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 \( \mathcal{L}(G) \) 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 \( |G:H| \).
element of the finite lattice \( \mathcal{L} \), we put

\[
\phi(a) = \inf \{ x \in \mathcal{L} \mid x < a \}
\]

(where the symbol \( x < a \) 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 \( \mathcal{L} \) is called **perfect** if it has no maximal elements that are modular.

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

**Proof.** Assume for a contradiction that \([x \lor y/0]\) contains a maximal element \( z \) that is modular. Since \( x \land z \) is modular in the perfect lattice \([x/0]\) and the lattices \([x \lor z/z]\) and \([x/x \land z]\) are isomorphic, it follows that \( x \land z = x \) and hence \( x \leq z \).

We obtain similarly that \( y \leq z \) and so \( z = x \lor y \), a contradiction. Therefore the lattice \([x \lor y/0]\) is perfect. \( \square \)

Let \( \mathcal{L} \) be a finite lattice. It follows from Lemma 2.1 that \( \mathcal{L} \) 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 \( \mathcal{L} \) and denoted by \( r(\mathcal{L}) \). Clearly, the lattice \( \mathcal{L} \) is perfect if and only if \( r(\mathcal{L}) = I \).

Recall that an element \( c \) of a finite lattice \( \mathcal{L} \) is called **cyclic** if the interval \([c/0]\) is a distributive lattice. Moreover, an element \( a \) of \( \mathcal{L} \) is said to be **modularly embedded** in \( \mathcal{L} \) if the interval \([a \lor c/0]\) is a modular lattice for each cyclic element \( c \) of \( \mathcal{L} \); a **modular chain** in \( \mathcal{L} \) is a chain of elements of \( \mathcal{L} \) 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 \( P(\mathcal{L}) \) of \( \mathcal{L} \) 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 \( x \prec y \leq a \) 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 \( \mathcal{L}(D_8) \) of the dihedral group of order 8.

In particular, \( P(\mathcal{L}) \) contains any element \( a \) of \( \mathcal{L} \) 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 \( P(\mathcal{L}(G)) \) 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 \( \mathcal{L} \), we let \( A_\mathcal{L} \) be the set of all atoms of \( \mathcal{L} \). For every prime number \( p \), we define two subsets of \( A_\mathcal{L} \), namely

\[
R_\mathcal{L}(p) = \{ a \in A_\mathcal{L} \mid \exists b \in P(\mathcal{L}) \text{ such that } a \leq b \text{ and } [b/\phi(b)] \simeq M_{p+1} \}.
\]
DETECTING THE INDEX OF A SUBGROUP IN THE SUBGROUP LATTICE

and

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

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

\[ \omega_\mathfrak{L}(a) = \min \{ p \in \mathbb{P} \mid a \in T_\mathfrak{L}(p) \} \]

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 \[3\], 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 \( \phi(K) \neq 1 \), \( (H, \phi(K)) \) is cyclic and

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

Thus \( H \) is not contained in \( K \), so that \( (H, \phi(K)) = H \times \phi(K) \), and in particular \( H \) and \( K \) have coprime orders. So \( (H, K)/\phi(K) \) 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 \( (H, K) \), and it follows that \( |K/\phi(K)| = q \) and \( |H| = p \). \( \Box \)

**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 $T_{\Sigma(G)}(p)$.

Indeed, this clearly implies that $0 < \omega_{\Sigma(G)}(H) \leq p$. If $H$ were contained in $T_{\Sigma(G)}(q)$ for some prime $q < p$, then by Lemma 3.2, $H \in R_{\Sigma(G)}(q)$ and so there would exist $Q \in P(\Sigma(G))$ 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 [1], Theorem 7.4.10). This would contradict the fact that $H \leq Q$ and $|H| = p > q$. Thus $\omega_{\Sigma(G)}(H) = p = |H|$.

To prove that $H \in T_{\Sigma(G)}(p)$, 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 $H \in R_{\Sigma(G)}(p)$. 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 $\phi(g) = (g^q)$ centralizes $S$, and in particular the subgroup $\langle H, \phi(g) \rangle$ is cyclic; furthermore, $\langle H, g \rangle/\phi(g)$ is non-abelian of order $pq$ and hence $[\langle H, g \rangle/\phi(g)] \simeq M_{p+1}$. So if $\phi(g) \neq \{1\}$, then $H \in S_{\Sigma(G)}(p)$; and if $\phi(g) = \{1\}$, then $\langle H, g \rangle \in P(\Sigma(G))$ and $H \in R_{\Sigma(G)}(p)$. In all cases, $H \in T_{\Sigma(G)}(p)$ 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 $|G| = \prod_{p \in \mathbb{P}} p^{a_p(\Sigma(G))}$.

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

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

**Theorem 3.4.** Let $G$ be a finite group. Then the weight $\|\Sigma(G)\|$ 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 $R = r(\Sigma(G))$ and Theorem 3.3 yields that

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

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 $\Sigma(G/R)$. The number of prime factors of $|G|$ is the sum of these two numbers, and hence it is $\|\Sigma(G)\|$.

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 $\|\Sigma(G)\| - \|\Sigma(H)\|$. 

4. Subgroups of finite index

It is well known that if $a$ and $b$ are modular elements of a lattice $\mathcal{L}$, then also $a \lor b$ is a modular element of $\mathcal{L}$; 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 $\mathcal{L}$ is called algebraic if each element of $\mathcal{L}$ is a join of compact elements).

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

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

$$y_i \leq y \land (x_i \lor b) = x_i \lor (b \land y) \leq a \lor (b \land y).$$

Thus $y \leq a \lor (b \land y)$, and so $a \lor (b \land y) = y$.

Suppose now that $z$ is an element of the interval $[b/a \land b]$, and put $c = (a \lor z) \land b$.

Let $(c_j)_{j \in J}$ be a collection of compact elements of $\mathcal{L}$ for which $c = \sup c_j$, and for each $j \in J$ let $X_j'$ be a finite subset of $X$ such that $c_j \leq x_j' \lor z$, where $x_j' = \sup X_j'$.

Since $x_j'$ is a modular element of $\mathcal{L}$, we have

$$c_j \leq (x_j' \lor z) \land b = z \lor (x_j' \land b) = z,$$

so that $c \leq z$ and hence $z = c = (a \lor z) \land b$. It follows that $a$ is a modular element of $\mathcal{L}$ (see [1], Theorem 2.1.5). $\square$

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

Let $\mathcal{L}$ be an infinite algebraic lattice. A maximal element $a$ of $\mathcal{L}$ 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 $\mathcal{L}$ and $[I/\text{core}_\mathcal{L}a]$ is a finite lattice;
2. there exists an automorphism $\varphi$ of $\mathcal{L}$ such that $a \land a^\varphi$ is a modular element of $\mathcal{L}$ and $[I/a \land a^\varphi]$ is a finite lattice with length 2 and at least 3 atoms;
3. for each automorphism $\varphi$ of $\mathcal{L}$, the element $a \land a^\varphi$ is modular in $\mathcal{L}$ and $[I/a \land a^\varphi] = \{a \land a^\varphi, a, a^\varphi, I\}$.

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

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

$$||b : a|| = ||[b/\text{core}_b a]| - ||[a/\text{core}_b a]|.$$
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 \(\text{core}_{\mathfrak{L}(G)} M = M\) or \(\text{core}_{\mathfrak{L}(G)} M = \text{core}_G M\) (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 \(M\) 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
\[||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)|||.
Since \(H_{i+1} / K_i\) is a finite group, it follows from Corollary 4.3 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 \(\varphi\) 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.
DETECTING THE INDEX OF A SUBGROUP IN THE SUBGROUP LATTICE

References


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