GROUPS AND LATTICES

PÉTER P. PÁLFY

Department of Algebra and Number Theory, Eötvös University
Budapest, P.O.Box 120, H–1518 Hungary

Dedicated to the memory of my father, József Pálfy (1922–2001)

Abstract

In this survey paper we discuss some topics from the theory of subgroup lattices. After giving a general overview, we investigate the local structure of subgroup lattices. A major open problem asks if every finite lattice occurs as an interval in the subgroup lattice of a finite group. Next we investigate laws that are valid in normal subgroup lattices. Then we sketch the proof that every finite distributive lattice is the normal subgroup lattice of a suitable finite solvable group. Finally, we discuss how far the subgroup lattice of a direct power of a finite group can determine the group.

1 Introduction

This survey paper is the written version of my four talks given at the Groups – St Andrews 2001 in Oxford conference. I selected some topics on subgroup lattices and normal subgroup lattices according to my personal taste and interest. These topics, of course, cannot cover all interesting and important parts of the theory. For a more complete overview the reader should consult the small book of Michio Suzuki [60] from 1956 and the more recent monograph by Roland Schmidt [54]. The latter one is a thick volume of 541 pages including 384 references. So it is clearly impossible to give a comprehensive survey here. My choice of topics was partly guided by the review of Schmidt's book by Ralph Freese [13].

The study of subgroup lattices has quite a long history, starting with Richard Dedekind's work [10] in 1877, including Ada Rottlaender's paper [47] from 1928 and later numerous important contributions by Reinhold Baer, Øystein Ore, Kenkichi Iwasawa, Leonid Efimovich Sadovskii, Michio Suzuki, Giovanni Zacher, Mario Curzio, Federico Menegazzo, Roland Schmidt, Stewart Stonehewer, Giorgio Busetto, and many-many others.

In Section 2 we will list some of the most remarkable results on subgroup lattices. Hints to the contents of Sections 3–6 will also be given there. These later sections are surveys of some particular topics, therefore proofs are very rarely given, and even then, they will be quite sketchy.

The lattice formed by all subgroups of a group will be denoted by $\mathrm{Sub}(G)$ and will be called the *subgroup lattice* of the group G. It is a *complete lattice*: any number of subgroups H_i have a *meet* (greatest lower bound) $\bigwedge H_i$, namely their intersection

$\bigcap H_i$, and a *join* (least upper bound) $\bigvee H_i$, namely the subgroup generated by all of them together. Notice that we denote the lattice operations by $\wedge$ and $\vee$.

An element $c \in \mathcal{L}$ in a complete lattice is called *compact* if

$$c \leq \bigvee_{i \in I} a_i \quad \text{implies} \quad c \leq \bigvee_{i \in J} a_i \text{ for a finite subset } J \subseteq I.$$

It is easy to see that $H \in \mathrm{Sub}(G)$ is compact if and only if H is a finitely generated subgroup of G. A complete lattice is called *algebraic* if every element is a join of compact elements. We see that subgroup lattices are always algebraic.

If the group is finite, it is a convenient way to visualize the lattice using its *Hasse diagram*, where the bottom element represents the identity subgroup 1, the top element the group itself, and between two elements of the lattice a line segment is drawn whenever the lower subgroup is a maximal subgroup in the upper one. An example is shown in Figure 1.

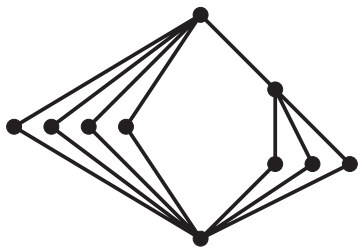


Figure 1. Hasse diagram of $\mathrm{Sub}(A_4)$

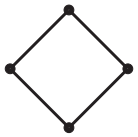
Our notation is mostly standard. For $H \leq G$ we denote by $\mathbf{N}_G(H)$, $\mathbf{C}_G(H)$ the normalizer and the centralizer of H in G, respectively. The center and the commutator subgroup of G is denoted by $\mathbf{Z}(G)$ and G'. The automorphism group and the inner automorphism group are written as $\mathrm{Aut}\, G$ and $\mathrm{Inn}\, G$. For normal subgroups we use the notation $N \lhd G$. The set of normal subgroups is a sublattice in $\mathrm{Sub}(G)$, it will be denoted by $\mathrm{Norm}(G)$. Intervals in lattices will be defined in Section 2, and in subgroup lattices they will be denoted as $\mathrm{Int}[H; G]$. The cyclic group of order n will be written as C_n, the dihedral group of degree n (and order $2n$) as D_n, the alternating and symmetric groups as A_n and S_n. Furthermore, $\mathrm{GF}(q)$ will denote the q-element field, and $F^\times$ the multiplicative group of a field F.

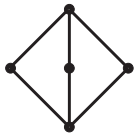
2 Overview

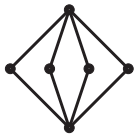
We start with some simple observations concerning subgroup lattices. Since we will mainly deal with finite groups, let us remark that the subgroup lattice $\mathrm{Sub}(G)$ is finite if and only if the group G is finite. For some small lattices it is easy to determine all groups that have the given lattice as subgroup lattice. For example,

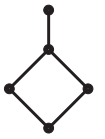
$\mathrm{Sub}(G) =$  if and only if G is cyclic of prime order;

$\mathrm{Sub}(G) =$  if and only if G is cyclic of order p^2 for a prime p;

$\mathrm{Sub}(G) =$  if and only if G is cyclic of order pq (with primes $p \neq q$);

$\mathrm{Sub}(G) =$  if and only if G is the four-element Klein group;

$\mathrm{Sub}(G) =$  if and only if either $G \cong C_3 \times C_3$ or $G \cong D_3$.

However, there is no group G with $\mathrm{Sub}(G) =$  .

So there are lattices which are subgroup lattices of infinitely many, of finitely many, of a unique, or of no group. That is, the correspondence $G \mapsto \mathrm{Sub}(G)$ is neither injective, nor surjective. This fact gives rise to two questions:

1. Which groups are uniquely determined by their subgroup lattices?
2. Which lattices are subgroup lattices?

The answer to the second question is very complicated, as given by B. V. Yakovlev [64] in 1974, based on his description of the subgroup lattices of free groups. We would be interested rather in the local structure of subgroup lattices, that is we would like to know what are the possible intervals in subgroup lattices. If $a < b$ are elements of a lattice $\mathcal{L}$, by the *interval* $\mathrm{Int}[a; b]$ we mean the sublattice formed by the intermediate elements:

$$\mathrm{Int}[a; b] = \{x \in \mathcal{L} \mid a \leq x \leq b\}.$$

In Section 3 we will see that every algebraic lattice can occur as an interval in the subgroup lattice of an infinite group. For finite groups, however, it is not known whether every finite lattice can be found as an interval in the subgroup lattice of a suitable finite group. The main subject of Section 3 will be a survey of results concerning this open problem.

An important line of investigations deals with groups whose subgroup lattices satisfy certain laws. As it follows from the following basic result, there is no non-trivial law that holds in the subgroup lattice of every group.

Theorem 2.1 (Whitman [63], 1946) *Every lattice is isomorphic to a sublattice of the subgroup lattice of some group.*

There is also a remarkable finite version of this embedding theorem.

Theorem 2.2 (Pudlák and Tůma [46], 1980) *Every finite lattice is isomorphic to a sublattice of the subgroup lattice of some finite group.*

The most familiar lattice law is the distributivity. Recall that a lattice $\mathcal{L}$ is called *distributive* if the following equivalent conditions hold for every $x, y, z \in \mathcal{L}$:

- $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$;
- $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$;
- $(x \vee y) \wedge (x \vee z) \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$.

One of the nicest results in the theory of subgroup lattices characterizes those groups which have distributive subgroup lattices.

Theorem 2.3 (Ore [37], 1937–38) *The subgroup lattice* $\mathrm{Sub}(G)$ *is distributive if and only if the group* G *is locally cyclic.*

Recall that a group G is said to be *locally cyclic*, if every finitely generated subgroup of G is cyclic. There are not too many such groups: a group G is locally cyclic if and only if it is isomorphic to a subgroup of either the additive group of the rationals $\mathbb{Q}$ or of its quotient group $\mathbb{Q}/\mathbb{Z}$.

Cyclic groups can be characterized by the properties that $\mathrm{Sub}(G)$ is distributive and satisfies the *ascending chain condition* (i.e., it contains no infinite chain of subgroups $H_1 < H_2 < H_3 < \ldots$). If $n = p_1^{k_1} \cdots p_r^{k_r}$, then the subgroup lattice of the cyclic group of order n is the direct product of chains of lengths $k_1, \ldots, k_r$, independently of the primes p_i.

The description of groups with modular subgroup lattices is quite complicated. As it is well known, a lattice $\mathcal{L}$ is called *modular* if for all $x, y, z \in \mathcal{L}$

$$x \geq z \Rightarrow x \wedge (y \vee z) = (x \wedge y) \vee z.$$

(In Section 4 we will give some equivalent conditions as well.) The subgroup lattices of abelian groups are modular, as it was discovered by Richard Dedekind [10] in 1877 for the case of the subgroup lattice of the additive group of the complex numbers. So we make the assumption that

$$G \text{ is nonabelian and } \mathrm{Sub}(G) \text{ is a modular lattice.}$$

The characterization consists of several pieces.

Theorem 2.4 (Iwasawa [23], 1943) *If* G *has elements of infinite order, then the torsion subgroup* $T(G)$ *of* G *is abelian,* $G/T(G)$ *is a torsion-free abelian group of rank one, etc.*

For the omitted details see [54, 2.4.11 Theorem].

Theorem 2.5 (Schmidt [53], 1986) *If G is a torsion group, then G is a direct product of Tarski groups, extended Tarski groups and a locally finite group, such that elements from different direct factors have coprime orders.*

A *Tarski group* is an infinite group in which every proper nontrivial subgroup has prime order. Tarski groups were first constructed by Olshanskii [35] in 1979. An *extended Tarski group* is such that $G/\mathbf{Z}(G)$ is a Tarski group of exponent p for some prime p, $\mathbf{Z}(G)$ is cyclic of order $p^r > 1$, and for every subgroup $H \leq G$, either $H \leq \mathbf{Z}(G)$ or $H \geq \mathbf{Z}(G)$ holds. The subgroup lattice of an extended Tarski group is shown in Figure 2. Note that extended Tarski groups do exist if p is sufficiently large (see Olshanskii [36]).

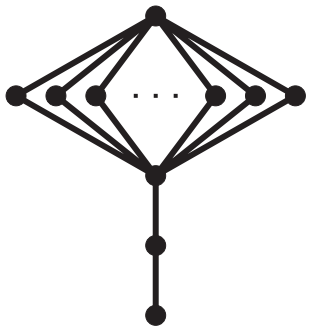


Figure 2. The subgroup lattice of an extended Tarski group

Theorem 2.6 (Iwasawa [23], 1943) *If G is a locally finite group, then G is a direct product of P^*-groups and locally finite p-groups, such that elements from different direct factors have coprime orders.*

By definition, a *P^*-group* is a semidirect product of an elementary abelian normal subgroup A with a cyclic group $\langle t \rangle$ of prime power order such that t induces a power automorphism ($tat^{-1} = a^r$ with a fixed r for all $a \in A$) of prime order on A. In fact, all these groups have modular subgroup lattices.

Theorem 2.7 (Iwasawa [23], 1943) *If G is a locally finite p-group, then either G is a direct product of the quaternion group with an elementary abelian 2-group, or G contains an abelian normal subgroup A of exponent p^k with cyclic quotient group G/A of order p^m and there exist an element $b \in G$ with $G = A\langle b \rangle$ and an integer s (which is at least 2 if $p = 2$) such that $s < k \leq s + m$ and $bab^{-1} = a^{1+p^s}$ for all $a \in A$.*

Again, all these groups have modular subgroup lattices.

Theorems 2.4, 2.5, 2.6, 2.7 together yield a complete characterization of non-abelian groups with modular subgroup lattices.

As we have seen, some lattice theoretic properties may correspond to some simple group theoretic ones, but sometimes the description of groups with subgroup

lattices of certain type (such as modular lattices) are awkward. Unfortunately, nice characterisations are rather rare. We list some (maybe all) of them now.

The *Jordan–Dedekind chain condition* means that all maximal chains in the lattice have the same length. Finite groups with such subgroup lattices have a beautiful description.

Theorem 2.8 (Iwasawa [22], 1941) *For a finite group G, the subgroup lattice* $\mathrm{Sub}(G)$ *satisfies the Jordan–Dedekind chain condition if and only if G is supersolvable.*

A lattice $\mathcal{L}$ is called *sectionally complemented* if for every $b < c \in \mathcal{L}$ there exists a $d \in \mathcal{L}$ such that $b \wedge d = 0$ (the smallest element of the lattice) and $b \vee d = c$. This lattice theoretic property also has a neat group theoretic counterpart.

Theorem 2.9 (Bechtell [6], 1965) *For a finite group G, the subgroup lattice* $\mathrm{Sub}(G)$ *is sectionally complemented if and only if every Sylow subgroup of G is elementary abelian.*

Sectionally complemented lattices are more general than *relatively complemented lattices*, in which for every $a < b < c \in \mathcal{L}$ the existence of a $d \in \mathcal{L}$ with $b \wedge d = a$ and $b \vee d = c$ is required (see Figure 3). So here we need an additional condition. By definition, G is a *T^*-group* if being a normal subgroup is a transitive relation among the subgroups of G, that is $A \lhd B \lhd C \leq G$ implies $A \lhd C$.

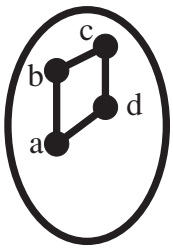


Figure 3. Relatively complemented lattice

Theorem 2.10 (Zacher [65], 1952) *For a finite group G, the subgroup lattice* $\mathrm{Sub}(G)$ *is relatively complemented if and only if every Sylow subgroup of G is elementary abelian and G is a T^*-group.*

We shall also investigate laws in normal subgroup lattices. One basic fact is that $\mathrm{Norm}(G)$ is always modular. There are even stronger laws that hold in normal subgroup lattices, as — for example — the arguesian law. We will deal with this subject in Section 4. Our main concern will be whether there exist laws that distinguish subgroup lattices of abelian groups from normal subgroup lattices in general.

In Section 5 we are going to show that every finite distributive lattice is the normal subgroup lattice of a finite solvable group. It does not seem feasible to describe which lattices can be normal subgroup lattices.

In general $\mathrm{Sub}(G)$ does not determine G uniquely. A lattice isomorphism between subgroup lattices $\mathrm{Sub}(G)$ and $\mathrm{Sub}(H)$ is called a *projectivity*. We restrict our attention — unless stated otherwise — to finite groups. Although there are cases when infinitely many groups share the same subgroup lattice, these lattices can be singled out easily.

Theorem 2.11 (Suzuki [59], 1951) *If* $\mathrm{Sub}(G)$ *has no chain as a direct factor, then there are only finitely many nonisomorphic groups* H *with* $\mathrm{Sub}(H) \cong \mathrm{Sub}(G)$.

Also certain — but by far not all — properties of groups are preserved by projectivities. Assume that $\mathrm{Sub}(G) \cong \mathrm{Sub}(H)$ for finite groups G, H.

- If G is cyclic, then H is also cyclic.
- If G is abelian, then H need not be abelian (even nilpotent).
- If G is a p-group which is neither cyclic, nor elementary abelian, then H is also a p-group (Suzuki [59], 1951).
- If G is solvable, then H is also solvable (Suzuki [59], 1951; Zappa [67], 1951; Schmidt [50], 1968).
- If G is simple, then H is also simple (Suzuki [59], 1951; extension to infinite groups: Zacher [66], 1982). Moreover, using the classification of finite simple groups, it follows that $H \cong G$.

Without using the classification (of course), Michio Suzuki proved a result which will motivate our investigations in the final Section 6.

Theorem 2.12 (Suzuki [59], 1951) *If* G *is a finite simple group and* $\mathrm{Sub}(H) \cong \mathrm{Sub}(G \times G)$, *then* $H \cong G \times G$.

We will look at the question, whether the lattice $\mathrm{Sub}(G \times \cdots \times G)$ can be used to characterize the group G.

3 Local stucture

In this section we are going to study the local structure of subgroup lattices, that is, the possible intervals $\mathrm{Int}[H;K] = \{X \mid H \leq X \leq K\}$ in subgroup lattices $\mathrm{Sub}(G)$ (where $H < K \leq G$). Clearly, we can restrict our attention to *top intervals* (what lattice theorists call *principal filters*), where $K = G$ (see Figure 4). Also, if $N \lhd G$ with $N \leq H$, then obviously $\mathrm{Int}[H;G] \cong \mathrm{Int}[H/N;G/N]$, hence we may — and will — always assume that H is *core-free*, i.e., $\bigcap_{g\in G} gHg^{-1} = 1$.

It is easy to see, that intervals in algebraic lattices are algebraic lattices themselves, hence every interval in a subgroup lattice is an algebraic lattice. Namely, a subgroup $X \in \mathrm{Int}[H;G]$ is a compact element of the interval if and only if it

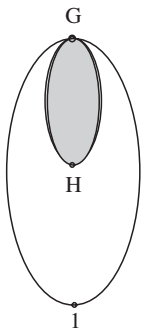


Figure 4. Top interval in Sub(G)

is finitely generated over H, i.e., $X = \langle H, g_1, \ldots, g_k \rangle$ for a suitable finite set of elements $g_1, \ldots, g_k \in G$.

Indeed, there is nothing more one can say about the local structure of subgroup lattices as the following deep result of Jiří Tůma shows.

Theorem 3.1 (Tůma [62], 1989) *For every algebraic lattice $\mathcal{L}$ there exist groups $H < G$ such that* $\mathrm{Int}[H; G] \cong \mathcal{L}$.

It should be noted that Tůma's ingenious construction always yields infinite groups G, even for finite lattices $\mathcal{L}$. Hence we have the following open problem.

Problem 3.2 Is it true that for every finite lattice $\mathcal{L}$ there exist finite groups $H < G$ such that $\mathrm{Int}[H; G] \cong \mathcal{L}$?

The problem actually originates from universal algebra, so let us make a short detour to this area. The reader should be reminded of Graham Higman's witty remarks about Cohn's *Universal Algebra* [19][1]:

"Universal algebra is something everyone ought to know about, though nobody should specialize in it (from which it might appear to follow that though everyone ought to read this book, nobody should have written it). From the point of view of the working algebraist, its main function is to remind him that there are several levels of generality at which work can profitably be done, and that, to get the best out of a method, it is necessary to set it at the right level."

In what follows I try to present a problem in universal algebra which had made me think that it is worthwhile specializing in universal algebra, before I realized that it is in fact a problem in group theory.

By an *algebra* $\mathbf{A} = (A; F)$ we mean a nonempty set A equipped with a set of operations F, that is, each $f \in F$ is a map $f : A^{n(f)} \to A$ for a suitable $n(f)$, called the *arity* of f. For example, in a group we have three operations: multiplication (binary), inverse (unary), and the identity element (considered a nullary operation $G^0 \to G$). In a lattice we have two binary operations: join and meet. The obvious definitions for subalgebras, homomorphisms, direct products make sense in this general setting as well.

[1] I thank Пeter Neumann for calling my attention to Higman's review.

However, for arbitrary algebras the kernel of a homomorphism $\varphi : \mathbf{A} \to \mathbf{B}$ cannot be defined in the way it is done in the case of groups, namely, as a preimage of a specific element of $\mathbf{B}$; not even for a homomorphism between lattices (cf. Figure 5).

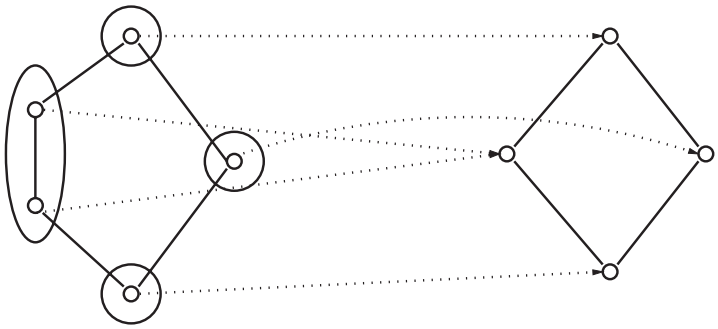


Figure 5. Kernel of a lattice homomorphism

Instead, the appropriate definition of the *kernel* gives a binary relation

$$\ker \varphi = \{(a, a') \in A^2 \mid \varphi(a) = \varphi(a')\}.$$

In fact, $\alpha = \ker \varphi$ is a *congruence relation*, that is, an equivalence relation compatible with all operations $f \in F$, i.e., if f is n-ary, and $a_1, \dots, a_n$, $a'_1, \dots, a'_n \in A$ are such that $(a_i, a'_i) \in \alpha$ for all $i = 1, \dots, n$ then

$$\Big(f(a_1, \dots, a_n), f(a'_1, \dots, a'_n)\Big) \in \alpha.$$

All congruence relations of an algebra $\mathbf{A}$ form an algebraic lattice $\operatorname{Con}\mathbf{A}$, the *congruence lattice* of $\mathbf{A}$. For a group G the congruence lattice is essentially the same as the normal subgroup lattice $\operatorname{Norm}(G)$. Apart from being algebraic there is no other general property of congruence lattices as the following classical result of universal algebra tells us.

Theorem 3.3 (Grätzer and Schmidt [15], 1963) *For every algebraic lattice $\mathcal{L}$ there exists an algebra $\mathbf{A}$ such that* $\operatorname{Con}\mathbf{A} \cong \mathcal{L}$.

If we have a group G and a subgroup $H < G$, then we can consider the permutation representation of G on the left cosets by H as a multi-unary algebra $\mathbf{A} = (G/H; G)$, where $g \in G$ as a unary operation sends the coset $xH \in G/H$ to gxH. Now it is easy to see that the congruence lattice of this multi-unary algebra, $\operatorname{Con}\mathbf{A} \cong \operatorname{Int}[H; G]$. So Tůma's Theorem 3.1 yields a new proof for the Grätzer–Schmidt Theorem.

Both of these proofs are inherently infinite. Namely, the basic idea — without going into technical details — can be summarized in the following steps, constructing recursively an infinite sequence of algebras (or groups) $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$, ... (see Figure 6):

1. take $\mathbf{A}_i$ and list all the "troubles" occurring in $\mathbf{A}_i$;

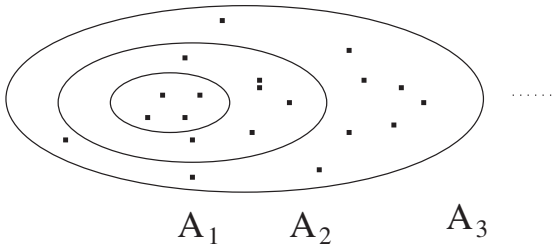


Figure 6. Infinite procedure

2. add new elements and extend the operations so that these "troubles" are eliminated and call the extended algebra $\mathbf{A}_{i+1}$;
3. repeat.

Finally, in $\mathbf{A} = \bigcup_{i=1}^{\infty} \mathbf{A}_i$ all "troubles" disappear, and it will have the required congruence lattice.

Clearly, every finite lattice is algebraic. Therefore, the finite version of the congruence lattice representation problem arises naturally.

Problem 3.4 Is it true that for every finite lattice $\mathcal{L}$ there exists a finite algebra $\mathbf{A}$ such that $\operatorname{Con} \mathbf{A} \cong \mathcal{L}$?

Although arbitrary algebras are allowed here, the core of the problem is group theoretic, as the following result shows.

Theorem 3.5 (Pálfy and Pudlák [42], 1980) *The following are equivalent:*
(i) Every finite lattice occurs as the congruence lattice of some finite algebra.
(ii) Every finite lattice occurs as an interval in the subgroup lattice of some finite group.

Using the multi-unary algebra arising from the permutation representation of G on the left cosets by H, it is obvious that (ii) implies (i). The point here is that the converse is also true. Note that, in the case when both statements were false, we do not claim that every finite lattice which is a congruence lattice of a finite algebra is in fact an interval in the subgroup lattice of a finite group. Quite possibly, there can be more lattices that are not intervals in subgroup lattices of finite groups, than lattices that are not congruence lattices of finite algebras.

The "tame congruence theory" developed by David Hobby and Ralph McKenzie [21] shows that in every finite algebra with a certain type of congruence lattice there are some subsets (the so-called minimal sets) on which the induced algebras are actually permutation groups with the same congruence lattice as the one of the original algebra. Therefore, Problem 3.4 in fact belongs to group theory, not to universal algebra.

Special attention has been given to finite lattices with the simplest structure. These lattices $\mathcal{M}_n$ consist of a smallest, a greatest, and n pairwise incomparable elements (see Figure 7).

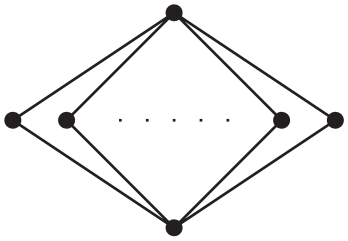


Figure 7. The lattice $\mathcal{M}_n$

Some of these lattices are easy to represent as intervals, even as subgroup lattices. Namely, $\mathcal{M}_1 = \mathrm{Sub}(C_{p^2})$ for any prime p; $\mathcal{M}_2 = \mathrm{Sub}(C_{pq})$ for any pair of distinct primes p, q; $\mathcal{M}_{p+1} = \mathrm{Sub}(C_p \times C_p)$ for each prime p, but also this is the subgroup lattice of any nonabelian group of order pq, where q is a prime divisor of $p-1$.

If $n = p^k + 1$ for some prime p and exponent $k \geq 1$, then it is also possible to find suitable intervals $\mathrm{Int}[H; G] = \mathcal{M}_n$. Namely, let V be the 2-dimensional vector space over the Galois field $\mathrm{GF}(p^k) = F$ and take

$$G = \{x \mapsto \lambda x + v \mid \lambda \in F^\times, v \in V\}, \quad H = \{x \mapsto \lambda x \mid \lambda \in F^\times\}.$$

Then every intermediate subgroup $H \leq K \leq G$ has the form

$$K = \{x \mapsto \lambda x + v \mid \lambda \in F^\times, v \in U\}$$

for a suitable subspace $U \leq V$, so $\mathrm{Int}[H; G]$ is just the lattice of subspaces of V.

For quite a while it had been conjectured that these are the only $\mathcal{M}_n$'s occurring as intervals in subgroup lattices of finite groups. However, this is not the case, as it was first pointed out by Walter Feit. In formulating his observation we shall use the following notation. If $p > 2$ is a prime and $d \mid (p-1)/2$ then up to conjugacy there is a unique subgroup of order pd in the alternating group A_p, which we will denote simply by $p \cdot d$.

Example 3.6 (Feit [11], 1983)

(1) $\mathcal{M}_7 = \mathrm{Int}[31 \cdot 5, A_{31}]$, the intermediate subgroups are the normalizer $31 \cdot 15$ of $31 \cdot 5$ and six subgroups isomorphic to $\mathrm{GL}_5(2)$.

(2) $\mathcal{M}_{11} = \mathrm{Int}[31 \cdot 3, A_{31}]$, the intermediate subgroups are the normalizer $31 \cdot 15$ of $31 \cdot 3$ and ten subgroups isomorphic to $\mathrm{PSL}_3(5)$.

These examples cannot be generalized (see also [40]).

Theorem 3.7 (Basile [5], 2001) *If* $\mathrm{Int}[H; G] \cong \mathcal{M}_n$ *with* $G = S_d$ *or* A_d, *then either* $n \leq 3$ *or one of the following holds:* $n = 5$, $d = 13$; $n = 7$, $d = 31$; $n = 11$, $d = 31$.

Much later a new series of examples was found by Andrea Lucchini.

Theorem 3.8 (Lucchini [31], 1994) *There exist intervals $\mathcal{M}_n$ in subgroup lattices of finite groups with*

$$n = q + 2 \quad \text{or} \quad n = \frac{q^t + 1}{q + 1} + 1,$$

where q is a prime power and t is an odd prime.

At present the smallest cases for which no occurrence of $\mathcal{M}_n$ is known are $n = 16$, 23, 35, ... In a seminal paper Baddeley and Lucchini [2] analyse the structure of a hypothetical group providing an example of an interval $\mathcal{M}_n$ with n not belonging to the set of known values. More precisely, they make the following assumptions.

Assumptions. Let $n > 50$,

$$n \notin \left\{ q + 1,\ \ q + 2,\ \ \frac{q^t + 1}{q + 1} + 1 \ \middle|\ q \text{ a prime power, } t \text{ an odd prime} \right\},$$

and assume that there exist finite groups $H < G$ such that $\mathrm{Int}[H; G] \cong \mathcal{M}_n$. Furthermore, let G be the smallest one among all groups with this property.

Then, by a result of Peter Köhler [27], G has a unique minimal normal subgroup M, and M is nonabelian (see [42]). So M is a direct product of isomorphic nonabelian simple groups. Let F denote one of the simple factors.

The case when $M \cap H \neq 1$ was dealt with by Lucchini [32] in 1994. He proved that in this case M itself is simple, so G is an *almost simple* group. So we suppose that $M \cap H = 1$. We distinguish two cases, namely, whether $MH = G$ or $MH < G$.

It can be shown that M is complemented in the second case as well, that is, $G = MK$ and $M \cap K = 1$ with a suitable subgroup $K > H$. Now G has the structure of a *twisted wreath product* of F and K.

Baddeley and Lucchini derive the following properties of the ingredients of this twisted wreath product:

- K is an almost simple group,
- H is a core-free maximal subgroup of K,
- $Q = \mathbf{N}_K(F)$ is a core-free subgroup of K,
- $K = QH$,
- the homomorphism $\varphi : Q \to \mathrm{Aut}\, F$ satisfies $\varphi(Q \cap H) \geq \mathrm{Inn}\, F$,
- $\varphi|_{Q \cap H}$ has no extension to any subgroup of H properly containing $Q \cap H$.

Furthermore, $n - 1$ is the number of those homomorphisms $\psi : Q \to \mathrm{Aut}\, F$ for which $\psi|_{Q \cap H} = \varphi|_{Q \cap H}$ and $\tilde{\psi} = \tilde{\varphi}$ hold, where $\tilde{\varphi}$ denotes the composition of φ with the natural homomorphism onto the outer automorphism group $\mathrm{Out}\, F = \mathrm{Aut}\, F / \mathrm{Inn}\, F$.

It should be noted, however, that no such example is known with $n \geq 3$.

The case $MH = G$ leads to even more complex technical conditions, which we cannot reproduce here in full detail. We only mention that in this case H has a unique minimal normal subgroup N, which is a direct product of isomorphic copies of a nonabelian simple group E, and F is isomorphic to a section of E.

These reductions raise several problems about simple groups. We quote only two of them here.

Problem 3.9 (Baddeley and Lucchini [2], 1997) Describe the maximal nonabelian simple sections of the nonabelian simple groups.

Problem 3.10 (Baddeley and Lucchini [2], 1997) Describe all pairs (F, L) where F is a nonabelian simple group and L is a group of automorphisms of F such that there is exactly one proper nontrivial L-invariant subgroup of F.

Another important development concerning the local structure of subgroup lattices of finite groups is a recent result of Ferdinand Börner. He was able to reduce Problem 3.2 to two special cases.

Theorem 3.11 (Börner [8], 1999) *Every finite lattice is an interval in the subgroup lattice of some finite group if and only if at least one of the following statements is true:*

(C) For every finite lattice $\mathcal{L}$ there exist finite groups $H < G$ such that $\mathrm{Int}[H;G] \cong \mathcal{L}$*, with the following properties: G has a unique minimal normal subgroup M, $M \cap H = 1$, $MH = G$, M is nonabelian, and if F denotes one of the simple direct factors of M and $Q = \mathbf{N}_H(F)$, then Q induces all inner automorphisms of F and Q is core-free in H.*

(D) For every finite lattice $\mathcal{L}$ which is generated by its coatoms (maximal elements) there exist finite groups $H < G$ such that $\mathrm{Int}[H;G] \cong \mathcal{L}$*, where G is an almost simple group and H is core-free in G.*

The condition on the lattice in (D) is not very restrictive, as every finite lattice can be embedded as an interval into a finite lattice which is generated by its coatoms. The key of Börner's tricky construction is to embed the given lattice as an interval into a larger lattice as it is vaguely sketched in Figure 8. If this larger lattice occurs as an interval in the subgroup lattice of a finite group, then this group must have a very restricted structure.

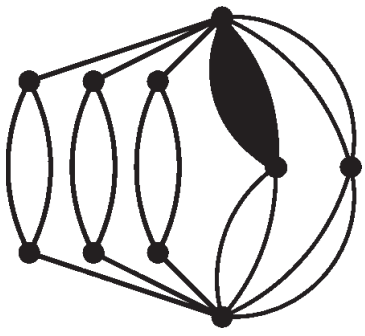


Figure 8. Börner's construction

Similar arguments can be found in a paper of Robert Baddeley [1]. The key words in these investigations are *quasiprimitive groups* and *twisted wreath products*.

Let me end this section with some speculation concerning statement (C). It is so restrictive that probably it can be proved to be false, and then the problem

would be reduced to the case of almost simple groups. Then it would remain to do a case-by-case analysis, like it has been done for the alternating and symmetric groups by Alberto Basile (see Theorem 3.7).

Although it seems unlikely that (C) is true, but if it is, it may be proved "combinatorially", without relying much on the structure of the simple group F (similarly as in Lucchini's construction proving Theorem 3.8).

Here we could summarize only the most important developments concerning Problem 3.2. Some other aspects of it are discussed in more detail in [41].

4 Laws in normal subgroup lattices

It is well-known that normal subgroup lattices are modular. Modular lattices can be defined via a number of equivalent conditions. The most useful form is an implication (Horn-formula):

$$X \geq Z \quad \Rightarrow \quad (X \wedge Y) \vee Z = X \wedge (Y \vee Z).$$

Since the left hand side is always smaller than or equal to the right hand side, it can be formulated as an inequality as well:

$$X \geq Z \quad \Rightarrow \quad (X \wedge Y) \vee Z \geq X \wedge (Y \vee Z).$$

The assumption $X \geq Z$ can be eliminated by replacing Z with $X \wedge Z$, thus obtaining the *modular law:*

$$(X \wedge Y) \vee (X \wedge Z) = X \wedge [Y \vee (X \wedge Z)].$$

A characterization of modular lattices can be given by a forbidden sublattice as well:

A lattice is modular if and only if it contains no sublattice  .

The modular law was discovered by Richard Dedekind [10] in 1877. He studied the subgroup lattice of the additive group of complex numbers, but the proof is clearly the same for the subgroup lattice of any abelian group. Dedekind called a subgroup "Modul" and denoted the join of two subgroups by $\mathfrak{a} + \mathfrak{b}$ and their meet by $\mathfrak{a} - \mathfrak{b}$. So the modular law in Dedekind's work appears in the form

$$(\mathfrak{a} - \mathfrak{b}) + (\mathfrak{a} - \mathfrak{c}) = \mathfrak{a} - (\mathfrak{b} + (\mathfrak{a} - \mathfrak{c}))$$

and its dual

$$(\mathfrak{a} + \mathfrak{b}) - (\mathfrak{a} + \mathfrak{c}) = \mathfrak{a} + (\mathfrak{b} - (\mathfrak{a} + \mathfrak{c}))$$

(see [10, p. 17]).

We will consider laws of normal subgroup lattices for various classes of groups. Let $\mathcal{V}$ be a class of groups, P, Q terms in the language of lattices (i.e., elements of the free lattice). $P \leq Q$ is a *law* in the normal subgroup lattices of $\mathcal{V}$ if for every

$G \in \mathcal{V}$ the inequality $P \leq Q$ holds in $\mathrm{Norm}(G)$ if we arbitrarily substitute normal subgroups of G for the variables in the terms P, Q and evaluate these terms in $\mathrm{Norm}(G)$. Of course, in $\mathrm{Norm}(G)$ the lattice operations are given by intersection and product:

$$X \wedge Y = X \cap Y, \quad X \vee Y = XY.$$

We will often use inequalities instead of equalities, but these are certainly equivalent to each other:

$$P \leq Q \iff P \vee Q = Q, \quad P = Q \iff P \vee Q \leq P \wedge Q.$$

There exist laws of normal subgroup lattices that are even stronger than modularity. The most important one is the *arguesian law* introduced by Bjarni Jónsson [24] in 1954. (The idea appeared earlier in a paper of Schützenberger [56] in 1945.) This is a translation of Desargues' Theorem from projective geometry into the language of lattices. Among the several equivalent formulations we prefer the following form:

$$X_1 \wedge \{Y_1 \vee [(X_2 \vee Y_2) \wedge (X_3 \vee Y_3)]\} \leq [(Q_{12} \vee Q_{23}) \wedge (Y_1 \vee Y_3)] \vee X_3,$$

where $Q_{ij} = (X_i \vee X_j) \wedge (Y_i \vee Y_j)$.

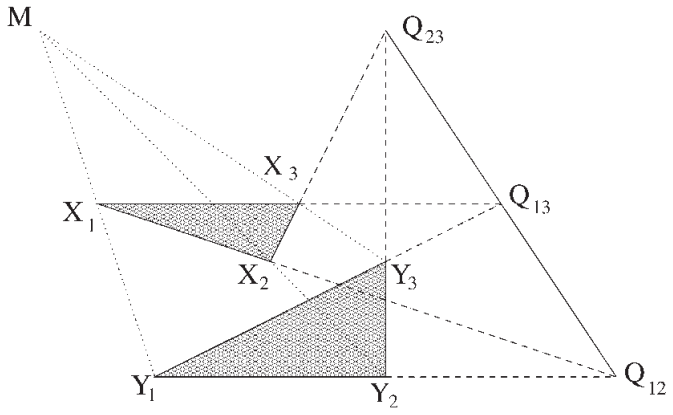


Figure 9. Desargues' Theorem

Consider the subspace lattice of a projective plane. There the join of two points is the line connecting them, the meet of two lines is their intersection point. Now if $X_1X_2X_3$ and $Y_1Y_2Y_3$ are triangles in a projective plane that are *perspective with respect to a point* (i.e., the lines X_1Y_1, X_2Y_2, X_3Y_3 go through a common point) then the left hand side of the arguesian law yields the point X_1, otherwise it yields the empty set. At the same time, the right hand side is $\geq X_1$ if and only if the two triangles are *perspective with respect to a line* (i.e., if the intersection of the corresponding sides X_iX_j and Y_iY_j are denoted by Q_{ij}, then the three points Q_{12}, Q_{13} and Q_{23} lie on one line). The reader is strongly advised to check this using Figure 9. It is a tedious but dull task to show that if the arguesian law holds for the points of the subspace lattice of a projective geometry then it holds for arbitrary

substitution of elements of the lattice (see [14, p. 207]). So the arguesian law holds in the subspace lattice of a projective plane if and only if Desargues' Theorem is true in the geometry. Since there are nonarguesian planes, the arguesian law is stronger than the modular law, as the subspace lattice is always modular.

Theorem 4.1 (Jónsson [24], 1954) *The arguesian law holds in the normal subgroup lattice of every group.*

In fact the arguesian law holds in every lattice consisting of permuting equivalence relations. (Two equivalence relations α and β are said to *permute* if $\beta \circ \alpha = \alpha \circ \beta$, where the *relational product* is defined by

$$\alpha \circ \beta = \{(a, b) \mid \exists c : (a, c) \in \alpha, (c, b) \in \beta\}.$$

For every normal subgroup $N \lhd G$ there corresponds an equivalence relation $\alpha_N = \{(a, b) \mid a, b \in G, a^{-1}b \in N\}$, and $\alpha_K \circ \alpha_N = \alpha_{KN} = \alpha_N \circ \alpha_K$, since $KN = NK$ for normal subgroups $N, K \lhd G$.)

Proof Let X_1, X_2, X_3, Y_1, Y_2, $Y_3 \lhd G$ and $x_1 \in X_1 \wedge \{Y_1 \vee [(X_2 \vee Y_2) \wedge (X_3 \vee Y_3)]\} = X_1 \cap Y_1[X_2Y_2 \cap X_3Y_3]$. Then there exist elements $x_i \in X_i$, $y_i \in Y_i$, $m \in G$ such that $x_1 = my_1^{-1}$ (using $Y_1M = MY_1^{-1}$) and $m = x_2y_2 = x_3y_3$. So we have $x_1y_1 = x_2y_2 = x_3y_3$, $x_2^{-1}x_1 = y_2y_1^{-1} \in Q_{12} = (X_1 \vee X_2) \wedge (Y_1 \vee Y_2)$, similarly $x_3^{-1}x_2 = y_3y_2^{-1} \in Q_{23}$, and multiplying these equations we obtain $x_3^{-1}x_1 = y_3y_1^{-1} \in Q_{12}Q_{23} \cap Y_1Y_3$. Taking the product with X_3 we see that $x_1 \in X_3(Q_{12}Q_{23} \cap Y_1Y_3)$ indeed. □

Mark Haiman [17] in 1987 discovered a sequence of laws, the *higher arguesian identities*

$$X_1 \wedge \left[Y_1 \vee \bigwedge_{i=2}^{n} (X_i \vee Y_i) \right] \leq \left[\bigvee_{i=1}^{n-1} Q_{i,i+1} \wedge (Y_1 \vee Y_n) \right] \vee X_n,$$

where $Q_{ij} = (X_i \vee X_j) \wedge (Y_i \vee Y_j)$, each one being strictly stronger than the previous one, that all hold in every lattice consisting of permuting equivalence relations. Later it was proved by Ralph Freese [12] that there is no finite basis for the laws of the class of all normal subgroup lattices. Like the modular and the arguesian laws, the higher arguesian identities hold not only in subgroup lattices of abelian groups (as suggested by the underlying geometry), but also in normal subgroup lattices of arbitrary groups. Based on such experiences a positive solution of the following problem had been expected.

Problem 4.2 (Jónsson [24], 1954; Birkhoff [7, p. 179], 1967) Can one embed the normal subgroup lattice of an arbitrary group into the subgroup lattice of an abelian group? Do all the laws of subgroup lattices of abelian groups hold in normal subgroup lattices?

Another reason pointing towards a positive solution was the following observation:

Proposition 4.3 *If $\mathcal{M}_3$ is a sublattice of* $\mathrm{Norm}(G)$ *with top element N, bottom element M, then N/M is abelian (see Figure 10).*

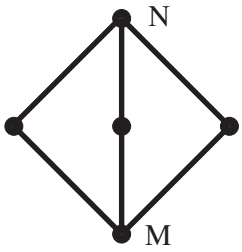


Figure 10. Abelian section in a normal subgroup lattice

However, together with my student Csaba Szabó we found another lattice identity with geometric background that shows that the normal subgroup lattice of some groups cannot be embedded into the subgroup lattice of any abelian group. A short proof for the nonembeddability of $\mathrm{Norm}(G)$ for a certain group G of order 2^9 is given in [25].

Theorem 4.4 (Pálfy and Szabó [44], 1995) *The six-cross law*
$$X_1 \wedge \{Y_1 \vee [(X_2 \vee Y_2) \wedge (X_3 \vee Y_3) \wedge (X_4 \vee Y_4)]\} \leq$$
$$(\{[(P_{12} \vee P_{34}) \wedge (P_{13} \vee P_{24})] \vee P_{23}\} \wedge \{X_4 \vee Y_1\}) \vee Y_4,$$
where $P_{ij} = (X_i \vee Y_j) \wedge (Y_i \vee X_j)$, holds in the subgroup lattice of every abelian group but fails in the normal subgroup lattice of the free group on five generators.

Another version of this law was given in [43].

Again, our six-cross law is a lattice theoretic translation of a geometric property (see Figure 11). Take four lines through a point, and two points X_i, Y_i on each of these lines ($i = 1, 2, 3, 4$). For each pair of lines define the cross point P_{ij} as the intersection of the lines X_iY_j and Y_iX_j. We say that the *six-cross theorem* holds in the projective plane, if the three lines $P_{12}P_{34}$, $P_{13}P_{24}$, and $P_{14}P_{23}$ go through a common point. (Actually, we need a more precise definition handling the degenerate cases as well, for example if some of the cross points coincide. An interesting case occurs when $P_{12} = P_{34}$, $P_{13} = P_{24}$, $P_{14} = P_{23}$. This is the famous Reye-configuration, see [20, §22]. For these details we refer to [44].) For a projective geometry the six-cross theorem is equivalent to Desargues' theorem, but their lattice theoretic counterparts differ. The six-cross law implies the arguesian law, but the converse does not hold.

Although in the formulation of Theorem 4.4 we used a free group, actually there exist finite quotients of the free group of rank 5 whose normal subgroup lattices do not satisfy the six-cross law. Moreover, it is enough to consider finite nilpotent groups, or p-groups, as the following lemma (see [34, p. 41]) shows.

Lemma 4.5 *Let $|G| = p_1^{k_1} \cdots p_n^{k_n}$, and P_i a Sylow p_i-subgroup of G for each $i = 1, \ldots, n$. Then* $\mathrm{Norm}(G)$ *is embedded into* $\mathrm{Norm}(P_1 \times \cdots \times P_n)$ *via $N \mapsto (N \cap P_1) \times \cdots \times (N \cap P_n)$.*

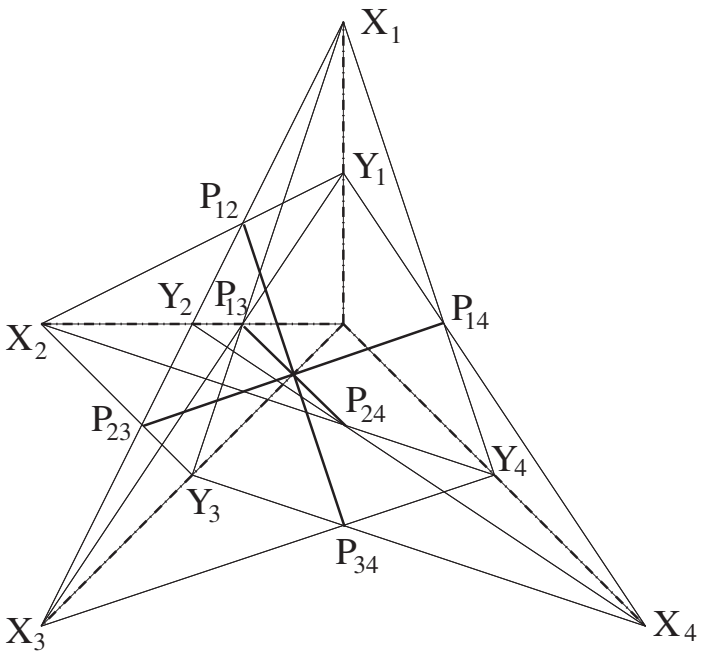


Figure 11. Six-cross theorem

So if the normal subgroup lattice of a finite group does not satisfy a certain law, then the same is true for at least one of its Sylow subgroups. If we want to work with a group of nilpotence class 2, then we better look for 2-groups, since for groups of odd order the following trick of Reinhold Baer yields an embedding of the normal subgroup lattice into the subgroup lattice of an abelian group defined on the same set of elements.

Lemma 4.6 (Baer [3], 1938) *If G of odd order has nilpotence class 2, then*

$$x + y = x^{1/2} y x^{1/2} \qquad (x^{1/2} = x^{(|G|+1)/2})$$

defines an abelian group operation.

Corollary 4.7 *If G of odd order has nilpotence class 2, then* $\mathrm{Norm}(G)$ *can be embedded into the subgroup lattice of an abelian group.*

Proof Denote by G^+ the abelian group defined in Lemma 4.6. Clearly every normal subgroup of G is a subgroup of G^+. We have to check that for every $X, Y \lhd G$ the lattice operations are the same in $\mathrm{Norm}(G)$ and in $\mathrm{Sub}(G^+)$. This is trivially true for the meet (intersection), and it is also true for the join, because the join in $\mathrm{Norm}(G)$ is a common upper bound for X and Y in $\mathrm{Sub}(G^+)$ as well, and the order formula yields that it is indeed the least upper bound:

$$|X \vee Y| = |XY| = \frac{|X| \cdot |Y|}{|X \cap Y|} = |X + Y|.$$

□

Therefore, we take the smallest noncommutative variety of 2-groups, namely let $\mathcal{V}$ be the group variety defined by $x^4 = 1$ and $x^2y = yx^2$. (This is the variety generated by any of the 8-element noncommutative groups.) In the (relatively) free groups $F_{\mathcal{V}}(r)$ in $\mathcal{V}$ with generators $g_1, \ldots, g_r$ the elements have a normal form

$$g_1^{\alpha_1} \cdots g_r^{\alpha_r} [g_1, g_2]^{\beta_{12}} [g_1, g_3]^{\beta_{13}} \cdots [g_{r-1}, g_r]^{\beta_{r-1,r}}$$

with $0 \le \alpha_i < 4$ $(1 \le i \le r)$, $0 \le \beta_{ij} < 2$ $(1 \le i < j \le r)$. Hence

$$|F_{\mathcal{V}}(r)| = 4^r 2^{r(r-1)/2} = 2^{(r^2+3r)/2}.$$

A tedious calculation gives that the normal subgroup lattice of $G = F_{\mathcal{V}}(5)$ of order 2^{20} does not satisfy the six-cross law. Namely, we have to choose $X_i = \langle g_i \rangle^G$, $Y_i = \langle g_i g_5 \rangle^G$ $(i = 1, \ldots, 4)$, where $\langle \ldots \rangle^G$ denotes the generated normal subgroup.

However, the six-cross law holds in the normal subgroup lattice of every group of odd order ([61]). Csaba Szabó [61] exhibited a law of the subgroup lattices of abelian groups that fails in the normal subgroup lattice of a group of order 3^{140}. (The calculations have been performed using GAP [55].)

For larger primes the embedding given by Lemma 4.6 can be generalized for groups of larger nilpotence class:

Theorem 4.8 (Groves [16], 1976) *If the nilpotence class of a finite p-group is less than p, then there exists a term defining an abelian group operation. Therefore, the normal subgroup lattice of such a group can be embedded into the subgroup lattice of an abelian group.*

In fact, the formula for the abelian group operation can be obtained from Lazard's inversion of the *Baker–Campbell–Hausdorff formula* (see [30])

$$x + y = xy[x, y]^{-1/2}[[x, y], x]^{1/12}[[x, y], y]^{-1/12} \cdots .$$

If the nilpotence class of the p-group is less than p, then this infinite product can be truncated at commutators of weight p or less, and the necessary roots in the group exist (as the denominators are not divisible by p). It is even enough to assume that every 3-generated subgroup has nilpotence class less than p. Is this the limit indeed?

Problem 4.9 For every prime p find a law of the subgroup lattices of abelian groups that fails in the normal subgroup lattice of a finite p-group of nilpotence class p.

We end this section by mentioning a nice result that the exponent of a group variety can be recovered from the laws satisfied by the normal subgroup lattices.

Theorem 4.10 (Herrmann and Huhn [18], 1975) *The law*

$$(X_1 \vee \ldots \vee X_n) \wedge (Y \vee Z) \le \bigvee_{i=1}^{n} [(X_1 \vee \ldots \vee X_{i-1} \vee Y \vee X_{i+1} \vee \ldots \vee X_n) \wedge (X_i \vee Z)]$$

holds in $\mathrm{Norm}(G)$ *for every group of exponent dividing n (i.e., $\forall g \in G : g^n = 1$), but if k does not divide n then it fails in* $\mathrm{Norm}(C_k^{n+1})$.

An excellent survey article related to the topics discussed in this section was written by Robert Burns and Sheila Oates-Williams [9].

5 Distributive normal subgroup lattices

It seems to be a difficult task to describe the possible normal subgroup lattices. In Section 4 we discussed certain laws that must hold in every normal subgroup lattice. However, these are not sufficient to characterize normal subgroup lattices, since this class of lattices is not closed for sublattices, as one can easily check that $\mathcal{M}_5$ is not isomorphic to the normal subgroup lattice of any group, although for each prime number p one has $\mathcal{M}_p \cong \mathrm{Norm}(C_p \times C_p)$.

In this section we have a modest goal to represent finite distributive lattices as normal subgroup lattices.

Theorem 5.1 *For every finite distributive lattice $\mathcal{D}$ there exists a finite group G such that* $\mathrm{Norm}(G) \cong \mathcal{D}$.

This result has an interesting history. It was first announced by Kuntzmann [28] in 1947. However, his proof was in error, and it could not be corrected, since he tried to construct a supersolvable group G for any finite distributive lattice $\mathcal{D}$. In fact, it is not difficult to show that not every finite distributive lattice can be represented as the normal subgroup lattice of a supersolvable group (see Figure 12). E. T. Schmidt [49, p. 101] listed Theorem 5.1 as an open problem, noting that Kuntzmann's proof was not correct.

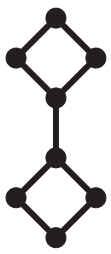


Figure 12. This is not the normal subgroup lattice of any supersolvable group

Finally, Howard Silcock [57] proved the theorem in 1977. He constructed a suitable group G as an iterated wreath product of nonabelian simple groups.

In 1986 I gave a natural construction which yields solvable groups (see [38], [39]). Now I am going to sketch this construction.

First recall a condition characterizing when $\mathrm{Norm}(G)$ is distributive. Remember that the *socle* of a group is the product of its minimal normal subgroups, and that two normal subgroups N_1 and N_2 are said to be *G-isomorphic*, if there is an isomorphism $\varphi : N_1 \to N_2$ such that $\varphi(gxg^{-1}) = g\varphi(x)g^{-1}$ for all $g \in G$ and $x \in N_1$.

Theorem 5.2 (Pazderski [45], 1987) *For a finite group G the normal subgroup lattice* $\mathrm{Norm}(G)$ *is distributive if and only if the socle of every quotient group G/N is a direct product of pairwise non-G/N-isomorphic minimal normal subgroups.*

We shall give a recursive proof of Theorem 5.1. In the groups we are going to construct every chief factor will be a Sylow subgroup, and so Pazderski's criterion will obviously be satisfied, hence the normal subgroup lattice will become distributive.

Let us start by choosing an atom $a \in \mathcal{D}$ and let $a' \in \mathcal{D}$ be a *pseudocomplement* of a, that is, a' is the largest element with $a' \wedge a = 0$. (By distributivity, if $b \wedge a = 0$ and $c \wedge a = 0$, then $(b \vee c) \wedge a = (b \wedge a) \vee (c \wedge a) = 0 \vee 0 = 0$, so the pseudocomplement exists.) Now by induction we can find a group H with $\mathrm{Norm}(H) \cong \mathrm{Int}[a; 1]$. Let us denote by $K \lhd H$ the normal subgroup corresponding to $a \vee a'$ at this isomorphism.

Next we choose a prime p not dividing $|H|$. Since in H/K no two minimal normal subgroups are isomorphic we can invoke a result of Kochendörffer [26] from 1948 guaranteeing the existence of a faithful irreducible representation of H/K over the p-element field. Let us denote the underlying module by V, and let us take the natural action of H on V with kernel K.

We claim that the semidirect product $G = VH$ will have the required normal subgroup lattice $\mathrm{Norm}(G) \cong \mathcal{D}$.

By the irreducibility of the action, V is a minimal normal subgroup of G. If $N \lhd G$, then either $N \geq V$ or $N \cap V = 1$. In the first case $N/V \lhd G/V \cong H$. In the second case $N \leq \mathbf{C}_G(V) = V \times K$, so $N \leq K$, since $(|N|, |V|) = 1$. Now it is clear that $\mathrm{Norm}(G) \cong \mathcal{D}$.

Since the subgroups of $G \times G$ containing the diagonal subgroup correspond to the normal subgroups of G, namely they have the form $H_N = \{(a, b) \in G \times G \mid aN = bN\}$ for $N \lhd G$, we obtain the following corollary related to the results of Section 3.

Corollary 5.3 *For every finite distributive lattice $\mathcal{D}$ there exists a finite group G such that for $H = \{(g, g) \mid g \in G\}$ we have* $\mathrm{Int}[H; G \times G] \cong \mathcal{D}$.

A similar idea, using higher powers, can be used to turn intervals upside-down (called the *dual lattice*).

Theorem 5.4 (Kurzweil [29], 1985) *The class of intervals in subgroup lattices of finite groups is closed under taking dual lattices.*

Proof Let $\mathcal{L} = \mathrm{Int}[H; G]$, with $|G : H| = n$ and take an arbitrary nonabelian simple group S. Consider the permutation representation of G on the cosets of H and let this permutation group act on S^n by permuting the coordinates. If $G^* = S^n G$ and $H^* = \{(s, \ldots, s) \mid s \in S\}G$, then it can be checked that $\mathrm{Int}[H^*; G^*]$ is isomorphic to the dual lattice of $\mathcal{L}$. □

6 Subgroup lattices of direct powers

The problem we are going to discuss in this section is motivated by the following classical result of Michio Suzuki.

Theorem 6.1 (Suzuki [59], 1951) *If G is a finite simple group and* $\mathrm{Sub}(H) \cong \mathrm{Sub}(G \times G)$*, then $H \cong G \times G$.*

This result was later generalized by Roland Schmidt.

Theorem 6.2 (Schmidt [51], 1981) *If G is a finite group with $G' = G$,* $\mathbf{Z}(G) = 1$*, and* $\mathrm{Sub}(H) \cong \mathrm{Sub}(G \times G)$*, then $H \cong G \times G$.*

However, we cannot always expect that $\mathrm{Sub}(H) \cong \mathrm{Sub}(G \times G)$ would imply $H \cong G \times G$. Namely, let p be a prime and q another prime, dividing $p - 1$. Then for any $d \geq 2$, $\mathrm{Sub}(C_p^d) \cong \mathrm{Sub}(G)$, where $G = A\langle b \rangle$ is a so-called *P-group* with $A = C_p^{d-1}$ and b of order q acting by a power automorphism on A ($bab^{-1} = a^r$, where $r^q \equiv 1, r \not\equiv 1 \pmod{p}$). Instead, we can ask the following question.

Problem 6.3 Does $\mathrm{Sub}(G \times G) \cong \mathrm{Sub}(H \times H)$ imply that G and H are isomorphic groups? In other words, does the subgroup lattice of the direct square uniquely determine the group?

Suzuki's Theorem 6.1 shows that for simple groups this is indeed the case. On the other end of the spectrum there are the abelian groups.

Theorem 6.4 (Lukács and Pálfy [33], 1986) *For a finite abelian group G, if* $\mathrm{Sub}(G \times G) \cong \mathrm{Sub}(H \times H)$*, then G and H are isomorphic.*

This result follows easily from the following observation.

Theorem 6.5 (Lukács and Pálfy [33], 1986) $\mathrm{Sub}(G \times G)$ *is modular if and only if G is abelian.*

Nevertheless, Problem 6.3 has a negative answer. Counterexamples are provided by the *Rottlaender groups* introduced by Ada Rottlaender [47] in 1928. Let $p, q \geq 5$ be primes with $q \mid p - 1$. Then there exists $r \not\equiv 1 \pmod{p}$ such that $r^q \equiv 1 \pmod{p}$. For each $\lambda \in \{2, \ldots, q-2\}$ we define the group

$$R_\lambda = \langle x, y, a \mid x^p = y^p = a^q = [x, y] = 1, axa^{-1} = x^r, aya^{-1} = y^{r^\lambda} \rangle.$$

Roland Schmidt observed the following.

Example 6.6 (Schmidt [51], 1981) $\mathrm{Sub}(R_\lambda \times R_\lambda) \cong \mathrm{Sub}(R_\mu \times R_\mu)$, but $R_\lambda \cong R_\mu$ only if $\lambda = \mu$ or $\lambda\mu \equiv 1 \pmod{q}$

However, it can be checked that for nonisomorphic Rottlaender groups R_λ, R_μ the third powers have nonisomorphic subgroup lattices:

$$\mathrm{Sub}(R_\lambda \times R_\lambda \times R_\lambda) \ncong \mathrm{Sub}(R_\mu \times R_\mu \times R_\mu).$$

This indicated that perhaps the answer to the following question might be positive.

Problem 6.7 Does $\mathrm{Sub}(G \times G \times G)$ uniquely determine G? (That is, assuming $\mathrm{Sub}(G \times G \times G) \cong \mathrm{Sub}(H \times H \times H)$, does it follow that G and H are isomorphic?)

Another result where third powers play a crucial role is the following one.

Theorem 6.8 (Baer [4], 1939) *Let G be an abelian p-group, H an abelian group. Assume that for each prime power p^k, if G contains an element of order p^k, then it contains at least three independent elements of this order (i.e., a subgroup isomorphic to $C_{p^k} \times C_{p^k} \times C_{p^k}$). Then every projectivity (lattice isomorphism) between* $\mathrm{Sub}(G)$ *and* $\mathrm{Sub}(H)$ *is induced by an isomorphism between the groups G and H.*

It should be noted, however, that one cannot hope to prove that every isomorphism between $\mathrm{Sub}(G \times \cdots \times G)$ and $\mathrm{Sub}(H \times \cdots \times H)$ is induced by a group isomorphism, as the following example shows.

Example 6.9 (Schmidt [52], 1982) Let p be a prime, q and r prime divisors of $p-1$, and let G be the direct product of the nonabelian groups of order pq and pr. Then for every $d \geq 1$, $\mathrm{Sub}(G^d)$ has lattice automorphisms (autoprojectivities) that are not induced by group automorphisms.

Note that the order of elements can be recovered from $\mathrm{Sub}(G \times G)$, and then from the subgroup lattices of higher powers as well.

Lemma 6.10 *If* $\mathrm{Sub}(X) \cong \mathcal{M}_n$, *then either*

(1) $X \cong C_{p^2}$ *and* $n = 1$; *or*

(2) $X \cong C_{pq}$ *and* $n = 2$; *or*

(3) $X \cong C_p \times C_p$ *and* $n = p + 1$; *or*

(4) X *is a nonabelian group of order* pq, $q \mid p-1$ *and* $n = p+1$.

Corollary 6.11 *If $P < G \times G$ has order p, then there exists $P < X_0 \leq G \times G$ such that* $\mathrm{Int}[1; X_0] \cong \mathcal{M}_{p+1}$ *(in fact, $X_0 \cong C_p \times C_p$), and if $P < X \leq G \times G$ is such that* $\mathrm{Int}[1; X] \cong \mathcal{M}_n$ *then either $n \leq 2$ or $n \geq p+1$. Hence*

$$p = \min\{n-1 \mid n > 2,\ \exists X > P : \mathrm{Int}[1; X] \cong \mathcal{M}_n\}.$$

So we can find the order of each minimal subgroup in $\mathrm{Sub}(G \times G)$. Furthermore, if $\mathrm{Int}[1; H]$ is a chain of length k, then $|H| = p^k$, where p is the order of the unique minimal subgroup contained in H. Thus p-subgroups can be identified, and the order of every subgroup can be determined.

Schmidt [54, 7.6.11 Problem] considers a closely related question. Let $\varphi : \mathrm{Sub}(G_1 \times \cdots \times G_n) \to \mathrm{Sub}(H)$ be a lattice isomorphism (projectivity), where all direct factors $G_1, \ldots, G_n$ are isomorphic to a given group G. Assume that $H = \varphi(G_1) \times \cdots \times \varphi(G_n)$. Does it follow that $\varphi(G_1) \cong G_1$? Concerning this problem there are some positive results, for example in the following cases:

- if G has a self-centralizing normal Hall subgroup (Schmidt [52], 1982);
- if G is a finite p-group and one of the the following holds:
  - (a) G has nilpotence class 2, $p \neq 2$, $n \geq 3$;
  - (b) G has class ≤ 4 and exponent p, $n \geq 2$;
  - (c) G is metabelian of exponent p, $n \geq p - 2$ (Schenke [48], 1987).

Only after the meeting in Oxford I heard about an apparently forgotten paper by Anne Penfold Street [58][2] that implicitly contains the negative solution of Problem 6.7.

Example 6.12 (Street [58], 1968) There exist nonisomorphic groups $(G, \circ)$ and $(G, *)$ on the same base set such that for each $n \geq 1$ their direct powers $(G, \circ)^n$ and $(G, *)^n$ have exactly the same subgroups.

Proof Let us choose prime numbers p and q subject to the following restrictions: $q \equiv 1 \pmod 3$, $p \equiv 1 \pmod{3q}$. Furthermore, let m have order 3 modulo p and let n have order 3 modulo q (i.e., $m^3 \equiv 1 \pmod p$ and $m \not\equiv 1 \pmod p$). Consider the group

$$G(m, n) = \langle s, t, u \mid s^p = t^q = u^3 = [s, t] = 1, usu^{-1} = s^m, utu^{-1} = t^n \rangle$$

and denote the operation also by $\circ$. If we define $x * y = xy[x, y]^{p-1}$ then it turns out that $*$ is also a group operation and the group defined this way is $G(m^2, n)$ which is not isomorphic to $G(m, n)$. Now $\circ$ can be expressed in the same way from $*$ (in the language of universal algebra $(G, \circ)$ and $(G, *)$ are *term equivalent*), therefore exactly the same subsets of the cartesian powers of the base set are closed for the operation $\circ$ that are closed for $*$, that is the powers of both groups have the same subgroup lattice. For the calculations the reader is referred to [58, Example V.(i)]. □

Thus even the subgroup lattices of all powers of G are not sufficient to determine the isomorphism type of G. However, it still may be true that if the subgroup lattices of some power distinguish two groups than already the third powers do.

Problem 6.13 If $\mathrm{Sub}(G \times G \times G) \cong \mathrm{Sub}(H \times H \times H)$, does it follow that G and H are term equivalent groups?

Acknowledgements. I would like to thank the organizers for inviting me to give a series of talks at the Groups – St Andrews 2001 in Oxford conference. The financial support from the organizers as well as from the Hungarian National Research Fund (OTKA) under grant no. T29132 is gratefully acknowledged.

[2] Thanks to Keith Kearnes for discovering this paper.

References

[1] R. Baddeley. *A new approach to the finite lattice representation problem.* Period. Math. Hungar. **36** (1998), 17–59.

[2] R. Baddeley and A. Lucchini. *On representing finite lattices as intervals in subgroup lattices of finite groups.* J. Algebra **196** (1997), 1–100.

[3] R. Baer. *Groups with abelian central quotient group.* Trans. Amer. Math. Soc. **44** (1938), 357–386.

[4] R. Baer. *The significance of the system of subgroups for the structure of the group.* Amer. J. Math. **61** (1939), 1–44.

[5] A. Basile. *Second maximal subgroups of the finite alternating and symmetric groups.* D.Phil. Thesis, Australian National University, Canberra, April 2001.

[6] H. Bechtell. *Elementary groups.* Trans. Amer. Math. Soc. **114** (1965), 355–362.

[7] G. Birkhoff. *Lattice Theory.* 3rd ed. American Mathematical Society Colloquium Publications, Vol. XXV, Amer. Math. Soc., Providence, RI, 1967.

[8] F. Börner. *A remark on the finite lattice representation problem.* Contributions to general algebra, 11 (Olomouc/Velké Karlovice, 1998), Verlag Johannes Heyn, Klagenfurt, 1999, 5–38.

[9] R. G. Burns and S. Oates-Williams. *Varieties of groups and normal-subgroup lattices — a survey.* Algebra Universalis **32** (1994), 145–152.

[10] R. Dedekind. *Über die Anzahl der Ideal-classen in den verschiedenen Ordnungen eines endlichen Körpers.* Festschrift zur Saecularfeier des Geburtstages von C. F. Gauss, Vieweg, Braunschweig, 1877, 1–55; see Ges. Werke, Band I, Vieweg, Braunschweig, 1930, 105–157.

[11] W. Feit. *An interval in the subgroup lattice of a finite group which is isomorphic to* M_7. Algebra Universalis **17** (1983), 220–221.

[12] R. Freese. *Finitely based modular congruence varieties are distributive.* Algebra Universalis **32** (1994), 104–114.

[13] R. Freese. *Subgroup lattices of groups by R. Schmidt.* Book review, Bull. Amer. Math. Soc. **33** (1996), 487–492.

[14] G. Grätzer. *General Lattice Theory.* Pure and Applied Mathematics, 75, Academic Press, New York–London; Lehrbücher und Monographien aus dem Gebiete der exakten Wissenschaften, Mathematische Reihe, Band 52, Birkhäuser-Verlag, Basel–Stuttgart, 1978.

[15] G. Grätzer and E. T. Schmidt. *Characterizations of congruence lattices of abstract algebras.* Acta Sci. Math. (Szeged) **24** (1963), 34–59.

[16] J. R. J. Groves. *Regular p-groups and words giving rise to commutative group operations.* Israel J. Math. **24** (1976), 73–77.

[17] M. D. Haiman. *Arguesian lattices which are not linear.* Bull. Amer. Math. Soc. (N.S.) **16** (1987), 121–123.

[18] C. Herrmann und A. Huhn. *Zum Begriff der Charakteristik modularer Verbände.* Math. Z. **144** (1975), 185–194.

[19] G. Higman. *Universal algebra by P. M. Cohn.* Book review, J. London Math. Soc. **41** (1966), 760.

[20] D. Hilbert und S. Cohn-Vossen. *Anschauliche Geometrie.* Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Band 37, Julius Springer, Berlin, 1932.

[21] D. Hobby and R. McKenzie. *The Structure of Finite Algebras.* Contemporary Mathematics, 76, Amer. Math. Soc., Providence, RI, 1988.

[22] K. Iwasawa. *Über die endlichen Gruppen und die Verbände ihrer Untergruppen.* J. Fac. Sci. Imp. Univ. Tokyo Sect. I **4** (1941), 171–199.

[23] K. Iwasawa. *On the structure of infinite M-groups.* Jap. J. Math. **18** (1943), 709–728.

[24] B. Jónsson. *Modular lattices and Desargues' theorem.* Math. Scand. **2** (1954), 295–314.
[25] E. W. Kiss and P. P. Pálfy. *A lattice of normal subgroups that is not embeddable into the subgroup lattice of an abelian group.* Math. Scand. **83** (1998), 169–176.
[26] R. Kochendörffer. *Über treue irreduzible Darstellungen endlicher Gruppen.* Math. Nachr. **1** (1948), 25–39.
[27] P. Köhler. *M_7 as an interval in a subgroup lattice.* Algebra Universalis **17** (1983), 263–266.
[28] J. Kuntzmann. *Contribution à l'étude des chaînes principales d'un groupe fini.* Bull. Sci. Math. (2) **71** (1947), 155–164.
[29] H. Kurzweil. *Endliche Gruppen mit vielen Untergruppen.* J. Reine Angew. Math. **356** (1985), 140–160.
[30] M. Lazard. *Sur les groupes nilpotents et les anneaux de Lie.* Ann. Sci. École Norm. Sup. (3) **71** (1954), 101–190.
[31] A. Lucchini. *Representation of certain lattices as intervals in subgroup lattices.* J. Algebra **164** (1994), 85–90.
[32] A. Lucchini. *Intervals in subgroup lattices of finite groups.* Comm. Algebra **22** (1994), 529–549.
[33] E. Lukács and P. P. Pálfy. *Modularity of the subgroup lattice of a direct square.* Arch. Math. (Basel) **46** (1986), 18–19.
[34] R. McKenzie. *Some interactions between group theory and the general theory of algebras.* Groups–Canberra 1989, Lecture Notes Math., vol. 1456, Springer, Berlin, 1990, 32–48.
[35] A. Yu. Olshanskii. *Infinite groups with cyclic subgroups.* Dokl. Akad. Nauk SSSR **245** (1979), 785–787 (in Russian); Translation in Soviet Math. Dokl. **20** (1979), 343–346.
[36] A. Yu. Olshanskii. *Geometry of Defining Relations in Groups.* Mathematics and its Applications (Soviet Series), 70, Kluwer Academic Publishers Group, Dordrecht, 1991.
[37] Ø. Ore. *Structures and group theory, I–II.* Duke Math. J. **3** (1937), 149–174; **4** (1938), 247–269.
[38] P. P. Pálfy. *On partial ordering of chief factors in solvable groups.* Manuscripta Math. **55** (1986), 219–232.
[39] P. P. Pálfy. *Distributive congruence lattices of finite algebras.* Acta Sci. Math. (Szeged) **51** (1987), 153–162.
[40] P. P. Pálfy. *On Feit's examples of intervals in subgroup lattices.* J. Algebra **116** (1988), 471–479.
[41] P. P. Pálfy. *Intervals in subgroup lattices of finite groups.* Groups'93 Galway/St Andrews, vol. 2, London Math. Soc. Lecture Note Ser., vol. 212, Cambridge University Press, Cambridge, 1995, 482–494.
[42] P. P. Pálfy and P. Pudlák. *Congruence lattices of finite algebras and intervals in subgroup lattices of finite groups.* Algebra Universalis **11** (1980), 22–27.
[43] P. P. Pálfy and Cs. Szabó. *An identity for subgroup lattices of abelian groups.* Algebra Universalis **33** (1995), 191–195.
[44] P. P. Pálfy and Cs. Szabó. *Congruence varieties of groups and abelian groups.* Lattice Theory and Its Applications (Darmstadt, 1991), Res. Exp. Math., 23, Heldermann Verlag, Lemgo, 1995, 163–183.
[45] G. Pazderski. *On groups for which the lattice of normal subgroups is distributive.* Beiträge Algebra Geom. **24** (1987), 185–200.
[46] P. Pudlák and J. Tůma. *Every finite lattice can be embedded in a finite partition lattice.* Algebra Universalis **10** (1980), 74–95.
[47] A. Rottlaender. *Nachweis der Existenz nicht-isomorpher Gruppen von gleicher Situ-*

ation der Untergruppen. Math. Z. **28** (1928), 641–653.

[48] M. Schenke. *Analoga des Fundamentalsatzes der projektiven Geometrie in der Gruppentheorie, I–II.* Rend. Sem. Mat. Univ. Padova **77** (1987), 255–303; **78** (1987), 175–225.

[49] E. T. Schmidt. *Kongruenzrelationen algebraischer Strukturen.* Mathematische Forschungsberichte, vol. XXV, VEB Deutscher Verlag der Wissenschaften, Berlin, 1969.

[50] R. Schmidt. *Eine verbandstheoretische Charakterisierung der auflösbaren und der überauflösbaren endlichen Gruppen.* Arch. Math. (Basel) **19** (1968), 449–452.

[51] R. Schmidt. *Der Untergruppenverband des direkten Produktes zweier isomorpher Gruppen.* J. Algebra **73** (1981), 264–272.

[52] R. Schmidt. *Untergruppenverbände endlicher Gruppen mit elementarabelschen Hallschen Normalteilern.* J. Reine Angew. Math. **334** (1982), 116–140.

[53] R. Schmidt. *Gruppen mit modularem Untergruppenverband.* Arch. Math. (Basel) **46** (1986), 118–124.

[54] R. Schmidt. *Subgroup Lattices of Groups.* de Gruyter Expositions in Mathematics, 14, Walter de Gruyter and Co., Berlin, 1994.

[55] M. Schönert et al. *Groups, Algorithms and Programming.* Lehrstuhl D für Mathematik, RWTH Aachen, 1992.

[56] M. Schützenberger. *Sur certains axiomes de la théorie des structures.* C. R. Acad. Sci. Paris **221** (1945), 218–220.

[57] H. L. Silcock. *Generalized wreath products and the lattice of normal subgroups of a group.* Algebra Universalis **7** (1977), 361–372.

[58] A. P. Street. *Subgroup-determining functions on groups.* Illinois J. Math. **12** (1968), 99–120.

[59] M. Suzuki. *On the lattice of subgroups of finite groups.* Trans. Amer. Math. Soc. **70** (1951), 345–371.

[60] M. Suzuki. *Structure of a Group and the Structure of its Lattice of Subgroups.* Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft 10, Springer-Verlag, Berlin–Göttingen–Heidelberg, 1956.

[61] Cs. Szabó. *Congruence varieties of abelian groups and groups* (in Hungarian). Thesis, Hungarian Academy of Sciences, Budapest, 1992.

[62] J. Tůma. *Intervals in subgroup lattices of infinite groups.* J. Algebra **125** (1989), 367–399.

[63] P. M. Whitman. *Lattices, equivalence relations, and subgroups.* Bull. Amer. Math. Soc. **52** (1946), 507–522.

[64] B. V. Yakovlev. *Conditions under which a lattice is isomorphic to the lattice of subgroups of a group.* Algebra i Logika **13** (1974), 694–712 (in Russian); Translation in Algebra and Logic **13** (1975), 400–412.

[65] G. Zacher. *Determinazione dei gruppi d'ordine finito relativemente complementati.* Rend. Accad. Sci. Fis. Mat. Napoli (4) **19** (1952), 200–206.

[66] G. Zacher. *Sulle immagini dei sottogruppi normali nelle proiettività.* Rend. Sem. Mat. Univ. Padova **67** (1982), 39–74.

[67] G. Zappa. *Sulla risolubilità dei gruppi finiti in isomorfismo reticolare con un gruppo risolubile.* Giorn. Mat. Battaglini (4) **4(80)** (1951), 213–225.