q(a_1, \ldots, a_k)$, and $(p(a_1, \ldots, a_k), q(a_1, \ldots, a_k)) \in \Phi \cap (A \times A)$. Hence $\zeta\Phi \cap (\zeta A \times \zeta A) \subseteq \zeta(\Phi \cap (A \times A))$ and thus $\zeta\Phi \cap (\zeta A \times \zeta A) = \zeta(\Phi \cap (A \times A))$. Thus $\zeta\Phi \cap (\zeta A \times \zeta A) = 0$ if and only if $\Phi \cap (A \times A) = \Theta$. We conclude that ζ induces a lattice isomorphism from $\mathfrak{F}(A(X, \mathfrak{V}), \Theta)$ to the lattice $\mathfrak{L}$ of all congruences Ψ on $\langle A(X, \mathfrak{V}); \Omega, \varkappa\rangle|(\Theta)$ satisfying $\Psi \cap (\zeta A \times \zeta A) = 0$.

By Lemma 3.11, the k-dimensional $\mathfrak{V}$-composition algebra $\langle A(X, \mathfrak{V}); \Omega, \varkappa\rangle|(\Theta)$ has the selector system $\zeta x_1 = s_1, \ldots, \zeta x_k = s_k$, and ζA is a subalgebra of $\langle A(X, \mathfrak{V}); \Omega\rangle|(\Theta)$ consisting of constants such that $\langle A(X, \mathfrak{V}); \Omega\rangle|(\Theta) = (\zeta A)(s_1, \ldots, s_k)$. Let $C(a)$ be the congruence class of a under Θ, then $(\Theta) \cap (A \times A) = \Theta$ implies that the mapping $C(a) \to \zeta a$ is an isomorphism η from $A|\Theta$ to ζA. Let σ be the composition extension of η, according to Th. 3.21, then $\sigma: (A|\Theta)(X, \mathfrak{V}) \to \langle A(X, \mathfrak{V}); \Omega\rangle|(\Theta)$ is a composition epimorphism. Let $p, q \in (A|\Theta)(X, \mathfrak{V})$, and $\sigma p = \sigma q$. Then there are representations $p = w(C(a_i), x_1, \ldots, x_k)$, $q = v(C(a_i), x_1, \ldots, x_k)$ of p, q as words, and $w(\zeta a_i, s_1, \ldots, s_k) = v(\zeta a_i, s_1, \ldots, s_k)$. Thus $w(a_i, x_1, \ldots, x_k)(\Theta)v(a_i, x_1, \ldots, x_k)$. By Lemma 4.34, there exists a finite chain $r_0, r_1, \ldots, r_t$ of polynomials of $A(X, \mathfrak{V})$ such that $w(a_i, x_1, \ldots, x_k) = r_0$, $v(a_i, x_1, \ldots, x_k) = r_t$ and $\varrho r_i = \varrho r_{i+1}$ where $\varrho = \vartheta(X)$. Hence $p = \varrho r_0 = \varrho r_t = q$ and σ is an isomorphism. The composition isomorphism $\sigma^{-1}: \langle A(X, \mathfrak{V}); \Omega\rangle|(\Theta) \to (A|\Theta)(X, \mathfrak{V})$ induces a lattice isomorphism from the congruence lattice of $\langle A(X, \mathfrak{V}); \Omega, \varkappa\rangle|(\Theta)$ to the lattice of full congruences of $(A|\Theta)(X, \mathfrak{V})$ mapping $\mathfrak{L}$ onto $\mathfrak{F}((A|\Theta)(X, \mathfrak{V}), 0)$. Since $\sigma^{-1}\zeta$ is a composition epimorphism from $A(X, \mathfrak{V})$ to $(A|\Theta)(X, \mathfrak{V})$ extending ϑ, we have $\sigma^{-1}\zeta = \varrho$ and the proposition is proved.

5. Full ideals over multioperator groups

5.1. Let $G = \langle G; +, -, 0, \Omega\rangle$ be an Ω-multioperator group. Since, by ch. 6, § 3, the class of Ω-multioperator groups is a variety, the algebras $F_k(G)$ and $P_k(G)$ are also Ω-multioperator groups. If G is an algebra of

the variety $\mathfrak{V}$ which is contained in the variety of Ω-multioperator groups, then $G(X, \mathfrak{V})$ is also an Ω-multioperator group.

5.11. Proposition. *Let $\mathfrak{V}$ be the variety of Ω-multioperator groups and $G = \langle G; +, -, 0, \Omega, \varkappa\rangle$ a k-dimensional $\mathfrak{V}$-composition algebra. Then G is an $\{\Omega, \varkappa\}$-multioperator group.*

Proof. We have only to show that $\varkappa 00 \dots 0 = 0$. But $\varkappa 0 g_1 \dots g_k = \varkappa(0+0)g_1 \dots g_k = \varkappa 0 g_1 \dots g_k + \varkappa 0 g_1 \dots g_k$, by the right-superdistributivity of $\varkappa$, hence $\varkappa 0 g_1 \dots g_k = 0$, for any $(g_1, \dots, g_k) \in G^k$. This proves the proposition and moreover shows, that 0 is a constant of G.

5.12. As a special case of Prop. 5.11, we get that, if G is any Ω-multioperator group, then $F_k(G)$ and $P_k(G)$ are $\{\Omega, \varkappa\}$-multioperator groups, and if $X = \{x_1, \dots, x_k\}$, $G \in \mathfrak{V}$, and $\mathfrak{V}$ is a variety of Ω-multioperator groups, then the composition algebra $G(X, \mathfrak{V})$ is an $\{\Omega, \varkappa\}$-multioperator group.

5.2. Let $\mathfrak{V}$ be the variety of Ω-multioperator groups and $\langle G; +, -, 0, \Omega, \varkappa\rangle$ any k-dimensional $\mathfrak{V}$-composition algebra. Then $G = \langle G; +, -, 0, \Omega\rangle$ is an Ω-multioperator group and $G_1 = \langle G; +, -, 0, \Omega, \varkappa\rangle$ is an $\{\Omega, \varkappa\}$-multioperator group. An ideal A of G is called a full ideal if A is also an ideal of G_1. Thus, by ch. 6, § 3, an ideal A of G is a full ideal if and only if $\varkappa g_0 g_1 \dots g_{\nu-1}(g_\nu + a)g_{\nu+1} \dots g_k - \varkappa g_0 g_1 \dots g_\nu \dots g_k \in A$, for all $a \in A$, and for all $(g_0, g_1, \dots, g_k) \in G^{k+1}$, $\nu = 0, 1, \dots, k$.

Let Φ be a congruence on G and $\ker \Phi$ the kernel of Φ. As shown in ch. 6, § 3, ker is a lattice isomorphism from the congruence lattice $\mathfrak{L}(G)$ to the ideal lattice $\mathfrak{R}(G)$. By definition, ker maps the set of all full congruences on G onto the set of all full ideals of G. Thus the ideal A of G is a full ideal if and only if $\ker^{-1} A$ is a full congruence. This correspondence enables us to derive a theorem on full ideals from every theorem on full congruences. Hence the results of § 4 can be stated in terms of full ideals of $G(X, \mathfrak{V})$.

5.3. Let $X = \{x_1, \dots, x_k\}$, G any algebra of $\mathfrak{V}$, a variety of Ω-multioperator groups. The full ideals of $G(X, \mathfrak{V})$ will be investigated.

5.31. Lemma. *An ideal A of $G(X, \mathfrak{V})$ is a full ideal if and only if $a \in A$ implies $\varkappa a p_1 \dots p_k \in A$, for any $(p_1, \dots, p_k) \in G(X, \mathfrak{V})^k$.*

Proof. Put $\Phi = \ker^{-1} A$, then $a \in A$ is equivalent to saying $a \Phi 0$. Let A be a full ideal, then Φ is a full congruence, hence, by Lemma 4.31, $a \in A$ implies $\varkappa a p_1 \dots p_k \Phi \varkappa 0 p_1 \dots p_k = 0$ since 0 is a constant of $G(X, \mathfrak{V})$. Hence $\varkappa a p_1 \dots p_k \in A$. Conversely, let $a \in A$ imply $\varkappa a p_1 \dots p_k \in A$, for any $(p_1, \dots, p_k) \in G(X, \mathfrak{V})^k$. Let $p_0 \Phi q_0$, then $(p_0 - q_0)\Phi 0$. We conclude $\varkappa(p_0 - q_0) p_1 \dots p_k \in A$, and right-superdistributivity of $\varkappa$ implies $\varkappa p_0 p_1 \dots p_k \Phi \varkappa q_0 p_1 \dots p_k$. Hence Φ is, by Lemma 4.31, a full congruence and A is a full ideal.

5.32. Let D be any ideal of G, and (D) the ideal of $G(X, \mathfrak{V})$ generated by D, i.e. (D) is the set-theoretical intersection of all ideals A of $G(X, \mathfrak{V})$ containing D.

5.33. Proposition. $(D) = \ker(\ker^{-1} D)$, *thus* (D) *is a full ideal.*

Proof. Set $B = \ker(\ker^{-1} D)$. If $a \in D$, then $a(\ker^{-1} D)0$, i.e. $a \in B$. Hence $(D) \subseteq B$. Let A be any ideal of $G(X, \mathfrak{V})$ such that $D \subseteq A$. If $a \ker^{-1} D\, b$, then $a \ker^{-1} A\, b$ whence $\ker^{-1} A$ is a congruence on $G(X, \mathfrak{V})$ containing $\ker^{-1} D$. Therefore $\ker^{-1} A \supseteq (\ker^{-1} D)$, and we conclude $A \supseteq B$ and so $(D) \supseteq B$. By Prop. 4.33, $(\ker^{-1} D)$ is a full congruence on $G(X, \mathfrak{V})$.

5.34. Let D be any ideal of G. Then $\{D\}$ will denote the set of all $p \in G(X, \mathfrak{V})$ such that $p(g_1, \dots, g_k) \in D$, for all $(g_1, \dots, g_k) \in G^k$.

5.35. Proposition. $\{D\} = \ker\{\ker^{-1} D\}$, *in particular,* $\{D\}$ *is a full ideal.*

Proof. Since 0 is a constant of $G(X, \mathfrak{V})$, we have $p \in \ker\{\ker^{-1} D\}$ if and only if $p(g_1, \dots, g_k) \in D$, for all $(g_1, \dots, g_k) \in G^k$, and, by Prop. 4.36, $\{\ker^{-1} D\}$ is a full congruence.

5.36. The full ideal $\{D\}$ is called the residue polynomial ideal of $G(X, \mathfrak{V})$ generated by D.

By Remark 4.37, Prop. 5.33, and Prop. 5.35, we get

$$\big(\bigcap(D_\nu \mid \nu \in I)\big) \subseteq \bigcap\big((D_\nu) \mid \nu \in I\big), \quad \text{and} \quad \{\bigcap(D_\nu \mid \nu \in I)\} = \bigcap(\{D_\nu\} \mid \nu \in I),$$

for any set $\{D_\nu \mid \nu \in I\}$ of ideals of G.

5.4. Theorem. *Let A be any full ideal of $G(X, \mathfrak{V})$. Then there exists a unique ideal D of G, the so-called enclosing ideal of A, such that $(D) \subseteq A \subseteq \{D\}$. We have $D = A \cap G$.*

Proof. Let Θ be the enclosing congruence of $\ker^{-1} A$ and $D = \ker \Theta$. Then $(\Theta) \subseteq \ker^{-1} A \subseteq \{\Theta\}$, hence $\ker(\ker^{-1} D) \subseteq A \subseteq \ker\{\ker^{-1} D\}$. This implies $(D) \subseteq A \subseteq \{D\}$. Let C be any ideal of G such that $(C) \subseteq A \subseteq \{C\}$, then $\ker^{-1}(C) \subseteq \ker^{-1} A \subseteq \ker^{-1}\{C\}$ whence $(\ker^{-1} C) \subseteq \ker^{-1} A \subseteq \{\ker^{-1} C\}$. By Th. 4.4, $\ker^{-1} C = \ker^{-1} D$, thus $C = D$. Moreover, $\Theta = (\ker^{-1} A) \cap (G \times G)$ implies $D = \ker \Theta = A \cap G$.

5.5. Theorem. *The set of all full ideals of $G(X, \mathfrak{V})$ constitutes a complete sublattice $\mathfrak{E}$ of the ideal lattice $\mathfrak{R}(G(X, \mathfrak{V}))$ of $G(X, \mathfrak{V})$. The mapping τ which assigns to each full ideal its enclosing ideal is a complete lattice epimorphism from $\mathfrak{E}$ to the ideal lattice $\mathfrak{R}(G)$ of G.*

Proof. This boils down to rewriting Th. 4.5 in terms of ideals, in the sense of § 5.2.

5.51. Corollary. *The intersection and the sum of any set of ideals of $\mathfrak{R}(G(X, \mathfrak{V}))$ where each ideal is a full ideal is again a full ideal.*

5.6. Next we are going to state Prop. 4.61 in terms of ideals. We remark that, by definition of enclosing ideals, the set of all full ideals of $G(X, \mathfrak{V})$ with the enclosing ideal D constitutes a complete sublattice $\mathfrak{E}(G(X, \mathfrak{V}), D)$ of the lattice $\mathfrak{E}$ of all full ideals of $G(X, \mathfrak{V})$.

5.61. Proposition. *Let D be any ideal of G and $\vartheta : G \to G|D$ the canonical epimorphism. Then the composition extension $\vartheta(X)$ of ϑ induces a lattice isomorphism from $\mathfrak{E}(G(X, \mathfrak{V}), D)$ to $\mathfrak{E}((G|D)(X, \mathfrak{V}), 0)$, 0 meaning the zero-ideal of $G|D$.*

Proof. It suffices to prove that, for every $A \in \mathfrak{E}(G(X, \mathfrak{V}), D)$, $\vartheta(X)A = (\ker)\vartheta(X)(\ker^{-1})A$. Then Prop. 4.61 will yield the proposition. But $b \in (\ker)\vartheta(X)(\ker^{-1})A$ implies $(b, 0) \in \vartheta(X)(\ker^{-1})A$, hence there exist elements $c, d \in G(X, \mathfrak{V})$ such that $\vartheta(X)c = b$, $\vartheta(X)d = 0$, and $c(\ker^{-1} A)d$. Therefore $c - d \in A$, and we have $b = \vartheta(X)(c-d) \in \vartheta(X)A$. Conversely, if $b \in \vartheta(X)A$, then we easily get $b \in (\ker)\vartheta(X)(\ker^{-1})A$.

6. Full ideals over commutative rings with identity

6.1. Let $\mathfrak{V}$ be the variety of commutative rings with identity regarded as algebras with the family $\{+, -, 0, \cdot, 1\}$ of operations. $\mathfrak{V}$ is a variety of Ω-multioperator groups where $\Omega = \{\cdot, 1\}$. Thus, for any $R \in \mathfrak{V}$, we may consider the full ideals of the Ω-multioperator group $R(x_1, \ldots, x_k, \mathfrak{V}) = R[x_1, \ldots, x_k]$, and we are ready to apply the results of §§ 5.3 to 5.6 to this particular case. So the intersection and the sum of ideals of $R[x_1, \ldots, x_k]$ which are full ideals are again full ideals, and the mapping τ which assigns to each full ideal its enclosing ideal is an epimorphism with respect to intersection and sum.

There is a third operation on the ideals of a ring, namely the product of two ideals for which we prove the following

6.11. Theorem. *Let U, V be full ideals of $R[x_1, \ldots, x_k]$. Then the ideal product UV is also a full ideal, and the mapping τ under which every full ideal is mapped onto its enclosing ideal, is an epimorphism with respect to forming ideal products.*

Proof. Let $w \in UV$, then $w = \sum_{i=1}^{n} u_i v_i$, $u_i \in U$, $v_i \in V$, $i = 1, \ldots, n$, for some n. Right-superdistributivity of $\varkappa$ and Lemma 5.31 imply, that, for $p_1, \ldots, p_k \in R[x_1, \ldots, x_k]$, $\varkappa w p_1 \ldots p_k = \sum_{i=1}^{n} \bar{u}_i \bar{v}_i$, $\bar{u}_i \in U$, $\bar{v}_i \in V$, $i = 1, \ldots, n$. Hence $\varkappa w p_1 \ldots p_k \in UV$ whence, by Lemma 5.31, UV is a full ideal. Since $\tau U \subseteq U$, $\tau V \subseteq V$, we have $(\tau U)(\tau V) \subseteq UV$ and therefore $((\tau U)(\tau V)) \subseteq UV$. If $w \in UV$, then $w = \sum_{i=1}^{n} u_i v_i$, $u_i \in U$, $v_i \in V$, $i = 1, \ldots, n$. Hence $w(r_1, \ldots, r_k) \in (\tau U)(\tau V)$, for all $(r_1, \ldots, r_k) \in R^k$ implying that $UV \subseteq \{(\tau U)(\tau V)\}$. Therefore $\tau(UV) = (\tau U)(\tau V)$.

6.12. Remark. If A, B are ideals of R, then $(AB) = (A)(B)$ and $\{AB\} \supseteq \{A\}\{B\}$. This will follow from

6.13. Lemma. *If C is any ideal of R, then the ideal (C) of $R[x_1, \ldots, x_k]$ consists of all polynomials of $R[x_1, \ldots, x_k]$ which have a normal form $\sum(a_\lambda \mathfrak{x}^\lambda \mid \lambda \in P)$ as in ch. 1, Th. 8.21, such that $a_\lambda \in C$, for all $\lambda \in P$.*

Proof. Let $C_1 = \{\sum(a_\lambda x^\lambda \mid \lambda \in P) \mid a_\lambda \in C, \text{ for all } \lambda \in P\}$. Certainly $C_1 \subseteq (C)$. Conversely, since $C \subseteq C_1$ and C_1 is an ideal of $R[x_1, \ldots, x_k]$, we also have $(C) \subseteq C_1$.

6.14. Lemma 6.13 implies that $(A)(B) \subseteq (AB)$, moreover $AB \subseteq (A)(B)$, hence $(AB) \subseteq (A)(B)$. By definition of $\{A\}$, $\{B\}$, and the ideal product, we get immediately $\{A\}\{B\} \subseteq \{AB\}$, and Remark 6.12 is proved.

A partial converse of Th. 6.11 can be proved:

6.15. Proposition. *Let W be any full ideal of $R[x_1, \ldots, x_k]$ such that the enclosing ideal C of W is the ideal product of some comaximal ideals A and B, i.e. $A+B = R$. Then $W = UV$ where U is a full ideal with enclosing ideal A and V is a full ideal with enclosing ideal B.*

Proof. We put $U = W+(A)$ and $V = W+(B)$. Then, by Cor. 5.51, U and V are full ideals, and, by Th. 5.5, U has the enclosing ideal $AB+A = A$ whereas V has the enclosing ideal $AB+B = B$. Moreover, $UV = WW+W(A)+W(B)+(A)(B) \subseteq W+(A)(B) = W+(C) = W$, by Remark 6.12. On the other hand, $U+V \supseteq A+B = R$ whence $U+V = R[x_1, \ldots, x_k]$. Hence $UV = U \cap V \supseteq W$ (see ch. 6, § 4.3).

6.2. Rings of polynomials over a commutative ring with identity possess some further operations which crop up in a fairly natural way, namely the partial derivations $\partial/\partial x_i = \partial_i$, $i = 1, \ldots, k$, of $R[x_1, \ldots, x_k]$. They can be used for constructing new full ideals from given full ideals.

6.21. Theorem. *Let V be any full ideal of $R[x_1, \ldots, x_k]$ and A its enclosing ideal. Then $V' = \{f \in R[x_1, \ldots, x_k] \mid f \in V, \partial_i f \in V, i = 1, \ldots, k\}$ is also a full ideal of $R[x_1, \ldots, x_k]$, A its enclosing ideal, and $V' \subseteq V$.*

V' is called the derivative of V.

Proof. V' is not empty since $0 \in V'$. Let $f, g \in V'$, then $f, g \in V$ and $\partial_i f, \partial_i g \in V$, $i = 1, \ldots, k$. Hence $f-g \in V$, $\partial_i(f-g) = \partial_i f - \partial_i g \in V$ implying that $f-g \in V'$. If $h \in R[x_1, \ldots, x_k]$, then $fh \in V$ and $\partial_i(fh) = (\partial_i f)h + f(\partial_i h) \in V$ whence $fh \in V'$. Thus V' is an ideal of $R[x_1, \ldots, x_k]$. Let $p_j \in R[x_1, \ldots, x_k]$, $j = 1, \ldots, k$, then, by Lemma 5.31, $\varkappa f p_1 \ldots p_k \in V$. Applying the chain rule for partial derivations, we get $\partial_i \varkappa f p_1 \ldots p_k = \sum_{\nu=1}^{k} [\varkappa(\partial_\nu f) p_1 \ldots p_k] \partial_i p_\nu \in V$, by Lemma 5.31. Thus $\varkappa f p_1 \ldots p_k \in V'$

so that, again by Lemma 5.31, V' is a full ideal. Clearly $V' \subseteq V$, in particular, $V' \subseteq \{A\}$. Also $A \subseteq V'$, hence $(A) \subseteq V'$ since V' is an ideal. This proves the proposition.

6.22. Lemma. *Let U, V be full ideals of $R[x_1, \ldots, x_k]$ such that $U \subseteq V$. Then $U' \subseteq V'$. If $\{V_\nu \mid \nu \in I\}$ is a set of full ideals and $D = \bigcap(V_\nu \mid \nu \in I)$, then $D' = \bigcap(V_\nu' \mid \nu \in I)$.*

Proof. The first assertion is obvious. As a consequence, $D' \subseteq \bigcap(V_\nu' \mid \nu \in I)$. Conversely, let $f \in \bigcap(V_\nu' \mid \nu \in I)$, then $f \in V_\nu$ and $\partial_i f \in V_\nu$, $\nu \in I$. Therefore $f \in D$, $\partial_i f \in D$ whence $f \in D'$.

6.23. For any full ideal V of $R[x_1, \ldots, x_k]$, we can now define $V^{(0)} = V$, $V^{(n)} = (V^{(n-1)})'$, $n = 1, 2, \ldots$. By Th. 6.21, every $V^{(n)}$ is a full ideal.

6.24. Proposition. *$V^{(n)}$ consists of all polynomials $f \in R[x_1, \ldots, x_k]$ such that the partial derivatives of the orders $k = 0, 1, \ldots, n$ of f are contained in V where a partial derivative of f of order 0 means f itself.*

Proof. By induction on n, using the definition of $V^{(n)}$.

6.25. Corollary. *Let V^n be the ideal product of n copies of V where V is a full ideal and $n \geqslant 1$ an integer. Then $V^n \subseteq V^{(n-1)}$.*

Proof. Let $f \in V^n$. Then f is a sum of elements $v_1 v_2 \ldots v_n, v_\nu \in V$. Applying sum and product rule for partial derivatives, we find that the partial derivatives of the orders $k \leqslant n-1$ of f are contained in V. Thus $V^n \subseteq V^{(n-1)}$.

6.3. Definition. A full ideal V of $R[x_1, \ldots, x_k]$ is called a D-full ideal if $V' = V$.

6.31. We want to characterize the D-full ideals of $R[x_1, \ldots, x_k] = S$. For this purpose, we consider the algebra $S = \langle S; +, -, 0, \cdot, 1, \varkappa, \partial_1, \ldots, \partial_k \rangle$. Setting $\Omega_1 = \{\cdot, 1, \varkappa, \partial_1, \ldots, \partial_k\}$, S becomes an Ω_1-multioperator group. Because of § 5.12, this is a consequence of $\partial_i 0 = 0$, $i = 1, \ldots, k$.

6.32. Theorem. *The ideals of the Ω_1-multioperator group S coincide with the D-full ideals of $R[x_1, \ldots, x_k]$.*

Proof. By ch. 6, Lemma 3.4, a subset V of S is an ideal of S if and only if it is a full ideal of $R[x_1, \ldots, x_k]$ and $\partial_i(g+a)-\partial_i g \in V$, for all $a \in V$, $g \in R[x_1, \ldots, x_k]$, $1 \leqslant i \leqslant k$. This is equivalent to saying that V is a full ideal and $\partial_i a \in V$, for all $a \in V$, i.e. V is a D-full ideal of $R[x_1, \ldots, x_k]$.

6.33. Corollary. *The intersection and the sum of a set of ideals of $R[x_1, \ldots, x_k]$ which are D-full ideals are also D-full ideals. The ideal product of any two D-full ideals is also a D-full ideal.*

Proof. The first assertion follows from Th. 6.32, and ch. 6, § 3.2. If U, V are D-full ideals and $p \in UV$, then $p = \sum_{\nu=1}^{n} u_\nu v_\nu$, $u_\nu \in U$, $v_\nu \in V$. Hence $\partial_i p = \sum_{\nu=1}^{n} ((\partial_i u_\nu)v_\nu + u_\nu \partial_i v_\nu) \in UV$, thus $(UV)' = UV$.

6.34. Corollary. *Let W be a D-full ideal of $R[x_1, \ldots, x_k]$ such that the enclosing ideal C of W is the ideal product of two comaximal ideals A and B. Then W can be represented as the ideal product of a D-full ideal U and a D-full ideal V having A and B, resp., as their enclosing ideal.*

The corollary will follow from

6.35. Lemma. *For any ideal C of R, the ideal (C) of $R[x_1, \ldots, x_k]$ is a D-full ideal.*

Proof. By Lemma 6.13, and the elementary properties of partial derivations.

6.36. Proof of Corollary 6.34. As the proof of Prop. 6.15 and by taking in account Cor. 6.33 and Lemma 6.35.

6.4. For any full ideal V of $R[x_1, \ldots, x_k]$, we define the D-core δV of V as the sum of all D-full ideals of $R[x_1, \ldots, x_k]$ contained in V. By Cor. 6.33, δV itself is a D-full ideal contained in V.

6.41. Proposition. *$\delta V = \bigcap(V^{(n)} \mid n \geqslant 0)$, and the enclosing ideals of V and δV coincide.*

Proof. We set $U = \bigcap(V^{(n)} \mid n \geqslant 0)$, then U is a full ideal of $R[x_1, \ldots, x_k]$. By Lemma 6.22, $U' = \bigcap(V^{(n+1)} \mid n \geqslant 0) = \bigcap(V^{(n)} \mid n \geqslant 1)$ whence $U \subseteq U'$. Thus U is a D-full ideal and $U \subseteq V$. We conclude $U \subseteq \delta V$. Conversely, let W be any D-full ideal such that $W \subseteq V$, then $W \subseteq V^{(n)}$, $n \geqslant 0$, again by Lemma 6.22, thus $W \subseteq U$. In particular, $\delta V \subseteq U$ showing that $\delta V = U$. Th. 6.21 and Th. 5.5 imply that V and δV have one and the same enclosing ideal.

6.42. Corollary. *If $\{V_\nu \mid \nu \in I\}$ is a set of full ideals and $D = \bigcap(V_\nu \mid \nu \in I)$, then $\delta D = \bigcap(\delta V_\nu \mid \nu \in I)$.*

Proof. By Prop. 6.41 and Lemma 6.22,

$$\delta D = \bigcap(D^{(n)} \mid n \geqslant 0) = \bigcap\big(\bigcap(V_\nu^{(n)} \mid \nu \in I) \mid n \geqslant 0\big) = \bigcap(\delta V_\nu \mid \nu \in I).$$

7. Full ideals over fields

7.1. Let Q be any field, then Q is in the variety $\mathfrak{V}$ of commutative rings with identity and we may apply all our results of § 6 to $Q[x_1, \ldots, x_k]$. The information that Q is a field yields, however, some more specific results on full ideals.

7.11. Theorem. *If Q is any infinite field, then $Q[x_1, \ldots, x_k]$ has no full ideals apart from the trivial ones.*

Proof. Let U be a full ideal of $Q[x_1, \ldots, x_k]$. Since Q has just the trivial ideals, the enclosing ideal of U is either Q or the zero ideal 0 of Q. The first case yields $U \supseteq (Q) = Q[x_1, \ldots, x_n]$, and the second case $U \subseteq \{0\}$. But then $f \in U$ implies $f(r_1, \ldots, r_k) = 0$, for all $(r_1, \ldots, r_k) \in Q^k$, whence $f = 0$. For $k = 1$, this follows from a well-known theorem on polynomials over fields, and induction on k proves the result. Therefore $U = 0$.

7.2. If Q is a finite field, then Th. 7.11 does not hold. For $x_1^{|Q|} - x_1 \in \{0\}$ as we know from a well-known theorem on finite fields, but $1 \notin \{0\}$. Thus $\{0\}$ is a non-trivial full ideal of $Q[x_1, \ldots, x_k]$. A complete classi-

fication of the full ideals of $Q[x_1, \ldots, x_k]$, Q finite, is known just for $k = 1$. This is achieved by

7.21. Theorem. *Let Q be a finite field of characteristic p and order q. Then every non-trivial full ideal V of $Q[x]$ can be uniquely represented as $V = (x^{q^{e_1}}-x)^{a_1} \cap (x^{q^{e_2}}-x)^{a_2} \cap \ldots \cap (x^{q^{e_r}}-x)^{a_r}$ where $r > 0$, $e_1 > e_2 > \ldots > e_r > 0$, $a_\nu > 0$, $\nu = 1, \ldots, r$, and $a_j > a_i$ if e_j is a proper divisor of e_i. Any such V is a non-trivial full ideal.*

Proof. Clearly, any such V is a non-trivial ideal. The principal ideal $(x^{q^e}-x)$ consists of those polynomials of $Q[x]$ which vanish for all elements of the extension field of order q^e of Q, hence, by Lemma 5.31, $(x^{q^e}-x)$ is a full ideal of $Q[x]$. By Th. 6.11 and Cor. 5.51, V is a full ideal. Next we show that every non-trivial full ideal V can be written as in the theorem. Since $Q[x]$ is a principal ideal domain, $V = (f)$, for some monic non-constant polynomial $f \in Q[x]$. Let C be the algebraic closure of Q and $c_1 \in C$ any root of f. If $g \in Q[x]$, then $xfg = f \circ g \in V$ whence $f \circ g = rf$, for some $r \in Q[x]$. Hence $f(g(c_1)) = r(c_1) f(c_1) = 0$. This implies that every element of the subfield $Q(c_1)$ of C is a root of f. Let $c_1 \neq c_2 \in Q(c_1)$, and a_i, $i = 1, 2$, be the multiplicities of c_i as roots of f. Then we have the factorization in $C[x]$

$$f = (x-c_1)^{a_1} (x-c_2)^{a_2} \ldots (x-c_s)^{a_s} \tag{7.21}$$

where $s > 1$, $c_i \neq c_j$, for $i \neq j$, $a_\nu > 0$, $\nu = 1, \ldots, s$. Let $g \in Q[x]$ such that $c_2 = g(c_1)$ and set

$$h = \begin{cases} g, & \text{for} \quad g'(c_1) \neq 0 \\ g + (x^{q^{e_1}}-x), & \text{for} \quad g'(c_1) = 0 \end{cases}$$

where e_1 is the degree of $Q(c_1)$ over Q. Then $h(c_1) = c_2$, and $h'(c_1) \neq 0$. By (7.21), we have

$$f \circ h = (h-c_1)^{a_1} (h-c_2)^{a_2} \ldots (h-c_s)^{a_s}.$$

c_1 is then a root of $f \circ h$ with multiplicity a_2. But $f \circ h \in V$ and thus is a multiple of f, hence $a_2 \geqslant a_1$. Since c_2 was chosen arbitrarily in $Q(c_1)$, we conclude that $(x^{q^{e_1}}-x)^{a_1} / f$. But c_1 was an arbitrary root of f in C, hence we can use any c_i for this argument. Thus

$$(f) \subseteq \cap_{i=1}^{s} (x^{q^{e_i}}-x)^{a_i} \tag{7.22}$$

where e_i denotes the degree of $Q(c_i)$ over Q. If this inclusion were not an equality, then $f = gv$ where v is the monic least common multiple of the polynomials $(x^{q^{e_i}}-x)^{a_i}$ and g is a non-constant polynomial of $Q[x]$. Then g has a root in C which is also a root c_i, say, of f. But $x-c_i$ divides $x^{q^{e_i}}-x$ whence $(x-c_i)^{a_i+1}$ divides f, a contradiction. We may order the right-hand side of (7.22) by decreasing e_i. Of all those ideals with the same e_i, we need just that one with the greatest a_i. In the representation of V thus obtained there may be an ideal $(x^{q^{e_j}}-x)^{a_j}$ such that e_j is a proper divisor of e_i and $a_j \leqslant a_i$. But then $(x^{q^{e_j}}-x)^{a_j}$ divides $(x^{q^{e_i}}-x)^{a_i}$, and we may drop $(x^{q^{e_j}}-x)^{a_j}$ in our representation. After completing this procedure whenever possible, we get a representation of V as in the theorem.

It remains to establish uniqueness. Suppose there are two representations of V as in the theorem, e.g.

$$V = (h) = \cap_{\nu=1}^{r} (x^{q^{e_\nu}}-x)^{a_\nu} = \cap_{\nu=1}^{s} (x^{q^{f_\nu}}-x)^{b_\nu}$$

where h is a monic, non-constant polynomial of $Q[x]$. Without loss of generality, we may assume $0 < r \leqslant s$. Every root of the polynomial $x^{q^{e_\nu}}-x$ is also a root of h, and conversely every root of h is a root of some $x^{q^{e_\nu}}-x$ since h divides the product of the $(x^{q^{e_\nu}}-x)^{a_\nu}$. Thus the sets of roots of h and of roots of all $x^{q^{e_\nu}}-x$ coincide. From the theory of finite fields we know that e_ν is the greatest degree over Q occurring amongst all the roots of $x^{q^{e_\nu}}-x$. Hence $e_1 = f_1$ since both equal the greatest degree over Q ocurring amongst the roots of h. If c is a root of h of degree e_1 over Q, then $x-c$ divides $x^{q^{e_1}}-x$, but $(x-c)^2$ does not, nor does $x-c$ divide any other $x^{q^{e_\nu}}-x$. But $(x^{q^{e_1}}-x)^{a_1}$ divides h which divides the product of all $(x^{q^{e_\nu}}-x)^{a_\nu}$. Thus a_1 is the multiplicity of c as a root of h, and arguing in the same manner for the second representation, we conclude $a_1 = b_1$. Suppose now that $e_\nu = f_\nu$, $a_\nu = b_\nu$, for $1 \leqslant \nu \leqslant t$, and

$$\cap_{\nu=1}^{t} (x^{q^{e_\nu}}-x)^{a_\nu} = \cap_{\nu=1}^{t} (x^{q^{f_\nu}}-x)^{b_\nu} = (g)$$

where g is a monic polynomial of $Q[x]$. Then $h = gk$, for some $k \in Q[x]$. Let

$$\cap_{\nu=t+1}^{r} (x^{q^{e_\nu}}-x)^{a_\nu} = (l)$$

for some monic $l \in Q[x]$, then $(h) = (g) \cap (l)$. If d is the monic greatest common divisor of g and l, then $h = gl/d$ whence $k = l/d$. Thus every root of k is a root of l, and hence a root of $x^{q^{e_v}} - x$, for some $v > t$. Therefore the maximal possible degree over Q of any root of k is e_{t+1}, and if c is a root of $x^{q^{e_{t+1}}} - x$ of degree e_{t+1} over Q then arguing as before we see that c, as a root of l, has the multiplicity a_{t+1}. By a well-known theorem on finite fields, $x - c$ divides $x^{q^{e_v}} - x$ where $v \leqq t$ if and only if e_{t+1} divides e_v. Since g is a least common multiple of the polynomials $(x^{q^{e_v}} - x)^{a_v}$, $v \leqq t$, the multiplicity of c, as a root of g, equals $a = \max a_v$ where v runs through those indices which satisfy $v \leqq t$ and e_{t+1}/e_v. By hypothesis, $a < a_{t+1}$ whence c, as a root of d has just multiplicity a thus, as a root of k, c has multiplicity $v = a_{t+1} - a > 0$. Therefore e_{t+1} is characterized by being the greatest of all degrees over Q of the roots of k, and so is f_{t+1}, by the same argument. If c is a root of k of the greatest possible degree, then c has multiplicity $a_{t+1} - \max a_v$ where v runs through all indices such that $v \leqq t$ and e_{t+1}/e_v, and, for the same reason c has multiplicity $b_{t+1} - \max b_v$ where $v \leqq t$ and f_{t+1}/f_v. We summarize and obtain $e_{t+1} = f_{t+1}$ and, by induction, $a_{t+1} = b_{t+1}$. Hence $e_v = f_v$, $a_v = b_v$, for $1 \leqq v \leqq r$. If $s > r$, then we could use the same argument as before. But now $k = 1$ while, on the other hand, k would have roots, a contradiction. Hence $r = s$, and the uniqueness is established.

7.3. Again let Q be a finite field of characteristic p and order q. With the information of Th. 7.21, it is now easy to determine all the D-full ideals of $Q[x]$. All to be done is to compute the D-core of every non-trivial full ideal of $Q[x]$. We do this first for the full ideal $W = (x^{q^e} - x)^a$. If $f \in W$, then $f = (x^{q^e} - x)^a g$, for some $g \in Q[x]$, thus

$$\partial_1 f = f' = (x^{q^e} - x)^a g' - a(x^{q^e} - x)^{a-1} g.$$

Hence $f' \in W$ if and only if $a(x^{q^e} - x)^{a-1} g \in W$. Therefore $W' = W$ if p/a while $W' = (x^{q^e} - x)^{a+1}$ if $p \nmid a$. By Prop. 6.41, $\delta W = (x^{q^e} - x)^{\bar{a}}$ where $\bar{a}$ is the least integer $m \geqq a$ being divisible by p. By Cor. 6.42, if $V = \bigcap_{v=1}^{r} (x^{q^{e_v}} - x)^{a_v}$ according to Th. 7.21, we have $\delta V = \bigcap_{v=1}^{r} (x^{q^{e_v}} - x)^{\bar{a}_v}$ where $\bar{a}_v$ is the least integer $m \geqq a_v$ being divisible by p. Cancelling redundant ideals in this representation of δV, we get a representation as

in Th. 7.21. Here all the a_v are divisible by p. Conversely, any ideal having such representation is a D-full ideal of $Q[x]$. We may state our results as

7.31. Theorem. *Let Q be a finite field of characteristic p and order q, and V a full ideal of $Q[x]$ represented as in Th. 7.21. Then V is a D-full ideal if and only if every exponent a_v is divisible by p.*

8. Residue polynomial ideals of Dedekind domains

8.1. Let $\mathfrak{V}$ be a variety of Ω-multioperator groups, A any algebra of $\mathfrak{V}$, $X = \{x_1, \ldots, x_k\}$, and D any ideal of A. Then by § 5.34, the residue polynomial ideal $\{D\}$ of $A(X, \mathfrak{V})$ consists of all $p \in A(X, \mathfrak{V})$ such that $p(g_1, \ldots, g_k) \in D$, for all $(g_1, \ldots, g_k) \in A^k$. By Prop. 5.35, $\{D\}$ is a full ideal of $A(X, \mathfrak{V})$. The elements of $\{D\}$ will be called "residue polynomials mod D".

What is the significance of considering residue polynomial ideals? Let $\eta : A \to B$ by any epimorphism of $\mathfrak{V}$-algebras. The diagram fig. 3.1 shows that $\beta = P_k(\eta)\,\sigma(A) = \sigma(B)\,\eta(X)$ is a composition epimorphism from $A(X, \mathfrak{V})$ to $P_k(B)$, and $p(\operatorname{Ker}\beta)\,q$ if and only if $p(g_1, \ldots, g_k)\,(\operatorname{Ker}\eta)\,q(g_1, \ldots, g_k)$, for all $(g_1, \ldots, g_k) \in A^k$. Thus $\operatorname{Ker}\beta = \{\operatorname{Ker}\eta\}$. Using the notation of ch. 6, § 3.2 and § 5.3, we get $\ker\beta = \ker \operatorname{Ker}\beta = \ker\{\operatorname{Ker}\eta\} = \ker\{\ker^{-1}\ker \operatorname{Ker}\eta\} = \{\ker \operatorname{Ker}\eta\} = \{\ker\eta\}$. Thus the residue polynomial ideals of $A(X, \mathfrak{V})$ are just the kernels of the composition epimorphisms β.

Now let $\mathfrak{V}$ be the variety of commutative rings with identity and R a ring of $\mathfrak{V}$. Again $R[x_1, \ldots, x_k]$ will stand for $R(X, \mathfrak{V})$ and will be called the ring of polynomials in $x_1, \ldots, x_k$ (over R). For any ideal D of R, we wish to get more information about $\{D\}$. If R is noetherian, then $R[x_1, \ldots, x_k]$ is also noetherian, thus $\{D\}$ could be characterized in this case by writing down some ideal basis for $\{D\}$. This will actually be done for the case where R is a Dedekind domain, and $R|D$ is finite. In particular, we may take R to be the ring of rational integers and $D \neq 0$.

Let S be any ring and B any ideal of S. $\ker^{-1} B$ is then the corresponding congruence on S. As usual we will write $a \equiv b \bmod B$ for $a(\ker^{-1} B)b$.

8.2. Having spelled out our next aim, we start by taking a Dedekind domain R and an ideal D of R such that $R|D$ is finite. We are looking for an ideal basis of $\{D\}$. If $D = R$ then $\{D\} = R[x_1, \ldots, x_k] = (1)$,

and if $D = 0$, then $R \cong R|0$ is finite and hence a field. In this case $|R| = q$, for some prime power q, and certainly $\{0\} \supseteq (x_1^q - x_1, \ldots, x_k^q - x_k)$ as follows from a well-known theorem on finite fields. On the other hand, we also know that, for $k = 1$, $\{0\} \subseteq (x_1^q - x_1)$. Let $f \in \{0\}$, then, by ch. 1, Th. 8.21, $f = (x_k^q - x_k)g + h$ where $g \in R[x_1, \ldots, x_k]$ and $h = \sum_{i=0}^{q-1} p_i(x_1, \ldots, x_{k-1})x_k^i$. Clearly $h \in \{0\}$. Therefore, for any $(r_1, \ldots, r_{k-1}) \in R^{k-1}$, we have $\sum_{i=0}^{q-1} p_i(r_1, \ldots, r_{k-1})x_k^i \in \{0\}$ whence $p_i(x_1, \ldots, x_{k-1}) \in \{0\}$, $0 \leqslant i \leqslant q-1$. By induction, $h \in (x_1^q - x_1, \ldots, x_{k-1}^q - x_{k-1})$, hence $f \in (x_1^q - x_1, \ldots, x_k^q - x_k)$. We conclude that $\{0\} = (x_1^q - x_1, \ldots, x_k^q - x_k)$.

Now let D be any non-trivial ideal of R such that $R|D$ is finite. Since R is Dedekind, D has, up to ordering, a unique factorization $D = \prod_{i=1}^{r} P_i^{e_i}$ where the P_i are pairwise distinct non trivial prime ideals of R and $e_i > 0$, $i = 1, \ldots, r$. It is also known that the ideals $P_i^{e_i}$ are pairwise comaximal. Since $P_i^{e_i} \subseteq \{P_i^{e_i}\}$, we see that also the ideals $\{P_i^{e_i}\}$ are pairwise comaximal. The product of comaximal ideals coincides with their intersection, thus by 5.36,

$$\{D\} = \left\{\prod_{i=1}^{r} P_i^{e_i}\right\} = \{\cap_{i=1}^{r} P_i^{e_i}\} = \cap_{i=1}^{r} \{P_i^{e_i}\} = \prod_{i=1}^{r} \{P_i^{e_i}\}.$$

Hence it suffices to determine ideal bases for the $\{P_i^{e_i}\}$. Since $D \subseteq P_i^{e_i} \subseteq P_i$, all the prime ideals P_i have finite factor rings $R|P_i$.

8.3. Let P be a non trivial prime ideal of R such that $R|P$ is finite. Then $R|P$ is a finite field of order q where $q = p^\nu$, for some prime p. We introduce a number-theoretical function ε_P which depends on P. Let λ be the function from the set of positive integers to the set of non-negative integers defined by $\lambda(k) = \max(\lambda | q^\lambda \text{ divides } k)$. Then ε_P shall be the function from the set of non-negative integers into itself defined by

$$\varepsilon_P(0) = 0, \quad \varepsilon_P(k) = \sum_{i=1}^{k} \lambda(i), \quad \text{for} \quad k > 0. \tag{8.31}$$

A well-known number-theoretical formula (see ch. 6, § 9.3) tells us that

$$\varepsilon_P(k) = \frac{k - s_q(k)}{q-1} \tag{8.32}$$

where $s_q(k)$ is the sum of the digits in the q-adic expansion of k. ε_P actually depends just on $|R|P|$, not on P itself. Whenever we keep P fixed, we will write ε for ε_P. For every integer $n \geqslant 0$ and every integer $1 \leqslant a \leqslant q-1$, we define elements $s(aq^n)$ as follows: $s(q^n)$, $s(2q^n)$, $\ldots$, $s((q-1)q^n)$ is an arbitrarily chosen full set of coset representatives for the non-zero elements in $P^n|P^{n+1}$ — by ch. 6, Lemma 4.52, $P^n|P^{n+1}$ consists, indeed, of q elements. Additionally we put $s(0) = 0$. If k is any non-negative integer and $k = a_m q^m + \ldots + a_1 q + a_0$ is the q-adic expansion of k, we define

$$r_k = s(a_m q^m) + \ldots + s(a_1 q) + s(a_0).$$

In particular, $r_{tq^n} = s(tq^n) \in P^n$, for $0 \leqslant t < q$.

8.31. Lemma. *Let $n \geqslant 0$ be an integer. Then $r_i \equiv r_k \bmod P^n$ if and only if $i \equiv k \bmod q^n$.*

Proof. The lemma holds obviously for $n = 0$, hence we may assume $n > 0$. Let $i = \sum a_t q^t$, $k = \sum b_t q^t$ be the q-adic expansion of i and k, resp., then $r_i = \sum s(a_t q^t)$, $r_k = \sum s(b_t q^t)$. If $i \equiv k \bmod q^n$, then, for $0 \leqslant t < n$, we have $a_t = b_t$, hence $s(a_t q^t) = s(b_t q^t)$, $0 \leqslant t < n$. As a consequence, $r_i \equiv \sum_{t<n} s(a_t q^t) = \sum_{t<n} s(b_t q^t) \equiv r_k \bmod P^n$. Conversely, if $r_i \equiv r_k \bmod P^n$, then $\sum_{t<n} s(a_t q^t) \equiv \sum_{t<n} s(b_t q^t) \bmod P^n$ whence $s(a_0 q^0) \equiv s(b_0 q^0) \bmod P$. Therefore $s(a_0 q^0) = s(b_0 q^0)$. By induction, $s(a_t q^t) = s(b_t q^t)$, $0 \leqslant t < n$, hence $a_t q^t = b_t q^t$, for $0 \leqslant t < n$. We conclude that $i \equiv \sum_{t<n} a_t q^t \equiv \sum_{t<n} b_t q^t \equiv k \bmod q^n$.

8.4. We define a sequence of polynomials $t_n \in R[x]$, $n = 0, 1, 2, \ldots$ by

$$t_0 = 1, \quad t_n = \prod_{i=0}^{n-1} (x - r_i), \quad \text{for } n > 0.$$

8.41. Lemma. *For every $n \geqslant 0$, we have $t_n \in \{P^{\varepsilon(n)}\}$, but $t_n(r_n) \notin P^{\varepsilon(n)+1}$. In particular, $t_n \notin \{P^{\varepsilon(n)+1}\}$.*

Proof. We first show that $t_n \in \{P^{\varepsilon(n)}\}$. For $\varepsilon(n) = 0$, this is obviously true. So we may assume that $\varepsilon(n) = m > 0$. Let $r \in R$ be arbitrarily chosen. Then there exist integers d_i, $0 \leqslant d_i < q$, $i = 0, 1, \ldots, m-1$, such

that $r \equiv s(d_0) \bmod P$, $r - s(d_0) \equiv s(d_1 q) \bmod P^2$, $\ldots$, $r - \sum_{i=0}^{m-2} s(d_i q^i) \equiv s(d_{m-1} q^{m-1}) \bmod P^m$, i.e. $r \equiv \sum_{t=0}^{m-1} s(d_t q^t) \bmod P^m$. Then, for $l = \sum_{t=0}^{m-1} d_t q^t$, we have $r \equiv r_l \bmod P^m$ and hence $t_n(r) \equiv t_n(r_l) \bmod P^m$. For $l < n$, obviously $t_n(r_l) = 0$. If $l \geqslant n$, then, by Lemma 8.31, if we set $S = \sum_{i=0}^{n-1} \lambda(l-i)$, we get $t_n(r_l) = \prod_{i=0}^{n-1} (r_l - r_i) \in P^S$, but $t_n(r_l) \notin P^{S+1}$. By (8.31) and (8.32), $S = \varepsilon(l) - \varepsilon(l-n) = (l - s_q(l))/(q-1) - [(l-n) - s_q(l-n)]/(q-1)$. But, since $s_q(a+b) \leqslant s_q(a) + s_q(b)$, we have $s_q(l) - s_q(l-n) \leqslant s_q(n)$. Hence $S \geqslant (n - s_q(n))/(q-1) = \varepsilon(n) = m$ whence $t_n(r) \equiv t_n(r_l) \equiv 0 \bmod P^m$. Similarly we show that $t_n(r_n) \notin P^{\varepsilon(n)+1}$. For $t_n(r_n) \notin P^{S+1}$, where $S = \varepsilon(n) - \varepsilon(0) = \varepsilon(n)$. This completes the proof.

8.5. Lemma. *Let $e \geqslant 0$ be an arbitrary integer. Every polynomial $f \in R[x]$ such that $f \in \{P^e\}$ and $[f] \leqslant m$ can be written as $f = \sum_{i=0}^{m} a_i t_i$ where $a_i \in P^{e-\varepsilon(i)}$ if $\varepsilon(i) < e$, and $a_i \in R$ if $\varepsilon(i) \geqslant e$. Every such polynomial belongs to $\{P^e\}$.*

Proof. The latter statement is a consequence of Lemma 8.41. Suppose $f \in \{P^e\}$, $[f] \leqslant m$. Then clearly $f = \sum_{i=0}^{m} a_i t_i$, for some $a_i \in R$. We have $f(0) = a_0$ whence $a_0 \in P^{e-\varepsilon(0)}$. By induction and Lemma 8.41, we conclude that $a_l t_l \in \{P^e\}$, for $l < j$, hence $g = \sum_{i=j}^{m} a_i t_i \in \{P^e\}$. Therefore $g(r_j) = a_j t_j(r_j) \in P^e$, hence $a_j \in P^{e-\varepsilon(j)}$, again by Lemma 8.41.

8.51. Theorem. *Let $0 \neq p \in P$, $b_i \in R$, $i = 0, 1, \ldots$, such that $P^i = (p^i, b_i)$, s the least integer such that $\varepsilon(qs) \geqslant e$, and $T_1 = \{t_{qs}\}$, $T_2 = \{p^{e-\varepsilon(qi)} t_{qi} \mid 0 \leqslant i < s\}$, $T_3 = \{b_{e-\varepsilon(qi)} t_{qi} \mid 0 \leqslant i < s\}$. Then $T_1 \cup T_2 \cup T_3$ is a basis for the ideal $\{P^e\}$. If, in particular, $P = (p)$, then $T_1 \cup T_2$ is a basis for $\{P^e\}$.*

Proof. By Lemma 8.5, $T_1 \cup T_2 \cup T_3 \subseteq \{P^e\}$. Let $f \in \{P^e\}$, then, by Lemma 8.5, $f = \sum_{i=0}^{m} a_i t_i$, $a_i \in P^{e-\varepsilon(i)}$, for $\varepsilon(i) < e$, and $a_i \in R$, for $\varepsilon(i) \geqslant e$. Obviously, for $n \geqslant 0$, t_n / t_{n+1}, and $\varepsilon(k+1) = \varepsilon(k)$ if $q \nmid k+1$. Hence,

for $l < s$, there exist elements c_i, $d_i \in R$ such that

$$\sum_{i=ql}^{ql+(q-1)} a_i t_i = t_{ql} \sum_{i=ql}^{ql+(q-1)} (c_i p^{e-\varepsilon(ql)} + d_i b_{e-\varepsilon(ql)}) (t_i / t_{ql})$$
$$= p^{e-\varepsilon(ql)} t_{ql} g + b_{e-\varepsilon(ql)} t_{ql} h,$$

for some g, $h \in R[x]$. This proves the first assertion. If $P = (p)$, we may set $b_i = 0$, for all i. This completes the proof.

8.6. We want to generalize Lemma 8.5 and Th. 8.51 to $R[x_1, \ldots, x_k]$. For this purpose, we introduce some new notations. Let N be the additive semigroup of non-negative integers and M_k the direct product of k copies of N. For any $r \in N$, and $\alpha \in M_k$, $r\alpha$ shall mean the element of M_k whose components are r-times the corresponding component of α. A partial order $\leqslant$ on M_k will be defined by $(m_1, \ldots, m_k) \leqslant (n_1, \ldots, n_k)$ if and only if $m_i \leqslant n_i$, $i = 1, \ldots, k$. Let $\varepsilon_{Pk} : M_k \to N$ be defined by $\varepsilon_{Pk}(m_1, \ldots, m_k) = \sum_{i=1}^{k} \varepsilon_P(m_i)$. In particular, we have $\varepsilon_{P1} = \varepsilon_P$ and again we abbreviate ε_{Pk} by writing ε_k instead. Finally, for all $\iota = (i_1, \ldots, i_k) \in M_k$, we define $t_\iota \in R[x_1, \ldots, x_k]$ by $t_\iota = t_{i_1}(x_1) \ldots t_{i_k}(x_k)$.

8.61. Lemma. *Let $e \geqslant 0$ be an arbitrary integer, $\mu = (m_1, \ldots, m_k) \in M_k$, and $f \in R[x_1, \ldots, x_k]$ such that $f \in \{P^e\}$ and, regarded as a polynomial in x_j over $R[x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_k]$, has degree $\leqslant m_j$, $j = 1, \ldots, k$. Then $f = \sum(a_\iota t_\iota \mid \iota \leqslant \mu)$ where $a_\iota \in P^{e-\varepsilon_k(\iota)}$, for $\varepsilon_k(\iota) < e$, and $a_\iota \in R$, for $\varepsilon_k(\iota) \geqslant e$. Any such polynomial belongs to $\{P^e\}$ and has degree $\leqslant m_j$ as a polynomial in x_j, $j = 1, \ldots, k$.*

Proof. Let f be a polynomial as in the hypothesis of the lemma. By Lemma 8.41, $t_{i_j}(x_j) \in \{P^{\varepsilon(i_j)}\}$, $j = 1, \ldots, k$, hence $t_\iota \in \{P^{\varepsilon_k(\iota)}\}$ whence $f \in \{P^e\}$. Since $[t_{i_j}(x_j)] = i_j$, we see that, for $\iota = (i_1, \ldots, i_k)$, t_ι is of degree i_j in x_j, and thus f is of degree $\leqslant m_j$ in x_j. Conversely, let $f \in \{P^e\}$ be of degree $\leqslant m_j$ in x_j, $j = 1, \ldots, k$. For $k = 1$, Lemma 8.5 yields the result. Let $k > 1$, then $f = \sum_{i_k=0}^{m_k} g_{i_k}(x_1, \ldots, x_{k-1}) t_{i_k}(x_k)$, which is obtained from the normal form for f as in ch. 1, Th. 8.21, by collecting all those summands containing equal powers of x_k and applying the division algorithm using $t_{m_k}(x_k)$, $t_{m_k-1}(x_k)$, $\ldots$, $t_0(x_k)$. We observe then that every $g_{i_k}(x_1, \ldots, x_{k-1})$ is of degree $\leqslant m_j$ in x_j, $j = 1, \ldots, k-1$. For any

$(r_1, \ldots, r_{k-1}) \in R^{k-1}$,

$$f(r_1, \ldots, r_{k-1}, x_k) = \sum_{i_k=0}^{m_k} g_{i_k}(r_1, \ldots, r_{k-1})\, t_{i_k}(x_k) \in \{P^e\}$$

and, by the same argument as in the proof of Lemma 8.5, we conclude that $g_{i_k}(x_1, \ldots, x_{k-1}) \in \{P^{e-\varepsilon(i_k)}\}$ if $\varepsilon(i_k) < e$. By induction, $g_{i_k}(x_1, \ldots, x_{k-1}) = \sum a_{(i_1, \ldots, i_{k-1}, i_k)} t_{i_1}(x_1) \ldots t_{i_{k-1}}(x_{k-1})$ where $a_{(i_1, \ldots, i_{k-1}, i_k)} \in \{P^{e-\varepsilon(i_k)-(\varepsilon(i_1)+\ldots+\varepsilon(i_{k-1}))}\} = \{P^{e-\varepsilon_k(\iota)}\}$ if $\varepsilon_k(\iota) < e$, and the sum extends over all $(i_1, \ldots, i_{k-1}) \leqslant (m_1, \ldots, m_{k-1})$. Substitution of this expression for the g_{i_k} into our expression for f completes the proof of the lemma.

8.62. Theorem. *Let p, b_i, s be defined as in Th. 8.51, $\alpha = (s, s, \ldots, s) \in M_k$, and $T_1 = \{t_{q\iota} \mid \iota \leqslant \alpha,\ \varepsilon_k(q\iota) \geqslant e\}$, $T_2 = \{p^{e-\varepsilon_k(q\iota)} t_{q\iota} \mid \iota \leqslant \alpha,\ \varepsilon_k(q\iota) < e\}$, $T_3 = \{b_{e-\varepsilon_k(q\iota)} t_{q\iota} \mid \iota \leqslant \alpha,\ \varepsilon_k(q\iota) < e\}$. Then $T_1 \cup T_2 \cup T_3$ is a basis for the ideal $\{P^e\}$ of $R[x_1, \ldots, x_k]$. In particular, if $P = (p)$, then $T_1 \cup T_2$ is a basis for $\{P^e\}$.*

Proof. Using Lemma 8.61, the proof runs along the same lines as that of Th. 8.51 and is thus left to the reader.

8.63. Remark. If R is the ring of rational integers, then $P = (p)$, for some prime p. Moreover $q = p$ and we can take $s(lq^i) = lq^i$, hence $r_l = l$, for $l = 0, 1, 2, \ldots$

9. Residue polynomial ideals over groups

9.1. In the preceding section, a description of the residue polynomial ideals of some special types of polynomial rings could be achieved comparatively easily. We know much less in the case of groups, however, the Kurosh subgroup theorem will at least tell us a lot about the group structure of the residue polynomial ideals of $G(X, \mathfrak{V}) = G[X]$ where $\mathfrak{V}$ is the variety of groups, G any group with group operation $\cdot$, and $X = \{x_1, \ldots, x_k\}$ a set of indeterminates. First we prove a qualitative result:

9.11. Theorem. *Let N be any normal subgroup of G, and $\{N\}$ the residue polynomial ideal of $G[X]$ generated by N. Then the group $V = \langle \{N\}, \cdot, {}^{-1}, 1 \rangle$ is isomorphic to a free product $F * K$ of a free group F and a group K which is the free product of some copies of N.*

Proof. According to ch. 1, Cor. 9.22, $G[X]$, $\{\varphi_1, \varphi_2\}$ is a free product of G and the free group $F(X, \mathfrak{V}) = F(X)$. By a well-known group-theoretical

result, there exist monomorphisms $\psi_i : F(x_i) \to F(X)$, $i = 1, \ldots, k$, such that $F(X)$, $\{\psi_1, \ldots, \psi_k\}$ is a free product of the groups $F(x_i)$. Thus $G[X] = F(x_1) * \ldots * F(x_k) * G$ where $*$ denotes the free product of groups as usual. Let $\eta : G \to G|N$ be the canonical epimorphism, then, by § 5.3, we have $V = \{N\} = \{p \mid p \in G[X]$ and $p(g_1, \ldots, g_k) \in N$, for all $(g_1, \ldots, g_k) \in G^k\}$, and it is easy to see that $V = \ker \sigma(G|N)\eta(X)$. Since V is a subgroup of a free product, we are ready for applying the Kurosh subgroup theorem (see ch. 6, § 6.7) to V and obtain since V is normal in $G[X]$)

$$V \cong F_1 * \Big[* \Big(* (V \cap F(x_j) \mid i \in I_j) \mid 1 \leqslant j \leqslant k \Big) \Big] * \Big[* (V \cap G \mid i \in I_0) \Big] \qquad (9.1)$$

where F_1 is a free group and I_j, $j = 0, 1, \ldots, k$, are suitable index sets. Since $V \cap F(x_j)$ is free as a subgroup of a free group, the free product of the first and second factor in (9.1) is a free group F. Moreover, $V \cap G = \{N\} \cap G = N$, by Th. 5.4, whence the third factor in (9.1) is a free product of some copies of N and the theorem is proved.

9.2. The Kurosh subgroup theorem also yields some quantitative information which, for finite G, enables us to determine the rank of F in $V \cong F * K$ as well as the number of free factors isomorphic to N in K. In the following, we keep the notation of Th. 9.11.

9.21. Proposition. *If G is a finite group, then K is the free product of $|P_k(G|N)|\,|N|/|G|$ copies of N while the rank of F equals*

$$1 + |P_k(G|N)|\,(k - |N|/|G|).$$

Proof. By the Kurosh subgroup theorem, $|I_0|$ is the number of cosets of $G[X]$ modulo GV. Since $V = \ker \sigma(G|N)\eta(X)$, we see that $G[X]|V \cong P_k(G|N)$ while $GV|V \cong G|V \cap G = G|N$. Hence $|I_0| = |P_k(G|N)|\,|N|/|G|$ which proves the first statement of the proposition. Similarly $|I_j|$ is the number of cosets of $G[X]$ modulo $F(x_j)V$, $j = 1, \ldots, k$. But $F(x_j)V|V \cong F(x_j)|V \cap F(x_j)$ and $V \cap F(x_j) = \{x_j^k \mid g^k \in N$, for all $g \in G\} = [x_j^e]$ where e is the exponent of $G|N$. Thus $F(x_j)V|V \cong C_e$, the cyclic group of order e which shows that $|I_j| = |P_k(G|N)|/e$. If $r(F)$ and $r(F_1)$ are the rank of F and F_1, respectively, then $r(F) = r(F_1) + k|P_k(G|N)|/e$, by definition of F since $r(V \cap F(x_j)) = 1$. But, again by the Kurosh subgroup theorem, $r(F_1) = k|P_k(G|N)| - |P_k(G|N)|\,|N|/|G| - k|P_k(G|N)|/e + 1$. Hence $r(F) = 1 + |P_k(G|N)|\,(k - |N|/|G|)$ which proves the proposition.

9.22. Corollary. *$\langle \ker \sigma(G);\ \cdot, {}^{-1}, 1\rangle$ is a free group. If G is finite, then this free group has rank $1+|P_k(G)|\,(k-1/|G|)$.*

Proof. By Th. 9.11 and Prop. 9.21 if we put $N = \{1\}$.

9.23. Remark. The actual description of the residue polynomials of $\{N\}$ is, in general, unknown, but a few results into this direction have been obtained. The reader is referred to ch. 5, § 1.

10. Derivation families with chain rule

10.1. Let R be a commutative ring with identity, $R[x_1, \ldots, x_k]$ the polynomial ring over R in the indeterminates $x_1, \ldots, x_k$, and $\partial_i = \partial/\partial x_i$, $i = 1, \ldots, k$, the partial derivations of $R[x_1, \ldots, x_k]$. This family $(\partial_1, \ldots, \partial_k)$ is a well-known example of a family of mappings $(\delta_1, \ldots, \delta_k)$, $\delta_i : R[x_1, \ldots, x_k] \to R[x_1, \ldots, x_k]$, $i = 1, \ldots, k$, such that, for any $f, g, g_1, \ldots, g_k \in R[x_1, \ldots, x_k]$ and $l = 1, \ldots, k$, the following equations are valid:

$$\delta_l(f+g) = \delta_l f + \delta_l g, \tag{10.11}$$

$$\delta_l(fg) = (\delta_l f)g + f(\delta_l g), \tag{10.12}$$

$$\delta_l \varkappa f g_1 \ldots g_k = \sum_{i=1}^{k} [\varkappa(\delta_i f) g_1 \ldots g_k]\, \delta_l g_i. \tag{10.13}$$

The problem arises of determining all the families $(\delta_1, \ldots, \delta_k)$ of such mappings satisfying (10.11), (10.12), (10.13). More generally, for any ring S, a mapping $\delta : S \to S$ is called a derivation of S if δ satisfies (10.11), (10.12) in the place of δ_l, for all $f, g \in S$. Substituting ∂_i for δ_i, $i = 1, \ldots, k$, in (10.13), we can read off the well-known chain rule. Thus we will call any family $(\delta_1, \ldots, \delta_k)$ of mappings $\delta_i : R[x_1, \ldots, x_k] \to R[x_1, \ldots, x_k]$, $i = 1, \ldots, k$, a derivation family with chain rule, or, in brief, a "C-derivation family" if this family satisfies (10.11), (10.12), (10.13).

It will be useful to adopt the following notation: Let $F = (f_{st})$ be any matrix with entries $f_{st} \in R[x_1, \ldots, x_k]$ and $\mathfrak{g} = (g_1, \ldots, g_k)$ a k-tuple of elements of $R[x_1, \ldots, x_k]$, then the matrix $(\varkappa f_{st} g_1 \ldots g_k)$ shall be denoted by $F \circ \mathfrak{g}$.

10.2. Let $(\delta_1, \ldots, \delta_k)$ be an arbitrary C-derivation family and $f, g_1, \ldots, g_k$ arbitrary elements of $R[x_1, \ldots, x_k]$. If $\varkappa f g_1 \ldots g_k$ is represented by

substituting $g_1, \ldots, g_k$ for $x_1, \ldots, x_k$ into the normal form of f as in ch. 1, § 8.2, and if we apply (10.11) and (10.12) to this representation, we obtain from a straightforward computation

$$\delta_l \varkappa f g_1 \ldots g_k = \sum_{i=1}^{k} [\varkappa(\partial_i f) g_1 \ldots g_k]\, \delta_l g_i. \tag{10.211}$$

But $\varkappa f x_1 \ldots x_k = f$, hence

$$\delta_l f = \sum_{i=1}^{k} (\delta_l x_i)(\partial_i f), \tag{10.212}$$

and tying (10.13) and (10.211) together and using the right-superdistributivity of $\varkappa$, we end up with

$$\sum_{i=1}^{k} (\delta_l g_i)[\varkappa(\delta_i f - \partial_i f) g_1 \ldots g_k] = 0, \quad l = 1, \ldots, k. \tag{10.213}$$

We now introduce a matrix notation where s is used for the row index while t means the column index: $G = (\delta_s g_t)$, $P = (\partial_s g_t)$, $D = (\delta_s x_t)$, $E = k \times k$-identity matrix, $O = k \times k$-zero matrix, thus G, P, D, O and E are $k \times k$-matrices. Moreover we introduce $k \times 1$-matrices $\mathfrak{c} = (\delta_s f - \partial_s f)$, $\mathfrak{d} = (\partial_s f)$, $\mathfrak{o} = (0)$, and $1 \times k$-matrices $\mathfrak{g} = (g_t)$ and $\mathfrak{x} = (x_t)$. Then (10.213) becomes

$$G(\mathfrak{c} \circ \mathfrak{g}) = \mathfrak{o}. \tag{10.214}$$

From (10.212) we get

$$G = DP \tag{10.215}$$

and

$$\mathfrak{c} = D\mathfrak{d} - \mathfrak{d} = (D-E)\mathfrak{d}. \tag{10.216}$$

(10.216) and right-superdistributivity of $\varkappa$ imply

$$\mathfrak{c} \circ \mathfrak{g} = (D \circ \mathfrak{g} - E)(\mathfrak{d} \circ \mathfrak{g}), \tag{10.217}$$

and using (10.214) and (10.215), we get

$$DP(D \circ \mathfrak{g} - E)(\mathfrak{d} \circ \mathfrak{g}) = \mathfrak{o}. \tag{10.218}$$

Since (10.218) holds for all f and $\mathfrak{g}$, we may take, in particular $f = x_j$, $j = 1, \ldots, k$, whence

$$DP(D \circ \mathfrak{g} - E) = O, \quad \text{for all} \quad \mathfrak{g} \in R[x_1, \ldots, x_k]^k. \tag{10.219}$$

On the other hand, if $D = (\delta_s x_t)$ is any $k \times k$-matrix over $R[x_1, \ldots, x_k]$ satisfying (10.219), an easy computation shows that the mappings δ_l, $l = 1, 2, \ldots, k$, defined by

$$\delta_l f = \sum_{i=1}^{k} (\delta_l x_i)(\partial_i f), \quad \text{for all} \quad f \in R[x_1, \ldots, x_k],$$

are derivations of $R[x_1, \ldots, x_k]$, i.e. (10.11) and (10.12) is satisfied (one could have taken any matrix D for this purpose). Thus (10.211), (10.212), (10.215), (10.216), and (10.217) hold, while the condition (10.219) yields (10.214) and also (10.213). The right-superdistributivity of $\varkappa$ and (10.211) yield (10.13), hence $(\delta_1, \ldots, \delta_k)$ is a C-derivation family.

Thus our problem boils down to determining the matrices D satisfying (10.219). If D is such a matrix, let

$$D = A_r + A_{r-1} + \ldots + A_1 + A_0 \tag{10.220}$$

be the representation of D according to ch. 1, § 8.3, that means A_i, $i = 0, 1, \ldots, r$, is a $k \times k$-matrix whose entries are forms of degree i. We first show that A_0 is a scalar matrix, i.e.

$$A_0 = dE, \quad \text{for some } d \in R. \tag{10.221}$$

For $k = 1$, (10.221) is obvious, hence assume that $k > 1$. Choose $\mathfrak{g}$ such that $g_l = x_1 \ldots x_k$ and $g_j = 0$, for $j \neq l$, then $P = (\partial_s g_t) = P_{k-1}$ is a matrix whose entries are forms of degree $k-1$. Right-superdistributivity of $\varkappa$ and (10.220) imply

$$D \circ \mathfrak{g} = (A_r \circ \mathfrak{g}) + (A_{r-1} \circ \mathfrak{g}) + \ldots + (A_1 \circ \mathfrak{g}) + A_0.$$

If q_i is a form of degree i, and q_{jl} a form of degree j, $l = 1, \ldots, k$, then $\varkappa q_i q_{j1} \ldots q_{jk}$ is a form of degree ij. Hence substituting our particularly chosen $\mathfrak{g}$ into (10.219) yields

$$(A_r + A_{r-1} + \ldots + A_1 + A_0) P_{k-1}(B_{rk} + B_{(r-1)k} + \ldots + B_k + (A_0 - E)) = O \tag{10.222}$$

where B_{ik}, $i = 1, \ldots, r$, is a $k \times k$-matrix whose entries are forms of degree ik. After performing the matrix multiplication, we obtain a sum where the only summand with entries of degree $k-1$ is $A_0 P_{k-1}(A_0 - E)$, hence

$$A_0 P_{k-1}(A_0 - E) = O. \tag{10.223}$$

Let $A_0 = (a_{st})$, $(x_1 \ldots x_k)/x_t = u_t$, $t = 1, \ldots, k$, and $E = (\delta_{st})$, then $A_0 P_{k-1}(A_0 - E) = (c_{st})$ where $c_{st} = (a_{lt} - \delta_{lt}) \sum_{i=1}^{k} a_{si} u_i$. Hence, by (10.223),

$$(a_{lt} - \delta_{lt}) A_0 = O, \quad t, l = 1, \ldots, k. \tag{10.224}$$

For $l \neq t$, we get $a_{lt} a_{ll} = 0$ and $(a_{ll} - 1) a_{lt} = 0$ whence $a_{lt} = 0$. Furthermore, $(a_{ll} - 1) a_{tt} = (a_{tt} - 1) a_{ll} = 0$ whence $a_{tt} = a_{ll}$. Thus $a_{tt} = d$, $t = 1, \ldots, k$, for some $d \in R$, and (10.221) is proved.

Now we substitute $(x_1, \ldots, x_k)$ for $\mathfrak{g}$ in (10.219), then $P = E$ and

$$D^2 = D. \tag{10.225}$$

Substituting (10.221) into (10.220) and (10.220) into (10.225) and considering the terms of degree 0 of the entries, we see that $d^2 = d$. Suppose that

$$D = A_r + A_{r-1} + \ldots + A_l + dE, \quad A_l \neq O, \quad l > 0. \tag{10.226}$$

Then, again substitution into (10.225) and comparison of the terms of degree l in the entries, gives

$$2\, dA_l = A_l. \tag{10.227}$$

Since $d^2 = d$, we have $dA_l = O$ and therefore $A_l = O$, a contradiction. Thus $D = dE$ where $d \in R$ and $d^2 = d$.

Conversely, if $D = dE$ where $d \in R$ and $d^2 = d$, then, for all $\mathfrak{g}$, $DP(D \circ \mathfrak{g} - E) = (dE) P (dE - E) = (d^2 - d) P = O$.

We summarize our results as

10.21. Theorem. *The C-derivation families of $R[x_1, \ldots, x_k]$ are exactly the families $(d\partial_1, \ldots, d\partial_k)$ where $d \in R$ is an idempotent.*

10.3. It is well-known that for idempotents d of commutative rings R with identity, dR is a direct summand of R, and $r \to dr$ is the projection from R to dR. Conversely, every projection of R onto a direct summand of R is a mapping $r \to dr$ where d is an idempotent. Thus we may state Theorem 10.21 also as

10.31. Proposition. *The C-derivation families of $R[x_1, \ldots, x_k]$ are exactly the families $(\delta_1, \ldots, \delta_k)$ of mappings from $R[x_1, \ldots, x_k]$ into itself such that $\delta_i = \pi(X)\partial_i$ where π is a projection from R to a direct summand of R.*

10.32. Corollary. *R is directly indecomposable if and only if the only C-derivation families of $R[x_1, \ldots, x_k]$ are the family of the partial derivations and the family consisting of a k-tuple of zero mappings.*

10.4. Remark. The investigations of § 10.2 also show that any family $(\delta_1, \ldots, \delta_k)$ of mappings from $R[x_1, \ldots, x_k]$ into itself satisfying (10.11) and (10.12) also satisfies (10.13) if and only if $|R| = 1$. Generally, we may ask for what rings R two of these three conditions ensure that the third condition is satisfied. This problem is by no means trivial and no complete answer is known as yet.

W. MÜLLER [1] could prove:

a) If the additive group of R is torsionfree, then (10.11) and (10.13) imply (10.12). That torsionfreeness cannot be dropped, is shown by taking the field of order 2 for R as a counterexample.

b) If $k \geqq 2$, then (10.12) and (10.13) imply (10.11). If $k = 1$ and R is an integral domain, then also (10.12) and (10.13) imply (10.11).

11. Polynomial vectors and polynomial function vectors

11.1. Let $\mathfrak{V}$ be any variety, Ω its system of operations, $k \geqq 1$ an integer, $\mathfrak{W}_k$ the variety of k-dimensional $\mathfrak{V}$-composition algebras, $A = \langle A; \Omega, \varkappa \rangle$ an algebra of $\mathfrak{W}_k$, and $A^k = \langle A^k; \Omega \rangle$ the direct product of k copies of the algebra $\langle A; \Omega \rangle$. We define a binary operation $\circ$, written by means of infix notation, in A^k by

$$(a_1, \ldots, a_k) \circ (b_1, \ldots, b_k) = (\varkappa a_1 b_1 \ldots b_k, \varkappa a_2 b_1 \ldots b_k, \ldots, \varkappa a_k b_1 \ldots b_k),$$

and consider the algebra $\mathcal{F}(A) = \langle A^k; \Omega, \circ \rangle$.

Let $\varrho : A \to B$ be any homomorphism of algebras of $\mathfrak{W}_k$. Then we define the mapping $\mathcal{F}(\varrho) : \mathcal{F}(A) \to \mathcal{F}(B)$ by $\mathcal{F}(\varrho)(a_1, \ldots, a_k) = (\varrho a_1, \ldots, \varrho a_k)$.

11.11. Theorem. *For any $A \in \mathfrak{W}_k$, the algebra $\mathcal{F}(A)$ is an algebra of the variety $\mathfrak{W}_1$ of 1-dimensional $\mathfrak{V}$-composition algebras. $\mathcal{F}(A)$ has a selector system if and only if A has. For any homomorphism $\varrho : A \to B$ the mapping $\mathcal{F}(\varrho) : \mathcal{F}(A) \to \mathcal{F}(B)$ is a homomorphism. If $\varepsilon : A \to A$ is the identity automorphism of A, then $\mathcal{F}(\varepsilon) : \mathcal{F}(A) \to \mathcal{F}(A)$ is the identity automorphism of $\mathcal{F}(A)$. Moreover, if $\varrho : A \to B$, and $\sigma : B \to C$ are homomorphisms,*

then $\mathcal{F}(\sigma\varrho) = \mathcal{F}(\sigma)\mathcal{F}(\varrho)$. $\mathcal{F}(\varrho)$ is a monomorphism (epimorphism, isomorphism) if and only if ϱ is a monomorphism (epimorphism, isomorphism).

Proof. As a direct product of k copies of $\langle A; \Omega \rangle$, the algebra $\langle \mathcal{F}(A); \Omega \rangle$ belongs to $\mathfrak{V}$. Superassociativity of $\varkappa$ implies associativity of $\circ$. Similarly, the right-superdistributivity of $\circ$ follows from the right-superdistributivity of $\varkappa$. A selector system for $\circ$ means an identity, and $(s_1, \ldots, s_k)$ actually is an identity if and only if $\{s_1, \ldots, s_k\}$ is a selector system for $\varkappa$. Straightforward computation shows that $\mathcal{F}(\varrho)$ is a homomorphism and all the remaining statements of the theorem are obvious.

11.12. Remark. In the language of category theory, Theorem 11.11 tells us that $\mathcal{F}$ is a covariant functor from the category of k-dimensional $\mathfrak{V}$-composition algebras to the category of 1-dimensional $\mathfrak{V}$-composition algebras.

11.13. Lemma. *Let A be any algebra of $\mathfrak{W}_k$ and B a subalgebra of A, then $\mathcal{F}(B)$ is a subalgebra of $\mathcal{F}(A)$. If A, B are algebras of $\mathfrak{W}_k$, then the mapping $\psi : \mathcal{F}(A \times B) \to \mathcal{F}(A) \times \mathcal{F}(B)$ defined by*

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

is an isomorphism.

Proof. The first statement is obvious, the second one follows from straightforward computation.

11.2. Let $\mathfrak{V}$ be any variety, Ω its system of operations, $k \geqq 1$ an integer, and $X = \{x_1, \ldots, x_k\}$. Since $A(X, \mathfrak{V})$, $F_k(A)$, and $P_k(A)$ are k-dimensional $\mathfrak{V}$-composition algebras, we can apply the functor $\mathcal{F}$ to these algebras:

a) The elements of $\mathcal{F}(A(X, \mathfrak{V}))$ are the k-tuples $(p_1, \ldots, p_k)$ of polynomials of $A(X, \mathfrak{V})$, being called polynomial vectors and denoted by small Gothic letters.

b) The elements of $\mathcal{F}(F_k(A))$ are the k-tuples $(\psi_1, \ldots, \psi_k)$ of functions from A^k to A.

11.21. Lemma. *The mapping $\varphi : \mathcal{F}(F_k(A)) \to F_1(A^k)$ defined by $\varphi(\psi_1, \ldots, \psi_k)(a_1, \ldots, a_k) = (\psi_1(a_1, \ldots, a_k), \ldots, \psi_k(a_1, \ldots, a_k))$, for all $(a_1, \ldots, a_k) \in A^k$, is a composition isomorphism.*

Proof. Obvious.

c) The elements of $\mathcal{F}(P_k(A))$ are the k-tuples $(\psi_1, \ldots, \psi_k)$ of polynomial functions from A^k to A. These elements will be called polynomial function vectors and denoted by small Gothic letters. By Lemma 11.13, $\mathcal{F}(P_k(A))$ is a subalgebra of $\mathcal{F}(F_k(A))$, hence $\varphi\mathcal{F}(P_k(A))$ is a subalgebra of $F_1(A^k)$.

11.22. Remark. $P_1(A^k)$ is a subalgebra of $\varphi\mathcal{F}(P_k(A))$ since $\varphi\mathcal{F}(P_k(A))$ is a subalgebra of $F_1(A^k)$ containing all constant functions of $F_1(A^k)$ and the projection $\xi_1 \in F_1(A^k)$; but, in general, $P_1(A^k) \subset \varphi\mathcal{F}(P_k(A))$. For example, let A be polynomially complete, $k > 1$, and $|A| > 1$. Then $P_k(A) = F_k(A)$, hence $\varphi\mathcal{F}(P_k(A)) = F_1(A^k)$. Since A^k is not simple, A^k cannot be 1-polynomially complete, thus $P_1(A^k) \subset \varphi\mathcal{F}(P_k(A))$.

11.3. Let $\sigma : A(X, \mathfrak{V}) \to P_k(A)$ be the canonical epimorphism. σ is, as we know, a composition epimorphism. Hence $\mathcal{F}(\sigma) : \mathcal{F}(A(X, \mathfrak{V})) \to \mathcal{F}(P_k(A))$ is an epimorphism and therefore $\beta = \varphi\mathcal{F}(\sigma) : \mathcal{F}(A(X, \mathfrak{V})) \to F_1(A^k)$ is a homomorphism such that

$$\beta(p_1, \ldots, p_k)(a_1, \ldots, a_k) = (p_1(a_1, \ldots, a_k), \ldots, p_k(a_1, \ldots, a_k)),$$
$$(a_1, \ldots, a_k) \in A^k.$$

By Th. 11.11, $\mathcal{F}(\sigma)$ and β are monomorphisms if and only if σ is. Clearly, β is an epimorphism if and only if A is k-polynomially complete.

Let A, B be algebras of $\mathfrak{V}$ and $\eta : A \to B$ an epimorphism. Then $\mathcal{F}(\eta(X, \mathfrak{V})) : \mathcal{F}(A(X, \mathfrak{V})) \to \mathcal{F}(B(X, \mathfrak{V}))$ and $\mathcal{F}(P_k(\eta)) : \mathcal{F}(P_k(A)) \to \mathcal{F}(P_k(B))$ are epimorphisms. If η is an isomorphism, so are $\eta(X, \mathfrak{V})$ and $P_k(\eta)$, hence $\mathcal{F}(\eta(X, \mathfrak{V}))$ and $\mathcal{F}(P_k(\eta))$ are isomorphisms too. The diagram fig. 3.1 remains commutative when $\mathcal{F}$ is applied to all the algebras and all the mappings there.

Let $U = A \times B$, τ_1 the decomposition homomorphism of $U(X, \mathfrak{V})$ and τ_2 the decomposition homomorphism of $P_k(U)$. Then

$$\mathcal{F}(\tau_1) : \mathcal{F}(U(X, \mathfrak{V})) \to \mathcal{F}(A(X, \mathfrak{V}) \times B(X, \mathfrak{V})),$$
$$\mathcal{F}(\tau_2) : \mathcal{F}(P_k(U)) \to \mathcal{F}(P_k(A) \times P_k(B))$$

are composition homomorphisms. By Lemma 11.13, there are isomorphisms

$$\psi_1 : \mathcal{F}(A(X, \mathfrak{V}) \times B(X, \mathfrak{V})) \to \mathcal{F}(A(X, \mathfrak{V})) \times \mathcal{F}(B(X, \mathfrak{V})),$$
$$\psi_2 : \mathcal{F}(P_k(A) \times P_k(B)) \to \mathcal{F}(P_k(A)) \times \mathcal{F}(P_k(B)),$$

hence

$$\psi_1\mathcal{F}(\tau_1) : \mathcal{F}(U(X, \mathfrak{V})) \to \mathcal{F}(A(X, \mathfrak{V})) \times \mathcal{F}(B(X, \mathfrak{V})),$$
$$\psi_2\mathcal{F}(\tau_2) : \mathcal{F}(P_k(U)) \to \mathcal{F}(P_k(A)) \times \mathcal{F}(P_k(B))$$

are homomorphisms. $\psi_1\mathcal{F}(\tau_1)$ and $\psi_2\mathcal{F}(\tau_2)$ are monomorphisms (epimorphisms, isomorphisms) if and only if τ_1 and τ_2, resp., are monomorphisms (epimorphisms, isomorphisms). Thus Prop. 3.53 and Th. 3.61 imply

11.31. Proposition. *The homomorphism* $\psi_2\mathcal{F}(\tau_2) : \mathcal{F}(P_k(A \times B)) \to \mathcal{F}(P_k(A)) \times \mathcal{F}(P_k(B))$ *is always a monomorphism. If* $\mathfrak{V}$ *is the variety of commutative rings with identity, then both the homomorphism*

$$\psi_1\mathcal{F}(\tau_1) : \mathcal{F}((A \times B)(X, \mathfrak{V})) \to \mathcal{F}(A(X, \mathfrak{V})) \times \mathcal{F}(B(X, \mathfrak{V}))$$

and $\psi_2\mathcal{F}(\tau_2) : \mathcal{F}(P_k(A \times B)) \to \mathcal{F}(P_k(A)) \times \mathcal{F}(P_k(B))$ *are isomorphisms.*

11.32. The diagram in fig. 3.2 yields another commutative diagram (fig. 3.3) if we apply $\mathcal{F}$ and define $\mathcal{F}(\sigma(A)) \times \mathcal{F}(\sigma(B))$ in the same way as $\sigma(A) \times \sigma(B)$ in § 3.42.

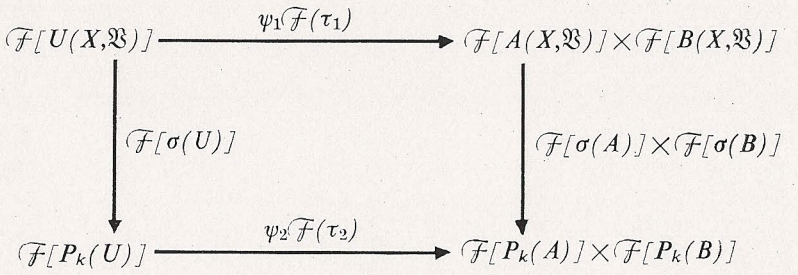


FIG. 3.3

11.4. Let $H = \langle H; \circ \rangle$ be a semigroup with identity, $\mathcal{E}(H)$ the subsemigroup of H consisting of the units of H—which is a group— and $\mathcal{R}(H)$ the subsemigroup of H consisting of the regular elements of H. Then $\mathcal{E}(H) \subseteq \mathcal{R}(H)$ while $\mathcal{E}(H) = \mathcal{R}(H)$ if and only if $\mathcal{R}(H)$ is a group. This is, in particular, the case if H is finite.

Let A be an algebra of $\mathfrak{V}$ and $X = \{x_1, \ldots, x_k\}$. If $\circ$ is the operation introduced in § 11.1, we observe that $\langle \mathcal{F}(F_k(A)); \circ \rangle$, $\langle \mathcal{F}(P_k(A)); \circ \rangle$, and $\langle \mathcal{F}(A(X, \mathfrak{V})); \circ \rangle$ are semigroups. Since $F_k(A)$, $P_k(A)$, and $A(X, \mathfrak{V})$ have a selector system each, these semigroups have identities, by Th. 11.11. In order to simplify our notation, we will write $\mathcal{E}(\ldots)$ for $\mathcal{E}(\mathcal{F}(\ldots))$ and $\mathcal{R}(\ldots)$ for $\mathcal{R}(\mathcal{F}(\ldots))$.

11.41. Lemma. *Let φ be the isomorphism of Lemma* 11.21. *Then $\varphi\mathcal{E}(F_k(A)) = \varphi\mathcal{R}(F_k(A)) = \mathrm{Sym}\,(A^k)$, the symmetric group over the elements of A^k. In particular, $\mathcal{E}(F_k(A)) = \mathcal{R}(F_k(A))$.*

Proof. Every element of $\mathrm{Sym}\,(A^k)$ has an inverse in $F_1(A^k)$. Furthermore, every element of $\varphi\mathcal{R}(F_k(A))$ is a regular element of $F_1(A^k)$ and thus a permutation of A^k. Hence $\mathrm{Sym}\,(A^k) \subseteq \varphi\mathcal{E}(F_k(A)) \subseteq \varphi\mathcal{R}(F_k(A)) \subseteq \mathrm{Sym}\,(A^k)$ which proves the lemma.

11.42. We set $\mathcal{F}(P_k(A)) \cap \varphi^{-1}\,\mathrm{Sym}\,(A^k) = \mathcal{S}(P_k(A))$. This is a subsemigroup of $\mathcal{F}(P_k(A))$ as follows from

11.43. Lemma. *$\mathcal{E}(P_k(A)) \subseteq \mathcal{S}(P_k(A)) \subseteq \mathcal{R}(P_k(A))$. If A is finite, then equality holds.*

Proof. We have $\mathcal{E}(P_k(A)) \subseteq \mathcal{F}(P_k(A))$ and $\mathcal{E}(P_k(A)) \subseteq \mathcal{E}(F_k(A)) = \varphi^{-1}\,\mathrm{Sym}\,(A^k)$. Furthermore, $\mathcal{S}(P_k(A)) = \varphi^{-1}\,\mathrm{Sym}\,(A^k) \cap \mathcal{F}(P_k(A)) = \mathcal{R}(F_k(A)) \cap \mathcal{F}(P_k(A)) \subseteq \mathcal{R}(P_k(A))$. If A is finite, then also $\mathcal{F}(P_k(A))$ is finite, thus $\mathcal{E}(P_k(A)) = \mathcal{R}(P_k(A))$.

11.44. Remark. In general, the inclusions in Lemma 11.43 are proper. We give examples. Let $k = 1$, and A the field of real numbers regarded as a commutative ring with identity. Then the element $\xi_1^3 \in P_1(A)$ is not in $\mathcal{E}(P_1(A))$ but certainly in $\mathcal{S}(P_1(A))$. For the second proper inclusion we get an example by taking $k = 1$ and, for A, the infinite cyclic group. Then $\xi_1^2 \notin \mathcal{S}(P_1(A))$, yet $\xi_1^2 \in \mathcal{R}(P_1(A))$.

11.45. Let $\sigma : A(X, \mathfrak{V}) \to P_k(A)$ be the canonical epimorphism and M a subset of $\mathcal{F}(P_k(A))$. As usual $\mathcal{F}(\sigma)^{-1}M$ denotes the set of all $\mathfrak{g} \in \mathcal{F}(A(X, \mathfrak{V}))$ such that $\mathcal{F}(\sigma)\mathfrak{g} \in M$. Lemma 11.43 implies

$$\mathcal{E}(A(X, \mathfrak{V})) \subseteq \mathcal{F}(\sigma)^{-1}\mathcal{E}(P_k(A)) \subseteq \mathcal{F}(\sigma)^{-1}\mathcal{S}(P_k(A)) \subseteq \mathcal{F}(\sigma)^{-1}\mathcal{R}(P_k(A)).$$

If $\boldsymbol{A}$ is finite, then both the second and third inclusion becomes an equality.

By definition, $\mathcal{S}(P_k(A))$ consists of all polynomial function vectors $\mathfrak{f} \in \mathcal{F}(P_k(A))$ such that $\varphi\mathfrak{f}$ is a permutation of A^k. These vectors will therefore be called polynomial permutations while the elements of $\mathcal{F}(\sigma)^{-1}\mathcal{S}(P_k(A))$ are named permutation polynomial vectors. For the sake of convenience, we abbreviate $\langle \mathcal{F}(P_k(A)); \circ \rangle = V_k(A)$ and $\langle \mathcal{S}(P_k(A)); \circ \rangle = U_k(A)$.

11.5. Let A, B be algebras of $\mathfrak{V}$ and $\eta : A \to B$ an epimorphism. As stated in § 11.3, $\mathcal{F}(P_k(\eta)) : V_k(A) \to V_k(B)$ is an epimorphism which we will also denote by $V_k(\eta)$. The question arises whether, for $\mathcal{C} = \mathcal{E}, \mathcal{S}, \mathcal{R}$, there is any relation between the subsemigroups $V_k(\eta)\mathcal{C}(P_k(A))$ and $\mathcal{C}(P_k(B))$ of $V_k(B)$. A preliminary answer is given by

11.51. Proposition. *$V_k(\eta)\,\mathcal{E}(P_k(A)) \subseteq \mathcal{E}(P_k(B))$. If B is finite, then $V_k(\eta)U_k(A) \subseteq U_k(B)$. If η is an isomorphism, then $V_k(\eta)$ maps $\mathcal{C}(P_k(A))$ isomorphically onto $\mathcal{C}(P_k(B))$, for $\mathcal{C} = \mathcal{E}, \mathcal{S}, \mathcal{R}$.*

Proof. The first assertion is evident. Also, if η is an isomorphism, then the third assertion is true for $\mathcal{C} = \mathcal{E}$ and $\mathcal{R}$. Let $\mathfrak{f} \in \mathcal{S}(P_k(A)) = U_k(A)$, then $\varphi\mathfrak{f} \in \mathrm{Sym}\,(A^k)$. Thus, for any $(u_1, \ldots, u_k) \in A^k$, there exists $(z_1, \ldots, z_k) \in A^k$ such that $\mathfrak{f} \circ (z_1, \ldots, z_k) = (u_1, \ldots, u_k)$. Hence, by definition of $V_k(\eta)$, $(V_k(\eta)\mathfrak{f}) \circ (\eta z_1, \ldots, \eta z_k) = (\eta u_1, \ldots, \eta u_k)$ whence $\varphi V_k(\eta)\mathfrak{f} : B^k \to B^k$ is surjective and is also injective if B is finite or η is an isomorphism. This proves the second assertion as well as the third assertion for $\mathcal{C} = \mathcal{S}$.

11.52. Remark. We shall see later on that, for various classes of algebras, $V_k(\eta)\,U_k(A) = U_k(B)$ always holds, if A is a finite algebra of such a class.

11.53. Remark. We have already seen that diagram fig. 3.1 remains commutative after applying $\mathcal{F}$ to it. As a consequence, we get that, for $\mathcal{C} = \mathcal{E}, \mathcal{S}, \mathcal{R}$, the inclusion $\mathcal{F}(\eta(X, \mathfrak{V}))\mathcal{F}(\sigma(A))^{-1}\mathcal{C}(P_k(A)) \subseteq \mathcal{F}(\sigma(B))^{-1}\mathcal{C}(P_k(B))$ holds if and only if $V_k(\eta)\mathcal{C}(P_k(A)) \subseteq \mathcal{C}(P_k(B))$. Hence if η is an isomorphism, then $\mathcal{F}(\eta(X, \mathfrak{V}))$ maps $\mathcal{F}(\sigma(A))^{-1}\mathcal{C}(P_k(A))$ isomorphically onto $\mathcal{F}(\sigma(B))^{-1}\mathcal{C}(P_k(B))$. Moreover, $\mathcal{F}(\eta(X, \mathfrak{V}))\mathcal{F}(\sigma(A))^{-1}\mathcal{C}(P_k(A)) = \mathcal{F}(\sigma(B))^{-1}\mathcal{C}(P_k(B))$ implies $V_k(\eta)\,\mathcal{C}(P_k(A)) = \mathcal{C}(P_k(B))$—however, the converse does not hold in general.

11.6. Let A, B be algebras of $\mathfrak{V}$, $U = A \times B$, and τ_2 the decomposition homomorphism of $P_k(U)$. Then, by Prop. 11.31, $\psi_2\mathcal{F}(\tau_2) : V_k(U) \to V_k(A) \times V_k(B)$ is a monomorphism. Again we may ask how $\mathcal{C}(P_k(U))$, $\mathcal{C} = \mathcal{E}, \mathcal{S}, \mathcal{R}$, behaves under $\psi_2\mathcal{F}(\tau_2)$.

11.61. Proposition. *For $\mathcal{C} = \mathcal{E}, \mathcal{S}$ and arbitrary U, the monomorphism $\psi_2\mathcal{F}(\tau_2)$ maps $\mathcal{C}(P_k(U))$ into $\mathcal{C}(P_k(A))\times\mathcal{C}(P_k(B))$.*

Proof. Since $\psi_2\mathcal{F}(\tau_2)(\xi_1, \ldots, \xi_k) = \psi_2(\tau_2\xi_1, \ldots, \tau_2\xi_k) = ((\xi_1, \ldots, \xi_k), (\xi_1, \ldots, \xi_k))$, i.e. $\psi_2\mathcal{F}(\tau_2)$ maps the identity of $V_k(U)$ onto the identity of $V_k(A)\times V_k(B)$, the assertion is proved for $\mathcal{C} = \mathcal{E}$. For $\mathcal{C} = \mathcal{S}$, we require the following

11.62. Lemma. *For any $\mathfrak{f} \in V_k(U)$ and any $((a_1, b_1), \ldots, (a_k, b_k)) \in U^k$, we have $\mathfrak{f} \circ ((a_1, b_1), \ldots, (a_k, b_k)) = ((u_1, v_1), \ldots, (u_k, v_k))$ if and only if $V_k(\pi_1)\mathfrak{f} \circ (a_1, \ldots, a_k) = (u_1, \ldots, u_k)$ and $V_k(\pi_2)\mathfrak{f} \circ (b_1, \ldots, b_k) = (v_1, \ldots, v_k)$ where π_1, π_2 are the projections from U to A and B, resp.*

Proof. Let $\mathfrak{f} = (\varphi_1, \ldots, \varphi_k)$, then

$$\mathfrak{f} \circ ((a_1, b_1), \ldots, (a_k, b_k)) =$$
$$= [(P_k(\pi_1)\varphi_1 \circ (a_1, \ldots, a_k), P_k(\pi_2)\varphi_1 \circ (b_1, \ldots, b_k)), \ldots,$$
$$(P_k(\pi_1)\varphi_k \circ (a_1, \ldots, a_k), P_k(\pi_2)\varphi_k \circ (b_1, \ldots, b_k))]$$

which proves the lemma.

By definition, for any algebra C, we have $\mathfrak{f} \in \mathcal{S}(P_k(C))$ if and only if, for any $(w_1, \ldots, w_k) \in C^k$, the equation $\mathfrak{f} \circ (c_1, \ldots, c_k) = (w_1, \ldots, w_k)$ has exactly one solution $(c_1, \ldots, c_k)$. By Lemma 11.62, $\mathfrak{f} \in \mathcal{S}(P_k(U))$ if and only if $V_k(\pi_1)\mathfrak{f} \in \mathcal{S}(P_k(A))$ and $V_k(\pi_2)\mathfrak{f} \in \mathcal{S}(P_k(B))$. Since $\psi_2\mathcal{F}(\tau_2)\mathfrak{f} = (V_k(\pi_1)\mathfrak{f}, V_k(\pi_2)\mathfrak{f})$, the proof of the proposition is completed.

11.63. Corollary. *The monomorphism $\psi_2\mathcal{F}(\tau_2)$ maps $U_k(U)$ onto $(U_k(A)\times U_k(B)) \cap \psi_2\mathcal{F}(\tau_2)V_k(U)$.*

Proof. This is an immediate consequence of the preceding proof.

11.64. Proposition. *If the monomorphism $\psi_2\mathcal{F}(\tau_2)$ is an isomorphism, then $\psi_2\mathcal{F}(\tau_2)$ maps $\mathcal{C}(P_k(U))$ onto $\mathcal{C}(P_k(A))\times\mathcal{C}(P_k(B))$, for $\mathcal{C} = \mathcal{E}, \mathcal{S}, \mathcal{R}$.*

Proof. For $\mathcal{C} = \mathcal{S}$, this follows from Cor. 11.63. If $\mathcal{C} = \mathcal{E}$ or $\mathcal{R}$, then we use the general fact that for a direct product of semigroups with identity $H = L\times M$ we always have $\mathcal{E}(H) = \mathcal{E}(L)\times\mathcal{E}(M)$ and $\mathcal{R}(H) = \mathcal{R}(L)\times\mathcal{R}(M)$.

11.65. Remark. Proposition 11.61 and diagram fig. 3.3 show that, for $\mathcal{C} = \mathcal{E}, \mathcal{S}$, the homomorphism $\psi_1\mathcal{F}(\tau_1)$ maps $\mathcal{F}(\sigma(U))^{-1}\mathcal{C}(P_k(U))$ into

$\mathcal{F}(\sigma(A))^{-1}\mathcal{C}(P_k(A))\times\mathcal{F}(\sigma(B))^{-1}\mathcal{C}(P_k(B))$. Together with Prop. 11.64, diagram fig. 3.3 also shows that if $\psi_1\mathcal{F}(\tau_1)$ is an epimorphism, then, for $\mathcal{C} = \mathcal{E}, \mathcal{S}, \mathcal{R}$, it maps $\mathcal{F}(\sigma(U))^{-1}\mathcal{C}(P_k(U))$ onto $\mathcal{F}(\sigma(A))^{-1}\mathcal{C}(P_k(A))\times\mathcal{F}(\sigma(B))^{-1}\mathcal{C}(P_k(B))$. Prop. 11.31 and Prop. 11.64 then imply

11.66. Proposition. *If $\mathfrak{V}$ is the variety of commutative rings with identity, then for $\mathcal{C} = \mathcal{E}, \mathcal{S}, \mathcal{R}$, the homomorphism $\psi_1\mathcal{F}(\tau_1)$ maps $\mathcal{F}(\sigma(U))^{-1}\mathcal{C}(P_k(U))$ isomorphically onto $\mathcal{F}(\sigma(A))^{-1}\mathcal{C}(P_k(A))\times\mathcal{F}(\sigma(B))^{-1}\mathcal{C}(P_k(B))$ and $\psi_2\mathcal{F}(\tau_2)$ maps $\mathcal{C}(P_k(U))$ isomorphically onto $\mathcal{C}(P_k(A))\times\mathcal{C}(P_k(B))$.*

12. Permutation polynomials and polynomial permutations

12.1. Let C be any algebra of the variety $\mathfrak{V}_k$ of k-dimensional $\mathfrak{V}$-composition algebras and S a subsemigroup of the semigroup $\langle\mathcal{F}(C); \circ\rangle$. An element $f \in C$ is called a "part of S" if there is an element $(f_1, \ldots, f_k) \in S$ such that $f = f_i$, for some $i = 1, \ldots, k$. The set of all parts of S will be denoted by $\mathcal{P}(S)$. Thus $\mathcal{P}(S)$ is a subset of C.

12.11. Lemma. *$\mathcal{P}$ has the following properties:*

a) *If $S \subseteq T$, then $\mathcal{P}(S) \subseteq \mathcal{P}(T)$.*

b) *If $\varrho : C \to D$ is any homomorphism, then $\varrho\mathcal{P}(S) = \mathcal{P}(\mathcal{F}(\varrho)S)$.*

c) *If $\varrho : B \to C$ is any epimorphism, then $\varrho^{-1}\mathcal{P}(S) = \mathcal{P}(\mathcal{F}(\varrho)^{-1}S)$.*

Proof. a) is obvious. Let $f \in \varrho\mathcal{P}(S)$, then there exists an element $(t_1, \ldots, t_k) \in S$ such that $f = \varrho t_i$, for some $i = 1, \ldots, k$, hence $f \in \mathcal{P}(\mathcal{F}(\varrho)S)$. This argument also works vice versa. Let $f \in \varrho^{-1}\mathcal{P}(S)$, i.e. $\varrho f \in \mathcal{P}(S)$, hence there exists an element of the form $(t_1, \ldots, \varrho f, \ldots, t_k) \in S$ and thus some $(u_1, \ldots, f, \ldots, u_k) \in \mathcal{F}(\varrho)^{-1}S$ whence $f \in \mathcal{P}(\mathcal{F}(\varrho)^{-1}S)$. Again the argument can be reversed.

12.12. Lemma. *If C contains a selector system $\{s_1, \ldots, s_k\}$ and if, for every permutation π of $(s_1, \ldots, s_k)$, the k-tuple $(\pi s_1, \ldots, \pi s_k)$ is in S, then f is a part of S if and only if there exist elements $f_2, \ldots, f_k \in C$ such that $(f, f_2, \ldots, f_k) \in S$.*

Proof. Straightforward.

12.2. We are going to apply the results of the preceding subsections to the case where $C = F_k(A)$, $P_k(A)$, and $A(X, \mathfrak{V})$, $X = \{x_1, \ldots, x_k\}$.

First of all let $C = F_k(A)$. The subset $\mathcal{P}(\mathcal{E}(F_k(A)))$ of $F_k(A)$ is called the set of permutation functions. Since, in this case, the hypothesis of Lemma 12.12 is satisfied, we conclude that $\varrho \in F_k(A)$ is a permutation function if and only if there exist functions $\varrho_2, \ldots, \varrho_k \in F_k(A)$ such that, for $\mathfrak{f} = (\varrho, \varrho_2, \ldots, \varrho_k)$, the mapping $\varphi\mathfrak{f}$ is a permutation of A^k. There is also another characterization of permutation functions, namely

12.21. Proposition. *A function $\varrho \in F_k(A)$ is a permutation function if and only if, for any $u \in A$, the set of all solutions in A of the equation $\varrho(x_1, \ldots, x_k) = u$ has cardinality $|A|^{k-1}$.*

Proof. Let $\varrho \in \mathcal{P}(\mathcal{E}(F_k(A)))$. Then there exist functions $\varrho_2, \ldots, \varrho_k \in F_k(A)$ such that, for any $(u, b_2, \ldots, b_k) \in A^k$, the system of equations $\varrho(x_1, \ldots, x_k) = u$, $\varrho_2(x_1, \ldots, x_k) = b_2, \ldots, \varrho_k(x_1, \ldots, x_k) = b_k$ has one and only one solution. Hence we can map the set of solutions of $\varrho(x_1, \ldots, x_k) = u$ bijectively onto the set of all elements $(u, b_2, \ldots, b_k) \in A^k$ which has cardinality $|A|^{k-1}$. Conversely let $M(u)$ be the set of all solutions of $\varrho(x_1, \ldots, x_k) = u$, for any $u \in A$ and suppose that $|M(u)| = |A|^{k-1}$. Then we can choose bijections $\psi_u : M(u) \to A^{k-1}$, for each $u \in A$, e.g. $\psi_u(a_1, \ldots, a_k) = (\varrho_2(a_1, \ldots, a_k), \ldots, \varrho_k(a_1, \ldots, a_k))$, where $\varrho_i \in F_k(A)$, $i = 2, \ldots, k$. Taking $\mathfrak{f} = (\varrho, \varrho_2, \ldots, \varrho_k)$, we find that $\varphi\mathfrak{f}$ is a permutation of A^k whence ϱ is a permutation function.

12.22. The elements of $S_k(A) = P_k(A) \cap \mathcal{P}(\mathcal{E}(F_k(A)))$, i.e. the set of polynomial functions which are also permutation functions, will be called permutation polynomial functions while, if $\sigma : A(X, \mathfrak{V}) \to P_k(A)$ is the canonical epimorphism, the elements of $\sigma^{-1}S_k(A)$ are called permutation polynomials. In other words, a permutation polynomial is a polynomial which "induces" a permutation function.

The next case we consider is where $C = P_k(A)$. Applying $\mathcal{P}$ to $\mathcal{E}(P_k(A))$, $\mathcal{S}(P_k(A))$, and $\mathcal{R}(P_k(A))$, we can again use Lemma 12.12 for testing elements of $P_k(A)$ whether or not they belong to one of these semigroups. As a consequence of Lemma 12.11, we obtain $\mathcal{P}(\mathcal{E}(P_k(A))) \subseteq \mathcal{P}(\mathcal{S}(P_k(A))) \subseteq \mathcal{P}(\mathcal{R}(P_k(A)))$. The elements of $\mathcal{P}(\mathcal{S}(P_k(A))) = SS_k(A)$ will be called strict permutation polynomial functions while the elements of $\sigma^{-1}SS_k(A)$ will be called strict permutation polynomials. This means that a polynomial function ψ is a strict permutation polynomial function if and only if there exist functions $\psi_2, \ldots, \psi_k \in P_k(A)$ such that, for $\mathfrak{f} = (\psi, \psi_2, \ldots, \psi_k)$, the mapping $\varphi\mathfrak{f}$ is a permutation of A^k while a strict permutation polynomial is a polynomial which "induces" a strict permutation polynomial function.

$S_k(A) \subseteq SS_k(A)$

12.23. Proposition. *Any strict permutation polynomial function is also a permutation polynomial function and any strict permutation polynomial is also a permutation polynomial. If $k = 1$ or the algebra A is polynomially complete, then also the converse holds.*

Proof. Evident.

12.3. Proposition. *Let A, B be algebras of $\mathfrak{V}$ and $\eta : A \to B$ an epimorphism. Then $P_k(\eta)\,\mathcal{P}(\mathcal{E}(P_k(A))) \subseteq \mathcal{P}(\mathcal{E}(P_k(B)))$. If $V_k(\eta)\,U_k(A) \subseteq U_k(B)$, then $P_k(\eta)\,SS_k(A) \subseteq SS_k(B)$, and if $V_k(\eta)\,U_k(A) = U_k(B)$, then $P_k(\eta)\,SS_k(A) = SS_k(B)$. If η is an isomorphism, then $P_k(\eta)$ maps $SS_k(A)$ bijectively onto $SS_k(B)$.*

Proof. This is a straightforward consequence of Prop. 11.51 in connection with Lemma 12.11.

12.31. Proposition. *Let A, B, η be as in Prop. 12.3. If A is finite and every congruence class of Ker η has one and the same order, then $P_k(\eta)\,S_k(A) \subseteq S_k(B)$. If η is an isomorphism, then $P_k(\eta)$ maps, in any case, $S_k(A)$ bijectively onto $S_k(B)$.*

Proof. If η is an isomorphism, then, by Prop. 3.31, $P_k(\eta)$ is also an isomorphism. $\varrho \in S_k(A)$ means that $\varrho \in P_k(A)$ and the equation $\varrho(x_1, \ldots, x_k) = u$ has a solution set of cardinality $|A|^{k-1}$, for all $u \in A$, by Prop. 12.21. Hence the equation $P_k(\eta)\,\varrho(x_1, \ldots, x_k) = \eta u$ has a solution set of cardinality $|A|^{k-1} = |B|^{k-1}$ whence $P_k(\eta)\varrho \in S_k(B)$, by Prop. 12.21 and the second assertion is proved.

Assume now that the hypothesis of the first assertion holds. Let $\varrho \in S_k(A)$, then again $\varrho \in P_k(A)$ and $\varrho(x_1, \ldots, x_k) = u$ has a solution set in A of cardinality $|A|^{k-1}$, for all $u \in A$. Let $v \in B$ and M the solution set for this equation where u runs through all elements of A such that $\eta u = v$. Let N be the set of solutions in B of the equation

$(P_k(\eta)\varrho)(x_1, \ldots, x_k) = v$, then the mapping $\eta^k : A^k \to B^k$, $\eta^k(z_1, \ldots, z_k) = (\eta z_1, \ldots, \eta z_k)$ maps M onto N. For any two elements $(z_1, \ldots, z_k)$, $(t_1, \ldots, t_k) \in A^k$, we have $(\eta z_1, \ldots, \eta z_k) = (\eta t_1, \ldots, \eta t_k)$ if and only if z_i (Ker η) t_i, $i = 1, \ldots, k$. By hypothesis, every congruence class of Ker η has cardinality $|A|/|B|$, hence every element of N is the image of exactly $(|A|/|B|)^k$ elements of A^k under η^k, and all these elements are in M. But $|M| = (|A|/|B|)\,|A|^{k-1}$, hence $|N|\,(|A|/|B|)^k = |A|^k/|B|$. Therefore $|N| = |B|^{k-1}$ and, by Prop. 12.21, $P_k(\eta)\varrho \in S_k(B)$.

12.32. Remark. Proposition 12.31 applies, in particular, to finite multi-operator groups and hence to finite rings and finite groups.

12.33. Remark. Let A, B, η be as in Prop. 12.3. Diagram fig. 3.1 shows that, for $T = SS_k$ and $T = S_k$, we have $\eta(X, \mathfrak{V})\,\sigma(A)^{-1}T(A) \subseteq \sigma(B)^{-1}T(B)$ if and only if $P_k(\eta)\,T(A) \subseteq T(B)$, and that, for η being an isomorphism, $\eta(X, \mathfrak{V})$ maps $\sigma(A)^{-1}T(A)$ bijectively onto $\sigma(B)^{-1}T(B)$.

12.4. Proposition. *Let A, B be algebras of $\mathfrak{V}$, $U = A \times B$, and τ_2 the decomposition homomorphism of $P_k(U)$. Then $\tau_2\mathcal{P}\big(\mathcal{E}(P_k(U))\big) \subseteq \mathcal{P}\big(\mathcal{E}(P_k(A))\big) \times \mathcal{P}\big(\mathcal{E}(P_k(B))\big)$ and $\tau_2 SS_k(U) \subseteq SS_k(A) \times SS_k(B)$. If τ_2 is an isomorphism, then τ_2 maps $\mathcal{P}\big(\mathcal{E}(P_k(U))\big)$ bijectively onto $\mathcal{P}\big(\mathcal{E}(P_k(A))\big) \times \mathcal{P}\big(\mathcal{E}(P_k(B))\big)$ and also $SS_k(U)$ bijectively onto $SS_k(A) \times SS_k(B)$.*

Proof. Let $\mathcal{C} = \mathcal{E}$ or $\mathcal{S}$. In Lemma 12.11 b), put $\varrho = \tau_2$, $C = P_k(U)$, and $D = P_k(A) \times P_k(B)$. Then, by Lemma 12.11 a) and Prop. 11.61, we get

$$\tau_2\mathcal{P}\big(\mathcal{C}(P_k(U))\big) = \mathcal{P}\big(\mathcal{F}(\tau_2)\,\mathcal{C}(P_k(U))\big) \subseteq \mathcal{P}\big(\psi_2^{-1}\big(\mathcal{C}(P_k(A)) \times \mathcal{C}(P_k(B))\big)\big).$$

In the case that τ_2 is an isomorphism, by Prop. 11.64, equality holds. But

$$\mathcal{P}\big(\psi_2^{-1}\big(\mathcal{C}(P_k(A)) \times \mathcal{C}(P_k(B))\big)\big) = \mathcal{P}\big(\mathcal{C}(P_k(A))\big) \times \mathcal{P}\big(\mathcal{C}(P_k(B))\big),$$

by definition of ψ_2 and the applicability of Lemma 12.12 to $\mathcal{C}(P_k(A))$ and $\mathcal{C}(P_k(B))$.

12.41. Proposition. *Let A, B be finite and $U = A \times B$. Then $\tau_2 S_k(U) \subseteq S_k(A) \times S_k(B)$, and if τ_2 is an isomorphism, then τ_2 maps $S_k(U)$ bijectively onto $S_k(A) \times S_k(B)$.*

Proof. Let π_i, $i = 1, 2$, be the projections of U. Then $\tau_2\varrho = (P_k(\pi_1)\varrho,\ P_k(\pi_2)\varrho)$, $\varrho \in P_k(U)$. Both U and π_i, $i = 1, 2$, satisfy the

hypothesis of Prop. 12.31, hence $\tau_2 S_k(U) \subseteq S_k(A) \times S_k(B)$. If τ_2 is an isomorphism and $(\varrho, \psi) \in S_k(A) \times S_k(B)$, then there exists an element $\chi \in P_k(U)$ such that $\tau_2\chi = (\varrho, \psi)$. Let $(a_i, b_i) \in U$, then $\chi((a_1, b_1), \ldots, (a_k, b_k)) = \big(P_k(\pi_1)\,\chi(a_1, \ldots, a_k),\ P_k(\pi_2)\,\chi(b_1, \ldots, b_k)\big) = \big(\varrho(a_1, \ldots, a_k), \psi(b_1, \ldots, b_k)\big)$. Hence, for any $(u, v) \in U$, the set of solutions in U of the equation $\chi(x_1, \ldots, x_k) = (u, v)$ has order $|A|^{k-1}\,|B|^{k-1} = |U|^{k-1}$ whence $\chi \in S_k(U)$, by Prop. 12.21, and the proof is completed.

12.42. Remark. Diagram fig. 3.2 implies that, for $T = SS_k$ and $T = S_k$, we have $\tau_1\sigma(U)^{-1}T(U) \subseteq \sigma(A)^{-1}T(A) \times \sigma(B)^{-1}T(B)$ if and only if $\tau_2 T(U) \subseteq T(A) \times T(B)$. If the latter condition holds and τ_1 is an epimorphism, then the first inclusion becomes an equality. This consideration together with Th. 3.61, Prop. 12.4, and Prop. 12.41 yields

12.43. Proposition. *If $\mathfrak{V}$ is the variety of commutative rings with identity and $U = A \times B$ in $\mathfrak{V}$, then τ_2 maps $SS_k(U)$ bijectively onto $SS_k(A) \times SS_k(B)$ while τ_1 maps $\sigma(U)^{-1}SS_k(U)$ bijectively onto $\sigma(A)^{-1}SS_k(A) \times \sigma(B)^{-1}SS_k(B)$. If, moreover, U is finite, an analogous result holds for S_k instead of SS_k.*

13. Subsemigroups defined by parametric words

13.1. Let $X = \{x_1, \ldots, x_k\}$ and A an algebra of the variety $\mathfrak{V}$. Then $\big\langle \mathcal{F}(A(X, \mathfrak{V})); \circ \big\rangle = C_k(A)$ is a semigroup of polynomial vectors. In order to stick to consistent notation, we will write $C_k(\eta)$ for $\mathcal{F}(\eta(X, \mathfrak{V}))$ where $\eta : A \to B$ is a homomorphism. In $C_k(A)$ we want to single out various special types of subsemigroups such as the set of all polynomial vectors x^l in $C_1(A)$ where A is a group and l runs through the integers, or the set of all polynomial vectors over a commutative ring A with identity where all the components are of degree 1. This section is devoted to the investigation of such subsemigroups. In order to be able to state our problems we give a few rather general definitions. Let $\mathcal{L}_0$ be a mapping which assigns, to each algebra A of $\mathfrak{V}$, a subsemigroup $\mathcal{L}_0(A)$ of $C_k(A)$. Then $\mathcal{L}_1 = \mathcal{F}(\sigma)\,\mathcal{L}_0$, $\sigma : A(X, \mathfrak{V}) \to P_k(A)$ being the canonical epimorphism, assigns a subsemigroup $\mathcal{L}_1(A)$ of $V_k(A)$ to each $A \in \mathfrak{V}$. We define $\mathcal{L}_2(A) = \mathcal{L}_0(A) \cap \mathcal{F}(\sigma)^{-1}U_k(A)$ which is either empty or a subsemigroup of $\mathcal{F}(\sigma)^{-1}U_k(A)$, then $\mathcal{L}_3 = \mathcal{F}(\sigma)\mathcal{L}_2$ assigns a subsemigroup of $U_k(A)$ or the empty set to each A of $\mathfrak{V}$. We get immediately $\mathcal{L}_3(A) = \mathcal{L}_1(A) \cap U_k(A)$. We cannot expect many results under these general conditions. Thus we

make an assumption. We say that $\mathcal{L}_0$ has property H_1 if $C_k(\eta)\,\mathcal{L}_0(A) = \mathcal{L}_0(B)$, for any two algebras A, B of $\mathfrak{V}$ and any epimorphism $\eta: A \to B$. Methods for the construction of such mappings $\mathcal{L}_0$ with property H_1 will be elaborated in §§ 13.2 and 13.3.

13.11. Lemma. *If $\mathcal{L}_0$ has property H_1, then:*

a) $V_k(\eta)\,\mathcal{L}_1(A) = \mathcal{L}_1(B)$;

b) $V_k(\eta)\,U_k(A) \subseteq U_k(B)$ *implies* $V_k(\eta)\,\mathcal{L}_3(A) \subseteq \mathcal{L}_3(B)$;

c) $C_k(\eta)\,\mathcal{L}_2(A) \subseteq \mathcal{L}_2(B)$ *if and only if* $V_k(\eta)\,\mathcal{L}_3(A) \subseteq \mathcal{L}_3(B)$.

Proof. a) follows from the definitions and diagram fig. 3.1, b) follows from $\mathcal{L}_3(A) = \mathcal{L}_1(A) \cap U_k(A)$ and a). c) The "only if" part follows from diagram fig. 3.1. Conversely let $V_k(\eta)\,\mathcal{L}_3(A) \subseteq \mathcal{L}_3(B)$, then $\mathcal{F}(\sigma(B))\,C_k(\eta)\,\mathcal{L}_2(A) \subseteq \mathcal{L}_1(B) \cap U_k(B)$, by diagram fig. 3.1, hence $C_k(\eta)\,\mathcal{L}_2(A) \subseteq \mathcal{L}_0(B) \cap \mathcal{F}(\sigma(B))^{-1}\,U_k(B) = \mathcal{L}_2(B)$.

13.12. Lemma. *Let $U = A \times B$ an algebra of $\mathfrak{V}$ and τ_1, τ_2 the decomposition homomorphisms of $U(X, \mathfrak{V})$ and $P_k(U)$, respectively. If $\mathcal{L}_0$ has property H_1, then $\psi_1\mathcal{F}(\tau_1)$ maps $\mathcal{L}_i(U)$ into $\mathcal{L}_i(A) \times \mathcal{L}_i(B)$, for $i = 0, 2$, and $\psi_2\mathcal{F}(\tau_2)$ maps $\mathcal{L}_i(U)$ into $\mathcal{L}_i(A) \times \mathcal{L}_i(B)$, for $i = 1, 3$.*

Proof. Let π_i, $i = 1, 2$, be the projections of U. Then $\psi_1\mathcal{F}(\tau_1)\mathfrak{f} = (C_k(\pi_1)\mathfrak{f}, C_k(\pi_2)\mathfrak{f})$ whence the lemma follows for $i = 0$. Similarly, with the aid of Lemma 13.11 a), we obtain the result for $i = 1$. By Prop. 11.61, $\psi_2\mathcal{F}(\tau_2)$ maps $U_k(U)$ into $U_k(A) \times U_k(B)$, hence, by Lemma 13.11 b), the lemma follows for $i = 3$, and finally for $i = 2$, by Lemma 13.11 c).

13.13. We define another property for $\mathcal{L}_0$: We say $\mathcal{L}_0$ has property H_2 if $\psi_1\mathcal{F}(\tau_1)$ maps $\mathcal{L}_0(U)$ onto $\mathcal{L}_0(A) \times \mathcal{L}_0(B)$. Again we postpone the construction of such mappings $\mathcal{L}_0$ to §§ 13.2 and 13.3.

13.14. Lemma. *If $\mathcal{L}_0$ has property H_2, then $\psi_1\mathcal{F}(\tau_1)$ induces an epimorphism, for $i = 0, 2$, and $\psi_2\mathcal{F}(\tau_2)$ induces an isomorphism, for $i = 1, 3$, from $\mathcal{L}_i(U)$ to $\mathcal{L}_i(A) \times \mathcal{L}_i(B)$.*

Proof. For $i = 0$, this is the hypothesis while, for $i = 1$, the lemma follows from diagram fig. 3.3 since $\psi_2\mathcal{F}(\tau_2)$ is injective, by Prop. 11.31. By Prop. 11.61, $\psi_2\mathcal{F}(\tau_2)$ maps $\mathcal{L}_3(U)$ into $\mathcal{L}_3(A) \times \mathcal{L}_3(B)$ and, by Cor. 11.63, this mapping is onto. For $i = 2$, the result is then again a consequence of diagram fig. 3.3.

13.2. We are now going to construct mappings $\mathcal{L}_0$ with property H_1, or properties H_1 and H_2. Some definitions will go ahead.

Let Ω be the family of operations of the variety $\mathfrak{V}$ and r a non-negative integer. A parametric word vector $\mathfrak{P}$ of order r is a mapping from the Cartesian product of r copies of the set of non-negative integers to the set of k-tuples of words over Ω in the indeterminates ${}_0w_i, {}_1w_i, \ldots, {}_kw_i$, $i = 1, 2, \ldots$ and $x_1, \ldots, x_k$, for $r > 0$, and a fixed k-tuple of this kind, for $r = 0$. A specialization vector of $\mathfrak{P}$ in the algebra $A \in \mathfrak{V}$ is a k-tuple of words in $A \cup \{x_1, \ldots, x_k\}$ we obtain from substituting an arbitrary word in $A \cup \{x_1, \ldots, x_r\}$ for each ${}_rw_i$ occurring in the k-tuple of words assigned by $\mathfrak{P}$ to each r-tuple of non-negative integers. In particular, we have to substitute an element of A for each ${}_0w_i$, and into a fixed k-tuple, if $r = 0$. The specialization $\mathfrak{P}(A)$ of $\mathfrak{P}$ in the algebra A is the set of all polynomial vectors of $\mathcal{F}(A(x_1, \ldots, x_k, \mathfrak{V}))$ which are represented by the specialization vectors of $\mathfrak{P}$ in A. Thus $\mathfrak{P}(A)$ is a subset of $C_k(A)$, for any A in $\mathfrak{V}$. The parametric word vector $\mathfrak{P}$ is called semigroup generating if $\mathfrak{P}(A)$ is a subsemigroup of $C_k(A)$, for every A in $\mathfrak{V}$.

Three examples will illustrate the concept of semigroup generating parametric word vectors. The first and second vector are of order 0 while the third one is of order k^2. It is easy to see that these parametric word vectors are, indeed, semigroup generating.

a) $\mathfrak{V}$ an arbitrary variety, $\mathfrak{P} = ({}_1w_1, {}_2w_1, \ldots, {}_kw_1)$.

b) $\mathfrak{V}$ the variety of commutative rings with identity,

$$\mathfrak{P} = ({}_0w_1x_1 + {}_0w_2,\ {}_1w_1x_2 + {}_1w_2,\ \ldots,\ {}_{k-1}w_1x_k + {}_{k-1}w_2).$$

c) $\mathfrak{V}$ the variety of commutative rings with identity, and $\mathfrak{P}$ mapping the k^2-tuple of non-negative integers $\mathfrak{k} = (n_{11}, \ldots, n_{1k}, n_{21}, \ldots, n_{kk})$ to the k-tuple of words

$$\mathfrak{P}(\mathfrak{k}) = ({}_0w_1x_1^{n_{11}}x_2^{n_{12}} \ldots x_k^{n_{1k}},\ {}_0w_2x_1^{n_{21}} \ldots x_k^{n_{2k}},\ \ldots,\ {}_0w_kx_1^{n_{k1}}x_2^{n_{k2}} \ldots x_k^{n_{kk}}).$$

13.3. Theorem. *If $\mathfrak{P}$ is a semigroup generating parametric word vector of arbitrary order, then the mapping $\mathcal{L}_0$ defined by $\mathcal{L}_0(A) = \mathfrak{P}(A)$ has property H_1.*

Proof. Let $\eta: A \to B$ be any epimorphism and $\mathfrak{f} \in \mathfrak{P}(A)$, then $\mathfrak{f}$ is represented by some specialization vector of $\mathfrak{P}$ in A. We obtain $C_k(\eta)\mathfrak{f}$ by replacing

each $a \in A$ in this specialization vector by $\eta a \in B$. Thus $C_k(\eta)\mathfrak{f}$ is represented by a specialization vector of $\mathfrak{P}$ in B, i.e. an element of $\mathfrak{P}(B)$ whence $C_k(\eta)\,\mathcal{L}_0(A) \subseteq \mathcal{L}_0(B)$. Conversely, if $\mathfrak{g} \in \mathfrak{P}(B)$, then $\mathfrak{g}$ is represented by some specialization vector of $\mathfrak{P}$ in B. If we replace each $b \in B$ in this vector by any inverse image $a \in A$ of b under η, we get a specialization vector of $\mathfrak{P}$ in A. This vector represents some $\mathfrak{f} \in \mathfrak{P}(A)$ and $C_k(\eta)\mathfrak{f} = \mathfrak{g}$ whence $\mathcal{L}_0(B) \subseteq C_k(\eta)\,\mathcal{L}_0(A)$. This completes the proof.

13.31. Theorem. *Suppose $\mathfrak{P}$ is a semigroup generating parametric word vector of order 0. Let $U = A \times B$ be a direct product of algebras of $\mathfrak{V}$ and assume that the decomposition homomorphism τ_1 of $U(x_1, \ldots, x_\nu, \mathfrak{V})$ is an epimorphism, for $\nu = 1, \ldots, k$. Then $\mathcal{L}_0 = \mathfrak{P}$ has property H_2.*

Proof. By Th. 13.3 and Lemma 13.12, $\psi_1\mathcal{F}(\tau_1)$ maps $\mathfrak{P}(U)$ into $\mathfrak{P}(A) \times \mathfrak{P}(B)$. Conversely, if $(\mathfrak{f}, \mathfrak{g}) \in \mathfrak{P}(A) \times \mathfrak{P}(B)$, then $\mathfrak{f}$ and $\mathfrak{g}$ are represented by specialization vectors of $\mathfrak{P}$ in A and B, resp. If ${}_\nu w_i$ occurs in $\mathfrak{P}$, let $u(a_j, x_1, \ldots, x_\nu)$, $v(b_j, x_1, \ldots, x_\nu)$ be the words which are substituted for ${}_\nu w_i$ in these specialization vectors. We choose $f \in U(x_1, \ldots, x_\nu, \mathfrak{V})$ such that $\tau_1 f \in A(x_1, \ldots, x_\nu, \mathfrak{V}) \times B(x_1, \ldots, x_\nu, \mathfrak{V})$ is just represented by the pair of these words and take a word ${}_\nu w_i(u_j, x_1, \ldots, x_\nu)$ in $U \cup \{x_1, \ldots, x_\nu\}$ representing f. If we subject every ${}_\nu w_i$ in $\mathfrak{P}$ to this procedure, we get a specialization vector of $\mathfrak{P}$ in U which represents some $\mathfrak{h} \in \mathfrak{P}(U)$ such that $\psi_1\mathcal{F}(\tau_1)\mathfrak{h} = (\mathfrak{f}, \mathfrak{g})$. This proves the theorem.

13.32. From Th. 3.61 we conclude that $\mathcal{L}_0 = \mathfrak{P}$ has property H_2 in the example a), b) of § 13.2 for $\mathfrak{V}$ being the variety of commutative rings with identity. Hence, in these cases, $\mathcal{L}_i(A \times B) \cong \mathcal{L}_i(A) \times \mathcal{L}_i(B)$, $i = 0, 1, 2, 3$.

13.4. Let $\mathfrak{V}$ be any variety. We want to construct new parametric word vectors from given ones. Let $\mathfrak{P}_1$, $\mathfrak{P}_2$ be parametric word vectors of the orders r and s, resp. We define a new parametric word vector of order $r+s$ by means of the following procedure:

Let $(m_1, \ldots, m_r, n_1, \ldots, n_s)$ be an $r+s$-tuple of non-negative integers and suppose that the images under $\mathfrak{P}_1$ contain the indeterminates ${}_0w_i$, ${}_1w_i$, $\ldots$, ${}_kw_i$ and $x_1, \ldots, x_k$ while the images under $\mathfrak{P}_2$ contain the indeterminates ${}_0v_j$, ${}_1v_j$, $\ldots$, ${}_lv_j$ and $y_1, y_2, \ldots, y_l$. Suppose that $\mathfrak{P}_1(m_1, \ldots, m_r) = \mathfrak{a}$ and $\mathfrak{P}_2(n_1, \ldots, n_s) = \mathfrak{b}$. In $\mathfrak{b}$ we replace each y_i by the new indeterminate x_{k+i}, each ${}_0v_j$ by the new indeterminate ${}_kw_{-j}$,

and each ${}_\nu v_j$, $\nu > 0$, by the new indeterminate ${}_{k+\nu}w_j$ (the negative index in ${}_kw_{-j}$ serves just to distinguish the new indeterminate from ${}_kw_j$ which occurs in $\mathfrak{a}$). Thus we have obtained a new l-tuple $\bar{\mathfrak{b}}$ from the old l-tuple $\mathfrak{b}$. We define a mapping $\mathfrak{Q} = \mathfrak{P}_2 \operatorname{wr} \mathfrak{P}_1$ by $(\mathfrak{P}_2 \operatorname{wr} \mathfrak{P}_1)(m_1, \ldots, m_r, n_1, \ldots, n_s) = (\mathfrak{a}, \bar{\mathfrak{b}})$, a $k+l$-tuple of words in the indeterminates ${}_0w_i$, ${}_1w_i, \ldots, {}_kw_i, {}_{k+1}w_i, \ldots, {}_{k+l}w_i, {}_kw_{-i}, x_1, \ldots, x_{k+l}$. Thus $\mathfrak{Q}$ is a parametric word vector. For $r = 0$ or $s = 0$, it is clear how we have to modify our construction. $\mathfrak{Q} = \mathfrak{P}_2 \operatorname{wr} \mathfrak{P}_1$ is called the wreath product of $\mathfrak{P}_2$ by $\mathfrak{P}_1$.

As a consequence of the definition we get that the wreath product is associative, i.e. $\mathfrak{P}_3 \operatorname{wr} (\mathfrak{P}_2 \operatorname{wr} \mathfrak{P}_1) = (\mathfrak{P}_3 \operatorname{wr} \mathfrak{P}_2) \operatorname{wr} \mathfrak{P}_1$. Thus we may omit brackets.

13.41. Lemma. *Let $\mathfrak{Q} = \mathfrak{P}_2 \operatorname{wr} \mathfrak{P}_1$. Then the specialization $\mathfrak{Q}(A)$ of $\mathfrak{Q}$ in A is the set M of all polynomial vectors $\mathfrak{f} = (\mathfrak{f}_1, \mathfrak{f}_2)$ of $C_{k+l}(A)$ such that $\mathfrak{f}_1 \in \mathfrak{P}_1(A)$ and $\mathfrak{f}_2 \in \overline{\mathfrak{P}}_2(A(x_1, \ldots, x_k, \mathfrak{V}))$ where $\overline{\mathfrak{P}}_2$ is the parametric word vector we get from replacing each y_i by x_{k+i} in the l-tuples of $\mathfrak{P}_2$.*

Proof. Every word in $A \cup \{x_1, \ldots, x_{k+\nu}\}$ is a word in $W(A \cup \{x_1, \ldots, x_k\}) \cup \{x_{k+1}, \ldots, x_{k+\nu}\}$ and vice versa. Thus the polynomial vectors of $\mathfrak{Q}(A)$ are exactly the polynomial vectors of M.

13.42. Theorem. *If the parametric word vectors $\mathfrak{P}_1$, $\mathfrak{P}_2$ are both semigroup generating, then the parametric word vector $\mathfrak{Q} = \mathfrak{P}_2 \operatorname{wr} \mathfrak{P}_1$ is also semigroup generating.*

Proof. We have to show that $\mathfrak{Q}(A)$ is a semigroup of $C_{k+l}(A)$, for all A in $\mathfrak{V}$. Let $\mathfrak{f} = (\mathfrak{f}_1, \mathfrak{f}_2)$, $\mathfrak{g} = (\mathfrak{g}_1, \mathfrak{g}_2) \in \mathfrak{Q}(A)$ and suppose $\mathfrak{f} \circ \mathfrak{g} = (\mathfrak{h}_1, \mathfrak{h}_2)$. By Lemma 13.41, $\mathfrak{f}_1, \mathfrak{g}_1 \in \mathfrak{P}_1(A)$, hence $\mathfrak{f}_1$ contains just $x_1, \ldots, x_k$ and we have therefore $\mathfrak{h}_1 = \mathfrak{f}_1 \circ \mathfrak{g}_1 \in \mathfrak{P}_1(A)$ by hypothesis. Again by Lemma 13.41, $\mathfrak{f}_2, \mathfrak{g}_2 \in \overline{\mathfrak{P}}_2(A(x_1, \ldots, x_k, \mathfrak{V}))$. In order to obtain an expression for $\mathfrak{h}_2$, we have to replace each x_i in $\mathfrak{f}_2$ by the i-th component of $\mathfrak{g}$. Since $\mathfrak{g}_1 \in \mathfrak{P}_1(A)$, the elements of $A(x_1, \ldots, x_k, \mathfrak{V})$ occurring in the components of $\mathfrak{f}_2$ are taken into elements of $A(x_1, \ldots, x_k, \mathfrak{V})$, and we obtain some element $\bar{\mathfrak{f}}_2 \in \overline{\mathfrak{P}}_2(A(x_1, \ldots, x_k, \mathfrak{V}))$ after replacing x_i, for $i = 1, \ldots, k$. Continuing by replacing the x_{k+i}, for $i = 1, \ldots, l$, we have to substitute now the i-th component of $\mathfrak{g}_2$ and finally end up with some vector $\mathfrak{h}_2$ which belongs to $\overline{\mathfrak{P}}_2(A(x_1, \ldots, x_k, \mathfrak{V}))$ since $\mathfrak{P}_2$ is semigroup generating. By Lemma 13.41, $\mathfrak{f} \circ \mathfrak{g} \in \mathfrak{Q}(A)$.

13.43. It is easy to see that, for any variety $\mathfrak{V}$ and $k = 1$, if $\mathfrak{P}$ is the parametric word vector ${}_1w_1$ of order 0, then the wreath product $\mathfrak{P}$ wr $\mathfrak{P}$ wr ... wr $\mathfrak{P}$ of k copies of $\mathfrak{P}$ is the parametric word vector of § 13.2, example a). If $\mathfrak{V}$ is the variety of commutative rings with identity, $k = 1$, and $\mathfrak{P}$ is the parametric word vector ${}_0w_1x_1 + {}_0w_2$ of order 0, then the wreath product of k copies of $\mathfrak{P}$ is the parametric word vector of § 13.2, example b) as one can easily see.

13.5. Let $\mathfrak{P}_1$ and $\mathfrak{P}_2$ be semigroup generating parametric word vectors of the orders r and s, resp., and $\mathfrak{Q} = \mathfrak{P}_2$ wr $\mathfrak{P}_1$. Then $\mathcal{L}_0 = \mathfrak{Q}$, $\mathcal{L}_0^1 = \mathfrak{P}_1$, $\mathcal{L}_0^2 = \mathfrak{P}_2$ are mappings as dealt with in § 13.1. Let A be any algebra of $\mathfrak{V}$, then $\mathcal{L}_1(A)$, $\mathcal{L}_3(A)$ (unless empty) are subsemigroups of $V_{k+l}(A)$, $\mathcal{L}_1^1(A)$ and $\mathcal{L}_3^1(A)$ (unless empty) are subsemigroups of $V_k(A)$, and $\mathcal{L}_1^2(A)$ and $\mathcal{L}_3^2(A)$ (unless empty) are subsemigroups of $V_l(A)$. Let $\sigma : A(x_1, \ldots, x_{k+l}, \mathfrak{V}) \to P_{k+l}(A)$, $\sigma_1 : A(x_1, \ldots, x_k, \mathfrak{V}) \to P_k(A)$, and $\sigma_2 : A(x_1, \ldots, x_l, \mathfrak{V}) \to P_l(A)$ be the canonical epimorphisms, and $\varphi, \varphi_1, \varphi_2$ the isomorphisms of Lemma 11.21 for $k+l$, k, and l, resp., instead of k. Let $\zeta : A^{k+l} \to A^k \times A^l$ be the bijection defined by $\zeta(a_1, \ldots, a_k, a_{k+1}, \ldots, a_l) = ((a_1, \ldots, a_k), (a_{k+1}, \ldots, a_l))$. Then the mapping $\tau : F_1(A^{k+l}) \to F_1(A^k \times A^l)$ $(\tau : \mathrm{Sym}(A^{k+l}) \to \mathrm{Sym}(A^k \times A^l))$ defined by $\tau f = \zeta f \zeta^{-1}$ is a semigroup (group) isomorphism.

Suppose now that $\mathfrak{f} \in \mathcal{L}_0(A) = \mathfrak{Q}(A)$. By Lemma 13.41, $\mathfrak{f} = (\mathfrak{f}_1, \mathfrak{f}_2)$ where $\mathfrak{f}_1 \in \mathfrak{P}_1(A)$ and $\mathfrak{f}_2 \in \overline{\mathfrak{P}}_2(A(x_1, \ldots, x_k, \mathfrak{V}))$. Therefore, for any $(\mathfrak{a}, \mathfrak{b}) \in A^k \times A^l$, we have

$$\begin{aligned}\zeta(\varphi\mathcal{F}(\sigma)\mathfrak{f})\zeta^{-1}(\mathfrak{a}, \mathfrak{b}) &= (\mathfrak{f}_1 \circ \mathfrak{a}, \mathfrak{f}_2(\mathfrak{a}) \circ \mathfrak{b}) \\ &= \big((\varphi_1\mathcal{F}(\sigma_1)\mathfrak{f}_1)\mathfrak{a}, (\varphi_2\mathcal{F}(\sigma_2)\mathfrak{f}_2(\mathfrak{a}))\mathfrak{b}\big).\end{aligned}$$

Hence

$$\tau\varphi(\mathcal{F}(\sigma)\mathfrak{f})(\mathfrak{a}, \mathfrak{b}) = \zeta(\varphi\mathcal{F}(\sigma)\mathfrak{f})\zeta^{-1}(\mathfrak{a}, \mathfrak{b}) = (\varkappa\mathfrak{a}, \lambda(\mathfrak{a})\mathfrak{b}) \tag{13.5}$$

where $\varkappa \in \varphi_1\mathcal{L}_1^1(A)$, $\lambda(\mathfrak{a}) \in \varphi_2\mathcal{L}_1^2(A)$. Thus $\tau\varphi$ maps $\mathcal{L}_1(A)$ monomorphically into the wreath product $\varphi_2\mathcal{L}_1^2(A)$ wr $\varphi_1\mathcal{L}_1^1(A)$, this time the wreath product is to be understood as the usual wreath product for semigroups.

13.51. Proposition. *The mapping $\tau\varphi$ maps $\mathcal{L}_1(A)$ monomorphically into the semigroup wreath product $\varphi_2\mathcal{L}_1^2(A)$ wr $\varphi_1\mathcal{L}_1^1(A)$. If A is finite, then also $\mathcal{L}_3(A)$ is mapped monomorphically into $\varphi_2\mathcal{L}_3^2(A)$ wr $\varphi_1\mathcal{L}_3^1(A)$ under $\tau\varphi$, and $\mathcal{L}_3(A)$ is mapped onto this wreath product if $\tau\varphi$ maps $\mathcal{L}_1(A)$ onto $\varphi_2\mathcal{L}_1^2(A)$ wr $\varphi_1\mathcal{L}_1^1(A)$.*

Proof. The first assertion has already been proved. Let $\mathfrak{g} \in \mathcal{L}_3(A)$, then $\mathfrak{g} \in U_{k+l}(A)$, thus $\varphi\mathfrak{g} \in \mathrm{Sym}(A^{k+l})$. Therefore $\zeta\varphi\mathfrak{g}\zeta^{-1} \in \mathrm{Sym}(A^k \times A^l)$. By

(13.5), $\zeta(\varphi\mathfrak{g})\zeta^{-1}(\mathfrak{a}, \mathfrak{b}) = (\varkappa\mathfrak{a}, \lambda(\mathfrak{a})\mathfrak{b})$ where $\varkappa \in F_1(A^k)$ and $\lambda(\mathfrak{a}) \in F_1(A^l)$. Hence $\varkappa$ is surjective and $\lambda(\mathfrak{a})$ is injective, for all $\mathfrak{a} \in A^k$. Since A is finite, $\varkappa$ and $\lambda(\mathfrak{a})$ are permutations which proves the second assertion. The third assertion can be proved by using (13.5) and the fact that if $\lambda(\mathfrak{a})$ and $\varkappa$ are permutations, so is the mapping on the left-hand side.

13.6. We ask for conditions under which $\tau\varphi$ maps $\mathcal{L}_1(A)$ isomorphically onto $\varphi_2\mathcal{L}_1^2(A)$ wr $\varphi_1\mathcal{L}_1^1(A)$. We first prove

13.61. Lemma. *The equation $\tau\varphi\mathcal{L}_1(A) = \varphi_2\mathcal{L}_1^2(A)$ wr $\varphi_1\mathcal{L}_1^1(A)$ holds if and only if, for any mapping $\vartheta : A^k \to \mathcal{L}_1^2(A)$, there exists a polynomial vector $\mathfrak{f}_2(x_1, \ldots, x_k, x_{k+1}, \ldots, x_{k+l}) \in \overline{\mathfrak{P}}_2(A(x_1, \ldots, x_k, \mathfrak{V}))$ such that*

$$\vartheta(a_1, \ldots, a_k) = \mathcal{F}(\sigma_2)\,\mathfrak{f}_2(a_1, \ldots, a_k, x_{k+1}, \ldots, x_{k+l}),$$

for all $(a_1, \ldots, a_k) \in A^k$.

Proof. $\mathcal{L}_1(A)$ consists of all elements $\mathcal{F}(\sigma)\mathfrak{f}$ such that $\mathfrak{f} \in \mathcal{L}_0(A)$. By Lemma 13.41, $\mathcal{L}_0(A)$ is the set of all polynomial vectors $\mathfrak{f} = (\mathfrak{f}_1, \mathfrak{f}_2)$ where $\mathfrak{f}_1 \in \mathfrak{P}_1(A)$ and $\mathfrak{f}_2 \in \overline{\mathfrak{P}}_2(A(x_1, \ldots, x_k, \mathfrak{V}))$. In § 13.5 we have seen that $(\tau\varphi\mathcal{F}(\sigma)\mathfrak{f})(\mathfrak{a}, \mathfrak{b}) = \big((\varphi_1\mathcal{F}(\sigma_1)\mathfrak{f}_1)\mathfrak{a}, (\varphi_2\mathcal{F}(\sigma_2)\mathfrak{f}_2(\mathfrak{a}))\mathfrak{b}\big)$. Since $\tau\varphi$ maps monomorphically from $\mathcal{L}_1(A)$ to $\varphi_2\mathcal{L}_1^2(A)$ wr $\varphi_1\mathcal{L}_1^1(A)$, it maps $\mathcal{L}_1(A)$ isomorphically onto this wreath product if and only if, for any $\varkappa \in \mathcal{L}_1^1(A)$ and any mapping $\vartheta : A^k \to \mathcal{L}_1^2(A)$, there exists some $\mathfrak{f}_1 \in \mathfrak{P}_1(A)$ and $\mathfrak{f}_2 \in \overline{\mathfrak{P}}_2(A(x_1, \ldots, x_k, \mathfrak{V}))$ such that $\mathcal{F}(\sigma_1)\mathfrak{f}_1 = \varkappa$ and

$$\mathcal{F}(\sigma_2)\,\mathfrak{f}_2(a_1, \ldots, a_k, x_{k+1}, \ldots, x_{k+l}) = \vartheta(a_1, \ldots, a_k),$$

for all $(a_1, \ldots, a_k) \in A^k$.

13.62. Theorem. *Let $\mathfrak{Q} = \mathfrak{P}_2$ wr $\mathfrak{P}_1$. $\tau\varphi$ maps $\mathcal{L}_1(A)$ isomorphically onto $\varphi_2\mathcal{L}_1^2(A)$ wr $\varphi_1\mathcal{L}_1^1(A)$ if $\mathfrak{P}_2$ is of order 0 and A is polynomially complete.*

Proof. We have to show that the hypothesis of Lemma 13.61. is satisfied. Let $\mathfrak{P}_2 = (g_1, \ldots, g_l)$ where $g_j = g_j({}_0v_i, {}_1v_i, \ldots, {}_lv_i, y_1, \ldots, y_l)$, $j = 1, 2, \ldots, l$, and $\vartheta : A^k \to \mathcal{L}_1^2(A)$ be any mapping. Then, for any $\mathfrak{a} = (a_1, \ldots, a_k) \in A^k$, we have $\vartheta\mathfrak{a} = (h_1, \ldots, h_l)$ where $h_j = g_j({}_0v_i(\mathfrak{a}), {}_1v_i(\mathfrak{a}, \xi_1), {}_2v_i(\mathfrak{a}, \xi_1, \xi_2), \ldots, {}_lv_i(\mathfrak{a}, \xi_1, \ldots, \xi_l), \xi_1, \ldots, \xi_l)$, $j = 1, 2, \ldots, l$. Since A is polynomially complete, for any ${}_rv_s$ occurring in g_j there exists a polynomial ${}_rw_s(x_1, \ldots, x_k, x_{k+1}, \ldots, x_{k+r}) \in A(x_1, \ldots, x_{k+r}, \mathfrak{V})$ such that, for any $\mathfrak{a} \in A^k$ we have

$${}_rw_s(a_1, \ldots, a_k, \xi_1, \ldots, \xi_r) = {}_rv_s(\mathfrak{a}, \xi_1, \ldots, \xi_r).$$

Substituting these polynomials into $\overline{\mathfrak{P}}_2$ of Lemma 13.41, we get a polynomial vector $\mathfrak{f}_2(x_1, \ldots, x_{k+l}) \in \overline{\mathfrak{P}}_2(A(x_1, \ldots, x_k, \mathfrak{V}))$. The j-th component of $\mathcal{F}(\sigma_2)\mathfrak{f}_2(a_1, \ldots, a_k, x_{k+1}, \ldots, x_l)$ is h_j, thus $\mathcal{F}(\sigma_2)\mathfrak{f}_2(a_1, \ldots, a_k, x_{k+1}, \ldots, x_l) = \vartheta(a_1, \ldots, a_k)$ and the hypothesis of Lemma 13.61 is satisfied.

13.63. Let us now apply Theorem 13.62 to our examples a) and b) of § 13.2 which, as stated in § 13.43 are wreath products of parametric word vectors of order 0. Th. 13.62 and Prop. 13.51 show that, if A is polynomially complete, then, in the case of example a), the semigroup $\mathcal{L}_1(A)$ is isomorphic to the wreath product of k copies of the symmetric semigroup of A and $\mathcal{L}_3(A)$ is isomorphic to the wreath product of k copies of the symmetric group of A. We also see that, if A is a finite field, then, in the case of example b), $\mathcal{L}_1(A)$ is isomorphic to the wreath product of k copies of the one-dimensional linear inhomogeneous semigroup of A and $\mathcal{L}_3(A)$ is isomorphic to the wreath product of k copies of the one-dimensional linear inhomogeneous group of A.

Remarks and comments

§ 1. MENGER [3] was the first person who fully realized the significance of the concept of superassociativity, and it was he who introduced selector systems. There are also papers by DICKER [1] and SKALA [1] on k-dimensional superassociative systems. MENGER [1] also introduced 1-dimensional composition rings and thus axiomatized the composition of functions from a ring into itself. MENGER and his school have written several papers on 1-dimensional composition rings which then bore the name of trioperational algebras; we refer to a survey on this work by MENGER [2], but also to ADLER [1]. Near-rings were introduced by ZASSENHAUS about 1935 (for a special case) and have been the subject of quite a lot of papers ever since whereas composition lattices have hardly been investigated (see MITSCH [1]). HION [1], [2], [3] considered $\mathfrak{V}$-composition algebras in general and related algebras for the first time.

Composition of functions on sets has been treated in many papers, mostly for the needs of formal logic, but sometimes also from a purely algebraic viewpoint (MENGER and WHITLOCK [1], WHITLOCK [1], SCHWEIZER and SKLAR [1]). The composition algebra $F_1(R)$ where R is a commutative ring with identity has been treated by NÖBAUER [16]. BERMAN and SILVERMAN [2] proved Th. 1.51 for the case that Ω contains just 2-ary operations, NÖBAUER [20] gave a proof in the general case.

§ 2. HULE [1], [2], was the first one to study the composition of polynomials and polynomial functions over arbitrary algebras. For commutative rings with identity and fields, in particular, the theory of composition of polynomials has been a tool for numerous branches of mathematics ever since the beginnings of algebra, but there was not a systematic approach until this century (a survey of papers on this subject will be given in our remarks and comments on §§ 6, 7 and on Ch. 4).

§ 3. Our definition of a constant was inspired by MENGER who defined constants for composition rings. Our condition of Prop. 3.51 is closely related to a concept of independence for algebras having the same type, which was introduced by FOSTER [3].

§ 4. The theory of full congruences in arbitrary polynomial algebras has been developed by HULE [1], [2]. For the results on full congruences of $F_k(A)$ which are quoted in § 4.2, we refer to BERMAN and SILVERMAN [1], NÖBAUER and PHILIPP [1], [2], and PHILIPP [1].

§ 6. MANNOS [1] has studied ideals of composition rings in general while a systematic theory on full ideals of polynomial rings over commutative rings with identity was subsequently developed by NÖBAUER [10]–[14]. A computation and discussion of the Jacobson radical (i.e. the intersection of all maximal full ideals) of an arbitrary polynomial ring $R[x_1, \ldots, x_k]$ with composition over a commutative ring R with identity is due to MLITZ [1]. It has been an outstanding problem for a long time to find all full ideals of the polynomial ring $\mathbf{Z}[x_1, \ldots, x_k]$, $\mathbf{Z}$ being the ring of rational integers. This problem has not even been solved for $k = 1$.

§ 7. A part of Th. 7.21 is due to MILGRAM [1], in its present form it was proved by NÖBAUER [23], Th. 7.31 has its origin in BURKE [1]. The problem of determining all full ideals of $Q[x_1, \ldots, x_k]$ for a finite field Q and $k > 1$ has not yet been solved. A first attack on this problem for $k = 2$ was launched by STUEBEN [1]. Recently CLAY and DOI [1] have computed the Jacobson radical and all maximal ideals of the near-ring $\langle K[x]; +, \varkappa \rangle$ where $\varkappa$ stands for the composition and K is a field, $|K| \neq 2$.

§ 8. DICKSON [5] called the polynomials of $\{D\}$ "residue polynomials mod D". Papers on residue polynomials over the rational integers are KEMPNER [1], [2], LITZINGER [1], NÖBAUER [2], [4], NIVEN and WARREN [1]. LEWIS [1] started with the investigation of residue polynomials for the case of arbitrary Dedekind domains. The approach of our book, however, has been used by LAUSCH [1] for $k = 1$ and generalized by AIGNER [1] to $k > 1$.

There is a connection between the residue polynomials of the ring $\mathbf{Z}$ of rational integers and the so-called integral-valued polynomials whose definition is: Let K be the field of rational numbers, then a polynomial $f \in K[x_1, \ldots, x_k]$ is called an integral-valued polynomial if $f(a_1, \ldots, a_k) \in \mathbf{Z}$, for all $(a_1, \ldots, a_k) \in \mathbf{Z}^k$. If (n) is an ideal of $\mathbf{Z}$, then evidently $f \in \mathbf{Z}[x_1, \ldots, x_k]$ is a residue polynomial mod (n) if and only if the polynomial $(1/n)f$ is integral-valued. For details of integral-valued polynomials we refer to CARLITZ [2], STRAUS [1], but there are also many other papers on this subject.

§ 10. The presentation of this section follows NÖBAUER [19].

§ 11. It is still an open problem to characterize all those 1-dimensional $\mathfrak{V}$-composition algebras which are isomorphic to some algebra $\mathcal{F}(A)$, for a suitable k-dimensional composition algebra A. We refer to ŠAIN [1] for the case where $\mathfrak{V}$ is the variety of sets. The considerations of this section were so far treated only for special varieties, mainly for commutative rings with identity (for a survey on relevant papers we refer to the remarks and comments on Ch. 4, § 4).

§ 12. Polynomial permutations, permutation polynomial vectors and permutation polynomials of A were investigated up to 1950 only for the case where $\mathfrak{V}$ is the variety of commutative rings with identity, A is a finite field and $k = 1$, but for this case an extensive literature had piled up (see remarks and comments on Ch. 4, §§ 8, 9). Later on, other commutative rings with identity were studied in this respect, then also $k = 1$ was dropped (see remarks and comments on Ch. 4, § 4). Furthermore in recent years also the variety of groups was object of investigations in this direction (see remarks and comments on Ch. 5) and more recently MITSCH [2] and SCHWEIGERT [1] treated permutation polynomials in the variety of lattices.

Our Prop. 12.21 is due to P. GRUBER.

§ 13. Several examples of subsemigroups of the semigroup $C_k(A)$ which are defined by parametric words are known for the case where $\mathfrak{V}$ is the variety of commutative rings with identity. The best known such example is the subsemigroup of polynomial vectors with linear forms as their components. This subsemigroup and the group of its permutation polynomial vectors have been studied in numerous papers. For other examples we refer to KALOUJNINE [1], NÖBAUER [3], [6], [8], [11], [17], [18].

CHAPTER 4

COMPOSITION OF POLYNOMIALS AND POLYNOMIAL FUNCTIONS OVER RINGS AND FIELDS

1. Prime factor decomposition with respect to composition

1.1. Let $\mathfrak{V}$ be any variety with Ω as its family of operations, A an algebra of $\mathfrak{V}$, $X = \{x_1, \ldots, x_k\}$ a set of indeterminates, and $\mathcal{F}(A(X, \mathfrak{V})) = \langle A(X, \mathfrak{V})^k; \Omega, \circ \rangle$ the algebra introduced in ch. 3, § 11. By ch. 3, Th. 11.11, this is a 1-dimensional $\mathfrak{V}$-composition algebra, thus the algebra $S = \langle A(X, \mathfrak{V})^k; \circ \rangle$ is a semigroup with identity. There is little known about the structure of S. Only for the case where $\mathfrak{V}$ is the variety of commutative rings with identity and A is a field (or sometimes, more generally, an integral domain) and $k = 1$, there exist some satisfactory results. The most interesting and important results will be derived in this and the subsequent sections.

1.2. Let $\mathfrak{V}$ be the variety of commutative rings with identity, D any integral domain of $\mathfrak{V}$, and x an indeterminate. We consider the semigroup $\langle D[x]; \circ \rangle = S$ which has x as identity. The degree $[f]$ of any polynomial $f \neq 0$ of $D[x]$ has been defined in ch. 1, § 8.3. It will be useful for our further considerations to set $[0] = 0$; then every polynomial will have some well-defined degree.

1.21. Proposition. *For any two polynomials $f, g \in S$, we have $[f \circ g] = [f][g]$.*

Proof. By ch. 1, Th. 8.11, f, g have normal forms that can be written as $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $g = b_m x^m + \ldots + b_1 x + b_0$. Then $f \circ g = f(g) = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_1 g + a_0$. If $[g] = 0$, we have $[f \circ g] = 0 = [f][g]$, and if $g \neq 0$, by ch. 1, Prop. 8.31, we have $[g^j] = j[g]$ for $j \geqslant 0$ whence $[f \circ g] = n[g] = [f][g]$.

1.22. Remark. The proof of Prop. 1.21 also shows that, for an arbitrary ring D of $\mathfrak{V}$, we have $[f \circ g] \leqslant [f][g]$.

1.23. Corollary. *The mapping $f \to [f]$ from S into the multiplicative semigroup of integers is a homomorphism ϑ.*

Proof. This is a restatement of Prop. 1.21.

1.24. Corollary. *If $f \in S$ has a right or a left inverse, then $[f] = 1$.*

Proof. By Cor. 1.23, since 1 is the only non-negative integer which has a multiplicative inverse.

1.25. Proposition. *Every $f \in S$ with $[f] \neq 0$ is a right-regular element of S.*

Proof. Suppose that $g \circ f = h \circ f$, then the right-superdistributivity of $\circ$ implies $(g-h) \circ f = 0$. We apply ϑ of Cor. 1.23 to this equation, then $g - h = a \in D$. Hence $0 = (g-h) \circ f = a \circ f = a$ and therefore $g = h$.

1.26. A polynomial $f \in S$ is called indecomposable if $[f] > 1$ and there is no representation of f of the form $f = f_1 \circ f_2$ where $[f_1] < [f]$ and $[f_2] < [f]$. E.g., every polynomial of prime degree is indecomposable.

1.27. Proposition. *Every $f \in S$ such that $[f] > 1$ has a representation of the form $f = f_1 \circ f_2 \circ \ldots \circ f_r$ where every f_i is indecomposable.*

Proof. By Prop. 1.21.

1.28. There arises now the question of in how many different ways f can be decomposed this way. Only for the case where D is a field of characteristic zero (for partial results for prime characteristic see FRIED and MACRAE [1]), a complete answer is known which we will elaborate in the remainder of this section and the subsequent one, leaning heavily on the definitions and results of ch. 6, § 5.

1.3. Let K be any field of characteristic zero and S the semigroup $\langle K[x]; \circ \rangle$. Since K is an integral domain, all the results of § 1.2 can be applied to K. An extension of Cor. 1.24 can be obtained for fields:

1.31. Proposition. *$f \in S$ has a right (left) inverse if and only if $[f] = 1$. In this case f has a unique inverse.*

Proof. "Only if" follows from Cor. 1.24. If $f = ax+b$, then $g = (1/a)\cdot(x-b)$ is an inverse of f which is unique since $\circ$ is associative.

1.32. A polynomial $f \in K[x]$ is called normed if its normal form according to ch. 1, Th. 8.11, is $f = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x$. Thus every normed polynomial is monic. If f, g are normed, then also fg and $f \circ g$ are normed.

1.33. Lemma. *Let U be any intermediate field of $K(x)$ such that U contains a polynomial of positive degree. Then there exists one and only one normed polynomial $h \in K[x]$ such that $U = K(h)$.*

Proof. By ch. 6, Lemma 5.8, $U = K(r)$ where $r \in K[x]$ and $[r] > 0$. But clearly $r = ah+b$ where $a \neq 0$ and b are suitable chosen elements of K and h is a normed polynomial, hence $K(r) = K(h)$. If k is any normed polynomial of $K[x]$ such that $U = K(k)$, then, by ch. 6, Lemma 5.81, $k = l \circ h$ and $h = m \circ k$ whence $[l] = 1$. Thus $k = ch+d$, $c, d \in K$, $c \neq 0$. Since h, k are normed, we conclude $c = 1$, $d = 0$, hence $k = h$.

1.34. Theorem. a) *Every polynomial $f \in S$ with $[f] > 1$ has a "prime factor decomposition" of the form*

$$f = l \circ f_1 \circ \ldots \circ f_r \tag{1.31}$$

where l is a linear polynomial and every f_i is a normed indecomposable polynomial.

b) *If*

$$f = m \circ g_1 \circ \ldots \circ g_s \tag{1.32}$$

is any other prime factor decomposition of f, then $l = m$, $r = s$, and the degrees $[g_i]$ can be paired off with the degrees $[f_j]$.

c) *The decomposition* (1.31) *can be transformed into the decomposition* (1.32) *by a finite number of steps of the following kind: From a decomposition $f = n \circ h_1 \circ \ldots \circ h_r$, select a "partial product" $h_i \circ h_{i+1}$ and replace it by a partial product $k_i \circ k_{i+1}$ of normed indecomposable polynomials k_i, k_{i+1} such that $h_i \circ h_{i+1} = k_i \circ k_{i+1}$.*

d) *There is only a finite number of different prime factor decompositions of f.*

Proof. Let $f = l \circ f_1 \circ \ldots \circ f_r$ be any prime factor decomposition, and $f_{r+1} = x$. In the chain $K(f) = K(f_1 \circ f_2 \circ \ldots \circ f_{r+1}) \subseteq K(f_2 \circ \ldots \circ f_{r+1}) \subseteq \ldots \subseteq K(f_r \circ f_{r+1}) \subseteq K(f_{r+1})$ of subfields of $K(x)$, every inclusion is proper, by ch. 6, Th. 5.71, since $[f_i] > 1$, for $i \leq r$. Let U be a field such that $K(f_v \circ f_{v+1} \circ \ldots \circ f_{r+1}) \subseteq U \subseteq K(f_{v+1} \circ \ldots \circ f_{r+1})$, for $1 \leq v \leq r$. By ch. 6, Lemma 5.8, $U = K(t)$, $t \in K[x]$, and by ch. 6, Lemma 5.81, there are $p, q \in K[x]$ such that $f_v \circ f_{v+1} \circ \ldots \circ f_{r+1} = p \circ t$, $t = q \circ f_{v+1} \circ \ldots \circ f_{r+1}$, hence $f_v \circ f_{v+1} \circ \ldots \circ f_{r+1} = p \circ q \circ f_{v+1} \circ \ldots \circ f_{r+1}$. By Prop. 1.25, $f_v = p \circ q$, thus $[p] = 1$ or $[q] = 1$ whence the chain above is a maximal chain. Thus every decomposition (1.31) of f yields some maximal chain $K(f) = S_0 \subset S_1 \subset \ldots \subset S_r = K(x)$ from $K(f)$ to $K(x)$ which we will call the chain belonging to this decomposition. The length of this chain equals the number of factors in the decomposition while, by ch. 6, Th. 5.71, $[S_i : S_{i-1}] = [f_i]$, $i = 1, \ldots, r$.

Clearly, if (1.32) yields the same maximal chain from $K(f)$ to $K(x)$, then $s = r$ and $K(f_v \circ f_{v+1} \circ \ldots \circ f_r) = K(g_v \circ g_{v+1} \circ \ldots \circ g_r)$, $1 \leq v \leq r$. Since f_i, g_i, $i = 1, \ldots, r$, are normed, Lemma 1.33 implies that $f_v \circ f_{v+1} \circ \ldots \circ f_r = g_v \circ g_{v+1} \circ \ldots \circ g_r$, $1 \leq v \leq r$, whence, by Prop. 1.25, $f_i = g_i$, $i = r, r-1, \ldots, 1$ and $l = m$. Hence every maximal chain from $K(f)$ to $K(x)$ belongs to at most one prime factor decomposition of f.

Next we will show that every such chain belongs to at least one prime factor decomposition of f so that we may consider maximal chains in the place of prime factor decompositions. Thus let $K(f) = S_0 \subset S_1 \subset \ldots \subset S_r = K(x)$ be any maximal chain from $K(f)$ to $K(x)$. By Lemma 1.33, there are normed polynomials u_i, $i = 0, 1, \ldots, r$, such that $S_i = K(u_i)$, in particular, $u_r = x$. By ch. 6, Lemma 5.81, we have $f = l \circ u_0$, $[l] = 1$, and $u_i = f_{i+1} \circ u_{i+1}$, $[f_{i+1}] > 1$, $i = 0, 1, \ldots, r-1$. Since u_i, u_{i+1} are normed, f_{i+1} is normed, too. Suppose that f_{i+1} is not indecomposable, say $f_{i+1} = p \circ q$ where $[p] < [f_{i+1}]$, $[q] < [f_{i+1}]$, then $u_i = p \circ (q \circ u_{i+1})$, and since $[p] > 1$, $[q] > 1$, we would have $S_i \subset K(q \circ u_{i+1}) \subset S_{i+1}$, contradiction. Hence $u_i = f_{i+1} \circ f_{i+2} \circ \ldots \circ f_r$, $i = r-1, r-2, \ldots, 0$, therefore $f = l \circ f_1 \circ f_2 \circ \ldots \circ f_r$, which is a prime factor decomposition of f, having $S_0 \subset S_1 \subset \ldots \subset S_r$ as its maximal chain.

We need some further property of the correspondence between maximal chains and prime factor decompositions. Let $S_0 \subset S_1 \subset \ldots \subset T_m \subset \ldots \subset S_r$ be a maximal chain which differs from $S_0 \subset S_1 \subset \ldots \subset S_m \subset \ldots \subset S_r$ only by the m-th member. Then f has a certain prime factor decomposition (1.32) corresponding to this maximal chain. Let

$T_m = K(v_m)$ where v_m is normed, then, as before, we get

$$f = l \circ u_0, \qquad u_i = f_{i+1} \circ u_{i+1}, \quad i = 0, 1, \ldots, m-2,$$
$$u_{m-1} = g_m \circ v_m, \qquad v_m = g_{m+1} \circ u_{m+1},$$
$$u_i = f_{i+1} \circ u_{i+1}, \quad i = m+1, \ldots, r-1.$$

By Prop. 1.25, $g_m \circ g_{m+1} = f_m \circ f_{m+1}$. Hence (1.32) becomes in this case

$$f = l \circ f_1 \circ \ldots \circ f_{m-1} \circ g_m \circ g_{m+1} \circ f_{m+2} \circ \ldots \circ f_r$$

where $g_m \circ g_{m+1} = f_m \circ f_{m+1}$.

The proof of the theorem now consists of translating the relevant results of ch. 6, § 5, into the language of prime factor decompositions. Hence a) holds since there exist maximal chains from $K(f)$ to $K(x)$. Since all f_i, g_i, are normed, b) is a consequence of ch. 6, Th. 5.86; c) also follows from part c) of this theorem while d) results from ch. 6, Remark 5.87.

2. Standard solutions of $p \circ q = r \circ s$

2.1. Theorem 1.34 shows that, in a finite number of steps, all the different prime factor decompositions of a polynomial f can be obtained from a given decomposition as soon as we know all the solutions of the equation

$$p \circ q = r \circ s \tag{2.1}$$

where p, q, r, s are normed indecomposable polynomials. This type of solution will be called a standard solution of (2.1). Indeed, let D be the given decomposition of f. Then we can determine the set D_1 of all decompositions of f, which are obtained from D by at most one replacement of two subsequent factors. In the same way, we can derive a set D_2, etc. Finally, by Th. 1.34 c), d), we end up with a set D_k of decompositions such that $D_{k+1} = D_k$. Hence D_k consists of all the different prime factor decompositions of f.

There seems to exist, so far, no explicit investigation of the problem to decide, whether or not a polynomial f is indecomposable, and of the problem, to determine a prime factor decomposition of a given polynomial. As A. SCHINZEL has pointed out, the first problem can be solved by considering all possibilities for a decomposition of f into two factors and deciding in every case whether the resulting system of equations for the unknown coefficients of these factors is solvable (which, of course, is rather tedious). Clearly then the second problem can also be solved.

2.2. We are now going to reduce the problem of finding the standard solutions of (2.1) in $K[x]$ where K is any field of characteristic zero.

2.21. Lemma. *Let $f \in K[x]$ be indecomposable over $K[x]$ and L any extension field of K. Then f is also indecomposable over $L[x]$.*

Proof. Suppose that $f = p \circ q$, $p, q \in L[x]$, then, for any $0 \neq c \in K$ and for any linear polynomial $l \in L[x]$, we have $(1/c)f = \left((1/c)p \circ l^{-1}\right) \circ (l \circ q)$ where l^{-1} is the inverse of l under $\circ$. For suitably chosen l and c, $q^* = l \circ q$ is normed and $f^* = (1/c)f$ is monic whence $p^* = (1/c)p \circ l^{-1}$ is also monic. Let $p^* = x^m + c_1 x^{m-1} + \ldots$, $q^* = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x$, $f^* = x^{nm} + b_1 x^{nm-1} + \ldots$, then $f^* = p^* \circ q^*$ yields

$$b_j = ma_j + w_{j-1}(a_1, \ldots, a_{j-1}), \quad j = 1, 2, \ldots, n-1,$$

where $w_0 = 0$ and $w_i(x_1, \ldots, x_i)$, $i = 1, 2, \ldots, n-2$, is some polynomial over the ring of rational integers. Thus $b_j \in K$ implies $a_j \in K$, $j = 1, 2, \ldots, n-1$, whence $q^* \in K[x]$. Assume that $p^* \notin K[x]$, then $p^* = u + v$ where $[v] < [u]$, $u \in K[x]$, $v \notin K[x]$, and the first coefficient of v is not in K. Hence $f^* - u \circ q^* = v \circ q^*$ and the left-hand side is in $K[x]$ while the right-hand side is not, contradiction. Thus $p^* \in K[x]$ and $f = cf^* = (cp^*) \circ q^*$ whence $[cp^*] = [f]$ or $[q^*] = [f]$. Therefore $[p] = [f]$ or $[q] = [f]$ and f is indecomposable over $L[x]$.

2.22. Corollary. *Let L be the algebraic closure of K. Then the standard solutions p, q, r, s of* (2.1) *in $K[x]$ are just those standard solutions of* (2.1) *in $L[x]$ which are polynomials of $K[x]$.*

2.23. Remark. Corollary 2.22 shows that we can restrict ourselves to algebraically closed fields K when solving (2.1).

2.3. A further reduction of the problem of solving (2.1) can be reached by classifying the solutions in the following way: Let p, q, r, s be a standard solution of (2.1) and $l \in K[x]$ an arbitrary linear polynomial. Then $p \circ (q \circ l) = r \circ (s \circ l)$. There exist unique linear polynomials $m_1, m_2 \in K[x]$ such that $m_1 \circ q \circ l$ and $m_2 \circ s \circ l$ are normed. Let $g = (p \circ m_1^{-1}) \circ (m_1 \circ q \circ l) = (r \circ m_2^{-1}) \circ (m_2 \circ s \circ l)$. Then there exists a unique linear polynomial $u \in K[x]$ such that $u \circ g$ is normed, hence $u \circ p \circ m_1^{-1}$, $m_1 \circ q \circ l$, $u \circ r \circ m_2^{-1}$, $m_2 \circ s \circ l$ is also a standard solution of (2.1). Any solution of that kind will be called conjugate to p, q, r, s. "Being conjugate" is an equivalence relation on the set S of all standard solutions of (2.1) and thus yields a partition of S. Our problem will be solved as soon as we know a full system of representatives of this partition.

If $q = s$, for a standard solution p, q, r, s, then, by Prop. 1.25, $p = r$. Any solution of the form p, q, p, q will be called a trivial solution. Each class of pairwise conjugate standard solutions consists either of trivial solutions or it contains no trivial solution. Of course, only the non-trivial solutions are of interest to us.

2.4. Our next aim is to derive two special classes of standard solutions of (2.1).

2.41. Let π be any prime, ϱ an integer, $0 < \varrho < \pi$, and $t \in K[x]$ monic. Then $x^\pi \circ (x^\varrho t(x^\pi)) = (x^\varrho t(x)^\pi) \circ x^\pi$. Thus if $x^\varrho t(x^\pi)$ is indecomposable, then $p = x^\pi$, $q = x^\varrho t(x^\pi)$, $r = x^\varrho t(x)^\pi$, $s = x^\pi$ is a standard solution of (2.1)—the indecomposability of $x^\varrho t(x)^\pi$ follows from Th. 1.34 b). A standard solution of this type is called a power solution. For $t = 1$, we get the power solution $p = x^\pi$, $q = x^\varrho$, $r = x^\varrho$, $s = x^\pi$, π being a prime.

2.42. Remark. So far no handy method could be developed to decide whether or not a polynomial $x^\varrho t(x^\pi)$ is indecomposable. Clearly if $\varrho + \pi[t]$ is a prime, $x^\varrho t(x^\pi)$ is indecomposable, and the equation $x^2((x^3)^4 + (x^3)^2) = (x(x^6 + x^3)) \circ x^2$ shows that otherwise the polynomial can be decomposable.

2.43. Let m be an integer and φ any real number. Then de Moivre's equation $(\cos\varphi + \mathrm{i}\sin\varphi)^m = \cos m\varphi + \mathrm{i}\sin m\varphi$ implies, for $m \geqslant 0$,

$$\cos m\varphi = (\cos\varphi)^m - \binom{m}{2}(\cos\varphi)^{m-2}(1-\cos^2\varphi) + \binom{m}{4}(\cos\varphi)^{m-4}(1-\cos^2\varphi)^2 - \ldots = t_m(\cos\varphi)$$

where t_m is a well-defined polynomial of degree m over ther ational integers, the so-called Čebyshev polynomial of the first kind of degree m. We first sum up some well-known results on Čebyshev polynomials which we will need later on:

2.44. Lemma. (i) *If $\mu, \nu \geqslant 0$, then $t_{\mu\nu} = t_\mu \circ t_\nu$.*

(ii) *If $\mu \geqslant 0$, then $t_\mu \circ (-x) = (-1)^\mu t_\mu$.*

(iii) *If $\mu \geqslant 0$, then t_μ satisfies the differential equation $\mu^2(1-t_\mu^2) = (1-x^2)t_\mu'^2$.*

Proof. (i) $t_{\mu\nu}(\cos\varphi) = \cos\mu\nu\varphi = \cos\mu(\nu\varphi) = t_\mu(\cos\nu\varphi) = t_\mu(t_\nu(\cos\varphi))$. Since $\cos\varphi$ ranges over an infinite set, we conclude $t_{\mu\nu}(x) = t_\mu(t_\nu(x))$.

(ii) $t_\mu(-\cos\varphi) = t_\mu(\cos(\pi-\varphi)) = \cos\mu(\pi-\varphi) = (-1)^\mu \cos\mu\varphi = (-1)^\mu t_\mu(\cos\varphi)$. Hence $t_\mu(-x) = (-1)^\mu t_\mu(x)$.

(iii) Differentiation of $\cos\mu\varphi = t_\mu(\cos\varphi)$ yields $\mu\sin\mu\varphi = t_\mu'(\cos\varphi)\sin\varphi$. Hence $\mu^2(1-t_\mu^2(\cos\varphi)) = (1-\cos^2\varphi)\,t_\mu'^2(\cos\varphi)$ whence $\mu^2(1-t_\mu^2) = (1-x^2)t_\mu'^2$.

2.45. Remark. Part (i) of Lemma 2.44 shows that t_μ is indecomposable if and only if μ is a prime. Moreover, $t_\mu \circ t_\nu = t_\nu \circ t_\mu$. Thus if μ, ν are primes and l_μ, l_ν, u are suitably chosen linear polynomials, then $p = u \circ t_\mu \circ l_\nu^{-1}$, $q = l_\nu \circ t_\nu$, $r = u \circ t_\nu \circ l_\mu^{-1}$, $s = l_\mu \circ t_\mu$ is a standard solution of (2.1). Such solution is called a Čebyshev solution.

2.46. Theorem. *Every non-trivial standard solution of the equation $p \circ q = r \circ s$ is conjugate to some power solution or to some Čebyshev solution.*

Proof. Theorem 2.46 will result from a whole bunch of lemmas, the proof of which will fill the remainder of this section.

.5. Proposition. *Let p, q, r, s be any non-trivial standard solution of* (2.1). *Then $[q] = [r] = \mu$, $[p] = [s] = \nu$ where $(\mu, \nu) = 1$.*

Proof. By hypothesis, we have $p \circ q = r \circ s = f$. Hence, by Prop. 1.25, $q \neq s$ while Lemma 1.33 implies $K(q) \neq K(s)$. Then the proof of Th. 1.34 shows that $K(f) \subset K(q) \subset K(x)$ and $K(f) \subset K(s) \subset K(x)$ are maximal chains of fields from $K(f)$ to $K(x)$. Thus $K(f) = K(q) \cap K(s)$ and $K(x) = K(q, s)$. By ch. 6, Th. 5.84, $[K(x) : K(q)] = [K(s) : K(f)]$, hence, by ch. 6, Th. 5.71, $[q] = [r]$ whence $[p] = [s]$. Furthermore ch. 6, Th. 5.84 b), implies $([q], [s]) = 1$ since $K(q, s) = K(x)$.

2.51. Lemma. *If $p \circ q = r \circ s = f$, then the minimal polynomials in the indeterminate y of the elements x over $K(f)$, $K(q)$, $K(s)$, q over $K(f)$, s over $K(f)$ are the polynomials $f(y)-f$, $q(y)-q$, $s(y)-s$, $p(y)-f$, and $r(y)-f$, respectively. The polynomial $p(y)-f$ remains irreducible over $K(s)$, and $r(y)-f$ remains irreducible over $K(q)$.*

Proof. The statement for the first three polynomials follows from ch. 6, Th. 5.71, while $[K(q) : K(f)] = [p]$, $[K(s) : K(f)] = [r]$ shows that $p(y)-f$ and $r(y)-f$ are the minimal polynomials for q and s, respectively. Since

$K(s)(q) = K(x)$ and $[K(x):K(s)] = [s] = [p]$ by Prop. 2.5, $p(y)-f$ must be irreducible over $K(s)$. Similarly $r(y)-f$ is irreducible over $K(q)$.

2.52. We define a binary relation $\sim$ on $K(x)$ by: $u \sim v$ means $u = ev$ where $e = +1$ or -1. Clearly, $\sim$ is a congruence on the multiplicative semigroup of $K(x)$. If $K(f)$ is an extension field of $K(g)$ and $h \in K(f)$, then, as in ch. 6, § 5.88, $\mathcal{N}_{f|g}(h)$ will denote the norm of h with respect to this extension.

2.53. Lemma. *If $c \in K$, then*

$$\mathcal{N}_{x|f}(x-c) \sim f-f(c), \quad \mathcal{N}_{x|q}(x-c) \sim q-q(c), \quad \mathcal{N}_{x|s}(x-c) \sim s-s(c), \tag{2.51}$$

$$\mathcal{N}_{q|f}(q-c) \sim f-p(c), \quad \mathcal{N}_{s|f}(s-c) \sim f-r(c), \tag{2.52}$$

$$\mathcal{N}_{x|s}(q-c) \sim f-p(c), \quad \mathcal{N}_{x|q}(s-c) \sim f-r(c). \tag{2.53}$$

Proof. Since $K(x-c) = K(x)$, we have $[K(x-c):K(f)] = [f]$, hence the minimal polynomial of $x-c$ over $K(f)$ is $f(y+c)-f$, and the constant term of this polynomial is $f(c)-f$. Thus $\mathcal{N}_{x|f}(x-c) \sim f-f(c)$. Similarly all the other relations of (2.51) and (2.52) are obtained. Since $K(s)(q-c) = K(s)(q)$, we have $[K(s)(q-c):K(s)] = [p]$, by Prop. 2.5, hence the minimal polynomial of $q-c$ over $K(s)$ is $p(y+c)-f$. Thus $\mathcal{N}_{x|s}(q-c) \sim f-p(c)$. Similarly the last relation follows.

2.54. Lemma. *Let, as before, $[q] = [r] = \mu$, $[p] = [s] = \nu$. Then*

$$p'(q)^{\mu}\,\mathcal{N}_{x|q}(q') \sim \mathcal{N}_{s|f}(r'(s))\,\mathcal{N}_{x|q}(s'), \tag{2.54}$$

$$r'(s)^{\nu}\,\mathcal{N}_{x|s}(s') \sim \mathcal{N}_{q|f}(p'(q))\,\mathcal{N}_{x|s}(q'). \tag{2.55}$$

Proof. Applying the chain rule to $f = p(q) = r(s)$, we get $f' = p'(q)q' = r'(s)s'$. Hence $\mathcal{N}_{x|q}(f') = \mathcal{N}_{x|q}(p'(q))\,\mathcal{N}_{x|q}(q') \sim p'(q)^{\mu}\,\mathcal{N}_{x|q}(q')$ and $\mathcal{N}_{x|q}(f') = \mathcal{N}_{x|q}(r'(s))\,\mathcal{N}_{x|q}(s') \sim \mathcal{N}_{s|f}(r'(s))\,\mathcal{N}_{x|q}(s')$. The last relation holds since K is algebraically closed whence we may write $r'(s) = \mu\prod(s-c_i)$, $c_i \in K$. By Lemma 2.53, $\mathcal{N}_{x|q}(r'(s)) \sim \mu^{\mu}\prod\mathcal{N}_{x|q}(s-c_i) \sim \mu^{\mu}\prod\mathcal{N}_{s|f}(s-c_i) \sim \mathcal{N}_{s|f}(r'(s))$ whence the last relation follows. (2.54) is then an immediate consequence; (2.55) is obtained in a similar way.

2.55. Lemma. *The linear polynomial $x-a_i$ divides $q-a$ if and only if $\mathcal{N}_{x|q}(x-a_i) \sim q-a$, and $x-a_i$ divides $s-a$ if and only if $\mathcal{N}_{x|s}(x-a_i) \sim s-a$. Furthermore $q-a_i$ divides $f-a \in K[q]$ if and only if $\mathcal{N}_{q|f}(q-a_i) \sim f-a$, and $s-a_i$ divides $f-a \in K[s]$ if and only if $\mathcal{N}_{s|f}(s-a_i) \sim f-a$.*

Proof. If $(x-a_i)/(q-a)$, then $q(a_i) = a$, therefore $q-a = q-q(a_i) \sim \mathcal{N}_{x|q}(x-a_i)$, by Lemma 2.53. Conversely $\mathcal{N}_{x|q}(x-a_i) \sim q-a$ implies $q-q(a_i) = q-a$, by Lemma 2.53, hence $(x-a_i)/(q-a)$. In all the other cases, a similar argument can be used.

2.56. By Lemma 2.53 and Lemma 2.55, there is, for each linear factor $q-a_i$ of $p'(q)$, a unique linear polynomial $f-k_i \in K[f]$ which is divisible by $q-a_i$. This polynomial $f-k_i$ is called the linear factor corresponding to $q-a_i$.

2.57. Proposition. *Let $\mu > \nu$. Then the set of linear factors corresponding to the linear factors of $p'(q)$ consists of at most two different polynomials.*

Proof. Let $q-a$ be any linear factor of $p'(q)$, w its multiplicity in $p'(q)$, and $q' = \mu\prod(x-b_i)$. Then $\mathcal{N}_{x|q}(q') \sim \mu^{\mu}\prod\mathcal{N}_{x|q}(x-b_i)$. By Lemma 2.55, the multiplicity of $q-a$ in $\mathcal{N}_{x|q}(q')$ equals the number v of factors $x-b_i$ of q' such that $(x-b_i)/(q-a)$. Hence the multiplicity of $q-a$ on the left-hand side of (2.54) equals $\mu w+v$. Similarly the multiplicity of $q-a$ in $\mathcal{N}_{x|q}(s')$ equals the number t of factors $x-c_i$ of s' such that $(x-c_i)/(q-a)$. The unique linear polynomial $f-k \in K[f]$ which is divisible by $q-a$ is $f-p(a)$. Since $(d/dq)(f-p(a)) = p'(q)$, the multiplicity of $q-a$ in $f-p(a)$ is $w+1$. If $r'(s) = \mu\prod(s-d_i)$, then $\mathcal{N}_{s|f}(r'(s)) \sim \mu^{\mu}\prod\mathcal{N}_{s|f}(s-d_i)$, hence, by Lemma 2.55, the multiplicity of $f-p(a)$ in $\mathcal{N}_{s|f}(r'(s))$ equals the number u of factors $s-d_i$ of r' such that $(s-d_i)/(f-p(a))$. Therefore the multiplicity of $q-a$ on the right-hand side of (2.54) equals $u(w+1)+t$. Hence $\mu w+v = u(w+1)+t$. Moreover $[r'] = \mu-1$ implies $u \leqslant \mu-1 < \mu$, hence

$$\begin{aligned}\mu-2u-t &= \mu w+v-\mu(w-1)-2u-v-t\\ &= u(w+1)-\mu(w-1)-2u-v = (u-\mu)(w-1)-v \leqslant 0,\end{aligned}$$

therefore $\mu \leqslant 2u+t$.

Suppose now that $(q-a_i)/(f-k_i)$, $i = 1, 2, 3$, where $k_1 \neq k_2 \neq k_3 \neq k_1$. Then we obtain the inequalities $\mu \leqslant 2u_i+t_i$, $i = 1, 2, 3$, where u_i, t_i stand for u, t if we substitute a_i for a. Hence $3\mu \leqslant 2(u_1+u_2+u_3)+t_1+t_2+t_3$. But by definition of u_i, t_i, we have $u_1+u_2+u_3 \leqslant \mu-1$, $t_1+t_2+t_3 \leqslant \nu-1 < \mu-1$, thus $3\mu < 3(\mu-1)$, contradiction. This proves the proposition.

2.58. Proposition. *If $\mu > \nu$ and the linear factors corresponding to the linear factors of $p'(q)$ are all equal, then the solution p, q, r, s of (2.1) is conjugate to some power solution.*

Proof. Let $f-k$ be the common linear factor corresponding to the linear factors of $p'(q)$ and $f-k = (q-a_1)^{t_1} \dots (q-a_v)^{t_v}$. If $w_i \geqslant 0$ is the multiplicity of $q-a_i$ in $p'(q)$, then, since $f' = p'(q)$, we have $t_i = w_i+1$. Thus $\nu = \sum_{i=1}^{v} t_i = v+\sum_{i=1}^{v} w_i = v+(v-1)$ hence $v = 1$, therefore $t_1 = \nu$, and

$$p(q) = f = (q-a)^{\nu}+k. \tag{2.56}$$

If ν were not a prime, say $\nu = \sigma\tau$, then $f = \big((q-a)^{\sigma}\big)^{\tau}+k$ whence $K(f) \subset K\big((q-a)^{\sigma}\big) \subset K(q)$, contradiction.

$K(x) = K(s)(q-a)$ implies that $K(x)$ is normal over $K(s)$ since, by (2.56), $q-a$ is a root of $y^{\nu}-\big(r(s)-k\big) \in K(s)[y]$ and K contains the ν-th roots of unity whence $K(s)(q-a)$ is a splitting field of $y^{\nu}-\big(r(s)-k\big)$ over $K(s)$. Furthermore, by a well-known theorem of Galois theory, the Galois group of $K(s)(q-a)$ over $K(s)$ is cyclic, thus $K(x)$ is a cyclic extension of $K(s)$.

By ch. 6, Th. 5.71, the polynomial $s(y)-s \in K(s)[y]$ is irreducible over $K(s)$ and has the root x in $K(x)$, thus $s(y)-s$ splits completely into linear factors over $K(x)$. Therefore $s(y)-s$ has ν different roots v_i, $i = 1, 2, \dots, \nu$, in $K(x)$. Since $K(v_i) = K(x)$, $i = 1, \dots, \nu$, a well-known theorem on transcendental extensions implies that $v_i = (b_ix+c_i)/(d_ix+e_i)$, $b_i, c_i, d_i, e_i \in K$. But $s(v_i) = s(x)$, hence if we substitute for v_i into this equation and multiply by a suitable power of d_ix+e_i, then we see that $(d_ix+e_i)/(b_ix+c_i)^{\nu}$, and we conclude that v_i is a linear polynomial of $K[x]$, $i = 1, \dots, \nu$.

Now let ω be a ν-th root of unity, σ a generator of the Galois group of $K(x)$ over $K(s)$, and

$$l = x+\omega(\sigma x)+\omega^2(\sigma^2 x)+ \dots +\omega^{\nu-1}(\sigma^{\nu-1}x)$$

the Lagrange resolvent. Since the $\sigma^i x$ are just the v_i and since there exists ω such that $K(s)(l) = K(x)$, we have $l = bx+c$ where $b, c \in K$, $b \neq 0$, for such ω. Furthermore $l^{\nu} \in K(s)$ implies $l^{\nu} = g \circ s$, for some $g \in K[x]$, by ch. 6, Lemma 5.81. Comparing the degrees in the last equation, we see that $[g] = 1$. Thus $s = m \circ x^{\nu} \circ l$ where $m, l \in K[x]$ are linear, and (2.56) implies that $p = m_1 \circ x^{\nu} \circ l_1$ where $m_1, l_1 \in K[x]$ are linear.

By substituting into (2.1), we obtain $m_1 \circ x^{\nu} \circ l_1 \circ q = r \circ m \circ x^{\nu} \circ l$, hence, if $0 \neq c \in K$, then $(m_1^{-1} \circ r \circ m) \circ x^{\nu} = (x^{\nu} \circ cx) \circ \big((1/c)x \circ l_1 \circ q \circ l^{-1}\big)$, thus $\big((1/c^{\nu})x \circ m_1^{-1} \circ r \circ m\big) \circ x^{\nu} = x^{\nu} \circ \big((1/c)x \circ l_1 \circ q \circ l^{-1}\big)$. We choose c in such a way that the polynomial in the bracket on the right-hand side and therefore also the polynomial in the bracket on the left-hand side becomes monic. Then the last equation becomes

$$x^{\nu} \circ \bar{q} = \bar{r} \circ x^{\nu} \tag{2.57}$$

where $\bar{q}, \bar{r} \in K[x]$ are monic. Let

$$\bar{q} = x^{\mu}+a_1x^{\mu-1}+ \dots, \quad \bar{r} = x^{\mu}+b_1x^{\mu-1}+ \dots,$$

then $(x^{\mu}+a_1x^{\mu-1}+\dots)^{\nu} = x^{\mu\nu}+b_1x^{\mu\nu-\nu}+\dots$. Coefficientwise comparison yields $a_1 = 0$, hence $a_2 = 0, \dots$, hence $a_{\nu-1} = 0$, similarly $a_{\nu+1} = 0$, $a_{\nu+2} = 0, \dots, a_{\nu+\nu-1} = 0$, etc. Thus $\bar{q} = x^{\mu}+a_{\nu}x^{\mu-\nu}+a_{2\nu}x^{\mu-2\nu}+ \dots +a_{k\nu}x^{\mu-k\nu}$ where $0 < \mu-k\nu < \nu$. If we set $\mu-k\nu = \varrho$, then $\bar{q} = x^{\varrho}t(x^{\nu})$, $t \in K[x]$. If we substitute into (2.57), then $x^{\nu} \circ x^{\varrho}t(x^{\nu}) = \bar{r} \circ x^{\nu}$ whence $\bar{r} \circ x^{\nu} = x^{\varrho}t(x)^{\nu} \circ x^{\nu}$, thus $\bar{r} = x^{\varrho}t(x)^{\nu}$, by Prop. 1.25.

Going back to the definitions of $\bar{q}$, $\bar{r}$, we now obtain

$$s = m \circ x^{\nu} \circ l, \qquad r = (m_1 \circ c^{\nu}x) \circ \bar{r} \circ m^{-1},$$
$$q = (l_1^{-1} \circ cx) \circ \bar{q} \circ l, \qquad p = m_1 \circ x^{\nu} \circ l_1 = (m_1 \circ c^{\nu}x) \circ x^{\nu} \circ \big((1/c)x \circ l_1\big)$$

and the proposition now follows from § 2.3.

2.6. By Prop. 2.57, we have now to investigate the case where the set of linear factors corresponding to the linear factors of $p'(q)$ consists of two different polynomials. We state Hypothesis (H): $f-k$, $f-k_1$ are the linear factors corresponding to the linear factors of $p'(q)$.

The assumption $\mu > \nu$ will not be needed.

2.61. Lemma. *If every linear factor of $f-k \in K[q]$ is a divisor of $p'(q)$, then $f-k_1$ has at least three different linear factors that are not divisors of $p'(q)$.*

Proof. By hypothesis, $f-k = (q-a_1)^{v_1+1} \dots (q-a_m)^{v_m+1}$ where $a_i \neq a_j$, for $i \neq j$, and $v_i > 0$, $i = 1, \dots, m$, since $(f-k)' = p'(q)$. Thus the greatest common divisor d of $f-k$ and $p'(q)$ is of degree $[d] = \sum_{i=1}^{m} v_i$. If $v_i = 1$, for $i = 1, \dots, m$, then $f-k$ would be the square of some polynomial $g \in K[q]$ whence $K(f) = K(f-k) = K(g^2)$, therefore $K(f) \subset K(g) \subseteq K(q)$, thus $K(g) = K(q)$ and $[g] = m = 1$. This would imply that $f-k = (q-a_1)^2$, hence $[p] = 2$, $[p'] = 1$. But the only linear factor of p'

cannot divide $f-k$ and $f-k_1$ simultaneously, by §2.56. Hence $\sum_{i=1}^{m} v_i > m$, furthermore $m+\sum_{i=1}^{m} v_i = [p] = v$, therefore $\sum_{i=1}^{m} v_i > (1/2)v$. Let d_1 be the greatest common divisor of $f-k_1$ and $p'(q)$. Then d and d_1 are relatively prime since $f-k$ and $f-k_1$ are, hence $(dd_1)/p'(q)$, thus $[dd_1] \leqslant v-1$. This implies $[d_1] \leqslant v-1-[d] < v/2-1$.

Let $f-k_1 = (q-c_1)^{w_1+1} \dots (q-c_n)^{w_n+1}$ where $c_i \neq c_j$, for $i \neq j$, then $[d_1] = \sum_{i=1}^{n} w_i$, therefore $\sum_{i=1}^{n} w_i < v/2-1$. Hence $n = v-\sum_{i=1}^{n} w_i > v/2+1$. If l is the number of indices i such that $w_i = 0$, then $v \geqslant l+2(n-l)$ whence $l \geqslant 2n-v > 2$, Q. E. D.

2.62. Lemma. *If the polynomial $f-k \in K[s]$ contains at least one linear factor $s-b$ which is not a divisor of $r'(s)$, and the polynomial $f-k_1 \in K[s]$ contains at least one such linear factor $s-b_1$ then each of these polynomials contains exactly one such linear factor, the polynomials satisfy the equation*

$$\mu^2(f-k)(f-k_1) = (s-b)(s-b_1)r'(s)^2,$$

and every linear factor of $r'(s)$ is either a divisor of $f-k$ or of $f-k_1$, but not all the linear factors of $r'(s)$ divide one and the same of these polynomials.

Proof. By hypothesis (H) we see that, $\mathcal{H}_{q|f}(p'(q)) = \mathcal{H}_{q|f}(v\prod(q-a_i)) \sim v^v(f-k)^v(f-k_1)^{v_1}$ where $v+v_1 = v-1$ and $vv_1 \neq 0$. Hence, by (2.55),

$$r'(s)^v \mathcal{H}_{x|s}(s') \sim v^v(f-k)^v(f-k_1)^{v_1}\mathcal{H}_{x|s}(q'). \tag{2.61}$$

Now let g be the product of all linear factors of $f-k$, and g_1 be the product of all linear factors of $f-k_1$, which do not divide $r'(s)$, then, by (2.61), $g^v g_1^{v_1}/\mathcal{H}_{x|s}(s')$. But, by (2.51), $\mathcal{H}_{x|s}(s')$ is a polynomial in s of degree $v-1$ whence $[g] = [g_1] = 1$, and the first assertion of the lemma is proved. Let $f-k = (s-b)(s-c_1)^{e_1} \dots (s-c_m)^{e_m}$ be the decomposition into linear factors of $f-k \in K[s]$, then $e_i \geqslant 2$, $i = 1, \dots, m$, hence $\mu = 1+\sum_{i=1}^{m} e_i \geqslant 1+2m$, thus $m \leqslant (\mu-1)/2$. Since $\sum_{i=1}^{m}(e_i-1)+m = \mu-1$, we have $\sum_{i=1}^{m}(e_i-1) \geqslant (\mu-1)/2$, therefore the greatest common divisor of

$r'(s)$ and $f-k$ is of degree $\geqslant (\mu-1)/2$. Similarly, the greatest common divisor of $r'(s)$ and $f-k_1$ is of degree $\geqslant (\mu-1)/2$. But since $f-k$ and $f-k_1$ are relatively prime, so are those greatest common divisors, thus their product divides $r'(s)$. But $[r'] = \mu-1$ whence each of these greatest common divisors is of degree $(\mu-1)/2$. Hence $\sum_{i=1}^{m}(e_i-1) = (\mu-1)/2$, implying that $m = (\mu-1)/2$, $e_i = 2$, $i = 1, \dots, m$. Thus

$$\begin{aligned} f-k &= (s-b)(s-c_1)^2 \dots (s-c_m)^2, \\ f-k_1 &= (s-b_1)(s-c_{11})^2 \dots (s-c_{m1})^2. \end{aligned} \tag{2.62}$$

Since $(s-c_1) \dots (s-c_m)(s-c_{11}) \dots (s-c_{m1})$ is a divisor of $r'(s)$ of degree $\mu-1$, we have

$$r'(s) = \mu(s-c_1) \dots (s-c_m)(s-c_{11}) \dots (s-c_{m1}) \tag{2.63}$$

which proves the second assertion of the lemma. The third assertion is a straightforward consequence of (2.62) and (2.63).

2.63. Remark. For proving (2.62) and (2.63), we required only the first statement of Lemma 2.62, but not hypothesis (H).

2.64. Lemma. *If $f-k$, $f-k_1 \in K[s]$ satisfy the hypothesis of Lemma 2.62, then each of the polynomials $f-k \in K[q]$ and $f-k_1 \in K[q]$ contains at least one linear factor that is not a divisor of $p'(q)$.*

Proof. We evaluate $\mathcal{H}_{s|f}(r'(s))$, using (2.62), (2.63), and Lemma 2.55, and then substitute into (2.54):

$$p'(q)^\mu \mathcal{H}_{x|q}(q') \sim \mathcal{H}_{x|q}(s')\,\mu^\mu(f-k)^{(\mu-1)/2}(f-k_1)^{(\mu-1)/2}. \tag{2.64}$$

Suppose that every linear factor of $f-k$ divides $p'(q)$, then, by Lemma 2.61, $f-k_1$ has at least three different linear factors that are not divisors of $p'(q)$. Let g be the product of these linear factors, then, by (2.64), $g^{(\mu-1)/2}/\mathcal{H}_{x|q}(q')$. But this is a contradiction since $[g] = 3$ whereas $[\mathcal{H}_{x|q}(q')] = \mu-1$. A similar argument works for $f-k_1$.

2.65. Lemma. *If the polynomials $f-k \in K[s]$, $f-k_1 \in K[s]$ satisfy the hypothesis of Lemma 2.62, then the polynomial $f-k \in K[q]$ contains exactly one linear factor $q-a$ that does not divide $p'(q)$, and $f-k_1 \in K[q]$*

contains exactly one linear factor $q-a_1$ that does not divide $p'(q)$. Moreover there are elements $d \neq d_1 \in K$ such that

$$\mu^2(q-a)(q-a_1) = (x-d)(x-d_1)q'(x)^2.$$

Proof. By the last statement of Lemma 2.62 and Lemma 2.64, we see that hypothesis (H) and the hypothesis of Lemma 2.62 is also satisfied for the solution r, s, p, q of equation (2.1), i.e. the statements of Lemma 2.62 hold if r, p and s, q change their places in the hypothesis. Hence Lemma 2.62 implies that $f-k$ contains exactly one linear factor $q-a$ that does not divide $p'(q)$, and $f-k_1$ contains exactly one linear factor $q-a_1$ that does not divide $p'(q)$. By (2.64), $(q-a)^{(\mu-1)/2}(q-a_1)^{(\mu-1)/2}/\mathcal{H}_{x|q}(q')$ whence

$$\mathcal{H}_{x|q}(q') \sim \mu^{\mu}(q-a)^{(\mu-1)/2}(q-a_1)^{(\mu-1)/2}. \tag{2.65}$$

If $q-a = (x-t_1)^{w_1+1} \ldots (x-t_n)^{w_n+1}$ is the decomposition of $q-a$ into linear factors of $K[x]$, $t_i \neq t_j$, for $i \neq j$, then Lemma 2.55 and Lemma 2.53 imply

$$f-k \sim \mathcal{H}_{q|f}(q-a) \sim \mathcal{H}_{x|s}(q-a) \sim (s-s(t_1))^{w_1+1} \ldots (s-s(t_n))^{w_n+1}.$$

But then (2.62) implies $w_i \leqq 1$, $i = 1, \ldots, n$. By (2.65), $q'(x)$ has exactly $(\mu-1)/2 = m$ linear factors which divide $q-a$ and $w_i \leqq 1$ implies that all these linear factors are different. Hence $w_i = 1$, for exactly $(\mu-1)/2$ indices i. Thus

$$\begin{aligned} q-a &= (x-d)(x-e_1)^2 \ldots (x-e_m)^2, \\ q-a_1 &= (x-d_1)(x-e_{11})^2 \ldots (x-e_{m1})^2. \end{aligned} \tag{2.66}$$

A similar argument as in Lemma 2.62 completes the proof.

2.7. Proposition. *If hypothesis* (H) *and the hypothesis of Lemma* 2.62 *are satisfied, then the solution p, q, r, s of* (2.1) *is conjugate to some Čebyshev solution.*

Proof. We require two lemmas which will be proved first.

2.71. Lemma. *Let σ be any positive integer. Then the differential equation*

$$\sigma^2(1-z^2) = (1-x^2)z'^2 \tag{2.71}$$

has the solutions $z = \pm t_\sigma(x)$, and these are the only solutions which are polynomials over K of degree σ.

Proof. Suppose that $z = a_0x^\sigma + a_1x^{\sigma-1} + \ldots + a_\sigma$ is a solution of (2.71). From substituting z into (2.71), we get for $i = 1, 2, \ldots, \sigma$,

$$-\sigma^2(2a_0a_i + w(a_1, \ldots, a_{i-1})) = -(2\sigma a_0(\sigma-i)a_i + v(a_0, a_1, \ldots, a_{i-1}))$$

where $w(x_1, \ldots, x_{i-1})$ and $v(x_0, \ldots, x_{i-1})$ are quadratic forms over the rational integers. Hence $2\sigma i a_0 a_i = f(a_0, \ldots, a_{i-1})$ where $f(x_0, x_1, \ldots, x_{i-1})$ is some quadratic form over the integers which is independent of z. Therefore

$$2\sigma i(a_i/a_0) = f(1, a_1/a_0, \ldots, a_{i-1}/a_0), \qquad i = 1, 2, \ldots, \sigma.$$

Hence $a_i/a_0 = \lambda_i$, $i = 1, \ldots, \sigma$, is a rational which does not depend on z. Thus, if t is any polynomial of degree σ which is a solution of (2.71), then every polynomial z of degree σ which is a solution of (2.71) satisfies $z = ct$ where $c \in K$. We substitute $z = ct$ into (2.71) and obtain $\sigma^2(1-c^2t^2) = (1-x^2)c^2t'^2 = c^2\sigma^2(1-t^2)$, hence $c = \pm 1$. Conversely $z = \pm t$ is a solution of (2.71). Moreover, $z = t_\sigma(x)$ is a solution of (2.71) by Lemma 2.44 (iii).

2.72. Lemma. *Let σ be any positive integer, $u, u_1, v, v_1, u \neq u_1, v \neq v_1$, any elements of K and $y = y(x)$ a polynomial of degree σ over K which satisfies the differential equation*

$$\sigma^2(y-u)(y-u_1) = (x-v)(x-v_1)y'^2. \tag{2.72}$$

Then there exist linear polynomials $l = ax+b$, $m = cx+d$ such that $z = l \circ y \circ m$ is a solution of (2.71).

Proof. By (2.72), $\sigma^2(y \circ m-u)(y \circ m-u_1) = (m-v)(m-v_1)(y' \circ m)^2$. Since $z' = a(y' \circ m)c$, we have

$$a^2c^2\sigma^2(l^{-1} \circ z-u)(l^{-1} \circ z-u_1) = (m-v)(m-v_1)z'^2.$$

Now we choose m, l suitably, namely

$$m = \tfrac{1}{2}(v_1-v)x + \tfrac{1}{2}(v_1+v), \quad l^{-1} = \tfrac{1}{2}(u_1-u)x + \tfrac{1}{2}(u_1+u). \tag{2.73}$$

Then the last equation becomes

$$\begin{aligned} \sigma^2[(v_1-v)^2/(u_1-u)^2] \cdot \tfrac{1}{2}(u_1-u)(z+1) \cdot \tfrac{1}{2}(u_1-u)(z-1) = \\ = \tfrac{1}{2}(v_1-v)(x+1) \cdot \tfrac{1}{2}(v_1-v)(x-1)z'^2 \end{aligned}$$

whence z is a solution of (2.71).

2.73. Proof of Proposition 2.7. By Lemma 2.62 and Lemma 2.65,

$$\begin{aligned}\mu^2(f-k)(f-k_1) &= (s-b)(s-b_1)r'(s)^2,\\ \mu^2(q-a)(q-a_1) &= (x-d)(x-d_1)q'(x)^2\end{aligned} \tag{2.74}$$

The proof of Lemma 2.65 shows that hypothesis (H) and the hypothesis of Lemma 2.62 are also satisfied for the solution r, s, p, q of (2.1), thus

$$\begin{aligned}\nu^2(f-k)(f-k_1) &= (q-a)(q-a_1)p'(q)^2,\\ \nu^2(s-b)(s-b_1) &= (x-d)(x-d_1)s'(x)^2.\end{aligned} \tag{2.75}$$

That a, a_1 and b, b_1 actually change their roles in (2.74), (2.75), follows from Lemma 2.62 and Lemma 2.65. That d, d_1 in (2.74), (2.75) are the same follows since $x-d, x-d_1$ are the only simple linear factors of $q-a$ and $q-a_1$, resp., by (2.66), and $q-a$, $q-a_1$ are the only simple linear factors of $f-k, f-k_1$, resp., by Lemma 2.65 whence, in both cases, $x-d, x-d_1$ are the only simple linear factors in $K[x]$ of $f-k, f-k_1$, resp.

Now (2.74), (2.75) are differential equations of the type as in (2.72), hence, by Lemma 2.72 and Lemma 2.71,

$$\begin{aligned} r(s) &= l_1^{-1}\circ\varepsilon_1 t_\mu\circ m_1^{-1}, \quad & q(x) &= l_2^{-1}\circ\varepsilon_2 t_\mu\circ m_2^{-1},\\ p(q) &= l_3^{-1}\circ\varepsilon_3 t_\nu\circ m_3^{-1}, \quad & s(x) &= l_4^{-1}\circ\varepsilon_4 t_\nu\circ m_4^{-1},\\ & \varepsilon_i = \pm 1, \quad i = 1,\dots,4.\end{aligned}$$

(2.73) implies $m_2^{-1} = m_4^{-1} = n$, $l_2^{-1} = m_3$, $l_4^{-1} = m_1$. Since $t_\sigma\circ\varepsilon_i x = (\varepsilon_i^\sigma x)\circ t_\sigma$ by Lemma 2.44 (ii) we obtain

$$\begin{aligned} q &= m_3\circ\varepsilon_2 x\circ t_\mu\circ n, & s &= m_1\circ\varepsilon_4 x\circ t_\nu\circ n,\\ p &= l_3^{-1}\circ\varepsilon_3 x\circ\varepsilon_2^\nu x\circ t_\nu\circ\varepsilon_2 x\circ m_3^{-1}, & r &= l_1^{-1}\circ\varepsilon_1 x\circ\varepsilon_4^\mu x\circ t_\mu\circ\varepsilon_4 x\circ m_1^{-1},\end{aligned}$$

and the proposition follows.

2.8. The proof of Th. 2.46 has now boiled down to showing that hypothesis (H) implies the hypothesis of Lemma 2.62. Throughout this subsection, we will assume that $\mu > \nu$ and hypothesis (H) holds.

2.81. Proposition. *Hypothesis* (H) *and* $\mu > \nu$ *imply that the hypothesis of Lemma* 2.62 *is satisfied.*

Proof. We will again require a few lemmas to prove the proposition.

2.82. Lemma. *If* $c \in K$, $(q-a)/(f-c)$, $(s-b)/(f-c)$, *then the polynomials* $q-a$, $s-b \in K[x]$ *have at least one linear factor in common.*

Proof. Let $f-c = (s-b)^m f_1$ where f_1 is not divisible by $s-b$. Coprimality of $s-b$ and f_1 then implies $u(s-b)+vf_1 = 1$, for some polynomials

$u, v \in K[s]$, hence $s(x)-b$ and $f_1(s(x))$ are also relatively prime in $K[x]$. If $q-a$ and $s-b$ were relatively prime, we would have $(q-a)/f_1(s(x)$ whence $f_1(s(x)) = (q(x)-a)h(x)$, for some $h(x) \in K[x]$. Hence $\mathcal{H}_{x|s}(f_1(s(x))) = \mathcal{H}_{x|s}(q(x)-a)\mathcal{H}_{x|s}(h(x))$. Lemma 2.53 and Lemma 2.55 imply $f_1(s)^\nu \sim (f-c)g(s)$, for some $g(s) \in K[s]$ whence $(s-b)/f_1(s)$, contradiction.

2.83. Lemma. *Let* $f-k = \prod_{i=1}^{m}(q-a_i)^{u_i} = \prod_{j=1}^{n}(s-b_j)^{v_j}$ *where the* a_i *and* b_j, *resp., are pairwise distinct elements of* K. *If* $u_i > 1$, *then* $q-a_i$ *and* $s'(x)$ *have some divisor* $x-c_i$ *in common. If* $v_j > 1$, *then* $s-b_j$ *and* $q'(x)$ *have some divisor* $x-c_j$ *in common.*

Proof. Let $x-c_i$ be a linear factor of $q-a_i$ of multiplicity g_i, then $x-c_i$ is a linear factor of $f-k$ of multiplicity $g_i u_i$. There is one and only one index j such that $(x-c_i)/(s-b_j)$. If e_{ij} is the multiplicity of $x-c_i$ as a factor of $s-b_j$, then $x-c_i$ has the multiplicity $e_{ij}v_j$ as a factor of $f-k$. Suppose that $q-a_i$ and $s'(x)$ are relatively prime, then $e_{ij} = 1$, hence $v_j = g_i u_i$. By Lemma 2.82, every $s-b_j$ has some linear factor in common with $q-a_i$ whence every v_j is divisible by u_i. Therefore $f-k = h(s)^{u_i}$, for some $h(s) \in K[s]$. This implies $K(f) = K(h^{u_i}) \subset K(h) \subseteq K(s)$. Hence $K(h) = K(s)$, $[h(s)] = 1$. Therefore $u_i = [r] = \mu$. But $f = k+\prod(q-a_i)^{u_i}$ and $[q] = \mu$ imply $\mu\nu = [f] \geqq \mu^2$ which contradicts $\mu > \nu$. Hence $q-a_i$ and $s'(x)$ have some linear factor in common. To prove the second assertion, we proceed in an analogous way to before and get $f-k = h(q)^{v_j}$, for some $h(q) \in K[q]$. Again $[h(q)] = 1$ and $v_j = [p] = \nu$. Hence $f = k+(q-a)^\nu$, thus $p'(q) = \nu(q-a)^{\nu-1}$ which contradicts hypothesis (H). Hence $s-b_j$ and $q'(x)$ have some linear factor in common if $v_j > 1$.

2.84. For the remainder of this subsection, we now assume that every linear factor of $f-k \in K[s]$ is a divisor of $r'(s)$. This will finally lead to a contradiction and thus will prove Lemma 2.62 so far as $f-k$ is concerned. But also the statement about $f-k_1$ will follow for reasons of symmetry.

2.85. Lemma. *Let* $f-k \in K[s]$ *have* n *different linear factors, then* $n < \mu/2$.

Proof. By hypothesis, every linear factor of $f-k \in K[s]$ is a divisor of $r'(s)$, thus every such linear factor has multiplicity $v_j > 1$ in $f-k$. Since

$\sum_{j=1}^{n} v_j = \mu$, we have $n \leqslant \mu/2$. If $n = \mu/2$, then $v_j = 2$, for $j = 1, \ldots, n$, whence $f-k = h(s)^2$ for some $h(s) \in K[s]$. As in the proof of Lemma 2.83, we would have $\mu = 2$, hence $v = 1$, contradiction. Hence $n < \mu/2$.

2.86. Lemma. *Let m be the number of all linear factors of $r'(s)$ which divide $f-k_1$. Then $m < \mu/4$.*

Proof. The number of all linear factors of $r'(s)$ dividing $f-k$ equals $\sum_{j=1}^{n} (v_j-1) = \mu-n$. By Lemma 2.85, $\mu-n = (\mu/2)+j$ where $j > 0$. Hence, by Lemma 2.55,

$$\mathcal{R}_{s\,|\,f}(r'(s)) \sim (f-k)^{(\mu/2)+j}(f-k_1)^m h(f) \tag{2.81}$$

where $h(f)$ and $(f-k)(f-k_1)$ are relatively prime. By (2.54),

$$p'(q)^{\mu}\mathcal{R}_{x\,|\,q}(q') \sim (f-k)^{(\mu/2)+j}(f-k_1)^m h(f)\mathcal{R}_{x\,|\,q}(s'). \tag{2.82}$$

Hence, if $(q-a)/(f-k)$ but $q-a$ does not divide $p'(q)$, then $(q-a)^{(\mu/2)+j}/\mathcal{R}_{x\,|\,q}(q')$. Since $[q'] = \mu-1$, there is at most one such $q-a$.

Suppose that e different factors $q-b_i$ of $f-k_1$ are not divisors of $p'(q)$. By (2.82), each of these factors occurs in $\mathcal{R}_{x\,|\,q}(q')$ with multiplicity $\geqslant m$. If t is the multiplicity of $q-b_i$ in $\mathcal{R}_{x\,|\,q}(q')$, then exactly t of the linear factors of $q'(x)$ are divisors of $q-b_i$. If $x-c$ is such a linear factor and v its multiplicity in $q'(x)$, then $(x-c)/(f(x)-k_1)$. Since $(f(x)-k_1)' = p'(q(x))q'(x)$, we see that $x-c$ has multiplicity v in the greatest common divisor d of $f(x)-k_1$ and $q'(x)$. Thus d is divisible by some product of linear factors of $q-b_i$ which has degree $t \geqslant m$. Hence $[d] \geqslant em$. On the other hand, (2.81) implies that $\mu-n+m = (\mu/2)+j+m \leqslant \mu-1$, thus $n \geqslant m+1$. Then, by Lemma 2.83, there are at least $m+1$ different linear factors of $q'(x)$ which are divisors of $f(x)-k$. Hence $[d] \leqslant \mu-m-2$, thus $em \leqslant \mu-m-2$. Therefore $m(e+1) < \mu$. By way of contradiction, assume now that $m \geqslant \mu/4$. Then $(\mu/4)(e+1) < \mu$ whence $e \leqslant 2$. Suppose that $f-k$ has no linear factor $q-a$ which is not a divisor of $p'(q)$, then, by Lemma 2.61, $e \geqslant 3$. Hence there is exactly one $q-a$ dividing $f-k$ but not dividing $p'(q)$. Then (2.82) implies that $(q-a)^{(\mu/2)+j}/\mathcal{R}_{x\,|\,q}(q')$ whence $(\mu/2)+j$ linear factors of $q'(x)$ divide $q-a$ and therefore also $f(x)-k$. Hence $[d] \leqslant \mu-1-(\mu/2)-j < \mu/2$. This implies $em < \mu/2$, thus $e(\mu/4) < \mu/2$ and $e \leqslant 1$. If $e = 0$, then, by Lemma 2.61, $f-k$ would

have at least three different linear factors $q-a$ not dividing $p'(q)$, contradiction. Thus $e = 1$. We summarize: There is exactly one linear factor $q-a$ of $f-k$ that is not a divisor of $p'(q)$ and exactly one linear factor $q-\bar{a}_1$ of $f-k_1$ that is not a divisor of $p'(q)$. Remark 2.63 implies that

$$\begin{aligned} f-k &= (q-a)(q-a_1)^2 \ldots (q-a_l)^2, \\ f-k_1 &= (q-\bar{a}_1)(q-a_{11})^2 \ldots (q-a_{l1})^2, \\ p'(q) &= v(q-a_1) \ldots (q-a_l)(q-a_{11}) \ldots (q-a_{l1}) \end{aligned} \tag{2.83}$$

where $l = (v-1)/2$. By Lemma 2.83, each $q-a_i$ has some divisor $x-c_i$ and each $q-a_{i1}$ has some divisor $x-c_{i1}$, which is also a divisor of $s'(x)$. Since all these divisors are different we see that $s'(x) = v(x-c_1) \ldots (x-c_l)(x-c_{11}) \ldots (x-c_{l1})$ and therefore

$$\mathcal{R}_{x\,|\,q}(s'(x)) \sim v^{\mu}(q-a_1) \ldots (q-a_l)(q-a_{11}) \ldots (q-a_{l1}). \tag{2.84}$$

Substitution of (2.83) and (2.84) into (2.82) yields, after computing the exponents of $q-a_{11}$ on either side of (2.82), the inequality $2m+1 \geqslant \mu$ whence $m \geqslant (\mu-1)/2$. On the other hand, (2.81) implies that $(\mu/2)+j+m \leqslant \mu-1$ whence $m < (\mu-1)/2$, contradiction. Hence $m < \mu/4$.

2.87. Proof of Proposition 2.81. It remains to lead the assumption made in § 2.84 to a contradiction. By hypothesis (H), there is at least one linear factor $q-a$ of $f-k$ which divides $p'(q)$. Therefore $q-a$ has multiplicity $u > 1$ in $f-k$. By Lemma 2.83, there is a linear factor $x-c$ dividing $q-a$ and $s'(x)$ whence the degree of the greatest common divisor of $f-k_1$ and $s'(x)$ is at most $v-2$. If $v = 2$, then $[p'] = 1$ which contradicts hypothesis (H). Hence $v > 2$. Thus we can find an integer g which is maximal with respect to $g(v-2) \leqslant \mu$, and $\mu > v$ implies that $g \geqslant 1$. Let $d \geqslant 1$ be the number of different factors $q-b_i$ of $f-k_1$ which are divisors of $p'(q)$ and w_i their multiplicities in $p'(q)$. Then (2.82) implies that

$$\mu w_i + u_i = m(w_i+1)+t_i \tag{2.85}$$

where u_i, t_i are suitable non-negative integers. Hence $(\mu-m)w_i = m+t_i-u_i$. By Lemma 2.86, $(3/4)\mu w_i < (\mu/4)+t_i-u_i$. Since $w_i \geqslant 1$, we have $t_i > 0$. Suppose that $t_i > \mu/gd$, for every index i, then $\sum t_i > \mu/g$. But t_i is just the number of linear factors of $s'(x)$ dividing $q-b_i$. If v is the multiplicity of such a linear factor $x-c$ in $s'(x)$, then $(x-c)/(f(x)-k_1)$

and $(f(x)-k_1)' = r'(s(x))s'(x)$ implies that $x-c$ has multiplicity v in the greatest common divisor of $f(x)-k_1$ and $s'(x)$. Hence this greatest common divisor is divisible by the product of these t_i linear factors of $s'(x)$, and thus has degree $\geqslant \sum t_i$. Therefore

$$\sum t_i \leqslant v-2. \tag{2.86}$$

This implies $\mu/g < v-2$, contradicting the definition of g. Hence there is at least one index j such that $t_j \leqslant \mu/gd$. By (2.85), $\mu w_j \leqslant m(w_j+1)+t_j \leqslant m(w_j+1)+\mu/gd$ whence by Lemma 2.86, $\mu/4 > m \geqslant (\mu/g(w_j+1))(w_j-1/gd)$. Hence $w_j+1 > 4w_j-4/gd$, thus $3w_j < 1+4/gd \leqslant 5$. Therefore $w_j = 1$. Thus $3 < 1+4/gd$ whence $gd < 2$. This can only be the case if $g = d = 1$. By definition of g, this means that $2(v-2) > \mu$ while the definition of d shows that $f-k_1$ has exactly one factor $q-b$ which divides $p'(q)$. Since $w_j = 1$, this factor has multiplicity 1 in $p'(q)$, hence multiplicity 2 in $f-k_1$. Hence $f-k_1$ has $v-2$ linear factors which are not divisors of $p'(q)$. Then, by (2.82), $\mathcal{H}_{x|q}(q')$ is divisible by at least $m(v-2)$ linear factors whence $\mu-1 \geqslant m(v-2)$. Therefore $m(v-2) < \mu$, hence $m \leqslant 1$. Substitution of $w_i = 1$ into (2.85) yields $\mu+u_i = 2m+t_i \leqslant 2+t_i$. But $2+t_i \leqslant v$ by (2.86). Hence $\mu \leqslant v$ which is the contradiction we needed, and the proposition is proved.

2.9. Proof of Theorem 2.46. By Prop. 2.5, every non-trivial standard solution of (2.1) is either of the form p, q, r, s or of the form r, s, p, q where p, q, r, s is a standard solution of (2.1) such that $[q] = [r] = \mu$, $[p] = [s] = v$, and $\mu > v$. By Prop. 2.57, Prop. 2.58, Prop. 2.81, and Prop. 2.7, this solution is conjugate to some power solution or to some Čebyshev solution.

3. Permutable chains over fields and integral domains

3.1. Let R be any commutative ring with identity and $\langle R[x]; \circ \rangle = S$. If $|R| > 1$, then S is a non-commutative semigroup, for $ax \circ (x+1) \neq (x+1) \circ ax$ if $a \neq 1$. The problem of determining all the commutative subsemigroups of S seems to be rather difficult. If R is an integral domain and C any commutative subsemigroup of S, then Cor. 1.23 implies that the set of the degrees of the polynomials in C constitutes a subsemigroup of the multiplicative semigroup of non-negative integers. C is called a permutable chain, or a P-chain (over R) if every polynomial in C is of

degree > 0, and for any $k > 0$, there exists a polynomial in C of degree k. This section is devoted to determining all the P-chains over fields and various other types of integral domains.

3.2. Let K be any field, $C = \{g_i | i \in I\}$ a P-chain and $l \in K[x]$ a linear polynomial. Evidently $C_1 = \{l^{-1} \circ g_i \circ l | i \in I\}$ is a P-chain, too. C_1 is called a conjugate (over K) of C. Also $l^{-1} \circ g \circ l$ and g will be called conjugate. Clearly conjugacy is an equivalence relation on the set of all P-chains over K and therefore induces some partition of this set. Thus all the P-chains over K will be known as soon as we are able to pick one representative for each class of this partition.

3.3. Two special P-chains are already known to us:

a) $\{x, x^2, x^3, \ldots\} = S$ is a P-chain over K being called the P-chain of powers.

b) By Lemma 2.44 (i), $\{t_1, t_2, t_3, \ldots\}$, t_i the i-th Čebyshev polynomial, is a P-chain over the field of rational numbers, thus $\{g_n = (2x) \circ t_n \circ (\frac{1}{2}x) | n = 1, 2, \ldots\}$ is also a P-chain over the field of rational numbers. Let us put $s_n = e^{in\varphi} + e^{-in\varphi}$, $n = 0, 1, 2, \ldots$, then $s_n s_1 = (e^{in\varphi} + e^{-in\varphi})(e^{i\varphi} + e^{-i\varphi}) = s_{n+1} + s_{n-1}$, $n = 1, 2, \ldots$. Hence $s_{n+1} = s_n s_1 - s_{n-1}$, $n = 1, 2, \ldots$, therefore

$$s_2 = s_1^2 - 2, \quad s_3 = s_1^3 - 3s_1 \tag{3.3}$$

and, by induction on n, we easily see that $s_n = f_n(s_1)$ where f_n is some monic polynomial of degree n over the rational integers. But the definition of s_n and Euler's formula imply that $s_n = 2 \cos n\varphi$ whence $2t_n(\cos \varphi) = 2 \cos n\varphi = f_n(s_1) = f_n(2 \cos \varphi)$. Thus $2t_n(x) = f_n(2x)$, hence $f_n = (2x) \circ t_n \circ (\frac{1}{2})x = g_n$, therefore g_n is monic.

3.31. Remark. Induction on n shows that the coefficient of x^{n-1} in the normal form of $f_n = g_n$ is zero, for $n \geqslant 2$.

3.32. Let $\mathbf{Z}$ be the domain of rational integers, L the prime field of K, $\eta : \mathbf{Z} \to L$ the unique ring homomorphism, and $\eta[x] : \mathbf{Z}[x] \to \eta\,\mathbf{Z}[x]$ the unique extension of η to a composition epimorphism (see ch. 3, § 3.22). Then $\{\eta[x]g_1, \eta[x]g_2, \ldots\} = T$ is a P-chain over $\eta\,\mathbf{Z}$. Since, by ch. 1, § 8.1, $\eta\,\mathbf{Z}[x]$ can be embedded into $K[x]$, we see that T is also a P-chain over K being called the P-chain of Čebyshev polynomials.

3.33. Theorem. *Every P-chain over K is some conjugate of either the P-chain of powers or the P-chain of Čebyshev polynomials. Thus there are exactly two different classes of P-chains over K.*

Proof. We require several lemmas which will fill the remainder of the subsequent subsection before we prove the theorem.

3.4. The second statement of the theorem on the non-conjugacy of the P-chains of powers and of Čebyshev polynomials can easily be seen: Let $l = ax+b$, then $l^{-1} \circ x^n \circ l = (1/a)(ax+b)^n - (b/a)$ where, for some $n \geqslant 2$, the coefficient of x^{n-1} differs from zero unless $b = 0$. Thus if $l^{-1} \circ x^n \circ l = g_n$, for all n, then $b = 0$ by Remark 3.31 whence $a^{n-1} = 1$, for all n. Therefore $a = 1$, but $S \neq T$ by (3.3), contradiction.
Let us now assume that K is algebraically closed.

3.41. Lemma. *If char $K \neq 2$ and $g \in K[x]$ is any polynomial of degree 2, then, for any $n \geqslant 1$, there exists at most one polynomial of degree n that is permutable with g. If char $K = 2$ and $g \in K[x]$ is any polynomial of degree 3, then, for any $n \geqslant 1$, there exists at most one polynomial of degree n that is permutable with g.*

Proof. Let char $K \neq 2$, $g = ax^2+bx+c$, $a \neq 0$, and $f = \sum_{i=0}^{n} a_i x^{n-i}$ of degree n and permutable with g, i.e. $g \circ f = f \circ g$. Then equating the coefficients of x^{2n} we obtain $aa_0^2 = a_0 a^n$ whence $a_0 = a^{n-1}$. The coefficients of x^{2n-i}, $i = 1, 2, \ldots, n-1$, on either side yield the equations

$$a(2a_0 a_i + q(a_1, a_2, \ldots, a_{i-1})) = l(a_0, a_1, \ldots, a_{i-1})$$

where q is a quadratic and l is a linear form over K. Thus $a_0, a_1, \ldots, a_{i-1}$ determine a_i uniquely, for $i = 1, \ldots, n-1$. Moreover, the coefficient of x^n on either side yields the equation

$$a(2a_0 a_n + q(a_1, a_2, \ldots, a_{n-1})) + ba_0 = l(a_0, a_1, \ldots, a_{n-1})$$

where again q is a quadratic and l is a linear form over K. Thus a_n is uniquely determined by $a_0, a_1, \ldots, a_{n-1}$.

If char $K = 2$, then let $g = ax^3+bx^2+cx+d$, $a \neq 0$ and $f = \sum_{i=0}^{n} a_i x^{n-i}$ a polynomial of degree n which is permutable with g. Again $g \circ f = f \circ g$ yields some conditions for the coefficients of x^{3n} and x^{3n-i}, $i = 1, \ldots, n$. In particular, the coefficients of x^{3n} give us $aa_0^3 = a_0 a^n$ whence $a_0^2 = a^{n-1}$ and since char $K = 2$, we see that a_0 is uniquely determined by a. The coefficients of x^{3n-i}, $i = 1, \ldots, n-1$ yield the equations

$$a(3a_0^2 a_i + c(a_0, \ldots, a_{i-1})) = l(a_0, a_1, \ldots, a_{i-1})$$

where c is a cubic and l is a linear form over K. Similarly,

$$a(3a_0^2 a_n + c(a_0, \ldots, a_{n-1})) + ba_0^2 = l(a_0, a_1, \ldots, a_{n-1})$$

where c is a cubic and l is a linear form over K. Thus again a_i, $i = 1, \ldots, n$, is uniquely determined by $a_0, a_1, \ldots, a_{i-1}$.

3.42. Corollary. *If P is any P-chain over K, then P contains exactly one polynomial of degree n, for every $n \geqslant 1$.*

Proof. Obvious.

3.43. Corollary. *If char $K \neq 2$ and $g_1 \in K[x]$, $[g_1] = 2$, or if char $K = 2$ and $g_2 \in K[x]$, $[g_2] = 3$, then g_1 and g_2, resp., belong to at most one P-chain.*

Proof. Obvious.

3.44. Lemma. *If char $K \neq 2$, $g \in K[x]$, and $[g] = 2$, then there is one and only one polynomial $m = x^2+d$ which is a conjugate of g. If char $K = 2$, $g \in K[x]$, and $[g] = 3$, then there is one and only one polynomial $m = x^3+dx+e$ which is a conjugate of g.*

Proof. Let char $K \neq 2$, $g = ax^2+bx+c$, $a \neq 0$, $l = ux+v$. Then $l^{-1} = (1/u)(x-v)$ whence, for any K,

$$\begin{aligned} l^{-1} \circ g \circ l &= (1/u)(a(ux+v)^2 + b(ux+v) + c - v) \\ &= aux^2 + (2av+b)x + (1/u)(g(v) - v). \end{aligned}$$

Hence $l^{-1} \circ g \circ l$, is of the form x^2+d if and only if $u = a^{-1}$, $v = -(2a)^{-1} b$. Thus there is exactly one l such that $l^{-1} \circ g \circ l$ is of the form as required. If char $K = 2$, and $g = a_1x^3+b_1x^2+c_1x+d_1$, $a_1 \neq 0$, $l = ux+v$, then, for any K,

$$\begin{aligned} l^{-1} \circ g \circ l &= (1/u)(a_1(ux+v)^3 + b_1(ux+v)^2 + c_1(ux+v) + d_1 - v) = \\ &= a_1u^2x^3 + (3a_1v+b_1)ux^2 + (3a_1v^2 + 2b_1v + c_1)x + (1/u)(g(v) - v). \end{aligned}$$

Hence $l^{-1}\circ g\circ l$ is of the form x^3+dx+e if and only if $u^2 = a_1^{-1}$, $v = -(3a_1)^{-1}b_1$. Since char $K = 2$ and K is algebraically closed, such u, $v \in K$ do exist and are uniquely determined by a_1, b_1. Thus $m = x^3+dx+e$ is uniquely determined by g.

3.45. Corollary. *If char $K \neq 2$, then every P-chain over K is a conjugate of one and only one P-chain which contains some quadratic polynomial x^2+a. If char $K = 2$, then every P-chain over K is a conjugate of one and only one P-chain which contains some cubic polynomial x^3+ax+b.*

Proof. By Cor. 3.42, Cor. 3.43, and Lemma 3.44.

3.46. Proposition. *If char $K \neq 2$, then the only P-chains which contain some quadratic polynomial x^2+a are the P-chain of powers and the P-chain of Čebyshev polynomials. These are also the only P-chains containing some cubic polynomial x^3+ax+b if char $K = 2$.*

Proof. The P-chain S has the property as in the proposition and T also has, by (3.3). We have to show that no other P-chains have this property.

Let char $K \neq 2$, and P any P-chain containing some polynomial x^2+a.

Case 1: char $K \neq 3$. Let $f = a_0x^3+a_1x^2+a_2x+a_3 \in P$, then $f(x^2+a) = f^2+a$ whence $f(-x)^2+a = f(x^2+a) = f(x)^2+a$. Thus $f(-x) = f(x)$ or $f(-x) = -f(x)$. Since $a_0 \neq 0$, we can only have $f(-x) = -f(x)$, thus $a_1 = a_3 = 0$. Then $a_0(x^2+a)^3+a_2(x^2+a) = (a_0x^3+a_2x)^2+a$ whence $a_0 = a_0^2$, i.e. $a_0 = 1$. Moreover, $3a_0a = 2a_0a_2$, hence $a_2 = \frac{3}{2}a$, and $3a_0a^2+a_2 = a_2^2$ whence $3a^2+\frac{3}{2}a = \frac{9}{4}a^2$. Thus $a = 0$ or $a = -2$.

Case 2: char $K = 3$. Let $f = b_0x^5+b_1x^4+b_2x^3+b_3x^2+b_4x+b_5 \in P$. As before, we conclude $f = b_0x^5+b_2x^3+b_4x$. Hence $b_0(x^2+a)^5+ +b_2(x^2+a)^3+b_4(x^2+a) = (b_0x^5+b_2x^3+b_4x)^2+a$. We compare the coefficients on either side of this equation and obtain $b_0 = b_0^2$, thus $b_0 = 1$; furthermore $5ab_0 = 2b_0b_2$, therefore $b_2 = a$, and $10b_0a^2+b_2 = b_2^2+2b_0b_4$ implies $b_4 = -a$. Finally $10b_0a^3 = 2b_2b_4$ yields $a^3 = a^2$ whence $a = 0$ or $a = 1 = -2$.

Thus in either case we have $a = 0$ or $a = -2$. Since $x^2 \in S$ while $x^2-2 \in T$ by (3.3), the P-chain P either is equal to S or to T, by Cor. 3.43.

Now let char $K = 2$, P any P-chain containing some polynomial x^3+ax+b, and $f = b_0x^5+b_1x^4+b_2x^3+b_3x^2+b_4x+b_5 \in P$. Then

$f(x^3+ax+b) = f^3+af+b$. Making abundant use of char $K = 2$, this equation reads as

$$(b_0(x^3+ax+b)+b_1)(x^{12}+a^4x^4+b^4)+(b_2(x^3+ax+b)+b_3)(x^6+a^2x^2+b^2)+$$
$$+ \ldots = (b_0^2x^{10}+b_1^2x^8+b_2^2x^6+b_3^2x^4+b_4^2x^2+b_5^2)(b_0x^5+b_1x^4+$$
$$+b_2x^3+b_3x^2+b_4x+b_5)+ \ldots$$

We compare the coefficients on either side of this equation. Then $b_0 = b_0^3$, thus $b_0 = 1$. Furthermore $0 = b_0^2b_1$ whence $b_1 = 0$, then $b_0a = b_1^2b_0+b_0^2b_2$ whence $b_2 = a$. Moreover $b_0b+b_1 = b_1^3+b_0^2b_3$ whence $b_3 = b$, and $0 = b_2^2b_0+b_1^2b_2+b_0^2b_4$ whence $b_4 = a^2$. Furthermore $0 = b_2^2b_1+b_1^2b_3+b_0^2b_5$ whence $b_5 = 0$. We continue with comparing the coefficients and obtain $b_2 = b_3^2b_0+b_2^3+b_1^2b_4$ whence $a = b^2+a^3$. Furthermore $0 = b_3^2b_1+b_2^2b_3+b_1^2b_5$ whence $a^2b = 0$. Thus $a^2b^2 = 0$ and therefore $a^3 = a^2b^2+a^5 = a^5$, i.e. $a^3(a^2-1) = 0$. Hence $a = 0$ or $a = 1 = -1$ and $a = b^2+a^3$ implies $b = 0$. Since $x^3 \in S$ while $x^3-x \in T$, by (3.3), again $P = S$ or $P = T$ follows.

3.47. Cor. 3.45 and Prop. 3.46 imply that Th. 3.33 is true if K is algebraically closed.

3.48. Proof of Theorem 3.33. Let K be an arbitrary field, and P any P-chain over K. By the preceding result, P is conjugate to $U = S$ or T in the algebraic closure L of K. Let $l = ux+v$ a linear polynomial over L that transforms P into U, then, if p_2 is the quadratic polynomial in P, we have $l^{-1}\circ p_2\circ l = x^2+d$ while, for the cubic polynomial $p_3 \in P$, we have $l^{-1}\circ p_3\circ l = x^3+ex$ where $d = 0$ or -2 and $e = 0$ or -3. Let $p_2 = ax^2+bx+c$, $p_3 = a_1x^3+b_1x^2+c_1x+d_1$, then $au = 1$, $2av+b = 0$, $3a_1v+b_1 = 0$. Thus, whatever the characteristic of K may be, $u, v \in K$, whence P is a conjugate of U over K which proves Th. 3.33.

3.5. Let J be any integral domain. We obtain all the P-chains over J if we determine all the P-chains of the quotient field K of J and pick those which consist of polynomials over J. By Th. 3.33, the P-chains over K are just $l^{-1}\circ S\circ l$, $l^{-1}\circ T\circ l$ where S is the P-chain of powers; T the P-chain of Čebyshev polynomials, and l an arbitrary linear polynomial of $K[x]$.

Thus we have to check which of these P-chains consist of polynomials over J.

3.51. Proposition. *Let J be any integrally closed domain, K the quotient field of J, and $l = ux+v$ a linear polynomial of $K[x]$. Then $l^{-1}\circ S\circ l$ is a P-chain over J if and only if $u, v \in J$ and $v^2-v \in Ju$ while $l^{-1}\circ T\circ l$ is a P-chain over J if and only if $u, v \in J$ and $v-2 \in Ju$.*

Proof. a) Let $l^{-1}\circ S\circ l$ be any P-chain over J, then both $l^{-1}\circ x^2\circ l$ and $l^{-1}\circ x^3\circ l$ belong to $J[x]$. Computing the normal forms of these polynomials, we see that $u \in J$, $2v \in J$, $(1/u)(v^2-v) \in J$, $3v^2 \in J$ whence $4v^2-3v^2 \in J$. Since J is integrally closed, we therefore have $u, v \in J$, $v^2-v \in Ju$. Conversely if $l = ux+v$ and $u, v \in J$, $v^2-v \in Ju$, then $l^{-1}\circ x^i\circ l \in J[x]$, $i = 1, 2, 3, \ldots$ which follows from a straightforward computation.

b) Let $l^{-1}\circ T\circ l$ be any P-chain over J, then both $l^{-1}\circ(x^2-2)\circ l$ and $l^{-1}\circ(x^3-3x)\circ l$ belong to $J[x]$. Computing the normal forms of these polynomials, we see that $u \in J$, $2v \in J$, $3v^2-3 \in J$ which, as in a), shows that $u, v \in J$. Moreover, for all $g_i \in T$, we have $l^{-1}\circ g_i\circ l \in J[x]$. Computing the constant terms of these polynomials, we obtain $g_i(v)-v \in Ju$, $i = 1, 2, 3, \ldots$ The case $i = 2$ yields $v^2-v-2 \in Ju$. By § 3.3, $g_{n+1} = g_n x - g_{n-1}$ whence $g_{n+1}(v) = g_n(v)v - g_{n-1}(v)$. Therefore $v^2-2v \in Ju$ and so $v-2 \in Ju$. Conversely if $l = ux+v$ satisfies the condition of the proposition, then $g_2(v)-v = v^2-v-2 \in Ju$. Suppose $g_i(v)-v \in Ju$, for $i \leqslant n$. Then $g_{n+1}(v)-v = g_n(v)v-g_{n-1}(v)-v = (g_n(v)-v)v-(g_{n-1}(v)-v)+(v^2-2v) \in Ju$. Thus $g_i(v)-v \in Ju$, $i = 1, 2, \ldots$, and a straightforward computation shows that $l^{-1}\circ g_i\circ l \in J[x]$, $i=1, 2, 3, \ldots$

3.52. A similar argument as in the proof of Prop. 1.31 can be used to show that, in the semigroup $\langle J[x]; \circ\rangle$, the elements which have an inverse are just the polynomials $l = ux+v$ where u is a unit of J. These elements form a group L with respect to the operation $\circ$. Two P-chains C and C_1 over J are called conjugate (over J) if there exists $l \in L$ such that $C_1 = l^{-1}\circ C\circ l$. Clearly conjugacy is an equivalence relation on the set of all P-chains over J.

3.53. Theorem. *Let J be any integrally closed domain. Then a full system of representatives for the classes of conjugate P-chains over J is given by the P-chains $(ux+v)^{-1}\circ S\circ(ux+v)$ and $(ux+2)^{-1}\circ T\circ(ux+2)$ where u runs through a full system U of representatives for the non-zero classes of associate elements of J and, for each u, the elements v run through a full system $V(u)$ of representatives for the idempotents of $J\,|\,Ju$.*

Proof. By Prop. 3.51, these P-chains are, indeed, P-chains over J. Furthermore, S and T are not conjugate over the quotient field of J, thus are not conjugate over J and, by considoring the polynomials of degree 2 or of degree 3, one can easily check that, in either type of P-chains, any two distinct P-chains are not conjugate over J. On the other hand, if u_1, $v_1 \in J$, $v_1^2-v_1 \in Ju_1$, then there exists a unit $e \in J$ and an element $u \in U$ such that $u_1 = eu$. Hence $v_1^2-v_1 \in Ju$, therefore we can find an element $v \in V(u)$ such that $v_1 = v+ku$. But $u_1x+v_1 = (ux+v)\circ(ex+k)$ whence $(u_1x+v_1)^{-1}\circ S\circ(u_1x+v_1)$ is a conjugate over J of $(ux+v)^{-1}\circ S\circ(ux+v)$. If $u_1, v_1 \in J$ and $v_1-2 \in Ju_1$, then again $u_1 = eu$, $u \in U$, $v_1 = 2+ku$ whence $u_1x+v_1 = (ux+2)\circ(ex+k)$ and we can proceed as before. Hence every P-chain is represented by one of the theorem. This completes the proof.

4. Permutation polynomial vectors and permutation polynomials over rings

4.1. Let R be any commutative ring with identity, D an ideal of R, $\eta(D): R \to R\,|\,D$ the canonical epimorphism, $\eta(D)(X): R[x_1, \ldots, x_k] \to (R\,|\,D)[x_1, \ldots, x_k]$ the unique extension of $\eta(D)$ to a composition epimorphism and $C_k(\eta(D)): C_k(R) \to C_k(R\,|\,D)$ the corresponding epimorphism as described in ch. 3, § 13.1.

4.11. Definition. A polynomial vector $\mathfrak{f} \in C_k(R)$ is called a permutation polynomial vector mod D if the polynomial vector $C_k(\eta(D))\,\mathfrak{f}$ is a permutation polynomial vector over $R\,|\,D$. A polynomial $p \in R[x_1, \ldots, x_k]$ is called a (strict) permutation polynomial mod D if the polynomial $\eta(D)(X)p$ is a (strict) permutation polynomial over $R\,|\,D$.

4.12. Lemma. a) *A polynomial vector $\mathfrak{f} = (p_1, \ldots, p_k)$ of $C_k(R)$ is a permutation polynomial vector mod D if and only if, for every $(r_1, \ldots, r_k) \in R^k$, the system of congruences*

$$p_i(x_1, \ldots, x_k) \equiv r_i \bmod D, \qquad i = 1, \ldots, k,$$

has a unique solution mod D.

b) *A polynomial $p \in R[x_1, \ldots, x_k]$ is a permutation polynomial mod D if and only if, for every $r \in R$, the set of incongruent solutions of the congruence*

$$p(x_1, \ldots, x_k) \equiv r \bmod D$$

has cardinality $|R|D|^{k-1}$.

c) *The polynomial $p \in R[x_1, \ldots, x_k]$ is a strict permutation polynomial mod D if and only if there exist polynomials $p_2, \ldots, p_k \in R[x_1, \ldots, x_k]$ such that the polynomial vector $(p, p_2, \ldots, p_k)$ is a permutation polynomial vector mod D.*

d) *Every strict permutation polynomial mod D is a permutation polynomial mod D.*

Proof. a) follows immediately from the definition of a permutation polynomial vector over $R|D$ (see ch. 3, § 11.45), b) is a consequence of ch. 3, Prop. 12.21, c) stems from ch. 3, § 12.22, and d) from ch. 3, Prop. 12.23.

4.2. Proposition. *Let C, D be ideals of R, $D \subseteq C$. If $R|C$ is finite, then every permutation polynomial vector mod D is also a permutation polynomial vector mod C, and every strict permutation polynomial mod D is also a strict permutation polynomial mod C. If $R|D$ is finite, then every permutation polynomial mod D is also a permutation polynomial mod C.*

Proof. a) Let $\mathfrak{f}$ be a permutation polynomial vector mod D, then $C_k(\eta(D))\mathfrak{f}$ is a permutation polynomial vector over $R|D$, thus – with the notation of ch. 3, § 3.22 — we have $\mathcal{F}(\sigma(R|D))\, C_k(\eta(D))\, \mathfrak{f} \in U_k(R|D)$. Let $\vartheta : R|D \to R|C$ be the unique epimorphism such that $\vartheta\eta(D) = \eta(C)$. Since $R|C$ is finite, ch. 3, Prop. 11.51 implies $\mathcal{F}(P_k(\vartheta)\, \sigma(R|D)\, \eta(D)\, (X))\, \mathfrak{f} \in U_k(R|C)$. But by diagram fig. 3.1 of ch. 3, we have $P_k(\vartheta)\, \sigma(R|D)\, \eta(D)\, (X) = \sigma(R|C)\, \vartheta(X)\, \eta(D)\, (X) = \sigma(R|C)\, \eta(C)\, (X)$, thus $\mathcal{F}(\sigma(R|C))\, C_k(\eta(C))\, \mathfrak{f} \in U_k(R|C)$ whence $\mathfrak{f}$ is a permutation polynomial vector mod C. The statement on strict permutation polynomials now follows from Lemma 4.11 c).

b) Let p be a permutation polynomial mod D, then $\eta(D)\, (X)p$ is a permutation polynomial over $R|D$, thus $\sigma(R|D)\, \eta(D)\, (X)p \in S_k(R|D)$. By ch. 3, Prop. 12.31, $P_k(\vartheta)\, \sigma(R|D)\, \eta(D)\, (X)p \in S_k(R|C)$. As in part a) of the proof, we conclude that p is a permutation polynomial mod C.

4.21. Proposition. *Let C, D be comaximal ideals of R and $E = CD$. Then a polynomial vector $\mathfrak{f} \in C_k(R)$ is a permutation polynomial vector mod E if and only if $\mathfrak{f}$ is a permutation polynomial vector mod C as well as mod D. A polynomial $p \in R[x_1, \ldots, x_k]$ is a strict permutation polynomial mod E if and only if p is a strict permutation polynomial mod C as well as mod D. If moreover $R|C$ and $R|D$ are finite, then p is a permutation polynomial mod E if and only if p is a permutation polynomial mod C as well as mod D.*

Proof. $\gamma : R|E \to R|C \times R|D$ defined by $\gamma\eta(E)r = (\eta(C)r, \eta(D)r)$ is an isomorphism, by the Chinese remainder theorem. Thus by ch. 3, Remark 11.53, $\mathfrak{f}$ is a permutation polynomial vector mod E if and only if $C_k(\gamma)\, C_k(\eta(E))\mathfrak{f}$ is a permutation polynomial vector over $R|C \times R|D$ which is, by ch. 3, Prop. 11.31 and Prop. 11.66, the case if and only if $\psi_1 \mathcal{F}(\tau_1)\, C_k(\gamma)\, C_k(\eta(E))\mathfrak{f}$ consists of a permutation polynomial vector over $R|C$ and a permutation polynomial vector over $R|D$. But by definition of ψ_1 and τ_1 (see ch. 3, § 11.3), we have $\psi_1 \mathcal{F}(\tau_1\gamma(X)\, \eta(E)\, (X))\mathfrak{f} = (C_k(\eta(C))\mathfrak{f},\ C_k(\eta(D))\mathfrak{f})$ whence the first statement follows. Similarly the other two statements are proved: By ch. 3, Remark 12.33, p is a (strict) permutation polynomial mod E if and only if $\gamma(X)\, \eta(E)\, (X)p$ is a (strict) permutation polynomial over $R|C \times R|D$. By ch. 3, Prop. 12.43, this is the case if and only if $\tau_1\gamma(X)\, \eta(E)\, (X)p$ is a pair consisting of (strict) permutation polynomials over $R|C$ and $R|D$, respectively. But $\tau_1\gamma(X)\, \eta(E)\, (X)p = (\eta(C)\, (X)p,\ \eta(D)\, (X)p)$ which completes the proof.

4.3. Let $\mathfrak{f} = (f_1, \ldots, f_k)$ be any polynomial vector in $x_1, \ldots, x_k$ over R, and $\Delta\mathfrak{f} = (\partial_t f_s)$ which is a $k \times k$-matrix over $R[x_1, \ldots, x_k]$ where $\partial_t f_s$ is the entry in the s-th row and t-th column, and $\partial_t = \partial/\partial x_t$ is the t-th partial derivation. $\partial\mathfrak{f}$ denotes the determinant of $\Delta\mathfrak{f}$, i.e. the Jacobian of $\mathfrak{f}$. Polynomial vectors over R will be regarded as $k \times 1$-matrices over $R[x_1, \ldots, x_k]$. If (u_{ik}), (v_{ik}) are both $m \times n$-matrices over a ring S and P is an ideal of S, then $(u_{ik}) \equiv (v_{ik}) \bmod P$ shall mean that $u_{ik} \equiv v_{ik} \bmod P$, for all pairs (i, k).

4.31. Proposition. *Let Q be any primary ideal of R with associated prime ideal P such that $R|Q$ is finite and $Q \neq P$. Then a polynomial vector $\mathfrak{f} = (f_1, \ldots, f_k)$ in $x_1, \ldots, x_k$ over R is a permutation polynomial vector mod Q if and only if*

a) *$\mathfrak{f}$ is a permutation polynomial vector mod P, and*

b) *the congruence $\partial\mathfrak{f}(x_1, \ldots, x_k) \equiv 0$ mod P has no solution in R.*

Proof. The proposition will follow from the following

4.32. Lemma. *Let Q be any primary ideal which is different from its associated prime ideal P. Then $q \in \{Q\}$ implies $\partial_i q \in \{P\}$, for any $q \in R[x_1, \ldots, x_k]$, $i = 1, 2, \ldots, k$.*

Proof. We have to show that $(\partial_i q)(r_1, \ldots, r_k) \in P$, for all $(r_1, \ldots, r_k) \in R^k$. It will suffice to prove that $p \in \{Q\}$ implies $p' \in \{P\}$, for all $p \in R[x]$, since then $q(x_i) = q(r_1, r_2, \ldots, x_i, \ldots, r_k) \in \{Q\}$ implies $q'(x_i) \in \{P\}$, $i = 1, 2, \ldots, k$. Let $a \in P$, $a \notin Q$, then, for any $r \in R$, Taylor's formula implies that $p(r+a) = p(r)+p'(r)a+p_2a^2+ \ldots +p_ma^m$ where $p_2, p_3, \ldots, p_m \in R$. Since $p(r+a) \in Q$, $p(r) \in Q$, we have $a(p'(r)+p_2a+ \ldots + p_ma^{m-1}) \in Q$. But $a \notin Q$ implies $p'(r) \in P$ since Q is primary and P its associated prime ideal.

4.33. Proof of Prop. 4.31. Let $\mathfrak{f}$ be any polynomial vector satisfying the conditions a) and b). Since there exists some integer $l > 0$ such that $P^l \subseteq Q$, it suffices to show that $\mathfrak{f}$ is a permutation polynomial vector mod P^n, $n = 1, 2, \ldots$, by Prop. 4.2. This will be done by induction on n. By a), $\mathfrak{f}$ is a permutation polynomial vector mod P, thus let us assume that $\mathfrak{f}$ is a permutation polynomial vector mod P^{n-1}, for some $n > 1$, and that $\mathfrak{k} \in R^k$ is arbitrary. We have to show that

$$\mathfrak{f} \circ (x_1, \ldots, x_k) \equiv \mathfrak{k} \bmod P^n \tag{4.31}$$

has a unique solution mod P^n. Then, by Lemma 4.12 a), $\mathfrak{f}$ is a permutation polynomial vector mod P^n. Let $\mathfrak{u} = (u_1, \ldots, u_k) \in R^k$ be any solution of the system

$$\mathfrak{f} \circ (x_1, \ldots, x_k) \equiv \mathfrak{k} \bmod P^{n-1} \tag{4.32}$$

which exists because of Lemma 4.12 a) and the induction hypothesis. Suppose $\mathfrak{v} = (v_1, \ldots, v_k)$ is a solution of (4.31). By induction hypothesis, $\mathfrak{v} = \mathfrak{u}+\mathfrak{l}$ where $\mathfrak{l} \in (P^{n-1})^k$, the k-th Cartesian power of P^{n-1}. Since $2(n-1) \geqslant n$, Taylor's formula yields

$$\mathfrak{f} \circ (\mathfrak{u}+\mathfrak{l}) \equiv (\mathfrak{f} \circ \mathfrak{u})+A\mathfrak{l} \bmod P^n \tag{4.33}$$

where $A = ((\partial_t f_s)(u_1, \ldots, u_k))$, whence

$$A\mathfrak{l} \equiv \mathfrak{k}-(\mathfrak{f} \circ \mathfrak{u}) \bmod P^n. \tag{4.34}$$

By b), $\operatorname{Det} A \not\equiv 0 \bmod P$ whence there exists some $k \times k$-matrix B over R such that $AB \equiv BA \equiv E \bmod P$ where E is the $k \times k$-identity matrix. Hence (4.34) implies that

$$\mathfrak{l} \equiv B(\mathfrak{k}-(\mathfrak{f} \circ \mathfrak{u})) \bmod P^n. \tag{4.35}$$

Thus there is at most one solution $\mathfrak{v} \bmod P^n$ of (4.31). The existence of such a solution now follows easily: Let $\mathfrak{v} = \mathfrak{u}+\mathfrak{l}$ where $\mathfrak{l}$ is picked as above. Then

$$\mathfrak{f} \circ \mathfrak{v} = \mathfrak{f} \circ (\mathfrak{u}+\mathfrak{l}) \equiv (\mathfrak{f} \circ \mathfrak{u})+AB(\mathfrak{k}-(\mathfrak{f} \circ \mathfrak{u})) \equiv \mathfrak{k} \bmod P^n,$$

by (4.33). Hence $\mathfrak{v}$ is a solution of (4.31).

Conversely let $\mathfrak{f}$ be any permutation polynomial vector mod Q. By Prop. 4.2, $\mathfrak{f}$ is also a permutation polynomial vector mod P. Moreover $\mathfrak{f}_1 = \mathcal{F}(\sigma(R|Q))\, C_k(\eta(Q))\, \mathfrak{f} \in U_k(R|Q)$, and since $R|Q$ is finite, $U_k(R|Q)$ is a group by ch. 3, Lemma 11.43. Thus $\mathfrak{f}_1$ has a inverse $\mathfrak{g}_1 \in U_k(R|Q)$. Let $\mathfrak{g}$ be any polynomial vector of $C_k(R)$ such that $\mathcal{F}(\sigma(R|Q))\, C_k(\eta(Q))\, \mathfrak{g} = \mathfrak{g}_1$. Then, if $\mathfrak{x} = (x_1, \ldots, x_k)$, we have $\mathcal{F}(\sigma(R|Q))\, C_k(\eta(Q))\, (\mathfrak{g} \circ \mathfrak{f}) = \mathcal{F}(\sigma(R|Q))\, C_k(\eta(Q))\mathfrak{x}$, thus $\mathfrak{g} \circ \mathfrak{f} = \mathfrak{x}+\mathfrak{h}$, $\mathfrak{h} = (h_1, \ldots, h_k) \in C_k(R)$, $h_i \in \{Q\}$, $i = 1, \ldots, k$. The chain rule for partial derivatives yields $\Delta(\mathfrak{g} \circ \mathfrak{f}) = (\Delta\mathfrak{g} \circ \mathfrak{f})\, \Delta\mathfrak{f}$. If δ_{ij} denotes the Kronecker symbol, we may write $\Delta(\mathfrak{g} \circ \mathfrak{f}) = \Delta(\mathfrak{x}+\mathfrak{h}) = (\partial_t(x_s+h_s)) = (\delta_{ts}+\partial_t h_s)$, and $\partial_t h_s \in \{P\}$, by Lemma 4.32. Hence $(\Delta\mathfrak{g} \circ \mathfrak{f})\, \Delta\mathfrak{f} = (\delta_{ts}+\partial_t h_s)$ and switching over to determinants, we get $(\partial\mathfrak{g} \circ \mathfrak{f})\, \partial\mathfrak{f} = |\delta_{ts}+\partial_t h_s| \equiv 1 \bmod \{P\}$. Therefore $(\partial\mathfrak{g} \circ \mathfrak{f})\, \partial\mathfrak{f} = 1+p$, $p \in \{P\}$, whence $\partial\mathfrak{f}(u_1, \ldots, u_k) \not\equiv 0 \bmod P$, for all $(u_1, \ldots, u_k) \in R^k$.

4.34. Proposition. *Let Q be any primary ideal of R with associated prime ideal P, $Q \neq P$, and $R|Q$ finite. Then a polynomial $f \in R[x_1, \ldots, x_k]$ is a strict permutation polynomial mod Q if and only if*

a) *f is a strict permutation polynomial mod P,*

b) *the system of congruences $\partial_i f(x_1, \ldots, x_k) \equiv 0$ mod P, $i = 1, \ldots, k$, has no solution in R.*

Proof. Let f be any polynomial satisfying a) and b), then $\eta(P)(X)f = g_1$ is a strict permutation polynomial over $R|P$. Thus we can find polynomials $g_2, \ldots, g_k$ in $x_1, \ldots, x_k$ over $R|P$ such that $\mathfrak{g} = (g_1, \ldots, g_k)$ is a permutation polynomial vector over $R|P$. If $|R|P| = n$, then in $R|P$

$\{x_i^n - x_i\} \in \{0\}$, $i = 1, \ldots, k$. Therefore, if h_{ij} are arbitrary polynomials over $R|P$, the polynomial vector

$$\mathfrak{h} = \left(g_1, g_2 + \sum_{j=1}^{k} h_{2j}(x_j^n - x_j), \ldots, g_k + \sum_{j=1}^{k} h_{kj}(x_j^n - x_j)\right) \tag{4.36}$$

is also a permutation polynomial vector over $R|P$. If we put $h_{1j} = 0$, $j = 1, \ldots, k$, then

$$\Delta\mathfrak{h} \equiv (\partial_t g_s - h_{st}) \bmod \{0\}. \tag{4.37}$$

If $(u_1, \ldots, u_k) = \mathfrak{u} \in (R|P)^k$, then by b), $(\partial_1 g_1(\mathfrak{u}), \partial_2 g_1(\mathfrak{u}), \ldots, \partial_k g_1(\mathfrak{u})) = (d_{11}(\mathfrak{u}), \ldots, d_{1k}(\mathfrak{u})) = \mathfrak{d}_1(\mathfrak{u})$ is not the zero vector. Since $R|P$ is a field, we may regard $(R|P)^k$ as an $R|P$-vectorspace, thus we can find vectors $\mathfrak{d}_i(\mathfrak{u}) = (d_{i1}(\mathfrak{u}), \ldots, d_{ik}(\mathfrak{u}))$, $i = 2, \ldots, k$, in $(R|P)^k$ such that $\mathfrak{d}_1(\mathfrak{u})$, $\mathfrak{d}_2(\mathfrak{u}), \ldots, \mathfrak{d}_k(\mathfrak{u})$ are $R|P$-linearly independent. The finiteness of $R|P$ moreover implies that $R|P$ is polynomially complete. Hence we can choose $h_{st} \in (R|P)[x_1, \ldots, x_k]$, $2 \leqq s \leqq k$, $1 \leqq t \leqq k$, such that $h_{st}(\mathfrak{u}) = \partial_t g_s(\mathfrak{u}) - d_{st}(\mathfrak{u})$, for all $\mathfrak{u} \in (R|P)^k$. When substituting these polynomials h_{st} into (4.36), the congruence (4.37) yields

$$(\Delta\mathfrak{h}) \circ \mathfrak{u} = (d_{st}(\mathfrak{u})).$$

Hence $(\partial\mathfrak{h})(u_1, \ldots, u_k) = |d_{st}(\mathfrak{u})| \neq 0$, for all $(u_1, \ldots, u_k) \in (R|P)^k$ because of the linear independence of $\mathfrak{d}_1(\mathfrak{u}), \ldots, \mathfrak{d}_k(\mathfrak{u})$. Let $f_i \in R[x_1, \ldots, x_k]$, $i = 2, \ldots, k$, such that $\eta(P)(X) f_i = g_i + \sum_{j=1}^{k} h_{ij}(x_j^n - x_j)$ then $\mathfrak{f} = (f, f_2, \ldots, f_k)$ is a permutation polynomial vector mod P, and $\eta(P)(X)\,\partial\mathfrak{f} = \partial\mathfrak{h}$ implies that $\partial\mathfrak{f}(x_1, \ldots, x_k) \equiv 0 \bmod P$ has no solution in R. By Prop. 4.31, $\mathfrak{f}$ is a permutation polynomial vector mod Q whence f is a strict permutation polynomial mod Q.

Conversely let f be any strict permutation polynomial mod Q then, by Prop. 4.2, f is also a strict permutation polynomial mod P. Moreover there exists $\mathfrak{f} = (f, f_2, \ldots, f_k)$ which is a permutation polynomial vector mod Q. Hence, by Prop. 4.31, $\partial\mathfrak{f}(u_1, \ldots, u_k) \not\equiv 0 \bmod P$, for all $(u_1, \ldots, u_k) \in R^k$, therefore the system $\partial_i f(x_1, \ldots, x_k) \equiv 0 \bmod P$, $i = 1, \ldots, k$, has no solution in R.

4.35. Corollary. *If $\mathfrak{f}(f)$ is a permutation polynomial vector (strict permutation polynomial) modulo some primary ideal Q of R with associated prime deal $P \neq Q$, $|R|Q|$ finite, then $\mathfrak{f}(f)$ is a permutation polynomial vector (strict permutation polynomial) modulo any primary ideal $\bar{Q}$ of R different from P, having P as the associated prime ideal and $|R|\bar{Q}|$ finite.*

4.4. Let R be any Dedekind domain and M an ideal of R such that $R|M$ is finite. The results of § 4.2 and § 4.3 yield a practical method of deciding whether or not a given polynomial vector $\mathfrak{f}$ in $x_1, \ldots, x_k$ over R is a permutation vector mod M or a given polynomial $f \in R[x_1, \ldots, x_k]$ is a strict permutation polynomial mod M. For if $M = P_1^{e_1} \ldots P_r^{e_r}$ where the prime ideals P_i are pairwise distinct, then $P_i^{e_i}$ and $P_j^{e_j}$ are comaximal primary ideals, for $i \neq j$, and $R|P_i^{e_i}$ is finite, for $i = 1, \ldots, r$. Thus we have just to investigate the behavior of $\mathfrak{f}$ or f, respectively, and of $\partial\mathfrak{f}$ or $\partial_1 f, \ldots, \partial_k f$, resp. modulo the prime ideals P_i. In particular, this method applies to the domains of the algebraic integers in algebraic number fields where the rational integers are a special case.

It is, however, not known yet how to decide whether or not a polynomial f is a permutation polynomial mod M. A result similar to Prop. 4.34 has not yet been derived. Nor do we know whether or not there are rings R, in particular finite residue class rings of Dedekind domains, such that not every permutation polynomial over R is a strict permutation polynomial.

5. Semigroups of polynomial function vectors and polynomial permutations over finite factor rings of Dedekind domains

5.1. Let R be any Dedekind domain, M an ideal of R such that $R|M$ is finite, and $V_k(R|M)$, $U_k(R|M)$ as in ch. 3, § 11.45. We recall that $V_k(R|M)$ is the semigroup of all polynomial function vectors, $U_k(R|M)$ consists of all polynomial permutations over $R|M$, and $U_k(R|M)$ is a subsemigroup of $V_k(R|M)$. Since $R|M$ is finite, $V_k(R|M)$ and $U_k(R|M)$ are also finite, and $U_k(R|M)$ is a group by ch. 3, Lemma 11.43. We observe that all results of this section will hold, in particular, for the case where R is the domain of rational integers and $M \neq \{0\}$.

5.2. In ch. 3, Prop. 11.51, we have proved the result: Let B be any finite, A any arbitrary algebra of a variety $\mathfrak{V}$, $\eta: A \to B$ an epimorphism, and $V_k(\eta): V_k(A) \to V_k(B)$ the extension of η to a composition epimorphism, then $V_k(\eta)U_k(A) \subseteq U_k(B)$. This result can be sharpened for $\mathfrak{V}$ being the variety of commutative rings with identity, and A, B finite residue class rings of a Dedekind domain R as follows:

5.21. Theorem. *Let R be any Dedekind domain, $A = R|M$ and $B = R|N$ finite residue class rings of R and $\eta: A \to B$ an epimorphism. Then $V_k(\eta)\, U_k(A) = U_k(B)$.*

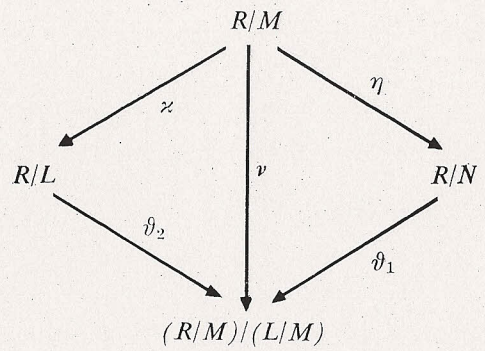


FIG. 4.1

Proof. By ch. 6, Prop. 3.3, ker Ker $\eta = L|M$ where L is some ideal of R such that $M \subseteq L$. Let $\varkappa: R|M \to R|L$ be defined by $\varkappa(a+M) = a+L$, for all $a \in R$, then ker Ker $\varkappa = L|M$. Thus if $\nu: R|M \to (R|M)|(L|M)$ is the canonical epimorphism, there are isomorphisms ϑ_1, ϑ_2, by ch. 1, Th. 1.51, such that the diagram fig. 4.1 is commutative. Hence $V_k(\eta) = V_k(\vartheta_1^{-1})\, V_k(\vartheta_2)\, V_k(\varkappa)$. Since ϑ_i, $i = 1, 2$, are isomorphisms, it is sufficient to show, by ch. 3, Prop. 11.51, that $V_k(\varkappa)\, U_k(R|M) = U_k(R|L)$. This, however, is a consequence of

5.22. Lemma. *If $R|M$ is finite, $L \supseteq M$, and $\mathfrak{f}$ is any permutation polynomial vector mod L, then there exists a permutation polynomial vector $\mathfrak{g}$ mod M such that $\mathfrak{g} \equiv \mathfrak{f}$ mod $\{L\}$.*

Proof. Let $M = P_1^{e_1} \dots P_r^{e_r}$ be the primary decomposition of M, then $L = P_1^{d_1} \dots P_r^{d_r}$ where $d_i \leqslant e_i$, $i = 1, \dots, r$.

Step 1. We show that there exist permutation polynomial vectors $\mathfrak{g}_i$ mod $P_i^{e_i}$, $i = 1, \dots, r$, such that $\mathfrak{g}_i \equiv \mathfrak{f}$ mod $\{P_i^{d_i}\}$. If $d_i = 0$, we may take $\mathfrak{g}_i = \mathfrak{x} = (x_1, \dots, x_k)$. If $d_i \geqslant 2$, then $\mathfrak{f}$ is a permutation polynomial vector mod $P_i^{d_i}$, by Prop. 4.21 whence, by Cor. 4.35, $\mathfrak{f}$ is also a permutation polynomial vector mod $P_i^{e_i}$, thus we may take $\mathfrak{g}_i = \mathfrak{f}$. Now let $d_i = 1$, then $\mathfrak{f}$ is a permutation polynomial vector mod P_i.

Let $|R|P_i| = n$ and $\mathfrak{f} = (f_1, \dots, f_k)$. Then, if $h_{sj} \in R[x_1, \dots, x_k]$ is arbitrary, the polynomial vector

$$\mathfrak{g}_i = \left(f_1 + \sum_{j=1}^{k} h_{1j}(x_j^n - x_j),\ \dots,\ f_k + \sum_{j=1}^{k} h_{kj}(x_j^n - x_j)\right)$$

satisfies $\mathfrak{g}_i \equiv \mathfrak{f}$ mod $\{P_i\}$. Moreover,

$$\partial \mathfrak{g}_i \equiv |(\partial_t f_s - h_{st})| \bmod \{P_i\}$$

Since $R|P_i$ is a finite field, thus polynomially complete, we can choose h_{st} such that $h_{st} \equiv \partial_t f_s - \delta_{st}$ mod $\{P_i\}$ where δ_{st} is the Kronecker symbol. Then $\partial \mathfrak{g}_i \equiv 1$ mod $\{P_i\}$ whence, by Prop. 4.31, $\mathfrak{g}_i$ is a permutation polynomial vector mod $P_i^{e_i}$.

Step 2. Since $P_i^{e_i} \subseteq \{P_i^{e_i}\}$, $i = 1, \dots, r$, the ideals $\{P_i^{e_i}\}$ are pairwise comaximal, hence the Chinese remainder theorem implies that there exists some polynomial vector $\mathfrak{g}$ such that $\mathfrak{g} \equiv \mathfrak{g}_i$ mod $\{P_i^{e_i}\}$, $i = 1, \dots, r$. By Prop. 4.21, $\mathfrak{g}$ is a permutation polynomial vector mod M. Since $\mathfrak{g} \equiv \mathfrak{f}$ mod $\{P_i^{d_i}\}$, $i = 1, \dots, r$, we have $\mathfrak{g} \equiv \mathfrak{f}$ mod $\{L\}$ by ch. 3, § 5.36.

5.3. The finiteness of A in Th. 5.21 is indispensable. The following lemma will yield a construction of such a counterexample.

5.31. Lemma. *Let R be any infinite Dedekind domain which has just finitely many units, and such that every factor ring modulo a non-trivial prime ideal is finite. Then $\partial \mathfrak{f}$ is a unit of R, for every permutation polynomial vector $\mathfrak{f}$ over R.*

Proof. By hypothesis, $\mathfrak{f}$ is a permutation polynomial vector mod (0), therefore, by Prop. 4.2 and the finiteness of $R|P^2$ which follows from ch. 6, Lemma 4.52, $\mathfrak{f}$ is also a permutation polynomial vector mod P^2, for every prime ideal $P \neq (0)$ in R. Hence, by Prop. 4.31, $\partial \mathfrak{f}(r_1, \dots, r_k) \not\equiv 0$ mod P, for any $(r_1, \dots, r_k) \in R^k$. Therefore $R\, \partial \mathfrak{f}(r_1, \dots, r_k) = R$, i.e. $\partial \mathfrak{f}(r_1, \dots, r_k)$ is a unit of R, for any $(r_1, \dots, r_k) \in R^k$. We now show by induction on k, that if $g(x_1, \dots, x_k) \in R[x_1, \dots, x_k]$ such that $g(r_1, \dots, r_k)$ is a unit of R for all $(r_1, \dots, r_k) \in R^k$, then g is a unit of R. This is true for $k = 1$ because of a well-known theorem on the number of roots of a polynomial. Suppose the assertion holds for $k-1$ instead of k, and let $g = \sum_{i=0}^{r} a_i(x_1, \dots, x_{k-1}) x_k^i$ such that, for arbitrary $(r_1, \dots, r_{k-1}) \in R^{k-1}$,

$g(r_1, \ldots, r_{k-1}, x_k) = \sum_{i=0}^{r} a_i(r_1, \ldots, r_{k-1}) x_k^i$ takes only units of R as values. As stated, $g(r_1, \ldots, r_{k-1}, x_k)$ is then a unit of R whence $a_i(x_1, \ldots, x_{k-1}) = 0$, for $i \geqslant 1$, and $a_0(x_1, \ldots, x_{k-1})$ assumes only units as values. By induction, $a_0(x_1, \ldots, x_{k-1})$ is a unit of R, thus g is a unit of R. In particular, $\partial\mathfrak{f}(x_1, \ldots, x_k)$ is a unit of R.

5.32. Remark. Since every element of $C_k(R)$ which has an inverse in $C_k(R)$, is a permutation polynomial vector over R by ch. 3, § 11.45, the following proposition would be a partial converse of Lemma 5.31: If R is any integral domain of characteristic zero and $\mathfrak{f} \in C_k(R)$ is a polynomial vector such that $\partial\mathfrak{f}$ is a unit of R, then $\mathfrak{f}$ has an inverse in $C_k(R)$. But no correct proof of this proposition for $k \geqslant 3$ is yet known.

5.33. We now construct the counterexample as announced at the beginning of this subsection. Let R be the ring of rational integers, $k = 1$, $A = R$, $B = R|(p)$, $p > 3$ a prime, and $\eta : R \to R/(p)$ the canonical epimorphism. Since R satisfies the conditions of Lemma 5.31, every permutation polynomial vector f over R satisfies either $f' = 1$ or $f' = -1$ whence $\{f = x+c,\ -x+c | c \in R\}$ is the totality of permutation polynomial vectors over R. Therefore $U_1(R) = \{e\xi+c |\ e = \pm 1,\ c \in R\}$ whence $|V_1(\eta)\, U_1(R)| = 2p$. But B is a finite field and therefore polynomially complete, thus $|U_1(B)| = p!$. Hence $V_k(\eta)\, U_1(R) \neq U_1(B)$.

5.4. Let E be any ideal of R such that $E = CD$ where C and D are comaximal ideals of R, and $\gamma : R|E \to R|C \times R|D$ the isomorphism as in the proof of Prop. 4.21. Then, by the results of ch. 3, § 11.3, $V_k(R|E) \cong V_k(R|C \times R|D) \cong V_k(R|C) \times V_k(R|D)$, and by ch. 3, § 11,6, $U_k(R|E) \cong U_k(R|C \times R|D) \cong U_k(R|C) \times U_k(R|D)$. Therefore, if $M = P_1^{e_1} \ldots P_s^{e_s}$ is the primary decomposition of M, we have $V_k(R|M) \cong V_k(R|P_1^{e_1}) \times \ldots \times V_k(R|P_s^{e_s})$ and $U_k(R|M) \cong U_k(R|P_1^{e_1}) \times \ldots \times U_k(R|P_s^{e_s})$. Thus for $R|M$ finite the structure of $V_k(R|M)$ and $U_k(R|M)$ will be determined as soon as we know the structure of $V_k(R|P^e)$, $U_k(R|P^e)$, for any prime ideal P of R, $e \geqslant 1$, where $R|P$ is finite. Since $R|P$ is also a field and therefore polynomially complete, $V_k(R|P)$ is isomorphic to the symmetric semigroup and $U_k(R|P)$ to the symmetric group of $(R|P)^k$, by ch. 3, Remark 11.22. Thus it remains to investigate the case $e > 1$.

5.5. We first introduce some new notation: As in ch. 3, § 8.6, let N be the additive semigroup of non-negative integers and M_k the direct product of k copies of N. On M_k, we introduce a partial order $\leqslant$ by $(m_1, \ldots, m_k) \leqslant (n_1, \ldots, n_k)$ if and only if $m_i \leqslant n_i$, $i = 1, \ldots, k$. Let $\varepsilon_{Pk} = \varepsilon_k : M_k \to N$ be defined by $\varepsilon_k(m_1, \ldots, m_k) = \sum_{i=1}^{k} \varepsilon(m_i)$ where $\varepsilon_P = \varepsilon$ is defined as in ch. 3, § 8.3. Moreover, let $\sigma : M_k \to N$ be defined by $\sigma(m_1, \ldots, m_k) = \sum_{i=1}^{k} m_i$, $\mathfrak{x} = (x_1, \ldots, x_k)$, $\mathfrak{x}^\iota = x_1^{i_1} \ldots x_k^{i_k}$, for $\iota = (i_1, \ldots, i_k) \in M_k$ (see ch. 1, § 8.2). Since every finite subset of M_k has an upper bound in M_k, we can write $f = \sum(a_\lambda \mathfrak{x}^\lambda |\ \lambda \leqslant \sigma)$, for every $f \in R[x_1, \ldots, x_k]$ where $a_\lambda \in R$ can be possibly zero, for some λ. If we regard the polynomial vectors over R as $k \times 1$-matrices, then every polynomial vector $\mathfrak{f} \in C_k(R)$ can be written as $\mathfrak{f} = \sum(\mathfrak{a}_\lambda \mathfrak{x}^\lambda |\ \lambda \leqslant \sigma)$, $\mathfrak{a}_\lambda$ regarded as $k \times 1$-matrices over R.

As in ch. 3, § 8.3, we set $|R|P| = q$. We deviate from the usual convention by setting $P^n = R$, for $n \leqslant 0$, and every ideal P of R and $a^n = 1$, for all $a \in R$ and $n \leqslant 0$.

A subset W of R^k for any e is called a vector system mod P^e if the mapping $\zeta : R^k \to (R|P^e)^k$ defined by $\zeta(a_1, a_2, \ldots, a_k) = (a_1 + P^e, \ldots, a_k + P^e)$ is such that the restriction of ζ to W is a bijection. If $a \in P$, $a \notin P^2$, W_1 a vector system mod P and W_{e-1} a vector system mod P^{e-1}, then, by ch. 6, Lemma 4.53, both the sets $W = \{\mathfrak{u} + a\mathfrak{v} |\ \mathfrak{u} \in W_1,\ \mathfrak{v} \in W_{e-1}\}$ and $\overline{W} = \{\mathfrak{v} + a^{e-1}\mathfrak{u} |\ \mathfrak{u} \in W_1,\ \mathfrak{v} \in W_{e-1}\}$ are vector systems mod P^e.

5.51. Lemma. *Let $a \in P$, $a \notin P^2$, $\iota = (i_1, \ldots, i_k) \in M_k$, and $d_\iota \in P^{e-\sigma(\iota)-\varepsilon_k(\iota)}$. Then there exists a polynomial $s_\iota \in \{P^e\}$ such that*

$$s_\iota = d_\iota a^{\sigma(\iota)} \mathfrak{x}^\iota + \sum(c_\lambda a^{\sigma(\lambda)} \mathfrak{x}^\lambda |\ \lambda < \iota) \tag{5.51}$$

and a polynomial $u_\iota \in \{P^{e-1}\}$ such that

$$u_\iota = d_\iota a^{\sigma(\iota)-1} \mathfrak{x}^\iota + \sum(b_\lambda a^{\sigma(\lambda)-1} \mathfrak{x}^\lambda |\ \lambda < \iota) \tag{5.52}$$

Proof. Let $s_\iota = d_\iota a^{\sigma(\iota)} t_\iota$ where t_ι has been defined in ch. 3, § 8.6. By the proof of ch. 3, Lemma 8.61, $t_\iota \in \{P^{\varepsilon_k(\iota)}\}$, hence $s_\iota \in \{P^e\}$. If we expand s_ι into power products of the indeterminates x_j, then we see that s_ι is as in (5.51). Similarly, $u_\iota = d_\iota a^{\sigma(\iota)-1} t_\iota \in \{P^{e-1}\}$ and is as in (5.52).

5.52. Lemma. *Let $0 \neq g \in \{P^e\}$ and $a_\mu \mathfrak{x}^\mu$ be the leading term of its normal form according to ch. 1, Th. 8.21. Then $a_\mu \in P^{e-\varepsilon_k(\mu)}$.*

Proof. By induction on k. For $k = 1$, the lemma has been proved in ch. 3, Lemma 8.5. Suppose the lemma holds for $k-1$, then let $g \in R[x_1, \ldots, x_k]$, $g \in \{P^e\}$ and $a_\mu \mathfrak{x}^\mu$, $\mu=(m_1, \ldots, m_k)$, its leading term. Let $g = \sum_{j=m_1}^{0} x_1^j h_j$, where $h_j \in R[x_2, \ldots, x_k]$, then $h_{m_1} \not\equiv 0$, and the normal form of h_{m_1} has the leading term $a_\mu \bar{\mathfrak{x}}^{\bar\mu}$ where $\bar{\mathfrak{x}} = (x_2, \ldots, x_k)$, $\bar\mu = (m_2, \ldots, m_k)$. For any $(v_2, \ldots, v_k) \in R^{k-1}$, the polynomial $g(x_1, v_2, \ldots, v_{k-1}) = \sum_{j=m_1}^{0} h_j(v_2, \ldots, v_{k-1}) x_1^j$ is in $\{P^e\}$. Since the lemma holds for $k = 1$, we conclude that $h_{m_1}(v_2, \ldots, v_{k-1}) \in P^{e-\varepsilon(m_1)}$ whence $h_{m_1} \in \{P^{e-\varepsilon(m_1)}\}$. By induction, $a_\mu \in P^{e-\varepsilon(m_1)-\varepsilon_{k-1}(\bar\mu)} = P^{e-\varepsilon_k(\mu)}$.

5.53. Lemma. *Let* $\mathfrak{w} = (w_1, \ldots, w_k) \in R^k$ *and* $\iota = (i_1, \ldots, i_k) \in M_k$. *Then there exists a polynomial* $t_{\mathfrak{w}\iota} \in R[x_1, \ldots, x_k]$ *such that, for any* $\mathfrak{r} = (r_1, \ldots, r_k) \in R^k$,

$$\begin{aligned} t_{\mathfrak{w}\iota}(\mathfrak{w}+\mathfrak{r}) &\equiv \mathfrak{r}^\iota \ mod\ P^e, \quad for \quad \mathfrak{w}+\mathfrak{r} \equiv \mathfrak{w}\ mod\ P, \\ t_{\mathfrak{w}\iota}(\mathfrak{w}+\mathfrak{r}) &\equiv 0\ mod\ P^e, \quad for \quad \mathfrak{w}+\mathfrak{r} \not\equiv \mathfrak{w}\ mod\ P. \end{aligned} \tag{5.53}$$

Proof. Let $E \subseteq R$ be any full set of representatives for the units of $R|P^e$. Then $c_1 = \prod(n | n \in E)$ also represents some unit of $R|P^e$, thus there exists some $c \in R$ such that $cc_1 \equiv 1 \bmod P^e$. Let $t_{00} = c\prod(x+n | n \in E)$ and $t_{0i} = (xt_{00})^i$, $i = 1, 2, \ldots$.

For $w \in R$, we set $t_{wi} = t_{0i}(x-w)$, $i = 1, 2, \ldots$. Then we claim

$$\begin{aligned} t_{00}(r) &\equiv 1 \bmod P^e, \quad \text{for} \quad r \equiv 0 \bmod P, \\ t_{00}(r) &\equiv 0 \bmod P^e, \quad \text{for} \quad r \not\equiv 0 \bmod P. \end{aligned} \tag{5.54}$$

For, $t_{00}(r) = c\prod(r+n | n \in E)$. Any $e \in R$ representing a unit of $R|P$ also represents a unit of $R|P^e$ by ch. 6, Lemma 4.51. Hence if $r \equiv 0 \bmod P$, then $\{r+n | n \in E\}$ is again a full system of representatives for the units of $R|P^e$ whence the first congruence of (5.54) follows. Furthermore if $r \not\equiv 0 \bmod P$, then $-r$ represents some unit of $R|P$ and therefore of $R|P^e$ whence $n \equiv -r \bmod P^e$, for some $n \in E$, and the second congruence follows. (5.54) implies that

$$\begin{aligned} t_{0i}(r) &\equiv r^i \bmod P^e, \quad \text{for} \quad r \equiv 0 \bmod P, \\ t_{0i}(r) &\equiv 0 \bmod P^e, \quad \text{for} \quad r \not\equiv 0 \bmod P. \end{aligned}$$

Thus

$$\begin{aligned} t_{wi}(w+r) &\equiv r^i \bmod P^e, \quad \text{for} \quad w+r \equiv w \bmod P, \\ t_{wi}(w+r) &\equiv 0 \bmod P^e, \quad \text{for} \quad w+r \not\equiv w \bmod P. \end{aligned}$$

Let $t_{\mathfrak{w}i} = t_{w_1 i_1}(x_1)\, t_{w_2 i_2}(x_2) \ldots t_{w_k i_k}(x_k)$. Then $t_{\mathfrak{w}i}$ satisfies (5.53).

5.54. Lemma. *Let* $a \in P$, $a \notin P^2$, *and* $g = \sum c_\lambda a^{\sigma(\lambda)} \mathfrak{x}^\lambda$ *such that* $g(\mathfrak{v}) \equiv 0$ *mod* P^e *for every* $\mathfrak{v}$ *of some vector system* W_{e-1} *mod* P^{e-1}. *Then* $g \in \{P^e\}$.

Proof. Let W_1 be a vector system mod P and $\overline{W} = \{\mathfrak{v}+a^{e-1}\mathfrak{u} |\ \mathfrak{u} \in W_1, \mathfrak{v} \in W_{e-1}\}$ as in the beginning of this subsection, then $g(\mathfrak{v}+a^{e-1}\mathfrak{u}) \equiv \sum c_\lambda a^{\sigma(\lambda)}(\mathfrak{v}+a^{e-1}\mathfrak{u})^\lambda \equiv \sum c_\lambda a^{\sigma(\lambda)} \mathfrak{v}^\lambda \equiv g(\mathfrak{v}) \bmod P^e$.

5.6. Let $\zeta : R^k \to (R|P^e)^k$ be the mapping as defined in § 5.5, and W any vector system mod P^e. Then ζ maps W onto $(R|P^e)^k$ bijectively. If $\varphi : \mathfrak{F}(F_k(R|P^e)) \to F_{\mathfrak{I}}((R|P^e)^k)$ denotes the composition isomorphism of ch. 3, Lemma 11.21, then let $\chi : V_k(R|P^e) \to \mathrm{Map}\,(W, (R|P^e)^k)$ (where Map (M, N) means the set of all mappings from a set M to a set N) be defined by $\chi\mathfrak{f} = (\varphi\mathfrak{f})\zeta$. If $(\varphi\mathfrak{f})\zeta = (\varphi\mathfrak{f}_1)\zeta$, then $\varphi\mathfrak{f} = \varphi\mathfrak{f}_1$, whence $\mathfrak{f} = \mathfrak{f}_1$. Thus χ is injective for any e. In order to determine the mappings of $V_k(R|P^e) = V_k$, it suffices to know the mappings of χV_k. But these are given by

5.61. Proposition. *Let* $a \in P$, $a \notin P^2$, $W = \{\mathfrak{f}+a\mathfrak{y} |\ \mathfrak{f} \in Z_1, \mathfrak{y} \in Z_{e-1}\}$ *a vector system mod* P^e *where* Z_1 *is a vector system mod* P *and* Z_{e-1} *a vector system mod* P^{e-1}, *and, for every integer* r, W_r *a vector system mod* P^r *containing the "zero vector"* $\mathfrak{v} = (0, 0, \ldots, 0)$. *Then the mappings*

$$\mathfrak{f}+a\mathfrak{y} \to \sum(\mathfrak{a}_{\mathfrak{f}\iota} a^{\sigma(\iota)} \mathfrak{y}^\iota | \iota \in M_k)\ mod\ P^e, \quad \mathfrak{a}_{\mathfrak{f}\iota} \in W_{e-\sigma(\iota)-\varepsilon_k(\iota)}, \tag{5.61}$$

are mappings of χV_k, *every mapping of* χV_k *has the form* (5.61), *and the mappings of* (5.61) *are pairwise distinct.*

Proof. a) Let $\vartheta \in \chi V_k$, then there exists $\mathfrak{f}_1 \in V_k(R|P^e)$ such that $\vartheta = (\varphi\mathfrak{f}_1)\zeta$, thus there is a polynomial vector $\mathfrak{f} \in C_k(R)$ such that ϑ is the mapping

$$\mathfrak{f}+a\mathfrak{y} \to \mathfrak{f} \circ (\mathfrak{f}+a\mathfrak{y}) \bmod P^e.$$

If $\eta = (e-1, \ldots, e-1) \in M_k$, then Taylor's formula yields

$$\mathfrak{f} \circ (\mathfrak{f}+a\mathfrak{y}) \equiv \sum(\mathfrak{b}_{\mathfrak{f}\iota} a^{\sigma(\iota)} \mathfrak{y}^\iota | \iota \leqslant \eta) \bmod P^e. \tag{5.62}$$

For any $\mathfrak{f} \in Z_1$, there is some $\mathfrak{a}_{\mathfrak{f}\eta} \in W_{e-\sigma(\eta)-\varepsilon_k(\eta)}$ such that $\mathfrak{b}_{\mathfrak{f}\eta} \equiv \mathfrak{a}_{\mathfrak{f}\eta} \bmod P^{e-\sigma(\eta)-\varepsilon_k(\eta)}$, thus $\mathfrak{b}_{\mathfrak{f}\eta} = \mathfrak{a}_{\mathfrak{f}\eta} + \mathfrak{d}_\eta$ where $\mathfrak{d}_\eta \in (P^{e-\sigma(\eta)-\varepsilon_k(\eta)})^k$. By Lemma 5.51, there exists a polynomial vector $\mathfrak{s}_\eta \in C_k(R)$ such that $\mathfrak{s}_\eta \in \{P^e\}^k$ and $\mathfrak{s}_\eta = \mathfrak{d}_\eta a^{\sigma(\eta)}\mathfrak{x}^\eta + \sum(\mathfrak{c}_\lambda a^{\sigma(\lambda)}\mathfrak{x}^\lambda \mid \lambda \prec \eta)$. Since $\mathfrak{s}_\eta \in \{P^e\}^k$, (5.62) implies that

$$\mathfrak{f} \circ (\mathfrak{k} + a\mathfrak{y}) \equiv a_{\mathfrak{f}\eta} a^{\sigma(\eta)}\mathfrak{y}^\eta + \sum(\mathfrak{b}^{(1)}_{\mathfrak{f}\iota} a^{\sigma(\iota)}\mathfrak{y}^\iota \mid \iota \prec \eta) \bmod P^e.$$

Let $N_0 = \{\iota \in M_k \mid \iota \preccurlyeq \eta\}$, $N_1 = N_0 - \{\eta\}$, η_1 be a maximal element of N_1 and apply the same procedure to η_1 instead of η, then take a maximal element of $N_2 = N_1 - \{\eta_1\}$ etc. In each step, $\mathfrak{b}^{(i)}_{\mathfrak{f}\eta_i}$ is replaced by $\mathfrak{a}_{\mathfrak{f}\eta_i} \in W_{e-\sigma(\eta_i)-\varepsilon_k(\eta_i)}$ while the other vectors $\mathfrak{b}^{(i)}_{\mathfrak{f}\tau}$ are changed only for $\tau \prec \eta_i$. Thus after a finite number of steps we arrive at $\mathfrak{f} \circ (\mathfrak{k} + a\mathfrak{y}) \equiv \sum(\mathfrak{a}_{\mathfrak{f}\iota} a^{\sigma(\iota)}\mathfrak{y}^\iota \mid \iota \preccurlyeq \eta) \bmod P^e$, for every $\mathfrak{y} \in Z_{e-1}$, where $\mathfrak{a}_{\mathfrak{f}\iota} \in W_{e-\sigma(\iota)-\varepsilon_k(\iota)}$, for every ι. Hence every $\vartheta \in \chi V_k$ is of the form (5.61).

b) We now show that every mapping of the form (5.61) belongs to χV_k. Let ϑ be such a mapping, then let $t_{\mathfrak{w}\iota}$ be as in Lemma 5.53, for $\mathfrak{w} \in Z_1$ and $\iota \in M_k$, and $\mathfrak{g} = \sum(\sum(\mathfrak{a}_{\mathfrak{w}\iota} t_{\mathfrak{w}\iota} \mid \iota \in M_k) \mid \mathfrak{w} \in Z_1)$, then this is a finite sum, indeed, since $W_{e-\sigma(\iota)-\varepsilon_k(\iota)} = \{\mathfrak{o}\}$ unless $\iota \preccurlyeq \eta$. By Lemma 5.53, we obtain

$$\begin{aligned}\mathfrak{g} \circ (\mathfrak{k} + a\mathfrak{y}) &= \sum\big(\sum(\mathfrak{a}_{\mathfrak{w}\iota} t_{\mathfrak{w}\iota}(\mathfrak{k} + a\mathfrak{y}) \mid \iota \in M_k) \mid \mathfrak{w} \in Z_1\big) \\ &\equiv \sum(\mathfrak{a}_{\mathfrak{f}\iota} t_{\mathfrak{f}\iota}(\mathfrak{k} + a\mathfrak{y}) \mid \iota \in M_k) \\ &\equiv \sum(\mathfrak{a}_{\mathfrak{f}\iota} a^{\sigma(\iota)}\mathfrak{y}^\iota \mid \iota \in M_k) \bmod P^e.\end{aligned}$$

Hence $\vartheta(\mathfrak{k} + a\mathfrak{y}) \equiv \mathfrak{g} \circ (\mathfrak{k} + a\mathfrak{y}) \bmod P^e$, for all $\mathfrak{k} + a\mathfrak{y} \in W$.

c) We have to show that the mappings of (5.61) are pairwise distinct. Suppose that

$$\sum(\mathfrak{a}_{\mathfrak{f}\iota} a^{\sigma(\iota)}\mathfrak{y}^\iota \mid \iota \in M_k) \equiv \sum(\mathfrak{b}_{\mathfrak{f}\iota} a^{\sigma(\iota)}\mathfrak{y}^\iota \mid \iota \in M_k) \bmod P^e, \quad \text{for all } \mathfrak{k} + a\mathfrak{y} \in W,$$

and let $\mathfrak{f} \in Z_1$. Then

$$\sum((\mathfrak{a}_{\mathfrak{f}\iota} - \mathfrak{b}_{\mathfrak{f}\iota}) a^{\sigma(\iota)}\mathfrak{y}^\iota \mid \iota \in M_k) \equiv \mathfrak{o} \bmod P^e, \quad \text{for all } \mathfrak{y} \in Z_{e-1}.$$

By Lemma 5.54, $\sum((\mathfrak{a}_{\mathfrak{f}\iota} - \mathfrak{b}_{\mathfrak{f}\iota}) a^{\sigma(\iota)}\mathfrak{x}^\iota \mid \iota \in M_k) \in \{P^e\}^k$. If $(\mathfrak{a}_{\mathfrak{f}\mu} - \mathfrak{b}_{\mathfrak{f}\mu}) a^{\sigma(\mu)}\mathfrak{x}^\mu$ is the leading term of this polynomial vector according to ch. 1, Th. 8.21, and $\mathfrak{a}_{\mathfrak{f}\mu} \neq \mathfrak{b}_{\mathfrak{f}\mu}$, then, by Lemma 5.52, $(\mathfrak{a}_{\mathfrak{f}\mu} - \mathfrak{b}_{\mathfrak{f}\mu}) a^{\sigma(\mu)} \in (P^{e-\varepsilon_k(\mu)})^k$, hence $\mathfrak{a}_{\mathfrak{f}\mu} \equiv \mathfrak{b}_{\mathfrak{f}\mu} \bmod P^{e-\sigma(\mu)-\varepsilon_k(\mu)}$ since $a \notin P^2$. By hypothesis, $\mathfrak{a}_{\mathfrak{f}\mu} = \mathfrak{b}_{\mathfrak{f}\mu}$, a contradiction. Hence $\mathfrak{a}_{\mathfrak{f}\iota} = \mathfrak{b}_{\mathfrak{f}\iota}$, for all $\iota \in M_k$.

5.62. Corollary. *If* $N(k, e) = \{\iota \in M_k \mid e - \sigma(\iota) - \varepsilon_k(\iota) > 0\}$ *and* $T = \sum(e - \sigma(\iota) - \varepsilon_k(\iota) \mid \iota \in N(k, e))$, *then*

$$\big|V_k(R|P^e)\big| = q^{Tkq^k}. \tag{5.63}$$

Proof. This is an immediate consequence of counting the mappings of (5.61) and applying ch. 6, Lemma 4.52.

5.63. As a special case of Cor. 5.62, we get $\big|V_k(R|P^2)\big| = q^{(k+2)kq^k}$.

5.7. By ch. 3, § 11.4, $U_k(R|P^e) = U_k$ is a subsemigroup of V_k – actually U_k is a group. We are now going to characterize those mappings of (5.61) that are elements of χU_k. Let $(0, 0, \ldots, 0) = o \in M_k$, $\delta_i = (0, \ldots, 1, \ldots, 0) \in M_k$ with 1 as the i-th component and 0 elsewhere, and Det $(\mathfrak{u}_1, \ldots, \mathfrak{u}_k)$ the determinant of the column vectors $\mathfrak{u}_1, \ldots, \mathfrak{u}_k \in R^k$ which sometimes is also denoted by $D(\mathfrak{u}_1, \ldots, \mathfrak{u}_k)$.

5.71. Proposition. *A mapping of the form* (5.61) *belongs to* χU_k *if and only if*

a) *The family* $\{\mathfrak{a}_{\mathfrak{f}o} \mid \mathfrak{f} \in Z_1\}$ *is a vector system mod* P, *and*

b) *Det* $(\mathfrak{a}_{\mathfrak{f}\delta_1}, \ldots, \mathfrak{a}_{\mathfrak{f}\delta_k}) \not\equiv 0$ *mod* P, *for every* $\mathfrak{f} \in Z_1$.

Proof. Let $\mathfrak{k} + a\mathfrak{y} \to \sum(\mathfrak{a}_{\mathfrak{f}\iota} a^{\sigma(\iota)}\mathfrak{y}^\iota \mid \iota \in M_k) \bmod P^e$ be a mapping of (5.61), then, by Prop. 5.61, there exists a polynomial vector $\mathfrak{g} \in C_k(R)$ such that

$$\mathfrak{g} \circ (\mathfrak{k} + a\mathfrak{y}) \equiv \sum \mathfrak{a}_{\mathfrak{f}\iota} a^{\sigma(\iota)}\mathfrak{y}^\iota \bmod P^e, \quad \text{for every } \mathfrak{k} + a\mathfrak{y} \in W. \tag{5.71}$$

Let $\mathfrak{y} = (y_1, \ldots, y_k)$, and $\partial_i \mathfrak{f} = (\partial_i f_1, \ldots, \partial_i f_k)$, for any polynomial vector $\mathfrak{f} = (f_1, \ldots, f_k)$. Then Taylor's formula implies

$$\mathfrak{g} \circ (\mathfrak{k} + a\mathfrak{y}) = \mathfrak{g} \circ \mathfrak{k} + a \sum_{i=1}^{k} [(\partial_i \mathfrak{g}) \circ \mathfrak{k}] y_i + a^2 \mathfrak{s}_{\mathfrak{k}} \circ \mathfrak{y} \tag{5.72}$$

where $\mathfrak{s}_{\mathfrak{k}} \in C_k(R)$ and $\mathfrak{s}_{\mathfrak{k}} \circ \mathfrak{o} = \mathfrak{o}$. Substitution of (5.72) into (5.71) yields

$$\mathfrak{g} \circ \mathfrak{k} + a \sum_{i=1}^{k} [(\partial_i \mathfrak{g}) \circ \mathfrak{k}] y_i + a^2 \mathfrak{s}_{\mathfrak{k}} \circ \mathfrak{y} \equiv \sum \mathfrak{a}_{\mathfrak{f}\iota} a^{\sigma(\iota)}\mathfrak{y}^\iota \bmod P^e. \tag{5.73}$$

for every $\mathfrak{y} \in Z_{e-1}$. There is exactly one $\mathfrak{y} \in Z_{e-1}$, such that $\mathfrak{y} \equiv \mathfrak{o} \bmod P^{e-1}$. If we substitute this particular $\mathfrak{y}$ into (5.73) and observe that $a \in P$, we get

$$\mathfrak{g} \circ \mathfrak{k} \equiv \mathfrak{a}_{\mathfrak{f}o} \bmod P^e. \tag{5.74}$$

Since $e \geqslant 2$, the congruence (5.73) remains valid if we replace P^e by P^2, thus (5.73) and (5.74) together with $a \in P$, $a \notin P^2$ imply that

$$\sum_{i=1}^{k} [(\partial_i \mathfrak{g}) \circ \mathfrak{k}] y_i \equiv \sum_{i=1}^{k} \mathfrak{a}_{\mathfrak{k}\delta_i} y_i \bmod P,$$

for all $\mathfrak{y} \in Z_{e-1}$, hence also for all $\mathfrak{y} \in R^k$. Thus taking $y_i = 1$ and $y_j = 0$, for $i \neq j$, we obtain $\mathfrak{a}_{\mathfrak{k}\delta_i} \equiv (\partial_i \mathfrak{g}) \circ \mathfrak{k} \bmod P$ whence

$$\operatorname{Det}(\mathfrak{a}_{\mathfrak{k}\delta_1}, \ldots, \mathfrak{a}_{\mathfrak{k}\delta_k}) \equiv (\partial \mathfrak{g}) \circ \mathfrak{k} \bmod P. \tag{5.75}$$

If $\mathfrak{k} + a\mathfrak{y} \to \sum \mathfrak{a}_{\mathfrak{k}\iota} a^{\sigma(\iota)} \mathfrak{y}^\iota \bmod P^e$ belongs to χU_k, then $\mathfrak{g}$ is a permutation polynomial vector mod P^e. Therefore by Prop. 4.31, $\mathfrak{g}$ is a permutation polynomial vector mod P and $(\partial \mathfrak{g}) \circ \mathfrak{k} \not\equiv 0 \bmod P$, for every $\mathfrak{k} \in Z_1$. Hence (5.74) and (5.75) show that a) and b) are satisfied. Conversely if these conditions are satisfied, then (5.74) implies that $\mathfrak{g}$ is a permutation vector mod P while (5.75) shows that $(\partial \mathfrak{g}) \circ \mathfrak{k} \not\equiv 0 \bmod P$, for all $\mathfrak{k} \in R^k$. Again by Prop. 4.31, $\mathfrak{g}$ is a permutation vector mod P^e, hence the given mapping is in χU_k.

5.72. Corollary. *If $\Phi_k(P)$ denotes the number of nonsingular $k \times k$-matrices over the field $R|P$ and T has the meaning of Cor.* 5.62, *then*

$$|U_k(R|P^e)| = q^k! \Phi_k(P)^{q^k} q^{(T-k-1)kq^k}. \tag{5.76}$$

Proof. By Prop. 5.61 and Prop. 5.71, we have $|U_k| = |V_k|\,(r/s)$ where $s = q^{ekq^k} q^{(e-1)k^2q^k}$ and $r = q^k! q^{(e-1)kq^k} [\Phi_k(P) q^{(e-2)k^2}]^{q^k}$. Then (5.63) implies (5.76).

5.73. As a special case of Cor. 5.72, we get $|U_k(R|P^2)| = q^k! \Phi_k(P)^{q^k} q^{kq^k}$. This follows from § 5.63.

5.74. Remark. It is well-known (see ch. 6, § 7.2) that $\Phi_k(P) = (q^k - 1) \cdot (q^k - q) \ldots (q^k - q^{k-1})$.

5.8. Proposition. *Let a, W, and W_r, r any integer, have the meaning of Prop.* 5.61. *Then the mappings*

$$\mathfrak{k} + a\mathfrak{y} \to \alpha\mathfrak{k} + a\left(\mathfrak{b}_{\mathfrak{k}o} + \sum_{\iota > o} \mathfrak{b}_{\mathfrak{k}\iota} a^{\sigma(\iota)-1} \mathfrak{y}^\iota\right) \text{ mod } P^e, \tag{5.81}$$

$$\alpha \in \text{Map}(Z_1, Z_1), \quad \mathfrak{b}_{\mathfrak{k}o} \in W_{e-1}, \quad \mathfrak{b}_{\mathfrak{k}\iota} \in W_{e-\sigma(\iota)-\varepsilon_k(\iota)},$$

are mappings of χV_k, every mapping of χV_k has the form (5.81), *and the mappings of* (5.81) *are pairwise distinct. A mapping of the form* (5.81) *belongs to χU_k if and only if α is a permutation of Z_1 and Det $(\mathfrak{b}_{\mathfrak{k}\delta_1}, \ldots, \mathfrak{b}_{\mathfrak{k}\delta_k}) \not\equiv 0$ mod P, for every $\mathfrak{k} \in Z_1$.*

Proof. Let $\vartheta \in \chi V_k$, then ϑ is of the form (5.61), by Prop. 5.61. By ch. 6, Lemma 4.53, $\mathfrak{a}_{\mathfrak{k}o} \equiv \alpha\mathfrak{k} + a\mathfrak{b}_{\mathfrak{k}o} \bmod P^e$ where $\alpha\mathfrak{k} \in Z_1$ and $\mathfrak{b}_{\mathfrak{k}o} \in W_{e-1}$. Hence ϑ is a mapping of (5.81). Conversely, every mapping ϑ of (5.81) is a mapping of (5.61) whence $\vartheta \in \chi V_k$. If any two mappings of (5.81) are equal, say

$$\mathfrak{k} + a\mathfrak{y} \to \alpha\mathfrak{k} + a\left(\mathfrak{b}_{\mathfrak{k}o} + \sum_{\iota > o} \mathfrak{b}_{\mathfrak{k}\iota} a^{\sigma(\iota)-1} \mathfrak{y}^\iota\right) \bmod P^e$$

and

$$\mathfrak{k} + a\mathfrak{y} \to \beta\mathfrak{k} + a\left(\mathfrak{c}_{\mathfrak{k}o} + \sum_{\iota > o} \mathfrak{c}_{\mathfrak{k}\iota} a^{\sigma(\iota)-1} \mathfrak{y}^\iota\right) \bmod P^e,$$

then, by Prop. 5.61, $\mathfrak{b}_{\mathfrak{k}\iota} = \mathfrak{c}_{\mathfrak{k}\iota}$, for any $\iota > o$, and $\mathfrak{k} \in Z_1$ while $\alpha\mathfrak{k} + a\mathfrak{b}_{\mathfrak{k}o} = \beta\mathfrak{k} + a\mathfrak{c}_{\mathfrak{k}o}$, for any $\mathfrak{k} \in Z_1$ whence $\alpha = \beta$ and $\mathfrak{b}_{\mathfrak{k}o} = \mathfrak{c}_{\mathfrak{k}o}$. Suppose now that a mapping ϑ of (5.81) belongs to χU_k. Rewriting ϑ in the form of (5.61) and applying Prop. 5.71, we see that Det $(\mathfrak{b}_{\mathfrak{k}\delta_1}, \ldots, \mathfrak{b}_{\mathfrak{k}\delta_k}) \not\equiv 0$ mod P, for every $\mathfrak{k} \in Z_1$ and that the family $\{\alpha\mathfrak{k} + a\mathfrak{b}_{\mathfrak{k}o} | \mathfrak{k} \in Z_1\}$ is a vector system mod P. Hence $\{\alpha\mathfrak{k} | \mathfrak{k} \in Z_1\}$ is a vector system mod P whence α is a permutation of Z_1. Conversely if a mapping ϑ of (5.81) is such that α is a permutation of Z_1 and Det $(\mathfrak{b}_{\mathfrak{k}\delta_1}, \ldots, \mathfrak{b}_{\mathfrak{k}\delta_k}) \not\equiv 0$ mod P, for all $\mathfrak{k}$, then rewriting of ϑ in the form (5.61) and applying Prop. 5.71 shows that $\vartheta \in \chi U_k$.

5.9. Lemma. *Let Q be any commutative ring with identity, A an ideal of Q and $H(A)$ the set of all polynomial vectors $\mathfrak{f} \in C_k(Q)$ of the form $\mathfrak{f} = \sum \mathfrak{a}_\lambda \mathfrak{x}^\lambda$ where $\mathfrak{a}_\lambda \equiv \mathfrak{o}$ mod $A^{\sigma(\lambda)-1}$, for every $\mathfrak{a}_\lambda$. Then $H(A)$ is a subsemigroup of $C_k(Q)$ containing the identity $\mathfrak{x}$ of $C_k(Q)$.*

Proof. Clearly the sum of any two polynomials $\sum a_\lambda \mathfrak{x}^\lambda$, $a_\lambda \equiv 0 \bmod A^{\sigma(\lambda)-1}$ for every a_λ, is again a polynomial of this form. Thus it suffices to prove: Let $\mu = (m_1, \ldots, m_k) \in M_k$, $a \in Q$, such that $a \equiv 0 \bmod A^{\sigma(\mu)-1}$, and $\mathfrak{g} = (g_1, \ldots, g_k) \in H(A)$ then if $a g_1^{m_1} \ldots g_k^{m_k} = \sum u_\lambda \mathfrak{x}^\lambda$, we have $u_\lambda \equiv 0 \bmod A^{\sigma(\lambda)-1}$, for every u_λ. This will follow as soon we have shown: For any integer $r \geqslant 0$, $a \in A^{r-1}$, and polynomials $h_j = \sum v_{j_{\iota_j}} \mathfrak{x}^{\iota_j}$, $v_{j_{\iota_j}} \in A^{\sigma(\iota_j)-1}$

for every ι_j, $j = 1, \ldots, r$, from $ah_1 \ldots h_r = \sum u_\lambda \mathfrak{x}^\lambda$ follows $u_\lambda \in A^{\sigma(\lambda)-1}$, for every u_λ. But $ah_1 \ldots h_r = \sum a v_{1\iota_1} \ldots v_{r\iota_r} \mathfrak{x}^{\iota_1 + \cdots + \iota_r}$ and $av_{1\iota_1} \ldots v_{r\iota_r} \in A^g$ where $g = r-1+\sigma(\iota_1)-1+ \ldots +\sigma(\iota_r)-1 = \sigma(\iota_1+ \ldots +\iota_r)-1$.

5.91. As before, let R be any Dedekind domain, P a prime ideal of R, and $R|P$ finite. In Lemma 5.9, take $Q = R|P^e$, $A = P|P^e$, then we obtain a subsemigroup $H(P|P^e) = H_k(P^e, P)$ of $C_k(R|P^e)$. Therefore $\mathcal{F}(\sigma(R|P^e))\ H_k(P^e, P) = S_k(P^e, P)$ is a subsemigroup of $V_k(R|P^e)$ while $S_k(P^e, P) \cap U_k(R|P^e) = T_k(P^e, P)$ is a subsemigroup of $U_k(R|P^e)$ containing $(\xi_1, \ldots, \xi_k)$ and is even a group. Let $e > 1$, $Z_{e-1} = W$ a vector system mod P^{e-1}, and $\chi_1 : V_k(R|P^{e-1}) \to \mathrm{Map}\ (W, (R|P^{e-1})^k)$ the injection being defined in an analogous manner as χ in § 5.6.

5.92. Proposition. *Let $a \in P$, $a \notin P^2$, Z_{e-1} a vector system mod P^{e-1}, and W_r a vector system mod P^r, containing $\mathfrak{o}$, for every integer r. Then*

$$\mathfrak{y} \to \mathfrak{d}_o + \sum_{\iota > o} \mathfrak{d}_\iota a^{\sigma(\iota)-1} \mathfrak{y}^\iota \ mod\ P^{e-1}, \qquad \mathfrak{y} \in Z_{e-1} \tag{5.91}$$

where $\mathfrak{d}_o \in W_{e-1}$, $\mathfrak{d}_\iota \in W_{e-\sigma(\iota)-\varepsilon_k(\iota)}$, for $\iota > o$, is an element of $\chi_1 S_k(P^{e-1}, P)$, every element of $\chi_1 S_k(P^{e-1}, P)$ is of the form (5.91), *and these mappings* (5.91) *are pairwise distinct. A mapping* (5.91) *belongs to $\chi_1 T_k(P^{e-1}, P)$ if and only if Det $(\mathfrak{d}_{\delta_1}, \ldots, \mathfrak{d}_{\delta_k}) \not\equiv 0$ mod P.*

Proof. We proceed as in the proof of Prop. 5.61.

a) Let $\tau \in \chi_1 S_k(P^{e-1}, P)$, then τ can be written as

$$\mathfrak{y} \to \sum a_\iota \mathfrak{y}^\iota \bmod P^{e-1}$$

where $\mathfrak{a}_\iota \equiv \mathfrak{o} \bmod P^{\sigma(\iota)-1}$, for all ι occurring in this sum. Since $Ra \subseteq P$, but $Ra \nsubseteq P^2$, we have $Ra^n + P^{e-1} = (Ra)^n + P^{e-1} = P^{\min(n, e-1)}$, for any n. Hence, for any $p \in P^n$, we have $p \equiv ua^{\min(n, e-1)} \bmod P^{e-1}$, for some $u \in R$. Taking η as in § 5.61, we conclude that τ is of the form

$$\mathfrak{y} \to \sum_{\iota \leqq \eta} \mathfrak{d}_\iota a^{\sigma(\iota)-1} \mathfrak{y}^\iota \bmod P^{e-1}.$$

Now we apply the same procedure as in the first part of the proof of Prop. 5.61, using Lemma 5.51, to show that τ can be written in the form (5.91).

b) By definition of $S_k(P^e, P)$, every mapping (5.91) belongs to $\chi_1 S_k(P^{e-1}, P)$.

c) Suppose two mappings with coefficients $\mathfrak{d}_\iota$, $\mathfrak{c}_\iota$ of (5.91) are equal, then $(\mathfrak{d}_o - \mathfrak{c}_o) + \sum_{\iota > o} (\mathfrak{d}_\iota - \mathfrak{c}_\iota) a^{\sigma(\iota)-1} \mathfrak{x}^\iota \in \{P^{e-1}\}^k$. Again we may argue as in the third part of the proof of Prop. 5.61 to show that $\mathfrak{d}_\iota = \mathfrak{c}_\iota$, for all ι.

d) Suppose that the mapping in (5.91) belongs to $\chi_1 T_k(P^{e-1}, P)$. Then $\mathfrak{d}_o + \sum_{\iota > o} \mathfrak{d}_\iota a^{\sigma(\iota)-1} \mathfrak{x}^\iota$ is a permutation polynomial vector mod P^{e-1}, whence, by Prop. 4.31, this is also a permutation polynomial vector mod P. Hence $\mathfrak{d}_o + \sum_{i=1}^{k} \mathfrak{d}_{\delta_i} \mathfrak{x}^{\delta_i}$ is also a permutation polynomial vector mod P. Therefore the system $\sum_{i=1}^{k} \mathfrak{d}_{\delta_i} \mathfrak{x}^{\delta_i} \equiv \mathfrak{o} \bmod P$ of linear congruences has just the trivial solution whence Det $(\mathfrak{d}_{\delta_1}, \ldots, \mathfrak{d}_{\delta_k}) \not\equiv 0 \bmod P$. Conversely if Det $(\mathfrak{d}_{\delta_1}, \ldots, \mathfrak{d}_{\delta_k}) \not\equiv 0 \bmod P$, then $\mathfrak{d}_o + \sum_{\iota > o} \mathfrak{d}_\iota a^{\sigma(\iota)-1} \mathfrak{x}^\iota$ satisfies both the conditions of Prop. 4.31. Hence such a mapping as (5.91) belongs to $\chi_1 T_k(P^{e-1}, P)$.

5.93. We set $(R|P)^k = K$ and $(R|P^{e-1})^k = L$. Let Z_1 be any vector system mod P, Z_{e-1} a vector system mod P^{e-1} and $\zeta_1 : Z_1 \to (R|P)^k$, $\zeta_{e-1} : Z_{e-1} \to (R|P^{e-1})^k$ be defined as ζ in § 5.5. Then $W = \{\mathfrak{f} + a\mathfrak{y} \mid \mathfrak{f} \in Z_1,\ \mathfrak{y} \in Z_{e-1}\}$ is a vector system mod P^e and $\varrho : W \to K \times L$ defined by $\varrho(\mathfrak{f} + a\mathfrak{y}) = (\zeta_1 \mathfrak{f}, \zeta_{e-1} \mathfrak{y})$ is a bijection. Let ζ be the mapping as defined in § 5.5. If $F_1(K \times L)$ denotes the symmetric semigroup of $K \times L$, then $\vartheta : V_k \to F_1(K \times L)$ which is defined by $\vartheta \mathfrak{f} = \varrho \zeta^{-1} (\varphi \mathfrak{f}) \zeta \varrho^{-1}$, is a monomorphism. Thus $V_k \cong \varrho \zeta^{-1} V_k \zeta \varrho^{-1} = \bar{V}_k$ and $U_k \cong \varrho \zeta^{-1} U_k \zeta \varrho^{-1} = \bar{U}_k$.

By Prop. 5.8, every mapping of $\bar{V}_k \subseteq F_1(K \times L)$ is of the form

$$(\bar{\mathfrak{f}}, \bar{\mathfrak{y}}) \to (\overline{\alpha \mathfrak{f}},\ \bar{\mathfrak{b}}_{\mathfrak{f}o} + \sum \bar{\mathfrak{b}}_{\mathfrak{f}\iota} \bar{a}^{\sigma(\iota)-1} \bar{\mathfrak{y}}^\iota)$$

where the bars mean the cosets mod P and mod P^{e-1}, resp. of which the element under the bar is a member. Hence every mapping of $\bar{V}_k$ can be written as

$$(\bar{\mathfrak{f}}, \bar{\mathfrak{y}}) \to (\alpha_1 \bar{\mathfrak{f}},\ \beta(\bar{\mathfrak{f}}) \bar{\mathfrak{y}}) \tag{5.92}$$

where $\alpha_1 = \zeta_1 \alpha \zeta_1^{-1} \in F_1(K)$ and $\beta(\bar{\mathfrak{f}}) \in \varphi S_k(P^{e-1}, P)$. Conversely by Prop. 5.8 and Prop. 5.92, every mapping (5.92) belongs to $\bar{V}_k$. We also conclude that a mapping (5.92) belongs to $\bar{U}_k$ if and only if α_1 is a permutation of K and $\beta(\bar{\mathfrak{f}}) \in \varphi T_k(P^{e-1}, P)$, for all $\mathfrak{f} \in Z_1$.

We recall the definition of the wreath product of two permutation groups and consider also its straightforward generalization to semigroups of mappings. Then we may summarize our results as

5.94. Theorem. *The semigroup $V_k(R|P^e)$ is isomorphic to the wreath product of the semigroup $\varphi S_k(P^{e-1}, P)$ by the symmetric semigroup $F_1((R|P)^k)$, and the group $U_k(R|P^e)$ is isomorphic to the wreath product of the group $\varphi T_k(P^{e-1}, P)$ by the symmetric group Sym $(R|P)^k$.*

6. Ideal power semigroups

6.1. Let Q be any commutative ring with identity, A an ideal of Q, and $H(A)$ the subsemigroup of $C_k(Q)$ defined in § 5.9. Clearly $H(Q) = C_k(Q)$ while $H((0)) = \{\mathfrak{a}_o + \sum \mathfrak{a}_{\delta_i} \mathfrak{x}^{\delta_i}\}$ which will be denoted by $L(Q)$. Moreover if A_1 is an ideal of Q such that $A_1 \subseteq A$, then $H(A_1) \subseteq H(A)$. We put $J(A) = H(A) \cap \mathcal{F}(\sigma)^{-1} U_k(Q)$ which is the set of all permutation polynomial vectors of $H(A)$. $J(A)$ contains the polynomial vector $\mathfrak{x}$, hence $J(A)$ is non-empty and therefore is a subsemigroup of $H(A)$. Furthermore we put $\mathcal{F}(\sigma) H(A) = S(A)$ which is a subsemigroup of $V_k(Q)$ and $\mathcal{F}(\sigma) J(A) = T(A)$ is a subsemigroup of $U_k(Q)$. $S(A)$ and $T(A)$ are related by $T(A) = S(A) \cap U_k(Q)$.

6.2. Proposition. *Let $\eta : Q \to Q_1$ be any epimorphism of rings with identity, $C_k(\eta) : C_k(Q) \to C_k(Q_1)$ and $V_k(\eta) : V_k(Q) \to V_k(Q_1)$ the epimorphisms defined in ch.* 3, § 11.3. *Then*

a) $C_k(\eta) H(A) = H(\eta A)$, $V_k(\eta) S(A) = S(\eta A)$.

b) $V_k(\eta) U_k(Q) \subseteq U_k(Q_1)$ *implies* $V_k(\eta) T(A) \subseteq T(\eta A)$. *If Q_1 is finite, the last inclusion always holds.*

c) $C_k(\eta) J(A) \subseteq J(\eta A)$ *if and only if* $V_k(\eta) T(A) \subseteq T(\eta A)$.

d) *If η is an isomorphism, then $C_k(\eta)$ maps $H(A)$ isomorphically onto $H(\eta A)$ and $J(A)$ isomorphically onto $J(\eta A)$, $V_k(\eta)$ maps $S(A)$ isomorphically onto $S(\eta A)$ and $T(A)$ isomorphically onto $T(\eta A)$.*

Proof. a) follows from the definition of $H(A)$ and ch. 3, diagram fig. 3.1.

b) follows from

$$V_k(\eta) T(A) \subseteq V_k(\eta) S(A) \cap V_k(\eta) U_k(Q) \subseteq S(\eta A) \cap U_k(Q_1) = T(\eta A).$$

The hypothesis of b) is satisfied if Q_1 is finite, by ch. 3, Prop. 11.51.

c) $C_k(\eta) J(A) \subseteq J(\eta A)$ implies $V_k(\eta) T(A) \subseteq T(\eta A)$, by ch. 3, diagram fig. 3.1. Conversely if $V_k(\eta) T(A) \subseteq T(\eta A)$, then, again by ch. 3, diagram fig. 3.1, $\mathcal{F}(\sigma) C_k(\eta) J(A) \subseteq \mathcal{F}(\sigma) J(\eta A) \subseteq U_k(Q_1)$, hence $C_k(\eta) J(A) \subseteq H(\eta A) \cap \mathcal{F}(\sigma)^{-1} U_k(Q_1) = J(\eta A)$.

d) If η is an isomorphism, then $C_k(\eta) : C_k(Q) \to C_k(Q_1)$ is an isomorphism, by ch. 1, Prop. 4.5 and ch. 3, Th. 11.11, and $C_k(\eta)$ maps $\mathcal{F}(\sigma)^{-1} U_k(Q)$ isomorphically onto $\mathcal{F}(\sigma)^{-1} U_k(Q_1)$, by ch. 3, Remark 11.53 whence the first part of d) follows. Similarly the second statement can be proved.

6.3. Proposition. *Let $Q = Q_1 \times Q_2$ be a direct product of commutative rings with identity, A_1, A_2 ideals of Q_1, Q_2, respectively, $\psi_1 \mathcal{F}(\tau_1) : C_k(Q_1 \times Q_2) \to C_k(Q_1) \times C_k(Q_2)$, $\psi_2 \mathcal{F}(\tau_2) : V_k(Q_1 \times Q_2) \to V_k(Q_1) \times V_k(Q_2)$ the composition isomorphisms of ch.* 3, *Prop.* 11.31. *Then $\psi_1 \mathcal{F}(\tau_1)$ induces isomorphisms from $H(A_1 \times A_2)$ to $H(A_1) \times H(A_2)$ and from $J(A_1 \times A_2)$ to $J(A_1) \times J(A_2)$. Similarly $\psi_2 \mathcal{F}(\tau_2)$ induces isomorphisms from $S(A_1 \times A_2)$ to $S(A_1) \times S(A_2)$ and from $T(A_1 \times A_2)$ to $T(A_1) \times T(A_2)$.*

Proof. By Prop. 6.2, $\psi_1 \mathcal{F}(\tau_1) H(A_1 \times A_2) \subseteq H(A_1) \times H(A_2)$. Since $A_1^r \times A_2^r = (A_1 \times A_2)^r$, this inclusion is an equality. By ch. 3, Prop. 11.66, $\psi_1 \mathcal{F}(\tau_1)$ maps $\mathcal{F}(\sigma)^{-1} U_k(Q)$ isomorphically onto $\mathcal{F}(\sigma)^{-1} U_k(Q_1) \times \mathcal{F}(\sigma)^{-1} U_k(Q_2)$, hence $\psi_1 \mathcal{F}(\tau_1)$ maps $J(A)$ into $J(A_1) \times J(A_2)$ and this mapping is onto since $\psi_1 \mathcal{F}(\tau_1)$ is a composition isomorphism from $C_k(Q)$ to $C_k(Q_1) \times C_k(Q_2)$. The second assertion follows from ch. 3, diagram fig. 3.3.

6.31. Remark. By ch. 6, § 4.6, every ideal of $Q_1 \times Q_2$ is of the form $A_1 \times A_2$, where A_i is an ideal of Q_i, $i = 1,2$.

6.4. Theorem. *Let Q be any commutative ring with identity and A a nilpotent ideal of Q. Then the subsemigroup $J(A)$ of $H(A)$ is equal to $\mathcal{E}(H(A))$, the group of units of $H(A)$, and therefore is a group. A polynomial vector $\mathfrak{f} = \sum \mathfrak{a}_\lambda \mathfrak{x}^\lambda$ of $H(A)$ belongs to $J(A)$ if and only if the determinant $D(\mathfrak{a}_{\delta_1}, \ldots, \mathfrak{a}_{\delta_k})$ is a unit of Q.*

Proof. Let l be the least integer such that $A^l = (0)$. If $\mathfrak{f} \in \mathcal{E}(H(A))$, then $\mathfrak{f} \in \mathcal{E}(C_k(Q))$, thus $\mathcal{F}(\sigma)\mathfrak{f} \in \mathcal{E}(\mathcal{F}(\sigma) C_k(Q)) = \mathcal{E}(V_k(Q)) \subseteq U_k(Q)$, by ch. 3, Lemma 11.43, whence $\mathfrak{f} \in J(A)$. Let now $\mathfrak{f} \in J(A)$ and $\mathfrak{f} = \sum \mathfrak{a}_\lambda \mathfrak{x}^\lambda$. Since $\mathcal{F}(\sigma)\mathfrak{f} \in T(A) \subseteq U_k(Q)$, the equation $\mathfrak{f} \circ \mathfrak{x} = \mathfrak{u}$ has a solution $\mathfrak{x}$,

for every $\mathfrak{u} \in Q^k$, hence $\mathfrak{f} \circ \mathfrak{x} \equiv \mathfrak{u} \bmod A$ has a solution $\mathfrak{x}$, for every $\mathfrak{u}$. Hence the system $\mathfrak{a}_0 + \sum_{i=1}^{k} \mathfrak{a}_{\delta_i} \mathfrak{x}^{\delta_i} \equiv \mathfrak{u} \bmod A$ of linear congruences also has a solution, for every $\mathfrak{u} \in Q^k$, thus the matrix $(\mathfrak{a}_{\delta_1}, \ldots, \mathfrak{a}_{\delta_k})$ of column vectors $\mathfrak{a}_{\delta_i}$ has a right inverse mod A. Hence the determinant $D(\mathfrak{a}_{\delta_1}, \ldots, \mathfrak{a}_{\delta_k}) = d$ is a unit mod A. Therefore there exist elements $u \in Q$, $a \in A$ such that $du = 1 - a$ whence $du(1 + a + a^2 + \ldots + a^{l-1}) = 1$. Thus d is a unit of Q. Hence we have to show that if $\mathfrak{f} \in H(A)$ and $D(\mathfrak{a}_{\delta_1}, \ldots, \mathfrak{a}_{\delta_k})$ is a unit of Q, then $\mathfrak{f} \in \mathcal{C}(H(A))$. Let $\mathfrak{Z}(H(A)) = \mathfrak{Z}$ the set of those elements $\mathfrak{f}$ satisfying our hypothesis. $\mathfrak{Z}$ is not empty since $\mathfrak{x} \in \mathfrak{Z}$. Let $\mathfrak{f}, \mathfrak{g} \in H(A)$, then using matrix notation for the linear coefficients of $\mathfrak{f}$, $\mathfrak{g}$, and $\mathfrak{f} \circ \mathfrak{g}$, we can write

$$\mathfrak{f} = \mathfrak{a}_o + F\mathfrak{x} + \sum_{\sigma(\lambda) \geqq 2} \mathfrak{a}_\lambda \mathfrak{x}^\lambda, \quad \mathfrak{g} = \mathfrak{b}_o + G\mathfrak{x} + \sum_{\sigma(\lambda) \geqq 2} \mathfrak{b}_\lambda \mathfrak{x}^\lambda,$$

$$\mathfrak{f} \circ \mathfrak{g} = \mathfrak{c}_o + C\mathfrak{x} + \sum_{\sigma(\lambda) \geqq 2} \mathfrak{c}_\lambda \mathfrak{x}^\lambda$$

where F, G, C are suitable $k \times k$-matrices over Q.

Then $\mathfrak{f} \circ \mathfrak{g} \equiv \mathfrak{a}_o + F\mathfrak{b}_o + FG\mathfrak{x} \bmod (A)$ whence $C \equiv FG \bmod A$, thus

$$|C| \equiv |F|\,|G| \bmod A \tag{6.4}$$

(6.4) shows that $\mathfrak{Z}$ is a subsemigroup of $H(A)$ since every unit mod A is also a unit of Q, by a preceding result. It now suffices to show that every element $\mathfrak{g}$ of $\mathfrak{Z}$ has a left inverse in $\mathfrak{Z}$. But if we show that $\mathfrak{g}$ has a left inverse in $H(A)$, we are done, by (6.4). Let $\mathfrak{g} = \mathfrak{a}_o + \sum_{\sigma(\lambda) \geqq 1} \mathfrak{a}_\lambda \mathfrak{x}^\lambda$, then $\mathfrak{g} = (\mathfrak{a}_o + \mathfrak{x}) \circ \sum_{\sigma(\lambda) \geqq 1} \mathfrak{a}_\lambda \mathfrak{x}^\lambda$. Since $\mathfrak{a}_o + \mathfrak{x}$ has a left inverse in $H(A)$, we can assume that $\mathfrak{g} = \sum_{\sigma(\lambda) \geqq 1} \mathfrak{a}_\lambda \mathfrak{x}^\lambda$. If $\mathfrak{g}$ has a left inverse, then clearly it is of the form $\sum_{\sigma(\lambda) \geqq 1} \mathfrak{b}_\lambda \mathfrak{x}^\lambda$. We proceed by induction on l. If $l = 1$, then $A = (0)$, thus $\mathfrak{g} = G\mathfrak{x}$ where G is a matrix and $|G|$ is a unit of Q. In this case, $\mathfrak{g}$ has a left inverse in $H(A)$, by a well-known theorem on matrices. Let $l > 1$ and $\mathfrak{g} = G\mathfrak{x} + \sum_{\sigma(\lambda) \geqq 2} \mathfrak{b}_\lambda \mathfrak{x}^\lambda$, G a matrix, and $|G|$ a unit of Q. We put $Q_1 = Q \,|\, A^{l-1}$ and let $\eta : Q \to Q \,|\, A^{l-1}$ be the canonical epimorphism. Then $(\eta A)^{l-1} = \eta A^{l-1} = (0)$. Let ηF be the matrix being obtained from applying η to each entry of F, F any matrix over Q, then $C_k(\eta)\mathfrak{g} = (\eta G)\mathfrak{x} + \sum_{\sigma(\lambda) \geqq 2} (\eta \mathfrak{b}_\lambda)\mathfrak{x}^\lambda \in \mathfrak{Z}(H(\eta A))$. By induction hypothesis, there exists $\bar{\mathfrak{f}} = \bar{F}\mathfrak{x} + \sum_{\sigma(\lambda) \geqq 2} \bar{\mathfrak{a}}_\lambda \mathfrak{x}^\lambda \in H(\eta A)$ such that $\bar{\mathfrak{f}} \circ C_k(\eta)\mathfrak{g} = \mathfrak{x}$. Let

$\mathfrak{f} = F\mathfrak{x} + \sum_{\sigma(\lambda) \geqq 2} \mathfrak{a}_\lambda \mathfrak{x}^\lambda \in H(A)$ such that $C_k(\eta)\mathfrak{f} = \bar{\mathfrak{f}}$, then $\mathfrak{f} \circ \mathfrak{g} = \mathfrak{x} + \mathfrak{h}$ where $\mathfrak{h} \equiv \mathfrak{o} \bmod (A^{l-1})$. Let G_1 be a matrix over Q such that $G_1 G = E$, the identity matrix, and $\mathfrak{g}_1 = G_1\mathfrak{x}$. Then $\mathfrak{g}_1 \circ \mathfrak{g} = \mathfrak{x} + \mathfrak{l}$ where $\mathfrak{l} \equiv \mathfrak{o} \bmod (A)$. If we set $\mathfrak{f}_1 = \mathfrak{f} - \mathfrak{h} \circ \mathfrak{g}_1$, then $\mathfrak{f}_1 \circ \mathfrak{g} = \mathfrak{f} \circ \mathfrak{g} - (\mathfrak{h} \circ \mathfrak{g}_1) \circ \mathfrak{g} = \mathfrak{x} + \mathfrak{h} - \mathfrak{h} \circ (\mathfrak{x} + \mathfrak{l})$. By Taylor's formula $\mathfrak{h} \circ (\mathfrak{x} + \mathfrak{l}) = \mathfrak{h} \circ \mathfrak{x} = \mathfrak{h}$ whence $\mathfrak{f}_1 \circ \mathfrak{g} = \mathfrak{x}$. But $H(A)$ is closed with respect to $+$, $-$, as remarked in the proof of Lemma 5.9, and therefore $\mathfrak{f}_1 \in H(A)$.

6.41. Corollary. *If A is a nilpotent ideal of Q, then $T(A) = \mathcal{C}(S(A))$, therefore $T(A)$ is a group.*

Proof. $J(A) = \mathcal{C}(H(A))$ implies $T(A) \subseteq \mathcal{C}(S(A))$. Conversely $\mathcal{C}(S(A)) \subseteq S(A) \cap U_k(A) = T(A)$.

6.42. Corollary. *If A is a nilpotent ideal of Q and $\eta : Q \to Q_1$ is an epimorphism such that ker Ker η is nilpotent, then $C_k(\eta)\, J(A) = J(\eta A)$ and $V_k(\eta)\, T(A) = T(\eta A)$.*

Proof. By Th. 6.4, $J(A) = \{\sum \mathfrak{a}_\lambda \mathfrak{x}^\lambda \in H(A) \mid D(\mathfrak{a}_{\delta_1}, \ldots, \mathfrak{a}_{\delta_k}) \text{ is a unit of } Q\}$. Since ηA is also nilpotent, we also have $J(\eta A) = \{\sum \mathfrak{b}_\lambda \mathfrak{x}^\lambda \in H(\eta A) \mid D(\mathfrak{b}_{\delta_1}, \ldots, \mathfrak{b}_{\delta_k}) \in \mathcal{C}(Q_1)\}$. Suppose we have already shown that $\eta^{-1}\mathcal{C}(Q_1) = \mathcal{C}(Q)$, then Prop. 6.2 a) implies $C_k(\eta)\, J(A) = J(\eta A)$ while the second assertion follows from the first one and ch. 3, diagram fig. 3.1. Thus it remains to show that $\eta^{-1}\mathcal{C}(Q_1) = \mathcal{C}(Q)$. Let $e \in \mathcal{C}(Q)$, then $\eta e \in \mathcal{C}(Q_1)$. Conversely if $e \in \eta^{-1}\mathcal{C}(Q_1)$ then there exists $f_1 \in Q_1$ such that $(\eta e) f_1 = 1$. Let $f \in Q$ such that $f_1 = \eta f$, then $\eta(ef) = 1$, hence $ef = 1 - a$ where $a \in$ ker Ker η. By hypothesis $ef(1 + a + \ldots + a^{m-1}) = 1$ for some m whence $e \in \mathcal{C}(Q)$.

7. Ideal power semigroups over factor rings of Dedekind domains

7.1. Let R be any Dedekind domain, U a non-trivial ideal of R, $\eta(U) : R \to R \,|\, U$ the canonical epimorphism, and W any ideal of R. Then $\eta(U)W = (W + U) \,|\, U$ is an ideal of $R \,|\, U$. Let G stand for any of the letters H, J, S, T of the preceding section. Our aim is to get information on the subsemigroups $G(\eta(U)W) = G_k(U, W)$ of $C_k(R \,|\, U)$, $V_k(R \,|\, U)$, respectively, using the results of § 6.

7.2. Suppose that $U = CD$ where C, D are comaximal ideals of R. Then $\gamma : R \,|\, U \to R \,|\, C \times R \,|\, D$, where $\gamma\eta(U)r = (\eta(C)r, \eta(D)r)$ is an isomorphism

(see the proof of Prop. 4.21). Also $\gamma\eta(U)W = \eta(C)W \times \eta(D)W$ whence $G_k(U,W) \cong G(\eta(C)W \times \eta(D)W) \cong G_k(C,W) \times G_k(D,W)$, by Prop. 6.2 d) and Prop. 6.3. Hence if $U = P_1^{e_1} \dots P_r^{e_r}$ is the primary decomposition of U, then $G_k(U,W) \cong G_k(P_1^{e_1},W) \times \dots \times G_k(P_r^{e_r},W)$.

Let P be any non-trivial prime ideal, $W \neq (0)$ an ideal of R such that $W = P^f Q$ where Q, P are comaximal ideals in R, and $f \geqslant 0$. Then $\eta(P^e)W = (\eta(P^e)P^f)(\eta(P^e)Q) = \eta(P^e)P^f$ since $\eta(P^e)Q = R|P^e$. Thus

$$G_k(P^e,W) = G(\eta(P^e)W) = G(\eta(P^e)P^f) = G_k(P^e,P^f). \tag{7.2}$$

We summarize the results so far obtained:

7.21. Proposition. *Let $G = H, J, S,$ or T, P_i, $i = 1, 2, \dots, r+s$ non-trivial prime ideals, $e_i > 0$, $f_i \geqslant 0$, $i = 1, \dots, r$, then*

$$G_k\left(\prod_{i=1}^{r} P_i^{e_i}, \prod_{i=1}^{r+s} P_i^{f_i}\right) \cong G_k(P_1^{e_1}, P_1^{f_1}) \times \dots \times G_k(P_r^{e_r}, P_r^{f_r}).$$

7.22. This proposition reduces the investigation of the semigroups $G_k(U,W)$, U non-trivial, W arbitrary ideal of R, to considering semigroups $G_k(P^e,(0))$ and $G_k(P^e,P^f)$ where P is a non-trivial prime ideal, $e > 0$, $f \geqslant 0$. If $f \geqslant e$, then $G_k(P^e,P^f) = G((0)) = G_k(P^e,(0))$.

7.3. By § 6.1, $H((0)) = L(R|P^e)$, the subsemigroup of $C_k(R|P^e)$ consisting of all polynomial vectors with linear polynomials as their components. Clearly $\mathfrak{F}(\sigma)$ maps $H((0))$ isomorphically onto $S((0))$ and therefore $J((0))$ isomorphically onto $T((0))$. By Th. 6.4, $J((0))$ is a group consisting of all those linear polynomial vectors whose determinant is a unit. The semigroup $H((0))$, and the group $J((0))$ in particular, have been studied very thoroughly in a great number of papers.

Furthermore $G_k(P^e,P^0) = G(R|P^e)$ which is one of the semigroups $C_k(R|P^e)$, $\mathfrak{F}(\sigma)^{-1}U_k(R|P^e)$, $V_k(R|P^e)$, $U_k(R|P^e)$. By Th. 5.94, the last two of these semigroups will be completely investigated—if $R|P$ is finite—as soon as the structure of $S_k(P^{e-1},P)$, $T_k(P^{e-1},P)$ is known while little is known about the first two semigroups.

7.4. The remainder of this section will be devoted to the semigroups $G_k(P^e,P^f)$ where $G = H, J, S,$ or T, P is a non-trivial prime ideal, $R|P$ finite, and $e > 0, f > 0$.

7.41. Proposition. *Let $r \leqslant e$ and $\vartheta : R|P^e \to R|P^r$ be the unique epimorphism such that $\vartheta\eta(P^e) = \eta(P^r)$. Then $G(\vartheta)\,G_k(P^e,P^f) = G_k(P^r,P^f)$ where $G(\vartheta) = C_k(\vartheta)$ if $G = H, J$ and $G(\vartheta) = V_k(\vartheta)$ if $G = S, T$.*

Proof. By Prop. 6.2, $C_k(\vartheta)\,H_k(P^e,P^f) = C_k(\vartheta)\,H(\eta(P^e)P^f) = H(\eta(P^r)P^f) = H_k(P^r,P^f)$ whence, by ch. 3, diagram fig. 3.1, the proposition also holds for $G = S$. Since $\eta(P^e)P^f$ is a nilpotent ideal of $R|P^e$, and ker Ker $\vartheta = P^r|P^e$, $r > 0$, is also a nilpotent ideal of $R|P^e$, Cor 6.42 implies that

$$C_k(\vartheta)\,J_k(P^e,P^f) = C_k(\vartheta)\,J(\eta(P^e)P^f) = J(\eta(P^r)P^f) = J_k(P^r,P^f)$$

which is also true for $r = 0$ since in this case, $|J_k(P^r,P^f)| = 1$. Again ch. 3, diagram fig. 3.1 proves the proposition for $G = T$.

7.42. Proposition. *$J_k(P^e,P^f)$ and $T_k(P^e,P^f)$ are groups.*

Proof. Since $G_k(P^e,P^f) = G(\eta(P^e)P^f)$ and $\eta(P^e)P^f$ is a nilpotent ideal of $R|P^e$, Th. 6.4 and Cor. 6.41 imply the statement of the proposition.

7.43. Proposition. *Let $\eta = \eta(P^e)$, $a \in P$, $a \notin P^2$, and W_r a vector system mod P^r containing the zero vector $\mathfrak{o}$, for any integer r. Then every polynomial vector*

$$C_k(\eta)\left(\mathfrak{d}_o + \sum_{\iota > o} \mathfrak{d}_\iota (a^f)^{\sigma(\iota)-1}\mathfrak{x}^\iota\right) \tag{7.4}$$

where $\mathfrak{d}_o \in W_e$, $\mathfrak{d}_\iota \in W_{e-f(\sigma(\iota)-1)}$, for $\iota \neq o$, belongs to $H_k(P^e,P^f)$, every element of $H_k(P^e,P^f)$ is of the form (7.4) *and the vectors* (7.4) *are pairwise distinct. A vector* (7.4) *belongs to $J_k(P^e,P^f)$ if and only if Det $(\mathfrak{d}_{\delta_1}, \dots, \mathfrak{d}_{\delta_k}) \not\equiv 0$ mod P.*

Proof. Let $\bar{\mathfrak{f}} \in H_k(P^e,P^f)$, then $\bar{\mathfrak{f}} = \sum \bar{\mathfrak{a}}_\iota \mathfrak{x}^\iota$ where $\bar{\mathfrak{a}}_\iota \equiv \mathfrak{o} \bmod (\eta P^f)^{\sigma(\iota)-1}$. But $Ra + P^e = P$ implies $\eta P = (R|P^e)(\eta a)$ whence $(\eta P^f)^{\sigma(\iota)-1} = \eta(Ra^{f(\sigma(\iota)-1)})$. Thus, for suitable $\mathfrak{b}_\iota \in R^k$, we have $\bar{\mathfrak{f}} = C_k(\eta)\left(\mathfrak{b}_o + \sum_{\iota > o} \mathfrak{b}_\iota (a^f)^{\sigma(\iota)-1}\mathfrak{x}^\iota\right)$. Since $\mathfrak{b}_\iota \equiv \mathfrak{d}_\iota \bmod P^{e-f(\sigma(\iota)-1)}$ if and only if $(a^f)^{\sigma(\iota)-1}\mathfrak{b}_\iota \equiv (a^f)^{\sigma(\iota)-1}\mathfrak{d}_\iota \bmod P^e$, we conclude that $\bar{\mathfrak{f}}$ is of the form (7.4). The other two statements on $H_k(P^e,P^f)$ are clear. Furthermore, by Th. 6.4, a vector (7.4) belongs to $J_k(P^e,P^f)$ if and only if $D(\eta\mathfrak{d}_{\delta_1}, \dots, \eta\mathfrak{d}_{\delta_k}) = \eta D(\mathfrak{d}_{\delta_1}, \dots, \mathfrak{d}_{\delta_k})$ is a unit of $R|P^e$. This is the case if and only if $D(\mathfrak{d}_{\delta_1}, \dots, \mathfrak{d}_{\delta_k}) \not\equiv 0 \bmod P$.

7.44. Remark. The greatest amongst the degrees of the polynomials in the vectors (7.4) is called the length of $H_k(P^e, P^f)$ and $J_k(P^e, P^f)$. Thus the length is the greatest integer l such that $e-f(l-1) > 0$, hence it is the least integer greater than or equal to e/f.

7.5. Proposition. *Let $a \in P$, $a \notin P^2$, Z_e a vector system mod P^e, W_r a vector system mod P^r containing the zero vector $\mathfrak{o}$, for all integers r, and χ the mapping defined in* § 5.6. *Then the mappings*

$$\mathfrak{y} \to \mathfrak{d}_o + \sum_{\iota > o} \mathfrak{d}_\iota (a^f)^{\sigma(\iota)-1} \mathfrak{y}^\iota \bmod P^e, \quad \mathfrak{y} \in Z_e, \tag{7.5}$$

from Z_e to $(R|P^e)^k$ where $\mathfrak{d}_o \in W_e$, $\mathfrak{d}_\iota \in W_{e-f(\sigma(\iota)-1)-\varepsilon_k(\iota)}$, $\iota < o$, belong to $\chi S_k(P^e, P^f)$, every mapping of $\chi S_k(P^e, P^f)$ has the form (7.5) *and the mappings of* (7.5) *are pairwise distinct. A mapping* (7.5) *belongs to $\chi T_k(P^e, P^f)$ if and only if Det $(\mathfrak{d}_{\delta_1}, \ldots, \mathfrak{d}_{\delta_k}) \not\equiv 0 \bmod P$.*

7.51. Remark. Prop. 5.92 is a special case of Prop. 7.5.

7.52. Lemma. *If $\iota = (i_1, \ldots, i_k) \in M_k$ and $d_\iota \in P^{e-f(\sigma(\iota)-1)-\varepsilon_k(\iota)}$ then there exists a polynomial $u_\iota \in \{P^e\}$ of the form $u_\iota = d_\iota a^{f(\sigma(\iota)-1)} \mathfrak{x}^\iota + \sum_{\lambda < \iota} b_\lambda a^{f(\sigma(\lambda)-1)} \mathfrak{x}^\lambda$.*

Proof. Using the same argument as in the proof of Lemma 5.51, we may take $u_\iota = d_\iota a^{f(\sigma(\iota)-1)} t_\iota$.

7.53. Proof of Prop. 7.5. We proceed along the same lines as in the proof of Prop. 5.92., now using Lemma 7.52 and also considering Prop. 7.43. The detailed proof is left to the reader.

7.54. Corollary. *If*

$$N = N(k, e, f) = \{\iota \in M_k \mid \iota > o,\ e-f(\sigma(\iota)-1) > 0\},$$
$$\bar{N} = \bar{N}(k, e, f) = \{\iota \in M_k \mid \iota > o,\ e-f(\sigma(\iota)-1)-\varepsilon_k(\iota) > 0\},$$
$$L = e+\sum(e-f(\sigma(\iota)-1) \mid \iota \in N), \quad \bar{L} = e+\sum(e-f(\sigma(\iota)-1)-\varepsilon_k(\iota) \mid \iota \in \bar{N})$$

and $\Phi_k(P)$ as in Cor. 5.72, *then, for $q = |R|P|$,*

$$|H_k(P^e, P^f)| = q^{Lk}, \quad |J_k(P^e, P^f)| = \Phi_k(P) q^{(L-k)k},$$
$$|S_k(P^e, P^f)| = q^{\bar{L}k}, \quad |T_k(P^e, P^f)| = \Phi_k(P) q^{(\bar{L}-k)k}.$$

Proof. By (7.4) and (7.5), using a simple counting argument.

7.55. Theorem. *Let $R|P$ be finite, $e > 0$, $f > 0$. Then the groups $J_k(P^e, P^f)$ and $T_k(P^e, P^f)$ are soluble if and only if the linear group $GL(k, R|P)$ is soluble. The group $U_k(R|P^e)$, $e > 1$, is soluble if and only if $GL(k, R|P)$ and the symmetric group Sym $(R|P)^k$ are soluble.*

Proof. By Prop. 7.41, there exists an epimorphism from $G_k(P^e, P^f)$ to $G_k(P, P^f) = G_k(P, (0))$, for $G = J$ and T. But $G_k(P, (0))$ is isomorphic to the group of all polynomial vectors over $R|P$ of the form $A\mathfrak{x}+\mathfrak{b}$, $|A| \neq 0$, by § 7.3. The mapping δ defined by $\delta(A\mathfrak{x}+\mathfrak{b}) = A$ is obviously an epimorphism whose image is $GL(k, R|P)$. Hence $GL(k, R|P)$ is a homomorphic image of $G_k(P^e, P^f)$ under some epimorphism ϑ. By Cor. 7.54, $|\ker \operatorname{Ker} \vartheta|$ is some power of q whence ker Ker ϑ is a p-group and therefore is soluble. Thus the first assertion of the theorem is true while the second statement follows from Th. 5.94 and well-known properties of wreath products.

7.56. Remark. From group theory we know that $GL(k, R|P)$ is soluble if and only if $k = 1$ or if $k = 2$ and $|R|P| = 2, 3$ while Sym $(R|P)^k$ is soluble if and only if $k = 1$, $|R|P| = 2, 3$ or $k = 2$, and $|R|P| = 2$.

7.6. By definition of the semigroups $G_k(P^e, P^f)$, the mapping $\mathcal{F}(\sigma)$ maps $H_k(P^e, P^f)$ onto $S_k(P^e, P^f)$ and $J_k(P^e, P^f)$ onto $T_k(P^e, P^f)$. The proof of Lemma 5.9 shows that $\langle H_k(P^e, P^f); +, -, \mathfrak{o}, \circ \rangle$ is an Ω-multioperator group where $\Omega = \langle \circ \rangle - H_k(P^e, P^f)$ is, in fact, a near-ring—and $J_k(P^e, P^f)$ is a group by Th. 6.4. Hence we see that $K_1 =$ ker Ker $\mathcal{F}(\sigma)|H_k(P^e, P^f)$ is an ideal of $H_k(P^e, P^f)$ and $K_2 =$ ker Ker $\mathcal{F}(\sigma)|J_k(P^e, P^f)$ is a normal subgroup of $J_k(P^e, P^f)$. We are going to derive some results on K_1 and K_2.

7.61. Lemma. *Let $\eta = \eta(P^e)$, $a \in P$, $a \notin P^2$, and W_r a vector system mod P^r containing the zero vector $\mathfrak{o}$, for every integer r. Then the polynomial vectors*

$$C_k(\eta)\left(\mathfrak{c}_o + \sum_{\iota > o} \mathfrak{c}_\iota (a^f)^{\sigma(\iota)-1} t_\iota\right) \tag{7.61}$$

belong to $H_k(P^e, P^f)$, every vector of $H_k(P^e, P^f)$ is of the form (7.61), *and the vectors of* (7.61) *are pairwise distinct if $\mathfrak{c}_o \in W_e$, $\mathfrak{c}_\iota \in W_{e-f(\sigma(\iota)-1)}$, $\iota > o$. A polynomial vector* (7.61) *belongs to $J_k(P^e, P^f)$ if and only if Det $(\mathfrak{c}_{\delta_1}, \ldots, \mathfrak{c}_{\delta_k}) \not\equiv 0 \bmod P$.*

Proof. Let $\mathfrak{f}$ be a vector (7.61). By definition of t_ι (see ch. 3, § 8.6), we have $t_\iota = \sum_{\lambda \leqslant \iota} a_{\iota\lambda}\mathfrak{x}^\lambda$ whence $\mathfrak{f} = C_k(\eta)\sum_{\lambda \geqslant o} \mathfrak{d}_\lambda \mathfrak{x}^\lambda$ where $\mathfrak{d}_\lambda = \sum_{\iota \geqslant \lambda} \mathfrak{c}_\iota a_{\iota\lambda}(a^f)^{\sigma(\iota)-1} = \mathfrak{d}_\lambda(a^f)^{\sigma(\lambda)-1}$, for some $\mathfrak{d}_\lambda$. Hence $\mathfrak{f} \in H_k(P^e, P^f)$. Suppose that some polynomial vector (7.61) equals $\mathfrak{o}$, but $\mathfrak{c}_\lambda(a^f)^{\sigma(\lambda)-1} \not\equiv \mathfrak{o} \bmod P^e$, for some λ. We take λ maximal in M_k with respect to this property, thus $\mathfrak{d}_\lambda \equiv \mathfrak{c}_\lambda(a^f)^{\sigma(\lambda)-1} \not\equiv \mathfrak{o} \bmod P^e$, a contradiction. Hence the polynomial vectors (7.61) are pairwise distinct. Since the number of polynomial vectors (7.61) equals the number of polynomial vectors (7.4), by Prop. 7.43 every element of $H_k(P^e, P^f)$ is of the form (7.61). If

$$C_k(\eta)\left(\mathfrak{c}_o + \sum_{\iota > o} \mathfrak{c}_\iota (a^f)^{\sigma(\iota)-1} t_\iota\right) = C_k(\eta)\left(\mathfrak{d}_o + \sum_{\iota > o} \mathfrak{d}_\iota (a^f)^{\sigma(\iota)-1}\mathfrak{x}^\iota\right),$$

then this equation also holds if $\eta = \eta(P)$. Hence $\mathfrak{c}_{\delta_j} \equiv \mathfrak{d}_{\delta_j} \bmod P$, $j = 1, \ldots, k$, thus $D(\mathfrak{c}_{\delta_1}, \ldots, \mathfrak{c}_{\delta_k}) \equiv D(\mathfrak{d}_{\delta_1}, \ldots, \mathfrak{d}_{\delta_k}) \bmod P$. Prop. 7.43 implies the last statement of the proposition.

7.62. Theorem. *The vectors*

$$\mathfrak{g} = C_k(\eta)\left(\mathfrak{u}_o + \sum_{o \prec \iota} \mathfrak{u}_\iota a^{\max\left(e-\varepsilon_k(\iota),\, f(\sigma(\iota)-1)\right)} t_\iota\right) \tag{7.62}$$

belong to K_1, every element of K_1 is of the form (7.62), *and the vectors* (7.62) *are pairwise distinct, if $\mathfrak{u}_\iota \in W_{\min\left(\varepsilon_k(\iota),\, e-f(\sigma(\iota)-1)\right)}$. The elements of K_2 are just the polynomial vectors*

$$\mathfrak{x} + \mathfrak{g} \tag{7.63}$$

where $\mathfrak{g}$ is a vector of (7.62), *and the vectors* (7.63) *are pairwise distinct.*

Proof. Suppose we have already proved the statement on K_1. Then every polynomial vector (7.63) belongs to $\mathcal{F}(\sigma)^{-1}U_k(R|P^e) \cap H_k(P^e, P^f) = J_k(P^e, P^f)$ and therefore to K_2. Conversely if $\mathfrak{f} \in K_2$, then $\mathfrak{f} - \mathfrak{x} \in K_1$, thus $\mathfrak{f}$ is a vector of (7.63). That the vectors of (7.63) are pairwise distinct is obvious.

We now prove the first assertion: Let $\mathfrak{g} \in K_1$, then, by Lemma 7.61, $\mathfrak{g}$ is of the form (7.61), and $\mathfrak{g} \in K_1$ implies that $\mathfrak{c}_o + \sum_{\iota > o} \mathfrak{c}_\iota (a^f)^{\sigma(\iota)-1} t_\iota \in \{P^e\}^k$. We claim that $\mathfrak{c}_\iota (a^f)^{\sigma(\iota)-1} \equiv \mathfrak{o} \bmod P^{e-\varepsilon_k(\iota)}$, for every ι. Suppose by way of contradiction, that ι is maximal in the lexicographic order of N^k with respect to $\mathfrak{c}_\iota (a^f)^{\sigma(\iota)-1} \not\equiv \mathfrak{o} \bmod P^{e-\varepsilon_k(\iota)}$. But then we have a contradiction to Lemma 5.52. Since, by the proof of Prop. 7.43, $\eta P = (R|P^e)(\eta a)$, thus $\eta P^{e-\varepsilon_k(\iota)} = (R|P^e)(\eta a^{e-\varepsilon_k(\iota)})$, we have $\mathfrak{c}_\iota (a^f)^{\sigma(\iota)-1} \equiv \mathfrak{v}_\iota a^{e-\varepsilon_k(\iota)} \bmod P^e$,

for some $\mathfrak{v}_\iota \in R^k$ and every ι. Hence we may replace $\mathfrak{c}_\iota (a^f)^{\sigma(\iota)-1}$ in (7.61) by $\mathfrak{v}_\iota a^{e-\varepsilon_k(\iota)}$, for every ι which satisfies $e - \varepsilon_k(\iota) > f(\sigma(\iota)-1)$ and so we obtain a representation for $\mathfrak{g}$ which is of the form (7.62) but without the condition on $\mathfrak{u}_\iota$ being taken in account. But $\varepsilon_k(\iota) \leqslant e - f(\sigma(\iota)-1)$ if and only if $f(\sigma(\iota)-1) \leqslant e - \varepsilon_k(\iota)$, thus

$$\min\left(\varepsilon_k(\iota),\, e - f(\sigma(\iota)-1)\right) + \max\left(e - \varepsilon_k(\iota),\, f(\sigma(\iota)-1)\right) = e \tag{7.64}$$

Hence if we replace an element $\mathfrak{u}_\iota$, $\iota > o$, in (7.62) by some $\bar{\mathfrak{u}}_\iota$ such that $\bar{\mathfrak{u}}_\iota \equiv \mathfrak{u}_\iota \bmod P^{\min\left(\varepsilon_k(\iota),\, e-f(\sigma(\iota)-1)\right)}$, the vector $\mathfrak{g}$ remains unchanged. Thus $\mathfrak{g}$ may be taken as in the theorem. Conversely, every element of (7.62) is of the form (7.61) and therefore belongs to $H_k(P^e, P^f)$. Moreover such an element belongs to $C_k(\eta)\{P^e\}^k$, by ch. 3, Lemma 8.61, and therefore to K_1. That the elements (7.62) are pairwise distinct follows from (7.64).

7.63. Corollary. *$\mathcal{F}(\sigma)$ maps $H_k(P^e, P^f)$ isomorphically onto $S_k(P^e, P^f)$ and $J_k(P^e, P^f)$ isomorphically onto $T_k(P^e, P^f)$ if and only if $e \leqslant f(q-1)$ where $q = |R|P|$.*

Proof. By Th. 7.62, $|K_2| = |K_1|$, hence we see that the restriction of $\mathcal{F}(\sigma)$ to $H_k(P^e, P^f)$, $J_k(P^e, P^f)$, resp., is an isomorphism if and only if $|K_1| = 1$. By Th. 7.62, this is the case if and only if $\min\left(\varepsilon_k(\iota),\, e - f(\sigma(\iota)-1)\right) \leqslant 0$ for every $\iota > o$. This is true if and only if $\varepsilon_k(\iota) > 0$ implies $e - f(\sigma(\iota)-1) \leqslant 0$. Since $\iota = (q, 0, \ldots, 0)$ implies $\varepsilon_k(\iota) = 1$, by ch. 3, (8.32) and also $\sigma(\iota) = q$, we have $e \leqslant f(q-1)$. Conversely, since $\varepsilon_k(\iota) > 0$ implies $\sigma(\iota) \geqslant q$, $e \leqslant f(q-1)$ yields the implication in question.

7.64. Lemma. *If $(i_1, \ldots, i_k) = \iota$, then max $\left(e - \varepsilon_k(\iota),\, f(\sigma(\iota)-1)\right) \geqslant e/2$.*

Proof. Suppose that the lemma fails to hold, then there exists some $\iota > o$ such that $f(\sigma(\iota)-1) < e/2 < \varepsilon_k(\iota)$. But $\varepsilon_k(\iota) = \sum_{r=1}^{k} \varepsilon(i_r)$, and by ch. 3, (8.32), we have $\varepsilon(i_r) = (i_r - s_q(i_r))/(q-1)$. By a well-known formula of elementary arithmetic, $s_q\left(\sum_{r=1}^{k} i_r\right) \leqslant \sum_{r=1}^{k} s_q(i_r)$, hence

$$\sum_{r=1}^{k} \varepsilon(i_r) = \left(\sum_{r=1}^{k} i_r - \sum_{r=1}^{k} s_q(i_r)\right)\Big/(q-1) \leqslant \varepsilon\left(\sum_{r=1}^{k} i_r\right) = \varepsilon(\sigma(\iota)).$$

Thus $f(\sigma(\iota)-1) < \varepsilon(\sigma(\iota))$ whence $\sigma(\iota) \leqslant \varepsilon(\sigma(\iota))$. But

$$\varepsilon(\sigma(\iota)) = (\sigma(\iota) - s_q(\sigma(\iota)))/(q-1) \leqslant \sigma(\iota) - s_q(\sigma(\iota)) < \sigma(\iota),$$

a contradiction.

7.65. Theorem. *Let* $\mathfrak{x}+\mathfrak{g}$ *be as in* (7.63), *then* $\mathfrak{x}+\mathfrak{g} \to \mathfrak{g}$ *defines a mapping* $\tau: K_2 \to \langle K_1; +, -, 0\rangle$ *and* τ *is an isomorphism.* $\langle K_1; +, -, 0\rangle$ *is isomorphic to the direct product of* k *copies of the direct product* $\prod(\langle R | P^{\min(\varepsilon_k(\iota),\, e-f(\sigma(\iota)-1))}; +, -, 0\rangle | \iota \in M_k)$ *and therefore is an abelian p-group.*

Proof. By Th. 7.62, $\tau: K_2 \to K_1$ is a bijection. Let n be the least integer greater than or equal to $e/2$, and $\mathfrak{f}_1, \mathfrak{f}_2 \in K_2$. By Th. 7.62, $\mathfrak{f}_1 = \mathfrak{x}+\mathfrak{g}_1$, $\mathfrak{f}_2 = \mathfrak{x}+\mathfrak{g}_2$ where $\mathfrak{g}_i \in K_1$, $i = 1, 2$, hence $\mathfrak{f}_1 \circ \mathfrak{f}_2 = \mathfrak{x}+\mathfrak{g}_2+\mathfrak{g}_1 \circ (\mathfrak{x}+\mathfrak{g}_2)$. By Th. 7.62 and Lemma 7.64, $\mathfrak{g}_i = C_k(\eta)a^n\mathfrak{h}_i$, $i = 1, 2$, for some $\mathfrak{h}_i \in C_k(R)$. Thus, since $2n \geqslant e$, Taylor's formula implies that $\mathfrak{g}_1 \circ (\mathfrak{x}+\mathfrak{g}_2) = C_k(\eta)(a^n\mathfrak{h}_1 \circ (\mathfrak{x}+a^n\mathfrak{h}_2)) = C_k(\eta)a^n\mathfrak{h}_1 = \mathfrak{g}_1$. Hence $\mathfrak{f}_1 \circ \mathfrak{f}_2 = \mathfrak{x}+\mathfrak{g}_1+\mathfrak{g}_2$, therefore $\tau(\mathfrak{f}_1 \circ \mathfrak{f}_2) = \mathfrak{g}_1+\mathfrak{g}_2 = \tau\mathfrak{f}_1+\tau\mathfrak{f}_2$. This means that τ is an isomorphism. The mapping which assigns to each $\mathfrak{g}$ of (7.62) the family $\{\mathfrak{u}_\iota \bmod P^{\min(\varepsilon_k(\iota),\, e-f(\sigma(\iota)-1))} | \iota \in M_k)\}$, is obviously an isomorphism from $\langle K_1; +, -, 0\rangle$ to $\prod(\langle R | P^{\min(\varepsilon_k(\iota),\, e-f(\sigma(\iota)-1))}; +, -, 0\rangle^k | \iota \in M_k)$.

7.7. By the homomorphism theorem, $S_k(P^e, P^f) \cong H_k(P^e, P^f)|K_1$, $T_k(P^e, P^f) \cong J_k(P^e, P^f)|K_2$. We have just investigated K_1 and K_2, so it is sufficient to discuss $H_k(P^e, P^f)$ and $J_k(P^e, P^f)$ in order to get some information on $S_k(P^e, P^f)$ and $T_k(P^e, P^f)$. The near-ring $H_k(P^e, P^f)$ has not been considered yet. There is something known about the group $J_k(P^e, P^f)$, in particular, for R being the ring of rational integers and $k = 1$. The farthest-reaching results for this particular case have been obtained by KOWOL [1]. All these investigations have turned out to be quite elaborate.

8. Characterization of permutation polynomials over finite fields

8.1. Permutation polynomials over finite fields in one indeterminate have already been considered as early as a century ago by HERMITE. Since then plenty of papers have been written on this topic whereas permutation polynomials over finite fields in more than one indeterminate had not been investigated until a few years ago with rather few results. This and the subsequent section are to develop the most remarkable aspects of the theory of permutation polynomials over a finite field K of order q in one indeterminate x.

8.2. The first and most fundamental problem is finding a method of deciding in the simplest possible way whether or not a given polynomial $f \in K[x]$ is a permutation polynomial. Basically there is always an answer, namely by computing the values of f for all elements of K, but this method does not give any deeper insight into the nature of permutation polynomials. In order to state and to prove a theorem due to HERMITE and DICKSON which shall illustrate what we mean by "deeper insight", we require the following definition: The reduction of a polynomial $f \in K[x]$ is the (well-defined) polynomial $g \in K[x]$ such that $[g] < q$ and $g \equiv f \bmod (x^q - x)$. Since $(x^q - x) = \{0\}$, we conclude that g is just the polynomial of least possible degree such that $\sigma g = \sigma f$. We can now state

8.21. Theorem. *A polynomial* f *over the finite field* K *of order* q *and characteristic* p *is a permutation polynomial if and only if*

a) f *has exactly one root in* K,

b) *The reduction of* f^t, $0 < t < q-1$, $t \not\equiv 0 \bmod p$, *has a degree less than or equal to* $q-2$.

The proof will depend on two lemmas which we are going to prove first.

8.22. Lemma. *Let* K *be a finite field of order* q *and* $s \in K$. *Then, if* $\pi_s = 1 - \sum_{j=q-1}^{0} s^{q-1-j}\xi^j$, *we have* $\pi_s s = 1$ *and* $\pi_s t = 0$, *for* $t \neq s$.

8.23. Corollary. *Let* $\varrho: K \to K$ *be any mapping. Then* $\varrho = \sum_{j=q-1}^{0} c_j\xi^j$ *where*

$$c_j = -\sum((\varrho s)s^{q-1-j} | s \in K), \quad j = 1, \ldots, q-1,$$
$$c_0 = \sum((\varrho s)(1-s^{q-1}) | s \in K).$$

Proof. $\pi_s s = 1 - \sum_{j=q-1}^{0} s^{q-1} = 1$. Furthermore

$$\xi\pi_s = s - s^q + \xi - \xi^q - \sum_{j=q-2}^{0} s^{q-1-j}\xi^{j+1} = s - \sum_{i=q-1}^{0} ss^{q-1-i}\xi^i = s\pi_s$$

whence $t(\pi_s t) = s(\pi_s t)$. Hence $\pi_s t = 0$, for $t \neq s$. Furthermore $\varrho = \sum((\varrho s)\pi_s | s \in K)$ implies the corollary.

8.24. Lemma. *Let* $a_1, \ldots, a_q$ *be any family of elements of a finite field* K *of order* q. *Then these elements are pairwise distinct if and only if*

$$\sum_{i=1}^{q} a_i^t = \begin{cases} 0, & \text{for } t = 1, 2, \ldots, q-2 \\ -1, & \text{for } t = q-1. \end{cases}$$

Proof. By Lemma 8.22, the elements $a_1, \ldots, a_q$ are pairwise distinct if and only if the polynomial function

$$\gamma = \sum_{i=1}^{q} \left(1 - \sum_{j=q-1}^{0} a_i^{q-1-j} \xi^j\right) = \sum_{j=q-1}^{0} \left(-\sum_{i=1}^{q} a_i^{q-1-j}\right) \xi^j$$

equals the constant function with value 1. Since $\{0\} = (x^q - x)$, this is true if and only if the condition of the lemma is satisfied.

8.25. Proof of Th. 8.21. By Cor. 8.23, the reduction of f^t is some polynomial $\sum_{j=q-1}^{0} c_j x^j$ where $c_{q-1} = -\sum(f(s)^t \mid s \in K)$. If f is a permutation polynomial, then a) holds obviously and by Lemma 8.24, $\sum(f(s)^t \mid s \in K) = 0$, $t = 1, \ldots, q-2$, whence b) follows. Conversely let a) and b) be satisfied. Then a) implies that $\sum(f(s)^{q-1} \mid s \in K) = -1$ while b) implies $\sum(f(s)^t \mid s \in K) = 0$, for $0 < t < q-1$, $t \not\equiv 0 \bmod p$. Since char $K = p$, we have $\sum(f(s)^{tp} \mid s \in K) = \left(\sum(f(s)^t \mid s \in K)\right)^p$ whence we can drop the hypothesis $t \not\equiv 0 \bmod p$. Hence Lemma 8.24 implies that f is a permutation polynomial.

8.26. Corollary. *If $d > 1$ is a divisor of $q-1$, then there is no permutation polynomial over K of degree d.*

8.3. Next we will characterize permutation polynomials from a quite different point of view. If K is any field and $f \in K[x]$, then $\Phi(f) = [f(x) - f(y)]/[x - y]$ is a polynomial of $K[x, y]$ which is a unique factorization domain. Let C be the algebraic closure of K. An irreducible polynomial $u \in K[x, y]$ is called absolutely irreducible if u is irreducible regarded as a polynomial of $C[x, y]$. This definition can be extended in the obvious way to polynomials u of $K[x_1, \ldots, x_n]$. A polynomial $f \in K[x]$ is called exceptional over K if no absolutely irreducible factor occurs in the prime factorization of $\Phi(f) \in K[x, y]$.

8.31. Theorem. *Let K be any field, $f \in K[x]$ exceptional over K, and char $K = 0$ or char $K > [f]$. Then $\sigma f \in P_1(K)$ is an injective polynomial function, thus f is a permutation polynomial if K is finite.*

(Recently S. D. COHEN [1], by means of algebraic number theory, has proved that, if K is finite, every exceptional polynomial over K—without any restriction—is a permutation polynomial).

The proof of this theorem depends on some lemmas we are going to prove first. C will denote any algebraic closure of K we keep fixed.

8.4. Every non-zero polynomial $u \in K[x, y]$ has a representation

$$u = p_0 x^n + p_1 x^{n-1} + \ldots + p_n \tag{8.41}$$

where $p_i \in K[y]$, $i = 0, \ldots, n$, $p_0 \neq 0$. If $p_0 \in K$, then u is called semimonic in x while u is called monic in x if $p_0 = 1$.

Let $u \in K[x, y]$ be semimonic in x. A splitting field of u over K is a subfield S of C which is a finite normal extension of K such that u, being regarded as a polynomial of $S[x, y]$, splits into absolutely irreducible factors. A splitting field of u over K is called minimal if it is contained in every splitting field of u over K.

8.41. Lemma. *Let $u \in K[x, y]$ be semimonic in x. Then u has one and only one minimal splitting field $S_K(u)$ over K.*

Proof. $p_0^{-1} u \in C[x, y]$ has a unique decomposition into irreducible polynomials, monic in x, up to the order, say

$$p_0^{-1} u = v_1 v_2 \ldots v_r \tag{8.42}$$

If we adjoin all the coefficients of the polynomials v_i and their conjugates to K, we obtain some finite normal extension field S of K which is a subfield of C. Since (8.42) also holds in S, this field is a splitting field of u over K. If T is any splitting field of u over K, then (8.42) is also the decomposition of $p_0^{-1} u$ into irreducible polynomials, monic in x, in $T[x, y]$. Thus, since T is normal over K, we have $T \supseteq S$. Hence S is a minimal splitting field of u over K.

8.42. Let S_K be a normal extension field of K and $v_1, v_2 \in S_K[x, y]$. v_1, v_2 are called conjugate over K if there is an automorphism α of S_K fixing K elementwise such that $\alpha[x, y] v_1 = v_2$. "Being conjugate" is obviously an equivalence relation in $S_K[x, y]$.

8.43. Lemma. *Let $w \in K[x, y]$ be monic in x and irreducible over K. Then any two divisors of w in $S_K(w)$ that are monic in x and irreducible, are conjugate over K.*

Proof. Let $Z = \{z \in S_K(w) \mid z \text{ separable over } K\}$, then Z is a subfield of $S_K(w)$. Since $S_K(w)$ is a finite normal extension of K, we conclude that Z is also a finite normal extension of K. Let

$$w = v_1 v_2 \dots v_r \tag{8.43}$$

be the decomposition of w into polynomials monic in x and irreducible over Z. If $\alpha \in \operatorname{Gal} Z|K$, the Galois group of Z over K, the automorphism $\alpha[x, y]$ of $Z[x, y]$ permutes the polynomials v_i. If $(\operatorname{Gal} Z|K)[x, y] = \{\alpha[x, y] \mid \alpha \in \operatorname{Gal} Z|K\}$, then the product of all the different elements of the orbit of v_1 under $(\operatorname{Gal} Z|K)[x, y]$ is a divisor of w. This product is, however a polynomial over K and monic in x, hence it equals w. Therefore the orbit of v_1 consists of $v_1, \dots, v_r$, and the lemma holds for $Z = S_K(w)$. If Z is a proper subfield of $S_K(w)$, then Z is not a splitting field of w, therefore, WLOG, we may assume that v_1 splits into at least two irreducible factors in $S_K(w)$, say

$$v_1 = v_{11} v_{12} \dots v_{1s} \tag{8.44}$$

where v_{1i} is monic in x and irreducible over $S_K(w)$. Let $\operatorname{char} K = p$, and e the exponent of the extension $S_K(w)|K$. Then $v_{1j}^{p^e} \in Z[x, y]$, for $j = 1, \dots, s$. On the other hand, (8.44) implies that

$$v_1^{p^e} = v_{11}^{p^e} v_{12}^{p^e} \dots v_{1s}^{p^e}. \tag{8.45}$$

Hence $v_{1j}^{p^e}$ is a divisor of $v_1^{p^e}$ in $Z[x, y]$. Since v_1 is irreducible over Z and $Z[x, y]$ is a unique factorization domain, $v_{1j}^{p^e} = v_1^{r_j}$, for some $r_j, j = 1, \dots, s$. Hence

$$v_{1j}^{p^e} = v_{11}^{r_j} v_{12}^{r_j} \dots v_{1s}^{r_j}; \tag{8.46}$$

hence, by the uniqueness of the prime factor decomposition in $S_K(w)$, all the elements v_{1j} are equal, therefore

$$v_1 = v_{11}^s \tag{8.47}$$

is the prime factor decomposition of v_1 in $S_K(w)$. If $\alpha \in \operatorname{Gal} Z|K$ such that $\alpha[x, y]v_1 = v_i$ and β is the extension of α to an automorphism of $S_K(w)$, then (8.47) implies

$$v_i = [\beta[x, y]v_{11}]^s \tag{8.48}$$

which is the prime factor decomposition of v_i in $S_K(w)$. Substitution of (8.48) into (8.43) yields the decomposition of w in $S_K(w)$ into factors which are monic in x and irreducible. Hence any two of these factors are conjugate to v_{11} over K.

8.5. Lemma. *Let $u \in K[x, y]$ be semimonic in x, $a = a(x, y)$ the form consisting of all terms of maximal degree in the normal form of u, $a(x, 0) \neq 0$, and $c \in K$ such that the polynomial $a(x, c) \in K[x]$ has no multiple roots. Then $S_K(u)$ is a subfield of the splitting field of $a(x, c)$ over K in C.*

Proof. Let D be the splitting field of $a(x, c)$ over K in C, and

$$p_0^{-1} u = u_1 u_2 \dots u_r \tag{8.51}$$

the decomposition of $p_0^{-1}u$ into polynomials monic in x and irreducible over D. If U is a finite generating set of $S_K(u)$ over K and T is the set of all elements of C conjugate over D to elements of U, then $L = D(T)$ is a finite normal extension of D containing $S_K(u)$ and is the least extension w.r.t. being a normal extension of D in C and containing $S_K(u)$. Clearly L is a splitting field of u over D, hence L is also a splitting field for every u_j over D. If every u_j is absolutely irreducible, then $D \supseteq S_K(u)$, and we are done. Hence we may assume, WLOG, that u_1 splits into at least two factors in L. Let

$$u_1 = u_{11} u_{12} \dots u_{1s} \tag{8.52}$$

be the decomposition of u_1 into polynomials monic in x and irreducible over L. Since $L \supseteq S_D(u_1)$, the elements u_{1j} are polynomials over $S_D(u_1)$. By Lemma 8.43, there is an automorphism α of $S_D(u_1)$ fixing D elementwise such that $\alpha[x, y]u_{1i} = u_{1j}$. Let $a_1 = a_1(x, y)$ and $a_{1j} = a_{1j}(x, y)$, $j = 1, \dots, s$, be the forms consisting of the terms of maximal degree in the normal form of u_1, u_{1j}, resp. Then $a_1 = a_{11} a_{12} \dots a_{1s}$ whence

$$a_1(x, c) = a_{11}(x, c)\, a_{12}(x, c) \dots a_{1s}(x, c) \tag{8.53}$$

By (8.51), a_1 divides a whence $a_1(x, c)$ divides $a(x, c)$. Since D is the splitting field of $a(x, c)$ in C, $a,(x, c)$ splits into linear factors in D and therefore in L. By (8.53), every $a_{1j}(x, c)$ splits into linear factors of D, thus $a_{1j}(x, c) \in D[x]$, $j = 1, \dots, s$. But $\alpha[x, y]u_{1i} = u_{1j}$ implies $\alpha[x, y]a_{1i} = a_{1j}$ whence $\alpha[x, y]\, a_{1i}(x, c) = a_{1j}(x, c)$. But α fixes D elementwise, therefore $a_{1i}(x, c) = a_{1j}(x, c)$, for all pairs (i, j). Since $a_1(x, c)$ divides $a(x, c)$ which, by hypothesis, has no multiple roots, $a_1(x, c) \in D$. Hence $a_1(x, y)$ is a multiple of y and $a(x, 0) = 0$, a contradiction. Thus every u_j is absolutely irreducible and the proof is complete.

8.6. Lemma. *Let $m > 0$ be an odd integer and $a \in K$. Then $x^m - a$ is either irreducible over K, or there exists $0 < d < m$, $d|m$ such that $x^d - b$ divides $x^m - a$ for some $b \in K$.*

Proof. Let $m = p$ be a prime and $x^p - a = fg$, $f, g \in K[x]$, $[f], [g] < p$. Then $x^p - a = \prod_{\nu=0}^{p-1} (x - \zeta_\nu c)$ where c is in the splitting field of $x^p - a$, and ζ_ν runs trough the p-th roots of unity. Hence $b = f(0) = \pm \zeta c^r$ where ζ is some p-th root of unity and $0 < r < p$. Therefore $(\pm b)^p = c^{rp} = a^r$. There exist integers u, v such that $ur + vp = 1$ whence $a = a^{ur+vp} = (\pm b)^{up} a^{vp}$. Therefore a is the p-th power of some element $a_1 \in K$ whence $x - a_1$ divides $x^p - a$. Now we use induction on m and assume that m is not a prime, and $x^m - a$ is not irreducible. Then every root of $x^m - a$ is of degree less than m over K. If p is a prime dividing m, $k = m/p$, and we assume that $x^k - a$ is not irreducible, then, by induction, $x^d - b$ divides $x^k - a$ for $d|k$, $d < k$ and $b \in K$ whence $x^{m/p} - a = (x^d - b)\, g(x)$, for some $g(x) \in K[x]$. Hence $x^m - a = (x^{dp} - b)\, g(x^p)$, $dp|m$, $dp < m$. Therefore we may assume that $x^k - a$ is irreducible over K. Let c be a root of $x^k - a$. By the first part of the proof, $x^p - c$ is either irreducible over $K(c)$ or has some linear factor in $K(c)$. in the first case e is a root of $x^p - c$, then $[K(e) : K] = [K(e) : K(c)][K(c) : K] = pk = m$, but $e^m = c^k = a$ implies $[K(e) : K] < m$, a contradiction. Therefore $x^p - c$ has some root $e \in K(c)$. If $\mathfrak{N}(s)$ denotes the norm of s w.r.t. $K(c)|K$, then k odd implies that $\mathfrak{N}(c) = (-1)^k (-a) = a$ while, on the other hand $\mathfrak{N}(c) = \mathfrak{N}(e^p) = \mathfrak{N}(e)^p$. Thus a is the p-th power of some $a_1 \in K$, therefore $x^m - a = (x^k)^p - a_1^p$, hence $x^m - a$ has the factor $x^k - a_1$ in $K[x]$.

8.61. Lemma. *Let char $K \nmid n$, $x^n - a$ be an irreducible polynomial in $K[x]$, c a root of $x^n - a$, and suppose 1 is the only n-th root of unity in K. Then K is the only subfield of $K(c)$ which is normal over K.*

Proof. We choose a subfield L of $K(c)$ maximal w.r.t. being normal over K, and assume, by way of contradiction, that L contains K properly. If $[K(c) : L] = d$, then $d|n$. Let $c_1, \ldots, c_d$ be the roots of the minimal polynomial for c over L. Since every c_i is a root of $x^n - a$, we have $c_i = c\zeta_i$ where ζ_i is an n-th root of unity. Hence $c_1 c_2 \ldots c_d = c^d \zeta$ where ζ is some n-th root of unity, on the other hand, $c_1 c_2 \ldots c_d \in L$, thus $\zeta \in K(c)$.

Hence $L(\zeta)$ is a subfield of $K(c)$. Since $L(\zeta)$ is a splitting field for some suitable polynomial over K, $L(\zeta)$ is normal over K, and the maximality of L implies that $\zeta \in L$. Therefore $c^d \in L$. Let $n = md$, and $x^m - a = fg$. Then $x^n - a = f(x^d)\, g(x^d)$ whence $x^m - a$ is also irreducible over K with c^d as a root. Therefore $[K(c^d) : K] = m = [L : K]$. Since $K(c^d) \subseteq L$, we have $L = K(c^d)$. Since L is normal over K, the polynomial $x^m - a$ splits into linear factors in $L[x]$, thus L contains every m-th root of unity. Let p be the least prime dividing m and ε a primitive p-th root of unity. Then $\varepsilon \in L$ and $[K(\varepsilon) : K]$ divides m. Hence $[K(\varepsilon) : K] = 1$ or $[K(\varepsilon) : K] \geqslant p$. But $[K(\varepsilon) : K] | (p-1)$ whence $\varepsilon \in K$, and char $K \neq p$ implies $\varepsilon \neq 1$. This is a contradiction since ε is also an n-th root of unity.

8.62. Lemma. *Let char $K \nmid n$ and suppose 1 is the only n-th root of unity in K. If $a \in K$, then there is some root $c \in C$ of $x^n - a$ such that $K(c) \cap K(\zeta) = K$, for every root of unity $\zeta \in C$.*

Proof. If n were even, then char K would be odd and $-1 \in K$ would be an n-th root of unity different from 1. Thus n is odd. Let d be the least divisor of n such that $x^n - a$ has some divisor $x^d - b \in K[x]$, then Lemma 8.6. implies that $x^d - b$ is irreducible in $K[x]$. Let c be a root of $x^d - b$. Since K contains no d-th root of unity apart from 1, Lemma 8.61 implies that K is the only subfield of $K(c)$ which is normal over K. If $\zeta \in C$ is a root of unity, then $K(\zeta)$ is a normal, separable, abelian extension of K, thus $K(c) \cap K(\zeta)$ is normal over K since $\mathrm{Gal}\, K(\zeta)|K$ is abelian. Hence $K(c) \cap K(\zeta) = K$.

8.7. Lemma. *Let $f \in K[x]$ be exceptional over K and $a, b \in K$, $a \neq b$, $f(a) = f(b)$. Then $f'(a) = f'(b) = 0$.*

Proof. Let $\Phi(f) = \varphi(x, y)$ as in § 8.3, then $\varphi(a, b) = 0$. Since $\varphi(x, y)$ is semimonic in x, this polynomial is the product of an element of K and factors that are monic in x and irreducible in $K[x, y]$. Since f is exceptional none of these factors is absolutely irreducible, therefore each such factor g splits into at least two absolutely irreducible factors in $S_K(\varphi)$, thus g splits into these factors in $S_K(g)$. By Lemma 8.43, these factors are conjugate over K. Hence there are at least two factors φ_1, φ_2 amongst the irreducible factors of φ in $S_K(\varphi)$ and therefore also amongst the irreducible factors of $u = f(x) - f(y)$ in $S_K(\varphi)$ such that $\varphi_1(a, b) =$

$= \varphi_2(a, b) = 0$. We conclude that $f'(a) = (\partial u)/(\partial x)(a, b) = 0$ and $f'(b) = -(\partial u)/(\partial y)(a, b) = 0$.

8.71. Lemma. *Let $f \in K[x]$ be exceptional over K and $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_r x^r$, char $K \nmid r$, $r > 1$, $a_r \neq 0$. Then 1 is the only r-th root of unity in K.*

Proof. Let

$$\Phi(f) = a_n u_1 u_2 \ldots u_t \tag{8.71}$$

be the decomposition of $\Phi(f) = \varphi$ into polynomials which are monic in x and irreducible over K, and $w = w(x, y)$, $w_j = w_j(x, y)$, $j = 1, \ldots, t$, the forms consisting of the terms of minimal degrees in the normal forms of φ, u_j, resp. Then

$$w = a_n w_1 w_2 \ldots w_t. \tag{8.72}$$

On the other hand,

$$w = a_r(x^r - y^r)/(x-y) = a_r \prod (x - \zeta_i y) \tag{8.73}$$

where ζ_i runs through all the roots of $(x^r-1)/(x-1)$ in C. Suppose there is an r-th root $\zeta \neq 1$ of unity in K. Then ζ is one of the elements ζ_i whence $x - \zeta y$ divides w. By (8.72), $x - \zeta y$ divides some w_i. WLOG, we may assume $x - \zeta y$ divides w_1. Since f is exceptional, the polynomial u_1 splits into $k > 1$ polynomials, monic in x and absolutely irreducible in $S_K(\varphi)$, thus u_1 also splits into these factors in $S_K(u_1)$. Then Lemma 8.43 implies that these polynomials are conjugate over K. Let $v_1, \ldots, v_k$ be the forms consisting of the terms of minimal degree of these polynomials, then these v_j are also conjugate over K, and

$$w_1 = v_1 v_2 \ldots v_k. \tag{8.74}$$

Since $x - \zeta y$ divides w_1, one of the polynomials v_j is divisible by $x - \zeta y$. But $\zeta \in K$ and the polynomials v_j are conjugate, hence $x - \zeta y$ divides every v_j. Therefore w has a multiple linear factor. But since char $K \nmid r$, this contradicts (8.73).

8.72. Lemma. *Let $f \in K[x]$ be exceptional over K of degree n, char $K \nmid n$, ζ a primitive n-th root of unity in C, and $L \subseteq C$ a finite extension of K such that $L \cap K(\zeta) = K$. Then f is also exceptional over L.*

Proof. Suppose f is not exceptional over L, then the polynomial $\Phi(f) = \varphi$ has some factor $g \in L[x, y]$ which is monic in x and absolutely irreducible, hence g is an irreducible divisor of φ in $S_K(\varphi)$. If $a = a(x, y)$ is the form consisting of the terms of maximal degree in the normal form of φ, then $a = a_n(x^n - y^n)/(x-y)$ whence $a(x, 0) \neq 0$ and $a(x, 1)$ has no multiple roots. By Lemma 8.5, $S_K(\varphi)$ is a subfield of $K(\zeta)$. Hence the coefficients of g are contained in $L \cap K(\zeta) = K$, and φ is not exceptional over K, contradiction.

8.73. Proof of Th. 8.31. Let $f \in K[x]$ be exceptional over K of degree n, char $K = 0$ or char $K > n$, and L an extension field of K in C which is maximal w.r.t. f being exceptional over L. The existence of such a field L follows from ZORN's Lemma. If $\sigma f \in P_1(L)$ is injective, $\sigma f \in P_1(K)$ is injective a fortiori, hence we can assume that f is not exceptional over any proper finite extension field of K in C. Suppose now that $\sigma f \in P_1(K)$ is not injective. Then there exist $a, b \in K$ such that $a \neq b$, $f(a) = f(b)$. Let $g = f((b-a)x + a) - f(a)$. Then if $0 \neq d \in K$, the polynomial $h = dg$ is exceptional over K, but not exceptional over any proper finite extension field of K in C, and $h(0) = h(1) = 0$. Let

$$h(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_r x^r, \quad a_r \neq 0,$$
$$h(x+1) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_s x^s, \quad b_s \neq 0.$$

For a suitable choice of d, we have $b_s = 1$. Since $h(0) = h(1) = 0$ implies $h'(0) = h'(1) = 0$, by Lemma 8.7, we have $r > 1$ and $s > 1$, and by hypothesis, r, s are not divisible by char K. Hence Lemma 8.71 shows that K contains no r-th and no s-th root of unity except 1. Let ζ be a primitive n-th root of unity in C. By Lemma 8.62, there exists some root c of $x^r - a_r$ such that $K(c) \cap K(\zeta) = K$. By Lemma 8.72, f is also exceptional over $K(c)$ whence $c \in K$. Similarly, there exists some root d of $x^s - c$ in K. Therefore $x^{rs} - a_r$ has the root d in K. We put $\Phi(h) = \varphi(x, y)$, then $h(x) - h(y) = (x-y)\varphi(x, y)$ whence $h(x^s) - h(y^r+1) = (x^s - y^r - 1)\varphi(x^s, y^r+1)$. Let $p(x, y)$ be the form consisting of the terms of minimal degree in the normal form of $\varphi(x^s, y^r+1)$, then

$$a_r x^{rs} - y^{rs} = -p(x, y). \tag{8.75}$$

Hence $-p(x/d, 1) = x^{rs} - 1 = q$. Since char $K \nmid rs$, 1 is a simple root of

q. Let

$$\varphi = a_n u_1 u_2 \dots u_k \tag{8.76}$$

be the decomposition into polynomials which are monic in x and irreducible over K. Then

$$\varphi(x^s, y^r+1) = a_n u_1(x^s, y^r+1) \dots u_k(x^s, y^r+1),$$

thus $p(x, y)$ is the product of the forms consisting of the terms of minimal degree of the polynomials $u_j(x^s, y^r+1)$. Since h is exceptional over K, every u_j splits into at least two irreducible factors in $S_K(\varphi)$ which are conjugate over K, by Lemma 8.43. Hence also every $u_j(x^s, y^r+1)$ splits into at least two factors which are conjugate over K, and so do the forms consisting of the terms of minimal degree in $u_j(x^s, y^r+1)$. Hence also $p(x, y)$ splits in $S_K(\varphi)$ such that there is at least one other factor to each factor which is conjugate. Thus $q = -p(x/d, 1)$ splits in the same way in $S_K(\varphi)$. Therefore every root of q in K is a multiple root which is a contradiction since 1 is a simple root of q.

8.8. Under what conditions does the converse of Th. 8.31 hold? That means we want to know under what conditions on K and $f \in K[x]$ it is true that σf injective implies that f is exceptional over K.

8.81. Theorem. *There exists a sequence $c_1, c_2, \dots$ of integers such that for any finite field K of order $q > c_n$ and $(n, \text{char } K) = 1$ the following statement is true: If $f \in K[x]$ is a permutation polynomial and $[f] = n > 1$, then f is exceptional over K.*

Proof. We require a lemma for the proof of the theorem.

8.82. Lemma. *There exists a monotonically increasing sequence $c_1, c_2, c_3, \dots$ of positive integers with the following property: If K is any finite field such that $|K| > c_d$, then, for every absolutely irreducible polynomial $p \in K[x, y]$ of degree d which is not of the form $a(y-x)$, the equation $p(x, y) = 0$ has a solution (x, y) in K such that $y \neq x$.*

Proof. We put $c_0 = 0$ and construct the sequence $c_0, c_1, c_2, \dots$ recursively: We choose c_d such that $c_d > c_{d-1}$ and $q-(d-1)(d-2)\sqrt{(q)}-k(d) > 2d+2$, for every $q > c_d$, where $k(d)$ is the constant of ch. 6, Th. 9.41. This is a

sequence we require. In order to show this we argue as follows. Let $|K| = q > c_d$, and $p \in K[x, y]$ an absolutely irreducible polynomial of degree d which is not of the form $a(y-x)$. Then $z^d p(x/z, y/z) = u(x, y, z)$ is an absolutely irreducible form of degree d of $K[x, y, z]$ since $u(x, y, z) = g_1 g_2$ implies $p(x, y) = g_1(x, y, 1)\, g_2(x, y, 1)$ whence one of the $g_i(x, y, 1)$ would be a constant, thus $g_i = bz^t$ and g_i itself is a constant. By ch. 6, Th. 9.41, if n is the number of non-equivalent solutions in K of $u(x, y, z) = 0$, then $n \geqslant q-(d-1)(d-2)\sqrt{(q)}-k(d)$, thus $n \geqslant 2d+3$. The number of non-equivalent solutions in K, where $z = 0$, is at most $d+2$, and the number of non-equivalent solutions where $z \neq 0$ and $y = x$ equals the number of different solutions in x of $u(x, x, 1) = p(x, x) = 0$. Since $p(x, y)$ is irreducible and not of the form $a(y-x)$, $p(x, y)$ is not divisible by $y-x$, hence $p(x, x) \in K[x]$ is not the zero polynomial whence $p(x, x) = 0$ has at most d solutions in K. Hence there is at least one solution of $u(x, y, z) = 0$ such that $z \neq 0$ and $x \neq y$, therefore $p(x, y) = 0$ has a solution in K as stated in the lemma.

8.83. Proof of Th. 8.81. Let $f \in K[x]$ be a permutation polynomial such that the hypothesis of the theorem is satisfied for the constant c_n of Lemma 8.82. If $\varphi = \Phi(f) \in K[x, y]$, then the equation $\varphi(x, y) = 0$ has no solution (x, y) in K such that $y \neq x$. Let $\varphi = a_n p_1 \dots p_r$ be the decomposition of φ into polynomials which are monic in x and irreducible over K. Suppose, by way of contradiction, that f is not exceptional, then, WLOG, p_1 is absolutely irreducible. We put $[p_1] = d$. If $p_1 = a(y-x)$, then $f(x)-f(y) = (x-y)^2 g(x, y)$, for some $g(x, y) \in K[x, y]$, hence $f'(y) = 2(x-y)\, g(x, y)-(x-y)^2 (\partial g(x, y)/\partial y)$, thus $f'(x) = 0$, a contradiction since $(n, \text{char } K) = 1$. Therefore p_1 is not of the form $a(y-x)$, and $|K| > c_n > c_d$. Hence $p_1(x, y) = 0$ has a solution in K such that $y \neq x$ and so has $\varphi(x, y) = 0$, by Lemma 8.82, a contradiction.

8.84. Remark. The hypothesis $(n, \text{char } K) = 1$ is indispensable, for x^p is a permutation polynomial if char $K = p$, but $x^p-y^p = (x-y)^p$ shows that x^p is not exceptional over K.

8.85. Lemma. *Let $f \in K[x]$ be exceptional over K of degree $n > 1$ and char $K \nmid n$. Then K contains no n-th root of unity except* 1.

Proof. We proceed almost in the same way as in the proof of Lemma 8.71, but replace "form consisting of the terms of minimal degree" by "form

consisting of the terms of maximal degree". The details of the proof are left to the reader.

8.86. Theorem. *If $n > 1$ is an integer and K is a finite field of order q such that $(q, n) = 1$, $(q-1, n) > 1$, and $q > c_n$, then there is no permutation polynomial of degree n in $K[x]$.*

Proof. Let ζ be any generator of the multiplicative group of K, then if $(q-1, n) = d > 1$, we see that $\zeta^{q-1/d}$ is an n-th root of unity different from 1. By Lemma 8.85, there is no exceptional polynomial of degree n in $K[x]$. By Th. 8.81, there is no permutation polynomial of degree n in $K[x]$.

8.87. Corollary. *Let $n > 0$ be even and K a finite field of order q such that $(q, n) = 1$ and $q > c_n$. Then there is no permutation polynomial of degree n in $K[x]$.*

Proof. Clear.

8.88. Remark. The hypothesis $(q-1, n) > 1$ is indispensable, for if $(q-1, n) = 1$, then x^n is a permutation polynomial in $K[x]$.

8.89. Remark. CARLITZ has conjectured that, for any even number $n > 0$, there exists a constant b_n such that, for any finite field K of odd order $q > b_n$, there is no permutation polynomial of degree n in K. Cor. 8.87 shows that this conjecture is true for $n = 2^m$. In all the other cases, the conjecture has been verified only for $n = 6$ (DICKSON [2]) and $n = 10$ (HAYES [1]) so far.

8.9. Th. 8.31 and Th. 8.81 together show: For every $n > 1$, there is a constant l_n such that, for any finite field K such that char $K > l_n$, a polynomial $f \in K[x]$ of degree n is a permutation polynomial if and only if f is exceptional over K. We may take $l_n = \max(c_n, n)$.

8.91. Remark. Th 8.86 and Cor. 8.87 tell us something about the nonexistence of permutation polynomials of given degree n in certain finite fields which is ultimately a consequence of the Riemann hypothesis for algebraic function fields over finite fields. This hypothesis, however, has

also some consequences for the existence of certain permutation polynomials over certain fields, such as

8.92. Theorem. *Let $e > 1$ be any integer. Then there exists some constant m_e such that, in any finite field of order q, $q \equiv 1 \bmod e$, $q > m_e$, there is an element $a \neq 0$ with the property: Every polynomial $f = x^c(x^{(q-1)/e} + a)^k$, $(c, q-1) = 1$, $k \geqslant 1$, is a permutation polynomial.*

Proof. Let K be a finite field of order q and $q \equiv 1 \bmod e$. Let $w \in K$ be of multiplicative order e and

$$y_s^e = \frac{w - w^s}{w-1} + \frac{w^s - 1}{w-1} x^e, \quad s = 2, 3, \ldots, e-1, \tag{8.91}$$

a system of equations in the unknowns $x, y_2, \ldots, y_{e-1}$. (8.91) satisfies the conditions of ch. 6, Th. 9.42. since $w - w^s \neq 0$, $w^s - 1 \neq 0$, and $(w - w^s/w-1)(w^t - 1/w-1) = (w - w^t/w-1)(w^s - 1/w-1)$ implies $w(w^t - w^s) = w^t - w^s$ whence $w = 1$ or $w^t = w^s$, thus $t = s$. Hence ch. 6, Th. 9.42 implies that, for $q > C$, where C is some positive constant, the number n of solutions of (8.91) in K satisfies $n \geqslant q/2$. But the number of those solutions of (8.91) for which $x^e = 0$ or 1, or w, or $(w^s - w/w^s - 1)$ is at most $(e+1)e^{e-2}$. Hence if $q > m_e$, for some suitable constant m_e, the system (8.91) has always a solution $x, y_2, \ldots, y_{e-1}$ such that x^e is different from 0, 1, w, and $(w^s - w/w^s - 1)$, $s = 2, 3, \ldots, e-1$. Let us choose such a solution $x, y_2, \ldots, y_{e-1}$ and put $a = (x^e - w/1 - x^e) \neq 0$. Then, for $2 \leqslant s \leqslant e-1$, we have

$$w^s + a = w^s + \frac{x^e - w}{1 - x^e} = \frac{(1-w^s)x^e + w^s - w}{1 - x^e} = \frac{(1-w)y_s^e}{1-x^e} = y_s^e(1+a).$$

Since $w^s + a \neq 0$, $1 \leqslant s \leqslant e$, we obtain

$$(w^s + a)^{(q-1)/e} = (1+a)^{(q-1)/e}, \quad 1 \leqslant s \leqslant e. \tag{8.92}$$

Let f be as in the theorem and suppose that for $u, v \in K$, $f(u) = f(v)$. Then $f(u)^{(q-1)/e} = f(v)^{(q-1)/e}$ whence

$$u^{c(q-1)/e}(u^{(q-1)/e} + a)^{k(q-1)/e} = v^{c(q-1)/e}(v^{(q-1)/e} + a)^{k(q-1)/e}. \tag{8.93}$$

If u or v equals zero, then also v or u, resp., equals zero, otherwise $w^s + a = 0$, for some s. If both u and v are different from zero, then $u^{(q-1)/e}$ and $v^{(q-1)/e}$ are e-th roots of unity, hence $u^{(q-1)/e} = w^r$

and $v^{(q-1)/e} = w^t$, for some r and t. Hence (8.93) can be written as

$$w^{rc}(w^r+a)^{k(q-1)/e} = w^{tc}(w^t+a)^{k(q-1)/e}. \tag{8.94}$$

Then (8.92) implies

$$w^{rc}(1+a)^{k(q-1)/e} = w^{tc}(1+a)^{k(q-1)/e}. \tag{8.95}$$

Since $a \neq -1$, we have $w^{rc} = w^{tc}$ whence $w^r = w^t$ since $(c, q-1) = 1$. Therefore $u^{(q-1)/e} = v^{(q-1)/e}$. But $f(u) = f(v)$ implies $u^c(u^{(q-1)/e}+a)^k = v^c(v^{(q-1)/e}+a)^k$. Since $w^s+a \neq 0$, for all s, we have $u^c = v^c$ and therefore $u = v$ since $(c, q-1) = 1$. We conclude that f is a permutation polynomial.

9. Semigroups of permutation polynomials and groups of polynomial permutations over finite fields

9.1. Let K be a finite field of order q and $\langle K[x]; \circ \rangle = S$ the semigroup of polynomials over K with polynomial composition $\circ$ as operation as in § 1.2. A polynomial $f \in K[x]$ is called regular if $f'(a) \neq 0$, for all $a \in K$.

9.11. Lemma. *The set S_1 of all regular polynomials of $K[x]$ is a subsemigroup of the semigroup S.*

Proof. The chain rule implies $(f \circ g)' = (f' \circ g)g'$ whence $f, g \in S_1$ implies $f \circ g \in S_1$, and S_1 is not empty since $x \in S_1$.

9.12. By ch. 3, § 11.45, the subset T of S consisting of all permutation polynomials over K is a subsemigroup of S. If U is any subsemigroup of T, then σU is a subsemigroup of $\sigma T = U_1(K) = \operatorname{Sym} K$, the latter equality holds since K is polynomially complete by ch. 1, Th. 12.21. Hence σU is a subgroup of Sym K. Conversely if W is a subgroup of Sym K, then clearly $\sigma^{-1}W$ is a subsemigroup of T.

9.13. Lemma. *The canonical epimorphism $\sigma: K[x] \to P_1(K)$ induces a mapping from the set of all semigroups of permutation polynomials onto the set of all subgroups of Sym K. Furthermore σ also induces a surjective mapping from the set of all semigroups of regular permutation polynomials to the set of all subgroups of Sym K.*

Proof. The first assertion has just been proved above. If U is a subsemigroup of T and $U_1 = U \cap S_1$ is not empty, then U_1 is also a subsemigroup of T. We have to show that, for any function $\pi \in P_1(K)$, there is a regular polynomial $g \in K[x]$ such that $\sigma g = \pi$. Let $f \in S$ such that $\sigma f = \pi$. Since ker Ker $\sigma = (x^q - x)$, we have $\sigma k = \pi$, for any $k = f + h(x^q - x)$. Since $k' \equiv f' - h \bmod \ker \operatorname{Ker} \sigma$, and K is polynomially complete, $k \in K[x]$ is regular, for some suitable $h \in K[x]$.

9.14. Remark. The importance of regular permutation polynomials stems from the fact that if Q is a primary ideal of the ring R with associated prime ideal P such that $R|Q$ is finite and $Q \neq P$, then $f \in R[x]$ is a permutation polynomial mod Q if and only if $\eta(P)(x)f$ is a regular permutation polynomial of the finite field $R|P$, by Prop. 4.31.

9.2. We are now going to consider some special classes of semigroups of permutation polynomials as recently investigated in various papers (e.g. WELLS [1]). Throughout this subsection, K will denote a finite field of order q, Q the multiplicative group of K, A the subgroup of Q of order m, and B_j, $j = 1, 2, \ldots, (q-1)/m = k$ the cosets of A. In each B_j, we select an element b_j.

9.21. Lemma. *The polynomial*

$$p_j = -m\left(\sum_{t=0}^{k-1} b_j^{(k-t)m} x^{tm}\right) \tag{9.21}$$

is the unique polynomial in $K[x]$ such that $[p_j] < q$, $p_j(0) = -m$, $p_j(y) = 1$ for $y \in B_j$, and $p_j(y) = 0$ otherwise.

Proof. Since $\{0\} = (x^q - x)$, there is at most one such polynomial. Furthermore $p_j(0) = -mb_j^{q-1} = -m$. If $y \in B_j$, then $y = b_j a$, $a \in A$, hence $y^m = b_j^m$ whence B_j is just the set of solutions of $x^m = b_j^m$ in K. Hence $p_j(y) = -mkb_j^{mk} = -(q-1) = 1$, for $y \in B_j$. Moreover (9.21) implies

$$xx^m p_j = -mx\left(b_j^m \sum_{t=0}^{k-1} b_j^{(k-t)m} x^{tm} + b_j^m(x^{q-1} - 1)\right),$$

hence $xx^m p_j \equiv x b_j^m p_j \bmod \{0\}$. Therefore $p_j(y) = 0$ if $y \neq 0$ and $y \notin B_j$.

9.22. Lemma. *Let G be a group of permutations of A, H a group of permutations of the set $B = \{b_1, \ldots, b_k\}$, and U the set of all polynomials $f \in K[x]$ of the form*

$$f = \sum_{t=1}^{k} (\varrho b_t)\, l_t(b_t^{-1}x)\, p_t \tag{9.22}$$

where $\varrho \in H$ and l_t, $t = 1, \ldots, k$, is a polynomial of $K[x]$ such that $l_t(0) = 0$ and $l_t(y) = \tau_t y$, for all $y \in A$, $\tau_t \in G$. Then every polynomial of U is a permutation polynomial, and σU is a subgroup of Sym K isomorphic to the wreath product of G by H.

Proof. Clearly $f(0) = 0$, and if $a \in A$, then, by Lemma 9.21, $f(b_i a) = (\varrho b_i)(\tau_i a)$. Hence f is a permutation polynomial. If $\chi : B \times A \to Q$ is defined by $\chi(b_i, a) = b_i a$, then χ is a bijection and $\chi^{-1}(\sigma f)\chi(b_i, a) = (\varrho b_i, \tau_i a)$. Thus $\chi^{-1}(\sigma f)\chi$ is an element of the wreath product W of G by H. Clearly $\sigma f \to \chi^{-1}(\sigma f)\chi$ is a bijection from σU to W and the inverse of this bijection is an isomorphism from W to σU.

9.23. Theorem. *Let m be a divisor of $q-1$, $k = (q-1)/m$, A the subgroup of Q of order m and $B = \{b_1, \ldots, b_k\}$ a system of representatives for the cosets B_j of A. Then:*

a) *The set U_1 of all permutation polynomials of the form $xg(x^m)$ where $g \in K[x]$ is a subsemigroup of T and σU_1 is isomorphic to the wreath product of the regular representation Z_m of A by the symmetric group Sym B of B.*

b) *The set U_2 of all permutation polynomials of the form $xg(x^m)^k$ is a subsemigroup of U_1, and σU_2 is isomorphic to the direct product of k copies of Z_m.*

c) *The set U_3 of all permutation polynomials of the form $x^r g(x^m)$ where $r > 0$, is a subsemigroup of T, and σU_3 is a group extension of σU_1 by the group of prime residue classes mod m.*

Proof. a) U_1 is obviously a subsemigroup of T. In Lemma 9.22, set $G = Z_m$ and $H = \text{Sym } B$. Then $l_t = a_t x + g_t$, where $a_t \in A$ and $g_t \in K[x]$ such that $g_t(y) = 0$, for $y \in \{0\} \cup A$. Hence U consists of all polynomials

$$f = \sum_{t=1}^{k} (\varrho b_t)\, a_t b_t^{-1} x p_t + \sum_{t=1}^{k} (\varrho b_t)\, g_t(b_t^{-1}x)\, p_t,$$

hence $\sigma U = \sigma V$ where $V \subseteq U$ is the set of all polynomials

$$h = \sum_{t=1}^{k} (\varrho b_t) a_t b_t^{-1} x p_t. \tag{9.23}$$

Every polynomial (9.23) is a permutation polynomial of the form

$$h = x \sum_{t=1}^{k} c_t p_t, \quad c_t \in Q. \tag{9.24}$$

Conversely such a polynomial (9.24) can be written as $h = \sum_{t=1}^{k} c_t b_t b_t^{-1} x p_t$. Since h maps $B_j = b_j A$ onto $c_j b_j A$ by Lemma 9.21, the $c_j b_j$'s form a full set of representatives for the cosets B_j whence $c_t b_t = (\varrho b_t) a_t$, for every t, where ϱ is a permutation of B. Hence V is the set of all permutation polynomials of the form (9.24). By (9.21), every such permutation polynomial belongs to U_1 whence $\sigma V \subseteq \sigma U_1$, and if conversely $f = xg(x^m) \in U_1$, then $f(b_j a) = b_j a g(b_j^m)$, for every $a \in A$, whence

$$\sigma f = \sigma\Big[x \sum_{t=1}^{k} g(b_t^m) p_t\Big].$$

Hence $\sigma U_1 \subseteq \sigma V$, and we conclude that $\sigma U_1 = \sigma U$. Lemma 9.22 completes the proof of part a).

b) U_2 is obviously a subsemigroup of U_1. Let $\varkappa : \sigma U_1 \to W$, where W is the wreath product of Z_m by Sym B, be an isomorphism and λ the epimorphism which maps every element of W onto the corresponding permutation of Sym B. We put $L = \ker \operatorname{Ker} \lambda\varkappa$. The proof of Lemma 9.22 shows that if h is of the form (9.23) then $\sigma h \in L$ if and only if ϱ is the identical permutation. Since $\sigma U_1 = \sigma V$, we have $L = \sigma R$ where

$$R = \Big\{x \sum_{t=1}^{k} a_t p_t \mid \ a_t \in A\Big\} = \Big\{x \sum_{t=1}^{k} d_t^k p_t \mid \ d_t \neq 0\Big\}.$$

Since

$$\sigma\Big[x \sum_{t=1}^{k} d_t^k p_t\Big] = \sigma\Big[x\Big(\sum_{t=1}^{k} d_t p_t\Big)^k\Big],$$

we have $L = \sigma R_1$ where R_1 is the set of all permutation polynomials of the form $x\Big(\sum_{t=1}^{k} d_t p_t\Big)^k$, and every such permutation polynomial belongs to U_2. Conversely if $f = xg(x^m)^k \in U_2$, then $f(b_j a) = b_j a g(b_j^m)^k$ implies $\sigma f = \sigma\Big[x\Big(\sum_{t=1}^{k} g(b_j^m) p_t\Big)^k\Big]$. Hence $\sigma U_2 = L$ which proves b).

c) U_3 is obviously a subsemigroup of T. If $f = x^r g(x^m) \in U_3$, and $(r, m) = d > 1$, then there exists $1 \neq z \in K$ such that $z^d = 1$ whence $z^r = z^m = 1$ and $f(z) = f(1)$. Hence $(r, m) = 1$. If $x^r g(x^m)$, $x^s h(x^m) \in U_3$ and $\sigma x^r g(x^m) = \sigma x^s h(x^m)$, then, for all $a \in A$, we have $a^r g(1) = a^s h(1)$.

Since $g(1) \neq 0$, $a^{r-s} = 1$, for all $a \in A$, whence $r \equiv s \bmod m$. Therefore we can define a mapping $\vartheta : \sigma U_3 \to$ group of prime residues mod m by $\vartheta\sigma(x^r g(x^m)) = r \bmod m$, which is obviously a homomorphism. Let $(r, m) = 1$, $n = \prod(\text{primes } p \mid p \nmid m \text{ and } p \mid q-1)$. If $b > 0$ is a solution of $b \equiv r \bmod m$, $b \equiv 1 \bmod n$, then $(b, q-1) = 1$ whence $x^b \in U_3$ and $\vartheta(\sigma x^b) = r \bmod m$. Hence ϑ is an epimorphism whose kernel is just σU_1.

9.3. Proposition. a) *The set L of all linear polynomials of $K[x]$ is a subsemigroup of S which is even a group. Every polynomial of L is a regular permutation polynomial.*

b) *L is isomorphic to the semidirect product of the additive group A of K by the multiplicative group Q of K. The canonical epimorphism $\sigma : K[x] \to P_1(K)$ maps L injectively into $P_1(K)$, hence $\sigma L \cong L$.*

Proof. Obvious.

9.31. A permutation polynomial of the form x^n is called a power permutation polynomial.

9.32. Proposition. *Let K be a finite field of order q and $\mathbf{Z}$ the ring of rational integers. Then*

a) *$N = \{x^n \in K[x] \mid n \geq 1\}$ is a commutative subsemigroup of S. A polynomial of N is a permutation polynomial if and only if $(n, q-1) = 1$ and is regular if and only if $n = 1$.*

b) *Let P be the semigroup of permutation polynomials of N. Then σN is isomorphic to the multiplicative semigroup of $\mathbf{Z}|(q-1)$ and $\sigma P \cong \mathcal{C}(\mathbf{Z}|(q-1))$. Hence $|\sigma P| = \varphi(q-1)$ where φ denotes the Euler φ-function.*

Proof. Obvious.

9.4. Lemma. *Let $\mathbf{Z}$ be the ring of rational integers, y_1, y_2 indeterminates and $k > 0$ an integer. Then $(k/(k-t))\binom{k-t}{t}$ is an integer, for $0 \leq t < k/2$ and $t \in \mathbf{Z}$, and*

$$y_1^k + y_2^k = \sum_{t=0}^{[k/2]} \frac{k}{k-t}\binom{k-t}{t}(-y_1y_2)^t(y_1+y_2)^{k-2t} \tag{9.41}$$

holds in $\mathbf{Z}[y_1, y_2]$ where $[k/2]$ denotes the greatest integer $t \leq k/2$.

Proof. This is an immediate consequence of Waring's formula (ch. 6, § 9.2).

9.41. Let R be a commutative ring with identity. A polynomial $g_k = g_k(a, x)$ over R of the form

$$g_k = \sum_{t=0}^{[k/2]} \frac{k}{k-t}\binom{k-t}{t}(-a)^t x^{k-2t} \tag{9.42}$$

where $k \geq 1$ is an integer and $a \in R$, is called a Dickson polynomial over R.

9.42. Remark. Dickson polynomials are closely related to Čebyshev polynomials of the first kind: If we substitute $y_1 = e^{i\varphi}$, $y_2 = e^{-i\varphi}$ in (9.41), then $2\cos k\varphi = g_k(1, 2\cos\varphi)$ whence, if t_k denotes the k-th Čebyshev polynomial, $2t_k(\cos\varphi) = g_k(1, 2\cos\varphi)$, i.e. $g_k(1, 2x) = 2t_k(x)$. If $R = K$ is a field and char $K \neq 2$, $a \neq 0$, and $\sqrt{(a)}$ is a square root of a in an extension field of K, and if the image of any polynomial $f \in \mathbf{Z}[x]$ under the extension of the epimorphism from $\mathbf{Z}$ to the prime field of K to a homomorphism from $\mathbf{Z}[x]$ to $K[x]$ which fixes x is again denoted by f, then

$$2t_k(x/2\sqrt{a}) = g_k(1, x/\sqrt{a}) = \sum_{t=0}^{[k/2]} \frac{k}{k-t}\binom{k-t}{t}(-1)^t(x/\sqrt{a})^{k-2t}$$
$$= (1/\sqrt{a})^k g_k(a, x)$$

hence

$$g_k(a, x) = 2(\sqrt{a})^k t_k(x/2\sqrt{a}). \tag{9.43}$$

Since $g_k(0, x) = x^k$, we will consider only Dickson polynomials $g_k(a, x)$ where $a \neq 0$.

9.43. Theorem. *If K is a finite field of order q and characteristic p and $0 \neq a \in K$, then a Dickson polynomial $g_k(a, x) \in K[x]$ is a permutation polynomial of K if and only if $(k, q^2-1) = 1$, and $g_k(a, x)$ is a regular permutation polynomial of K if and only if $(k, p(q^2-1)) = 1$.*

Proof. Let $z \neq 0$ be any element of an arbitrary extension field of K, then the substitution $y_1 = z$, $y_2 = a/z$ in (9.41) yields

$$g_k(a, z+(a/z)) = z^k + (a/z)^k. \tag{9.44}$$

Each of the q quadratic equations in K,

$$x^2-rx+a=0, \quad r\in K, \tag{9.45}$$

has two solutions (which may possibly coincide) in some extension field H of K of order q^2. Let $M(a)$ be the subset of H consisting of all those elements of H which are solutions of an equation (9.45). If $0\neq u\in K$, then $u+(a/u)=r$ whence $u\in M(a)$. Suppose $u\in M(a)\smallsetminus K$ and $x^2-rx+a=0$ is an equation (9.45) which is satisfied by u. Since $\vartheta z=z^q$ defines an automorphism $\vartheta\in \operatorname{Gal} H|K$, also u^q is a solution of this equation. Hence $u^{q+1}=a$. Conversely if $u\in H$ and $u^{q+1}=a$, then $u+(a/u)=u+u^q=r\in K$ whence $u\in M(a)$. Therefore

$$M(a)=\{u\in H| \quad u^{q-1}=1 \quad \text{or} \quad u^{q+1}=a\}. \tag{9.46}$$

Suppose now that $(k, q^2-1)=1$, and $g_k(a, s)=g_k(a, t)$, for some elements $s, t\in K$. Let $u, v\in H$ such that $u+(a/u)=s$ and $v+(a/v)=t$, then (9.44) implies $u^k+(a/u)^k=v^k+(a/v)^k$ whence $u^k=v^k$ or $u^k=(a/v)^k$. Therefore $u=v$ or $u=a/v$, thus $s=t$, and g_k is a permutation polynomial.

Now suppose that $(k, q^2-1)=d>1$. If d is even, then q is odd and k is even whence $g_k(a, x)$ contains only even powers of x, by (9.42). If $0\neq c\in K$, then $c\neq -c$, but $g_k(a, c)=g_k(a, -c)$, hence g_k is not a permutation polynomial. If d is odd, then there exists an odd prime p such that $p|d$, hence $p|k$ and $p|(q-1)$, or $p|k$ and $p|(q+1)$. In the first case, there are p elements $v\in K$ with $v^p=1$, and these elements also satisfy $v^k=1$ whence $g_k(a, v+a/v)=1+a^k$, for all these elements v, but $v_1+a/v_1=v_2+a/v_2$ implies $v_1=v_2$ or $v_1=a/v_2$, hence there are at least two different elements $w_i=v_i+a/v_i$, $i=1, 2$, in K such that $g_k(a, w_1)=g_k(a, w_2)$. In the second case there are p elements $v\in H$ such that $v^p=1$ and therefore also $v^{q+1}=1$. If t is a solution of $u^{q+1}=a$, then $\{tv|\ v^{q+1}=1\}$ is the set of all solutions of $u^{q+1}=a$, hence there are p elements u such that $u^{q+1}=a$ which have equal p-th powers and therefore also equal k-th powers. Again by (9.44), we conclude that $g_k(a, w)=g_k(a, w_1)$ for two different elements $w, w_1\in K$. So in either case g_k is not a permutation polynomial.

Let z be an indeterminate and $K(z)$ the field of rational functions in z over K. Since $K(z)$ is an extension field of K, (9.44) also holds for $z\in K(z)$. We differentiate (9.44) and obtain

$$g_k'(a, z+(a/z))\,(1-(a/z^2))=kz^{k-1}-k(a^k/z^{k+1}),$$

hence

$$g_k'(a, z+(a/z))=k\frac{(z^2)^k-a^k}{z^{k-1}(z^2-a)}=\frac{k}{z^{k-1}}\sum_{j=0}^{k-1}(z^2)^{k-1-j}a^j=\frac{k}{z^{k-1}}h(z) \tag{9.47}$$

where $h(z)\in K[z]$. Hence $z^{k-1}g_k'(a, z+(a/z))=kh(z)$, thus (9.47) holds for every $z\neq 0$ of an arbitrary extension field of K. Let g_k be a regular permutation polynomial, then $(k, q^2-1)=1$. If $s\in K$, then let $u\in H$ such that $u+(a/u)=s$. Then (9.47) implies $g_k'(a, s)=(k/u^{k-1})h(u)$ whence $(k, p(q^2-1))=1$. Conversely if $(k, p(q^2-1))=1$, then g_k is a permutation polynomial of K. Suppose there is some $s\in K$ such that $g_k'(a, s)=0$, then, for $u+(a/u)=s$, we have $h(u)=0$. Hence $(u^2-a)h(u)=(u^2)^k-a^k=0$, therefore $u^2=a$. But then $h(u)=\sum_{j=0}^{k-1}a^{k-1}=ka^{k-1}=0$, a contradiction since $p\nmid k$. Hence g_k is a regular permutation polynomial.

9.5. For an arbitrary $b\in K$, (9.42) implies $g_k(ab^2, x)=\sum_{t=0}^{[k/2]}(k/k-t)\binom{k-t}{t}\cdot(-a)^t b^k b^{-(k-2t)}x^{k-2t}=b^k g_k(a, (1/b)x)$. Hence, if char $K=2$, then every polynomial $g_k(a, x)\in K[x]$, $a\neq 0$, can be obtained from composition of $g_k(1, x)$ by linear polynomials $ux\in K[x]$, and if char $K\neq 2$, composition of either $g_k(1, x)$ or $g_k(u, x)$, u being a fixed non-square of K, by linear polynomials $ux\in K[x]$. In the second case, we can also obtain every $g_k(a, x)\in K[x]$, $a\neq 0$, from composition of $g_k(1, x)$ by linear polynomials $ux\in H[x]$ where H is an extension field of K of order q^2. Thus, in a certain sense, all the Dickson polynomials $g_k(a, x)$, $a\neq 0$, can be "reduced" to the Dickson polynomial $g_k(1, x)=h_k(x)$. We will therefore restrict ourselves to this particular type for the remainder of this section.

If K is the field of rationals, then (9.43) shows that $g_k(1, x)=2t_k(x/2)=g_k$ where g_k is the polynomial which has been introduced in § 3.3. Hence, for an arbitrary field K, the set $V=\{g_k(1, x)\,|\,k\geq 1\}$ is just the P-chain over K of Čebyshev polynomials of § 3.32, which proves

9.51. Proposition. *The set $V=\{h_n=g_n(1, x)|\ n\geq 1\}$ is a commutative subsemigroup of S which is isomorphic to the multiplicative semigroup I of positive integers.*

9.52. Proposition. *Let K be any finite field of order q and characteristic p, W the semigroup consisting of the permutation polynomials of V, W_1 the*

semigroup of all regular permutation polynomials of V, and $v = q^2-1$, for $p = 2$, $v = (q^2-1)/2$, for $p \neq 2$. If $C(1)$ denotes the subgroup of $\mathcal{L}(\mathbf{Z}|(v))$ generated by $\{1 \bmod v, -1 \bmod v, q \bmod v, -q \bmod v\}$ which is of order 2, for $q \leqslant 3$, and of order 4 otherwise, then σV is isomorphic to the factor semigroup of the multiplicative semigroup of $\mathbf{Z}|(v)$ mod $C(1)$, and $\sigma W = \sigma W_1$ is isomorphic to the factor group of $\mathcal{L}(\mathbf{Z}|(v))$ mod $C(1)$.

Proof. $\vartheta k = \sigma h_k$ defines an epimorphism $\vartheta : I \to \sigma V$. The kernel Ker ϑ of ϑ is a congruence on I. Let $C(l)$ be the congruence class of $l \in I$ under Ker ϑ. Then $k \in C(l)$ if and only if $\vartheta k = \vartheta l$ which is equivalent to $h_k(s) = h_l(s)$, for every $s \in K$. If $M(1)$ is defined as in the proof of Th. 9.43, then (9.44) shows that $h_k(s) = h_l(s)$, for every $s \in K$, is equivalent to $u^k + (1/u^k) = u^l + (1/u^l)$, for every $u \in M(1)$. This is true if and only if $u^k = u^l$ or $u^k = 1/u^l$, for every $u \in M(1)$. Let w be a generator of the multiplicative group of H, then (9.46) implies

$$M(1) = \{u | u = w^{m(q+1)} \quad \text{or} \quad u = w^{n(q-1)}\}. \tag{9.5}$$

Hence $u^k = u^l$ or $u^k = 1/u^l$ for every $u \in M(1)$ if and only if $w^{k(q+1)} = w^{l(q+1)}$ or $w^{k(q+1)} = w^{-l(q+1)}$ and $w^{k(q-1)} = w^{l(q-1)}$ or $w^{k(q-1)} = w^{-l(q-1)}$. Therefore $k \in C(l)$ if and only if k is a solution of one of the following four systems of congruences:

$$\begin{array}{ll} k \equiv l \bmod q-1 & k \equiv l \bmod q-1 \\ k \equiv l \bmod q+1 & k \equiv -l \bmod q+1 \\ \\ k \equiv -l \bmod q-1 & k \equiv -l \bmod q-1 \\ k \equiv l \bmod q+1 & k \equiv -l \bmod q+1 \end{array}$$

If v is defined as in the proposition, a straightforward computation shows that the solutions k are the positive ones among the integers $l+tv$, $lq+tv$, $-lq+tv$, $-l+tv$ where t runs through the integers. Hence if $k \equiv l \bmod v$, then $k \in C(l)$. If J is the multiplicative semigroup of $\mathbf{Z}|(v)$, then $\eta(l \bmod v) = \sigma h_l$ defines an epimorphism $\eta : J \to \sigma V$. In order to simplify our notation, we will subsequently write a for $a \bmod v$ and $C(a)$ for the congruence class of a under Ker η. Then $C(l) = \{l, -l, lq, -lq\} = lC(1)$. But $C(1) = \{1, -1, q, -q\}$ is a subsemigroup of the units of $\mathbf{Z}|(v)$, hence $C(1)$ is a group. By Th. 9.43, $h_k \in W$ if and only if $(k, q^2-1) = 1$ which is equivalent to $(k, v) = 1$. Hence η maps the group E of units of $\mathbf{Z}|(v)$ onto σW, and the ideal kernel of $\eta : E \to \sigma W$ is $E \cap C(1) = C(1)$. Furthermore, by Th. 9.43, $h_k \in W_1$ if and only if $(k, p(q^2-1)) = 1$. Since $(p, q^2-1) = 1$, every element of E contains some positive integer k with $(k, p(q^2-1)) = 1$, thus $\sigma W_1 = \sigma W$. If $|C(1)| < 4$, then $a \equiv 1 \bmod v$ where $a = -1$, or q, or $-q$. An easy calculation shows that this is the case if and only if $q \leqslant 3$, and that $q \leqslant 3$ implies $|C(1)| = 2$.

10. Permutation spectra of polynomials

10.1. Let A be any algebra of a variety $\mathfrak{V}$, $X = \{x_1, \ldots, x_k\}$ a set of indeterminates, and $\mathfrak{C}$ a subset of the congruence lattice $\mathfrak{L}(A)$ of A. For any $\Theta \in \mathfrak{L}(A)$, $\eta(\Theta) : A \to A|\Theta$ shall denote the canonical epimorphism, $\eta(\Theta)(X) : A(X, \mathfrak{V}) \to (A|\Theta)(X, \mathfrak{V})$ shall denote the extension of $\eta(\Theta)$ to a composition epimorphism and $C_k(\Theta) : C_k(A) \to C_k(A|\Theta)$ the corresponding epimorphism.

For any $\mathfrak{f} \in C_k(A)$, we define the $\mathfrak{C}$-permutation spectrum of $\mathfrak{f}$ by

$$\text{Spec}(\mathfrak{C}, \mathfrak{f}) = \{\Theta \in \mathfrak{C} | \ C_k(\Theta)\mathfrak{f} \text{ is a permutation polynomial vector of } A|\Theta\}.$$

Similarly we define the $\mathfrak{C}$-permutation spectrum and strict $\mathfrak{C}$-permutation spectrum of $f \in A(X, \mathfrak{V})$ by

$$\text{(Strict) Spec}(\mathfrak{C}, f) = \{\Theta \in \mathfrak{C} | \ \eta(\Theta)(X)f \text{ is a (strict) permutation polynomial of } A|\Theta\}.$$

If A is an Ω-multioperator group, then by ch. 6, § 3, there is a bijection from $\mathfrak{L}(A)$ to the ideal lattice $\mathfrak{R}(A)$ of A, thus we can interpret $\mathfrak{C}$ also as a subset of $\mathfrak{R}(A)$ and Θ as an ideal of A in our definitions.

Permutation spectra have so far been studied just in the case $n = 1$ for certain Dedekind domains. This section is to work out the most important of these results.

10.2. Let $\mathfrak{V}$ be the variety of commutative rings with identity, then every algebra R of $\mathfrak{V}$ is a multioperator group, thus we will use the interpretation of spectra in terms of ideals of R. As in ch. 3, the composition of polynomial vectors will be denoted by $\circ$, and if $f \in R[x_1, \ldots, x_k]$, and $\mathfrak{g} = (g_1, \ldots, g_k)$ is a polynomial vector, we will write $f(g_1, \ldots, g_k) = f \circ \mathfrak{g}$ as in ch. 3, § 2.

10.21. Proposition. *Let R be a commutative ring with identity and $\mathfrak{C}$ the set of all ideals D of R such that $R|D$ is finite. If $f \in R[x_1, \ldots, x_k]$ and $\mathfrak{f}, \mathfrak{g} \in C_k(R)$, and if we set Spec $(\mathfrak{C}, \ ) =$ Spec, then:*

a) *Strict Spec $f \subseteq$ Spec f,*

b) *Spec $(\mathfrak{f} \circ \mathfrak{g}) =$ Spec $\mathfrak{f} \cap$ Spec $\mathfrak{g}$,*
Spec $(f \circ \mathfrak{g}) \supseteq$ Spec $f \cap$ Spec $\mathfrak{g}$,
Strict Spec $(f \circ \mathfrak{g}) \supseteq$ Strict Spec $f \cap$ Spec $\mathfrak{g}$.

c) *If* $D \in$ *Spec* $\mathfrak{f}$ (*Spec* f, *Strict Spec* f) *and* $C \supseteq D$, *then* $C \in$ *Spec* $\mathfrak{f}$ (*Spec* f, *Strict Spec* f).

Proof. a) follows from ch. 3, Prop. 12.23.

b) $D \in \text{Spec } \mathfrak{f} \cap \text{Spec } \mathfrak{g}$ if and only if $R|D$ is finite and $C_k(\eta(D))\mathfrak{f}$, $C_k(\eta(D))\mathfrak{g}$ are permutation polynomial vectors of $R|D$ which is true if and only if $R|D$ is finite and $C_k(\eta(D))\,(\mathfrak{f} \circ \mathfrak{g})$ is a permutation polynomial vector of $R|D$ which is equivalent to $D \in \text{Spec } (\mathfrak{f} \circ \mathfrak{g})$. If $D \in \text{Spec } f \cap \text{Spec } \mathfrak{g}$, then $R|D$ is finite, $\eta(D)\,(X)f$ is a permutation polynomial, and $C_k(\eta(D))\mathfrak{g}$ is a permutation polynomial vector of $R|D$. Therefore there are functions $f_2, \ldots, f_k \in F_k(R|D)$ such that $\varphi(\sigma\eta(D)\,(X)f, f_2, \ldots, f_k) = \pi$ is a permutation of $(R|D)^k$ and $\varphi\mathcal{F}(\sigma)C_k(\eta(D))\mathfrak{g} = \varrho$ is also a permutation of $(R|D)^k$. Hence $\pi\varrho = \varphi(\sigma\eta(D)\,(X)\,(f \circ \mathfrak{g}), h_2, \ldots, h_k)$, for some $h_i \in F_k(R|D)$, is a permutation of $(R|D)^k$, thus $\eta(D)\,(X)\,(f \circ \mathfrak{g})$ is a permutation polynomial of $R|D$. Similarly we can prove the third assertion of b).

c) If $D \in \text{Spec } \mathfrak{f}$, then $R|D$ is finite, and $\mathfrak{f}$ is a permutation polynomial vector mod D. Then $R|C$ is finite, thus by Prop. 4.2, $\mathfrak{f}$ is a permutation polynomial vector mod C whence $C \in \text{Spec } \mathfrak{f}$. The proof of the other two assertions runs along the same lines.

10.22. Lemma. *Let* R *be a Dedekind domain and Spec be defined as in Prop.* 10.21. *Then:*

a) *If* $E = CD$ *where* C, D *are comaximal ideals in* R, *then* $E \in$ *Spec* $\mathfrak{f}$ (*Spec* f, *Strict Spec* f) *if and only if* C, $D \in$ *Spec* $\mathfrak{f}$ (*Spec* f, *Strict Spec* f).

b) *If* P *is a prime ideal and* $Q = P^e$, $e > 1$, *then* $Q \in$ *Spec* $\mathfrak{f}$ (*Strict Spec* f) *if and only if* $P^2 \in$ *Spec* $\mathfrak{f}$ (*Strict Spec* f).

Proof. a) $E \in \text{Spec } \mathfrak{f}$ if and only if $R|E$ is finite and $\mathfrak{f}$ is a permutation polynomial vector mod E. By the Chinese remainder theorem and Prop. 4.21, this is true if and only if $R|C$ and $R|D$ are finite and $\mathfrak{f}$ is a permutation polynomial vector mod C and mod D, i.e. C, $D \in \text{Spec } \mathfrak{f}$. Similar arguments work for Spec f and Strict Spec f.

b) $Q \in \text{Spec } \mathfrak{f}$ if and only if $R|Q$ is finite and $\mathfrak{f}$ is a permutation polynomial vector mod Q. By ch. 6, Lemma 4.52, and Cor. 4.35, this is true if and only if $R|P^2$ is finite and $\mathfrak{f}$ is a permutation polynomial vector mod P^2, i.e. $P^2 \in \text{Spec } \mathfrak{f}$. The argument for Strict Spec is similar.

10.23. Theorem. *Let* R *be any Dedekind domain,* $\mathfrak{P} = \mathfrak{P}(\mathfrak{f})$ *the set of all prime ideals of Spec* $\mathfrak{f}$ *and* $\mathfrak{Q} = \mathfrak{Q}(\mathfrak{f})$ *the set of all prime ideals* $Q \in \mathfrak{P}(\mathfrak{f})$ *with* $Q^2 \in$ *Spec* $\mathfrak{f}$. *Then Spec* $\mathfrak{f}$ *is the set of all ideals* D *of the form*

$$D = P_1 P_2 \ldots P_r Q_1^{e_1} \ldots Q_s^{e_s}$$

where $r+s > 0$, $P_1, \ldots, P_r, Q_1, \ldots, Q_s$ *are pairwise distinct prime ideals, such that* $P_i \in \mathfrak{P}(\mathfrak{f}) - \mathfrak{Q}(\mathfrak{f})$, $i = 1, \ldots, r$, *and* $Q_j \in \mathfrak{Q}(\mathfrak{f})$, $j = 1, \ldots, s$, $e_j \geqslant 1$. *This assertion remains valid if* $\mathfrak{f}$ *is replaced by* f *and Spec by Strict Spec.*

Proof. This is an immediate consequence of Prop. 10.21 c) and Lemma 10.22.

10.24. Lemma. *Let* $P \neq (0)$, R *be any ideal of* $\mathfrak{P}(\mathfrak{f})$, $\mathfrak{P}(f)$ *resp. Then* $P \in \mathfrak{Q}(\mathfrak{f})$ *if and only if* $\partial\mathfrak{f}(u_1, \ldots, u_k) \not\equiv 0 \bmod P$, *for every* $(u_1, \ldots, u_k) \in R^k$, $P \in \mathfrak{Q}(f)$ *if and only if there is no* $(u_1, \ldots, u_k) \in R^k$ *such that* $\partial_i f(u_1, \ldots, u_k) \equiv 0 \bmod P$, $i = 1, \ldots, k$, *resp.*

Proof. This is nothing other than Prop. 4.31 and Prop. 4.34.

10.25. Th. 10.23 shows that Spec $\mathfrak{f}$ and Strict Spec f are completely determined by the pair $(\mathfrak{P}, \mathfrak{Q})$ of sets of prime ideals. We will call $(\mathfrak{P}, \mathfrak{Q})$ the basis pair of Spec $\mathfrak{f}$, Strict Spec f, resp. The following two questions arise:

a) How can one find the basis pair for a given polynomial vector $\mathfrak{f}$ or a polynomial f?

b) What pairs $(\mathfrak{P}, \mathfrak{Q})$ of prime ideal sets can be basis pairs for suitable polynomial vectors or polynomials?

We do not intend to attack this problems in general, but will give some results for the case where $k = 1$ and R is the Dedekind domain of rational integers. The reader may work out how far these results carry over to the domains of integers in algebraic number fields of finite degree.

10.3. Let R be the domain of rational integers and $R[x]$ the polynomial ring over R in one indeterminate x. The three notions of $\mathfrak{C}$-permutation spectra clearly coincide. Thus only Spec $(\mathfrak{C}, f)$, for $f \in R[x]$, has to be considered. Since R is a principal ideal domain, every ideal D in R can be written as $D = (d)$ where $d \geqslant 0$ is a unique integer. Thus we can describe Spec $(\mathfrak{C}, f)$ as a set of non-negative integers. $\mathfrak{C}$ will again denote the set of all ideals D of R such that $R|D$ is finite, and Spec $f =$ Spec $(\mathfrak{C}, f)$.

Rewriting the results of 10.2 we obtain:

$$\text{Spec}\,(f\circ g) = \text{Spec}\,f \cap \text{Spec}\,g. \tag{10.3}$$

If $d \in \text{Spec}\,f$ and c/d, then $c \in \text{Spec}\,f$, and Spec f is uniquely determined by its basis pair which consists of the set $\mathfrak{P} = \mathfrak{P}(f)$ of all primes of Spec f and the set $\mathfrak{Q} = \mathfrak{Q}(f)$ of all primes $q \in \mathfrak{P}(f)$ with $q^2 \in \text{Spec}\,f$. Moreover a prime $p \in \mathfrak{P}(f)$ is in $\mathfrak{Q}(f)$ if and only if $f'(u) \not\equiv 0 \bmod p$, for every $u \in R$, i.e. if $\eta(p)\,(x)f$ is regular.

10.31. Remark. If $\mathfrak{B}$ is the set of all ideals of R, then $\mathfrak{B} = \mathfrak{C} \cup \{(0)\}$. By § 5.33, the permutation polynomials of $R|(0) = R$ are just $ex+c$, $e = \pm 1$, thus we know Spec $(\mathfrak{B}, f)$ as soon as we know f and Spec f.

10.4. Theorem. *Let $S = \langle R[x];\ \circ \rangle$ be the semigroup consisting of the polynomials over R with the polynomial composition $\circ$ as operation, H the subsemigroup of S which is generated by the linear polynomials $ax+b$, the powers x^n with odd $n > 1$, and the Dickson polynomials $g_n(a, x)$, $a \neq 0$, $(n, 6) = 1$, $n > 1$, and L the subsemigroup of H which is generated by the polynomials $ax+b$ and $g_n(a, x)$ of H. Then $\mathfrak{P}(f)$ is infinite for every $f \in H$. If $f \in H$, then $\mathfrak{Q}(f)$ is infinite if and only if $f \in L$.*

Proof. Let $f \in H$, then f is of the form

$$f = f_1 \circ f_2 \circ \ \dots\ \circ f_t \tag{10.41}$$

where each f_i equals either some $ax+b$, or some x^n, or some $g_n(a, x)$ which satisfies the conditions of the theorem. Hence (10.3) implies

$$\mathfrak{P}(f) = \mathfrak{P}(f_1) \cap \mathfrak{P}(f_2) \cap \ \dots\ \cap \mathfrak{P}(f_t), \tag{10.42}$$

$$\mathfrak{Q}(f) = \mathfrak{Q}(f_1) \cap \mathfrak{Q}(f_2) \cap \ \dots\ \cap \mathfrak{Q}(f_t). \tag{10.43}$$

Since $R|(p)$ is a finite field for every prime p, we can apply our results of §§ 9.3 and § 9.4. Prop. 9.3 implies $\mathfrak{P}(ax+b) = \{p|\ p \in \mathfrak{P},\ a \not\equiv 0 \bmod p\}$ where $\mathfrak{P}$ denotes the set of all primes, hence $\mathfrak{P}(ax+b)$ consists of almost all primes. Prop. 9.32 implies that $\mathfrak{P}(x^n) = \{p|\ p \in \mathfrak{P}$ and $(p-1, n) = 1\}$. If $n = r_1^{e_1} \dots r_s^{e_s}$ is the prime factor decomposition of n, then $\mathfrak{P}(x^n)$ is the set of all primes p such that $p \not\equiv 1 \bmod r_i$, $i = 1, \dots, s$. Th. 9.43 and Prop. 9.32 imply that $\mathfrak{P}(g_n(a, x)) = U \cup V$ where $U = \{p|\ p \in \mathfrak{P},\ a \not\equiv 0 \bmod p,\ (p^2-1, n) = 1\}$ and $V = \{p|\ p \in \mathfrak{P},\ a \equiv 0 \bmod p,\ (p-1, n) = 1\}$. If $n = r_1^{e_1} \dots r_s^{e_s}$ is the prime factor decomposition of n, then

U is the set of all primes p such that $p \not\equiv \pm 1 \bmod r_i$, $i = 1, \dots, s$, and $a \not\equiv 0 \bmod p$ while V is the set of all primes p such that $p \not\equiv 1 \bmod r_i$, $i = 1, \dots, s$, and $a \equiv 0 \bmod p$.

Suppose now that $f \in H$, and $[f] = m = u_1^{e_1} \dots u_s^{e_s} v_1^{d_1} \dots v_t^{d_t}$ is the prime factor decomposition of $[f]$ where $u_1, \dots, u_s$ are those primes which occur in the degrees of the factors x^n in (10.41) but not in the degrees of the factors $g_n(a, x)$ while $v_1, \dots, v_t$ are the remaining primes. Let $\overline{\mathfrak{P}}(f)$ be the set of all primes which belong to those residue classes $C(b) \bmod u_1 \dots u_s v_1 \dots v_t$ for which $b \not\equiv 1 \bmod u_i$, $i = 1, \dots, s$, $b \not\equiv \pm 1 \bmod v_i$, $i = 1, \dots, t$. Then $\mathfrak{P}(f)$ is obtained from $\overline{\mathfrak{P}}(f)$ by adding and removing a finite number of primes. Indeed, any prime of these residue classes belongs to $\mathfrak{P}(x^n)$, for every x^n in (10.41), and to $\mathfrak{P}(g_n(a, x))$, for every $g_n(a, x)$ in (10.41) whence, by (10.42), all of these primes which are not divisors of a, for some $ax+b$ of (10.41), belong to $\mathfrak{P}(f)$. Conversely by (10.42), all primes of $\mathfrak{P}(f)$ except finitely many are contained in $\overline{\mathfrak{P}}(f)$. Hence $\mathfrak{P}(f)$ and $\overline{\mathfrak{P}}(f)$ differ by only finitely many primes. By hypothesis, $u_i \neq 2$, $i = 1, \dots, s$, $v_j \neq 2, 3$, $j = 1, \dots, t$. Hence by the Chinese remainder theorem, there are exactly $(u_1-1) \dots (u_s-1)(v_1-2) \dots (v_t-2)$ residue classes $C(b) \bmod u_1 \dots u_s v_1 \dots v_t$ for which $b \not\equiv 1 \bmod u_i$, $i = 1, \dots, s$, $b \not\equiv \pm 1 \bmod v_i$, $i = 1, \dots, t$, and $(u_1-2) \dots (u_s-2) \cdot (v_1-3) \dots (v_t-3)$ residue classes are prime residue classes. By Dirichlet's theorem, each of these classes contains infinitely many primes (but the other residue classes contain only primes of the set $\{u_1, \dots, u_s, v_1, \dots, v_t\}$). Hence $\mathfrak{P}(f)$ is infinite.

We have $\mathfrak{Q}(ax+b) = \mathfrak{P}(ax+b)$, $\mathfrak{Q}(x^n) = \phi$ and $\mathfrak{Q}(g_n(a, x)) = \{p|\ p \in \mathfrak{P},\ a \not\equiv 0 \bmod p,\ (p(p^2-1), n) = 1\}$ by Prop. 9.3, Prop. 9.32, and Th. 9.43. Thus if $n = r_1^{e_1} \dots r_s^{e_s}$ is the prime factor decomposition of n, then $\mathfrak{Q}(g_n(a, x)) = \{p \in \mathfrak{P}(g_n(a, x))|\ a \not\equiv 0 \bmod p,\ p \neq r_i,\ i = 1, \dots, s\}$. By (10.43), if $f \in H \setminus L$, then $\mathfrak{Q}(f) = \phi$. If, however, $f \in L$ then by (10.43) we see that $\mathfrak{P}(f)$ and $\mathfrak{Q}(f)$ differ by only finitely many primes, hence $\mathfrak{Q}(f)$ is infinite.

10.5. The question now arises whether there are any other polynomials $f \in R[x]$ apart from those in H for which $\mathfrak{P}(f)$ is infinite. It was SCHUR who stated the conjecture that this was not the case, and he himself could prove, that this was true for polynomials f of certain degrees, e.g. polynomials of prime degree. Recently M. FRIED gave a general proof of SCHUR's conjecture which leans heavily on rather intricate tools and deep

results in the theory of complex functions and is therefore beyond the scope of this book. We will state FRIED's result and two consequences of it which will follow immediately from Th. 10.4 and its proof.

10.51. Theorem. *$\mathfrak{P}(f)$ is infinite if and only if $f \in H$, and $\mathfrak{Q}(f)$ is infinite if and only if $f \in L$.*

10.52. Corollary. *Every infinite $\mathfrak{P}(f)$ can be obtained by adding to and removing from some set T of primes finitely many primes. Such a set T of primes consists of the primes of all prime residue classes $C(b)$ mod l where $l = u_1 \dots u_s v_1 \dots v_t$, with u_i, v_j pairwise distinct primes, $u_i \neq 2$, $v_j \neq 2, 3$, $b \not\equiv 1$ mod u_i, $i = 1, \dots, s$, and $b \not\equiv \pm 1$ mod v_i, $i = 1, \dots, t$.*

10.53. Corollary. *If $\mathfrak{P}(f)$ is infinite, then $\mathfrak{Q}(f)$ is either empty or differs from $\mathfrak{P}(f)$ by only finitely many primes.*

10.6. Theorem. *Let $\mathfrak{Q} = \{q_1, \dots, q_s\}$, $\mathfrak{R} = \{p_1, \dots, p_r\}$ be finite disjoint sets of primes (possibly empty). Then there exist monic polynomials $f \in R[x]$ of arbitrarily large degrees such that $\mathfrak{P}(f) = \mathfrak{Q} \cup \mathfrak{R}$ and $\mathfrak{Q}(f) = \mathfrak{Q}$.*

Proof. If $\mathfrak{Q} \cup \mathfrak{R}$ is empty, then $f = x^{2n} - x^{2n-2}$, $n \geqslant 2$, has the required property. Suppose $\mathfrak{Q} \cup \mathfrak{R}$ is not empty. Set $q = q_1 \dots q_s$ if $\mathfrak{Q}$ is not empty, $q = 1$ otherwise, and $p = p_1 \dots p_r$ if $\mathfrak{R}$ is not empty, $p = 1$ otherwise. Throughout the proof the sum over an empty set will be 0 while the product over an empty set will be 1. We choose positive integers u, v such that $u > v$ and $x^u - x^v \in \{pq\}$ which is possible because of the finiteness of $R[x]|\{pq\}$. Furthermore we choose $k \geqslant 2$ integral such that $w = kupq + 1$ is a prime—by Dirichlet's theorem, there are infinitely many such k. Let

$$g = x^{kupq+1} - x^{kvpq+1}. \tag{10.6}$$

Then $g \in \{pq\}$ and $g' \in \{pq\}$. Furthermore let

$$h = g + \sum_{m=1}^{r} (pq/p_m)\, x^{p_m} + \sum_{n=1}^{s} (pq/q_n)x,$$

which is a monic polynomial of degree w. It follows easily that $h \equiv (pq/q_i)\, x \bmod \{q_i\}$ and $h' \equiv (pq/q_i) \bmod \{q_i\}$. Thus h is a permutation polynomial mod q_i and moreover $q_i \in \mathfrak{Q}(h)$, $i = 1, \dots, s$. Similarly,

$h \equiv (pq/p_i)\, x \bmod \{p_i\}$ and $h' \equiv 0 \bmod \{p_i\}$, hence $p_i \in \mathfrak{P}(h)$, but $p_i \notin \mathfrak{Q}(h)$, $i = 1, \dots, r$.

Suppose $\mathfrak{P}(h)$ is infinite. Then by Th. 10.51 (we need just the weaker result of SCHUR) $h \in H$. Since $[h] = w$ is a prime, h is of the form $a(a_1x + b_1)^w + b$ or of the form $ag_w(c, a_1x + b_1) + b$. If $b_1 \neq 0$, then such a polynomial contains a non-zero term dx^{w-1}, and if $b_1 = 0$, then such a polynomial contains, apart from the leading term, only a constant term or it contains a non-zero term dx^{w-2}. But $(kupq+1) - (kvpq+1) = kpq(u-v) \geqslant 4$, and $kvpq + 1 > \max(p_1, p_2, \dots, p_r, 1)$, hence h is certainly not a polynomial of this form, contradiction. Therefore $\mathfrak{P}(h)$ is finite, thus $\mathfrak{P}(h) = \mathfrak{Q} \cup \mathfrak{R} \cup \mathfrak{T}$ where $\mathfrak{T} = \{b_1, \dots, b_t\}$ is a finite set of primes disjoint from $\mathfrak{Q} \cup \mathfrak{R}$ such that $\mathfrak{Q} \subseteq \mathfrak{Q}(h) \subseteq \mathfrak{Q} \cup \mathfrak{T}$. Set $b = b_1 b_2 \dots b_t$ and choose a positive integer z such that $z \equiv 1 \bmod pq$, $z \equiv 0 \bmod b$, and positive integers l, m such that $l > m$ and $x^l - x^m \in \{pqb\}$. If $e = x^{lpq} - x^{mpq} + zx$, then $\mathfrak{Q} \cup \mathfrak{R} \subseteq \mathfrak{Q}(e)$, but $\mathfrak{T} \cap \mathfrak{P}(e) = \phi$. By (10.42) and (10.43), if $d = h \circ e$, then $\mathfrak{P}(d) = \mathfrak{Q} \cup \mathfrak{R}$, $\mathfrak{Q}(d) = \mathfrak{Q}$. Let $k = \prod_{i=1}^{r} (p_i^2 - 1) \prod_{j=1}^{s} q_j(q_j^2 - 1)$ and $h_n = g_n(1, x)$. If $(n, k) = 1$, then $\mathfrak{P}(h_n) \supseteq \mathfrak{Q} \cup \mathfrak{R}$ and $\mathfrak{Q}(h_n) \supseteq \mathfrak{Q}$, by the proof of Th. 10.4, whence by (10.42) and (10.43), if $f = d \circ h_n$, then $\mathfrak{P}(f) = \mathfrak{Q} \cup \mathfrak{R}$ and $\mathfrak{Q}(f) = \mathfrak{Q}$. Clearly f is monic and there are infinitely many n with $(n, k) = 1$. This proves Th. 10.6.

Remarks and comments

§§ 1, 2. If R is a commutative ring with identity and $\circ$ means the composition of polynomials, then the set $R[x]$ of all elements of the polynomial ring $\langle R[x]; +, \cdot \rangle$ can also be viewed as an algebra $\langle R[x]; \circ \rangle$, i.e. as a semigroup, as an algebra $\langle R[x]; +, \circ \rangle$, i.e. as a near-ring, as an algebra $\langle R[x]; \cdot, \circ \rangle$, and as an algebra $\langle R[x]; +, \cdot, \circ \rangle$, i.e. as a composition ring. In this book we treat just the first and the last case. To the best of our knowledge the third case has never been looked at, but there are a few papers which consider the near-ring $\langle R[x]; +, \circ \rangle$—mainly for R being a field—or certain subnear-rings of it (ORE [1], [2], CARCANAGUE [1], [2], RIHA [1], CLAY and DOI [1]).

The semigroup $\langle R[x]; \circ \rangle$ has been studied mainly for R being a field, and apart from the topics of our §§ 1–3, also the automorphism group of this semigroup has been examined (FADELL and MAGILL [1], ŠAIN [2]).

Most of the results and problems referring to $\langle R[x]; \circ \rangle$ also make sense for the superassociative system $\langle R[x_1, \ldots, x_k]; \varkappa \rangle$, $\varkappa$ being the composition of polynomials, or for the semigroup $\mathcal{T}(\langle R[x_1, \ldots, x_k]; \varkappa \rangle)$, but for $k > 1$, almost nothing has been done in this direction save GOODSTEIN [1], [2] on generating systems of $\langle R[x_1, \ldots, x_k]; \varkappa \rangle$.

Th. 1.34 and Th. 2.46 have been essentially proved by RITT [1], for the case that K is the field of complex numbers, by means of rather deep methods of the theory of complex functions. The purely algebraic proofs of these theorems for arbitrary fields of characteristic zero which are contained in our book are due to ENGSTRÖM [1] (Th. 1.34) and H. LEVI [1] (Th. 2.46). FRIED and MACRAE [1] have given a different algebraic proof of Th. 1.34. This proof admits also a generalization of the main statements of Th. 1.34 to fields of characteristic $p > 0$ as long as the degree $[f]$ of the polynomial f is less than p. Apart from this result nothing is known so far about the decomposition into indecomposable polynomials over fields of characteristic $p > 0$, nor over integral domains other than fields.

§ 3. A systematic study of permutable elements in the semigroup $\langle K[x]; \circ \rangle$ where K is a field of characteristic 0 is due to JACOBSTHAL [1] who gave a proof of our Th. 3.33 for this case. For arbitrary fields, KAUTSCHITSCH [1] could prove this theorem. He also found a similar result for the semigroup of all formal power series in one indeterminate without a constant term over a field with respect to the composition. Th. 3.53 in its general form is due to NIEDERREITER. AF HÄLLSTRÖM [1] introduced the semipermutability of elements in $\langle K[x]; \circ \rangle$ which is an interesting generalization of permutability.

§ 4. For the case of polynomials in one indeterminate over the ring of rational integers, this section is due to NÖBAUER [1] (see also NÖBAUER [2], CAVIOR [2], ZANE [1], KELLER and OLSON [1], for general Dedekind domains we refer to SCHÖNIGER [1]). Polynomial vectors in several indeterminates were investigated by NÖBAUER [4] for the ring of rational integers, for arbitrary Dedekind domains by AIGNER [1].

NÖBAUER [22] also introduced and investigated permutation polynomials and strict permutation polynomials in more than one indeterminate over rings, this paper contains the conditions of § 4. Moreover, there is a proof in this paper that, in the ring of rational integers and for arbitrary

$a \neq 0$, every permutation polynomial mod (a) is a strict permutation polynomial mod (a), this proof is, however, wrong. So it remains an open problem, even for most of the factor rings of the rational integers, whether or not every permutation polynomial is a strict permutation polynomial. A very interesting characterization of permutation polynomial vectors over the field K of real numbers is due to BIAŁYNICKI-BIRULA and ROSENLICHT [1] who used topological methods: A k-dimensional polynomial vector $\mathfrak{f}$ over the real numbers is a permutation polynomial vector if and only if the mapping $\varphi\mathfrak{f} : K^k \to K^k$ induced by $\mathfrak{f}$ is injective. P. CHOWLA [1] studied an interesting class of polynomials related to permutation polynomials.

§ 5. Comparing Th. 5.21 with Ch. 5, Th. 3.3, one may expect that Th. 5.21 is open to a considerable generalization. This, however, has not been done yet.

The semigroups $V_k(R|M)$ and even more $U_k(R|M)$ have been examined by NÖBAUER for the case where R is the ring of rational integers, first for $k = 1$ (see NÖBAUER [1], [2], [5]), then also for $k > 1$ (see NÖBAUER [4], [9]). If R is an arbitrary Dedekind domain, then results were obtained by LAUSCH [1] for $k = 1$, and AIGNER [1] for arbitrary k. Our presentation follows AIGNER's paper. Recently the unit group $\mathcal{E}(\mathbf{Z}|(n)[x])$ of the semigroup $\mathbf{Z}|(n)[x]$ with respect to the composition was discussed by SUVAK [1] ($\mathbf{Z}$ denotes the ring of rational integers).

§§ 6, 7. For R being the ring $\mathbf{Z}$ of rational integers and $k = 1$, ideal power semigroups were originally investigated by NÖBAUER [7], [9]. The structure of special cases of the groups $J_k(P^e, P^f)$ was discussed by FERSCHL and NÖBAUER [1], FEICHTINGER [1] for $R = \mathbf{Z}$ and $k = 1$, and DIRNBERGER [1] for $R = \mathbf{Z}$ and $k > 1$. For more general classes of rings, we refer to LAUSCH [2], SCHITTENHELM [1], and AIGNER [1]. Our presentation follows partly AIGNER's paper and sometimes makes use of the papers of LAUSCH and DIRNBERGER.

§ 8. As announced in the remarks and comments to Ch. 3, § 12, we now give some references for the extensive literature about permutation polynomials in one indeterminate over finite fields. For a survey of the work on this subject prior to 1920 we refer to DICKSON [4]. During this period it was DICKSON himself who contributed substantially to this subject (see DICKSON [1], [2], [3]). Recently, mainly CARLITZ and his school, but also several other authors, have taken up this subject again and widened

our knowledge through some interesting contributions (CARLITZ [1], [3], [4], [5], [6], [7], CAVIOR [1], S. CHOWLA [1], S. CHOWLA and H. ZASSENHAUS [1], LAWKINS [1], LONDON and ZIEGLER [1], RÉDEI [1]). There is also some recent work on permutation polynomials over finite fields in several indeterminates (KURBATOV and STARKOV [1], LIDL [1], [2], LIDL and NIEDERREITER [1], NIEDERREITER [1], [2], [3]).

Our proof of Th. 8.21 is due to GWEHENBERGER [1], Th. 8.31 is a result of MAC CLUER [1] (for the case that K is a finite field there is a much simpler proof of this theorem by WILLIAMS [1]). Th. 8.81 was proved by HAYES [1] (for a similar result see DAVENPORT and LEWIS [1]), and the results of § 8.8 are also due to HAYES [1]. CARLITZ and WELLS have proved Th. 8.92.

§ 9. Papers on groups of polynomial permutations over finite fields, mainly for one indeterminate, are numerous and deal with generating sets of such groups (CARLITZ [1], [6], WELLS [2]), with the distribution of the minimal possible degrees of the polynomials representing the permutations of these groups (WELLS [3]) and various other questions (AHMAD [1], CARLITZ and HAYES [1], FRYER [1], [2]).

Th. 9.23 is due to WELLS [1], but our proof stems from GWEHENBERGER [1]. Related results can be found in AHMAD [2] and FILLMORE [1]. The generalization of the groups σP of Prop. 9.32 from finite fields to finite residue class rings of the integers can be found in NÖBAUER [3]. DICKSON [1], [2] introduced the permutation polynomials that now bear his name, in these papers our Th. 9.43 has essentially been proved. Prop. 9.52 is due to NÖBAUER [27]. The generalization of the group σW of this proposition from finite fields to finite residue class rings of the integers was recently discussed by LAUSCH, MÜLLER and NÖBAUER [1]. Dickson polynomials were generalized to the case of several indeterminates recently by LIDL and WELLS [1].

§ 10. The theory of spectra in this section was started by NÖBAUER [24], [25] for the case of one indeterminate and the rational integers. We follow closely these papers. For contributions to SCHUR's conjecture prior to FRIED's solution of this problem, see SCHUR [1], WEGNER [1], KURBATOV [1], [2]. Spectra in more than one indeterminate and spectra over varieties other than the variety of commutative rings with identity have so far not been investigated.

CHAPTER 5

COMPOSITION OF POLYNOMIALS AND POLYNOMIAL FUNCTIONS OVER GROUPS

1. The concept of length

1.1. Let $\mathfrak{V}$ be the variety of groups as defined in ch. 1, § 2.4, Ω the set of its operations, G any group, and $X = \{x_1, \ldots, x_k\}$ a set of indeterminates. As in ch. 1, § 9.2, we set $G(X, \mathfrak{V}) = G[X]$ and also $F(X, \mathfrak{V}) = F(X)$ which denotes the free group with free generating set X. From specializing the general definition of σ in ch. 1, Prop. 6.41, we obtain the canonical epimorphism $\sigma_k(G) : G[X] \to P_k(G)$ which describes the connection between polynomials and polynomial functions over G. Let $\varepsilon : G \to F(X)$ be the homomorphism that maps every $g \in G$ onto the identity e of $F(X)$ and $\iota : F(X) \to F(X)$ the identity automorphism of $F(X)$. By ch. 1, Th. 4.31, there is a unique homomorphism $\lambda : G[X] \to F(X)$ such that $\varepsilon = \lambda\varphi_1$, $\iota = \lambda\varphi_2$ which means – if we observe the definitions of φ_1, φ_2 — that $\lambda g = e$, for every $g \in G$, and $\lambda x_i = x_i$, $i = 1, \ldots, k$. Clearly λ is an epimorphism. We set $\lambda = \lambda_k(G)$ which we call the length epimorphism (of $G[X]$). The normal subgroup $\lambda_k(G) \ker \sigma_k(G)$ of $F(X)$ is called the length of $G[X]$ and will be denoted by $L_k(G)$.

1.11. Lemma. *$H \cong G$ implies $L_k(H) = L_k(G)$.*

Proof. Let $\vartheta : H \to G$ be any isomorphism and $\vartheta[X] : H[X] \to G[X]$ its extension to an isomorphism according to ch. 1, Prop. 4.5. Then $\lambda_k(H) = \lambda_k(G)\,\vartheta[X]$ whence $L_k(H) = \lambda_k(G)\,\vartheta[X] \ker \sigma_k(H)$. But by diagram fig. 3.1 of ch. 3, $\vartheta[X] \ker \sigma_k(H) = \ker \sigma_k(G)$ which proves the lemma.

1.12. Proposition. *$L_k(G)$ is a verbal subgroup of $F(X)$.*

Proof. By ch. 6, § 6.72, it is sufficient to show that $w(x_1, \ldots, x_k) \in L_k(G)$ implies $w(w_1(x_1, \ldots, x_k), \ldots, w_k(x_1, \ldots, x_k)) \in L_k(G)$, for any k elements $w_i(x_1, \ldots, x_k) \in F(X)$, $i = 1, \ldots, k$. Let $f(x_1, \ldots, x_k) \in \ker \sigma_k(G)$ such that $\lambda_k(G) f(x_1, \ldots, x_k) = w(x_1, \ldots, x_k)$. By definition of $\ker \sigma_k(G)$, we

have $f(w_1(g_1, \ldots, g_k), \ldots, w_k(g_1, \ldots, g_k)) = 1$, for all $g_1, \ldots, g_k \in G$ whence $f(w_1(x_1, \ldots, x_k), \ldots, w_k(x_1, \ldots, x_k)) \in \ker \sigma_k(G)$. Therefore $\lambda_k(G) f(w_1(x_1, \ldots, x_k), \ldots, w_k(x_1, \ldots, x_k)) = w(w_1(x_1, \ldots, x_k), \ldots, w_k(x_1, \ldots, x_k)) \in L_k(G)$.

1.13. Proposition. *$G[X]\,|\,ker\ \sigma_k(G)\ ker\ \lambda_k(G) \cong F(X)\,|\,L_k(G)$.*

Proof. $F(X)\,|\,L_k(G) \cong \lambda_k(G)\,G[X]\,|\,\lambda_k(G) \ker \sigma_k(G) \cong G[X]\,|\ker \sigma_k(G) \ker \lambda_k(G)$ by the second isomorphism theorem of group theory.

1.14. Proposition. *If N is a normal subgroup of G, then $L_k(G) \subseteq L_k(G\,|\,N)$.*

Proof. Let $\vartheta : G \to G\,|\,N$ be the canonical epimorphism and $\vartheta[X] : G[X] \to (G\,|\,N)[X]$ its extension to an epimorphism which fixes X elementwise (see ch. 1, Prop. 4.5). Then the diagram fig. 5.1 is commutative. Hence $L_k(G) = \lambda_k(G) \ker \sigma_k(G) = \lambda_k(G\,|\,N)\,\vartheta[X] \ker \sigma_k(G)$. But $\vartheta[X] \ker \sigma_k(G) \subseteq \ker \sigma_k(G\,|\,N)$, by ch. 3, diagram fig. 3.1 whence $L_k(G) \subseteq L_k(G\,|\,N)$.

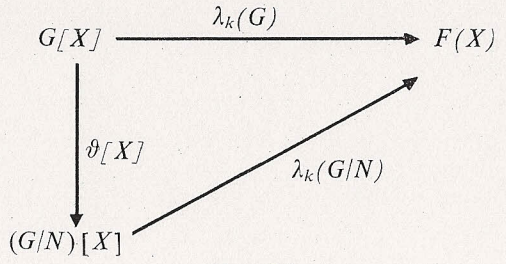


FIG. 5.1

1.2. Proposition. *Let G_1, G_2 be any two groups. Then $L_k(G_1 \times G_2) = L_k(G_1) \cap L_k(G_2)$.*

Proof. By Prop. 1.14 and Lemma 1.11, $L_k(G_1 \times G_2) \subseteq L_k(G_1) \cap L_k(G_2)$. Conversely let $w \in L_k(G_1) \cap L_k(G_2)$. Then there exist $f_i \in \ker \sigma_k(G_i)$, $i = 1, 2$, such that $\lambda_k(G_i) f_i = w$, $i = 1, 2$. Let $\varphi_2 : F(X) \to (G_1 \times G_2)[X]$ be the homomorphism which fixes X elementwise and $\iota_i : G_i \to G_1 \times G_2$, $i = 1, 2$, the inclusion monomorphisms (see ch. 6, § 6.4). Since ch. 1, Prop. 4.5 remains valid if we replace "epimorphism" by "homomorphism" and "onto" by "to" as one can easily see, ι_i can be extended to a homomorphism $\iota_i[X] : G_i[X] \to (G_1 \times G_2)[X]$ which fixes X elementwise. Let $f = (\iota_1[X] f_1)(\iota_2[X] f_2)(\varphi_2 w)^{-1} \in (G_1 \times G_2)[X]$. Then $\sigma_k(G_1 \times G_2) f$ maps every element of $G_1 \times G_2$ onto 1, thus $f \in \ker \sigma_k(G_1 \times G_2)$. Moreover $\lambda_k(G_1 \times G_2) f = w$. Hence $w \in \lambda_k(G_1 \times G_2) \ker \sigma_k(G_1 \times G_2) = L_k(G_1 \times G_2)$.

1.21. Proposition. *Let $G = G_1 \times G_2$. Then ker $\lambda_k(G)$ ker $\sigma_k(G)\,|\,$ker $\sigma_k(G) \cong$ ker $\lambda_k(G_1)$ ker $\sigma_k(G_1)\,|\,$ker $\sigma_k(G_1) \times$ ker $\lambda_k(G_2)$ ker $\sigma_k(G_2)\,|\,$ker $\sigma_k(G_2)$.*

Proof. Let ι_i be defined as in the proof of Prop. 1.2, $(f_1, f_2) \in \ker \lambda_k(G_1) \times \ker \lambda_k(G_2)$ and $\tau : \ker \lambda_k(G_1) \times \ker \lambda_k(G_2) \to \ker \lambda_k(G) \ker \sigma_k(G)\,|\ker \sigma_k(G)$ be the mapping defined by $\tau(f_1, f_2) = (\iota_1[X] f_1)(\iota_2[X] f_2) \ker \sigma_k(G)$. That τ has the required range follows from

$$\lambda_k(G)(\iota_1[X] f_1)(\iota_2[X] f_2) = (\lambda_k(G_1) f_1)(\lambda_k(G_2) f_2) = 1.$$

Moreover τ is a homomorphism since

$$\tau[(f_1, f_2)(g_1, g_2)] = (\iota_1[X] f_1)(\iota_1[X] g_1)(\iota_2[X] f_2)(\iota_2[X] g_2) \ker \sigma_k(G),$$
$$\tau(f_1, f_2)\,\tau(g_1, g_2) = (\iota_1[X] f_1)(\iota_2[X] f_2)(\iota_1[X] g_1)(\iota_2[X] g_2) \ker \sigma_k(G),$$

and, for arbitrary $(a, b) \in G$, we have

$$[\sigma_k(G)(\iota_1[X] g_1)(\iota_2[X] f_2)](a, b) = (g_1(a), 1)(1, f_2(b)) =$$
$$= [\sigma_k(G)(\iota_2[X] f_2)(\iota_1[X] g_1)](a, b).$$

τ is an epimorphism, for let $f \in \ker \lambda_k(G)$, $\pi_i : G \to G_i$, $i = 1, 2$, the projections and $\pi_i[X] : G[X] \to G_i[X]$, $i = 1, 2$, the extensions to composition epimorphisms. Then

$$\tau(\pi_1[X] f, \pi_2[X] f) = (\iota_1[X] \pi_1[X] f)(\iota_2[X] \pi_2[X] f) \ker \sigma_k(G) = f \ker \sigma_k(G)$$

since

$$[\sigma_k(G)(\iota_1[X] \pi_1[X] f)(\iota_2[X] \pi_2[X] f)](a, b) =$$
$$= ((\pi_1[X] f)(a), 1)(1, (\pi_2[X] f)(b)) = (\sigma_k(G) f)(a, b).$$

By definition of τ, we have $(f_1, f_2) \in \ker \tau$ if and only if $(\iota_1[X] f_1)(\iota_2[X] f_2) \in \ker \sigma_k(G)$ which is equivalent to $f_i \in \ker \sigma_k(G_i) \cap \ker \lambda_k(G_i)$. Hence ker $\lambda_k(G)$ ker $\sigma_k(G)\,|\,$ker $\sigma_k(G) \cong$ ker $\lambda_k(G_1) \times$ ker $\lambda_k(G_2)\,|\,$(ker $\sigma_k(G_1) \cap$ ker $\lambda_k(G_1)) \times$ (ker $\sigma_k(G_2) \cap$ ker $\lambda_k(G_2)) \cong$ [ker $\lambda_k(G_1)$ ker $\sigma_k(G_1)\,|\,$ker $\sigma_k(G_1)] \times$ [ker $\lambda_k(G_2)$ ker $\sigma_k(G_2)\,|\,$ker $\sigma_k(G_2)$] by the first isomorphism theorem of group theory.

1.22. Corollary. *If G_1, G_2 are finite groups and $G = G_1 \times G_2$, then the decomposition homomorphism τ of $P_k(G)$ is an isomorphism if and only if $L_k(G_1)\, L_k(G_2) = F(X)$.*

Proof. We know from ch. 3, Prop. 3.53, that $\tau : P_k(G) \to P_k(G_1) \times P_k(G_2)$ is a monomorphism. Thus τ is an isomorphism if and only if $|P_k(G)| = |P_k(G_1)|\,|P_k(G_2)|$, i.e.

$$\big|G[X] \mid \ker \sigma_k(G)\big| = \big|G_1[X] \mid \ker \sigma_k(G_1)\big|\,\big|G_2[X] \mid \ker \sigma_k(G_2)\big|.$$

This is equivalent to

$$\big|G[X] \mid \ker \sigma_k(G) \ker \lambda_k(G)\big|\,\big|\ker \sigma_k(G) \ker \lambda_k(G) \mid \ker \sigma_k(G)\big| =$$

$$= \prod_{i=1}^{2} \big|G_i[X] \mid \ker \sigma_k(G_i) \ker \lambda_k(G_i)\big|\,\big|\ker \sigma_k(G_i) \ker \lambda_k(G_i) \mid \ker \sigma_k(G_i)\big|.$$

By Prop. 1.21 and Prop. 1.13, this is true if and only if $\big|F(X)|L_k(G)\big| = \big|F(X)|L_k(G_1)\big|\,\big|F(X)|L_k(G_2)\big|$, and by Prop. 1.2, if and only if $\big|F(X)|L_k(G_1) \cap L_k(G_2)\big| = \big|F(X)|L_k(G_1)\big|\,\big|F(X)|L_k(G_2)\big|$. By the first isomorphism theorem, this is equivalent to saying $\big|L_k(G_1)\, L_k(G_2)|L_k(G_2)\big| = \big|F(X)|L_k(G_2)\big|$ which holds if and only if $L_k(G_1)\, L_k(G_2) = F(X)$.

1.3. Proposition. *Let G be any finite group and p a prime. Suppose $A_p(X)$ is the verbal subgroup of $F(X)$ generated by x_1^p and $x_1^{-1}x_2^{-1}x_1x_2$, for $|X| \geqslant 2$, and generated by x^p, for $X = \{x\}$, then $L_k(G) \subseteq A_p(X)$ if and only if G possesses some central p-chief factor.*

Proof. Let $H|K$ be a central p-chief factor of G. Since by Prop. 1.14, $L_k(G) \subseteq L_k(G|K)$, the "if" part of the proposition will be proved if we show that $L_k(G) \subseteq A_p(X)$ whenever G has some central minimal normal p-subgroup N which, by ch. 6, § 6.51, is cyclic of order p. Suppose $w \in L_k(G)$. Then there exists $f \in \ker \sigma_k(G)$ such that $\lambda_k(G) f = w$. Let $m_1, \ldots, m_k \in N$, then $1 = f(m_1, \ldots, m_k) = f(1, \ldots, 1)\, w(m_1, \ldots, m_k) = w(m_1, \ldots, m_k)$ since N is central in G. Hence $w = 1$ is a law for N. But every k-variable law for N is of the form $v = 1$ where $v \in A_p(X)$ (see ch. 6, Lemma 6.73). Hence $w \in A_p(X)$ and $L_k(G) \subseteq A_p(X)$.

Conversely let $L_k(G) \subseteq A_p(X)$ and $x \in X$. Then, since the subgroup of $F(X)$ generated by x is a free group, we have $L_k(G) \cap F(x) \subseteq A_p(X) \cap F(x)$ and therefore $L_1(G) \subseteq A_p(x)$. Let N be a minimal normal subgroup of G and $L_1(G, N) = \{w \in F(x) \mid$ there exists $f \in G[x]$ such that $\lambda_1(G) f = w$ and $f(n) = 1$, for all $n \in N\}$. Then $L_1(G, N)$ is a subgroup of $F(x)$ and $L_1(N) \subseteq L_1(G, N)$. We distinguish two cases: Case a): N is non-abelian. Then $N = N_1 \times N_2 \times \ldots \times N_k$, $N_i \cong N_j$, $i, j = 1, \ldots, k$, and N_i is simple non-abelian (cf. ch. 6, § 6.51). By a result which will be proved in § 2.43, $L_1(N_i) = F(x)$ whence Prop. 1.2 implies that $L_1(N) = F(x)$. Let $L_1(N) \circ L_1(G|N)$ be the set of all elements of $F(x)$ which we obtain from substituting the elements of $L_1(G|N)$ into the elements of $L_1(N)$. Clearly $L_1(N) \circ L_1(G|N) \subseteq L_1(G)$. Since $x \in L_1(N)$, we obtain $L_1(G|N) \subseteq L_1(G) \subseteq A_p(x)$. Case b): N is abelian. Let $L_1(G, N) \circ L_1(G|N)$ be the set of all elements of $F(x)$ which we obtain from substituting the elements of $L_1(G|N)$ into the elements of $L_1(G, N)$. Then $L_1(G, N) \circ L_1(G|N) \subseteq L_1(G) \subseteq A_p(x)$. Since p is a prime, we have either $L_1(G, N) \subseteq A_p(x)$ or $L_1(G|N) \subseteq A_p(x)$. If $L_1(G, N) \subseteq A_p(x)$, then N is a p-group, for otherwise there exists some prime $q \neq p$ such that $A_q(x) \subseteq L_1(N) \subseteq L_1(G, N) \subseteq A_p(x)$, contradiction. Let K be the prime field of characteristic p, and regard N as a KG-module where G acts on N by conjugation (cf. ch. 6, § 7.5). The annihilator $\operatorname{An} N$ of N in KG is a maximal two-sided ideal in KG since $KG|\operatorname{An} N$ is a simple ring (see ch. 6, § 7.4). Let $\sum (k_g g \mid g \in G) \in \operatorname{An} N$, $k_g \in K$, and k_g' integers representing $k_g \in K \cong \mathbf{Z}|(p)$. Then $\prod (g x^{k_g'} g^{-1} \mid g \in G) \in G[x]$, where the factors are arranged arbitrarily, maps every element of N onto 1. Thus $x^{\sum k_g'} \in L_1(G, N) \subseteq A_p(x) = [x^p]$. Hence $p / \sum k_g'$, i.e. $\sum k_g = 0$. But the set $I = \{\sum (k_g g \mid g \in G) \mid k_g \in K, \sum k_g = 0\}$ is a two-sided ideal in KG such that $\operatorname{An} N \subseteq I$. Therefore $\operatorname{An} N = I$, by the maximality of $\operatorname{An} N$. Hence $g - 1 \in \operatorname{An} N$, for every $g \in G$, thus $gng^{-1} = n$, for all $g \in G$, $n \in N$, i.e. N is central.

The proof concludes with an induction argument on the length l of a chief series of G. If $l = 1$, then G is simple. If G were non-abelian, then by a), $F(x) = L_1(G) \subseteq A_p(x)$, contradiction. Hence G is a simple abelian group and thus obviously possesses a central p-chief factor. Suppose now that the proposition is true for $l-1$ instead of l, and let N be a minimal normal subgroup of G. Then by a), b), N is a central p-chief factor of G, or $L_1(G|N) \subseteq A_p(x)$. In the second case, $G|N$ has some central p-chief factor by induction which is isomorphic to some central p-chief factor of G.

1.4. Proposition. *If a $k+1$-ary operation $\varkappa$ is defined in $F(X)$ by $\varkappa w_0 w_1 \ldots w_k = w_0(w_1, \ldots, w_k)$, then the algebra $\langle F(X); \Omega, \varkappa \rangle$ is a k-dimensional*

composition group with selector system and the epimorphism $\lambda_k(G) : G[X] \to F(X)$ *is a composition epimorphism. In particular,* $\ker \lambda_k(G)$ *is a full ideal of* $G[X]$.

Proof. By ch. 1, Cor. 9.22, we have $F(X) = \{1\}[X]$. Thus by ch. 3, Prop. 2.24, $\langle F(X); \Omega, \varkappa\rangle$ is a k-dimensional composition group with selector system. Clearly $\lambda_k(G)$ is the unique extension of the epimorphism $G \to \{1\}$ to an epimorphism from $G[X]$ to $\{1\}[X]$ fixing X elementwise whence it is a composition epimorphism, by ch. 3, § 3.22. The last assertion follows from ch. 3, § 4.1.

2. Distributively generated composition groups and polynomial functions over groups

2.1. In ch. 3, § 11.1, the functor $\mathcal{F}$ from the category of k-dimensional $\mathfrak{V}$-composition algebras to the category of 1-dimensional $\mathfrak{V}$-composition algebras has been introduced, $\mathfrak{V}$ being any variety. Taking the variety of groups for $\mathfrak{V}$, the functor $\mathcal{F}$ becomes a functor from the category of k-dimensional composition groups to the category of near-rings. Some special classes of composition groups and the effect of $\mathcal{F}$ on these classes will be investigated now.

First we define: Let $G = \langle G; +, -, 0, \varkappa\rangle$ be a k-dimensional composition group where $+$ is the (not necessarily commutative) group operation, $-$ the inverse operation, 0 the identity, and $\varkappa$ the composition. An element $d \in G$ is called a distributive element if $\varkappa d(a_1+b_1)\dots(a_k+b_k) = \varkappa d a_1 \dots a_\kappa + \varkappa d b_1 \dots b_k$, for all $a_1, \dots, a_k, b_1, \dots, b_k \in G$. A k-dimensional composition group $G = \langle G; +, -, 0, \varkappa\rangle$ is called a distributively generated (d.g.) k-dimensional composition group if there exist distributive elements $d_i \in G$, $i \in I$, such that $\langle G; +, -, 0\rangle = [\{d_i \mid i \in I\}]$ – i.e., G regarded as an ordinary group has a generating set consisting of distributive elements. For $k = 1$, we obtain the well-known concept of a distributively generated near-ring. Clearly every homomorphic image of a d.g. k-dimensional composition group is again a d.g. k-dimensional composition group.

2.11. Proposition. *If* G *is a d.g. k-dimensional composition group, then* $\mathcal{F}(G)$ *is a d.g. near-ring.*

Proof. Let $\langle G; +, -, 0\rangle = [\{d_i \mid i \in I\}]$, $d_i \in G$ distributive. Then $\langle \mathcal{F}(G); +, -, 0\rangle = [\bigcup(\{(d_i, 0, \dots, 0), (0, d_i, \dots, 0), \dots, (0, 0, \dots, d_i)\} \mid i \in I)]$. Hence it suffices to show that any element $(0, \dots, d_i, \dots, 0) \in \mathcal{F}(G)$ is distributive w.r.t. the composition $\circ$ in $\mathcal{F}(G)$. Let $(a_1, \dots, a_k)$, $(b_1, \dots, b_k) \in \mathcal{F}(G)$, then

$$
\begin{aligned}
&(0, \dots, d_i, \dots, 0) \circ [(a_1, \dots, a_k)+(b_1, \dots, b_k)] = \\
&\quad = (0, \dots, d_i, \dots, 0) \circ (a_1+b_1, \dots, a_k+b_k) \\
&\quad = (0, \dots, \varkappa d_i(a_1+b_1) \dots (a_k+b_k), \dots, 0) \\
&\quad = (0, \dots, \varkappa d_i a_1 \dots a_k + \varkappa d_i b_1 \dots b_k, \dots, 0) \\
&\quad = (0, \dots, \varkappa d_i a_1 \dots a_k, \dots, 0) + (0, \dots, \varkappa d_i b_1 \dots b_k, \dots, 0) \\
&\quad = (0, \dots, d_i, \dots, 0) \circ (a_1, \dots, a_k) + (0, \dots, d_i, \dots, 0) \circ (b_1, \dots, b_k).
\end{aligned}
$$

2.12. Lemma. *Let* G *be any d.g. k-dimensional composition group and* A *a normal subgroup of* $\langle G; +, -, 0\rangle$. *Then* A *is a full ideal in* G *if and only if* $\varkappa a c_1 \dots c_k \in A$ *and* $\varkappa c 0 \dots a \dots 0 \in A$, *for any* $a \in A$, $c_1, \dots, c_k$, $c \in G$.

Proof. Let A be a full ideal in G, $a \in A$, $c_1, \dots, c_k \in G$, then by ch. 3, § 5.2, $\varkappa a c_1 \dots c_k - \varkappa 0 c_1 \dots c_k \in A$. But $\varkappa 0 c_1 \dots c_k = 0$ since $\varkappa$ is superdistributive, thus $\varkappa a c_1 \dots c_k \in A$. Moreover if $c \in G$, then again by ch. 3, § 5.2, $\varkappa c 0 \dots a \dots 0 - \varkappa c 0 \dots 0 \in A$. But since c is a sum of distributive elements and additive inverses of distributive elements and $\varkappa d 0 \dots 0 = 0$, for any distributive element $d \in G$, superdistributivity again yields $\varkappa c 0 \dots 0 = 0$. Conversely, let A satisfy the hypothesis of the lemma, $c_0, \dots, c_k \in G$, $a \in A$. Then $\varkappa(c_0+a)c_1 \dots c_k - \varkappa c_0 c_1 \dots c_k = \varkappa c_0 c_1 \dots c_k + \varkappa a c_1 \dots c_k - \varkappa c_0 c_1 \dots c_k \in A$ since $\varkappa$ is superdistributive and A is normal in $\langle G; +, -, 0\rangle$. Moreover if $1 \leqslant \nu \leqslant k$ then $\varkappa c_0 \dots (c_\nu+a) \dots c_k - \varkappa c_0 \dots c_\nu \dots c_k \in A$ whenever c_0 is distributive, for $\varkappa c_0 \dots (c_\nu+a) \dots c_k - \varkappa c_0 \dots c_\nu \dots c_k = \varkappa c_0 \dots c_\nu \dots c_k + \varkappa c_0 0 \dots a \dots 0 - \varkappa c_0 \dots c_\nu \dots c_k$, and if c_0 is not distributive, then c_0 is a sum of distributive elements and additive inverses of distributive elements, and again the superdistributivity of $\varkappa$ yields the same result as is easily checked. Hence by ch. 3, § 5.2, A is a full ideal.

2.13. Proposition. *Let* G *be a d.g. k-dimensional composition group with selector system* $s_1, \dots, s_k$. *Then* $\mathcal{F}(G)$ *is a simple near-ring if and only if* G *is a simple k-dimensional composition group.*

Proof. Assume that G is not simple, and let A be a non-trivial full ideal in G. Then A^k is a normal subgroup of $\mathcal{F}(G)$. Moreover if $(a_1, \ldots, a_k) \in A^k, (g_1, \ldots, g_k), (h_1, \ldots, h_k) \in G^k$, then $(g_1+a_1, \ldots, g_k+a_k) \circ (h_1, \ldots, h_k) - (g_1, \ldots, g_k) \circ (h_1, \ldots, h_k) \in A^k$ and $(g_1, \ldots, g_k) \circ (h_1+a_1, \ldots, h_k+a_k) - (g_1, \ldots, g_k) \circ (h_1, \ldots, h_k) \in A^k$ whence A^k is a non-trivial full ideal of $\mathcal{F}(G)$. Therefore $\mathcal{F}(G)$ is non-simple.

Conversely suppose that G is simple and A is a non-zero full ideal in $\mathcal{F}(G)$. Then there is a non-zero element $(a_1, \ldots, a_k) \in A$. Assume that $a_i \neq 0$, then the set A_i of all i-th components of elements of A contains a non-zero element. We will show that A_i is a full ideal in G. Clearly A_i is a subgroup of $\langle G; +, -, 0\rangle$ and is moreover normal in G. Let $c_1, \ldots, c_k \in G$, $a \in A_i$, and $(a_1, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_k) \in A$. Then $(a_1, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_k) \circ (c_1, \ldots, c_k) = (\varkappa a_1 c_1 \ldots c_k, \ldots, \varkappa a c_1 \ldots c_k, \ldots, \varkappa a^k c_1 \ldots c_k) \in A$, hence $\varkappa a c_1 \ldots c_k \in A_i$, for all $c_1, \ldots, c_k \in G$. Let $c \in G$, then $(0, \ldots, \varkappa c 0 \ldots 0 s_i 0 \ldots 0, \ldots, 0) \circ (a_1, \ldots, a, \ldots, a_k) = (0, \ldots, \varkappa\varkappa c 0 \ldots 0 s_i 0 \ldots 0 a_1 \ldots a_k, \ldots, 0) = (0, \ldots, \varkappa c 0 \ldots a \ldots 0, \ldots, 0) \in A$ by the superassociativity of $\varkappa$, hence $\varkappa c \ldots 0 a 0 \ldots 0 \in A_i$, for all $c \in G$. By Lemma 2.12, A_i is a full ideal of G whence $A_i = G$ by simplicity of G. Hence, for any $a \in G$, there exist elements $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_k \in G$ such that $(a_1, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_k) \in A$. If $(0, \ldots, s_i, \ldots, 0) \in \mathcal{F}(G)$ has s_i as its j-th component, $j = 1, \ldots, k$, then $(0, \ldots, s_i, \ldots, 0) \circ (a_1, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_k) = (0, \ldots, a, \ldots, 0) \in A$, by Lemma 2.12 where a occurs as the j-th component. But $\{(0, \ldots, a, \ldots, 0) \mid a \in G, j = 1, \ldots, k\}$ additively generates G whence $A = \mathcal{F}(G)$. Hence $\mathcal{F}(G)$ is simple.

2.2. Let N be a normal subgroup of a group G and $k \geqslant 1$ an integer. By $P_k(G, N)$ we will denote the set of all mappings obtained by restricting the action of the elements of $P_k(G)$ to N^k while $\bar{P}_k(G, N) = \{\varphi \in P_k(G, N) \mid \varphi(1, 1, \ldots, 1) = 1\}$. Clearly $\bar{P}_k(G, N) \subseteq F_k(N)$. The set $\bar{P}_k(G, G) = \{\varphi \in P_k(G) \mid \varphi(1, 1, \ldots, 1) = 1\}$ is a composition subgroup of the k-dimensional composition group $P_k(G)$ and the mapping from $\bar{P}_k(G, G)$ onto $\bar{P}_k(G, N)$ which maps every element of $\bar{P}_k(G, G)$ onto its restriction to N^k, is a composition epimorphism whence $\bar{P}_k(G, N)$ is a composition subgroup of the k-dimensional composition group $F_k(N)$. Hence $\mathcal{F}(\bar{P}_k(G, N))$ is a subnear-ring of $\mathcal{F}(F_k(N))$. For N being a minimal normal subgroup of a finite group G, some structural results on $\mathcal{F}(\bar{P}_k(G, N))$ will be obtained. We have to distinguish two cases: a) N is abelian, then N is an elementary abelian p-group, for some prime p. b) N is non-abelian.

2.3. First we deal with case a) and view N as a KG-module where G acts on N by conjugation and K is the prime field of characteristic p. In particular, we will write $\sum[(\sum \alpha_{ij} g_i) n_j \mid n_j \in N, g_i \in G]$ instead of $\prod(\prod g_i n_j^{\alpha_{ij}} g_i^{-1} \mid n_j \in N, g_i \in G)$ where α_{ij} are integers. The proof of the following proposition requires some ring-theoretical results (see ch. 6, § 7).

2.31. Proposition. *Let G be a finite group and N an elementary abelian minimal normal p-subgroup of G, for some prime p. Then $\mathcal{F}(\bar{P}_k(G, N))$ is a simple ring.*

Proof. Let $\varphi : \mathcal{F}(F_k(N)) \to F_1(N^k)$ be the composition isomorphism of ch. 3, Lemma 11.21. All we have to show is that $\varphi\mathcal{F}(\bar{P}_k(G, N))$ is a simple ring. Let $\psi \in \varphi\mathcal{F}(\bar{P}_k(G, N))$, then, by ch. 1, Th. 9.21,

$$\psi(n_1, \ldots, n_\varkappa) = \left(\sum_{j=1}^{k} (\sum (\alpha_{ij1} g_i \mid g_i \in G)) n_j, \ldots, \sum_{j=1}^{k} (\sum (\alpha_{ijk} g_i \mid g_i \in G)) n_j \right) \tag{2.3}$$

and any such mapping belongs to $\varphi\mathcal{F}(\bar{P}_k(G, N))$, as one can easily check. Let $\operatorname{An} N$ be the annihilator ideal of N in KG, then we may regard N also as a faithful irreducible $KG \mid \operatorname{An} N$-module. Hence by a well-known theorem of representation theory, $KG \mid \operatorname{An} N$ is a simple ring, thus a full matrix ring over some finite field. On the other hand, (2.3) shows that $\varphi\mathcal{F}(\bar{P}_k(G, N))$ is isomorphic to the full $k \times k$-matrix ring over $KG \mid \operatorname{An} N$, hence also isomorphic to some full matrix ring over a finite field and thus is a simple ring.

2.4. Lemma. *Let G be any finite group and N a non-abelian minimal normal subgroup of G. Then $\bar{P}_k(G, N) = \{\varphi \in F_k(N) \mid \varphi(1, \ldots, 1) = 1\}$.*

Proof. We apply ch. 1, Prop. 12.5, putting $A = N^k$ and taking for H the set of those mappings of $P_k(G, N)$ which map N^k to N. Then H is a subgroup of F such that conditions a) and c) are satisfied. Let π_1, π_2 be two distinct elements of N^k, then $\xi_i \pi_1 \neq \xi_i \pi_2$, for at least one projection $\xi_i \in H$ whence also condition b) holds. Hence $H = F_k(N)$ and thus $\bar{P}_k(G, N) = \{\varphi \in H \mid \varphi(1, \ldots, 1) = 1\} = \{\varphi \in F_k(N) \mid \varphi(1, \ldots, 1) = 1\}$.

2.41. Remark. If G is any group and N is a normal subgroup of G, then $\bar{P}_k(G, N)$ is a d.g. k-dimensional composition group. Indeed, $[\{g\xi_i g^{-1} | i = 1, \ldots, k, g \in G\}] = \langle \bar{P}_k(G, N); \cdot, {}^{-1}, 1\rangle$ and $g\xi_i g^{-1}$ is distributive, for all $g \in G$ and all projections ξ_i.

2.42. Proposition. *If G is any finite group and N a non-abelian minimal normal subgroup of G, then $\mathcal{F}(\bar{P}_k(G, N))$ is a simple d.g. near-ring.*

Proof. Let U be a non-zero full ideal of $\bar{P}_k(G, N)$. If we identify N with the group of constant functions of $F_k(N)$, then UN is a subgroup of $\langle F_k(N); \cdot, {}^{-1}, 1\rangle$ since, for $\varphi_1, \varphi_2 \in U$, $n_1, n_2 \in N$, we have

$$(\varphi_1 n_1)(\varphi_2 n_2) = \varphi_1(n_1\varphi_2 n_1^{-1})(n_1 n_2) = \varphi_1(\varkappa(n_1\xi_1 n_1^{-1})\varphi_2\, 1 \ldots 1)(n_1 n_2) \in UN,$$

by Lemma 2.12 where ξ_1 is the first projection of $F_k(N)$ and thus $n_1\xi_1 n_1^{-1} \in \bar{P}_k(G, N)$. We now apply ch. 1, Prop. 12.5 setting $A = N^k$ and $H = UN$. Clearly condition a) is satisfied. Let $r \in G$, $\psi \in U$, then $r^{-1}\xi_1 r \in \bar{P}_k(G, N)$ whence, by Lemma 2.12, $\varkappa(r^{-1}\xi_1 r)\psi\, 1 \ldots 1 = r^{-1}\psi r \in U$, thus $\varphi \in H$ and $r \in G$ implies $r^{-1}\varphi r \in UN$. Hence also condition c) holds. Suppose there exist elements $\mathfrak{n}_1, \mathfrak{n}_2 \in N^k$ such that $\mathfrak{n}_1 \neq \mathfrak{n}_2$ while $\psi\mathfrak{n}_1 = \psi\mathfrak{n}_2$, for all $\psi \in UN$. WLOG, we can assume that $\mathfrak{n}_1 \neq (1, \ldots, 1)$. For any $n \in N$, we choose $\eta(\mathfrak{n}_1, n) \in F_k(N)$ such that $\eta(\mathfrak{n}_1, n)\mathfrak{n}_1 = n$ and $\eta(\mathfrak{n}_1, n)\mathfrak{n} = 1$, for $\mathfrak{n} \neq \mathfrak{n}_1$. By Lemma 2.4, $\eta(\mathfrak{n}_1, n) \in \bar{P}_k(G, N)$. Hence, for any $\mathfrak{n} \in N^k$, we have $\varkappa\psi\eta(\mathfrak{n}_1, \xi_1\mathfrak{n}) \ldots \eta(\mathfrak{n}_1, \xi_k\mathfrak{n}) \in UN$ since U is a full ideal of $\bar{P}_k(G, N)$. Therefore

$$\begin{aligned}\psi\mathfrak{n} &= \varkappa\psi\eta(\mathfrak{n}_1, \xi_1\mathfrak{n}) \ldots \eta(\mathfrak{n}_1, \xi_k\mathfrak{n})\mathfrak{n}_1 \\ &= \varkappa\psi\eta(\mathfrak{n}_1, \xi_1\mathfrak{n}) \ldots \eta(\mathfrak{n}_1, \xi_k\mathfrak{n})\mathfrak{n}_2 = \psi(1, 1, \ldots, 1).\end{aligned}$$

Therefore $UN \subseteq N$, i.e. $U \subseteq N$ and U would be the zero-ideal of $\bar{P}_k(G, N)$. Hence also condition b) is satisfied. Therefore $UN = F_k(N)$, and this implies that $\bar{P}_k(G, N) = \bar{P}_k(G, N) \cap UN = U(\bar{P}_k(G, N) \cap N) = U$. Hence $\bar{P}_k(G, N)$ is simple. Prop. 2.13 yields the result.

2.43. Corollary. *If G is a finite simple non-abelian group, then $L_k(G) = F(X)$, for any k.*

Proof. As in § 1, let $\sigma_k(G) : G[X] \to P_k(G)$ be the canonical epimorphism and $\lambda_k(G) : G[X] \to F(X)$ the length-epimorphism. Then, by Prop. 1.4,

$\ker \lambda_k(G)$ is a full ideal of $G[X]$, hence $\sigma_k(G) \ker \lambda_k(G)$ is a full ideal of $P_k(G)$. Therefore $\sigma_k(G) \ker \lambda_k(G) \cap \bar{P}_k(G, G)$ is a full ideal of $\bar{P}_k(G, G)$. By the proof of Prop. 2.42, $\bar{P}_k(G, G)$ is simple, thus $\sigma_k(G) \ker \lambda_k(G) \cap \bar{P}_k(G, G)$ equals either $\{1\}$ or $\bar{P}_k(G, G)$. In the first case, we arrive at a contradiction when taking any $g \in G$, $g \neq 1$ and $h \in G$ such that h does not centralize g, for then, with the notation of Prop. 2.42, for $\mathfrak{n}_1 \in G^k$, $\mathfrak{n}_1 \neq (1, 1, \ldots, 1)$, we obtain $1 \neq \eta(\mathfrak{n}_1, h)^{-1} g\eta(\mathfrak{n}_1, h)g^{-1} \in \sigma_k(G) \ker \lambda_k(G) \cap \bar{P}_k(G, G)$. Hence $\bar{P}_k(G, G) \subseteq \sigma_k(G) \ker \lambda_k(G) \subseteq P_k(G)$. But the group $P_k(G) | \bar{P}_k(G, G)$ is isomorphic to G, hence is simple, and $\xi_1 \in \bar{P}_k(G, G)$, $(\varkappa(a\xi_1)b_1 \ldots b_k)(\varkappa ab_1 \ldots b_k)^{-1} = ab_1a^{-1} \notin \bar{P}_k(G, G)$, for $b_1 \neq 1$, shows that $\bar{P}_k(G, G)$ is not a full ideal of $P_k(G)$ by ch. 3, § 5.2. Hence $\sigma_k(G) \ker \lambda_k(G) = P_k(G)$, therefore $\ker \sigma_k(G) \ker \lambda_k(G) = G[X]$. Thus, by Prop. 1.13, $L_k(G) = F(X)$.

3. On polynomial permutations over groups

3.1. Let G be a group and $X = \{x_1, \ldots, x_k\}$ a set of indeterminates. In ch. 3, § 11.45, the semigroup $U_k(G)$ of all polynomial permutations of G^k has been introduced. If we recall ch. 3, §§ 11.42, 11.43, we note that $U_k(G)$ consists of all polynomial function vectors $\mathfrak{f}$ of $\mathcal{F}(P_k(G))$ such that $\varphi\mathfrak{f}$ is a permutation of G^k, and that, for finite G, $U_k(G)$ coincides with the group of units of the near-ring $\mathcal{F}(P_k(G))$. Let $G_0(X) = \{f \in G[X] | f(1, 1, \ldots, 1) = 1\}$. Then $G_0(X)$ is a composition subgroup of the k-dimensional composition group $G[X]$. By Prop. 1.4, $G_0(X) \cap \ker \lambda_k(G)$ is a full ideal of $G_0(X)$. Moreover $\ker \sigma_k(G) \subseteq G_0(X)$ and $G_0(X) | \ker \sigma_k(G) \cong \bar{P}_k(G, G)$ which, by Remark 2.41, is a distributively generated k-dimensional composition group with a selector system. Let $\varkappa : G_0(X) \to G_0(X) | \ker \sigma_k(G)$ be the canonical composition group epimorphism. Then $\varkappa(G_0(X) \cap \ker \lambda_k(G))$ is a full ideal of $G_0(X) | \ker \sigma_k(G)$. Hence $\ker \sigma_k(G)(G_0(X) \cap \ker \lambda_k(G))$ is a full ideal of $G_0(X)$. Let

$$\mu_G : G_0(X) | \ker \sigma_k(G) \to G_0(X) | \ker \sigma_k(G)\,(G_0(X) \cap \ker \lambda_k(G)) \quad (3.1)$$

be the canonical epimorphism. Then μ_G is a composition group epimorphism whence $\mathcal{F}(\mu_G)$ is a near-ring epimorphism from a distributively generated near-ring with identity, by Prop. 2.11. As a consequence of ch. 6. Prop. 8.51, we obtain:

3.11. Proposition. *Let G be a finite group, and*

$$\mu_G : G_0(X)|\ker \sigma_k(G) \to G_0(X)|\ker \sigma_k(G)\,(G_0(X)\cap \ker \lambda_k(G))$$

the canonical epimorphism. Then $\mathcal{F}(\mu_G)\,\mathcal{E}\big(\mathcal{F}\big(G_0(X)|\ker \sigma_k(G)\big)\big) = \mathcal{E}\big(\mathcal{F}\big(G_0(X)|\ker \sigma_k(G)\,(G_0(X)\cap \ker \lambda_k(G))\big)\big)$.

3.12. The restriction of $\mathcal{F}(\mu_G)$ to $\mathcal{E}\big(\mathcal{F}\big(G_0(X)|\ker \sigma_k(G)\big)\big)$ will be denoted by $\mathcal{E}(\mathcal{F}(\mu_G))$. With this notation, we now prove

3.2. Proposition. *Let $G = G_1\times G_2$ be a finite group. Then*

$$\ker \mathcal{E}(\mathcal{F}(\mu_G)) \cong \ker \mathcal{E}(\mathcal{F}(\mu_{G_1}))\times \ker \mathcal{E}(\mathcal{F}(\mu_{G_2})).$$

Proof. Let $\vartheta : G_0(X) \to G_0(X)|\ker \sigma_k(G)$, $\vartheta_i : G_{i0}(X) \to G_{i0}(X)|\ker \sigma_k(G_i)$ be the canonical epimorphisms, $i = 1, 2$, and $\iota_i[X] : G_i[X] \to (G_1\times G_2)[X]$ the homomorphisms as in the proof of Prop. 1.2. Then $\iota_i[X]G_{i0}(X) \subseteq G_0(X)$, $i = 1, 2$. If $\pi_i[X] : G[X] \to G_i[X]$ denotes the extensions of the projections $\pi_i : G \to G_i$, $i = 1, 2$, to composition epimorphisms, then $\pi_i[X]\,G_0(X) \subseteq G_{i0}(X)$. Let $\psi : \mathcal{F}(G_1\times G_2) \to \mathcal{F}(G_1)\times \mathcal{F}(G_2)$ be the isomorphism as in ch. 3, Lemma 11.13, and define a mapping $\varphi : \ker \mathcal{E}(\mathcal{F}(\mu_{G_1}))\times\ker \mathcal{E}(\mathcal{F}(\mu_{G_2})) \to \ker \mathcal{E}(\mathcal{F}(\mu_G))$ as follows: If $(\mathfrak{u}_1, \mathfrak{u}_2)\in \ker \mathcal{E}(\mathcal{F}(\mu_{G_1}))\times\ker \mathcal{E}(\mathcal{F}(\mu_{G_2}))$, then choose counterimages $\bar{\mathfrak{u}}_i$ of $\mathfrak{u}_i$ under $\mathcal{F}(\vartheta_i)$ such that $\bar{\mathfrak{u}}_i \in \mathfrak{x}\mathcal{F}\big(G_{i0}(X)\cap \ker \lambda_k(G_i)\big)$. This choice can be made, indeed, since if $\bar{\mathfrak{v}}_i$ is any counterimage of $\mathfrak{u}_i$ under $\mathcal{F}(\vartheta_i)$, then $\bar{\mathfrak{v}}_i \in \mathfrak{x}\mathcal{F}\big(\ker \sigma_k(G_i)\,(G_{i0}(X)\cap \ker \lambda_k(G_i))\big)$. We now set $\varphi(\mathfrak{u}_1, \mathfrak{u}_2) = \mathcal{F}(\vartheta)\,(\mathcal{F}(\iota_1[X])\,\bar{\mathfrak{u}}_1\mathfrak{x}^{-1}\mathcal{F}(\iota_2[X])\bar{\mathfrak{u}}_2)$. Then if $\mathfrak{g}\in G^k = \mathcal{F}(G)$ and $\psi\mathfrak{g} = (\mathfrak{a}, \mathfrak{b})$, we have

$$\begin{aligned}\psi\big[(\mathcal{F}(\iota_1[X])\,\bar{\mathfrak{u}}_1\mathfrak{x}^{-1}\mathcal{F}(\iota_2[X])\bar{\mathfrak{u}}_2)\circ\mathfrak{g}\big] &= \\ = \psi\big[\big((\mathcal{F}(\iota_1[X])\bar{\mathfrak{u}}_1\mathfrak{x}^{-1})\circ\mathfrak{g}\big)\,\mathfrak{g}\big((\mathcal{F}(\iota_2[X])\mathfrak{x}^{-1}\bar{\mathfrak{u}}_2)\circ\mathfrak{g}\big)\big] &= \\ = \big((\bar{\mathfrak{u}}_1\circ\mathfrak{a})\mathfrak{a}^{-1}\mathfrak{a},\ \mathfrak{b}\mathfrak{b}^{-1}(\bar{\mathfrak{u}}_2\circ\mathfrak{b})\big) = (\bar{\mathfrak{u}}_1\circ\mathfrak{a},\ \bar{\mathfrak{u}}_2\circ\mathfrak{b}).&\end{aligned}$$

Hence $\mathcal{F}(\sigma_k(G))\,(\mathcal{F}(\iota_1[X])\,\bar{\mathfrak{u}}_1\mathfrak{x}^{-1}\mathcal{F}(\iota_2[X])\bar{\mathfrak{u}}_2)$ is independent of the choice of the $\bar{\mathfrak{u}}_i$, hence $\varphi(\mathfrak{u}_1, \mathfrak{u}_2)$ is well defined.

Since $\mathfrak{u}_i\in \mathcal{E}\big(\mathcal{F}\big(G_{i0}(X)|\ker \sigma_k(G_i)\big)\big)$, $\bar{\mathfrak{u}}_i$ is a permutation polynomial vector of G_i^k, hence the last equation shows that $\mathcal{F}(\iota_1[X])\,\bar{\mathfrak{u}}_1\mathfrak{x}^{-1}\mathcal{F}(\iota_2[X])\bar{\mathfrak{u}}_2$ induces a surjective mapping from G^k into itself and thus is a permutation polynomial vector of G^k. Hence $\varphi(\mathfrak{u}_1, \mathfrak{u}_2)\in \mathcal{E}\big(\mathcal{F}\big(G_0(X)|\ker \sigma_k(G)\big)\big)$.

Moreover

$$\begin{aligned}\mathcal{F}(\lambda_k(G))\,(\mathcal{F}(\iota_1[X])\,\bar{\mathfrak{u}}_1\mathfrak{x}^{-1}\mathcal{F}(\iota_2[X])\bar{\mathfrak{u}}_2) &= \mathcal{F}(\lambda_k(G_1))\,\bar{\mathfrak{u}}_1\mathfrak{x}^{-1}\mathcal{F}(\lambda_k(G_2))\bar{\mathfrak{u}}_2 \\ &= \big(\mathcal{F}(\lambda_k(G_1))\bar{\mathfrak{u}}_1\mathfrak{x}^{-1}\big)\,\mathfrak{x}\big(\mathcal{F}(\lambda_k(G_2))\big)\mathfrak{x}^{-1}\bar{\mathfrak{u}}_2 = \mathfrak{x}\end{aligned}$$

whence $(\mathcal{F}(\iota_1[X])\bar{\mathfrak{u}}_1\mathfrak{x}^{-1}\mathcal{F}(\iota_2[X])\bar{\mathfrak{u}}_2)\mathfrak{x}^{-1}\in \mathcal{F}\big(\ker\sigma_k(G)\,(G_0(X)\cap\ker\lambda_k(G))\big)$. Therefore $\varphi(\mathfrak{u}_1, \mathfrak{u}_2)\in \ker \mathcal{E}(\mathcal{F}(\mu_G))$.

If $\varphi(\mathfrak{u}_1, \mathfrak{u}_2) = \varphi(\mathfrak{v}_1, \mathfrak{v}_2)$, and $\bar{\mathfrak{u}}_i$, $\bar{\mathfrak{v}}_i$ are counterimages of $\mathfrak{u}_i$, $\mathfrak{v}_i$ as used for defining φ, then $(\bar{\mathfrak{u}}_1\circ\mathfrak{a},\ \bar{\mathfrak{u}}_2\circ\mathfrak{b}) = (\bar{\mathfrak{v}}_1\circ\mathfrak{a},\ \bar{\mathfrak{v}}_2\circ\mathfrak{b})$, for any $(\mathfrak{a}, \mathfrak{b})\in \mathcal{F}(G_1)\times\mathcal{F}(G_2)$, hence $\mathfrak{u}_1 = \mathfrak{v}_1$, $\mathfrak{u}_2 = \mathfrak{v}_2$, i.e. φ is injective.

Let $\mathfrak{w}\in\ker \mathcal{E}(\mathcal{F}(\mu_G))$, $\bar{\mathfrak{w}}$ be a counterimage of $\mathfrak{w}$ under $\mathcal{F}(\vartheta)$ such that $\bar{\mathfrak{w}}\in\mathfrak{x}\mathcal{F}(G_0(X)\cap\ker\lambda_k(G))$. Then $\mathcal{F}(\pi_i[X])\bar{\mathfrak{w}}\in\mathfrak{x}\mathcal{F}\big(G_{i0}(X)\cap\ker\lambda_k(G_i)\big)$. If $\mathfrak{g}\in\mathcal{F}(G)$ and $\psi\mathfrak{g} = (\mathfrak{a}, \mathfrak{b})$, then $\psi(\bar{\mathfrak{w}}\circ\mathfrak{g}) = \big(\mathcal{F}(\pi_1[X])\bar{\mathfrak{w}}\circ\mathfrak{a},\ \mathcal{F}(\pi_2[X])\bar{\mathfrak{w}}\circ\mathfrak{b}\big)$ which shows that $\mathcal{F}(\pi_i[X])\bar{\mathfrak{w}}$ is a permutation polynomial vector of G_i^k since $\bar{\mathfrak{w}}$ is a permutation polynomial vector of G^k. Hence

$$\mathcal{F}(\vartheta_i)\,\mathcal{F}(\pi_i[X])\,\bar{\mathfrak{w}}\in\mathcal{E}\big(\mathcal{F}\big(G_{i0}(X)|\ker\sigma_k(G_i)\big)\big).$$

Moreover $\mathcal{F}(\lambda_k(G_i))\,\mathcal{F}(\pi_i[X])\,\bar{\mathfrak{w}} = \mathcal{F}(\lambda_k(G))\,\bar{\mathfrak{w}} = \mathfrak{x}$, hence

$$\mathcal{F}(\pi_i[X])\,\bar{\mathfrak{w}}\mathfrak{x}^{-1}\in\mathcal{F}\big(\ker\sigma_k(G_i)\,(G_{i0}(X)\cap\ker\lambda_k(G_i))\big).$$

Therefore $\mathcal{F}(\vartheta_i)\,\mathcal{F}(\pi_i[X])\,\bar{\mathfrak{w}}\in\ker\mathcal{E}(\mathcal{F}(\mu_{G_i}))$. Furthermore

$$\begin{aligned}\varphi\big(\mathcal{F}(\vartheta_1)\,\mathcal{F}(\pi_1[X])\,\bar{\mathfrak{w}},\ \mathcal{F}(\vartheta_2)\,\mathcal{F}(\pi_2[X])\,\bar{\mathfrak{w}}\big) &= \\ = \mathcal{F}(\vartheta)\,\big(\mathcal{F}(\iota_1[X])\,\mathcal{F}(\pi_1[X])\,\bar{\mathfrak{w}}\big)\,\mathfrak{x}^{-1}(\mathcal{F}(\iota_2[X])\,\mathcal{F}(\pi_2[X])\,\bar{\mathfrak{w}}).&\end{aligned}$$

Again, if $\mathfrak{g}\in\mathcal{F}(G)$, $\psi\mathfrak{g} = (\mathfrak{a}, \mathfrak{b})$, then

$$\begin{aligned}\psi\big(\mathcal{F}(\iota_1[X])\,\mathcal{F}(\pi_1[X])\,\bar{\mathfrak{w}}\mathfrak{x}^{-1}\mathcal{F}(\iota_2[X])\,\mathcal{F}(\pi_2[X])\,\bar{\mathfrak{w}}\circ\bar{\mathfrak{x}}\big) &= \\ = \big(\mathcal{F}(\pi_1[X])\,\bar{\mathfrak{w}}\circ\mathfrak{a},\ \mathcal{F}(\pi_2[X])\,\bar{\mathfrak{w}}\circ\mathfrak{b}\big) = \psi(\bar{\mathfrak{w}}\circ\bar{\mathfrak{g}})&\end{aligned}$$

hence

$$\varphi\big(\mathcal{F}(\vartheta_1)\,\mathcal{F}(\pi_1[X])\,\bar{\mathfrak{w}},\ \mathcal{F}(\vartheta_2)\,\mathcal{F}(\pi_2[X])\,\bar{\mathfrak{w}}\big) = \mathcal{F}(\vartheta)\,\bar{\mathfrak{w}} = \mathfrak{w}.$$

Hence φ is also surjective, that means φ is bijective. Let $\mathfrak{w}_1, \mathfrak{w}_2\in\ker\mathcal{E}(\mathcal{F}(\mu_G))$ and $\bar{\mathfrak{w}}_1$, $\bar{\mathfrak{w}}_2$ counterimages under $\mathcal{F}(\vartheta)$ as before. Then $\bar{\mathfrak{w}}_1\circ\bar{\mathfrak{w}}_2\in\mathfrak{x}\mathcal{F}(G_0(X)\cap\ker\lambda_k(G))$ since $G_0(X)\cap\ker\lambda_k(G)$ is a full ideal of $G_0(X)$. As $\pi_i[X]$ and ϑ_i are composition epimorphisms, we obtain

$$\begin{aligned}\varphi^{-1}(\mathfrak{w}_1\circ\mathfrak{w}_2) &= \big(\mathcal{F}(\vartheta_1)\,\mathcal{F}(\pi_1[X])\,(\bar{\mathfrak{w}}_1\circ\bar{\mathfrak{w}}_2),\ \mathcal{F}(\vartheta_2)\,\mathcal{F}(\pi_2[X])\,(\bar{\mathfrak{w}}_1\circ\bar{\mathfrak{w}}_2)\big) \\ &= \big(\mathcal{F}(\vartheta_1)\,\mathcal{F}(\pi_1[X])\,\bar{\mathfrak{w}}_1,\ \mathcal{F}(\vartheta_2)\,\mathcal{F}(\pi_2[X])\,\bar{\mathfrak{w}}_1\big) \\ &\quad\circ\big(\mathcal{F}(\vartheta_1)\,\mathcal{F}(\pi_1[X])\,\bar{\mathfrak{w}}_2,\ \mathcal{F}(\vartheta_2)\,\mathcal{F}(\pi_2[X])\,\bar{\mathfrak{w}}_2\big) \\ &= (\varphi^{-1}\mathfrak{w}_1)\circ(\varphi^{-1}\mathfrak{w}_2).\end{aligned}$$

Hence φ^{-1} is an isomorphism and so is φ.

3.3. Theorem. *Let G be a finite group, $\eta: G \to H$ an epimorphism, and $P_k(\eta): P_k(G) \to P_k(H)$ the extension to a composition epimorphism. Then $\mathcal{F}(P_k(\eta))\, U_k(G) = U_k(H)$.*

Proof. By ch. 3, Prop. 11.51, $\mathcal{F}(P_k(\eta))\, U_k(G) \subseteq U_k(H)$. Let $\mathfrak{n} = (1, 1, \ldots, 1) \in G^k$ and $\mathfrak{y} = (\xi_1, \ldots, \xi_k) \in P_k(G)$. By definition, $\bar{P}_k(G, G) = \{\varphi \in P_k(G) \mid \varphi\mathfrak{n} = 1\}$ whence $P_k(\eta)\, \bar{P}_k(G, G) \subseteq \bar{P}_k(H, H)$. Conversely, if $\psi \in \bar{P}_k(H, H)$ and $\chi \in P_k(G)$ such that $P_k(\eta)\, \chi = \psi$, then $\eta(\chi\mathfrak{n}) = \psi\mathfrak{n} = 1$. Thus $(\chi\mathfrak{n})^{-1}\chi \in \bar{P}_k(G, G)$ and $P_k(\eta)\,((\chi\mathfrak{n})^{-1}\chi) = \eta(\chi\mathfrak{n})^{-1} P_k(\eta)\, \chi = \psi$. Hence $P_k(\eta)\, \bar{P}_k(G, G) = \bar{P}_k(H, H)$, therefore $\mathcal{F}(P_k(\eta))\, \mathcal{F}(\bar{P}_k(G, G)) = \mathcal{F}(\bar{P}_k(H, H))$. By § 2.2 and § 3.1, $\bar{P}_k(G, G)$ is a d.g. composition subgroup of $P_k(G)$ containing the selector system of $P_k(G)$, hence by Prop. 2.11, $\mathcal{F}(\bar{P}_k(G, G))$ is a d.g. subnear-ring of $\mathcal{F}(P_k(G))$ containing the identity of $\mathcal{F}(P_k(G))$ which shows that $\mathcal{E}(\mathcal{F}(\bar{P}_k(G, G))) \subseteq \mathcal{E}(\mathcal{F}(P_k(G))) = U_k(G)$ since G is finite. Clearly $\mathcal{F}(\bar{P}_k(G, G))$ is also finite, therefore a result of LAUSCH (ch. 6, Prop. 8.51) implies that $\mathcal{F}(P_k(\eta))\, \mathcal{E}(\mathcal{F}(\bar{P}_k(G, G))) = \mathcal{E}(\mathcal{F}(\bar{P}_k(H, H)))$. Hence $\mathcal{F}(P_k(\eta))\, U_k(G) \supseteq \mathcal{E}(\mathcal{F}(\bar{P}_k(H, H))) = \{\mathfrak{f} \in U_k(H) \mid \mathfrak{f} \circ \mathfrak{n} = \mathfrak{n}\}$. Moreover $\mathcal{F}(P_k(\eta))\, U_k(G) \supseteq \{\mathfrak{h}\mathfrak{y} \mid \mathfrak{h} \in H^k\}$. But for any $\mathfrak{f} \in U_k(H)$, we have $\mathfrak{f} = (\mathfrak{f} \circ \mathfrak{n})\, \mathfrak{y} \circ (\mathfrak{f} \circ \mathfrak{n})^{-1}\mathfrak{f}$, thus $\mathcal{F}(P_k(\eta))\, U_k(G) \supseteq U_k(H)$.

3.31. Theorem. *Let G_1, G_2 be two finite groups and $G = G_1 \times G_2$. Then the decomposition homomorphism $\psi_2\mathcal{F}(\tau_2)$ for $P_k(G)$ maps $U_k(G)$ isomorphically onto $U_k(G_1) \times U_k(G_2)$ if and only if either $L_k(G_1)\, L_k(G_2) = F(X)$, or $k = 1$ and $L_1(G_1)\, L_1(G_2) = [x^2]$.*

Proof. By ch. 3, Prop. 11.61, $\psi_2\mathcal{F}(\tau_2)$ maps $U_k(G)$ monomorphically to $U_k(G_1) \times U_k(G_2)$, hence also surjectively if and only if $|U_k(G_1)|\,|U_k(G_2)| = |U_k(G)|$. But, for any group G, $\mathfrak{f} \in U_k(G)$ has a unique representation $\mathfrak{f} = \mathfrak{h}\mathfrak{y} \circ \mathfrak{g}$ where $\mathfrak{h} \in G^k$ and $\mathfrak{g} \in \mathcal{F}(\bar{P}_k(G, G)) \cap U_k(G) = \mathcal{E}(\mathcal{F}(\bar{P}_k(G, G)))$, and any such element belongs to $U_k(G)$. Hence

$$|U_k(G)| = |G^k|\,|\mathcal{E}(\mathcal{F}(\bar{P}_k(G, G)))| = |G|^k\,|\mathcal{E}(\mathcal{F}(G_0(X) \mid \ker \sigma_k(G)))|$$

by § 3.1. Thus $\psi_2\mathcal{F}(\tau_2)$ acts surjectively on $U_k(G)$ if and only if

$$|\mathcal{E}(\mathcal{F}(G_0(X) \mid \ker \sigma_k(G)))| = \prod_{i=1}^{2} |\mathcal{E}(\mathcal{F}(G_{i0}(X) \mid \ker \sigma_k(G_i)))|$$

and this is, by Prop. 3.2, equivalent to

$$|\mathcal{E}(\mathcal{F}(\mu_G))\, \mathcal{E}(\mathcal{F}(G_0(X) \mid \ker \sigma_k(G)))| = \prod_{i=1}^{2} |\mathcal{E}(\mathcal{F}(\mu_{G_i}))\, \mathcal{E}(\mathcal{F}(G_{i0}(X) \mid \ker \sigma_k(G_i)))|.$$

For an arbitrary group G, we have $\ker \sigma_k(G) \subseteq G_0(X)$, therefore $\ker \sigma_k(G)\,(G_0(X) \cap \ker \lambda_k(G)) = G_0(X) \cap \ker \sigma_k(G) \ker \lambda_k(G)$. By the first isomorphism theorem of group theory and Prop. 1.13,

$$G_0(X) \mid \ker \sigma_k(G)(G_0(X) \cap \ker \lambda_k(G)) \cong$$
$$\cong G_0(X) \ker \sigma_k(G) \ker \lambda_k(G) \mid \ker \sigma_k(G) \ker \lambda_k(G) \cong F(X) \mid L_k(G)$$

since $G_0(X) \ker \lambda_k(G) = G[X]$. Since $\ker \sigma_k(G)$ and $\ker \lambda_k(G)$ are full ideals of $G[X]$ and $L_k(G) = \lambda_k(G) \ker \sigma_k(G)$ is a full ideal of $F(X)$, and the isomorphism theorems also hold for ideals of multi-operator groups, this isomorphism is a composition isomorphism. Hence our last condition is satisfied if and only if $|\mathcal{E}(\mathcal{F}(F(X) \mid L_k(G)))| = \prod_{i=1}^{2} |\mathcal{E}(\mathcal{F}(F(X) \mid L_k(G_i)))|$. If $w \in F(X)$, $\tilde{w}$ will denote the coset $wL_k(G)$. We define a mapping $\vartheta: \operatorname{Aut}(F(X) \mid L_k(G)) \to \mathcal{F}(F(X) \mid L_k(G))$ by $\vartheta\alpha = (\alpha\tilde{x}_1, \ldots, \alpha\tilde{x}_k)$. Certainly ϑ is injective. Moreover $\vartheta(\alpha\beta) = (\alpha(\beta\tilde{x}_1), \ldots, \alpha(\beta\tilde{x}_k)) = (\beta\tilde{x}_1 \circ (\alpha\tilde{x}_1, \ldots, \alpha\tilde{x}_k), \ldots, \beta\tilde{x}_k \circ (\alpha\tilde{x}_1, \ldots, \alpha\tilde{x}_k)) = \vartheta\beta \circ \vartheta\alpha$ and if ε denotes the identical automorphism, then $\vartheta\varepsilon = (\tilde{x}_1, \ldots, \tilde{x}_k)$. Hence $\vartheta\alpha \in \mathcal{E}(\mathcal{F}(F(X) \mid L_k(G)))$. Conversely if $(w_1(\tilde{x}_1, \ldots, \tilde{x}_k), \ldots, w_k(\tilde{x}_1, \ldots, \tilde{x}_k)) \in \mathcal{E}(\mathcal{F}(F(X) \mid L_k(G)))$, then the mapping α: $F(X) \mid L_k(G) \to F(X) \mid L_k(G)$ defined by $\alpha(w(\tilde{x}_1, \ldots, \tilde{x}_k)) = w(w_1(\tilde{x}_1, \ldots, \tilde{x}_k), \ldots, w_k(\tilde{x}_1, \ldots, \tilde{x}_k))$ is a well-defined automorphism. Thus ϑ maps $\operatorname{Aut} F(X) \mid L_k(G)$ bijectively onto $\mathcal{E}(\mathcal{F}(F(X) \mid L_k(G)))$ and our last condition is equivalent to

$$|\operatorname{Aut} F(X) \mid L_k(G)| = \prod_{i=1}^{2} |\operatorname{Aut} F(X) \mid L_k(G_i)|. \tag{3.3}$$

We set $wL_k(G_i) = {}_i\tilde{w}$, $i = 1, 2$. Let ϑ_i be the mapping we obtain from ϑ by replacing G by G_i. Since, by Prop. 1.2, $L_k(G) = L_k(G_1) \cap L_k(G_2)$, the mapping $\zeta: F(X) \mid L_k(G) \to F(X) \mid L_k(G_1) \times F(X) \mid L_k(G_2)$ defined by $\zeta\tilde{w} = ({}_1\tilde{w}, {}_2\tilde{w})$ is certainly a composition monomorphism. Thus $\mathcal{F}(\zeta)$: $\mathcal{F}(F(X) \mid L_k(G)) \to \mathcal{F}(F(X) \mid L_k(G_1) \times F(X) \mid L_k(G_2))$ is a composition monomorphism. Hence there exists a composition monomorphism $\eta: \mathcal{F}(F(X) \mid L_k(G)) \to \mathcal{F}(F(X) \mid L_k(G_1)) \times \mathcal{F}(F(X) \mid L_k(G_2))$ which maps the identity w.r.t. the composition of the first algebra to the identity w.r.t. the composition of the second one and therefore $\mathcal{E}(\mathcal{F}(F(X) \mid L_k(G)))$ into $\mathcal{E}(\mathcal{F}(F(X) \mid L_k(G_1))) \times \mathcal{E}(\mathcal{F}(F(X) \mid L_k(G_2)))$. If $\alpha \in \operatorname{Aut} F(X) \mid L_k(G)$ and $\eta\vartheta\alpha = (\mathfrak{u}_1, \mathfrak{u}_2)$, then we set $\varkappa\alpha = (\vartheta_1^{-1}\mathfrak{u}_1, \vartheta_2^{-1}\mathfrak{u}_2)$. Thus $\varkappa: \operatorname{Aut} F(X) \mid L_k(G) \to \operatorname{Aut} F(X) \mid L_k(G_1) \times \operatorname{Aut} F(X) \mid L_k(G_2)$ is a monomorphism.

Suppose now that (3.3) is satisfied, then $\varkappa$ is an isomorphism. The k-generator group $G = F(X)|L_k(G)$ has normal subgroups $N_i = L_k(G_i)|L_k(G)$, $i = 1, 2$, which satisfy $N_1 \cap N_2 = 1$. Let ${}_i\tilde{w}_{i1}, \ldots, {}_i\tilde{w}_{ik}$ be a generating set for $F(X)|L_k(G_i)$. Since $L_k(G_i)$ is a full ideal of $F(X)$ and $F(X)|L_k(G_i)$ is finite by Prop. 1.13, there exists $\alpha_i \in \operatorname{Aut} F(X)|L_k(G_i)$ such that $\alpha_i\, {}_i\tilde{x}_j = {}_i\tilde{w}_{ij}$, $j = 1, \ldots, k$. Set $\alpha = \varkappa^{-1}(\alpha_1, \alpha_2)$. Then $\eta\vartheta\alpha = (\vartheta_1\alpha_1, \vartheta_2\alpha_2)$. Set $\vartheta\alpha = (\tilde{v}_1, \ldots, \tilde{v}_k)$, then this is a generating set of $F(X)|L_k(G)$, and ${}_i\tilde{v}_j = {}_i\tilde{w}_{ij}$, $j = 1, \ldots, k$. Hence $\tilde{v}_j \subseteq {}_1\tilde{w}_{1j} \cap {}_2\tilde{w}_{2j}$, i.e. $v_j L_k(G) \subseteq w_{1j} L_k(G_1) \cap w_{2j} L_k(G_2)$. Therefore the hypothesis of ch. 6, Lemma 6.9 is satisfied. The lemma implies that either $F(X)|L_k(G) = L_k(G_1)\,|\,L_k(G) \times L_k(G_2)|L_k(G)$ i.e. $F(X) = L_k(G_1)L_k(G_2)$, or $|F(X)\,|\,L_k(G_1)L_k(G_2)| = 2$. Since $L_k(G_1)L_k(G_2) = V$ is a full ideal, in the second case $x_i \notin V$, thus if $k > 1$, we would have $x_2 x_1^{-1} \in V$ whence $x_1 \in V$, contradiction. Therefore $k = 1$ and $L_1(G_1)L_1(G_2) = [x^2]$.

Conversely let $L_k(G_1)L_k(G_2) = F(X)$. Then by Cor. 1.22, the decomposition homomorphism τ_2 of $P_k(G)$ is an isomorphism, and by ch. 3, § 11.3, $\psi_2\mathcal{F}(\tau_2)$ is an isomorphism. If, however, $k = 1$ and $L_1(G_1)L_1(G_2) = [x^2]$, then let $L_1(G_1) = [x^{l_1}]$ and $L_1(G_2) = [x^{l_2}]$. It follows $(l_1, l_2) = 2$. $L_1(G) = L_1(G_1) \cap L_1(G_2)$ implies $L_1(G) = [x^l]$ where l is the least common multiple of l_1 and l_2. Since $|\operatorname{Aut} F(x)\,|\,[x^n]| = \varphi(n)$, φ being Euler's φ-function, (3.3) holds if $\varphi(l) = \varphi(l_1)\varphi(l_2)$. WLOG, assume that $l_1 = 2n_1$, $l_2 = 2^r n_2$, $r \geqslant 1$, n_1, n_2 odd positive integers, $(n_1, n_2) = 1$. Thus $l = 2^r n_1 n_2$, hence $\varphi(l) = 2^{r-1}\varphi(n_1)\varphi(n_2) = \varphi(l_1)\varphi(l_2)$ as required.

3.32. Corollary. *If G_1, G_2 are two finite groups and $(|G_1|, |G_2|) = 1$, then $\psi_2\mathcal{F}(\tau_2)$ maps $U_k(G_1 \times G_2)$ isomorphically onto $U_k(G_1) \times U_k(G_2)$.*

Proof. $(|G_1|, |G_2|) = 1$ implies $L_k(G_1)L_k(G_2) = F(X)$.

4. Further results on the group of polynomial permutations over a finite group

4.1. Let G be a finite group and $U_k(G)$ the group of its k-dimensional polynomial permutations which, by § 3.1, coincides with the group of units of the near-ring $\mathcal{F}(P_k(G))$. This section is devoted to various structural properties of $U_k(G)$. Since $\mathcal{F}(P_k(G))$ is, in general, not a d.g. near-ring, but $\mathcal{F}(\bar{P}_k(G, G))$ is, by Remark 2.41, it is of advantage to investigate first of all the group $\bar{U}_k(G) = \mathcal{E}(\mathcal{F}(\bar{P}_k(G, G))) = U_k(G) \cap \mathcal{F}(\bar{P}_k(G, G))$ in order to utilize some results of ch. 6 on d.g. near-rings.

4.11. Theorem. *Let $|G| \neq 1$. If $\bar{U}_k(G)$ is soluble, then G is soluble and either*

(i) *$k = 1$ and, for every chief factor $H|K$ of G, the group $\operatorname{Aut}_G(H|K)$ of automorphisms of $H|K$ induced by the inner automorphisms of G is abelian or $|H|K| = 4$ or 9, or*

(ii) *$k = 2$ and G is a supersoluble (2, 3)-group.*

Proof. Let $\bar{U}_k(G)$ be soluble. Since the mapping $\gamma: G \to \bar{U}_k(G)$ defined by $\gamma g = (g^{\xi_1} g^{-1}, \ldots, g^{\xi_k} g^{-1})$ is a homomorphism with $\ker \gamma = Z(G)$, the centre of G, $G|Z(G)$ is soluble and so is G. Let $H|K$ be a chief factor of G, then $H|K$ is a p-chief factor, for some prime p. One checks easily that $(H|K)^k$ is an $\mathcal{F}(\bar{P}_k(G, G))$-group in the sense of ch. 6, § 8, where the rôle of S is taken by the set of elements $(1, 1, \ldots, g^{-1}\xi_j g, \ldots, 1)$ and the action of $\mathcal{F}(\bar{P}_k(G, G))$ on $(H|K)^k$ is defined by

$$(\varphi_1, \ldots, \varphi_k) \circ (h_1 K, \ldots, h_k K) = (\varphi_1(h_1, \ldots, h_k)K, \ldots, \varphi_k(h_1, \ldots, h_k)K).$$

$(H|K)^k$ is even a minimal $\mathcal{F}(\bar{P}_k(G, G))$-group since $\mathcal{F}(\bar{P}_k(G, G))$ contains all the elements of the form $(1, 1, \ldots, \xi_j, \ldots, 1)$. The mapping $\sigma: \mathcal{F}(\bar{P}_k(G, G)) \to F_1((H|K)^k)$ defined by $(\sigma\mathfrak{f}) \circ \mathfrak{h} = \mathfrak{f} \circ \mathfrak{h}$, $\mathfrak{f} \in \mathcal{F}(\bar{P}_k(G, G))$, $\mathfrak{h} \in (H|K)^k$ is a near-ring homomorphism whence $\ker \sigma$ is a full ideal of $\mathcal{F}(\bar{P}_k(G, G))$. With the notation of § 2.3 and the result therein, we find that, for any $\varphi \in \bar{P}_k(G, G)$,

$$\varphi(h_1, \ldots, h_k)K = \sum_{j=1}^{k} \Big(\sum \alpha_{ij}(g_i K) \,|\, g_i K \in G|K\Big) h_j K.$$

Hence as in § 2.3, $\sigma\mathcal{F}(\bar{P}_k(G, G))$ is isomorphic to the full $k \times k$-matrix ring over $K_p(G|K)\,|\,\mathrm{An}(H|K)$ where K_p denotes the field of p elements. But by § 2.3, $K_p(G|K)\,|\,\mathrm{An}(H|K)$ is a simple ring, thus is isomorphic to some full matrix ring of degree m over some finite field L containing K_p. Therefore $\sigma\mathcal{F}(\bar{P}_k(G, G))$ is isomorphic to the full matrix-ring L_{km} of degree km over the finite field L of characteristic p.

By ch. 6, Prop. 8.51, $\sigma\mathcal{E}(\mathcal{F}(\bar{P}_k(G, G))) = \mathcal{E}(\sigma\mathcal{F}(\bar{P}_k(G, G))) \cong \mathcal{E}(L_{km})$. Since $\bar{U}_k(G)$ is soluble, also $\mathcal{E}(L_{km})$ is soluble. By a well-known result on linear groups this is the case only if either (i) $km = 1$, or (ii) $km = 2$, $p = 2$ or 3 and $L = K_p$.

(i) $km = 1$ implies $k = 1$ and $m = 1$. Hence $K_p(G|K)\,|\,\mathrm{An}(H|K) \cong L$. Since $\operatorname{Aut}_G(H|K)$ is isomorphic to a subgroup of the multiplicative semigroup of $K_p(G|K)\,|\,\mathrm{An}(H|K)$, it is cyclic, therefore abelian.

(ii) $km = 2$. Case 1: $k = 1$, $m = 2$. By our previous results, $K_p(G|K)|\mathrm{An}(H|K)$ is isomorphic to the full matrix ring R_2 of degree 2 over K_p. Hence $H|K$ is a faithful irreducible R_2-module. By ch. 6, § 74, this implies that $H|K$ is a vector space of dimension 2 over K_p. Hence $|H|K| = 4$ or 9, since p must be 2 or 3. Case 2: $k = 2$, $m = 1$. The same argument as in Case 1 shows that $\dim_{K_p}(H|K) = 1$ whence $|H|K| = 2$ or 3. In either case $k = 1$ or 2. If $k = 1$, then condition (i) of Th. 4.11 is satisfied while if $k = 2$, then every chief factor of G has order 2 or 3 whence G is a supersoluble (2, 3)-group.

4.12. Theorem. *If G is soluble and either* (i) *or* (ii) *of Th.* 4.11 *is satisfied, then $U_k(G)$ is soluble.*

Proof. By induction on $|G|$. If $|G| = 1$, then $|U_k(G)| = 1$, hence $U_k(G)$ is soluble. Let N be a minimal normal subgroup of G, then the canonical epimorphism $\eta : G \to G|N$ induces an epimorphism $\mathcal{F}(P_k|(\eta)) = U_k(\eta) : U_k(G) \to U_k(G|N)$. Since $G|N$ also satisfies (i) or (ii), $U_k(G|N)$ is soluble by induction, and it remains to show that $\ker U_k(\eta)$ is soluble.

Now $\ker U_k(\eta) = \{\mathfrak{u} \in U_k(G) | \mathfrak{g}^{-1}(\mathfrak{u} \circ \mathfrak{g}) \in N^k$, for all $\mathfrak{g} \in G^k\}$, thus $\mathfrak{u} \circ \mathfrak{g} = \mathfrak{g}\mathfrak{n}(\mathfrak{u}, \mathfrak{g})$, $\mathfrak{n}(\mathfrak{u}, \mathfrak{g}) \in N^k$. Furthermore, for any $\mathfrak{n} \in N^k$, $\mathfrak{g} \in G^k$, we have $\mathfrak{u} \circ (\mathfrak{g}\mathfrak{n}) = (\mathfrak{u} \circ \mathfrak{g})\tau(\mathfrak{u}, \mathfrak{g})\mathfrak{n}$ where $\tau(\mathfrak{u}, \mathfrak{g})$ is some endomorphism of N^k. Moreover $\tau(\mathfrak{u}, \mathfrak{g})$ is bijective, and $\varphi = a_1\xi_{i_1}a_2\xi_{i_2} \ldots a_s\xi_{i_s}a_{s+1} \in P_k(G)$ implies $\varphi(g_1n_1, \ldots, g_kn_k) = a_1g_{i_1}a_2g_{i_2} \ldots a_sg_{i_s}a_{s+1}(a_2g_{i_2} \ldots a_sg_{i_s}a_{s+1})^{-1}$ $n_{i_1}(a_2g_{i_2} \ldots a_sg_{i_s}a_{s+1})(a_3g_{i_3} \ldots a_sg_{i_s}a_{s+1})^{-1} \ldots$, hence $(\varphi \circ \mathfrak{g})^{-1}(\varphi \circ \mathfrak{g}\mathfrak{n}_1\mathfrak{n}_2) = (\varphi \circ \mathfrak{g})^{-1}(\varphi \circ \mathfrak{g}\mathfrak{n}_1)(\varphi \circ \mathfrak{g})^{-1}(\varphi \circ \mathfrak{g}\mathfrak{n}_2)$ since N is abelian. Therefore $\mathfrak{u} \circ (\mathfrak{g}\mathfrak{n}) = \mathfrak{g}\mathfrak{n}(\mathfrak{u}, \mathfrak{g})\tau(\mathfrak{u}, \mathfrak{g})\mathfrak{n}$, for all $\mathfrak{u} \in \ker U_k(\eta)$. For each $\mathfrak{g} \in G^k$, we obtain some mapping $\delta(\mathfrak{g}) : \ker U_k(\eta) \to \mathrm{Sym}\, N^k$, the symmetric group of N^k, defined by $(\delta(\mathfrak{g})\mathfrak{u})\mathfrak{n} = \mathfrak{n}(\mathfrak{u}, \mathfrak{g})\tau(\mathfrak{u}, \mathfrak{g})\mathfrak{n}$ since $\mathfrak{u} \in U_k(G)$. Moreover $\mathfrak{g}(\delta(\mathfrak{g})(\mathfrak{u}_1 \circ \mathfrak{u}_2))\mathfrak{n} = (\mathfrak{u}_1 \circ \mathfrak{u}_2) \circ (\mathfrak{g}\mathfrak{n}) = \mathfrak{u}_1 \circ (\mathfrak{g}(\delta(\mathfrak{g})\mathfrak{u}_2)\mathfrak{n}) = \mathfrak{g}(\delta(\mathfrak{g})\mathfrak{u}_1) \cdot (\delta(\mathfrak{g})\mathfrak{u}_2)\mathfrak{n} = \mathfrak{g}(\delta(\mathfrak{g})\mathfrak{u}_1 \circ \delta(\mathfrak{g})\mathfrak{u}_2)\mathfrak{n}$ hence $\delta(\mathfrak{g})(\mathfrak{u}_1 \circ \mathfrak{u}_2) = \delta(\mathfrak{g})\mathfrak{u}_1 \circ \delta(\mathfrak{g})\mathfrak{u}_2$. Therefore $\delta(\mathfrak{g})$ is a homomorphism. Furthermore $|\bigcap(\ker \delta(\mathfrak{g}) | \mathfrak{g} \in G^k)| = 1$ whence $\ker U_k(\eta)$ can be embedded into the direct product of all $\delta(\mathfrak{g}) \ker U_k(\eta)$. All that remains is to show that $\delta(\mathfrak{g}) \ker U_k(\eta)$ is soluble, for all $\mathfrak{g} \in G^k$. We choose $\mathfrak{g} \in G^k$ arbitrary and define $\varphi : \delta(\mathfrak{g}) \ker U_k(\eta) \to \mathrm{Aut}\, N^k$ by $\varphi(\delta(\mathfrak{g})\mathfrak{u}) = \tau(\mathfrak{u}, \mathfrak{g})$. This is a well-defined mapping, for if $\delta(\mathfrak{g})\mathfrak{u} = \delta(\mathfrak{g})\mathfrak{v}$, then $(\delta(\mathfrak{g})\mathfrak{u})\mathfrak{e} = (\delta(\mathfrak{g})\mathfrak{v})\mathfrak{e}$, $\mathfrak{e} = (1, 1, \ldots, 1) \in N^k$. Hence $\mathfrak{n}(\mathfrak{u}, \mathfrak{g}) = \mathfrak{n}(\mathfrak{v}, \mathfrak{g})$, thus $\tau(\mathfrak{u}, \mathfrak{g}) = \tau(\mathfrak{v}, \mathfrak{g})$. Moreover $\mathfrak{n}(\mathfrak{u} \circ \mathfrak{v}, \mathfrak{g})\tau(\mathfrak{u} \circ \mathfrak{v}, \mathfrak{g})\mathfrak{n} = (\delta(\mathfrak{g})\mathfrak{u} \circ \delta(\mathfrak{g})\mathfrak{v})\mathfrak{n} = (\delta(\mathfrak{g})\mathfrak{u})\,\mathfrak{n}(\mathfrak{v}, \mathfrak{g})\tau(\mathfrak{v}, \mathfrak{g})\mathfrak{n} = \mathfrak{n}(\mathfrak{u}, \mathfrak{g})\tau(\mathfrak{u}, \mathfrak{g})\,\mathfrak{n}(\mathfrak{v}, \mathfrak{g})\,(\tau(\mathfrak{u}, \mathfrak{g}) \circ \tau(\mathfrak{v}, \mathfrak{g}))\mathfrak{n}$. If we set $\mathfrak{n} = \mathfrak{e}$, then the first factors cancel and $\tau(\mathfrak{u} \circ \mathfrak{v}, \mathfrak{g}) = \tau(\mathfrak{u}, \mathfrak{g}) \circ \tau(\mathfrak{v}, \mathfrak{g})$. Hence φ is a homomorphism. If $\delta(\mathfrak{g})\mathfrak{u} \in \ker \varphi$, then $(\delta(\mathfrak{g})\mathfrak{u})\mathfrak{n} = \mathfrak{n}(\mathfrak{u}, \mathfrak{g})\mathfrak{n}$, hence $\ker \varphi$ is isomorphic to some subgroup of N^k and therefore soluble. But $\varphi\delta(\mathfrak{g}) \ker U_k(\eta)$ is a subgroup of $\mathrm{Aut}\, N^k$. If (ii) holds or (i) holds and $|N| = 4$ or 9, then $\mathrm{Aut}\, N^k$ is isomorphic to GL(2, 2) or GL(2, 3) which is soluble. If, however, $k = 1$, and $\mathrm{Aut}_G N$ is abelian, then any two elements $\tau(\mathfrak{u}, \mathfrak{g})$ commute since every $\tau(\mathfrak{u}, \mathfrak{g})$ in the endomorphism ring of N can be written as a sum of elements of $\mathrm{Aut}_G N$, and again $\varphi\delta(\mathfrak{g}) \ker U_k(\eta)$ is soluble.

4.13. Corollary. *If G is a finite group, then $U_k(G)$ is soluble if and only if G is soluble and either*

(i) *$k = 1$ and, for every chief factor $H|K$ of G, $\mathrm{Aut}_G(H|K)$ is abelian, or $|H|K| = 4$ or 9; or*

(ii) *$k = 2$ and G is a supersoluble (2, 3)-group; or*

(iii) $|G| = 1$.

4.2. Proposition. *If G is a finite group, then the radical J of $\mathcal{F}(\bar{P}_k(G, G))$ is nilpotent.*

Proof. Let $H|K$ be a chief factor of G, then as in the proof of Th. 4.11, $(H|K)^k$ is a minimal $\mathcal{F}(\bar{P}_k(G, G))$-group. If $\mathfrak{f} \in J$, then by definition of J, $\mathfrak{f}$ annihilates $(H|K)^k$, i.e. $\mathfrak{f} \circ (h_1, \ldots, h_k) \in K^k$ for all $(h_1, \ldots, h_k) \in H^k$. Hence if l is the chief series length of G, then J^l consists of the zero mapping only (i.e. the mapping where every element has the image $(1,1 \ldots, 1)$. Thus J is nilpotent.

4.21. Proposition. *Every minimal $\mathcal{F}(\bar{P}_k(G, G))$-group is $\mathcal{F}(\bar{P}_k(G, G))$-isomorphic to some $H^k|K^k$ where $H|K$ is some chief factor of G.*

Proof. By ch. 6, Prop. 8.43, every minimal $\mathcal{F}(\bar{P}_k(G, G))$-group is isomorphic to some $\mathcal{F}(\bar{P}_k(G, G))\mathfrak{i}|J\mathfrak{i}$, for some idempotent $\mathfrak{i} \in \mathcal{F}(\bar{P}_k(G, G))$ where $\mathfrak{i}$ is non-zero, since J is nilpotent by Prop. 4.2. But $\mathfrak{i}$ cannot annihilate $H^k|K^k$, for every chief factor $H|K$ of G, otherwise $\mathfrak{i}$ is the zero mapping. So we can choose some chief factor $H|K$ such that $\mathfrak{i}(H^k|K^k) \neq K^k$. Hence there exists $m \in H^k|K^k$ with $(\mathcal{F}(\bar{P}_k(G, G))\mathfrak{i})m \neq K^k$. Since $(\mathcal{F}(\bar{P}_k(G, G))\mathfrak{i})m$ is also an $\mathcal{F}(\bar{P}_k(G, G))$-group, the minimality of $H^k|K^k$ implies $(\mathcal{F}(\bar{P}_k(G, G))\mathfrak{i})m = H^k|K^k$. The mapping

$\mathfrak{f}\mathfrak{i} \to (\mathfrak{f}\mathfrak{i})m$, $\mathfrak{f} \in \mathcal{F}(\bar{P}_k(G, G))$ is an $\mathcal{F}(\bar{P}_k(G, G))$-homomorphism from $\mathcal{F}(\bar{P}_k(G, G))\mathfrak{i}$ to $H^k | K^k$ and is surjective, and its kernel contains $J\mathfrak{i}$, by ch. 6, Prop. 8.43. Hence, by the minimality of $\mathcal{F}(\bar{P}_k(G, G))\mathfrak{i}|J\mathfrak{i}$, the kernel equals $J\mathfrak{i}$. Therefore $\mathcal{F}(\bar{P}_k(G, G))\mathfrak{i}\,|\,J\mathfrak{i} \cong H^k | K^k$.

4.22. Corollary. *With the notation of ch. 6, § 8, $J = \bigcap \mathfrak{l}_{\mathcal{F}(\bar{P}_k(G, G))}(H^k | K^k)$, the intersection being taken over a full set of pairwise non-$\mathcal{F}(\bar{P}_k(G, G))$-isomorphic factors $H^k | K^k$ where $H | K$ are chief factors of G.*

4.3. Proposition. *Let G be any finite abelian group. Then $U_k(G)$ is isomorphic to a semidirect product of G^k by a group isomorphic to $\mathcal{L}(M(k, \exp G))$ where $M(k, \exp G)$ denotes the ring of $k \times k$-matrices over the integers modulo $\exp G$.*

Proof. Every $\varphi \in \mathcal{F}(\bar{P}_k(G, G))$ can be written uniquely as $\varphi = (\xi_1^{a_{11}} \dots \xi_k^{a_{1k}}, \dots, \xi_1^{a_{k1}} \dots \xi_k^{a_{kk}})$ where a_{ij} is an integer, $0 \leqslant a_{ij} < \exp G$, and it is evident that $\vartheta : \mathcal{F}(\bar{P}_k(G, G)) \to M(k, \exp G)$ defined by $\vartheta\varphi = (a_{ij} \bmod \exp G)$ is an isomorphism from the multiplicative semigroup of $\mathcal{F}(\bar{P}_k(G, G))$ to the multiplicative semigroup of $M(k, \exp G)$. Hence $\bar{U}_k(G) = \mathcal{L}(\mathcal{F}(\bar{P}_k(G, G))) \cong \mathcal{L}(M(k, \exp G))$. If we set $\mathfrak{x} = (\xi_1, \dots, \xi_k)$ then for any $\varphi \in \bar{U}_k(G)$, $\mathfrak{c} \in G^k$, we have $\varphi \circ \mathfrak{c}\mathfrak{x} = (\varphi \circ \mathfrak{c})\mathfrak{x} \circ \varphi$. Since every element of $U_k(G)$ is of the form $\mathfrak{g}\mathfrak{x} \circ \varphi$ where $\varphi \in \bar{U}_k(G)$ and $\mathfrak{g} \in G^k$, it follows that $C = \{\mathfrak{c}\mathfrak{x} \mid \mathfrak{c} \in G^k\}$ is a normal subgroup of $U_k(G)$, and clearly $C \cong G^k$, moreover $C\bar{U}_k(G) = U_k(G)$ and $C \cap \bar{U}_k(G) = \{1\}$.

4.4. Let $F(X)$ be the free group on $X = \{x_1, \dots, x_k\}$ and $\mathbf{Z}^+$ the additive group of integers. Then $\eta_i : F(X) \to \mathbf{Z}^+$ defined by $\eta_i x_j = \delta_{ij}$, $1 \leqslant i, j \leqslant k$, where δ_{ij} is the Kronecker symbol describes a group homomorphism. Let $M(k, 0)$ be the ring of $k \times k$-matrices over $\mathbf{Z}$, and G a group. Then $\zeta_k(G) : \mathcal{F}(G[X]) \to M(k, 0)$ defined by $\zeta_k(G)\mathfrak{f} = \zeta_k(G)(f_1, \dots, f_k) = (a_{ij})$ where $a_{ij} = \eta_j \lambda_k(G) f_i$ is a near-ring epimorphism as one can easily check.

4.41. Theorem. *If $G \neq \{1\}$ is a finite p-group, then $\mathfrak{f} \in \mathcal{F}(G[X])$ is a permutation polynomial vector if and only if p does not divide $\det \zeta_k(G)\mathfrak{f}$.*

Proof. By induction on $|G|$. If $|G| = p$, then G is abelian, hence for any $\mathfrak{f} \in \mathcal{F}(G[X])$ with $\zeta_k(G)\mathfrak{f} = (a_{ij})$, we have $\mathcal{F}(\sigma_k(G))\mathfrak{f} = (g_1 \xi_1^{a_{11}} \dots \xi_k^{a_{1k}}, \dots,$

$g_k \xi_1^{a_{k1}} \dots \xi_k^{a_{kk}})$. By Prop. 4.3, $\mathfrak{f}$ is a permutation polynomial vector if and only if $p \nmid \det \zeta_k(G)\mathfrak{f}$. Suppose now that $|G| > p$, and N is a minimal normal subgroup of G. Then $|N| = p$ and $N \subseteq Z(G)$, the centre of G. Let $\eta : G \to G|N$ be the canonical epimorphism and $\eta[X] : G[X] \to (G|N)[X]$ its extension to a composition epimorphism. If $\mathfrak{f}$ is a permutation polynomial vector of G, then by ch. 3, § 11.5, $\mathcal{F}(\eta[X])\mathfrak{f}$ is also a permutation polynomial vector of $G|N$. By induction, p does not divide $\det \zeta_k(G|N)\, \mathcal{F}(\eta[X])\mathfrak{f} = \det \zeta_k(G)\mathfrak{f}$. Conversely let $p \nmid \det \zeta_k(G)\mathfrak{f}$, then $p \nmid \det \zeta_k(G|N)\, \mathcal{F}(\eta[X])\mathfrak{f}$, hence by induction, $\mathcal{F}(\eta[X])\mathfrak{f}$ is a permutation polynomial vector of $G|N$. Thus if $\mathfrak{g}, \mathfrak{g}_1 \in G^k$ and $\mathfrak{g}\mathfrak{g}_1^{-1} \notin N^k$, then $\mathfrak{f} \circ \mathfrak{g} \neq \mathfrak{f} \circ \mathfrak{g}_1$. If, however, $\mathfrak{g}\mathfrak{g}_1^{-1} \in N^k$, then $\mathfrak{g}_1 = \mathfrak{g}\mathfrak{z}$ with $\mathfrak{z} \in N^k \subseteq Z(G)^k$. Hence $\mathfrak{f} \circ \mathfrak{g}_1 = \mathfrak{f} \circ \mathfrak{g}\mathfrak{z} = (\mathfrak{f} \circ \mathfrak{g})(\mathfrak{d} \circ \mathfrak{z})$ where $\mathfrak{d} = (\xi_1^{a_{11}} \dots \xi_k^{a_{1k}}, \dots, \xi_1^{a_{k1}} \dots \xi_k^{a_{kk}})$. Since $p \nmid \det (a_{ik})$, $\mathfrak{d}$ is a polynomial permutation of $Z(G)^k$, by Prop. 4.3, whence $\mathfrak{f} \circ \mathfrak{g}_1 = \mathfrak{f} \circ \mathfrak{g}$ implies $\mathfrak{z} = \mathrm{e}$, i.e. $\mathfrak{g}_1 = \mathfrak{g}$. Hence $\mathfrak{f}$ is a permutation polynomial vector of G.

4.42. Corollary. *If $G \neq \{1\}$ is a finite nilpotent group, then $\mathfrak{f} \in \mathcal{F}(G[X])$ is a permutation polynomial vector if and only if $(\det \zeta_k(G)\mathfrak{f}, |G|) = 1$.*

Proof. G is a direct product of its Sylow p-subgroups G_{p_i}, p_i being pairwise distinct primes. Repeated application of Cor. 3.32 together with Th. 4.41 yields the result.

4.43. Theorem. *Let $G \neq \{1\}$ be a finite p-group. Then $|U_k(G)| = |\mathrm{GL}(k, p)|\, p^t$, for some integer $t > 0$, and $U_k(G)$ is a group extension of some p-group by the group $\mathrm{GL}(k, p)$.*

Proof. Let N be a maximal normal subgroup of G, $\eta : G \to G|N$ the canonical epimorphism and $\mathcal{F}(P_k(\eta)) : \mathcal{F}(P_k(G)) \to \mathcal{F}(P_k(G|N))$ the corresponding near-ring epimorphism. If $\mathcal{F}(\bar{P}_k(\eta, \eta))$ denotes the restriction of $\mathcal{F}(P_k(\eta))$ to $\mathcal{F}(\bar{P}_k(G, G))$, then certainly $\mathcal{F}(\bar{P}_k(\eta, \eta))\, \mathcal{F}(\bar{P}_k(G, G)) = \mathcal{F}(\bar{P}_k(G|N, G|N))$ and $\ker \mathcal{F}(\bar{P}_k(\eta, \eta)) = \mathfrak{l}_{\mathcal{F}(\bar{P}_k(G, G))}(G^k | N^k)$. Since G is a p-group, every chief factor $H|K$ of G is a group of order p, being contained in $Z(G|K)$. Hence an element of $\mathcal{F}(\bar{P}_k(G, G))$ is contained in $\mathfrak{l}_{\mathcal{F}(\bar{P}_k(G, G))}(H^k | K^k)$ if and only if, for every polynomial vector $\mathfrak{f}$ representing this element, we have $\zeta_k(G)\mathfrak{f} = pA$ where A is some integral $k \times k$-matrix. Thus, by Cor. 4.22, $\ker \mathcal{F}(\bar{P}_k(\eta, \eta)) = J$, the radical of $\mathcal{F}(\bar{P}_k(G, G))$. Since $(\xi_1^p, \dots, \xi_k^p) \in J$ and, by Prop. 4.2, J is nilpotent,

the (additive) order of every element of J is a power of p whence $|J| = p^s$ for some integer s. Now $\mathcal{F}(\bar{P}_k(\eta, \eta))\mathfrak{f} \in \mathcal{E}\big(\mathcal{F}(\bar{P}_k(G|N, G|N))\big)$ if and only if $\mathfrak{f} \in \mathcal{E}\big(\mathcal{F}(\bar{P}_k(G, G))\big)$, by Th. 4.41. Hence $\big|\mathcal{E}\big(\mathcal{F}(\bar{P}_k(G, G))\big)\big| = \big|\mathcal{E}\big(\mathcal{F}(\bar{P}_k(G|N, G|N))\big)\big| \, |J|$. Since $G|N$ is abelian, Prop. 4.3. implies $|U_k(G)| = |G|^k \, \big|\mathcal{E}\big(\mathcal{F}(\bar{P}_k(G, G))\big)\big| = |G|^k \, |\mathrm{GL}(k,p)| \, |J| = |\mathrm{GL}(k,p)| \, p^t$. By Th. 3.3, $\mathcal{F}\big(P_k(\eta)\big) U_k(G) = U_k(G|N)$. Since $\big|G|N\big| = p$, the group $U_k(G|N)$ has a normal subgroup C such that $U_k(G|N)|C \cong \mathrm{GL}(k,p)$, by Prop. 4.3, hence the remaining assertion of the theorem follows from the second isomorphism theorem.

4.44. Corollary. *If G is a finite group, then $U_k(G)$ is nilpotent if and only if either $|G| = 1$, or $k = 1$ and G is a 2-group.*

Proof. If $|G| = 1$, then $|U_k(G)| = 1$, and if $k = 1$ and G is a 2-group, then by Th. 4.43, $|U_1(G)| = |\mathrm{GL}(1, 2)|2^t = 2^t$, hence $U_1(G)$ is nilpotent.

Conversely let $|G| \neq 1$ and $U_k(G)$ be nilpotent. Since the set of all $(a\xi_1, \ldots, a\xi_k)$ constitutes a subgroup of $U_k(G)$ isomorphic to G, G itself is nilpotent, i.e. G is a direct product of its Sylow p_i-subgroups G_{p_i}. By Cor. 3.32, every $U_k(G_{p_i})$ is nilpotent whence, by Th. 4.43, every $\mathrm{GL}(k, p_i)$ is nilpotent thus $k = 1$. Let G be any finite group and $\varphi \in Z\big(U_1(G)\big)$. Then since ξ^{-1} and $g\xi$, $g \in G$, belong to $U_1(G)$, we have $\varphi^{-1} = \xi^{-1} \circ \varphi = \varphi \circ \xi^{-1}$ and $g\varphi = g\xi \circ \varphi = \varphi \circ g\xi$. Hence $\varphi(1) = \varphi(gg^{-1}) = g\varphi(g^{-1}) = g\varphi^{-1}(g)$ thus $\varphi(g) = \varphi(1)^{-1}g$, for any $g \in G$. Therefore $\varphi = a\xi$, $a \in G$ whence $\xi^{-1}a^{-1} = a\xi^{-1}$. We conclude that $a^2 = 1$ and see that, for odd $|G|$, the group $U_1(G)$ cannot be nilpotent. Hence G has G_2 as its only Sylow p-subgroup, i.e. G is a 2-group.

5. Characterization of classes of groups by properties of their permutation polynomials

5.1. Theorem. *A finite group G is abelian if and only if every $\varphi \in U_1(G)$ can be written as $\varphi = a\xi^l$, $a \in G$, l an integer.*

Proof. The "only if" part of the theorem is evident. Suppose that every polynomial permutation φ of G can be written as $\varphi = a\xi^k$. Then, for each $b \in G$, there exists some integer $l(b)$ such that $\xi b = b\xi^{l(b)}$, i.e. $b^{-1}\xi b = \xi^{l(b)}$. Hence the group of inner automorphisms of G is abelian, i.e., $G|Z(G)$ is abelian whence G is nilpotent (of class $\leqslant 2$). Moreover

$b^{l(b)-1} = 1$ whence the order $o(b)$ of b divides $l(b)-1$. Since G is nilpotent, there exists $h \in G$ such that $o(h) = \exp G$ whence $\exp G/(l(h)-1)$. Hence $\xi^{l(b)} = \xi$ and $h^{-1}\xi h = \xi$. Therefore $h \in Z(G)$ and $\exp Z(G) = \exp G$. For $z \in Z(G)$, $b \in G$, we have $z^{l(b)} = b^{-1}zb = z$, hence $\exp G \,|\, (l(b)-1)$ and $\xi^{l(b)} = \xi$. Therefore $\xi b = b\xi$, for all $b \in G$, i.e. G is abelian.

5.2. Theorem. *Let $k > 0$ be an integer, $X = \{x_1, \ldots, x_k\}$, and G a finite group. If, for every $\mathfrak{f} \in \mathcal{F}(G[X])$, $(\det \zeta_k(G)\mathfrak{f}, |G|) = 1$ implies that $\mathfrak{f}$ is a permutation polynomial vector, then G is nilpotent.*

Proof. a) Assume $k = 1$. We use induction on $|G|$. Certainly the theorem is true for $|G| = 1$. Suppose the hypothesis of our theorem holds. Now let $|G| > 1$, and M be a maximal subgroup of G such that $|M|$ and $|G|$ have the same prime divisors. By ch. 1, Th. 9.11, $M[x]$ is a subgroup of $G[x]$, and for any $f \in M[x]$, certainly $(\zeta_1(M)f, |M|) = 1$ implies $(\zeta_1(G)f, |G|) = 1$. Thus if $f \in M[x]$ and $(\zeta_1(M)f, |M|) = 1$, f is a permutation polynomial of M and by induction, M is nilpotent. Now suppose that M is a maximal subgroup of G such that $|M|$ and $|G|$ have not the same prime divisors, and let p_i, $i = 1, \ldots, r$, be those primes with $p_i/|G|$, $p_i \nmid |M|$. Let $f \in M[x]$ and $(\zeta_1(M)f, |M|) = 1$. Then we can choose an integer l with $l \equiv 0 \bmod |M|$, $l \equiv 1 - \zeta_1(G)f \bmod p_i$, $i = 1, 2, \ldots, r$, and set $g = x^l f$. Then $\zeta_1(G)g = l + \zeta_1(G)f$ whence $\zeta_1(G)g \equiv \zeta_1(G)f \bmod |M|$ and $\zeta_1(G)g \equiv 1 \bmod p_i$. Therefore $(\zeta_1(G)g, |G|) = 1$ and by assumption, g is a permutation polynomial of G, furthermore $g(m) = m^l f(m) = f(m)$, for all $m \in M$. Hence f is a permutation polynomial of M. By induction, M is also nilpotent in this case. Therefore G is a group all of whose maximal subgroups are nilpotent. By ch. 6, § 6.53, G is nilpotent or $|G| = p^a q^b$, $p \neq q$ primes, G has a normal Sylow p-subgroup P, and all Sylow q-subgroups of G are cyclic. We want to show that the second alternative is impossible: Assume, that G is not nilpotent. Let $f \in (G|Z(G))[x]$, $\big(\zeta_1(G|Z(G))f, |G|Z(G)|\big) = 1$, $\vartheta : G \to G|Z(G)$ be the canonical epimorphism and $\vartheta[x] : G[x] \to (G|Z(G))[x]$ its extension to a composition epimorphism. We choose $g \in G[x]$ such that $(\zeta_1(G)g, |G|) = 1$ and $\sigma_1\big(G|Z(G)\big)\vartheta[x]g = \sigma_1\big(G|Z(G)\big)f$. Such a g can be found by a procedure similar to that used in the first part of the proof. Then g is a permutation polynomial of G whence f is a permutation polynomial of $G|Z(G)$. Unless $Z(G) = 1$, $G|Z(G)$ is nilpotent by induction and so would

G be, contradiction. Therefore $Z(G) = 1$. Let $Q = [h]$ be a fixed Sylow q-subgroup of G, then $G = PQ$. Since $Z(G) = 1$, ch. 6, § 6.53 implies $|Q| = q$ and P is elementary abelian. Moreover if P_1 is a normal subgroup of G and P_1 is properly contained in P, then P_1Q is nilpotent, thus abelian whence $P_1 \subseteq Z(G)$. Hence P is a minimal normal subgroup of G which we will regard as an irreducible KG-module where K is the field of order p and G acts by conjugation as usual. Let T be the representation of G over K afforded by P. If $T(h)$ had 1 as an eigenvalue, then there would exist some $1 \neq r \in P$ such that $hrh^{-1} = r$ whence $r \in Z(G)$, contradiction. Hence T is a non-trivial representation. Let $f(z) = u_0 + u_1 z + \ldots + u_s z^s$ be the characteristic polynomial for $T(h)$, then $f(1) \neq 0$. We choose integers $v_0, v_1, \ldots, v_s$ representing $u_0, \ldots, u_s \in K$, respectively, and an integer m such that $m \equiv 0 \mod p$, $m \equiv 1 - v_0 - \ldots - v_s \mod q$. Let $f = x^m x^{v_0} h x^{v_1} h \ldots h x^{v_s} h^{-s} \in G[x]$. Then $\zeta_1(G) f = m + v_0 + \ldots + v_s$ whence $\zeta_1(G) f \not\equiv 0 \mod p$ and $\zeta_1(G) f \equiv 1 \mod q$. Therefore $(\zeta_1(G) f, |G|) = 1$, hence by hypothesis, f is a permutation polynomial of G. On the other hand, for any $t \in P$, we have $f(t) = t^m t^{v_0} h t^{v_1} h \ldots h t^{v_s} h^{-s} = t^{v_0}(h t^{v_1} h^{-1}) \cdot (h^2 t^{v_2} h^{-2}) \ldots (h^s t^{v_s} h^{-s})$. Or when switching to additive notation, $f(t) = f(T(h))t = 0$, by the CAYLEY–HAMILTON equation (see ch. 6, § 7.2) which contradicts the just obtained result that f is a permutation polynomial. Hence G is nilpotent.

b) $k > 1$. If G is not nilpotent, then by a) there exists a polynomial $f(x_1) \in G[x_1]$ such that $(\zeta_1(G) f(x_1), |G|) = 1$ and $f(x_1)$ is not a permutation polynomial. Let $\mathfrak{f} = (f(x_1), x_2, \ldots, x_k) \in \mathcal{F}(G[X])$, then $\mathfrak{f}$ is not a permutation polynomial vector, but $(\det \zeta_k(G)\, \mathfrak{f}, |G|) = (\det \zeta_1(G) f(x_1), |G|) = 1$.

5.3. Theorem. *If G is a finite nilpotent group of class $c(G) \leqslant 2$, then $U_1(G)$ is the set of all polynomial functions $\varphi = a\xi^l b$, $a, b \in G$, $(l, |G|) = 1$.*

Proof. Certainly every polynomial function of this form belongs to $U_1(G)$. Conversely let $\varphi \in U_1(G)$, then $\varphi = a_1 \xi^{l_1} a_2 \xi^{l_2} \ldots a_r \xi^{l_r} a_{r+1}$, $a_i \in G$, l_i integers. Since $c(G) \leqslant 2$, the commutator group of G is contained in $Z(G)$, and by ch. 6, § 6.53, we have $[ab, c] = [a, c]\,[b, c]$ and $[a, bc] = [a, b]\,[a, c]$, $a, b, c \in G$. Hence

$$\varphi = a_1 \ldots a_{r+1} \xi^{l_1 + \ldots + l_r} [\xi^{l_1}, a_2]\,[\xi^{l_1 + l_2}, a_3] \ldots [\xi^{l_1 + \ldots + l_r}, a_{r+1}]$$
$$= a_1 \ldots a_{r+1} \xi^{l_1 + \ldots + l_r} [\xi, a_2^{l_1} a_3^{l_1 + l_2} \ldots a_{r+1}^{l_1 + l_2 + \ldots + l_r}].$$

By Cor. 4.42, $(\sum_{i=1}^{r} l_i, |G|) = 1$, hence there exists $h \in G$ such that $h^{\sum_{i=1}^{r} l_i} = a_2^{l_1} a_3^{l_1 + l_2} \ldots a_{r+1}^{l_1 + l_2 + \ldots + l_r}$. Thus

$$\varphi = a_1 \ldots a_{r+1} \xi^{l_1 + l_2 + \ldots + l_r} [\xi, h^{l_1 + l_2 + \ldots + l_r}]$$
$$= a_1 \ldots a_{r+1} \xi^{l_1 + l_2 + \ldots + l_r} [\xi^{l_1 + \ldots + l_r}, h] = a_1 \ldots a_{r+1} h^{-1} \xi^{l_1 + \ldots + l_r} h.$$

5.31. Corollary. *If G is a finite nilpotent group of class 2, φ Euler's φ-function, and $H(G) = \{g \in G \mid g^{-1} \xi g = \xi^{e(g)}$, for some integer $e(g)\}$, then*

$$|U_1(G)| = \frac{|G|^2 \varphi(\exp G)}{|H(G)|}.$$

Proof. By Th. 5.3, $U_1(G) = \{u\xi^l v \mid u, v \in G, 0 \leqslant l < \exp G, (l, \exp G) = 1\}$. Amongst these $|G|^2 \varphi(\exp G)$ (not necessarily pairwise distinct) functions, we have to determine under what conditions $a\xi^l b = c\xi^m d$. Suppose this holds for $a, b, c, d \in G$, $0 \leqslant l$, $m < \exp G$, $(l, \exp G) = (m, \exp G) = 1$, then $a = cdb^{-1}$ whence $db^{-1} \xi^l b d^{-1} = \xi^m$, and if $\bar{l} l \equiv 1 \mod \exp G$, then $db^{-1} \xi b d^{-1} = \xi^{\bar{l} m}$. Hence $bd^{-1} = h \in H(G)$, thus $d = h^{-1} b$, $c = ah$, and $m \equiv l e(h) \mod \exp G$. If conversely, $d = h^{-1} b$, $c = ah$, $h \in G(H)$, and $m \equiv l e(h) \mod \exp G$, then $c\xi^m d = ah \xi^{l e(h)} h^{-1} b = a(hh^{-1} \xi h h^{-1})^l b = a\xi^l b$.

5.32. The converse of Th. 5.3 is not true as the following example shows: Let $G = S_3$, the symmetric group on three letters. The polynomial functions $a\xi^{\pm 1} b$, $a, b \in S_3$, belong to $U_1(S_3)$ and are pairwise distinct since $Z(S_3) = \{1\}$. Hence $|U_1(S_3)| \geqslant 72$. However, the cosets mod A_3, the alternating group on three letters, are blocks for $U_1(S_3)$ as a permutation group on S_3. Since there are exactly two blocks of three elements each, we conclude that $|U_1(S_3)| \leqslant 2!\,(3!)^2 = 72$. Hence $|U_1(S_3)| = 72$ whence every mapping of $U_1(S_3)$ has the form $a\xi^l b$. S_3 is, however, not nilpotent. Yet there is a partial converse of Th. 5.3 if we restrict the prime divisors of $|G|$:

5.33. Theorem. *If G is a finite group of odd order and every $\varphi \in U_1(G)$ is of the form $\varphi = a\xi^r b$, $a, b \in G$, then G is nilpotent of class $c(G) \leqslant 3$. If furthermore $(|G|, 6) = 1$, then $c(G) \leqslant 2$.*

Proof. By ch. 6, § 6.53, it suffices to show that a and $b^{-1}ab$ commute, for any two elements $a, b \in G$. Since $(|G|, 2) = 1$, $xg^{-1}xg = xg^2 \circ x^2 \circ xg^{-1}$ is a permutation polynomial, for any $g \in G$. Hence there exists an integer $l(g)$ and an element $a(g) \in G$ such that $\xi g^{-1} \xi g = a(g)^{-1} \xi^{l(g)} a(g)$, $(l(g), |G|) = 1$. Let $\bar{l}(g)$ be a solution of $\bar{l}(g)\, l(g) \equiv 1 \mod |G|$, then $\xi^{\bar{l}(g)} g^{-1} \xi^{\bar{l}(g)} g =$

$= a(g)^{-1}\xi a(g)$ is an inner automorphism of G. Hence $\xi^{2\bar{l}(g)}g^{-1}\xi^{2\bar{l}(g)}g = \xi^{\bar{l}(g)}g^{-1}\xi^{\bar{l}(g)}g\xi^{\bar{l}(g)}g^{-1}\xi^{\bar{l}(g)}g$, for all $g \in G$. Therefore $\xi^{\bar{l}(g)}(g^{-1}\xi^{\bar{l}(g)}g) = (g^{-1}\xi^{\bar{l}(g)}g)\xi^{\bar{l}(g)}$. Since $\xi^{\bar{l}(g)}$ is a polynomial permutation, we obtain $t(g^{-1}tg) = (g^{-1}tg)t$, for all $t, g \in G$. This completes the proof.

Remarks and comments

§§ 1–5. Polynomial permutations on groups were originally discussed by LAUSCH, NÖBAUER and SCHWEIGER [1], [2], for $k = 1$, and by NÖBAUER [26], for $k > 1$. The concept of length in the case of one indeterminate (in a form which is somewhat different from that in our book) has been introduced by S. D. SCOTT [1] who also proved Prop. 1.3 for this case. Some of the methods of § 2 originate from FRÖHLICH [1]. The case $k = 1$ of Th. 4.12 has been proved implicitly in LAUSCH, NÖBAUER and SCHWEIGER [1], the proof for the general case in our book is due to LAUSCH. Th. 4.11 has also been proved by LAUSCH, after some preliminary work had been done in LAUSCH [5]. The characterizations of certain classes of groups by properties of their permutation polynomials in § 5 are due to LAUSCH, NÖBAUER and SCHWEIGER [2], LAUSCH and SCHWEIGER [1], and LAUSCH [3]. An explicit computation of the group $U_1(G)$, for various finite non-abelian groups G, has been performed by SCHUMACHER [1]. For a connection between $U_1(G)$ and the automorphism group of G, we can only refer to TROTTER [1].

CHAPTER 6

APPENDIX

1. Sets

1.1. In this section we will give a brief survey of those basic concepts and theorems on sets that are used in the book. For more detailed information and proofs of the theorems, we refer to standard texts, e.g. KAMKE [1].

A set is a collection of objects, these being called elements or members of the set. As usual we write $a \in A$ to indicate that a is an element of the set A, and $a \notin A$ in the opposite case. A set B is called a subset of the set A if every element of B is an element of A, we write in this case $B \subseteq A$. The set $P(A)$ of all subsets of A is called the power set of A. If B is a proper subset of A, i.e. there exists $a \in A$, $a \notin B$, then we write $B \subset A$. The union $A \cup B$ of the sets A, B is the set of all elements which belong to at least one of the sets A, B. The intersection $A \cap B$ of A, B is the set of all elements which belong to both A and B and $A - B = \{a \mid a \in A, a \notin B\}$ is the difference of A, B. The empty set ϕ is the set consisting of no element. ϕ is a subset of every set. Two sets A, B are called disjoint if $A \cap B = \phi$.

Let I be an arbitrary set. If for every $i \in I$, there is some set A_i defined, then we speak of the family $(A_i \mid i \in I)$ of sets. $\cup(A_i \mid i \in I) = \{a \mid a \in A_i$ for at least one $i \in I\}$ is called the union of this family while $\cap(A_i \mid i \in I) = \{a \mid a \in A_i$ for all $i \in I\}$ is called the intersection of this family.

It is well-known that intuitive set theory sometimes leads to contradictions, thus one has to introduce the concept of classes for "very large" sets. In this book, however, the distinction between classes and sets is, in fact, not essential.

1.2. Let A, B be two sets. A mapping (or function) φ from A to B $(\varphi: A \to B)$ is a rule which assigns some element $\varphi a \in B$ to each $a \in A$. B is called the range of φ. Sometimes the mapping φ will also be written as $a \to \varphi a$. The element φa is called the image of a under φ, and if $\varphi a = b$, $a \in A$, then a is called an inverse image or counterimage of b under φ.

The set consisting of the images of all $a \in A$ will be denoted by φA.

The mapping $\varphi: A \to B$ is called injective or an injection if every $b \in B$ has at most one counterimage under φ while φ is called surjective or a surjection if $\varphi A = B$ and bijective or a bijection if φ is injective and surjective. A surjective mapping is also called a mapping „onto", whereas a mapping „into" is not necessarily surjective. Sometimes we use the following

Lemma. *If A is a finite set and $\varphi: A \to A$ is injective or surjective, then φ is bijective.*

Let $\varphi: A \to B$ be any mapping and $A_1 \subseteq A$. Then the mapping $\varphi_1: A_1 \to B$ defined by $\varphi_1 a = \varphi a$, for every $a \in A_1$, is called the restriction of φ to A_1 while φ is called an extension of φ_1 to A. Sometimes we write $\varphi_1 = \varphi | A_1$.

Let $\varphi: A \to B$ be a mapping and $C \subseteq A \cap B$. We say that φ fixes C (elementwise) if $\varphi c = c$, for all $c \in C$.

If $\varphi: A \to B$, $\psi: B \to C$, then $\psi\varphi a = \psi(\varphi a)$ defines a mapping $\psi\varphi: A \to C$ being called the product or the composition of the mappings ψ, φ. For any three mappings χ, ψ, φ, we have $(\chi\psi)\varphi = \chi(\psi\varphi)$ whenever both sides of the equation are defined. The mapping $\varepsilon: A \to A$ with $\varepsilon a = a$, for all $a \in A$, is called the identical or identity mapping of A. ε satisfies $\varepsilon\varphi = \varphi$, $\varphi\varepsilon = \varphi$, for every mapping φ to or from A, respectively. If $\varphi: A \to B$ is bijective, then $\varphi^{-1}: B \to A$ defined by $\varphi^{-1}(\varphi a) = a$, for all $\varphi a \in B$, $a \in A$, is again bijective. φ^{-1} is called the inverse of φ.

A (finite) diagram consists of a finite family of sets and a finite set of mappings between the sets of this family which can be drawn in such a manner that the sets are represented by points and the mappings $\varphi: A \to B$ by arrows linking the points which represent A, B. A diagram is called commutative if any two sequences of arrows between two points A and B represent one and the same mapping, e.g. diagram fig. 6.1 is commutative if $\varkappa\psi = \varphi$.

A family of elements of the set A with index set I is a mapping $\varphi: I \to A$. We set $\varphi i = a_i$ and write $(a_i | i \in I)$ for this family. Any restriction φ_1 of φ to a subset I_1 of I is called a subfamily of $(a_i | i \in I)$. Sometimes we also speak of systems and subsystems instead of families or subfamilies. If I is the set of positive integers, then $(a_i | i \in I)$ is a sequence, and if I is finite, then $(a_i | i \in I)$ is called a finite sequence.

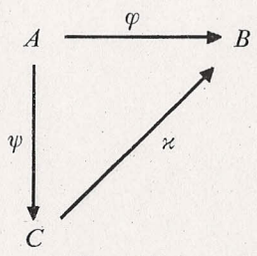


FIG. 6.1

1.3. Let $(A_i | i \in I)$ be a family of sets. The Cartesian product $D = \prod(A_i | i \in I)$ of this family is the set of all families $(a_i | i \in I)$ of elements of $\bigcup(A_i | i \in I)$ such that $a_i \in A_i$, for all $i \in I$. If $d = (a_i | i \in I) \in D$ and $j \in I$, then $a_j \in A_j$ is called the j-th component of d. If $I = \{1, 2, \ldots, k\}$, then we write $A_1 \times A_2 \times \ldots \times A_k$ for $\prod(A_i | i \in I)$ and if $A_i = A$, $i = 1, \ldots, k$, then we write A^k for $A_1 \times \ldots \times A_k$. We call A^k a Cartesian power of A.

Let $k > 0$ be an integer and A a set. By a k-place function or k-ary operation on A, we understand a mapping $\varphi: A^k \to A$. A subset $B \subseteq A$ is said to be closed under φ if $\varphi(b_1, \ldots, b_k) \in B$ whenever $(b_1, \ldots, b_k) \in B^k$.

1.4. Let A be a set. A binary relation Θ on A is a subset of A^2. For $(a, b) \in \Theta$ we will write $a \Theta b$.

A binary relation Θ on A is called an equivalence relation if Θ is reflexive, transitive, and symmetric, i.e. the following three conditions hold, for any $a, b, c \in A$:

(i) $a \Theta a$;

(ii) $a \Theta b$, $b \Theta c$ imply $a \Theta c$;

(iii) $a \Theta b$ implies $b \Theta a$.

Equivalence relations on A are strongly tied up with partitions of A. A partition of the set A is a set of non-empty subsets of A such that every $a \in A$ is an element of exactly one of these subsets. The subsets are called classes or blocks of the partition, and the subset containing $a \in A$ is called the class of a, denoted by $C(a)$. Every element of a class C of a partition is called a representative of C. By a (full) system of representatives of a partition of A, we understand a subset $R \subseteq A$ such that $R \cap C$ consists of exactly one element, for every class C. The connection between partitions and equivalence relations of A can now be expressed by a

Theorem. *Let ϑ be any partition of A. If we define the binary relation $\Theta(\vartheta)$ on A by: $a\Theta(\vartheta)b$ if and only if a, b are in the same class of ϑ, then $\Theta(\vartheta)$ is an equivalence relation. The mapping φ from the set of all partitions of A to the set of all equivalence relations on A defined by $\varphi\vartheta = \Theta(\vartheta)$, for every partition ϑ, is bijective.*

The classes of the partition, corresponding to the equivalence relation Θ, are called equivalence classes under Θ.

1.5. Let A be any set. A binary relation $\leqslant$ on A is called a partial order (relation) if $\leqslant$ is reflexive, transitive and antisymmetric, i.e., for all $a, b, c \in A$, the following conditions hold:

(i) $a \leqslant a$;

(ii) $a \leqslant b$, $b \leqslant c$ imply $a \leqslant c$;

(iii) $a \leqslant b$ and $b \leqslant a$ imply $a = b$.

The pair $\langle A; \leqslant\rangle$ is called a partially ordered set. We write $a < b$ if $a \leqslant b$ but not $a = b$.

A partial order relation $\leqslant$ on A is called a total order (relation) if also

(iv) $a \leqslant b$ or $b \leqslant a$, for all $a, b \in A$,

is satisfied. $\langle A; \leqslant\rangle$ where $\leqslant$ is a total order relation, is called a totally ordered set or a chain.

Let $\langle A; \leqslant\rangle$ be a partially ordered set. An element $a \in A$ is called a maximal element of A if $a \leqslant b$ implies $a = b$ and a is called a minimal element of A if $b \leqslant a$ implies $b = a$. $a \in A$ is the greatest element of A if $b \leqslant a$, for all $b \in A$, and a is the least element of A if $a \leqslant b$, for all $b \in A$. Clearly A has at most one greatest (least) element being denoted by $\max A$ ($\min A$).

Let B be a subset of the partially ordered set $\langle A; \leqslant\rangle$. Then $B^2 \cap (\leqslant)$ is a partial order relation on B which will again be denoted by $\leqslant$. $a \in A$ is an upper (lower) bound of B if $b \leqslant a$ ($a \leqslant b$), for all $b \in B$. A very important theorem gives a condition for the existence of maximal elements:

Zorn's lemma. *Let $\langle A; \leqslant\rangle$ be a partially ordered set such that every totally ordered subset $\langle B; \leqslant\rangle$ of A has an upper bound. Then A has a maximal element.*

In most cases this theorem is applied when A is a subset of the power set $P(M)$ of some set M and $a \leqslant b$ means that a is a subset of b.

Let $\langle A; \leqslant\rangle$ and $\langle B; \leqslant\rangle$ be partially ordered sets. A mapping $\varphi : A \to B$ is an order homomorphism if $a_1 \leqslant a_2$ always implies $\varphi a_1 \leqslant \varphi a_2$. A surjective order homomorphism is called an order epimorphism. If $A = B$, then φ is an order endomorphism. If φ is bijective and φ^{-1} is also an order homomorphism, then φ is called an order isomorphism.

Let $\langle A_i; \leqslant\rangle$, $i = 1, \ldots, k$, be partially ordered sets and D the Cartesian product of these sets. We define a relation $\leqslant$ on D by $(a_1, \ldots, a_k) \leqslant (b_1, \ldots, b_k)$ if and only if there is an index $1 \leqslant i \leqslant k+1$ such that $a_1 = b_1, \ldots, a_{i-1} = b_{i-1}$, $a_i < b_i$. Then $\leqslant$ is a partial order relation on D, the so-called lexicographic partial order relation of D. If all $\langle A_i; \leqslant\rangle$ are totally ordered sets, so is $\langle D; \leqslant\rangle$.

1.6. The sets A, B are called equipotent if there exists a bijective mapping $\varphi : A \to B$. Equipotence of sets is reflexible, transitive, and symmetric. The class of all sets which are equipotent to some set A is called the cardinality or cardinal $|A|$ of the set A. If moreover $\varphi : I \to A$ is a family of elements of A with index set I, then the cardinality of this family will mean $|\varphi I|$. If A is a finite set, then the cardinality $|A|$ is called finite and if A is infinite, then $|A|$ is called infinite. The finite cardinalities can be identified with the non-negative integers. The cardinality $|N|$ of the set N of positive integers is denoted by $\aleph_0$ and a set A with $|A| = \aleph_0$ is called a countable set.

Let $(\mathfrak{m}_i | i \in I)$ be a family of cardinals. The sum and product of this family are well-defined cardinals if we define them as follows: Take any family $(A_i | i \in I)$ of sets such that $|A_i| = \mathfrak{m}_i$, for all $i \in I$, and $A_i \cap A_j = \phi$, for $i \neq j$, and set $\sum(\mathfrak{m}_i | i \in I) = \left|\bigcup(A_i | i \in I)\right|$. Take any family $(A_i | i \in I)$ of sets such that $|A_i| = \mathfrak{m}_i$, for all $i \in I$, and set $\prod(\mathfrak{m}_i | i \in I) = \left|\prod(A_i | i \in I)\right|$. Important special cases are $\mathfrak{m}_1 + \mathfrak{m}_2$ and $\mathfrak{m}_1 \mathfrak{m}_2$, the sum and the product, resp., of two cardinals $\mathfrak{m}_1$ and $\mathfrak{m}_2$. If $\mathfrak{m}_i = \mathfrak{m}$, for all $i \in I$, then $\sum(\mathfrak{m}_i | i \in I) = |I|\,\mathfrak{m}$.

Let $\mathfrak{m}, \mathfrak{n}$ be two cardinals, and I a set with $|I| = \mathfrak{n}$. If $(\mathfrak{m}_i | i \in I)$ is a family of cardinals with $\mathfrak{m}_i = \mathfrak{m}$, for all $i \in I$, then we define $\mathfrak{m}^{\mathfrak{n}} = \prod(\mathfrak{m}_i | i \in I)$, which is well-defined. For any set A, $|P(A)| = 2^{|A|}$.

Let $\mathfrak{m}, \mathfrak{n}$ be two cardinals. We write $\mathfrak{m} \leqslant \mathfrak{n}$ if and only if there exist sets A, B with $|A| = \mathfrak{m}$, $|B| = \mathfrak{n}$ such that there is an injective mapping $\varphi : A \to B$. If C is an arbitrary set of cardinals, then $\leqslant$ is a total order relation on C. If $\mathfrak{n}$ is a finite cardinal, then $\mathfrak{n} < \aleph_0$, and if $\mathfrak{n}$ is infinite then $\aleph_0 \leqslant \mathfrak{n}$. If B is a subset of A, then $|B| \leqslant |A|$. If $(A_i | i \in I)$ is a family of

sets, then $|\bigcup(A_i|i\in I)| \leqslant \sum(|A_i||i\in I)$. If $(\mathfrak{m}_i|i\in I)$, $(\mathfrak{n}_i|i\in I)$ are families of cardinals such that $\mathfrak{m}_i \leqslant \mathfrak{n}_i$, for all $i\in I$, then $\sum(\mathfrak{m}_i|i\in I) \leqslant \sum(\mathfrak{n}_i|i\in I)$ and $\prod(\mathfrak{m}_i|i\in I) \leqslant \prod(\mathfrak{n}_i|i\in I)$. If $\mathfrak{m}_1 \leqslant \mathfrak{m}_2$ and $\mathfrak{n}$ is an arbitrary cardinal, then $\mathfrak{m}_1^{\mathfrak{n}} \leqslant \mathfrak{m}_2^{\mathfrak{n}}$.

If $\mathfrak{m}$ or $\mathfrak{n}$ is an infinite cardinal, then $\mathfrak{m}+\mathfrak{n} = \max(\mathfrak{m}, \mathfrak{n})$ and if moreover $\mathfrak{m} \neq 0$, $\mathfrak{n} \neq 0$, then $\mathfrak{m}\mathfrak{n} = \max(\mathfrak{m}, \mathfrak{n})$. If $\mathfrak{m}$ is an infinite and $\mathfrak{n}$ is a finite cardinal, then $\mathfrak{m}^{\mathfrak{n}} = \mathfrak{m}$. For any set A we have $|A| < |P(A)|$.

1.7. A partial order relation $\leqslant$ on the set A is called a well ordering if every non-empty subset of A has a least element w.r.t. $\leqslant$. A partially ordered set $\langle A; \leqslant\rangle$ is called well ordered if $\leqslant$ is a well ordering.

Theorem. (Well ordering principle). *On every non-empty set A, one can define a well ordering $\leqslant$.*

Two well ordered sets A, B are called isomorphic if there exists an order isomorphism $\varphi : A \to B$. "Isomorphic" for well ordered sets is reflexive, transitive, and symmetric. The class of all well ordered sets isomorphic to some given well ordered set A is called the ordinal of A. The ordinal of the empty set is denoted by 0, the ordinal of the set $\{1, 2, \ldots, n\}$ ordered by the usual order relation of the integers will be denoted by n.

Let α, β be two ordinals. We write $\alpha \leqslant \beta$ if and only if there exist well ordered sets A, B with ordinal α, β, respectively, such that there is an injective order homomorphism $\varphi : A \to B$. If O is an arbitrary set of ordinals, then $\leqslant$ is a well order relation on O. If α is an arbitrary ordinal, then the ordinal of the set $\langle G; \leqslant\rangle$ of all ordinals $\gamma < \alpha$ is just α.

1.8. Induction is frequently used throughout the book. The principle of this powerful method will now be described briefly:

Let a be a non-negative integer and the statement $\varphi(m)$ be defined for all integers $m \geqslant a$. Suppose that

(i) $\varphi(a)$ holds and

(ii) if $\varphi(n)$ holds, for $a \leqslant n < m$, then $\varphi(m)$ holds.

Then $\varphi(m)$ holds for all integers $m \geqslant a$.

An important generalization of induction is the transfinite induction:

Let α, δ be ordinals with $\alpha < \delta$ and the statement $\varphi(\mu)$ be defined for all ordinals μ with $\delta \geqslant \mu \geqslant \alpha$. Suppose that

(i) $\varphi(\alpha)$ holds and

(ii) if $\varphi(\gamma)$ holds for $\alpha \leqslant \gamma < \mu$, then $\varphi(\mu)$ holds.

Then $\varphi(\mu)$ holds for all ordinals μ with $\delta \geqslant \mu \geqslant \alpha$.

1.9. A binary (i.e. 2-ary) operation $*$ on a set M (written with infix notation) is called a ssociative if $x*(y*z) = (x*y)*z$, for all $x, y, z\in M$; commutative if $x*y = y*x$, for all $x, y\in M$; and idempotent if $x*x = x$ for all $x\in M$. Let $*$ and $\circ$ be binary operations on M. The operation $\circ$ is called right (left) distributive w.r.t. $*$ if $(x*y)\circ z = (x\circ z)*(y\circ z)$ (if $z\circ(x*y) = (z\circ x)*(z\circ y)$), for all $x, y, z\in$M. Let $*$ be a binary operation on M. An element $i\in M$ is called a right (left) identity for $*$ if $a*i = a$ (if $i*a = a$), for all $a\in M$. If i is a right as well as a left identity for $*$, then i is called an identity for $*$. There exists at most one such identity.

2. Lattices

2.1. All those results from lattice theory which are used in this book will now be reviewed in brief. For more detailed information, we refer to standard texts (e.g. Szász [1]).

An algebra $\langle L; \cup, \cap\rangle$ where $\cup, \cap$ are binary operations is called a lattice if both $\cup$ and $\cap$ are associative and commutative and if moreover the "absorption laws" $a\cup(a\cap b) = a$, $a\cap(a\cup b) = a$ are satisfied for all $a, b\in L$.

There is some close relation between lattices and certain partially ordered sets. Let $\langle A; \leqslant\rangle$ be any partially ordered set and B a subset of A. A least (greatest) element of the set of upper (lower) bounds of B – which, of course, need not always exist – is called a least upper (greatest lower) bound of B. We will write $\cup(b|b\in B)$ for the least upper bound of B and $\cap(b|b\in B)$ for the greatest lower bound of B.

Theorem. *Let $\langle L; \cup, \cap\rangle$ be a lattice. We define a binary relation $\leqslant$ on L by: $a \leqslant b$ if and only if $a\cup b = b$. Then $\langle L; \leqslant\rangle = \vartheta L$ is a partially ordered set where $\cup(a, b)$ and $\cap(a, b)$ exist, for any subset $\{a, b\} \subseteq L$, and $\cup(a, b) = a\cup b$, $\cap(a, b) = a\cap b$. If, conversely, $\langle L; \leqslant\rangle$ is a partially ordered set where $\cup(a, b)$ and $\cap(a, b)$ always exist, then we obtain a*

lattice $\langle L; \cup, \cap \rangle = \eta L$ *when defining* $a \cup b = \cup(a, b)$, $a \cap b = \cap(a, b)$. *Moreover* $\eta(\vartheta L) = L$, *for any lattice* L, *and* $\vartheta(\eta L) = L$, *for any partially ordered set* L *where* $\cup(a, b)$ *and* $\cap(a, b)$ *always exist.*

2.2. A lattice L is called a complete lattice if $\cup(b \mid b \in B)$ and $\cap(b \mid b \in B)$ exist in the corresponding partially ordered set ϑL, for any $B \subseteq L$. For proving completeness of a given lattice one sometimes uses the

Lemma. *A partially ordered set* $\langle A; \leqslant \rangle$ *corresponds to some complete lattice if and only if* A *has a greatest element and, for any non-empty subset* $B \subseteq A$, *there exists* $\cap(b \mid b \in B)$.

Let L be a complete lattice. A subset M of L is called a complete sublattice of L if, for every subset $B \subseteq M$, we have $\cup(b \mid b \in B) \in M$ and $\cap(b \mid b \in B) \in M$.

2.3. A lattice L is called a distributive lattice if $\cup$ is right distributive w.r.t. $\cap$ and $\cap$ is right distributive w.r.t. $\cup$.

Let $\langle L; \cup, \cap \rangle$ be a lattice. A right identity for $\cup$ – there exists at most one such identity – is called a zero of L and denoted by 0, and similarly a right identity for $\cap$ is called an identity of L, denoted by 1. An element $a \in L$ is a zero (identity) of L if and only if a is the least (greatest) element of the corresponding partially ordered set ϑL.

Let L be a distributive lattice with zero and identity. L is a Boolean algebra if, for any $a \in L$, there exists a unique element $a' \in L$ such that $a \cup a' = 1$ and $a \cap a' = 0$.

2.4. Let L, M be two lattices. A homomorphism (epimorphism, isomorphism) $\varphi : L \to M$ from the algebra L to the algebra M is called a lattice homomorphism (epimorphism, isomorphism). If $\varphi : L \to M$ is a lattice homomorphism (epimorphism), then φ is also an order homomorphism (epimorphism) from ϑL to ϑM, but the converse is not always true. φ is, however, a lattice isomorphism if and only if φ is an order isomorphism. Let L, M be complete lattices. A lattice homomorphism (epimorphism) $\varphi : L \to M$ is called complete if $\varphi \cup(b \mid b \in B) = \cup(\varphi b \mid b \in B)$ and $\varphi \cap(b \mid b \in B) = \cap(\varphi b \mid b \in B)$, for all subsets $B \subseteq L$.

2.5. An algebra $\langle S; \cap \rangle$ is called a semilattice if $\cap$ is associative, commutative, and idempotent.

3. Multioperator groups

3.1. This section is to exhibit what is needed in the book from the theory of multioperator groups. Since just very few books contain some material on this subject, we give the proofs in full.

Assume $+$ is a 2-ary operation, written with infix notation, $-$ is a 1-ary operation, and 0 is a 0-ary operation. Let $\Omega = \{\omega_i \mid i \in I\}$ be a family of operations, indexed by the set I of all ordinals $\iota < o$ where o is an arbitrary ordinal. Let $T = \{n_i \mid i \in I\}$ be the type of Ω. We define:

An algebra $G = \langle G; +, -, 0, \Omega \rangle$ is called an Ω-multioperator group if

1) $\langle G; +, -, 0 \rangle$ is a group with $+$ as group operation, $-$ the operation of forming the inverse, and 0 the identity;

2) $\omega_i 0 \ldots 0 = 0$, for any $\omega_i \in \Omega$ with $n_i > 0$.

Thus e.g. every group $\langle G; +, -, 0 \rangle$ and every ring $\langle R; +, -, 0, \cdot \rangle$ is a multioperator group.

3.11. Proposition. *For any* Ω, *the class* $\mathfrak{M}$ *of* Ω*-multioperator groups is a variety.*

This follows from the fact that "$\langle G; +, -, 0 \rangle$ being a group" can be stated by means of laws.

3.2. Assume $G = \langle G; +, -, 0, \Omega \rangle$ is an Ω-multioperator group. Let Θ be any congruence on G and $C(a)$ the congruence class of the element $a \in G$ under Θ. We define the kernel $\ker \Theta$ of Θ by $\ker \Theta = C(0)$. A subset A of G is called an ideal of G if there is some congruence Θ on G such that $\ker \Theta = A$. If φ is a homomorphism from the Ω-multioperator group G to some algebra H, then the ideal kernel $\ker \varphi$ of φ will be the ideal $\ker \operatorname{Ker} \varphi$.

3.21. Proposition. *Assume that* $A = \ker \Theta$. *Then* A *is a normal subgroup of* $\langle G; +, -, 0 \rangle$ *and* Θ *is induced by the partition of this group into the cosets of the normal subgroup* A.

Proof. By hypothesis $A = C(0)$ whence A is a subgroup. Moreover $c \Theta b$ if and only if $c \in b + A$ but also if and only if $c \in A + b$. Thus $b + A = A + b = C(b)$ whence A is a normal subgroup of $\langle G; +, -, 0 \rangle$ and also the second statement follows.

3.22. Corollary. *The mapping which maps every congruence Θ of the Ω-multioperator group G onto its kernel, is a bijection from the congruence lattice $\mathfrak{L}(G)$ to the set of all ideals of G.*

Proof. Evident.

3.23. From ch. 1, § 1.5 and the definition of an ideal, we see that the subsets $\{0\}$ and G of G are ideals, the so-called zero ideal and unit ideal, respectively. Together they are called the trivial ideals of G. Cor. 3.22 shows that the multioperator group G is simple if and only if G has no non-trivial ideals.

If A is an ideal of G and Θ the congruence such that $\ker\Theta = A$, then we will write $G|A$ for the factor algebra $G|\Theta$.

Let $\mathfrak{N}(G)$ be the set of all ideals of G. The set-theoretical inclusion $\subseteq$ is a partial order relation on $\mathfrak{N}(G)$. If $\Theta_1, \Theta_2 \in \mathfrak{L}(G)$, then $\Theta_1 \leqslant \Theta_2$ if and only if $\ker\Theta_1 \subseteq \ker\Theta_2$. Hence the mapping $\ker : \mathfrak{L}(G) \to \langle\mathfrak{N}(G); \subseteq\rangle$ is an order isomorphism and $\ker^{-1}$ is also an order isomorphism. Therefore $\langle\mathfrak{N}(G); \subseteq\rangle$ is a complete lattice. Let $M = \{A_i | i \in I\}$ be a non-empty subset of $\mathfrak{N}(G)$ and set $\ker^{-1} A_i = \Theta_i$. Then by ch. 1, § 1.6, the greatest lower bound of M is $\ker \cap(\Theta_i | i \in I)$ where $\cap$ means the set-theoretical intersection. Since $a \in \ker \cap\Theta_i$ if and only if $a \in \cap \ker\Theta_i$, we conclude that the greatest lower bound of M is the set-theoretical intersection $\cap(A_i | i \in I)$ which therefore is again an ideal. The least upper bound S of M is $\ker\Phi$ where Φ is the least upper bound of the set $\ker^{-1} M$. Thus $a \in S$ if and only if $a\Phi 0$. By ch. 1, § 1.6, this is true if and only if there are congruences $\Theta_{i_1}, \ldots, \Theta_{i_r}$ in $\ker^{-1} M$ and elements $c_1, \ldots, c_{r-1} \in G$ such that $a\Theta_{i_1}c_1$, $c_1\Theta_{i_2}c_2, \ldots, c_{r-1}\Theta_{i_r}0$. This is equivalent to $a - c_1 = a_{i_1} \in A_{i_1}$, $c_1 - c_2 = a_{i_2} \in A_{i_2}$, $\ldots$, $c_{r-2} - c_{r-1} = a_{i_{r-1}} \in A_{i_{r-1}}$, $c_{r-1} = a_{i_r} \in A_{i_r}$, i.e.

$$a = a_{i_1} + a_{i_2} + \ldots + a_{i_r} \quad \text{where} \quad r \geqslant 1, \quad a_{i_\nu} \in A_{i_\nu}, \quad \nu = 1, \ldots, r. \tag{3.2}$$

Thus S is the set of all elements of the form (3.2). This set is called the sum of the set $M = \{A_i | i \in I\}$ of ideals and is, of course, itself an ideal. Hence

3.24. Theorem. *The set $\mathfrak{N}(G)$ of all ideals of the Ω-multioperator group G being partially ordered by set-theoretical inclusion, is a complete lattice, the so-called ideal lattice of G. If M is a non-empty subset of $\mathfrak{N}(G)$, then the greatest lower bound of M is the set-theoretical intersection of the ideals of M and the least upper bound of M is the sum of the ideals of M. The mapping $\ker : \mathfrak{L}(G) \to \mathfrak{N}(G)$ is a lattice isomorphism.*

3.25. Let P be a subset of G. The ideal of G generated by P is the intersection of all ideals of G containing P.

3.3. Proposition. *Let G be an Ω-multioperator group, D an ideal of G, and $\mathfrak{C}$ the sublattice of $\mathfrak{N}(G)$ consisting of all ideals $B \supseteq D$ of G. Then the canonical epimorphism $\vartheta : G \to G|D$ induces a lattice isomorphism from $\mathfrak{C}$ to the lattice $\mathfrak{N}(G|D)$. Moreover ϑ maps the set of all subalgebras of G containing D bijectively to the set of all subalgebras of $G|D$.*

Proof. We set $\Theta = \ker^{-1} D$. Let α be the lattice isomorphism of ch. 1, Th. 1.71. Then $(\ker)\alpha(\ker^{-1}) : \mathfrak{C} \to \mathfrak{N}(G|D)$ is a lattice isomorphism. But $a \in (\ker)\alpha(\ker^{-1})B$ means $a(\alpha \ker^{-1} B)0$ which is equivalent to $a = \vartheta u$, $u(\ker^{-1} B)0$, for some $u \in G$, i.e. $a \in \vartheta B$. Hence $(\ker)\alpha(\ker^{-1})B = \vartheta B$, for every $B \in \mathfrak{C}$. Let U be any subalgebra of $G|D$ and εU the set of the inverse images of its elements under ϑ. Then εU is a subalgebra of G containing D. On the other hand, ϑ maps every subalgebra of G containing D to a subalgebra of $G|D$. Moreover $\vartheta\varepsilon$ and $\varepsilon\vartheta$ are the identical mapping whence ϑ is bijective.

3.4. Lemma. *A subset A of the Ω-multioperator group G is an ideal of G if and only if*

a) *A is a normal subgroup of $\langle G; +, -, 0\rangle$,*

b) *if ω_i is an arbitrary operation of Ω with $n_i > 0$, then, for any $a \in A$, $(g_1, \ldots, g_{n_i}) \in G^{n_i}$, and $1 \leqslant \nu \leqslant n_i$, we have*

$$\omega_i g_1 \ldots g_{\nu-1}(g_\nu + a)g_{\nu+1} \ldots g_{n_i} - \omega_i g_1 \ldots g_{\nu-1} g_\nu g_{\nu+1} \ldots g_{n_i} \in A.$$

Proof. Let A be an ideal of G. Then $A = \ker\Theta$ whence by Prop. 3.21, A is a normal subgroup of $\langle G; +, -, 0\rangle$ and Θ is induced by the partition of G into the cosets of A. Hence $(g_\nu + a)\Theta g_\nu$, therefore $\omega_i g_1 \ldots (g_\nu + a) \ldots g_{n_i} \Theta \omega_i g_1 \ldots g_\nu \ldots g_{n_i}$ i.e. b) holds. Suppose now that a), b) are satisfied. Then the equivalence relation being induced by the partition of G into cosets of A is some congruence Θ and $\ker\Theta = A$. Hence A is an ideal.

3.41. Remark. Lemma 3.4 shows that for a group, regarded as a multi-operator group, the ideals are just the normal subgroups while for rings, regarded as multioperator groups, the ideals are the two-sided ideals in the sense of ring theory.

3.5. Proposition. (First isomorphism theorem for multioperator groups). *Let G be any Ω-multioperator group, U a subalgebra of G, and A an ideal of G. Then $U+A$ is a subalgebra of G, A is an ideal of $U+A$, $U\cap A$ is an ideal of U, and $U+A/A \cong U/U\cap A$.*

Proof. By the first isomorphism theorem for groups, $U+A$ is a subgroup of G. Since $0\in A$, we have $\omega_i \in U+A$ for any ω_i with $n_i = 0$, and if $u_1+a_1, \ldots, u_{n_i}+a_{n_i} \in U+A$, and ω_i is an n_i-ary operation of Ω, $n_i > 0$, then by Lemma 3.4, $\omega_i(u_1+a_1)\ldots(u_{n_i}+a_{n_i})-\omega_i u_1 \ldots u_{n_i} \in A$ whence $U+A$ is a subalgebra of G. A is an ideal of $U+A$ and $U\cap A$ is an ideal of U, by the first isomorphism theorem of group theory and Lemma 3.4. Also by the first isomorphism theorem of group theory, $\alpha : U+A|A \to U|U\cap A$, defined by $\alpha(u+A) = u+(U\cap A)$, is a group isomorphism. One checks easily that α is also a homomorphism w.r.t. the operations $\omega_i \in \Omega$.

3.51. Proposition. (Second isomorphism theorem for multioperator groups). *Let $\varphi: G \to H$ be any epimorphism of Ω-multioperator groups, B an ideal of H, and $A = \{a\in G|\varphi a \in B\}$. Then A is an ideal of G and $H|B \cong G|A$.*

Proof. By the second isomorphism theorem of group theory and Lemma 3.4, A is an ideal of G. Also, by the second isomorphism theorem of group theory, the mapping $\alpha : G|A \to H|B$, defined by $\alpha(g+A) = \varphi g+B$, is a group isomorphism. One checks easily that α is a homomorphism also w.r.t. the operations $\omega_i \in \Omega$.

4. Rings

4.1. Ring-theoretical definitions and results that are used in this book will now be compiled, but proofs will be given only for less widely-known lemmas. Moreover some important facts about roots and partial derivatives of polynomials over commutative rings with identity —even though they are well-known—will be proved for the sake of

completeness since they are frequently used in this book. We refer the reader to standard books like RÉDEI [2], VAN DER WAERDEN [1], [2] and ZARISKI-SAMUEL [1] for some further information.

A ring is an algebra $\langle R; +, \cdot\rangle$ with two binary operations $+$, $\cdot$ such that $\langle R; +\rangle$ is a commutative group whose identity is 0; $\cdot$ is associative and right and left distributive w.r.t. $+$. If $\cdot$ is also commutative, then R is called a commutative ring, and if $\cdot$ has a (left) identity, then R is called a ring with (left) identity.

Let R be any ring. An element $a\in R$ is called nilpotent if $a^n = 0$, for some integer $n > 0$. $a \neq 0$ is a zero divisor if there exists $0 \neq b \in R$ such that $ab = 0$. An idempotent $a \in R$ is an element with $a^2 = a$.

An (integral) domain is a commutative ring R with identity and without zero divisors, i.e. $ab = 0$ implies $a = 0$ or $b = 0$, for all $a, b \in R$. A (not necessarily commutative) ring K with identity 1 such that $\{a\in K|a \neq 0\}$ forms a group w.r.t. the multiplication is called a skew-field, and a commutative skew-field is a field.

Every field is an integral domain and every finite integral domain is a field. Moreover every finite skew-field is a field. A commutative ring with identity is a field if and only if it is a simple algebra with at least two elements.

Let D be any integral domain, then there is (up to isomorphisms that fix D) exactly one field K that contains D as a subring such that every $d\in K$ can be written as $d = ab^{-1}$, $a, b \in D$. K is then called the quotient field of D. An integral domain D is called integrally closed if every $x\in K$ that satisfies some equation $x^n+d_{n-1}x^{n-1}+\ldots+d_1x+d_0 = 0$, $d_i \in D$ belongs to D where K is the quotient field of D.

Let D be any integral domain. If $1 \in D$ has no finite order in the additive group of D, then D is said to be of characteristic 0, and if 1 is of additive order p, then D is of characteristic p. Such a number p is always a prime. We write char D for the characteristic of D. If char $D = p > 0$, then $(a+b)^p = a^p+b^p$, for all $a, b \in D$.

If R is a ring with identity, then a unit of R is an element $e\in R$ such that $de = ed = 1$, for some $d\in R$. The set of all units of R constitutes a group w.r.t. the multiplication. In a commutative ring R with identity, $b\in R$ is called an associate of $a\in R$ if $b = ae$, for some unit $e\in R$. The relation "being associated with" is an equivalence relation on R.

4.2. Let R be a commutative ring with identity. An element $b \in R$ is a divisor of $a \in R$ if $a = bc$, for some $c \in R$. If b is a divisor of a, we say b divides a or a is divisible by b and write $b|a$. If $b|a$, then b is called a proper divisor of a whenever b is not associated with a, and is called a non-trivial divisor if b is neither associated with a nor a unit of R. A non-zero element $p \in R$ is called an irreducible element of R if it is not a unit of R and has no non trivial divisor. (Sometimes we shall also say prime element instead of irreducible element).

An integral domain R is a unique factorization domain (UFD) if every non-zero non-unit $a \in R$ is a product of a finite number of irreducible elements and, for any two factorizations of such an element $a \in R$ into irreducible elements, there is a bijection between the two sets of factors such that each factor of the one factorization is mapped to an associate. If R is a UFD, then the polynomial ring $R[x]$ is also a UFD.

Let R be a UFD. If $p \in R$ is an irreducible element and $a \in R$, then the number of associates of p occurring in a decomposition of a into irreducible factors is called the multiplicity of p in a. The element a is square free if every irreducible element $p \in R$ has at most multiplicity 1 in a.

Let $a_1, \ldots, a_r$ be elements of the UFD R. An element $d \in R$ is a greatest common divisor (g.c.d) of $a_1, \ldots, a_r$, denoted by $(a_1, \ldots, a_r)$ if $d|a_i$, $i = 1, \ldots, r$ and if $c|a_i$, $i = 1, \ldots, r$, implies $c|d$, for any $c \in R$. An element $v \in R$ is a least common multiple (l.c.m.) of $a_1, \ldots, a_r$, denoted by $[a_1, \ldots, a_r]$ if $a_i|v$, $i = 1, \ldots, r$, and if $a_i|w$, $i = 1, \ldots, r$, implies $v|w$, for all $w \in R$. Greatest common divisors and least common multiples exist for any elements $a_1, \ldots, a_r \in R$, and are uniquely determined up to associates. If the irreducible $p \in R$ has multiplicity m_i in a_i, $i = 1, \ldots, r$, then p has multiplicity $\min(m_i | 1 \leqslant i \leqslant r)$ in $(a_1, \ldots, a_r)$ and multiplicity $\max(m_i | 1 \leqslant i \leqslant r)$ in $[a_1, \ldots, a_r]$. If $a, b \in R$, then $(a, b)\,[a, b] = ab$. The elements $a, b \in R$ are called relatively prime if $(a, b) = 1$. The elements $a_1, \ldots, a_r \in R$ are called pairwise relatively prime or coprimal if $(a_i, a_j) = 1$, for $i \neq j$. If $(a, b) = d$, then $a|d$, $b|d$ are relatively prime.

4.3. Let R be any ring. A non-empty subset $I \subseteq R$ is a left (right) ideal of R if $a, b \in I$ implies $a - b \in I$ and $a \in I$, $r \in R$ implies $ra \in I$ ($ar \in I$). An ideal of R is a left and right ideal of R (this definition coincides with

that in § 3 if we regard R as a multioperator group $\langle R; +, -, 0, \cdot \rangle$). If I is an ideal of R, then $a\Theta(I)b$ if and only if $a - b \in I$ defines some congruence $\Theta(I)$ on R, and Θ is a bijection from the set of all ideals of R to the set of all congruences on R. For $a\Theta(I)\,b$, usually $a \equiv b \bmod I$ is written and $R|I$ means $R|\Theta(I)$. The ideals $\{0\}$, the zero ideal, and R, the unit ideal, are called the trivial ideals of R.

For the remainder of this subsection, let R be a commutative ring with identity. If $a_1, \ldots, a_r \in R$, then the set $(a_1, \ldots, a_r) = \{t_1a_1 + \ldots + t_ra_r | t_i \in R\}$ is an ideal of R, the ideal generated by $a_1, \ldots, a_r$. $a_1, \ldots, a_r$ is called a finite ideal basis of the ideal I if $I = (a_1, \ldots, a_r)$. I is a principal ideal if $I = (a)$, for some $a \in R$; we then write $u \equiv v \bmod a$ instead of $u \equiv v \bmod (a)$. Clearly $(a) = Ra$.

If A, B are ideals of R, then their intersection $A \cap B$ and their sum $A + B = \{a + b | a \in A, b \in B\}$ which is sometimes denoted by (A, B) are also ideals. Moreover $AB = \left\{\sum_{i \in I} a_i b_i | a_i \in A, b_i \in B, I \text{ finite}\right\}$ is again an ideal, the product of A, B. Intersection, sum, and product of ideals satisfy the commutative and the associative law, and the product is distributive w.r.t. the sum. If $A = (a_1, \ldots, a_r)$, $B = (b_1, \ldots, b_s)$, then $AB = (a_1b_1, a_1b_2, \ldots, a_1b_s, a_2b_1, \ldots, a_rb_1, \ldots, a_rb_s)$. A^n shall mean the product of n equal ideals A.

Two ideals A, B are called comaximal if $A + B = R$. The ideals $A_1, \ldots, A_r$ are called pairwise comaximal if A_i, A_j are comaximal whenever $i \neq j$. If $A_1, \ldots, A_r$ are pairwise comaximal, then $A_1 \ldots A_r = A_1 \cap \ldots \cap A_r$, and any system of congruences $x \equiv a_i \bmod A_i$, $i = 1, \ldots, r$, has a solution in R which is unique mod $A_1 \ldots A_r$ (this is the well-known Chinese remainder theorem). Moreover if $C(a)$ denotes the congruence class of a under the congruence $\Theta(A_1 \ldots A_r)$ and $C_i(a)$, $i = 1, \ldots, r$, denotes the congruence class of a under $\Theta(A_i)$, then $\varphi C(a) = (C_1(a), \ldots, C_r(a))$ defines a ring isomorphism $\varphi : R|A_1 \ldots A_r \to (R|A_1) \times \ldots \times (R|A_r)$.

An ideal P of R is called a prime ideal of R if $R|P$ is an integral domain while an ideal Q is a primary ideal of R if every zero divisor in $R|Q$ is nilpotent. If Q is a primary ideal of R, then $\{b \in R | b^m \in Q$, for some integer $m > 0\}$ is a prime ideal of R, the so-called radical of Q or the prime ideal associated with Q. If Q, P are ideals of R, then Q is primary with associated prime ideal P if and only if: (i) $Q \subseteq P$, (ii) if $b \in P$, then $b^m \in Q$, for some integer $m > 0$, and (iii) if $ab \in Q$, $a \notin Q$, then $b \in P$.

If there is a positive integer n such that $P^n \subseteq Q$, then the least such integer is called the exponent of Q.

An ideal N of R is called nilpotent if $N^n = \{0\}$ for some integer $n > 0$.

4.4. A principal ideal domain (PID) is an integral domain R such that every ideal of R is principal. Every PID is a UFD. If $a_1, \ldots, a_r \in R$ and $d = (a_1, \ldots, a_r)$, then there exist elements $t_1, \ldots, t_r \in R$ such that $d = t_1a_1 + \ldots + t_ra_r$. An ideal (a) of R is a non-trivial prime ideal if and only if a is irreducible. For $a \neq 0$, the factor ring $R|(a)$ is a field if and only if a is irreducible.

A Euclidean domain is an integral domain R such that there exists a function φ from $R - \{0\}$ to the set of non-negative integers with (i) b/a implies $\varphi(b) \leqslant \varphi(a)$, for any non-zero elements $a, b \in R$, and (ii) if $0 \neq b, a \in R$, then there exist $q, r \in R$ with $a = bq + r$ and either $r = 0$ or $\varphi(r) < \varphi(b)$. Every Euclidean domain is a PID. The common examples of Euclidean domains are the ring of rational integers and the polynomial ring $K[x]$ over any field K.

4.5. A commutative ring R with identity is called noetherian if every ideal of R has a finite ideal basis. If R is noetherian, then the polynomial ring $R[x_1, \ldots, x_k]$ over R is also noetherian.

A Dedekind domain is a integral domain R where every ideal of R is a product of a finite number of prime ideals of R. Every Dedekind domain is noetherian and integrally closed. Every PID is Dedekind. The best known examples of Dedekind domains are the integral domains consisting of all algebraic integers in a finite extension field of the field of rational numbers. In particular, the ring of rational integers is Dedekind. If $A \subseteq B$ for two ideals of a Dedekind domain R, then there exists some ideal C in R such that $A = BC$.

Let R be a Dedekind domain. Then every non-trivial ideal A of R can be represented as a product of non-trivial prime ideals, and this representation, the so-called primary decomposition of A, is unique up to the order of the factors. If P is a non-trivial prime ideal of R, and A is a non-zero ideal, then the number of factors P in the decomposition of A into prime ideals is called the multiplicity of P in A. If a prime ideal P has multiplicity m_i in the ideals A_i, $i = 1, \ldots, r$, then P has the multiplicity $\min(m_i | 1 \leqslant i \leqslant r)$ in the sum and the multiplicity $\max(m_i | 1 \leqslant i \leqslant r)$ in the intersection of these ideals. Hence any two

powers $P_1^{e_1}, P_2^{e_2}$ of different non-trivial prime ideals P_1, P_2 are comaximal. An ideal Q of R is primary if and only if Q is a power of some prime ideal P, and this prime ideal is just the radical of Q.

Let R be a Dedekind domain, and A a non-trivial ideal of R. Then $R|A$ has only principal ideals, and if $0 \neq a \in A$, then there exists $b \in A$ such that $A = (a, b)$. Subsequently let R be a Dedekind domain.

4.51. Lemma. *Let P be a prime ideal of R. If $a \in R$ and the class $C(a)$ under $\Theta(P)$ is a unit of $R|P$, then the class $C_1(a)$ under $\Theta(P^e)$ is a unit of $R|P^e$.*

Proof. By hypothesis, there is $b \in R$, $p \in P$ such that $ab = 1 - p$ whence $ab(1 + p + \ldots + p^{e-1}) = 1 - p^e$.

4.52. Lemma. *Let P be a non-trivial prime ideal of R and $e > 0$ an integer. Then there exists a bijective mapping from P^e/P^{e+1} to R/P.*

Proof. Since every ideal of $R|P^{e+1}$ is principal, so is $P^e|P^{e+1}$. Say $P^e|P^{e+1} = (C(r))$ where $r \in P^e$ and $C(r)$ is the class of r under $\Theta(P^{e+1})$. Hence the equation $C(a) = C(r)\,C(x)$ has a solution $x \in R$, for any $C(a) \in P^e|P^{e+1}$. One verifies easily that the set $\vartheta C(a)$ of all solutions x of this equation is a class under $\Theta(P)$, that $\vartheta C(a) = \vartheta C(b)$ implies $C(a) = C(b)$, and that every element of $R|P$ is an image under ϑ.

4.53. Lemma. *Let P be a non-trivial prime ideal of R such that $|R|P|$ is finite, $e \geqslant 2$ an integer, $a \in P$ and $a \notin P^2$. If W_1 is a vector system mod P, W_{e-1} a vector system mod P^{e-1} (cf. ch. 4) then the sets $W = \{\mathfrak{u} + a\mathfrak{v} \mid \mathfrak{u} \in W_1, \mathfrak{v} \in W_{e-1}\}$ and $\overline{W} = \{\mathfrak{v} + a^{e-1}\mathfrak{u} \mid \mathfrak{u} \in W_1, \mathfrak{v} \in W_{e-1}\}$ are vector systems mod P^e.*

Proof. Let $|R|P| = r$, then by Lemma 4.52, $|W| = |\overline{W}| = |W_1|\,|W_{e-1}| = r^k(r^{e-1})^k = |R|P^e|^k$. If in W, $\mathfrak{u} + a\mathfrak{v} \equiv \mathfrak{u}_1 + a\mathfrak{v}_1 \bmod P^e$, then $\mathfrak{u} \equiv \mathfrak{u}_1 \bmod P$ whence $\mathfrak{u} = \mathfrak{u}_1$ and $\mathfrak{v} = \mathfrak{v}_1$, hence W is a vector system mod P^e. A similar argument shows that $\overline{W}$ is a vector system mod P^e.

4.6. Let R_1, R_2 be commutative rings with identity and $R = R_1 \times R_2$. Then for every ideal $A \subseteq R$, there exist ideals A_i of R_i, $i = 1, 2$, such that $A = A_1 \times A_2$. Moreover $A^n = A_1^n \times A_2^n$.

A commutative ring R with identity is called the inner direct product or the direct sum of its subrings R_1, R_2 if the mapping $\varphi: R_1 \times R_2 \to R$, defined by $\varphi(r_1, r_2) = r_1 + r_2$ is an isomorphism. If $d \in R$ is an idempotent, then R is the inner direct product of its subrings (d) and $(1-d)$ and if, conversely, R is the inner direct product of its subrings R_1, R_2, then there is an idempotent $d \in R$ such that $R_1 = (d)$ and $R_2 = (1-d)$. A commutative ring R with identity is called directly indecomposable if, in any representation of R as an inner direct product of subrings R_1, R_2, we have $|R_i| = 1$, for at least one i.

4.7. Let R be a commutative ring with identity, $R[x]$ the polynomial ring in x over R, and $f \in R[x]$. An element $a \in R$ is a root of f if $f(a) = 0$.

4.71. Lemma. *If a is a root of f, then the polynomial $x-a$ is a divisor of f in $R[x]$.*

Proof. We can write $f = (x-a)g+r$ where $g \in R[x]$, $r \in R$. If we substitute a for x, then $r = 0$ by the principle of substitution.

4.72. The greatest integer k such that $(x-a)^k$ is a divisor of f is called the multiplicity of a as a root of f.

4.73. Proposition. *Let R be any integral domain, $0 \neq f \in R[x]$ a polynomial of degree $[f]$, a_i, $i = 1, \ldots, r$, distinct roots of f, and k_i, $i = 1, \ldots, r$, the multiplicities of these roots. Then $k_1 + \ldots + k_r \leqslant [f]$ and f is divisible in $R[x]$ by the polynomial $(x-a_1)^{k_1} \ldots (x-a_r)^{k_r}$.*

Proof. The first statement follows from the second one and ch. 1, Prop. 8.31. We have $f = (x-a_1)^{k_1} g_1$. Suppose $f = (x-a_1)^{k_1} \ldots (x-a_{i-1})^{k_{i-1}} \cdot (x-a_i)^l g_{il}$ where $0 \leqslant l < k_i$. Then, since $R[x]$ is an integral domain, we have $(x-a_i)^{k_i-l} g = (x-a_1)^{k_1} \ldots (x-a_{i-1})^{k_{i-1}} g_{il}$, for some $g \in R[x]$. If we substitute a_i for x, and observe that R is an integral domain, we obtain $g_{il}(a_i) = 0$ whence $f = (x-a_1)^{k_1} \ldots (x-a_i)^{l+1} \bar{g}_{il}$, for some $\bar{g}_{il} \in R[x]$.

4.74. Proposition. *Let R be any integral domain of characteristic zero, and a a root of the non-zero polynomial $f \in R[x]$ of multiplicity k. Then a is a root of f' of multiplicity $k-1$.*

Proof. By hypothesis, $f = (x-a)^k g$ where $g \in R[x]$ and $g(a) \neq 0$. Hence $f' = k(x-a)^{k-1} g + (x-a)^k g' = (x-a)^{k-1}(kg + (x-a)g')$. If $(x-a)^k$ were a divisor of f', then a would be a root of the second factor whence $kg(a) = 0$. But then $k \cdot 1 = 0$, a contradiction.

4.75. Corollary. *If R is an arbitrary commutative ring with identity and a is a root of f of multiplicity $k > 1$, then a is also a root of f'.*

Proof. As in Prop. 4.74.

4.8. Let R be a commutative ring with identity and $R[x_1, \ldots, x_k]$ the polynomial ring over R in $x_1, \ldots, x_k$. For $1 \leqslant i \leqslant k$, we define mappings $\partial/\partial x_i = \partial_i : R[x_1, \ldots, x_k] \to R[x_1, \ldots, x_k]$ by: If $f \in R[x_1, \ldots, x_k]$ and $f = \sum a_{(l_1, \ldots, l_k)} x_1^{l_1} \ldots x_k^{l_k}$ is the normal form of f according to ch. 1, Th. 8.21, then $\partial_i f = \sum l_i a_{(l_1, \ldots, l_k)} x_1^{l_1} \ldots x_i^{l_i - 1} \ldots x_k^{l_k}$. The mapping ∂_i is called the i-th partial derivation of $R[x_1, \ldots, x_k]$ and $\partial_i f$ is called the i-th partial derivative of f. If $k = 1$, then we write x instead of x_1, $\mathrm{d}/\mathrm{d}x$ for $\partial/\partial x$, and f' for $(\mathrm{d}/\mathrm{d}x)f$.

4.81. Theorem. *Let R be a commutative ring with identity, $R[x_1, \ldots, x_k]$ a polynomial ring over R, ∂_i the i-th partial derivation of $R[x_1, \ldots, x_k]$, $\varkappa$ the composition of polynomials, and f, g, $g_1, \ldots, g_k \in R[x_1, \ldots, x_k]$. Then*

(i) $\partial_i a = 0$, *for* $a \in R$,
(ii) $\partial_i(f+g) = \partial_i f + \partial_i g$,
(iii) $\partial_i(fg) = (\partial_i f)g + f(\partial_i g)$
(iv) $\partial_i \varkappa f g_1 \ldots g_k = \sum_{\nu=1}^{k} (\varkappa(\partial_\nu f) g_1 \ldots g_k)\, \partial_i g_\nu$ (*"chain rule"*).

Proof. (i) and (ii) are obvious. Since (ii) and the distributive law for rings hold, we have to prove (iii) only for $f = a x_1^{l_1} \ldots x_k^{l_k}$, $g = b x_1^{m_1} \ldots x_k^{m_k}$, $a, b \in R$. Then $\partial_i(fg) = (l_i + m_i) ab x_1^{l_1 + m_1} \ldots x_i^{l_i + m_i - 1} \ldots x_k^{l_k + m_k} = (\partial_i f)g + f(\partial_i g)$. Similarly, since (ii) holds and $\varkappa$ is right superdistributive w.r.t. $+$, we have to prove (iv) only for $f = a x_1^{l_1} \ldots x_k^{l_k}$, $a \in R$. Then $\varkappa f g_1 \ldots g_k = a g_1^{l_1} \ldots g_k^{l_k}$. Repeated application of (iii) leads to

$$\partial_i \varkappa f g_1 \ldots g_k = \sum_{\nu=1}^{k} l_\nu a g_1^{l_1} \ldots g_\nu^{l_\nu - 1} \ldots g_k^{l_k} \partial_i g_\nu = \sum_{\nu=1}^{k} [\varkappa(\partial_\nu f) g_1 \ldots g_k] \partial_i g_\nu .$$

4.82. Let $f \in R[x_1, \ldots, x_k]$, $r \geqslant 1$ an integer, $1 \leqslant i_\nu \leqslant k$, $\nu = 1, \ldots, r$. Then the mapping $\partial_{i_1} \partial_{i_2} \ldots \partial_{i_r} : R[x_1, \ldots, x_k] \to R[x_1, \ldots, x_k]$ is called a partial derivation of order r of $R[x_1, \ldots, x_k]$ and $\partial_{i_1} \partial_{i_2} \ldots \partial_{i_r} f$ a partial derivative of order r of f.

4.83. Lemma. *If $[f] = n$, then all partial derivatives of order $t > n$ of f are zero.*

Proof. The application of a partial derivation ∂_i to a polynomial f either decreases $[f]$ by at least 1, or $\partial_i f = 0$.

4.84. Theorem (Taylor's formula). *Assume that $f \in R[x_1, \ldots, x_k]$ with $[f] = n$ and $a_1, \ldots, a_k, g_1, \ldots, g_k$ are elements of a commutative ring S with identity containing R as a subring. Then*

$$f(a_1+g_1, \ldots, a_k+g_k) = f(a_1, \ldots, a_k) + \sum_{i_1=1}^{k} (\partial_{i_1} f)(a_1, \ldots, a_k) g_{i_1}$$
$$+ (1/2!) \sum_{i_1, i_2=1}^{k} (\partial_{i_1} \partial_{i_2} f)(a_1, \ldots, a_k) g_{i_1} g_{i_2} + \ldots$$
$$+ (1/n!) \sum_{i_1, i_2, \ldots, i_n=1}^{k} (\partial_{i_1} \partial_{i_2} \ldots \partial_{i_n} f)(a_1, \ldots, a_k) g_{i_1} \ldots g_{i_n}.$$

Proof. By Th. 4.81, (ii), Lemma 4.83, and the right superdistributivity of $\varkappa$ w.r.t. $+$, Th. 4.84 is true for all $f \in R[x_1, \ldots, x_k]$ if it is true for $f = a x_1^{l_1} \ldots x_k^{l_k}$, $a \in R$. The left-hand side of Taylor's formula is then $a(a_1+g_1)^{l_1} \ldots (a_k+g_k)^{l_k}$. Using the distributive laws, we expand this expression. Then, for any k-tuple $(r_1, \ldots, r_k)$ of non-negative integers with $r_1 + \ldots + r_k \leqslant [f]$, the term with second factor $g_1^{r_1} \ldots g_k^{r_k}$ has as its first factor $(l_1!/r_1!(l_1-r_1)!) \ldots (l_k!/r_k!(l_k-r_k)!) a a_1^{l_1-r_1} \ldots a_k^{l_k-r_k}$ if $r_i \leqslant l_i$, $i = 1, \ldots, k$, and zero otherwise. On the right-hand side of Taylor's formula, the term with second factor $g_1^{r_1} \ldots g_k^{r_k}$ has as its first factor $(1/(r_1+ \ldots +r_k)!)((r_1+ \ldots +r_k)!/r_1! \ldots r_k!)(l_1!/(l_1-r_1)!) \ldots (l_k!/(l_k-r_k)!) a a_1^{l_1-r_1} \ldots a_k^{l_k-r_k}$ if $r_i \leqslant l_i$, $i = 1, \ldots, k$, and zero otherwise.

4.85. Let $R[x_1, \ldots, x_k]$ be the polynomial ring in $x_1, \ldots, x_k$ over a commutative ring R with identity and $\mathfrak{f} = (f_1, \ldots, f_k)$ an element of $R[x_1, \ldots, x_k]^k$. The Jacobian determinant $\partial \mathfrak{f}$ of $\mathfrak{f}$ is the determinant of the $k \times k$-matrix $\Delta \mathfrak{f} = (\partial_t f_s)$ where s means the row and t the column index.

5. Fields

5.1. First we are going to review standard concepts and results on fields that are used in this book (for details cf. RÉDEI [2], VAN DER WAERDEN [1], ZARISKI-SAMUEL [1]). Then we treat, in more detail, a few results on the rational function field $K(x)$ which are crucial for some sections of ch. 4, and are not so well-known, as we believe.

Let K be any field. A subset S of K is called a subfield if S is a subring of K which is a field. S is a proper subfield of K if $S \subset K$. A proper subfield S of K is called a maximal subfield of K if there is no proper subfield S_1 with $S \subset S_1$. If $(S_i | i \in I)$ is a family of subfields of K, then $\bigcap (S_i | i \in I)$ is also a subfield of K. Let S be a subfield of K and U a subset of K, then the intersection of all subfields of K containing $S \cup U$ will be denoted by $S(U)$, and we say that $S(U)$ is obtained from S by adjoining U.

A field P is called a prime field if P has no proper subfield. Up to ring isomorphism, the prime fields are just the field of rational numbers and the factor rings $\mathbf{Z}|(p)$ where $\mathbf{Z}$ is the ring of rational integers and p is a prime. Any field K has exactly one prime field P amongst its subfields, being called the prime field of K.

Let K be a field. A field L containing K as a (proper) subfield is called a (proper) extension field of K. The extension field L of K is called a simple extension of K if there is $u \in L$ such that $L = K(u)$. Any extension field L of K can be viewed as a K-vector space w.r.t. addition and multiplication in L, the dimension of which is called the degree $[L : K]$ of L over K. If $[L : K]$ is finite, then L is called a finite extension field of K. If $a \in L$, then $[K(a) : K]$ is called the degree of a over K. If L is a finite extension field of K, and M is a finite extension field of L, then M is a finite extension field of K and $[M : K] = [M : L][L : K]$. Let L and L_1 be extension fields of K. An isomorphism $\varphi : L \to L_1$ is called a K-isomorphism if φ fixes K; if $L = L_1$, then φ is called a K-automorphism. Two extension fields L, L_1 of K are called K-equivalent if there is a K-isomorphism from L to L_1.

5.2. Let K be any field and $K[x]$ the polynomial ring in x over K. A transcendental element over K is an element a of an extension field of K such that $f \in K[x]$, $f(a) = 0$ implies $f = 0$, otherwise a is called algebraic over K.

Let a be algebraic over K. Then there is exactly one monic irreducible polynomial $p \in K[x]$ such that $p(a) = 0$, and $f(a) = 0$ implies p/f, for

any $f \in K[x]$. The polynomial p is called the minimal polynomial of a over K. $[p]$ equals the degree of a over K.

An extension field L of K is called an algebraic extension of K or algebraic over K if every element of L is algebraic over K. Otherwise we speak of a transcendental extension of K. If L is a finite extension field of K, then L is algebraic over K, and there exists a finite subset $\{a_1, \ldots, a_r\}$ of L such that $L = K(a_1, \ldots, a_r)$. Conversely, if $a_1, \ldots, a_r \in L$ are algebraic over K, then $K(a_1, \ldots, a_r)$ is a finite extension field of K.

A field L is called algebraically closed if every element which is algebraic over L belongs to L. If K is an arbitrary field, then there exists an extension field C of K which is an algebraic extension of K and algebraically closed, and any two such fields are K-equivalent. C is called an algebraic closure of K.

Let L be an extension field of K. Two elements $a, b \in L$ are called conjugate over K if they are algebraic over K and have the same minimal polynomial over K.

Let L be a finite extension field of K, $a \in L$, $u_1, \ldots, u_n$ any K-basis for L. Then $au_i = \sum_{j=1}^{n} b_{ij} u_j$, $b_{ij} \in K$, $i = 1, \ldots, n$. The determinant of the $n \times n$-matrix (b_{ij}) is independent of the choice of the basis $u_1, \ldots, u_n$ and is called the norm $\mathcal{N}_{L|K}(a)$ of $a \in L$ over K. We have $\mathcal{N}_{L|K}(a_1 a_2) = \mathcal{N}_{L|K}(a_1)\,\mathcal{N}_{L|K}(a_2)$, if $a_1, a_2 \in L$. If $a \in L$, $[K(a) : K] = m$, $[L : K(a)] = n$, and c is the constant term of the minimal polynomial of a over K, then $\mathcal{N}_{L|K}(a) = (-1)^{mn} c^n$.

Let K be any field and $f \in K[x]$ a non-constant polynomial. Then there exists an extension field L of K such that f is the product of linear factors in $L[x]$ and such that L is obtained from K by adjoining the roots of f in L. Such a field L is called a splitting field for f over K. Any two splitting fields for f over K are K-equivalent. An extension field L of K is called a normal extension of K if L is algebraic over K and every irreducible polynomial $f \in K[x]$, which has one root in L, is the product of linear factors in $L[x]$. An extension field L of K is a finite normal extension of K if and only if L is a splitting field for f over K, for some $f \in K[x]$. If L is a finite normal extension of K and M is a subfield of L containing K, then every K-isomorphism from M to any subfield of L can be extended to an automorphism of L. For any finite extension field L of K, there exists a finite normal extension N of K which contains L such that there

is no proper subfield M of N which contains L and is a normal extension of K. N is called a least normal extension field of $L|K$.

5.3. Let K be any field. A separable polynomial of $K[x]$ is an irreducible polynomial $f \in K[x]$ such that $f' \neq 0$, otherwise f is called inseparable. An element separable over K is an element a algebraic over K such that the minimal polynomial of a over K is separable; otherwise a is called inseparable. An algebraic extension L of K is called separable over K if every $a \in L$ is separable over K, otherwise L is called inseparable. If char $K = 0$, then every algebraic extension of K is separable.

If L is an algebraic extension of K, then the subset S of L consisting of all elements of L which are separable over K is a subfield of L containing K. If L is a normal extension of K, then S is also a normal extension of K. Let L be a finite extension of K, char $L = p$, and S the subfield of L consisting of the elements of L which are separable over K. Then there is an integer $e \geqslant 0$ such that $a^{p^e} \in S$, for every $a \in L$. The least such e is called the exponent of the extension $L|K$.

5.4. Let K be any field and $n > 0$ an integer. An n-th root of unity over K is an element z of an extension field of K which is a root of the polynomial $x^n - 1$. A primitive n-th root of unity is an n-th root of unity which is not an m-th root of unity, for all $m < n$. If char K does not divide n, then there are always primitive n-th roots of unity over K, and for any primitive n-th root of unity z, the degree of z over K divides $\varphi(n)$, φ being the Euler φ-function.

5.5. Let L be any finite normal separable extension of the field K. Then the set G of all K-automorphisms of L is a finite group w.r.t. the composition of mappings, the so-called Galois group of L over K. We have $|G| = [L : K]$. The fundamental theorem of Galois theory tells us that there is a bijective mapping from the set of all subgroups of G to the set of all subfields of L containing K. An abelian (cyclic) extension of K is a finite normal separable extension L of K such that the Galois group of L over K is abelian (cyclic). If L is an abelian extension of K, then every subfield of L containing K is a normal extension of K. If K is a field and n a positive integer such that char K does not divide n and K contains n n-th roots of unity, then the splitting field of any polynomial $x^n - a \in K[x]$ over K is a cyclic extension of K. If, conversely, $L = K(a)$ is a cyclic extension of K,

$[L:K]$ is a prime $q \neq \text{char } K$, K contains q q-th roots of unity, and σ is a K-automorphism of L generating the Galois group of L over K, then there exists a q-th root of unity $z \in K$ such that the "Lagrange resolvent" $l = a+z(\sigma a)+z^2(\sigma^2 a)+ \ldots +z^{q-1}(\sigma^{q-1}a)$ satisfies $l^q \in K$ and $K(l) = L$.

5.6. Let K be a finite field. Then char $K = p$, a prime, and $|K|$ is a power of p. Conversely if $p^e > 1$ is a power of the prime p, there is, up to isomorphism, exactly one field K of order p^e. If K is a finite field, then $\{a \in K \mid a \neq 0\}$ is a cyclic group w.r.t. the multiplication in K. If K is a finite field and $|K| = q$, then every element of K is a root of the polynomial $x^q - x \in K[x]$.

If K is a finite field of order p^e, then every subfield S of K has order p^f where $f|e$ and conversely for every p^f with $f|e$, there exists exactly one subfield of K of order p^f. If $|K| = p^e$ and S is a subfield of K of order p^f, then K is a finite extension field of S and $[K:S] = e/f$. Every automorphism ϑ of K is of the form $\vartheta a = a^{p^r}$, $a \in K$, $r = 0, 1, \ldots, e-1$, and the S-automorphisms of K are those automorphisms of K for which r is divisible by f.

5.7. Let K be any field. The quotient field Q of $K[x]$ is called the field of rational functions in x over K and is denoted by $K(x)$. $K[x]$ is a subring of $K(x)$ whence $K(x)$ is an extension field of K. An "intermediate field of $K(x)$" is a subfield of $K(x)$ which contains K.

5.71. Theorem. *If $r \in K(x)$, $r \notin K$, then r is transcendental over K and $K(x)$ is algebraic over $K(r)$. If $r \in K(x)$, then $K(r) = K(x)$ if and only if r is of the form $(ax+b)/(cx+d)$ and $r \notin K$. If $r \in K[x]$, then the degree $[K(x):K(r)]$ equals the degree $[r]$ of r.*

5.72. Theorem (Lüroth). *Every intermediate field $S \neq K$ of $K(x)$ is a simple transcendental extension field of K, i.e., there is an element $r \in K(x)$ which is transcendental over K such that $S = K(r)$.*

5.73. In the subsequent subsections, we will derive a few results on intermediate fields of $K(x)$ which are not too well known. Throughout these subsections we assume that char $K = 0$ (though some results of these subsections will also hold for arbitrary fields K).

5.8. Lemma. *Let U be an intermediate field of $K(x)$ which contains a polynomial $f \in K[x]$ of positive degree. Then there is a polynomial $r \in K[x]$ of positive degree such that $U = K(r)$.*

Proof. By Th. 5.72, $U = K(r)$ for some $r \in K(x)$, whence $r = g/h$, $g, h \in K[x]$. If $[g] < [h]$, we put $s = 1/r$, then $U = K(s)$, and if $[g] = [h]$, then we put $s = 1/(r-a) = h/(g-ah)$ where $a \in K$ is chosen in such a way that $[g-ah] < [h]$. Again $U = K(s)$. Therefore we can assume that $[g] > [h]$. Moreover we may assume that $(g, h) = 1$, otherwise we cancel by the g.c.d. of g and h. If $f \in U$, then $f = u(r)/v(r)$, $u, v \in K[x]$, whence $fv(r) = u(r)$. Let $u = \sum_{i=0}^{m} a_i x^i$, $v = \sum_{i=0}^{n} b_i x^i$, $a_m \neq 0$, $b_n \neq 0$. Then

$$f h^m \sum_{i=0}^{n} b_i g^i h^{n-i} = h^n \sum_{i=0}^{m} a_i g^i h^{m-i}. \tag{5.81}$$

Since the degrees of the polynomials on either side of (5.81) are equal and $[g] > [h]$, we have $[f]+m[h]+n[g] = n[h]+m[g]$ whence $m > n$. By (5.81), h divides $a_m g^m$. Since $(g, h) = 1$ and $K[x]$ is a UFD, we conclude $[h] = 0$ whence $r \in K[x]$. Clearly $[r] > 0$.

5.81. Lemma. *Let $g \in K[x]$ and $k \in K(g) \cap K[x]$. Then there exists $p \in K[x]$ such that $k = p(g)$.*

5.82. Corollary. *Let $g \in K[x]$, $[g] > 0$, and $h \in K(g) \cap K[x]$ be of minimal positive degree. Then $K(h) = K(g)$.*

Proof. If $[g] = 0$, then the lemma is obviously true. If $[g] > 0$, then $k = u(g)/v(g)$, $u, v \in K[x]$, whence $u(g) = kv(g)$. On the other hand, $u = vp+t$, $p, t \in K[x]$ such that $[t] < [v]$ or $t = 0$. Hence $u(g) = v(g)\,p(g)+t(g)$. This implies

$$v(g)\,(k-p(g)) = t(g). \tag{5.82}$$

By Th. 5.71, $t \neq 0$ implies $t(g) \neq 0$, thus $v(g) \neq 0$ and $k-p(g) \neq 0$. By (5.82), this contradicts $[t] < [v]$. Hence $t = 0$, $u(g) = v(g)\,p(g)$ which implies $k = p(g)$.

Let h be as in the corollary. Then $[h] \leqslant [g]$, and by Lemma 5.81, also $[h] \geqslant [g]$, thus $[h] = [g]$. Moreover, by Lemma 5.81, $h = p(g)$, for some $p \in K[x]$, whence $[p] = 1$. Therefore $p = ax+b$, $0 \neq a$, $b \in K$ and $K(h) = K(g)$.

5.83. Lemma. *Let* $f(x) = a_0x^{rn}+a_1x^{rn-1}+ \ldots$ *be a polynomial of* $K[x]$ *of degree* $rn \neq 0$. *Then there exists exactly one monic polynomial* g *of degree* n *in* $K[x]$ *such that* $[f-a_0g^r] < (r-1)n$ *or* $f-a_0g^r = 0$.

Proof. If $g = x^n+b_1x^{n-1}+ \ldots +b_{n-1}x+b_n$, then $g^r = x^{rn}+(rb_1)x^{rn-1}+ +(rb_2+w_1(b_1))x^{rn-2}+ \ldots +(rb_n+w_{n-1}(b_1, \ldots, b_{n-1}))x^{rn-n}+ \ldots$ where $w_i(x_1, \ldots, x_i)$, $i=1, \ldots, n-1$, is a polynomial over the ring of rational integers. If we additionally define $w_0 = 0$, then $f-a_0g^r = c_1x^{rn-1}+c_2x^{rn-2}+ \ldots +c_nx^{rn-n}+ \ldots$ where $c_i = a_i-a_0[rb_i+w_{i-1}(b_1, \ldots, b_{i-1})]$, $1 \leqslant i \leqslant n$. Clearly the system $a_i-a_0[rb_i+w_{i-1}(b_1, \ldots, b_{i-1})] = 0$, $1 \leqslant i \leqslant n$, of equations in $b_1, \ldots, b_n$, has exactly one solution in K.

5.84. Theorem. *Let* $f, g \in K[x]$ *be polynomials of positive degree such that the intermediate field* $D = K(f) \cap K(g)$ *of* $K(x)$ *contains a polynomial of positive degree, and* $H = K(f, g)$. *Then:*

a) *If* k *is a polynomial of minimal positive degree in* D, *then* $D = K(k)$ *and* $[k]$ *equals the least common multiple* v *of* $[f]$, $[g]$.

b) *If* h *is a polynomial of minimal positive degree in* H, *then* $H = K(h)$, *and* $[h]$ *is the greatest common divisor* x *of* $[f]$, $[g]$.

c) $[H : K(f)] = [K(g) : D]$ *and* $[H : K(g)] = [K(f) : D]$.

d) *If* D *is a maximal subfield of* $K(f)$ *and of* $K(g)$, *then* $K(f)$ *and* $K(g)$ *are maximal subfields of* H.

Proof. Since both D and H contain a polynomial of positive degree, the first satements of *a*), *b*) follow from Lemma 5.8 and Cor. 5.82. If $p \in K[x]$, $0 \neq a \in K$, then $K(ap) = K(p)$. Hence we can assume that f, g, h, k are monic.

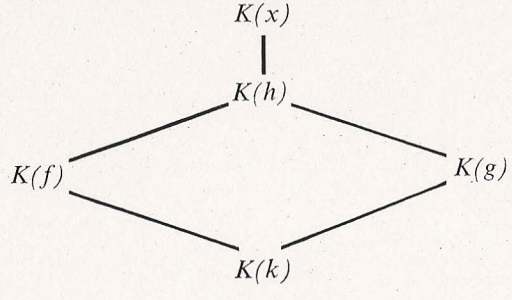


FIG. 6.2

By Th. 5.71, $[k]$ is divisible by $[f]$, $[g]$ whence $v/[k]$. Let $[k] = rv$. By Lemma 5.81, there exist polynomials $p, q \in K[x]$ such that $k = p(f) = q(g)$. Since k, f, g are monic, p and q are monic. Moreover $[p][f] = [q][g] = [k]$. Since $vd = [f][g]$, we have $[p] = rv/[f] = r[f][g]/[f]d = rm$ where $m = [g]/d$, and similarly $[q] = rn$ where $n = [f]/d$. By Lemma 5.83, there are monic polynomials s, $t \in K[x]$, $[s] = m$, $[t] = n$ such that $[p-s^r] < (r-1)m$, $[q-t^r] < (r-1)n$. Hence $[p(f)-s(f)^r] < (r-1)\,m[f] = (r-1)v$, and similarly $[q(g)-t(g)^r] < (r-1)v$. Hence $[s(f)^r-t(g)^r] < (r-1)v$, i.e. $[s(f)-t(g)]\,[s(f)^{r-1}+s(f)^{r-2}t(g)+ \ldots +t(g)^{r-1}] < (r-1)v$. Every term of the second factor on the left-hand side is monic and of degree $(r-1-i)[s][f]+i[t][g] = (r-1-i)v+iv = (r-1)v$. Since char $K = 0$, the second factor as a whole is thus of degree $(r-1)v$. Hence $s(f)-t(g) = 0$, therefore $s(f) = t(g) = w \in K[x]$ where $[w] = m[f] = v$ and $w \in K(f) \cap K(g) = K(k)$. By Lemma 5.81, $[w] \geqslant [k]$ whence $v \geqslant rv$, thus $r = 1$ and $[k] = v$.

Furthermore $[K(h) : K(k)] = [K(f)(g) : K(f)]\,[K(f) : K(k)]$. But $K(g) = K(k)(g)$ and $[K(g) : K(k)] = [k]/[g] = v/[g] = n$ implies $[K(f)(g) : K(f)] \leqslant n$. On the other hand, $[K(f) : K(k)] = m$, $(m, n) = 1$, and m and n divide $[K(h) : K(k)]$. Hence $[K(h) : K(k)] = mn$. Therefore $[h] = [K(x) : K(h)] = [k]/mn = v/mn = d$. Thus a), b) hold. Since $[f][g] = vd$, c) follows.

Finally, suppose that the hypothesis of d) is satisfied and that U is a field between $K(f)$ and $K(h)$. By Lemma 5.8, $U = K(l)$, $l \in K[x]$. We have $K(k) \subseteq K(l) \cap K(g) \subseteq K(g)$. If $K(l) \cap K(g) = K(g)$, then $K(l) = K(f, g) = K(h)$. Suppose now that $K(l) \cap K(g) = K(k)$. Since $K(l, g) = K(h)$, a) and b) imply that $([l], [g]) = ([f], [g])$ and $[[l], [g]] = [[f], [g]]$ whence $[l][g] = [f][g]$. Therefore $[l] = [f]$, hence $K(l) = K(f)$.

5.85. A chain of fields $K_0 \subset K_1 \subset \ldots \subset K_r$ is called a maximal chain if every member is a maximal subfield of the subsequent one.

5.86. Theorem. *Let* $f \in K[x]$ *be of positive degree and*

$$K(f) = S_0 \subset S_1 \subset \ldots \subset S_m \subset S_{m+1} = K(x),$$
$$K(f) = T_0 \subset T_1 \subset \ldots \subset T_n \subset T_{n+1} = K(x)$$

be two maximal chains of subfields from $K(f)$ *to* $K(x)$. *Then*

a) $m = n$.

b) *The degrees* $[S_i : S_{i-1}]$ *can be paired off with the degrees* $[T_j : T_{j-1}]$.

c) *The first chain can be transformed into the second one by applying finitely many times the following procedure: Take any member of the first chain different from* S_0 *and* S_{m+1} *and replace this member by a different field such that the new chain becomes again a maximal chain.*

Proof. WLOG, we may assume $m \leqq n$. Suppose that i is the greatest index such that $S_i = T_i$. We proceed by induction on $m+1-i$. If $m+1-i = 0$, nothing has to be proved. Now let $m+1-i = e > 0$. Then the two chains are

$$\mathfrak{R}_1 : S_0 \subset S_1 \subset \ldots \subset S_{m-e+1} \subset S_{m-e+2} \subset \ldots \subset S_{m+1},$$
$$\mathfrak{R}_2 : S_0 \subset S_1 \subset \ldots \subset S_{m-e+1} \subset T_{m-e+2} \subset \ldots \subset T_{n+1}$$

where $S_{m-e+2} \neq T_{m-e+2}$. Let H be the field $S_{m-e+2}(T_{m-e+2})$. Since S_{m-e+1} is a maximal subfield of S_{m-e+2} and T_{m-e+2}, we have $S_{m-e+1} = S_{m-e+2} \cap T_{m-e+2}$. By Lemma 5.8, S_{m-e+2}, T_{m-e+2} satisfy the hypothesis of Th. 5.84 whence d) implies that S_{m-e+2}, T_{m-e+2} are maximal subfields of H. Now we take any maximal chain $H \subset H_1 \subset \ldots \subset K(x)$ from H to $K(x)$ which can always be done since $[K(x) : H]$ is finite, and consider the two maximal chains

$$\overline{\mathfrak{R}}_1 : S_0 \subset S_1 \subset \ldots \subset S_{m-e+1} \subset S_{m-e+2} \subset H \subset H_1 \subset \ldots \subset K(x),$$
$$\overline{\mathfrak{R}}_2 : S_0 \subset S_1 \subset \ldots \subset S_{m-e+1} \subset T_{m-e+2} \subset H \subset H_1 \subset \ldots \subset K(x).$$

By induction, a), b), c) hold for the chains $\mathfrak{R}_1$ and $\overline{\mathfrak{R}}_1$. Hence the number of members in $\overline{\mathfrak{R}}_2$ equals the number of members in $\mathfrak{R}_1$. Again by induction, a), b), c) hold for the chains $\overline{\mathfrak{R}}_2$ and $\mathfrak{R}_2$. By Th. 5.84 c), also the chains $\overline{\mathfrak{R}}_1$, $\overline{\mathfrak{R}}_2$ satisfy a), b), c) whence the theorem is proved.

5.87. Remark. The number of different maximal chains of subfields from $K(f)$ to $K(x)$ is finite.

Proof. By Th. 5.71, $K(x)$ is algebraic of degree $[f]$ over $K(f)$. Since $\operatorname{char} K = 0$, $K(x)$ is separable over $K(f)$. Let N be a least normal extension field of $K(x)|K(f)$ (see § 5.2). Then N is of finite degree over $K(f)$ and is separable over $K(f)$. By the fundamental theorem of Galois theory, the number of fields between $K(f)$ and N is finite, therefore – a fortiori – the number of fields between $K(f)$ and $K(x)$ is finite. Hence there is only a finite number of maximal chains from $K(f)$ to $K(x)$.

5.88. Let f, g be two non-constant polynomials of $K[x]$ such that $K(g) \subseteq K(f)$. $\mathcal{N}_{f|g}(h)$ will denote the norm $\mathcal{N}_{K(f)|K(g)}(h)$ of an element h in the finite algebraic extension $K(f)$ of $K(g)$. Then $\mathcal{N}_{f|g}(h)$ equals – up to the sign – the $[K(f) : K(g)(h)]$-th power of the constant term of the minimal polynomial of h over $K(g)$ and $\mathcal{N}_{f|g}(h_1 h_2) = \mathcal{N}_{f|g}(h_1)\,\mathcal{N}_{f|g}(h_2)$, for all $h_1, h_2 \in K(f)$.

5.9. Let K be a field and $K(x)$ the field of rational functions in x over K. Let $\partial : K(x) \to K(x)$ be defined by: If $r = u/v$, $u, v \in K[x]$, then $\partial r = (vu' - uv')/v^2$. ∂ is well-defined since, if $r = u_1/v_1$ is the unique representation of r as a quotient of polynomials $u_1, v_1 \in K[x]$ such that $(u_1, v_1) = 1$ and v_1 is monic, then $u = tu_1$, $v = tv_1$, $t \in K[x]$. Hence $(vu' - uv')/v^2 = (v_1 u_1' - u_1 v_1')/v_1^2$. ∂ is an extension of the derivation d/dx of $K[x]$, we will write therefore $\partial = d/dx$, set $(d/dx)r = r'$, and will call r' the derivative of r.

5.91. Theorem. *Let* $r, s \in K(x)$ *and* $f \in K[x]$. *Then:*

(i) $(r+s)' = r' + s'$,

(ii) $(rs)' = r's + rs'$,

(iii) $f(r)' = f'(r)r'$.

Proof. We set $r = u/v$, $s = u_1/v_1$ and compute either side of (i) and (ii). (iii) follows easily from (i) and (ii).

6. Semigroups and groups

6.1. Very little is used in this book from the theory of semigroups, but quite a lot from group theory. Both will be reviewed now, details can be found in books like HUPPERT [1], KUROŠ [1], SPECHT [1]. At the end of this section we will also prove a few lemmas which are not so well-known.

A semigroup is an algebra $\langle S; \cdot \rangle$ with an associative binary operation $\cdot$. If $\cdot$ is also commutative, S is called a commutative semigroup. If S is a semigroup and U, V are subsets of S, then the "complex product" UV is defined to be the set $\{uv \mid u \in U, v \in V\}$. U^n will denote the complex

product of n factors U. If U is an arbitrary subset of S, then the subsemigroup $[U]$ generated by U is just $[U] = \cup(U^n | n = 1, 2, 3, \ldots)$.

Let S be a semigroup with identity 1. If $u \in S$, then $v \in S$ is called a left (right) inverse of u if $vu = 1$ ($uv = 1$). If v is a right as well as a left inverse of u, then v is called an inverse of u. Every element of S has at most one inverse. The elements of S that possess inverses are called the units of S. The set of all units of S is a subsemigroup $E = \mathcal{E}(S)$ of S, and E is a group.

If S is a commutative semigroup with identity 1 and H is a subsemigroup of S that is a group such that $1 \in H$, then the set of all subsets aH of S is a semigroup w.r.t. complex multiplication, the so-called factor semigroup of S modulo H. If $|S|$ is finite, then the factor semigroup is of order $|S|/|H|$.

Let S be any semigroup. A left (right) regular element of S is an element $a \in S$ such that $au = av$ ($ua = va$) implies $u = v$, for all $u, v \in S$. a is called regular if a is right as well as left regular. An idempotent is an element $a \in S$ such that $a^2 = a$.

A partially ordered semigroup is a semigroup S together with a partial order relation $\leqslant$ such that $a \leqslant b$ implies $ax \leqslant bx$ and $xa \leqslant xb$, for all $x \in S$. If $\leqslant$ is a total order relation, then S is called a totally ordered semigroup.

6.2. A group is a semigroup G with identity such that every element of G possesses an inverse. A semigroup with identity such that every element has a left inverse is a group. An abelian group is a commutative group.

Let U be a subgroup of G. A subset aU, $a \in G$, of G isca lled a left coset of G modulo U while the subsets Ua are called right cosets of G modulo U. The set of all left (right) cosets of G modulo U is a partition of G. The cardinality of the set of all blocks of this partition is equal for left and right cosets and is denoted by $[G : U]$. If G is a finite group and U is a subsemigroup of G, then U is a subgroup of G. The order of any subgroup of a finite group G divides the order of G. A proper subgroup U of G is called maximal if $U \subset V$ implies $V = G$, for any subgroup V of G.

Let G be a group and $g \in G$. The order of g is the order of the subgroup $[g]$ generated by g. A torsionfree group is a group with no element $g \neq 1$ of finite order. Let p, q be two distinct primes, then a group G is called a p-group if the order of every element of G is a power of p, and G is called a (p, q)-group if the order of every element of G is a product of powers of p and q. A group G is called cyclic if $G = [g]$, for some $g \in G$. Any group of prime order is cyclic. If G is a finite cyclic group, then G has exactly one subgroup of order d, for any divisor d of $|G|$. If the order of the elements in a group G is bounded, there exists a least positive integer n such that $g^n = 1$, for all $g \in G$, and n is called the exponent $\exp G$ of G. An elementary abelian group is an abelian group G with $\exp G = p$ where p is a prime.

The set $\operatorname{End} G$ of all endomorphisms of a group G is a semigroup w.r.t. the composition of mappings. The set $\operatorname{Aut} G$ of all automorphisms of a group G is a group w.r.t. the composition of mappings. $\vartheta \in \operatorname{Aut} G$ is called an inner automorphism of G if $\vartheta g = aga^{-1}$, for all $g \in G$ and some $a \in G$. The set $\operatorname{In} G$ of all inner automorphisms of G is a subgroup of $\operatorname{Aut} G$. Two subgroups H_1, H_2 (elements h_1, h_2) of G are called conjugate if $\vartheta H_1 = H_2 (\vartheta h_1 = h_2)$, for some $\vartheta \in \operatorname{In} G$. If G is a finite cyclic group, then $|\operatorname{Aut} G| = \varphi(|G|)$ where φ is the Euler φ-function.

Let G be any group and $\Omega \subseteq \operatorname{End} G$. If we regard $\omega_i \in \Omega$ as a 1-ary operation on G, then, since $\omega_i 1 = 1$, for all $\omega_i \in \Omega$, G together with Ω is an Ω-multioperator group $(G; \Omega)$, in short an Ω-group. The subalgebras of $(G; \Omega)$ are called Ω-admissible subgroups of G. If Ω is the set of all endomorphisms, automorphisms, inner automorphisms of G, resp., then the Ω-admissible subgroups of G are called fully invariant, characteristic, normal, resp. If T is a subset of G and $[\Omega]$ is the subsemigroup of $\operatorname{End} G$ generated by Ω, then the subalgebra $[T]$ of $(G; \Omega)$ generated by T is the set of all elements $g \in G$ of the form $g = (\omega_{i_1} t_{i_1}^{\varepsilon_1})(\omega_{i_2} t_{i_2}^{\varepsilon_2}) \ldots (\omega_{i_n} t_{i_n}^{\varepsilon_n})$ where n is some integer, $\omega_{i_k} \in [\Omega]$, $t_{i_k} \in T$, $\varepsilon_k = \pm 1$, $k = 1, \ldots, n$. If $[T] = G$, then T is called an Ω-generating set for G. An n-generator Ω-group G is an Ω-group with a generating set of cardinality n. A 1-generator Ω-group is called monogenic.

6.3. $N \lhd G$ will mean that N is a normal subgroup of G. The normal subgroups G and $\{1\}$ of G are called the trivial normal subgroups of G. A non-trivial normal subgroup N of G is called a minimal normal subgroup of G if $M \subset N$ implies $M = \{1\}$, for any normal subgroup M of G and is called a maximal normal subgroup of G if $N \subset M$ implies $M = G$, for any normal subgroup M of G.

If $N \lhd G$, then the partitions of G into left cosets and right cosets modulo N coincide and the equivalence relation corresponding to this partition is a congruence ϑN on G. The mapping ϑ is a bijection from

the set of all normal subgroups to the set of all congruences on G, and we will write $G|N$ for $G|\vartheta N$. A group G is simple if and only if G has just the trivial normal subgroups. A finite abelian group G is simple if and only if $|G| = 1$ or $|G| = p$, for some prime p.

First isomorphism theorem. *If U is a subgroup and N is a normal subgroup of G, then UN is a subgroup of G, $U \cap N$ is a normal subgroup of U, and $UN|N \cong U|U \cap N$. An isomorphism $\alpha : UN|N \to U|U \cap N$ is given by $\alpha(uN) = u(U \cap N)$, $u \in U$.*

Second isomorphism theorem. *Let $\varphi : G \to H$ be an epimorphism from the group G to the group H, $N \lhd H$, and $M = \{g \in G | \varphi g \in N\}$. Then $M \lhd G$ and $G|M \cong H|N$. An isomorphism $\alpha : G|M \to H|N$ is given by $\alpha(gM) = (\varphi g)N$.*

If $N \lhd G$, then every $\alpha \in \operatorname{In} G$ induces an automorphism of N, and the set of all automorphisms of N induced by automorphisms of $\operatorname{In} G$ is a subgroup of $\operatorname{Aut} N$.

Let G be an Ω-group. Then the Ω-admissible normal subgroups of G are just the ideals of the multioperator group $(G; \Omega)$, by Lemma 3.4. If V is an arbitrary and N a normal Ω-admissible subgroup of G, then VN is the Ω-admissible subgroup generated by $V \cup N$.

6.4. Assume that $(G_i | i \in I)$ is a family of groups and let $G = \prod(G_i | i \in I)$ be the direct product of this family. For any $k \in I$, the mapping $\iota_k : G_k \to G$ defined by $\iota_k g = (a(i) | i \in I)$ where $a(k) = g$ and $a(i) = 1$, for $i \neq k$, is a monomorphism from G_k to G, the so-called inclusion monomorphism from G_k to G. A group G is called the inner direct product of its subgroups $U_1, \ldots, U_n$ if $\varphi : U_1 \times \ldots \times U_n \to G$, $\varphi(u_1, \ldots, u_n) = u_1 u_2 \ldots u_n$ is an isomorphism. Subsequently "direct product" will always mean "inner direct product". A finite group G is elementary abelian if and only if G is the direct product of a finite number of groups of order p where p is some fixed prime.

Let G be a group, N a normal subgroup, and H a subgroup of G. Then G is called the semidirect product of N by H if $NH = G$ and $N \cap H = \{1\}$, and H in this case is called a semidirect factor or a retract of G.

A group extension of a group N by a group H is a group G such that $N \lhd G$ and $G|N \cong H$.

6.5. Let G be a group. The set $Z(G) = \{z \in G |\ zg = gz, \text{ for all } g \in G\}$ is called the centre of G. The centre is a characteristic, thus a normal subgroup of G and $\operatorname{In} G \cong G|Z(G)$. If G is a finite p-group, then $|Z(G)| > 1$. A subgroup U of G is called central if $U \subseteq Z(G)$. An element $z \in G$ centralizes $g \in G$ if $zg = gz$.

Let G be a finite group. The intersection of all maximal subgroups of G is denoted by $\Phi(G)$ and is called the Frattini subgroup of G. $\Phi(G)$ is a normal subgroup of G. If G is a p-group, then $G|\Phi(G)$ is elementary abelian.

6.51. Let G be any group. If K and H are normal subgroups of G such that $K \subset H$ and $H|K$ is a minimal normal subgroup of $G|K$, then $H|K$ is called a chief factor of G. $H|K$ is called a central chief factor if $H|K \subseteq Z(G|K)$ and a p-chief factor if $H|K$ is a p-group.

A finite series $G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_n = \{1\}$ of subgroups of G is called a composition series of G if H_i is a maximal normal subgroup of H_{i-1}, $i = 1, \ldots, n$, and is called a chief series of G of length n if each H_i is normal in G and $H_{i-1}|H_i$ is a chief factor of G, $i = 1, \ldots, n$. The factor groups H_{i-1}/H_i are called the factors of the series.

Theorem. *Let G possess a composition series. Then G possesses a chief series, any two chief series of G have the same length and, up to the order and isomorphism, the same factors. Every chief factor of G is the direct product of a finite number of isomorphic simple groups.*

A finite group G is called soluble if all the chief factors of G are abelian (and hence elementary abelian). G is called supersoluble if all the chief factors of G are cyclic (hence of prime order). Therefore every supersoluble group is soluble. Every subgroup and every factor group of a soluble (supersoluble) group is soluble (supersoluble). If $N \lhd G$ and N and $G|N$ are soluble, then G is soluble.

6.52. Let G be a finite group and p a prime dividing $|G|$. If p^a is the greatest power of p dividing $|G|$, then any subgroup of G of order p^a is called a Sylow p-subgroup of G. A Sylow p-subgroup always exists and any two Sylow p-subgroups of G are conjugate.

6.53. Let G be a group and $g, h \in G$. Then we define the commutator $[g, h]$ of g and h by $[g, h] = g^{-1}h^{-1}gh$. If S, T are two subsets of G, then

$[S, T] = [[s, t] | s \in S, t \in T]$ i.e. the subgroup generated by all $[s, t]$. The subgroup $[G, G] = G'$ of G is called the commutator subgroup of G. The lower central series of G is the series $G_0 = G$, $G_i = [G_{i-1}, G]$, $i = 1, 2, \ldots$, of subgroups of G.

A group G is called nilpotent if $G_n = \{1\}$, for some n. The least such integer n is called the class of G.

Every subgroup and every factor group of a nilpotent group is nilpotent. Every minimal normal subgroup of a nilpotent group G is contained in $Z(G)$. A finite group G is nilpotent if and only if G is the direct product of its Sylow subgroups. Every finite p-group is nilpotent. Every finite nilpotent group is supersoluble and a fortiori soluble.

Theorem (Schmidt–Rédei–Iwasawa). *Let G be a finite non-nilpotent group such that every proper subgroup of G is nilpotent. Then:*

a) $|G| = p^a q^b$ *where $p \neq q$ are primes, $a, b > 0$, G has a normal Sylow p-subgroup, and the Sylow q-subgroups are cyclic.*

b) *If S is a Sylow p-subgroup or a Sylow q-subgroup of G, then $\Phi(S) \subseteq Z(G)$.*

Let G be a nilpotent group of class 2. Then $G' \subseteq Z(G)$ and $[ab, c] = [a, c][b, c]$, $[a, bc] = [a, b][a, c]$, for all $a, b, c \in G$.

Theorem (Levi). *If, in any group G, $ab^{-1}ab = b^{-1}aba$, for all $a, b \in G$, then G is nilpotent and of class $\leqslant 3$. If moreover G has no elements of order 3, then G is of class $\leqslant 2$.*

6.6. Let M be any set. Then the set of all mappings from M to M is a semigroup $S(M)$ with identity w.r.t. the composition of mappings. This semigroup is called the symmetric semigroup of M. An element of $S(M)$ is called a permutation of M if it is a bijective mapping from M to M. The permutations of M are just the units of the semigroup $S(M)$ whence the set of all permutations of M is a group w.r.t. the composition of mappings. This group is called the symmetric group Sym M of M. If M is finite, then $|\text{Sym } M| = |M|!$. Any subsemigroup of $S(M)$ is called a mapping semigroup on M, and any subgroup of Sym M is called a permutation group on M.

Let G be a permutation group on M. If $a, b \in M$, we will write $a \sim b$ if and only if there is some $\pi \in G$ such that $\pi a = b$. $\sim$ is an equivalence relation on M, and the blocks of the corresponding partition of M are called orbits of G on M.

Let G be an arbitrary group and $a \in G$. Then $(\varrho a)g = ag$, $g \in G$, defines a permutation ϱa of G, and $\varrho : G \to \text{Sym } G$ is a monomorphism. The permutation group ϱG on G is called the regular representation of G.

Suppose that $M = \{1, 2, \ldots, n\}$. Then

$$A_n = \left\{ \pi \in \text{Sym } M \;\middle|\; \prod_{i<j} (\pi i - \pi j) = \prod_{i<j} (i-j),\ i, j = 1, \ldots, n \right\}$$

is a normal subgroup of Sym M of order $n!/2$ and is called the alternating group on M.

6.61. Let G be any mapping semigroup on M and H a mapping semigroup on N. Suppose that $\alpha \in G$, $\beta(m) \in H$, for all $m \in M$, then $\omega(m, n) = (\alpha m, \beta(m)\, n)$ defines a mapping $\omega : M \times N \to M \times N$. The set W of all mappings of $S(M \times N)$ of this kind is a mapping semigroup on $M \times N$ which is called the wreath product of H by G and is denoted by Hwr$G$. If G and H are permutation groups, so is Hwr$G$.

Let G, H be permutation groups on M, N, resp. and $W = H\text{wr}G$. If $\omega \in W$ and $\omega(m, n) = (\alpha m, \beta(m)\, n)$, then we set $\vartheta\omega = \alpha$. Then $\vartheta : W \to G$ is an epimorphism and $\ker \vartheta$ is isomorphic to the direct product $\prod (H(m) | m \in M)$ where $H(m) = H$, for all $m \in M$. If M and H are finite, then Hwr$G$ is soluble if and only if G and H are soluble.

Let G be a finite and H an arbitrary group. Let $R = \{(g, \varphi) |\ g \in G, \varphi : G \to H\}$ and define a binary operation $\cdot$ on R by $(g_1, \varphi_1)(g_2, \varphi_2) = (g_1 g_2, \psi)$ where $\psi g = (\varphi_1 g)\, \varphi_2(g g_1)$. Then $\langle R; \cdot \rangle$ is a group which is called the regular wreath product of H by G and also denoted by Hwr$G$.

6.7. Let F be a free group, then any two free generating sets for F are of equal cardinality which is called the rank $r(F)$ of F. Every subgroup of a free group is again a free group.

Let $\mathfrak{V}$ be the variety of groups. Then a free product in $\mathfrak{V}$ exists for any family of groups. If $(G_i | i \in I)$ is a family of groups, then their free product in $\mathfrak{V}$ will be denoted by $*(G_i | i \in I)$, or if $i = 1, \ldots, n$, by $G_1 * \ldots * G_n$. If F is the free group with free generating set $\{x_i | i \in I\}$ and $F(x_i)$ is the free group with free generating set $\{x_i\}$, then $F = *(F(x_i) | i \in I)$. If G is a free product of the family $(G_i | i \in I)$ and every G_i is a free product of the family $(H_{ij} | j \in J(i))$, then G is a free product of the family $(H_{ij} | i \in I,$

$j \in J(i)$). The free product of free groups F_i is itself a free group F, and the rank of this free group equals the sum of the ranks $r(F_i)$.

Let G be a group and $(A_i | i \in I)$ be a family of subgroups of G. Then G is the free product of this family if $[\cup(A_i | i \in I)] = G$ and if every $g \in G$, $g \neq 1$, can be uniquely represented in the form $g = a_1 \dots a_n$, $n \geqslant 1$, $a_k \neq 1$, $k = 1, \dots, n$, $a_k \in A_{i_k}$, $i_k \neq i_{k+1}$, $k = 1, \dots, n-1$.

The KUROSH subgroup theorem gives information on the subgroups of a free product. We need the following special case of this theorem:

Let $G = *(G_i | i \in I)$ be a free product of a family of groups and H a normal subgroup of G. Then H can be represented as

$$H = F * \big(*(*(U_{ik} | k \in K_i) | i \in I) \big)$$

where $U_{ik} \cong H \cap G_i$, for all $k \in K_i$, $|K_i| = [G : G_i H]$, and F is a free group such that $r(F) + [G:H] + \sum (|K_i| \, | i \in I) = |I| \, [G:H] + 1$.

Let $(G_i | i \in I)$ be a family of groups and $(\varphi_i | i \in I)$ a family of monomorphisms from a group B to G_i. Then there exists a group A such that (i) B is a subgroup of A, (ii) for every $i \in I$, there is a monomorphism $\gamma_i : G_i \to A$ the restriction onto $\varphi_i B$ of which is φ_i^{-1}, (iii) $[\cup(\gamma_i G_i | i \in I)] = A$, and (iv) $(\gamma_i G_i) \cap [(\cup \gamma_k G_k | k \in I, \ k \neq i)] = B$, and such that every group with these four properties is a homomorphic image of A. The group A which we obtain if we perform the embedding of B into G_i by φ_i, for all $i \in I$, and then the embedding of the groups so obtained into G by γ_i is called a free product of the family $(G_i | i \in I)$ with amalgamated subgroup B.

6.71. Let $F(X)$ be the free group with free generating set $X = \{x_i | i \in I\}$, $W = \{w_j | j \in J\}$ a set of words in $Y = \{y_i | i \in I\}$, y_i being indeterminates, and R the normal subgroup of $F(X)$ which is generated by all words $w_j(x_i)$, $j \in J$. If, for all $i \in I$, we denote the class $C(x_i)$ of the factor group $F(X) | R$ also by y_i, we obtain a group G which is called the group generated by the family $(y_i | i \in I)$ and defined by the relations $w_j = 1$, $j \in J$. If H is an arbitrary group with a generating set $\{a_i | i \in I\}$ which satisfies the relations $w_j(a_i) = 1$, $j \in J$, then the mapping $\vartheta : Y \to H$, $\vartheta y_i = a_i$, $i \in I$, can be extended to an epimorphism from G to H.

Let us consider a special case of this construction: Let $m \neq 1, 2$ be a non-negative integer, $Y = \{a, b\}$, $W = \{a^2, b^m, (ab)^2\}$. Then the group D_m generated by $\{a, b\}$ and defined by the relations $a^2 = b^m = (ab)^2 = 1$ is called a dihedral group. If $m = 0$, then D_m is an infinite group, and if $m > 0$, then $|D_m| = 2m$, a is of order 2 and for $m \neq 0$, b is of order m.

6.72. Let $Y = \{y_i | i \in I\}$ be a set of indeterminates, $W = \{w_j(y_{j_1}, \dots y_{j_{n_j}}) | j \in J\}$ a set of words in Y over the group operations, G an arbitrary group, and $W(G) = \{w_j(g_1, \dots, g_{n_j}) | \ j \in J, g_k \in G\}$. The subgroup $[W(G)]$ is called the verbal subgroup of G generated by W. If F is a free group, then the set of all verbal subgroups of F coincides with the set of all fully invariant subgroups of F.

6.73. Lemma. *Let N be a finite elementary abelian p-group, $Y = \{y_1, \dots, y_k\}$ a finite set of indeterminates, A_p the verbal subgroup of the free group $F(x_1, \dots, x_k)$ generated by y_1^p and $y_1^{-1} y_2^{-1} y_1 y_2$, for $k \geqslant 2$, and by y_1^p, for $k = 1$, and $w(y_1, \dots, y_k) = 1$ a law for N. Then $w(x_1, \dots, x_k) \in A_p$.*

Proof. Since every finite elementary abelian p-group is the direct product of cyclic groups of order p, $w(y_1, \dots, y_k) = 1$ is also a law for the elementary abelian group N_1 of order p^k. The group G, generated by $y_1, \dots, y_k$ and defined by the relations $y_i^p = 1$, $i = 1, \dots, k$, $y_i^{-1} y_j^{-1} y_i y_j = 1$, $i, j = 1, \dots, k$, is elementary abelian of order p^k, hence isomorphic to N_1. Thus $w(y_1, \dots, y_k) = 1$ is also a law for G whence $w(x_1, \dots, x_k)$ is contained in the normal subgroup R of $F(x_1, \dots, x_k)$ which is generated by the elements x_i^p and $x_i^{-1} x_j^{-1} x_i x_j$. But since these elements are also contained in A_p and A_p is fully invariant, hence normal in $F(x_1, \dots, x_k)$, we have $R \subseteq A_p$.

6.8. Proposition. *Let G be a group, A, B subgroups of G and $\mu : A \to B$ an isomorphism. Then there exists an extension group H of G and $t \in H$ such that $\mu a = t^{-1} a t$, for all $a \in A$.*

6.81. Corollary. *Two elements a, b of a group G are conjugate in a suitable extension group of G if and only if they have the same order.*

Proof. The corollary is an immediate consequence of the proposition. Let $K = G[u]$ and $L = G[v]$ where u, v are indeterminates, and set $U = [G \cup u^{-1} A u] \subseteq K$. Then $U = G * u^{-1} A u$ since every $w \in U$ can be represented in the form $w = g_0 u^{-1} a_1 u g_1 u^{-1} a_2 u \dots g_{r-1} u^{-1} a_r u g_r$ where $r \geqslant 0$, $a_j \in A$, $a_j \neq 1$, $g_j \in G$, $g_j \neq 1$, $j = 1, \dots, r-1$, and this repre-

sentation is unique, by ch. 1, Th. 9.11. Similarly for $V = [G \cup vBv^{-1}] \subseteq L$, we have $V = G * vBv^{-1}$. Hence there is an isomorphism $\sigma: U \to V$ which fixes G such that $\sigma(u^{-1}au) = v(\mu a)\, v^{-1}$, for every $a \in A$. Let H be the free product of K and L with amalgamated subgroup U according to this isomorphism, then G is a subgroup of H, and if we put $t = uv$, then $t^{-1}at = v^{-1}u^{-1}auv = v^{-1}v(\mu a)\, v^{-1}v = \mu a$, for all $a \in A$.

6.9. Lemma. *Let G be an n-generator group and N_1, N_2 normal subgroups of G such that $N_1 \cap N_2 = \{1\}$. If, for each pair of generating sets $\{e_1N_1, \ldots, e_nN_1\}$ and $\{f_1N_2, \ldots, f_nN_2\}$ for $G|N_1, G|N_2$ resp., there exists a generating set $\{g_1, \ldots, g_n\}$ for G such that $g_i \in e_iN_1 \cap f_iN_2$, $i = 1, \ldots, n$, then either $G = N_1 \times N_2$ or $[G : N_1N_2] = 2$.*

Proof. Suppose that $\{g_1, \ldots, g_n\}$ is a generating set for G. Then $\{g_1N_1, \ldots, g_nN_1\}$ generates $G|N_1$ and $\{g_iN_2, g_2N_2, \ldots, g_nN_2\}$ generates $G|N_2$. Hence there are $g_i' \in G$, $i = 1, \ldots, n$, such that $[g_1', \ldots, g_n'] = G$ and $g_1' \in g_1N_1 \cap g_iN_2$, $g_i' \in g_iN_1 \cap g_1N_2$. Then $g_1g_i^{-1} = (g_1g_1'^{-1})(g_i'g_i^{-1}) \in N_1N_2$ whence $G|N_1N_2$ is cyclic. Moreover $[g_1^{-1}N_1, \ldots, g_n^{-1}N_1] = G|N_1$, hence we can find $g_i'' \in G$, $i = 1, \ldots, n$, such that $[g_1'', \ldots, g_n''] = G$ and $g_i'' \in g_i^{-1}N_1 \cap g_iN_2$. Therefore $g_i^2 = (g_ig_i''^{-1})(g_i''g_i) \in N_2N_1 = N_1N_2$ whence $|G|N_1N_2| \leqslant 2$.

6.91. Lemma. *Let n be a positive integer, G an n-generator Ω-group, and N a finite Ω-admissible normal subgroup of G. Then, for each Ω-generating set $\{f_1N, \ldots, f_nN\}$ of the Ω-factor group $G|N$, there exists an Ω-generating set $\{e_1, \ldots, e_n\}$ of G such that $e_i \in f_iN$, $i = 1, \ldots, n$.*

Proof. Let $\mathfrak{T}$ be the set of all Ω-subgroups V of G such that $VN = G$. If $V \in \mathfrak{T}$, then $f_iN = v_iN$, for some $v_i \in V$, $i = 1, \ldots, n$. By the first isomorphism theorem for multioperator groups, there is an isomorphism $\alpha: G|N \to V|V \cap N$ such that $\alpha(vN) = v(V \cap N)$, $v \in V$, whence the set of all $v_i(V \cap N) = V \cap v_iN = V \cap f_iN$ is an Ω-generating set for $V|V \cap N$. Therefore $V = [(V \cap f_1N) \cup (V \cap f_2N) \cup \ldots \cup (V \cap f_nN) \cup (V \cap N)]$. Since N is finite, we conclude that $\mathfrak{T}$ is also finite. Hence $\mathfrak{T}$ contains only finitely many maximal Ω-subgroups and every proper Ω-subgroup in $\mathfrak{T}$ is contained in at least one maximal Ω-subgroup in $\mathfrak{T}$. If every maximal Ω-subgroup of G contains N, then $\mathfrak{T} = \{G\}$ whence $[f_1, \ldots, f_n] = G$. Otherwise let $M_1, \ldots, M_r$ be just those maximal Ω-subgroups of G which

do not contain N, i.e. all maximal Ω-subgroups in $\mathfrak{T}$. For an arbitrary Ω-subgroup U of G, we set

$$\varepsilon(U) = \begin{cases} 0, & \text{for } UN \neq G, \\ 1, & \text{for } UN = G. \end{cases}$$

Then the number of all systems

$$\{e_1, \ldots, e_n\}, \qquad e_i \in f_iN, \qquad i = 1, \ldots, n, \tag{6.9}$$

which are contained in U, is given by $|N \cap U|^n \varepsilon(U)$. For if $UN = G$, then $U \cap f_iN = v_i(U \cap N)$, for some $v_i \in U$ and if $UN \neq G$, then at least one of the $U \cap f_iN$ is empty. Hence the number of all systems (6.9) that are not contained in any proper Ω-subgroup of G is

$$\Phi(N) = |N|^n + \sum_{k=1}^{r} \sum_{i_1 < i_2 < \ldots < i_k} (-1)^k |N \cap M_{i_1} \cap \ldots \cap M_{i_k}|^n \varepsilon(M_{i_1} \cap \ldots \cap M_{i_k}).$$

$\Phi(N)$ does not depend on the particular choice of the generating set $\{f_1N, \ldots, f_nN\}$. Since G is an n-generator Ω-group, there exists such a generating set which yields a system (6.9) that is not contained in any proper Ω-subgroup of G. Hence $\Phi(N) \neq 0$.

7. Linear algebra and representation theory

7.1. This section is devoted to linear algebra and representations, but will be reviewed just briefly. For further information, we refer to standard books, such as CURTIS–REINER [1], HUPPERT [1], RÉDEI [2].

Let R be an arbitrary ring and m, n positive integers. An $m \times n$-array

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

of elements $a_{ik} \in R$, $i = 1, \ldots, m$, $k = 1, \ldots, n$, is called an $m \times n$-matrix over R. A brief notation for such a matrix A is $A = (a_{ik})$.

The sum $A + B$ of any two $m \times n$-matrices $A = (a_{ik})$, $B = (b_{ik})$ is defined to be the $m \times n$-matrix $A + B = (a_{ik} + b_{ik})$. If $A = (a_{ik})$ is an $m \times n$-matrix and $B = (b_{ik})$ is an $n \times p$-matrix, then we define the product AB to be the $m \times p$-matrix $AB = (c_{ik})$ where $c_{ik} = \sum_{t=1}^{n} a_{it}b_{tk}$. If $A = (a_{ik})$

is an $m\times n$-matrix and $c\in R$, then cA and Ac are $m\times n$-matrices defined by $cA=(ca_{ik})$, $Ac=(a_{ik}c)$. The $m\times n$-zero matrix O_{mn} is the matrix (a_{ik}) with $a_{ik}=0$, for all pairs (i,k), and if R has an identity 1, then the $m\times m$-identity matrix is the matrix $E_m=(\delta_{ik})$ where $\delta_{ik}=0$, for $i\neq k$, and $\delta_{ik}=1$, for $i=k$, i. e. δ_{ik} is the so-called Kronecker symbol.

If, in any of the following equations, one side is defined, so is the other side and the equation holds:

$$A+B=B+A,\quad (A+B)+C=A+(B+C),\quad (AB)C=A(BC),$$
$$A(B+C)=AB+AC,\quad (B+C)A=BA+CA,$$
$$c(A+B)=cA+cB,\quad (c+d)A=cA+dA,\quad (cd)A=c(dA),$$

where A, B, C are matrices over R and c, $d\in R$. If A is an $m\times n$-matrix, then $A+O_{mn}=O_{mn}+A=A$, $E_mA=AE_n=A$.

These equations show that, for any m, the set of all $m\times m$-matrices over R is a ring w.r.t. $+$ and $\cdot$ as just defined which is called the full $m\times m$-matrix ring R_m over R. If R has an identity, then R_m also has an identity. Then the group of all units of R_m is called the general linear group $\mathrm{GL}(m, R)$ of dimension m over R.

Theorem. *If S is a skewfield, then every full matrix ring S_m over S is simple. Conversely, if R is a simple ring such that $|R|\neq 1$, $ab\neq 0$, for at least one pair (a, b) of elements $a, b\in R$, and every descending chain $L_1\supset L_2\supset L_3\supset\ldots$ of left ideals L_i in R is finite, then R is isomorphic to a full matrix ring over some skewfield S.*

7.2. Let R be a commutative ring with identity, $A=(a_{ik})$ an $m\times m$-matrix over R, and $M=\{1, 2, \ldots, m\}$. We define the determinant $|A|$ of A by

$$|A|=\sum(\varepsilon(\pi)a_{1\pi 1}a_{2\pi 2}\ldots a_{m\pi m}|\pi\in \mathrm{Sym}\, M),\quad \varepsilon(\pi)=-1 \text{ if } \pi\notin A_m,$$
$$\varepsilon(\pi)=1 \text{ if } \pi\in A_m.$$

Sometimes we write $|A|=\det A$. If A, B are any two $m\times m$-matrices over R, then $|AB|=|A|\,|B|$. Moreover the mapping $\det: R_m\to R$ is an epimorphism of (multiplicative) semigroups. A matrix $A\in R_m$ is a unit of R_m if and only if $|A|$ is a unit of R.

A matrix $A\in R_m$ is called unimodular if $|A|=1$. The set $\mathrm{SL}(m, R)$ of all unimodular matrices of R_m is a subgroup of $\mathrm{GL}(m, R)$. Let $A\in R_m$ and $\mathfrak{b}$ be an $m\times 1$-matrix over R, then $\pi\mathfrak{x}=A\mathfrak{x}+\mathfrak{b}$, $\mathfrak{x}\in R^m$, defines a

mapping $\pi\in S(R^m)$. The set of all these mappings is a subsemigroup of $S(R^m)$, the so-called inhomogeneous linear semigroup of dimension m over R. In this semigroup, the subset of all mappings with $|A|$ being a unit is a group, the inhomogeneous linear group of dimension m over R.

If R is a finite field of order p^t, then we write $\mathrm{GL}(m, R)=\mathrm{GL}(m, p^t)$. We have $|\mathrm{GL}(m, p^t)|=(p^{mt}-1)(p^{mt}-p^t)\ldots(p^{mt}-p^{(m-1)t})$. The group $\mathrm{GL}(m, p^t)$ is soluble if and only if $m=1$ or $m=2$ and $p^t=2, 3$. $\mathrm{GL}(m, p^t)$ is nilpotent if and only if $m=1$.

Let A be an $m\times m$-matrix over R and set $E_m=E$. Then $xE-A$ is an $m\times m$-matrix over $R[x]$ whence $|xE-A|$ is a polynomial of $R[x]$, the so-called characteristic polynomial of A. If $|xE-A|=x^m+a_1x^{m-1}+\ldots+a_m$, then $A^m+a_1A^{m-1}+\ldots+a_{m-1}A+a_mE=O_{mm}$ (Cayley–Hamilton equation). The roots of the characteristic polynomial of A are called the eigenvalues of A.

Let A be an $m\times m$-matrix over the field K and $\mathfrak{o}$ the $m\times 1$-matrix where all elements are 0. Then the "system of linear equations" $A\mathfrak{x}=\mathfrak{o}$ has a solution $\mathfrak{x}\neq\mathfrak{o}$ in K^m if and only if A is singular, i.e. $|A|=0$.

7.3. An abelian group $\langle M; +, -, 0\rangle$ is also called a module. Let R be a ring with identity. An R-module (or left R-module) is an abelian group $\langle M; +, -, 0\rangle$ together with a mapping from $R\times M$ to M, $(r, m)\to rm$, such that $(r+s)m=rm+sm$, $r(m+n)=rm+rn$, $(rs)m=r(sm)$, $1m=m$, for all $r, s\in R$, $m, n\in M$.

If K is a field, then a K-module V is called a vector space over K or K-vector space. The elements of V are called vectors, and the identity 0 of V the zero vector. The family $v_1, \ldots, v_n\in V$ is called linearly independent if $r_1v_1+\ldots+r_nv_n=0$ implies $r_i=0$, $i=1, \ldots, n$; otherwise linearly dependent. If, for any integer $d\geqq 0$, there exists a family of d linearly independent elements in V, but every family of $n>d$ elements is linearly dependent, then we set $d=\dim V=\dim_K V$ and call d the dimension of V. Then every family of d linearly independent elements is called a basis of V. If $m<\dim V$ and $v_1, \ldots, v_m$ are linearly independent, then there exist elements $v_{m+1}, \ldots, v_n\in V$ such that $v_1, \ldots, v_n$ is a basis of V. If $v_1, \ldots, v_n$ is a basis of V, then any $w\in V$ can be uniquely represented as $w=\sum_{k=1}^{n} r_kv_k$, $r_k\in K$. If $w_1, \ldots, w_n\in V$ and $w_i=\sum_{k=1}^{n} r_{ik}v_k$, then $w_1, \ldots, w_n$ are linearly independent if and only if $\det(r_{ik})\neq 0$.

Let V be any vector space over K. An endomorphism (automorphism) of V is an endomorphism (automorphism) φ of $\langle V; +, -, 0\rangle$ such that $\varphi(kv) = k\varphi(v)$, for all $k \in K$, $v \in V$. If $\varphi_1+\varphi_2$ and $\varphi_1\varphi_2$ are defined, for endomorphisms φ_1, φ_2 of V, by $(\varphi_1+\varphi_2)v = \varphi_1 v+\varphi_2 v$, $(\varphi_1\varphi_2)v = \varphi_1(\varphi_2 v)$, then the set $\mathrm{Hom}_K(V, V)$ of all endomorphisms of V is a ring with identity. The units of $\mathrm{Hom}_K(V, V)$ are just the automorphisms of V, they form a group Aut V. If $\dim V = n$, then $\mathrm{Hom}_K(V, V) \cong K_n$ as rings, and Aut $V \cong \mathrm{GL}(n, K)$.

7.4. Let M be an R-module. A submodule of M is a subgroup U of $\langle M; +, -, 0\rangle$ such that $ru \in U$, for all $r \in R$, $u \in U$. The submodules $\{0\}$ and M of M are called the trivial submodules. M is irreducible if M has no non-trivial submodules. An isomorphism (homomorphism) $\varphi : M \to N$ of R-modules is an isomorphism (homomorphism) from $\langle M; +, -, 0\rangle$ to $\langle N; +, -, 0\rangle$ such that $\varphi(rm) = r\varphi(m)$, for all $r \in R$, $m \in M$.

Let M be an R-module. Then the set $\mathrm{An}\, M = \{r \in R \mid rm = 0, \text{ for all } m \in M\}$ is an ideal of R, the so-called annihilator of M. M is called faithful if $\mathrm{An}\, M = \{0\}$. If M is an arbitrary R-module, then M is a faithful $R|\mathrm{An}\, M$-module under the action $(r+\mathrm{An}\, M)m = rm$, $r \in R$, $m \in M$. If R is a ring where every descending chain $L_1 \supset L_2 \supset \ldots$ of left ideals is finite, and if R possesses a faithful, irreducible R-module M, then R is a simple ring.

Let K_n be the full $n \times n$-matrix ring over a field K. Then every irreducible K_n-module can be regarded as a vector space over K and its dimension is n.

7.5. Let G be a group and V a vector space over the field K. A homomorphism $\delta : G \to \mathrm{Aut}\, V$ is called a representation of G on V. If $\delta g = 1$ for all $g \in G$, then δ is called a trivial representation. If $\dim V = n$ and $\sigma : \mathrm{Hom}_K(V, V) \to K_n$ is an isomorphism, then $\sigma\delta$ is called a matrix representation of G over K afforded by V.

Let G be a finite group, K any field, and KG the set of all formal sums $\sum(k_g g \mid g \in G)$, $k_g \in K$. In KG we define $\sum k_g g+\sum l_g g = \sum(k_g+l_g)g$, $(\sum k_g g)(\sum l_g g) = \sum(\sum k_h l_{h^{-1}g} \mid h \in G)g$. Then $\langle KG; +, \cdot\rangle$ is a ring with identity which is called the group ring of G over K.

Let V be a vector space over K and δ a representation of G on V. If we define $(\sum k_g g)v = \sum k_g((\delta g)v)$, for any $\sum k_g g \in KG$, $v \in V$, then V becomes a KG-module. The representation δ of G is called irreducible if V is an

irreducible KG-module. All these concepts are used in the special situation that $K = K_p$, the field of prime order p, $V = N$, a minimal abelian normal p-subgroup of G regarded as a K_p-vector space by means of $n_1+n_2 = n_1 n_2$, $(k1)n = n^k$, for any integer $k \geq 0$, and $(\delta g)n = gng^{-1}$.

8. Near-rings

8.1. Near-rings and distributively generated (d.g.) near-rings, in particular, have been defined in ch. 3, § 1.3 and ch. 5, § 2. This section shall present some basic facts on d.g. near-rings as they are applied in ch. 5. Since there does not exist a book on near-rings so far, every result will be proved here.

Let $\langle A; +, \cdot\rangle = A$ be a d.g. near-ring with an identity 1 for $\cdot$, and S a generating set for $\langle A; +, -, 0\rangle$ consisting of distributive elements. An (additively written) group M together with a mapping $\beta : A \times M \to M$, $\beta(a, m) = am$, is called an (A, S)-group or—if S is kept fixed—an A-group if

$$\begin{aligned}
(a_1+a_2)m &= a_1 m+a_2 m, & a_1, a_2 \in A, \quad m \in M,\\
s(m_1+m_2) &= sm_1+sm_2, & s \in S, \quad m_1, m_2 \in M,\\
(s_1 s_2)m &= s_1(s_2 m), & s_1, s_2 \in S, \quad m \in M,\\
1m &= m, & m \in M.
\end{aligned}$$

Let M be an A-group. A subgroup N of M is called an A-subgroup of M if $an \in N$, for all $a \in A$, $n \in N$. A non-zero A-group M is called a minimal A-group if M contains no non-trivial A-subgroups.

If M is an A-group and N is a normal A-subgroup of M, then the factor group $M|N$ becomes an A-group by virtue of $a(m+N) = am+N$, and $M|N$ is called an A-factor group of M.

Let M_1, M_2 be two A-groups. An A-homomorphism (isomorphism, epimorphism) is a group homomorphism (isomorphism, epimorphism) $\varphi : M_1 \to M_2$ such that $\varphi(am) = a(\varphi m)$, for all $a \in A$, $m \in M$. If $\varphi : M_1 \to M_2$ is an A-epimorphism, then $\ker \varphi$ is a normal A-subgroup of M_1 and M_2 is A-isomorphic to the A-factor group $M_1|\ker \varphi$.

Note that A itself is an A-group through the left multiplication by elements of A. If U is an A-subgroup of A and $b \in A$, then Ub is also an A-subgroup of A.

We say that A satisfies the minimum condition for A-subgroups if every set of A-subgroups of A has a minimal element w.r.t. to the inclu-

sion of sets, or equivalently, if every chain $U_1 \supset U_2 \supset \dots$ of A-subgroups is finite.

Throughout this section, we will assume that A is a d.g. near-ring with identity 1 and minimum condition for A-subgroups.

8.2. An element $a \in A$ is called nilpotent if $a^n = 0$, for some positive integer n. An A-subgroup U of A is a nil A-subgroup if every $u \in U$ is nilpotent. An A-subgroup U of A is nilpotent if there exists a positive integer n such that $U^n = \{0\}$, where U^n means the complex product.

Let $U_1, \dots, U_n$ be A-subgroups of A. Then $U_1 \circ U_2 \circ \dots \circ U_n$ is defined to be the A-subgroup of A generated by $U_1 U_2 \dots U_n$. This does not necessarily imply $(U_1 \circ U_2) \circ U_3 = U_1 \circ (U_2 \circ U_3)$, but $U_1 \circ (U_2 b) = (U_1 \circ U_2) b$, $b \in A$, is always true since $U_1 \circ U_2$ is the set of all finite sums $\sum a_j u_{1j} u_{2j}$, $a_j \in A$, $u_{ij} \in U_i$, $i = 1, 2$.

8.21. Theorem. *Every nil A-subgroup of A is nilpotent.*

Proof. Let U be any nil A-subgroup of A and set $U^{(0)} = U$, $U^{(n)} = U^{(n-1)} \circ U^{(n-1)}$, $n = 1, 2, \dots$. The minimum condition implies $U^{(k)} = U^{(k+1)}$, for some k. Suppose $U^{(k)} \neq \{0\}$, then there exists an A-subgroup I of A minimal w.r.t. $U^{(k)} \circ I \neq \{0\}$, again by the minimum condition. Choose $b \in I$ such that $U^{(k)} b \neq \{0\}$. Then $U^{(k)} b$ is an A-subgroup of A which is contained in I and $U^{(k)} \circ (U^{(k)} b) = (U^{(k)} \circ U^{(k)}) b = U^{(k+1)} b = U^{(k)} b \neq \{0\}$, whence $U^{(k)} b = I$. Hence there exists an element $u \in U^{(k)}$ such that $b = ub$. Therefore $b = ub = u^2 b = \dots = u^r b = 0$, for some r, since $u \in U$ and U is a nil A-subgroup, contradiction. Hence $U^{(k)} = \{0\}$, therefore $U^{2^k} = \{0\}$.

8.3. Let M be an A-group and X any set of elements in M. The set $\mathfrak{l}_A(X) = \{a \in A \mid ax = 0, \text{ for all } x \in X\}$ is called the left annihilator of X in A. If $X = \{x\}$, we will write $\mathfrak{l}_A(X) = \mathfrak{l}_A(x)$.

8.31. Proposition. *Let M be an A-group and X a set of elements in M. Then $\mathfrak{l}_A(X)$ is an A-subgroup of A.*

Proof. Let $x \in X$, $a_1, a_2 \in A$, $a_1 x = a_2 x = 0$, then $(a_1 + a_2)x = a_1 x + a_2 x = 0$, and $(-a_1)x = -a_1 x = 0$. Moreover if $a \in A$, then $(aa_1)x = a(a_1 x) = 0$ since $\langle A; + \rangle$ is generated by S.

8.32. Theorem. *Every non-nilpotent A-subgroup U of A contains an idempotent element $e \neq 0$.*

Proof. Since the minimum condition holds for A, it suffices to prove the theorem for the case that every proper A-subgroup of U is nilpotent. Since U is non-nilpotent, there exists a non-nilpotent element $u_0 \in U$, by Th. 8.21, hence $U = Uu_0$, for if $Uu_0 \subset U$, then Uu_0 would be nilpotent whence u_0^2 would be nilpotent, contradiction. Hence there exists $u_1 \in U$ such that $u_0 = u_1 u_0$, and u_1 is non-nilpotent, otherwise we would have $u_0 = u_1 u_0 = u_1^2 u_0 = \dots = u_1^s u_0 = 0$, for some s, contradiction. Hence $U = Uu_1$, and again there is a non-nilpotent element $u_2 \in U$ such that $u_1 = u_2 u_1$. If we continue this procedure, we obtain a sequence $u_0, u_1, u_2, \dots$ of non-nilpotent elements in U such that $U = Uu_i$ and $u_i = u_{i+1} u_i$, $i = 0, 1, 2, \dots$. This yields a chain $\mathfrak{l}_A(u_0) \supseteq \mathfrak{l}_A(u_1) \supseteq \dots$ of A-subgroups of A, and by the minimum condition, we have $\mathfrak{l}_A(u_{k+1}) = \mathfrak{l}_A(u_k)$. Since $u_k = u_{k+1} u_k$, we conclude $(u_{k+1} - 1)u_k = 0$, hence $u_{k+1} - 1 \in \mathfrak{l}_A(u_k) = \mathfrak{l}_A(u_{k+1})$. Therefore $(u_{k+1} - 1)u_{k+1} = 0$ i.e. $u_{k+1}^2 = u_{k+1}$. Hence $u_{k+1} \in U$ is an idempotent.

8.33. Corollary. *Every minimal non-nilpotent A-subgroup U of A is of the form $U = Ae$ where e is an idempotent of A.*

8.34. Proposition. *Every set $\{e_1, e_2, \dots\}$ of non-zero idempotents of A such that $e_{i+1} \in \mathfrak{l}_A(\{e_1, \dots, e_i\})$, $i = 1, 2, \dots$, is finite.*

Proof. Suppose the opposite is true, then by the minimum condition, $\mathfrak{l}_A(\{e_1, \dots, e_k\}) = \mathfrak{l}_A(\{e_1, \dots, e_{k+1}\})$, for some k. But then $e_{k+1} \in \mathfrak{l}_A(\{e_1, \dots, e_{k+1}\})$ whence $e_{k+1}^2 = 0$, contradiction.

8.35. Corollary. *There exists a finite set $\{Ae_1, \dots, Ae_n\}$ of minimal non-nilpotent A-subgroups of A, e_i idempotent, $i = 1, \dots, n$, such that $e_{i+1} \in \mathfrak{l}_A(\{e_1, \dots, e_i\})$, $i = 1, \dots, n-1$, and such that there is no non-zero idempotent $e_{n+1} \in \mathfrak{l}_A(\{e_1, \dots, e_n\})$.*

Proof. Since A is non-nilpotent as $1 \in A$, there is a minimal non-nilpotent A-subgroup Ae_1 of A. Take any minimal non-nilpotent A-subgroup Ae_2 of $\mathfrak{l}_A(\{e_1\})$, then $e_2 \in \mathfrak{l}_A(\{e_1\})$. Then choose a minimal non-nilpotent A-subgroup Ae_3 of $\mathfrak{l}_A(\{e_1, e_2\})$, etc. By Prop. 8.34, this procedure must

terminate after finitely many steps, i.e. there is no non-zero idempotent $e_{n+1} \in \mathfrak{l}_A(\{e_1, \ldots, e_n\})$ for some n.

8.36. Proposition. *Let $\{Ae_1, \ldots, Ae_n\}$ be a set of minimal non-nilpotent A-subgroups of A such that all e_i are idempotents, $e_{i+1} \in \mathfrak{l}_A(\{e_1, \ldots, e_i\})$, $i = 1, 2, \ldots, n-1$, and there is no non-zero idempotent $e_{n+1} \in \mathfrak{l}_A(\{e_1, \ldots, e_n\})$. Then $L = \mathfrak{l}_A(\{e_1, \ldots, e_n\})$ is a nilpotent A-subgroup of A, and every element $a \in A$ can be written uniquely as $a = a_1 + a_2 + \ldots + a_n + l$, $a_k \in Ae_k$, $k = 1, \ldots, n$, $l \in L$.*

Proof. Suppose L is not nilpotent. Then by Th. 8.32 and Cor. 8.33, L contains a minimal non-nilpotent A-subgroup Ae_{n+1} where e_{n+1} is an idempotent, and $e_{n+1} \in \mathfrak{l}_A(\{e_1, \ldots, e_n\})$, contradiction. The second statement will follow from: Every element $a \in A$ can be written uniquely as $a = a_1 + \ldots + a_i + l_i$, $a_k \in Ae_k$, $k = 1, 2, \ldots, i$, and $l_i \in \mathfrak{l}_A(\{e_1, \ldots, e_i\})$. We will prove this by induction on i: for $i = 1$, we have $A = Ae_1 + \mathfrak{l}_A(e_1)$ since, for any $a \in A$, $a = ae_1 + (-ae_1 + a)$ and $-ae_1 + a \in \mathfrak{l}_A(e_1)$. Moreover $Ae_1 \cap \mathfrak{l}_A(e_1) = 0$, hence this decomposition is unique. Let $j \geqslant 1$. By induction, $a = a_1 + \ldots + a_j + l_j$, $a_k \in Ae_k$, $k = 1, \ldots, j$, $l_j \in \mathfrak{l}_A(\{e_1, \ldots, e_j\})$. If we put $l_{j+1} = -l_j e_{j+1} + l_j$, then $a_{j+1} = l_j e_{j+1} \in Ae_{j+1}$ and $l_{j+1} \in \mathfrak{l}_A(\{e_1, \ldots, e_{j+1}\})$. Suppose that $a = a_1 + \ldots + a_{j+1} + l_{j+1} = a_1' + \ldots + a_{j+1}' + l_{j+1}'$, $a_k, a_k' \in Ae_k$, $k = 1, \ldots, j+1$, $l_{j+1}, l_{j+1}' \in \mathfrak{l}_A(\{e_1, \ldots, e_{j+1}\})$. Then $(a_{j+1} + l_{j+1})e_k = 0 = (a_{j+1}' + l_{j+1}')e_k$, $k = 1, \ldots, j$. By induction, $a_k = a_k'$, for $k = 1, \ldots, j$, and $a_{j+1} + l_{j+1} = a_{j+1}' + l_{j+1}'$. Hence $-a_{j+1}' + a_{j+1} = l_{j+1}' - l_{j+1} \in Ae_{j+1} \cap \mathfrak{l}_A(e_{j+1})$. Therefore $a_{j+1} = a_{j+1}'$, $l_{j+1} = l_{j+1}'$.

8.4. The intersection of all A-subgroups U of A such that there is a minimal A-group M with $U = \mathfrak{l}_A(M)$ is called the radical $J(A)$ of A.

8.41. Proposition. *$J(A)$ contains every nilpotent A-subgroup of A.*

Proof. Suppose not, then there exists some nilpotent A-subgroup U of A and minimal A-group M such that $UM \neq \{0\}$. Then $Um \neq \{0\}$, for some $m \in M$ whence $Um = M$. Hence, for some $u \in U$, $m = um = u^2m = \ldots = u^sm = 0$, for some s, since U is nilpotent: contradiction.

8.42. Proposition. *Let M be an A-group. Then $\mathfrak{l}_A(M)$ is a normal A-subgroup of A and $\mathfrak{l}_A(M)a \subseteq \mathfrak{l}_A(M)$, for all $a \in A$.*

Proof. By Prop. 8.31, $\mathfrak{l}_A(M)$ is an A-subgroup of A. Let $x \in \mathfrak{l}_A(M)$, $a \in A$, $m \in M$. Then $(-a+x+a)m = -am + xm + am = 0$. Moreover, $(xa)m = x(am) = 0$.

8.43. Proposition. *Suppose the radical J of A is nilpotent, and Ae is a minimal non-nilpotent A-subgroup of A, e idempotent. Then $Je = Ae \cap J$, and Je is a proper A-subgroup of Ae which contains every proper A-subgroup of Ae. Furthermore Je is a normal subgroup of Ae, and for every minimal A-group M, there exists some minimal non-nilpotent A-subgroup Ae of A, e idempotent, such that M is A-isomorphic to the A-factor group $Ae \mid Je$.*

Proof. By Prop. 8.42, J is a normal A-subgroup of A, and $Ja \subseteq J$, for all $a \in A$, thus $Je \subseteq J$, whence $Je \subseteq Ae \cap J$; but also $Ae \cap J \subseteq Je$ since e is an idempotent. Therefore $Je = Ae \cap J$, hence by the first isomorphism theorem of group theory, $Je \lhd Ae$. Since J is nilpotent, also $Ae \cap J$ is nilpotent, hence $Ae \cap J$ is properly contained in Ae. Let U be an arbitrary proper A-subgroup of Ae, then U is nilpotent. By Prop. 8.41, $U \subseteq J$ whence $U \subseteq Ae \cap J = Je$. Now let M be a minimal A-group, $\{Ae_1, \ldots, Ae_n\}$ a set of minimal non-nilpotent A-subgroups of A as in Cor. 8.35, and $L = \mathfrak{l}_A(\{e_1, \ldots, e_n\})$. Then $M = AM = Ae_1M + \ldots + Ae_nM + LM$, by Prop. 8.36. Since L is nilpotent, $L \subseteq J$ whence $LM = \{0\}$. Therefore there exists an idempotent e_i such that $Ae_iM \neq \{0\}$. Thus we can find an element $m \in M$ such that $Ae_im \neq \{0\}$, hence $Ae_im = M$ by minimality of M. If we define an A-epimorphism $\varphi : Ae_i \twoheadrightarrow M$ by $\varphi(ae_i) = ae_im$, then $M \cong Ae_i \mid \ker\varphi$. $\ker\varphi$ is a proper normal A-subgroup of Ae_i whence $\ker\varphi = Je_i$, i.e. $M \cong Ae_i \mid Je_i$.

8.5. We recall ch. 3, Prop. 5.11, which tells us that every near-ring $\langle A; +, -, 0, \cdot \rangle$ may be regarded as a $\{\cdot\}$-multioperator group. Let $A = \langle A; +, -, 0, \cdot, 1 \rangle$ be a near-ring with identity and $\mathcal{E}(A)$ the group of units of the semigroup $\langle A; \cdot, 1 \rangle$.

8.51. Proposition. *Let A be a d.g. near-ring with identity 1 and minimum condition for A-subgroups, and $\varphi : A \twoheadrightarrow B$ a near-ring epimorphism. If $\ker\varphi$ is finite, then $\varphi\mathcal{E}(A) = \mathcal{E}(B)$.*

Proof. By the homomorphism theorem, it suffices to show: If I is a finite

ideal of A and $u+I$ a unit of $A|I$, then there exists an element $i \in I$ such that $u+i$ is a unit of A.

By the minimum condition, there exists a positive integer $k = k(v)$ such that $Av^k = Av^{k+1}$, for all $v \in A$. Let $u, v \in A$ such that $vu = 1$, then $A = Av^k u^k = Av^{k+1}u^k = Av$ whence $1 = av$, for some $a \in A$. But $u = 1u = avu = a$ whence $1 = uv$. Since S additively generates A, we can regard A as a monogenic S-group with S-generator 1. By Lemma 3.4, I is a finite S-admissible normal subgroup of the S-group A, and $1+I$ is an S-generator of the S-factor group $A|I$. Since $u+I$ is a unit of $A|I$ and S additively generates A, we conclude that $u+I$ is an S-generator of $A|I$. Hence by Lemma 6.91, there exists an S-generator $u+i$ of A where $i \in I$. Thus by § 6.2, $1 = \sum_{i=1}^{k} t_i(u+i)$ where $t_i \in A$, $i = 1, \ldots, k$, whence $v(u+i) = 1$, for some $v \in A$, i.e. $u+i$ is a unit of A.

9. Miscellaneous

9.1. In this section, we collect various definitions and results from quite divergent branches of mathematics which are used at some place in this book. Not all of these results are well-known, but since some of the proofs are far beyond the scope of this book, we will restrict ourselves to giving references.

First we deal with the concepts of category and functor: Let $\mathfrak{C}$ be a class of objects $A, B, C, \ldots$, and suppose that, for any ordered pair (A, B) of objects in $\mathfrak{C}$, there is a set $\mathrm{Mor}(A, B)$ such that $\mathrm{Mor}(A, B) \cap \mathrm{Mor}(C, D) = \phi$ if $(A, B) \neq (C, D)$. For any ordered triple (A, B, C) in $\mathfrak{C}$, let $\omega(A, B, C) : \mathrm{Mor}(A, B) \times \mathrm{Mor}(B, C) \to \mathrm{Mor}(A, C)$ be defined to be a mapping (we will write $\omega(A, B, C)(f, g) = gf$) such that: For any four objects $A, B, C, D \in \mathfrak{C}$ and all $f \in \mathrm{Mor}(A, B)$, $g \in \mathrm{Mor}(B, C)$, $h \in \mathrm{Mor}(C, D)$, we have $h(gf) = (hg)f$; for any $A \in \mathfrak{C}$, there exists a morphism $1_A \in \mathrm{Mor}(A, A)$ such that $f1_A = f$, for any $B \in \mathfrak{C}$ and $f \in \mathrm{Mor}(A, B)$; and $1_A g = g$, for any $C \in \mathfrak{C}$ and $g \in \mathrm{Mor}(C, A)$. Then the triple consisting of the class $\mathfrak{C}$, the class of all $\mathrm{Mor}(A, B)$, and the class of all $\omega(A, B, C)$ is called a category which will be denoted briefly by $\mathfrak{C}$.

As an example, we may take any variety $\mathfrak{V}$ for $\mathfrak{C}$, and the set of all homomorphisms $\mu : A \to B$ for $\mathrm{Mor}(A, B)$ while $\omega(A, B, C)$ will be the composition of mappings.

Let $(\mathfrak{C}, \mathrm{Mor}_{\mathfrak{C}}, \omega_{\mathfrak{C}}) = \mathfrak{C}$ and $(\mathfrak{D}, \mathrm{Mor}_{\mathfrak{D}}, \omega_{\mathfrak{D}}) = \mathfrak{D}$ be two categories, $\mathcal{F} : \mathfrak{C} \to \mathfrak{D}$ a mapping and $\mathcal{F}(A, B) : \mathrm{Mor}_{\mathfrak{C}}(A, B) \to \mathrm{Mor}_{\mathfrak{D}}(\mathcal{F}(A), \mathcal{F}(B))$ a mapping. For any pair (A, B) of objects in $\mathfrak{C}$ we will write $\mathcal{F}(A, B)f = \mathcal{F}(f)$. If $\mathcal{F}(gf) = \mathcal{F}(g)\mathcal{F}(f)$ for all $A, B, C \in \mathfrak{C}$, $f \in \mathrm{Mor}_{\mathfrak{C}}(A, B)$, $g \in \mathrm{Mor}_{\mathfrak{C}}(B, C)$, and $\mathcal{F}(1_A) = 1_{\mathcal{F}(A)}$ for all $A \in \mathfrak{C}$, then the pair consisting of the mapping $\mathcal{F}$ and the family $\mathcal{F}(A, B)$ is called a covariant functor from the category $\mathfrak{C}$ into the category $\mathfrak{D}$.

9.2. Waring's formula. Let $\mathbf{Z}$ be the ring of rational integers, $y_1, \ldots, y_k$ indeterminates and n a positive integer. For every positive integer i, let $W_i^{(n)} \in \mathbf{Z}[y_1, \ldots, y_k]$ be the sum of those terms in the expansion of $(y_1 + \ldots + y_k)^i$ into monomials $cy_1^{e_1} \ldots y_k^{e_k}$ for which $e_1 + 2e_2 + \ldots + ke_k = n$. Then the polynomial $W_n = \sum_{i=1}^{n} [(-1)^i n/i] W_i^{(n)}$ belongs to $\mathbf{Z}[y_1, \ldots, y_k]$. If $x_1, \ldots, x_k$ are indeterminates and $a_t = (-1)^t \sum (x_{i_1} \ldots x_{i_t} | i_1 < \ldots < i_t)$, $t = 1, \ldots, k$, then $W_n(a_1, \ldots, a_k) = x_1^n + \ldots + x_k^n$.

We refer the reader to RÉDEI [2] for a detailed proof.

9.3. We continue with a few number-theoretical results that can be found in almost every text on number theory.

Let $\mathbf{Z}$ be the ring of rational integers, n a positive integer, (n) the principal ideal with basis n, and $\mathbf{Z}|(n)$ the corresponding factor ring of order n. The group $\mathcal{L}(\mathbf{Z}|(n))$ of units of $\mathbf{Z}|(n)$ is called the group of prime residue classes mod n. We call $\varphi(n) = |\mathcal{L}(\mathbf{Z}|(n))|$ the Euler φ-function. If $n = ab$ and $(a, b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$, and if p is a prime and $e \geqslant 1$, then $\varphi(p^e) = p^e(1 - 1/p)$.

Let $q > 1$ be a fixed integer. Then any integer $k \geqslant 0$ can be written uniquely as $k = a_m q^m + a_{m-1} q^{m-1} + \ldots + a_0$ where $m \geqslant 0$ and $0 \leqslant a_i < q$, $i = 0, 1, \ldots, m$. This representation is called the q-adic expansion of k and $s_q(k) = a_m + \ldots + a_0$ is called the sum of digits of this expansion. If k and l are arbitrary positive integers, then $s_q(k+l) \leqslant s_q(k) + s_q(l)$, and if we put $\lambda(i) = \max(\lambda | q^\lambda \text{ divides } i)$, then $\sum_{i=1}^{k} \lambda(i) = (k - s_q(k))/(q-1)$.

In contrast to these very elementary results, the famous DIRICHLET theorem is very deep. It is used at the end of ch. 4 and can be stated as follows:

If a, b are positive rational integers and $(a, b) = 1$, then the arithmetic progression $an+b$, $n = 1, 2, 3, \ldots$ contains infinitely many primes.

9.4. WEIL [1] has proved the RIEMANN hypothesis for algebraic function fields over finite fields. Two of its consequences are the theorem of LANG and WEIL on the number of rational points of varieties in finite fields and a theorem of CARLITZ and WELLS which we need here.

Let K be a finite field of order q, and $\sim$ the equivalence relation on $K\times K\times K$ defined by: $(b_1, b_2, b_3) \sim (a_1, a_2, a_3)$ if and only if there is $0 \neq l \in K$ such that $b_i = la_i$, $i = 1, 2, 3$. Then a special case of the LANG–WEIL theorem is the following

9.41. Theorem. *Let $u \in K[x, y, z]$ be an absolutely irreducible form of degree $d > 0$ and n the number of non-equivalent solutions in K of the equation $u(x, y, z) = 0$. Then*

$$|n-q| \leqslant (d-1)(d-2)\sqrt{(q)}+k(d)$$

where $k(d)$ is a constant which depends only on d.

For a proof, we refer to LANG and WEIL [1].

Now we state the CARLITZ-WELLS result:

9.42. Theorem. *Let K be a finite field of order q; $a_1, \ldots, a_r, b_1, \ldots, b_r$ non-zero elements of K such that $a_ib_j \neq a_jb_i$, for $i \neq j$; $k, k_1, \ldots, k_r$ positive integers and n the number of solutions in K of the system*

$$y_i^{k_i} = a_i+b_ix^k, \qquad i = 1, \ldots, r,$$

of equations in $x, y_1, \ldots, y_r$. Then $n = q+O(q^{1/2})\,(q \to \infty)$, i.e. $|n-q| \leqslant Cq^{1/2}$, for some $C > 0$.

For a proof, we refer to CARLITZ-WELLS [1].

9.5. Finally we state some elementary results from analysis: The complex exponential function e^z, for $z = i\varphi$, φ being real, satisfies $e^{i\varphi} = \cos\varphi + i\sin\varphi$ which is a special case of EULER's formula and implies DE MOIVRE's equation $(\cos\varphi+i\sin\varphi)^n = \cos n\varphi+i\sin n\varphi$, for any integer n. We have $\cos(\pi-\varphi) = -\cos\varphi$. If, for any differentiable real function f, ∂f denotes the first derivative, then $\partial\cos\varphi = -\sin\varphi$, and if g is also a differentiable function, then $\partial(f\circ g) = (\partial f\circ g)\,\partial g$. If f is a polynomial in x over the field of real numbers and σ is the canonical mapping from the ring of polynomials to the ring of polynomial functions, then $\partial(\sigma f) = \sigma f'$.

Remarks and comments

§ 1–9. The concept of a multioperator group is due to HIGGINS [1]. KUROŠ [2] contains the elements of the theory of multioperator groups. § 5.8 follows ENGSTRÖM [1], Th. 5.86 was also proved by a different method in the paper by FRIED and MAC RAE [1]. Prop. 6.8 is due to HIGMAN, B. H. NEUMANN and H. NEUMANN [1], Lemma 6.91 is a result of GASCHÜTZ [1]. The theory of d.g. near-rings with minimum condition as contained in § 8 has been developed by LAUSCH [7], using some ideas of BEIDLEMAN [1], [2]. Prop. 8.51 was proved by LAUSCH [6].

BIBLIOGRAPHY

ABIAN, A.

[1] On the solvability of infinite systems of Boolean polynomial equations. Colloq. Math. **21** (1970), 27–30.

ACZÉL, J.

[1] Über die Gleichheit der Polynomfunktionen auf Ringen. Acta Sci. Math. (Szeged) **21** (1960), 105–107.

ADLER, I.

[1] Composition rings. Duke Math. J. **29** (1962), 607–623.

AHMAD, S.

[1] The cycle structure of permutation polynomials of the form x^k over GF(q). J. Combinatorial Theory **6** (1969), 370–374.

[2] Split dilations of finite cyclic groups with applications to finite fields. Duke Math. J. **37** (1970), 547–554.

AIGNER, M.

[1] Über Gruppen von Restklassen nach Restpolynomidealen in Dedekindschen Integritätsbereichen. Diss. Univ. Wien 1964.

ALLENBY, R. B.

[1] Adjunctions of roots to nilpotent groups. Proc. Glasgow Math. Assoc. **7** (1966), 109–118.

ANDREOLI, G.

[1] Algebricità delle funzioni booleane. Ricerca (Napoli) (2) **13** (1962) gennaio–aprile, 1–6.

[2] Una proprietà caratteristica per la soluzione dei sistemi di equazioni booleane e loro discussione. Ricerca (Napoli) (2) **13** (1962) maggio–agosto, 1–9.

BEIDLEMAN, J. C.

[1] Distributively generated near-rings with descending chain condition. Math. Z. **91** (1966), 65–69.

[2] Nonsemi-simple distributively generated near-rings with minimum condition. Math. Ann. **170** (1967), 206–213.

BERMAN, G. and R. J. SILVERMAN

[1] Simplicity of near-rings of transformations. Proc. Amer. Math. Soc. **10** (1959), 456–459.

[2] Embedding of algebraic systems. Pacific J. Math. **10** (1960), 777–786.

BIAŁYNICKI-BIRULA, A. and M. ROSENLICHT

[1] Injective morphisms of real algebraic varieties. Proc. Amer. Math. Soc. **13** (1962), 200–203.

BOKUT', L. A.

[1] Theorems of imbedding in the theory of algebras. Colloq. Math. **14** (1966), 349–353 (in Russian).

BURKE, J. C.

[1] Remarks concerning tri-operational algebra. Rep. Math. Colloquium (2) **7** (1946), 68–72.

CAHEN, P. J. et J. L. CHABERT

[1] Coefficients et valeurs d'un polynôme. Bull. Sci. math. II. Sér. **95** (1971), 295 – 304.

CARCANAGUE, J.

[1] Propriétés des q-polynomes. C.R. Acad. Sci. Paris Sér. A–B **265** (1967), A 415–A 418.

[2] q-polynomes abéliens sur un corps K. C.R. Acad. Sci. Paris Sér. A–B **265** (1967), A 496–A 499.

CARLITZ, L.

[1] Permutations in a finite field. Proc. Amer. Math. Soc. **4** (1953), 538.

[2] A note on integral-valued polynomials. Indag. Math. **21** (1959), 294–299.

[3] A theorem on permutations in a finite field. Proc. Amer. Math. Soc. **11** (1960), 456–459.

[4] A note on permutation functions over a finite field. Duke Math. J. **29** (1962), 325–332.

[5] Some theorems on permutation polynomials. Bull. Amer. Math. Soc. **68** (1962), 120–122.

[6] A note on permutations in an arbitrary field. Proc. Amer. Math. Soc. **14** (1963), 101.

[7] Permutations in finite fields. Acta Sci. Math. (Szeged) **24** (1963), 196–203.

[8] Functions and polynomials mod p^n. Acta Arith. **9** (1964), 67–78.

CARLITZ, L. and D. R. HAYES

[1] Permutations with coefficients in a subfield. Acta Arith. 21 (1972), 131–135.

CARLITZ, L. and C. WELLS

[1] The number of solutions of a special system of equations in a finite field. Acta Arith. **12** (1966), 77–84.

CAVIOR, S. R.

[1] A note on octic permutation polynomials. Math. Comp. **17** (1963), 450–452.

[2] Uniform distribution of polynomials modulo m. Amer. Math. Monthly **73** (1966), 171–172.

CHOWLA, P.

[1] On some polynomials which represent every natural number exactly once. Norske Vid. Selsk. Forh. (Trondheim) **34** (1961), 8–9.

CHOWLA, S.

[1] On substitution polynomials mod p. Norske Vid. Selsk. Forh. (Trondheim) **41** (1968), 4–6.

CHOWLA, S. and H. ZASSENHAUS

[1] Some conjectures concerning finite fields. Norske Vid. Selsk. Forh. (Trondheim) **41** (1968), 34–35.

CLAY, J. R. and D. K. DOI
[1] Maximal ideals in the near ring of polynomials over a field. Proc. on the Colloq. on Rings, Modules and Radicals, Keszthely (Hungary) 1971, pp. 117–133.
COHEN, S. D.
[1] The distribution of polynomials over finite fields. Acta Arith. **17** (1970), 255–271.
COHN, P. M.
[1] Universal algebra. Harper and Row, New York 1965.
CURTIS, C. W. and I. REINER
[1] Representation theory of finite groups and associative algebras. Interscience Publishers, New York 1962.
DAVENPORT, H. and D. J. LEWIS
[1] Notes on congruences I. Quart. J. Math. Oxford (2), **14** (1963), 51–60.
DICKER, R. M.
[1] The substitutive law. Proc. London Math. Soc. **13** (1963), 493–510.
DICKSON, L. E.
[1] Analytic functions suitable to represent substitutions. Amer. J. Math. **18** (1896), 210–218.
[2] The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. Ann. of Math. **11** (1896–97), 65–120.
[3] Linear groups. Teubner, Leipzig 1901. Reprint: Dover, New York 1958.
[4] History of the theory of numbers, Vol. III. Carnegie Institution, Washington 1923.
[5] Introduction to the theory of numbers. University Press, Chicago 1929.
DIRNBERGER, J.
[1] Über eine Klasse von ganzzahligen Polynomgruppen in mehreren Unbestimmten. Diss. Univ. Wien 1964.
DÖRGE, K.
[1] Bemerkungen über Elimination in beliebigen Mengen mit Operationen. Math. Nachr. **4** (1951), 282–297.
[2] Über die Lösbarkeit allgemeiner algebraischer Gleichungssysteme und einige weitere Fragen. Math. Ann. **171** (1967), 1–21.
DÖRGE, K. und H. K. SCHUFF
[1] Über Elimination in beliebigen Mengen mit allgemeinsten Operationen. Math. Nachr. **10** (1953), 315–330.
DUEBALL, F.
[1] Bestimmung von Polynomen aus ihren Werten mod p^n. Math. Nachr. **3** (1949), 71–76.
ENGSTRÖM, H. T.
[1] Polynomial substitutions. Amer. J. Math. **63** (1941), 249–255.
ERDÉLYI, M.
[1] Systems of equations over non commutative groups. Publ. Math. Debrecen **7** (1960), 310–315.
FADELL, A. G. and K. D. MAGILL
[1] Automorphisms of semigroups of polynomials. Compositio Math. **21** (1969), 233–239.

FEICHTINGER, G.
[1] Über eine Klasse von Polynomgruppen. Diss. Univ. Wien 1963.
FERSCHL, F. und W. NÖBAUER
[1] Über eine Klasse von auflösbaren Gruppen. Monatsh. Math. **62** (1958), 324–344.
FILLMORE, J.
[1] A note on split dilations defined by higher residues. Proc. Amer. Math. Soc. **18** (1967), 171–174.
FOSTER, A. L.
[1] Generalized "Boolean" theory of universal algebras. I. Subdirect sums and normal representation theorem. Math. Z. **58** (1953), 306–336.
[2] Generalized "Boolean" theory of universal algebras. II. Identities and subdirect sums of functionally complete algebras. Math. Z. **59** (1953), 191–199.
[3] The identities of—and unique subdirect factorization within—classes of universal algebras. Math. Z. **62** (1955), 171–188.
[4] Ideals and their structure in classes of operational algebras. Math. Z. **65** (1956), 70–75.
[5] An existence theorem for functionally complete universal algebras. Math. Z. **71** (1959), 69–82.
[6] Functional completeness in the small. Algebraic structure theorems and identities. Math. Ann. **143** (1961), 29–58.
[7] Functional completeness in the small. II. Algebraic cluster theorem. Math. Ann. **148** (1962), 173–191.
[8] Semi-primal algebras: Characterization and normal-decomposition. Math. Z. **99** (1967), 105–116.
[9] Congruence relations and functional completeness in universal algebras; structure theory of hemiprimals. I. Math. Z. **113** (1970), 293–308.
FOSTER, A. L. and A. PIXLEY
[1] Semicategorical algebras. I. Semi-primal algebras. Math. Z. **83** (1964), 147–169.
FRIED, M. D.
[1] On a conjecture of Schur. Michigan Math. J. **17** (1970), 41–55.
FRIED, M. D. and R. E. MACRAE
[1] On the invariance of chains of fields. Illinois J. Math. **13** (1969), 165–171.
FRÖHLICH, A.
[1] The near-ring generated by the inner automorphisms of a finite simple group. J. London Math. Soc. **33** (1958), 95–107.
FRYER, K. D.
[1] Note on permutations in a finite field. Proc. Amer. Math. Soc. **6** (1955), 1–2.
[2] A class of permutation groups of prime degree. Canad. J. Math. **7** (1955), 24–34.
FUJIWARA, T.
[1] On the existence of algebraically closed algebraic extensions. Osaka J. Math. **8** (1956), 23–33.
GASCHÜTZ, W.
[1] Zu einem von B. H. und H. Neumann gestellten Problem. Math. Nachr. **14** (1955), 249–252.

GERSTENHABER, M. and O. S. ROTHAUS
[1] The solution of sets of equations in groups. Proc. Nat. Acad. Sci. U.S.A. **48** (1962), 1531–1533.
GILMER, R. W.
[1] R-automorphisms of $R[X]$. Proc. London Math. Soc. (3) **18** (1968), 328–336.
GOODSTEIN, R. L.
[1] Polynomial generators over Galois fields. J. London Math. Soc. **36** (1961), 29–32.
[2] Polynomial generators over finitely generated rings. J. London Math. Soc. **38** (1963), 79–80.
[3] The solution of equations in a lattice. Proc. Roy. Soc. Edinburgh Sect. A **67** (1965/67), 231–242.
GRÄTZER, G.
[1] Notes on lattice theory II: On Boolean functions. Rev. Roumaine Math. Pures Appl. **7** (1962), 693–697.
[2] Boolean functions on distributive lattices. Acta Math. Acad. Sci. Hungar. **15** (1964), 195–201.
[3] Universal algebra. Van Nostrand, Princeton, 1968.
GWEHENBERGER, G.
[1] Über die Darstellung von Permutationen durch Polynome und rationale Funktionen. Diss. TH Wien 1970.
AF HÄLLSTRÖM, G.
[1] Über halbvertauschbare Polynome. Acta Acad. Åbo. Ser. B **21** (1957), Nr. 2, 20 pp.
HAYES, D.
[1] A geometric approach to permutation polynomials over a finite field. Duke Math. J. **34** (1967), 293–305.
HEISLER, J.
[1] A characterization of finite fields. Amer. Math. Monthly **74** (1967), 537–538.
HIGGINS, P. J.
[1] Groups with multiple operators. Proc. London Math. Soc. (3) **6** (1956), 366–416.
HIGMAN, G., B. H. NEUMANN and H. NEUMANN
[1] Embedding theorems for groups. J. London Math. Soc. **24** (1949), 247–254.
HION, JA. V.
[1] Ω-ringoids, Ω-rings and their representations. Trudy Moskov. Mat. Obšč. **14** (1965), 3–47 (in Russian).
[2] Ω-ringoids, Ω-rings and their representations. Tartu Riikl. Ül. Toimetised Vih. **192** (1966), 3–11 (in Russian).
[3] m-ary Ω-ringoids. Sibirsk. Mat. Ž. **8** (1967), 174–194 (in Russian).
HOANG KI
[1] S-complete groups, SR-groups, SD-groups. Sibirsk. Mat. Ž. **10** (1969), 1427–1430 (in Russian).
HOSSZÚ, M.
[1] Notes on vanishing polynomials. Acta Sci. Math. (Szeged) **21** (1960), 108–110.
HULE, H.
[1] Über Polynome und algebraische Gleichungen in universalen Algebren. Diss. Univ. Wien 1968.

[2] Polynome über universalen Algebren. Monatsh. Math. **73** (1969), 329–340.
[3] Algebraische Gleichungen über universalen Algebren. Monatsh. Math. **74** (1970), 50–55.
HUPPERT, B.
[1] Endliche Gruppen I. Springer, Berlin 1967.
ISAACS, I. M.
[1] Systems of equations and generalized characters in groups. Canad. J. Math. **22** (1970), 1040–1046.
JACOBSTHAL, E.
[1] Über vertauschbare Polynome. Math. Z. **63** (1955), 243–276.
KAISER, H. K.
[1] Vollständigkeit in universalen Algebren. Diss. Univ. Wien 1972.
KALOUJNINE, L.
[1] La structure des p-groupes de Sylow des groupes symetriques finis. Ann. Sci. École Norm. Sup. (3) **65** (1948), 239–276.
KAMKE, E.
[1] Theory of sets. Dover, New York 1950.
KAUTSCHITSCH, H.
[1] Kommutative Teilhalbgruppen der Kompositionshalbgruppe von Polynomen und formalen Potenzreihen. Monatsh. Math. **74** (1970), 421–436.
KELLER, G. and F. R. OLSON
[1] Counting polynomial functions. Duke Math. J. **35** (1968), 835–838.
KEMPNER, A. J.
[1] Polynomials and their residue systems. Trans. Amer. Math. Soc. **22** (1921), 240–288.
[2] Polynomials of several variables and their residue systems. Trans. Amer. Math. Soc. **27** (1925), 287–298.
KERTÉSZ, A.
[1] Vorlesungen über Artinsche Ringe. Akadémiai Kiadó, Budapest 1968.
KNOEBEL, A. R.
[1] Simplicity vis-à-vis functional completeness. Math. Ann. **189** (1970), 299–307.
KOWOL, G.
[1] Über die Struktur einer Klasse von auflösbaren Gruppen. Monatsh. Math. **76** (1972), 306–316.
KURBATOV, V. A.
[1] A generalization of a theorem of Schur on a class of algebraic functions. Mat. Sb. **21** (63) (1947), 133–140 (in Russian).
[2] On the monodromy group of an algebraic function. Mat. Sb. **25** (67) (1949), 51–94 (in Russian).
KURBATOV, V. A. and N. G. STARKOV
[1] The analytic representation of permutations. Sverdlovsk. Gos. Ped. Inst. Učen. Zap. **31** (1965), 151–158.
KUROŠ, A. G.
[1] The theory of groups, Vol. I and Vol. II. Second English edition. Chelsea Publishing Comp., New York 1960.

[2] Lectures on general algebra. Chelsea Publishing Comp., New York 1963.

LANG, S. and A. WEIL
[1] Number of points of varieties in finite fields. Amer. J. Math. **76** (1954), 819–827.

LAUSCH, H.
[1] Über Halbgruppen aus Polynomabbildungen von Restklassenringen. Monatsh. Math. **69** (1965), 151–166.
[2] Zweigliedrige Gruppen über kommutativen Ringen mit Einselement. Monatsh. Math. **69** (1965), 326–338.
[3] Eine Charakterisierung nilpotenter Gruppen der Klasse 2. Math. Z. **93** (1966), 206–209.
[4] Functions on groups with multiple operators. J. London Math. Soc. **42** (1967), 698–700.
[5] Zur Theorie der Polynompermutationen über endlichen Gruppen. Arch. Math. (Basel) **19** (1968), 284–288.
[6] An application of a theorem of Gaschütz. Bull. Austral. Math. Soc. **1** (1969), 381–384.
[7] Idempotents and blocks in Artinian d.g. near rings with identity element. Math. Ann. **188** (1970), 43–52.

LAUSCH, H., W. MÜLLER und W. NÖBAUER
[1] Über die Struktur einer durch Dicksonpolynome dargestellten Permutationsgruppe des Restklassenrings mod *n*. J. Reine Angew. Math. **260** or **261**.

LAUSCH, H., W. NÖBAUER und F. SCHWEIGER
[1] Polynompermutationen auf Gruppen. Monatsh. Math. **69** (1965), 410–423.
[2] Polynompermutationen auf Gruppen II. Monatsh. Math. **70** (1966), 118–126.

LAUSCH, H. and F. SCHWEIGER
[1] Characterization of groups by monomials. J. Algebra **6** (1967), 115–122.

LAWKINS, W. F.
[1] Permutation polynomials of finite fields. M.A. Thesis Univ. of Tennessee 1966.

LEVI, H.
[1] Composite polynomials with coefficients in an arbitrary field of characteristic zero. Amer. J. Math. **64** (1942), 389–400.

LEVIN, F.
[1] Solutions of equations over groups. Bull. Amer. Math. Soc. **68** (1962), 603–604.
[2] One variable equations over groups. Arch. Math. (Basel) **15** (1964), 179–188.
[3] One variable equations over semigroups. Bull. Austral. Math. Soc. **2** (1970), 247–252.

LEWIS, D. J.
[1] Ideals and polynomial functions. Amer. J. Math. **78** (1956), 71–77.

LIDL, R.
[1] Über Permutationspolynome in mehreren Unbestimmten. Monatsh. Math. **75** (1971), 432–440.
[2] Über die Darstellung von Permutationen durch Polynome. Abh. Math. Sem. Univ. Hamburg **37** (1972), 108–111.
[3] Über Permutationsfunktionen in mehreren Unbestimmten. Acta Arith. **20** (1972), 291–296.

LIDL, R. and H. NIEDERREITER
[1] On orthogonal systems and permutation polynomials in several variables. Acta Arith. 22 (1972), 307–315.

LIDL, R. and C. WELLS
[1] Čebyšev polynomials in several variables. J. R. A. Math. **255** (1972), 104–111.

LITZINGER, M.
[1] A basis for residual polynomials in *n* variables. Trans. Amer. Math. Soc. **37** (1935), 216–225.

LONDON, D. and Z. ZIEGLER
[1] Functions over the residue field modulo a prime. J. Austral. Math. Soc. **7** (1967), 410–416.

LYNDON, R. C.
[1] Dependence in groups. Colloq. Math. **14** (1966), 275–283.

MACCLUER, C. R.
[1] On a conjecture of Davenport and Lewis concerning exceptional polynomials. Acta Arith. **12** (1967), 289–299.

MANNOS, M.
[1] Ideals in tri-operational algebras. I. Rep. Math. Colloquium (2) **7** (1946), 73–79.

MAURER, W. D. and J. L. RHODES
[1] A property of finite simple nonabelian groups. Proc. Amer. Math. Soc. **16** (1965), 552–554.

MENGER, K.
[1] Tri-operational algebra. Rep. Math. Colloquium (2) **5–6** (1944), 3–10.
[2] The algebra of functions: past, present, future. Rend. Mat. e Appl. (5) **20** (1961), 409–430.
[3] Superassociative systems and logical functors. Math. Ann. **157** (1964), 278–295.

MENGER, K. and H. J. WHITLOCK
[1] Two theorems on the generation of systems of functions. Fund. Math. **58** (1966), 229–240.

MILGRAM, A. N.
[1] Saturated polynomials. Rep. Math. Colloquium (2) **7** (1946), 65–67.

MITSCH, H.
[1] Trioperationale Algebren über Verbänden. Diss. Univ. Wien 1967.
[2] Über Polynome und Polynomfunktionen auf Verbänden. Monatsh. Math. **74** (1970), 239–243.

MLITZ, R.
[1] Ein Radikal für universale Algebren und seine Anwendung auf Polynomringe mit Komposition. Monatsh. Math. **75** (1971), 144–152.

MÜLLER, W.
[1] Eindeutige Abbildungen mit Summen-, Produkt- und Kettenregel im Polynomring. Monatsh. Math. **73** (1969), 354–367.

MYCIELSKI, J. and C. RYLL-NARDZEWSKI
[1] Equationally compact algebras. II. Fund. Math. **61** (1967/68), 271–281.

NEUMANN, B. H.
[1] A note on algebraically closed groups. J. London Math. Soc. **27** (1952), 247–249.

[2] The isomorphism problem for algebraically closed groups. Word problems, Decision problems and the Burnside problem in group theory, pp. 553–562, Amsterdam 1973.
[3] Algebraically closed semigroups. Studies in Pure Math. pp. 185–194, London 1971.

NEUMANN, H.
[1] Varieties of groups. Springer, Berlin 1967.

NIEDERREITER, H.
[1] Permutation polynomials in several variables over finite fields. Proc. Japan Acad. **46** (1970), 1001–1005.
[2] Orthogonal systems of polynomials in finite fields. Proc. Amer. Math. Soc. **28** (1971), 415–422.
[3] Permutation polynomials in several variables. Acta Sci. Math. (Szeged) **33** (1972), 53–58.

NIVEN, I. and L. J. WARREN
[1] A generalization of Fermat's theorem. Proc. Amer. Math. Soc. **8** (1957), 306–313.

NÖBAUER, W.
[1] Über einen Satz von Eckmann. Diss. Univ. Wien 1950.
[2] Über Gruppen von Restklassen nach Restpolynomidealen. Österr. Akad. Wiss. Math.-Natur. Kl. S.-B. II. **162** (1953), 207–233.
[3] Über eine Gruppe der Zahlentheorie. Monatsh. Math. **58** (1954), 181–192.
[4] Gruppen von Restklassen nach Restpolynomidealen in mehreren Unbestimmten. Monatsh. Math. **59** (1955), 118–145.
[5] Gruppen von Restpolynomidealrestklassen nach Primzahlpotenzen. Monatsh. Math. **59** (1955), 194–202.
[6] Über die Formengruppe. Monatsh. Math. **59** (1955), 305–317.
[7] Eine Verallgemeinerung der eindimensionalen linearen Gruppe mod *n*. Monatsh. Math. **60** (1956), 249–256.
[8] *M*-Untergruppen von Restklassengruppen. Monatsh. Math. **60** (1956), 269–287.
[9] Über eine Klasse von *M*-Untergruppen. Monatsh. Math. **61** (1957), 195–208.
[10] Über die Operation des Einsetzens in Polynomringen. Math. Ann. **134** (1958), 248–259.
[11] Die Operation des Einsetzens bei Polynomen in mehreren Unbestimmten. J. Reine Angew. Math. **201** (1959), 207–220.
[12] Zur Theorie der Vollideale. Monatsh. Math. **64** (1960), 176–183.
[13] Zur Theorie der Vollideale II. Monatsh. Math. **64** (1960), 335–348.
[14] Über die Ableitungen der Vollideale. Math. Z. **75** (1961), 14–21.
[15] Die Operation des Einsetzens bei rationalen Funktionen. Österr. Akad. Wiss. Math.-Natur. Kl. S.-B. II **170** (1962), 35–84.
[16] Funktionen auf kommutativen Ringen. Math. Ann. **147** (1962), 166–175.
[17] Gruppen von linear gebrochenen Permutationen mod *n*. Monatsh. Math. **66** (1962), 219–226.
[18] Durch linear gebrochene Substitutionen in mehreren Variablen erzeugte Permutationsgruppen mod *n*. Monatsh. Math. **67** (1963), 117–124.
[19] Derivationssysteme mit Kettenregel. Monatsh. Math. **67** (1963), 36–49.

[20] Über die Darstellung von universalen Algebren durch Funktionenalgebren. Publ. Math. Debrecen **10** (1963), 151–154.
[21] Bemerkungen über die Darstellung von Abbildungen durch Polynome und rationale Funktionen. Monatsh. Math. **68** (1964), 138–142.
[22] Zur Theorie der Polynomtransformationen und Permutationspolynome. Math. Ann. **157** (1964), 332–342.
[23] Über die Vollideale und Permutationspolynome eines Galoisfeldes. Acta Math. Acad. Sci. Hungar. **16** (1965), 37–42.
[24] Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen. Monatsh. Math. **69** (1965), 230–238.
[25] Polynome, welche für gegebene Zahlen Permutationspolynome sind. Acta Arith. **11** (1966), 437–442.
[26] Mehrdimensionale Polynompermutationen auf endlichen Gruppen. Monatsh. Math. **71** (1967), 148–155.
[27] Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen. J. Reine Angew. Math. **231** (1968), 215–219.

NÖBAUER, W. und W. PHILIPP
[1] Über die Einfachheit von Funktionenalgebren. Monatsh. Math. **66** (1962), 441–452.
[2] Die Einfachheit der mehrdimensionalen Funktionenalgebren. Arch. Math. (Basel) **15** (1964), 1–5.

ORE, O.
[1] On a special class of polynomials. Trans. Amer. Math. Soc. **35** (1933), 559–584.
[2] Contributions to the theory of finite fields. Trans. Amer. Math. Soc. **36** (1934), 243–274.

PHILIPP, W.
[1] Über die Einfachheit von Funktionenalgebren über Verbänden. Monatsh. Math. **67** (1963), 259–268.

PIXLEY, A. F.
[1] Functionally complete algebras generating distributive and permutable classes. Math. Z. **114** (1970), 361–372.

QUACKENBUSH, R. W.
[1] Demi-semi-primal algebras and Mal'cev-type conditions. Math. Z. **122** (1971), 166–176.

RÉDEI, L.
[1] Über eindeutig umkehrbare Polynome in endlichen Körpern. Acta Sci. Math. (Szeged) **11** (1946–48), 85–92.
[2] Algebra I. Pergamon Press, Oxford 1967.

RÉDEI, L. und T. SZELE
[1] Algebraisch-zahlentheoretische Betrachtungen über Ringe I. Acta Math. **79** (1947), 291–320.
[2] Algebraisch-zahlentheoretische Betrachtungen über Ringe II. Acta Math. **82** (1950), 209–241.

RIHA, W.
[1] Zur Theorie der Oreschen Polynomringe. Diss. Univ. Wien 1966.

RITT, J. F.
[1] Prime and composite polynomials. Trans. Amer. Math. Soc. **23** (1922), 51–66.
ROUSSEAU, G.
[1] Completeness in finite algebras with a single operation. Proc. Amer. Math. Soc. **18** (1967), 1009–1013.
RUDEANU, S.
[1] On Boolean equations. An. Sti. Univ. "Al. I. Cuza" Iasi Sect. I a Mat. **6** (1960), 520–522.
[2] Boolean functions and functions of Sheffer. Acad. R.P. Române Stud. Cerc. Mat. **12** (1961), 553–566.
[3] Irredundant solutions of boolean and pseudo-boolean equations. Rev. Roumaine Math. Pures Appl. **11** (1966), 183–188.
[4] On functions and equations in distributive lattices. Proc. Edinburgh Mat. Soc. (2) **16** (1968/69), 49–54.
[5] On elimination in Boolean algebra. Hitotsubashi J. Arts Sci. **10** (1969), 74–75.
ŠAIN, B. M.
[1] Theory of semigroups as a theory of superpositions of many-place functions. Interuniv. Sci. Sympos. General Algebra Tartu Gos. Univ. 1966, 169–190 (in Russian).
[2] Automorphisms of polynomial semigroups. Semigroup Forum **1** (1970), 279–281.
SCHIEK, H.
[1] Adjunktionsproblem und inkompressible Relationen. Math. Ann. **146** (1962), 314–320.
SCHITTENHELM, R.
[1] Dreigliedrige Gruppen über kommutativen Ringen mit Einselement. Diss. Univ. Wien 1967.
SCHÖNIGER, W.
[1] Über Kongruenzen in Ringen. Diss. Univ. Wien 1951.
SCHWEIGERT, D.
[1] Zur Theorie der Verbandspolynome. Diss. TH Wien 1972.
SCHWEIZER, B. and A. SKLAR
[1] The algebra of multiplace vector-valued functions. Bull. Amer. Math. Soc. **73** (1967), 510–515.
SCHUFF, H. K.
[1] Über Wurzeln von Gruppenpolynomen. Math. Ann. **124** (1952), 294–297.
[2] Zur Darstellung von Polynomen über Verbänden. Math. Nachr. **11** (1954), 1–4.
[3] Polynome über allgemeinen algebraischen Systemen. Math. Nachr. **13** (1955), 343–366.
SCHUMACHER, F.
[1] Über die Polynompermutationen der endlichen Gruppen. Diss. Univ. Wien 1970.
SCHUR, I.
[1] Über den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz über algebraische Funktionen. S. B. Preuß. Akad. Wiss. Berlin 1923, 123–134.

SCOGNAMIGLIO, G.
[1] Interpolazione per le funzioni algebriche booleane. Giorn. Mat. Battaglini (5) **9** (89) (1961), 14–41.
SCOTT, S. D.
[1] The arithmetic of polynomial maps over a group and the structure of certain permutational polynomial groups. I. Monatsh. Math. **73** (1969), 250–267.
SCOTT, W. R.
[1] Algebraically closed groups. Proc. Amer. Math. Soc. **2** (1951), 118–121.
SHAFAAT, A.
[1] Self dual lattice polynomials. J. Natur. Sci. and Math. **5** (1965), 227–230.
SHODA, K.
[1] Zur Theorie der algebraischen Erweiterungen. Osaka J. Math. **4** (1952), 133–143.
[2] Über die nicht algebraischen Erweiterungen algebraischer Systeme. Proc. Japan Acad. **30** (1954), 70–73.
[3] Bemerkungen über die Existenz der algebraisch abgeschlossenen Erweiterung. Proc. Japan Acad. **31** (1955), 128–130.
SIERPIŃSKI, W.
[1] Sur les fonctions de plusiers variables. Fund. Math. **33** (1945), 169–173.
SKALA, H.
[1] Irreducibly generated algebras. Fund. Math. **67** (1970), 31–37.
SŁOMIŃSKI, J.
[1] On the solving of systems of equations over quasi-algebras and algebras. Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. **10** (1962), 627–635.
SOLOMON, L.
[1] The solution of equations in groups. Arch. Math. (Basel) **20** (1969), 241–247.
SPECHT, W.
[1] Gruppentheorie. Springer, Berlin 1956.
SPIRA, R.
[1] Polynomial interpolation over commutative rings. Amer. Math. Monthly **75** (1968), 638–640.
STRAUS, E.
[1] On the polynomials, whose derivatives have integral values at the integers. Proc. Amer. Math. Soc. **2** (1951), 24–27.
STUEBEN, E. F.
[1] Ideals in two place tri-operational algebras. Monatsh. Math. **69** (1965), 177–182.
SUVAK, J. A.
[1] Full ideals and their ring groups for commutative rings with identity. Diss. Univ. of Arizona 1971.
SZÁSZ, G.
[1] Introduction to lattice theory. Academic Press, New York 1963.
TROTTER, H. F.
[1] Groups in which raising to a power is an automorphism. Canad. Math. Bull. **8** (1965), 825–827.
VAN DER WAERDEN, B. L.
[1] Algebra, Erster Teil. Springer, Berlin 1966.

[2] Algebra, Zweiter Teil. Springer, Berlin 1967.

WEGLORZ, B.

[1] Equationally compact algebras. I. Fund. Math. **59** (1966), 289–298.

[2] Equationally compact algebras. III. Fund. Math. **60** (1967), 89–93.

WEGNER, U.

[1] Über die ganzzahligen Polynome, die für unendlich viele Primzahlmoduln Permutationen liefern. Diss. Univ. Berlin 1928.

WEIL, A.

[1] On the Riemann hypothesis in function fields. Proc. Nat. Acad. Sci. U.S.A. **27** (1941), 345–347.

WELLS, C.

[1] Groups of permutation polynomials. Monatsh. Math. **71** (1967), 248–262.

[2] Generators for groups of permutation polynomials. Acta Sci. Math. (Szeged) **29** (1968), 167–176.

[3] The degrees of permutation polynomials over finite fields. J. Combinatorial Theory **7** (1969), 49–55.

WENZEL, G. H.

[1] On (S, A, m)-atomic compact relational systems. Math. Ann. **194** (1971), 12–18.

WERNER, H.

[1] Eine Charakterisierung funktional vollständiger Algebren. Arch. Math. (Basel) **21** (1970), 381–385.

WHITLOCK, H. J.

[1] A composition algebra for multiplace functions. Math. Ann. **157** (1964), 167–178.

WILLIAMS, K. S.

[1] On exceptional polynomials. Canad. Math. Bull. **11** (1968), 279–282.

ZANE, B.

[1] Uniform distribution modulo m of monomials. Amer. Math. Monthly **71** (1964), 162–164.

ZARISKI, O. and P. SAMUEL

[1] Commutative Algebra, Vol. I. Van Nostrand, Princeton 1958.

AUTHOR INDEX

SUBJECT INDEX