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

\begin{align}
(1) & \quad [r + s] = [r] + [s] + rs[2], \quad r, s \in R, \\
(2) & \quad [rs] = r^2[s] + s[r], \quad r, s \in R.
\end{align}

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

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

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

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

\[
(6) \quad \text{if } r^2 - r = 2s \text{ then } [r] = s[2],
\]

\[
(7) \quad \text{if } s \text{ is invertible then } [s^{-1}] = -s^{-3}[s].
\]

**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 \([s^{-1}] = -s^{-3}[s]\). \( \blacksquare \)

**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

\[
(1') \quad f(r + s) = f(r) + f(s) + rsf(2), \quad r, s \in R,
\]

\[
(2') \quad f(rs) = r^2f(r) + sf(r), \quad r, s \in R,
\]

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 \( i : R \to RS \) and \( i : M \to MS \) 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

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

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,

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

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

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

by (1') and the analogue of (4) for $f$, and
\[
fs\left(\frac{a}{s}\right) - \left(\frac{a}{s}\right)^2 \left(\frac{b}{s}\right) - \frac{b}{s}\fs\left(\frac{a}{s}\right)
\]
\[
= \fs\left(\frac{ab}{s^2}\right) - \left(\frac{a}{s}\right)^2 \fs\left(\frac{b}{s}\right) - \frac{b}{s}\fs\left(\frac{a}{s}\right)
\]
\[
= \left(\frac{f(ab)}{s^2} - \left(\frac{ab}{s^2}\right)^2 \frac{f(s^2)}{s^2}\right) - \left(\frac{a}{s}\right)^2 \left(\frac{f(b)}{s} - \left(\frac{b}{s}\right)^2 \frac{f(s)}{s}\right)
\]
\[
- \frac{b}{s}\left(\frac{f(a)}{s} - \left(\frac{a}{s}\right)^2 \frac{f(s)}{s}\right)
\]
\[
= \left(\frac{f(ab)}{s^2} - \left(\frac{a}{s}\right)^2 \frac{f(b)}{s} - \frac{b}{s} \frac{f(a)}{s}\right)
\]
\[
- \left(\frac{a}{s}\right)^2 \left(\frac{f(b)}{s^2} - \left(\frac{b}{s}\right)^2 \frac{f(s)}{s}\right) - \frac{b}{s} \frac{f(s)}{s}
\]
\[
= \frac{a^2 f(b) + bf(a)}{s^2} - \frac{a^2 f(b)}{s^3} - \frac{bf(a)}{s^2}
\]
\[
- \left(\frac{a}{s}\right) \frac{2b}{s} \left(\frac{f(s^2) - sf(s)}{s^2} - \frac{f(s)}{s}\right)
\]
\[
= \frac{a^2(b^2 - b)f(s)}{s^4} - \frac{a^2 b(b - 1)f(s)}{s^4} = 0
\]

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

Now we are ready to prove

**Proposition.** There exists an \( \Rs - \text{isomorphism} \ C(R)_S \cong C(\Rs) \) such that

\[
\left[\frac{r}{s}\right] \mapsto \frac{1}{s} \left[\frac{r}{s}\right].
\]

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

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

The universal property yields an \( \Rs - \text{homomorphism} \) \( g : C(R_S) \to C(R)_S \) such that

\[
g\left(\left[\frac{r}{s}\right]\right) = \left[\frac{r}{s}\right] - \left(\frac{r}{s}\right)^2 \left[\frac{s}{s}\right].
\]
On the other hand, we have a homomorphism $C(i) : C(R) \to C(R_S)$ over $i : R \to R_S$ defined by $C(i)(x) = \frac{x}{1}$, 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,

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

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

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

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.** $I(R) \text{Ker}(P) = 0$.

**Proof.** Let $x = \sum_i a_i [r_i] \in \text{Ker}(P)$, 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 $x = \sum_i a_i [r_i] \in \text{Ker}(P)$, 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

$$\sum_i a_i r_i^2 = \sum_i a_i [r_i^2] + c[2] = \sum_i a_i^2 [r_i^2] + \sum_i r_i^2 [a_i] + c[2]$$

$$= \sum_i a_i^2 (r_i^2 + r_i) [r_i] + \sum_i r_i^2 [a_i] + c[2],$$

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

where $c, d$ are constants.
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 \( x = \sum_i a_i [r_i] \in \text{Ker}(P) \) 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 \( \text{Ker}(P) = 0 \).

**Case 2:** \( I(R) \) is the maximal ideal (this means that the quotient field of \( R \) has exactly two elements). Let \( x \in \text{Ker}(P) \). 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 \( \text{Ker}(P) = 0 \).

5. **Proof of the theorem: general case.** Let \( x = \sum_i a_i [r_i] \in \text{Ker}(P) \). 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**


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)