Commentationes Mathematicae Universitatis Carolinae

Pavol Zlatoš

On the ring of the variety of algebras over a ring

Commentationes Mathematicae Universitatis Carolinae, Vol. 24 (1983), No. 2, 325--334

Persistent URL: http://dml.cz/dmlcz/106230

Terms of use:

© Charles University in Prague, Faculty of Mathematics and Physics, 1983

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://project.dml.cz

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE
24,2(1983)

ON THE RING OF THE VARIETY OF ALGEBRAS OVER A RING

PAVOL ZLATOŠ

Abstract: Using the tools of the commutator theory we can assign to every congruence modular variety V of universal algebras a ring R(V), reducing the study of many properties of algebras in V to the study of modules over R(V). In the present paper R(V) is computed for the varieties of all algebras and all commutative algebras over a commutative ring A.

Key words: Congruence modular variety, commutator, ring of a variety, algebra over a ring.

Classification: Primary 08B10, 13C99, 16A06
Secondary 08A30, 16A89

In [2], for every congruence modular variety V of universal algebras, a ring R(V) is constructed in such a way that each block of an Abelian congruence of any algebra in V naturally becomes a module over R(V). In particular, each Abelian algebra in V becomes a module over R(V). (All rings and algebras over rings are assumed to be associative. Throughout the whole paper - except the last section - a ring always means a ring with unit 1 which has to be preserved by ring homomorphisms, a module over a ring A is always a left, unitary module over A and an algebra over a commutative ring A is always a left, unitary algebra over A.)

Further, V is congruence distributive iff R(V) is trivial, i.e. R(V) can serve as a measure of nondistributivity of V. The construction of R(V) preserves the equivalence of varieties as well, i.e. if V and W are equivalent varieties (equivalent means "having the same terms" - see e.g. [3], Appendix 3) then the rings R(V) and R(W) are isomorphic. This fact will be employed quite often in the present paper.

For the variety Mod A of modules over a ring A, one obtains the expected isomorphism R(Mod A) $\cong$ A as immediately follows by an easy computation from the definition of R(V). In any variety V the Abelian algebras constitute a subvariety Va, R(Va) is in general a homomorphic image of R(V) and the variety Mod R(Va) is equivalent to the variety obtained from Va by picking one element as 0 in each algebra in Va. This enables us to reduce many questions on Abelian varieties to the study of varieties of modules (see [2] for applications as well as for all the notions carrying the predicate "Abelian").

From the fact that R(Mod A) $\cong$ A naturally arises the question what does R(V) look like for the varieties Alg A and CAlg A of all algebras and all commutative algebras, respectively, over a commutative ring A. This question is answered in the following

<u>Theorem</u>. Let A be a commutative ring. Then

(i) R(CAlg A) $\cong$ A[x] and

(ii) R(Alg A) $\cong$ A[x,y].

The authors formulated the following problem in [2]:

"Compute R(Groups) and R(Commutative rings)."

The answer to the second question is a part of the Corollary to the Theorem, since the variety of commutative rings is equivalent to CAlg Z and so does the variety of all rings to Alg Z (Z is the ring of integers).

<u>Corollary</u>. (i) R(Commutative rings) $\cong$ Z[x] and
(ii) R(Rings) $\cong$ Z[x,y].

The first question of the problem was answered by B. Sivák [6] who computed R(V) for a large class of varieties of groups. In particular, he proved R(Groups) = $Z[x,x^{-1}]$.

1. <u>Preliminaries</u>. We follow the terminology and denotation of [2], cf. also [3]. For fundamentals concerning the commutator theory either [2] or [4] can serve as the most facile guide. Instead of repeating the general definition of the ring R(V) of a congruence modular variety V, we are going to describe its construction only for V s possessing terms +, - and 0 of usual arities defining the group structure on every member of V. This special case enables us to give a slightly easier definition, nevertheless, sufficient for our purpose. The isomorphism with the product of the original definition in [2] can be easily verified.

Let F(x,y) be the free algebra over two generators x and y in V. Cg(x,y) is the principal congruence identifying x and y, and P(V) is the coset of 0 in Cg(x,y), i.e. P(V) consists of all binary terms r satisfying the identity r(x,x) = 0 in V. Let us introduce a binary operation $\Diamond$ on P(V) by

$$r \Diamond s = r(s + y, y)$$

(The noncommon symbol for the multiplication $\Diamond$ is used to distinguish it from the ordinary ring multiplication.) One can easily verify that $\diamond$ is well defined, associative, has $e = x - y$ as unit and satisfies the right distributive law with respect to the addition +. Now let K be the restriction of the commutator congruence $[Cg(x,y), Cg(x,y)]$ to the set P(V). The fact that K preserves + and - is trivial. From the properties of the commutator (see [2]) it follows that K preserves $\diamond$, too. Hence, K is a congruence of $\langle P(V); +, -, 0, \diamond, e\rangle$. We refer to [2] again for the proof that the additive group of the quotient P(V)/K is already Abelian and the left distributive law is also satisfied. Hence, by factorization of P(V) modulo K a ring $R(V) = \langle R(V); +, -, 0, \diamond, e\rangle$ together with the canonical homomorphism $p: P(V) \longrightarrow R(V)$ is obtained.

Let A be a commutative ring. A[x] is its polynomial ring in one variable x, A[x,y] is its polynomial ring in two commuting variables x and y, i.e. A[x,y] consists of all formal finite sums of the form $\sum a(i,j).x^i.y^j$ where $a(i,j) \in A$. $A\langle x,y\rangle$ denotes the polynomial ring over A in two noncommuting variables x and y, i.e. $A\langle x,y\rangle$ consists of all formal finite sums of the form $\sum a(w).w$, where $a(w) \in A$ and w runs over the set $\{x,y\}^*$ of all finite words in the two-element alphabet x, y. The crucial fact is that the free commutative A-algebra with two generators is isomorphic to A[x,y] and the free A-algebra with two generators is isomorphic to $A\langle x,y\rangle$.

We presuppose some standard knowledge on tensor products of modules and algebras over a commutative ring (see e.g. [1]). The tensor product sign $\otimes$ always denotes the tensor product over a fixed commutative ring A. The omitting of the index A in $\otimes_A$ hardly can cause any confusion. We summarize all the facts needed in the following

<u>Lemma</u>. Let A be a commutative ring.

(a) $A[x] \otimes A[y] \cong A[x,y]$.

(b) $A[x]$ is free as an A-module over $\{x\}^*$ and so is $A\langle x,y\rangle$ over $\{x,y\}^*$ hence both are A-flat.

(c) Let $i:M' \longrightarrow M$, $j:N' \longrightarrow N$ be injective homomorphisms of A-modules, with M, N′ flat. Then $i \otimes j:M' \otimes N' \longrightarrow M \otimes N$ is injective, too.

(d) Let $f:M \longrightarrow M''$, $g:N \longrightarrow N''$ be surjective homomorphisms of A-modules.

(i) $f \otimes g:M \otimes N \longrightarrow M'' \otimes N''$ is surjective, too, and its kernel is generated by all elements $u \otimes v \in M \otimes N$ such that $u \in \mathrm{Ker}\, f$ or $v \in \mathrm{Ker}\, g$.

(ii) If both M, N are A-flat then $\mathrm{Ker}\, f \otimes g = \mathrm{Ker}\, f \otimes N + M \otimes \mathrm{Ker}\, g$ since both summands can be considered as subnodules of $M \otimes N$.

The Lemma will be employed in the next section without any explicit referring to it.

2. <u>Proof of the result</u>. The idea of the proof consists in producing some homomorphisms between Abelian groups, some of them equipped with a multiplication $\diamond$ possessing a unit element e and in additional definition of $\diamond$ on the remaining ones in such a way that the considered homomorphisms will preserve both $\diamond$ and e. Then by factorization one obtains the desired isomorphisms.

Though (i) can be deduced by an easy reasoning as a corollary to the proof of (ii), we prefer to give first the more transparent proof of (i) separately, and only after it modify its idea to the more general case (ii).

<u>Proof of (i)</u>: The free commutative A-algebra with two generators is isomorphic to $A[x,y]$. The congruence $Cg(x,y)$ is represented by the principal ideal $(x - y)$ which serves also as a carrier of $P(\mathrm{Calg}\ A)$, and the commutator $[Cg(x,y), Cg(x,y)]$ corresponds to the principal ideal $((x - y).(x - y))$. The mapping $f: A[x,y] \longrightarrow P(\mathrm{CAlg}\ A)$ given by $f(r) = r.(x - y)$ is a homomorphism of Abelian groups. Let us define $\diamond$ on $A[x,y]$ by

$$r \diamond s = r(f(s) + y, y).s.$$

Then $\diamond$ is a binary operation on $A[x,y]$ with unit $e = 1$ and both $\diamond$ and e are preserved by f. The composition $p \circ f$ is a surjective homomorphism of Abelian groups preserving $\diamond$ and e with kernel $(x - y)$. Now, the group endomorphism $r \mapsto r(x,x)$ of $A[x,y]$ has the same kernel and its range is $A[x]$. But $\diamond$ coincides with the common multiplication on $A[x]$ and both $\diamond$ and e are preserved by this endomorphism. This completes the proof (see Diagram 1).

$$\begin{array}{ccc} A[x,y] & \xrightarrow{\quad f \quad} & P(\mathrm{CAlg}\ A) \\ \downarrow & & \downarrow p \\ A[x] & \overset{\sim}{=\!=\!=} & R(\mathrm{CAlg}\ A) \end{array}$$

Diagram 1.

<u>Proof of (ii)</u>: The free algebra on two generators over A is isomorphic to $A\langle x,y\rangle$. The mapping $g: A\langle x,y\rangle \times A\langle x,y\rangle \longrightarrow$ $\longrightarrow P(\mathrm{Alg}\ A)$ given by $g(r,s) = r.(x - y).s$ is A-bilinear hence inducing a group homomorphism $f: A\langle x,y\rangle \otimes A\langle x,y\rangle \longrightarrow P(\mathrm{Alg}\ A)$. Let us define $\diamond$ on $A\langle x,y\rangle \otimes A\langle x,y\rangle$ by extension of

$$r \otimes s \diamond t \otimes u = r(g(t,u) + y, y).t \otimes u.s(g(t,u) + y, y)$$

forced by the right distributive law and by

$r \otimes s \diamond (t \otimes u + v \otimes w) =$

$$r(g(t,u) + g(v,w) + y,y).t \otimes u.s(g(t,u) + g(v,w) + y,y)$$
$$+ r(g(t,u) + g(v,w) + y,y).v \otimes w.s(g(t,u) + g(v,w) + y,y).$$

$\diamond$ is again a binary operation on $A\langle x,y\rangle \otimes A\langle x,y\rangle$ with unit $e = 1$ and both $\diamond$ and e are preserved by f. The composition $p \circ f$ is a surjective homomorphism of Abelian groups preserving $\diamond$ and e as well. Its kernel is the ideal $(x - y) \otimes \otimes A\langle x,y\rangle + A\langle x,y\rangle \otimes (x - y)$ i.e. the same as the kernel of the group endomorphism of $A\langle x,y\rangle \otimes A\langle x,y\rangle$ given by the extension of $r \otimes s \mapsto r(x,x) \otimes s(y,y)$. Its range is $A[x] \otimes A[y]$ considered as a subalgebra of $A\langle x,y\rangle \otimes A\langle x,y\rangle$. But $\diamond$ coincides with the common multiplication on $A[x] \otimes A[y]$ and is preserved by the endomorphism as well as e. The isomorphism $A[x] \otimes \otimes A[y] \cong A[x,y]$ completes the proof (see Diagram 2).

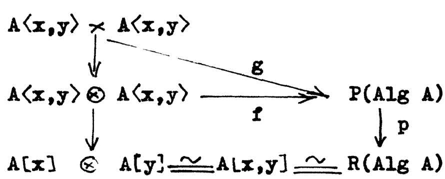

Diagram 2.

<u>Remark</u>. One can ask whether (ii) cannot be proved in an essentially simpler manner avoiding the use of tensor products, since neither the formulation of the problem nor the result contain a reference to it.

3. <u>Filling some gaps</u>. In this last section we are going to acquit our debt consisting in ignoring of some classes of

rings, modules and algebras. In most cases we reduce them to the previous results. The facts stated below (except (C)) follow either from the observation that equivalent varieties have isomorphic rings or from an easy computation (including (C)) modifying the proof of the Theorem if necessary.

(A) Bimodules. Let A and B be two rings (with unit). The variety Mod A-B of (unitary) A-left B-right bimodules is equivalent to Mod $A \otimes_Z B$, hence $R(\text{Mod } A\text{-}B) \cong A \otimes_Z B$.

(B) Algebras over noncommutative rings. Let A be a ring (with unit). Let C be its largest commutative quotient. (One has to factorize A modulo the ideal generated by all elements of the form a.b - b.a in A.) The varieties Alg A and Alg C are equivalent, hence $R(\text{Alg } A) \cong C[x,y]$. Similarly in the case of commutative algebras over A one obtains $R(\text{CAlg}) \cong C[x]$.

(C) Algebras without unit. Let A be a commutative ring with unit. Let Alg′A (CAlg′A) be the variety of all (commutative) unitary algebras over A in general without unit. Then $R(\text{Alg}'A) \cong R(\text{Alg } A) \cong A[x,y]$ and $R(\text{CAlg}'A) \cong R(\text{CAlg } A) \cong A[x]$. The isomorphism indicated follows from the fact that the principal ideal (x - y) in $A\langle x,y\rangle$ (A[x,y]) is contained in the ideal (x) + (y) the last being isomorphic to the free algebra over two generators in Alg′A (CAlg′A). Details are left to the reader.

(D) Modules over rings without unit. Let $A = \langle A;+,-,0,.\rangle$ be a ring (in general without unit) and Md A is the variety of (in general nonunitary) modules over A. Let $Z \times A$ be the extension of A to a ring with unit. The additive group structure is defined componentwise and $\langle 1,0\rangle$ serves as a unit for multiplication given by

$$\langle m,a\rangle.\langle n,b\rangle = \langle mn, mb + na + a.b\rangle$$

(see e.g. [5]). Again the equivalence of varieties Md A and Mod $Z \times A$ of unitary modules over $Z \times A$ implies the ring isomorphism $R(\text{Md } A) \cong Z \times A$. This shows that the transition from Md A to Mod R(Md A) presents the effect of unitarization.

(E) Algebras over rings without unit. Similarly as in the previous case the variety Ag A of (in general nonunitary) algebras over A is equivalent to the variety Alg $Z \times A$ of unitary algebras over $Z \times A$. The same argument works in the commutative case. Hence $R(\text{CAg } A) \cong (Z \times A)[x]$ and $R(\text{Ag } A) \cong (Z \times A)[x,y]$.

Some further results can be obtained combining (A) - (E).

R e f e r e n c e s

[1] C. FAITH: Algebra: Rings, Modules and Categories I, Springer-Verlag, Berlin-Heidelberg-New York, 1973.

[2] R.S. FREESE and R.N. MCKENZIE: The commutator, an overview, preprint, 1981.

[3] G. GRÄTZER: Universal Algebra, 2 nd edition, Springer-Verlag, New York-Heidelberg-Berlin, 1979.

[4] H.P. GUMM: Geometrical methods in congruence modular algebras, preprint, Darmstadt, 1981.

[5] N.H. MCCOY: The theory of rings, MacMillan, New York, 1964.

[6] B. SIVÁK: On the ring of some varieties of groups, in preparation.

Katedra algebry a teórie čísel, Matematicko-fyzikálna fakulta
Univerzity Komenského
Mlynská dolina
842 15 Bratislava
Czechoslovakia

(Oblatum 11.4. 1983)