On the equational theory of submodule lattices.

By Christian Herrmann

Equational problems for modular lattices have been studied for a long time, although available results have been established only under significant syntactical difficulties (see e.g. the papers of RALPH FRESE and ALEIT MITSCHKE in this volume). Furthermore, they have been more or less partial in nature. For lattices of submodules things become surprisingly easy, by simply making use of well known algebraic facts. As a by-product algebraic results can be extended by lattice theoretic methods. §1-3 are based on joint work of the author and A. HUHN; the results in §4 have been partially reported in [6].

§1 The two basic lemmas.

For $p$ prime, $n \leq \infty$, $k \leq \infty$, let $L(p, k, n)$ be the lattice of subgroups of the $n$-th power of the cyclic group $\mathbb{Z}_p^k$ of order $p^k$ or of the quasicyclic $p$-group $\mathbb{Z}_{p^\infty}$. If $\mathbb{M}_R$ is a unitary $R$-module, then $L(\mathbb{M}_R)$ denotes the lattice of $R$-submodules of $\mathbb{M}_R$. The lattice varieties generated by all normal subgroup lattices of groups or subgroup lattices of abelian groups or complemented modular lattices will be written as $\mathcal{N}$ or $\mathcal{R}$ or $\mathcal{C}$. $\mathcal{A}$ shall denote the variety generated by $\mathcal{N} \cup \mathcal{A}$. 
Lemma 1. $L(M_R)$ is in the variety generated by all lattices $L(p,k,n)$ where $k < \infty$, $p^k$ divides the characteristic of $R$, and $n$ is less than or equal to the cardinality of a generating set of the $P$-module $M_p$, where $P$ is the subring of $R$ generated by the unit element.

Corollary 2. $A$ is generated by the finite primary lattices $L(p,k,n)$ ($p$ prime, $k,n < \infty$).

Sketch of proof. $L(M_R)$ is a sublattice of $L(M_p)$ and $L(M_p)$ is in the variety generated by the submodule lattices of its finitely generated submodules. By the Homomorphism Theorem these are sublattices of the $L(P^n)$. Now, if $P$ is finite and $|P| = p_1^{k_1} \cdots p_m^{k_m}$, then $P \cong \prod_{i=1}^m (\mathbb{Z}_{p_i^{k_i}})^n$ and $L(P^n) \cong \bigotimes_{i=1}^m L(p_i^{k_i},n)$. If, finally, $P$ is isomorphic to the ring $\mathbb{Z}$ of integers, then we use the fact that a system of linear diophantine equations is solvable in $\mathbb{Z}$ iff it is solvable in all $\mathbb{Z}_{p_i^{k_i}}$ and the following construction: To each lattice polynomial $w$ attach a system $\tilde{w}(x_i, y_i, \lambda_k)$ of linear equations in variables $x_i, y_i, \lambda_k$ such that for any elements $a_i, \ldots, a_n, b_i^1, \ldots, b_n^m$ of a $R$-module $M_R \langle a_1, \ldots, a_n \rangle$ $R \in w_1^{a_1} \cdots b_n^m$, then $w(a_i, b_i^j, \lambda_k)$ holds iff the system $\tilde{w}(a_i, b_i^j, \lambda_k)$ is solvable with values of the $\lambda_k$ in $R$. This can be easily done by induction over the length of $w$. Hence, if all $R$-submodules of $M_R$ are
generated by at most \( n \) elements, the inequality \( w = v \) is valid in \( L(M^*_R) \) if and only if, for any choice of constants \( a_i, b_i \) in \( M_R \), the solvability of \( \tilde{w}(a_i, b_i, \lambda_k) \) implies the solvability of \( \tilde{v}(a_i, b_i, \mu_k) \) over \( R \).

**Lemma 3.** If \( M_R \) is the \( \mathcal{F} \)-ultraproduct of the modules \( M_{R_i} \), then the \( \mathcal{F} \)-ultraproduct of the lattices \( L(M^*_R) \) is a sublattice of \( L(M_R) \), containing all finitely generated \( R \)-submodules.

The proof is by the classical model theoretic method of correspondences between classes: consider the structures \((M_R, L(M_R), \Phi)\), \( \Phi \) being the relation \( a \in U \) on \( M \times L(M_R) \) (c.f. MAKKAI, McNULTY [13]).

**Corollary 4.** \( \mathcal{L} \) is generated by subspace lattices of finite projective geometries over prime fields and arbitrary non-desarguesian planes.

---

§2 Lattices generated by a frame.

In [9] A. HUHN introduced the concept of an \( n \)-diamond in a lattice: a sequence \( a_0, \ldots, a_n \) of elements such that any \( n \)-element subset is independent in the interval

\[
\left[ \frac{1}{n} \sum a_i, \frac{n}{\sum a_i} \right].
\]

It is called a frame in \( L \), if \( \prod a_i = 0_L \).
and $\sum a_i = 1$. If $L$ is modular, a frame in the usual sense can be derived and vice versa.

**Theorem 5.** For $n \geq 3$ there is a complete list of all subdirectly irreducible lattices in $\mathcal{N}$ which are generated by an $n$-diamond:

- the rational projective geometry $L(Q^n_Q)$;
- the lattices $L(p, k, n)$, where $p$ is prime and $k \leq \infty$;
- the duals of the $L(p, \infty, n)$, where $p$ is prime.

The generating $n$-diamond is given, up to automorphism, by the submodules $e_0 = (x, \ldots, x)$, $e_i = (0, \ldots, 0, x, 0, \ldots, 0)$, with $x$ in the $i$-th entry, for $i = 1, \ldots, n$.

The following notation has been used: For $k_1, \ldots, k_n$ in $R$ and variables $x_1, \ldots, x_n$ not necessarily distinct we have

$$(k_1 x_1, \ldots, k_n x_n) = \{ (k_1 a_1, \ldots, k_n a_n) \mid a_i \in M \text{ and } x_i = x_j \Rightarrow a_i = a_j \},$$

a submodule of $M_R^n$.

The proof consists of the following main steps:

1) Reduction to $\mathcal{A}$: If the lattice of normal subgroups of $G$ contains an $n$-frame ($n \geq 3$), then $G$ is abelian.

2) If $L$ is a sublattice of any $L(p, k, n)$ ($k \leq \infty$) generated by an $n$-diamond, then $L$ is a $\{0, \ldots, n\}$-subdirect product (in the sense of Wille [18]) of lattices $L(p_i, k_i, n)$, each generated by the diamond $e_0, \ldots, e_n$. 
5) By Corollary 2 the lattice $F\mathcal{A}(P_n)$ freely generated in $\mathcal{A}$ by an $n$-diamond is a $\{0, \ldots, n\}$-subdirect product of the lattices $L(p,k,n)$ ($p$ prime, $k < \infty$) with generators $e_0, \ldots, e_n$.

4) Any subdirectly irreducible lattice in $\mathcal{A}$ which is generated by an $n$-diamond is, using the Lemma in JÖNSSON [12], a homomorphic image of the sublattice $M$ generated by $[e_i]_{\mathcal{F}}$ (i=0, ..., n) in $F\mathcal{A}(P_n)/\mathcal{F}$ for a suitable ultrafilter $\mathcal{F}$ on the set $\{p^k \mid p \text{ prime}, k < \infty\}$. Now, if $p \to \infty$ in $\mathcal{F}$, then $M = L(Q, n)$ is proved with the method of Lemma 3. If, on the other hand, $k \to \infty$ for fixed $p$, then $M$ is a subdirect product of $L(p, \infty, n)$ and its dual. But the only nontrivial homomorphic image of these lattices is $L(p, 1, n)$.

Corollary 6. The subdirectly irreducible lattices in $\mathcal{C}$ generated by an $n$-diamond are, for $n > 3$, exactly those in the above list and, for $n=3$, those in the above list as well as nondesarguesian planes generated by four points.
§3 Applications to equational classes

In order to apply Theorem 5 we need polynomials

\[ d_i(x_0, \ldots, x_3) \ (i=0, \ldots, 3) \] such that in any modular lattice the following holds: For any choice of \( x_0, \ldots, x_3 \) the \( d_i(x_0, \ldots, x_3) \) \((i=0, \ldots, 3)\) are equal to each other or form a 3-diamond; if \( x_0, \ldots, x_3 \) is a 3-diamond, then \( x_i = d_i(x_0, \ldots, x_3) \) \((i=0, \ldots, 3)\). Such polynomials are defined in A. HUHUN [8]:

\[
\begin{align*}
    d_0(x_0, \ldots, x_3) &= \frac{3}{i=1} b_i(x_0, \ldots, x_3) + a_0(x_0, \ldots, x_3) \\
    d_i(x_0, \ldots, x_3) &= \frac{3}{j=1, j \neq i} b_j(x_0, \ldots, x_3) \text{ for } i=1, 2, 3
\end{align*}
\]

where \( a_0(x_0, \ldots, x_3) = x_0 \cdot \sum_{i=1}^{3} x_i \), \( a_i(x_0, \ldots, x_3) = \sum_{j=1, j \neq i}^{3} x_j \),

\[
    v(x_0, \ldots, x_3) = \frac{3}{i=1} a_0(x_0, \ldots, x_3) + a_i(x_0, \ldots, x_3)
\]

\[
    b_i(x_0, \ldots, x_3) = a_i(x_0, \ldots, x_3) \cdot v(x_0, \ldots, x_3) + \sum_{j=1}^{3} x_j \cdot \sum_{k=1, k=j}^{3} x_k
\]

for \( i=1, 2, 3 \).

Now we can define inductively \( w_0(x_0, \ldots, x_3) = d_3(x_0, \ldots, x_3) \)

\[ w_{n+1}(x_0, \ldots, x_3) = \left[ w_n(x_0, \ldots, x_3) + d_0(x_0, \ldots, x_3) \cdot d_2(x_0, \ldots, x_3) \right] + d_1(x_0, \ldots, x_3) + d_2(x_0, \ldots, x_3) \cdot d_3(x_0, \ldots, x_3) \]

Lemma 7. \( w_n(e_0, \ldots, e_3) = (0, nx, x) \) in any module \( M_R \).
Theorem 8. The lattice identity $w_n(x_0, \ldots, x_3) = d_3(x_0, \ldots, x_3)$
is valid in $L(M_R)$ if and only if the greatest common divisor of the additive
orders of any three weakly independent elements of $M$ divides $n$.

Theorem 9. Each lattice $L(p,k,n)$ $(n \geq 3, k \geq \infty)$ is splitting
in $L(p,k)$. For $k > 1$ splitting universal disjunctions are "length $\leq 3"
or $d_3(x_0, \ldots, x_3) \cdot w_p k(x_0, \ldots, x_3) \leq d_3(x_0, \ldots, x_3) \cdot w_p k-1(x_0, \ldots, x_3)$,
and for $k=1$, they are "length $\leq 3$ and $L(p,k,n)$ not order em-
beddable" or $d_3(x_0, \ldots, x_3) \cdot w_p(x_0, \ldots, x_3) \leq x$. We remark that
$L(p,1,n)$ is a lattice, projective, finitely projected, and bounded epimorph-
phic image of a free lattice.

Theorem 10. If $\mathcal{L}$ is any class of lattices contained in $\mathcal{J}$
and containing all sublattices of lattices $L(V, k)$ where $V, k$
is any five dimensional vector space over a field of characteristic zero, then $\mathcal{L}$
cannot be defined by a finite set of first order axioms.

The proof is immediate by the following Lemma 11 and the
fact that a nontrivial ultraproduct of $L_{p,q}$'s is embeddable
in a $L(V, k)$, (see [3]).

Lemma 11. There is an identity valid in $\mathcal{J}$ which does not
hold, for $p \neq q$, in the Arguesian lattice $L_{p,q} = [0, a] \cup [b, 1]$,
with $b < a$, $[0, a] \neq L(p, 1, 3)$, and $[b, 1] \neq L(q, 1, 3)$ - cf. JONNSON [11].
§4 Lattices with four generators.

In [1] the authors asked for a complete list of subdirectly irreducible modular lattices with four generators; the solution is still distant.

**Lemma 12.** Any lattice listed in Theorem 5 is generated by four elements.

Furthermore, with the methods of [7] it is possible to construct from a sufficiently large partial sublattice of a lattice $L(p, 2, 3)$ a non-desarguesian uniform Hjelmslev plane with four generators.

The systems of generators and a partial converse of the lemma stem from the work of GELFAND and PONOMAREV [3] on linear spaces with four subspaces.

If $V$ is a linear space with subspaces $V_1, \ldots, V_4$, then $(V, V_1, \ldots, V_4)$ is called a quadruple. It is called *indecomposable*, if there is no non-trivial complementary pair $A, B$ of subspaces such that $V_i = A \cap V_i + B \cap V_i$ for $i = 1, \ldots, 4$.

**Lemma 13.** If $L = \langle v_1, \ldots, v_4 \rangle$ is subdirectly irreducible and can be embedded in the subspace lattice of a linear space of finite dimension, then there is an indecomposable quadruple $(V, V_1, \ldots, V_4)$ (with $V$ of finite dimension over an algebraically closed field $F$) and an isomorphism of $L$ onto the sublattice $\langle V_1, \ldots, V_4 \rangle$ of $L(V_F)$ mapping $v_i$ onto $V_i$ for $i = 1, \ldots, 4$. 
Theorem 14. (GELFAND, PONOMAREV [3]) The indecomposable quadruples of finite dimensions over an algebraically closed field \( F \) are given (up to isomorphism, permutation, and duality) by the following list:

1) \((F^{2n}, (x^n, 0^n), (0^n, x^n), (x^n, x^n), (x^1, y^{n-1}, x^1, y^{n-1} + x^1))\)
   with \( x^n \in F \setminus \{0, 1\} \).

2a) \((F^{2n+1}, (x^{n+1}, 0^n), (0^{n+1}, x^n), (x^1, y^n, y^n), (x^n, 0^1, x^n))\),
   b) \((F^{2n}, (x^n, 0^n), (0^n, x^n), (x^1, y^{n-1}, y^{n-1}, 0^1), (x^n, x^n))\).

3a) \((F^{2n+1}, (x^n, 0^{n+1}), (0^n, x^{n+1}), (x^n, x^1, 0^1), (x^n, 0^1, x^n))\),
   b) \((F^{2n}, (x^n, 0^n), (0^n, x^n), (0^1, x^n-1, x^n-1, 0^1), (x^n, x^n))\).

4) \((F^{2n+1}, (x^n, 0^{n+1}), (0^n, x^n, 0^1), (0, x_1, \ldots x_{n-1}, x_1, \ldots x_n, x_n),\)
   \((x_1, \ldots x_n, 0, x_1, \ldots x_n))\).

Let \( S(n, 4) \) be the lattice of fig.1 and \( \text{FM}(J_4^4) \) the modular lattice freely generated by \( J_4^4 \) (cf. fig.2 and [17]).

Lemma 15. \( V_1, \ldots V_4 \subseteq L(V_F) \) is in cases 1)-4) isomorphic to \( M_4, S(m, 4), L(P^{m}_{p}) \) where \( m = 2n+1 \) or \( m = 2n \) and \( P \) the prime field of \( F \), respectively.

Theorem 16. If \( L \) is subdirectly irreducible in \( \mathfrak{C} \) and generated by four elements, then \( L \) is isomorphic either to a nondesarguesian plane or one of the following lattices:

\( M_4, S(m, 4), L(P^{m}_{p}) \) \( P \) a prime field, \( \text{FM}(J_4^4) \) or its dual.

Sketch of proof. Similarly as in the proof of Theorem 3 we
have to study ultraproducts of lattices listed in Lemma 15. As there is only a finite number of types, we may assume that all components are of the same type. In case 1) there is nothing to do; in 2) the ultraproduct is again of breadth two, hence we may use the result of FRESE[2] that any subdirectly irreducible breadth two modular lattice with four generators is \( S(m,4) \), \( FM(J_1^4) \) or its dual. But the sublattice \( M \) generated by \( V_1, \ldots, V_4 \) in the ultraprodudct can be visualized and decomposed in a straightforward manner.

3), 4): If \( m \) is fixed, then \( M \subseteq L(P^m_p) \) follows trivially.

If \( m \to \infty \), then we consider structures
\[
(P^m_p, \text{L}(P^m_p), V_1, \ldots, V_4, \phi, I, J, K, \nu, \omega, \nu_1^0, \omega_1^0, \nu_1, \omega_1, \nu_2, \omega_2, \nu_3, \omega_3) \quad \text{such that:}
\]
\[
(P^m_p, V_1, \ldots, V_4) \text{ is the given quadruple; } \phi \text{ is defined as in Lemma 3; } I = \{1, \ldots, n\}, J = \{n+1, \ldots, 2n+1\} \text{ in case 3a), } J = \{n+1, \ldots, 2n\} \text{ in cases 3b) and 4); } K = \emptyset \text{ in cases 3a) and b); and } K = \{2n+1\} \text{ in cases 4)} ; I \text{ and } J \text{ are equipped with the partial order of taking the successor; } \phi \text{ is the mapping from } I \text{ onto } J \text{ with } \phi(i) = i + n ; \nu \text{ is the mapping from } P^m_x(I \cup J \cup K) \text{ into } P \text{ such that } \nu(a, i) \text{ is the } i \text{th coordinate of } a ; 1_i = 1, \nu_1 = n, \omega_1 = 2n+1 \text{ in case 3a), and } \omega_1 = 2n \text{ in cases 3b) and 4).}

In any of the cases 3a), 3b), and 4) we have formulas \( \alpha_1, \ldots, \alpha_4 \) in the first order language of these structures such that for any \( m \) and \( P \) \( v_i = \{ x | x \in P^m \text{ and } \alpha_i(x) \} \) holds for \( i = 1, \ldots, 4 \).

Now, in the ultraproduct we have a vector space \( V = P^{I \cup J \cup K} \) and \( v_i = \{ x | x \in V \text{ and } \alpha_i(x) \} \) is valid as well.
Let $I_1$ and $I_\infty$ be the subalgebras of $I \cup J$ generated by $\{1^1_1, 1^1_J\}$ and $\{1^\infty_1, 1^\infty_J\}$, resp., and $I_\lambda = (I \cup J) - (I_1 \cup I_\infty)$. Define $A_\gamma = \{f \in V \text{ and } (f, i) = 0 \text{ for all } i \in I_\gamma\}$, a subspace of $V$, for $\gamma \in \{1, \infty\}$ or $\gamma = \infty$ and case 3a, b) ; $A_\infty = \{f \in V \text{ and } (f, i) = 0 \text{ for all } i \in I_\infty\}$ in case 4).

Then $A_1, A_\infty, A_\infty$ yield a direct decomposition of the quadruple $(V, V_1, \ldots, V_4)$ into three quadruples $(A_\gamma, V_1^\gamma, \ldots, V_4^\gamma)$ $(\gamma = 1, \infty, \infty)$, thus a subdirect decomposition of $M$ into three factors.

But for $\gamma = 1, \infty$ and case 3a, b) $V_1^1, \ldots, V_4^\infty$ together with $0$ and $V$ form a partial lattice $J_1^4$ ; hence they generate a lattice $FM(J_1^4)$ (cf. [1]). In case 4) from $V_1^\infty, \ldots, V_4^\infty$ we get a partial lattice $J_1^4$ (fig. 3) which generates a third subdirect power $FM(J_1^4)$ (see [14]). In any case, $M$ is a finite subdirect power of $FM(J_1^4)$ and the only subdirectly irreducible epimorphic images of $M$ are $\bar{M}_4$ and $FM(J_1^4)$.

§5 Word problems.

HUTCHINSON [10] proved that in a quasivariety $\mathcal{C}$ of modular lattices such that $L(R^\infty_R) \notin \mathcal{C}$ for a nontrivial ring $R$ there is a finitely presented lattice with seven generators which has an unsolvable word problem (cf. FRESESE [2], too).

The attempts on the word problem for free modular lattices $FM(n)$ by SCHÜTZENBERGER [16] and GLUHOV [14] may be regarded as unsuccessful (cf. WHITMAN [17] and HERRMANN [8]). The following solvability results do, however, hold. Here
\(m^N\) denotes the class of all modular lattices of primitive length \(\leq n\) and primitive breadth \(\leq m\).

**Theorem 17.** (FREESE 2) In \(M\) the word problem in four generators is solvable.

**Theorem 18.** For \(n \leq 6\) and \(m \leq 3\) or \(n \leq \omega\) and \(m \leq 2\) the word problem in \(m^N\) is solvable.

**Theorem 19.** In \(C\) the word problem in four generators is solvable.

**Theorem 20.** The word problems for the free lattices \(FC(n)\) and \(FA(n)\) are solvable.

Proof. By Theorem 16 any four generated lattice in \(C\) is embeddable in a complemented modular lattice. Hence a Horn formula in four variables is valid in \(C\) if and only if it can be derived from the finite set of axioms of complemented modular lattices by a calculus of first order logic. On the other hand the four variable Horn formulas not valid in \(C\) are enumerable by Theorem 16, too.

Theorem 20 is an immediate consequence of Corollaries 2 and 4 and the fact that \(C\) and \(A\) can be defined by enumerable sets of identities. For \(C\) these are just the identities derivable from the axioms of a complemented modular lattice; for \(A\) this
follows by the result of SCHBIN[15] that the class of lattices embeddable in subgroup lattices of abelian groups can be recursively defined.

\[
\begin{align*}
[0,1] &= S(8,4) \\
[0,a] &= S(7,4)
\end{align*}
\]

Fig. 1

\[
\begin{align*}
1 &= a+b=a+c=a+d=b+d=c+d \\
0 &= ab=ac=ad=bc=bd=cd
\end{align*}
\]

Fig. 2

\[
\begin{align*}
1 &= a+c=a+d=b+d \\
0 &= ab=ac=ad=bc=bd=cd
\end{align*}
\]

Fig. 3
Literature.

2. R. Freese, Breadth two modular lattices, this volume
5. C. Herrmann, W. Poguntke, Axiomatic classes of lattices of normal subgroups, mimeographed notes, Darmstadt 1972
7. C. Herrmann, Modulare Verbände von Länge 6, This volume
8. C. Herrmann, Concerning M. M. Gluhov's paper on the word problem for free modular lattices, to appear
10. G. Hutchinson, Recursively unsolvable word problems of modular lattices and diagram-chasing, to appear
14. C. Sauer, W. Seibert, R. Wille, On free modular lattices over partial lattices with four generators, this volume