Bohuslav Sivák

The structure of the rings assigned to group varieties

Mathematica Slovaca, Vol. 35 (1985), No. 2, 169--173

Persistent URL: http://dml.cz/dmlcz/136386

Math. Slovaca 35, 1985, No. 2, 169—173

THE STRUCTURE OF THE RINGS ASSIGNED TO GROUP VARIETIES

BOHUSLAV SIVÁK

Recall a construction which assignes to each congruence-modular variety $\mathcal{V}$ some ring $R(\mathcal{V})$ [1].

Let $\mathcal{V}$ be a congruence-modular variety and let F_2 be the $\mathcal{V}$-free algebra generated by $\{x, y\}$. Let us denote Γ the least congruence on F_2 which identifies x and y. Let $\pi\colon F_2 \to F_2/[\Gamma, \Gamma]$ be the natural projection on the factor-algebra, $\bar{\Gamma} = \pi(\Gamma)$, $R(\mathcal{V}) = [y]\bar{\Gamma}$. The ring operations on $R(\mathcal{V})$ are the following ones:

$$\begin{aligned} u(x, y) + v(x, y) &= d(u(x, y), y, v(x, y)),\\ u(x, y) \cdot v(x, y) &= u(v(x, y), y),\\ -u(x, y) &= d(y, u(x, y), y),\\ 1 = x, &\quad 0 = y. \end{aligned}$$

In this definition, d is the ternary difference term in $\mathcal{V}$.

We shall consider only the case $\mathcal{V} \subseteq \mathcal{G}$, where $\mathcal{G}$ is the variety of all groups. Each term $u(x, y) \cdot y)$ can be written in the form

$$u(x, y) = u'(x, y) \cdot y$$

and trivially:

$$u(x, x) = x \Leftrightarrow u'(x, x) = 1.$$

Since $R(\mathcal{V})$ contains exactly the classes of idempotent terms, the definition of $R(\mathcal{V})$ can be modified in the following way: $R(\mathcal{V}) = [1]\bar{\Gamma}$ (i.e., $R(\mathcal{V})$ contains exactly the classes of terms u satisfying $u(x, x) = 1$.)

$$\begin{aligned} u(x, y) \otimes v(x, y) &= u(x, y) \cdot v(x, y) \quad \text{(the product in } \pi(F_2))\\ u(x, y) \odot v(x, y) &= u(v(x, y) \cdot y, y)\\ \ominus u(x, y) &= (u(x, y))^{-1} \qquad \text{(the inverse element in } \pi(F_2))\\ 1 = xy^{-1}, &\quad 0 = yy^{-1} \end{aligned}$$

Lemma 1. *$u(x, x) = 1$ in $\mathcal{V}$ if and only if there exists $\bar{u}$ such that $\bar{u} = u$ in $\mathcal{V}$ and $\bar{u}(x, x) = 1$ in $\mathcal{G}$.*

Proof. $\bar{u}(x, y) = u(x, y) \cdot u^{-1}(x, x)$ proves $\Rightarrow$. The implication $\Leftarrow$ is trivial.

Corollary. *The subgroup of F_2 which corresponds to $[\Gamma, \Gamma]$ is generated by the set of all elements of the form*

$$u(x, y) \cdot v(x, y) \cdot u^{-1}(x, y) \cdot v^{-1}(x, y),$$

where $u(x, x) = v(x, x) = 1$ in $\mathscr{G}$.

Proof. The terms u satisfying $u(x, x) = 1$ in $\mathscr{G}$ form a subgroup of F_2 corresponding to the congruence Γ.

Lemma 2. *If $u(x, x) = 1$ in $\mathscr{G}$, then $u = v_1 \dots v_k$ in $\mathscr{G}$, where each v_i has the form $x^n y^{-n}$ or $y^n x^{-n}$, $n \in Z$.*

Proof. The term $u(x, y)$ can be written as a product of powers of x and y. The proof can be done by the induction on the number of these powers.

Corollary. *The subgroup of F_2 which corresponds to $[\Gamma, \Gamma]$ is generated by the set of all elements conjugated with the elements of the form*

$$u(x, y) \cdot v(x, y) \cdot u^{-1}(x, y) \cdot v^{-1}(x, y),$$

where u and v have the form $x^n y^{-n}$ or $y^n x^{-n}$, $n \in Z$.

Lemma 3. *The additive semigroup of the ring $R(\mathscr{V})$ is generated by the set of all elements of the form $x^n y^{-n}$ or $y^n x^{-n}$, $n \in Z$.*

Corollary. *The additive group of the ring $R(\mathscr{V})$ is generated by the set $\{x^n y^{-n} \mid n \in Z\}$.*

Definition. *For each $n \in N$, let us denote*

$$a_n = x^n y^{-n}, \quad b_n = y^{-n} x^n.$$

Remark. In $R(\mathscr{V})$, the elements a_n, b_n have the additive inverse elements

$$\ominus a_n = y^n x^{-n}, \quad \ominus b_n = x^{-n} y^n.$$

Lemma 4. *Let us denote $s = b_1 = y^{-1}x$.* Then

$$b_n = s^n \oplus s^{n-1} \oplus \dots \oplus s \quad (\textit{the powers in } R(\mathscr{V}))$$

for each $n \in N$.

Proof. It suffices to prove $b_n \ominus b_{n-1} = s^n$ for $n \geqslant 2$. We shall do it by the induction on n. For $n = 2$ we have:

$$s^2(x, y) = s(s(x, y) \cdot y, y) = s(y^{-1}xy, y) = y^{-2}xy = \\ = (y^{-2}x^2)x^{-1}y) = b_2 \ominus b_1.$$

Assume that $n > 2$ and that $s^{n-1} = b_{n-1} \ominus b_{n-2} = (y^{1-n}x^{n-1}) \cdot (x^{2-n}y^{n-2}) = y^{n-2}$. Then

$$s^n(x, y) = s^{n-1}(s(x, y) \cdot y, y) = s^{n-1}(y^{-1}xy, y) = y^{1-n} \cdot y^{-1}xy \cdot y^{n-1} =$$
$$= y^{-n}xy^{n-1} = (y^{-n}x^n)(x^{1-n}y^{n-1}) = b_n \ominus b_{n-1}.$$

Lemma 5. *Let us denote* $t = yxy^{-2}$. *Then*

$$a_n = t^{n-1} \oplus t^{n-2} \oplus \ldots \oplus t \oplus 1$$

(the powers and the unit in $R(\mathscr{V})$*) for each* $n \in N$.

Proof. It suffices to prove $a_{n+1} \ominus a_n = t^n$ for $n \geq 1$. We shall do it by the induction on n. For $n = 1$ we have:

$$t^1(x, y) = yxy^{-2} = (yx^{-1})(x^2y^{-2}) = \ominus a_1 \oplus a_2 = a_2 \ominus a_1.$$

Assume that $n > 1$ and that $t^{n-1} = a_n \ominus a_{n-1} = (x^ny^{-n})(y^{n-1}x^{1-n}) = x^ny^{-1}x^{1-n}$. Then

$$t^n(x, y) = t^{n-1}(t(x, y) \cdot y, y) = t^{n-1}(yxy^{-1}, y) =$$
$$= (yxy^{-1})^n \cdot y^{-1} \cdot (yxy^{-1})^{1-n} = yx^ny^{-1}y^{-1}yx^{1-n}y^{-1} = yx^ny^{-1}x^{1-n}y^{-1} =$$
$$= (yx^{-1}) \cdot (x^{n+1}y^{-n-1})(y^nx^{-n})(xy^{-1}) = \ominus 1 \oplus a_{n+1} \ominus a_n \oplus 1 = a_{n+1} \ominus a_n.$$

Lemma 6. $s \odot t = t \odot s = 1$ *in* $R(\mathscr{V})$.

Proof. $(s \odot t)(x,y) = s(t(x, y) \cdot y, y) = s(yxy^{-1}, y) = y^{-1} \cdot yxy^{-1} = xy^{-1}$, $(t \odot s)(x, y) = t(s(x, y) \cdot y, y) = t(y^{-1}xy, y) = y \cdot y^{-1}xy \cdot y^{-2} = xy^{-1}$. The term xy^{-1} is the unit of $R(\mathscr{V})$.

Theorem 1. *The ring* $R(\mathscr{V})$ *is generated by the elements* $s = y^{-1}x$, $t = yxy^{-2}$. *This two elements commutate in* $R(\mathscr{V})$.

Corollary. *The ring* $R(\mathscr{V})$ *is isomorphic to the factor ring of* $Z[p, q]$ *by some ideal containing the element* $1 - pq$.

Corollary. *The ring* $R(\mathscr{V})$ *is commutative.*

Theorem 2. *The ring* $R(\mathscr{G})$ *is isomorphic to* $Z[p, q]/(1 - pq)$, *the isomorphism is defined by* $1 \mapsto 1$, $\bar{p} \mapsto y^{-1}x$, $\bar{q} \mapsto yxy^{-2}$.

Proof. Each element of $R(\mathscr{G})$ can be written in the form

$$c_0 \oplus c_1s \oplus c_2s^2 \oplus \ldots \oplus c_ks^k \oplus d_1t \oplus d_2t^2 \oplus \ldots \oplus d_mt^m,$$

where c_i, $d_j \in Z$. It suffices to prove that such a representation is unique, i.e. that the zero element of $R(\mathscr{G})$ has only the trivial representation of this type. Trivially,

$$0 = c_0 \oplus c_1s \oplus c_2s^2 \oplus \ldots \oplus c_ks^k \oplus d_1t \oplus d_2t^2 \oplus \ldots \oplus d_mt^m$$

if and only if

$$0 = d_m \oplus d_{m-1}s \oplus \ldots \oplus d_2s^{m-2} \oplus d_1s^{m-1} \oplus c_0s^m \oplus c_1s^{m+1} \oplus \ldots \oplus c_ks^{m+k}.$$

Therefore, we have to prove that the elements $1, s, s^2, \ldots$ are Z-linearly independent. By Lemma 4, it suffices to prove that $b_1, b_2, b_3, \ldots$ are Z-linearly independent. This proof will be done if we find a group G and its elements x, y such that:

(1) The elements of the form $x^n y^{-n}$ or $y^n x^{-n}$, $n \in Z$, commute in G.

(2) No equality of the form

$$(y^{-1}x)^{e_1}(y^{-2}x^2)^{e_2} \ldots (y^{-n}x^n)^{e_n} = 1, \quad e_i \in Z,\ n \in N,$$

holds in G except in the case $e_1 = \ldots = e_n = 0$. Now we shall construct such a group. Let us denote

$$M = \{f \mid f\colon Z \to Z \text{ has a finite support and } \sum_{i \in Z} f(i) = 0\},$$

$$G = Z \times M.$$

We define the operation $*$ on G in the following way:

$$(m, f) * (n, g) = (m + n, h), \text{ where } h(i) = f(i + n) + g(i).$$

The direct calculations whow that $(G, *)$ is a group with the neutral element $(0, o)$, $o\colon Z \to Z$, $o(i) = 0$. Let us denote

$$\varphi_k(i) = \begin{cases} 1 & \text{if } i + k = 0 \\ -1 & \text{if } i = 0 \\ 0 & \text{otherwise} \end{cases} \quad \text{for } 0 \neq k \in Z,$$

$$x = (1, \varphi_1), \quad y = (1, o).$$

Easy calculations give $y^{-n} = (-n, o)$, $x^n = (n, \varphi_n)$, therefore $y^{-n}x^n = (-n, o) * (n, \varphi_n) = (0, \varphi_n)$, $x^n y^{-n} = (0, \psi_n)$, where $\psi_n(i) = -\varphi_n(-i)$.

As all elements of the form $(0, f)$ commute in $(G, *)$, the condition (1) is satisfied. The condition (2) is a consequence of the equalities

$$(y^{-i}x^i)^{e_i} = \underbrace{(0, \varphi_i) * \ldots * (0, \varphi_i)}_{e_i\text{-times}} = (0, e_i\varphi_i),$$

$$(y^{-1}x)^{e_1} * \ldots * (y^{-n}x^n)^{e_n} = \left(0, \sum_{i=1}^{n} e_i\varphi_i\right)$$

and the linear independence of the functions φ_i.

Remark. The ring $R(\mathcal{V})$ is a homomorphic image of $R(\mathcal{G})$ for each subvariety $\mathcal{V} \subseteq \mathcal{G}$. This ring can be sometimes easily determined. For instance, if $\mathcal{V}$ is the subvariety of all abelian groups, then $R(\mathcal{V}) \cong Z$. If $\mathcal{V}$ is the subvariety of $\mathcal{G}$ determined by the identity $xy^2 = y^2x$, then $R(\mathcal{V})$ is isomorphic to $Z[w]/(w^2, 2w)$. (In this case, $w = s \ominus 1$.)

The assignment $\mathcal{V} \mapsto R\mathcal{V})$ is not injective. If $\mathcal{K}$ is the subvariety of $\mathcal{G}$ determined by the identity $[[x, y], [z, t]] = 1$, then $R(\mathcal{V}) \cong R(\mathcal{V} \cap \mathcal{K})$ for each $\mathcal{V} \subseteq \mathcal{G}$. For instance, $R(\mathcal{K}) \cong R(\mathcal{G})$.

REFERENCES

[1] FREESE, R. S., McKENZIE, R.: The commutator, an overview (preprint).

Received January 6, 1983

Katedra matematiky Pedagogickej fakulty
Tajovského 40
975 49 Banská Bystrica

СТРУКТУРА КОЛЕЦ, СВЯЗАННЫХ С МНОГООБРАЗИЯМИ ГРУПП

Bohuslav Sivák

Резюме

В работе найдено строение колец $R(\mathcal{V})$ поставленых модулярным многообразиям $\mathcal{V}$ для случая многообразий групп. Доказано, что для многообразия всех групп это кольцо изоморфно $Z[p, q]/(1-pq)$ и для других многообразий групп оно является гомоморфным образом этого кольца. Таким образом, вде кольца $R(\mathcal{V})$ коммутативны.