Algebra Universalis, **8** (1978) 269–309 Birkhäuser Verlag, Basel

A test for identities satisfied in lattices of submodules

GEORGE HUTCHINSON AND GÁBOR CZÉDLI

Abstract. Suppose R is ring with 1, and $\mathbf{H}\mathscr{L}(R)$ denotes the variety of modular lattices generated by the class of lattices of submodules of all R-modules. An algorithm using Mal'cev conditions is given for constructing integers $m \geqq 0$ and $n \geqq 1$ from any given lattice polynomial inclusion formula $d \subset e$. The main result is that $d \subset e$ is satisfied in every lattice in $\mathbf{H}\mathscr{L}(R)$ if and only if there exists x in R such that $(m \cdot 1)x = n \cdot 1$ in R, where $0 \cdot 1 = 0$ and $k \cdot 1 = 1 + 1 + \ldots + 1$ (k times) for $k \geqq 1$. For example, this "divisibility" condition holds for $m = 2$ and $n = 1$ if and only if $1 + 1$ is an invertible element of R, and it holds for $m = 0$ and $n = 12$ if and only if the characteristic of R divides 12. This result leads to a complete classification of the lattice varieties $\mathbf{H}\mathscr{L}(R)$, R a ring with 1. A set of representative rings is constructed, such that for each ring R there is a unique representative ring S satisfying $\mathbf{H}\mathscr{L}(R) = \mathbf{H}\mathscr{L}(S)$. There is exactly one representative ring with characteristic k for each $k \geqq 1$, and there are continuously many representative rings with characteristic zero. If R has nonzero characteristic, then all free lattices in $\mathbf{H}\mathscr{L}(R)$ have recursively solvable word problems. A necessary and sufficient condition on R is given for all free lattices in $\mathbf{H}\mathscr{L}(R)$ to have recursively solvable word problems, if R is a ring with characteristic zero. All lattice varieties of the form $\mathbf{H}\mathscr{L}(R)$ are self-dual. A variety $\mathbf{H}\mathscr{L}(R)$ is a congruence variety, that is, it is generated by the class of congruence lattices of all members of some variety of algebras. A family of continuously many congruence varieties related to the varieties $\mathbf{H}\mathscr{L}(R)$ is constructed.

§1. Introduction

A lattice is said to be representable by R-modules if it is embeddable in the lattice of submodules of some R-module. The class $\mathscr{L}(R)$ of all lattices representable by R-modules is known to be a quasivariety, that is, to be axiomatizable by universal Horn sentences (see [10: pp. 311–312]). In particular, $\mathscr{L}(R)$ admits isomorphic images, sublattices, and products including the trivial lattice, and so the class $\mathbf{H}\mathscr{L}(R)$ of homomorphic images of lattices representable by R-modules is a variety of (modular) lattices by Birkhoff's theorem characterizing varieties (see [5: Thm. 2, p. 152]). These varieties are natural objects for studying lattice identities satisfied in all lattices of submodules of modules over a fixed ring. If R is a field, then $\mathbf{H}\mathscr{L}(R)$ is a variety generated by Arguesian projective geometry lattices, that is, by lattices of subspaces of vector spaces over R. If R is the ring of integers, then $\mathbf{H}\mathscr{L}(R)$ is generated by all lattices of subgroups of abelian groups.

Presented by G. Grätzer. Received April 20, 1976. Accepted for publication in final form March 31, 1977.

Clearly, any lattice identity is satisfied in every member of $\mathscr{L}(R)$ if and only if it is satisfied in every member of $\mathbf{H}\mathscr{L}(R)$, and so the word problems for free lattices are the same for the quasivariety and the variety it generates.

Given a ring R with 1, let R-**Mod** denote the variety of left R-modules. The operations of R-**Mod** are additive group operations $\{+, -, 0\}$ plus unary scalar multiplication operations $\bar{r}$ for each r in R, and the identities are as usual, including $1x = x$. For M in R-**Mod**, let $\mathbf{Su}(M)$ denote the lattice of submodules of M and $\mathbf{Con}(M)$ the lattice of congruences of M. By [1: Thm. 1, p. 159], $\mathbf{Su}(M)$ and $\mathbf{Con}(M)$ are isomorphic lattices. We shall also use $\mathbf{Su}(V)$ and $\mathbf{Con}(V)$ to denote the subalgebra and congruence lattices for algebras V of other types.

In the theory of rings with 1, a term is a ring polynomial, obtained from variables and the constants 0 and 1 by sum, negation and product operations. A term obtained from variables, 0 and 1 by at most sum and negation operations is said to be productless. A formula is a system of ring equations if it is the existential closure of a conjunction of one or more equalities between terms. If each term of a system of ring equations is productless, then the system is said to be productless. For example,

$$(\exists x)(\exists y)[(x + x = (-y) + 1) \,\&\, (y + y = 0) \,\&\, (x = 0)]$$

is a productless system of ring equations. Suppose that $\sum$ is a first-order lattice-theoretic sentence that is satisfied in every lattice in $\mathscr{L}(R)$. By model theoretic methods, M. Makkai and G. McNulty [17] showed that there exists a system of ring equations $\sum_0$ satisfied in R such that $\sum$ is satisfied throughout $\mathscr{L}(S)$ for any ring S satisfying $\sum_0$. For any integers m and n, let $D(m, n)$ be the ring divisibility condition $(\exists x)(m \cdot x = n \cdot 1)$, where $m \cdot x$ denotes the m-th additive multiple of x. Note that $D(m, n)$ is a productless system of ring equations of a simple kind.

In the second section, we develop the ring divisibility test corresponding to any given lattice polynomial inclusion formula $d \subset e$. Since $\mathbf{Su}(M)$ and $\mathbf{Con}(M)$ are isomorphic lattices, $d \subset e$ is satisfied throughout $\mathbf{H}\mathscr{L}(R)$ iff $d \subset e$ is satisfied in $\mathbf{Con}(M)$ for every M in R-**Mod**. By Mal'cev's Theorem [5: Thm. 4, p. 172], R-**Mod** has permutable congruences. That is, $x \vee y = x \circ y = y \circ x$ for x and y in $\mathbf{Con}(M)$, where $x \circ y$ denotes composition of relations. If we replace meet by intersection and join by composition everywhere in the lattice polynomial d, we obtain a polynomial d° in intersection and composition, and we can define e° from e similarly. By the above, $d \subset e$ is satisfied in $\mathbf{Con}(M)$ iff $d^\circ \subset e^\circ$ is satisfied whenever congruences on M are substituted for the variables of d° and e°. But R. Wille's procedure [20: Satz 6.15, p. 76] can be used to generate a strong Mal'cev condition $\Xi(d^\circ, e^\circ)$ such that $d^\circ \subset e^\circ$ is satisfied for all congruences of M for every M in R-**Mod** iff $\Xi(d^\circ, e^\circ)$ is satisfied for the variety R-**Mod**. Now, every

polynomial $f(x_1, x_2, \ldots, x_n)$ for R-**Mod** is identically equal to some R-linear polynomial $\sum_{i=1}^{n} \bar{r}_i(x_i)$. Using this fact, we find that $\Xi(d^\circ, e^\circ)$ holds for R-**Mod** iff a certain productless system of ring equations $\Omega(d, e)$ is satisfied in R. Therefore, $d \subset e$ is satisfied throughout $\mathbf{H}\mathcal{L}(R)$ iff the productless system of ring equations $\Omega(d, e)$ is satisfied in R. Now, we can use an old matrix diagonalization method to show that any productless system of ring equations is ring equivalent to the conjunction of finitely many divisibility conditions. Analysis of divisibility conditions in a ring shows, first, that the set of divisibility conditions satisfied in a ring with nonzero characteristic k depends only on k. Second, for rings with zero characteristic, we also consider invariants called degrees of invertibility of primes. For p prime and R a ring with 1, the degree of invertibility $\theta(R, p)$ of p in R is the cardinal number in the interval $[0, \omega]$, ω equal to aleph-null, such that $\theta(R, p) = \omega$ if $D(p^{\beta+1}, p^\beta)$ is not satisfied in R for all $\beta \geqq 0$, and otherwise $\theta(R, p)$ is the smallest β such that $D(p^{\beta+1}, p^\beta)$ is satisfied in R. It is showed that the set of divisibility conditions satisfied in an R having characteristic zero is uniquely determined by the function of degrees of invertibility

$$p \mapsto \theta(R, p): P \to [0, \omega],$$

where P is the set of all primes. Using this analysis, a recursive procedure is given for constructing a single divisibility condition that is ring equivalent to any given conjunction of finitely many ring divisibility conditions. Combining these methods, we obtain the desired algorithm for constructing a ring divisibility test $D(m, n)$ that is satisfied in R if and only if $d \subset e$ is satisfied throughout $\mathbf{H}\mathcal{L}(R)$. The second section concludes with some immediate consequences of the ring divisibility test for inclusion formulas.

In the third section, we first construct the set of representative rings. For nonzero characteristic $k \geqq 1$, we can use the ring $\mathbf{Z}_k$ of integers modulo k. Given any function $f: P \to [0, \omega]$, we construct a ring R_f with characteristic zero such that $\theta(R_f, p) = f(p)$ for all primes p. C. Herrmann and A. Huhn [8] defined lattice identities corresponding to special ring divisibility conditions of form $D(0, n)$ or $D(m, 1)$. By extensive use of their methods, we construct lattice identities $\eta(m, n)$ for $m, n \geqq 2$ and $\Delta(m, n)$ for $m \geqq 0$ and $n \geqq 1$, such that $D(m, n)$ satisfied in R, $\eta(m, n)$ satisfied throughout $\mathbf{H}\mathcal{L}(R)$ and $\Delta(m, n)$ satisfied throughout $\mathbf{H}\mathcal{L}(R)$ are all equivalent statements for any ring R with 1. It is then possible to show that $\mathbf{H}\mathcal{L}(R) = \mathbf{H}\mathcal{L}(\mathbf{Z}_k)$ iff R has characteristic k for $k \geqq 1$, and $\mathbf{H}\mathcal{L}(R) = \mathbf{H}\mathcal{L}(R_f)$ iff R has characteristic zero and $\theta(R, p) = f(p)$ for each prime p, completing the lattice variety classification. The inclusion and join relationships between the varieties $\mathbf{H}\mathcal{L}(R)$, in the complete lattice of varieties of meet and join algebras, are given next.

For each nontrivial ring R with 1, it is known that there are finitely-presented lattices having recursively unsolvable word problems for $\mathbf{H}\mathscr{L}(R)$ (see [11: Thm. 1, p. 386] and [15]). In subsequent work [12: Thm. 2], it is shown that there is a five-generator, one-relation lattice presentation with unsolvable word problem with respect to each of the varieties $\mathbf{H}\mathscr{L}(R)$. Recent work of C. Herrmann and A. Huhn [6,7] proves that free lattices have solvable word problems in certain varieties $\mathbf{H}\mathscr{L}(R)$, and certain other related varieties. In particular, they show this for $\mathbf{H}\mathscr{L}(\mathbf{Z})$ and all $\mathbf{H}\mathscr{L}(\mathbf{Z}_k)$, $k \geqq 1$, and for the variety generated by all vector subspace lattices, the variety generated by all complemented modular lattices, and the variety generated by all abelian subgroup lattices and all complemented modular lattices [7: Kor. 9, Kor. 11, p. 452]. Using the ring divisibility test, we obtain direct confirmation of the solvability of free lattice word problems in $\mathbf{H}\mathscr{L}(\mathbf{Z}_k)$, $k \geqq 1$. For zero characteristic, free lattices in $\mathbf{H}\mathscr{L}(R)$ have solvable word problems if and only if $f^*(j, p) = \min\{j, \theta(R, p)\}$ is a recursive function for $j \geqq 1$ and p prime. (This is true if $p \mapsto \theta(R, p)$ is recursive on the set of primes p.) If R is torsion-free or a (von Neumann) regular ring with characteristic zero, it is shown that $\mathbf{H}\mathscr{L}(R)$ depends only on the set of primes $P_0 = \{p \in P: p \cdot 1$ is invertible in $R\}$, and free lattices have solvable word problems in $\mathbf{H}\mathscr{L}(R)$ if and only if P_0 is a recursive set of primes. Section 3 concludes with the verification that $\mathbf{H}\mathscr{L}(R)$ is a self-dual variety for all rings R with 1, by [13].

In the fourth section, we discuss the application of our results to congruence varieties of lattices. Certain varieties of algebras are constructed by using the operations and equations of Mal'cev conditions as the operations and identities of the constructed varieties. The set N of positive integers is considered as a lattice under the partial order of divisibility. A one-one correspondence is given between the continuously many ideals of N and the congruence varieties corresponding to certain of these constructed varieties of algebras.

There is an appendix dealing with computer implementation of the ring divisibility test algorithm.

The joint authorship of this paper occurred under unusual circumstances. The first author alone submitted the original manuscript under this title to Algebra Universalis. The second author circulated his independent work in summary form in May, 1976, and submitted a manuscript to the Colloquia Mathematica János Bolyai Math. Soc. in July, 1976. Both authors independently constructed similar algorithms for reducing submodule lattice inclusion formulas to ring divisibility conditions. The current approach of §2 and the appendix combines features from both methods. Both authors also independently constructed lattice identities corresponding to ring divisibility conditions, using the methods of Herrmann and Huhn. (Those of Prop. 6 for the first author; Prop. 5 for the second.) With this exception, the results concerning lattice variety classification, the word problem,

and self-duality in §3 are due to the first author. The congruence variety analysis of §4 is due to the second author. When the large overlap between the two authors' concurrent work was discovered, the present joint paper combining the two was agreed upon.

The authors thank the referee for helpful suggestions, especially a modification of the proofs of Props. 5 and 6 that results in a shorter and clearer verification. Helpful suggestions by András Huhn, Christian Herrmann and Ralph Freese are also gratefully acknowledged.

2. Reduction of lattice identities to ring divisibility conditions

We first describe R. Wille's procedure for constructing a Mal'cev condition characterizing satisfaction for congruences of an inclusion relation between polynomials in intersection and composition. The procedure given here has been tailored to our purposes, but the modifications are minor. Parallel to our development of the procedure, we give an example of its application. We label the alternating passages of procedure and example to avoid confusion.

Procedure. Suppose $d \subset e$ is a lattice polynomial inclusion formula, and every variable of d and e appears in the list $x_1, x_2, \ldots, x_n$. As before, d° and e° denote the polynomials obtained from d and e, respectively, by replacing meet by intersection and join by composition throughout.

Let C_n denote the set of polynomials in the operations of intersection and composition on the variables $x_1, x_2, \ldots, x_n$, $n \geqq 1$. Given an algebra U of type τ, the set $\mathrm{Rel}(U)$ of all relations on U (subsets of $U \times U$) has intersection and composition operations defined as usual. (Write $x \circ y$ for composition: $\langle u, v\rangle \in x \circ y$ iff there exists w such that $\langle u, w\rangle \in x$ and $\langle w, v\rangle \in y$.) An inclusion formula $c \subset c_0$ on C_n is said to be satisfied for congruences in the algebra of relations of U if $c \subset c_0$ holds in $\mathrm{Rel}(U)$ whenever congruences $\theta_1, \theta_2, \ldots, \theta_n$ of U replace the variables $x_1, x_2, \ldots, x_n$, respectively. Given c in C_n, we define a finite sequence $F_0(c), F_1(c), \ldots, F_t(c)$ of lists of formulas, each formula being a finite sequence of symbols of form $\langle a_i, a_j\rangle \in c_0$, where a_i and a_j are variables in $\{a_i : i \geqq 1\}$ and c_0 is in C_n. The recursive definition is as follows: First, $F_0(c)$ is the list containing the one formula $\langle a_1, a_2\rangle \in c$. For $k > 0$, $F_k(c)$ and all subsequent terms are undefined if $F_{k-1}(c)$ has no k-th formula. Suppose $F_{k-1}(c)$ has k-th formula $\langle a_i, a_j\rangle \in c_0$. If $c_0 = c_1 \cap c_2$ for some c_1, c_2 in C_n, then $F_k(c)$ is obtained by adding the two formulas $\langle a_i, a_j\rangle \in c_1$ and $\langle a_i, a_j\rangle \in c_2$ to the end of list $F_{k-1}(c)$. If $c_0 = c_1 \circ c_2$ for some c_1, c_2 in C_n, then $F_k(c)$ is obtained by adding the two formulas $\langle a_i, a_p\rangle \in c_1$ and $\langle a_p, a_j\rangle \in c_2$ to the end of the list $F_{k-1}(c)$, where p is the smallest positive integer such that the variable a_p doesn't occur in any formula of the list $F_{k-1}(c)$. If

c_0 is a variable x_i, $i \leqq n$, then $F_k(c) = F_{k-1}(c)$. It is not difficult to verify that this procedure terminates for any c in C_n, and so we can define $F(c)$ to be the final list of formulas $F_t(c)$, such that $F_{t+1}(c)$ is undefined. (The number of formulas in the list $F(c)$ equals the length of the polynomial c, that is, the number of occurrences of intersection, composition and variable symbols in c. The polynomials of C_n appearing in formulas of $F(c)$ subsequent to the first are just the component parts of the polynomial c, at all levels.)

The procedure for computing $\Xi(d^\circ, e^\circ)$ from d and e begins as follows: Compute $F(d^\circ)$ and $F(e^\circ)$, and modify $F(e^\circ)$ to obtain $F^*(e^\circ)$ by replacing each variable a_i by the variable f_i in every formula of the list. Suppose $\{a_1, a_2, \ldots, a_m\}$ and $\{f_1, f_2, \ldots, f_s\}$ are the sets of variables appearing in the formulas of $F(d^\circ)$ and $F^*(e^\circ)$, respectively, excluding the variables $x_1, x_2, \ldots, x_n$ of C_n. Clearly, m equals two plus the number of composition operators in d°, and similarly for s and e°. (In the subsequent analysis of Mal'cev conditions for a variety $\mathscr{V}$ of algebras of type τ, we will use $\{a_1, a_2, \ldots, a_m\}$ as a free generating set for the free $\mathscr{V}$-algebra on m generators, and $f_i = f_i(a_1, a_2, \ldots, a_m)$ will be a τ-polynomial for each $i \leqq s$.)

EXAMPLE. The Fano identity of R. Wille (see [19: p. 134] and [10: Ex. 1, p. 319]) is known to be satisfied throughout $\mathscr{L}(R)$ if and only if R has characteristic two or is trivial. This identity is $d \subset e$, where:

$$d = (x_1 \vee x_2) \wedge (x_3 \vee x_4)$$

$$e = [(x_1 \vee x_3) \wedge (x_2 \vee x_4)] \vee [(x_1 \vee x_4) \wedge (x_2 \vee x_3)].$$

By our definition, we have:

$$d^\circ = (x_1 \circ x_2) \cap (x_3 \circ x_4)$$

$$e^\circ = [(x_1 \circ x_3) \cap (x_2 \circ x_4)] \circ [(x_1 \circ x_4) \cap (x_2 \circ x_3)].$$

Computing recursively, we have $F(d^\circ) = F_7(d^\circ)$ as given below.

1. $\langle a_1, a_2 \rangle \in d^\circ$
2. $\langle a_1, a_2 \rangle \in x_1 \circ x_2$
3. $\langle a_1, a_2 \rangle \in x_3 \circ x_4$
4. $\langle a_1, a_3 \rangle \in x_1$
5. $\langle a_3, a_2 \rangle \in x_2$
6. $\langle a_1, a_4 \rangle \in x_3$
7. $\langle a_4, a_2 \rangle \in x_4$

Again, $F^*(e^\circ)$, corresponding to $F_{15}(e^\circ)$, is given below.

1. $\langle f_1, f_2\rangle \in e^\circ$
2. $\langle f_1, f_3\rangle \in (x_1 \circ x_3) \cap (x_2 \circ x_4)$
3. $\langle f_3, f_2\rangle \in (x_1 \circ x_4) \cap (x_2 \circ x_3)$
4. $\langle f_1, f_3\rangle \in x_1 \circ x_3$
5. $\langle f_1, f_3\rangle \in x_2 \circ x_4$
6. $\langle f_3, f_2\rangle \in x_1 \circ x_4$
7. $\langle f_3, f_2\rangle \in x_2 \circ x_3$
8. $\langle f_1, f_4\rangle \in x_1$
9. $\langle f_4, f_3\rangle \in x_3$
10. $\langle f_1, f_5\rangle \in x_2$
11. $\langle f_5, f_3\rangle \in x_4$
12. $\langle f_3, f_6\rangle \in x_1$
13. $\langle f_6, f_2\rangle \in x_4$
14. $\langle f_3, f_7\rangle \in x_2$
15. $\langle f_7, f_2\rangle \in x_3$

Note that $m = 4$ and $s = 7$ for our example.

Procedure. Construct partitions $\phi_1, \phi_2, \ldots, \phi_n$ of $\{a_1, a_2, \ldots, a_m\}$ corresponding to the variables $x_1, x_2, \ldots, x_n$ of d° and e° as follows: For each k, $k \leqq n$, ϕ_k is the smallest partition of $\{a_1, a_2, \ldots, a_m\}$ such that a_i and a_j belong to the same block of ϕ_k for every formula $\langle a_i, a_j\rangle \in x_k$ in the list $F(d^\circ)$. If x_k doesn't occur in d°, then ϕ_k is the discrete partition $\{\{a_i\}\colon i \leqq m\}$. For any partition ϕ of $\{a_1, a_2, \ldots, a_m\}$, let $\phi^*(a_i)$ for $i \leqq m$ denote a_j, where j is the smallest integer such that a_i and a_j belong to the same block of ϕ.

EXAMPLE. By analysis of $F(d^\circ)$, we have for the Fano identity:

$$\phi_1 = \{\{a_1, a_3\}, \{a_2\}, \{a_4\}\}, \quad \phi_2 = \{\{a_1\}, \{a_2, a_3\}, \{a_4\}\},$$
$$\phi_3 = \{\{a_1, a_4\}, \{a_2\}, \{a_3\}\}, \quad \phi_4 = \{\{a_1\}, \{a_2, a_4\}, \{a_3\}\}.$$

Therefore, $\phi_1^*(a_1) = a_1$, $\phi_1^*(a_2) = a_2$, $\phi_1^*(a_3) = a_1$, $\phi_1^*(a_4) = a_4$, and so on.

Procedure. A formula in $F^*(e^\circ)$ of form $\langle f_i, f_j\rangle \in x_k$ for $k \leqq n$ is said to be operation-free. Each operation-free formula $\langle f_i, f_j\rangle \in x_k$ of $F^*(e^\circ)$ is said to produce the corresponding polynomial equation

$$f_i(\phi_k^*(a_1), \phi_k^*(a_2), \ldots, \phi_k^*(a_m)) = f_j(\phi_k^*(a_1), \phi_k^*(a_2), \ldots, \phi_k^*(a_m)).$$

We say that the Mal'cev condition $\Xi(d^\circ, e^\circ)$ is satisfied for a variety $\mathcal{V}$ of algebras of type τ if there exist τ-polynomials $f_i(a_1, a_2, \ldots, a_m)$ for $i \leqq s$ such that each polynomial equation produced by an operation-free formula of $F^*(e^\circ)$ is an

identity for $\mathcal{V}$ and the two special equations $a_1 = f_1(a_1, a_2, \ldots, a_m)$ and $a_2 = f_2(a_1, a_2, \ldots, a_m)$ are also identities for $\mathcal{V}$. (The two variables appearing in the initial formula $\langle f_1, f_2 \rangle \in e^\circ$ of $F^*(e^\circ)$ have a special role.)

EXAMPLE. For the Fano identity, $\Xi(d^\circ, e^\circ)$ is satisfied in a variety $\mathcal{V}$ of algebras of type τ if there exist τ-polynomials $f_i(a_1, a_2, a_3, a_4)$ for $i \leqq 7$ such that the following ten polynomial equations are identities for $\mathcal{V}$:

1. $f_1(a_1, a_2, a_1, a_4) = f_4(a_1, a_2, a_1, a_4)$
2. $f_4(a_1, a_2, a_3, a_1) = f_3(a_1, a_2, a_3, a_1)$
3. $f_1(a_1, a_2, a_2, a_4) = f_5(a_1, a_2, a_2, a_4)$
4. $f_5(a_1, a_2, a_3, a_2) = f_3(a_1, a_2, a_3, a_2)$
5. $f_3(a_1, a_2, a_1, a_4) = f_6(a_1, a_2, a_1, a_4)$
6. $f_6(a_1, a_2, a_3, a_2) = f_2(a_1, a_2, a_3, a_2)$
7. $f_3(a_1, a_2, a_2, a_4) = f_7(a_1, a_2, a_2, a_4)$
8. $f_7(a_1, a_2, a_3, a_1) = f_2(a_1, a_2, a_3, a_1)$
9. $a_1 = f_1(a_1, a_2, a_3, a_4)$
10. $a_2 = f_2(a_1, a_2, a_3, a_4)$

Here, the first eight equations are produced by the operation-free formulas of $F^*(e^\circ)$ (the last eight), and the last two equations are the special equations for f_1 and f_2.

THEOREM 1 (R. Wille). *Suppose $\mathcal{V}$ is a variety of algebras of type τ, and d° and e° are polynomials in intersection and composition on the variables $x_1, x_2, \ldots, x_n$. Let V_m be the free $\mathcal{V}$-algebra, freely generated by $\{a_1, a_2, \ldots, a_m\}$, and let $\phi_1, \phi_2, \ldots, \phi_n$ be the partitions of $\{a_i : i \leqq m\}$ constructed from $F(d^\circ)$ as described above. Let $g^* : C_n \to \mathrm{Rel}(V_m)$ be the unique homomorphism of intersection and composition such that $g^*(x_k)$ is the τ-congruence of V_m generated by ϕ_k for each $k \leqq n$. Then the following are equivalent statements:*

(1) *$d^\circ \subset e^\circ$ is satisfied for congruences in $\mathrm{Rel}(U)$ for every U in $\mathcal{V}$.*

(2) *$g^*(d^\circ) \subset g^*(e^\circ)$ in $\mathrm{Rel}(V_m)$.*

(3) *The Mal'cev condition $\Xi(d^\circ, e^\circ)$ is satisfied for $\mathcal{V}$.*

Proof. Assume the hypotheses. Clearly (1) implies (2).

Assume (2). By an induction going from bottom to top of the list $F(d^\circ)$, we see that $\langle a_i, a_j \rangle \in g^*(c)$ is true whenever $\langle a_i, a_j \rangle \in c$ is a formula of $F(d^\circ)$. In particular, $\langle a_1, a_2 \rangle \in g^*(d^\circ)$ is true. By assumption, we have $g^*(d^\circ) \subset g^*(e^\circ)$, and so $\langle a_1, a_2 \rangle \in g^*(e^\circ)$ also. By an induction from top to bottom of the list $F^*(e^\circ)$, we can show

that there exist elements $z_1, z_2, \ldots, z_s$ of V_m such that $a_1 = z_1$, $a_2 = z_2$ and $\langle z_i, z_j\rangle \in g^*(c)$ is true if $\langle f_i, f_j\rangle \in c$ is a formula of the list $F^*(e^\circ)$. Let W_m be the free τ-algebra of τ-polynomials on the variables $\{a_1, a_2, \ldots, a_m\}$, and let $\alpha: W_m \to V_m$ be the unique τ-homomorphism such that $\alpha(a_i) = a_i$ for $i \leqq m$. Since α is onto, we can choose a τ-polynomial f_i such that $\alpha(f_i) = z_i$, for each $i \leqq s$. By [5: Thm. 1, pp. 169–170], $a_i = z_i$ in V_m implies that $a_i = f_i(a_1, a_2, \ldots, a_m)$ is an identity of $\mathcal{V}$ for $i = 1, 2$. So, the special equations of $\Xi(d^\circ, e^\circ)$ are identities for $\mathcal{V}$. Suppose $\langle f_i, f_j\rangle \in x_k$ is an operation-free formula of $F^*(e^\circ)$. Let $A_{m,k} = \{\phi_k^*(a_p) : p \leqq m\}$. (For example, $A_{4,2} = \{a_1, a_2, a_4\}$ if $\phi_2 = \{\{a_1\}, \{a_2, a_3\}, \{a_4\}\}$.) Let $W_{m,k}$ be the free τ-algebra of all τ-polynomials on $A_{m,k}$, and let $V_{m,k}$ be the free $\mathcal{V}$-algebra on $A_{m,k}$. Let $\beta: W_{m,k} \to V_{m,k}$ be the unique τ-homomorphism such that $\beta(a_p) = a_p$ for each a_p in $A_{m,k}$. Define τ-homomorphisms $h: W_m \to W_{m,k}$ and $h^*: V_m \to V_{m,k}$ by $h(a_p) = h^*(a_p) = \phi_k^*(a_p)$ for each $p \leqq m$, using the free τ-algebra and free $\mathcal{V}$-algebra properties. So, we obtain the commutative diagram below.

$$\begin{array}{ccc} W_m & \xrightarrow{h} & W_{m,k} \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ V_m & \xrightarrow{h^*} & V_{m,k} \end{array}$$

Now $h^*(a_p) = h^*(a_q)$ whenever a_p and a_q are in the same block of ϕ_k, so $h^*(v_1) = h^*(v_2)$ whenever $\langle v_1, v_2\rangle$ is in $g^*(x_k)$. But $\langle z_i, z_j\rangle \in g^*(x_k)$ because $\langle f_i, f_j\rangle \in x_k$ is in the list $F^*(e^\circ)$. Therefore, $h^*(z_i) = h^*(z_j)$. Using the diagram commutativity and τ-homomorphism properties, we have:

$$\beta(f_i(\phi_k^*(a_1), \phi_k^*(a_2), \ldots, \phi_k^*(a_m))) = \beta h(f_i(a_1, a_2, \ldots, a_m)) =$$
$$h^*\alpha(f_i) = h^*(z_i) = h^*(z_j) = h^*\alpha(f_j) =$$
$$\beta h(f_j(a_1, a_2, \ldots, a_m)) = \beta(f_j(\phi_k^*(a_1), \phi_k^*(a_2), \ldots, \phi_k^*(a_m))).$$

But then the equation $f_i(\phi_k^*(a_1), \ldots, \phi_k^*(a_m)) = f_j(\phi_k^*(a_1), \ldots, \phi_k^*(a_m))$ produced by the operation-free formula $\langle f_i, f_j\rangle \in x_k$ is an identity for $\mathcal{V}$, by [5: Thm. 1, pp. 169–170] again. Therefore, the Mal'cev condition $\Xi(d^\circ, e^\circ)$ is satisfied for $\mathcal{V}$, using the indicated τ-polynomials $f_1, f_2, \ldots, f_s$. This proves that (2) implies (3).

Now suppose $\Xi(d^\circ, e^\circ)$ is satisfied in $\mathcal{V}$, say by τ-polynomials $f_i(a_1, a_2, \ldots, a_m)$ for $i \leqq s$. Let U be any $\mathcal{V}$-algebra, and let $\gamma(x_1)$, $\gamma(x_2)$, $\ldots$, $\gamma(x_n)$ be any congruences on U. As before, $\gamma^*(c)$ in $\mathrm{Rel}(U)$ can be uniquely defined for each c in C_n. Suppose $\langle y_1, y_2\rangle$ is in $\gamma^*(d^\circ)$. By induction from top to bottom of the list $F(d^\circ)$, there exist $y_3, y_4, \ldots, y_m$ in U such that $\langle y_i, y_j\rangle \in \gamma^*(c)$ if $\langle a_i, a_j\rangle \in c$ is a formula of $F(d^\circ)$. Then an induction from bottom to top of $F^*(e^\circ)$

shows that

$$\langle f_i(y_1, y_2, \ldots, y_m), f_j(y_1, y_2, \ldots, y_m)\rangle \in \gamma^*(c)$$

if $\langle f_i, f_j\rangle \in c$ is a formula of $F^*(e^\circ)$. (For formulas $\langle f_i, f_j\rangle \in x_k$, we use the hypothesis that $f_i(\phi_k^*(a_1), \ldots, \phi_k^*(a_m)) = f_j(\phi_k^*(a_1), \ldots, \phi_k^*(a_m))$ is an identity of V and the result that $\gamma(x_k)$ identifies y_p and y_q if a_p and a_q belong to the same block of ϕ_k.) In particular,

$$\langle f_1(y_1, y_2, \ldots, y_m), f_2(y_1, y_2, \ldots, y_m)\rangle \in \gamma^*(e^\circ),$$

and so $\langle y_1, y_2\rangle$ is in $\gamma^*(e^\circ)$ by the two special identities of $\Xi(d^\circ, e^\circ)$. Therefore $\gamma^*(d^\circ) \subset \gamma^*(e^\circ)$, so $d^\circ \subset e^\circ$ is satisfied for congruences in Rel (U). So, (3) implies (1), completing Thm. 1.

The above proof is essentially the same as the proof given by R. Wille in [20]. For the reader's convenience, we have gathered and elaborated arguments appearing in several different places in the book, and have omitted parts of Wille's analysis that are not needed here.

To compute $\Omega(d, e)$, we modify the previously described method for computing $\Xi(d^\circ, e^\circ)$.

Procedure. After construction of $F(d^\circ)$, $F^*(e^\circ)$ and $\phi_1, \phi_2, \ldots, \phi_n$, we introduce ring variables r_{ij} for $i \leqq s$ and $j \leqq m$. (In later analysis, $f_i(a_1, a_2, \ldots, a_m) = \sum_{j=1}^m \overline{r_{ij}}(a_j)$ for $i \leqq s$ in R-**Mod**.) For each operation-free formula $\langle f_i, f_j\rangle \in x_k$ of $F^*(e^\circ)$ and each block A of ϕ_k, the associated ring equation is

$$\sum \{r_{ip} : a_p \in A\} = \sum \{r_{jp} : a_p \in A\}.$$

In addition, we have $2m$ special ring equations

$$r_{ij} = \delta_{ij} \quad \text{(Kronecker delta)},$$

for $i = 1, 2$ and $j \leqq m$. (In effect, we are equating coefficients of the identities of $\Xi(d^\circ, e^\circ)$ produced by the operation-free formulas of $F^*(e^\circ)$ and by the two special identities $a_1 = f_1$ and $a_2 = f_2$.)

Define $\Omega(d, e)$ to be the existential closure of the conjunction of all ring equations associated with operation-free formulas of $F^*(e^\circ)$ and blocks of the corresponding partitions, plus the $2m$ Kronecker delta equations. Since every term of $\Omega(d, e)$ is 0, 1 or a sum of one or more variables, $\Omega(d, e)$ is a productless system of ring equations.

EXAMPLE. For the Fano identity, we obtain 24 ring equalities corresponding to eight operation-free terms of $F^*(e^\circ)$, each associated with a partition having three blocks. They are given in the 8×3 array below.

$$\begin{array}{lll}
r_{11}+r_{13}=r_{41}+r_{43} & r_{12}=r_{42} & r_{14}=r_{44}\\
r_{41}+r_{44}=r_{31}+r_{34} & r_{42}=r_{32} & r_{43}=r_{33}\\
r_{11}=r_{51} & r_{12}+r_{13}=r_{52}+r_{53} & r_{14}=r_{54}\\
r_{51}=r_{31} & r_{52}+r_{54}=r_{32}+r_{34} & r_{53}=r_{33}\\
r_{31}+r_{33}=r_{61}+r_{63} & r_{32}=r_{62} & r_{34}=r_{64}\\
r_{61}=r_{21} & r_{62}+r_{64}=r_{22}+r_{24} & r_{63}=r_{23}\\
r_{31}=r_{71} & r_{32}+r_{33}=r_{72}+r_{73} & r_{34}=r_{74}\\
r_{71}+r_{74}=r_{21}+r_{24} & r_{72}=r_{22} & r_{73}=r_{23}
\end{array}$$

We also have the 2×4 array of Kronecker delta ring equalities below.

$$\begin{array}{llll}
r_{11}=1 & r_{12}=0 & r_{13}=0 & r_{14}=0\\
r_{21}=0 & r_{22}=1 & r_{23}=0 & r_{24}=0
\end{array}$$

By the definition, $\Omega(d, e)$ is the existential closure of the conjunction of the 32 equations above.

Using ordinary arguments in the theory of rings with 1, we can show that $\Omega(d, e)$ is equivalent to $1+1=0$. Specifically, the formula matrix of $\Omega(d, e)$, a system of 32 equations in 28 variables, is equivalent to the conjunction of $1+1=0$ and 28 equations given by setting $[r_{ij}]_{i\leqq 7, j\leqq 4}$ equal to the matrix:

$$\begin{bmatrix}
1 & 0 & 0 & 0\\
0 & 1 & 0 & 0\\
1 & 0 & 1 & 1\\
0 & 0 & 1 & 0\\
1 & 1 & 1 & 0\\
0 & 0 & 0 & 1\\
1 & 1 & 0 & 1
\end{bmatrix}$$

By previous analysis, the Fano identity is satisfied throughout $\mathscr{L}(R)$ if and only if R has characteristic two or is trivial [10: p. 319]. Our next theorem thus agrees with the known result for the Fano identity.

THEOREM 2. *Suppose R is a ring with 1 and d and e are lattice polynomials on $x_1, x_2, \ldots, x_n$. Then the formula $d \subset e$ is satisfied in every lattice representable by R-modules if and only if the productless system of ring equations $\Omega(d, e)$ is satisfied in R. There is a recursive procedure for computing $\Omega(d, e)$ from d and e.*

Proof. Assume the hypotheses. Using the discussion in the introduction and Thm. 1, $d \subset e$ is satisfied in every lattice representable by R-modules iff $d \subset e$ is satisfied in the lattice of congruences of each R-module M iff $d^\circ \subset e^\circ$ is satisfied for congruences in the algebra of relations of each R-module M iff $\Xi(d^\circ, e^\circ)$ is satisfied for R-**Mod**.

If $\Omega(d, e)$ is satisfied in R via an assignment $g(r_{ij})$ of elements of R for $i \leqq s$ and $j \leqq m$, it is easily checked that $\Xi(d^\circ, e^\circ)$ is satisfied via $f_i(a_1, a_2, \ldots, a_m) = \sum_{j=1}^m \overline{g(r_{ij})}(a_j)$ for $i \leqq s$.

Suppose $\Xi(d^\circ, e^\circ)$ is satisfied in R-**Mod** via $f_i(a_1, a_2, \ldots, a_m)$ for $i \leqq s$. Now every polynomial in R-**Mod** is equivalent to some R-linear polynomial, so we can choose $g(r_{ij})$ in R for $i \leqq s$ and $j \leqq m$ such that $f_i(a_1, a_2, \ldots, a_m) = \sum_{j=1}^m \overline{g(r_{ij})}(a_j)$ is an identity of R-**Mod** for all $i \leqq s$. Furthermore, we have R-linear uniqueness: If $\sum_{j=1}^m \overline{y_j}(a_j) = \sum_{j=1}^m \overline{z_j}(a_j)$ is an identity of R-**Mod** for $y_1, y_2, \ldots, y_m$ and $z_1, z_2, \ldots, z_m$ in R, then $y_j = z_j$ for all $j \leqq m$. Using the identity of $\Xi(d^\circ, e^\circ)$ corresponding to an operation-free formula $\langle f_i, f_j \rangle \in x_k$ of $F^*(e^\circ)$, we see that $\sum_{p=1}^m \overline{g(r_{ip})}(\phi_k^*(a_p)) = \sum_{p=1}^m \overline{g(r_{jp})}(\phi_k^*(a_p))$ is an identity of R-**Mod**. If we convert both these sums to equivalent R-linear polynomials and use R-linear uniqueness, we obtain the associated ring equations $\sum \{g(r_{ip}) : a_p \in A\} = \sum \{g(r_{jp}) : a_p \in A\}$ for each block A of ϕ_k, satisfying the equations of $\Omega(d, e)$ associated with $\langle f_i, f_j \rangle \in x_k$. Similarly, we can apply R-linear uniqueness to the identities $\sum_{j=1}^m \overline{g(r_{ij})}(a_j) = a_i = \sum_{j=1}^m \overline{\delta_{ij}}(a_j)$ for $i = 1, 2$, obtained from the special equations of $\Xi(d^\circ, e^\circ)$. This leads to satisfaction of the Kronecker delta equations $g(r_{ij}) = \delta_{ij}$ in R for $i = 1, 2$ and $j \leqq m$. Therefore, $\Omega(d, e)$ is satisfied in R via $g(r_{ij})$ for $i \leqq s$ and $j \leqq m$. We omit the proof that $\Omega(d, e)$ is recursively computable from d and e; there is little difficulty in constructing the required procedure from the definitions. (See the appendix for computer implementation.) This completes Thm. 2.

Given an integer k and a term t of the theory of rings with 1, let $k \cdot t$ denote the additive multiple of t by k, defined recursively by $0 \cdot t = 0$, $k \cdot t = (k-1) \cdot t + t$ for $k > 0$, and $k \cdot t = -(|k| \cdot t)$ for $k < 0$. Note that $(k_1 + k_2) \cdot r = k_1 \cdot r + k_2 \cdot r$, $k_1 \cdot (k_2 \cdot r) = k_1 k_2 \cdot r$ and $(k_1 \cdot r_1)(k_2 \cdot r_2) = k_1 k_2 \cdot r_1 r_2$ for integers k_1 and k_2 and r, r_1, r_2 in any ring with 1. Furthermore, each element $k \cdot 1$ for integer k is in the center of R. This notation is used when it is convenient to regard R as an associative algebra with unit over the ring $\mathbf{Z}$ of integers.

The productless system of ring equations of form $(\exists x)(m \cdot x = n \cdot 1)$ for

integers m and n is called the "divisibility condition" for $\langle m, n\rangle$, and is denoted by $D(m, n)$, as before. For example, $D(2, 1)$ denotes $(\exists x)(0+x+x=0+1)$, which is satisfied in a ring R with 1 if and only if $1+1$ is an invertible element of R. Now, the divisibility condition for $\langle m, n\rangle$ is equivalent to the divisibility condition for $\langle |m|, |n|\rangle$ in any ring with 1. Furthermore, $D(m, 0)$ for $m \geqq 0$ is satisfied in any ring with 1, and so is ring equivalent to $D(1, 1)$, say. Defining $D(m, n)$ to be a "normal" divisibility condition if $m \geqq 0$ and $n \geqq 1$, we have shown that each divisibility condition is equivalent to some normal divisibility condition.

We now analyze divisibility conditions in rings R with 1.

DEFINITION. For $k \geqq 1$ and p prime, let expt (k, p), the exponent of p in k, denote the largest β, $\beta \geqq 0$, such that p^β divides k. As before, the degree of invertibility $\theta(R, p)$ is the smallest $\beta \geqq 0$ such that $D(p^{\beta+1}, p^\beta)$ is satisfied in R, with $\theta(R, p) = \omega$ if $D(p^{\beta+1}, p^\beta)$ is not satisfied in R for any $\beta \geqq 0$. Note that $D(p^{\beta+1}, p^\beta)$ is satisfied in R if and only if $\beta \geqq \theta(R, p)$. We will use the abbreviation g.c.d. for the greatest common divisor of a pair of integers.

PROPOSITION 1. *Let R be a ring with 1 with characteristic j, and suppose $m \geqq 0$ and $n \geqq 1$. If $j \geqq 1$, then $D(m, n)$ is satisfied in R if and only if the g.c.d. of m and j divides n. Furthermore, $\theta(R, p) =$ expt (j, p) for all primes p if $j \geqq 1$. If $j = 0$, then $D(m, n)$ is satisfied in R if and only if $m > 0$ and $\theta(R, p) \leqq$ expt (n, p) for all primes p such that* expt $(n, p) <$ expt (m, p).

Proof. Assume the hypotheses, and suppose $j \geqq 1$. Let c be the g.c.d. (m, j), so m/c and j/c are integers and $c = ma + jb$ for some integers a and b. If c divides n, then $m \cdot (a(n/c) \cdot 1) = (c - jb)(n/c) \cdot 1 = n \cdot 1 - b(n/c) \cdot (j \cdot 1) = n \cdot 1$ in R, since $j \cdot 1 = 0$. So, $D(m, n)$ is satisfied in R.

Now suppose $D(m, n)$ is satisfied in R, say $m \cdot r = n \cdot 1$ for r in R. Let $n = \sigma c + \tau$ for integers σ and τ, $0 \leqq \tau < c$. Then $\tau(j/c) \cdot 1 = (n - \sigma c)(j/c) \cdot 1 = (j/c) \cdot (n \cdot 1) - \sigma \cdot (j \cdot 1) = (j/c) \cdot (m \cdot r) = (j \cdot 1)(m/c \cdot r) = 0$ in R, so $\tau = 0$ and c divides n. (If $\tau > 0$, then $0 < \tau(j/c) < j$ and $\tau(j/c) \cdot 1 = 0$ in R, contradicting $j =$ char (R).) This proves the first part.

For p prime, $D(p^{\beta+1}, p^\beta)$ is satisfied in R iff the g.c.d. $(p^{\beta+1}, j)$ divides p^β iff $\beta \geqq$ expt (j, p). So, $\theta(R, p) =$ expt (j, p) for each prime p.

Now assume $j = 0$. Suppose $D(m, n)$ is satisfied in R, say $m \cdot r = n \cdot 1$ for r in R. Clearly $m > 0$, since $j = 0$. Let p be a prime such that $\beta =$ expt $(n, p) <$ expt (m, p). Then $p^{\beta+1}$ divides m and $n = p^\beta u$ for some u not divisible by p.

Choose integers a and b with $pa+ub=1$. Now $bm \cdot r = bn \cdot 1 = p^\beta ub \cdot 1 = p^\beta(1-pa) \cdot 1 = p^\beta \cdot 1 - p^{\beta+1}a \cdot 1$. Therefore, $p^{\beta+1} \cdot x = p^\beta \cdot 1$ for $x = (m/p^{\beta+1})b \cdot r + a \cdot 1$ in R, and so $D(p^{\beta+1}, p^\beta)$ is satisfied in R. Therefore $D(m, n)$ satisfied in R implies $m > 0$ and $\theta(R, p) \leqq \text{expt}(n, p)$ for all primes p such that $\text{expt}(n, p) < \text{expt}(m, p)$.

Suppose $m > 0$ and $\theta(R, p) \leqq \text{expt}(n, p)$ whenever $\text{expt}(n, p) < \text{expt}(m, p)$, for all primes p. We prove $D(m, n)$ is satisfied in R by induction on the number k of prime divisors of m. If $k = 0$, then $D(1, n)$ is satisfied in any ring with 1. So, let $k > 0$ and choose a prime p dividing m, and assume the induction hypothesis. Let $\beta = \text{expt}(n, p)$ and $\kappa = \text{expt}(m, p)$. Since m/p^κ has $k-1$ prime divisors, $(m/p^\kappa) \cdot r = (n/p^\beta) \cdot 1$ for some r in R by the induction hypothesis. If $\beta \geqq \kappa$, then $m \cdot (p^{\beta-\kappa} \cdot r) = p^\beta(m/p^\kappa) \cdot r = p^\beta(n/p^\beta) \cdot 1 = n \cdot 1$, so $D(m, n)$ is satisfied in R. If $\beta < \kappa$, then $p^{\beta+1} \cdot r_0 = p^\beta \cdot 1$ for some r_0 in R by the hypothesis that $\theta(R, p) \leqq \text{expt}(n, p)$ whenever $\text{expt}(n, p) < \text{expt}(m, p)$. *So*, $m \cdot r r_0^{\kappa-\beta} = ((m/p^\kappa) \cdot r)(p^\kappa \cdot r_0^{\kappa-\beta}) = ((n/p^\beta) \cdot 1)(p^\beta \cdot 1) = n \cdot 1$ in R, and again $D(m, n)$ is satisfied in R. This completes Prop. 1.

From Prop. 1, we see that the satisfiability of $D(m, n)$ in R is completely determined by m, n and $\text{char}(R)$ if $\text{char}(R) \geqq 1$. If $\text{char}(R) = 0$, then the satisfiability of $D(m, n)$ in R is completely determined by m, n and the degrees of invertibility $\theta(R, p)$ for primes p dividing m, in particular those for which $\text{expt}(n, p) < \text{expt}(m, p)$.

The results of Prop. 1 suggest that any finite number of arbitrary divisibility conditions are ring equivalent to an appropriate single divisibility condition. We now construct recursive functions for reducing two divisibility conditions, the first normal, to one normal divisibility condition.

DEFINITION. Let m_1, n_1, m_2 and n_2 be integers such that $m_1 \geqq 0$ and $n_1 \geqq 1$. Recursive functions $f(m_1, n_1, m_2, n_2)$ and $g(m_1, n_1, m_2, n_2)$ are defined by cases. Below, let m denote $f(m_1, n_1, m_2, n_2)$ and n denote $g(m_1, n_1, m_2, n_2)$. (It is intended that $m \geqq 0$ and $n \geqq 1$ and $D(m, n)$ is ring equivalent to $D(m_1, n_1)$ & $D(m_2, n_2)$ in all cases.)

CASE 1. If $n_2 = 0$, then let $m = m_1$ and $n = n_1$.

CASE 2. If $n_2 \neq 0$ and $m_1, m_2 = 0$, then let $m = 0$ and $n = \text{g.c.d.}\ (n_1, |n_2|)$.

CASE 3. Suppose $m_2, n_2 \neq 0$ and $m_1 = 0$. Then let $m = 0$. Define n to be a divisor of n_1, $1 \leqq n \leqq n_1$, determined from its prime power factorization. Factor n_1, $|m_2|$ and $|n_2|$ into prime powers, and for each prime p dividing n_1, let $\text{expt}(n, p) = \text{expt}(|n_2|, p)$ if $\text{expt}(|n_2|, p) < \text{expt}(|m_2|, p)$ and $\text{expt}(|n_2|, p) < \text{expt}(n_1, p)$, and let $\text{expt}(n, p) = \text{expt}(n_1, p)$ otherwise.

CASE 4. Suppose $m_1, n_2 \neq 0$ and $m_2 = 0$. Then $m = 0$ and n is a positive divisor of $|n_2|$. For each prime p dividing $|n_2|$, let $\text{expt}(n, p) = \text{expt}(n_1, p)$ if $\text{expt}(n_1, p) < \text{expt}(m_1, p)$ and $\text{expt}(n_1, p) < \text{expt}(|n_2|, p)$, let $\text{expt}(n, p) = \text{expt}(|n_2|, p)$ otherwise.

CASE 5. Suppose $m_1, m_2, n_2 \neq 0$. Then m and n are positive divisors of $|m_1 m_2|$, computed by prime factorization. Suppose p is a prime dividing $|m_1 m_2|$. For $i = 1, 2$, let $x_i = \text{expt}(|n_i|, p)$ if $\text{expt}(|n_i|, p) < \text{expt}(|m_i|, p)$, and $x_i = \omega$ (plus infinity) otherwise. If $x_1 = x_2 = \omega$, let $\text{expt}(m, p) = \text{expt}(n, p) = 0$. Otherwise, let $\text{expt}(n, p)$ be the minimum of $\{x_1, x_2\}$, and $\text{expt}(m, p) = \text{expt}(n, p) + 1$.

EXAMPLE. Suppose $m_1 = 7840$, $n_1 = 280$, $m_2 = -756$ and $n_2 = 1584$. Then $m = f(m_1, n_1, m_2, n_2)$ and $n = g(m_1, n_1, m_2, n_2)$ are defined by case five. The prime factorizations are:

$$m_1 = 2^5 5^1 7^2, \quad n_1 = 2^3 5^1 7^1, \quad |m_2| = 2^2 3^3 7^1, \quad |n_2| = 2^4 3^2 11^1.$$

The primes dividing $|m_1 m_2|$ are 2, 3, 5 and 7, and we have:

$\text{expt}(n, 2) = \min\{3, \omega\} = 3$, $\text{expt}(m, 2) = 4$

$\text{expt}(n, 3) = \min\{\omega, 2\} = 2$, $\text{expt}(m, 3) = 3$.

$\text{expt}(n, 5) = \text{expt}(m, 5) = 0$.

$\text{expt}(n, 7) = \min\{1, 0\} = 0$, $\text{expt}(m, 7) = 1$.

Therefore, $m = 2^4 3^3 5^0 7^1 = 3024$ and $n = 2^3 3^2 5^0 7^0 = 72$.

PROPOSITION 2. *Suppose m_1, n_1, m_2 and n_2 are integers such that $m_1 \geqq 0$, $n_1 \geqq 1$, $m = f(m_1, n_1, m_2, n_2)$ and $n = g(m_1, n_1, m_2, n_2)$. Then $m \geqq 0$ and $n \geqq 1$, and $D(m, n)$ is satisfied in any ring R with 1 if and only if $D(m_1, n_1)$ and $D(m_2, n_2)$ are satisfied in R.*

We omit the proof, which is obtained by straightforward applications of Prop. 1, case by case.

We are now ready to describe the procedure which recursively constructs a divisibility condition $D(m(\Omega), n(\Omega))$ which is ring equivalent to any given productless system of ring equations Ω. Roughly, each equation $\mu = \nu$ of Ω corresponds to some nonhomogeneous $\mathbf{Z}$-linear equation, the left side a $\mathbf{Z}$-linear combination of the variables of Ω and the right side an integer multiple of the

ring unit. An integer matrix M and column vector V are constructed, corresponding to the productless system of equations Ω. In the next stage, a matrix A and vector U are formed by an old method of diagonalizing integer matrices. In 1879, Frobenius [4] used this method to study solutions modulo k of the integer matrix equation $MX = V$, X an unknown column vector. The classical proofs of the basis theorem for finitely-generated abelian groups also use this method [18: pp. 260–271]. In a weakened form, the theorem asserts that a diagonal matrix product $A = BMC = [a_{ij}]$, $a_{ij} = 0$ if $i \neq j$, can be computed from any rectangular integer matrix M, where B and C are (square) invertible integer matrices with integer inverses (see [16: Thm. 15, p. 361]). We will then verify that Ω is ring equivalent to a productless system of ring equations corresponding to A and the column vector $U = BV$. However, this system is ring equivalent to a conjunction of divisibility conditions because A is diagonal, and so Ω is ring equivalent to a single normal divisibility condition by iteration of Prop. 2.

PROCEDURE. Given a productless system Ω of ring equations, let $z_1, z_2, \ldots, z_t$ denote the variables of Ω, arranged in the order of the existential quantifiers of Ω, for example. We assume that $t \geqq 1$; if Ω contains no variables, then it is replaced by the equivalent formula $(\exists z_1)\Omega$. If the conjuncts of the formula matrix of Ω are equations $\mu_i = \nu_i$ of productless terms for $i \leqq s$, then we can recursively construct an $s \times t$ integer matrix $M = [m_{ij}]$ and an integer column vector $V = [v_i]$ of length s such that $\mu_i = \nu_i$ is ring equivalent to $\sum_{j=1}^{t} m_{ij} \cdot z_j = v_i \cdot 1$ for each $i \leqq s$. The ordered pair (M, V) is called the "matrix system" corresponding to Ω.

EXAMPLE. Suppose Ω is the productless system of ring equations:

$$(\exists x)(\exists y)(\exists w)([x + (-(y + (-x))) = y + (-1)] \,\&\, [(y + y) + y = (-x) + w]).$$

The 2×3 matrix system (M, V) for Ω is given by:

$$M = \begin{bmatrix} 2 & -2 & 0 \\ 1 & 3 & -1 \end{bmatrix} \quad \text{and} \quad V = \begin{bmatrix} -1 \\ 0 \end{bmatrix}.$$

PROCEDURE. Let $\mathcal{M}_n(\mathbf{Z})$ denote the ring of $n \times n$ integer matrices for $n \geqq 1$. From the $s \times t$ matrix system (M, V) for Ω, compute a diagonal $s \times t$ matrix $A = BMC = [a_{ij}]$ and the corresponding s-vector $U = BV = [u_i]$, where B is invertible so that B and B^{-1} are in $\mathcal{M}_s(\mathbf{Z})$ and C is invertible so that C and C^{-1} are in $\mathcal{M}_t(\mathbf{Z})$. The method is described in [16: pp. 361–364] and also discussed in the appendix.

If $s \leqq t$, let $d_i = a_{ii}$ for $i \leqq s$. If $s > t$, let $d_i = a_{ii}$ for $i \leqq t$, and let $d_i = 0$ for $t+1 \leqq i \leqq s$. Recursively define integer sequences $m_0, m_1, \ldots, m_s$ and $n_0, n_1, \ldots, n_s$, beginning with $m_0 = n_0 = 1$. For $0 < i \leqq s$, define:

$$m_i = f(m_{i-1}, n_{i-1}, d_i, u_i) \quad \text{and} \quad n_i = g(m_{i-1}, n_{i-1}, d_i, u_i).$$

Finally, define $m(\Omega) = m_s$ and $n(\Omega) = n_s$. Note that $m(\Omega) \geqq 0$ and $n(\Omega) \geqq 1$ by recursion using Prop. 2.

THEOREM 3. *Suppose R is a ring with 1, Ω is a productless system of ring equations, and $m = m(\Omega)$ and $n = n(\Omega)$ are integers obtained by the procedure given above. Then $m(\Omega)$ and $n(\Omega)$ are recursively computable from Ω, and Ω is satisfied in R if and only if the normal divisibility condition $(\exists x)(m \cdot x = n \cdot 1)$ is satisfied in R.*

Proof. Assume the hypotheses. It is clear that $m(\Omega)$ and $n(\Omega)$ can be computed recursively from Ω by the definitions. (See the appendix for further details.)

Let $\mathcal{M}_n(R)$ denote the ring of $n \times n$ matrices over R. To each $m \times n$ integer matrix $X = [x_{ij}]$, there corresponds an $m \times n$ matrix $X^R = [x_{ij} \cdot 1]$ with entries in R. It is easily verified that $(XY)^R = X^R Y^R$ if X and Y are $n \times k$ and $k \times m$ integer matrices, respectively. Also, $(I_n)^R$ is the identity matrix of $\mathcal{M}_n(R)$ if I_n is the identity matrix of $\mathcal{M}_n(\mathbf{Z})$. It follows that $(X^{-1})^R = (X^R)^{-1}$ if X has an inverse X^{-1} in the ring $\mathcal{M}_n(\mathbf{Z})$.

By the construction of (M, V) from Ω, it is easily seen that Ω is satisfied in R iff there exists a t-vector Z on R such that $M^R Z = V^R$. Defining B and B^{-1} in $\mathcal{M}_s(\mathbf{Z})$ and C and C^{-1} in $\mathcal{M}_t(\mathbf{Z})$ as in the procedure, we have $M^R Z = V^R$ iff $B^R M^R C^R (C^R)^{-1} Z = B^R V^R$ iff $A^R (C^R)^{-1} Z = U^R$, with $A = BMC$ and $U = BV$ as before. So, there exists a t-vector Z on R such that $M^R Z = V^R$ iff there exists a t-vector Y on R such that $A^R Y = U^R$. (Take $Y = (C^R)^{-1} Z$ if Z exists, and take $Z = C^R Y$ if Y exists.)

Let $Y = [y_j]$ be a t-vector on R. Suppose $s \leqq t$, and define $d_i = a_{ii}$ for $i \leqq s$, as before. Since A is diagonal, $A^R Y = [d_i \cdot y_i]_{i \leqq s}$. Therefore, $A^R Y = U^R$ iff $d_i \cdot y_i = u_i \cdot 1$ for $i \leqq s$. Alternatively, assume $s > t$, and define $d_i = a_{ii}$ for $i \leqq t$ and $d_i = 0$ for $t+1 \leqq i \leqq s$. Then $A^R Y = U^R$ iff $d_i \cdot y_i = u_i \cdot 1$ for $i \leqq t$ and $0 = u_i \cdot 1$ for $t+1 \leqq i \leqq s$. Whether $s \leqq t$ or $s > t$, therefore, there exists a t-vector Y on R such that $A^R Y = U^R$ iff there exist $y_1, y_2, \ldots, y_s$ in R such that $d_i \cdot y_i = u_i \cdot 1$ for $i \leqq s$. Therefore, Ω is satisfied in R if and only if the s divisibility conditions $D(d_i, u_i)$, $i \leqq s$, are satisfied in R. By recursion on the definitions using Prop. 2,

$D(m(\Omega), n(\Omega))$ is satisfied in R if and only if $D(1, 1)$ and the s divisibility conditions above are satisfied in R. Therefore, Ω is satisfied in R if and only if the normal divisibility condition $(\exists x)(m(\Omega) \cdot x = n(\Omega) \cdot 1)$ is satisfied in R, proving Thm. 3.

COROLLARY 1. *If R is a ring with 1 and the set of divisibility conditions satisfied in R is recursive, then the word problem for the free lattice L with denumerably many generators in $\mathbf{H}\mathscr{L}(R)$ is recursively solvable. In particular, the word problem for L is solvable if R has nonzero characteristic.*

Proof. Assuming the hypotheses, equality of words in L occurs if and only if the corresponding lattice identity is satisfied in every lattice in $\mathbf{H}\mathscr{L}(R)$ [5: Thm. 1, pp. 169–170]. The result then follows directly from Thms. 2 and 3 and Prop. 1. If R has characteristic $j \geqq 1$, then $d \prec e$ in L if and only if the g.c.d. of $m(\Omega(d, e))$ and j divides $n(\Omega(d, e))$.

COROLLARY 2. *Let R and S be rings with 1. Then $\mathbf{H}\mathscr{L}(R) = \mathbf{H}\mathscr{L}(S)$ if the set of divisibility conditions satisfied in R and in S are the same. If R and S have the same nonzero characteristic, then $\mathbf{H}\mathscr{L}(R) = \mathbf{H}\mathscr{L}(S)$. If R and S both have characteristic zero and the degrees of invertibility $\theta(R, p)$ and $\theta(S, p)$ are equal for each prime p, then $\mathbf{H}\mathscr{L}(R) = \mathbf{H}\mathscr{L}(S)$.*

Proof. Again Thms. 2 and 3 and Prop. 1 suffice, since $\mathbf{H}\mathscr{L}(R)$ and $\mathbf{H}\mathscr{L}(S)$ are varieties and so are determined by the lattice identities satisfied in all their member lattices.

A surprising consequence of this result is that $\mathbf{H}\mathscr{L}(R)$ depends only on the additive group structure of R and the position of the ring unit in that group; one need not know the ring multiplication of R in order to determine $\mathbf{H}\mathscr{L}(R)$.

COROLLARY 3. *Suppose $R = \prod_{i \in I} R_i$ is the product ring formed from an indexed family $\{R_i\}_{i \in I}$ of rings with 1. Then $\mathbf{H}\mathscr{L}(R)$ is the join $\bigvee \{\mathbf{H}\mathscr{L}(R_i) : i \in I\}$ in the complete lattice of all varieties of meet and join algebras.*

Proof. Assume the hypotheses. It suffices to show that any arbitrary lattice identity is satisfied throughout $\mathbf{H}\mathscr{L}(R)$ if and only if it is satisfied throughout $\mathbf{H}\mathscr{L}(R_i)$ for all i in I. But any normal divisibility condition is clearly satisfied in R iff it is satisfied in R_i for all i in I, and so the result follows from Thms. 2 and 3.

Combining Thms. 2 and 3, we note two special cases. For a lattice polynomial inclusion formula $d \prec e$, let $m = m(\Omega(d, e))$ and $n = n(\Omega(d, e))$. First, $d \prec e$ is

satisfied in every lattice representable by modules if and only if $m = n = 1$. (Clearly $m > 0$, and so m_i and n_i must have been defined from case 1 or 5 of the definitions of f and g for each i, $0 < i \leqq s$. So, n divides m by recursion through the sequences m_i and n_i, $0 \leqq i \leqq s$. But $D(m, n)$ is not satisfied in $\mathbf{Z}$ if $0 < n < m$, and the only other possible outcome is $m = n = 1$.) Second, if $d \subset e$ is not satisfied throughout $\mathbf{H}\mathscr{L}(R)$ for any nontrivial R, then $m = 0$ and $n = 1$. (Note that $D(m, n)$ is satisfied in the field of rationals $\mathbf{Q}$ for $m > 0$, and $D(0, n)$ is satisfied in $\mathbf{Z}_n$ for $n > 1$.)

§3. Lattice variety classification and the word problem.

The reduction of lattice identities to ring divisibility conditions makes possible a detailed analysis of the lattice varieties of the form $\mathbf{H}\mathscr{L}(R)$. Before beginning this study, we insert a preparatory result and corollary.

PROPOSITION 3. *Suppose R and S are rings with 1, and there exists a function $f: R \to S$ preserving addition and satisfying $f(1) = 1$. (Ring multiplication is not necessarily preserved by f.) Then every divisibility condition satisfied in R is also satisfied in S, and so $\mathbf{H}\mathscr{L}(S) \subset \mathbf{H}\mathscr{L}(R)$.*

Proof. Assume the hypotheses. If $m \cdot r = n \cdot 1$ for some r in R, then $m \cdot f(r) = n \cdot 1$ in S. So, every divisibility condition satisfied in R is also satisfied in S, and therefore $\mathbf{H}\mathscr{L}(S) \subset \mathbf{H}\mathscr{L}(R)$ by Thms. 2 and 3.

COROLLARY 4. *Suppose R is a ring with 1, and S is a subring of the ring $\mathscr{M}_n(R)$ of $n \times n$ matrices over R. If S contains rI for every r in R, where I is the $n \times n$ identity matrix over R, then $\mathbf{H}\mathscr{L}(R) = \mathbf{H}\mathscr{L}(S)$.*

Proof. Assume the hypotheses. Clearly, $r \mapsto rI$ is a ring homomorphism $R \to S$ preserving 1. Let B_{11} denote the upper left element of the matrix B. Then $B \mapsto B_{11}$ is a function $S \to R$ preserving addition and mapping I to 1, although it is not a ring homomorphism in general. However, $\mathbf{H}\mathscr{L}(R) = \mathbf{H}\mathscr{L}(S)$ then follows from Prop. 3, proving Cor. 4.

We next show that the degrees of invertibility of primes are completely independent and unrestricted parameters for rings with characteristic zero.

DEFINITION. Let $\mathbf{Q}$ denote the field of rationals. For p prime, let $\mathbf{Q}_p$ be the subring of $\mathbf{Q}$ generated by $\{1/q : q \in P - \{p\}\}$, where P denotes the set of all primes.

Note that every prime except p is invertible in $\mathbf{Q}_p$, but $\theta(\mathbf{Q}_p, p) = \omega$. Let $\mathbf{Z}[X]$ denote the commutative ring of all polynomials on the variables $X = \{x_p : p \in P\}$ with integer coefficients; we will use the fact that $\mathbf{Z}[X]$ is the free ring generated by X in the variety of commutative rings with 1. If $f: P \to [0, \omega]$ is an arbitrary function from the set of primes P into the segment $[0, \omega]$ of cardinal numbers, then R_f denotes the ring $\mathbf{Z}[X]/\mathbf{a}(f)$, where $\mathbf{a}(f)$ is the ideal of $\mathbf{Z}[X]$ generated by:

$$\{p^{f(p)+1} \cdot x_p - p^{f(p)} \cdot 1 : p \in P, f(p) < \omega\}.$$

(For example, if $f(2) = 3$ and $f(p) = \omega$ for odd primes p, then $\mathbf{a}(f)$ is the principal ideal of $\mathbf{Z}[X]$ generated by $16 \cdot x_2 - 8 \cdot 1$.)

PROPOSITION 4. *For any function $f: P \to [0, \omega]$, R_f is a commutative ring with characteristic zero such that $\theta(R_f, p) = f(p)$ for each prime p.*

Proof. Clearly R_f is a commutative ring with 1, and R_f has characteristic zero because there is a ring homomorphism $g: R_f \to \mathbf{Q}$ preserving 1 such that $g(x_p + \mathbf{a}(f)) = 1/p$ for all primes p. If $f(p) = \omega$, then there is a ring homomorphism $g_p: R_f \to \mathbf{Q}_p$ preserving 1 such that $g_p(x_p + \mathbf{a}(f)) = 0$ and $g_p(x_q + \mathbf{a}(f)) = 1/q$ for q in $P - \{p\}$. Since $\theta(\mathbf{Q}_p, p) = \omega$, we also have $\theta(R_f, p) = \omega$ by Prop. 3.

Suppose $f(p) < \omega$. By construction, $D(p^{f(p)+1}, p^{f(p)})$ is satisfied via $x_p + \mathbf{a}(f)$ in R_f. So, $\theta(R_f, p) \leqq f(p)$. Let S equal $\mathbf{Q}_p[x_p]/\mathbf{b}$, the quotient of the polynomial ring on x_p with coefficients in $\mathbf{Q}_p$ divided by the principal ideal $\mathbf{b}$ generated by $p^{f(p)+1} \cdot x_p - p^{f(p)} \cdot 1$. There exists a ring homomorphism $h: R_f \to S$ preserving 1 such that $h(x_p + \mathbf{a}(f)) = x_p + \mathbf{b}$ and $h(x_q + \mathbf{a}(f)) = 1/q + \mathbf{b}$ for q in $P - \{p\}$. Suppose $D(p^{\beta+1}, p^\beta)$ is satisfied in R_f, and so is satisfied in S by Prop. 3, and so $p^{\beta+1} \cdot u - p^\beta \cdot 1 = (p^{f(p)+1} \cdot x_p - p^{f(p)} \cdot 1)v$ for some u, v in $\mathbf{Q}_p[x_p]$. If $\beta < f(p)$, then $D(p^{\beta+1}, p^\beta)$ is satisfied in $\mathbf{Q}_p[x_p]$, and hence in $\mathbf{Q}_p$ by Prop. 3 using the ring homomorphism $\mathbf{Q}_p[x_p] \to \mathbf{Q}_p$ obtained by replacing x_p by 0, and this contradicts $\theta(\mathbf{Q}_p, p) = \omega$. Therefore, $\beta \geqq f(p)$, and so $\theta(R_f, p) \geqq f(p)$, completing Prop. 4.

We now construct lattice identities on four and five variables that discriminate according to ring divisibility conditions. The methods of C. Herrmann and A. Huhn are extensively used. In [8], they define identities χ_k and ε_k for $k \geqq 2$ which distinguish between varieties $\mathbf{H}\mathscr{L}(R)$ according to certain divisibility conditions. Specifically, χ_k is satisfied throughout $\mathbf{H}\mathscr{L}(R)$ iff the characteristic of R divides k, that is, $D(0, k)$ is satisfied in R. Also, ε_k is satisfied throughout $\mathbf{H}\mathscr{L}(R)$ iff $k \cdot 1$ is invertible in R, that is, $D(k, 1)$ is satisfied in R. In unpublished work, A. Huhn has obtained lattice identities corresponding to other divisibility conditions. The two authors' separate approaches are given next.

DEFINITION. For variables x_1, x_2, x_3, x_4, recursively define:

$$b = (x_1 \wedge x_3) \vee (x_2 \wedge x_4),$$

$$c_1 = d_1 = (x_1 \wedge x_2) \vee (x_3 \wedge x_4),$$

$$c_{i+1} = \{[(c_i \wedge b) \vee (x_2 \wedge x_3)] \wedge x_1\} \vee (x_3 \wedge x_4)$$

and

$$d_{i+1} = \{[(d_i \wedge b) \vee (x_1 \wedge x_4)] \wedge x_2\} \vee (x_3 \wedge x_4).$$

Then define $\eta(m, n)$ on x_1, x_2, x_3, x_4, x_5 to be the identity:

$$q \subset \{[(c_{m-1} \wedge b) \vee x_5] \wedge x_2\} \vee d_{n-1},$$

where

$$q = b \wedge [(x_1 \wedge x_4) \vee (x_2 \wedge x_3)] \wedge x_5,$$

for all $m, n \geqq 2$.

DEFINITION. Let lattice polynomials d and e_k, f_k for $k \geqq 0$ on the variables x_1, x_2, x_3, x_4 be given by the following recursion equations:

$$d = (x_1 \vee x_2) \wedge (x_3 \vee x_4),$$

$$e_0 = x_1, \quad e_{k+1} = (f_{k+1} \vee d) \wedge (x_1 \vee x_3)$$

$$f_0 = x_2, \quad f_{k+1} = (e_k \vee x_4) \wedge (x_2 \vee x_3).$$

(By substitution, we can obtain recursion relations expressing e_{k+1} as a polynomial in e_k, x_1, x_2, x_3, x_4 for $k \geqq 0$ and f_{k+1} as a polynomial in f_k, x_1, x_2, x_3, x_4 for $k \geqq 1$.) Then we define lattice identities $\Delta(m, n)$ for $m \geqq 0$ and $n \geqq 1$ by the following expression:

$$d \subset x_2 \vee e_n \vee f_m.$$

This defines the two sets η and Δ of lattice identities.

We remark that the identities χ_k and ε_k for $k \geqq 2$ given in [8] are expressible

(with notation changed), respectively by:

$$f_{k-1} \subset d \vee [(x_1 \vee x_3) \wedge (x_2 \vee x_4)]$$

and

$$d^* \wedge [(x_1 \wedge x_3) \vee (x_2 \wedge x_4)] \subset f_k^* \vee x_2,$$

where e^* denotes the polynomial dual to a given lattice polynomial e. C. Herrmann (private communication) remarks that $f_n \subset f_m \vee x_1 \vee x_2$ is also equivalent to $D(m, n)$ for the ring.

Note that the η and Δ identities are all inclusions of a small lattice polynomial in a lattice polynomial constructed by a recursion formula. In this situation, it is often easier to determine equivalent ring divisibility conditions by the use of Thm. 1(2) than by the general method of Thms. 2 and 3. Of course, we can transfer the computation from the algebra of relations on a free R-module to its lattice of submodules. In the next two propositions, we use this method to verify the appropriate properties of our lattice identities.

PROPOSITION 5. *Suppose $m, n \geqq 2$ and R is a ring with 1. Then $\eta(m, n)$ is satisfied in every lattice in $\mathbf{HL}(R)$ if and only if the divisibility condition $D(m, n)$ is satisfied in R.*

PROOF. Assume the hypotheses. Let $\eta(m, n)$ be $q \subset e$, where q is defined above and e denotes the lattice polynomial on the right side of the inclusion. Compute $F(q^\circ)$ and the associated partitions of $\{a_1, a_2, a_3, a_4\}$ as follows:

$$\phi_1 = \{\{a_1, a_3, a_4\}, \{a_2\}\}, \quad \phi_2 = \{\{a_1\}, \{a_2, a_3, a_4\}\},$$
$$\phi_3 = \{\{a_1, a_3\}, \{a_2, a_4\}\}, \quad \phi_4 = \{\{a_1, a_4\}, \{a_2, a_3\}\},$$
$$\phi_5 = \{\{a_1, a_2\}, \{a_3\}, \{a_4\}\}.$$

Let V_4 denote the free R-module on $\{a_1, a_2, a_3, a_4\}$, so $\sum_{i=1}^4 r_i a_i = 0$ in V_4 for r_i in R, $i \leqq 4$, implies that $r_i = 0$ for $i \leqq 4$. Let $g(x_k)$ be the congruence on V_4 generated by ϕ_k for $k \leqq 5$, and let $g^*: C_5 \to \mathrm{Rel}(V_4)$ preserve intersection and composition such that $g^*(x_k) = g(x_k)$ for $k \leqq 5$. By Thm. 1, $q^\circ \subset e^\circ$ is satisfied for congruences in $\mathrm{Rel}(M)$ for every M in R-**Mod** if and only if $g^*(q^\circ) \subset g^*(e^\circ)$. For M in R-**Mod**, let $\mathbf{Su}(M)$ denote the lattice of submodules of M, so $\mathbf{Su}(M)$ and $\mathbf{Con}(M)$ are isomorphic lattices. Defining $h(x_1) = R(a_1 - a_3) + R(a_1 - a_4)$, $h(x_2) = R(a_2 - a_3) + R(a_2 - a_4)$, $h(x_3) = R(a_1 - a_3) + R(a_2 - a_4)$, $h(x_4) = R(a_1 - a_4) + R(a_2 - a_3)$ and $h(x_5) = R(a_1 - a_2)$ in $\mathbf{Su}(V_4)$, we see that $g(x_k)$ in $\mathbf{Con}(V_4)$ corresponds to $h(x_k)$ in $\mathbf{Su}(V_4)$ for $k \leqq 5$. Let W_5 be the meet and join algebra of all lattice polynomials on $\{x_1, x_2, x_3, x_4, x_5\}$, and let $h^*: W_5 \to \mathbf{Su}(V_4)$ be

the unique meet and join homomorphism such that $h^*(x_k) = h(x_k)$ for $k \leqq 5$. Since R-**Mod** is a congruence-permutable variety, it follows that $q \subset e$ is satisfied in every lattice in $\mathbf{H}\mathscr{L}(R)$ if and only if $h^*(q) \subset h^*(e)$ in $\mathbf{Su}(V_4)$.

By direct computations in $\mathbf{Su}(V_4)$, we see that:

$$h^*(b) = R(a_1 - a_3) + R(a_2 - a_3), \quad \text{and for } k \geqq 1,$$
$$h^*(c_k) = R(k \cdot a_1 + a_2 - (k+1) \cdot a_3) + R(a_1 + a_2 - a_3 - a_4),$$
$$h^*(d_k) = R(a_1 + k \cdot a_2 - (k+1) \cdot a_3) + R(a_1 + a_2 - a_3 - a_4).$$

It follows that $h^*(q) \subset h^*(e)$ in $\mathbf{Su}(V_4)$ if and only if:

$$R(a_1 - a_2) \subset R(m \cdot a_2 - m \cdot a_3) + R(a_1 + (n-1) \cdot a_2 - n \cdot a_3) + R(a_1 + a_2 - a_3 - a_4).$$

The condition above is equivalent to the existence of r_1, r_2, r_3 in R such that:

$$a_1 - a_2 = r_1(m \cdot a_2 - m \cdot a_3) + r_2(a_1 + (n-1) \cdot a_2 - n \cdot a_3) + r_3(a_1 + a_2 - a_3 - a_4).$$

Since V_4 is free, it follows that the above equation holds if and only if $r_2 = 1$, $r_3 = 0$ and $m \cdot (-r_1) = n \cdot 1$ in R. So, $h^*(q) \subset h^*(e)$ if and only if the divisibility condition $D(m, n)$ is satisfied in R. This proves Prop. 5.

PROPOSITION 6. *Suppose $m \geqq 0$, $n \geqq 1$ and R is a ring with 1. Then $\Delta(m, n)$ is satisfied in every lattice in $\mathbf{H}\mathscr{L}(R)$ if and only if the divisibility condition $D(m, n)$ is satisfied in R.*

Proof. It is possible to verify Prop. 6 using [10: 311–318], as was done in the earliest proof. However, the method of Thm. 1(2) is selfcontained and shorter, so we outline it here.

Let e denote $x_2 \vee e_n \vee f_m$, so $\Delta(m, n)$ is $d \subset e$ with $d = (x_1 \vee x_2) \wedge (x_3 \vee x_4)$ as above. Construct $F(d^\circ)$ and the associated partitions as for the Fano identity example. Similar to Prop. 5, we have the unique meet and join homomorphism $h^*: W_4 \to \mathbf{Su}(V_4)$ such that $h(x_1) = R(a_1 - a_3)$, $h(x_2) = R(a_2 - a_3)$, $h(x_3) = R(a_1 - a_4)$ and $h(x_4) = R(a_2 - a_4)$ in $\mathbf{Su}(V_4)$. By the argument above, $d \subset e$ is satisfied in every lattice in $\mathbf{H}\mathscr{L}(R)$ if and only if $h^*(d) \subset h^*(e)$. Again computing, we see that:

$$h^*(d) = R(a_1 - a_2),$$
$$h^*(f_k) = R(k \cdot a_1 + a_2 - a_3 - k \cdot a_4) \quad \text{for} \quad k \geqq 0,$$
$$h^*(e_k) = R((k+1) \cdot a_1 - a_3 - k \cdot a_4) \quad \text{for} \quad k \geqq 0.$$

Therefore, $h^*(d) \subset h^*(e)$ in $\mathbf{Su}(V_4)$ if and only if:

$$R(a_1 - a_2) \subset R(a_2 - a_3) + R((n+1) \cdot a_1 - a_3 - n \cdot a_4) + R(m \cdot a_1 + a_2 - a_3 - m \cdot a_4).$$

We can then show that $h^*(d) \subset h^*(e)$ if and only if $D(m, n)$ is satisfied in R, by an argument similar to the proof of Prop. 5. This proves Prop. 6.

We can now complete the classification of all distinct lattice varieties generated by lattices of submodules over a fixed ring. As previously noted, the rings $\mathbf{Z}_k$ for $k \geqq 1$ and R_f for $f: P \to [0, \omega]$ are in one-one correspondence with the distinct lattice varieties of this kind.

THEOREM 4. *Suppose R is a ring with 1. Then $\mathbf{H}\mathscr{L}(R) = \mathbf{H}\mathscr{L}(\mathbf{Z}_k)$ if and only if R has characteristic k, $k \geqq 1$. Furthermore, $\mathbf{H}\mathscr{L}(R) = \mathbf{H}\mathscr{L}(R_f)$ for $f: P \to [0, \omega]$ if and only if R has characteristic zero and $f(p)$ equals the degree of invertibility $\theta(R, p)$ of p in R for all primes p.*

Proof. It follows from consideration of the identities χ_k of [8: Satz 5, p. 188] or $\Delta(0, k)$ of Prop. 6 that $\mathbf{H}\mathscr{L}(R) = \mathbf{H}\mathscr{L}(S)$ implies that R and S are rings with the same characteristic. Therefore, $\mathbf{H}\mathscr{L}(R) = \mathbf{H}\mathscr{L}(\mathbf{Z}_k)$ if and only if R has characteristic k, $k \geqq 1$, by Cor. 2.

Suppose $\mathbf{H}\mathscr{L}(R) = \mathbf{H}\mathscr{L}(R_f)$ for $f: P \to [0, \omega]$. Then R has zero characteristic by the above. Using Prop. 4 and considering the lattice identities $\eta(p^{\beta+1}, p^\beta)$ of Prop. 5 or $\Delta(p^{\beta+1}, p^\beta)$ of Prop. 6, we see that $\theta(R, p) = \theta(R_f, p) = f(p)$ for all primes p. Finally, if R has characteristic zero and $\theta(R, p) = f(p)$ for all primes p, then $\mathbf{H}\mathscr{L}(R) = \mathbf{H}\mathscr{L}(R_f)$ by Prop. 4 and Cor. 2. This proves Thm. 4.

It is not difficult now to give the inclusion and join relations between the varieties $\mathbf{H}\mathscr{L}(R)$ for all rings R with 1, in the complete lattice $\mathscr{U}$ of all varieties of meet and join algebras. By Thm. 4, we need only consider the rings $\mathbf{Z}_k$ for $k \geqq 1$ and R_f for $f: P \to [0, \omega]$.

THEOREM 5. *Let $j, k \geqq 1$ and $f, g: P \to [0, \omega]$. Then:*

(1) $\mathbf{H}\mathscr{L}(\mathbf{Z}_j) \subset \mathbf{H}\mathscr{L}(\mathbf{Z}_k)$ *if and only if j divides k.*

(2) $\mathbf{H}\mathscr{L}(\mathbf{Z}_j) \subset \mathbf{H}\mathscr{L}(R_f)$ *if and only if* $\operatorname{expt}(j, p) \leqq f(p)$ *for all primes p.*

(3) $\mathbf{H}\mathscr{L}(R_f) \subset \mathbf{H}\mathscr{L}(\mathbf{Z}_j)$ *is always false.*

(4) $\mathbf{H}\mathscr{L}(R_f) \subset \mathbf{H}\mathscr{L}(R_g)$ *if and only if $f(p) \leqq g(p)$ for all primes p.*

(5) *Suppose R_i is a ring with characteristic n_i, for all i in some nonempty index set I. If $\{n_i : i \in I\}$ is a bounded set of integers not containing zero, then it has a least common multiple n, and $\mathbf{H}\mathscr{L}(\mathbf{Z}_n)$ is the join of all the varieties $\mathbf{H}\mathscr{L}(R_i)$, $i \in I$, in the*

complete lattice of varieties $\mathcal{U}$. If $\{n_i : i \in I\}$ is unbounded or contains zero, then it has no least common multiple. In this case, the join in $\mathcal{U}$ of all $\mathbf{HS}(R_i)$, $i \in I$, is $\mathbf{HS}(R_f)$, where $f(p) = \sup\{\theta(R_i, p) : i \in I\}$ for all primes p.

Proof. Assume the hypotheses. If j divides k, then there is a ring homomorphism $\mathbf{Z}_k \to \mathbf{Z}_j$ preserving 1, and so $\mathbf{HS}(\mathbf{Z}_j) \subset \mathbf{HS}(\mathbf{Z}_k)$ by Prop. 3. If $\mathbf{HS}(\mathbf{Z}_j) \subset \mathbf{HS}(\mathbf{Z}_k)$, then $\Delta(0, k)$ is satisfied throughout $\mathbf{HS}(\mathbf{Z}_j)$, and so j divides k, by Prop. 6. This proves part (1).

Suppose $\exp(j, p) \leqq f(p)$ for all primes p. Then $(\exists x)(j \cdot x = m \cdot 1)$ has no solution in R_f for any m, $0 < m < j$, since otherwise $\exp(j, p) \leqq \exp(m, p)$ for all primes p by Props. 1 and 4, which contradicts $0 < m < j$. Therefore, the ideal $(j \cdot 1)R_f$ of R_f doesn't contain $m \cdot 1$ for $0 < m < j$, so $R_f/(j \cdot 1)R_f$ is a ring with characteristic j. Since there is a cononical ring homomorphism $R_f \to R_f/(j \cdot 1)R_f$ preserving 1, we have $\mathbf{HS}(\mathbf{Z}_j) = \mathbf{HS}(R_f/(j \cdot 1)R_f) \subset \mathbf{HS}(R_f)$ by Thm. 4 and Prop. 3. Suppose $\mathbf{HS}(\mathbf{Z}_j) \subset \mathbf{HS}(R_f)$, so $\Delta(p^{f(p)+1}, p^{f(p)})$ is satisfied in $\mathbf{HS}(\mathbf{Z}_j)$ for each prime p such that $f(p) < \omega$, by Props. 4 and 6. But then $\exp(j, p) \leqq f(p)$ for each prime p by Props. 1 and 6, proving part (2).

Clearly $\mathbf{HS}(R_f) \subset \mathbf{HS}(\mathbf{Z}_j)$ is always false, since $\Delta(0, j)$ is satisfied throughout $\mathbf{HS}(\mathbf{Z}_j)$ but not throughout $\mathbf{HS}(R_f)$ by Prop. 6. This proves part (3).

Suppose $f(p) \leqq g(p)$ for all primes p. Then $R_f = \mathbf{Z}[X]/\mathbf{a}(f)$ and $R_g = \mathbf{Z}[X]/\mathbf{a}(g)$ for the commutative ring $\mathbf{Z}[X]$ and certain ideals $\mathbf{a}(f)$ and $\mathbf{a}(g)$ such that $\mathbf{a}(g) \subset \mathbf{a}(f)$, using the definitions. So, there is a ring homomorphism $R_g \to R_f$ preserving 1, and $\mathbf{HS}(R_f) \subset \mathbf{HS}(R_g)$ by Prop. 3. Suppose $\mathbf{HS}(R_f) \subset \mathbf{HS}(R_g)$, so $\Delta(p^{\beta+1}, p^{\beta})$ is satisfied in $\mathbf{HS}(R_f)$ whenever it is satisfied in $\mathbf{HS}(R_g)$ for any prime p and $\beta \geqq 0$. It follows by Props. 4 and 6 that $f(p) \leqq g(p)$ for every prime p, proving part (4).

Suppose $R = \prod_{i \in I} R_i$ for some nonempty family $\{R_i\}_{i \in I}$ of rings with 1. By Cor. 3, $\mathbf{HS}(R)$ is the join in $\mathcal{U}$ of all the varieties $\mathbf{HS}(R_i)$, $i \in I$. If $\{n_i : i \in I\}$ has a least common multiple n, then R has characteristic n, and so $\mathbf{HS}(R) = \mathbf{HS}(\mathbf{Z}_n)$ by Thm. 4. Suppose $\{n_i : i \in I\}$ is unbounded or contains zero. Then R has characteristic zero. Clearly, $D(p^{\beta+1}, p^{\beta})$ is satisfied in R if and only if it is satisfied in R_i for all i in I, for p prime and $\beta \geqq 0$. Therefore, $f(p) = \sup\{\theta(R_i, p) : i \in I\}$ is the degree of invertibility of p in R, and so $\mathbf{HS}(R) = \mathbf{HS}(R_f)$ by Thm. 4. This proves (5), completing the proof of Thm. 5.

Note that $\mathbf{HS}(\mathbf{Q}) \subset \mathbf{HS}(R)$ if and only if R has characteristic zero by Thm. 5(3, 4) and Thm. 4. So, the minimal nontrivial varieties of form $\mathbf{HS}(R)$ for rings R with 1 are $\mathbf{HS}(\mathbf{Q})$ and $\mathbf{HS}(\mathbf{Z}_p)$ *for* p prime, the field cases, by Thm. 5(1, 2, 3). The unique largest variety of form $\mathbf{HS}(R)$ is clearly $\mathbf{HS}(\mathbf{Z})$.

In general, the intersection of varieties of form $\mathbf{HS}(R)$ for rings R with 1 need not be of the same form. For example, $\mathbf{HS}(\mathbf{Z}_2) \cap \mathbf{HS}(\mathbf{Q})$ contains all distributive

lattices, among others. However, a ring R with 1 such that $\mathbf{H}\mathscr{L}(R) \subset \mathbf{H}\mathscr{L}(\mathbf{Z}_2) \cap \mathbf{H}\mathscr{L}(\mathbf{Q})$ is trivial, so $\mathbf{H}\mathscr{L}(R) \neq \mathbf{H}\mathscr{L}(\mathbf{Z}_2) \cap \mathbf{H}\mathscr{L}(\mathbf{Q})$ because $\mathbf{H}\mathscr{L}(R)$ then contains only the trivial lattice.

In Cor. 1, we noted that word problems for free lattices in $\mathbf{H}\mathscr{L}(R)$ are recursively solvable if R has nonzero characteristic. The next result deals with rings of characteristic zero. Essentially, free lattices in $\mathbf{H}\mathscr{L}(R)$ have solvable word problems if we can recursively decide whether $\theta(R, p) = k$ for primes p and finite k, even if we can't recursively decide whether $\theta(R, p) = \omega$ or not.

THEOREM 6. *Suppose R is a ring with characteristic zero and $\theta(R, p)$ is the degree of invertibility of p in R for each prime p. Then the word problem for the free $\mathbf{H}\mathscr{L}(R)$-lattice L on denumerably many generators is recursively solvable if and only if $f^*(j, p) = \min\{j, \theta(R, p)\}$ is a recursive function on $\{j : j \geqq 1\} \times P$. In particular, the word problem for L is recursively solvable if $p \mapsto \theta(R, p)$ is a recursive function on the set of primes P.*

PROOF. Assume the hypotheses. If the word problem for L is recursively solvable, we can compute $f^*(j, p)$ as follows: $f^*(j, p) = j$ if all the formulas $\Delta(p^{k+1}, p^k)$ for $0 \leqq k < j$ are not true for L, and otherwise $f^*(j, p)$ is the smallest k such that $\Delta(p^{k+1}, p^k)$ is true for L. By Prop. 6, $f^*(j, p) = k < j$ if and only if $\theta(R, p) = k$ for $k < j$. So, the indicated procedure computes $\min\{j, \theta(R, p)\}$ for $j \geqq 1$ and p prime.

Suppose $f^*(j, p)$ is recursively computable, and d and e are lattice polynomials on the generating set $\{x_i : i \geqq 1\}$ for L. Let $m = m(\Omega(d, e))$ and $n = n(\Omega(d, e))$. By Thms. 2 and 3, $d \subset e$ in L if and only if $D(m, n)$ is satisfied in R. If $m = 0$, then $d \subset e$ is false in L. Assuming $m, n \geqq 1$ and using Prop. 1, $d \subset e$ in L iff $\theta(R, p) \leqq \operatorname{expt}(n, p)$, or equivalently $f^*(n, p) \leqq \operatorname{expt}(n, p)$, for all primes p such that $\operatorname{expt}(n, p) < \operatorname{expt}(m, p)$. Since f^* is recursive and there are only finitely many primes dividing m, there is a recursive procedure solving the word problem for L.

If $p \mapsto \theta(R, p)$ is recursive, then $f^*(j, p) = \min\{j, \theta(R, p)\}$ is recursive, so the word problem for L is solvable. This completes Thm. 6.

COROLLARY 5. *Suppose R is a torsion-free ring with 1, and P_0 is the set of primes p such that $p \cdot 1$ is invertible in R. Then $\mathbf{H}\mathscr{L}(R)$ depends only on P_0, and the free $\mathbf{H}\mathscr{L}(R)$-lattice on denumerably many generators has a recursively solvable word problem if and only if P_0 is a recursive set of primes.*

Proof. Assume the hypotheses. If $D(p^{\beta+1}, p^\beta)$ is satisfied in R via r for any $\beta \geqq 0$, then $p^\beta \cdot (p \cdot r - 1) = 0$, and so p is in P_0 since R is torsion-free. So,

$\theta(R, p) = 0$ for p in P_0 and $\theta(R, p) = \omega$ for p in $P - P_0$. Then $f^*(j, p) = j(1 - \chi(p))$, where $\chi(p)$ is the characteristic function of the set P_0 in P. Therefore, f^* is recursively computable if and only if χ is recursively computable. It follows that the word problem for L is solvable if and only if P_0 is a recursive set of primes, by Thm. 6. Since R has characteristic zero, $\mathbf{H}\mathscr{L}(R)$ depends only on P_0 because $\theta(R, p)$ is determined by P_0, using Thm. 4. This proves Cor. 5.

Since the unitary subrings of the rational field $\mathbf{Q}$ are torsion-free, Cor. 5 applies. These rings are uniquely determined by their invertible primes; the function $P_0 \mapsto \mathbf{Q}(P_0)$ is a one-one correspondence from subsets P_0 of P to unitary subrings of $\mathbf{Q}$ if $\mathbf{Q}(P_0)$ is the unitary subring generated by $\{1/p : p \in P_0\}$ [9: p. 86].

COROLLARY 6. *Suppose R is a (von Neumann) regular ring with zero characteristic, and P_0 is the set of primes p such that $p \cdot 1$ is invertible in R. Then $\mathbf{H}\mathscr{L}(R)$ depends only on P_0, and the free $\mathbf{H}\mathscr{L}(R)$-lattice on denumerably many generators has a recursively solvable word problem if and only if P_0 is a recursive set of primes.*

Proof. Assume the hypotheses. For p prime, there exists r in R such that $(p \cdot 1)r(p \cdot 1) = p \cdot 1$, by the regularity of R. Since $p \cdot 1$ is central in R, it follows that $D(p^2, p)$ is satisfied in R. So, every prime p has degree of invertibility 0 or 1 in R, and $f^*(j, p) = \theta(R, p) = 1 - \chi(p)$ for all $j \geqq 1$ and primes p. Therefore, L has a solvable word problem if and only if P_0 is a recursive set, and P_0 determines $\mathbf{H}\mathscr{L}(R)$, as in Cor. 5. This proves Cor. 6.

Regular rings R with arbitrary sets of invertible primes can be formed from appropriate products of $\mathbf{Q}$ and $\mathbf{Z}_p$ for p prime. In any such product, $p \cdot 1$ is invertible in R if and only if $\mathbf{Z}_p$ is not a factor of R.

We remark that less is known of the quasivariety classification problem. That is, only partial results are available for classifying the lattice quasivarieties $\mathscr{L}(R)$, R a ring with 1. The major result of [9] is the following: For rings R and S with 1, $\mathscr{L}(R) \subset \mathscr{L}(S)$ if and only if for each small exact subcategory $\mathscr{C}$ of R-**Mod**, there exists an exact embedding functor $\mathscr{C} \to S$-**Mod**. In [9: Thm. 5, p. 88], a number of results parallel to Thm. 5 are given. Two results are worth special mention. First, if R is a ring with nonzero square-free characteristic k, then $\mathscr{L}(R) = \mathscr{L}(\mathbf{Z}_k)$ [9: Thm. 5(6)]. Second, if R is a torsion-free ring, then $\mathscr{L}(R)$ depends only on the set of primes invertible in R [9: Thm. 5(8)], similar to Cor. 5. It is not known whether $\mathscr{L}(R) = \mathbf{H}\mathscr{L}(R)$ for any ring R with 1. However, equality does not always hold, as the next result shows.

COROLLARY 7. *There exists a ring R with 1 such that $\mathscr{L}(R) \neq \mathbf{H}\mathscr{L}(R)$.*

Proof. For each $k \geqq 4$ divisible by p^2 for some prime p, there exists a ring R with characteristic k such that $\mathscr{L}(R)$ is a proper subclass of $\mathscr{L}(\mathbf{Z}_k)$ [9: p. 92]. Since $\mathscr{L}(\mathbf{Z}_k) \subset \mathbf{H}\mathscr{L}(\mathbf{Z}_k) = \mathbf{H}\mathscr{L}(R)$ by Thm. 4, such an R suffices to prove Cor. 7.

We conclude this section with the verification that lattices of submodules generate self-dual varieties.

THEOREM 7. *For any ring R with 1, a lattice identity is satisfied in every lattice representable by R-modules if and only if the dual identity is also satisfied in every lattice representable by R-modules. That is, $\mathbf{H}\mathscr{L}(R)$ is a self-dual variety of lattices.*

Proof. It follows from [13: Thm. 3] that the quasivariety $\mathscr{L}(R)$ is self-dual if R is a commutative ring with 1. Therefore, $\mathbf{H}\mathscr{L}(R)$ is self-dual if R is commutative. Since $\mathbf{Z}_k$ for $k \geqq 1$ and R_f for $f: P \to [0, \omega]$ are commutative, Thm. 7 then follows from Thm. 4.

§4. Congruence varieties of lattices.

If $\mathscr{V}$ is a variety of algebras of some type τ, the class of congruence lattices $\{\mathbf{Con}(V): V \in \mathscr{V}\}$ generates a variety of lattices that is called a "congruence variety" (see B. Jónsson [14]). We note that $\mathbf{H}\mathscr{L}(R)$ is generated by the class $\{\mathbf{Con}(M): M \in R\text{-}\mathbf{Mod}\}$, and so is a congruence variety, for each ring R with 1. A recent result announced by R. Freese [3] is rather surprising: Any modular but not distributive congruence variety contains either $\mathbf{H}\mathscr{L}(\mathbf{Q})$ or $\mathbf{H}\mathscr{L}(\mathbf{Z}_p)$ for some prime p. If R is a division ring, then $\mathbf{H}\mathscr{L}(R)$ equals $\mathbf{H}\mathscr{L}(\mathbf{Q})$ or $\mathbf{H}\mathscr{L}(\mathbf{Z}_p)$ according to whether R has characteristic zero or prime p, by Thm. 4 or [9: Thm. 5(10)]. Thus, the varieties generated by projective geometry lattices over a fixed division ring are minimal with respect to all modular but not distributive congruence varieties, not just those of form $\mathbf{H}\mathscr{L}(R)$. Also, Freese announces that a join of congruence varieties is a congruence variety, if there is a fixed n such that each congruence variety of the join is obtained from a variety of algebras with n-permutable congruences. (Compare with Thm. 5(5).) In a private communication, Freese notes that the congruence variety $\mathscr{C}$ obtained from any subvariety $\mathscr{V}$ of R-**Mod** for any ring R with 1 satisfies $\mathscr{C} = \mathbf{H}\mathscr{L}(S)$ for a suitable quotient ring S of R. Specifically, $S = R/\mathbf{a}$, where:

$$\mathbf{a} = \{r \in R: rm = 0 \text{ for all } m \text{ in each } M \text{ in } \mathscr{V}\}.$$

Freese's argument, slightly modified, is as follows: Clearly $\mathbf{a}$ is a two-sided ideal of R. Every A in $\mathcal{V}$ can be regarded as an S-module by defining $(r+\mathbf{a})v = rv$ for r in R and v in A. Since $\mathbf{Con}(A)$ is the same for A regarded as R-module and as S-module, $\mathscr{C} \subset \mathbf{H}\mathscr{L}(S)$. Now let $X = S - \{0\}$, and for each s in X, choose r_s in R and x_s in some R-module M_s of $\mathcal{V}$ such that $s = r_s + \mathbf{a}$ and $r_s x_s \neq 0$. Let M denote the R-submodule of $\prod_{s\in X} M_s$ generated by the element $\langle x_s\rangle_{s\in X}$. Then M is in $\mathcal{V}$, and so M^α (the product of α copies of M) is in $\mathcal{V}$ for any cardinal α. Also, M is clearly isomorphic as an S-module to the ring S regarded as a left S-module. Therefore, if N is in S-**Mod**, then $\mathbf{Con}(N)$ is isomorphic to an interval sublattice of $\mathbf{Con}(M^\alpha)$ for sufficiently large α, and $\mathbf{H}\mathscr{L}(S) \subset \mathscr{C}$ follows. Furthermore, Freese considers modules over rings R not having a unit, and shows that no new congruence varieties are obtained, by the following argument. Suppose $\mathcal{V}$ is a subvariety of the variety of all left R-modules, where R has no unit and so the identity $1x = x$ doesn't apply for R-modules. A ring R_1 with unit is constructed having the same additive group structure as $R \times \mathbf{Z}$, and the ring multiplication given by:

$$\langle r_1, n_1\rangle\langle r_2, n_2\rangle = \langle r_1 r_2 + n_1 \cdot r_2 + n_2 \cdot r_1, n_1 n_2\rangle \text{ for } r_1, r_2 \text{ in } R \text{ and } n_1, n_2 \text{ in } \mathbf{Z}.$$

Given an R-module M, a unital R_1-module M_1 is constructed with the same additive group structure as M and scalar multiplication given by:

$$\langle r, n\rangle v = rv + n \cdot v \text{ (additive multiple), for } r \text{ in } R,\ n \text{ in } \mathbf{Z},\ v \text{ in } M.$$

Since $\mathbf{Con}(M) = \mathbf{Con}(M_1)$ for all M, the congruence varieties corresponding to $\mathcal{V}$ and to the subvariety $\mathcal{V}_1 = \{M_1 : M \in \mathcal{V}\}$ of R_1-**Mod** are the same. Note that the congruence variety corresponding to all R-modules for R without unit is always $\mathbf{H}\mathscr{L}(\mathbf{Z})$, since any abelian group can be made into an R-module with the same congruence lattice by defining all scalar products to be zero.

DEFINITION. Consider the congruence varieties $\mathbf{H}\mathscr{L}(\mathbf{Z}_m)$ for $m \geqq 1$, and $\mathbf{H}\mathscr{L}(\mathbf{Z})$. The set $\{m : m \geqq 1\}$ can be made into a lattice N when partially ordered by divisibility. (That is, meet is g.c.d. and join is least common multiple for two integers of N.) By abuse of notation, we shall consider sets of congruence varieties (see [5: p. 172]). In particular, let $\mathscr{K}$ denote $\{\mathbf{H}\mathscr{L}(\mathbf{Z}_m) : m \geqq 1\}$, and let $\mathscr{C}(\Sigma)$ denote all congruence varieties $\mathcal{V}$ such that every member of the set of identities Σ is satisfied in every lattice in $\mathcal{V}$.

THEOREM 8. *Suppose $\mathcal{K}_0 \subset \mathcal{K}$. Then the following are equivalent:*
(1) *$\mathcal{K}_0 = \mathcal{K} \cap \mathscr{C}(\Sigma)$ for some set Σ of lattice identities.*
(2) *$\{m : \mathbf{H}\mathscr{L}(\mathbf{Z}_m) \in \mathcal{K}_0\}$ is an ideal of the lattice N.*
(3) *There exist integers $m_j \geqq 0$ and $n_j \geqq 1$ for j in some index set J such that:*

$$\mathcal{K}_0 = \{\mathbf{H}\mathscr{L}(\mathbf{Z}_m) : \text{g.c.d. } (m_j, m) \text{ divides } n_j \text{ for all } j \in J\}.$$

Proof. Assume (1), and choose Σ so that each σ in Σ is a lattice polynomial inclusion formula $d \subset e$. Define $m_\sigma = m(\Omega(d, e))$ and $n_\sigma = n(\Omega(d, e))$. As in Cor. 1, σ is satisfied throughout $\mathbf{H}\mathscr{L}(\mathbf{Z}_m)$ iff the g.c.d. (m_σ, m) divides n_σ. Therefore, (1) implies (3).

It can be shown that any set of the form:

$$\{m \in N: \text{g.c.d. } (m_j, m) \text{ divides } n_j,\ j \in J\},$$

all $m_j \geqq 0$ and $n_j \geqq 1$, is an ideal of N. Therefore, (3) implies (2).

Assume (2), that $H = \{m : \mathbf{H}\mathscr{L}(\mathbf{Z}_m) \in \mathcal{K}_0\}$ is an ideal of N. Let $f : P \to [0, \omega]$ be defined by $f(p) = \sup\{\beta : p^\beta \in H\}$, and define

$$\Sigma = \{\eta(p^{f(p)+1}, p^{f(p)}):\ p \in P, f(p) < \omega\}.$$

(If $f(p) = 0$, let $\eta(p, 1)$ denote the identity ε_p of [8: p. 190].) From Props. 1 and 5 and [8: Satz 6], it follows without much difficulty that $\mathcal{K}_0 = \mathcal{K} \cap \mathscr{C}(\Sigma)$. Therefore, (2) implies (1), completing Thm. 8.

DEFINITION. Suppose H is an ideal of N. Let $f : P \to [0, \omega]$ be given by $f(p) = \sup\{\beta : p^\beta \in H\}$, and let Σ_H be the set of lattice identities:

$$\{\eta(p^{f(p)+1}, p^{f(p)}):\ p \in P,\ f(p) < \omega\}.$$

Define a variety $\mathcal{V}_H$ of algebras of type τ_H as follows: Type τ_H consists of abelian group operations $\{+, -, 0\}$ together with operations corresponding to each σ in Σ_H. The identities defining $\mathcal{V}_H$ are the standard abelian group axioms for $\{+, -, 0\}$ plus identities corresponding to each σ in Σ_H. If σ in Σ_H is $d \subset e$, then the operations and identities corresponding to σ are just the operations and equations, respectively, of the Mal'cev condition $\Xi(d^\circ, e^\circ)$, with different elements of Σ_H assigned disjoint sets of operations. This defines the variety $\mathcal{V}_H$ of τ_H-algebras, and $\mathscr{C}_H$ denotes the corresponding congruence variety of lattices, which is generated by the class $\{\mathbf{Con}(V) : V \in \mathcal{V}_H\}$.

THEOREM 9. *$H \mapsto \mathscr{C}_H$ determines a one-one function from the set of all of the continuously many ideals of N into the set of congruence varieties contained in* $\mathbf{H}\mathscr{L}(\mathbf{Z})$.

Proof. The abelian group axioms ensure that $\mathscr{V}_H$ has permutable congruences. So, $d \subset e$ and $d^\circ \subset e^\circ$ are equivalent statements for $\mathbf{Con}(V)$, given V in $\mathscr{V}_H$. Therefore, any lattice polynomial inclusion $d \subset e$ is satisfied throughout $\mathscr{C}_H$ if and only if $\Xi(d^\circ, e^\circ)$ is satisfied for $\mathscr{V}_H$. It follows immediately that each σ in Σ_H is satisfied throughout $\mathscr{C}_H$.

Every algebra V in $\mathscr{V}_H$ has an abelian group reduct A with corresponding $\mathbf{Z}$-module A^*. So, $\mathbf{Con}(V)$ is a sublattice of $\mathbf{Con}(A^*)$, since congruence lattice operations are obtained by restriction of equivalence relation lattice operations [5: Cor. 2, p. 51]. It follows that $\mathscr{C}_H \subset \mathbf{H}\mathscr{L}(\mathbf{Z})$.

Suppose $m \in H$ and M is in $\mathbf{Z}_m$-$\mathbf{Mod}$. So, each σ in Σ_H is satisfied in $\mathbf{Con}(M)$. We can define V in $\mathscr{V}_H$ with the same abelian group structure as M and additional operations for each σ in Σ_H defined via Thms. 1 and 2, such that $\mathbf{Con}(V) = \mathbf{Con}(M)$. Therefore, $\mathbf{H}\mathscr{L}(\mathbf{Z}_m) \subset \mathscr{C}_H$ if $m \in H$.

Suppose m is not in H. By the definition of Σ_H and Prop. 1, there exists $d \subset e$ in Σ_H which is not satisfied throughout $\mathbf{H}\mathscr{L}(\mathbf{Z}_m)$. Therefore $\mathbf{H}\mathscr{L}(\mathbf{Z}_m)$ is not contained in $\mathscr{C}_H$. So, $\mathbf{H}\mathscr{L}(\mathbf{Z}_m) \subset \mathscr{C}_H$ if and only if $m \in H$, $m \geqq 1$. It follows that $\mathscr{C}_H = \mathscr{C}_K$ implies $H = K$ for ideals H and K of N. That is, $H \mapsto \mathscr{C}_H$ is a one-one function, which completes Thm. 9.

The construction of $\mathscr{C}_H$ has some resemblance to the construction of the ring R_f and corresponding congruence variety $\mathbf{H}\mathscr{L}(R_f)$ in Prop. 4. We ask below whether these two methods lead to the same congruence varieties.

PROBLEM. Let $f: P \to [0, \omega]$, and define $H(f)$ to be the ideal of N such that $m \in H(f)$ iff $\exp(m, p) \leqq f(p)$ for each prime p. Is $\mathscr{C}_{H(f)} = \mathbf{H}\mathscr{L}(R_f)$ in general? (It is clear that $\mathbf{H}\mathscr{L}(R_f) \subset \mathscr{C}_{H(f)}$.)

Appendix. Computer implementation of the word problem algorithm.

The central result of this paper is the algorithm for producing a ring divisibility test $D(m, n)$ from an arbitrary lattice polynomial inclusion formula $d \subset e$. A FORTRAN computer program for computing $m = m(\Omega(d, e))$ and $n = n(\Omega(d, e))$ has been designed and tested by the first author, and may be obtained upon request. The computation is feasible for lattice polynomials of moderate length. For example, $\Delta(4, 2)$ is $d \subset e$ for polynomials d and e of lengths 7 and 101, respectively. To verify that $D(4, 2)$ is the equivalent ring divisibility condition

required diagonalization of an 153×137 initial matrix system (M, V), and took less than one second on an IBM 370/168 computer.

In this appendix, we describe the computer version of our algorithm. There are two significant modifications of the discussion of §2. First, it is possible to entirely avoid analysis of strings of characters or their Gödel numbers. That is, the computation can be restricted to integer arithmetic and comparison operations on integers and integer vectors and matrices only. Second, the variables r_{ij} of $\Omega(d, e)$ for $i = 1, 2$ can be directly eliminated by means of the Kronecker delta equations. Instead of the $s \times t$ initial matrix system of §2, we diagonalize an equivalent $(s-2m) \times (t-2m)$ system.

The main program of our system inputs the lattice polynomial pairs for analysis and calls a computational subroutine for analysis of each pair. To express a lattice polynomial as a sequence of integers, it may be converted to Polish notation and then each lattice operation or variable replaced by a code integer. The system we use replaces join by -2, meet by -1, and the variable x_i by i for $i \geqq 1$.

EXAMPLE. $(x_1 \vee x_2) \wedge (x_1 \vee x_3)$ is $\wedge \vee x_1 x_2 \vee x_1 x_3$ in (forward) Polish notation, and so corresponds to the sequence of integers:

$$-1, -2, 1, 2, -2, 1, 3.$$

Of course, many methods of generating or reading lattice polynomial pairs can be used with our system, so long as the required pair of integer sequences is generated and input to the computational subroutine.

The analysis of a lattice polynomial pair may be divided into six stages: lattice polynomial syntax checking and analysis, computation of F-lists, computation of partitions $\phi_1, \phi_2, \ldots, \phi_n$ corresponding to the variables $x_1, x_2, \ldots, x_n$, generation of the (modified) initial matrix system, diagonalization of the matrix system, and reduction of the resulting divisibility conditions to a single normal divisibility condition.

Suppose $m_1, m_2, \ldots, m_n$ is an arbitrary sequence of "code" integers, (-1, -2 or positive). Recursively define a corresponding "valency" sequence $v_0, v_1, \ldots, v_n$, beginning with $v_0 = 0$. For $0 < i \leqq n$, $v_i = v_{i-1} + 1$ if m_i represents meet or join ($m_i \in \{-1, -2\}$), and $v_i = v_{i-1} - 1$ if m_i represents a variable ($m_i \geqq 1$). (See [2: pp. 118–119] for a related concept of valency and its properties.) In our implementation, two-row matrices X_d and X_e are generated corresponding to the lattice polynomials d and e for evaluation of the word problem $d \subset e$. In each case, the

first row is the input sequence of code integers, and the second row is the valency sequence excluding v_0.

EXAMPLE. For $d = (x_1 \vee x_2) \wedge (x_3 \vee x_4)$, the coding and valency sequences are used to form the 2×7 matrix X_d as follows:

$$\begin{bmatrix} -1 & -2 & 1 & 2 & -2 & 3 & 4 \\ 1 & 2 & 1 & 0 & 1 & 0 & -1 \end{bmatrix}.$$

A sequence of code integers represents a (unique) lattice polynomial e if and only if its valency sequence has last term -1 and all other terms nonnegative. So, it is easily determined by computing the valency sequence whether the input sequence of integers is syntactically correct. If $m_1, m_2, \ldots, m_n$ encodes a lattice polynomial e, then e has n constituent parts (including e itself). For $k \leqq n$, the k-th constituent part e_k of e corresponds to an interval subsequence $m_k, m_{k+1}, \ldots, m_r$ of the given sequence, beginning at m_k as shown. The length of the subsequence can be determined from the valency sequence by the condition that $v_r < v_{k-1}$ and $v_i \geqq v_{k-1}$ for $k \leqq i < r$. (In the example, $(m_2, m_3, m_4) = (-2, 1, 2)$ is the constituent part of d for $k = 2$ because $v_4 < v_1$ and $v_2, v_3 \geqq v_1$, where $(v_1, v_2, v_3, v_4) = (1, 2, 1, 0)$.) Note that if m_k represents a variable ($m_k \geqq 1$), then $v_k < v_{k-1}$ and e_k is the variable represented by m_k alone.

A $3 \times n$ integer matrix Y can be conveniently used to compute the F-list of a lattice polynomial e of length n. If the u-th formula of $F(e^\circ)$ is $\langle a_i, a_j \rangle \in (e_k)^\circ$, where e_k is the k-th constituent of e, then column u of Y is formed by entering i, j and k, respectively. The computation adapts the procedure for generating the partial F-lists $F_u(e^\circ)$, $0 \leqq u \leqq n$. Since $F_0(e^\circ)$ is the single formula $\langle a_1, a_2 \rangle \in e^\circ$ and $e = e_1$, the first column of Y is given the coordinates 1, 2 and 1, respectively. Suppose $0 < u \leqq n$, and $F_{u-1}(e^\circ)$ contains t formulas, so that we assume that the first t columns of Y have been completed, $t \geqq u$. In particular, entries i, j and k have been computed for the coordinates of column u. If e_k is a variable ($m_k \geqq 1$), then $F_u(e^\circ) = F_{u-1}(e^\circ)$ and Y is not changed in the u-th step. Otherwise, m_k is in $\{-1, -2\}$, and columns $t+1$ and $t+2$ of Y must be formed in the u-th step. Suppose $m_k, m_{k+1}, \ldots, m_r$ is the code integer sequence corresponding to e_k, $r \geqq k+2$. Then there exists a unique s, $k < s < r$, such that e_{k+1} has integer sequence $m_{k+1}, m_{k+2}, \ldots, m_s$ and e_{s+1} has integer sequence $m_{s+1}, m_{s+2}, \ldots, m_r$. (Here, e_k is a binary meet or join of its constituents e_{k+1} and e_{s+1}.) Of course, s can be computed by determining the length of e_{k+1} from the valency sequence as previously described. If $m_k = -1$, the u-th step is completed by entering $i, j, k+1$ and $i, j, s+1$ into the matrix Y in columns $t+1$ and $t+2$, respectively. Suppose $m_k = -2$, and p is the smallest positive integer not appearing in the

first t coordinates of rows 1 and 2 of Y. Then the u-th step is completed by entering $i, p, k+1$ and $p, j, s+1$ in columns $t+1$ and $t+2$ of Y, respectively.

EXAMPLE. For $d=(x_1 \vee x_2) \wedge (x_3 \vee x_4)$, the completed matrix Y is given below:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 3 & 1 & 4 \\ 2 & 2 & 2 & 3 & 2 & 4 & 2 \\ 1 & 2 & 5 & 3 & 4 & 6 & 7 \end{bmatrix}.$$

Since $m_k = m_1 = -1$ for $u=1$, the computation corresponding to $F_1(d^\circ)$ enters $1, 2, k+1$ and $1, 2, s+1$ into columns 2 and 3, respectively. Since d_2 corresponds to (m_2, m_3, m_4) as previously noted, $s+1=5$.

Note that the third row of Y is a permutation of $1, 2, \ldots, n$ in all cases. The F-list stage of the computation is completed by computation of the three-row matrices Y_d and Y_e corresponding to the input lattice polynomials d and e.

Partitions ϕ of $\{a_1, a_2, \ldots, a_m\}$ are conveniently represented by integer sequences of length m such that the i-th integer is j if $\phi^*(a_i) = a_j$. (Recall that $\phi^*(a_i) = a_j$ if j is the smallest integer such that a_i and a_j belong to the same block of ϕ.)

EXAMPLE. $\{\{a_1, a_3\}, \{a_2\}, \{a_4\}\}$ is represented by $(1, 2, 1, 4)$.

Therefore, computation of the partitions $\phi_1, \phi_2, \ldots, \phi_n$ corresponding to the lattice polynomial variables $x_1, x_2, \ldots, x_n$ can be arranged in an $n \times m$ integer matrix Z. Initially, each row of Z is set to $1, 2, \ldots, m$, corresponding to the discrete partition $\{\{a_i\} : i \leqq m\}$. We then sequentially examine the columns of the F-list matrix Y_d corresponding to the first input polynomial d. Suppose column u of Y_d contains i, j and k, respectively. If m_k, that is, $X_d(1, k)$, is -1 or -2, then no action is needed. Otherwise, m_k is positive, representing some variable. In this case, we modify row m_k of Z to combine the block containing a_i and the block containing a_j in the corresponding partition ϕ.

EXAMPLE. Suppose row m_k of Z is:

[1 2 1 4 2 6 4 2 1].

If the blocks containing a_i and a_j for $i=7$ and $j=8$ are to be combined for ϕ, we see that the corresponding entries are 4 and 2. Clearly, the required action is to

replace each 4 by a 2, with the resulting row m_k for Z below:

[1 2 1 2 2 6 2 2 1].

After all the columns of Y_d have been processed, Z contains the full description of the partitions $\phi_1, \phi_2, \ldots, \phi_n$. It is easy to obtain an n-vector J such that $J(k)$ is the number of blocks in ϕ_k during the computation of Z. This completes the third stage of the word problem analysis.

We are now prepared to generate the initial matrix system (M_0, V_0). For appropriate s and t, M_0 is an $s \times t$ integer matrix and V_0 is an s-vector. In the implementation, it is convenient to use the $s \times (t+1)$ matrix $[M_0 \mid V_0]$ (V_0 in column $t+1$). Since we use the Kronecker delta equations to eliminate variables, the number of system equations s equals the number of equations corresponding to the operation-free formulas of $F(e^\circ)$, for the second input polynomial e. Beginning with $s = 0$, add the partition block count $J(k)$ to s for each occurrence of a positive k in the sequence for e (top row of X_e). Terms -1 and -2 in the sequence are neglected. The number of system variables t must also be computed. During the F-list computation, the numbers m of variables $\{a_1, a_2, \ldots, a_m\}$ and q of variables $\{f_1, f_2, \ldots, f_q\}$ are computed. (They are the maximum entries of the top row of Y_d and of Y_e, respectively.) Since the system variables are r_{ij} for $i \leqq q$ and $j \leqq m$, and the variables r_{ij} for $i = 1, 2$ are eliminated by the Kronecker delta equations, we take $t = (q-2)m$ except in the case $q = 2$. If $q = 2$, so $(q-2)m = 0$, we take $t = 1$.

To generate the initial matrix system (M_0, V_0), we first set all matrix system entries to zero. The nonzero entries of (M_0, V_0) are then computed and set by a nested recursion. In the outer recursion, the columns of the F-list matrix Y_e are examined. Say that i, j and k, respectively, are the coordinates of column u of Y_e. If m_k, that is, $X_e(1, k)$, is -1 or -2, then no action is taken in the u-th step. Suppose $m_k \geqq 1$, and the first x rows for (M_0, V_0) have already been computed. The inner recursion computes rows $x+1, x+2, \ldots, x+J(m_k)$ of (M_0, V_0) in the u-th step, each row corresponding to a block of the partition ϕ described in row m_k of Z. Suppose X is a block of ϕ and the corresponding equation is to be entered in row w of the matrix system. Recall that the corresponding equation of $\Omega(d, e)$ is $\sum \{r_{ip} : p \in X\} = \sum \{r_{jp} : p \in X\}$. The variables r_{ij} for $i = 1, 2$ and $j \leqq m$ are to be eliminated by the Kronecker delta equations, so the columns of M_0 correspond consecutively to the variables:

$$r_{31}, r_{32}, \ldots, r_{3m}, r_{41}, r_{42}, \ldots, r_{4m}, \ldots, r_{q1}, r_{q2}, \ldots, r_{qm}.$$

If i equals 1 or 2, then the left side of the above equation equals 1 if i is in X and 0 otherwise, by the Kronecker delta equations. So, coordinate w of V_0 is set to

-1 or 0 accordingly. For $i \geqq 3$, the w-th coordinate of each column of M_0 corresponding to a variable r_{ip} for p in X is set to 1. Similarly, 1 or 0 is added appropriately to coordinate w of V_0 if j equals 1 or 2, according to whether j is in X or not. For $j \geqq 3$, 1 is subtracted from the w-th coordinate of each column corresponding to a variable r_{jp} for p in X.

EXAMPLE. Suppose $m = 3$ and $q = 4$, so the columns of M_0 correspond to r_{31}, r_{32}, r_{33}, r_{41}, r_{42} and r_{43}, respectively. If $i = 1$, $j = 4$ and $X = \{1, 3\}$ is the block of ϕ corresponding to row w, then the corresponding equation $r_{11} + r_{13} = r_{41} + r_{43}$ becomes $(-1) \cdot r_{41} + (-1) \cdot r_{43} = (-1) \cdot 1$ on substitution of $r_{11} = 1$ and $r_{13} = 0$ and rearranging terms, and so row w of (M_0, V_0) is set to:

$$[0 \quad 0 \quad 0 \quad -1 \quad 0 \quad -1] \text{ and } [-1].$$

The double recursion described above completes the fourth stage, generation of the initial matrix system (M_0, V_0).

The fifth stage, diagonalization of (M_0, V_0), is implemented by using the well-known "elementary" row and column operations. If $M = BM_0C$ and $V = BV_0$ for matrices B and C which are invertible elements of $\mathcal{M}_s(\mathbf{Z})$ and $\mathcal{M}_t(\mathbf{Z})$, respectively, we call (M, V) a "fundamental system." Let M and M' be $s \times t$ integer matrices and V and V' integer s-vectors below. The row operations R1, R2 and R3 and the column operations C1, C2 and C3 modify fundamental systems so that the results are again fundamental systems.

(R1) If M' is obtained from M by transposing two rows and V' is obtained from V by transposing the corresponding coordinates, then (M', V') is an R1-transformation of (M, V).

(R2) If M' is obtained from M by multiplying a row by -1 and V' is obtained from V by multiplying the corresponding coordinate by -1, then (M', V') is an R2-transformation of (M, V).

(R3) If M' is obtained from M by adding an integer multiple of one row to another and V' is obtained from V by adding the same integer multiple of the corresponding first coordinate to the corresponding second coordinate, then (M', V') is an R3-transformation of (M, V).

(C1) If M' is obtained from M by transposing two columns, then (M', V) is a C1-transformation of (M, V).

(C2) If M' is obtained from M by multiplying some column by -1, then (M', V) is a C2-transformation of (M, V).

(C3) If M' is obtained from M by adding an integer multiple of one column to a second column, then (M', V) is a C3-transformation of (M, V).

Suppose Ω is a productless system of ring equations with initial matrix system (M_0, V_0). The row operations correspond to operations on Ω which replace the system of equations with an equivalent system; the column operations correspond to operations on Ω obtained by introducing a new system of variables by forming suitable $\mathbf{Z}$-linear combinations of the previous variables.

In the diagonalization procedure, a sequence (M_k, V_k), $0 \leqq k \leqq u$, of fundamental systems is recursively constructed. For each k, M_k has the block form:

$$\begin{bmatrix} A_k & B_k \\ C_k & D_k \end{bmatrix},$$

where A_k is a $k \times k$ diagonal matrix, B_k and C_k are zero matrices of dimensions $k \times (t-k)$ and $(s-k) \times k$, respectively, and D_k is an $(s-k) \times (t-k)$ integer matrix. By convention, the initial matrix system has the above block form with $D_0 = M_0$ and A_0, B_0 and C_0 dropping out. The u-th final fundamental system (M_u, V_u) satisfies either that D_u is a zero matrix or u equals s or t; M_u is a diagonal matrix in all these cases. Of course, we again drop B_u, C_u or D_u appropriately from the block form in the cases $u = s$ or $u = t$. We describe below the construction of (M_1, V_1) from (M_0, V_0), assuming that M_0 is not a zero matrix. The general iterative step from (M_{k-1}, V_{k-1}) to (M_k, V_k) is similar, except that A_{k-1}, B_{k-1} and C_{k-1} remain unchanged in this case. That is, this step is performed solely by row and column transformations of the submatrix D_{k-1} of M_{k-1} and the corresponding part of V_{k-1} (the last $s-k+1$ coordinates).

As subsequently specified, we perform R3 and C3-transformations successively, beginning with (M_0, V_0), until we obtain a fundamental system (M', V'), with $M' = [m'_{ij}]$ such that some nonzero $a = m'_{ij}$ divides every element of M'. Following [18: pp. 236–237], perform an R1, a C1, and a C2-transformation on (M', V'), as needed, to obtain a fundamental system (M'', V'') for $M'' = [m''_{ij}]$ such that $m''_{11} = |a|$, where $|a|$ also divides every element of M''. By $s-1$ R3-transformations adding integer multiples $-(m''_{i1}/|a|)$ times row 1 to row i for $2 \leqq i \leqq s$, we obtain a fundamental system (M^*, V^*) for $M^* = [m^*_{ij}]$ such that $m^*_{11} = |a|$ and $m^*_{i1} = 0$ for $2 \leqq i \leqq s$. Similarly, $t-1$ C3-transformations of (M^*, V^*) lead to a fundamental system (M_1, V_1) with $M_1 = [m^{(1)}_{ij}]$ such that $m^{(1)}_{11} = |a|$, $m^{(1)}_{i1} = 0$ for $2 \leqq i \leqq s$, and $m^{(1)}_{1j} = 0$ for $2 \leqq j \leqq t$. Most of the computation time required for the word problem analysis is used for the diagonalization procedure. For the steps above, we apply two observations to reduce computation time. First, for each i, $2 \leqq i \leqq s$, no R3-transformation of the i-th row of the system is needed if a test shows that $m''_{i1} = 0$. Second, the $t-1$ C3-transformations described above change only the first row of the matrix, since at the point of computation the first column has all zero coordinates except for m^*_{11}. So, these C3-transformations can

be computed simply by setting to zero all coordinates of the top row except for the first.

To make the above procedure recursive, it suffices to give a method for computing (M', V'). For a nonzero $s \times t$ matrix $N = [n_{ij}]$, let mag (N) denote the smallest value for $|n_{ij}|$ taken over all nonzero elements of N. Suppose that (N, W) is an $s \times t$ system with nonzero matrix N, such that mag (N) doesn't divide every element of N. It suffices to give an algorithm E constructing an $s \times t$ system (N', W') with nonzero matrix N' such that mag $(N') <$ mag (N), using finitely many R3 and C3-transformations beginning with (N, W). Given such an E, we can iteratively apply it, beginning with $(N_0, W_0) = (M_0, V_0)$, to obtain a sequence (N_i, W_i), $i \geqq 0$, of fundamental systems for Ω. The process must terminate, since mag (N_i) for $i \geqq 0$ is a strictly decreasing sequence of positive integers, and the final term of the sequence has the desired property for (M', V').

Assuming the above hypotheses for (N, W) with $N = [n_{ij}]$, define E as follows: First, find an element n_{ij} such that $|n_{ij}| =$ mag (N), and an element n_{vw} not divisible by n_{ij}. If n_{ij} doesn't divide n_{vj}, so $n_{vj} = \sigma n_{ij} + \tau$ for integers σ and τ, $0 < \tau < |n_{ij}|$, then let (N', W') be the R3-transformation of (N, W) adding $-\sigma$ times row i to row v, so mag $(N') \leqq \tau <$ mag (N). (In some cases, fewer iterations of algorithm E are required to compute (M', V') if $-\sigma$ is replaced by $-\sigma - 1$ for $n_{ij} > 0$ or $-\sigma + 1$ for $n_{ij} < 0$.) Again, let (N', W') be an appropriate C3-transformation of (N, W) if n_{ij} doesn't divide n_{iw}. In the remaining case, $i \neq v$ and $j \neq w$, and $n_{vj} = an_{ij}$ and $n_{iw} = bn_{ij}$ for some integers a and b. If we add $-a$ times row i to row v and then $-b$ times column j to column w, we obtain (N'', W'') with $N'' = [n''_{ij}]$ such that $n''_{ij} = n_{ij}$, $n''_{iw} = n''_{vj} = 0$ and $n''_{vw} = n_{vw} - abn_{ij}$. Let τ be the g.c.d. of n_{ij} and n''_{vw}, so $\tau = \sigma_1 n_{ij} + \sigma_2 n''_{vw}$ for integers σ_1 and σ_2 computable from the Euclidean algorithm. Since n_{ij} doesn't divide n_{vw} or n''_{vw}, we have $0 < \tau < |n_{ij}|$. Therefore, we can define (N', W') from (N'', W'') by an R3-transformation adding σ_1 times row i to row v followed by a C3-transformation adding σ_2 times column w to column j, obtaining mag $(N') \leqq \tau <$ mag (N) again. This defines algorithm E in all cases. Obviously E has the required properties, including recursiveness. A considerable saving of computation time can be obtained for the repeated searches to determine mag (N) for a matrix N. If $|n_{ij}| = 1$ for some n_{ij} found in N, then mag $(N) = 1$ and n_{ij} divides every entry of N. In our implementation, we test whether the current minimum nonzero magnitude of the matrix entries equals one after searching each row. If the test is successful, then no further matrix rows are searched, and the computation proceeds to the completion of the diagonalization step beginning from the fundamental system (M', V').

EXAMPLE. Suppose Ω is a productless system of ring equations having the

initial matrix system (M_0, V_0), with 2×4 matrix and 2-vector given by:

$$(M_0, V_0) = \left[\begin{array}{cccc|c} 12 & -6 & 0 & 24 & 5 \\ 10 & 18 & -48 & 18 & 24 \end{array}\right].$$

(This matrix system does not arise from a lattice word problem.)

Let R3$(i, j \cdot k)$ denote the R3-transformation obtained by adding j times row k to row i, and let C3$(i, j \cdot k)$ denote the corresponding C3-transformation. We compute (M', V') by a single application of algorithm E with $n_{ij} = n_{12}$ and $n_{vw} = n_{21}$, obtaining:

$$(M', V') = \left[\begin{array}{cccc|c} 0 & -6 & 0 & 24 & 5 \\ 46 & 2 & -48 & -102 & -1 \end{array}\right],$$

by the operations R3$(2, 3 \cdot 1)$, C3$(1, 2 \cdot 2)$, R3$(2, -8 \cdot 1)$ and C3$(2, -1 \cdot 1)$. The first diagonalization step is then completed by interchanging the two rows, interchanging columns 1 and 2, and then the operations R3$(2, 3 \cdot 1)$, C3$(2, -23 \cdot 1)$, C3$(3, 24 \cdot 1)$ and C3$(4, 51 \cdot 1)$. The partially diagonalized system (M_1, V_1) is given by:

$$(M_1, V_1) = \left[\begin{array}{cccc|c} 2 & 0 & 0 & 0 & -1 \\ 0 & 138 & -144 & -282 & 2 \end{array}\right].$$

The diagonalized system (M_2, V_2) of order 2 is then completed by C3$(3, 1 \cdot 2)$, interchanging columns 2 and 3, multiplying column 2 by -1, C3$(3, -23 \cdot 2)$ and C3$(4, 47.2)$. The resulting system is:

$$(M_2, V_2) = \left[\begin{array}{cccc|c} 2 & 0 & 0 & 0 & -1 \\ 0 & 6 & 0 & 0 & 2 \end{array}\right].$$

Note that $m_{11} = 2$ is the g.c.d. of the elements of M_0 and $m_{22} = 6$ is the g.c.d. of the elements of $D_1 = [138 \quad -144 \quad -282]$. In general, m_{jj} for $j \leqq u$ is the g.c.d. of the elements of D_{j-1} in this procedure. This completes the description of the diagonalization process.

The final stage of the computation, reduction of a number of divisibility conditions to one normal divisibility condition, is simply a recursion iteratively applying the functions f and g of Prop. 2. We remark that all trivial diagonal elements $a_{jj} = 1$ can be disregarded, since $D(1, 1)$ & $D(1, x)$ reduces to $D(1, 1)$ by cases 1 and 5 of the definitions. This stage is most easily designed using a subroutine for prime power factorization of any positive integer j. That is, a two-row matrix containing pairs $(p, \text{expt}(j, p))$ for all primes p dividing j is

computed. The combined fifth and sixth stages above can be used for the analysis of arbitrary productless systems of ring equations, beginning from the initial matrix system.

In our implementation, some auxiliary information is printed, in addition to the main computation $m = m(\Omega(d, e))$ and $n = n(\Omega(d, e))$. Special messages are given for the "extreme" outcomes: The ring is trivial if $m = 0$ and $n = 1$; the ring is arbitrary if $m = n = 1$. If $m = 0$, the prime power factorization of n is given, that is, all pairs $(p, \text{expt}(n, p))$ are printed for primes p dividing n. Supposing $0 < n < m$, we note that $\text{expt}(m, p) = \text{expt}(n, p) + 1$ for every prime p dividing m. So, $D(m, n)$ is satisfied in R if and only if $\theta(R, p) \leqq \text{expt}(n, p)$ for every prime p dividing m (such primes need not divide n), by Prop. 1. In this case, we print the degree of invertibility maximums, that is, the pairs $(p, \text{expt}(n, p))$ for all primes p dividing m.

In operation, the algorithm described may fail either because insufficient computer storage is available or in the unlikely event of arithmetic overflow. More complicated algorithms could be designed to accommodate the computation where it is not possible to hold the entire matrix system in the computer's internal storage. For example, more variables of $\Omega(d, e)$ could be eliminated during generation of the initial matrix system. Also, the matrices generated by the algorithm are sparse, that is, they have a large percentage of zero entries. So, alternative techniques for representing matrices by lists of nonzero entries or by partitioning into submatrices could be considered. Finally, a general algorithm based on Thm. 1(2) may be possible (see Props. 5 and 6). However, such methods have not been pursued at this writing.

REFERENCES

[1] G. BIRKHOFF, "Lattice Theory". Third ed., Amer. Math. Soc. Colloquium Publications XXV, Providence, R.I., 1967.

[2] P. M. COHN, "Universal Algebra". Harper & Row, New York, 1967.

[3] R. FREESE, Minimal modular congruence varieties. Abstract 76T-A14, Amer. Math. Soc. Notices *23* (1976), No. 1, A-4.

[4] G. FROBENIUS, Theorie der linearen Formen mit ganzen Coefficienten. J. reine und angewandte Math. *86* (1879), 146–208.

[5] G. GRÄTZER, "Universal Algebra". Van Nostrand, Princeton, N.J., 1968.

[6] C.HERRMANN, On the equational theory of submodule lattices. Proc. University of Houston Lattice Theory Conference, 105–118, Houston, 1973.

[7] C. HERRMANN and A. HUHN, Zum Wortproblem für freie Untermodulverbände. Archiv für Math. *26* (1975), 449–453.

[8] —— and ——, Zum Begriff der Charakteristik modularer Verbände. Math. Zeitschrift *144* (1975), 185–194.

[9] G. HUTCHINSON, On classes of lattices representable by modules. Proc. University of Houston Lattice Theory Conference, 69–94, Houston, 1973.

[10] ——, On the representation of lattices by modules. Trans. Amer. Math. Soc. *209 (1975), 311–351.*
[11] ——, Recursively unsolvable word problems of modular lattices and diagram-chasing. J. of Algebra *26* (1973), 385–399.
[12] ——, Embedding and unsolvability theorems for modular lattices. Algebra Universalis 7 (1977), 47–84.
[13] ——, A duality principle for lattices and categories of modules. J. of Pure and Applied Algebra, in press.
[14] B. JÓNSSON, Varieties of algebras and their congruence varieties. Proc. of the International Congress of Mathematicians, Vancouver, 1974.
[15] L. LIPSHITZ, The undecidability of the word problems for projective geometries and modular lattices. Trans. Amer. Math. Soc. *193* (1974), 171–180.
[16] S. MACLANE and G. BIRKHOFF, "Algebra". MacMillan, New York, 1967.
[17] M. MAKKAI and G. MCNULTY, Universal Horn axiom systems for lattices of submodules. Algebra Universalis 7 (1977), 25–31.
[18] O. SCHREIER and E. SPERNER, "Introduction to Modern algebra and Matrix Theory". Chelsea, New York, 1951.
[19] R. WILLE, Primitive Länge und primitive Weite bei modularen Verbänden. Math. Zeitschrift *108* (1969), 129–136.
[20] R. WILLE, "Kongruenzklassengeometrien". Springer-Verlag Lecture Notes in Mathematics No. 113, Berlin, Heidelberg and New York, 1970.

National Institutes of Health
Bethesda, Maryland
U.S.A.

Jósef Attila Tudományegyetem Bolyai Intézete
Szeged
Hungary