The Australian National University

ON THE RINGS ASSIGNED TO VARIETIES OF GROUPS OR RINGS

L. G. KOVÁCS

RESEARCH REPORT NO. 40 - 1985

DEPARTMENT OF MATHEMATICS, IAS

Mathematical Sciences Research Centre

Austral. Nat. Univ. MSRC Research Report No. 40 - 1985

AMS Classification: 08 B 10,
20 E 10

On the rings assigned to varieties of groups or rings

L. G. Kovács

1. Introduction

In §9 of an unpublished but much quoted preprint [2], Freese and McKenzie defined an (associative) ring $R(\mathcal{V})$ to each congruence-modular variety $\mathcal{V}$. Further, for any abelian congruence β of an algebra A in $\mathcal{V}$, and for each element a of A, they defined an $R(\mathcal{V})$-module structure on the β-class of a (in which a plays the role of zero). Their Problem 9.5 asks: calculate $R(\mathcal{V})$ when $\mathcal{V}$ is the variety of all groups or the variety of all (associative) rings. In a very recent paper [4], Sivák answered (in effect) that in the first case $R(\mathcal{V})$ is the integral group ring of the infinite cyclic group. Another proof of this result will be given here, and it will be noted that a generator of this cyclic group acts on the β-class of a as (group) conjugation by a. For the second case of Problem 9.5, it will be shown that then $R(\mathcal{V})$ is the ring of all polynomials in two (commuting) indeterminates with integer coefficients. Further, on the β-class of a one indeterminate acts as $a + b \mapsto a + ab$ and the other as $a + b \mapsto a + ba$ (where b ranges through the ideal associated with β). The concluding section will contain remarks on $R(\mathcal{V})$ when $\mathcal{V}$ is an arbitrary variety of groups.

2. Preliminaries

For notation and terminology in general, the reader is referred to Freese and McKenzie [2].

We must recall the definition of $R(\mathcal{V})$ and of its action. Let F be the free algebra of $\mathcal{V}$ freely generated by u and v; denote by γ the smallest congruence on F such that $(u, v) \in \gamma$, and by π the natural homomorphism of F onto $F/[\gamma, \gamma]$; let $\pi(\gamma)$ be the congruence on $\pi(F)$ corresponding to γ. The elements of $R(\mathcal{V})$ are to be the elements of the $\pi(\gamma)$-class of $\pi(v)$.

For any algebra A in $\mathcal{V}$ and for any $a, b \in A$, let $\varphi_{a,b}$ denote the homomorphism of F into A which maps u to a and v to b. Let d denote a ternary difference term of $\mathcal{V}$. Write addition and multiplication in $R(\mathcal{V})$ as $\oplus$ and $\otimes$, to distinguish them from the corresponding operation(s) in $\mathcal{V}$. Then

$$\pi(r) \oplus \pi(s) = \pi(d(r, v, s))$$

and

$$\pi(r) \otimes \pi(s) = \varphi_{\pi(s),\, \pi(v)}(r)$$

for all $\pi(r)$, $\pi(s)$ in $R(\mathcal{V})$. It was shown by Freese and McKenzie (loc. cit.) that $\oplus$ and $\otimes$ are well defined by these equations, do not depend on the choice of d, and make $R(\mathcal{V})$ into an associative ring with $\pi(v)$ as zero and $\pi(u)$ as 1.

Further, if β is an abelian congruence on an algebra A in $\mathcal{V}$ and if $a \in A$, then the β-class of a is a left $R(\mathcal{V})$-module with respect to

$$a' \oplus a'' = d(a', a, a'')$$

and

$$\pi(r) \otimes a' = \varphi_{a',\, a}(r)$$

[for all (a, a'), (a, a'') in β and $\pi(r)$ in $R(V)$]. In this module a plays the role of zero.

As is well known, for any variety V of groups one may choose d as $d(x, y, z) = xy^{-1}z$, while for a V consisting of rings d may be taken as $d(x, y, z) = x - y + z$. A congruence on a group or ring is abelian if its kernel is a commutative group or a zeroring, respectively.

3. Groups

Let V be the variety of all groups, an let d be chosen as above. Then γ is the congruence modulo the normal closure, say N, of $v^{-1}u$ in F, and $\pi(F)$ is the quotient of F modulo the commutator subgroup N' of N. Set $w = v^{-1}u$; note that w and v form another free generating set for F. The set $\{v^{-n}wv^{n} \mid n \in \mathbb{Z}\}$ obviously generates N, and it is an elementary exercise from first principles to show that it does so freely. Consequently, $\{\pi(v^{-n}wv^{n}) \mid n \in \mathbb{Z}\}$ freely generates $\pi(N)$ as abelian group. The infinite cyclic group $\langle\pi(v)\rangle$ generated by $\pi(v)$ acts on $\pi(N)$ by conjugation in $\pi(F)$, so $\pi(N)$ is naturally a module for the integral group ring $\mathbb{Z}\langle\pi(v)\rangle$; the previous sentence yields that it is in fact a free $\mathbb{Z}\langle\pi(v)\rangle$-module, freely generated as such by $\pi(w)$. To match multiplicative notation in this module $\pi(N)$, the action of $\mathbb{Z}\langle\pi(v)\rangle$ will be written exponentially; thus we write $\pi(w)^{t} = \Pi\pi(v^{-n}wv^{n})^{t(n)}$ when t is the element $\Sigma t(n)\pi(v)^{n}$ of the group ring. [Both Π and Σ are taken with n ranging over $\mathbb{Z}$; also, $t(n) \in \mathbb{Z}$ for all n and $t(n) = 0$ for almost all n.]

By definition, the elements of $R(V)$ are precisely the elements of $\pi(F)$ congruent to $\pi(v)$ modulo $\pi(N)$. The foregoing therefore

yields that

$$\rho : \mathbb{Z}\langle\pi(v)\rangle \to R(V) , \quad t \mapsto \pi(v)\ \pi(w)^t$$

is a bijection. It is straightforward to verify that this ρ is a ring isomorphism. Indeed, now

$$\pi(r) \oplus \pi(s) = \pi(d(r, v, s)) = \pi(rv^{-1}s) = \pi(r)\ \pi(v)^{-1}\pi(s)$$

so $\rho(t) \oplus \rho(t') = \rho(t) \cdot \pi(v)^{-1} \cdot \rho(t') =$

$$= \pi(v)\ \pi(w)^t \pi(v)^{-1}\pi(v)\ \pi(w)^{t'} =$$

$$= \pi(v)\ \pi(w)^{t+t'} =$$

$$= \rho(t + t') .$$

Next, let s be any element of F such that $\pi(s) = \rho(t')$: then $\varphi_{\pi(s),\ \pi(v)}(w) = \varphi_{\rho(t'),\pi(v)}(v^{-1}u) = \pi(v)^{-1}\rho(t') = \pi(w)^{t'}$ and, of course, $\varphi_{\pi(s),\pi(v)}(v) = \pi(v)$. Define the element r of F as $r = v\Pi(v^{-n}wv^n)^{t(n)}$: then $\pi(r) = \rho(t)$. Thus

$$\rho(t) \otimes \rho(t') = \pi(r) \otimes \pi(s) =$$

$$= \varphi_{\pi(s),\ \pi(v)}(r) =$$

$$= \pi(v)\Pi(\pi(v)^{-n}\pi(w)^{t'}\pi(v)^n)^{t(n)} =$$

$$= \pi(v)\Pi\pi(w)^{t't(n)\pi(v)^n}$$

$$= \pi(v)\ \pi(w)^{t't}$$

$$= \rho(t't)$$

$$= \rho(tt')$$

as required (the last step coming from the commutativity of $\mathbb{Z}\langle\pi(v)\rangle$) .

Finally, let a be an element and B an abelian normal subgroup in a group A : we need to show that $\rho(\pi(v)) \otimes a' = a^{-1}a'a$ for all a' in the coset Ba . This holds because $\rho(\pi(v)) = \pi(v)\pi(w)^{\pi(v)} = \pi(v^{-1}uv)$ so $\rho(\pi(v)) \otimes a'$ is by definition $\varphi_{a', a}(v^{-1}uv)$.

4. Rings

Now let V be the variety of all associative rings with 1 (or without insisting on 1) , and set $w = u - v$. It is clear that F is also free on w and v [as $u \mapsto w$, $v \mapsto v$ and $u \mapsto u + v$, $v \mapsto v$ define an inverse pair of endomorphisms of F]. The kernel of γ is now the two-sided ideal I generated by w , and the kernel of $[\gamma, \gamma]$ is I^2 : thus $\pi(I)$ has an additive basis consisting of the $\pi(v^i w v^j)$ with i, j nonnegative integers. Now $R(V)$ is the coset $\pi(v) + \pi(I)$, so each element of it is uniquely expressible as $\pi(v) + \Sigma a_{ij}\pi(v^i w v^j)$ with $a_{ij} \in \mathbb{Z}$ for all i, j and $a_{ij} = 0$ for almost all i , j . Differently put: $\rho : \Sigma a_{ij}x^i y^j \mapsto \pi(v + \Sigma a_{ij}v^i s v^j)$ defines a bijection from the commutative polynomial ring $\mathbb{Z}[x, y]$ onto $R(V)$.

It is straightforward to verify that this is an isomorphism of rings. Indeed, the additive nature of the map is quite obvious. To deal with multiplication, let $r = v + \Sigma r_{ij}v^i w v^j$, $s = v + \Sigma s_{kl}v^k w v^l$, and define t_{mn} by $(\Sigma r_{ij}x^i y^j)(\Sigma s_{kl}x^k y^l) = \Sigma t_{mn}\ x^m y^n$: since $\varphi_{\pi(s), \pi(v)}$ maps w to $\pi(s - v)$ and v to $\pi(v)$,

$$\pi(r) \otimes \pi(s) = \varphi_{\pi(s), \pi(v)}(r) =$$

$$= \pi(v) + \Sigma r_{ij}\pi(v)^i \pi(\Sigma s_{kl}v^k w v^l)\pi(v)^j =$$

$$= \pi(v + \Sigma t_{mn}v^m w v^n) .$$

Now let $a \in A \in V$ and B an ideal in A with $B^2 = 0$. As $\varphi_{a+b,a}(w) = (a+b) - a = b$ and $\rho(x) = \pi(v + vw)$,

$$\rho(x) \otimes (a+b) = \varphi_{a+b,a}(v + vw) = a + ab ;$$

similarly, $\rho(y) = \pi(v + wv)$ and so

$$\rho(y) \otimes (a+b) = \varphi_{a+b,a}(v + wv) = a + ba .$$

5. Remarks

Take up the situation in Section 3. The group $\pi(F)$ or F/N' is known as the restricted standard wreath product of the two infinite cyclic groups generated by $\pi(w)$ and $\pi(v)$, respectively, with $\pi(N)$ the "base group". Keeping this F, N, π, change V to an arbitrary variety of groups, and let H be the verbal subgroup of $\pi(F)$ corresponding to V [that is, the smallest normal subgroup of $\pi(F)$ modulo which the quotient lies in V]. The set $\{t \in \mathbb{Z}\langle\pi(w)\rangle \mid \pi(w)^t \in H\}$ is then an ideal in this group ring, and the quotient modulo this ideal is the ring assigned to this V. Consequently, as Sivâk noted in [4], $R(V)$ depends only on the metabelian groups contained in V, and is usually easy enough to calulcate.

This encourages one to raise the question: just what are all the rings assigned to group varieties? Equivalently, can one somehow describe all verbal subgroups in the wreath product of two infinite cycles? This is a small fragment of the general question of identifying all varieties of metabelian groups. That larger problem has been reduced by Bryce [1] to the prime-power-exponent case which remains open. It would be interesting to check out whether (the relevant fragment of) Bryce's argument reduces our problem to finding the verbal subgroups of prime-

-power index in our wreath product. If it does, then one is in effect left with the task of understanding verbal subgroups in the wreath product of two finite cyclic groups, the order of each cycle being a power of the same prime.

This residual question does not appear to be anything like as difficult as the still incomplete exploration of varieties of metabelian nilpotent groups of prime-power exponent. For, in such a finite wreath product one has a reasonable overview of all normal subgroups. The key points, special cases of results of Leedham-Green and Newman [3], seem to be the following. Let W be the wreath product of two cyclic groups G, H, of orders p^m and p^n, say. There exist $n + 1$ uniserial H-modules $X_0, X_1, \ldots, X_n$ such that the base group of W viewed as an H-module is (isomorphic to) a section (that is, quotient of a submodule) of the direct sum $X_0 \oplus \ldots \oplus X_n$. In general, all sections of a direct sum of two modules are understood once one knows all isomorphisms between sections of the direct summands. In a sum with more than two summands one can attempt to proceed inductively: first elaborate the possible sections of $X_0 \oplus X_1$, then the isomorphisms of these with sections of X_2, then consider sections of $(X_0 \oplus X_1) \oplus X_2$, and so on. In general, this can get out of hand very rapidly, but in the present case one should be able to keep it under control. The initial information is that two sections of an X_i are isomorphic if and only if they have the same composition length, and elementary (that is, of exponent p) if and only if that length is at most 1 when $i = 0$, at most $p^{i-1}(p-1)$ when $i > 0$. For $i \neq j$, a section of X_i is isormorphic to a section of X_j if and only if they are both elementary and have the same length; if that length is $k\,(>0)$, the number of relevant isomorphisms is $p^{k-1}(p-1)$.

Yet another reason to be optimistic about this problem lies in the fact that these wreath products are free algebras of rank 1 in suitable (congruence-modular) varieties of what Bryce called bi-groups and B.I. Plotkin's school calls group pairs or group representations. The study of all "verbal" congruences on this free algebra is a natural and basic problem which should be capable of resolution. The verbal subgroups we want are the kernels of some of these congruences: so a conclusive solution of that problem would create an extremely helpful framework for approaching ours: a framework containing much less irrelevant material than the discussion of all normal subgroups indicated above.

Received for Research Reports November 20, 1985.

References

[1] R.A. Bryce, "Metabelian groups and varieties", Philos. Trans. Roy. Soc. London 266 (1970), 281-355.

[2] Ralph S. Freese and Ralph N. McKenzie, "The commutator, an overview", preprint, 1981?

[3] C.R. Leedham-Green and M.F. Newman, "Space groups and groups of prime-power order I", Arch. Math. 35 (1980), 193-202.

[4] Bohuslav Sivák, "The structure of the rings assigned to group varieties", Math. Slovaca 35 (1985), No. 2, 169-173.