PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 133, Number 4, Pages 979–985
S 0002-9939(04)07638-5
Article electronically published on September 16, 2004

DETECTING THE INDEX OF A SUBGROUP IN THE SUBGROUP LATTICE

M. DE FALCO, F. DE GIOVANNI, C. MUSELLA, AND R. SCHMIDT

(Communicated by Jonathan I. Hall)

Abstract. A theorem by Zacher and Rips states that the finiteness of the index of a subgroup can be described in terms of purely lattice-theoretic concepts. On the other hand, it is clear that if G is a group and H is a subgroup of finite index of G, the index $|G:H|$ cannot be recognized in the lattice $\mathfrak{L}(G)$ of all subgroups of G, as for instance all groups of prime order have isomorphic subgroup lattices. The aim of this paper is to give a lattice-theoretic characterization of the number of prime factors (with multiplicity) of $|G:H|$.

1. Introduction

For every group G, we shall denote by $\mathfrak{L}(G)$ the lattice of all subgroups of G. If G and $\bar{G}$ are groups, an isomorphism from the lattice $\mathfrak{L}(G)$ onto the lattice $\mathfrak{L}(\bar{G})$ is also called a *projectivity* from G onto $\bar{G}$; one of the main problems in the theory of subgroup lattices is to find group properties that are invariant under projectivities. In 1980, Zacher [5] and Rips proved independently that any projectivity from a group G onto a group $\bar{G}$ maps each subgroup of finite index of G to a subgroup of finite index of $\bar{G}$. In addition, Zacher gave a lattice-theoretic characterization of the finiteness of the index of a subgroup in a group; other characterizations were given by Schmidt [3]. On the other hand, it is clear that if G is a group and H is a subgroup of finite index of G, the index $|G:H|$ cannot be recognized in the subgroup lattice $\mathfrak{L}(G)$, as for instance all groups of prime order have the same lattice of subgroups.

The aim of this paper is to find an arithmetic invariant related to the index of a subgroup and preserved under projectivities. In fact, if H is a subgroup of finite index of any group G, we will give a lattice-theoretic characterization of the number of prime factors (with multiplicity) of $|G:H|$, so that this number can be detected in the lattice $\mathfrak{L}(G)$.

Most of our notation is standard and can be found in [2]; for definitions and properties concerning lattices and subgroup lattices we refer to the monograph [4]. In particular, if $\mathfrak{L}$ is any complete lattice, the smallest and the largest element of $\mathfrak{L}$ will be denoted by 0 and I, respectively; moreover, for each pair (a,b) of elements of $\mathfrak{L}$ such that $a \leq b$, we put $[b/a] = \{x \in \mathfrak{L} \mid a \leq x \leq b\}$. If a is any non-zero

Received by the editors October 8, 2003 and, in revised form, December 1, 2003.
2000 *Mathematics Subject Classification.* Primary 20E15.

element of the finite lattice $\mathfrak{L}$, we put

$$\phi(a) = \inf\{x \in \mathfrak{L} \mid x <\!\cdot\, a\}$$

(where the symbol $x <\!\cdot\, a$ means that x is a maximal (proper) element of the lattice $[a/0]$). Finally, for each positive integer n we will denote by M_n the lattice of length 2 with n atoms.

2. The weight of a finite lattice

A finite lattice $\mathfrak{L}$ is called *perfect* if it has no maximal elements that are modular.

Lemma 2.1. *Let $\mathfrak{L}$ be a finite lattice, and let x and y be elements of $\mathfrak{L}$ such that the intervals $[x/0]$ and $[y/0]$ are perfect lattices. Then also the lattice $[x \vee y/0]$ is perfect.*

Proof. Assume for a contradiction that $[x \vee y/0]$ contains a maximal element z that is modular. Since $x \wedge z$ is modular in the perfect lattice $[x/0]$ and the lattices $[x \vee z/z]$ and $[x/x \wedge z]$ are isomorphic, it follows that $x \wedge z = x$ and hence $x \leq z$. We obtain similarly that $y \leq z$ and so $z = x \vee y$, a contradiction. Therefore the lattice $[x \vee y/0]$ is perfect. □

Let $\mathfrak{L}$ be a finite lattice. It follows from Lemma 2.1 that $\mathfrak{L}$ contains a largest element r such that the interval $[r/0]$ is a perfect lattice; such an element r will be called the *perfect radical* of $\mathfrak{L}$ and denoted by $r(\mathfrak{L})$. Clearly, the lattice $\mathfrak{L}$ is perfect if and only if $r(\mathfrak{L}) = I$.

Recall that an element c of a finite lattice $\mathfrak{L}$ is called *cyclic* if the interval $[c/0]$ is a distributive lattice. Moreover, an element a of $\mathfrak{L}$ is said to be *modularly embedded* in $\mathfrak{L}$ if the interval $[a \vee c/0]$ is a modular lattice for each cyclic element c of $\mathfrak{L}$; a *modular chain* in $\mathfrak{L}$ is a chain of elements of $\mathfrak{L}$ of the form

$$0 = a_0 < a_1 < \ldots < a_t = I$$

such that a_{i+1} is modularly embedded in $[I/a_i]$ for each non-negative integer $i < t$.

For our purposes, we will consider the subset $P(\mathfrak{L})$ of $\mathfrak{L}$ consisting of all elements a satisfying the following conditions:

- the lattice $[a/0]$ has a modular chain;
- every interval of $[a/0]$ is directly indecomposable;
- if $x <\!\cdot\, y \leq a$ and $[x/0]$ is a chain of length 2, then either $[y/0]$ is a modular lattice or it is isomorphic to the subgroup lattice $\mathfrak{L}(D_8)$ of the dihedral group of order 8.

In particular, $P(\mathfrak{L})$ contains any element a of $\mathfrak{L}$ such that $[a/0]$ is a modular lattice whose intervals are directly indecomposable. Note also that, in the special case of the subgroup lattice of a finite group G, it turns out that the elements of $P(\mathfrak{L}(G))$ are precisely the primary subgroups and the P-subgroups of G (see [4], Theorem 7.4.10). Here a group is called a *P-group* if it is the semidirect product of an abelian normal subgroup A of prime exponent by a group $\langle x \rangle$ of prime order such that x induces on A a power automorphism; in particular, all abelian groups of prime exponent are P-groups.

For a finite lattice $\mathfrak{L}$, we let $A_{\mathfrak{L}}$ be the set of all atoms of $\mathfrak{L}$. For every prime number p, we define two subsets of $A_{\mathfrak{L}}$, namely

$$R_{\mathfrak{L}}(p) = \{a \in A_{\mathfrak{L}} \mid \exists b \in P(\mathfrak{L}) \text{ such that } a \leq b \text{ and } [b/\phi(b)] \simeq M_{p+1}\}$$

and

$$S_{\mathfrak{L}}(p) = \{a \in A_{\mathfrak{L}} \mid \exists b \in \mathfrak{L} \text{ such that } [b/0] \text{ is a chain, } \phi(b) \neq 0, [a \vee \phi(b)/0] \text{ is distributive and } [a \vee b/\phi(b)] \simeq M_{p+1}\};$$

furthermore, we let $T_{\mathfrak{L}}(p) = R_{\mathfrak{L}}(p) \cup S_{\mathfrak{L}}(p)$ and

$$T_{\mathfrak{L}} = \bigcup_{p \in \mathbb{P}} T_{\mathfrak{L}}(p),$$

where $\mathbb{P}$ is the set of all prime numbers. Then, clearly, $T_{\mathfrak{L}} \subseteq A_{\mathfrak{L}}$ and in general $T_{\mathfrak{L}} \neq A_{\mathfrak{L}}$, for instance if $\mathfrak{L}$ is a non-trivial chain. Finally, for every atom a of $\mathfrak{L}$, we define

$$\omega_{\mathfrak{L}}(a) = \text{Min}\{p \in \mathbb{P} \mid a \in T_{\mathfrak{L}}(p)\}$$

if $a \in T_{\mathfrak{L}}$ and $\omega_{\mathfrak{L}}(a) = 0$ if $a \in A_{\mathfrak{L}} \setminus T_{\mathfrak{L}}$. Then

$$\omega_{\mathfrak{L}} : A_{\mathfrak{L}} \longrightarrow \mathbb{P} \cup \{0\}$$

is a well-defined map described entirely in the (finite) lattice $\mathfrak{L}$.

An element $x \in \mathfrak{L}$ is called a *p-element* of $\mathfrak{L}$ if $\omega_{\mathfrak{L}}(a) = p$ for every atom a of $[x/0]$. As usual, the length $l(\mathfrak{L})$ of $\mathfrak{L}$ is the largest length of a chain in $\mathfrak{L}$, and we denote the largest length of a chain consisting of p-elements in $\mathfrak{L}$ by $\ell_p(\mathfrak{L})$. The *weight* $||\mathfrak{L}||$ of $\mathfrak{L}$ is now defined by

$$||\mathfrak{L}|| = \ell([I/r(\mathfrak{L})]) + \sum_{p \in \mathbb{P}} \ell_p([r(\mathfrak{L})/0]),$$

where $r(\mathfrak{L})$ is the perfect radical of $\mathfrak{L}$ defined above.

3. The order of a finite group

It is well known that a finite group is perfect if and only if its subgroup lattice is perfect (see [4], Theorem 5.3.3). It follows that for any finite group G, the perfect radical of the lattice $\mathfrak{L}(G)$ is the largest perfect subgroup of G (and so it coincides with the soluble residual of G).

Lemma 3.1. *Let H be a minimal subgroup of a finite group G, and let p be a prime number. If $H \in S_{\mathfrak{L}(G)}(p)$, then $|H| = p$.*

Proof. Since $H \in S_{\mathfrak{L}(G)}(p)$, there exists a cyclic subgroup K of prime power order such that $\phi(K) \neq \{1\}$, $\langle H, \phi(K)\rangle$ is cyclic and

$$[\langle H, K\rangle/\phi(K)] \simeq M_{p+1}.$$

Thus H is not contained in K, so that $\langle H, \phi(K)\rangle = H \times \phi(K)$, and in particular H and K have coprime orders. So $\langle H, K\rangle/\phi(K)$ cannot be a p-group, and hence it is non-abelian of order pq where $p > q \in \mathbb{P}$. Thus $[H, K] \neq \{1\}$ and $[H, \phi(K)] = \{1\}$. Therefore K cannot be normal in $\langle H, K\rangle$, and it follows that $|K/\phi(K)| = q$ and $|H| = p$. □

Lemma 3.2. *Let G be a finite group having no normal Sylow complement. Then $\omega_{\mathfrak{L}(G)}(H) = |H|$ for every minimal subgroup H of G.*

Proof. Let $|H| = p$. We claim that it suffices to show that H belongs to $T_{\mathfrak{L}(G)}(p)$.

Indeed, this clearly implies that $0 < \omega_{\mathfrak{L}(G)}(H) \leq p$. If H were contained in $T_{\mathfrak{L}(G)}(q)$ for some prime $q < p$, then by Lemma 3.1, $H \in R_{\mathfrak{L}(G)}(q)$ and so there would exist $Q \in P(\mathfrak{L}(G))$ such that $H \leq Q$ and $[Q/\phi(Q)] \simeq M_{q+1}$. In this case, Q would be a q-group or a P-group of order qr with $q \geq r \in \mathbb{P}$ (see [4], Theorem 7.4.10). This would contradict the fact that $H \leq Q$ and $|H| = p > q$. Thus $\omega_{\mathfrak{L}(G)}(H) = p = |H|$.

To prove that $H \in T_{\mathfrak{L}(G)}(p)$, consider a Sylow p-subgroup S of G containing H. If S is not cyclic, then we may consider a smallest non-cyclic subgroup P of S containing H. Every maximal subgroup of P containing H is cyclic and hence $[P/\phi(P)] \simeq M_{p+1}$; thus $H \in R_{\mathfrak{L}(G)}(p)$. So suppose that S is cyclic. Since G is not p-nilpotent, we have $S \leq C_G(S) < N_G(S)$ (see [2], 10.1.8), and for some prime $q \neq p$ there exists an element $g \in N_G(S)$ with order q^n inducing an automorphism of order q in S. Then $\phi(\langle g\rangle) = \langle g^q\rangle$ centralizes S, and in particular the subgroup $\langle H, \phi(\langle g\rangle)\rangle$ is cyclic; furthermore, $\langle H, g\rangle/\phi(\langle g\rangle)$ is non-abelian of order pq and hence $[\langle H, g\rangle/\phi(\langle g\rangle)] \simeq M_{p+1}$. So if $\phi(\langle g\rangle) \neq \{1\}$, then $H \in S_{\mathfrak{L}(G)}(p)$; and if $\phi(\langle g\rangle) = \{1\}$, then $\langle H, g\rangle \in P(\mathfrak{L}(G))$ and $H \in R_{\mathfrak{L}(G)}(p)$. In all cases, $H \in T_{\mathfrak{L}(G)}(p)$ as we wanted to show. □

We can now prove the following result, which provides a purely lattice-theoretic description of the order of a finite group having no normal Sylow complement, in particular of any finite perfect group.

Theorem 3.3. *Let G be a finite group having no normal Sylow complement. Then* $|G| = \prod_{p\in\mathbb{P}} p^{\ell_p(\mathfrak{L}(G))}$.

Proof. It follows from Lemma 3.2 that for each prime number p, the p-elements of the lattice $\mathfrak{L}(G)$ are precisely the p-subgroups of G. In particular, if P is any Sylow p-subgroup of G, we have that $|P| = p^{\ell_p(\mathfrak{L}(G))}$. The theorem follows. □

For an arbitrary finite group G, the order of G cannot be recognized in $\mathfrak{L}(G)$. But we can describe the number of prime factors of $|G|$ in $\mathfrak{L}(G)$.

Theorem 3.4. *Let G be a finite group. Then the weight $||\mathfrak{L}(G)||$ of the subgroup lattice of G is the number of prime factors of the order of G (with multiplicity).*

Proof. Let R be the soluble residual of G. Then $R = r(\mathfrak{L}(G))$ and Theorem 3.3 yields that

$$\sum_{p\in\mathbb{P}} \ell_p([r(\mathfrak{L}(G))/0]) = \sum_{p\in\mathbb{P}} \ell_p(\mathfrak{L}(R))$$

is the number of prime factors of $|R|$. Since G/R is soluble, the number of prime factors of $|G/R|$ is just the length of the lattice $\mathfrak{L}(G/R)$. The number of prime factors of $|G|$ is the sum of these two numbers, and hence it is $||\mathfrak{L}(G))||$. □

The above theorem has the following obvious consequence.

Corollary 3.5. *Let H be a subgroup of the finite group G. Then the number of prime factors of the index $|G : H|$ (with multiplicity) is $||\mathfrak{L}(G)|| - ||\mathfrak{L}(H)||$.*

4. Subgroups of finite index

It is well known that if a and b are modular elements of a lattice $\mathfrak{L}$, then also $a \vee b$ is a modular element of $\mathfrak{L}$; in the case of the lattice of all subgroups of a group G, it has been proved that the join of any collection of modular subgroups of G is likewise a modular subgroup (see [1], Proposizione 1.2). As G. Zacher pointed out to one of the authors, this property also holds for arbitrary algebraic lattices (recall that a complete lattice $\mathfrak{L}$ is called *algebraic* if each element of $\mathfrak{L}$ is a join of compact elements).

Lemma 4.1. *Let $\mathfrak{L}$ be an algebraic lattice, and let X be a non-empty set of modular elements of $\mathfrak{L}$. Then also $\sup X$ is a modular element of $\mathfrak{L}$.*

Proof. Put $a = \sup X$, and let b be any element of $\mathfrak{L}$. Consider an element y of the interval $[a \vee b/a]$, and let $(y_i)_{i \in I}$ be a collection of compact elements of $\mathfrak{L}$ such that $y = \sup\limits_{i \in I} y_i$. For each $i \in I$ there exists a finite subset X_i of X such that $y_i \leq x_i \vee b$, where $x_i = \sup X_i$; clearly, x_i is a modular element of $\mathfrak{L}$, and hence

$$y_i \leq y \wedge (x_i \vee b) = x_i \vee (b \wedge y) \leq a \vee (b \wedge y).$$

Thus $y \leq a \vee (b \wedge y)$, and so $a \vee (b \wedge y) = y$.

Suppose now that z is an element of the interval $[b/a \wedge b]$, and put $c = (a \vee z) \wedge b$. Let $(c_j)_{j \in J}$ be a collection of compact elements of $\mathfrak{L}$ for which $c = \sup\limits_{j \in J} c_j$, and for each $j \in J$ let X'_j be a finite subset of X such that $c_j \leq x'_j \vee z$, where $x'_j = \sup X'_j$. Since x'_j is a modular element of $\mathfrak{L}$, we have

$$c_j \leq (x'_j \vee z) \wedge b = z \vee (x'_j \wedge b) = z,$$

so that $c \leq z$ and hence $z = c = (a \vee z) \wedge b$. It follows that a is a modular element of $\mathfrak{L}$ (see [4], Theorem 2.1.5). □

Let $\mathfrak{L}$ be an algebraic lattice, and let a be any element of $\mathfrak{L}$. The largest modular element m of $\mathfrak{L}$ such that $m \leq a$ is called the *modular core* of a in $\mathfrak{L}$, and is denoted by $core_{\mathfrak{L}}a$. Clearly, the element a is modular if and only if $a = core_{\mathfrak{L}}a$; note also that if $core_{\mathfrak{L}}a < a$, then a cannot be modular in the lattice $[I/core_{\mathfrak{L}}a]$. If a and b are elements of $\mathfrak{L}$ such that $a < b$, the modular core of a in $[b/0]$ will also be denoted by $core_b a$.

Let $\mathfrak{L}$ be an infinite algebraic lattice. A maximal element a of $\mathfrak{L}$ is called *f-maximal* if the interval $[a/0]$ is infinite and a satisfies one of the following conditions:

(1) a is not modular in $\mathfrak{L}$ and $[I/core_{\mathfrak{L}}a]$ is a finite lattice;
(2) there exists an automorphism φ of $\mathfrak{L}$ such that $a \wedge a^{\varphi}$ is a modular element of $\mathfrak{L}$ and $[I/a \wedge a^{\varphi}]$ is a finite lattice with length 2 and at least 3 atoms;
(3) for each automorphism φ of $\mathfrak{L}$, the element $a \wedge a^{\varphi}$ is modular in $\mathfrak{L}$ and $[I/a \wedge a^{\varphi}] = \{a \wedge a^{\varphi}, a, a^{\varphi}, I\}$.

It follows from the definition that if a is any f-maximal element of $\mathfrak{L}$, the lattice $[I/core_{\mathfrak{L}}a]$ is finite; note also that both conditions (2) and (3) above force the element a to be modular in $\mathfrak{L}$.

Let $\mathfrak{L}$ be an infinite algebraic lattice, and let a and b be elements of $\mathfrak{L}$ such that $a < b$ and a is f-maximal in $[b/0]$; since the lattices $[a/core_b a]$ and $[b/core_b a]$ are finite, we can define the *lattice index* $||b : a||$ of a in b by the position

$$||b : a|| = ||[b/core_b a]|| - ||[a/core_b a]||.$$

In particular, if a is an f-maximal and modular element of $[b/0]$, we have $||b:a|| = ||[b/a]|| = 1$.

Let G be an infinite group; a subgroup M of G is called *f-maximal* if M is an f-maximal element of the lattice $\mathfrak{L}(G)$. Actually, the f-maximal subgroups of G are precisely the maximal subgroups of finite index; in fact, the following lattice characterization of the finiteness of the index of a subgroup holds.

Lemma 4.2. *Let G be an infinite group, and let H be a proper subgroup of G. Then H has finite index in G if and only if there exists a finite chain $H = H_0 < H_1 < \ldots < H_t = G$ such that H_i is an f-maximal subgroup of H_{i+1} for each $i = 0, 1, \ldots, t-1$.*

Proof. Suppose first that the index $|G : H|$ is finite, and let

$$H = H_0 < H_1 < \ldots < H_t = G$$

be a maximal chain of subgroups between H and G. Then the subgroup H_i is infinite and maximal in H_{i+1} for each $i = 0, 1, \ldots, t-1$; moreover, since $|H_{i+1} : H_i|$ is finite, we have that H_i is an f-maximal subgroup of H_{i+1} (see [3], Satz 3). The converse statement follows from the same result. □

We also need the following known result; it shows that if M is an f-maximal subgroup of an infinite group G, then either $core_{\mathfrak{L}(G)}M = M$ or $core_{\mathfrak{L}(G)}M = core_G M$ (the usual core of M in G in the group-theoretical sense).

Lemma 4.3 (see [3], Lemma 3)**.** *Let G be a group, and let M be a maximal subgroup of finite index of G. If M is not modular in G, then the largest modular subgroup of G contained in M is normal in G.*

Theorem 4.4. *Let G be an infinite group, and let H be a proper subgroup of finite index of G. Then the number of prime factors of $|G : H|$ (with multiplicity) is the sum $\sum_{i=0}^{t-1} ||H_{i+1} : H_i||$, where*

$$H = H_0 < H_1 < \ldots < H_t = G$$

is a finite chain of subgroups such that H_i is an f-maximal subgroup of H_{i+1} for each $i = 0, 1, \ldots, t-1$.

Proof. Assume first that H_i is a modular subgroup of H_{i+1} for some non-negative integer $i < t$, so that $||H_{i+1} : H_i|| = 1$ as we already observed; on the other hand, it is well known that in this case the index $|H_{i+1} : H_i|$ is a prime number (see [4], Lemma 5.1.2). Suppose now that H_i is not modular in H_{i+1}, and let K_i be the normal core of H_i in H_{i+1}. By Lemma 4.3, K_i is the largest modular subgroup of H_{i+1} contained in H_i, and hence we have

$$\begin{aligned} ||H_{i+1} : H_i|| &= ||[H_{i+1}/K_i]|| - ||[H_i/K_i]|| \\ &= ||\mathfrak{L}(H_{i+1}/K_i)|| - ||\mathfrak{L}(H_i/K_i)||. \end{aligned}$$

Since H_{i+1}/K_i is a finite group, it follows from Corollary 3.5 that the lattice index $||H_{i+1} : H_i||$ is the number of prime factors of $|H_{i+1}/K_i : H_i/K_i| = |H_{i+1} : H_i|$. The theorem is proved. □

Corollary 4.5. *Let φ be a projectivity between the groups G and $\bar{G}$, and let H be a subgroup of finite index of G. Then the indices $|G : H|$ and $|\bar{G} : H^\varphi|$ have the same number of prime factors.*

References

[1] E. Previato: "Gruppi in cui la relazione di Dedekind è transitiva", *Rend. Sem. Mat. Univ. Padova* 54 (1975), 215–231. MR0466319 (57:6199)

[2] D.J.S. Robinson: "A Course in the Theory of Groups", *Springer*, Berlin (1992). MR1261639 (94m:20001)

[3] R. Schmidt: "Verbandstheoretische Charakterisierungen der Endlichkeit des Indexes einer Untergruppe in einer Gruppe", *Arch. Math. (Basel)* 42 (1984), 492–495. MR0756887 (86g:20035)

[4] R. Schmidt: "Subgroup Lattices of Groups", *de Gruyter*, Berlin (1994). MR1292462 (95m:20028)

[5] G. Zacher: "Una caratterizzazione reticolare della finitezza dell'indice di un sottogruppo in un gruppo", *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.* (8) 69 (1980), 317–323. MR0690298 (84f:20027)

Dipartimento di Matematica e Applicazioni, Università di Napoli "Federico II", Complesso Universitario Monte S. Angelo, Via Cintia, I - 80126 Napoli, Italy
E-mail address: mdefalco@unina.it

Dipartimento di Matematica e Applicazioni, Università di Napoli "Federico II", Complesso Universitario Monte S. Angelo, Via Cintia, I - 80126 Napoli, Italy
E-mail address: degiovan@unina.it

Dipartimento di Matematica e Applicazioni, Università di Napoli "Federico II", Complesso Universitario Monte S. Angelo, Via Cintia, I - 80126 Napoli, Italy
E-mail address: cmusella@unina.it

Mathematisches Seminar, Universität Kiel, Ludwig-Meyn Strasse 4, D - 24098 Kiel, Germany
E-mail address: schmidt@math.uni-kiel.de