9. Modular and Semimodular Lattices

To dance beneath the diamond sky with one hand waving free ...
–Bob Dylan

The modular law was invented by Dedekind to reflect a crucial property of the lattice of subgroups of an abelian group, or more generally the lattice of normal subgroups of a group. In this chapter on modular lattices you will see the lattice theoretic versions of some familiar theorems from group theory. This will lead us naturally to consider semimodular lattices.

Likewise, the lattice of submodules of a module over a ring is modular. Thus our results on modular lattices apply to the lattice of ideals of a ring, or the lattice of subspaces of a vector space. These applications make modular lattices particularly important.

The smallest nonmodular lattice is $\mathcal{N}_5$, which is called the *pentagon*. Dedekind's characterization of modular lattices is simple [5].

Theorem 9.1. *A lattice is modular if and only if it does not contain the pentagon as a sublattice.*

Proof. Clearly, a modular lattice cannot contain $\mathcal{N}_5$ as a sublattice. Conversely, suppose $\mathcal{L}$ is a nonmodular lattice. Then there exist $x > y$ and z in $\mathcal{L}$ such that $x \wedge (y \vee z) > y \vee (x \wedge z)$. Now the lattice freely generated by x, y, z with $x \geq y$ is shown in Figure 9.1; you should verify that it is correct. The elements $x \wedge (y \vee z)$, $y \vee (x \wedge z)$, z, $x \wedge z$ and $y \vee z$ form a pentagon there, and likewise in $\mathcal{L}$. Since the pentagon is subdirectly irreducible and $x \wedge (y \vee z)/y \vee (x \wedge z)$ is the critical quotient, these five elements are distinct. $\square$

Birkhoff [1] showed that there is a similar characterization of distributive lattices within the class of modular lattices. The *diamond* is $\mathcal{M}_3$, which is the smallest nondistributive modular lattice.

Theorem 9.2. *A modular lattice is distributive if and only if it does not contain the diamond as a sublattice.*

Proof. Again clearly, a distributive lattice cannot have a sublattice isomorphic to $\mathcal{M}_3$. Conversely, let $\mathcal{L}$ be a nondistributive modular lattice. Then, by Lemma 8.2, there exist x, y, z in $\mathcal{L}$ such that $(x \vee y) \wedge (x \vee z) \wedge (y \vee z) > (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$. Now the free modular lattice $\mathcal{F}_{\mathbf{M}}(3)$ is diagrammed in Figure 9.2; again you should
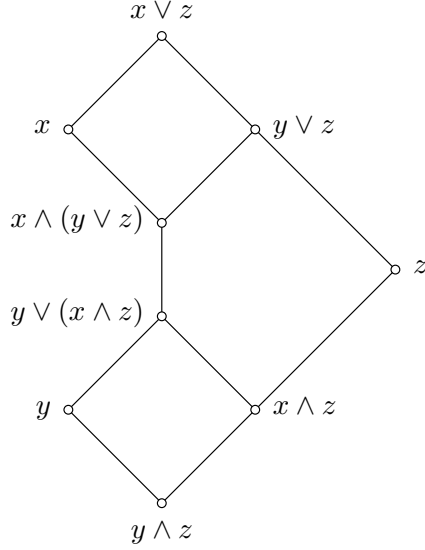
FIGURE 9.1: $\mathrm{FL}(\mathbf{2} + \mathbf{1})$

verify that it is correct.[1] The interval between the two elements above is a diamond in $\mathcal{F}_{\mathbf{M}}(3)$, and the corresponding elements will form a diamond in $\mathcal{L}$.

The details go as follows. The middle elements of our diamond should be

$$[x \wedge (y \vee z)] \vee (y \wedge z) = [x \vee (y \wedge z)] \wedge (y \vee z)$$
$$[y \wedge (x \vee z)] \vee (x \wedge z) = [y \vee (x \wedge z)] \wedge (x \vee z)$$
$$[z \wedge (x \vee y)] \vee (x \wedge y) = [z \vee (x \wedge y)] \wedge (x \vee y)$$

where in each case the equality follows from modularity. The join of the first pair of elements is (using the first expressions)

$$
\begin{aligned}
[x \wedge (y \vee z)] \vee (y \wedge z) \vee [y \wedge (x \vee z)] \vee (x \vee z) &= [x \wedge (y \vee z)] \vee [y \wedge (x \vee z)] \\
&= [(x \wedge (y \vee z)) \vee y] \wedge (x \vee z) \\
&= (x \vee y) \wedge (x \vee z) \wedge (y \vee z).
\end{aligned}
$$

Symmetrically, the other pairs of elements also join to $(x \vee y) \wedge (x \vee z) \wedge (y \vee z)$. Since the second expression for each element is dual to the first, each pair of these three elements meets to $(x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$. Because the diamond is simple, the five elements will be distinct, and hence form a sublattice isomorphic to $\mathcal{M}_3$. $\quad\square$

---

[1] Recall from Chapter 7, though, that $\mathcal{F}_{\mathbf{M}}(n)$ is infinite and has an unsolvable word problem for $n \geq 4$.

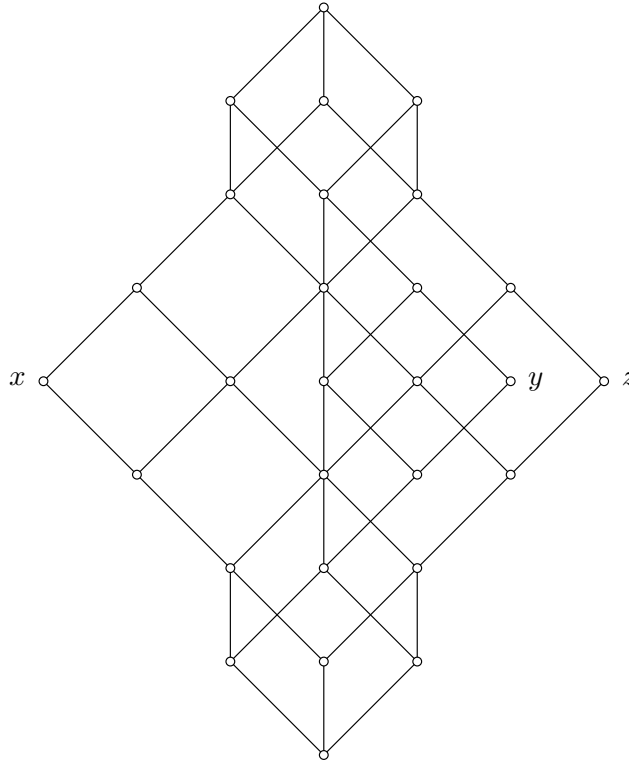FIGURE 9.2: $\mathcal{F}_{\mathbf{M}}(3)$

Corollary. *A lattice is distributive if and only if it has neither $\mathcal{N}_5$ nor $\mathcal{M}_3$ as a sublattice.*

The preceding two results tell us something more about the bottom of the lattice Λ of lattice varieties. We already know that the trivial variety $\mathbf{T}$ is uniquely covered by $\mathbf{D} = \mathrm{HSP}(\mathbf{2})$, which is in turn covered by $\mathrm{HSP}(\mathcal{N}_5)$ and $\mathrm{HSP}(\mathcal{M}_3)$. By the Corollary, these are the only two varieties covering $\mathbf{D}$.

Much more is known about the bottom of Λ. Both $\mathrm{HSP}(\mathcal{N}_5)$ and $\mathrm{HSP}(\mathcal{M}_3)$ are covered by their join $\mathrm{HSP}\{\mathcal{N}_5, \mathcal{M}_3\} = \mathrm{HSP}(\mathcal{N}_5 \times \mathcal{M}_3)$. George Grätzer and Bjarni Jónsson ([8], [11]) showed that $\mathrm{HSP}(\mathcal{M}_3)$ has two additional covers, and Jónsson and Ivan Rival [12] proved that $\mathrm{HSP}(\mathcal{N}_5)$ has exactly fifteen other covers, each generated by a finite subdirectly irreducible lattice. You are encouraged to try and find these covers. Because of Jónsson's Lemma, it is never hard to tell if $\mathrm{HSP}(\mathcal{K})$ covers $\mathrm{HSP}(\mathcal{L})$ when $\mathcal{K}$ and $\mathcal{L}$ are finite lattices; the hard part is determining whether your list of covers is complete. Since a variety generated by a finite lattice can have infinitely many covering varieties, or a covering variety generated by an infinite subdirectly irreducible lattice, this can only be done near the bottom of Λ; see [16].

100

Now we return to modular lattices. For any two elements a, b in a lattice $\mathcal{L}$ there are natural maps $\mu_a : (a \vee b)/b \rightarrow a/(a \wedge b)$ and $\nu_b : a/(a \wedge b) \rightarrow (a \vee b)/b$ given by

$$\mu_a(x) = x \wedge a$$
$$\nu_b(x) = x \vee b.$$

Dedekind showed that these maps play a special role in the structure of modular lattices.

Theorem 9.3. *If a and b are elements of a modular lattice $\mathcal{L}$, then μ_a and ν_b are mutually inverse isomorphisms, whence $(a \vee b)/b \cong a/(a \wedge b)$.*

Proof. Clearly, μ_a and ν_b are order preserving. They are mutually inverse maps by modularity: for if $x \in (a \vee b)/b$, then

$$\nu_b\mu_a(x) = b \vee (a \wedge x) = (b \vee a) \wedge x = x$$

and, dually, $\mu_a\nu_b(y) = y$ for all $y \in a/(a \wedge b)$. $\square$

Corollary. *In a modular lattice, $a \succ a \wedge b$ if and only if $a \vee b \succ b$.*

For groups we actually have somewhat more. The First Isomorphism Theorem says that if $\mathcal{A}$ and $\mathcal{B}$ are subgroups of a group $\mathcal{G}$, and $\mathcal{B}$ is normal in $\mathcal{A} \vee \mathcal{B}$, then the quotient groups $\mathcal{A}/\mathcal{A} \wedge \mathcal{B}$ and $\mathcal{A} \vee \mathcal{B}/\mathcal{B}$ are isomorphic.

A lattice $\mathcal{L}$ is said to be *semimodular* (or *upper semimodular*) if $a \succ a \wedge b$ implies $a \vee b \succ b$ in $\mathcal{L}$. Equivalently, $\mathcal{L}$ is semimodular if $u \succ v$ implies $u \vee x \succeq v \vee x$, where $a \succeq b$ means a covers or equals b. The dual property is called *lower semimodular*. Traditionally, *semimodular* by itself always refers to upper semimodularity. Clearly the Corollary shows that modular lattices are both upper and lower semimodular. A strongly atomic, algebraic lattice that is both upper and lower semimodular is modular. (See Theorem 3.7 of [3]; you are asked to prove the finite dimensional version of this in Exercise 3.)

Dedekind proved in his seminal paper of 1900 that every maximal chain in a finite dimensional modular lattice has the same length. The proof extends naturally to semimodular lattices.

Theorem 9.4. *Let $\mathcal{L}$ be a semimodular lattice and let $a < b$ in $\mathcal{L}$. If there is a finite maximal chain from a to b, then every chain from a to b is finite, and all the maximal ones have the same length.*

Proof. We are given that there is a finite maximal chain in b/a, say

$$a = a_0 \prec a_1 \prec \cdots \prec a_n = b.$$

If $n = 1$, i.e., $a \prec b$, then the theorem is trivially true. So we may assume inductively that it holds for any interval containing a maximal chain of length less than n.

Let C be another maximal chain in b/a. If, perchance, $c \geq a_1$ for all $c \in C - \{a\}$, then $C - \{a\}$ is a maximal chain in b/a_1. In that case, $C - \{a\}$ has length $n - 1$ by induction, and so C has length n.

Thus we may assume that there is an element $d \in C - \{a\}$ such that $d \not\geq a_1$. Moreover, since b/a_1 has finite length, we can choose d such that $d \vee a_1$ is minimal, i.e., $e \vee a_1 \geq d \vee a_1$ for all $e \in C - \{a\}$. We can show that $d \succ a$ as follows. Suppose not. Then $d > e > a$ for some $e \in L$; since C is a maximal chain containing a and d, we can choose $e \in C$. Now $a_1 \succ a = d \wedge a_1 = e \wedge a_1$. Hence by semimodularity $d \vee a_1 \succ d$ and $e \vee a_1 \succ e$. But the choice of d implies $e \vee a_1 \geq d \vee a_1 \succ d > e$, contradicting the second covering relation. Therefore $d \succ a$.

Now we are quickly done. As a_1 and d both cover a, their join $a_1 \vee d$ covers both of them. Since $a_1 \vee d \succ a_1$, every maximal chain in $b/(a_1 \vee d)$ has length $n - 2$. Then every chain in b/d has length $n - 1$, and C has length n, as desired. $\square$

Now let $\mathcal{L}$ be a semimodular lattice in which every principal ideal $\downarrow x$ has a finite maximal chain. Then we can define a *dimension function* δ on $\mathcal{L}$ by letting $\delta(x)$ be the length of a maximal chain from 0 to x:

$$\delta(x) = n \quad \text{if} \quad 0 = c_0 \prec c_1 \prec \cdots \prec c_n = x.$$

By Theorem 9.4, δ is well defined. For semimodular lattices the properties of the dimension function can be summarized as follows.

Theorem 9.5. *If $\mathcal{L}$ is a semimodular lattice and every principal ideal has only finite maximal chains, then the dimension function on $\mathcal{L}$ has the following properties.*

(1) $\delta(0) = 0$,
(2) $x > y$ *implies* $\delta(x) > \delta(y)$,
(3) $x \succ y$ *implies* $\delta(x) = \delta(y) + 1$,
(4) $\delta(x \vee y) + \delta(x \wedge y) \leq \delta(x) + \delta(y)$.

Conversely, if $\mathcal{L}$ is a lattice that admits an integer valued function δ satisfying (1)–(4), then $\mathcal{L}$ is semimodular and principal ideals have only finite maximal chains.

Proof. Given a semimodular lattice $\mathcal{L}$ in which principal ideals have only finite maximal chains, properties (1) and (2) are obvious, while (3) is a consequence of Theorem 9.4. The only (not very) hard part is to establish the inequality (4). Let x and y be elements of $\mathcal{L}$, and consider the join map $\nu_x : y/(x \wedge y) \to (x \vee y)/x$ defined by $\nu_x(z) = z \vee x$. Recall that, by semimodularity, $u \succ v$ implies $u \vee x \succeq v \vee x$. Hence ν_x takes maximal chains in $y/(x \wedge y)$ to maximal chains in $(x \vee y)/x$. So the length of $(x \vee y)/x$ is at most that of $y/(x \wedge y)$, i.e.,

$$\delta(x \vee y) - \delta(x) \leq \delta(y) - \delta(x \wedge y)$$

which establishes the desired inequality.

102

Conversely, suppose $\mathcal{L}$ is a lattice that admits a function δ satisfying (1)–(4). Note that, by (2), $\delta(x) \geq \delta(z)+2$ whenever $x > y > z$; hence if $x \geq z$ and $\delta(x) = \delta(z)+1$, then $x \succ z$.

To establish semimodularity, assume $a \succ a \wedge b$ in $\mathcal{L}$. By (3) we have $\delta(a) = \delta(a \wedge b) + 1$, and so by (4)

$$\delta(a \vee b) + \delta(a \wedge b) \leq \delta(a) + \delta(b)$$
$$= \delta(a \wedge b) + 1 + \delta(b)$$

whence $\delta(a \vee b) \leq \delta(b) + 1$. As $a \vee b > b$, in fact $\delta(a \vee b) = \delta(b) + 1$ and $a \vee b \succ b$, as desired.

For any $a \in L$, if $a = a_k > a_{k-1} > \cdots > a_0$ is any chain in $\downarrow a$, then $\delta(a_j) > \delta(a_{j-1})$ so $k \leq \delta(a)$. Thus every chain in $\downarrow a$ has length at most $\delta(a)$. $\square$

For modular lattices, the map μ_x is an isomorphism, so we obtain instead equality. It also turns out that we can dispense with the third condition, though this is not very important.

Theorem 9.6. *If $\mathcal{L}$ is a modular lattice and every principal ideal has only finite maximal chains, then*

(1) $\delta(0) = 0$,
(2) $x > y$ *implies* $\delta(x) > \delta(y)$,
(3) $\delta(x \vee y) + \delta(x \wedge y) = \delta(x) + \delta(y)$.

Conversely, if $\mathcal{L}$ is a lattice that admits an integer-valued function δ satisfying (1)–(3), then $\mathcal{L}$ is modular and principal ideals have only finite maximal chains.

At this point, it is perhaps useful to have some examples of semimodular lattices. The lattice of equivalence relations **Eq** X is semimodular, but nonmodular for $|X| \geq 4$. The lattice in Figure 9.3 is semimodular, but not modular.[2] We will see more semimodular lattices as we go along, arising from group theory (subnormal subgroups) in this chapter and from geometry in Chapter 11.

For our applications to group theory, we need a supplement to Theorem 9.4. This in turn requires a definition. We say that a quotient a/b *transposes up* to c/d if $a \vee d = c$ and $a \wedge d = b$. We then say that c/d *transposes down* to a/b. We then define *projectivity* to be the smallest equivalence relation on the set of all quotients of a lattice $\mathcal{L}$ that contains all transposed pairs $\langle x/(x \wedge y), (x \vee y)/y \rangle$. Thus a/b is projective to c/d if and only if there exists a sequence of quotients

---

[2]One standard trick to construct semimodular lattices is to take a finite dimensional modular lattice $\mathcal{L}$, of dimension n say, so that $\delta(1) = n$. Choose an integer $k < n$, and remove all elements $x \in L$ with $k \leq \delta(x) < n$. (Alternatively, take the join semilattice congruence collapsing all these elements to 1.) The result is a semimodular lattice $\widehat{\mathcal{L}}$ of dimension k. The lattice in Figure 9.3 was obtained by applying this method to the lattice of subsets of a four element set. See Exercise 1 of Chapter 11.
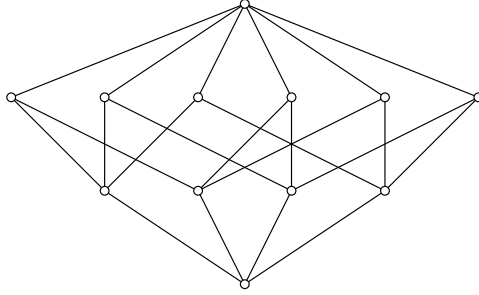
$a/b = a_0/b_0, a_1/b_1, \ldots, a_n/b_n = c/d$ such that a_i/b_i and a_{i+1}/b_{i+1} are transposes (up or down).

The strengthened version of Theorem 9.4 goes thusly. This can be (and was originally) obtained by a slight extension of Dedekind's arguments. The proof given here is due to George Grätzer and the author [9].

Theorem 9.7. *Let C and D be two maximal chains in a finite length semimodular lattice, say*

$$0 = c_0 \prec c_1 \prec \cdots \prec c_n = 1$$
$$0 = d_0 \prec d_1 \prec \cdots \prec d_n = 1.$$

Then there is a permutation π of the set $\{1, \ldots, n\}$ such that c_i/c_{i-1} is projective in two steps (up-down) to $d_{\pi(i)}/d_{\pi(i)-1}$ for all i.

Proof. Again, the proof is by induction on the length n. The statement is obvious for $n \leq 2$, so assume $n > 2$. The argument is illustrated in Figure 9.4.

Let k be the largest integer with $c_1 \not\leq d_k$, noting $k < n$. If $k = 0$, then $c_1 = d_1$ and the statement follows by the induction hypothesis. So we can assume that $k > 0$.

For $0 \leq j \leq n$, let $e_j = c_1 \vee d_j$. Note that $e_0 = c_1$ and $e_k = e_{k+1} = d_{k+1}$, and indeed $e_j = d_j$ for $j \geq k + 1$. Now

$$c_1 = e_0 \prec e_1 \prec \cdots \prec e_k = e_{k+1} \prec e_{k+2} \prec \cdots \prec e_n = 1$$

is a maximal chain in the interval $1/c_1$. By induction, there is an bijective map $\sigma : \{2, \ldots, n\} \to \{1, \ldots, k, k+2, \ldots, n\}$ such that, for $i > 1$, each interval c_i/c_{i-1} is projective up to some prime interval u_i/v_i in $\mathcal{L}$, which in turn projects down to $e_{\sigma(i)}/e_{\sigma(i)-1}$. For $j \leq k$, e_j/e_{j-1} projects down to d_j/d_{j-1}, while for $j > k+1$ we have $e_j/e_{j-1} = d_j/d_{j-1}$. Meanwhile, $c_1/0$ projects up to d_{k+1}/d_k. So we may take π to be the permutation with $\pi(i) = \sigma(i)$ for $i \neq 1$, and $\pi(1) = k + 1$. $\square$
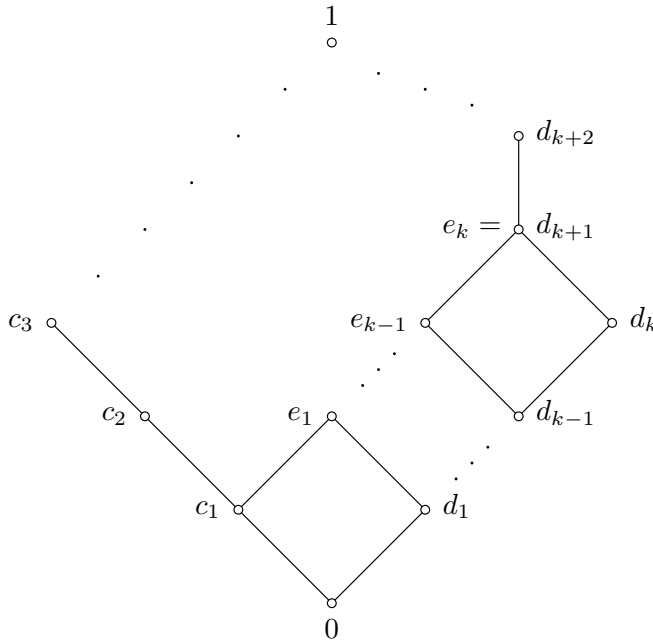
FIGURE 9.4

Theorems 9.4 and 9.7 are important in group theory. A *chief series* of a group $\mathcal{G}$ is a maximal chain in the lattice of normal subgroups $\mathcal{N}(\mathcal{G})$. Since $\mathcal{N}(\mathcal{G})$ is modular, our theorems apply.

Corollary. *If a group $\mathcal{G}$ has a finite chief series of length k,*

$$\{1\} = N_0 < N_1 < \cdots < N_k = \mathcal{G}$$

then every chief series of $\mathcal{G}$ has length k. Moreover, if

$$\{1\} = H_0 < H_1 < \cdots < H_k = \mathcal{G}$$

is another chief series of $\mathcal{G}$, then there is a permutation π of $\{1,\ldots,k\}$ such that $H_i/H_{i-1} \cong N_{\pi(i)}/N_{\pi(i)-1}$ for all i.

A subgroup H is *subnormal* in a group $\mathcal{G}$, written $H \lhd\lhd \mathcal{G}$, if there is a chain in **Sub** $\mathcal{G}$,

$$H = H_0 \lhd H_1 \lhd \ldots \lhd H_k = \mathcal{G}$$

with each H_{i-1} normal in H_i (but H_j need not be normal in $\mathcal{G}$ for $j < k$). Herman Wielandt proved that the subnormal subgroups of a finite group form a lattice [20].

Theorem 9.8. *If $\mathcal{G}$ is a finite group, then the subnormal subgroups of $\mathcal{G}$ form a lower semimodular sublattice $\mathcal{SN}(\mathcal{G})$ of* **Sub** $\mathcal{G}$.

105

Proof. Let H and K be subnormal in $\mathcal{G}$, with say

$$H = H_0 \lhd H_1 \lhd \ldots \lhd H_m = \mathcal{G}$$
$$K = K_0 \lhd K_1 \lhd \ldots \lhd K_n = \mathcal{G}.$$

Then $H \cap K_i \lhd H \cap K_{i+1}$, and so we have the series

$$H \cap K \lhd H \cap K_1 \lhd H \cap K_2 \lhd \ldots H \cap \mathcal{G} = H \lhd H_1 \lhd \ldots \lhd \mathcal{G}.$$

Thus $H \cap K \lhd\lhd \mathcal{G}$. Note that this argument shows that *if H, $K \lhd\lhd \mathcal{G}$ and $K \leq H$, then $K \lhd\lhd H$.*

The proof that $\mathcal{SN}(\mathcal{G})$ is closed under joins is a bit trickier. Let H, $K \lhd\lhd \mathcal{G}$ as before. Without loss of generality, H and K are incomparable. By induction, we may assume that $|\mathcal{G}|$ is minimal and that the result holds for larger subnormal subgroups of $\mathcal{G}$, i.e.,

(1) the join of subnormal subgroups is again subnormal in any group $\mathcal{G}'$ with $|\mathcal{G}'| < |\mathcal{G}|$,

(2) if $H < L \lhd\lhd \mathcal{G}$, then $L \vee K \lhd\lhd \mathcal{G}$; likewise, if $K < M \lhd\lhd \mathcal{G}$, then $H \vee M \lhd\lhd \mathcal{G}$.

If there is a subnormal proper subgroup S of $\mathcal{G}$ that contains both H and K, then H and K are subnormal subgroups of S (by the observation above). In that case, $H \vee K \lhd\lhd S$ by the first assumption, whence $H \vee K \lhd\lhd \mathcal{G}$. Thus we may assume that

(3) no subnormal proper subgroup of $\mathcal{G}$ contains both H and K.

Combining this with assumption (2) yields

(4) $H_1 \vee K = \mathcal{G} = H \vee K_1$.

Finally, if both H and K are normal in $\mathcal{G}$, then so is $H \vee K$. Thus we may assume (by symmetry) that

(5) H is not normal in $\mathcal{G}$, and hence $H < H_1 \leq H_{m-1} < \mathcal{G}$.

Now $\mathcal{G}$ is generated by the set union $H_1 \cup K$ by assumption (4), so we must have $x^{-1}Hx \neq H$ for some $x \in H_1 \cup K$. But $H \lhd H_1$, so $k^{-1}Hk \neq H$ for some $k \in K$.

However, $k^{-1}Hk$ is a subnormal subgroup of H_{m-1}, because

$$k^{-1}Hk \lhd k^{-1}H_1 k \lhd \ldots \lhd k^{-1}H_{m-1}k = H_{m-1}$$

as $H_{m-1} \lhd \mathcal{G}$. Applying assumption (1) with $\mathcal{G}' = H_{m-1}$, we find that $H \vee k^{-1}Hk$ is a subnormal subgroup of H_{m-1}, and hence of $\mathcal{G}$. Moreover, $H < H \vee k^{-1}Hk \leq H \vee K$, whence $(H \vee k^{-1}Hk) \vee K = H \vee K$. Using assumption (2) with $L = H \vee k^{-1}Hk$, it follows that $H \vee K = L \vee K$ is subnormal in $\mathcal{G}$, as desired.

Finally, if $H \vee K \succ H$ in $\mathcal{SN}(\mathcal{G})$, then $H \lhd H \vee K$: by the observation after the first argument, H and $H \vee K$ both subnormal and $H \leq H \vee K$ makes $H \lhd\lhd H \vee K$, and since it is a covering relation in $\mathcal{SN}(\mathcal{G})$ then $H \lhd H \vee K$. Moreover, $(H \vee K)/H$ is simple. By one of the group isomorphism theorems, $K/(H \wedge K)$ is likewise simple, so $K \succ H \wedge K$. Thus $\mathcal{SN}(\mathcal{G})$ is lower semimodular. $\square$

A maximal chain in $\mathcal{SN}(\mathcal{G})$ is called a *composition series* for $\mathcal{G}$. As $\mathcal{SN}(\mathcal{G})$ is lower semimodular, the duals of Theorems 9.4 and 9.7 yield the Jordan-Hölder structure theorem for groups.

Corollary. *If a finite group $\mathcal{G}$ has a composition series of length n,*

$$\{1\} = H_0 \lhd H_1 \lhd \ldots \lhd H_n = \mathcal{G}$$

then every composition series of $\mathcal{G}$ has length n. Moreover, if

$$\{1\} = K_0 \lhd K_1 \lhd \ldots \lhd K_n = \mathcal{G}$$

is another composition series for $\mathcal{G}$, then there is a permutation π of $\{1, \ldots, n\}$ such that $K_i/K_{i-1} \cong H_{\pi(i)}/H_{\pi(i)-1}$ for all i.

Historical note. The Jordan-Hölder theorem provides a good example of the interaction between groups and lattice theory, with a long history. For the interestd reader, the primary references are, in order, Jordan [13], Hölder [10], Dedekind [5], Schreier [18], Zassenhaus [21], and Wielandt [20]. Secondary sources are Burnside Chap. V [2], Zassenhaus Chap. II.5 [22], and Birkhoff (1963 ed.) Chap. III.7 [1]. Slick modern proofs are in Grätzer and Nation [9] and Czedli and Schmidt [4].

A *finite decomposition* of an element $a \in L$ is an expression $a = \bigwedge Q$ where Q is a finite set of meet irreducible elements. If $\mathcal{L}$ satisfies the ACC, then every element has a finite decomposition. We have seen that every element of a finite distributive lattice has a unique irredundant decomposition. In a finite dimensional modular lattice, an element can have many different finite decompositions, but the number of elements in any irredundant decomposition is always the same. This is a consequence of the following replacement property (known as the Kurosh-Ore Theorem).

Theorem 9.9. *If a is an element of a modular lattice and*

$$a = q_1 \wedge \ldots \wedge q_m = r_1 \wedge \ldots \wedge r_n$$

are two irredundant decompositions of a, then $m = n$ and for each q_i there is an r_j such that

$$a = r_j \wedge \bigwedge_{k \neq i} q_k$$

is an irredundant decomposition.

Proof. Let $a = \bigwedge Q = \bigwedge R$ be two irredundant finite decompositions (dropping the subscripts temporarily). Fix $q \in Q$, and let $\overline{q} = \bigwedge(Q - \{q\})$. By modularity, $q \vee \overline{q}/q \cong \overline{q}/q \wedge \overline{q} = \overline{q}/a$. Since q is meet irreducible in $\mathbf{L}$, this implies that a is meet irreducible in $\overline{q}/a$. However, $a = \overline{q} \wedge \bigwedge R = \bigwedge_{r \in R}(\overline{q} \wedge r)$ takes place in $\overline{q}/a$, so we must have $a = \overline{q} \wedge r$ for some $r \in R$.

Next we observe that $a = r \wedge \bigwedge(Q - \{q\})$ is irredundant. For if not, we would have $a = r \wedge \bigwedge S$ irredundantly for some proper subset $S \subset Q - \{q\}$. Reapplying

the first argument to the two decompositions $a = r \wedge \bigwedge S = \bigwedge Q$ with the element r, we obtain $a = q' \wedge \bigwedge S$ for some $q' \in Q$, contrary to the irredundance of Q.

It remains to show that $|Q| = |R|$. Let $Q = \{q_1, \ldots, q_m\}$ say. By the first part, there is an element $r_1 \in R$ such that $a = r_1 \wedge \bigwedge(Q - \{q_1\}) = \bigwedge R$ irredundantly. Applying the argument to these two decompositions and q_2, there is an element $r_2 \in R$ such that $a = r_1 \wedge r_2 \wedge \bigwedge(Q - \{q_1, q_2\}) = \bigwedge R$. Moreover, r_1 and r_2 are distinct, for otherwise we would have $a = r_1 \wedge \bigwedge(Q - \{q_1, q_2\})$, contradicting the irredundance of $a = r_1 \wedge \bigwedge(Q - \{q_1\})$. Continuing, we can replace q_3 by an element r_3 of R, distinct from r_1 and r_2, and so forth. After m steps, we obtain $a = r_1 \wedge \cdots \wedge r_m$, whence $R = \{r_1, \ldots, r_m\}$. Thus $|Q| = |R|$. $\square$

With a bit of effort, this can be improved to a *simultaneous* exchange theorem.

Theorem 9.10. *If a is an element of a modular lattice and $a = \bigwedge Q = \bigwedge R$ are two irredundant finite decompositions of a, then for each $q \in Q$ there is an $r \in R$ such that*
$$a = r \wedge \bigwedge(Q - \{q\}) = q \wedge \bigwedge(R - \{r\}).$$

The proof of this, and much more on the general theory of decompositions in lattices, can be found in Crawley and Dilworth [3]; see also Dilworth [7].

Now Theorems 9.9 and 9.10 are exactly what we want in a finite dimensional modular lattice. However, in algebraic modular lattices, finite decompositions into meet irreducible elements need not coincide with the (possibly infinite) decomposition into completely meet irreducible elements given by Birkhoff's Theorem. Consider, for example, the chain $\mathcal{C} = (\omega + 1)^d$, the dual of $\omega + 1$. This satisfies the ACC, and hence is algebraic. The least element of $\mathcal{C}$ is meet irreducible, but not completely meet irreducible. In the direct product $\mathcal{C}^n$, the least element has a finite decomposition into n meet irreducible elements, but every decomposition into completely meet irreducibles is necessarily infinite.

Fortunately, the proof of Theorem 9.9 adapts nicely to give us a version suitable for algebraic modular lattices.

Theorem 9.11. *Let a be an element of a modular lattice. If $a = \bigwedge Q$ is a finite, irredundant decomposition into completely meet irreducible elements, and $a = \bigwedge R$ is another decomposition into meet irreducible elements, then there exists a finite subset $R' \subseteq R$ with $|R'| = |Q|$ such that $a = \bigwedge R'$ irredundantly.*

The application of Theorem 9.11 to subdirect products is immediate.

Corollary. *Let $\mathcal{A}$ be an algebra such that $\mathbf{Con}\,\mathcal{A}$ is a modular lattice. If $\mathcal{A}$ has a finite subdirect decomposition into subdirectly irreducible algebras, then every irredundant subdirect decomposition of $\mathcal{A}$ into subdirectly irreducible algebras has the same number of factors.*

A more important application is to the theory of direct decompositions of congruence modular algebras. The corresponding congruences form a complemented

sublattice of **Con** $\mathcal{A}$. This subject is treated thoroughly in Chapter 5 of McKenzie, McNulty and Taylor [15].

Let us close this section by mentioning a nice combinatorial result about finite modular lattices, due to R. P. Dilworth [6].

Theorem 9.12. *In a finite modular lattice $\mathcal{L}$, let $J_k(\mathcal{L})$ be the set of elements that cover exactly k elements, and let $M_k(\mathcal{L})$ be the set of elements that are covered by exactly k elements. Then $|J_k(\mathcal{L})| = |M_k(\mathcal{L})|$ for any integer $k \geq 0$.*

In particular, the number of join irreducible elements in a finite modular lattice is equal to the number of meet irreducible elements. In fact, Joseph Kung proved that in a finite modular lattice, there is a bijection $m : J(\mathcal{L}) \cup \{0\} \to M(\mathcal{L}) \cup \{1\}$ such that $x \leq m(x)$; see Kung [14] and Reuter [17].

We will return to modular lattices in Chapter 12. The standard reference for semimodular lattices is the book by Manfred Stern [19].

Exercises for Chapter 9

1. (a) Prove that a lattice $\mathcal{L}$ is distributive if and only if it has the property that $a \vee c = b \vee c$ and $a \wedge c = b \wedge c$ imply $a = b$.

(b) Show that $\mathcal{L}$ is modular if and only if, whenever $a \geq b$ and $c \in L$, $a \vee c = b \vee c$ and $a \wedge c = b \wedge c$ imply $a = b$.

2. Show that every finite dimensional distributive lattice is finite.

3. Prove that if a finite dimensional lattice is both upper and lower semimodular, then it is modular.

4. Prove that the following conditions are equivalent for a strongly atomic, algebraic lattice.

   (i) $\mathcal{L}$ is semimodular: $a \succ a \wedge b$ implies $a \vee b \succ b$.

   (ii) If a and b both cover $a \wedge b$, then $a \vee b$ covers both a and b.

   (iii) If b and c are incomparable and $b \wedge c < a < c$, then there exists x such that $b \wedge c < x \leq b$ and $a = c \wedge (a \vee x)$.

5. Let $\mathcal{L}$ be a finite length semimodular lattice, and let C be any maximal chain in $\mathcal{L}$. Prove that any congruence relation on $\mathcal{L}$ is uniquely determined by its restriction to C. (Use Theorem 9.7) (George Grätzer)

6. Let a and b be elements of a finite dimensional semimodular lattice, and let $\nu_b : a/(a \wedge b) \to (a \vee b)/b$ by $\nu_b(x) = x \vee b$. Show that ν_b is a join embedding, i.e., one-to-one and join-preserving.

7. (a) Find infinitely many simple modular lattices of width 4.

(b) Prove that the variety generated by all lattices of width ≤ 4 contains subdirectly irreducible lattices of width ≤ 4 only.

8. Prove that every arguesian lattice is modular.

9. Let $\mathcal{L}$ be a lattice, and suppose there exist an ideal I and a filter F of $\mathcal{L}$ such that $L = I \cup F$ and $I \cap F \neq \emptyset$.

   (a) Show that $\mathcal{L}$ is distributive if and only if both I and F are distributive.

(b) Show that $\mathcal{L}$ is modular if and only if both I and F are modular.

(R. P. Dilworth)

10. Show that modular lattices satisfy the equation

$$x \wedge (y \vee (z \wedge (x \vee t))) = x \wedge (z \vee (y \wedge (x \vee t))).$$

11. Let C and D be two chains in a modular lattice $\mathcal{L}$. Prove that $C \cup D$ generates a distributive sublattice of $\mathcal{L}$. (Bjarni Jónsson)

12. Let a and b be two elements in a modular lattice $\mathcal{L}$ such that $a \wedge b = 0$. Prove that the sublattice generated by $\downarrow a \cup \downarrow b$ is isomorphic to the direct product $\downarrow a \times \downarrow b$.

13. Prove Theorem 9.11. (Mimic the proof of Theorem 9.9.)

14. Let $\mathcal{A} = \prod_{i \in \omega} \mathbb{Z}_2$ be the direct product of countably many copies of the two element group. Describe two decompositions of 0 in **Sub** $\mathcal{A}$, say $0 = \bigwedge Q = \bigwedge R$, such that $|Q| = \aleph_0$ and $|R| = 2^{\aleph_0}$.

References

1. G. Birkhoff, *Lattice Theory*, First edition, Colloquium Publications, vol. 25, Amer. Math. Soc., Providence, R. I., 1940.
2. W. Burnside, *Theory of Groups of Finite Order*, Reprinted by Dover Publications, New York, 1955, Cambridge University Press, Cambridge, 1911.
3. P. Crawley and R. P. Dilworth, *Algebraic Theory of Lattices*, Prentice-Hall, Englewood Cliffs, N. J., 1973.
4. G. Czedli and E.T. Schmidt, *The Jordan-Hölder theorem with uniqueness for groups and semimodular lattices*, Algebra Universalis (2011).
5. R. Dedekind, *Über die von drei Moduln erzeugte Dualgruppe gemeinsamen Teiler*, Math. Annalen **53** (1900), 371–403, reprinted in Gesammelte mathematische Werke, Vol. 2, pp. 236–271, Chelsea, New York, 1968.
6. R. P. Dilworth, *Proof of a conjecture on finite modular lattices*, Ann. of Math. **60** (1954), 359–364.
7. R. P. Dilworth, *Structure and Decomposition Theory*, Proceedings of Symposia on Pure Mathematics: Lattice Theory, vol. II, Amer. Math. Soc., Providence, R. I., 1961.
8. G. Grätzer, *Equational classes of lattices*, Duke Jour. Math. **33** (1966), 613–622.
9. G. Grätzer and J.B. Nation, *A new look at the Jordan-Hölder theorem for semimodular lattices*, Algebra Universalis **64** (2011), 309–311.
10. O. Hölder, *Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen*, Math. Ann. **34** (1889), 33 ff..
11. B. Jónsson, *Equational classes of lattices*, Math. Scand. **22** (1968), 187–196.
12. B. Jónsson and I. Rival, *Lattice varieties covering the smallest non-modular variety*, Pacific J. Math. **82** (1979), 463–478.
13. C. Jordan, *Traité des substitutions et des équations algébiques*, Gauthier-Villars, Paris, 1870.
14. J.P.S. Kung, *Matchings and Radon transforms in lattices, I: Consisent lattices*, Order **2** (1985), 105–112.
15. R. McKenzie, G. McNulty and W. Taylor, *Algebras, Lattices, Varieties*, vol. I, Wadsworth and Brooks-Cole, Belmont, CA, 1987.
16. J. B. Nation, *A counterexample to the finite height conjecture*, Order **13** (1996), 1–9.

17. K. Reuter, *Matchings for linearly indecomposable modular lattices*, Discrete Math. **63** (1987), 245–249.
18. O. Schreier, *Über den J-H'schen Satz*, Abh. Math. Sem. Univ. Hamburg **6** (1928), 300–302.
19. M. Stern, *Semimodular Lattices: Theory and Applications*, Cambridge University Press, Cambridge, 1999.
20. H. Wielandt, *Eine Verallgemeinerung der invarianten Untergruppen*, Math. Zeit. **45** (1939), 209–244.
21. H. Zassenhaus, *Zum Satz von Jordan-Hölder-Schreier*, Abh. Math. Sem. Univ. Hamburg **10** (1934), 106–108.
22. H. Zassenhaus, *Theory of Groups*, 2nd. ed. 1958, Chelsea, 1949.