BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 55, No. 4, 2007

Relations between Elements $r^2 - r$

by

Andrzej PRÓSZYŃSKI

Presented by Andrzej SCHINZEL

Summary. We prove that generating relations between the elements $[r] = r^2 - r$ of a commutative ring are the following: $[r + s] = [r] + [s] + rs[2]$ and $[rs] = r^2[s] + s[r]$.

1. Introduction. Let R be a commutative ring with 1. In [2], the author introduced the ideal $I(R) = I_2(R)$ generated by all elements of the form $r^2 - r$, where $r \in R$, and proved that it is precisely the intersection of all maximal ideals of index 2 in R [2, Proposition 5.5]. This ideal is permanently used in all considerations concerning relations satisfied by mappings of higher degrees (see [2]–[5]). The motivation for this paper is also similar: the main result will be used in [1] to find generating relations for mappings of degree 5; however, it is fully independent of the theory of higher degree mappings. The result is the following

THEOREM. *Let $C(R)$ be the R-module generated by the elements $[r]$, $r \in R$, with relations*

$$[r + s] = [r] + [s] + rs[2], \qquad r, s \in R, \tag{1}$$

$$[rs] = r^2[s] + s[r], \qquad r, s \in R. \tag{2}$$

Then there exists an R-isomorphism $P : C(R) \to I(R)$ such that $P([r]) = r^2 - r$ for $r \in R$.

First of all, observe that elements $r^2 - r$ satisfy relations (1)–(2). Therefore there exists an R-epimorphism $P : C(R) \to I(R)$ defined by the above formula and we must prove that it is injective. Moreover, note some consequences of (1) and (2), pointed out in [5, Corollary 5.1.4]:

2000 *Mathematics Subject Classification*: 13C13, 13C05, 11E76.

Key words and phrases: ideals of commutative rings, generators and relations, higher degree mappings.

LEMMA 1. *For any* $r, s \in R$ *we have*

(3) $(r^2 - r)[s] = (s^2 - s)[r]$,

(4) $2[r] = (r^2 - r)[2],\ [2r] = (2r^2 - r)[2]$,

(5) $[r] = [1 - r],\ [0] = [1] = 0,\ [2] = [-1]$,

(6) *if* $r^2 - r = 2s$ *then* $[r] = s[2]$,

(7) *if* s *is invertible then* $[s^{-1}] = -s^{-3}[s]$.

Proof. Relation (3) follows from the two symmetric versions of (2). The first equality in (4) is obtained from (3), and gives the other one using (1).

(5) The equalities $[0] = [1] = 0$ follow from (2) for $r, s = 0$ or 1. Hence by (1) and (3) we obtain

$$0 = [1] = [r] + [1 - r] + (r - r^2)[2] = [r] + [1 - r] - 2[r] = [1 - r] - [r].$$

This also gives $[2] = [-1]$.

(6) Using (1) and (5) we get

$$[r - r^2] = r^2[1 - r] + (1 - r)[r] = (r^2 - r + 1)[r] = (2s + 1)[r].$$

On the other hand, $[r - r^2] = [2(-s)] = (2s^2 + s)[2]$ by (4), and hence

$$[r] = (2s^2 + s)[2] - 2s[r] = (2s^2 + s)[2] - s(r^2 - r)[2] = s[2]$$

because of (4).

(7) It follows from (5) and (2) that $0 = [1] = [ss^{-1}] = s^2[s^{-1}] + s^{-1}[s]$ and so $[s^{-1}] = -s^{-3}[s]$. ∎

2. The functor C and C-functions. Any unitary ring homomorphism $i : R \to R'$ induces the module homomorphism $C(i) : C(R) \to C(R')$ over i such that $C(i)([r]) = [i(r)]$. Then C is obviously a functor. We prove that it commutes with localizations. First of all, define *C-functions* over R as functions $f : R \to M$, where M is an R-module, satisfying the conditions

(1′) $$f(r + s) = f(r) + f(s) + rsf(2), \quad r, s \in R,$$

(2′) $$f(rs) = r^2 f(s) + sf(r), \quad r, s \in R,$$

and consequently, the analogs of (3)–(7). Observe that $C(R)$ is a universal object with respect to C-functions over R; this means that any C-function can be uniquely expressed as a composition of the canonical C-function $c : R \to C(R),\ c(r) = [r]$, and an R-homomorphism defined on $C(R)$.

EXAMPLE. The analog of (6) shows that any C-function f over the ring $\mathbb{Z}$ of integers is of the form $f(r) = \frac{r^2 - r}{2}a$, where $a = f(2)$. Since $I(\mathbb{Z}) = (2)$ is a free $\mathbb{Z}$-module, it follows from the universal property that the element a can be chosen arbitrarily.

Let S be a multiplicatively closed set in R and let $i : R \to R_S$ and $i : M \to M_S$ be the canonical homomorphisms.

LEMMA 2. *For any C-function $f : R \to M$ there exists a unique C-function $f_S : R_S \to M_S$ satisfying the condition $f_S(i(r)) = i(f(r))$ for $r \in R$. It is given by the formula*

$$f_S\left(\frac{r}{s}\right) = \frac{f(r)}{s} - \left(\frac{r}{s}\right)^2 \frac{f(s)}{s}.$$

Proof. The condition means that $f_S\left(\frac{r}{1}\right) = \frac{f(r)}{1}$ for $r \in R$. Let $s \in S$. If f_S is a C-function then

$$\begin{aligned} \frac{f(r)}{1} = f_S\left(\frac{r}{1}\right) &= f_S\left(\left(\frac{r}{s}\right)\left(\frac{s}{1}\right)\right) \\ &= \left(\frac{r}{s}\right)^2 f_S\left(\frac{s}{1}\right) + \left(\frac{s}{1}\right) f_S\left(\frac{r}{s}\right) \\ &= \left(\frac{r}{s}\right)^2 \frac{f(s)}{1} + \left(\frac{s}{1}\right) f_S\left(\frac{r}{s}\right), \end{aligned}$$

which gives the required formula. This proves the uniqueness of f_S.

To prove that f_S is properly defined, it suffices to check that the right hand side of the formula remains the same if we replace r by rt and s by st for any $t \in S$. By $(2')$, we compute that, in fact,

$$\begin{aligned} \frac{f(rt)}{st} - \left(\frac{rt}{st}\right)^2 \frac{f(st)}{st} &= \frac{r^2 f(t) + t f(r)}{st} - \left(\frac{r}{s}\right)^2 \frac{s^2 f(t) + t f(s)}{st} \\ &= \frac{f(r)}{s} - \left(\frac{r}{s}\right)^2 \frac{f(s)}{s}. \end{aligned}$$

It remains to prove $(1')$ and $(2')$ for f_S. Let $\frac{a}{s}$ and $\frac{b}{s}$ be arbitrary elements of R_S. Then

$$\begin{aligned} f_S\left(\frac{a}{s} + \frac{b}{s}\right) &= f_S\left(\frac{a+b}{s}\right) = \frac{f(a+b)}{s} - \left(\frac{a+b}{s}\right)^2 \frac{f(s)}{s} \\ &= \frac{f(a)}{s} + \frac{f(b)}{s} + \frac{abf(2)}{s} - \left(\left(\frac{a}{s}\right)^2 + \left(\frac{b}{s}\right)^2 + \frac{2ab}{s^2}\right) \frac{f(s)}{s} \\ &= \left(\frac{f(a)}{s} - \left(\frac{a}{s}\right)^2 \frac{f(s)}{s}\right) + \left(\frac{f(b)}{s} - \left(\frac{b}{s}\right)^2 \frac{f(s)}{s}\right) + \frac{abf(2)}{s} - \frac{ab}{s^2} \frac{2f(s)}{s} \\ &= f_S\left(\frac{a}{s}\right) + f_S\left(\frac{b}{s}\right) + \frac{abf(2)}{s} - \frac{ab}{s^2} \frac{(s^2 - s)f(2)}{s} \\ &= f_S\left(\frac{a}{s}\right) + f_S\left(\frac{b}{s}\right) + \frac{a}{s}\frac{b}{s}\frac{f(2)}{1} = f_S\left(\frac{a}{s}\right) + f_S\left(\frac{b}{s}\right) + \frac{a}{s}\frac{b}{s} f_S\left(\frac{2}{1}\right) \end{aligned}$$

by $(1')$ and the analogue of (4) for f, and

$$
\begin{aligned}
f_S\Big(\frac{a}{s}\,\frac{b}{s}\Big) - \Big(\frac{a}{s}\Big)^2 f_S\Big(\frac{b}{s}\Big) - \frac{b}{s} f_S\Big(\frac{a}{s}\Big)
&= f_S\Big(\frac{ab}{s^2}\Big) - \Big(\frac{a}{s}\Big)^2 f_S\Big(\frac{b}{s}\Big) - \frac{b}{s}\, f_S\Big(\frac{a}{s}\Big)\\
&= \Big(\frac{f(ab)}{s^2} - \Big(\frac{ab}{s^2}\Big)^2 \frac{f(s^2)}{s^2}\Big) - \Big(\frac{a}{s}\Big)^2 \Big(\frac{f(b)}{s} - \Big(\frac{b}{s}\Big)^2 \frac{f(s)}{s}\Big)\\
&\quad - \frac{b}{s}\Big(\frac{f(a)}{s} - \Big(\frac{a}{s}\Big)^2 \frac{f(s)}{s}\Big)\\
&= \Big(\frac{f(ab)}{s^2} - \Big(\frac{a}{s}\Big)^2 \frac{f(b)}{s} - \frac{b}{s}\,\frac{f(a)}{s}\Big)\\
&\quad - \Big(\frac{a}{s}\Big)^2 \Big(\Big(\frac{b}{s}\Big)^2 \frac{f(s^2)}{s^2} - \Big(\frac{b}{s}\Big)^2 \frac{f(s)}{s} - \frac{b}{s}\,\frac{f(s)}{s}\Big)\\
&= \Big(\frac{a^2 f(b) + b f(a)}{s^2} - \frac{a^2 f(b)}{s^3} - \frac{b f(a)}{s^2}\Big)\\
&\quad - \Big(\frac{a}{s}\Big)^2 \frac{b}{s}\Big(\frac{b}{s}\,\frac{f(s^2) - s f(s)}{s^2} - \frac{f(s)}{s}\Big)\\
&= \frac{a^2(s^2 - s) f(b)}{s^4} - \frac{a^2 b}{s^3}\Big(\frac{b}{s}\,\frac{s^2 f(s)}{s^2} - \frac{f(s)}{s}\Big)\\
&= \frac{a^2(b^2 - b) f(s)}{s^4} - \frac{a^2 b(b-1) f(s)}{s^4} = 0
\end{aligned}
$$

by $(2')$ and the analogue of (3) for f. This completes the proof. ∎

Now we are ready to prove

PROPOSITION. *There exists an R_S-isomorphism $C(R)_S \approx C(R_S)$ such that*

$$\frac{[r]}{s} \leftrightarrow \frac{1}{s}\Big[\frac{r}{1}\Big].$$

Proof. Applying Lemma 2 to the canonical C-function $c : R \to C(R)$, $c(r) = [r]$, we obtain a C-function $c_S : R_S \to C(R)_S$ over R_S,

$$c_S\Big(\frac{r}{s}\Big) = \frac{[r]}{s} - \Big(\frac{r}{s}\Big)^2 \frac{[s]}{s}.$$

The universal property yields an R_S-homomorphism $g : C(R_S) \to C(R)_S$ such that

$$g\Big(\Big[\frac{r}{s}\Big]\Big) = \frac{[r]}{s} - \Big(\frac{r}{s}\Big)^2 \frac{[s]}{s}.$$

On the other hand, we have a homomorphism $C(i) : C(R) \to C(R_S)$ over $i : R \to R_S$ defined by $C(i)([r]) = \left[\frac{r}{1}\right]$, which gives an R_S-homomorphism $h : C(R)_S \to C(R_S)$ such that

$$h\left(\frac{[r]}{s}\right) = \frac{1}{s}\left[\frac{r}{1}\right].$$

Observe that $h = g^{-1}$. In fact,

$$g\left(h\left(\frac{[r]}{s}\right)\right) = \frac{1}{s}\, g\left(\left[\frac{r}{1}\right]\right) = \frac{1}{s}\left(\frac{[r]}{1} - \left(\frac{r}{1}\right)^2\frac{[1]}{1}\right) = \frac{[r]}{s}$$

by (5). On the other hand, using (7) and (2) we compute that

$$\begin{aligned} h\left(g\left(\left[\frac{r}{s}\right]\right)\right) &= h\left(\frac{[r]}{s} - \left(\frac{r}{s}\right)^2\frac{[s]}{s}\right) \\ &= \frac{1}{s}\left[\frac{r}{1}\right] - \frac{r^2}{s^3}\left[\frac{s}{1}\right] = \frac{1}{s}\left[\frac{r}{1}\right] + \left(\frac{r}{1}\right)^2\left[\frac{1}{s}\right] = \left[\frac{r}{1}\frac{1}{s}\right] = \left[\frac{r}{s}\right]. \end{aligned}$$

Hence h is an isomorphism, as required. ∎

Finally, note that also $I(R)_S = I(R_S)$, as follows, for example, from [2, Lemma 5.1].

3. Some lemmas about the kernel of P. Let us consider the kernel of the R-homomorphism $P : C(R) \to I(R)$, $P([r]) = r^2 - r$ for $r \in R$. Our first observation is the following

LEMMA 3. $I(R)\mathrm{Ker}(P) = 0$.

Proof. Let $x = \sum_i a_i[r_i] \in \mathrm{Ker}(P)$, that is, $\sum_i a_i(r_i^2 - r_i) = 0$. Then by (3) we obtain $(r^2 - r)x = \sum_i a_i(r^2 - r)[r_i] = \sum_i a_i(r_i^2 - r_i)[r] = 0[r] = 0$. ∎

The next lemma plays a key role in our considerations.

LEMMA 4. *Let $x = \sum_i a_i[r_i] \in \mathrm{Ker}(P)$, where one of the r_i is 2. If all a_i belong to $I(R)^k$ for some $k \geq 0$ then $x = \sum_i b_i[r_i]$ where all b_i belong to $I(R)^{2k+1}$.*

Proof. By the assumption, $\sum_i a_i r_i^2 = \sum_i a_i r_i$. Observe that

$$\begin{aligned} \left[\sum_i a_i r_i^2\right] &= \sum_i [a_i r_i^2] + c[2] = \sum_i a_i^2[r_i^2] + \sum_i r_i^2[a_i] + c[2] \\ &= \sum_i a_i^2(r_i^2 + r_i)[r_i] + \sum_i r_i^2[a_i] + c[2], \end{aligned}$$

$$\left[\sum_i a_i r_i\right] = \sum_i [a_i r_i] + d[2] = \sum_i a_i[r_i] + \sum_i r_i^2[a_i] + d[2],$$

where $c = \sum_{i<j} a_i a_j r_i^2 r_j^2$, $d = \sum_{i<j} a_i a_j r_i r_j$. Since the above two elements are equal, we obtain

$$x = \sum_i a_i[r_i] = \sum_i a_i^2(r_i^2 + r_i)[r_i] + (c-d)[2]$$
$$= \sum_i a_i^2(r_i^2 + r_i)[r_i] + \sum_{i<j} a_i a_j (r_i^2 r_j^2 - r_i r_j)[2].$$

This completes the proof, because $r_i^2 + r_i$ and $r_i^2 r_j^2 - r_i r_j$ belong to $I(R)$. ∎

The above lemma immediately yields the following

COROLLARY. *Let $x = \sum_i a_i[r_i] \in \mathrm{Ker}(P)$ and let M denote the submodule of $C(R)$ generated by all $[r_i]$ and $[2]$. Then $x \in \bigcap_{k=0}^{\infty} I(R)^k M$.*

4. Proof of the theorem: noetherian case. Suppose that R is noetherian. By the Proposition and the remark concluding Section 2 we can assume that R is, in fact, local and noetherian. Then we have the following two cases:

CASE 1: $I(R) = R$ (this means that the quotient field of R has more than two elements). Then Lemma 3 gives $\mathrm{Ker}(P) = 0$.

CASE 2: $I(R)$ is the maximal ideal (this means that the quotient field of R has exactly two elements). Let $x \in \mathrm{Ker}(P)$. Define the submodule M as in the Corollary and observe that it is a finitely generated module over a local noetherian ring. Then the intersection in the Corollary is zero by the Krull intersection theorem, and consequently $x = 0$. This proves that $\mathrm{Ker}(P) = 0$.

5. Proof of the theorem: general case. Let $x = \sum_i a_i[r_i] \in \mathrm{Ker}(P)$. Define the subring S of R generated by all the elements a_i and r_i. Since S is a finitely generated ring, it is obviously noetherian, and hence the previous part of the proof shows that $P : C(S) \to I(S)$ is iso. Let $i : S \to R$ denote the injection. Then $x = (C(i))(y)$, where $y = \sum_i a_i[r_i] \in C(S)$. Since $P(y) = P(x) = 0$ we conclude that $y = 0$ and consequently $x = 0$. This completes the proof.

References

[1] M. Maciejewski and A. Prószyński, *Mappings of degree 5, part I*, in preparation.

[2] A. Prószyński, *Forms and mappings. I: Generalities*, Fund. Math. 122 (1984), 219–235.

[3] —, *Forms and mappings. III: Regular m-applications*, Comment. Math. 28 (1989), 305–330.

[4] —, *Forms and mappings. IV: Degree 4*, Bull. Polish Acad. Sci. Math. 37 (1989), 269–278.

[5] A. Prószyński, *Mappings of higher degrees*, WSP Bydgoszcz, 1987 (in Polish).

Andrzej Prószyński
Kazimierz Wielki University
85-072 Bydgoszcz, Poland
E-mail: apmat@ukw.edu.pl

Received May 26, 2007;
received in final form June 15, 2007 (7603)