n-distributive lattices versus projective geometries

Gábor Czédli (Szeged)

1. Rudiments on lattices

By a *partially ordered set*, shortly *poset*, we mean a pair $(L, \leq)$ where "$\leq$" is a reflexive (i.e, $(\forall x \in L)(x \leq x)$), antisymmetric $((\forall x, y \in L)(x \leq y \;\&\; y \leq x \implies x = y))$ and transitive $((\forall x, y, z \in L)(x \leq y \;\&\; y \leq z \implies x \leq z))$ relation on the non-empty set L. If $\emptyset \neq H \subseteq L$, $a \in L$ and for any $h \in H \quad a \leq h$ then a is a *lower bound* of H. If for any other lower bound b of H we have $b \leq a$ then a is called *the greatest lower bound* or *meet* or *infimum* of H. In this case the following notations apply: $a = \inf H$, $\quad a = \bigwedge H$, $a = \bigwedge_{h \in H} h$, and even $a = h_1 \wedge h_2 \wedge \ldots \wedge h_n$ when $H = \{h_1, h_2, \ldots, h_n\}$. The concept of *the least upper bound* or *join* or *supremum* is defined dually and is denoted by $\sup H$, $\bigvee H$, $\quad \bigvee_{h \in H} h$, and $h_1 \vee h_2 \vee \ldots \vee h_n$ when $H = \{h_1, h_2, \ldots, h_n\}$. Note that $\bigwedge H$ and $\bigvee H$ need not exist but if they do then they are uniquely determined.

If $a \wedge b$ and $a \vee b$ exist for any $a, b \in L$ then L is called a *lattice*. If $\sup H$ and $\inf H$ exist for any non-empty subset H of L then L is called a *complete lattice*. In a laticce $L \quad \wedge$ and $\vee$ can be considered as binary operations. Both operations are commutative, associative, idempotent (i.e., $x \wedge x = x = x \vee x$) and they obey the *absorption laws* $x \wedge (x \vee y) = x$ and $x \vee (x \wedge y) = x$.

Example 1. For a set A let $\mathcal{P}(A)$ denote the set of all subsets of A. Then $(\mathcal{P}(A), \subseteq)$ is a complete lattice. In this lattice the $\bigwedge$ and $\bigvee$ coincide with the intersection $\bigcap$ and the union $\bigcup$, respectively.

Example 2. Let $|$ denote the divisibility relation on the set $\mathrm{N} = \{1, 2, 3, \ldots\}$ of natural numbers. I.e., $a \mid b \iff (\exists c \in \mathrm{N})(ac = b)$. Then $(\mathrm{N}, |)$ is a complete lattice where the join and meet are the least common multiple and the greatest common divisor, respectively. This lattice is not complete; e.g. $\bigvee \mathrm{N}$ does not exist.

If $L = (L, \leq)$ is a poset, $a \in L$ and a is an upper bound of L then a is called the greatest element of L and is denoted by 1 or 1_L. If 1_L exists then it is uniquely determined. The dual notion, the smallest element of L is denoted by $0 = 0_L$. We will write $a < b$, $a \geq b$ and $a > b$ to denote $a \leq b \;\&\; a \neq b$, $b \leq a$ and $b < a$, respectively. If $a < b$ but $a < c < b$ holds for no $c \in L$ then we say that b *covers* a, in notation $a \prec b$. A finite poset is uniquely determined by the covering relation $\prec$. This allows us to give a finite poset, in particular a finite lattice, by its *Hasse diagram*. The diagram of a poset L is a graph in wich the vertices represent the elements of L and the edges represent the covering relation. If $a \prec b$ in L then the vertex representing a is placed lower then the vertex representing b and these two vertices are connected by an edge. For $A = \{a, b, c\}$ the lattice $\mathcal{P}(A)$ from

TEMPUS JEP-0153 LECTURE SERIES

n-distributive lattices versus projective geometries

held in Potenza, May 18–30, 1992

by

Gábor Czédli (Szeged)

1. Rudiments on lattices

By a *partially ordered set*, shortly *poset*, we mean a pair $(L, \leq)$ where "$\leq$" is a reflexive (i.e, $(\forall x \in L)(x \leq x)$), antisymmetric $((\forall x, y \in L)(x \leq y \ \&\ y \leq x \implies x = y))$ and transitive $((\forall x, y, z \in L)(x \leq y \ \&\ y \leq z \implies x \leq z))$ relation on the non-empty set L. If $\emptyset \neq H \subseteq L$, $a \in L$ and for any $h \in H \quad a \leq h$ then a is a *lower bound* of H. If for any other lower bound b of H we have $b \leq a$ then a is called *the greatest lower bound* or *meet* or *infimum* of H. In this case the following notations apply: $a = \inf H$, $\quad a = \bigwedge H$, $a = \bigwedge_{h \in H} h$, and even $a = h_1 \wedge h_2 \wedge \ldots \wedge h_n$ when $H = \{h_1, h_2, \ldots, h_n\}$. The concept of *the least upper bound* or *join* or *supremum* is defined dually and is denoted by $\sup H$, $\bigvee H$, $\quad \bigvee_{h \in H} h$, and $h_1 \vee h_2 \vee \ldots \vee h_n$ when $H = \{h_1, h_2, \ldots, h_n\}$. Note that $\bigwedge H$ and $\bigvee H$ need not exist but if they do then they are uniquely determined.

If $a \wedge b$ and $a \vee b$ exist for any $a, b \in L$ then L is called a *lattice*. If $\sup H$ and $\inf H$ exist for any non-empty subset H of L then L is called a *complete lattice*. In a laticce $L \quad \wedge$ and $\vee$ can be considered as binary operations. Both operations are commutative, associative, idempotent (i.e., $x \wedge x = x = x \vee x$) and they obey the *absorption laws* $x \wedge (x \vee y) = x$ and $x \vee (x \wedge y) = x$.

Example 1. For a set A let $\mathcal{P}(A)$ denote the set of all subsets of A. Then $(\mathcal{P}(A), \subseteq)$ is a complete lattice. In this lattice the $\bigwedge$ and $\bigvee$ coincide with the intersection $\bigcap$ and the union $\bigcup$, respectively.

Example 2. Let $\mid$ denote the divisibility relation on the set $\mathbf{N} = \{1, 2, 3, \ldots\}$ of natural numbers. I.e., $a \mid b \iff (\exists c \in \mathbf{N})(ac = b)$. Then $(\mathbf{N}, \mid)$ is a complete lattice where the join and meet are the least common multiple and the greatest common divisor, respectively. This lattice is not complete; e.g. $\bigvee \mathbf{N}$ does not exist.

If $L = (L, \leq)$ is a poset, $a \in L$ and a is an upper bound of L then a is called the greatest element of L and is denoted by 1 or 1_L. If 1_L exists then it is uniquely determined. The dual notion, the smallest element of L is denoted by $0 = 0_L$. We will write $a < b$, $a \geq b$ and $a > b$ to denote $a \leq b \ \&\ a \neq b$, $b \leq a$ and $b < a$, respectively. If $a < b$ but $a < c < b$ holds for no $c \in L$ then we say that b *covers* a, in notation $a \prec b$. A finite poset is uniquely determined by the covering relation $\prec$. This allows us to give a finite poset, in particular a finite lattice, by its *Hasse diagram*. The diagram of a poset L is a graph in wich the vertices represent the elements of L and the edges represent the covering relation. If $a \prec b$ in L then the vertex representing a is placed lower then the vertex representing b and these two vertices are connected by an edge. For $A = \{a, b, c\}$ the lattice $\mathcal{P}(A)$ from

Example 1 is depicted on Figure 1. (Figures are at the end of the paper.) The diagram of a poset determines L in the following way: $a \leq b$ iff there is an ascending path (maybe of length 0) from a to b in the diagram.

If L is a lattice and $0, 1 \in L$ exist then L is called a *bounded lattice*. Note that every finite lattice is bounded while the lattice $(\mathbf{N}, |)$ of Example 2 is not. The elements covering 0 in a bounded lattice are called *atoms*. If $a \wedge b = 0$ and $a \vee b = 1$ then b is called a *complement* of a. An element in a bounded lattice need not have a complement and, if exists, the complement need not be unique, as illustrated in Figure 2. If each element of L has at least one complement then L is said to be a *complemented lattice*. E.g., $(\mathcal{P}(A), \subseteq)$ is a complemented lattice where, for $X \subseteq A$, $A \setminus X$ is the (unique) complement of X.

A subset C of a poset L is called a *chain* if for any $x, y \in L \quad x \leq y$ or $y \leq x$. If C is a chain in L and for any $a \in L \setminus C \quad C \cup \{a\}$ is not a chain then C is called a *maximal chain* in L.

An important but quite evident observation on lattices is that any notion or statement has its dual counterpart, which is obtained via replacing $\leq$ by $\geq$. E.g., the dual of infimum is supremeum, the dual of 1 is 0, the dual of a chain or poset or lattice is itself, etc. The *Duality Principle* states that if a statement is true for lattices then so is the dual statement. (Indeed, by dualizing the proof of the original statement we obtain a proof of the dual one.)

We have not seen too many examples of lattices so far. This will be remedied by

Theorem 1. If a poset L has a greatest element and for any non-empty subset H of $L \quad \bigwedge H$ exists then L is a complete lattice.

Proof. We need to show the existence of suprema. Let H be a non-empty subset of L. Denote the set of upper bounds of H by X. Since $1 \in X$, X is not empty and $c = \bigwedge X$ exists. Given an $h \in H$, $h \leq x$ holds for every $x \in X$ by the definition of X. Thus h is a lower bound of X, yielding $h \leq \bigwedge X = c$. Since this is true for any h, c is an upper bound of H. On the other hand, for any other upper bound d of $H \quad d \in X \implies c \leq d$, whence c is the least upper bound, alias supremum, of H. ■

Example 3.

$(\mathcal{N}(G), \subseteq)$ where $\mathcal{N}(G)$ is the set of normal subgroups of a given group G,
$(\mathrm{Sub}(G), \subseteq)$ where $\mathrm{Sub}(G)$ is the set of subgroups of a given group G,
$(\mathcal{I}(R), \subseteq)$ where $\mathcal{I}(R)$ is the set of ideals of a given ring R, and
$(\mathrm{Sub}(V), \subseteq)$ where $\mathrm{Sub}(V)$ is the set of subspaces of a given vector space V, etc.
are complete lattices.

These examples demonstrate that lattices frequently occur as "companion stuctures". With the help of Theorem 1 we show that $(\mathcal{N}(G), \subseteq)$ is a complete lattice; the rest of these examples can be verified the same way. Let $H = \{B_i : i \in I\}$ be a set of normal subgroups of G. It is well-known (and this is the key property wich makes our example a complete lattice) that the set-theoretic intersection $B = \bigcap_{i \in I} B_i$ is also a normal subgroup of G. Hence B belongs to $\mathcal{N}(G)$. Since $B \subseteq B_i$ for all $i \in I$, B is a lower bound of H. If C is another lower bound of H then $(\forall i \in I)(C \subseteq B_i)$ implies $C \subseteq B$. Hence B is the greatest lower bound of H, i.e., $B = \bigwedge H$. Since G is the greates element of $\mathcal{N}(G)$, Theorem 1 applies and $(\mathcal{N}(G), \subseteq)$ is a complete lattice indeed.

2. Rudiments on projective geometry

Consider a triple $G = (P, L, \mathbf{I})$ where P is a non-empty set (its element are called points), L is an arbitrary set (its elements are called lines) and $\mathbf{I} \subseteq P \times L$. $\mathbf{I}$ is called the incidence relation and $p \mathbf{I} \ell$ is also worded as p is on the line ℓ or ℓ goes through the point p. G is called a *projective geometry* if the following three axioms are fulfilled:

(i) Each line $\ell \in L$ goes through at least two distinct points $p_1, p_2 \in P$;

(ii) For any two distinct points $p \neq q \in P$ there exists exactly one line $\ell \in L$ which goes through p and q (this line will be denoted by ℓ_{pq}).

(iii) For any points $p, q, r, x, y \in P$ and any lines $\ell_1, \ell_2 \in L$ satisfying $p \mathbf{I} \ell_1$, $q \mathbf{I} \ell_1$, $x \mathbf{I} \ell_1$, $p \mathbf{I} \ell_2$, $r \mathbf{I} \ell_2$ and $y \mathbf{I} \ell_2$ there exist lines ℓ_3, $\ell_4 \in L$ and a point $z \in P$ such that $q \mathbf{I} \ell_3$, $r \mathbf{I} \ell_3$, $z \mathbf{I} \ell_3$, $x \mathbf{I} \ell_4$, $y \mathbf{I} \ell_4$ and $z \mathbf{I} \ell_4$ (cf. Figure 3).

In particular (when no points and lines in Figure 3 coincide), (iii) yields that if a line ℓ_4 intersects two sides (namely ℓ_1 and ℓ_2) of a triangle (whose vertices are p, q, r) then it has to intersect the third side (namely ℓ_3) of this triangle. This is the so-called *Pasch Axiom.*

Given a projective geometry $G = (P, L, \mathbf{I})$, a subset H of P is called a subspace if for any two *distinct* points $p, q \in X$ and any $r \in P$ if r is on the line ℓ_{pq} then $r \in X$. In particular, P, any one-element subset of P and the $\emptyset$ are subspaces. It is easy to see that the intersection of an arbitrary family of subspaces is a subspace again. This has two important consequences. Firstly, for any $H \subseteq P$ we may speak of the subspace $[H]$ *spanned* by H, this is the intersection of all subspaces including H. Secondly, if $\mathcal{L}(G)$ is the set of all subspaces of G then $\mathcal{L}(G) = (\mathcal{L}(G), \subseteq)$ is a complete lattice. (This follows from Theorem 1 the same way as for normal subgroups previously.)

For later references we need an explicit description of the join in $\mathcal{L}(G)$. If $X, Y \in \mathcal{L}(G)$ then

$$X \vee Y = X \cup Y \cup \{r \in P : (\exists p \in X)(\exists q \in Y)(p \neq q \;\&\; r \mathbf{I} \ell_{pq})\}.$$

Note that this is a statement not a definition! However, this course is mainly on lattices not on projective geometries, so we do not prove it. (The only non-trivial step in the proof is to show that the set on the right-hand side is a subspace.) For later references we formulate the

Exchange Property. If X is a subspace and p, q are points of a projective geometry G such that $q \in X \vee \{p\}$ and $q \notin X$ then $p \in X \vee \{q\}$. (The join is understood in $\mathcal{L}(G)$.)

Proof. We may assume that $p \neq q$. Clearly, $p \notin X$. By the description of join in $\mathcal{L}(G)$ there is a point $r \in X$ such that $q \mathbf{I} \ell_{rp}$, cf. Figure 4. Since $r \neq q$ by $q \notin X$, we infer $\ell_{rp} = \ell_{rq}$. Therefore $p \mathbf{I} \ell_{rq} = \ell_{rp}$, and $p \in X \vee \{q\}$ follows from the description of join. ■

A projective geometry is called *finite dimensional* if $P = [H]$ for some finite $H \subseteq P$. If $[\{a_0, a_1, \ldots, a_n\}] = P$ and, for $i = 0, 1, \ldots, n$, $a_i \notin [\{a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n\}]$ then we say that the points $a_0, a_1, \ldots, a_n$ form a *basis* in G. It is easy to see that if G is finite dimensional than it has a finite basis. (Indeed, start from a finite H with $[H] = P$ and omit the "superfluous" points from H.) The dimension of G is defined to be the smallest n such that G has an n-element basis. (It is known that the number of elements in a basis is unique. Yet, we will not use this fact in the sequel. We will deduce it from certain properties of $\mathcal{L}(G)$, i.e., with the help of lattice theory.)

3. Properties of $\mathcal{L}(G)$

Lemma 1. For any projective space G, $\mathcal{L}(G)$ is a complemented lattice.

Proof. Let $X \in \mathcal{L}(G)$ and consider the poset $H = (\{Y \in \mathcal{L}(G) : X \cap Y = \emptyset\}, \subseteq)$. H is not empty as $\emptyset \in H$. If $C = \{Y_i : i \in I\}$ is a chain in H then put $Z = \bigcup_{i \in I} Y_i$. We claim that $Z \in \mathcal{L}(G)$. Suppose $p \neq q \in Z$ and a point r is on the line ℓ_{pq}, we have to show that $r \in Z$. Now $p \in Y_i$ and $q \in Y_j$ for some $i, j \in I$. Since C is a chain, $Y_i \subseteq Y_j$ can be assumed. Then $p, q \in Y_j$ and $r \in Y_j \subseteq Z$ follows from the fact that Y_j is a subspace. Thus $Z \in \mathcal{L}(G)$, and Z is evidently an uper bound of C. Therefore Zorn's Lemma applies and H has a maximal element. Let Y denote a maximal element of H. We claim that Y is a complement of X. Since $Y \in H$, $X \wedge Y = X \cap Y = \emptyset$. Suppose $X \vee Y \neq P$, and choose a point $p \notin X \vee Y$. Then $Y \subset Y \vee \{p\}$ and the maximality of Y gives $X \cap (Y \vee \{p\}) \neq \emptyset$. So we can choose a point q from $X \cap (Y \vee \{p\})$. Now $q \in Y \vee \{p\})$ and, by $X \cap Y = \emptyset$, $q \notin Y$. The Exchange Property yields $p \in Y \vee \{q\} \subseteq Y \vee X = X \vee Y$, a contradiction. ■

A lattice L is called *modular* if for any $x, y, z \in L$

$$x \leq z \implies (x \vee y) \wedge z = x \vee (y \wedge z).$$

Sometimes we use modularity on complicated expressions where the subterms corresponding to x, y and z may occur in different order (as the operations are commutative). Therefore it is worth adopting the following convention: whenever the modular law is applied then (before its application, i.e. on the left-hand side of the "=") x is underlined and z is doubly underlined. E.g., we may write

$$\underline{(a \wedge x)} \vee (\underline{\underline{(a \vee b \vee c)}} \wedge (x \wedge z)) = (a \vee b \vee z) \wedge ((a \wedge x) \vee (x \wedge z)).$$

(Here we used modularity "from right to left" with $a \wedge x$, $x \wedge z$ and $a \vee b \vee z$ acting as x, y, z, respectively.)

Another important class of lattices is the class of distributive lattices. A lattice L is called *distributive*, if $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ holds for any $x, y, z \in L$. It is an easy exercise to prove that any distributive lattice obeys the dual law $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ and any distributive lattice is modular.

A non-empty subset H of a latice L is called a sublattice if $(\forall x, y \in H)(x \wedge y \in H \;\&\; x \vee y \in H)$. (It is important to point out that here the meet and join are taken in L not in H.) Two lattices, L_1 and L_2, are said to be *isomorphic* if there is a bijection $\alpha\colon L_1 \to L_2$ such that $(\forall x, y \in L_1)(x \leq y \iff x\alpha \leq y\alpha)$. An equivalent definition: $L_1 \cong L_2$ iff there are monotone maps $\alpha\colon L_1 \to L_2$ and $\beta\colon L_2 \to L_1$ such that $\alpha\beta$ is the identical map on L_1 and $\beta\alpha$ is the identical map on L_2. Modularity can be characterized by sublattices:

Dedekind's Modularity Criterion. A lattice L is modular iff no sublattice of L is isomorphic to N_5 (cf. Figure 5).

For example, L_1 on Figure 6 is modular (and even distributive) while L_2 is not modular as the indicated elements form a sublattice isomorphic to N_5.

Lemma 2. For any projective geometry $G = (P, L, \mathbf{I})$, $\mathcal{L}(G)$ is modular

Proof. Let $X, Y, Z \in \mathcal{L}(G)$ with $X \le Z$, i.e., $X \subseteq Z$. First we show $(X \vee Y) \wedge Z \subseteq X \vee (Y \wedge Z)$. Let $p \in (X \vee Y) \wedge Z$. We may assume that $p \notin X$ and $p \notin Y$ as otherwise $p \in X \cup (Y \cap Z) \subseteq X \vee (Y \wedge Z)$. Then there are distinct points $x \in X$ and $y \in Y$ such that $p \,\mathbf{I}\, \ell_{xy}$. Now x, y, p are three distinct points on the same line. Since $x \in X \subseteq Z$ and $p \in Z$, $y \in Z$. Hence $y \in Y \cap Z = Y \wedge Z$ and $p \in X \vee (Y \wedge Z)$.

The converse inclusion "$\supseteq$" will be shown in a much more general setting. Namely, we show that every lattice satisfies the so-called *modular inequality*

$$x \le z \implies (x \vee y) \wedge z \ge x \vee (y \wedge z).$$

Indeed, we have to use only the definition of the operations to argue as follows: $x \vee y \ge x$ and $z \ge x$ yield $(x \vee y) \wedge z \ge x$, $x \vee y \ge y \ge y \wedge z$ and $z \ge y \wedge z$ imply $(x \vee y) \wedge z \ge y \wedge z$, and now we conclude the desired inequality. ∎

4. More about modular lattices

Given a lattice L and $a \le b \in L$, the set $\{x \in L : a \le x \le b\}$ is called the *interval* determined by a and b and is denoted by $[a, b]$. Clearly, any interval is a sublattice of L.

Theorem 2. (The Isomorphism Theorem for Modular Lattices) If L is a modular lattice and $a, b \in L$ then the intervals $[a \wedge b, a]$ and $[b, a \vee b]$ are isomorphic. The map $\alpha\colon [a \wedge b, a] \to [b, a \vee b]$, $x \mapsto x \vee b$ is a lattice isomorphism whose inverse is $\beta\colon [b, a \vee b] \to [a \wedge b, a]$, $y \mapsto y \wedge a$ (cf. Figure 7).

Proof. α is clearly monotone, i.e., $x_1 \le x_2 \implies x_1\alpha \le x_2\alpha$, and so is β. By the absorption law, $(a \wedge b)\alpha = b$ and $a\alpha = a \vee b$. Since α is monotone, it maps $[a \wedge b, a]$ into $[b, a \vee b]$. Similarly, β maps $[b, a \vee b]$ into $[a \wedge b, a]$. For $x \in [a \wedge b, a]$ we have $x(\alpha\beta) = (x\alpha)\beta = (x \vee b)\beta = (\underline{x} \vee b) \wedge \underline{\underline{a}} = x \vee (a \wedge b) = x$, thus $\alpha\beta$ is the identical map, and so is β by duality. ∎

If C is a chain then $|C| - 1$ is called te length of C. E.g., the length of $\{0, a, 1\}$ in Figure 2 is 2. The length of a lattice L is defined to be the supremum of $\{|C| : C$ is a chain in $L\}$, this is a non-negative integer or ∞.

Theorem 3. (Jordan –Hölder Chain Condition for Modular Lattices) If L is a modular lattice of finite length then any two maximal chains in L have the same length.

Proof. Consider a maximal chain $C = \{c_0 < c_1 < \cdots < c_n\}$ in L. Since C is maximal, $0 = c_0 \prec c_1 \cdots \prec c_n = 1$. (In fact, this is equivalent to the maximality of C.)

E.g., if c_0 were not the least element of L then $c_0 \not\leq a$ would hold for some $a \in L$ and $c_0 \wedge a < c_0 < \cdots < c_n$ would be a larger chain. Via induction on n we are going to show that for any maximal chain $\{0 = d_0 \prec d_1 \prec \cdots \prec d_k = 1\}$ $k = n$. If $n = 0$ or $n = 1$ then $|L| = n + 1$ and C is the only maximal chain L. Assume, as an induction hypotheses, that the theorem holds for all modular lattices having at least one maximal chain shorter than n. First, let us consider the case $c_1 \neq d_1$, cf. Figure 8. Put $e_2 = c_1 \vee d_1$, and consider a maximal chain $\{e_2 \prec e_3 \prec \cdots \prec e_t = 1\}$ in the interval $[e_2, 1]$. Since the intersection of any two distinct atoms is zero, the Isomorhism Theorem yields $[0, c_1] \cong [d_1, e_2]$ and $[0, d_1] \cong [c_1, e_2]$. Therefore e_2 covers c_1 and d_1. Applying the induction hypothesis to the interval $[c_1, 1]$ we infer that the length $t - 1$ of the maximal chain $\{c_1 \prec e_2 \prec e_3 \cdots \prec e_t\}$ is $n - 1$. Therefore $t = n$. Since $\{d_1 \prec e_2 \prec e_3 \prec \cdots \prec e_t = 1\}$ is a maximal chain of length $t - 1 = n - 1$ again, the induction hypothesis applies to the interval $[d_1, 1]$ and implies that the length $k - 1$ of the maximal chain $\{d_1 \prec d_2 \cdots \prec d_k\}$ is $n - 1$. Hence $k = n$, indeed. The second case, when $c_1 = d_1$ is much simpler: we can apply the induction hypothesis to the maximal chain $\{d_1 \prec d_2 \prec \cdots \prec d_k\}$ in the interval $[c_1, 1]$ and conclude $k = n$. ■

In a modular lattice L of finite length we define the *height* $h(a)$ of an element $a \in L$ as the length of $[0, a]$. By the previous theorem, $h(a)$ is the length of *any* maximal chain between 0 and a.

Theorem 4. If a, b are elements in a modular lattice of finite length then $h(a) + h(b) = h(a \wedge b) + h(a \vee b)$.

Proof. Let $0 = x_0 \prec x_1 \prec \cdots \prec x_n = a \wedge b$, $a \wedge b = y_0 \prec y_1 \prec \cdots \prec y_m = a$ and $a \wedge b = z_0 \prec z_1 \prec \cdots \prec z_k = b$ be maximal chains in the intervals $[0, a \wedge b]$, $[a \wedge b, a]$ and $[a \wedge b, b]$, respectively (cf. Figure 9). In particular, $h(a \wedge b) = n$. By the isomorphism theorem, $b = y_0 \alpha \prec y_1 \alpha \prec \cdots \prec y_m \alpha = a \vee b$ is a maximal chain in $[b, a \vee b]$. Now the chains $0 = x_0 \prec x_1 \prec \cdots \prec x_n = a \wedge b = y_0 \prec y_1 \prec \cdots \prec y_m = a$, $0 = x_0 \prec x_1 \prec \cdots \prec x_n = a \wedge b = z_0 \prec z_1 \prec \cdots \prec z_k = b$ and $0 = x_0 \prec x_1 \prec \cdots \prec x_n = a \wedge b = z_0 \prec z_1 \prec \cdots \prec z_k = b = y_0 \alpha \prec y_1 \alpha \prec \cdots \prec y_m \alpha = a \vee b$ are maximal in the interval determined by their first and last members, whence $h(a) = n + m$, $h(b) = n + k$, $h(a \vee b) = n + k + m$, and the theorem follows. ■

Lemma 3. Let $a_1, a_2, \ldots, a_n$ be atoms in a modular lattice such that, for $1 \leq i \leq n$, $a_1 \vee \ldots \vee a_{i-1} \vee a_{i+1} \ldots \vee a_n \neq a_1 \vee a_2 \vee \ldots \vee a_n$. then $h(a_1 \vee a_2 \vee \ldots \vee a_n) = n$.

Proof. The statement is evident for $n \leq 1$. Assume that it is true for the join of $n-1$ atoms. Since $a_1 \vee a_2 \vee \ldots \vee a_{n-1} \neq a_1 \vee a_2 \vee \ldots \vee a_n$, $a_n \not\leq a_1 \vee a_2 \vee \ldots \vee a_{n-1}$. Thus $a_n \wedge (a_1 \vee a_2 \vee \ldots \vee a_{n-1}) < a_n$, so $a_n \wedge (a_1 \vee a_2 \vee \ldots \vee a_{n-1}) = 0$ as a_n is an atom. Therefore, applying the induction hypothesis and Theorem 4, we can compute: $h(a_1 \vee a_2 \vee \ldots \vee a_n) = h(a_1 \vee a_2 \vee \ldots \vee a_{n-1}) + h(a_n) - h((a_1 \vee a_2 \vee \ldots \vee a_{n-1}) \wedge a_n) = (n-1) + 1 - h(0) = n$. ■

Lemma 4. Let $a \leq b$ in a modular lattice. Then $h(a) = h(b) \implies a = b$ and $h(a) = h(b) - 1 \implies a \prec b$.

Proof. Obvious by definitions and Theorem 3. ■

A lattice is called relatively complemented if any of its intervals is a complemented lattice.

Theorem 5. Every complemented modular lattice is relatively complemented.

Proof. Let $[a, b]$ be an interval and let $x \in [a, b]$. By the assumption, x has a complement $y \in L$. Since $\underline{x} \vee ((a \vee y) \wedge \underline{b}) = (x \vee (a \vee y)) \wedge b = ((x \vee a) \vee y)) \wedge b = (x \vee y) \wedge b = 1 \wedge b = b$ and $x \wedge ((a \vee y) \wedge b) = (x \wedge \overline{b}) \wedge (a \vee y) = \underline{\underline{x}} \wedge (\underline{a} \vee y) = (x \wedge y) \vee a = 0 \vee a = a$, $((a \vee y) \wedge b)$ is a relative complement of x in $[a, b]$. ■

5. A lattice characterization of projective geometries

For a modular lattice M let P be the set of atoms in M, let $L = \{a \vee b : a, b \in P,\ a \neq b\}$, and define $\mathcal{G}(M)$ as $(P, L, \leq)$. According to the following theorem, the study of projective geometries is equivalent to that of complemented modular lattices.

Theorem 6. Let n be a natural number. If G is an n-dimensional projective geometry then $\mathcal{L}(G)$ is a complemented modular lattice of length $n+1$ and $G \cong \mathcal{G}(\mathcal{L}(G))$. Conversely, if M is a complemented modular lattice of length $n+1$ then $\mathcal{G}(M)$ is an n-dimensional projective geometry and $\mathcal{L}(\mathcal{G}(M)) \cong M$.

Proof. By Lemmas 1 and 2, $\mathcal{L}(G)$ is a complemented modular lattice. We claim that

(1) if $\{a_0, a_1, \ldots, a_n\}$ is a basis in G then the length of $\mathcal{L}(G)$ is $n+1$.

To verify (1) first we observe that for $j \geq 1$ the subspaces $\{a_0\}$, $\{a_1\}, \ldots, \{a_j\}$ satisfy the premises of Lemma 3 since for $0 \leq i \leq j$ we have $a_i \notin [\{a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n\}] \supseteq [\{a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_j\}] = \{a_0\} \vee \ldots \vee \{a_{i-1}\} \vee \{a_{i+1}\} \vee \ldots \vee \{a_j\}$ but $a_i \in \{a_0\} \vee \{a_1\} \vee \ldots \vee \{a_j\}$. Thus $h(\{a_0\} \vee \{a_1\} \vee \ldots \vee \{a_j\}) = j+1$ by Lemma 3, and $\emptyset \prec \{a_0\} \prec \{a_0\} \vee \{a_1\} \prec \cdots \prec \{a_0\} \vee \{a_1\} \vee \ldots \vee \{a_n\} = P$ by by Lemma 4. This maximal chain shows that the length of M is $n+1$.

It is clear from the definitions that $G \cong \mathcal{G}(\mathcal{L}(G))$.

Now let M be a complemented modular lattice of length $n+1$. Clearly, $\mathcal{G}(M)$ satisfies (i) in the definition of projective geometries. If a and b are distinct points on a line $\ell = c \vee d$ then $a \leq \ell\ \&\ b \leq \ell \implies a \vee b \leq \ell$. Therefore $a \vee b = c \vee d = \ell$ by Lemmas 3 and 4, showing the uniqueness of ℓ. Thus (ii) is fulfilled. In order to check (iii) let $p, q, r, x, y \in P$ such that p, q, x and p, r, y are colinear, cf. Figure 3. It is easy but a bit long to see that (iii) holds when $|\{p, q, r, x, y\}| < 5$ or p, q, r are colinear; we omit these details. (Note that in this case we can always choose $z \in \{p, q, r, x, y\}$.) Suppose $|\{p, q, r, x, y\}| = 5$ and p, q, r are not colinear, i.e. $r \not\leq p \vee q$. Then $\ell_1 = p \vee q$, $\ell_2 = p \vee r$ and we may chose $\ell_3 = q \vee r$, $\ell_4 = x \vee y$ and $z = \ell_3 \wedge \ell_4$. Since $\ell_3 \vee \ell_4 = q \vee r \vee x \vee y = (q \vee x) \vee (r \vee y) = (q \vee p) \vee (p \vee r) = (p \vee p) \vee q \vee r = p \vee q \vee r$, we obtain $h(\ell_3 \vee \ell_4) = 3$ from Lemma 3. From Theorem 4 it follows $h(z) = h(\ell_3 \wedge \ell_4) = h(\ell_3) + h(\ell_4) - h(\ell_3 \vee \ell_4) = 2 + 2 - 3 = 1$, implying that z is a point. This proves (iii).

We have seen that $\mathcal{G}(M)$ is a projective geometry. Let S be a subspace in $\mathcal{G}(M)$. Consider the set $U = \{a_1 \vee \ldots \vee a_n : 0 \leq k < \infty,\ a_1, \ldots, a_n \in S\}$. (Here the empty join, where $k = 0$, is 0.) Since $U \subseteq M$ and M is of finite length, there exists a finite maximal chain in U. The greatest element, denoted by v, of this maximal chain is clearly $\bigvee S$. (Here and in the sequel the lattice operations are taken in M.) Indeed, if $v \not\geq b$ for some $b \in S$ then the chain could be extended by adding $v \vee b$ to it.

The argument above shows that

(2) $\bigvee S$ can be represented as $a_1 \vee \ldots \vee a_k$.

Suppose k is minimal, then for $i = 1, 2, \ldots, k$ $\quad a_1 \vee \ldots \vee a_{i-1} \vee a_{i+1} \ldots \vee a_k \neq a_1 \vee a_2 \vee \ldots \vee a_k$. We claim that

(3) $S = \{p \in P : p \leq \bigvee S\}$,

which we show for any subspace S via induction on k. If $k = 0$ or $k = 1$ then $S = \emptyset$ or $S = \{a_1\}$ and (3) is evident. Assume that (3) is valid for $k - 1$ (and for any subspace) where $k > 1$. To show the $\supseteq$ inclusion in (3), let $p \in P$ and $p \leq \bigvee S$. If $p \leq a_1 \vee \ldots \vee a_{k-1}$ then $p \in [\{a_1, \ldots, a_{k-1}\}] \subseteq S$. Therefore we may assume that $p \not\leq a_1 \vee \ldots \vee a_{k-1}$ and, of course, also that $p \neq a_k$. Then $p \leq p \vee a_k = (p \vee a_k) \wedge \bigvee S = \underline{\underline{(p \vee a_k)}} \wedge (a_1 \vee \ldots \vee a_{k-1} \vee \underline{a_k}) = a_k \vee ((p \vee a_k) \wedge (a_1 \vee \ldots \vee a_{k-1})) = a_k \vee c$ where c denotes $(p \vee a_k) \wedge (a_1 \vee \ldots \vee a_{k-1})$. Since $h(a_1 \vee \ldots \vee a_{k-1}) = k - 1$, $h(p \vee a_k) = 2$, and $h(p \vee a_k \vee a_1 \vee \ldots \vee a_{k-1}) = h(p \vee \bigvee C) = h(\bigvee C) = h(a_1 \vee \ldots \vee a_k) = k$ by Lemma 3, $h(c) = h((p \vee a_k) \wedge (a_1 \vee \ldots \vee a_{k-1})) = (k-1) + 2 - k = 1$ follows from Theorem 4. Hence c is a point. Since $c \leq a_1 \vee \ldots \vee a_{k-1}$, the induction hypothesis implies $c \in [\{a_1, \ldots, a_{k-1}\}] \subseteq S$. Since $p \leq a_k \vee c$ and $a_k \neq c$, p is on the line $a_k \vee c = \ell_{a_k c}$. Then $p \in S$ follows from the fact that S is a subspace. The converse inclusion $S \subseteq \{p \in P : p \leq \bigvee S\}$ being trivial, we have shown (3).

Now it is clear from (3) that the map α: $\mathcal{L}(\mathcal{G}(M)) \to M$, $\quad S \mapsto \bigvee S$ is monotone and injective. (Note that $\bigvee S$ exists by (2), so α is well-defined.) To show that α is surjective first we show that each element d of M is the join of certain atoms. In fact, with $c = \bigvee\{p : p \in P \;\&\; p \leq d\}$ we claim $d = c$. Clearly, $c \leq d$. Suppose $c \neq d$, then $c < d$. By Theorem 6, c has a complement e in the interval $[0, d]$. Since $c \neq d = c \vee e$, $e \neq 0$. Let q be an atom in $[0, e]$. (Since $h(e) \leq h(1) < \infty$, any *finite* maximal chain in $[0, e]$ contains an atom, so this q exists.) From $q \leq e < d$ we infer $q \leq c$, whence $q \leq c \wedge e = 0$ is a contradiction. Therefore $c = d$. It is evident that $\{p : p \leq d \;\&\; p \in P\} \in \mathcal{L}(\mathcal{G}(M))$, and by $c = d$ this is an α-preimage of d. Therefore α is surjective. Suppose now that for $S_1, S_2 \in \mathcal{L}(\mathcal{G}(M))$ $\quad S_1\alpha \leq S_2\alpha$. Then $\bigvee S_1 \leq \bigvee S_2$ and $S_1 \subseteq S_2$ is implied by (3). Therefore α is an isomorphism.

Since any element of M is a join of atoms, $\bigvee P = 1$. Applying (2) to $S = P$ we obtain $a_0, a_1, \ldots, a_k \in P$ such that $a_0 \vee \ldots \vee a_k = 1$ and, for every i, $a_0 \vee \ldots \vee a_{i-1} \vee a_{i+1} \vee \ldots \vee a_k \neq 1$. From Lemma 3 and $h(1) = n + 1$ (the length of M) it follows that $k = n$. Further, (3) implies that $[a_0, a_1, \ldots, a_n] = P$. (Indeed, if $S \in \mathcal{L}(\mathcal{G}(M))$ contains all the a_i then $1 \geq \bigvee S \geq a_0 \vee a_1 \vee \ldots \vee a_n \geq 1$ yields $\bigvee S = 1$, which implies $S = P$ by (3).) For any i, $\{p \in P : p \leq a_0 \vee \ldots \vee a_{i-1} \vee a_{i+1} \vee \ldots \vee a_n\}$ is a subspace (by the surjectivity of α) which contains all a_j but a_i. Hence $a_i \notin [\{a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n\}]$. Consequently $\{a_0, a_1, \ldots, a_n\}$ is a basis in $\mathcal{G}(M)$, proving that $\mathcal{G}(M)$ is n-dimensional. ■

Corollary 1. Any two bases in a finite dimensional projective geometry have the same number of elements.

Proof. This follows from (1) in the previous proof. ■

Although Corollary 1 is a well-known fact in projective geometry, it is worth mentioning that we have proved it by means of lattice theory.

6. n-distributivity and n-diamonds

Let n be a fixed positive integer. After *A. P. Huhn*, a lattice called n-distributive, if it satisfies the identity

$$(\mathrm{D}_n) \qquad x \wedge \bigvee_{i=0}^{n} y_i = \bigvee_{j=0}^{n} \Big(x \wedge \bigvee_{\substack{i=0 \\ i\neq j}}^{n} y_i\Big).$$

Note that (D_1) is $x \wedge (y_0 \vee y_1) = (x \wedge y_1) \vee (x \wedge y_0)$, which is (equivalent to) the usual distributive law $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ (modulo lattice theory). While (D_1) implies modularity, for $n > 1$ (D_n) does not. Our aim is to characterize *modular* n-distributive lattices similarly to Dedekind's Criterion.

Let $\mathbf{b} = (b_0, b_1, \ldots, b_{n+1}) \in L^{n+2}$. We say that $\mathbf{b}$ satisfies the *n-diamond identities*, in short (n-DE) holds for $\mathbf{b}$, if for any $I, J \subseteq \{0, 1, \ldots, n+1\}$ and $k \in \{0, 1, \ldots, n+1\}$ such that $|I| = n+1$, $|J| = n$ and $k \notin J$ we have

$$\bigvee_{i\in I} b_i = \bigvee_{i=0}^{n+1} b_i \quad \text{and} \quad b_k \wedge \bigvee_{i\in J} b_i = \bigwedge_{i=0}^{n+1} b_i .$$

From now on let us fix the notations $u = u_{\mathbf{b}} = \bigwedge_{i=0}^{n+1} b_i$ and $v = v_{\mathbf{b}} = \bigvee_{i=0}^{n+1} b_i$. Then ($n$-DE) means $\bigvee_{i\in I} b_i = v$ and $b_k \wedge \bigvee_{i\in J} b_i = u$.

If $\mathbf{b} \in L^{n+2}$ satisfies (n-DE) and $b_0, b_1, \ldots, b_{n+1}$ are pairwise distinct then we say that $\mathbf{b}$ is an *n-diamond* (or, if we do not want to specify n, a *Huhn diamond*) in L. The elements u and v are called the bottom and top of $\mathbf{b}$, respectively.

For example, consider the lattice M_3 in Figure 10. The triple (b_0, b_1, b_2) is a 1-diamond in M_3. In the literature, the lattice M_3 is frequently referred to as a diamond.

Example 4. If G is an n-dimensional projective geometry and $a_0, a_1, \ldots, a_{n+1}$ are points of G such that any $n+1$ of them form a basis then $(\{a_0\}, \{a_1\}, \ldots, \{a_{n+1}\})$ is an n-diamond in $\mathcal{L}(G)$.

Theorem 7. (Huhn's n-distributivity Criterion) For a modular lattice L, L is n-distributive iff L contains no n-diamond.

Since the only difference between a 1-diamond and a diamond (i.e. M_3) is the lack or presence of u and v, a lattice contains a 1-diamond iff it has a sublattice isomorphic to M_3. Further, as we have mentioned already, (1-)distributivity implies modularity. Therefore the following theorem is a particular case, namely the case $n = 1$, of the previous one.

Birkhoff's Distributivity Criterion. A modular lattice is distributive iff it contains no sublattice isomorphic to M_3. In other words (including Dedekind's Criterion): a lattice is distributive iff it has neither a sublattice isomorphic to N_5 nor a sublattice isomorphic to M_3.

We will prove Huhn's Criterion for $n = 1$ only. However, the basic properties of n-diamonds we are going to develop in the sequel are needed in the general proof (for $n \geq 1$). From now on let L be a fixed *modular* lattice.

Lemma 5. If $\mathbf{b} = (b_0, \ldots, b_{n+1})$ satisfies (n-DE) then either $b_0, b_1, \ldots, b_{n+1}, u, v$ are pairwise distinct and $\mathbf{b}$ is an n-diamond, or $b_0 = b_1 = \cdots = b_{n+1} = u = v$.

Proof. Suppose the first possibility fails. If two of the b_i, say b_0 and b_1, coincide then $u = \bigwedge_{i=0}^{n+1} b_i \leq b_0 \wedge b_1 = b_0 \wedge b_0 = b_0 = b_0 \wedge b_1 \leq b_0 \wedge \bigvee_{i=1}^{n} b_i = u$, whence one of the b_i coincides with u. Since $u \leq b_i \leq v$, the same is true when $u = v$. If one of the b_i, say b_0, coincides with v then $u = b_0 \wedge \bigvee_{i=1}^{n} b_i = v \wedge \bigvee_{i=1}^{n} b_i = \bigvee_{i=1}^{n} b_i \geq b_1 \geq u$, whence one of the b_i, namely b_1, coincides with v. So we may assume that $u = b_0$. Since the role of $b_0, b_1, \ldots, b_{n+1}$ is symmetric, it suffices to show that another b_i, say b_{n+1}, equals u. Indeed, $b_{n+1} = b_{n+1} \wedge v = b_{n+1} \wedge \bigvee_{i=0}^{n} b_i = b_{n+1} \wedge (b_0 \vee \bigvee_{i=1}^{n} b_i) = b_{n+1} \wedge (u \vee \bigvee_{i=1}^{n} b_i) = b_{n+1} \wedge \bigvee_{i=1}^{n} b_i = u$. Finally, since all the b_i are equal, their join v also equals them. ■

The proof of Theorem 7 for $n = 1$. If $\mathbf{b} = (b_0, b_1, b_2)$ is an 1-diamond in L then, using (1-DE), we have $b_0 \wedge (b_1 \vee b_2) = b_0 \wedge v = b_0$ and $(b_0 \wedge b_1) \vee (b_0 \wedge b_2) = u \vee u = u$. Since $b_0 \neq u$ by Lemma 5, L is not distributive.

To show the converse, for an arbitrary $(x_0, x_1, x_2) \in L^3$ we define $u = (x_0 \wedge x_1) \vee (x_0 \wedge x_2) \vee (x_1 \wedge x_2)$, $v = (x_0 \vee x_1) \wedge (x_0 \vee x_2) \wedge (x_1 \vee x_2)$, and for $i = 0, 1, 2$ $\quad b_i = (u \vee x_i) \wedge v$. Since any member of the meet in v is greater than or equal to any member of the join in u (e.g., $x_0 \wedge x_2 \leq x_2 \leq x_1 \vee x_2$), we conclude that $u \leq v$. Now u and v are duals of each other. The dual of b_i is $(\underline{v} \wedge x_i) \vee \underline{u} = v \wedge (x_i \vee u) = b_i$. We claim that $\mathbf{b} = (b_0, b_1, b_2)$ satisfies (1-DE). Since the role of b_0, b_1 and b_2 are symmetric, we need to check $b_0 \wedge b_1 = u$ and $b_0 \vee b_1 = v$. But the second equation is just the dual of the first, whence, by the Duality Principle, it suffices to verify the first equation. Let us compute: $b_0 \wedge b_1 = (u \vee x_0) \wedge v \wedge (u \vee x_1) \wedge v = (u \vee x_0) \wedge (u \vee x_1) \wedge v$. Since $x_0 \geq (x_0 \wedge x_1) \vee (x_0 \wedge x_2) \implies u \vee x_0 = (x_1 \wedge x_2) \vee x_0$ and, similarly, $u \vee x_1 = (x_0 \wedge x_2) \vee x_1$, we have $b_0 \wedge b_1 = ((x_1 \wedge x_2) \vee x_0) \wedge ((x_0 \wedge x_2) \vee x_1) \wedge (x_0 \vee x_1) \wedge (x_0 \vee x_2) \wedge (x_1 \vee x_2)$. Omitting all meetands for which there is a smaller one we obtain $b_0 \wedge b_1 = \underline{\underline{((x_1 \wedge x_2) \vee x_0)}} \wedge (\underline{(x_0 \wedge x_2)} \vee x_1) = (x_0 \wedge x_2) \vee ((\underline{(x_1 \wedge x_2)} \vee x_0) \wedge \underline{\underline{x_1}}) = (x_0 \wedge x_2) \vee (x_1 \wedge x_2) \vee (x_0 \wedge x_1) = u$, indeed. Therefore $\mathbf{b}$ satisfies (1-DE). We also need the following calculations: $(x_0 \wedge (x_1 \vee x_2)) \wedge v = x_0 \wedge (x_1 \vee x_2) \wedge (x_0 \vee x_1) \wedge (x_0 \vee x_2) \wedge (x_1 \vee x_2) = x_0 \wedge (x_1 \vee x_2)$, and $(x_0 \wedge (x_1 \vee x_2)) \wedge u = x_0 \wedge (x_1 \vee x_2) \wedge ((x_0 \wedge x_1) \vee (x_0 \wedge x_2) \vee (x_1 \wedge x_2)) = \underline{\underline{x_0}} \wedge (\underline{(x_0 \wedge x_1) \vee (x_0 \wedge x_2)} \vee (x_1 \wedge x_2)) = (x_0 \wedge x_1 \wedge x_2) \vee (x_0 \wedge x_1) \vee (x_0 \wedge x_2) = (x_0 \wedge x_1) \vee (x_0 \wedge x_2)$.

Now assume that there is no 1-diamond in L. Then $u = v$ by Lemma 5 and we obtain $x_0 \wedge (x_1 \vee x_2) = (x_0 \wedge (x_1 \vee x_2)) \wedge v = (x_0 \wedge (x_1 \vee x_2)) \wedge u = (x_0 \wedge x_1) \vee (x_0 \wedge x_2)$. Since x_0, x_1 and x_2 were arbitrary, L is distributive. ■

For tough calculations in modular lattices we often need

Lemma 6. Any modular lattice satisfies the so-called *shearing identity* $x \wedge (y \vee z) = x \wedge ((y \wedge (x \vee z)) \vee z)$.

Proof. $x \wedge ((y \wedge (x \vee z)) \vee z) = x \wedge (y \vee z) \wedge (x \vee z) = x \wedge (y \vee z)$. ■

The following statements helps to understand how an n-diamond looks like.

Theorem 8. Let $\mathbf{b} = (b_0, b_1, \ldots, b_{n+1})$ be an n-diamond in a modular lattice L, and let I be an $n+1$ element subset of $\{0, 1, \ldots, n+1\}$. Let S denote the sublattice generated by $\{b_i : i \in I\}$. Then S is isomorphic to the lattice $(\mathcal{P}(I), \subseteq)$ (cf. Example 1) and the atoms of S are exactly the $b_i \quad (i \in I)$.

Proof. We may assume that $I = \{0, 1, \ldots, n\}$. Consider the map $\alpha\colon \mathcal{P}(I) \to L$, $X \mapsto \bigvee_{i \in X} b_i$. (The empty join, when $I = \emptyset$, is understod as u.) Clearly, α preserves the joins, i.e., $(X \cup Y)\alpha = X\alpha \vee Y\alpha$. The case of the meets will be settled in two steps, first only for the special case $X \cap Y = \emptyset$. Assume $X \cap Y = \emptyset$. If $X = Y = \emptyset$ then $(X \cap Y)\alpha = X\alpha \wedge Y\alpha$ is evident, so assume this is not the case and let k be the largest element of $X \cup Y$. Via induction on k we show that $X\alpha \wedge Y\alpha = u \quad (= \emptyset\alpha = (X \cap Y)\alpha)$. This is clear when $k = 1$, for X or Y is empty. For $k > 1$ we may assume that $k \in Y$, define $Z = Y \setminus \{k\}$ and, by using the shearing identity, the $k-1 \mapsto k$ step runs as follows:

$$(u \leq)\ X\alpha \wedge Y\alpha = \bigvee_{i \in X} b_i \wedge \bigvee_{i \in Y} b_i = \bigvee_{i \in X} b_i \wedge (b_k \vee \bigvee_{i \in Z} b_i) =$$

$$\bigvee_{i \in X} b_i \wedge ((b_k \wedge (\bigvee_{i \in X} b_i \vee \bigvee_{i \in Z} b_i)) \vee \bigvee_{i \in Z} b_i) \leq$$

$$\bigvee_{i \in X} b_i \wedge ((b_k \wedge \bigvee_{\substack{i=0 \\ i \neq k}}^{n} b_i) \vee \bigvee_{i \in Z} b_i) =$$

$$\bigvee_{i \in X} b_i \wedge (u \vee \bigvee_{i \in Z} b_i) = \bigvee_{i \in X} b_i \wedge \bigvee_{i \in Z} b_i\,,$$

which is u by the induction hypothesis.

Now let $X, Y \subseteq I$ be arbitrary. Then there are pairwise disjoint sets $A, B, C \subseteq I$ such that $X = A \cup C$ and $Y = B \cup C$. Then $X\alpha \wedge Y\alpha = (A \cup C)\alpha \wedge (B \cup C)\alpha = (A\alpha \vee C\alpha) \wedge (B\alpha \vee C\alpha) = (A\alpha \wedge (B\alpha \vee C\alpha)) \vee C\alpha = (A\alpha \wedge (B \cup C)\alpha)) \vee C\alpha$. But A and $B \cup C$ being disjoint this equals $u \vee C\alpha = C\alpha = (X \cap Y)\alpha$. Therefore α is a homomorphism.

Suppose α is not injective, say $C\alpha = D\alpha$ for some $C \neq D \in \mathcal{P}(I)$. Put $A = C \cap D$ and $B = C \cup D$. Then $A\alpha = (C \cap D)\alpha = C\alpha \wedge D\alpha = C\alpha \wedge C\alpha = C\alpha \vee C\alpha = C\alpha \vee D\alpha = (C \cup D)\alpha = B\alpha$. Choose a $k \in B \setminus A$. Then

$$u \leq b_k \wedge A\alpha = b_k \wedge \bigvee_{i \in A} b_i \leq b_k \wedge \bigvee_{\substack{i=0 \\ i \neq k}}^{n} b_i = u$$

yields $u = b_k \wedge A\alpha$. Since $b_k \wedge B\alpha = b_k \wedge \bigvee_{i \in B} b_i = b_k$, we obtain $b_k = b_k \wedge B\alpha = b_k \wedge A\alpha = u$ which, in virtue of Lemma 5, contradicts the fact that $\mathbf{b}$ is an n diamond. This proves the injectivity of α.

Now α maps the atoms (i.e. the singleton subsets) of $\mathcal{P}(I)$ onto the b_i $(i = 0, 1, \ldots, n)$. Clearly, $\{X\alpha : X \in \mathcal{P}(I)\}$ is the smallest sublattice of L containing all the b_i as $\mathcal{P}(I)$ is the smallest sublattice of itself containing all the atoms. Thus $S = \{X\alpha : X \in \mathcal{P}(I)\}$ and α: $\mathcal{P}(I) \to S$ is surjective. ■

In the view of Theorem 8 a 2-diamond can be imagined as the collection of the atoms of four "cubes", (i.e., sublattices isomorphic to the lattice on Figure 1) such that any two of these cubes have two atoms in common (visually, any two cubes have a common face), and these four cubes have the same top and bottom, cf. Figure 11.

On some further results

The connection between projective geometries and n-distributive lattices is much deeper than one may perhaps guess from Example 4. First we need some definitions. An element a in a complete lattice L is called *compact* if, for any $\emptyset \neq H \subseteq L$, $a \leq \bigvee H$ implies the existence of a finite subset X of H such that $a \leq \bigvee X$. If each element of a complete lattice L is can be represented as a join of certain set of compact elements then L is said to be an *algebraic latice.* E.g., all lattices in Example 3 are algebraic.

A projectiv geometry is called *non-degenerate* if any of its lines goes through at least three distinct points. From lattice theoretic point of view nondegenerate projective geometries are the building stones of all projective geometries, for it is known (from *F. Maeda*'s or *J. Hashimoto*'s stronger results, cf. [2] or [5]) that for any projective geometry G there is a set of non-degenerate projective geometries $\{G_i : i \in I\}$ such that $\mathcal{L}(G)$ is the direct product of the lattices $\mathcal{L}(G_i)$, $i \in I$.

Now the connection between projective geometries and n-distributive lattices is revealed by

Theorem 9. (*A. P. Huhn*) Let M be an algebraic lattice. Then M is n-distributive iff no sublattice of M is isomorphic to the lattice of subspaces of an n-dimensional non-degenerate projective geometry.

Since for $n \geq 3$ the subspace lattice of an n-dimensional nondegenerate projective geometry is isomorphic to the lattice of all subspaces of an $(n+1)$-dimensional vectorspace over an appropriate skew field (*van Staudt, O. Veblen* and *W. H. Young, O. Frink, etc., cf.* [2] *or* [5]), the theorem above is particularly strong when $n \geq 3$.

To conlude this notes let us mention one recent direction where Theorem 9 and the theory of n-diamonds have found some applications. This is the theory of congruence implications.

The *type* of an algebra is the set of operation symbols (together with their arities) which we use to denote the fundamental operations. E.g., the type of lattices is $\{\wedge, \vee\}$ where the arity of both operation symbols is 2 (i.e., they are binary operations). If two algebras are of the same type then they are called *similar.* For example, a ring and a field are similar but a lattice and a ring are not. Let τ be a type and Γ be a set of identities corresponding to τ. The class of algebras of type τ satisying Γ is called the *equational class* determined by Γ. E.g., the class of distributive lattices is an equational class while the class of complemented lattices is not (because the satisfaction of identities is inherited by sublattices but complementedness does not). The congruence relations of an algebra A form an algebraic lattice, denoted by $(\mathrm{Con}(A), \subseteq)$. Let μ and ν be two lattice identities. We write $\mu \overset{c}{\Rightarrow} \nu$ iff for any equational class $\mathcal{V}$ if $(\mathrm{Con}(A), \subseteq)$ satisfies μ for every algebra $A \in \mathcal{V}$ then $(\mathrm{Con}(A), \subseteq)$ satisfies ν for every algebra $A \in \mathcal{V}$. This is an interesting implication among lattice identities, e.g. $(\mathrm{D}_n) \overset{c}{\Rightarrow} (\mathrm{D}_1)$ for any $n > 1$, although there are lattices (e.g. M_3) that satisfy (D_n) but fail to satisfy (D_1).

Many of the results on $\overset{c}{\Rightarrow}$ are deduced from Theorem 9 and the properties of n-diamonds, cf., e.g., [8–10].

References

This part will be very restricted. First we list the basic books on lattices; they cover the majority of the preceding paragraphs. For the rest we list some research papers as well.

Books:

[1] G. Birkhoff: *Lattice Theory*, 3rd edition, Coll. Publ. XXV, American Mat. Soc., Providence, R. I., 1967.

[2] P. Crawley and R. P. Dilworth: *Algebraic Theory of Lattices*, Prentice-Hall, N. J., 1973.

[3] B. A. Davey and H. A. Priestley: *Introduction to Lattices and Order*, Cambridge University Press, 1990.

[4] G. Grätzer: *Lattice Theory: First Concepts and Distributive Lattices*, W. H. Freeman and Co., San Francisco, 1971.

[5] G. Grätzer: *General Lattice Theory*, Birkhäuser, Basel, 1978.

[6] R. N. McKenzie, G. F. McNulty and W. F. Taylor: *Algebras, Lattices and Varieties*, vol. I, Wadsworth and Brooks, Monterey, California, 1987.

[7] M. Stern: *Semimodular Lattices*, Teubner-Texte zur Mathematik, Stuttgart—Leipzig, 1991.

Research papers:

[8] G. Czédli: How are diamond identities implied in congruence varieties? *Algebra Universalis*, to appear.

[9] G. Czédli and R. Freese: On congruence distributivity and modularity, *Algebra Universalis* **17** (1983) 216–219.

[10] R. Freese, C. Herrmann and A. P. Huhn, On some identities valid in modular congruence varieties, *Algebra Universalis* **12** (1981) 322–334.

[11] C. Herrmann and A. P. Huhn: Lattices of normal subgroups which are generated by frames, *Coll. Math. Soc. J. Bolyai 14* (1974), 97–136.

[11] A. P. Huhn: Schwach Distributive Verbände. I, *Acta Sci Math. (Szeged)* **23** (1972) 295–305.

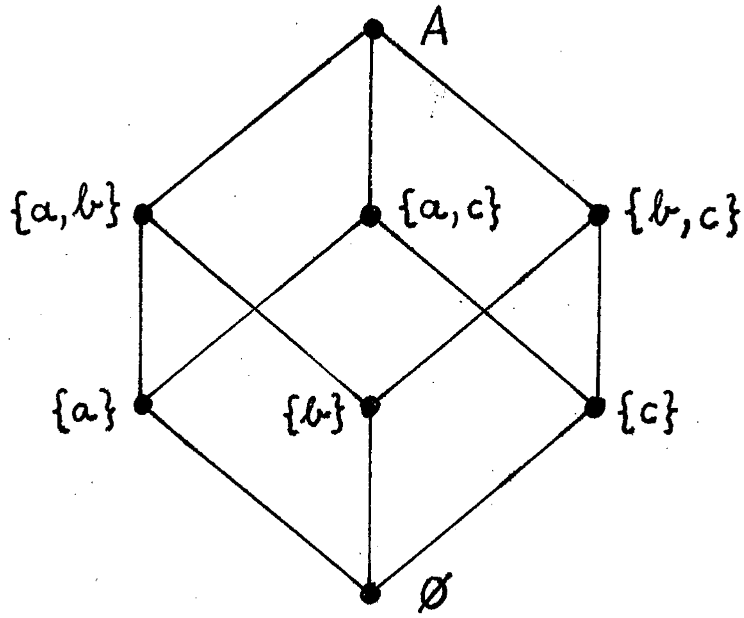

Figure 1

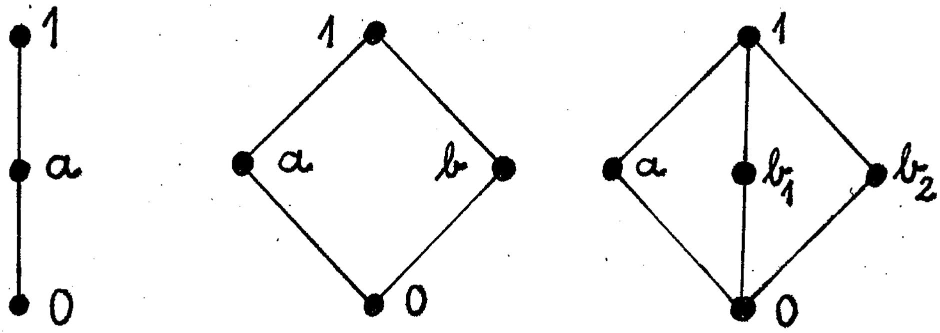

Figure 2

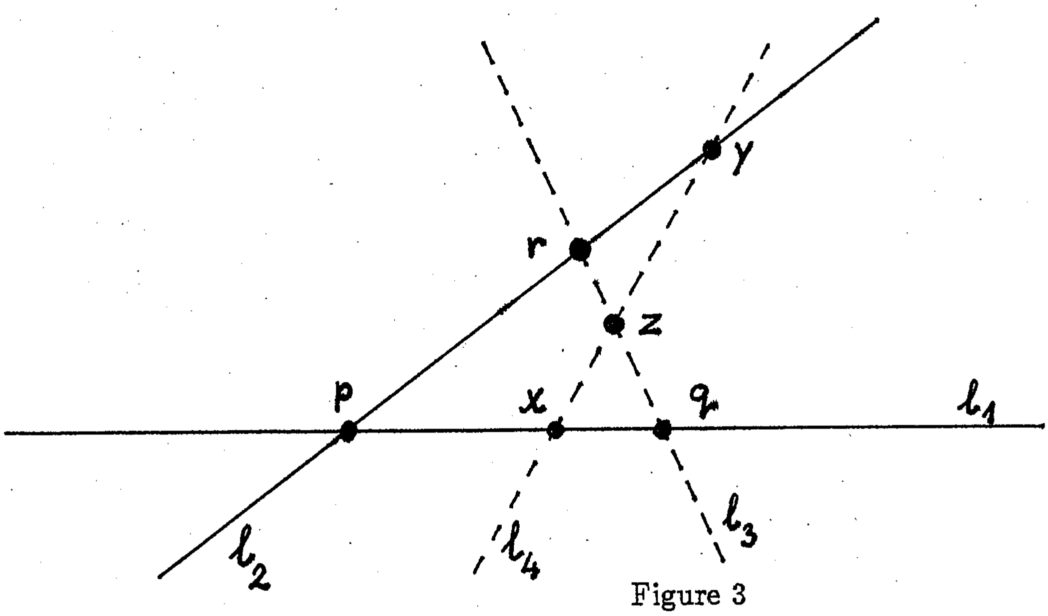

Figure 3

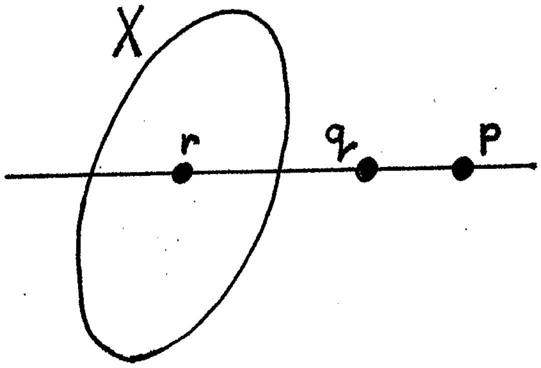

Figure 4

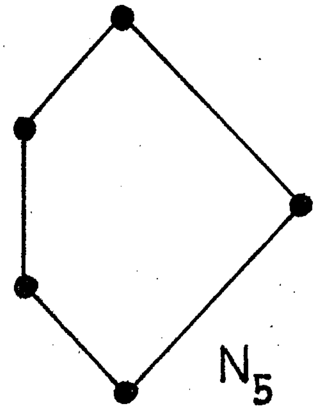

Figure 5

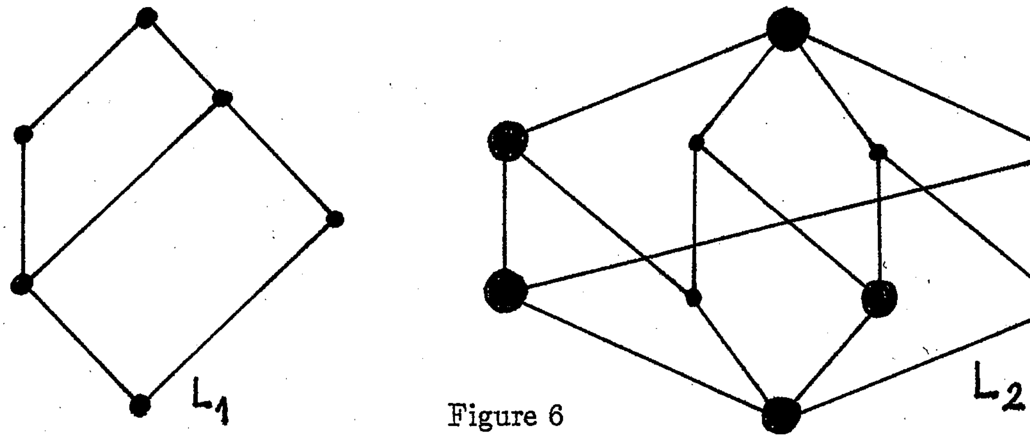

Figure 6

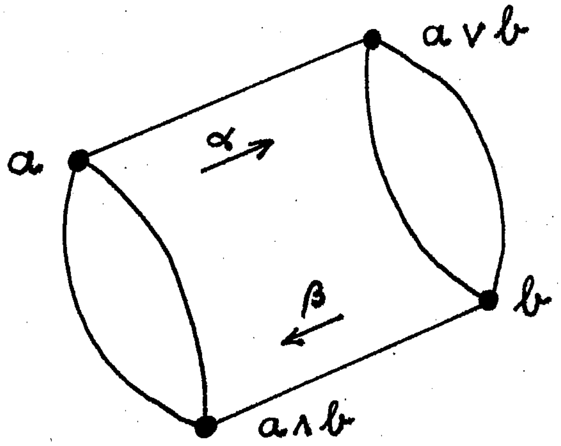

Figure 7

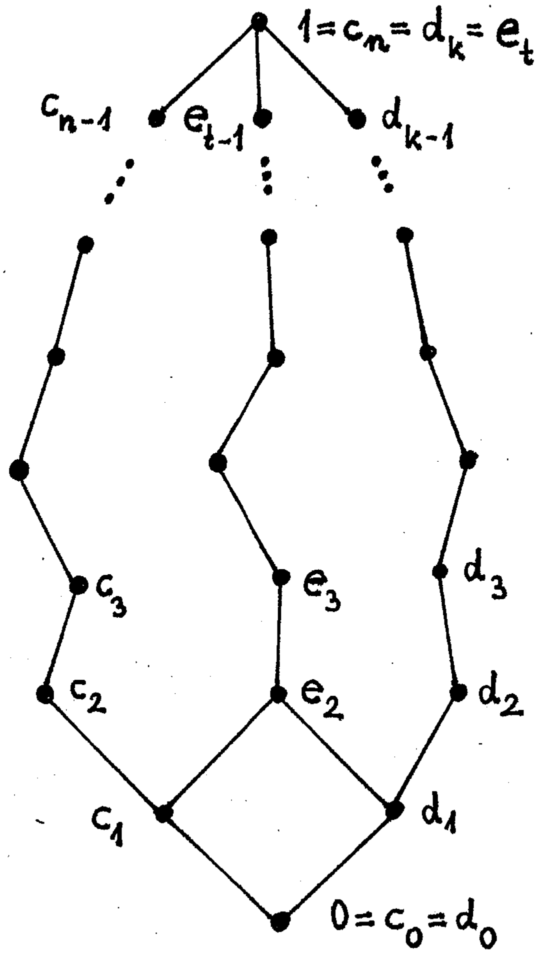

Figure 8

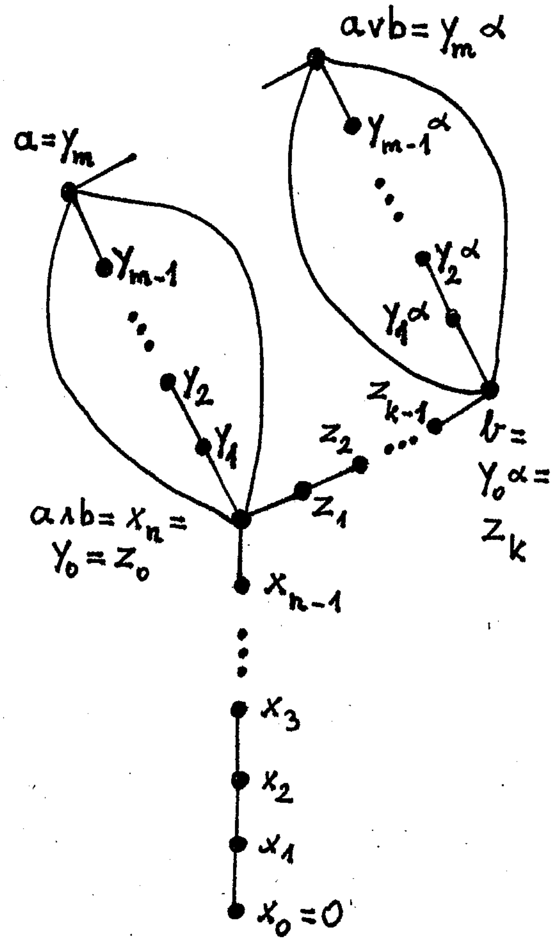

Figure 9

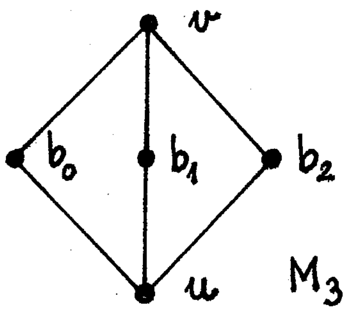

Figure 10

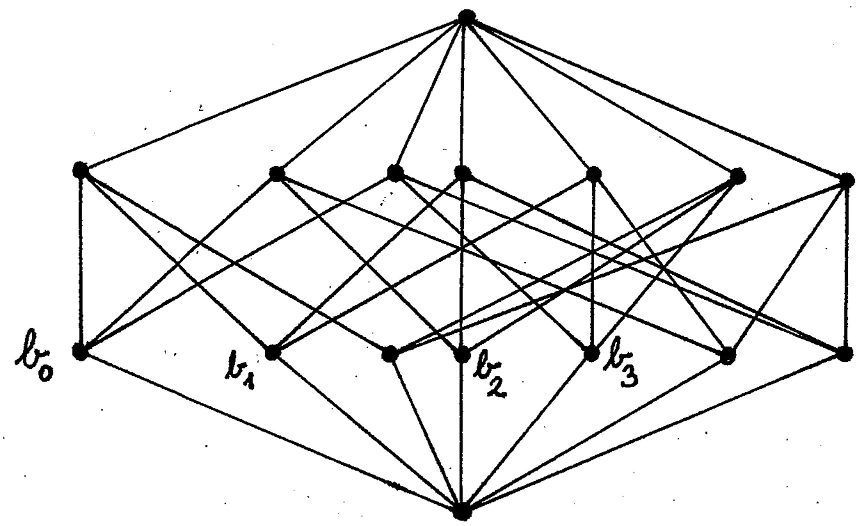

Figure 11