COLLOQUIUM MATHEMATICUM

VOL. 131 2013 NO. 2

FINITE GROUPS WITH MODULAR CHAINS

BY

ROLAND SCHMIDT (Kiel)

Abstract. In 1954, Kontorovich and Plotkin introduced the concept of a modular chain in a lattice to obtain a lattice-theoretic characterization of the class of torsion-free nilpotent groups. We determine the structure of finite groups with modular chains. It turns out that this class of groups lies strictly between the class of finite groups with lower semimodular subgroup lattice and the projective closure of the class of finite nilpotent groups.

1. Introduction. Many lattice-theoretic characterizations of classes of groups can be obtained by translating a suitable definition of the class into lattice theory, that is, by replacing concepts appearing in this definition by lattice-theoretic concepts that are equivalent to them or nearly so. The first to use this idea were Kontorovich and Plotkin who in 1954 introduced the concept of a modular chain in a lattice (as translation of a central series of a group) to obtain a lattice-theoretic characterization of the class of torsion-free nilpotent groups (see [3] or [6, Theorem 7.2.3]).

In this paper we want to study finite groups G whose subgroup lattice $L(G)$ has a modular chain. Since every central series of G is a modular chain in $L(G)$, this class of groups contains the class $\mathfrak{N}^*$ of all projective images of finite nilpotent groups. We also consider some slightly stronger lattice-theoretic properties. It is easy to construct finite lattices with these properties which have maximal chains of different lengths and therefore do not satisfy the Jordan–Dedekind chain condition (see Examples 2.7 and 2.12). For subgroup lattices of finite groups, however, we can show that all properties considered are equivalent and that the following holds.

Theorem A. *The subgroup lattice of a finite group is lower semimodular if it has a modular chain.*

The converse is not true although lower semimodularity is a translation of a strong normalizer condition into lattice theory [6, p. 233], another possible definition of nilpotency for finite groups. By Ito's theorem (see [2]

2010 *Mathematics Subject Classification*: Primary 20D30; Secondary 06C10.
Key words and phrases: finite group, subgroup lattice, nilpotent group, lower semimodular lattice, modular chain.

DOI: 10.4064/cm131-2-3

or [6, Theorem 5.3.11]), $L(G)$ is lower semimodular if and only if G is supersoluble and induces an automorphism group of at most prime order in every chief factor. In particular, these groups have a Sylow tower. The structure of finite groups with a modular chain is much more restricted.

THEOREM B. *Let G be a finite group. Then $L(G)$ has a modular chain if and only if G has a Sylow tower $1 = P_0 < \cdots < P_n = G$ such that for all $i \in \{1, \dots, n\}$, every complement K_i/P_{i-1} to the Sylow p_i-subgroup P_i/P_{i-1} of G/P_{i-1} satisfies either*

(a) $G/P_{i-1} = P_i/P_{i-1} \times K_i/P_{i-1}$, *or*
(b) $|K_i/P_{i-1} : C_{K_i/P_{i-1}}(P_i/P_{i-1})|$ *is a prime dividing* $p_i - 1$ *and* $C_{P_i/P_{i-1}}(K_i/P_{i-1}) \trianglelefteq P_i/P_{i-1}$.

In particular, K_i induces an automorphism group of at most prime order in the normal Sylow subgroup P_i/P_{i-1}, not only in the chief factors of G between P_i and P_{i-1}. It is well-known [6, p. 54] that the projective closure $\mathfrak{N}^*$ of the class $\mathfrak{N}$ of finite nilpotent groups is the class of coprime direct products of finite primary and P-groups. Several lattice-theoretic characterizations of this class of groups are given in [7]. Theorem B shows that $\mathfrak{N}^*$ is strictly smaller than the class of finite groups with modular chains and we finally prove that it is not possible to find a (better) lattice-theoretic translation, "L-central chain", say, of a central series for which $\mathfrak{N}^*$ would be the class of groups G such that $L(G)$ has an L-central chain.

All groups and lattices considered are finite. Our notation is standard (see [4] or [6]) except that we write $H \cup K$ for the group generated by the subgroups H and K of the group G. The least and greatest elements of the lattice L are denoted by 0 and I, respectively, a minimal nontrivial element of L is an *atom* of L, elements with the dual property are called *antiatoms*, and for $a, b \in L$ such that $a \leq b$, we let $[b/a] = \{x \in L \,|\, a \leq x \leq b\}$. For short, we say that G is a *group with a modular chain* if $L(G)$ has a modular chain, and that G is an *LM-group* if $L(G)$ is lower semimodular.

2. Proof of Theorem A. We first give the definition of a modular chain in a finite lattice [6, 7.2.1]. Recall that a lattice L is *modular* if for all $x, y, z \in L$ the modular law holds:

- If $x \leq z$, then $x \cup (y \cap z) = (x \cup y) \cap z$.

An element $m \in L$ is *modular in* L, if

- $x \cup (m \cap z) = (x \cup m) \cap z$ for all $x, z \in L$ with $x \leq z$, and
- $m \cup (y \cap z) = (m \cup y) \cap z$ for all $y, z \in L$ with $m \leq z$.

For a group G, a modular element of $L(G)$ is called *modular* in G.

DEFINITION 2.1. Let L be a finite lattice, 0 its least and I its greatest element. Then

(a) $c \in L$ is called *cyclic* if $[c/0]$ is distributive,
(b) $\mathcal{C}(L)$ is the set of cyclic elements of L,
(c) $a \in L$ is *modularly embedded* in L if $[a \cup c/0]$ is a modular lattice for all $c \in \mathcal{C}(L)$, and
(d) $0 = a_0 \leq \cdots \leq a_n = I$ is a *modular chain* in L if a_{i+1} is modularly embedded in $[I/a_i]$ for all $i = 0, \ldots, n-1$.

If G is a finite group, then by Ore's theorem [6, 1.2.4], $\mathcal{C}(L(G))$ consists of the cyclic subgroups of G. Furthermore, a subgroup A of G is central if and only if $A \cup X$ is abelian for every cyclic subgroup X of G. Since every abelian group has modular subgroup lattice [6, 2.1.4], it is clear that every central subgroup of G is modularly embedded in $L(G)$ and every central series of G is a modular chain in $L(G)$. In addition, every normal subgroup of G is modular in $L(G)$ ([6, 2.1.3]) and Kontorovich and Plotkin included this in their definition of a modularly embedded or, as they called it, d-central element of a lattice. We also consider their original property.

DEFINITION 2.2. The element a of the lattice L is called *d-central* in L if a is modular and modularly embedded in L. A chain $0 = a_0 \leq \cdots \leq a_n = I$ in L is called *d-central* if a_{i+1} is d-central in $[I/a_i]$ for all $i = 0, \ldots, n-1$.

Clearly, every d-central chain is a modular chain, and it is also rather obvious that a modular chain need not be d-central (see Example 2.7). For subgroup lattices of finite groups, however, a deep theorem of Previato's (see [5] or [6, Theorem 5.1.13]) implies that every modular chain is d-central.

PROPOSITION 2.3. *Let G be a finite group.*

(a) *Suppose that $A \leq B \leq G$ and that A is modular in G. If B is modularly embedded in $[G/A]$, then B is modular in G.*
(b) *If $1 = A_0 \leq \cdots \leq A_n = G$ is a modular chain in $L(G)$, then every A_i is modular in G.*
(c) *Every modular chain in $L(G)$ is d-central.*

Proof. (a) Let $X \leq G$ be cyclic of prime power order. Then $L(X)$ is a chain and by [6, 2.1.5], $[A \cup X/A] \simeq [X/A \cap X]$ since A is modular in G. Thus $[A \cup X/A]$ is distributive and since B is modularly embedded in $[G/A]$, it follows that $[B \cup X/A]$ is modular. Hence B is modular in $[B \cup X/A]$ and by [6, 2.1.6(c)], B is modular in $B \cup X$. Now Previato's theorem [6, 5.1.13] implies that B is modular in G.

(b) follows from (a) by a trivial induction and, clearly, implies (c). ∎

By Proposition 2.3, we only have to study modular chains. We want to show next that these have the same inheritance properties as central series.

For this we need the following simple result which generalizes Ore's theorem on finite groups with distributive subgroup lattices and also holds for infinite groups.

PROPOSITION 2.4. *If G is a group and $H \le G$ is such that $[G/H]$ is a finite distributive lattice, then there exists $x \in G$ such that $G = \langle H, x\rangle$.*

Proof. Suppose that this is false and let G, H be a counterexample. Then $[G/H]$ is finite and so we may assume that H is maximal in G such that the assertion does not hold. Clearly, there exists $M \le G$ such that H is a maximal subgroup of M and hence $M = \langle H, x\rangle$ with $x \in M \setminus H$. Since $[G/M]$ is distributive, the maximality of H implies that there exists $y \in G$ such that $G = \langle M, y\rangle = \langle H, x, y\rangle$. Let $K_1 = \langle H, y\rangle$ and $K_2 = \langle H, xy\rangle$. Then $K_1 \cup K_2 \ge \langle H, x, y\rangle = G$. Since H is a counterexample, $K_i < G$, therefore $x \notin K_i$ and so $M \cap K_i = H$ for $i = 1, 2$. The distributivity of $[G/H]$ yields

$$M = M \cap G = M \cap (K_1 \cup K_2) = (M \cap K_1) \cup (M \cap K_2) = H,$$

a contradiction. ∎

To prove the desired inheritance properties, we again have to look at the situation in Proposition 2.3(a).

LEMMA 2.5. *Let G be a finite group, let $A \le B \le G$ and suppose that A is modular in G and B is modularly embedded in $[G/A]$.*

(a) *If $A \le D_1 \le D_2 \le B$, then D_2 is modularly embedded in $[G/D_1]$.*
(b) *If $H \le G$, then $B \cap H$ is modularly embedded in $[H/A \cap H]$.*
(c) *For M modular in G, $B \cup M$ is modularly embedded in $[G/A \cup M]$.*

Proof. If $x \in G$, then by [6, 2.1.5 and 1.2.4], $[A \cup \langle x\rangle/A] \simeq [\langle x\rangle/\langle x\rangle \cap A]$ is distributive, and since B is modularly embedded in $[G/A]$, it follows that

($\star$) $[B \cup \langle x\rangle/A]$ is a modular lattice.

(a) Let $X \in \mathcal{C}([G/D_1])$. By 2.4 there exists $x \in X$ such that $X = D_1 \cup \langle x\rangle$. By ($\star$), $[B \cup \langle x\rangle/A]$ is modular, and since $A \le D_1 \le D_2 \cup X \le B \cup \langle x\rangle$, it follows that $[D_2 \cup X/D_1]$ is modular.

(b) Let $X \in \mathcal{C}([H/A \cap H])$. By 2.4 there exists $x \in X$ such that $X = (A \cap H) \cup \langle x\rangle$, and again by ($\star$), $[B \cup X/A]$ is modular. By [6, 2.1.5],

$$[(B \cap H) \cup X/((B \cap H) \cup X) \cap A] \simeq [(B \cap H) \cup X \cup A/A].$$

Since $A \cap H \le (B \cap H) \cup X \le H$, we have $((B \cap H) \cup X) \cap A = A \cap H$, and since $B \cap H$, X, A are all contained in $B \cup X$, the lattice $[(B \cap H) \cup X/A \cap H]$ is isomorphic to an interval in $[B \cup X/A]$ and hence is modular.

(c) Let $X \in \mathcal{C}([G/A \cup M])$. By 2.4 there exists $x \in X$ such that $X = (A \cup M) \cup \langle x\rangle$. By [6, 2.1.6], $A \cup M$ is modular in G. Since $(B \cup M) \cup X =$

$(B \cup \langle x \rangle) \cup (A \cup M)$, it follows from [6, 2.1.5] that

$$[(B \cup M) \cup X/A \cup M] \simeq [B \cup \langle x \rangle/(B \cup \langle x \rangle) \cap (A \cup M)].$$

This is an interval in $[B \cup \langle x \rangle/A]$ and hence, by $(\star)$, it is modular. ∎

Proposition 2.6. *Let* G *be a finite group and let* $1 = A_0 \leq \cdots \leq A_n = G$ *be a modular chain in* $L(G)$.

(a) *Every refinement of this chain is a modular chain; in particular, this holds for every maximal chain in* $L(G)$ *which contains all the* A_i.
(b) *If* $H \leq G$, *then* $1 = A_0 \cap H \leq \cdots \leq A_n \cap H = H$ *is a modular chain in* $L(H)$.
(c) *If* $M \leq G$ *is modular in* G, *then* $M = A_0 \cup M \leq \cdots \leq A_n \cup M = G$ *is a modular chain in* $[G/M]$.

Proof. By assumption and 2.3, every A_i is modular in G and A_{i+1} is modularly embedded in $[G/A_i]$. Therefore 2.5 implies that $A_{i+1} \cap H$ and $A_{i+1} \cup M$ are modularly embedded in $[H/A_i \cap H]$ and $[G/A_i \cup M]$, respectively. Thus (b) and (c) hold. And if $1 = B_0 \leq \cdots \leq B_m = G$ is a refinement of the given chain, then for every $j \in \{0, \ldots, m-1\}$ there exists $i \in \{0, \ldots, n-1\}$ such that $A_i \leq B_j \leq B_{j+1} \leq A_{i+1}$. By 2.5(a), B_{j+1} is modularly embedded in $[G/B_j]$ and so also (a) holds. ∎

In particular, Proposition 2.6 shows that every subgroup and every factor group of a group with modular chain also has a modular chain. Since its proof uses Propositions 2.3 and 2.4, it is not surprising that none of the statements in Proposition 2.6 holds for arbitrary finite lattices. The following example illustrates this and also that d-central chains do not behave much better.

Example 2.7. Let L^* be the lattice whose Hasse diagram is given in Figure 1 and let L be the interval $[I/0]$ in L^*. By [6, 2.1.5], m is modular

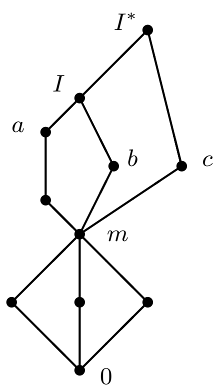

Fig. 1

in L^*, a is modular in L but not in L^*, and b and c are not modular in L and L^*, respectively. Since $\mathcal{C}(L^*) = \mathcal{C}(L)$ consists of 0 and the three atoms of L, it follows that $0 < a < I$ is a d-central chain in L, and $0 < b < I$ and $0 < c < I^*$ are modular chains in L and L^*, respectively, which are not d-central. Furthermore, since a and I are not modularly embedded in $[I/m]$, the following chains are not modular chains:

(a) the refinement $0 < m < a < I$ of $0 < a < I$ in L;
(b) the intersection $0 < m = c \cap I < I = I^* \cap I$ of $0 < c < I^*$ with L;
(c) the union $m = m \cup 0 < a = m \cup a < I$ of $0 < a < I$ with m.

It is a well-known theorem of Baer's that a group G is hypercentral (and therefore a finite group is nilpotent) if and only if every nontrivial factor group of G has a nontrivial centre. Using Definitions 2.1 and 2.2, we can translate this condition into two lattice properties.

DEFINITION 2.8. Let L be a finite lattice. We say that $L \in \mathfrak{B}$ (respectively, $L \in \mathfrak{B}^*$) if for every modular element $a < I$ of L there exists $b \in L$ such that $a < b$ and b is modularly embedded (respectively, d-central) in $[I/a]$.

We want to show that for subgroup lattices of finite groups, our four lattice-theoretic translations of the existence of a central series and of Baer's property all are equivalent. For finite lattices, we have the following.

LEMMA 2.9. *Let L be a finite lattice and suppose that $L \in \mathfrak{B}^*$.*

(a) *If m is modular in L, then $[I/m] \in \mathfrak{B}^*$.*
(b) *L has a d-central chain.*

Proof. (a) Let a be a modular element of $[I/m]$ such that $a < I$. Then by [6, 2.1.6(c)], a is modular in L and since $L \in \mathfrak{B}^*$, there exists $b \in L$ such that $a < b$ and b is d-central in $[I/a]$. In particular, $b \in [I/m]$ and so $[I/m] \in \mathfrak{B}^*$.

(b) We use induction on $|L|$ and may assume that $|L| \geq 2$. Since $L \in \mathfrak{B}^*$, there exists $a_1 \in L$ such that $0 < a_1$ and a_1 is d-central in $[I/0] = L$. In particular, a_1 is modular in L, hence $[I/a_1] \in \mathfrak{B}^*$ by (a), and the induction hypothesis implies that $[I/a_1]$ has a d-central chain $a_1 \leq \cdots \leq a_n = I$. Then $0 \leq a_1 \leq \cdots \leq a_n$ is a d-central chain in L. ∎

THEOREM 2.10. *The following properties of the finite group G are equivalent:*

(a) *$L(G)$ has a modular chain.*
(b) *$L(G)$ has a d-central chain.*
(c) *$L(G) \in \mathfrak{B}$.*
(d) *$L(G) \in \mathfrak{B}^*$.*

Proof. By 2.3(c), properties (a) and (b) are equivalent, by 2.3(a) so are (c) and (d), and by Lemma 2.9, (d) implies (b); hence it suffices to show that (a) implies (c). So suppose that $1 = A_0 \le \cdots \le A_n = G$ is a modular chain in $L(G)$ and that A is a proper modular subgroup of G. Then by 2.6(c), $A = A \cup A_0 \le \cdots \le A \cup A_n = G$ is a modular chain in $[G/A]$. Since $A < G$, there exists $i \in \{0, \ldots, n-1\}$ such that $A = A \cup A_i$ and $A < A \cup A_{i+1} =: B$. Then B is modularly embedded in $[G/A \cup A_i] = [G/A]$ and it follows that $L(G) \in \mathfrak{B}$. ∎

By Lemma 2.9, every lattice in $\mathfrak{B}^*$ has a d-central chain and, by definition, lies in $\mathfrak{B}$; likewise, every lattice with a d-central chain has a modular chain. But these are the only implications between the four properties in Theorem 2.10 which hold for arbitrary finite lattices. For, the lattice L^* in Example 2.7 has a modular chain but no d-central chain, and its sublattice $L = [I/0]$ has a d-central chain; both lattices do not belong to $\mathfrak{B}$ since neither $[I/m]$ nor $[I^*/m]$ has a nontrivial modularly embedded element.

And the lattice L whose Hasse diagram is given in Figure 2 lies in $\mathfrak{B}$ and has none of the other three properties. For, since $c \in \mathcal{C}(L)$ and $c \cup x = I$ for

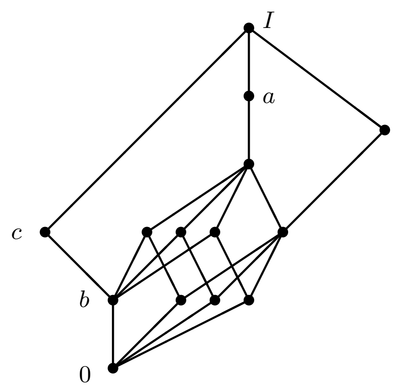

Fig. 2

every $x \in L \setminus \{0, b, c\}$, it is clear that b is the unique nontrivial modularly embedded element in L and that $[I/b]$ has no such element; therefore L has no modular chain. Since [6, 2.1.5] shows that 0, a, I are the only modular elements in L, it follows that $L \in \mathfrak{B}$ and $L \notin \mathfrak{B}^*$. Thus L has the desired properties.

We come to the proof of Theorem A.

Theorem 2.11. *If G is a finite group and $L(G)$ has a modular chain, then $L(G)$ is lower semimodular.*

Proof. We use induction on $|G|$, may assume that $G \neq 1$, and first note that it suffices to prove the following:

($\star$) There exists $N \trianglelefteq G$ such that $|N| \in \mathbb{P}$ and $|G/C_G(N)| \in \mathbb{P} \cup \{1\}$.

For, then 2.6(c) implies that $L(G/N)$ has a modular chain and therefore is lower semimodular by the induction assumption. By Ito's theorem [6, 5.3.11], G/N is supersoluble and G induces automorphism groups of at most prime order in the chief factors above N. By ($\star$), this also holds for the chief factor N, and G is supersoluble. Again by Ito's theorem, $L(G)$ is lower semimodular.

To prove ($\star$), we consider a minimal subgroup A in the first nontrivial term of a modular chain in $L(G)$. Clearly, A is modularly embedded in $L(G)$ and by 2.3(a), A is modular in G.

Suppose first that $A \trianglelefteq G$. If $A \leq Z(G)$, then ($\star$) holds; so let $A \not\leq Z(G)$. By definition, $|A| = p$ is a prime and hence $G/C_G(A)$ is cyclic; let $x \in G$ be such that $G = C_G(A)\langle x\rangle$. Since A is modularly embedded in $L(G)$, $A\langle x\rangle$ has modular subgroup lattice. Since $\langle x\rangle/C_{\langle x\rangle}(A)$ operates faithfully on A, Iwasawa's theorem [6, 2.4.4] implies that $A\langle x\rangle/C_{\langle x\rangle}(A)$ is nonabelian of order pq for some prime q. Thus $|G/C_G(A)| = q$ and ($\star$) holds with $N = A$.

Now suppose that A is not normal in G. If A is permutable in G, then by [6, 5.2.9], $Z(G) \neq 1$ and ($\star$) holds. And if A is not permutable in G, then by [6, 5.1.9], $G = A^G \times K$ with nonabelian P-group A^G and $(|A^G|, |K|) = 1$. Then every normal subgroup N of prime order in A^G satisfies $|G/C_G(N)| = |A| \in \mathbb{P}$ and ($\star$) holds. ∎

None of the lattices displayed in Figures 1 and 2 is lower semimodular; they even do not satisfy the Jordan–Dedekind chain condition. However, $\mathfrak{B}^*$ is the strongest of the properties we have considered. Therefore we finally show that also $\mathfrak{B}^*$ does not imply lower semimodularity.

EXAMPLE 2.12. Let $p \in \mathbb{P}$ and $4 \leq k \in \mathbb{N}$, suppose that H is an elementary abelian group of order p^k (of course, $p = 2$ and $k = 4$ suffice to get the desired example) and let $A_1, \dots, A_n$ be the maximal subgroups of H. The lattice $\mathcal{L}$ is obtained from $L(H)$ by adjoining elements $B_0, B_1, \dots, B_n$ and I such that I is the greatest element and the trivial subgroup of H is the least element 0 of $\mathcal{L}$; H and all the B_i are pairwise different antiatoms of $\mathcal{L}$; A_i is the unique antiatom in $[B_i/0]$ for $i = 1, \dots, n$; and $A_1 \cap A_2$ is the unique antiatom in $[B_0/0]$.

Since $k \geq 4$, $A_1 \cap A_2$ is not cyclic and hence $\mathcal{C}(\mathcal{L})$ consists of the subgroups of order at most p of H. Therefore H is modularly embedded in $\mathcal{L}$. In addition, [6, 2.1.5] shows that H is modular in $\mathcal{L}$ and we claim that $0, H, I$ are the only modular elements of $\mathcal{L}$.

For, if $i \neq j$ and $j \geq 1$, then $[B_i \cup B_j/B_i]$ is a chain of length 1 and $[B_j/B_i \cap B_j]$ has length at least 2; therefore B_i is not modular in $\mathcal{L}$. And if $0 < A < H$, there exist $i, j \in \{1, \ldots, n\}$ such that $A \leq A_i \leq B_i$ and $A \not\leq B_j$. Then A_j is the unique antiatom in $[B_j/A \cap B_j]$ whereas $[A \cup B_j/A] = [I/A]$ contains the antiatoms H and B_i. Thus A is not modular in $\mathcal{L}$.

Since H is d-central in $\mathcal{L}$, it follows that $\mathcal{L} \in \mathfrak{B}^*$. But, clearly, $\mathcal{L}$ does not satisfy the Jordan–Dedekind chain condition; in particular, $\mathcal{L}$ is not lower semimodular. If we omit B_0 in our example, we still obtain a lattice in $\mathfrak{B}^*$ which is not lower semimodular (but satisfies the Jordan–Dedekind chain condition); this also works for $k = 3$.

3. Proof of Theorem B. By Theorem A and Ito's theorem, every finite group with modular chain is supersoluble and hence has a Sylow tower. To determine the structure of these groups, we therefore have to consider finite groups with a normal Sylow subgroup.

LEMMA 3.1. *Let p and q be different primes and suppose that $G = PQ$ where P is a normal p-subgroup, $|Q| = q$ and $1 < C_P(Q) < P$. If A is a minimal subgroup of G which is modularly embedded in $L(G)$, then $A \leq C_P(Q)$.*

Proof. Suppose that $A \not\leq C_P(Q)$ and let $N \leq C_P(Q)$ be such that $|N| = p$. Then $X = NQ$ is cyclic of order pq. Since A is modularly embedded in $L(G)$, $A \cup X^g$ has modular subgroup lattice for every $g \in G$ and therefore is nilpotent by Iwasawa's theorem [6, 2.4.4] because it contains an element of order pq. In particular, $A \cup X$ is nilpotent and since $A \not\leq C_P(Q)$, it follows that $|A| = q$. So $A = Q$ is the Sylow q-subgroup of $A \cup X$. But since $C_P(Q) < P$, there exists $g \in G \setminus N_G(Q)$ and the nilpotent group $A \cup X^g$ has two different Sylow q-subgroups Q and Q^g, a contradiction. ∎

LEMMA 3.2. *Let $G = PK$ where P is a normal Sylow p-subgroup of G and $P \cap K = 1$. If $L(G)$ has a modular chain, then*

(a) $|K : C_K(P)| = q \in \mathbb{P} \cup \{1\}$ *where* $q \mid p - 1$, *and*
(b) $C_P(K) \trianglelefteq G$.

Proof. (a) By Theorem A, $L(G)$ is lower semimodular and therefore by Ito's theorem, G is supersoluble.

We show first that $|K : C_K(P)| \in \mathbb{P} \cup \{1\}$. Let G be a minimal counterexample to this assertion and let H be a maximal subgroup of K. Since G is supersoluble, $|K : H| = r \in \mathbb{P}$. By 2.6, $L(PH)$ has a modular chain and the minimality of G yields $|H : C_H(P)| \in \mathbb{P} \cup \{1\}$; since G is a counterexample, $H > C_H(P)$, so $|H : C_H(P)| = s \in \mathbb{P}$ and $C_H(P) = C_K(P) =: N$. Clearly, $N \trianglelefteq G$ and by 2.6, $L(G/N)$ has a modular chain. So if $N \neq 1$, the minimality of G would imply that for $F/N = C_{K/N}(PN/N)$ we would have

$|K : F| \in \mathbb{P} \cup \{1\}$ and $[P, F] \le P \cap N = 1$. But G is a counterexample, a contradiction. So $N = 1$, that is, we have shown that

(1) $|K| = rs$ where $r, s \in \mathbb{P}$ and $C_K(P) = 1$.

Now suppose, for a contradiction, that there exists a minimal subgroup of G which is modularly embedded in $L(G)$ but not contained in P. Then by Sylow's theorem there exists such a subgroup A with $A < K$. By 2.3, A is modular in G. If A were permutable in G, then $A \trianglelefteq PA$, as a permutable Sylow subgroup of this group; therefore $PA = P \times A$, but this would contradict (1). Thus A is not permutable in G and so by [6, 5.1.9], $G = A^G \times W$ with a nonabelian P-group A^G and $(|A^G|, |W|) = 1$. By (1), $P \not\le W$, hence $P \le A^G$ and then $A^G = PA$; but $G = PA \times W$ contradicts (1). Thus

(2) P contains every modularly embedded atom of $L(G)$.

By assumption, $L(G)$ has a modular chain and hence by 2.1 (or 2.6(a)) there exists a modularly embedded atom A of $L(G)$. By (2), $A \le P$ and since A is modular in G (by 2.3), it follows that

$$A = A \cup (K \cap P) = (A \cup K) \cap P \trianglelefteq A \cup K.$$

If K is not cyclic, then $C_K(A) \ne 1$ since $\operatorname{Aut} A$ is cyclic. If K is cyclic, then AK has modular subgroup lattice since A is modularly embedded in $L(G)$; by Iwasawa's theorem, $C_K(A) \ne 1$. Hence in both cases there exists $Q \le C_K(A)$ such that $|Q| = q \in \mathbb{P}$. By (1), $1 < A \le C_P(Q) < P$. Therefore if B is any modularly embedded atom of $L(G)$, then by (2), $B \le P$ and hence B is modularly embedded in $L(PQ)$; by 3.1, $B \le C_P(Q)$. So if M is the group generated by all modularly embedded atoms of $L(G)$, we have

(3) $M \trianglelefteq G$ and $1 < M \le C_P(Q) < P$.

By 2.6, $L(G/M)$ has a modular chain and the minimality of G and (1) imply that $TM/M \le C_{KM/M}(P/M)$ for some minimal subgroup T of K. Thus $[P, T] \le M$ and since $P = [P, T]C_P(T)$ (see [4, 8.2.7]) and $M < P$, it follows that $C_P(T) \ne 1$. By (1), $T \not\le C_G(P)$ and hence $1 < C_P(T) < P$. Again by (2) and 3.1 applied to PT, every modularly embedded atom of $L(G)$ is contained in $C_P(T)$; hence $M \le C_P(T)$. So T centralizes P/M and M and therefore by [4, 8.2.2], T centralizes P. This contradicts (1) and we have shown that $|K : C_K(P)| = q \in \mathbb{P} \cup \{1\}$.

Finally, suppose that $|K : C_K(P)| = q \in \mathbb{P}$. Then by [4, 8.2.2] there exists a chief factor U/V of G contained in P which is not centralized by K. Since G is supersoluble, $|U/V| = p$ and hence $q \mid p - 1$. This proves (a).

(b) Again let G be a minimal counterexample and let $N = C_K(P)$. Then $N \trianglelefteq G$ and if $N \ne 1$, the minimality of G would imply that $C_P(K)N/N = C_{PN/N}(K/N) \trianglelefteq G/N$ and hence $C_P(K) = P \cap C_P(K)N \trianglelefteq G$. This contradiction shows that $N = 1$. Since $C_P(K)$ is not normal, $1 < C_P(K) < P$ and by (a), $|K| = q \in \mathbb{P}$. Again let M be the group generated by all modularly embedded atoms of $L(G)$. Since $L(G)$ has a modular chain, $M \neq 1$ and by 3.1, $M \leq C_P(K)$. The minimality of G implies that $C_{P/M}(KM/M) \trianglelefteq G/M$. By [4, 8.2.2], $C_{P/M}(KM/M) = C_{P/M}(K) = C_P(K)M/M = C_P(K)/M$ and hence $C_P(K) \trianglelefteq G$, a final contradiction. This proves Lemma 3.2. ■

Conversely, we show the following.

LEMMA 3.3. *Let $p, q \in \mathbb{P}$ be such that $q \mid p-1$ and let $G = PK$ where P is a normal Sylow p-subgroup of G and $P \cap K = 1$; suppose that $C_P(K) \trianglelefteq G$ and $|K : C_K(P)| = q$. If A/B is a chief factor of G such that $C_P(K) \leq B$ and $A \leq P$, then $|A/B| = p$ and A is modularly embedded in $[G/B]$.*

Proof. Clearly, A/B is an elementary abelian p-group which is centralized by P. Therefore the cyclic group $K/C_K(P)$ of order q operates irreducibly on A/B and since $q \mid p-1$, it follows [1, p. 166] that $|A/B| = p$.

Let $X \in \mathcal{C}([G/B])$. Then X/B is cyclic and hence there exists $x \in G$ such that $X = B\langle x\rangle$. If x centralizes A/B, then AX/B is abelian and hence $[A \cup X/B]$ is modular, which we want to show. So suppose that x does not centralize A/B and write $x = x_1x_2$ where $x_i \in \langle x\rangle$, x_1 is a p-element and x_2 is a p'-element. Then $x_1 \in P$ centralizes A/B and therefore x_2 does not. Since $|G/C_K(P)| = |P|q$, it follows that $|\langle x_2\rangle : \langle x_2\rangle \cap C_K(P)| = q$; by Sylow's theorem there exists $g \in G$ such that $x_2 \in K^g$ and hence $K^g = \langle x_2\rangle C_K(P)$. Then $x_1 \in C_P(x_2) = C_P(K^g) = C_P(K)^g \leq B$ and therefore $X = B\langle x_2\rangle$. If we write $x_2 = yz$ where $y, z \in \langle x_2\rangle$, y is a q-element and z is a q'-element, then $z \in C_K(P)$ centralizes $A\langle y\rangle$ and hence $AX/B = A\langle y\rangle/B \times \langle z\rangle B/B$. Now $A\langle y\rangle/B$ is a P^*-group [6, p. 69] since y induces an automorphism of order q in A/B; by Iwasawa's theorem, $L(AX/B)$ is modular. Thus A is modularly embedded in $[G/B]$. ■

We can now prove Theorem B. We state it in a slightly different version which might sometimes be easier to use.

THEOREM 3.4. *Let G be a finite group. Then $L(G)$ has a modular chain if and only if G has a Sylow system $\{S_1, \ldots, S_n\}$ with Sylow p_i-subgroups S_i such that for every $i \in \{1, \ldots, n-1\}$, $S_i \trianglelefteq T_i := S_i \ldots S_n$ and either*

(a) *$T_i = S_i \times T_{i+1}$, or*
(b) *$|T_{i+1} : C_{T_{i+1}}(S_i)|$ is a prime dividing $p_i - 1$ and $C_{S_i}(T_{i+1}) \trianglelefteq S_i$.*

Proof. If G is a p-group, then $L(G)$ has a modular chain and the theorem holds trivially. So assume that $|G|$ is divisible by at least two primes.

If $L(G)$ has a modular chain, then by Theorem A and Ito's theorem, G is supersoluble. Let $p_1 > \cdots > p_n$ be the primes dividing $|G|$ and let

$\{S_1, \dots, S_n\}$ be a Sylow system of G with $S_i \in \mathrm{Syl}_{p_i}(G)$ for all i [1, p. 665]. Then for every $i \in \{1, \dots, n-1\}$, $T_i := S_i \dots S_n$ is a supersoluble subgroup of G and hence $S_i \trianglelefteq T_i$ [1, p. 716]. By 2.6, $L(T_i)$ has a modular chain and therefore (a) and (b) follow from Lemma 3.2.

To prove the converse, we use induction on $|G|$. By assumption, we have $S_1 \trianglelefteq T_1 = G$ and either $G = S_1 \times T_2$ or (b) holds for $i = 1$. In both cases, $C_{S_1}(T_2) \trianglelefteq S_1T_2 = G$. So if $1 = A_0 \leq \dots \leq A_r = S_1$ is part of a chief series of G through $C_{S_1}(T_2)$ and S_1, then A_i is modularly embedded in $[G/A_{i-1}]$ for all $i = 1, \dots, r$: this follows from Lemma 3.3 for $A_i > C_{S_1}(T_2)$ and is trivial for $A_i \leq C_{S_1}(T_2)$ since those chief factors A_i/A_{i-1} are central in G. The induction assumption implies that $L(T_2)$ has a modular chain. If we combine the chain $A_0 \leq \dots \leq A_r$ and the image of a modular chain in $L(T_2)$ under the natural isomorphism from $L(T_2)$ onto $[G/S_1]$, we obtain a modular chain in $L(G)$. ∎

Proof of Theorem B. It is easy to see that Theorem B follows from Theorem 3.4 (and conversely) since the conditions given in these theorems are equivalent. For, if $\{S_1, \dots, S_n\}$ is a Sylow system with the properties stated in Theorem 3.4, then for every $i \in \{1, \dots, n\}$, $P_i := S_1 \dots S_i$ is normal in G and $1 = P_0 < \dots < P_n = G$ is a Sylow tower with $P_i/P_{i-1} \simeq S_i$ and $G/P_{i-1} \simeq T_i$. The natural isomorphism from T_i onto G/P_{i-1} maps T_{i+1} onto a complement K_i/P_{i-1} to P_i/P_{i-1} for which (a) and (b) of Theorem B are satisfied. Since all these complements are conjugate, (a) and (b) hold in general.

Conversely, if $1 = P_0 < \dots < P_n = G$ is a Sylow tower in G with the properties given in Theorem B, then G is soluble and therefore has a Sylow system $\{S_1, \dots, S_n\}$ with $S_i \in \mathrm{Syl}_{p_i}(G)$ for $i = 1, \dots, n$. If $T_i := S_i \dots S_n$, then again $G/P_{i-1} \simeq T_i$ and (a) and (b) of Theorem B imply (a) and (b) of Theorem 3.4 for the complement T_{i+1} to S_i in T_i. ∎

As already mentioned in the introduction, Theorem B (or Lemma 3.2) implies that if G is an LM-group, then $L(G)$ in general does not have a modular chain. For example, by Ito's theorem, the direct product of two LM-groups is an LM-group [6, 5.3.12], but for $p, q \in \mathbb{P}$ with $q \mid p-1$, a direct product G of two (or more) nonabelian groups of order pq does not satisfy (a) of Lemma 3.2 and therefore $L(G)$ has no modular chain. And the semidirect product G of a cyclic group of order p^2 with a faithfully operating cyclic group of order pq is an LM-group which satisfies (a) but not (b) of Lemma 3.2; therefore again $L(G)$ has no modular chain.

On the other hand, every semidirect product $G = P \rtimes Q$ of an abelian p-group P with an arbitrary q-group Q inducing an automorphism of order q in P satisfies (b) of Theorem 3.4 (if $q \mid p-1$) and therefore $L(G)$ has a modular chain; but $G \in \mathfrak{M}^*$ only if G is a P-group [6, p. 54]. This is somewhat disappointing but it is easy to see that it is impossible to obtain a lattice-theoretic characterization of $\mathfrak{N}^*$ as the class of groups whose subgroup lattices have a, let us call it, "L-central chain" even if one uses a better lattice-theoretic approximation of "central subgroup" than "modularly embedded element" in the definition of an L-central chain; at least not if one requires that every minimal subgroup of $Z(G)$ has this lattice-theoretic property in $L(G)$.

REMARK 3.5. Suppose that "L-central" is a lattice-theoretic property such that for every atom A of the subgroup lattice of a finite group G, the following holds:

($\star$) If $A \le Z(G)$, then A is L-central in $L(G)$.

Define an *L-central chain* in a lattice L by replacing "modularly embedded" in 2.1(d) by "L-central". Then if p, q, r are pairwise different primes such that $r \mid q-1$ and $qr \mid p-1$, the subgroup lattices of the following groups G have L-central chains:

(a) $G = A \times (B \rtimes Q)$ where A is an abelian and B an elementary abelian p-group and Q is a q-group inducing a power automorphism of order q in B. Here $G \in \mathfrak{N}^*$ if and only if $A = 1$ and $|Q| = q$.
(b) $G = A \times (B \rtimes H)$ where A and B are as in (a) and H is a nonabelian P-group of order $q^k r$ ($k \in \mathbb{N}$) inducing a power automorphism of order r in B. Here $G \notin \mathfrak{N}^*$.

Proof. (a) Let $N = A \times C_Q(B)$. Then $N \trianglelefteq G$ and the chief factors of G below N are central since Q is a q-group. Therefore if $1 = A_0 \le \cdots \le A_n = N$ is part of a chief series of G, then by ($\star$), A_i is L-central in $[G/A_{i-1}]$ for all $i = 1, \ldots, n$. By [6, §2.2], G/N is a P-group of order $p^m q$ for some $m \in \mathbb{N}$ and hence is lattice-isomorphic to an elementary abelian group T of order p^{m+1}. Again by ($\star$), $L(T)$ and hence also $[G/N]$ has an L-central chain $N = A_n < \cdots < A_{n+m+1} = G$. Then $1 = A_0 \le \cdots \le A_{n+m+1} = G$ is an L-central chain in $L(G)$. Since G is a $\{p, q\}$-group which is not nilpotent, $G \in \mathfrak{N}^*$ if and only if G is a P-group; thus (a) holds.

(b) follows from (a) since by [6, Theorem 4.1.6], $G = A \times (B \rtimes H)$ is lattice-isomorphic to $\bar{G} = A \times (B \rtimes K)$ where K is an elementary abelian group of order q^{k+1} inducing a power automorphism of order q in B. Indeed, if $H = QR$ with $|Q| = q^k$ and $|R| = r$, the identity σ on $N = A \times B$ and any projectivity τ from H to K with $Q^\tau = C_K(B)$ trivially satisfy conditions (1) and (2) of that theorem. By (a), $\bar{G}$ has an L-central chain and hence also G does. Finally, $G \notin \mathfrak{N}^*$ since R operates nontrivially on B and on Q. ∎

REFERENCES

[1] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.
[2] N. Ito, *Note on (LM)-groups of finite orders*, Kōdai Math. Sem. Rep. 3 (1951), 1–6.
[3] P. G. Kontorovich and B. I. Plotkin, *Lattices with an additive basis*, Mat. Sb. 35 (77) (1954), 187–192 (in Russian).
[4] H. Kurzweil and B. Stellmacher, *The Theory of Finite Groups. An Introduction*, Springer, New York, 2004.
[5] E. Previato, *Una caratterizzazione dei sottogruppi di Dedekind di un gruppo finito*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) 59 (1975), 643–650.
[6] R. Schmidt, *Subgroup Lattices of Groups*, de Gruyter Expo. Math. 14, de Gruyter, Berlin, 1994.
[7] R. Schmidt, *On the subgroup lattice index problem in finite groups*, Israel J. Math., to appear.

Roland Schmidt
Mathematisches Seminar
Universität Kiel
Ludewig-Meyn-Str. 4
D-24098 Kiel, Germany
E-mail: schmidt@math.uni-kiel.de

Received 22 March 2013 (5905)