Algebra Universalis, 35 (1996) 425–445

0002-5240/96/030425-21$01.50 + 0.20/0
© 1996 Birkhäuser Verlag, Basel

Submodule lattice quasivarieties and exact embedding functors for rings with prime power characteristic*

G. Czédli and G. Hutchinson

Abstract. Given rings R with prime power characteristic p^k, quasivarieties $\mathscr{L}(R)$ of lattices generated by lattices of submodules of R-modules are studied. An algebra of expressions d not dependent on R is developed, such that each such d uniquely determines a two-sides ideal d_R of R. The main technical result is that $\mathscr{L}(R) \subseteq \mathscr{L}(S)$ makes all implications of the form $d_S = S \Rightarrow d_R = R$ true, for any such expression d. The proof makes use of the known equivalence between $\mathscr{L}(R) \subseteq \mathscr{L}(S)$ and existence of an exact embedding functor R-**Mod** $\to S$-**Mod**. For $k \geq 2$, the ordered set $\mathscr{W}(p^k)$ of all lattice quasivarieties $\mathscr{L}(R)$, R having characteristic p^k, is shown to be large and complicated, with ascending and descending chains and antichains having continuously many elements. More precisely, $\mathscr{W}(p^k)$ has a subset which is order isomorphic to the Boolean algebra of all subsets of a denumerably infinite set. Also, given any prime power p^k, $k \geq 2$, a ring R can be constructed so that $\mathscr{L}(R)$ and $\mathscr{L}(R^{\mathrm{op}})$ for the opposite ring R^{op} are distinct elements of $\mathscr{W}(p^k)$.

1. Introduction

For rings R with unit, the lattices $\mathrm{Su}({}_RM)$ of submodules of R-modules ${}_RM$ are among the most important examples of modular lattices. A lattice L is called *representable by R-modules* if it is isomorphic to a sublattice of some $\mathrm{Su}({}_RM)$. The class $\mathscr{L}(R)$ of all lattices representable by R-modules,

$$\mathscr{L}(R) = \mathrm{S}\{\mathrm{Su}({}_RM) \colon {}_RM \text{ is an } R\text{-module}\},$$

is known to be a quasivariety of lattices [15]. So, $\mathscr{L}(R)$ admits products, ultraproducts and direct limits, and is axiomatizable by a set of universal Horn sentences for lattices.

As usual, R-**Mod** denotes the abelian category of (left) R-modules and R-linear homomorphisms. It is known that $\mathscr{L}(R) \subseteq \mathscr{L}(S)$ iff there exists an exact embedding

Presented by R. Freese.

Received April 20, 1992; accepted in final form April 19, 1995.

* Research partially supported by Hungarian National Foundation for Scientific Research grant no. 1903.

functor R-**Mod** $\rightarrow S$-**Mod** ([13, Theorem 1, p. 108]; also see [11, 12]). So, this paper may equally be considered a study of exact embedding functors between module categories. Since there are many powerful methods for constructing exact embedding functors, the abelian category connection is quite useful.

We will consider rings with prime power characteristic p^k. For any two such rings R and S, the lattice varieties $\mathbf{H}\mathscr{L}(R)$ and $\mathbf{H}\mathscr{L}(S)$ are equal iff R and S have the same (prime power) characteristic [14, Corollary 2, p. 286]. (Here, $\mathbf{H}\mathscr{L}(R)$ denotes the homomorphic images of lattices in $\mathscr{L}(R)$, etc.) The case $k = 1$ also simplifies: If R and S have the same prime characteristic p, then $\mathscr{L}(R) = \mathscr{L}(S)$ [11, Theorem 5(6), p. 88]. For $k \geq 2$, much less is known about these quasivarieties. There are examples of rings R and S with characteristic 4 such that $\mathscr{L}(R) \neq \mathscr{L}(S)$ [4, 11].

In this paper, we develop and apply a method for distinguishing such lattice quasivarieties, based on properties of ring ideals. Suppose R is a ring with characteristic p^k, p prime and $k \geq 2$. We first identify certain special two-sided ideals of R, which can be described by expressions not depending upon R. Recall that the set $\mathrm{Su}({}_R R_R)$ of two-sided ideals of R has a $(\mathbf{0}, \mathbf{1})$ modular lattice structure for join $X \vee Y = X + Y$ and meet $X \wedge Y = X \cap Y$. There are also products:

$$X \cdot Y = \left\{ \sum_{i=1}^{n} x_i y_i : x_i \in X \text{ and } y_i \in Y \text{ for } i \leq n \right\},$$

usually written as just XY. In addition, we consider two unary operations for $\mathrm{Su}({}_R R_R)$, denoted by $\downarrow$ and $\uparrow$ and defined as the image and inverse image under multiplication by p:

$$\downarrow X = pX = \{pv : v \in X\},$$
$$\uparrow X = p^{-1}[X] = \{v \in R : pv \in X\}.$$

We can form *constant* algebraic polynomials e, generated from $\mathbf{0}$ and $\mathbf{1}$ by binary operations $\vee$, $\wedge$ and $\cdot$ and unary operations $\downarrow$ and $\uparrow$. (For example, take $e = (\uparrow\mathbf{0})(\uparrow\mathbf{0}) \vee \uparrow(\downarrow\mathbf{1} \wedge \uparrow\mathbf{0})$.) Each such e can be identified with a two-sided ideal e_R of R using the concrete operations above. To motivate the following, we observe that it is possible to show that e_R annihilates certain R-modules using only the abelian category structure for R-**Mod**. First, note that $\mathbf{0}$ annihilates all R-modules, and $\mathbf{1}$ annihilates zero R-modules. Suppose we know that d_R annihilates ${}_R M$ and e_R annihilates ${}_R N$. If ${}_R M$ is a submodule or homomorphic image of ${}_R N$, then $d_R \vee e_R$ annihilates ${}_R M$. Also, $d_R \wedge e_R$ annihilates ${}_R M \oplus {}_R N$. Furthermore, we see that $d_R e_R$ annihilates ${}_R P$ if there is a short exact sequence:

$$0 \longrightarrow {}_RM \xrightarrow{h} {}_RP \xrightarrow{k} {}_RN \longrightarrow 0$$

(Given v in P, r in d_R and s in e_R, we have $k(sv) = 0$, so $h(u) = sv$ for some u in M, so $rsv = h(ru) = 0$.) Finally, if N is isomorphic to pM (the image of $1_M + \cdots + 1_M$, p times), then $\uparrow d_R$ annihilates ${}_RN$ and $\downarrow e_R$ annihilates ${}_RM$.

Suppose that R and S are rings with characteristic p^k, and for some such polynomial e we have $e_R \neq R$ and $e_S = S$. The above considerations suggest that there may be no exact embedding functor F: R-**Mod** → S-**Mod**. Given such an F, we might hope to construct an abelian category diagram in R-**Mod** containing a nonzero ${}_RM$ such that e_R annihilates ${}_RM$, and then use abelian category structure to force the conclusion that e_S annihilates $F({}_RM)$. But then $e_S = S$ implies that $F({}_RM) = 0$, which contradicts the hypothesis that F is an embedding. As noted previously, this construction would also prove noninclusion of the corresponding lattice quasivarieties: $\mathscr{L}(R) \not\subseteq \mathscr{L}(S)$.

In §2, we prove the main result suggested by the discussion above. That is, we show that $\mathscr{L}(R) \subseteq \mathscr{L}(S)$ for rings with characteristic p^k implies:

$$\{e \in \mathscr{P}_0 : e_R = R\} \supseteq \{e \in \mathscr{P}_0 : e_S = S\},$$

where $\mathscr{P}_0$ denotes the set of polynomials on **0** and **1** generated by $\vee$, $\wedge$, $\cdot$, $\downarrow$ and $\uparrow$. So, any element of $\mathscr{P}_0$ is a potential starting point for proving inequality of $\mathscr{L}(R)$ and $\mathscr{L}(S)$. The motivation by diagrams above is not actually used in the proof, which relies on the methods of Fuller and Hutchinson [7].

We have not included the ring ideal residuation operations for $\mathrm{Su}({}_RR_R)$ (given as $\cdot.$ and $.\cdot$ in [2, pp. 325–327]) in this formulation. The reason is that the critical Lemma 2.7a in §2 does not seem to be provable if the context is extended by adding these two operations.

If R^{op} denotes the ring opposite to R, the lattice quasivariety $\mathscr{L}(R^{\mathrm{op}})$ is lattice-dual to $\mathscr{L}(R)$ [12, Theorem 3, p. 118]. That is:

$$\mathscr{L}(R^{\mathrm{op}}) = \{L^{\mathrm{op}} : L \in \mathscr{L}(R)\}.$$

Of course, $\mathscr{L}(R)$ is self-dual if R is a commutative ring, and it is also true that $\mathscr{L}(R)$ is self-dual for many noncommutative rings. (For example, $\mathscr{L}(R)$ is self-dual if R is the ring of $n \times n$ matrices over a commutative ring S, since then R is Morita equivalent to S, and so $\mathscr{L}(R) = \mathscr{L}(S)$.) In §3, we show that $\mathscr{L}(R)$ is not always self-dual. For p prime and $k \geq 2$, we construct a ring R with characteristic p^k such that $\mathscr{L}(R^{\mathrm{op}}) \neq \mathscr{L}(R)$. Note also that there are no (covariant) exact embedding functors R-**Mod** → R^{op}-**Mod** for such R. The examples are based on the noncommutativity of multiplication in $\mathrm{Su}({}_RR_R)$ with respect to polynomials in $\mathscr{P}_0$.

In the final section, we consider the ordered set $\mathcal{W}(p^k)$. This consists essentially of all lattice quasivarieties $\mathcal{L}(R)$ ordered by inclusion, for rings R with characteristic p^k. Alternatively, consider all pairs $\langle R, S\rangle$ of rings with characteristic p^k such that there exists an exact embedding functor R: **Mod** $\to S$-**Mod**. Then $\mathcal{W}(p^k)$ is essentially the poset of equivalence classes of rings induced by this reflective and transitive relation. It is shown that $\mathcal{W}(p_k)$ has power of continuum whenever $k \geq 2$, with continuous ascending and descending chains and continuous antichains. In particular, $\mathcal{W}(p^k)$ always contains a subset that is order isomorphic to the lattice of subsets of a denumerably infinite set. The proof is based on the selection of an *independent* denumerable subset $\{d_n : n \in H_0\}$ of $\mathcal{P}_0$. That is, for any subset H of the denumerable set H_0, a ring $R(H)$ of characteristic p^k is constructed so that for all n in H_0,

$$d_n = \mathbf{1} \text{ in } \mathrm{Su}({}_{R(H)}R(H)_{R(H)}) \quad \text{iff } n \in H.$$

All the required distinctness and noninclusion properties between the elements of $\mathcal{W}(p^k)$ corresponding to quasivarieties $\mathcal{L}(R(H))$ then follow from Theorem 2.7, the main result of §2. The required inclusions are proved by the construction of appropriate ring homomorphisms, which lead to exact embedding functors by change of rings.

2. Modules and annihilator ideals for rings with prime power characteristic

We first recall a useful selection of known sufficient and equivalent conditions relevant to submodule lattice representability.

PROPOSITION 2.1. *Suppose R and S are rings with unit. Each of the following conditions implies $\mathcal{L}(R) \subseteq \mathcal{L}(S)$, and* 2.1a *is equivalent to $\mathcal{L}(R) \subseteq \mathcal{L}(S)$*:

2.1a. *There exists an exact embedding functor F: R-*$\mathbf{Mod} \to S$-$\mathbf{Mod}$ [11, 13].

2.1b. *There exists a ring homomorphism $S \to R$ preserving* 1. (*Then there is an exact embedding functor R-*$\mathbf{Mod} \to S$-$\mathbf{Mod}$ *by change of rings.*)

2.1c. *There exists a bimodule ${}_RK_S$ such that ${}_RK$ is a projective generator.* (*Then* $\mathrm{Hom}_R({}_RK_S, -)$ *is an exact embedding functor R-*$\mathbf{Mod} \to S$-$\mathbf{Mod}$.)

In the following, we introduce a new condition equivalent to $\mathcal{L}(R) \subseteq \mathcal{L}(S)$ that is based on the analysis of Fuller and Hutchinson [7].

DEFINITIONS AND PROPERTIES 2.2. A right R-module M_R is called *1-flat* if for any $r_1, r_2, \ldots, r_n$ in R, there are $a_1, a_2, \ldots, a_n$ in R such that $\Sigma_{i=1}^n a_i r_i = 0$, and given any $v_1, v_2, \ldots, v_n$ in M_R such that $\Sigma_{i=1}^{n} v_i r_i = 0$, there is some v in M_R such that $va_i = v_i$ for each $i \leq n$.

Say that M_R has the *left invertibility property* if for all r in R, $Mr = M$ implies that $r_0 r = 1_R$ for some r_0 in R.

Let $|X|$ denote the cardinality of any set X.

2.2a. If M_R is 1-flat, then it is flat [1, Lemma 19.19, p. 228]. In fact, it is *strongly flat* in the sense of [7].

2.2b. $Rr = R$ iff $r_0 r = 1_R$ for some r_0 in R. For any M_R, $Rr = R$ implies that $Mr = M$.

THEOREM 2.3. *Suppose R and S are rings with unit. Let $_RK$ denote a free R-module with a set of generators of cardinality $\beta \geq \aleph_0 + |R|$, and let T denote the ring of R-endomorphisms of $_RK$, written with left to right composition*: $(st)(v) = t(s(v))$. *Then there is an exact embedding functor F: R-**Mod** $\rightarrow$ S-**Mod** iff there exists a bimodule $_SN_T$ such that N_T is 1-flat and has the left invertibility property.*

Proof. Assume the hypotheses, and suppose such an F exists. For $n \geq 1$, let $K^{(n)}$ denote $_RK \oplus {}_RK \oplus \cdots \oplus {}_RK$, n times, and note that $|K^{(n)}| = \beta$ since $\beta \geq \aleph_0 + |R|$. For any r: $K^{(n)} \rightarrow K$ in R-**Mod**, there exists a: $K \rightarrow K^{(n)}$ such that $\langle a, r\rangle$ is exact, since $_RK$ is free on β generators. Now $_SF(K)_T$ is a bimodule if we define $wt = F(t)(w)$ for t: $_RK \rightarrow {}_RK$ and w in $F(K)$. Taking $m = 1$, the proof of [7, Proposition 4, pp. 386–387] shows that $F(K)_T$ is 1-flat. If $N_T = F(K)_T$ and $Nt = N$, then $\operatorname{Im} F(t) = Nt = N = \operatorname{Ker} 0_N = \operatorname{Ker} F(0_K)$. Since exact embedding functors reflect exact pairs [5, Theorem 3.21, p. 66], it follows that $\operatorname{Im} t = \operatorname{Ker} 0_K = K$, so $t_0 t = 1_T$ for some t_0 in T, by choosing $t_0(x)$ in $t^{-1}[x]$ for each free generator x of K. So, N_T has the left invertibility property.

Now assume that there is such a bimodule $_SN_T$. The bimodule structure yields a ring homomorphism κ: $T \rightarrow \operatorname{End}(_SN)$ preserving 1, defined by $\kappa(t)(v) = vt$ for v in N and t in T. If κ preserves and reflects exactness, then there is an exact embedding functor F: R-**Mod** $\rightarrow$ S-**Mod** by [7, Theorem 10, p. 390]. (F is constructed by composing $\operatorname{Hom}(_RK_T, -)$ from R-**Mod** to T-**Mod** by 2.1c, with the exact functor $_SN \oplus_T -$ from T-**Mod** into S-**Mod**.) In fact, the proof of this theorem only requires that κ preserve exactness and reflect epimorphisms (that is, surjections). Suppose $\langle s, t\rangle$ is exact in R-**Mod** for s, t in T. Clearly $\operatorname{Im} \kappa(s) \subseteq \operatorname{Ker} \kappa(t)$. Let v be in $\operatorname{Ker} \kappa(t)$, so $vt = 0$. Since N_t is 1-flat, there are w in N and a in T such that $v = wa$ and $at = 0$. Then $\operatorname{Im} a \subseteq \operatorname{Ker} t = \operatorname{Im} s$, so $bs = a$ for some b in T. Then $v = \kappa(s)(wb) \in \operatorname{Im} \kappa(s)$, so $\langle \kappa(s), \kappa(t)\rangle$ is exact. Also, suppose $\kappa(t)$ is onto, so $Nt = \operatorname{Im} \kappa(t) = N$. By left invertibility for N_T, we have $t_0 t = 1_T$ for some t_0 in T, hence t is onto. So, κ preserves exactness and reflects epimorphisms. □

DEFINITION AND PROPERTIES 2.4. Define the algebraic type

$$\sigma = \langle \mathbf{0}, \mathbf{1}, \vee, \wedge, \cdot, \uparrow, \downarrow \rangle, \text{ with arities } \langle 0, 0, 2, 2, 2, 1, 1 \rangle.$$

If R is a ring with characteristic p^k, then $\mathrm{Su}({}_R R_R)$ is a σ-algebra as described in §1. The congruence lattice $\mathrm{Con}(R)$ is isomorphic to $\mathrm{Su}({}_R R_R)$, so $\mathrm{Con}(R)$ can also be regarded as a σ-algebra. In the following, we list some σ-polynomial equations that are satisfied in any such $\mathrm{Su}({}_R R_R)$ or $\mathrm{Con}(R)$. (We use exponents for repeated products, and also to indicate repeated application of unary operations $\uparrow$ or $\downarrow$.)

2.4a. $\langle \mathbf{0}, \mathbf{1}, \vee, \wedge \rangle$ is a $(\mathbf{0}, \mathbf{1})$ modular lattice.

2.4b. All σ-operations, hence all σ-polynomials c, are monotonic. That is, $c(x_1, \ldots, x_n) \leq c(y_1, \ldots, y_n)$ if $x_i \leq y_i$ for $i \leq n$.

2.4c. Multiplication is associative with unit $\mathbf{1}$, so $xy \leq x \wedge y$.

2.4d. $x(y \vee z) = xy \vee xz$ and $(x \vee y)z = xz \vee yz$.

2.4e. $\downarrow x \leq x \leq \uparrow x$.

2.4f. $\uparrow \downarrow x = x \vee \uparrow \mathbf{0}$ and $\downarrow \uparrow x = x \wedge \downarrow \mathbf{1}$.

2.4g. $(\downarrow x)y = \downarrow (xy) = x(\downarrow y)$.

2.4h. $\downarrow (x \vee y) = \downarrow x \vee \downarrow y$.

2.4i. $(\downarrow \mathbf{1})^k = \mathbf{0}$.

2.4j. $\uparrow^k \mathbf{0} = \mathbf{1}$ and $\downarrow^k \mathbf{1} = \mathbf{0}$. (But $\uparrow^{k-1} \mathbf{0} \neq \mathbf{1}$ and $\downarrow^{k-1} \mathbf{1} \neq \mathbf{0}$.)

Our σ-algebras differ from the usual residuated integral cl-semigroup structure for $\mathrm{Su}({}_R R_R)$ by addition of $\downarrow$ and $\uparrow$ operations, and deletion of residuation operations ($.\cdot$ and $\cdot .$).

DEFINITION AND PROPERTIES 2.5. Let $\mathscr{P}_0$ denote the absolutely free σ-algebra of all *constant* σ-polynomials, that is, σ-polynomials generated by $\mathbf{0}$ and $\mathbf{1}$ only, with no variables. Let η_R denote the unique σ-homomorphism from $\mathscr{P}_0$ into $\mathrm{Su}({}_R R_R)$, so that $\eta_R(e) = e_R$ for each e in $\mathscr{P}_0$.

Note that $\{e \in \mathscr{P}_0 \colon e_R = R\}$ is the equivalence class $\theta_R[\mathbf{1}] = \eta_R^{-1}[R]$ of the congruence θ_R on $\mathscr{P}_0$ induced by η_R.

2.5a. For any ring R with characteristic p^k, the subset $\eta_R^{-1}[R]$ of $\mathscr{P}_0$ contains $\mathbf{1}$ and is closed under products, intersections and the inverse image operation $\uparrow$, and admits joints $d \vee e$ such that either d or e is in $\eta_R^{-1}[R]$. (Obviously, $\mathbf{1} = \mathbf{1}\mathbf{1} = \mathbf{1} \wedge \mathbf{1} = \uparrow \mathbf{1} = d_R \vee \mathbf{1} = \mathbf{1} \vee e_R$ in $\mathrm{Su}({}_R R_R)$ by 2.4.)

An equation $\mathscr{L}(R) = \mathscr{L}(S)$ does not imply that η_R and η_S induce the same congruence on $\mathscr{P}_0$ in general, as we see by simple examples. Let $\mathbf{Z}$ denote the ring of integers and $\mathbf{Z}(p^k) = \mathbf{Z}/p^k\mathbf{Z}$ below.

PROPOSITION 2.6. *Let* $R = \mathbf{Z}(p^k)$ *and* $S = \mathbf{Z}(p^k) \times \mathbf{Z}(p)$ *for* p *prime and* $k \geq 2$. *Then* R *and* S *are rings with characteristic* p^k *such that* $\mathscr{L}(R) = \mathscr{L}(S)$. *If* $d = \downarrow^{k-1}\mathbf{1}$ *and* $e = \uparrow\mathbf{0}$, *then* $\eta_R(d) = \eta_R(e)$ *but* $\eta_S(d) \neq \eta_S(e)$.

Proof. There are ring homomorphisms $R \to S$ and $S \to R$ preserving 1, so $\mathscr{L}(R) = \mathscr{L}(S)$ by 2.1b. Clearly $\eta_R(d) = p^{k-1}R = \eta_R(e)$ but $\eta_S(d) = p^{k-1}S \neq \{s \in S: ps = 0\} = \eta_S(e)$. □

We now prove the main result of this section.

THEOREM 2.7. *Suppose* R *and* S *are rings with characteristic* p^k, p *prime and* $k \geq 2$. *If* $\mathscr{L}(R) \subseteq \mathscr{L}(S)$, *then* $\{e \in \mathscr{P}_0: e_R = R\} \supseteq \{e \in P_0: e_S = S\}$.

Proof. Assume the hypotheses, and let ${}_RK = {}_RR^{(\beta)}$ be the free R-module on a set X of β generators, for $\beta \geq \aleph_0 + |R|$. Let T be the ring of R-endomorphisms ${}_RK \to {}_RK$, written left to right, so T has characteristic p^k also. By 2.3, there exists a bimodule ${}_SN_T$ such that N_T is 1-flat and has the left invertibility property. We need:

LEMMA 2.7a. *If* e *is in* $\mathscr{P}_0$, *then* $e_sN \subseteq Ne_T$.

LEMMA 2.7b. *If* e *is in* $\mathscr{P}_0$ *and* $h: K \to K$ *is in* e_T, *then* $\operatorname{Im} h \subseteq e_RK$.

Both lemmas are proved by induction on the length of the σ-polynomial e.

Elementary arguments verify 2.7a when e is $\mathbf{0}$ or $\mathbf{1}$, when e is $\downarrow d$ for d such that $d_SN \subseteq Nd_T$, and when e is cd or $c \vee d$ with $c_SN \subseteq Nc_T$ and $d_SN \subseteq Nd_T$. If $e = \uparrow d$ with $d_SN \subseteq Nd_T$, then w in $\uparrow d_SN$ implies that $pw = \Sigma_{i=1}^n v_it_i$ for v_i in N and t_i in d_T, $i \leq n$. So, we have $za = w$ and $zb_i = v_i$ for some z in N and $a, b_1, \ldots, b_n$ in T satisfying $ap - \Sigma_{i=1}^n b_it_i = 0$, since N_T is 1-flat. (Identify p with the central element $1_T + \cdots + 1_T$, p times, in T.) Then $pa \in d_T$, so $w = za \in N\uparrow d_T$, proving $\uparrow d_SN \subseteq N\uparrow d_T$. The case $e = c \wedge d$ completes the induction, and it suffices to show that $Nc_T \wedge Nd_T \subseteq N(c_T \wedge d_T)$. Suppose $y \in Nc_T \wedge Nd_T$, so $y = \Sigma_{i=1}^n v_is_i = \Sigma_{j=1}^m w_jt_j$, for v_i in N and $s_i \in c_T$, $i \leq n$, and w_j in N and t_j in d_T, $j \leq m$. Since N_T is 1-flat, we have x in N, a_i in T for $i \leq n$ and b_j in T for $j \leq m$ such that $xa_i = v_i$ for $i \leq n$, $xb_j = w_j$ for $j \leq m$, and $\Sigma_{i=1}^n a_is_i - \Sigma_{j=1}^m b_jt_j = 0$. But then $q = \Sigma_{i=1}^n a_is_i = \Sigma_{j=1}^m b_jt_j \in c_T \wedge d_T$, proving that $y = xq$ is in $N(c_T \wedge d_T)$. This completes the proof for Lemma 2.7a.

Observe that $\Sigma_{i=1}^n r_ix_i$ is in e_RK for distinct $x_1, x_2, \ldots, x_n$ in the free generating set X for ${}_RK$ iff each r_i is in e_R, $i \leq n$. The proof of Lemma 2.7b follows by routine computations, which we omit.

Suppose $e_S = S$. Then $N = e_S N = N e_T$ using 2.7a. Since ${}_RK$ is free on β generators and $|{}_RK| = \beta$, there exists t_1 in T such that $\operatorname{Im} t_1 = e_R K$, and any h in T such that $\operatorname{Im} h \subseteq e_R K$ equals tt_1 for some t in T. By 2.7b, it follows that $e_T \subseteq Tt_1$, so $N = Ne_T = NTt_1 = Nt_1$, so $t_0 t = 1_T$ for some t_0 in T by the left invertibility hypothesis for N_T. Then t_1 is onto and $K = \operatorname{Im} t_1 = e_R K$. As noted above, $1_R x \in e_R K$ for x in X implies $1_R \in e_R$, so that $e_R = R$. □

The converse of Theorem 2.7 remains an open question.

PROBLEM 1. Do there exist rings R and S with characteristic p^k such that $\eta_R^{-1}[R] \supseteq \eta_S^{-1}[S]$ and $\mathscr{L}(R) \nsubseteq \mathscr{L}(S)$?

Note added at final revision. For additional information on Problem 1, see G. Czédli. Some lattice Horn sentences for submodules of prime power characteristic, Acta Math. Hungar. *65* (2) (1994), 195–201.

3. Opposite rings that have different classes of representable lattices

Except for multiplication, the σ-polynomial operations on $\mathrm{Su}({}_RR_R)$ depend only on the structure of R as an additive group. To study the opposite ring R^{op}, consider duals of σ-polynomials obtained by reversing products and leaving everything else unchanged.

DEFINITIONS AND PROPERTIES 3.1. If R is a ring with 1 and characteristics p^k, then R^{op} will denote the set $\{r^*: r \in R\}$ with the operations $r^* + s^* = (r+s)^*$ and $r^*s^* = (sr)^*$, as usual. So, R^{op} is a ring with unit 1^* and characteristic p^k.

For e in $\mathscr{P}_0$, define e^{op} recursively by the equations $\mathbf{0}^{\mathrm{op}} = \mathbf{0}$, $\mathbf{1}^{\mathrm{op}} = \mathbf{1}$, $(c \vee d)^{\mathrm{op}} = c^{\mathrm{op}} \vee d^{\mathrm{op}}$, $(c \wedge d)^{\mathrm{op}} = c^{\mathrm{op}} \wedge d^{\mathrm{op}}$, $(\uparrow c)^{\mathrm{op}} = \uparrow(c^{\mathrm{op}})$, $(\downarrow c)^{\mathrm{op}} = \downarrow(c^{\mathrm{op}})$ and (reversing) $(cd)^{\mathrm{op}} = d^{\mathrm{op}} c^{\mathrm{op}}$.

3.1a. For all e in $\mathscr{P}_0$, $(e^{\mathrm{op}})^{\mathrm{op}} = e$.

PROPOSITION 3.2. *If R is a ring with characteristic p^k and S is the opposite ring R^{op}, then $e_S = \{r^* \in S: r \in e_R^{\mathrm{op}}\}$ for all e in $\mathscr{P}_0$. In particular, $e_S = S$ iff $e_R^{\mathrm{op}} = R$.*

COROLLARY 3.3. *If R is a ring with characteristic p^k and $\mathscr{L}(R) = \mathscr{L}(R^{\mathrm{op}})$, then $\{e \in \mathscr{P}_0: e_R = R\} = \{e^{\mathrm{op}}: e \in \mathscr{P}_0$ and $e_R = R\}$.*

The proof follows from 2.7, 3.1a and 3.2.

It is known that $\mathscr{L}(R) \subseteq \mathscr{L}(S)$ implies $\mathscr{L}(R^{\mathrm{op}}) \subseteq \mathscr{L}(S^{\mathrm{op}})$, since there are contravariant exact embedding functors R^{op}-**Mod** → R-**Mod** and S-**Mod** → S^{op}-**Mod** by dual modules (or see [12, Theorem 3, p. 118]). This yields:

COROLLARY 3.4. *If* $\mathscr{L}(R) \subseteq \mathscr{L}(R^{\mathrm{op}})$, *then* $\mathscr{L}(R) = \mathscr{L}(R^{\mathrm{op}})$.

To construct S with characteristic p^k such that $\mathscr{L}(S) \neq \mathscr{L}(S^{\mathrm{op}})$, it suffices to find S and a σ-polynomial e such that $e_S \neq S$ but $e_S^{\mathrm{op}} = S$. A simple example is obtained by taking $e = \uparrow^{k-1}(\uparrow\mathbf{0}\uparrow(\uparrow\mathbf{0}\uparrow\mathbf{0}))$, as shown next.

THEOREM 3.5. *If p is prime and $k \geq 2$, then there exists a ring S with p^{k+7} elements and characteristic p^k such that* $\mathscr{L}(S) \neq \mathscr{L}(S^{\mathrm{op}})$.

Proof. Assume the hypotheses. Let $c = \uparrow\mathbf{0}$, so $e = \uparrow^{k-1}(c\uparrow(cc))$ and $e^{\mathrm{op}} = \uparrow^{k-1}(\uparrow(cc)c)$. To prove $1 \in e_S^{\mathrm{op}}$, it suffices to prove $p^{k-1} \in (\uparrow(cc)c)_S$, hence it suffices that $xy = p^{k-1}$ for some x in $(\uparrow(cc))_S$ and y in c_S, and so it suffices that there exist x, y, z and w in S such that $xy = p^{k-1}$, $px = zw$ and $py = pz = pw = 0$. Note that x^2 and yx must be nonzero in S to avoid $p^{k-1}x = 0$, which would lead to $px = 0$ in the case $k = 2$. In the ring S we construct, every element will be a $\mathbf{Z}$-linear combination of the elements:

$$1,\ x,\ x^2,\ xy,\ y,\ z \text{ and } w.$$

Based on the above list, define the $\mathbf{Z}$-module (abelian group):

$$A = C(p^k) \oplus C(p^2) \oplus C(p) \oplus C(p) \oplus C(p) \oplus C(p) \oplus C(p),$$

where $C(p^j)$ is cyclic of order p^j. Define

$$a_i = \langle 0, \ldots, 0, g_i, 0, \ldots, 0\rangle \text{ in } A \text{ for } i = 1, 2, \ldots, 7\rangle,$$

where g_i generates the ith factor of A. So, a_1 has order p^k, a_2 has order p^2, and a_3 through a_7 have order p. Also, $\{a_1, a_2, \ldots, a_7\}$ generates A as a weak basis. That is, for any integers $n_1, n_2, \ldots, a_7$, $\Sigma_{i=1}^{7} n_i a_i = 0$ implies that $n_i a_i = 0$ for $i \leq 7$. Let End(A) denote the ring of $\mathbf{Z}$-linear endomorphisms $A \to A$, again with left to right composition. Since A is a 7-term coproduct of cyclic groups in $\mathbf{Z}$-**Mod**, any λ in End(A) is uniquely determined by the 7-tuple $\langle\lambda(a_i)\rangle_{i \leq 7}$ in A^7, and λ can be defined by any choice of such $\langle\lambda(a_i)\rangle_{i \leq 7}$ provided only that $p^j a_i = 0$ must imply $p^j\lambda(a_i) = 0$ for $i \leq 7$. In the table below, we define seven elements of End(A) by listing the corresponding values $\lambda(a_1), \ldots, \lambda(a_7)$ in a column beneath λ. The nonzero entries in this table are motivated by the desired relations $\lambda_1 = 1$, $\lambda_x\lambda_y = p^{k-1}\lambda_1$ and $\lambda_z\lambda_w = p\lambda_x$, and the trivialities $\lambda_x\lambda_x = \lambda_{xx}$ and $\lambda_y\lambda_x = \lambda_{yx}$. Although they are not needed for the formal definitions, the correspondence on the left may assist the reader ($\lambda_u(a_i) = na_j$ if a_i corresponds to v and na_j to vu).

	λ_1	λ_x	λ_{xx}	λ_{yx}	λ_y	λ_z	λ_w
$a_1 \leftrightarrow 1$	a_1	a_2	a_3	a_4	a_5	a_6	a_7
$a_2 \leftrightarrow x$	a_2	a_3	0	$p^{k-1}a_2$	$p^{k-1}a_1$	0	0
$a_3 \leftrightarrow x^2$	a_3	0	0	0	$p^{k-1}a_2$	0	0
$a_4 \leftrightarrow yx$	a_4	0	0	0	0	0	0
$a_5 \leftrightarrow y$	a_5	a_4	0	0	0	0	0
$a_6 \leftrightarrow z$	a_6	0	0	0	0	0	pa_2
$a_7 \leftrightarrow w$	a_7	0	0	0	0	0	0

Let U denote the set $\{\lambda_1, \lambda_x, \lambda_{xx}, \lambda_{yx}, \lambda_y, \lambda_z, \lambda_w\}$. We observe that λ_1 is the unit 1_A of End(A) and has order p^k, λ_x has order p^2, and the other members of U have order p. We compute the multiplication table for elements of U:

	λ_1	λ_x	λ_{xx}	λ_{yx}	λ_y	λ_z	λ_w
λ_1	λ_1	λ_x	λ_{xx}	λ_{yx}	λ_y	λ_z	λ_w
λ_x	λ_x	λ_{xx}	0	$p^{k-1}\lambda_x$	$p^{k-1}\lambda_1$	0	0
λ_{xx}	λ_{xx}	0	0	0	$p^{k-1}\lambda_x$	0	0
λ_{yx}	λ_{yx}	0	0	0	0	0	0
λ_y	λ_y	λ_{yx}	0	0	0	0	0
λ_z	λ_z	0	0	0	0	0	$p\lambda_x$
λ_w	λ_w	0	0	0	0	0	0

Define S to be the **Z**-submodule of End(A) generated by U, that is:

$$S = \mathbf{Z}\lambda_1 + \mathbf{Z}\lambda_x + \mathbf{Z}\lambda_{xx} + \mathbf{Z}\lambda_{yx} + \mathbf{Z}\lambda_y + \mathbf{Z}\lambda_z + \mathbf{Z}\lambda_w.$$

By the multiplication table for U and ring distributivity, S is a subring of End(A) with unit λ_1. Since $\{\lambda(a_1) : \lambda \in U\} = \{a_1, a_2, \ldots, a_7\}$, U is a weak basis for S, so S is a ring with characteristic p^k and p^{k+7} elements. Again defining $c = \uparrow\mathbf{0}$, we compute the appropriate two-sided ideals of S:

$$c_S = \mathbf{Z}p^{k-1}\lambda_1 + \mathbf{Z}p\lambda_x + \mathbf{Z}\lambda_{xx} + \mathbf{Z}\lambda_{yx} + \mathbf{Z}\lambda_y + \mathbf{Z}\lambda_z + \mathbf{Z}\lambda_w,$$

$$c_S c_S = \mathbf{Z}p\lambda_x,$$

$$\uparrow(c_S c_S) = \mathbf{Z}p^{k-1}\lambda_1 + \mathbf{Z}\lambda_x + \mathbf{Z}\lambda_{xx} + \mathbf{Z}\lambda_{yx} + \mathbf{Z}\lambda_y + \mathbf{Z}\lambda_z + \mathbf{Z}\lambda_w,$$

$$\uparrow(c_S c_S)c_S = \mathbf{Z}p^{k-1}\lambda_1 + \mathbf{Z}p\lambda_x,$$

$$c_S \uparrow(c_S c_S) = \mathbf{Z}\lambda_{yx} + \mathbf{Z}p\lambda_x.$$

Now $p^{k-1}\lambda_1$ is not in $c_S\uparrow(c_S c_S)$, since U is a weak basis for S. But $p^{k-1}\lambda_1$ is in $\uparrow(c_S c_S)c_S$, so λ_1 is in e_S^{op} but not in e_S. Therefore, $e_S^{\mathrm{op}} = S$ and $e_S \neq S$, proving $\mathscr{L}(S) \neq \mathscr{L}(S^{\mathrm{op}})$. □

To assist in understanding the result, we recall the diagram approach of §1. Consider the pair of short exact sequences in S-**Mod**:

$$0 \to pA \to B \to pC \to 0 \quad \text{and} \quad 0 \to pB \to D \to pE \to 0.$$

Then z annihilates pA and w annihilates pC, so $px = zw$ annihilates B and x annihilates pB. But y annihilates pE, so $xy = p^{k-1}$ annihilates D. For S^{op}-**Mod**, $p^{k-1}D = 0$ follows from the dual short exact sequences:

$$0 \to pC \to B \to pA \to 0 \quad \text{and} \quad 0 \to pE \to D \to pB \to 0.$$

If there was an exact embedding functor F: S-**Mod** → S^{op}-**Mod**, then S-**Mod** would also have this dual property. So, an alternative approach to providing 3.5 would be to construct the dual pair of short exact sequences in S-**Mod** with $p^{k-1}D \neq 0$. (We do not assert that the alternative proof can be carried out exactly as stated, although the actual proof is based on a similar idea.)

4. The semilattice of lattice quasivarieties for rings with prime power characteristic

In this section, we study the ordered set $\mathscr{W}(p^k)$ of lattice quasivarieties $\mathscr{L}(R)$ for rings R with a fixed characteristic p^k. In the cases of interest, $\mathscr{W}(p^k)$ is a join semilattice, with a large and complicated structure.

DEFINITIONS 4.1. Let $\mathscr{W}$ denote the set of all quasivarieties of lattices, ordered by inclusion. For $m \geq 2$, let

$$\mathscr{R}(m) = \{R\colon R \text{ is a ring with unit having characteristic } m\},$$

and let $\mathscr{W}(m) = \{\mathscr{L}(R)\colon R \in \mathscr{R}(m)\} \subseteq \mathscr{W}$, also ordered by inclusion. Note that we have disregarded foundational problems, which may be avoided in many standard ways. (For example, quasivarieties are universal Horn classes, and so can be axiomatized by certain countable sets of implicational sentences for lattices. Alternatively, we may represent $\mathscr{K}$ by a set of its finitely generated members, taking one representative for each isomorphism class, since an arbitrary lattice L is in $\mathscr{K}$ iff every finitely generated sublattice of L is in $\mathscr{K}$.)

4.1a. $\mathscr{W}$ is a complete lattice, with complete meets obtained by taking intersections of quasivarieties, and complete joins characterized by the condition that $\mathscr{L}$ is in the join iff L satisfies every implicational sentence for lattices which is satisfied in every factor of the join. (Apply [2, Theorem 19, p. 123] to lattices and such implicational sentences.)

Note the following application of well-known results.

PROPOSITION 4.2. *If R and S are any rings with unit, then $\mathscr{L}(R) \vee \mathscr{L}(S) = \mathscr{L}(R \times S)$ in $\mathscr{W}$. In particular, $\mathscr{W}(p^k)$ is a join subsemilattice of $\mathscr{W}$.*

Proof. For any rings R and S with unit, $\mathscr{L}(R) \vee \mathscr{L}(S) \subseteq \mathscr{L}(R \times S)$ by 2.1b. If M is an $R \times S$-module, then $\langle 1, 0\rangle M$ is in R-Mod and $\langle 0, 1\rangle M$ is in S-Mod, with

$$\mathrm{Su}({}_{R\times S}M) \approx \mathrm{Su}({}_R\langle 1, 0\rangle M) \times \mathrm{Su}({}_S\langle 0, 1\rangle M)$$

in an obvious way. It follows easily that $\mathscr{L}(R \times S) = \mathscr{L}(R) \vee \mathscr{L}(S)$. The second part follows because $\mathscr{R}(p^k)$ is closed under products. □

PROPOSITION 4.3. *If p is prime and $k \geq 2$, then $\mathscr{W}(p^k)$ has the largest element $\mathscr{L}(\mathbf{Z}(p^k))$ and smallest element $\mathscr{L}(S_0)$, where S_0 is the* $\mathbf{Z}$-endomorphism ring of

$$B = C(p)^{(\omega)} \oplus C(p^2)^{(\omega)} \oplus \cdots \oplus C(p^k)^{(\omega)},$$

and $C(p^j)^{(\omega)}$ is an $\omega = \aleph_0$ direct power of cyclic groups of order p^j.

Proof. Obviously $\mathscr{L}(\mathbf{Z}(p^k))$ and $\mathscr{L}(S_0)$ are in $\mathscr{W}(p_k)$. Suppose $R \in \mathscr{R}(p^k)$. Since there exists a unique ring homomorphism $\mathbf{Z}(p^k) \to R$, we have $\mathscr{L}(R) \subseteq \mathscr{L}(\mathbf{Z}(p^k))$ by 2.1b. So, $\mathscr{L}(\mathbf{Z}(p^k))$ is the largest element of $\mathscr{W}(p^k)$.

By [15, Corollary 3, p. 30], if every finite system of ring equations which is solvable in R is also solvable in S, then $\mathscr{L}(S) \subseteq \mathscr{L}(R)$. So, there exists a finite or denumerable subring S of R such that $\mathscr{L}(S) = \mathscr{L}(R)$. Let

$${}_SM = S \oplus pS \oplus p^2S \oplus \cdots \oplus p^{k-1}S.$$

Since $p^kM = 0$, M (as an abelian group) is a direct sum of cyclic groups, each of order p^j for some $j \leq k$, by Kulikov's theorem (see [6, Theorem 17.1, p. 87]). Note that $p^{k-j}S$ has a cyclic direct summand of order p^j for $1 \leq j \leq k$, and so M has cyclic direct summands of all orders $p, p^2, \ldots, p^k$. But then the direct power ${}_SN = {}_SM^{(\omega)}$ is isomorphic to B as an abelian group, since M is denumerable.

A left S-module N corresponds to a ring homomorphism $S \to \mathrm{End}_{\mathbf{Z}}(N)^{\mathrm{op}}$ preserving 1 by [1, p. 26] (we compose left-to-right). Then $\mathscr{L}(S_0^{\mathrm{op}}) = \mathscr{L}(\mathrm{End}_{\mathbf{Z}}(N)^{\mathrm{op}}) \subseteq \mathscr{L}(\mathrm{S}) = \mathscr{L}(\mathrm{R})$ by 2.1b, and so $\mathscr{L}(S_0^{\mathrm{op}})$ is the smallest element of $\mathscr{W}(p^k)$. But then $\mathscr{L}(S_0) = \mathscr{L}(S_0^{\mathrm{op}})$ is smallest for $\mathscr{W}(p^k)$, using 3.4. □

We have been unable to settle some obvious questions about $\mathscr{W}(p^k)$ and its relationship to $\mathscr{W}$.

PROBLEM 2. Does $\mathscr{W}(p^k)$ admit all infinite $\mathscr{W}$-joins of its members? Does it admit all infinite $\mathscr{W}$-meets, or all finite $\mathscr{W}$-meets, of its members? Is $\mathscr{W}(p^k)$ a complete lattice, or even a lattice?

PROBLEM 3. Is $\mathscr{W}(p^k)$ order-isomorphic to $\mathscr{W}(q^k)$ for distinct primes p and q?

As noted in §1, $\mathscr{W}(p)$ is a singleton for p prime, by well-known results: $\mathscr{W}(p) = \{\mathscr{L}(S)\}$ for $S = \mathbf{Z}(p)$ since $R \in \mathscr{R}(p)$ implies $\mathscr{L}(R) \subseteq \mathscr{L}(S)$ by 2.1b and $\mathscr{L}(S) \subseteq \mathscr{L}(R)$ by 2.1a using the tensor product functor ${}_RR_S \otimes_S -$ corresponding to the free S-module R_S (S is a field). For $k \geq 2$ and p prime, we will show that $\mathscr{W}(p^k)$ has the largest possible cardinality (power of continuum $\aleph$, the cardinality of $\mathscr{W}$), and that $\mathscr{W}(p^k)$ is very complicated by the explicit criterion defined next.

DEFINITIONS AND PROPERTIES 4.4. Let $\mathbf{P}$ denote the Boolean algebra of all subsets of a denumerably infinite set X, ordered by inclusion. An ordered set $(Y, \leq)$ is called $\mathbf{P}$-*large* if there is a subset Y_0 of Y such that $\mathbf{P}$ is order-isomorphic to $(Y_0, \leq_0)$ for the order $\leq_0$ induced by $\leq$ on Y_0. The following facts are well known:

4.4a. If $(Y, \leq)$ is $\mathbf{P}$-large, then it has antichains with continuously many elements. (For example, there are continuously many pairwise incomparable subsets $X \cup X'$ of $\mathbf{Z}$, with $X \subseteq \{j : j \geq 1\}$ and $X' = \{-j : j \geq 1 \text{ and } j \notin X\}$.)

4.4b. If $(Y, \leq)$ is $\mathbf{P}$-large, then it has chains of continuously many elements isomorphic to the ordered set of real numbers $\mathbf{R}$. (For example, consider the cut sets $\{q \in \mathbf{Q} : q < r\}$ of the field of rationals $\mathbf{Q}$ corresponding to each r in $\mathbf{R}$.)

Hereafter, we consider a fixed prime p and fixed $k \geq 2$. To prove $\mathscr{W}(p^k)$ is **P**-large, we construct elements d_n in $\mathscr{P}_0$ (see 2.5) for $n \geq 2k$, and then show that a ring $R(H)$ in $\mathscr{W}(p^k)$ can be constructed from any subset $H \supseteq \{2k\}$ of $\{n: n \geq 2k\}$ so that $(d_n)_{R(H)} = R(H)$ iff $n \in H$. (We assume $2k$ is in H to avoid $H = \varnothing$, without loss of generality.)

DEFINITIONS 4.5. Let $H_0 = \{n: n \geq 2k\}$. Abbreviate $\uparrow^{k-1}$ by $\Uparrow$, so

$$\Uparrow K = \{r \in R: p^{k-1}r \in K\}$$

for K in $\mathrm{Su}({}_R R_R)$. Define elements $e_{j,n}$ in $\mathscr{P}_0$ for $n \in H_0$ by induction on j:

$$e_{0,n} = \mathbf{0},$$

$$e_{j,n} = (\Uparrow e_{j-1,n})^n \qquad \text{for } 1 \leq j \leq n-1.$$

For n in H_0, let $d_n = \Uparrow e_{n-1,n}$, and say that τ_n is satisfied in a ring R of $\mathscr{R}(p^k)$ if $(d_n)_R = R$.

DEFINITIONS AND PROPERTIES. Suppose $2k \in H \subseteq H_0$. Using the variables:

$$Y(H) = \{y_{n,i}: n \in H, 1 \leq i \leq n-1\},$$

form the free polynomial ring $F(H) = \mathbf{Z}(p^k)[Y(H)]$ on $Y(H)$ with coefficients in $\mathbf{Z}(p^k)$. Let $J(H)$ denote the ideal of $F(H)$ generated by:

$$\{y_{n,i}^n - p^{k-1}y_{n,i-1}: n \in H, 1 \leq i \leq n-1\} \cup \{p^{k-1}y_{n,n-1}: n \in H\}.$$

Here and in the sequel, $y_{n,0} = 1$ in $F(H)$. Finally, define $R(H) = F(H)/J(H)$. So, $R(H)$ is a commutative ring with 1.

Next, we describe the structure of $R(H)$. Hereafter, H will denote a fixed subset of $\{n: n \geq 2k\}$ containing $2k$.

DEFINITIONS AND PROPERTIES 4.7. Let $B = \{(n, i): n \in H, 1 \leq i \leq n-1\}$, and let W denote the set of all functions $w: B \to \mathbf{N}_0 = \{0, 1, 2, \ldots\}$ such that $w(n, i) = 0$ for all but finitely many elements of B. Note that associative and commutative sums $w + z$ can be defined pointwise for w, z in W.

Say that w in W has a *high power* if $w(n, i) \geq n$ for some (n, i) in B and has a *last variable* if $w(n, n-1) > 0$ for some n in H. Let U denote the set of all functions

u in W with no high power and no last variable (that is, $u(n, i) < n$ for all (n, i) in B, and $u(n, n-1) = 0$ for all n in H). Let V denote the set of all functions v in W with no high power and at least one last variable (that is, $v(n, i) < n$ for all (n, i) in B, and $v(n, n-1) > 0$ for at least one n in H). Let $\mathbf{U}$ denote the set of all finite subsets of U, and $\mathbf{V}$ the set of all finite subsets of V.

As usual, a *monomial* in $F(H)$ is a product $\alpha \prod_{(n,i) \in B} y_{n,i}^{w(n,i)}$ for α in $\mathbf{Z}(p^k)\backslash\{0\}$ and w in W. Every element of $F(H)$ is expressible as a sum of monomials obtained from distinct elements of W: the empty sum is 0 in $F(H)$ by convention. Let $x_{n,i} = y_{n,i} + J(H)$ in $R(H)$ for (n, i) in B, and $x_{n,0} = 1 + J(H)$ for n in H. Let y^w denote the product $\prod_{(n,i) \in B} y_{n,i}^{w(n,i)}$ in $F(H)$ for w in W, and $x^w = \prod_{(n,i) \in B} x_{n,i}^{w(n,i)} = y^w + J(H)$ in $R(H)$.

A monomial αy^w in $F(H)$, $\alpha \in \mathbf{Z}(p^k)\backslash\{0\}$ and $w \in W$, is called *reduced* if $w \in U$ or if $w \in V$ and $\alpha \in \{1, 2, \ldots, p^{k-1} - 1\} \subset \mathbf{Z}(p^k)$.

4.7a. $F(H)$ is free as a $\mathbf{Z}(p^k)$-module, with basis the set $\{y^w : w \in W\}$.

4.7b. Let c in W be given by $c(n, i) = 0$ for all (n, i) in B, so $c \in U$. Then $1y^c$ is the ring unit for $F(H)$, so $1x^c$ is the ring unit for $R(H)$.

4.7c. If v is in V, then $p^{k-1}y^v$ is in $J(H)$, and for $\alpha \in \mathbf{Z}(p^k)$, αy^v is in $\beta y^v + J(H)$ for some β in $\{0, 1, \ldots, p^{k-1} - 1\}$. (See 4.6, and let β be the remainder of α after division by p^{k-1}.)

4.7d. Suppose w in W has a variable $y_{n,i}$ and high power, and z in W satisfies $z(n, i) = w(n, i) - n$, $z(n, i-1) = w(n, i-1) + 1$ if $i > 1$, and $z(m, j) = w(m, j)$ otherwise. Then αy^w is in $p^{k-1}\alpha y^z + J(H)$, and αy^w is in $J(H)$ if z is not in U. (Use 4.6 and 4.7c, and note that $p^{2k-2} = 0$ in $\mathbf{Z}(p^k)$.)

We now show that every element of $R(H)$ is uniquely representable in $F(H)$ by a sum of reduced monomials obtained from distinct elements of $U \cup V$.

PROPOSITION 4.8. *Each $f + J(H)$ in $R(H)$, f in $F(H)$, has a canonical form*:

$$f + J(H) = \sum_{u \in C} \alpha_u y^u + \sum_{v \in D} \beta_v y^v + J(H),$$

where $C \in \mathbf{U}$, $D \in \mathbf{V}$, $\alpha_u \in \mathbf{Z}(p_k)\backslash\{0\}$ for all u in C, and $\beta_v \in \{1, 2, \ldots, p^{k-1} - 1\}$ for all v in D. (By convention, $C = D = \varnothing$ represents 0 *in $R(H)$.) The sets C and D and coefficients $\{\alpha_u : u \in C\}$ and $\{\beta_v : v \in D\}$ are uniquely determined.*

Proof. To show that every element of $R(H)$ is representable by a sum of reduced monomials, it suffices to show that every non-reduced monomial αy^w in $F(H)$ is either in $J(H)$ or in $\delta y^z + J(H)$ for some reduced monomial δy^z. If w has no high power, then it is in V since αy^w is not reduced, and so αy^w is in $J(H)$ or in

$\beta y^w + J(H)$ for βy^w reduced by 4.7c. If w has a high power, then αy^w is in $J(H)$ or $\delta y^z + J(H)$ for a suitable reduced monomial δy^z by 4.7d and the above.

To show that C, D and all α_u and β_v are uniquely determined for a given $f + J(H), f = \Sigma_{u \in C} \alpha_u y^u + \Sigma_{v \in D} \beta_v y^v$, it suffices to show that $C = D = \emptyset$ if f is in $J(H)$. But then $f = f_0$ in $F(H)$, where:

$$f_0 = \sum_{(n,i) \in P} g_{n,i} \cdot (y^n_{n,i} - p^{k-1} y_{n,i-1}) + \sum_{n \in Q} h_n \cdot p^{k-1} y_{n,n-1},$$

for finite subsets $P \subseteq B$ and $Q \subseteq H$, and elements $g_{n,i} \in F(H)$ for (n, i) in P and $h_n \in F(H)$ for n in Q.

If we express f_0 as a $\mathbf{Z}(p^k)$-linear combination of basis elements in $F(H)$ by 4.7a, then each monomial summand either has a high power or is a multiple of p^{k-1}. But then $D = \emptyset$, since a reduced βy^v for β in $\{1, 2, \ldots, p^{k-1} - 1\}$ and v in V is not a sum of such terms plus reduced monomials δy^w with $w \neq v$.

Suppose $C \neq \emptyset$, with u in C. Since u contains no high powers and no last variables, there is a δ in $\mathbf{Z}(p^k) \backslash \{0\}$ such that δy^u is a summand of a $\mathbf{Z}(p^k)$-linear combination of basis elements equal to $g_{n,i} \cdot (-p^{k-1} y_{n,i-1})$ for some (n, i) in P, by 4.7a. Expressing $g_{n,i}$ as a $\mathbf{Z}(p^k)$-linear combination of basis elements, it has a summand monomial $\kappa y^{u'}$ such that $-p^{k-1}\kappa = \delta$ in $\mathbf{Z}(p^k)$ and u' in U satisfies $u'(m, j) = u(m, j)$, except that $u'(n, i-1) = u(n, i-1) - 1$ if $i > 1$. Define $u'' : B \to \mathbf{N}_0$ by $u''(m, j) = u'(m, j)$ for $(m, j) \neq (n, i)$ and $u''(n, i) = u'(n, i) + n = u(n, i) + n$. Then $\kappa y^{u''}$ is a summand of $g_{n,i} \cdot y^n_{n,i}$, and $y_{n,i}$ is the only variable with a high power in u''. From $-p^{k-1}\kappa = \delta \neq 0$, we have $p \nmid \kappa$ in $\mathbf{Z}(p^k)$. Since all the other summands of f_0 not obtained from $g_{n,i} \cdot y^n_{n,i}$ have either *another* variable with high power or a coefficient divisible by p, $f = f_0$ cannot hold, and $C = \emptyset$. □

COROLLARY 4.9. *$R(H)$ is in $\mathscr{R}(p^k)$, so $\mathscr{L}(R(H))$ is in $\mathscr{W}(p^k)$.*

Proof. Use 4.7b and 4.8.

PROPOSITION 4.10. *If $n \in H \subseteq H_0$, then 4.10a holds for $j = 1, 2, \ldots, n$, and τ_n is satisfied for $R(H)$.*

4.10a. $y_{n,n-j} + J(H) \in (\Uparrow e_{j-1,n})_{R(H)}$.

Proof. First, verify 4.10a by induction. Note that $p^{k-1} y_{n,n-1}$ is in $J(H)$ for $n \in H$, so $y_{n,n-1} + J(H)$ is in $(\Uparrow e_{0,n})_{R(H)}$. This proves 4.10a for $j = 1$, so assume 4.10a as induction hypothesis, for $1 \leq j < n$. Using 4.6, we have:

$$p^{k-1} y_{n,n-(j+1)} + J(H) = y^n_{n,n-j} + J(H) \in (\Uparrow e_{j-1,n})^n_{R(H)} = (e_{j,n})_{R(H)},$$

and 4.10a for $j+1$ follows, completing the induction. By 4.10a with $j=n$:

$$1_{R(H)} = y_{n,0} + J(H) \in (\Uparrow e_{n-1,n})_{R(H)} = (d_n)_{R(H)},$$

from which it follows that τ_n holds for $R(H)$. □

By close analysis, we will see that τ_n is not satisfied in $R(H)$ when n is in $H_0 \backslash H$. The remaining desired results then follow quickly.

DEFINITIONS AND PROPERTIES 4.11. Fix H and n with $2k \in H \subseteq H_0$ and $n \in H_0 \backslash H$. For $0 \leq j \leq n-1$ and w in W, say that the predicate last (j, w) holds iff there exists $m > n$, $m \in H$, such that

$$w(m, m-2) + w(m, m-3) + \cdots + w(m, m-j-1) \geq 1,$$

and that last*(j, w) holds iff

$$\sum_{\substack{m \in H \\ m > n}} [w(m, m-2) + w(m, m-3) + \cdots + w(m, m-j-1)] \geq 2.$$

By convention, any empty sums equal zero. In particular, the sums above are taken as empty if $j = 0$.

4.11a. For all w, last$(0, w)$ and last*$(0, w)$ do not hold.

4.11b. If last$(j, 2)$ holds, then so does last(s, w) for $j < s \leq n-1$.

4.11c. If last(j, w) holds, then so does last$(j, w+z)$ for all z in W. If last*(j, w) holds, then so does last*$(j, w+z)$ for all z in W.

4.11d. If last(j, w) and last(j, z) both hold, then last*$(j, w+z)$ holds. If last*(j, w) holds, then last(j, w) holds.

PROPOSITION 4.12. *Suppose n is in $H_0 \backslash H$, and L_j is the $\mathbf{Z}(p^k)$-submodule of $R(H)$ generated by $W_j = U_{j1} \cup U_{j2} \cup V_0$ for $j = 0, 1, \ldots, n-1$, where*:

$$U_{j1} = \{1x^u \colon u \in U \text{ and } last(j, u)\},$$

$$U_{j2} = \{px^z \colon z \in U \text{ and not } last(j, z)\},$$

$$V_0 = \{1x^v \colon v \in V\}.$$

Then L_j is an ideal of $R(H)$ which satisfies 4.12a *for $j = 0, 1, \ldots, n-1$, and τ_n is not satisfied in $R(H)$.*

4.12a. $(\Uparrow e_{j,n})_{R(H)} \subseteq L_j$.

Proof. Assume the hypotheses, and suppose that $0 \leq j \leq n - 1$. By 4.7a, L_j is an ideal if αx^{w+z} is in L_j for all w in W and αx^z in W_j. By 4.7d, x^{w+z} is a multiple of p^{k-1} if $w + z$ has a high power, and then αx^{w+z} is in L_j by 4.8. If $w + z$ has a last variable and no high power, then $1x^{w+z}$ is in $V_0 \subseteq L_j$. Otherwise, $w + z$ is in U, hence z is in U. Then αx^{w+z} is in L_j if last$(j, w + z)$, and also if not last$(j, w + z)$ because then not last(j, z) holds by 4.11c and p divides α by 4.8. Therefore, each L_j is an ideal of $R(H)$.

Next, verify 4.12a by induction on j. If $j = 0$, then 4.12a follows from 4.8, 4.11a and $\Uparrow\mathbf{0} = \downarrow\mathbf{1}$ for $\mathbf{Z}(p^k)$. So, assume 4.12a as induction hypothesis, $0 \leq j < n - 1$. Let K denote the $\mathbf{Z}(p^k)$-submodule of $R(H)$ generated by $K^* \cup V_0$, where:

$$K^* = \{1x^u\colon u \in U \text{ and last}^*(j, u)\} \cup \{px^u\colon u \in U \text{ and last}(j + 1, u)\}.$$

To prove that $L_j^n \subseteq K$, it suffices by ring distributivity to show that αx^w is in K for $\alpha = \alpha_1\alpha_2, \ldots, \alpha_n$ and $w = w_1 + w_2 + \cdots + w_n$, where $\alpha_s x^{w_s}$ is in W_j for $s = 1, 2, \ldots, n$. Since 0 is in K, we assume $\alpha x^w \neq 0$.

Suppose that w has no high power. If w has a last variable, then $1x^w$ is in V_0, hence αx^w is in K. Suppose w has no last variable, so $w \in U$. Then no w_s has a last variable, hence all $\alpha_s x^{w_s}$ are in $U_{j1} \cup U_{j2}$ by 4.8. But $\alpha = 0$ if more than k elements α_s are equal to p, hence by 4.8 at least $n - k \geq k \geq 2$ elements $\alpha_s x^{w_s}$ are in U_{j1}. Since last(j, w_s) for two or more s values implies last$^*(j, w)$ by 4.11c,d, αx^w is in K.

Now suppose that w has a high power, say $w(m, i) \geq m$ for $(m, i) \in B$. Define z in W by $z(m, i) = w(m, i) - m$, $z(m, i - 1) = w(m, i - 1) + 1$ if $i > 1$, and $z(s, t) = w(s, t)$ otherwise. By 4.7d, $\alpha x^w = p^{k-1}\alpha x^z$, and $\alpha x^w \neq 0$ implies $z \in U$ and $p \nmid \alpha$, hence no $\alpha_s x^{w_s}$ is in U_{j2}. If some $\alpha_s x^{w_s}$ is in U_{j1}, then last(j, w) holds by 4.11c, so either last(j, z) holds or $m > n$ and $m - j - 1 \leq i \leq m - 2$, so last$(j + 1, z)$ holds by 4.11b or because $z(m, i - 1) > 0$, hence $\alpha x^w = p^{k-1}\alpha x^z$ is in K. Otherwise, $\alpha_s x^{w_s}$ is in V_0 for all $s \leq n$. Then z in U implies that $i = m - 1$, $w_s(m, m - 1) > 0$ for all $s \leq n$, $w(m, m - 1) = m$ and $z(m, m - 2) > 0$. But then $m \geq n$, and so $m > n$ since $m \in H$ and $n \notin H$. Therefore, last$(1, z)$ holds, and $\alpha x^w = p^{k-1}\alpha x^z$ is in K by 4.11b. This completes the proof that $L_j^n \subseteq K$.

Suppose $f \in \Uparrow(L_j^n)$, and $f = \Sigma_{u \in C}\, \alpha_u x^u + \Sigma_{v \in D}\, \beta_v x^v$ as in 4.8. Using 4.7c,

$$p^{k-1}f = \sum_{u \in C} p^{k-1}\alpha_u x^u \in L_j^n \subseteq K.$$

By the uniqueness in 4.8, either $p \mid \alpha_u$ or last$^*(j, u)$ holds or last$(j + 1, u)$ holds for each u in C. If $p \mid \alpha_u$, obviously $\alpha_u x^u$ is in L_{j+1}. Now last$^*(j, u)$ implies last$(j + 1, u)$ by 4.11b,d, and so $\alpha_u x^u$ is in L_{j+1} in the last two cases. Then $V_0 \subseteq L_{j+1}$ implies $f \in L_{j+1}$, so:

$$(\Uparrow e_{j+1,n})_{R(H)} = \Uparrow((\Uparrow e_{j,n})^n)_{R(H)} \subseteq \Uparrow(L_j^n) \subseteq L_{j+1},$$

using 4.12a and the above. This completes the induction, and so 4.12a holds for $0 \leq j \leq n-1$.

By 4.12a with $j = n-1$, $(d_n)_{R(H)} = (\Uparrow e_{n-1,n})_{R(H)} \subseteq L_{n-1}$. Since $1_{R(H)}$ is not in L_{n-1} by 4.7b and 4.8, τ_n is not satisfied in $R(H)$. □

Our theorem follows; the ordered set of lattice quasivarieties obtained from rings with characteristic p^k has a subset isomorphic to the set of all subsets of a denumerable set.

THEOREM 4.13. *Let p be prime and $k \geq 2$. then $\mathscr{W}(p^k)$ is* **P**-*large, using the function assigning $\mathscr{L}(R(H))$ to any H such that $2k \in H \subseteq \{n: n \geq 2k\}$. In particular, $\mathscr{W}(p^k)$ has power of continuum with continuous antichains and continuous ascending and descending chains.*

Proof. By 4.9, we can assign $\mathscr{L}(R(H))$ in $\mathscr{W}(p^k)$ to any such H. Suppose $\{2k\} \subseteq H_j \subseteq H_0$ for $j = 1, 2$. Then $H_1 \supseteq H_2$ iff $\mathscr{L}(R(H_1)) \subseteq \mathscr{L}(R(H_2))$. The forward implication follows from 2.1b since the obvious ring homorphism $F(H_2) \rightarrow F(H_1) \rightarrow F(H_1)/J(H_1)$ annihilates $J(H_2)$ by 4.6. The reverse implication follows by 4.10 and 4.12, because n in H_2 implies that τ_n is satisfied in $\mathscr{L}(R(H_2))$, hence in $\mathscr{L}(R(H_1))$, hence n is in H_1. Therefore, $\mathscr{W}(p^k)$ is **P**-large since **P** is order isomorphic to $\langle\{H: 2k \in H \subseteq H_0\}, \supseteq\rangle$. (Recall that **P** is isomorphic to its order dual by set complementation.) The rest follows from 4.4a,b. □

This result easily extends to rings with non-square-free characteristic. Rings with composite characteristic are reducible to products of rings with prime power characteristic in the usual way.

PROPOSITION 4.14. *Suppose $m \geq 2$ and the prime power factorization of m is $p_1^{k(1)} p_2^{k(2)} \cdots p_s^{k(s)}$, for s distinct primes p_j and positive integers $k(j)$. Then there is a join semilattice isomorphism*:

$$\lambda: \mathscr{W}(m) \rightarrow \mathscr{W}(p_1^{k(1)}) \times \mathscr{W}(p_2^{k(2)}) \times \cdots \times \mathscr{W}(p_s^{k(s)}).$$

For R of characteristic m, λ is defined by:

$$\lambda(\mathscr{L}(R)) = \langle \mathscr{L}(R/p_1^{k(1)}R), \mathscr{L}(R/p_2^{k(2)}R), \ldots, \mathscr{L}(R/p_s^{k(s)}R)\rangle.$$

The reciprocal λ_* of λ is defined for R_j in $\mathscr{R}(p_j^{k(j)})$, $j \leq s$, by:

$$\lambda_*\langle \mathscr{L}(R_1), \mathscr{L}(R_2), \ldots, \mathscr{L}(R_s)\rangle = \mathscr{L}(R_1 \times R_2 \times \cdots \times R_s).$$

Proof. Suppose $\mathscr{L}(R) \subseteq \mathscr{L}(S)$ for R and S in $\mathscr{R}(m)$. For $j \leq s$, exact embedding functors F from 2.1a and G_j, H_j from 2.1b in the diagram below can be completed to a commutative square by a unique exact embedding functor F_j:

$$\begin{tikzcd}
R/p_j^{k(j)}R\text{-}\mathbf{Mod} \arrow[r, "F_j"] \arrow[d, "G_j"'] & S/p_j^{k(j)}S\text{-}\mathbf{Mod} \arrow[d, "H_j"'] \\
R\text{-}\mathbf{Mod} \arrow[r, "F"] & S\text{-}\mathbf{Mod}
\end{tikzcd}$$

Then $\mathscr{L}(R/p_j^{k(j)}R) \subseteq \mathscr{L}(S/p_j^{k(j)}S)$ in $\mathscr{W}(p_j^{k(j)})$ for $j \leq s$ by 2.1a, and so λ is a well-defined and order-preserving function. Clearly λ_* is well-defined and preserves order by 4.2. We omit the standard computations verifying that λ and λ_* are reciprocal bijections. □

COROLLARY 4.15. *Suppose $m \geq 2$. If m is a square-free integer (a product of distinct primes), then $\mathscr{W}(m)$ is the singleton $\{\mathscr{L}(\mathbf{Z}(m))\}$. If m is not square-free, then $\mathscr{W}(m)$ is* **P**-*large.*

The first part was proved in [11, Theorem 5(6), p. 88]; it also follows from 4.14 because each $\mathscr{W}(p)$ equals $\{\mathscr{L}(\mathbf{Z}(p))\}$. The second part follows easily from 4.13 and 4.14, since m then has a factor p^k for $k \geq 2$.

REFERENCES

[1] ANDERSON, F. W. and FULLER, K. R., *Rings and Categories of Modules*, Springer Verlag, New York, Heidelberg and Berlin, 1973.

[2] BIRKHOFF, G., *Lattice Theory*, third ed., Amer. Math. Soc. Colloquium Publications 25, Amer. Math. Soc., 1967.

[3] BURRIS, S. and SANKAPPANAVAR, H. P., *A Course in Universal Algebra*, Springer, 1981.

[4] CZÉDLI, G. and HUTCHINSON, G., *An irregular Horn sentence in submodule lattices*, Acta Sci. Math. (Szeged) *51* (1987), 35–38.

[5] FREYD, P. J., *Abelian Categories, An Introduction to the Theory of Functors*, Harper and Row, 1964.

[6] FUCHS, L., *Infinite Abelian Groups, Volume I*, Academic Press, New York, 1970.

[7] FULLER, K. R. and HUTCHINSON, G., *Exact embedding functors and left coherent rings*, Proc. Amer. Math. Soc. *104* (1988), 385–391.

[8] GRÄTZER, G., *Universal Algebra*, second ed., Springer Verlag, 1979.

[9] HUTCHINSON, G., *Modular lattices and abelian categories*, J. Algebra *19* (1971), 156–184.

[10] HUTCHINSON, G., *Recursively unsolvable word problems of modular lattices and diagram-chasing*, J. Algebra *26* (1973), 385–399.

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

[12] HUTCHINSON, G., *A duality principle for lattices and categories of modules*, J. Pure Appl. Algebra *10* (1977), 115–119.

[13] Hutchinson, G., *Exact embedding functors between categories of modules*, J. Pure Appl. Algebra *25* (1982), 107–111.

[14] Hutchinson, G. and Czédli, G., *A test for identities satisfied in lattices of submodules*, Algebra Universalis *8* (1978), 269–309.

[15] Makkai, M. and McNulty, G., *Universal Horn axiom systems for lattices of submodules*, Algebra Universalis *7* (1977), 25–31.

G. Czédli
JATE Bolyai Institute
Aradi vértanúk tere 1
H-6720 Szeged
Hungary
e-mail: czedli@math.u-szeged.hu

G. Hutchinson
Department of Mathematics
University of Maryland
College Park, MD 20742
U.S.A.
e-mail: ghutch@math.umd.edu