Proc. Univ. of Houston
Lattice Theory Conf..Houston 1973

ON CLASSES OF LATTICES REPRESENTABLE BY MODULES

by

George Hutchinson

Division of Computer Research and Technology
National Institutes of Health, Public Health Service
Department of Health, Education and Welfare, Bethesda, Md. 20014

ABSTRACT

For a ring R with 1, let $\mathcal{L}(R)$ denote the class of lattices representable in submodule lattices of R-modules. It is shown that the binary ring predicate $\mathcal{L}(R) \subset \mathcal{L}(S)$ is related to the existence of exact embedding functors R-Mod $\longrightarrow$ S-Mod. The predicate $\mathcal{L}(R) \subset \mathcal{L}(S)$ can be evaluated in general if it can be evaluated for rings with the same characteristic. Furthermore, only rings with zero or prime power characteristic need be considered. Necessary and sufficient conditions on R are given such that $\mathcal{L}(R) = \mathcal{L}(S)$ for S a unitary subring of the field of rationals or for S the ring of integers modulo n, n a prime or a product of distinct primes.

AMS(MOS) Classification: Primary 06A30, 13C99.

Given a ring R with unit, a lattice L is "representable by R-modules" if there exists a unitary left R-module M such that L is embeddable in the lattice of submodules of M. Of course, embeddability in the lattice of submodules of M is equivalent to embeddability in the lattice of congruences of M [1: VII, Thm. 1, p. 159]. In the following, we consider the general problem:

For which rings with unit R and S is every lattice representable by R-modules also representable by S-modules?

Our attack on this problem uses abelian category methods in addition to the methods of modular lattice theory. Let us first introduce some notation. Hereafter, R and S will denote rings with unit. The lattice of submodules of a left unitary R-module M will be denoted $\Gamma(M;R)$. The class of all lattices representable by R-modules will be denoted $\mathfrak{L}(R)$. Hence, our general problem is the study of the binary ring predicate $\mathfrak{L}(R) \subset \mathfrak{L}(S)$ for various choices of R and S.

Let R-Mod denote the abelian category of all R-modules and R-linear maps between them. If β is a cardinal number, we will also consider R-Mod(β), the category of all R-modules with cardinality less than β and all R-linear maps between such modules. Note that R-Mod(β) is an exact subcategory of R-Mod if β is infinite. Let card(X) denote the cardinality of a set X.

To digress momentarily, we remark that $\mathfrak{L}(R)$ is a "quasivariety" of lattices, that is, $\mathfrak{L}(R)$ is the class of all lattices satisfying some set of universal Horn formulas. (A universal lattice Horn formula is of form:

$$(x_1, x_2, \ldots, x_m)\ ((e_1 = e_2 \ \& \ \ldots \ \& \ e_{2n-3} = e_{2n-2}) \Rightarrow e_{2n-1} = e_{2n}),$$

where $e_1, e_2, \ldots, e_{2n}$ are lattice polynomials in the variables $x_1, x_2, \ldots, x_m$.) This was proved by a model theoretic argument in general [4: Thm. 6], and was proved by discovery of a constructive procedure for generating infinite Horn formula axiomatizations of $\mathfrak{L}(R)$ in the commutative case [6, 7: Main Thm.]. In [4: Thm. 3], a result is obtained implying that $\mathfrak{L}(R)$ is not finitely first-order axiomatizable if R is the ring of integers, or if R is the field of rationals, or if R is any ring between the integers and the rationals (that is, any unitary subring of the rationals). In [10], another model theory approach yields the following results: (1) If R is a ring defined on a recursive set of natural numbers with recursive ring operations of addition and multiplication, then there is a primitive recursive set of universal Horn formulas characterizing $\mathfrak{L}(R)$. (2) Suppose that a "term" is 0, 1 or a variable $y_1, y_2, \ldots, y_n$, and an "equation" is $t_1 + t_2 = t_3$ or $t_1 t_2 = t_3$ for terms t_1, t_2 and t_3. For any rings R and S with unit, either $\mathfrak{L}(R) \subset \mathfrak{L}(S)$ or there exists a system of equations that is true in S for some assignment of elements of S to $y_1, y_2, \ldots, y_n$ but which is false in R for every assignment of elements of R to $y_1, y_2, \ldots, y_n$.

Let us now return to consideration of the predicate $\mathfrak{L}(R) \subset \mathfrak{L}(S)$. We begin by stating a conjecture:

For any rings R and S with unit, $\mathfrak{L}(R) \subset \mathfrak{L}(S)$ if and only if there exists an exact embedding functor $R\text{-Mod} \longrightarrow S\text{-Mod}$.

We will not prove this conjecture as stated, but will prove a slightly weaker version for our first theorem. Specifically, we will prove $\mathfrak{L}(R) \subset \mathfrak{L}(S)$ equivalent to the following:

For every infinite cardinal β, there exists an exact embedding functor $R\text{-Mod}(\beta) \longrightarrow S\text{-Mod}$.

The following propositions lead up to the proof of this result.

Prop. 1. If there exists an exact embedding functor $R\text{-Mod} \longrightarrow S\text{-Mod}$, then $\mathfrak{L}(R) \subset \mathfrak{L}(S)$.

Prop. 2. If there exists a ring homomorphism $S \longrightarrow R$ preserving 1, then $\mathfrak{L}(R) \subset \mathfrak{L}(S)$.

Prop. 3. If there exists a bimodule M (left S-module, right R-module) which is faithfully flat as an R-module, then $\mathfrak{L}(R) \subset \mathfrak{L}(S)$. (M is "faithful" if $M \otimes_R M_0 = 0$ implies $M_0 = 0$ for all M_0 in R-Mod.)

To prove $\mathfrak{L}(R) \subset \mathfrak{L}(S)$, it suffices to show that $\Gamma(M;R)$ is in $\mathfrak{L}(S)$ for each M in R-Mod. Suppose $F:\text{R-Mod} \longrightarrow \text{S-Mod}$ is an exact embedding functor. Then F induces a lattice embedding $F_0:\Gamma(M;R) \longrightarrow \Gamma(F(M);S)$ defined by $F_0[f] = [Ff]$ for $[f]$ a subobject of M. (See [5: p. 183] for relevant information. Note also that we have identified the lattice of submodules of M with the lattice of subobjects of M in R-Mod, and similarly for $F(M)$ in S-Mod.) This proves Prop. 1.

If there exists a ring homomorphism $h:S \longrightarrow R$ preserving 1, it is well-known (and easily verified) that the "change of rings" operation [2: p. 28ff] $M \longrightarrow M_{(h)}$ induces an exact embedding $\text{R-Mod} \longrightarrow \text{S-Mod}$. So, Prop. 2 follows from Prop. 1.

The hypotheses of Prop. 3, interpreted, assert that $M \otimes_R -$ is an exact functor that reflects zero objects (that is, every inverse image of a zero object is zero). But then $M \otimes_R -$ is an exact embedding functor [11: II, 7.2, p. 57]. Therefore, Prop. 3 also follows from Prop. 1.

To prove that $\mathfrak{L}(R) \subset \mathfrak{L}(S)$ implies existence of an exact embedding functor $\text{R-Mod}(\beta) \longrightarrow \text{S-Mod}$, we make use of the "abelian" lattice concept of [5]. By [5: Main Thm.], a functor A can be constructed, taking an abelian lattice L into a small abelian category A_L, and taking a lattice homomorphism $b:L \longrightarrow M$ of abelian lattices into an exact functor $\mathbf{A}_b\colon \mathbf{A}_L \longrightarrow \mathbf{A}_M$. If b is a lattice embedding, then $\mathbf{A}_b$ reflects zero objects by [5: 3.16, p. 172], and so $\mathbf{A}_b$ is an embedding functor by [11: II, 7.2, p. 57].

Definition. Let β be an infinite cardinal number, regarded as the set of smaller ordinals. Let R_β be the free R-module with β generators, with free generating set $\{ x_\delta\colon \delta \in \beta \}$. A submodule M of R_β has "bounded support" if there exists a subset A of β such that card(A) < β and M is contained in the submodule of R_β generated by $\{x_\delta\colon \delta \in A\}$. Let $\Gamma_b(R_\beta;R)$ denote the set of submodules of R_β with bounded support.

Prop. 4. If β is an infinite cardinal, then $\Gamma_b(R_\beta;R)$ is an ideal of $\Gamma(R_\beta;R)$, and is an abelian lattice.

Proof: Modify the proof of [5: 4.2]. We will only outline the proof that any M in $\Gamma_b(R_\beta;R)$ can be "tripled". Choose $A \subset \beta$ such that card(A) < β and M is contained in the submodule generated by $\{ x_\delta\colon \delta \in A \}$. Since card($\beta$ - A) = β, we can choose $B \subset \beta - A$ and a bijection $\theta\colon A \longrightarrow B$. Now each m in M can be expressed uniquely as a sum $\sum_{\delta\in A} r_\delta x_\delta$, where all but finitely many of the coefficients r_δ equal zero. Then define:

$$M_1 = \{ \sum_{\delta\in A} r_\delta x_{\theta(\delta)} \colon \sum_{\delta\in A} r_\delta x_\delta \in M \},$$

$$M_2 = \{ \sum_{\delta\in A} r_\delta (x_\delta - x_{\theta(\delta)}) \colon \sum_{\delta\in A} r_\delta x_\delta \in M \}.$$

It is easily shown that M_1 and M_2 are in $\Gamma_b(R_\beta;R)$ and that M, M_1 and M_2 generate the five-element modular lattice of length two.

Prop. 5. If M is in R-Mod and $\beta > \aleph_0 + \text{card}(M)$, then there exists a lattice embedding $\Gamma(M;R) \longrightarrow \Gamma_b(R_\beta;R)$.

Proof: Assume the hypotheses. Let $\gamma = \text{card}(M)$, and extend a bijection $f_0:\gamma \longrightarrow M$ to an R-linear epimorphism $f:R_\gamma \longrightarrow M$ by the free module property. Then $\Gamma(M;R)$ is isomorphic to the interval sublattice $[\ker f, R_\gamma]$ of R_γ. Since R_γ can be regarded as a bounded submodule of R_β, there exists an embedding $\Gamma(M;R) \longrightarrow \Gamma(R_\gamma;R) \longrightarrow \Gamma_b(R_\beta;R)$.

Prop. 6. If M is an R-module with generating set G, then

$$\text{card}(M) \leqq \aleph_0 + \text{card}(R) + \text{card}(G).$$

Proof: Let X be the set $\bigcup_{n=1}^{\infty} (R^n \times G^n)$, and define the function m from X onto M given by:

$$m((r_1, r_2, \ldots, r_n), (g_1, g_2, \ldots, g_n)) = \sum_{i=1}^{n} r_i g_i.$$

If $\gamma = \aleph_0 + \text{card}(R) + \text{card}(G)$, then:

$$\text{card}(M) \leqq \text{card}(X) \leqq \sum_{n=1}^{\infty} (\gamma^n)^2 = \gamma.$$

In the next two propositions, we will use the definitions and notations of [5] without reference.

Prop. 7. Let L be an ideal of some $\Gamma(M;R)$, and Hom_R denote Hom in R-Mod. If $A, B: \mathbf{2} \longrightarrow L$ are r-disjoint, then there is a one-one correspondence $\nu: S(A, B) \longrightarrow \mathrm{Hom}_R(A^1/A^0, B^1/B^0)$ given by:

$$\nu(f)\ (x + A^0) = (x + f^-) \cap B^1,$$

for $f: \mathbf{T} \longrightarrow L$ in $S(A, B)$ and $x \in A^1$, and

$$\nu^{-1}(h)^- = \{x - y: x \in A^1, y \in B^1, h(x + A^0) = y + B^0\},$$

for $h: A^1/A^0 \longrightarrow B^1/B^0$ in R-Mod. Furthermore,

$$\ker \nu(f) = K(f)/A^0 \quad \text{and} \quad \mathrm{im}\ \nu(f) = I(f)/B^0.$$

If $A, B, C: \mathbf{2} \longrightarrow L$ is a mixed sequence, $f \in S(A, B)$ and $g \in S(B, C)$, then $\nu(g \circ f) = \nu(g)\nu(f)$. Also, f is isorepresentative if and only if $\nu(f)$ is an isomorphism, and $\nu(f^{-1}) = \nu(f)^{-1}$ in that case.

Proof: Assume the hypotheses. Using the known relations between A^1, A^0, B^1, B^0 and f^-, we can show that $(x + f^-) \cap B^1$ is a coset in B^1/B^0 for $x \in A^1$, and $\nu(f)$ so defined is R-linear. Straightforward computations prove that $\nu^{-1}(h)^-$ is in L, $A^0 \vee B^0 \subset \nu^{-1}(h)^- \subset A^1 \vee B^1$, $B^1 \vee \nu^{-1}(h)^- = A^1 \vee B^1$ and $B^1 \wedge \nu^{-1}(h)^- = B^0$. So, $\nu^{-1}(h): \mathbf{T} \longrightarrow L$ in $S(A, B)$ can be defined as above. We also omit the computations proving that $\nu^{-1}\nu(f) = f$, $\nu\nu^{-1}(h) = h$, $\ker \nu(f) = K(f)/A^0$ and $\mathrm{im}\ \nu(f) = I(f)/B^0$.

Let $k = \nu^{-1}(\nu(g)\nu(f))$ in $S(A, C)$. By definition $k^{-} \subset A^1 \vee C^1$. Suppose $x - z \in k^{-}$, with $x \in A^1$, $z \in C^1$ and $\nu(g)\nu(f)(x + A^0) = z + C^0$. Choose $y \in B^1$ with $\nu(f)(x + A^0) = y + B^0$, and observe that $x - y \in f^{-}$ and $y - z \in g^{-}$, so $x - z \in f^{-} \vee g^{-}$ and

$$k^{-} \subset (g \circ f)^{-} = (f^{-} \vee g^{-}) \wedge (A^1 \vee C^1).$$

So, $k = g \circ f$ by [5: 3.4], proving $\nu(g \circ f) = \nu(g)\nu(f)$. Using the formulas for $\ker \nu(f)$ and $\operatorname{im} \nu(f)$ and [5: **3.21**], f is isorepresentative if and only if $\nu(f)$ is an isomorphism. If $h{:}A^1/A^0 \longrightarrow B^1/B^0$ is an isomorphism, then $\nu^{-1}(h)^{-} = \nu^{-1}(h^{-1})^{-}$ by direct computation. Then, $\nu(f^{-1}) = \nu(f)^{-1}$ follows.

Prop. 8. Let β be an infinite nondenumerable cardinal, $\beta > \operatorname{card}(R)$, and let $L = \Gamma_b(R_\beta; R)$. Then there exists a full exact embedding equivalence functor $F{:}\, \mathbf{A}_L \longrightarrow R\text{-Mod}(\beta)$, given by $F(A) = A^1/A^0$ and $F([f_2, f_1]) = \nu(f_2)\nu(f_1)$.

Proof: Assume the hypotheses. If $A^0 \subset A^1$ in L, then $\operatorname{card}(A^1/A^0) < \beta$ by Prop. 6, and A^1/A^0 is in $R\text{-Mod}(\beta)$. There is no problem in verifying that F is well-defined and is a full exact embedding functor, by Prop. 7 and [5: 3.13, 3.15, 3.17, 3.19, 3.25]. To prove that F is an equivalence functor, it suffices to show that every M in $R\text{-Mod}(\beta)$ is isomorphic to $F(A)$ for some A in $\mathbf{A}_L$ [9: IV.4, Thm. 1, p. 91]. Let $\operatorname{card}(M) = \gamma < \beta$, and choose an R-linear epimorphism $f{:}R_\gamma \longrightarrow M$

as in the proof of Prop. 5. Now R_γ can be regarded as a bounded submodule of R_β, so $F(A)$ is isomorphic to M for $A^0 = \ker f \subset R_\gamma = A^1$ in L.

We can now prove:

Theorem 1. Let R and S be rings with unit. Then $\mathfrak{L}(R) \subset \mathfrak{L}(S)$ if and only if there exists an exact embedding functor $R\text{-Mod}(\beta) \longrightarrow S\text{-Mod}$ for every infinite cardinal β.

Corollary. $\mathfrak{L}(R) \subset \mathfrak{L}(S)$ if and only if there exists an exact embedding functor $C \longrightarrow S\text{-Mod}$ for every small exact subcategory C of $R\text{-Mod}$.

Proof: By a slight modification of the proof of Prop. 1, we can show that $\mathfrak{L}(R) \subset \mathfrak{L}(S)$ if there exists an exact embedding functor $R\text{-Mod}(\beta) \longrightarrow S\text{-Mod}$ for every infinite β.

Assume $\mathfrak{L}(R) \subset \mathfrak{L}(S)$. To prove the theorem, it suffices to show that there exists an exact embedding functor $R\text{-Mod}(\beta) \longrightarrow S\text{-Mod}$ whenever $\beta > \aleph_0 + \text{card}(R)$. (If $\delta < \gamma$, then $R\text{-Mod}(\delta)$ is an exact subcategory of $R\text{-Mod}(\gamma)$.) So, assume $\beta > \aleph_0 + \text{card}(R)$, and choose $\gamma > \aleph_0 + \text{card}(S)$ such that there exist lattice embeddings:

$$\Gamma_b(R_\beta;R) \xrightarrow{f} \Gamma(M;S) \xrightarrow{g} \Gamma_b(S_\gamma;S),$$

using $\mathfrak{L}(R) \subset \mathfrak{L}(S)$ to obtain f and Prop. 5 to obtain g. Let $L(R)$ denote $\Gamma_b(R_\beta;R)$ and $L(S)$ denote $\Gamma_b(S_\gamma;S)$, and construct an exact embedding $R\text{-Mod}(\beta) \longrightarrow S\text{-Mod}$ by composing:

$$\text{R-Mod}(\beta) \xrightarrow{F_1} \mathbf{A}_{L(R)} \xrightarrow{F_2} \mathbf{A}_{L(S)} \xrightarrow{F_3} \text{S-Mod}(\gamma) \xrightarrow{F_4} \text{S-Mod}.$$

Here, F_4 is an exact inclusion functor, and F_1 and F_3 are exact embeddings obtained from the equivalences of Prop. 8. The functor F_2 equals $\mathbf{A}_{gf}\colon \mathbf{A}_{L(R)} \longrightarrow \mathbf{A}_{L(S)}$, which is an exact embedding by the discussion following Prop. 3. This proves Thm. 1.

Half of the corollary is proved by adapting the proof of Prop. 1. Since every small exact subcategory of R-Mod is an exact subcategory of R-Mod(β) for sufficiently large β, the other half of the corollary follows from the theorem.

There is a foundational point worth mentioning. The construction of the reciprocal functor to the equivalence functor $F\colon \mathbf{A}_L \longrightarrow \text{R-Mod}(\beta)$ in Prop. 8 using [9: IV.4, Thm. 1, p. 91] seems to require the strong axiom of choice (there exists a choice function for the class of all nonempty sets). However, the corollary of Thm. 1 can be proved using a slightly modified version of Prop. 8 requiring only the ordinary axiom of choice. Furthermore, most of the consequences of Thm. 1 hereafter can also be proved using the corollary.

In the remainder of the text, we will sometimes treat integers as members of an arbitrary ring R with unit. In each case, the integer n is identified with the additive multiple $n \cdot 1$ of the ring unit ($2 = 1 + 1$ in R, etc.). Note that an integer n is a central element of R, so nR is a two-sided principal ideal of R. If p is a prime number and $j \geqq 0$, we will say that p is "j-invertible" in R if $p^j(pr - 1) = 0$ for some r in R. If p is 0-invertible in R, then p is invertible as a ring element of R. If p is j-invertible in R, then it is k-invertible for $k > j$. Also, p is k-invertible in R if $\text{char}(R) = p^k m$ for relatively prime p and m.

The next theorem gives some simple tests for proving that $\mathfrak{L}(R) \subset \mathfrak{L}(S)$ is false in various cases.

Theorem 2. Let $\mathfrak{L}(R) \subset \mathfrak{L}(S)$, and let a and b be integers such that b divides a. If $ax + b = 0$ for some x in S, then $ax + b = 0$ for some x in R. Therefore, char(R) divides char(S). Also, for any prime p and $j \geqq 0$, p is j-invertible in R if p is j-invertible in S.

Proof: Assume the hypotheses. Using Thm. 1, choose an exact embedding functor $F: R\text{-Mod}(\beta) \longrightarrow S\text{-Mod}$ for $\beta > \aleph_0 + \text{card}(R)$. For any S-module M, $\text{im}(b \cdot 1_M) \supset \text{im}(a \cdot 1_M)$ because b divides a. Conversely, $\text{im}(b \cdot 1_M) \subset \text{im}(a \cdot 1_M)$ because $ax + b = 0$ for some x in S. In particular, $\text{im}(b \cdot 1_{F(R)}) = \text{im}(a \cdot 1_{F(R)})$. Since F is an exact embedding, $\text{im}(b \cdot 1_R) = \text{im}(a \cdot 1_R)$ [3: pp. 65-66]. So, $b \in \text{im}(a \cdot 1_R)$, and therefore $ax + b = 0$ for some x in R.

Letting $a = 0$ and $b = \text{char}(S)$, we see that $\text{char}(S) = 0$ in R, and so char(R) divides char(S). (By convention, 0 divides 0.)

If p is j-invertible in S, then $ax + b = 0$ has a solution in S, hence in R, for $a = p^{j+1}$ and $b = -p^j$. Therefore, p is j-invertible in R. This proves Thm. 2.

More information on ring characteristics is given by:

Theorem 3. Let R and S have characteristics m and n, respectively. Then $\mathcal{L}(R) \subset \mathcal{L}(S)$ if and only if $\mathcal{L}(R) \subset \mathcal{L}(S/mS)$, and m divides n and $\mathrm{char}(S/mS) = m$ in this case.

Proof: Assume the hypotheses, and that $m \neq 0$ (the case $m = 0$ is trivial). Since $\mathcal{L}(S/mS) \subset \mathcal{L}(S)$ by Prop. 2, $\mathcal{L}(R) \subset \mathcal{L}(S/mS)$ implies $\mathcal{L}(R) \subset \mathcal{L}(S)$. Assume $\mathcal{L}(R) \subset \mathcal{L}(S)$, and suppose M is an R-module. By Thm. 1, let $F{:}R\text{-Mod}(\beta) \longrightarrow S\text{-Mod}$ be an exact embedding for some $\beta > \aleph_0 + \mathrm{card}(R) + \mathrm{card}(M)$. Then F induces an embedding homomorphism $\Gamma(M;R) \longrightarrow \Gamma(F(M);S)$, as usual. Since $\mathrm{char}(R) = m$ and F is additive, $m\cdot 1_{F(M)} = F(m\cdot 1_M) = F(0) = 0$. Therefore, $s_0 x = 0$ if $s_0 \in mS$ and $x \in F(M)$. But then we can make $F(M)$ into a S/mS-module M_0, retaining the additive structure of $F(M)$ and defining $(s + mS)x = sx$ for $s \in S$ and $x \in M_0 = F(M)$. Clearly $\Gamma(M_0;S/mS)$ is isomorphic to $\Gamma(F(M);S)$, and so $\Gamma(M;R)$ is in $\mathcal{L}(S/mS)$. This proves $\mathcal{L}(R) \subset \mathcal{L}(S/mS)$.

If $d = \mathrm{char}(S/mS)$, clearly d divides m. If $\mathcal{L}(R) \subset \mathcal{L}(S/mS)$, then m divides d by Thm. 2, and so $m = d$. By Thm. 2, m divides n if $\mathcal{L}(R) \subset \mathcal{L}(S)$.

Using Thm. 3, we can evaluate the ring predicate $\mathcal{L}(R) \subset \mathcal{L}(S)$ in general if we can evaluate it for rings with the same characteristic. After some preparation, we will prove that only rings with zero or prime power characteristic need be considered.

Prop. 9. Let $\text{char}(R) = \text{char}(S) = ab$, where a and b are relatively prime positive integers. Then $\mathcal{L}(R) \subset \mathcal{L}(S)$ if and only if $\mathcal{L}(R/aR) \subset \mathcal{L}(S)$ and $\mathcal{L}(R/bR) \subset \mathcal{L}(S)$.

Proof: Assume the hypotheses. Suppose $\mathcal{L}(R) \subset \mathcal{L}(S)$. Then $\mathcal{L}(R/aR) \subset \mathcal{L}(S)$ and $\mathcal{L}(R/bR) \subset \mathcal{L}(S)$ by Prop. 2.

Now assume that $\mathcal{L}(R/aR) \subset \mathcal{L}(S)$ and $\mathcal{L}(R/bR) \subset \mathcal{L}(S)$. Let M be an R-module. Make M/aM into an R/aR-module by defining:

$$(r + aR)(m + aM) = rm + aM \quad \text{for} \quad r \in R \quad \text{and} \quad m \in M,$$

and make M/bM into an R/bR-module similarly. Let $L = \Gamma(M;R)$, and let L_a and L_b denote the interval sublattices $[aM, M]$ and $[bM, M]$ of L, respectively. We can verify that L_a and L_b are isomorphic to $\Gamma(M/aM;R/aR)$ and $\Gamma(M/bM;R/bR)$, respectively. Therefore, there exist lattice embeddings $f:L_a \longrightarrow \Gamma(M_1;S)$ and $g:L_b \longrightarrow \Gamma(M_2;S)$ for some S-modules M_1 and M_2. Then $f \times g:L_a \times L_b \longrightarrow \Gamma(M_1;S) \times \Gamma(M_2;S)$ is a lattice embedding. Also, $i:\Gamma(M_1;S) \times \Gamma(M_2;S) \longrightarrow \Gamma(M_1 \times M_2;S)$ given by $i(N_1, N_2) = N_1 \times N_2$ is a lattice embedding.

Let $au + bv = 1$ for some integers u and v, since a and b are relatively prime. For any $m \in M$, $aum \in aM$ and $bvm \in bM$, so $m = (au + bv)m \in aM \vee bM$, proving $M = aM \vee bM$. Furthermore, if $m \in aM \wedge bM$, then $m = am_1 = bm_2$ for some m_1 and m_2 in M. Therefore, $am = abm_2 = 0 = bam_1 = bm$, since $\operatorname{char}(R) = ab$. But then $m = uam + vbm = 0$, proving $aM \wedge bM = 0$. Finally, suppose $M' \in L$. Then $M' = M' \wedge (aM \vee bM) = (M' \wedge aM) \vee (M' \wedge bM)$, since $m = aum + bvm \in (M' \wedge aM) \vee (M' \wedge bM)$ if $m \in M'$. Therefore, aM, bM and M' generate a distributive sublattice of L [1: Thm. 12, p. 37]. Now define functions as follows:

$$h: L \longrightarrow L_a \times L_b \text{ given by } h(M') = (M' \vee aM, M' \vee bM).$$

$$h^*: L_a \times L_b \longrightarrow L \text{ given by } h^*(M', M'') = M' \wedge M''.$$

Then $h^*h(M') = (M' \vee aM) \wedge (M' \vee bM) = M' \vee (aM \wedge bM) = M'$ for all $M' \in L$. Also, if $M' \supset aM$ and $M'' \supset bM$, then:

$$hh^*(M', M'') = ((M' \wedge M'') \vee aM, (M' \wedge M'') \vee bM) = (M', M''),$$

since $aM \vee (M'' \wedge M') = (aM \vee M'') \wedge M' = M'$ by modularity and $aM \vee M'' \supset aM \vee bM = M$, and similarly $(M' \wedge M'') \vee bM = M''$. Since h and h^* preserve order, they are reciprocal lattice isomorphisms between L and $L_a \times L_b$. We have proved that L is in $\mathcal{L}(S)$ by the embedding:

$$L \xrightarrow{h} L_a \times L_b \xrightarrow{f \times g} \Gamma(M_1;S) \times \Gamma(M_2;S) \xrightarrow{i} \Gamma(M_1 \times M_2;S).$$

So, $\mathfrak{L}(R) \subset \mathfrak{L}(S)$, completing the proof.

Prop. 10. Let p be a prime, $t > 0$ and $j = \min A$ for:

$$A = \{t\} \cup \{k\colon p \text{ is } k\text{-invertible in } R\}.$$

Then $\operatorname{char}(R/p^tR) = p^j$. If $\operatorname{char}(R) \neq 0$ and n divides $\operatorname{char}(R)$, then $\operatorname{char}(R/nR) = n$.

Proof: Assume the hypotheses. Since $p^t \in p^tR$, $\operatorname{char}(R/p^tR) = p^d$ for some d, $0 \leqq d \leqq t$. If $0 \leqq k < d$, then p^k isn't in p^tR. But then $p^k(pr - 1) = 0$ is false for all $r \in R$, since otherwise $p^tr^{t-k} = p^k$. So, $d \leqq \min A$. If $d = t$, then $\min A \leqq d$, so assume $d < t$. Then $p^tr = p^d$ for some r in R, so $p^d(pr_0 - 1) = 0$ for $r_0 = p^{t-d-1}r$. So, p is d-invertible in R, and $\min A \leqq d$. This proves that $d = \min A$ in all cases.

Now suppose $m = \operatorname{char}(R) \neq 0$ and n divides m. Let $d = \operatorname{char}(R/nR)$, so d divides n. To prove $\operatorname{char}(R/nR) = n$, it suffices to show that p^k divides n implies p^k divides d, for any prime p and $k > 0$. Assuming that p^k divides n and using n divides m, let $m = xp^k$. Now $\operatorname{char}(R/p^kR) = p^j$ for some j, $0 \leqq j \leqq k$. If $j < k$, then there exists r in R such that $p^{j+1}r = p^j$, by the above. But then $xp^j = xp^kr^{k-j} = mr^{k-j} = 0$ in R, contradicting $m = \operatorname{char}(R)$. Therefore,

$\mathrm{char}(R/p^kR) = p^k$. Since $nR \subset p^kR$ because p^k divides n, there is a ring homomorphism $R/nR \longrightarrow R/p^kR$ preserving 1, and so $\mathfrak{L}(R/p^kR) \subset \mathfrak{L}(R/nR)$ by Prop. 2. Therefore, p^k divides d by Thm. 2, proving that $\mathrm{char}(R/nR) = n$.

We now prove that the predicate $\mathfrak{L}(R) \subset \mathfrak{L}(S)$ can be evaluated for rings with the same nonzero characteristic if it can be evaluated for rings with the same prime power characteristic.

Theorem 4. Let $\mathrm{char}(R) = \mathrm{char}(S) = n \neq 0$, and $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ for distinct primes $p_1, p_2, \ldots, p_t$ and any positive integers $k_1, k_2, \ldots, k_t$. Then $\mathfrak{L}(R) \subset \mathfrak{L}(S)$ if and only if $\mathfrak{L}(R/p_i^{k_i}R) \subset \mathfrak{L}(S/p_i^{k_i}S)$ and $\mathrm{char}(R/p_i^{k_i}R) = \mathrm{char}(S/p_i^{k_i}S) = p_i^{k_i}$ for all $i \leqq t$.

Proof: Assume the hypotheses. Suppose $\mathfrak{L}(R) \subset \mathfrak{L}(S)$, and let $p = p_i$ and $k = k_i$ for some i, $i \leqq t$. Then $\mathrm{char}(R/p^kR) = p^k$ by Prop. 10, and $\mathfrak{L}(R/p^kR) \subset \mathfrak{L}(R) \subset \mathfrak{L}(S)$ by Prop. 2. Therefore, $\mathfrak{L}(R/p^kR) \subset \mathfrak{L}(S/p^kS)$ and $\mathrm{char}(S/p^kS) = p^k$ by Thm. 3.

Now assume that $\mathfrak{L}(R/p^kR) \subset \mathfrak{L}(S/p^kS)$ for $p^k = p_i^{k_i}$, all $i \leqq t$. To prove $\mathfrak{L}(R) \subset \mathfrak{L}(S)$, use induction on t. If $t = 1$, $n = p_1^{k_1}$ and the result is trivial. Assume $t > 1$, and let $a = p_1^{k_1}$ and $b = n/a = p_2^{k_2} \cdots p_t^{k_t}$. If $R' = R/bR$ and $S' = S/bS$, then $\mathfrak{L}(R/p^kR) \subset \mathfrak{L}(S/p^kS)$ implies $\mathfrak{L}(R'/p^kR') \subset \mathfrak{L}(S'/p^kS')$ for $p^k = p_i^{k_i}$, $i = 2, 3, \ldots, t$. Since $\mathrm{char}(R') = \mathrm{char}(S') = b$ by Prop. 10, and b has $t - 1$ prime factors, $\mathfrak{L}(R/bR) = \mathfrak{L}(R') \subset \mathfrak{L}(S') = \mathfrak{L}(S/bS) \subset \mathfrak{L}(S)$, by the induction hypothesis and Prop. 2. Since $\mathcal{L}(R/aR) \subset \mathcal{L}(S)$ by Prop. 2, $\mathcal{L}(R) \subset \mathcal{L}(S)$ by Prop. 9. This completes the proof.

We turn now to consideration of some particular rings. Two types of ring are especially important: the homomorphic images $\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z}$ of the ring $\mathbf{Z}$ of integers, and the unitary subrings of the field $\mathbf{Q}$ of rationals.

Let P denote the set of prime numbers, and let P_R denote the subset of P of primes invertible in R:

$$P_R = \{p \in P: p^{-1} \text{ exists in } R\}.$$

Given any subset P_0 of P, let $\mathbf{Q}(P_0)$ denote the unitary subring of $\mathbf{Q}$ generated by $\{p^{-1}: p \in P_0\}$. It is easily proved that the unitary subrings of $\mathbf{Q}$ are in one-one correspondence with the subsets of P via the reciprocal bijections:

$$R \longrightarrow P_R, \qquad P_0 \longrightarrow \mathbf{Q}(P_0).$$

(That is, $P_0 = P_{\mathbf{Q}(P_0)}$ if $P_0 \subset P$, and $R = \mathbf{Q}(P_R)$ if $\mathbf{Z} \subset R \subset \mathbf{Q}$.)

In the next theorem, we give the basic lattice representability relationships between rings of these types, and some other relationships between lattice representability by these special rings and lattice representability for arbitrary rings satisfying certain tests. A proposition preparing for the use of Prop. 3 is inserted first.

Prop. 11. Let M be a flat right R-module, and let kM denote $\mathrm{im}(k\cdot 1_M)$ for $k \geqq 0$. If $R = \mathbb{Z}_n$ for some $n \geqq 2$, then M is faithfully flat if $dM \neq M$ for every proper divisor d of n. If $R = \mathbb{Q}(P_0)$ for some $P_0 \subset P$, then M is faithfully flat if $pM \neq M$ for every prime p not in P_0.

Proof: Assume the hypotheses. To prove M is faithful, it suffices to show that $M \otimes_R R/u \neq 0$ for every proper left ideal u of R. (If M_0 is nonzero, there is an R-linear monomorphism $R/u \longrightarrow M_0$ for some proper or trivial u. Since M is flat, $M \otimes_R R/u \longrightarrow M \otimes_R M_0$ is a monomorphism. Since $M \otimes_R R \approx M \neq 0$, $M \otimes_R R/u \neq 0$ for all proper u implies $M \otimes_R M_0 \neq 0$ whenever $M_0 \neq 0$.) If $R = \mathbb{Z}_n$ or $R = \mathbb{Q}(P_0)$, then every proper left ideal of R equals kR for some $k > 1$. But:

$$M \otimes_R R/kR \approx M \otimes_R (R \otimes_{\mathbb{Z}} \mathbb{Z}_k) \approx (M \otimes_R R) \otimes_{\mathbb{Z}} \mathbb{Z}_k \approx M/kM,$$

using well-known properties of tensor products. So, it suffices to show that $kM \neq M$ if kR is a proper ideal of R. If $R = \mathbb{Z}_n$, every proper ideal of R equals dR for some proper divisor d of n. So, M is faithful if $dM \neq M$ for such d. If $R = \mathbb{Q}(P_0)$, then kR is a proper ideal if there exists a prime p not in P_0 such that p divides k. But then $kM \subset pM$, so M is faithful if $pM \neq M$ for every prime p not in P_0. This proves Prop. 11.

Theorem 5. Suppose n, $m \geqq 2$ and P_1 and P_2 are subsets of P. Then:

(1) $\mathcal{L}(Z_n) \subset \mathcal{L}(Z_m)$ iff n divides m.

(2) $\mathcal{L}(Z_n) \subset \mathcal{L}(Q(P_1))$ iff no prime in P_1 divides n.

(3) $\mathcal{L}(Q(P_1)) \subset \mathcal{L}(Z_n)$ is always false.

(4) $\mathcal{L}(Q(P_1)) \subset \mathcal{L}(Q(P_2))$ iff $P_1 \supset P_2$.

(5) If $\mathrm{char}(R) = n$, then $\mathcal{L}(R) \subset \mathcal{L}(Z_n)$.

(6) If $\mathrm{char}(R) = n$ and n is a prime or a product of distinct primes, then $\mathcal{L}(R) = \mathcal{L}(Z_n)$.

(7) If $\mathrm{char}(R) = 0$, then $\mathcal{L}(R) \subset \mathcal{L}(Q(P_R))$.

(8) If R is torsion-free, then $\mathcal{L}(R) = \mathcal{L}(Q(P_R))$.

(9) If $\mathrm{char}(R) = 0$, then $\mathcal{L}(R) = \mathcal{L}(Q(P_R))$ iff every prime p which is j-invertible in R for some $j \geqq 1$ is invertible in R.

(10) If some unitary subring of R is a field, then $\mathcal{L}(R) = \mathcal{L}(Q)$ if $\mathrm{char}(R) = 0$, and $\mathcal{L}(R) = \mathcal{L}(Z_p)$ if $\mathrm{char}(R) = p$, p prime.

Proof: Assume the hypotheses. If char(R) = n, then R has a unitary subring isomorphic to $\mathbb{Z}_n$. If char(R) = 0, then R has a unitary subring isomorphic to $\mathbb{Q}(P_R)$, since integers are central elements of R. Using Prop. 2 and Thm. 2, we can then verify parts (1), (3), (4), (5) and (7). If $\mathfrak{L}(\mathbb{Z}_n) \subset \mathfrak{L}(\mathbb{Q}(P_1))$, then each p in P_1 is invertible in $\mathbb{Z}_n$ by Thm. 2, and so p doesn't divide n. This proves half of (2); the converse follows from Prop. 2 and the observation that $\mathbb{Q}(P_1)/n\mathbb{Q}(P_1)$ is isomorphic to $\mathbb{Z}_n$ if no prime in P_1 divides n.

Suppose char(R) = n, where n is prime or a product of distinct primes, and let M denote R considered as a bimodule (left R-module, right $\mathbb{Z}_n$-module). Now $\mathbb{Z}_n$ is a semisimple ring [12: p. 71], hence it is a regular ring [12: Thm. 4.11, p. 78]. Therefore, M is flat as a right $\mathbb{Z}_n$-module [12: Thm. 4.24, p. 86]. Given a proper divisor d of n, d is not invertible in R and so $dM \neq M$. So, M is faithfully flat by Prop. 11. Therefore, $\mathfrak{L}(\mathbb{Z}_n) \subset \mathfrak{L}(R)$ by Prop. 3, and then part (6) follows from part (5).

Suppose R is torsion-free, and let M denote R considered as a bimodule (left R-module, right $\mathbb{Q}(P_R)$-module). Now $\mathbb{Q}(P_R)$ is a principal ideal domain, and so is a Prüfer ring [12: p. 73]. Therefore, M is flat as a right $\mathbb{Q}(P_R)$-module [12: Thm. 4.23, p. 85]. Given p prime not in P_R, p is not invertible in R and so $pM \neq M$. Therefore, M is faithfully flat by Prop. 11, and $\mathcal{L}(\mathbf{Q}(P_R)) \subset \mathcal{L}(R)$ by Prop. 3. Then part (8) follows from part (7).

Suppose $\mathcal{L}(R) = \mathcal{L}(\mathbf{Q}(P_R))$ and p is a j-invertible prime in R for some $j \geqq 1$. Then $p^j(pr - 1) = 0$ for some r in $\mathbf{Q}(P_R)$ by Thm. 2, and so p is invertible in $\mathbf{Q}(P_R)$ since $pr - 1$ must equal 0. Therefore, p is invertible in R. Now suppose $\text{char}(R) = 0$ and every j-invertible prime of R is invertible. Let t denote the two-sided ideal of all torsion elements of R ($r \in t$ if $nr = 0$ for some positive integer n), and let $S = R/t$. Then S is a nontrivial torsion-free ring, and clearly $P_R \subset P_S$. If $p \in P_S$, then $px = 1 + z$ for some x in R and z in t. So, $k(px - 1) = 0$ for some $k > 0$. Let $k = p^j m$, where p and m are relatively prime. So, $pu + mv = 1$ for certain integers u and v. Let $r = mvx + u$ in R. Then $p^j(pr - 1) = p^j(pmvx + pu - pu - mv) = vk(px - 1) = 0$. So, p is j-invertible in R, and therefore $p \in P_R$ by hypothesis. That is, $P_R = P_S$. But then

$$\mathcal{L}(\mathbf{Q}(P_R)) = \mathcal{L}(\mathbf{Q}(P_S)) = \mathcal{L}(S) \subset \mathcal{L}(R) \subset \mathcal{L}(\mathbf{Q}(P_R)),$$

by parts (7) and (8) and Prop. 2. This proves part (9).

Part (10) follows immediately from parts (6) and (8). (If R contains a unitary subring which is a field of characteristic zero, then R is torsion-free and $\mathbf{Q}(P_R) = \mathbf{Q}$.) This proves Thm. 5.

For arbitrary $n \geqq 2$, the author has been unable to establish a necessary and sufficient condition on R so that $\mathcal{L}(R) = \mathcal{L}(\mathbf{Z}_n)$. However, the final result sheds some light on this problem.

Prop. 12. Let $\mathrm{char}(R) = p^u$ for prime p and $u > 1$. If there exist r_1 and r_2 in R and integers i, j and k such that $1 \leqq i, j, k \leqq u - 1$, $i + j + k < 2u$, $r_1 r_2 = p^i$, $p^j r_1 = 0$ and $p^k r_2 = 0$, then $\mathcal{L}(R) \neq \mathcal{L}(\mathbf{Z}_{p^u})$.

Proof: Assume the hypotheses, and suppose $\mathcal{L}(R) = \mathcal{L}(\mathbf{Z}_{p^u})$. By Thm. 1, there exists an exact embedding $F: \mathbf{Z}_{p^u}\text{-Mod}(\aleph_0) \longrightarrow R\text{-Mod}$. Let M denote $\mathbf{Z}_{p^u}$ as an object of $\mathbf{Z}_{p^u}\text{-Mod}(\aleph_0)$. Since $(p^{u-k} \cdot 1_M, p^k \cdot 1_M)$ is exact, so is $(p^{u-k} \cdot 1_{F(M)}, p^k \cdot 1_{F(M)})$. Let v be in $F(M)$. Then $p^k r_2 v = 0$, since $p^k r_2 = 0$ in R. So, $p^{u-k} v_0 = r_2 v$ for some v_0 in $F(M)$. But then $p^{u-1} v = p^{u-1-i} p^i v = p^{u-1-i} r_1 r_2 v = p^{u-1-i} r_1 p^{u-k} v_0 = p^{2u-i-j-k-1} p^j r_1 v_0 = 0$, using the hypotheses. Therefore, $F(p^{u-1} \cdot 1_M) = p^{u-1} \cdot 1_{F(M)} = 0$. But $p^{u-1} \cdot 1_M \neq 0$, contradicting the embedding property for F. This proves Prop. 12.

Given $P_0 \subset P$ and $P_0 \neq P$, one can easily construct a ring R with characteristic zero such that $P_R = P_0$ but $\mathcal{L}(R) \neq \mathcal{L}(\mathbf{Q}(P_0))$. For example, choose a prime p not in P_0 and $j \geqq 1$, and let R

denote the quotient of the polynomial ring $\mathbf{Q}(P_0)[y]$ divided by the principal ideal generated by $p^j(py - 1)$. Then $\mathrm{char}(R) = 0$, $P_R = P_0$ and p is j-invertible but not invertible in R. So, $\mathfrak{L}(R) \neq \mathfrak{L}(\mathbf{Q}(P_0))$ by Thm. 5(9).

Another family of counterexamples is related to Prop. 12. Suppose $n \geqq 2$ and n is not square-free, that is, $n = p^2 m$ for some prime p and integer m. Let R be the quotient ring of the polynomial ring $\mathbf{Z}_n[y]$ divided by the ideal generated by the polynomials py and $y^2 - pm$. We omit the proof that R is a commutative ring with characteristic n and pn elements; each element of R is representable by a polynomial $uy + v$ with $0 \leqq u < p$ and $0 \leqq v < n$. Assume $\mathfrak{L}(R) = \mathfrak{L}(\mathbf{Z}_n)$, and construct an exact embedding $F: \mathbf{Z}_n\text{-Mod}(\aleph_0) \longrightarrow R\text{-Mod}$. Let M equal $\mathbf{Z}_n$ as an object of $\mathbf{Z}_n\text{-Mod}(\aleph_0)$, and note that $(pm\cdot 1_{F(M)}, p\cdot 1_{F(M)})$ is exact because $(pm\cdot 1_M, p\cdot 1_M)$ is exact. Suppose $v \in F(M)$: since $pyv = 0$ there exists v_0 in $F(M)$ such that $pmv_0 = yv$. But then $pmv = y^2 v = ypmv_0 = 0$, since $pm = y^2$ and $py = 0$ in R. Then $F(pm\cdot 1_M) = pm\cdot 1_{F(M)} = 0$ and $pm\cdot 1_M \neq 0$ leads to contradiction. So, R is a ring with characteristic n but $\mathfrak{L}(R) \neq \mathfrak{L}(\mathbf{Z}_n)$. We remark that this R is also a counterexample for the converse of Thm. 2. That is, the equation $ax + b = 0$ for integers a and b has a solution in R if and only if it has a solution in $\mathbf{Z}_n$, but $\mathfrak{L}(R) \neq \mathfrak{L}(\mathbf{Z}_n)$.

References

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

2. H. Cartan and S. Eilenberg, "Homological Algebra." Princeton University Press, Princeton, N. J., 1956.

3. P. J. Freyd, "Abelian Categories: An Introduction to the Theory of Functors." Harper & Row, New York, 1964.

4. C. Herrmann and W. Poguntke, Axiomatic classes of lattices of normal subgroups. Technische Hochschule Darmstadt Preprint No. 12, Darmstadt, West Germany, 1972.

5. G. Hutchinson, Modular lattices and abelian categories. J. of Algebra 19 (1971), 156-184.

6. G. Hutchinson, On the representation of lattices by modules. Manuscript, 1972.

7. G. Hutchinson, The representation of lattices by modules. Bull. Amer. Math. Soc. 79 (1973), 172-176.

8. B. Jónsson, On the representation of lattices. Math. Scand. 1 (1953), 193-206.

9. S. MacLane, "Categories for the Working Mathematician." Springer-Verlag, New York, Heidelberg and Berlin, 1971.

10. G. McNulty and M. Makkai, manuscript, 1972.

11. B. Mitchell, "Theory of Categories." Academic Press, New York and London, 1965.

12. J. Rotman, "Notes on Homological Algebra". Van Nostrand Reinhold, New York, 1970.