C.R. Math. Rep. Acad. Sci. Canada

Vol. XI, No. 3 **June 1989 juin**

CONTENTS

JORDAN AND RIGHT ALTERNATIVE COUNTEREXAMPLES

IRVIN ROY HENTZEL AND DAVID POKRASS JACOBS

Abstract. In the free commutative power associative algebras, we show that the Jordan associator (aa, b, a) does not square to zero and is not in the left, right, or middle nucleus. We show the same properties for (aa, a, b). These and some other questions were answered by constructing a counterexample. We contrast this approach with the characteristic function type proof that was used to show that in a right alternative algebra, the cube of the alternator need not be zero.

Presented by P. Ribenboim, F.R.S.C.

Introduction. Given a variety defined by multilinear identities, we attempt to create a basis of the free algebra of the variety. Since the defining identities are multilinear, the free algebra decomposes into the direct sum of its homogeneous submodules. If the ring of scalars is a field or at least a principal ideal domain, a concept of dimension of these homogeneous submodules exists. For most varieties, the dimension of these submodules grows rapidly. There are a few atypical varieties where the basis of the free algebra is known. The common ones are associative, non-associative, and commutative. Less well known are the alternative on three generators (see [6] and [7]) and strongly $(-1, 1)$ on two generators (see [1]). Whenever the scalars are a field, a basis certainly exists, but except for the above examples, there seem to be no recognizable pattern, and the complete (infinite) basis cannot be described. The reason for wanting a basis and an algorithm for expressing elements in terms of the basis, is that then one can decide whether or not two elements are equal. To test if an expression were an identity, one would simply write it in terms of the basis and check to see if all coefficients of the basis elements were zero. For this type of use one does not need a basis of the entire algebra. One only needs a basis of the one relevant homogeneous summand.

The dynamic programming approach that we describe is robust enough for several current problems. Several applications are given.

Dynamic Programming. The process [3] we call dynamic programming consists of choosing a basis of degree one products, then degree two, then degree three, etc. The concept of degree requires that the identities of the algebra be homogeneous. We furthermore assume that the defining identities are multilinear. That is, homogeneous and degree one in each variable. The characteristic of the underlying field often plays a substantial role. For our work we use the rationals Q, the integers Z, and the Galois fields Z_p for p a prime. Computationally, Z_p is nice since we are protected from arithmetic overflow. There is a great deal of similarity between identities of the algebras over Q, Z, or Z_p, and often, but not always, a proof or counterexample in one system also works in the other two systems. The prime $p = 103$ is a convenient prime to use because the residues can be stored in 8 bits of storage. Of course, there are other primes with this property also.

Dynamic programming targets a particular identity in question. If that polynomial has n $a's$ and m $b's$, the program computes a series of bases for each of the homogeneous submodules with r $a's$ and s $b's$ where $0 \leq r \leq n$ and $0 \leq s \leq m$. When it is studying r $a's$ and s $b's$, then for all choices of i and j which satisfy $0 \leq i \leq r$ and $0 \leq j \leq s$, it first computes the space of all products of basis elements from the space of i $a's$ and j $b's$ and that of $r-i$ $a's$ and $s-j$ $b's$. From the combined collection of these products is chosen a basis of the homogeneous submodule of r $a's$ and s $b's$. This basis and the formulas which express the non-basis products in terms of the basis are stored.

This scheme has practical value as long as the number of basis elements does not grow too quickly.

We have applied it to commutative, power associative algebras with success.

The Jordan law in a commutative ring is $(aa, b, a) \equiv ((aa)b)a - (aa)(ba) \equiv 0$. In [2] this identity was weakened to $2((ab)b)b + a((bb)b) - 3(a(bb))b \equiv 0$. This weaker form no longer implies power associativity. Yet, each Jordan associator, (aa, b, a), lies in the middle nucleus [2, Lemma 7], and the ideal generated by the set of all Jordan associators is nilpotent of index 2.

After the surprising result in [2], we suspected that the Jordan associator $(aa, b, a) \equiv ((aa)b)a - (aa)(ba)$ in a commutative, power associative algebra would square to zero or perhaps reside in the middle or left nucleus. This turned out not to be the case.

Theorem. *In the free commutative power associative algebra over Z_p $p = 103$, the following polynomials are not zero.*

(1) $(a^2, b, a)(a^2, b, a)$
(2) $(a^2, a, b)(a^2, a, b)$
(3) $(a^2, (a^2, a, b), b)$
(4) $((a^2, a, b), a, a)$
(5) $(b, (b, a^2, a), a)$
(6) $(((b, a, a), a, a), a, a)$
(7) $(a^2, a, (a^2, b, a))$
(8) $(a^2, (a^2, (a^2, b, a), a), a)$

We tried to find pairs x, y of nonzero elements such that the product $xy = 0$. Letting x be successively (9), (10), (11), we searched for a nonzero combination y of basis elements using at most 3 $a's$ and 1 b such that $xy = 0$. There were none. We can say that none of (9), (10), or (11) is a zero divisor with any nonzero homogeneous polynomial having at most 3 $a's$ and 1 b.

(9) (a^2, b, a)
(10) (a^2, a, b)
(11) $2((ba)a)a + ((aa)a)b - 3((aa)b)a.$

We always truncated the algebras by assigning zero to all products with more than the number of a's or b's needed for the expression we were examining. The largest dimension we used was for 6 a's and 2 b's. That dimension was 171. The largest total degree used was 9 a's and 1'b. That dimension was 85.

Corollary. *In the free commutative power associative algebra over Z, the same 11 results are true.*

PROOF: Any ring is an algebra over the integers. Since the results are false for some ring, they are false for the free ring over the integers.

We do not know if the results are also true over the rationals.

Right Alternative Algebras.

We wish to add a remark about another technique used to prove that polynomials are not zero in the free ring of some variety. We proved that in the free right alternative ring with generators a and b, the cube of (a, a, b) was not zero (see [4] and [5].)

Let $X = \{x_1, x_2, \ldots, x_9\}$. Let $F[X]$ be the free nonassociative algebra in indeterminates X over any commutative ring F with identity element. We produced a function defined on the basis of monomials of $F[X]$. When this function is extended linearly to all of $F[X]$, it maps to zero everything in the T-ideal generated by the right alternative law. This function maps the multilinear linearized form of $(a, a, b)^3$ to 1, the unit of F. Thus the linearized form of $(a, a, b)^3$ is not zero. A homogeneous (but not necessarily multilinear) identity always implies that its completely linearized form is also an identity. We thus conclude that the original expression $(a, a, b)^3$ is not an identity in a right alternative algebra over any commutative algebra. This result answered an open question since it is known that $(a, a, b)^4 = 0$, see [8, Theorem 2, pp. 344–345].

REFERENCES

1. I. R. Hentzel, *The characterization of* $(-1,1)$ *rings*, J. Alg. 30 (1974), p. 236-258.
2. I. R. Hentzel and L. A. Peresi, *Almost Jordan rings*, Proc. Amer. Math. Soc. (to appear).
3. I. R. Hentzel and D. Pokrass Jacobs, *A dynamic programming method for free algebras*, submitted.
4. I. R. Hentzel and D. Pokrass Jacobs, "Verification of non-identities," Proc. 1988 ISSAC, Springer -Verlag (to appear).
5. I. R. Hentzel and D. Pokrass Jacobs, *In a right alternative algebra an alternator need not cube to zero, Abstracts of the A.M.S., Jan 1988.* Abstracts 839-17-01
6. A. V. Il'tyakov, *Free alternative algebras of rank 3*, Algebra and Logic 23 no. 2 (1984), p. 98-113.
7. N. S. Prokhanov, *Basis problem for a free alternative* Φ*-algebra*, Siberian Math. J. 21 no. 4 (1980), p. 579-583.
8. K. A. Zhevlakov, A. M. Slin'ko, I. P. Shestakov, and A. I. Shirshov, "Rings that are Nearly Associative," translated by H. Smith, Academic Press, 1982.

Irvin Roy Hentzel
Department of Mathematics
Iowa State University
Ames, Iowa 50011

David Pokrass Jacobs
Department of Computer Science
Clemson University
Clemson, South Carolina 29634-1906

Received November 11, 1988

AN APPLICATION OF AN IMPLICIT FUNCTION THEOREM TO A PARTIAL DIFFERENTIAL EQUATION

Á. Száz

Presented by J. Aczel, F.R.S.C.

ABSTRACT

Using a generalized implicit function theorem, we describe the solutions of a linear homogeneous partial differential equation of the first order.

1. INTRODUCTION

In this note, we show that a generalized implicit function theorem, which involves the solution of the functional equation

$$F(x,\phi(x,z)) = z ,$$

can be used to directly prove a useful assertion about the functional dependence of the solutions of the differential equation

$$D_1u(x,y) + D_2u(x,y)\, f(x,y) = 0 .$$

Note that this particular equation is closely related to the standard equation $y'(x)=f(x,y(x))$, and plays an important role in the solution of some quasilinear equations [2, pp. 301 and 333] .

2. THE RESULT

Let X and Y be Banach spaces over $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$. Denote by $L(X,Y)$ the space of all continuous linear maps of X into Y. Moreover, let $L_o(X,Y)$ be the set of all bijective members of $L(X,Y)$.

Let f be a C^o map of an open subset D of $X \times Y$ into $L(X,Y)$, and consider the differential equation

$$(1) \qquad D_1 u(x,y) + D_2 u(x,y)\, f(x,y) = 0 .$$

A C^1 map u of D into a Banach space Z over $\mathbb{K}$ may be called a global C^1 solution of the equation (1) if the equality (1) holds for all $(x,y) \in D$.

Now, as a direct application of a generalized implicit function theorem, we can prove

THEOREM. *If*

$$u_o : D \to Z_o$$

is a C^1 *solution of* (1) *and* $(x_o,y_o) \in D$ *such that*

$$D_2 u_o(x_o,y_o) \in L_o(Y,Z_o),$$

then there are open neighbourhoods Ω *and* W *of the points* (x_o,y_o) *and* $u_o(x_o,y_o)$, *respectively, such that for any further* C^1 *solution*

$$u : D \to Z$$

of (1) *there exists a* C^1 *map* Ψ *of* W *into* Z *such that*

$$u(x,y) = \Psi(u_o(x,y))$$

for all $(x,y) \in \Omega$.

PROOF. By a slight improvement of the generalized implicit function theorem of [1, p. 28], there are open neighbourhoods U, V and W of the points x_o, y_o and $u_o(x_o,y_o)$, respectively, such that there exists a unique map ϕ of $U \times W$ into V such that

$$u_o(x,\phi(x,z)) = z$$

for all $x \in U$ and $z \in W$. Moreover, this map ϕ is also C^1.

Here, because of the opennness of $L_o(Y,Z_o)$, we may assume that

$$D_2u_o(x,y) \in L_o(Y,Z_o)$$

for all $x \in U$ and $y \in V$. And, thus by the chain rule, we can also state that

$$D_1\phi(x,z) = -(D_2u_o(x,\phi(x,z)))^{-1} D_1u_o(x,\phi(x,z))$$

for all $x \in U$ and $z \in W$.

Hence, since now we also have

$$D_1u_o(x,\phi(x,z)) + D_2u_o(x,\phi(x,z)) f(x,\phi(x,z)) = 0$$

for all $x \in U$ and $z \in W$, it is clear that

$$D_1\phi(x,z) = f(x,\phi(x,z))$$

for all $x \in U$ and $z \in W$.

Thus, by defining

$$h_z(x) = u(x,\phi(x,z))$$

for all $x \in U$ and $z \in W$, we can at once state that

$$h_z'(x) = D_1u(x,\phi(x,z)) + D_2u(x,\phi(x,z)) f(x,\phi(x,z)) = 0$$

for all $x \in U$ and $z \in W$.

This shows that the map h_z is constant on the components of U for any $z \in W$. Thus, by letting U_o be the component of U containing the point x_o, we can define a C^1 map Ψ of W into Z such that

$$\Psi(z) = u(x,\phi(x,z))$$

for all $x \in U_o$ and $z \in W$.

Now, by taking the open neighbourhood

$$\Omega = u_o^{-1}(W) \cap (U_o \times V)$$

of the point (x_o,y_o), we can also state that

$$\Psi(u_o(x,y)) = u(x,\phi(x,u_o(x,y))) = u(x,y)$$

for all $(x,y) \in \Omega$.

Namely, if $(x,y) \in \Omega$, then by the definitions of Ω and ϕ, we clearly have

$$u_o(x,\phi(x,u_o(x,y))) = u_o(x,y).$$

And hence, because of the unicity of ϕ the equality

$$\phi(x,u_o(x,y)) = y$$

follows.

REMARK. As a trivial converse to this theorem, we can also state that if $u_o : D \to Z_o$ is a C^1 solution of (1) and $u : D \to Z$ such that for each $(x_o,y_o) \in D$ there are open neighbourhoods Ω and W of (x_o,y_o) and $u_o(x_o,y_o)$, respectively, and a C^1 map Ψ of W into Z such that $u(x,y) = \Psi(u_o(x,y))$ for all $(x,y) \in \Omega$, then u is also a C^1 solution of (1).

3. A PARTICULAR CASE

Let U and V be open subsets of X and Y, respectively. Moreover, let A and B be C^1 maps of U and V into X, respectively, such that $B'(y) \in L_o(Y,X)$ for all $y \in V$.

Then, the differential equation

$$D_1u(x,y) + D_2u(x,y)\, B'(y)^{-1} A'(x) = 0 \tag{2}$$

is an important particular case of the equation (1).

And, to apply the above results, one can at once see that the map u_o defined on $U \times V$ by

$$u_o(x,y) = A(x) - B(y)$$

is a C^1 solution of (2) such that $D_2u_o(x,y) \in L_o(Y,X)$ for all $(x,y) \in U \times V$.

Note that the basic equations $D_1u(x,y) = 0$ and

$$D_1u(x,y) + D_2u(x,y) = 0$$

are particular cases of (2), while the Cauchy-Riemann equation

$$D_1u(x,y) + i\, D_2u(x,y) = 0,$$

with $x, y \in \mathbb{R}$, is not a particular case of (2).

REFERENCES

[1] A. Avez, Differential Calculus, John Wiley and Sons, New York, 1986.

[2] W.W. Stepanow, Lehrbuch der Differentialgleichungen, Deutscher Verlag der Wissenschaften, Berlin, 1956.

Received February 3, 1989

Department of Mathematics
Lajos Kossuth University
H-4010 Debrecen, Hungary

Measures for the algebraic independence of the values of Mahler type functions

by

Paul-Georg Becker and Kumiko Nishioka

Presented by P. *Ribenboim*, F.R.S.C.

In 1985, Yu. V. Nesterenko found a measure of the algebraic independence for the values of functions of Mahler type. The measure was effective only with respect to the height of the polynomials. Here we establish a measure which is effective in both height and degree of the polynomials.

Using commutative algebra Nesterenko obtained a very good measure of the algebraic independence for the values of functions of Mahler type.

Theorem [Nesterenko [4]]. Let $f_1(z),\dots,f_m(z)$ be power series in z with coefficients in an algebraic number field K, which converge in some neighborhood U of the point $z = 0$, which satisfy the equalities

$$f_i(z^d) = a_i(z)f_i(z)+b_i(z), \quad a_i(z),b_i(z) \in K(z), \quad i = 1,\dots,m,$$

where d is an integer, $d \geq 2$, and which are algebraically independent over $\mathbb{C}(z)$. Suppose that α is an algebraic number, $\alpha \in U$, $0 < |\alpha| < 1$, and the numbers $\alpha,\alpha^d,\alpha^{d^2},\dots$ are distinct from the poles of the functions $a_i(z)$ and $b_i(z)$. Then there exists a function $\varphi(s)$ such that, for any H and $s \geq 1$ with $H \geq \varphi(s)$ and for any polynomial $R \in \mathbb{Z}[x_1,\dots,x_m]$ whose degree does not exceed s and whose coefficients are not greater than H in absolute value, the following inequality holds:

$$|R(f_1(\alpha),\ldots,f_m(\alpha))| > H^{-\gamma s^m},$$

where γ is a positive constant which depends only on α and the functions $f_1,\ldots,f_m$.

The above function $\varphi(s)$ is ineffective in the parameter s. We can make it effective by proving an upper estimate for the zero order of $P(f_1(z),\ldots,f_m(z))$ at $z = 0$ where $P(x_1,\ldots,x_m)$ is a polynomial.

The first author gave in [2] a measure of the algebraic independence of these numbers but his result is not as sharp as the measure of Nesterenko. It was established without using tools from commutative algebra.

1. Estimate for the zero order. - For a formal power series $f(z) \in \mathbb{C}[[z]]$, $\operatorname{ord} f(z)$ denotes the zero order of $f(z)$ at $z = 0$. By using the analogous results to Nesterenko [4] over the polynomial ring $\mathbb{C}[z]$, we have the following theorem.

<u>Theorem 1.</u> <u>Let</u> $f_1(z),\ldots,f_m(z) \in \mathbb{C}[[z]]$ <u>be formal power series satisfying the functional equations</u>

$$f_i(z^d) = \frac{A_i(z,f_1(z),\ldots,f_m(z))}{A_0(z,f_1(z),\ldots,f_m(z))} \quad (1\le i\le m),$$

<u>where</u> $d \ge 2$ <u>is an integer and</u> $A_i(z,x_1,\ldots,x_m) \in \mathbb{C}[z,x_1,\ldots,x_m]$ $(0\le i\le m)$ <u>are polynomials with</u> $\operatorname{tot deg}_{\underline{x}} A_i \le t$.
Suppose that $t^m < d$ and $Q(z,x_1,\ldots,x_m) \in \mathbb{C}[z,x_1,\ldots,x_m]$ is a nonzero polynomial with $\deg_z Q \le M$, $\operatorname{tot deg}_{\underline{x}} Q \le N$ where $M \ge N \ge 1$. If $Q(z,f_1(z),\ldots,f_m(z)) \not\equiv 0$, then

$$\operatorname{ord} Q(z, f_1(z), \ldots, f_m(z)) \leq C M N^m N^{(m^2 \log t)/(\log d - m \log t)}$$

where C is a positive constant depending only on the functions $f_1, \ldots, f_m$.

2. Measures of the algebraic independence. - As a consequence of Theorem 1, Nesterenko's Theorem can be improved in the following way.

<u>Theorem 2. Let</u> $A(z)$ <u>be a</u> $m \times m$ <u>matrix and</u> $B(z)$ <u>be a m-dimensional vector whose entries are rational functions of z with algebraic coefficients. Let</u> $F(z) = (f_1(z), \ldots, f_m(z))^t$ <u>be a vector of formal power series with algebraic coefficients which converge in some neighborhood</u> U <u>of the point</u> $z = 0$ <u>and satisfy</u>

$$F(z^d) = A(z)F(z) + B(z),$$

<u>where</u> $d \geq 2$ <u>is an integer and which are algebraically independent over</u> $\mathbb{C}(z)$. <u>Suppose that</u> α <u>is an algebraic number</u>, $\alpha \in U$, $0 < |\alpha| < 1$, <u>and the numbers</u> $\alpha, \alpha^d, \alpha^{d^2}, \ldots$ <u>are distinct to each pole of both</u> $A(z)$ <u>and</u> $B(z)$.

<u>Then, for any</u> H <u>and</u> $s \geq 1$ <u>and for any polynomial</u> $R \in \mathbb{Z}[x_1, \ldots, x_m]$ <u>whose degree does not exceed</u> s <u>and whose coefficients are not greater than</u> H <u>in absolute value, the following inequality holds:</u>

(1) $$|R(f_1(\alpha), \ldots, f_m(\alpha))| > \exp(-\gamma s^m(\log H + s^{2m+2})),$$

<u>where</u> γ <u>is a positive constant depending only on</u> α <u>and on the functions</u> $f_1, \ldots, f_m$.

If $F(z)$ satisfies the functional equation

$$F(z) = A(z)F(z^d) + B(z)$$

where the entries of $A(z)$ and $B(z)$ are polynomials in z with algebraic coefficients, we can refine inequality (1) by using the method applied in Becker-Landeck [1].

Theorem 3. *Let* $A(z)$ *be a* $m \times m$ *matrix and* $B(z)$ *be a* m*-dimensional vector whose entries are polynomials in* z *with algebraic coefficients. Let* $F(z) = (f_1(z),\dots,f_m(z))^t$ *be a vector of formal power series with algebraic coefficients which converge in some neighborhood* U *of the point* $z = 0$ *and satisfy*

$$F(z) = A(z)F(z^d) + B(z),$$

where $d \geq 2$ *is an integer and which are algebraically independent over* $\mathbb{C}(z)$. *Suppose that* α *is an algebraic number,* $\alpha \in U$, $0 < |\alpha| < 1$, *and the numbers* $\alpha, \alpha^d, \alpha^{d^2}, \dots$ *are distinct to each zero of* $\det A(z)$.

Then for any H *and* $s > 1$ *and for any polynomial* $R \in \mathbb{Z}[x_1,\dots,x_m]$ *whose degree does not exceed* s *and whose coefficients are not greater than* H *in absolute value, the following inequality holds*:

$$|R(f_1(\alpha),\dots,f_m(\alpha))| > \exp(-\gamma s^m(\log H + s^{m+2}\log s)),$$

where γ *is a positive constant depending only on* α *and on the functions* $f_1,\dots,f_m$.

3. Examples. - Let $d \geq 2$ be an integer and $f(z) = \sum_{n=0}^{\infty} z^{d^n}$. Then by

Theorem 1 in Loxton and van der Poorten [3], $f(z),\dots,f(z^{d-1})$ are algebraically independent over $\mathbb{C}(z)$. Further $\{f^{(\lambda)}(z^i)\}_{1\le i\le d-1,\lambda\ge 0}$ where $f^{(\lambda)}(z) = (z\frac{z}{dz})^{\lambda} f(z)$, are algebraically independent over $\mathbb{C}(z)$ by the same theorem and satisfy the functional equations

$$f^{(\lambda)}(z^i) = d^{\lambda} f^{(\lambda)}(z^{di}) + z^i.$$

Hence we can apply Theorem 3 to the values $\{f^{(\lambda)}(\alpha^i)\}_{1\le i\le d-1,\lambda\ge 0}$ for any algebraic number α with $0 < |\alpha| < 1$.

[1] P.-G. Becker-Landeck, Transcendence measures by Mahler's transcendence method, Bull.Austral.Math.Soc. 33 (1986), 59-65.

[2] P.-G. Becker-Landeck, Maße für algebraische Unabhängigkeit nach einer Methode von Mahler, Acta Arithm. 50 (1988), 279 - 293.

[3] J.H. Loxton and A.J. van der Poorten, Algebraic independence properties of the Fredholm series, J.Austral.Math.Soc. (Ser.A) 26 (1978), 31-45.

[4] Yu.V. Nesterenko, On a measure of the algebraic independence of the values of certain functions, Mat.Sb. 128 (170) (1985); English translation in Math. USSR Sb. 56 (1987), 545-567.

Mathem. Institut der Universität zu Köln
Weyertal 86-90, D-5000 Köln 41

Department of Mathematics
Nara Women's University
Kita-Uoya Nishimachi, Nara 630, Japan

Received February 13, 1989

UNE BORNE POUR UNE SOLUTION ENTIERE POSITIVE PARTICULIERE D'UNE EQUATION LINEAIRE

Jean-Luc LAMBERT
Laboratoire d'informatique de Paris-Nord
Département de Mathématiques et Informatique
Centre scientifique et polytechnique
Université de Paris-Nord
Avenue Jean-Baptiste Clément
93 430 Villetaneuse

Presented by P. Ribenboim, F.R.S.C.

Résumé Nous prouvons que si l'équation diophantienne $c + \sum_{i=1}^{n} a_i x_i = \sum_{j=1}^{m} b_j y_j$ où $a_i \in \mathbb{N}^*$, $b_j \in \mathbb{N}^*$ et $c \in \mathbb{N}$ admet une solution positive, elle en admet une $(x, y) \in \mathbb{N}^n \times \mathbb{N}^m$ telle que

$$\prod_{i=1}^{n} (1 + x_i) \leq \operatorname*{Max}_{j=1}^{m} b_j$$

et que pour tout $z \leq y$ satisfaisant $\sum_{j=1}^{m} b_j (y_j - z_j) \geq c$ on ait

$$\prod_{j=1}^{m} (1 + z_j) \leq \operatorname*{Max}_{i=1}^{n} a_i$$

A BOUND FOR A PARTICULAR POSITIVE INTEGER SOLUTION OF A LINEAR EQUATION

Abstract We prove that if the diophantine equation $c + \sum_{i=1}^{n} a_i x_i = \sum_{j=1}^{m} b_j y_j$ where $a_i \in \mathbb{N}^*$, $b_j \in \mathbb{N}^*$ and $c \in \mathbb{N}$ has a positive solution, it has a positive solution $(x, y) \in \mathbb{N}^n \times \mathbb{N}^m$ such that

$$\prod_{i=1}^{n} (1 + x_i) \leq \operatorname*{Max}_{j=1}^{m} b_j$$

and for any $z \leq y$ satisfying $\sum_{j=1}^{m} b_j (y_j - z_j) \geq c$ one has

$$\prod_{j=1}^{m} (1 + z_j) \leq \operatorname*{Max}_{i=1}^{n} a_i$$

Introduction Comme dans notre précédente note ([2]) nous cherchons à limiter, par la détermination de bornes sur les solutions éventuelles, l'énumération implicite lors de la recherche d'une solution positive pour une équation diophantienne linéaire (pour un exposé de la méthode d'énumération implicite voir par exemple [3] pour une synthèse des bornes connues voir le chapître 17 de [4]). Nous nous intéressons cette fois à l'équation (1):

$$c + \sum_{i=1}^{n} a_i x_i = \sum_{j=1}^{m} b_j y_j$$

où $c \in \mathbb{N}$, $a_i \in \mathbb{N}^*$, $b_j \in \mathbb{N}^*$ et où les inconnues $x \in \mathbb{N}^n$ et $y \in \mathbb{N}^m$. Le résultat que nous avons établi dans [1] permet d'affirmer que si l'équation (1) admet une solution, elle en admet une telle que

$$\sum_{i=1}^{n} x_i \leq \operatorname*{Max}_{j=1}^{m} b_j - 1 \text{ et } \sum_{j=1}^{m} y_j \leq \operatorname{Max}\left(\operatorname*{Max}_{i=1}^{n} a_i, c\right)$$

ce qui n'est pas très fort. Le résultat de [2] donne une borne sur le produit des variables. Pour au moins une solution:

$$\prod_{i=1}^{n} (1 + x_i) \leq c + \sum_{i=1}^{n} a_i x_i + 1 \quad \text{et} \quad \prod_{j=1}^{m} (1 + y_j) \leq \sum_{j=1}^{m} b_j y_j + 1$$

Par une modification judicieuse des techniques de preuve de nos deux précédents articles nous obtenons qu'au moins une solution satisfait:

$$\prod_{i=1}^{n} (1 + x_i) \leq \operatorname*{Max}_{j=1}^{m} b_j$$

Une borne similaire mais plus complexe est prouvée pour y.

Le théorème On désigne par $\leq$ l'ordre produit cartésien sur $\mathbb{N}^n$ ou $\mathbb{N}^m$ de l'ordre sur $\mathbb{N}$; on note $x < y$ si $x \leq y$ et $x \neq y$.
D'autre part on désigne par $\leq_{lex}$ l'ordre lexicographique sur $\mathbb{N}^n$:

$$x \leq_{lex} y \Leftrightarrow x = y \text{ ou il existe } i \text{ tel que } x_1 = y_1, \ldots, x_{i-1} = y_{i-1}, x_i < y_i$$

qui est total et compatible avec l'addition.

Nous montrons le résultat suivant:

Théorème *Soit l'équation*

$$c + \sum_{i=1}^{n} a_i x_i = \sum_{j=1}^{m} b_j y_j$$

où $a_i \in \mathbb{N}^*$, $c \in \mathbb{N}$, $b_j \in \mathbb{N}^*$, $x \in \mathbb{N}^n$, $y \in \mathbb{N}^m$.

Si l'équation admet une solution, elle en admet une (x^*, y^*) *telle que*

i) $\prod_{i=1}^{n} (1 + x_i^*) \leq \operatorname*{Max}_{j=1}^{m} b_j$

ii) *Pour tout vecteur* $z \in \mathbb{N}^m$, $z \leq y^*$ *tel que* $\sum_{j=1}^{m} b_j (y_j^* - z_j) \geq c$ *on ait*

$$\prod_{j=1}^{m} (1 + z_j) \leq \operatorname*{Max}_{i=1}^{n} a_i$$

Preuve On pose $a.x = \sum_{i=1}^{n} a_i x_i$, $b.y = \sum_{j=1}^{m} b_j y_j$. Supposons que l'équation admette une solution alors elle en admet une minimisant pour l'ordre lexicographique le vecteur

$$(a.x,\ x_1,\dots,\ x_n,\ y_1,\dots,\ y_m)$$

soit (x^*, y^*) cette solution. Montrons qu'elle satisfait i) et ii).

i) Construisons une suite $(y^k)_{0 \le k \le s}$ de $\mathbb{N}^m$ telle que:

$$0 = y^0 < y^1 \dots < y^s = y^*$$
$$\sum_{j=1}^{m} y_j^k = k$$

comme $a.x^* \le b.y^*$, il est clair que pour tout $x \le x^*$ il existe k tel que

$$b.y^k \le a.x < b.y^{k+1} \le b.y^k + \operatorname{Max}_{j=1}^{m} b_j$$

posons $r(x) = a.x - b.y^k$, on a $0 \le r(x) < \operatorname{Max}_{j=1}^{m} b_j$ (plusieurs valeurs peuvent convenir pour r(x), on choisit l'une d'entre elles).

Il ne peut exister x_1 et x_2 tels que $x_1 \le x^*$, $x_2 \le x^*$ et $r(x_1) = r(x_2)$ car alors si $k_1$et k_2 vérifient

$$r(x_1) = a.x_1 - b.y^{k_1}$$
$$r(x_2) = a.x_2 - b.y^{k_2}$$

supposons que $k_1 \ge k_2$ alors

$$a.(x_1 - x_2) = b.(y^{k_1} - y^{k_2}) = b.y \text{ où } 0 \le y \le y^*$$

Maintenant $y > 0$ est impossible car alors $b.y > 0$ et $(x^* - x_1 + x_2, y^* - y)$ est une solution de (1) telle que $a.(x^* - x_1 + x_2) < a.x^*$ ce qui est contradictoire avec la minimalité de $(a.x^*, x^*, y^*)$. Donc $y = 0$ mais comme un des vecteurs $x^* - x_1 + x_2$ ou $x^* - x_2 + x_1$ est plus petit que x^* pour l'ordre lexicographique, (x^*, y^*) ne minimise pas $(a.x, x_1,\dots, x_n, y_1,\dots, y_m)$. Une contradiction.

Comme il existe $\prod_{i=1}^{n} (1 + x_i^*)$ vecteurs $x \le x^*$ pour lesquels r(x) prendra $\operatorname{Max}_{j=1}^{m} b_j$ valeurs; et que ces valeurs sont toutes distinctes on conclut

$$\prod_{i=1}^{n} (1 + x_i^*) \le \operatorname{Max}_{j=1}^{m} b_j$$

ii) Soit $z^* \le y^*$ posons $c_1 = b.(y^* - z^*)$, on obtient (2):

$$a.x^* = c_1 - c + b.z^*$$

avec $c_1 - c \geq 0$. Montrons que le couple (x^*, z^*) minimise dans l'ensemble des solutions de (2) le m + n + 1-uplet $(b.z^*, z^*, x^*)$ pour l'ordre lexicographique. En effet dans le cas contraire il existerait (x', z') solution de (2) telle que

a) $a.x' < a.x^*$ (car $b.z' < b.z^*$)
ou b) $z' <_{lex} z^*$ et $a.x' = a.x^*$
ou c) $x' <_{lex} x^*$ et $z' = z^*$, $a.x' = a.x^*$

ce qui est contradictoire avec la minimalité de $(a.x^*, x^*, y^*)$ (dans les cas a) et c) $(x', y^* - z^* + z')$ contredit la minimalité, dans le cas b) il faut considérer $(x^*, y^* - z^* + z')$).

L'application du résultat de i) fournit alors:

$$\prod_{j=1}^{m} (1 + z_j^*) \leq \operatorname{Max}_{i=1}^{n} a_i$$

Références bibliographiques

[1] J.L. LAMBERT, Une borne pour les générateurs des solutions entières positives d'une équation diophantienne linéaire, *C.R. Acad.Sci. Paris*, 305, série I, 1987, p 39-40.
[2] J.L. LAMBERT, Une borne pour une solution optimale entière particulière d'un problème linéaire à matrice de contraintes strictement positive, *C.R. Acad. Sci.*, 307, Série I, 1988, p 193-195.
[3] G.L. NEMHAUSER, L.A. WOLSEY, *Integer and combinatorial optimization*, J. Wiley & Sons, 1988.
[4] A. SCHRIJVER, *Theory of linear and integer programming*, Wiley, New-York, 1986.

Received February 16, 1989

Quotients of quasi-hereditary algebras

István Ágoston

Presented by V. Dlab, F.R.S.C.

Abstract: The notion of a quasi-hereditary algebra was introduced by Cline, Parshall and Scott [1] in their study of representations of complex Lie algebras and algebraic groups. Some of the basic properties were described by Dlab and Ringel [3]. The following question, related to the concept of the heredity measure of an algebra (see [2]) seemed to be of interest: does a minimal heredity ideal of a quasi-hereditary algebra always belong to a heredity chain, i.e. is the quotient of a quasi-hereditary algebra by a heredity ideal always quasi-hereditary? The purpose of this short note is to provide counterexamples to answer this question in the negative and to show that for algebras with less than four simple nonisomorphic modules the answer is positive.

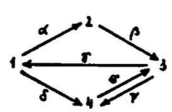
1. The counterexamples. Let us first recall some basic definitions and fix our notation. Let A be a finite dimensional algebra over a field k. Let us denote with N the radical of A. An idempotent ideal J in A is called a heredity ideal if the right ideal J_A is a projective A-module and JNJ=0. The ring A is called quasi-hereditary if there exists a chain of ideals in A:

$$0 = J_0 \subseteq J_1 \subseteq \ldots \subseteq J_m = A$$

such that J_i/J_{i-1} is a heredity ideal in A/J_{i-1} for each i=1,...,m. Such a chain will be called a heredity chain. Let $(e_1,e_2,\ldots,e_n)$ be a complete sequence (ordered set) of primitive orthogonal idempotents in A. We say that such a sequence forms a heredity sequence if the ideals $J_1=Ae_nA$, $J_2=A(e_{n-1}+e_n)A,\ldots$, $J_n=(e_1+e_2+\ldots+e_n)A=A$ form a heredity chain. The indecomposable projective module e_iA will be denoted by P_i while the corresponding simple module (i.e. the top of P_i) by S_i.

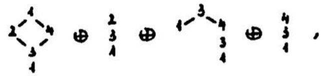
The following example shows that quotients of quasi-hereditary algebras over a (minimal) heredity ideal are not necessarily quasi-hereditary.

Example: Let A be the path algebra of the graph

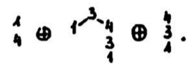


modulo the ideal $\langle \alpha\beta-\delta\sigma, \beta\psi, \psi\alpha, \psi\delta, \sigma\psi \rangle$. Then A is a quasi-hereditary algebra of finite representation type, the ideal $I=Ae_2A$ is a heredity ideal but the quotient algebra A/I is not quasi-hereditary.

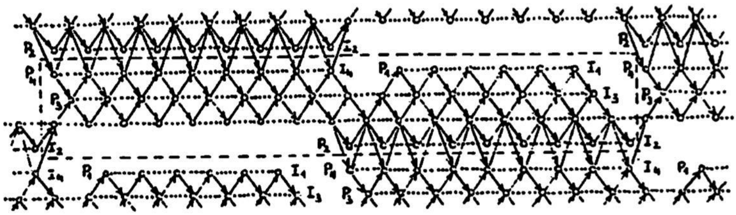
If we index the simple types by the corresponding vertices, the regular representation of A has the form

$A_A =$ 

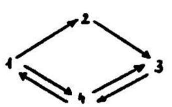
while that of $B = A/J$ can be written as follows:

$B_B =$ 

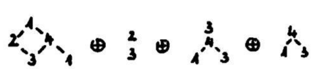
The following is the Auslander–Reiten graph of A (it has 57 vertices).



Remark: Some other examples also might be of interest. Consider the following shallow (see [4]) quasi-hereditary algebra over the graph

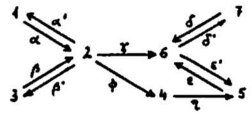


namely

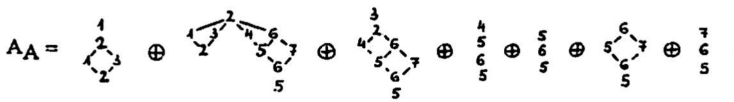
$A_A =$ 

Here $J = Ae_2A$ is a heredity ideal such that A/J is not quasi-hereditary.

Both our examples are algebras of global dimension 4. The results of [3] imply that there are no counterexamples of global dimension 2. Hence we may ask the question whether there is a quasi-hereditary algebra of global dimension 3 which will provide a counterexample. To this end, let us modify Yamagata's example of an algebra of global dimension 3 which is not quasi-hereditary [6]. Take the quotient of the path algebra of the graph



modulo the ideal $\langle \alpha'\alpha - \beta'\beta, \delta'\delta - \varepsilon'\varepsilon, \beta\beta', \alpha\gamma, \beta\alpha', \gamma\varepsilon' - \phi\eta, \delta\delta', \varepsilon\delta', \alpha\phi \rangle$:



Here $J=Ae_4A$ is a heredity ideal such that the quotient algebra A/J is not quasi-hereditary.

Let us note that both algebras presented in this remark are of infinite representation type.

2. Algebras with three isomorphism classes of simple modules. In this section we intend to show that our previous example was in some sense minimal.

Proposition: Let A be a quasi-hereditary algebra with three isomorphism classes of simple modules. If J is a heredity ideal then the algebra A/J is quasi-hereditary.

Proof: We may assume that A is basic. So let (e_1,e_2,e_3) be a heredity sequence of A. Let us denote the composition length of the $\mathrm{End}(P_i)$-module $\mathrm{Hom}_A(P_i,P_j)$ by c_{ij}. Thus c_{ij} is the number of factors in any composition series of P_j which are isomorphic to S_i.

Let us observe that if Ae_iA and Ae_jA are two heredity ideals for $i\neq j$ then either c_{ij} or c_{ji} must be 0; otherwise, we would get a proper embedding of P_i into itself.

Now there are two cases to be considered: J is generated either by e_1 or by e_2. These cases are quite similar but not fully symmetric, so we shall proceed by a case-by-case analysis.

(a) Assume first that $J = Ae_2A$ and $c_{23}=0$. Then the radical $\mathrm{rad}\,P_3$ of P_3 is clearly a direct sum of copies of S_1, since neither S_2 nor S_3 can appear in $\mathrm{rad}\,P_3$ and the simple modules have no self-extensions. If we calculate now the number c_{11}, we may use the fact that (e_1,e_2,e_3) is a heredity sequence and get:

$$c_{11} = c_{31}c_{13} + c_{21}(c_{12} - c_{32}c_{13}) + 1.$$

On the other hand if we assume that A/J is not quasi-hereditary then the ideal $\bar{A}\bar{e}_3\bar{A}$

of $\bar{A}$=A/J is no longer projective and thus

$$c_{11} - c_{21}c_{12} < 1 + (c_{31} - c_{21}c_{32})c_{13}.$$

Hence we get a contradiction.

(b) Now, assume that J = Ae_2A and c_{32}=0. Similarly as in case (a), we get that the radical of P_2 is a direct sum of copies of S_1 and again we can compute the number c_{11}. First, from the heredity sequence we find that

$$c_{11} = c_{31}c_{13} + (c_{21} - c_{31}c_{23})c_{12} + 1.$$

On the other hand the assumption that A/J is not quasi-hereditary implies that

$$c_{11} - c_{21}c_{12} < 1 + c_{31}(c_{13} - c_{23}c_{12}),$$

a contradiction.

(c) Let us turn now to the case when J = Ae_1A. First let c_{13}=0. Then, similarly to the previous case, we see that the radical of P_3 is a direct sum of copies of S_2 and that $c_{22} = c_{32}c_{23} + 1$. Assuming that A/J is not quasi-hereditary, we calculate easily that

$$c_{22} - c_{12}c_{21} < 1 + (c_{32} - c_{12}c_{31})c_{23}$$

that is

$$c_{22} < 1 + c_{32}c_{23} + c_{12}(c_{21} - c_{31}c_{23}).$$

Hence, $c_{12}(c_{21} - c_{31}c_{23}) \neq 0$. But if $c_{12} \neq 0$ then rad P_1 is a direct sum of copies of P_3 since (e_1, e_2, e_3) is a heredity sequence, and thus $c_{21}=c_{31}c_{23}$, a contradiction.

(d) Finally, let us consider the case when J = Ae_1A and c_{31}=0. Then the radical rad P_1 is a direct sum of copies of S_2, and since (e_1, e_2, e_3) is a heredity sequence, rad P_2 is a direct sum of copies of P_3. But then A/J is obviously quasi-hereditary.

This completes the proof of Proposition.

Note: While preparing the manuscript I learned that A. Wiedemann has also studied the quotients of quasi-hereditary algebras and that in [5] he gives an example of a quasi-hereditary algebra with five simple types such that its factor modulo a heredity ideal is not quasi-hereditary.

REFERENCES

[1] E. Cline, B. Parshall and. L.L. Scott: Finite dimensional algebras and heighest weight categories, *J. Reine Angew. Math.* 391 (1988), 85-99.

[2] V. Dlab: The heredity measure of an algebra, to appear in *Bull. Austral. Math. Soc.* 40 (1989).

[3] V. Dlab and C.M. Ringel: Quasi-hereditary algebras, to appear in *Ill. J. Math.* 33 (1989)

[4] V. Dlab and C.M. Ringel: The dimension of a quasi-hereditary algebra, to appear in *Proc. Banach Centre, Warszawa,* 1989.

[5] A. Wiedemann: Quotients of quasi-hereditary algebras, preprint

[6] K. Yamagata: Letter to V. Dlab (March 16, 1988.)

Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario
Canada, K1S 5B6

Recieved March 15, 1989

ON THE COMPLETE CONGRUENCE LATTICE OF A COMPLETE LATTICE WITH AN APPLICATION TO UNIVERSAL ALGEBRA

G. Grätzer, F.R.S.C.

Abstract. It is proved that every complete lattice is isomorphic to the lattice of complete congruence relations of a suitable complete lattice. This is then applied to obtain a direct proof of the independence of the congruence lattice, the subalgebra lattice, and the automorphism group of an infinitary algebra, due to W. A. Lampe and the author.

The following result was conjectured by R. Wille in 1983 (see K. Reuter and R. Wille [10]):

THEOREM 1. *Every complete lattice L isomorphic to the lattice of complete congruence relations of a suitable complete lattice K.*

For a finite lattice L, this was proved by S.-K. Teo [11].

A closely related question was raised in G. Birkhoff [1] in 1945: Is every complete lattice isomorphic to the lattice of congruence relations of a suitable (infinitary) algebra? In 1948, G. Birkhoff restated this question in [2] for finitary algebras.

The finitary problem was solved in G. Grätzer and E. T. Schmidt [5]. Some alternative proofs appeared: W. A. Lampe [6], P. Pudlák [8], E. T. Schmidt [9]; however, none provided a direct construction.

G. Grätzer and W. A. Lampe dealt with the infinitary case in 1971–1972, and obtained, in particular, an affirmative answer to Birkhoff's 1945 question. Since the algebra to be constructed was infinitary, the two step transfinite construction of the finitary case became even more complex, see Appendix 7 of [4] for full details; see also E. Nelson [7].

As an application of Theorem 1, we prove a result of G. Grätzer and W. A. Lampe, *loc.cit.*, on the independence of the related structures of an infinitary algebra:

THEOREM 2. *Let L_c and L_s be complete lattices with more than one element, and let G be a group. Then there exists an infinitary algebra $\mathfrak{A}$ such that the congruence lattice of $\mathfrak{A}$ is isomorphic to L_c, the subalgebra lattice of $\mathfrak{A}$ is isomorphic to L_s, and the automorphism group of $\mathfrak{A}$ is isomorphic to G.*

PROOF[1] OF THEOREM 1: A *coloring* of a chain C is a map φ from the prime intervals of C to $L - \{0\}$. Following S.-K. Teo [11], for a chain C and coloring φ, we define the lattice $C(\varphi)$ as follows: the lattice $C(\varphi)$ is C^2 augmented with the elements $m(\mathfrak{p}_1, \mathfrak{p}_2)$ whenever $\mathfrak{p}_1 = [x_1, y_1]$ and $\mathfrak{p}_2 = [x_2, y_2]$ are prime intervals of C and $\mathfrak{p}_1\varphi = \mathfrak{p}_2\varphi$; we require that the elements $\langle x_1, x_2\rangle, \langle x_1, y_2\rangle, \langle y_1, x_1\rangle, \langle y_1, y_2\rangle, m(\mathfrak{p}_1, \mathfrak{p}_2)$ form a sublattice of $C(\varphi)$ isomorphic to $\mathfrak{M}_3$.

This research was supported by the NSERC of Canada.

[1] This outline is based on a proof by the author and H. Lakser; it is much simpler than the original proof.

L is the complete lattice we want to represent. We shall be dealing with subsets

$$X \subseteq L - \{0\} \text{ with } |X| > 1.$$

Let

$$X = \{x_\gamma \mid \gamma < \zeta^X\}, \text{ where } 1 < \zeta^X \leq \zeta = |L - \{0\}|.$$

Let $\{X^\delta \mid \delta < \chi\}$ denote the family of all such sets; we write $X^\delta = \{x_\gamma^\delta \mid \gamma < \zeta^\delta\}$.

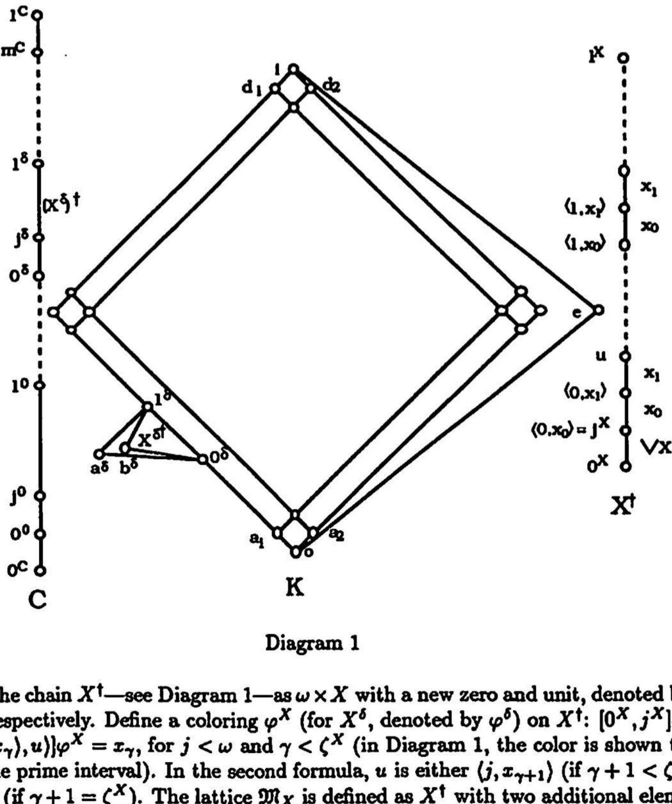


Diagram 1

Define the chain $X^\dagger$—see Diagram 1—as $\omega \times X$ with a new zero and unit, denoted by 0^X and 1^X, respectively. Define a coloring φ^X (for X^δ, denoted by φ^δ) on $X^\dagger$: $[0^X, j^X]\varphi^X = \bigvee X$; $[\langle j, x_\gamma\rangle, u)]\varphi^X = x_\gamma$, for $j < \omega$ and $\gamma < \zeta^X$ (in Diagram 1, the color is shown to the right of the prime interval). In the second formula, u is either $\langle j, x_{\gamma+1}\rangle$ (if $\gamma + 1 < \zeta^X$) or $\langle j+1, x_0\rangle$ (if $\gamma + 1 = \zeta^X$). The lattice $\mathfrak{M}_X$ is defined as $X^\dagger$ with two additional elements: a^X and b^X (for X^δ, a^δ and b^δ); $X^\dagger$ is a complete sublattice of $\mathfrak{M}_X$, and $0^X \prec a^X \prec 1^X, 0^X \prec b^X \prec 1^X$.

For every X^δ, $\delta < \chi$, we construct the chain $(X^\delta)^\dagger$, and form $\Sigma\{(X^\delta)^\dagger \mid \delta < \chi\}$, the ordinal sum of these chains . We obtain the chain C—see Diagram 1—by adding a zero and unit element, and a new dual atom, 0^C, 1^C, and m^C, respectively.

We define a coloring φ of C; for a prime interval $\mathfrak{p}$ of C, let $\mathfrak{p}\varphi = \mathfrak{p}\varphi^{\delta}$ if $\mathfrak{p}$ is a prime interval of X^{δ} for some $\delta < \chi$; otherwise, let $\mathfrak{p}\varphi = 1$.

Now define the lattice K—see Diagram 1—as $C(\varphi)$ augmented with the elements a^{δ} and b^{δ} for $\delta < \chi$, and the element e so that a^{δ}, b^{δ}, and $X^{\delta} \times \{0^C\}$ form a sublattice isomorphic to $\mathfrak{M}_{X^{\delta}}$, and e is a common complement of all elements (excepting the zero o and the unit i).

For $x \in L - \{0, 1\}$, and for $v, w \in C$, $v \leq w$, define a binary relation Φ^x on C as follows:

$$v \equiv w \pmod{\Phi^x} \text{ iff } \mathfrak{p}\varphi \leq x \text{ for every prime interval } \mathfrak{p} \in [v, w].$$

Obviously, Φ^x is a complete congruence on C and $(\Phi^x)^2$ as a congruence on C^2 uniquely extends to a complete congruence Θ^x on $C(\varphi)$.

For $x = 0$, let $\Theta^0 = \omega$, the zero congruence; for $x = 1$, let $\Theta^1 = \iota$, the unit congruence. Then $x \to \Theta^x$ is an isomorphism between L and the lattice of complete congruences of K, establishing Theorem 1.

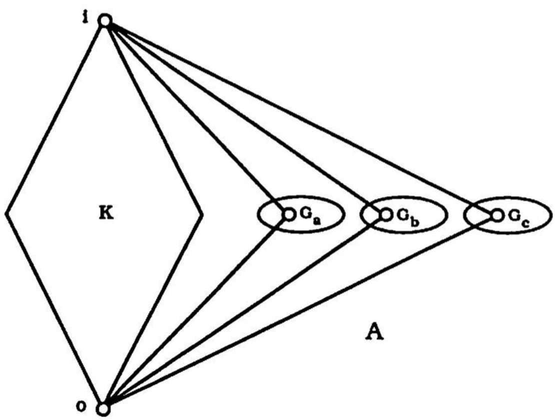


Diagram 2

PROOF OF THEOREM 2: Let $A = K \cup ((L_s - \{0\}) \times G)$—see Diagram 2—where K is the lattice of Theorem 1 for L_c. We make A into a complete lattice by extending the partial ordering of K: $o \prec \langle a, g\rangle \prec i$. The algebra $\mathfrak{A}$ is this complete lattice with the following additional operations: (i) for all $k \in K$, anullary operation k; (ii)for all $h \in G$, a unary operation f_h defined by $f_h(\langle a, g\rangle) = \langle a, hg\rangle$ for $b \in L - \{0\}$, $g \in G$, and $f_h(k) = o$ for $k \in K$; (iii) for all $a, b \in L_s - \{0\}$, a unary operation $f_{a,b}$, $a \leq b$, defined by $f_{a,b}(\langle b, g\rangle) = \langle a, g\rangle$ for $g \in G$, and $f_{a,b}(x) = o$, otherwise; (iv) an infinitary operation Σ: $\Sigma(X \times \{g\}) = \langle \bigvee X, g\rangle$ for $X \subseteq L_s - \{0\}$, $g \in G$, and $\Sigma(Y) = o$ otherwise.

The congruences of $\mathfrak{A}$ are the complete congruences of K trivially extended to $\mathfrak{A}$. The subalgebras of $\mathfrak{A}$ are $S_a = K \cup \{\langle b, g\rangle \mid b \leq a\}$, for $a \in L_s$. The automorphisms are α_h, for $h \in G$, defined by $k\alpha_h = k$, for $k \in K$ and $\langle b, g\rangle\alpha_h = \langle b, gh\rangle$. Thus Theorem 2 follows.

REFERENCES

1. G. Birkhoff, *Universal Algebra*, in "Proc. First Canadian Math. Congress, Montreal, 1945. University of Toronto Press, Toronto," 1946, pp. 310–326.
2. G. Birkhoff, "Lattice Theory," Amer. Math. Soc. Colloq. Publ. vol. 25, revised edition. Amer. Math. Soc., New York, N. Y., 1948.
3. G. Grätzer, "General Lattice Theory," Academic Press, New York, N. Y; Birkhäuser Verlag, Basel; Akademie Verlag, Berlin, 1978.
4. G. Grätzer, "Universal Algebra. Second Edition," Springer Verlag, New York, Heidelberg, Berlin, 1979.
5. G. Grätzer and E. T. Schmidt, *Characterizations of congruence lattices of abstract algebras*, Acta Sci. Math. (Szeged) 24 (1963), 34–59.
6. W. A. Lampe, *On the congruence lattice characterization theorem*, Trans. Amer. Math. Soc. 182 (1973), 43–60.
7. E. Nelson, *The Independence of the Subalgebra Lattice, Congruence Lattice, and Automorphism Group of an Infinitary Algebra*, J. Pure and Appl. Alg. 17 (1980), 187–201.
8. P. Pudlák, *A new proof of the congruence lattice representation theorem*, Algebra Universalis 6 (1976), 269–275.
9. E. T. Schmidt, "Kongruenzrelationen algebraischer Strukturen," Math. Forschungberichte, XXV. VEB Deutcher Verlag der Wissenschaften, Berlin, 1967.
10. K. Reuter and R. Wille, *Complete congruence relations of complete lattices*, Acta Sci. Math. (Szeged) 51 (1987), 319–327.
11. S.-K. Teo, *Representing finite lattices as complete congruence lattices of complete lattices*, Abstracts of papers presented to the Amer. Math. Soc. 88T-06-207.

Keywords. Complete lattice, congruence lattice, complete congruence, infinitary universal algebra, subalgebra lattice, automorphism group.
1980 *Mathematics subject classifications*: Primary 08A65, 06A23; Secondary 08A30, 06B10.

Department of Mathematics
University of Manitoba
Winnipeg, Man. R3T 2N2
Canada

Received April 1, 1989

Totally Integrally Closed Rings of Continuous Functions and Rings of Quotients

R. Macoosh and R. Raphael

Presented by J. Lambek, F.R.S.C.

Abstract

A commutative ring R is called totally integrally closed [1] if for any ring homomorphism $\alpha : S \to R$ and any integral extension T of S there is a homomorphism $T \to R$ extending α. For X a completely regular Hausdorff space, Hochster [4] proved that the following are equivalent:

(a). X is extremally disconnected,

(b). $C(X)[i]$ is totally integrally closed,

(c). $C^*(X)[i]$ is totally integrally closed.

Hochster's proof is topological and lengthy and so it is interesting to observe that the same result follows more easily from the theory of rings of quotients.

Let $R \subset S$ be commutative rings with the same identity. S is an essential extension of R if every nonzero ideal of S has nonzero contraction to R. If S is essential and integral over R then S is called an algebraic extension of R [6, 2.1]. A ring with no proper algebraic extension is said to be algebraically closed. Algebraically closed rings coincide with totally integrally closed rings and must be semiprime [1, p. 702] and [6, pp. 1142–1143]. If R is semiprime then R has an algebraic closure $\Omega(R)$, an algebraically closed algebraic extension of R that is unique up to isomorphism over R. Rings of quotients arise in this context, for example:

Proposition 1 [6, 2.10]. If R is semiprime then $\Omega(R)$ is the integral closure of R in $\Omega(Q(R))$, where $Q(R)$ denotes the complete ring of quotients of R.

We now consider function rings. As usual, X will be completely regular, $C(X)$ is the ring of continuous real-valued functions on X, $B(C(X))$ is the algebra of idempotents of $C(X)$ and $C(X)[i]$ will be the ring of continuous complex-valued functions on X.

The complete ring of quotients of $C(X)$, denoted $Q(X)$, is studied in [2]. There $Q(X)$ is represented as the set of all continuous real-valued functions on X modulo a natural equivalence relation. We shall need two results from [2].

Proposition 2 (a). A dense open subset V of X induces a natural monomorphism $C(X) \to C(V)$ (p. 10). (b). $B(C(X)) = B(Q(X))$ precisely when X is extremally disconnected (p. 91).

Proposition 3. The following are equivalent:

(a). X is extremally disconnected,

(b). $C(X)$ is integrally closed in $Q(X)$,

(c). $C^*(X)$ is integrally closed in $Q(X)$.

Proof. (a) ⇒ (b). Suppose X is extremally disconnected. Let $f \in Q(X)$, then $f \in C(V)$ for some dense open V and $f^2 + 1 \in C(V)$ is a unit. If f is integral over $C(X)$ then so is $f^2 + 1$ and we have an equation

$$(f^2+1)^n + g_1(f^2+1)^{n-1} + \ldots + g_n = 0, \quad g_i \in C(X). \tag{1}$$

Multiplication of (1) by $1/(f^2+1)^n$ yields

$$1 + \frac{g_1}{(f^2+1)} + \ldots + \frac{g_n}{(f^2+1)^n} = 0$$

from which we obtain after rearranging terms

$$\frac{1}{(f^2+1)}\left[g_1 + \ldots + \frac{g_n}{(f^2+1)^{n-1}}\right] = -1.$$

Since $1/(f^2+1)$ is bounded it has an extension to a function h in $C(X)$ [3, 1H] so that $-(g_1 + \ldots + g_n h^{n-1}) \in C(X)$ agrees on V with $f^2 + 1$. As well, $f/(f^2+1) \in C(V)$ is bounded and hence has an extension h' in $C(X)$. Therefore $-(g_1 + \ldots + g_n h^{n-1})h'$ is in $C(X)$ and agrees on V with f.

(b) ⇒ (c). It is easy to see that $C^*(X)$ is integrally closed in $C(X)$ and hence that (c) follows from (b).

(c) ⇒ (a). If $C^*(X)$ is integrally closed in $Q(X)$ then all the idempotents of $Q(X)$ lie in $C^*(X)$ and Proposition 2(b) applies. □

Proposition 4. The following are equivalent:

(a). X is extremally disconnected,

(b). $C(X)[i]$ is totally integrally closed,

(c). $C^*(X)[i]$ is totally integrally closed.

Proof. (a) ⇒ (b). Clearly $C(X)[i]$ is algebraic over $C(X)$. For X extremally disconnected we show $C(X)[i] = \Omega(C(X))$. By Proposition 1, $\Omega(C(X))$ is the integral closure of $C(X)$ in $\Omega(Q(X))$. By [6, 6.1] the elements of $\Omega(Q(X))$ have the form $f + gi$ with $f, g \in Q(X)$. If $f + gi$ is integral over $C(X)$ each of f, g is integral over $C(X)$ so that f and g belong to $C(X)$ by Proposition 3.

(b) ⇒ (c). As Hochster remarks this is true because it is easily seen that $C^*(X)[i]$ is integrally closed in $C(X)[i]$.

(c) ⇒ (a). Let S denote the integral closure of $C^*(X)$ in $Q(X)$. Then $B(S) = B(Q(X))$. If $C^*(X)[i]$ is totally integrally closed then $C^*(X)[i]$ contains a copy of S because S is a ring of quotients of $C^*(X)$. Therefore $B(C^*(X)) = B(Q(X))$ and we apply Proposition 2(b). □

References

[1] E. Enochs, *Totally integrally closed rings*, Proc. Amer. Math. Soc., 19 (1968), 701–706.

[2] N. J. Fine, L. Gillman and J. Lambek, Rings of Quotients of Rings of Functions, McGill University Press, Montréal, 1965.

[3] L. Gillman and M. Jerison, Rings of Continuous Functions, Springer–Verlag, New York, 1976.

[4] M. Hochster, *Rings of continuous functions and totally integrally closed rings*, Proc. Amer. Math. Soc., 25 (1970), 439–442.

[5] J. Lambek, Lectures on Rings and Modules, Chelsea Publ. Co., New York, 1986.

[6] R. Raphael, *Algebraic extensions of commutative regular rings*, Cdn. Jour. Math., 22 (1970), 1133–1155.

Department of Mathematics
Concordia University
Loyola Campus
7141 Sherbrooke St. W.
Montreal, Québec
H4B 1R6

Received April 13, 1989

Mailing Addresses

1. I. Ágoston
Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada K1S 5B6

2. P.-G. Becker
Mathem. Institut der Universität zu Köln
Weyertal 86-90
D-5000 Köln 41, West Germany

3. G. Grätzer
Department of Mathematics
University of Manitoba
Winnipeg, Manitoba, Canada R3T 2N2

4. I.R. Hentzel
Department of Mathematics
Iowa State University
Ames, Iowa 50011 U.S.A.

5. D.P. Jacobs
Department of Computer Science
Clemson University
Clemson, South Carolina 29634-1906 U.S.A.

6. J.L. Lambert
Département do Mathématique et Informatique
Centre Scientifique et Polytechnique
Université de Paris-Nord
Avenue Jean-Baptiste Clément
93 430 Villetaneuse, France

7. R. Macoosh
Department of Mathematics
Concordia University - Loyola Campus
7141 Sherbrooke St. W.
Montreal, Quebec, Canada H4B 1R6

8. K. Nishioka
Department of Mathematics
Nara Women's University
Kita-Uoya Nishimachi, Nara 630, Japan

9. R. Raphael
Department of Mathematics
Concordia University - Loyola Campus
7141 Sherbrooke St. W.
Montréal, Québec, Canada H4B 1R6

10. Á. Száz
Department of Mathematics
Lajos Kossuth University
H-4010 Debrecen, Hungary