Studia Scientiarum Mathematicarum Hungarica 16 (1981), 45—60

ON PROPERTIES OF RINGS THAT CAN BE CHARACTERIZED BY INFINITE LATTICE IDENTITIES

GÁBOR CZÉDLI

Dedicated to the memory of László Rédei (1900—1980)

1. Introduction

Suppose R is a ring with 1 (throughout the paper rings always have 1), and $\mathscr{C}(R)$ denotes the class of lattices that are isomorphic to the lattice of submodules of some (unitary left) R-module. $\mathscr{C}(R)$ consists of algebraic lattices. The submodule lattice and the lattice of congruences of an arbitrary R-module are isomorphic (cf. BIRKHOFF [1, Theorem 1, p. 159]), therefore $\mathscr{C}(R)$ can also be defined as the class of lattices that are isomorphic to the congruence lattices of R-modules. A lattice variety $\mathscr{U}$ is said to be a congruence variety (cf. JÓNSSON [7]) if it is generated by the congruence lattices of members of some variety $\mathscr{V}$ of universal algebras. Let **Con** (R) denote the lattice variety generated by $\mathscr{C}(R)$. Since $\mathscr{M}(R)$, the class of unitary left R-modules, is a variety, **Con** (R) is a congruence variety.

In the present paper in *lattice terms and identities* infinitary join and infinitary meet operations are also allowed. I.e., a lattice term or identity can be *finite*, if it is a lattice term or identity in the usual sense, or *infinite*, otherwise. We can mention the join infinite distributive identity (cf. GRÄTZER [3, Lemma II. 4. 10]) as a classical example for infinite lattice identities.

Our aim is to investigate the connection between properties of rings R and lattice identities holding in $\mathscr{C}(R)$. Investigations of this kind for finite lattice identities were started in HERRMANN and HUHN's paper [5]. The case of finite lattice identities was settled in [6]. The results of the present paper are taken from the author's thesis [2].

2. Lattice terms and identities

In this section an appropriate definition of lattice terms and identities is given.

Let K be an index set with power $\varkappa \geqq 2$ and let X be a nonempty set of variables. We define the K-terms over X by the following recursion. Set $T_0(K, X)=X$. Suppose $T_\beta(K, X)$ has already been defined for all ordinals β being less than α. Then let $T_\alpha(K, X)$ be the set of all $\bigvee(p_\iota\colon \iota\in I)$ and $\bigwedge(p_\iota\colon \iota\in I)$ where $I\subseteq K$, $2\leqq |I|$, and for all $\iota\in I$ there is an ordinal $\beta_\iota<\alpha$ such that $p_\iota\in T_{\beta_\iota}(K, X)$. (Note that $\bigvee(p_\iota\colon \iota\in I)$ can be considered as the abbreviation of the more precise pair $(\vee, \dot\bigcup\{\{p_\iota\}|\iota\in I\})$ where $\dot\bigcup$ stands for the disjoint union. Thus the operation symbols $\vee$ and $\wedge$ are commutative by definition.) Finally, let $T(K, X)=\bigcup\{T_\alpha(K, X)|\ |\alpha|<\max(\varkappa^+, \omega)\}$

1980 *Mathematics Subject Classification.* Primary 06B99; Secondary 08B05.

Key words and phrases. Mal'cev conditions for infinite lattice identities, congruence varieties of module varieties, divisibility conditions in rings, submodule lattices.

where $\varkappa^+$ denotes the smallest cardinal greater than $\varkappa=|K|$ and ω is the smallest infinite cardinal. Now $T(K, X)$ is the set of K-terms over X. Note that for $I\subseteq K$, $p_\iota\in T(K, X)$ $\bigvee(p_\iota: \iota\in I)$ and $\bigwedge(p_\iota: \iota\in I)$ also belong to $T(K, X)$, as it follows from an easy calculation with cardinals. Moreover, given a complete lattice L, to any lattice term p over X there corresponds a *polynomial* $p\colon L^X\to L$, also denoted by p, which is defined via the following natural recursion: for $g\in L^X$ and $p=\bigwedge(p_\iota: \iota\in I)$ set $p(g)=\bigwedge(p_\iota(g): \iota\in I)$, the case of $\bigvee$ is similar, and $p(g)=g(p)$ for $p\in X$.

Now, lattice identities (over X) are defined to be strings $p\leqq q$ where p and q are lattice terms (over X). A lattice identity $p\leqq q$ over X is said to hold in a complete lattice L, in notation $L\models p\leqq q$, if $p(g)\leqq q(g)$ for any $g\in L^X$.

Finally we mention that, disregarding the commutativity of operations, lattice terms in the usual sense over X and K-terms over X, where K is two-element, coincide.

3. Mal'cev type conditions for lattice identities

The procedure to be presented here is a transfinite generalization of Wille's one [9] (cf. also Pixley [8]). However, we have chosen a pictorial approach.

Given a lattice term p, we define $\mathrm{Rd}(p)$, the set of *reduced terms of p*, by the following recursion: $\mathrm{Rd}(p)=\{p\}$ for p variable;

$\mathrm{Rd}\big(\bigwedge(p_\iota: \iota\in I)\big) = \{\bigwedge(p'_\iota: \iota\in I)\,|\,p'_\iota\in\mathrm{Rd}(p_\iota)$ for all $\iota\in I\}$; and

$\mathrm{Rd}\big(\bigvee(p_\iota: \iota\in I)\big) = \{\bigvee(p'_\iota: \iota\in J)\,|\,J\subseteq I$, J is finite and at least two-element, and $p'_\iota\in\mathrm{Rd}(p_\iota)$ for all $\iota\in J\}\cup\bigcup_{\iota\in I}\mathrm{Rd}(p_\iota)$.

A term p is said to be *reduced* if $p\in\mathrm{Rd}(p)$.

A binary relation $\leqq_r$ can be introduced on $\mathrm{Rd}(p)$ as follows: $p_1\leqq_r p_2$ iff $p_1\in\mathrm{Rd}(p_2)$ $(p_1, p_2\in\mathrm{Rd}(p))$.

Proposition 3.1. *Let p be a lattice term. The relation $\leqq_r$ is a quasi-ordering (i.e., a reflexive and transitive relation) over the set* $\mathrm{Rd}(p)$. *Moreover, this relation is directed, i.e., for any p_1, $p_2\in\mathrm{Rd}(p)$ there exists $p_3\in\mathrm{Rd}(p)$ such that $p_1\leqq_r p_3$ and $p_2\leqq_r p_3$.*

Proof. The proof is an easy induction, therefore only one step will be detailed. Suppose $p=\bigvee(p_\iota: \iota\in I)$ and $\mathrm{Rd}(p_\iota)$ is directed for $\iota\in I$. Let $\bar p$, $p'\in\mathrm{Rd}(p)$. Then $\bar p=\bigvee(\bar p_\iota: \iota\in J)$ and $p'=\bigvee(p'_\iota: \iota\in K)$ where $J, K\subseteq I$, $1\leqq|J|$, $|K|<\omega$, $\bar p_\iota\in\mathrm{Rd}(p_\iota)$ for $\iota\in J$, and $p'_\iota\in\mathrm{Rd}(p_\iota)$ for $\iota\in K$. (In case $|J|=1$ or $|K|=1$ $\bar p=\bar p_\iota$ or $p'=p'_\iota$ is the precise form.) By the induction hypothesis, for any $\iota\in J\cap K$, there exists $p^*_\iota\in\mathrm{Rd}(p_\iota)$ such that $\bar p_\iota$, $p'_\iota\in\mathrm{Rd}(p^*_\iota)$. Define $p^*=\bigvee(q_\iota: \iota\in J\cup K)$ where $q_\iota=p^*_\iota$ for $\iota\in J\cap K$, $q_\iota=\bar p_\iota$ for $\iota\in J\setminus K$, and $q_\iota=p'_\iota$ for $\iota\in K\setminus J$. Then $p^*\in\mathrm{Rd}(p)$, $\bar p\leqq_r p^*$ and $p'\leqq_r p^*$, i.e. p is directed. The omitted part of the proof is even more trivial. Q. e. d.

Now with any *reduced* term p over X a graph $G(p)$ will be associated. The edges of $G(p)$ will be coloured by the elements of X, i.e., by the variables of p. Two vertices, the left and right *endpoints*, will have special role. In the figures these endpoints will always be placed on the left-hand side and on the right-hand side, respectively.

If p is a variable then let $G(p)$ be the following graph which consists of a single edge coloured by p. 

We obtain $G(\wedge(p_\iota\colon \iota\in I))$ from the graphs $G(p_\iota)$ by the following way: take the disjoint union of the graphs $G(p_\iota)$, $\iota\in I$, and identify the left (right, resp.) endpoints of $G(p_\iota)$, $\iota\in I$. The obtained graph is $G(p)$, in which the identified endpoints of $G(p_\iota)$ have turned into the new ones.

Now suppose I is a finite at least two-element set and $G(p_\iota)$, $\iota\in I$, has already been defined. Choose an arbitrary ordering of I, say $I=\{\iota_1, \iota_2, \ldots, \iota_n\}$, take the disjoint union of the graphs $G(p_{\iota_j})$ $(j=1, \ldots, n)$, and for $j=1, \ldots, n-1$ identify the right endpoint of $G(p_{\iota_j})$ and the left endpoint of $G(p_{\iota_{j+1}})$. The graph we have obtained is $G(\vee(p_\iota\colon \iota\in I))$, its left (right, resp.) endpoint is the left (right, resp.) endpoint of $G(p_{\iota_1})$ (of $G(p_{\iota_n})$, resp.).

Since, as it is easy to check, reduced terms do not contain infinitary joins (and conversely), $G(p)$ has been defined. Although this definition of $G(p)$ is not quite unique, it depends on the ordering of I, the lack of uniqueness is not important. In what follows $G(p)$ will mean an *arbitrarily fixed* graph that corresponds to the above definition, *the* graph of p. (The definition of $G(p)$ could be completely unique, but this is not worth the complication.)

For example, for $p=((x_1\wedge x_2)\vee(x_3\wedge x_4))\wedge((x_1\wedge x_3)\vee(x_2\wedge x_4))$, $G(p)$ is the graph given in Figure 1. (The vertices of $G(p)$ are denoted by ordinals.)

Given two reduced terms p, q over X, $G(p\leqq q)$, the graph associated with the identity $p\leqq q$, will be defined as follows. (This definition is not unique again, but any graph obtained by it can be considered *the* graph $G(p\leqq q)$). Suppose the ordinal $\gamma=\{\alpha|\alpha<\gamma\}$ is the vertex set of $G(p)$ so that 0 is the left endpoint and 1 is the right one. For $x\in X$ let Θ_x be the smallest equivalence relation over γ under which the two endpoints of any x-coloured edge of $G(p)$ collapse. Now we obtain $G(p\leqq q)$ from $G(q)$ by preserving the edges and vertices of $G(q)$ but, for all $x\in X$, replacing the colour x by Θ_x on all x-coloured edges. For example, if $q=(x_1\wedge x_4)\vee(x_2\wedge x_3)$ and p is the term defined in the previous example then $G(p\leqq q)$ is the graph given in Figure 2.

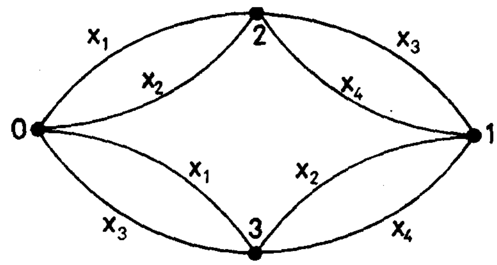


Fig. 1

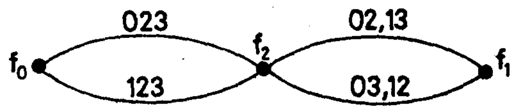


Fig. 2

In Figure 2 the equivalences are given by the corresponding partitions, and a partition over $\gamma=\{0, 1, 2, 3\}$ is given by listing its non-trivial blocks. I.e., $\{\{0, 2, 3\}, \{1\}\}=023$, $\{\{0, 2\}, \{1, 3\}\}=02, 13$, etc.

In connection with $G(p\leqq q)$ a Mal'cev type condition $M(p\leqq q)$ will be defined as follows. Let $F=\{f_\iota\colon \iota<\delta\}$ be the vertex set of $G(p\leqq q)$ such that f_0 is the left endpoint and f_1 is the right one. For any equivalence relation π over γ and $\alpha\in\gamma$ we set $\alpha\pi=\min\{\beta|(\alpha,\beta)\in\pi\}$. The elements f_ι of F will be considered as γ-ary terms of an unspecified type. (For the definition of γ-ary terms cf. GRÄTZER [4]. Any γ-ary term contains only finitely many relevant variables.) With any Θ_x-coloured edge connecting the vertices f_ι and f_x we associate the identity

$$f_\iota(y_{\alpha\Theta_x}\colon \alpha<\gamma)=f_x(y_{\alpha\Theta_x}\colon \alpha<\gamma).$$

Now let $M(p\leqq q)$ be the following condition for varieties of algebras:

"For any $f_\iota\in F$ there exists a γ-ary term $f_\iota(y_\alpha\colon \alpha<\gamma)$ such that the endpoint identities $f_\iota(y_\alpha\colon \alpha<\gamma)=y_\iota$, $\iota=0,1$, and all the identities associated with edges of $G(p\leqq q)$ are satisfied".

For example, for $G(p\leqq q)$ from Figure 2, $M(p\leqq q)$ is the following condition: "There are quaternary terms f_0, f_1, f_2 such that the identities

$$f_0(y_0,y_1,y_2,y_3)=y_0,\quad f_1(y_0,y_1,y_2,y_3)=y_1,$$

$$f_0(y_0,y_1,y_0,y_0)=f_2(y_0,y_1,y_0,y_0),$$

$$f_0(y_0,y_1,y_1,y_1)=f_2(y_0,y_1,y_1,y_1),$$

$$f_2(y_0,y_1,y_0,y_1)=f_1(y_0,y_1,y_0,y_1),$$

$$f_2(y_0,y_1,y_1,y_0)=f_1(y_0,y_1,y_1,y_0) \text{ are satisfied".}$$

One can consider the graph $G(p\leqq q)$ as a tool for describing $M(p\leqq q)$ in a shorter and more handlable way. A variety $\mathcal{V}$ is said to be congruence permutable if any of its algebras has permutable congruences. The congruence lattice of an algebra A will be denoted by Con (A). Now we can formulate the following

THEOREM 3.2. *For any lattice identity $p\leqq q$ and an arbitrary congruence permutable variety $\mathcal{V}$ the following two conditions are equivalent:*

(i) *The identity $p\leqq q$ holds in* Con (A) *for all $A\in\mathcal{V}$;*

(ii) *For any $\bar p\in \mathrm{Rd}(p)$ there exists $\bar q\in\mathrm{Rd}(q)$ such that the condition $M(\bar p\leqq\bar q)$ holds in $\mathcal{V}$.*

Moreover, the Mal'cev type condition $M(\bar p\leqq\bar q)$ is strengthening in $\bar p$ and weakening in $\bar q$. I.e., whenever $p'\leqq_r\bar p$, $\bar q\leqq_r q'\in\mathrm{Rd}(q)$ and $\mathcal{U}$ is a variety satisfying $M(\bar p\leqq\bar q)$, then $M(p'\leqq\bar q)$ and $M(\bar p\leqq q')$ also hold in $\mathcal{U}$.

REMARK. For a finite lattice identity $p\leqq q$ the theorem is a special case of WILLE's one ([9], cf. also PIXLEY [8]). A very similar, formally the same theorem that holds for any (not necessarily congruence permutable) variety could be also stated by changing the definitions of $\mathrm{Rd}(p)$ and $G(\bar p)$, but now we intend to deal with congruence permutable varieties only.

The proof is a transfinite generalization of Wille's one, the only essential difference is the use of transfinite induction instead of simple induction. Therefore our approach will be sketchy. The proof requires several preliminary statements.

CLAIM 3.3. *If p is a lattice term and $\bar p\in\mathrm{Rd}(p)$, then the identity $\bar p\leqq p$ holds in any complete lattice.*

The proof, an easy induction, will be omitted.

CLAIM 3.4. *Suppose p is a lattice term over X, A is a universal algebra with permutable congruences,* $\Phi_x \in \mathrm{Con}(A)$ *for* $x \in X$, *and* $a_0, a_1 \in A$. *Then* $(a_0, a_1) \in p(\Phi_x\colon x \in X)$ *if and only if* $(a_0, a_1) \in \bar{p}(\Phi_x\colon x \in X)$ *for some* $\bar{p} \in \mathrm{Rd}(p)$.

Since $\bigvee(\Phi_\iota\colon \iota \in I) = \bigcup_{\substack{J \subseteq I \\ J \text{ finite}}} \bigvee(\Phi_\iota\colon \iota \in J)$ holds for $\Phi_\iota \in \mathrm{Con}(A)$, Claim 3.3 makes the proof a trivial induction.

CLAIM 3.5. *Suppose p is a reduced lattice term over X, A is an algebra with permutable congruences,* $\Phi_x \in \mathrm{Con}(A)$ *for* $x \in X$, *and* $a_0, a_1 \in A$. *Then* $(a_0, a_1) \in p(\Phi_x\colon x \in X)$ *iff there exist elements* $a_\alpha \in A$ *for* $1 < \alpha < \gamma$ *such that for any edge of* $G(p)$, *say* $\alpha \bullet\!\!\xrightarrow{\;x\;}\!\!\bullet\, \beta$, *we have the corresponding* $(a_\alpha, a_\beta) \in \Phi_x$. *(Here the ordinal* γ *means the vertex set of* $G(p)$.)

The proof, which is a trivial induction, is omitted.

The following lemma is not only the main step in the proof, it gives stronger result for certain lattice identities.

LEMMA 3.6. *Suppose* $p \leqq q$ *is a lattice identity over X and p is reduced. Let the ordinal* γ *be the vertex set of* $G(p)$ (0 *and* 1 *are the endpoints), and consider the equivalence relations* Θ_x *over* γ *that we have introduced defining graphs associated with lattice identities. Then for an arbitrary congruence permutable variety* $\mathcal{V}$ *the following three conditions are equivalent:*

(i) *The identity* $p \leqq q$ *holds in the congruence lattice of any member of* $\mathcal{V}$;

(ii) *There exists* $\bar{q} \in \mathrm{Rd}(q)$ *such that the condition* $M(p \leqq \bar{q})$ *holds in* $\mathcal{V}$;

(iii) *Let* $F_{\mathcal{V}}(\gamma)$ *be the free* $\mathcal{V}$*-algebra generated by the set* $\gamma = \{\alpha | \alpha < \gamma\}$, *and let* Θ'_x *be the congruence relation of* $F_{\mathcal{V}}(\gamma)$ *generated by the relation* Θ_x. *Then* $p(\Theta'_x\colon x \in X) \leqq q(\Theta'_x\colon x \in X)$.

Moreover, if q is also reduced then (ii) *can be replaced by*

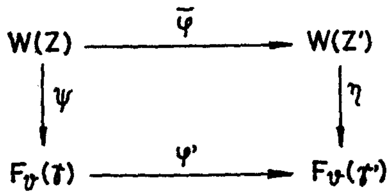
(ii′) $M(p \leqq q)$ *holds in* $\mathcal{V}$.

PROOF. Only (iii)→(ii) and (ii)→(i) have to be shown.

(iii) *implies* (ii). Suppose $\mathcal{V}$ is of type τ and (iii) holds. Lemma 3.4 yields $(0, 1) \in p(\Theta'_x\colon x \in X)$, thus $(0, 1) \in q(\Theta'_x\colon x \in X)$. Therefore, by Claim 3.4, there exists $\bar{q} \in \mathrm{Rd}(q)$ (and, moreover, Claim 3.3 yields that we can choose $\bar{q} = q$ if q is reduced) such that $(0, 1) \in \bar{q}(\Theta'_x\colon x \in X)$. Let the ordinal $\delta = \{\alpha | \alpha \leqq \delta\}$ be the vertex set of $G(\bar{q})$, 0 and 1 being the endpoints. By Claim 3.5 there are elements $a_\alpha \in F_{\mathcal{V}}(\gamma)$, $\alpha < \delta$, such that $a_0 = 0$, $a_1 = 1$, and $(a_\mu, a_\nu) \in \Theta'_x$ holds for any x-coloured edge connecting the vertices μ and ν in $G(\bar{q})$. Since γ generates $F_{\mathcal{V}}(\gamma)$, $a_\iota = f_\iota(\alpha\colon \alpha < \gamma)$ holds for some γ-ary τ-terms f_ι, $\iota < \delta$. Fix an arbitrary edge $\mu \bullet\!\!\xrightarrow{\;x\;}\!\!\bullet\, \nu$ of $G(\bar{q})$ and consider the map $\varphi\colon \gamma \to \gamma$, $\alpha\varphi = \alpha\Theta_x = \min\{\beta | (\alpha, \beta) \in \Theta_x\}$. Evidently, $\mathrm{Ker}\,\varphi = \Theta_x$. Set $Z = \{z_\alpha\colon \alpha < \gamma\}$, $Z' = \{z_{\alpha\varphi}\colon \alpha < \gamma\}$, and $\gamma' = \{\alpha\varphi | \alpha < \gamma\} = \gamma\varphi$. Consider $W(Z)$ and $W(Z')$, the absolutely free τ-algebras generated by Z and Z', respectively, and the free $\mathcal{V}$-algebras $F_{\mathcal{V}}(\gamma)$ and $F_{\mathcal{V}}(\gamma')$. Let us define the following four epimorphisms:

$$\varphi'\colon F_{\mathcal{V}}(\gamma) \to F_{\mathcal{V}}(\gamma'),\quad f(\alpha\colon \alpha < \gamma)\varphi' = f(\alpha\varphi\colon \alpha < \gamma);$$
$$\bar{\varphi}\colon W(Z) \to W(Z'),\quad f(z_\alpha\colon \alpha < \gamma)\bar{\varphi} = f(z_{\alpha\varphi}\colon \alpha < \gamma);$$
$$\psi\colon W(Z) \to F_{\mathcal{V}}(\gamma),\quad f(z_\alpha\colon \alpha < \gamma)\psi = f(\alpha\colon \alpha < \gamma); \quad \text{and}$$
$$\eta\colon W(Z') \to F_{\mathcal{V}}(\gamma'),\quad f(z_{\alpha\varphi}\colon \alpha < \gamma)\eta = f(\alpha\varphi\colon \alpha < \gamma).$$

Then the following diagram commutes.



Since $\Theta_x \subseteq \operatorname{Ker} \varphi'$ implies $\Theta'_x \subseteq \operatorname{Ker} \varphi'$, we obtain $a_\mu \varphi' = a_\nu \varphi'$. By the commutativity of the diagram we can compute: $f_\mu(\alpha\varphi\colon \alpha<\gamma) = f_\mu(z_{\alpha\varphi}\colon \alpha<\gamma)\eta = f_\mu(z_\alpha\colon \alpha<\gamma)\bar{\varphi}\eta = f_\mu(z_\alpha\colon \alpha<\gamma)\psi\varphi' = f_\mu(\alpha\colon \alpha<\gamma)\varphi' = a_\mu\varphi' = a_\nu\varphi' = f_\nu(\alpha\colon \alpha<\gamma)\varphi' = f_\nu(z_\alpha\colon \alpha<\gamma)\psi\varphi' = f_\nu(z_\alpha\colon \alpha<\gamma)\bar{\varphi}\eta = f_\nu(z_{\alpha\varphi}\colon \alpha<\gamma)\eta = f_\nu(\alpha\varphi\colon \alpha<\gamma)$, i.e., $f_\mu(\alpha\varphi\colon \alpha<\gamma) = f_\nu(\alpha\varphi\colon \alpha<\gamma)$ holds in $\mathcal{V}$. Since $f_\iota(\alpha\colon \alpha<\gamma) = \iota$ also holds for $\iota = 0, 1$, $\mathcal{V}$ satisfies (ii) (and (ii′) in case q is reduced).

(ii′) *implies* (i). Suppose (ii) holds in $\mathcal{V}$, $A \in \mathcal{V}$, $\Phi_x \in \operatorname{Con}(A)$ for $x \in X$, and $(a_0, a_1) \in p(\Phi_x\colon x \in X)$. By Claim 3.5 there exist $a_\alpha \in A$, $1 < \alpha < \gamma$, such that $(a_\mu, a_\nu) \in \Phi_x$ for any edge $\mu \overset{x}{\bullet\!\!-\!\!-\!\!\bullet} \nu$ of $G(p)$. Consider the elements $f_\iota(a_\alpha\colon \alpha<\gamma)$, $\iota<\delta$, that we obtain by $M(p \leqq \bar{q})$. If $f_\mu \overset{\Theta_x}{\bullet\!\!-\!\!-\!\!\bullet} f_\nu$ is an edge of $G(p \leqq \bar{q})$ then, by making use of the corresponding identity,

$$f_\mu(a_\alpha\colon \alpha<\gamma)\Phi_x f_\mu(a_{\alpha\Theta_x}\colon \alpha<\gamma) = f_\nu(a_{\alpha\Theta_x}\colon \alpha<\gamma)\Phi_x f_\nu(a_\alpha\colon \alpha<\gamma).$$

Thus, by Claims 3.5 and 3.3,

$$(a_0, a_1) = \big(f_0(a_\alpha\colon \alpha<\gamma),\ f_1(a_\alpha\colon \alpha<\gamma)\big) \in \bar{q}(\Phi_x\colon x \in X) \subseteq q(\Phi_x\colon x \in X).$$

Q. e. d.

Now we can prove Theorem 3.2. Suppose (i) holds. Then, by Claim 3.3, for any $\bar{p} \in \operatorname{Rd}(p)$ $\bar{p} \leqq q$ holds in $\operatorname{Con}(A)$ for all $A \in \mathcal{V}$. Hence (ii) follows from Lemma 3.6. Now let (ii) be assumed, and consider an arbitrary family of congruences Φ_x, $x \in X$, from $\operatorname{Con}(A)$, $A \in \mathcal{V}$, and a pair (a_0, a_1) in $p(\Phi_x\colon x \in X)$. Then, by Claim 3.4, $(a_0, a_1) \in \bar{p}(\Phi_x\colon x \in X)$ for some $\bar{p} \in \operatorname{Rd}(p)$. But, by (ii) and Lemma 3.6, $\bar{p} \leqq q$ holds in $\operatorname{Con}(A)$, whence $(a_0, a_1) \in q(\Phi_x\colon x \in X)$. Condition (i) has been shown.

Suppose now that $\bar{p} \in \operatorname{Rd}(p)$, $\bar{q} \in \operatorname{Rd}(q)$, $p' \leqq_r \bar{p}$, $\bar{q} \leqq_r q' \in \operatorname{Rd}(q)$, and $\mathcal{U}$ is a variety satisfying $M(\bar{p} \leqq \bar{q})$. By making use of Lemma 3.6 and Claim 3.3 we obtain that both $p' \leqq \bar{p}$ and $\bar{p} \leqq q'$ hold in $\operatorname{Con}(A)$ for all $A \in \mathcal{U}$. Now Lemma 3.6 (ii′) yields that $M(p' \leqq \bar{q})$ and $M(\bar{p} \leqq q')$ hold in $\mathcal{U}$. Theorem 3.2 has been proved.

4. The main theorem

Before stating the main theorem some preliminaries are needed. Remember that rings always have 1 and modules are unitary left modules. For integers $m, n \geqq 0$ let $D(m, n)$ denote the sentence (in the first-order language of rings with 1) "$(\exists x)(mx = n \cdot 1)$" where $k \cdot y$ or ky is an abbreviation for $y + y + \ldots + y$ (k times) or 0 (if $k = 0$). $D(m, n)$ is called a *divisibility condition.* The concept of *weakening divisibility condition* is defined as follows. We say that a set H of divisibility conditions holds in a ring R if any member of H holds in R. Suppose we are given a nonempty, directed partially ordered set $(I, \leqq)$ and, for all $\iota \in I$, a set H_ι of divisibility conditions such that whenever $\iota \leqq \varkappa \in I$ and H_ι holds in a ring R then $H_\varkappa$ also holds in R. Then the sentence "there exists $\iota \in I$ such that H_ι holds" is called a weakening divisibility condition.

HUTCHINSON [6, Corollary 3] has shown that the lattice varieties $\mathbf{Con}(R)$, R is a ring, form a lattice under the inclusion. Moreover, in this lattice the joins are the usual joins of varieties. To describe this lattice it is worth using the notion of spectrum. Let P denote the set of prime numbers. Then S_R, the *spectrum of a ring R*, is the function S_R: $\{0\} \cup P \to [0, \omega]$ defined by

$$S_R(0) = \text{the characteristic of } R = \min\{n \mid 1 \leqq n < \omega \text{ and } D(0, n) \text{ holds in } R\}$$

(where $\min \emptyset = 0$), and, for $p \in P$,

$$S_R(p) = \min\{n \mid 0 \leqq n < \omega \text{ and } D(p^{n+1}, p^n) \text{ holds in } R\}$$

(where $\min \emptyset = \omega$). Hutchinson [6, Propositions 1 and 4] has shown that a function S: $\{0\} \cup P \to [0, \omega]$ is the spectrum of some ring if and only if either $S(0)=0$ or for any $p \in P$ $S(p) = \max\{k \mid p^k \text{ divides } S(0)\}$. Let L be the set of all possible spectra, i.e.,

$$L = \{S \mid S\colon \{0\} \cup P \to [0, \omega] \text{ and } S(0) \neq 0 \text{ implies}$$

$$S(p) = \max\{k \mid p^k \text{ divides } S(0)\} \text{ for all } p \in P\}.$$

We make L a lattice by introducing the following partial ordering: for $S_1, S_2 \in L$ let $S_1 \leqq S_2$ mean that $S_1(0)$ divides $S_2(0)$ and $S_1(p) \leqq S_2(p)$ for any $p \in P$. The join S of S_γ $(\gamma \in \Gamma)$ in L can be described as follows. If $\{S_\gamma(0) \mid \gamma \in \Gamma\}$ is a bounded set of integers not containing zero then let $S(0)$ be the least common multiple of $S_\gamma(0)$ $(\gamma \in \Gamma)$. Otherwise $S(0)=0$ and, for $p \in P$, $S(p)$ is the supremum of $\{S_\gamma(p) \mid \gamma \in \Gamma\}$.

Now the map $\mathbf{Con}(R) \to S_R$ is an isomorphism from the lattice of varieties $\mathbf{Con}(R)$ (R is a ring) onto L (cf. Hutchinson [6, Propositions 1, 4, and Theorem 5]). Therefore the lattice $\{\mathbf{Con}(R) \mid R \text{ ring}\}$ is satisfactorily described by L, and it is advantageous to use the latter. Moreover, any of $\mathbf{Con}(R)$, S_R, and $\{D(m, n) \mid D(m, n)$ holds in $R\}$ uniquely determines the two others (cf. [6, Corollary 2 and Proposition 6]).

A lattice identity λ is said to be correct if, for any two rings R_1, R_2, $\mathbf{Con}(R_1) = \mathbf{Con}(R_2)$ and $\mathscr{C}(R_1) \models \lambda$ implies $\mathscr{C}(R_2) \models \lambda$.

The following theorem states that exactly the weak divisibility conditions are the ring properties that can be characterized by correct lattice identities.

THEOREM 4.1. *For any nonempty subset I of L the following three conditions are equivalent:*

(i) *There is a correct lattice identity λ such that, for any ring R, $S_R \in I$ iff λ holds in $\mathscr{C}(R)$;*

(ii) *There is a weak divisibility condition D such that, for any ring R, $S_R \in I$ if and only if D holds in R;*

(iii) *I is an ideal of the lattice L.*

This theorem will be sharpened in the following sections, e.g., for any ideal I a suitable λ_I will be constructed.

5. (iii) implies (i)

In this section the first part of the proof of Theorem 4.1 will be presented.

Consider two reduced lattice terms p and q over X. The following system of ring equations, denoted by $E(p\leqq q)$, will be associated with the Mal'cev type condition $M(p\leqq q)$. Let $\{r_\alpha^\beta|\alpha<\gamma,\ \beta<\delta\}$ be the set of variables of $E(p\leqq q)$ where the ordinals γ and δ are the vertex sets of $G(p)$ and $G(q)$, respectively. Let $E(p\leqq q)$ consist of the equations $r_\iota^\iota=1$, $r_\alpha^\iota=0$ $(\iota=0, 1,\ \alpha\neq\iota)$, which are the so-called *endpoint equations*, and, for any edge $f_\mu \bullet\!\!\overset{\pi}{\text{———}}\!\!\bullet f_\nu$ of the graph $G(p\leqq q)$ and any block C of the partition determined by the equivalence π, of the equation $\sum_{\alpha\in C} r_\alpha^\mu=\sum_{\alpha\in C} r_\alpha^\nu$. A system $\{r_\alpha^\beta|\alpha<\gamma,\ \beta<\delta\}$ of elements of a ring R is said to be a solution of $E(p\leqq q)$, if for any $\beta<\delta$ $\{\alpha|r_\alpha^\beta\neq 0$ and $\alpha<\gamma\}$ *is finite* and the equations of $E(p\leqq q)$ hold.

Claim 5.1. *Let p and q be reduced lattice terms and R be a ring. Then $M(p\leqq q)$ holds in $\mathcal{M}(R)$ iff $E(p\leqq q)$ is solvable in R.*

Proof. If $\{r_\alpha^\beta|\alpha<\gamma,\ \beta<\delta\}$ is a solution of $E(p\leqq q)$ in R, then $M(p\leqq q)$ is satisfied in $\mathcal{M}(R)$ by the module terms $f_\beta(x_\alpha\colon \alpha<\gamma)=\sum_{\alpha<\gamma} r_\alpha^\beta x_\alpha$ $(\beta<\delta)$. To check the converse note that for any term $f_\beta(x_\alpha\colon \alpha<\gamma)$ in $\mathcal{M}(R)$ there exist a *unique* system of coefficients $(r_\alpha^\beta\colon \alpha<\gamma)$ such that $f_\beta(x_\alpha\colon \alpha<\gamma)=\sum_{\alpha<\gamma} r_\alpha^\beta x_\alpha$ identically holds in $\mathcal{M}(R)$ and $\{\alpha|r_\alpha^\beta\neq 0,\ \alpha<\gamma\}$ is finite. Thus the identities of $M(p\leqq q)$ yield that $\{r_\alpha^\beta|\alpha<\gamma,\ \alpha<\delta\}$ is a solution of $E(p\leqq q)$ in R. Q. e. d.

Let us mention that Claim 5.1 has the following surprising consequence (compare with the consequence to Corollary 2 in [6]): $\mathcal{C}(R)\models\lambda$ (and, in particular, **Con** (R)) depends only on the additive group structure of R. Indeed, if $E(y;\ p\leqq q)$ denotes the system of equations obtained from $E(p\leqq q)$ by replacing 1 by y everywhere, then $E(p\leqq q)$ is solvable in R iff for any $y\in R$ $E(y\colon p\leqq q)$ is solvable in R. (If the elements r_α^β form a solution of $E(p\leqq q)$ then yr_α^β form a solution of $E(y;\ p\leqq q)$.) But the solvability of $E(y;\ p\leqq q)$ depends merely on the additive group structure of R. Thus Theorem 3.2 and Claim 5.1 apply.

Now the quaternary lattice terms p, e_m and $d_{m,n}$ over $X=\{x_0, x_1, x_2, x_3\}$ will be defined for non-negative integers m, n by the following recursion:

$$p = (x_0\vee x_1)\wedge(x_2\vee x_3), \quad e_0 = x_0,$$
$$e_{k+1} = (((e_k\vee x_3)\wedge(x_1\vee x_2))\vee p)\wedge(x_0\vee x_2), \quad \text{and}$$
$$d_{m,n} = ((e_n\wedge(e_m\vee x_0\vee x_3))\vee x_1\vee x_2)\wedge p.$$

Definition. Given a ring R, $\mathbf{a}^i=(a_0^i, a_1^i, a_2^i, a_i^3)\in R^4$ $(i=0, 1)$ and a reduced lattice term q over $X=\{x_0, x_1, x_2, x_3\}$. Let $E(\mathbf{a}^0, q, \mathbf{a}^1)$ denote the system of equations which is obtained from $E(p\leqq q)$ by omitting the endpoint equations and adding the new equations $r_j^i=a_j^i$ $(i=0, 1,\ j=0, 1, 2, 3)$.

Proposition 5.2. *For any ring R, non-negative integer n, and $\mathbf{a}^0, \mathbf{a}^1\in R^4$ $E(\mathbf{a}^0, e_n, \mathbf{a}^1)$ is solvable in R if and only if there exists $r\in R$ such that $a_0^1=a_0^0-(n+1)r$, $a_1^1=a_1^0$, $a_2^1=a_2^0+r$, and $a_3^1=a_3^0+nr$.*

PROOF. The proof goes via induction. Since $G(p\leqq e_0)$ is f_0 •——^{02}——• f_1, $E(\mathbf{a}^0, e_0, \mathbf{a}^1)$ consists of $r^i_j=a^i_j$ $(i<2,\ j<4)$, $r^0_0+r^0_2=r^1_0+r^1_2$, $r^0_1=r^1_1$, $r^0_3=r^1_3$. Hence the case $n=0$ is trivial.

Suppose the statement is true for n and consider $G(p\leqq e_{n+1})$ on Figure 3.

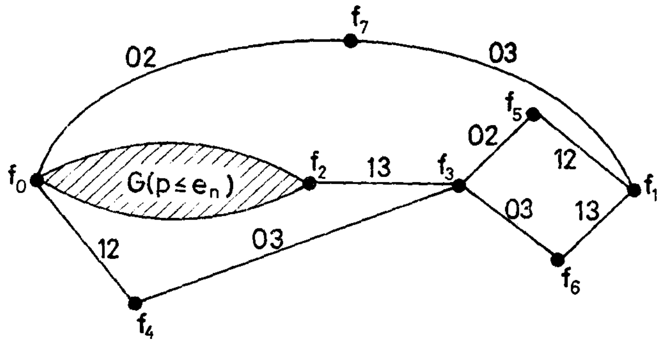


Fig. 3

(The vertices $f_8, f_9, \ldots$, if they exist, are inside of $G(p\leqq e_n)$.) A reference to an equation of $E(\mathbf{a}^0, e_{n+1}, \mathbf{a}^1)$ associated with the edge f_i •————• f_j often will be denoted by "$\overset{ij}{=}$".

Suppose the components of the vectors $\mathbf{a}^i=(a^i_0, a^i_1, a^i_2, a^i_3)\in R^4$ form a solution of $E(\mathbf{a}^0, e_{n+1}, \mathbf{a}^1)$. By the induction hypothesis

(1) $$a^2_0 = a^0_0-(n+1)r, \quad a^2_1 = a^0_1, \quad a^2_2 = a^0_2+r, \quad a^2_3 = a^0_3+nr$$

hold for some $r\in R$. Compute: $a^3_0+a^3_3\overset{34}{=}a^4_0+a^4_3\overset{04}{=}a^0_0+a^0_3$ and $a^3_1+a^3_2\overset{34}{=}a^4_1+a^4_2\overset{04}{=}a^0_1+a^0_2$. On the other hand, $a^3_0\overset{23}{=}a^2_0\overset{(1)}{=}a^0_0-(n+1)r$ and $a^3_2\overset{23}{=}a^2_2\overset{(1)}{=}a^0_2+r$. Comparing these equations we obtain

$$a^3_1 = a^3_1+a^3_2-a^3_2 = a^0_1+a^0_2-(a^0_2+r) = a^0_1-r$$

and

$$a^3_3 = a^3_0+a^3_3-a^3_0 = a^0_0+a^0_3-(a^0_0-(n+1)r) = a^0_3+(n+1)r,$$

i.e.,

(2) $$a^3_0 = a^0_0-(n+1)r, \quad a^3_1 = a^0_1-r, \quad a^3_2 = a^0_2+r, \quad a^3_3 = a^0_3+(n+1)r.$$

Similarly,

$$a^1_1\overset{17}{=}a^7_1\overset{07}{=}a^0_1, \quad a^1_2\overset{16}{=}a^6_2\overset{36}{=}a^3_2\overset{(2)}{=}a^0_2+r,$$

$$a^1_3\overset{15}{=}a^5_3\overset{35}{=}a^3_3\overset{(2)}{=}a^0_3+(n+1)r,$$

and so

$$a^1_0 = (a^1_0+a^1_1+a^1_2+a^1_3)-(a^1_1+a^1_2+a^1_3)\overset{17}{=}(a^7_0+a^7_1+a^7_2+a^7_3)-$$
$$-(a^0_1+a^0_2+r+a^0_3+(n+1)r)\overset{07}{=}(a^0_0+a^0_1+a^0_2+a^0_3)-$$
$$-(a^0_1+a^0_2+a^0_3+(n+2)r) = a^0_0-(n+2)r.$$

We have obtained all the four required equations between $\mathbf{a}^0$ and $\mathbf{a}^1$.

Conversely, suppose $a_0^1=a_0^0-(n+2)r$, $a_1^1=a_1^0$, $a_2^1=a_2^0+r$, and $a_3^1=a_3^0+(n+1)r$. Define $\mathbf{a}^2$ by $a_0^2=a_0^0-(n+1)r$, $a_1^2=a_1^0$, $a_2^2=a_2^0+r$, $a_3^2=a_3^0+nr$. By the induction hypothesis there exist $a_j^i\in R$ $(i\geqq 8,\ j<4)$ such that the equations associated with the edges of the subgraph $G(p\leqq e_n)$ are satisfied. Defining

$$a_0^3 = a_0^0-(n+1)r,\quad a_1^3 = a_1^0-r,\quad a_2^3 = a_2^0+r,\quad a_3^3 = a_3^0+(n+1)r,$$
$$a_0^4 = a_0^0,\quad a_1^4 = a_1^0-r,\quad a_2^4 = a_2^0+r,\quad a_3^4 = a_3^0,$$
$$a_0^5 = a_0^0-(n+2)r,\quad a_1^5 = a_1^0-r,\quad a_2^5 = a_2^0+2r,\quad a_3^5 = a_3^0+(n+1)r,$$
$$a_0^6 = a_0^0-(n+2)r,\quad a_1^6 = a_1^0-r,\quad a_2^6 = a_2^0+r,\quad a_3^6 = a_3^0+(n+2)r,$$
$$a_0^7 = a_0^0-r,\quad a_1^7 = a_1^0,\quad a_2^7 = a_2^0+r,\quad a_3^7 = a_3^0$$

and using Figure 3 it is easy to check that all the remaining equations of $E(\mathbf{a}^0, e_{n+1}, \mathbf{a}^1)$ are satisfied. Q. e. d.

PROPOSITION 5.3. *For any ring R, non-negative integers m, n and $\mathbf{a}^0$, $\mathbf{a}^1\in R^4$ $E(\mathbf{a}^0, d_{m,n}, \mathbf{a}^1)$ is solvable in R if and only if there exist $r, s\in R$ such that $ms=nr$ and $a_0^1=a_0^0-r$, $a_1^1=a_1^0+r$, $a_2^1=a_2^0$, $a_3^1=a_3^0$.*

PROOF. Consider the graph $G(p\leqq d_{m,n})$ on Figure 4. (The vertices f_8, f_9, ... are inside of $G(p\leqq e_m)$ or $G(p\leqq e_n)$.)

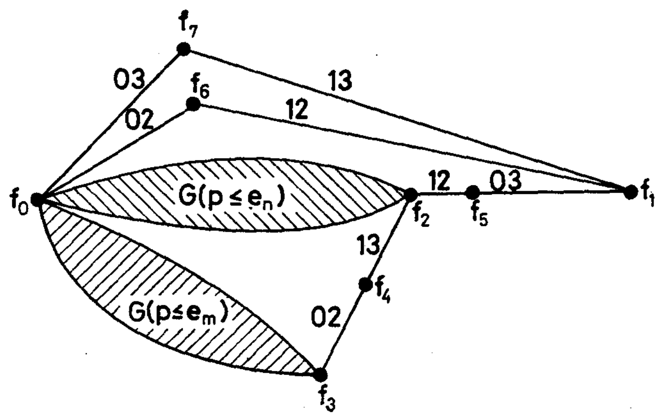


Fig. 4

First let us assume that $E(\mathbf{a}^0, d_{m,n}, \mathbf{a}^1)$ is solvable in R, and the components of the vectors $\mathbf{a}^i=(a_0^i, a_1^i, a_2^i, a_3^i)\in R^4$ form a solution. By Proposition 5.2 there are elements r, s in R such that

$$\begin{aligned} &a_0^2 = a_0^0-(n+1)r,\quad a_1^2 = a_1^0,\quad a_2^2 = a_2^0+r,\quad a_3^2 = a_3^0+nr,\\ &a_0^3 = a_0^0-(m+1)s,\quad a_1^3 = a_1^0,\quad a_2^3 = a_2^0+s,\quad a_3^3 = a_3^0+ms. \end{aligned} \tag{3}$$

Compute:

$$a_2^1 \overset{17}{=} a_2^7 \overset{07}{=} a_2^0,\quad a_3^1 \overset{16}{=} a_3^6 \overset{06}{=} a_3^0,\quad a_0^1 = (a_0^1+a_3^1)-a_3^1 \overset{15}{=} (a_0^5+a_3^5)-$$
$$-a_3^0 \overset{25}{=} (a_0^2+a_3^2)-a_3^0 \overset{(3)}{=} (a_0^0-(n+1)r+a_3^0+nr)-a_3^0 = a_0^0-r,$$

and

$$a_1^1 = a_1^1 + a_2^1 - a_2^1 \overset{15}{=} a_1^5 + a_2^5 - a_2^0 \overset{25}{=} a_1^2 + a_2^2 - a_2^0 \overset{(3)}{=} a_1^0 + a_2^0 + r - a_2^0 = a_1^0 + r.$$

On the other hand,

$$nr = a_1^0 + a_3^0 + nr - a_1^0 - a_3^0 \overset{(3)}{=} a_1^2 + a_3^2 - a_1^0 - a_3^0 \overset{24}{=} a_1^4 + a_3^4 - a_1^0 - a_3^0 \overset{34}{=} a_1^3 + a_3^3 - a_1^0 -$$

$$- a_3^0 \overset{(3)}{=} a_1^0 + a_3^0 + ms - a_1^0 - a_0^3 = ms.$$

Conversely, suppose $ms = nr$, $a_0^1 = a_0^0 - r$, $a_1^1 = a_1^0 + r$, $a_2^1 = a_2^0$, and $a_3^1 = a_3^0$ hold for some $r, s \in R$. Define

$$a_0^2 = a_0^0 - (n+1)r, \quad a_1^2 = a_1^0, \quad a_2^2 = a_2^0 + r, \quad a_3^2 = a_3^0 + nr,$$

$$a_0^3 = a_0^0 - (m+1)s, \quad a_1^3 = a_1^0, \quad a_2^3 = a_2^0 + s, \quad a_3^3 = a_3^0 + ms,$$

$$a_0^4 = a_0^0 - (n+1)r, \quad a_1^4 = a_1^0, \quad a_2^4 = a_2^0 + r, \quad a_3^4 = a_3^0 + ms,$$

$$a_0^5 = a_0^0 - (n+1)r, \quad a_1^5 = a_1^0 + r, \quad a_2^5 = a_2^0, \quad a_3^5 = a_3^0 + nr,$$

$$a_0^6 = a_0^0 - r, \quad a_1^6 = a_1^0, \quad a_2^6 = a_2^0 + r, \quad a_3^6 = a_3^0,$$

$$a_0^7 = a_0^0 - r, \quad a_1^7 = a_1^0, \quad a_2^7 = a_2^0, \quad a_3^7 = a_3^0 + r,$$

and choose a_j^i $(i \geqq 8,\ j < 4)$ by Proposition 5.2. Then, by making use of Proposition 5.2 and Figure 4, it is easy to check that we have a solution of $E(\mathbf{a}^0, d_{m,n}, \mathbf{a}^1)$ in R. Q. e. d.

PROPOSITION 5.4. *Let Γ be a non-empty index set and for $\gamma \in \Gamma$ let A_γ be a non-empty subset of $\{0, 1, 2, \ldots\} \times \{0, 1, 2, \ldots\}$. Then for any ring R the following two conditions are equivalent:*

(i) *The identity $p \leqq \bigvee(\bigwedge(d_{m,n}\colon (m, n) \in A_\gamma)\colon \gamma \in \Gamma)$ holds in $\mathscr{C}(R)$;*

(ii) *The system of the following equations*

$$\sum_{\gamma \in \Gamma} r_\gamma = 1$$

$$m s_{\gamma, m, n} = n r_\gamma \quad \textit{for all} \quad \gamma \in \Gamma,\ (m, n) \in A_\gamma$$

(where r_γ and $s_{\gamma,m,n}$ are variables) is solvable in R. (Note that if $r_\gamma \in R$ $(\gamma \in \Gamma)$ form a solution of the single equation $\sum_{\gamma \in \Gamma} r_\gamma = 1$ then, by definition, $r_\gamma = 0$ for all but finitely many γ.)

PROOF. By Lemma 3.6 (i) is equivalent to the condition: $M(p \leqq \bigvee(\bigwedge(d_{m,n}\colon (m, n) \in A_\gamma)\colon \gamma \in \Delta))$ holds in $\mathscr{M}(R)$ for some finite subset $\Delta = \{\gamma_1, \gamma_2, \ldots, \gamma_k\}$ of Γ. This is equivalent to: $E(p \leqq \bigvee(\bigwedge(d_{m,n}\colon (m, n) \in A_\gamma)\colon \gamma \in \Delta))$ is solvable in R, by Claim 5.1. But this is equivalent to: there exist $\mathbf{a}^0 = (1, 0, 0, 0)$, $\mathbf{a}^1, \mathbf{a}^2, \ldots, \mathbf{a}^k = (0, 1, 0, 0)$ in R^4 such that for $i = 1, 2, \ldots, k$ and for all $(m, n) \in A_{\gamma_i}$ $E(\mathbf{a}^{i-1}, d_{m,n}, \mathbf{a}^i)$ is solvable in R. By Proposition 5.3 this is equivalent to: there exist r_{γ_i}, $s_{\gamma_i, m, n} \in R$, $\mathbf{a}^0, \mathbf{a}^i \in R^4$ $(i = 1, 2, \ldots, k, (m, n) \in A_{\gamma_i})$ such that $\mathbf{a}^0 = (1, 0, 0, 0)$, $\mathbf{a}^k = (0, 1, 0, 0)$, $\mathbf{a}^i = (a_0^{i-1} - r_{\gamma_i}, a_1^{i-1} + r_{\gamma_i}, a_2^{i-1}, a_3^{i-1})$, and $m s_{\gamma_i, m, n} = n r_{\gamma_i}$. But this is clearly equivalent to: there exist r_{γ_i}, $s_{\gamma_i,m,n}\in R$ $(i=1, 2, ..., k, (m, n)\in A_{\gamma_i})$ such that

$$\sum_{i=1}^{k} r_{\gamma_i} = 1, \quad ms_{\gamma_i,m,n} = nr_{\gamma_i}.$$

Since for $\gamma\in\Gamma\setminus\Delta$ we can choose $r_\gamma=s_{\gamma,m,n}=0$, the above condition is equivalent to (ii). Q. e. d.

COROLLARY 5.5. *For arbitrary integers $m, n\geqq 0$ and a ring R the identity $p\leqq d_{m,n}$ holds in $\mathscr{C}(R)$ (or, equivalently, in* **Con** *(R)) iff the divisibility condition $D(m, n)$ holds in R.*

Now for any ideal I of the lattice L an identity λ_I will be defined. If $S(0)\neq 0$ for all $S\in I$ then let λ_I be $p\leqq\bigvee(d_{0,S(0)}: S\in I)$. Otherwise, if $S(0)=0$ for some $S\in I$, let λ_I be $p\leqq\bigvee(\bigwedge(d_{q^{S(q)+1},q^{S(q)}}: q\in P$ and $S(q)<\omega): S\in I)$. Now we can formulate the following

THEOREM 5.6. *Let I be an ideal of L. Then λ_I is a correct lattice identity, and, for any ring R, the following three conditions are equivalent:*
(i) $S_R\in I$;
(ii) *λ_I holds in $\mathscr{C}(R)$;*
(iii) *λ_I holds in* **Con** *(R^4) where R^4 is considered a module over R in the natural way.*

Note that the Theorem remains true if we replace R^4 by R^3 in (iii). The proof of this remark, which is based on HERRMANN and HUHN's method [5], will not be presented here.

PROOF. Since $G(p)$ has four vertices and R^4 is the free algebra on four generators in $\mathscr{M}(R)$, the equivalence of (ii) and (iii) follows from Lemma 3.6.

Now let us consider the case $S(0)\neq 0$ for all $S\in I$. Then, by Proposition 5.4, (ii) is equivalent to the solvability of the system T of following equations:

$$\sum_{S\in I} r_S = 1$$

$$0 = S(0)r_S \quad \text{for all} \quad S\in I.$$

Suppose T is solvable in R and $r_S\in R$ $(S\in I)$ form a solution. Set

$$\{S_1, ..., S_k\} = \{S|S\in I \text{ and } r_S\neq 0\}$$

and define S to be $S_1\vee S_2\vee...\vee S_k$. Since I is an ideal, $S\in I$. Moreover, $S(0)$ is the least common multiple of $S_1(0), ..., S_k(0)$, which implies $0\neq S(0)=t_i S_i(0)$ for suitable integers t_i, $i=1, 2, ..., k$. Now

$$S(0)\cdot 1 = S(0)\cdot\sum_{i=1}^{k} r_{S_i} = \sum_{i=1}^{k} S(0)\cdot r_{S_i} = \sum_{i=1}^{k} t_i S_i(0) r_{S_i} = \sum_{i=1}^{k} t_i\cdot 0 = 0,$$

showing that $S_R(0)$, the characteristic of R, divides $S(0)$. Hence $S_R\leqq S$, implying $S_R\in I$.

Conversely, if $S_R\in I$ then $r_{S_R}=1$, $r_S=0$, $(S\in I\setminus\{S_R\})$ is a solution of T in R.

Now consider the case $0 \in \{S(0) | S \in I\}$. By Proposition 5.4 (ii) is equivalent to the solvability of the system H of following equations:

$$\sum_{S \in I} r_S = 1$$

$$q^{S(q)+1} \cdot s_{S,q} = q^{S(q)} r_S \quad \text{for all} \quad S \in I,\ q \in P,\ S(q) < \omega.$$

Let r_S, $r_{S,q}$ form a solution of H. Choose a finite subset J of I such that $0 \in \{S(0) | S \in J\}$ and $\{r_S | S \in I \setminus J\} = \{0\}$. Defining S' to be $\vee(S\colon S \in J)$ we have $S' \in I$. Since I is an ideal, $S_R \leqq S'$ would be sufficient to show $S_R \in I$. Evidently, $S_R(0)$ divides $S'(0) = 0$. If $S'(q) < \omega$ for $q \in P$ then

$$q^{S'(q)} \cdot 1 = q^{S'(q)} \cdot \sum_{S \in J} r_S = \sum_{S \in J} q^{S'(q)} \cdot r_S = \sum_{S \in J} q^{S'(q)-S(q)} q^{S(q)} r_S =$$

$$= \sum_{S \in J} q^{S'(q)-S(q)} q^{S(q)+1} \cdot s_{S,q} = \sum_{S \in J} q^{S'(q)+1} s_{S,q} = q^{S'(q)+1} \cdot \sum_{S \in J} s_{S,q}.$$

Hence $D(q^{S'(q)+1}, q^{S'(q)})$ holds in R, which implies $S_R \leqq S'$.

Conversely, if $S_R \in I$ then, by the definition of spectrum, $r_{S_R} = 1$, $r_S = 0$ $(S \in I \setminus \{S_R\})$ can be completed to a solution of H in R.

Finally, the equivalence of (i) and (ii) evidently yields the correctness λ_I. Q. e. d.

We conclude this section with two *examples,* both follow from Theorem 5.6 evidently. The identity $p \leqq \vee(d_{0,2i+1}\colon 1 \leqq i < \omega)$ holds in $\mathscr{C}(R)$ iff $S_R(0)$, the characteristic of R, is an odd natural number, while $p \leqq \vee(\wedge(d_{q,1}\colon q \in P \setminus Q)\colon Q$ is a finite subset of $P)$ holds in $\mathscr{C}(R)$ iff for all but finitely many $q \in P$ $D(q, 1)$ holds in R (i.e. $q \cdot 1$ is an invertible element in R).

6. (i) implies (iii)

In this section the following stronger statement will be proved:

THEOREM 6.1. *Let λ be a correct lattice identity. Then the set $I = \{S_R | R$ is a ring and λ holds in $\mathscr{C}(R)\}$ is an ideal of L. Moreover, if λ is finite (i.e., a lattice identity in the usual sense) then I is a principal ideal of L.*

REMARK. Since L is complete, the intersection of arbitrary principal ideals is principal again. So, if we consider a set $\{\lambda_\gamma\colon \gamma \in \Gamma\}$ of *finite* lattice identities, $\{R_S | \mathscr{C}(R) \models \lambda_\gamma$ for all $\gamma \in \Gamma\}$ is a principal ideal of L. But many ideals of L is not principal. Therefore there are ring-properties characterizable by lattice identities which cannot be characterized even by *sets* of finite lattice identities. Two such properties were characterized in the examples of the previous section.

The proof requires some preliminary statements. For any $S \in L$ a ring R_S will be defined in the following manner. If $S(0) \neq 0$, let R_S be $Z/S(0)$, a factor ring of the ring Z of integers. If $S(0) = 0$ then consider $F(X)$, the free commutative ring with 1 over the set $X = \{x_p | p \in P\}$, and its congruence Θ_S generated by $\Phi_S = \{(p^{S(p)+1} \cdot x_p,\ p^{S(p)} \cdot 1) | p \in P$ and $S(p) < \omega\}$, and let R_S be the factor ring $F(X)/\Theta_S$.

Proposition 6.2 (Hutchinson [6, Proposition 4 and the proof of Theorem 5]). *For* $S\in L$ *the spectrum of* R_S *is* S, *and whenever* $S_1\leqq S_2$ *then* R_{S_1} *is a homomorphic image of* R_{S_2}.

Proof. Only the case $n=S_1(0)\neq 0$ and $S_2(0)=0$ will be handled since the rest is similar and it is explicit in [6]. For any $p\in P$ let y_p be such an element of $R_{S_1}=Z/n$ for which $p^{S_1(p)+1}\cdot y_p=p^{S_1(p)}\cdot 1$ holds. Consider the homomorphism $\varphi\colon F(X)\to Z/n$, $1\mapsto 1$, $x_p\mapsto y_p$. By the Second Isomorphism Theorem it suffices to show $\Theta_{S_2}\subseteq \operatorname{Ker}\varphi$. Therefore $\Phi_{S_2}\subseteq\operatorname{Ker}\varphi$ is also sufficient. Suppose

$$(p^{S_2(p)+1}\cdot x_p,\ p^{S_2(p)}\cdot 1)\in\Phi_{S_2}.\quad \text{Since}\quad S_2(p)\geqq S_1(p),\quad \text{we have}$$

$$(p^{S_2(p)+1}\cdot x_p)\varphi = p^{S_2(p)+1}\cdot y_p = p^{S_2(p)-S_1(p)}\cdot p^{S_1(p)+1}\cdot y_p = p^{S_2(p)-S_1(p)}\cdot p^{S_1(p)}\cdot 1 =$$
$$= p^{S_2(p)}\cdot 1 = (p^{S_2(p)}\cdot 1)\varphi.\quad \text{Q. e. d.}$$

Let us cite the following

Proposition 6.3 ([6, Corollary 3]). *Suppose* $R=\prod_{\gamma\in\Gamma} R_\gamma$ *is the direct product of rings* R_γ, $\gamma\in\Gamma$. *Then* $\mathbf{Con}(R)$ *is the join* $\bigvee(\mathbf{Con}(R_\gamma)\colon \gamma\in\Gamma)$ *in the complete lattice of all lattice varieties.*

The following statement is also needed:

Claim 6.4. *Let* R *be the direct product of rings* R_1 *and* R_2, *and let* $p\leqq q$ *be an arbitrary lattice identity. Then* $p\leqq q$ *holds in* $\mathscr{C}(R)$ *iff it holds both in* $\mathscr{C}(R_1)$ *and* $\mathscr{C}(R_2)$.

Proof. Observe that, for $\bar p\in\operatorname{Rd}(p)$ and $\bar q\in\operatorname{Rd}(q)$, $E(\bar p\leqq\bar q)$ is solvable in R iff it is solvable both in R_1 and R_2. Therefore, by Theorem 3.2 and Claim 5.1, $\mathscr{C}(R)\models p\leqq q$ implies $\mathscr{C}(R_i)\models p\leqq q$ for $i=1,2$. Conversely, if $\mathscr{C}(R_i)\models p\leqq q$, $i=1,2$, then for any $\bar p\in\operatorname{Rd}(p)$ there exists $q_i\in\operatorname{Rd}(q)$ such that $M(\bar p\leqq q_i)$ holds in $\mathscr{M}(R_i)$. Since $\operatorname{Rd}(q)$ is directed and $M(\bar p\leqq q')$ is weakening in q', there exists $\bar q\in\operatorname{Rd}(q)$ such that $M(\bar p\leqq\bar q)$ holds in $\mathscr{M}(R_i)$ for $i=1,2$. Therefore $E(\bar p\leqq\bar q)$ is solvable in R_1, R_2, and, consequently, in R. Now Theorem 3.2 and Claim 5.1 yield that $p\leqq q$ holds in $\mathscr{C}(R)$. Q. e. d.

Proof of Theorem 6.1. Let S_1, $S_2\in I$. By Proposition 6.2 and the correctness of λ, λ holds in $\mathscr{C}(R_{S_1})$ and $\mathscr{C}(R_{S_2})$. Therefore, by Claim 6.4, λ holds in $\mathscr{C}(R_{S_1}\times R_{S_2})$. Proposition 6.3 together with the isomorphism between L and the lattice $\{\mathbf{Con}(R)|\ |R \text{ ring}\}$ yield that the spectrum of $R_{S_1}\times R_{S_2}$ is $S_1\vee S_2$. Hence $S_1\vee S_2$ belongs to I.

Now suppose $S_1\in I$ and $S_2\leqq S_1$. Then λ holds in $\mathscr{C}(R_{S_1})$. Since the solvability of $E(\bar p\leqq\bar q)$ is preserved under taking homomorphic images, λ holds in $\mathscr{C}(R_{S_2})$. Hence $S_2\in I$, and I is an ideal.

For λ finite consider the ring $R=\prod_{S\in I} R_S$. Then, by Propositions 6.2 and 6.3, $S_R=\bigvee(S\colon S\in I)$. On the other hand, by Proposition 6.3, λ holds in $\mathscr{C}(R)$. Hence I is a principal ideal with greatest element S_R. Q. e. d.

7. The equivalence of (ii) and (iii)

Suppose $H=(\exists\gamma\in\Gamma)(H_\gamma)$ is a weak divisibility condition. Let $\{S_R|H_\gamma$ holds in $R\}$ be denoted by J_γ. Then $\{S_R|H$ holds in $R\}$ is equal to the *directed* union $\bigcup_{\gamma\in\Gamma} J_\gamma$. So it is sufficient to show that J_γ $(\gamma\in\Gamma)$ is an ideal. But $J_\gamma=\bigcap_{D(m,n)\in H_\gamma}\{S_R|\ D(m,n)$ holds in $R\}=\bigcap_{D(m,n)\in H_\gamma}\{S_R|p\leqq d_{m,n}$ holds in $\mathscr{C}(R)\}$ is a (principal) ideal by Corollary 5.5 and Theorem 6.1.

Conversely, let I be an ideal of L. For $S\in I$ let H_S be the set of divisibility conditions that hold in R_S. Since divisibility conditions are preserved under taking homomorphic images, by Proposition 6.2 $H=(\exists S\in I)(H_S)$ is a weak divisibility condition. We claim that $I=\{S_R|H$ holds in $R\}$. Since $S_{R_S}=S$, the $\subseteq$ inclusion is trivial. Suppose H, say H_S $(S\in I)$ holds in R. Then $\{D(0,S(0))\}\cup\{D(p^{S(p)+1},p^{S(p)})|$ $p\in P,\ S(p)<\omega\}$, a subset of H_S, also holds in R. Thus we have $S_R\leqq S$, implying $S_R\in I$. Q. e. d.

8. Non-correct lattice identities

First we show the existence of non-correct lattice identities.

Proposition 8.1. *The lattice identity*

$$\lambda:\ p\leqq d_{2,1}\vee\bigwedge(d_{q,1}:\ 2\neq q\in P)$$

is not correct (where p, $d_{m,1}$ are terms defined in Section 5).

Proof. Proposition 5.4 yields that for a ring R λ holds in $\mathscr{C}(R)$ iff the system E of equations $r_1+r_2=1$, $2s_1=r_1$, $qs_q=r_2$ $(2\neq q\in P)$ is solvable in R. It is trivial that E is not solvable in Z, the ring of integers. On the other hand, if $2^\beta p_1^{\alpha_1}\dots p_t^{\alpha_t}$ is the prime factorization of a natural number k then $r_2=p_1^{\alpha_1}\dots p_t^{\alpha_t}$ can be completed to a solution of E in Z/k, the factor ring of integers modulo k. Therefore E is solvable in $Z^*=\prod_{k>1} Z/k$ as well. However, the description of the lattice L and Proposition 6.3 yield that Z and Z^* have the same spectrum. Q. e. d.

Remark. For nonnegative integers m,n and a ring R let $\frac{mR}{n}$ mean the ideal $\{x\in R|m\cdot r=n\cdot x$ for some $r\in R\}$ of R. As a common generalization of the identities occurring in Corollary 5.5, Theorem 5.6, and Proposition 8.1 we have: For any lattice term $q(x_{m,n}:\ m\geqq 0,\ n\geqq 0)$ and a ring R the identity $p(x_0,x_1,x_2,x_3)\leqq q\big(d_{m,n}(x_0,x_1,x_2,x_3):\ m\geqq 0,\ n\geqq 0\big)$ holds in $\mathscr{C}(R)$ if and only if $R\subseteq q\left(\frac{mR}{n}:\ m\geqq 0,\ n\geqq 0\right)$ holds in the ideal lattice of R. The proof is very similar to that of Proposition 5.4, therefore it will be omitted.

Finally, we present a sufficient condition for lattice identities to be correct. Theorem 5.6 shows that this condition is not necessary.

Proposition 8.2. *Let p and q be lattice terms. If $p\leqq q$ does not contain infinitary meets then $p\leqq q$ is correct.*

PROOF. Since, for $\bar{p} \in \mathrm{Rd}(p)$ and $\bar{q} \in \mathrm{Rd}(q)$, $\bar{p}$ and $\bar{q}$ are finite, so are $G(\bar{p})$ and $G(\bar{q})$. Thus $E(\bar{p} \leqq \bar{q})$ is a *finite* system of *finite* equations. Therefore, as it is shown in [6, Theorem 3 and Proposition 1], $E(\bar{p} \leqq \bar{q})$ is correct, i.e., if it is solvable in R_1 and $S_{R_2} = S_{R_1}$ then it is solvable in R_2 as well. Q. e. d.

REMARK. Even a stronger result is true, namely if the lattice term q does not contain infinitary meets then $p \leqq q$ is correct for *any* lattice term p. The proof is almost the same as that of Proposition 8.2, but instead of referring to [6] we should have to show directly (with the Frobenius' method as in [6]) that certain infinite systems containing finitely many variables are also correct. Because of its length the detailed proof will be omitted.

REFERENCES

[1] BIRKHOFF, G., *Lattice theory,* Third edition, American Mathematical Society Colloquium Publications, Vol. XXV, American Mathematical Society, Providence, R. I., 1967. *MR* **37** #2638.
[2] CZÉDLI, G., Congruence varieties, Thesis, Attila József University, Szeged, 1979 (in Hungarian).
[3] GRÄTZER, G., *General lattice theory,* Lehrbücher und Monographien aus dem Gebiete der exakten Wissenschaften, Mathematische Reihe, Band 52, Birkhäuser-Verlag, Basel—Stuttgart, 1978; Akademie-Verlag, Berlin, 1978. *MR* **80c**: 06001a.
[4] GRÄTZER, G., *Universal algebra,* Second edition, Springer-Verlag, Berlin—Heidelberg—New York, 1979. *MR* **80g**: 08001.
[5] HERRMANN, C. and HUHN, A. P., Zum Begriff der Charakteristik modularer Verbände, *Math. Z.* **144** (1975), 185—194. *MR* **52** #5503.
[6] HUTCHINSON, G. and CZÉDLI, G., A test for identities satisfied in lattices of submodules, *Algebra Universalis* **8** (1978), 269—309. *MR* **57** #9621.
[7] JÓNSSON, B., Congruence varieties, *Algebra Universalis* **10** (1980), 355—394. *MR* **81e**: 08004.
[8] PIXLEY, A. F., Local Malcev conditions, *Canad. Math. Bull.* **15** (1972), 559—568. *MR* **46** #8942.
[9] WILLE, R., *Kongruenzklassengeometrien,* Lecture Notes in Mathematics, Vol. 113, Springer-Verlag, Berlin—New York, 1970. *MR* **41** #6759.

(Received September 16, 1981)

JÓZSEF ATTILA TUDOMÁNYEGYETEM
BOLYAI INTÉZETE
ARADI VÉRTANÚK TERE 1
H—6720 SZEGED
HUNGARY

82-2992 — Szegedi Nyomda — F. v.: Dobó József igazgató