BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 62, No. 1, 2014

COMMUTATIVE ALGEBRA

On n-derivations and Relations between Elements $r^n - r$ for Some n

by

Maciej MACIEJEWSKI and Andrzej PRÓSZYŃSKI

Presented by Andrzej SCHINZEL

Summary. We find complete sets of generating relations between the elements $[r] = r^n - r$ for $n = 2^l$ and for $n = 3$. One of these relations is the n-derivation property $[rs] = r^n[s] + s[r]$, $r, s \in R$.

1. Introduction. Let R be a commutative ring with 1. In [2], the second author introduced the ideals $I_n(R)$ generated by all elements $r^n - r$ where $r \in R$. It follows from [2, Proposition 5.5] that $I_n(R)$ is precisely the intersection of all maximal ideals M of R such that $|R/M| - 1$ divides $n - 1$ (in particular, for $n = 3$ this means that $|R/M| = 2$ or 3). These ideals are used to find relations satisfied by mappings of higher degrees (see [2]–[5]). The main result of [6] determines generating relations for the elements $r^2 - r$. The purpose of this paper is to find generating relations for the generators $r^n - r$ of $I_n(R)$, where n is a power of 2 or $n = 3$ (Theorem 1). This will be used in [1] to find generating relations for mappings of degree 5; however, the present paper is independent of the theory of higher degree mappings.

If f is a mapping between R-modules and $f(0) = 0$ then we define by induction the functions $\Delta^m f$ in m variables as follows: $\Delta^1 f = f$ and

$$(\Delta^{m+1} f)(x_0, \ldots, x_m) = (\Delta^m f)(x_0 + x_1, x_2, \ldots, x_m) - (\Delta^m f)(x_0, x_2, \ldots, x_m) - (\Delta^m f)(x_1, x_2, \ldots, x_m).$$

Then we have the following formula:

$$f(x_1 + \cdots + x_m) = \sum_{k=1}^{m} \sum_{1<i_1<\cdots<i_k<m} (\Delta^k f)(x_{i_1}, \ldots, x_{i_k}). \tag{1}$$

2010 *Mathematics Subject Classification*: 13C13, 13C05, 11E76.

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

DOI: 10.4064/ba62-1-4

2. Definition and properties of n-derivations and the functor D. Let n be a fixed natural number. By an *n-derivation* over R we will mean a function $f\colon R \to M$, where M is an R-module, satisfying the following condition:

$$(\mathrm{D}_n) \qquad f(rs) = r^n f(s) + sf(r), \qquad r, s \in R.$$

For example, the function $f\colon R \to R$, $f(r) = r^n - r$, is an n-derivation. On the other hand, any (ordinary) derivation is a 1-derivation (observe that we do not assume additivity in our definition).

LEMMA 1. *If f is an n-derivation then for any $r, s \in R$ we have*

(i) $(r^n - r)f(s) = (s^n - s)f(r)$,

(ii) $f(0) = f(1) = 0$,

(iii) *if s is invertible then* $f(s^{-1}) = -s^{-n-1}f(s)$,

(iv) $f(r^2) = (r^n + r)f(r)$,

(v) $f(r^2 s) = r^{2n}f(s) + (r^n s + rs)f(r)$,

(vi) $f(r^3) = (r^{2n} + r^{n+1} + r^2)f(r)$,

(vii) $f(r^{2^k}) = ((r^{2^{k-1}})^n + r^{2^{k-1}})((r^{2^{k-2}})^n + r^{2^{k-2}}) \ldots (r^n + r)f(r)$,

(viii) $(\Delta^k f)(tr_1, \ldots, tr_k) = t^n(\Delta^k f)(r_1, \ldots, r_k)$ *for* $k \geq 2$, $t, r_1, \ldots, r_k \in R$.

If we denote $\tilde{f}(r, s) = sf(r) - rf(s) = s^n f(r) - r^n f(s)$ *for* $r, s \in R$ *then*

(ix) $\tilde{f}(tr, ts) = t^{n+1}\tilde{f}(r, s)$ *for any* $r, s, t \in R$.

Proof. Relation (i) follows from the two symmetric versions of (D_n). The equalities $f(0) = f(1) = 0$ follow from (D_n) for $r = s = 0$ or 1. Using (D_n) and (ii) we obtain $0 = f(1) = f(s \cdot s^{-1}) = s^n f(s^{-1}) + s^{-1}f(s)$, and this gives (iii). Equality (iv) follows from (D_n), (v) from (iv) and (D_n), (vi) from (v), and (vii) by induction from (iv). Moreover, (viii) holds for $k = 2$ since

$$\begin{aligned}(\Delta^2 f)(tr, ts) &= f(tr + ts) - f(tr) - f(ts)\\ &= t^n f(r + s) + (r + s)f(t) - t^n f(r) - rf(t) - t^n f(s) - sf(t)\\ &= t^n(f(r + s) - f(r) - f(s)) = t^n(\Delta^2 f)(r, s),\end{aligned}$$

and for $k > 2$ by induction. Finally, we prove (ix):

$$\tilde{f}(tr, ts) = ts(t^n f(r) + rf(t)) - tr(t^n f(s) + sf(t)) = t^{n+1}\tilde{f}(r, s). \ ■$$

Let $D(R) = D^{(n)}(R)$ denote the R-module generated by all elements $\langle r \rangle$, $r \in R$, with the relations

$$(\mathrm{D}_n) \qquad \langle rs \rangle = r^n \langle s \rangle + s\langle r \rangle, \qquad r, s \in R.$$

Any unitary ring homomorphism $i\colon R \to R'$ induces a module homomorphism $D(i)\colon D(R) \to D(R')$ over i such that $D(i)(\langle r \rangle) = \langle i(r) \rangle$. This shows that D is a functor. Observe that $D(R)$ is a universal object with respect to n-derivations over R, in the sense that any n-derivation can be uniquely expressed as the composition of the canonical n-derivation $d\colon R \to D(R)$, $d(r) = \langle r \rangle$, and an R-homomorphism defined on $D(R)$.

In particular, the n-derivation $f\colon R \to R$, $f(r) = r^n - r$, gives

COROLLARY 1. *There exists an R-homomorphism $P\colon D(R) \to I_n(R)$ such that $P(\langle r \rangle) = r^n - r$ for $r \in R$.*

We now prove that D commutes with localizations. Let S be a multiplicatively closed set in R and let $i\colon R \to R_S$ and $i\colon M \to M_S$ be the canonical homomorphisms, $i(r) = \frac{r}{1}$, $i(m) = \frac{m}{1}$.

PROPOSITION 1. *For any n-derivation $f\colon R \to M$ there exists a unique n-derivation $f_S\colon R_S \to M_S$ satisfying the condition $f_S(i(r)) = i(f(r))$ for $r \in R$. It is given by the formula*

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

or equivalently

$$f_S\left(\frac{r}{s}\right) = \frac{\tilde{f}(r,s)}{s^{n+1}} = \frac{sf(r) - rf(s)}{s^{n+1}}. \tag{3}$$

Moreover, for any $k \geq 2$,

$$(\Delta^k f_S)\left(\frac{r_1}{t}, \dots, \frac{r_k}{t}\right) = \frac{(\Delta^k f)(r_1, \dots, r_k)}{t^n}. \tag{4}$$

Proof. First observe that the right hand sides of (2) and (3) are equal for any n-derivation f. Indeed, the definition of $\tilde{f}$ gives

$$\frac{f(r)}{s} - \left(\frac{r}{s}\right)^n \frac{f(s)}{s} = \frac{s^n f(r) - r^n f(s)}{s^{n+1}} = \frac{\tilde{f}(r,s)}{s^{n+1}}.$$

The required 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 an n-derivation then

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

which gives (2). This proves the uniqueness of f_S.

Now we define f_S by (3). To prove that f_S is properly defined, it suffices to check that the formula remains the same if we replace r by tr and s by ts for any $t \in S$. But this follows from Lemma 1(ix).

It follows by induction that (4) holds for $t = 1$. Then the general case follows from Lemma 1(viii).

It remains to prove (D_n) for f_S. Let $\frac{a}{s}$ and $\frac{b}{s}$ be arbitrary elements of R_S. Using formula (3) we obtain

$$
\begin{aligned}
f_S\Big(\frac{a}{s}\,\frac{b}{s}\Big) &- \Big(\frac{a}{s}\Big)^n f_S\Big(\frac{b}{s}\Big) - \frac{b}{s} f_S\Big(\frac{a}{s}\Big)\\
&= \frac{s^2 f(ab) - abf(s^2)}{s^{2n+2}} - \frac{a^n}{s^n}\frac{sf(b) - bf(s)}{s^{n+1}} - \frac{b}{s}\frac{sf(a) - af(s)}{s^{n+1}}\\
&= \frac{s^2 f(ab) - abf(s^2)}{s^{2n+2}} - \frac{a^n s^2 f(b) - a^n bsf(s)}{s^{2n+2}} - \frac{bs^{n+1} f(a) - abs^n f(s)}{s^{2n+2}}\\
&= \frac{s^2(f(ab) - a^n f(b) - s^{n-1} bf(a)) - ab(f(s^2) - a^{n-1} sf(s) - s^n f(s))}{s^{2n+2}}\\
&= \frac{s^2(b - bs^{n-1})f(a) - ab(s - sa^{n-1})f(s)}{s^{2n+2}}\\
&= \frac{bs((s - s^n)f(a) - (a - a^n)f(s))}{s^{2n+2}} = 0
\end{aligned}
$$

by (D_n) and Lemma 1(i) for f. This completes the proof. ∎

PROPOSITION 2. *There exists an R_S-isomorphism $D(R)_S \approx D(R_S)$ such that* $\frac{\langle r\rangle}{s} \leftrightarrow \frac{1}{s}\big\langle \frac{r}{1}\big\rangle$.

Proof. Proposition 1 applied to the canonical n-derivation $d\colon R \to D(R)$, $d(r) = \langle r\rangle$, gives an n-derivation $d_S\colon R_S \to D(R)_S$ over R_S,

$$d_S\Big(\frac{r}{s}\Big) = \frac{\langle r\rangle}{s} - \Big(\frac{r}{s}\Big)^n \frac{\langle s\rangle}{s}.$$

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

$$g\Big(\Big\langle \frac{r}{s}\Big\rangle\Big) = d_S\Big(\frac{r}{s}\Big) = \frac{\langle r\rangle}{s} - \Big(\frac{r}{s}\Big)^n \frac{\langle s\rangle}{s}.$$

On the other hand, the homomorphism $D(i)\colon D(R) \to D(R_S)$ over $i\colon R \to R_S$, defined by $D(i)(\langle r\rangle) = \langle \frac{r}{1}\rangle$, gives an R_S-homomorphism $h\colon D(R)_S \to D(R_S)$ such that

$$h\Big(\frac{\langle r\rangle}{s}\Big) = \frac{1}{s}\Big\langle \frac{r}{1}\Big\rangle.$$

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

$$g\Big(h\Big(\frac{\langle r\rangle}{s}\Big)\Big) = \frac{1}{s} g\Big(\Big\langle \frac{r}{1}\Big\rangle\Big) = \frac{1}{s}\Big(\frac{\langle r\rangle}{1} - \Big(\frac{r}{1}\Big)^n \frac{\langle 1\rangle}{1}\Big) = \frac{\langle r\rangle}{s}$$

by Lemma 1(ii). On the other hand, using Lemma 1(iii) and (D) we compute that

$$h\left(g\left(\left\langle\frac{r}{s}\right\rangle\right)\right) = h\left(\frac{\langle r\rangle}{s} - \left(\frac{r}{s}\right)^n \frac{\langle s\rangle}{s}\right) = \frac{1}{s}\left\langle\frac{r}{1}\right\rangle - \frac{r^n}{s^{n+1}}\left\langle\frac{s}{1}\right\rangle$$
$$= \frac{1}{s}\left\langle\frac{r}{1}\right\rangle + \left(\frac{r}{1}\right)^n\left\langle\frac{1}{s}\right\rangle = \left\langle\frac{r}{1}\,\frac{1}{s}\right\rangle = \left\langle\frac{r}{s}\right\rangle.$$

Hence h is an isomorphism, as required. ■

3. C-functions of degree $n = 2^l$. Let n be a fixed natural number of the form $n = 2^l$, $l = 1, 2, \ldots$. By a *C-function of degree n over R* we will mean any n-derivation $f\colon R \to M$ satisfying the additional condition

$$(\mathrm{C}_n) \qquad f(r+s) = f(r) + f(s) + p(r,s)f(-1), \qquad r, s \in R,$$

or equivalently

$$(\mathrm{C}'_n) \qquad (\Delta^2 f)(r,s) = p(r,s)f(-1), \qquad r, s \in R,$$

where

$$p(r,s) = \sum_{k=1}^{n-1} \frac{1}{2}\binom{n}{k} r^{n-k}s^k$$

(note that $\frac{1}{2}\binom{n}{k} \in \mathbb{Z}$ for $k = 1, \ldots, n-1$ because of the shape of n). Using generalized Newton symbols

$$\begin{aligned}(i_1, \ldots, i_k) &= \frac{(i_1 + \cdots + i_k)!}{i_1! \ldots i_k!} \\ &= \binom{i_1 + \cdots + i_k}{i_k}\binom{i_1 + \cdots + i_{k-1}}{i_{k-1}} \cdots \binom{i_1 + i_2}{i_2} \\ &= (i_1 + \cdots + i_{k-1}, i_k)(i_1, \ldots, i_{k-1})\end{aligned}$$

we define the following generalization of $p(r,s)$:

$$p(r_1, \ldots, r_k) = \sum \frac{1}{2}(i_1, \ldots, i_k) r_1^{i_1} \ldots r_k^{i_k},$$

where the sum is over all systems of non-negative integers $i_1 \ldots, i_k$ such that $i_1 + \cdots + i_k = n$ and at least two i_j are non-zero (then all the coefficients in the sum are integers).

LEMMA 2. *For any $r_1, \ldots, r_k, r_{k+1} \in R$ we have*

(i) $p(r_1, \ldots, r_k, r_{k+1}) = p(r_1 + \cdots + r_k, r_{k+1}) + p(r_1, \ldots, r_k)$,
(ii) $f(\sum_{i=1}^k r_i) = \sum_{i=1}^k f(r_i) + p(r_1, \ldots, r_k)f(-1)$

provided that f is a C-function of degree n.

Proof. (i) The generalized Newton formula shows that

$$\begin{aligned}
p(r_1+\cdots+r_k, r_{k+1}) &= \sum_{\substack{j_1+j_2=n\\ j_1,j_2>0}} \frac{1}{2}(j_1,j_2)(r_1+\cdots+r_k)^{j_1} r_{k+1}^{j_2}\\
&= \sum_{\substack{j_1+j_2=n\\ j_1,j_2>0}} \sum_{i_1+\cdots+i_k=j_1} \frac{1}{2}(j_1,j_2)(i_1,\ldots,i_k)(r_1^{i_1}\cdots r_k^{i_k})r_{k+1}^{j_2}\\
&= \sum_{\substack{i_1+\cdots+i_{k+1}=n\\ i_1+\cdots+i_k>0,\, i_{k+1}>0}} \frac{1}{2}(i_1+\cdots+i_k, i_{k+1})(i_1,\ldots,i_k) r_1^{i_1}\cdots r_k^{i_k} r_{k+1}^{i_{k+1}}\\
&= \sum_{\substack{i_1+\cdots+i_{k+1}=n\\ i_1+\cdots+i_k>0,\, i_{k+1}>0}} \frac{1}{2}(i_1,\ldots,i_k,i_{k+1}) r_1^{i_1}\cdots r_{k+1}^{i_{k+1}}.
\end{aligned}$$

Since $(i_1,\ldots,i_k,0)=(i_1,\ldots,i_k)$, the above is equal to $p(r_1,\ldots,r_k,r_{k+1}) - p(r_1,\ldots,r_k)$, as required.

(ii) For $k=2$ see (C_n). If (ii) holds for some $k\ge 2$ then, by (C_n) and (i),

$$\begin{aligned}
f\Big(\sum_{i=1}^{k+1} r_i\Big) &= f\Big(\sum_{i=1}^{k} r_i + r_{k+1}\Big)\\
&= f\Big(\sum_{i=1}^{k} r_i\Big) + f(r_{k+1}) + p\Big(\sum_{i=1}^{k} r_i, r_{k+1}\Big)f(-1)\\
&= \sum_{i=1}^{k} f(r_i) + p(r_1,\ldots,r_k)f(-1) + f(r_{k+1}) + p(r_1+\cdots+r_k, r_{k+1})f(-1)\\
&= \sum_{i=1}^{k+1} f(r_i) + p(r_1,\ldots,r_{k+1})f(-1). \ \blacksquare
\end{aligned}$$

Since $n=2^l$ is even, we have $(-1)^n-(-1)=2$, and hence Lemma 1(i) gives $2f(r)=(r^n-r)f(-1)$. The function $f\colon R\to R$, $f(r)=r^n-r$, is a C-function of degree n. Indeed, it is an n-derivation and

$$\begin{aligned}
(r+s)^n-(r+s)-(r^n-r)-(s^n-s) &= \sum_{k=0}^{n}\binom{n}{k} r^{n-k}s^k - r^n - s^n\\
&= 2\sum_{k=1}^{n-1}\frac{1}{2}\binom{n}{k} r^{n-k}s^k = 2p(r,s) = p(r,s)f(-1)
\end{aligned}$$

by the Newton binomial formula. Later, we prove that it is a universal C-function of degree n (Theorem 1).

4. C-functions of degree 3. By a *C-function of degree* 3 *over* R we will mean any 3-derivation $f\colon R\to M$ satisfying the following additional conditions for any $a, b, r, s, t \in R$:

(C1) $$3sf(r) - 3rf(s) = (r - s)(\Delta^2 f)(r, s),$$

(C2) $$(\Delta^2 f)(ar^3, bs^3) - (\Delta^2 f)(ar, bs) = 3a^2bf(r^2s) + 3ab^2f(rs^2),$$

(C3) $$(\Delta^2 f)(r + s, t) = (\Delta^2 f)(r, t) + (\Delta^2 f)(s, t) + rstf(2).$$

Observe that conditions (C1) and (C3) can be replaced respectively by

(C1′) $$3\tilde{f}(r, s) = (r - s)(\Delta^2 f)(r, s),$$

(C3′) $$(\Delta^3 f)(r, s, t) = rstf(2).$$

Lemma 3. *If $f: R \to M$ is a C-function of degree 3 then for any $r, s, t \in R$ and for any finite set of $r_i \in R$ we have*

(i) $$6f(r) = (r^3 - r)f(2),$$

(ii) $$(t^3 - t)(\Delta^2 f)(r, s) = (3r^2s + 3rs^2)f(t),$$

(iii) $$\Delta^4 f = 0,$$

(iv) $$f\Big(\sum_i r_i\Big) = \sum_i f(r_i) + \sum_{i<j}(\Delta^2 f)(r_i, r_j) + \sum_{i<j<k} r_i r_j r_k f(2).$$

Proof. Equality (i) is given by Lemma 1(i) for $n = 3$ and $s = 2$. Property (ii) is obtained from the definition of $\Delta^2 f$ and Lemma 1(i). Indeed,

$$\begin{aligned}(t^3 - t)(\Delta^2 f)(r, s) &= (t^3 - t)(f(r + s) - f(r) - f(s)) \\ &= ((r + s)^3 - (r + s))f(t) - (r^3 - r)f(t) - (s^3 - s)f(t) \\ &= (3r^2s + 3rs^2)f(t).\end{aligned}$$

Equality (iii) holds, since $\Delta^3 f$ is trilinear by (C3′). Finally, (iv) follows from the formula (1) of the introduction, (C3′) and (iii) above. ∎

Example 1. We show that the mapping $f: R \to R$, $f(r) = r^3 - r$, is a C-function of degree 3. First observe that

(5) $$(\Delta^2 f)(r, s) = 3r^2s + 3rs^2, \qquad (\Delta^3 f)(r, s, t) = 6rst.$$

Indeed,

$$\begin{aligned}(\Delta^2 f)(r, s) &= f(r + s) - f(r) - f(s) \\ &= (r + s)^3 - (r + s) - (r^3 - r) - (s^3 - s) = 3r^2s + 3rs^2, \\ (\Delta^3 f)(r, s, t) &= (\Delta^2 f)(r + s, t) - (\Delta^2 f)(r, t) - (\Delta^2 f)(s, t) \\ &= 3(r + s)^2t + 3(r + s)t^2 - (3r^2t + 3rt^2) - (3s^2t + 3st^2) = 6rst.\end{aligned}$$

We will check conditions (C1), (C2), (C3′):

(C1) $3sf(r) - 3rf(s) - (r-s)(\Delta^2 f)(r,s)$
$$= 3s(r^3 - r) - 3r(s^3 - s) - (r-s)(3r^2s + 3rs^2) = 0,$$

(C2) $(\Delta^2 f)(ar^3, bs^3) - (\Delta^2 f)(ar, bs) - 3a^2bf(r^2s) - 3ab^2f(rs^2)$
$$= 3(ar^3)^2bs^3 + 3ar^3(bs^3)^2 - (3(ar)^2bs + 3ar(bs)^2)$$
$$-3a^2b((r^2s)^3 - r^2s) - 3ab^2((rs^2)^3 - rs^2)$$
$$= 3a^2b(r^6s^3 - r^2s - r^6s^3 + r^2s) + 3ab^2(r^3s^6 - rs^2 - r^3s^6 + rs^2) = 0,$$

and (C3′) follows directly from (5) because $f(2) = 6$.

5. The functors $C = C^{(n)}$. If $n = 2^l$ then we denote by $C(R) = C^{(n)}(R)$ the R-module generated by the elements $[r]$, $r \in R$, with the relations

(D) $$[rs] = r^n[s] + s[r], \quad r, s \in R,$$

(C) $$[r+s] = [r] + [s] + p(r,s)[-1], \quad r, s \in R.$$

If $n = 3$ then we denote by $C(R) = C^{(3)}(R)$ the R-module generated by the elements $[r]$, $r \in R$, with the relations

(D) $$[rs] = r^3[s] + s[r], \quad r, s \in R,$$

(C1) $$3s[r] - 3r[s] = (r-s)[r,s], \quad r, s \in R,$$

(C2) $$[ar^3, bs^3] - [ar, bs] = 3a^2b[r^2s] + 3ab^2[rs^2], \quad a, b, r, s \in R,$$

(C3) $$[r+s, t] = [r,t] + [s,t] + rst[2], \quad r, s, t \in R,$$

where $[r,s] = [r+s] - [r] - [s] = (\Delta^2[\ ])(r,s)$.

Let $n = 2^l$ or 3. Any unitary ring homomorphism $i\colon R \to R'$ induces a module homomorphism $C(i)\colon C(R) \to C(R')$ over i such that $C(i)([r]) = [i(r)]$. This shows that C is a functor. Observe that $C(R)$ is a universal object with respect to C-functions of degree n over R, meaning that any C-function of degree n can be uniquely expressed as a composition of the canonical C-function $c\colon R \to C(R)$, $c(r) = [r]$, and an R-homomorphism defined on $C(R)$.

In particular, the C-function $f\colon R \to R$, $f(r) = r^n - r$, gives

COROLLARY 2. *There exists an R-homomorphism $P\colon C(R) \to I_n(R)$ such that $P([r]) = r^n - r$ for $r \in R$.*

Our goal is to show that P is an isomorphism (Theorem 1). As a first step, we prove that C commutes with localizations. Let S be a multiplicatively closed set in R and let $i\colon R \to R_S$ and $i\colon M \to M_S$ be the canonical homomorphisms, $i(r) = \frac{r}{1}$, $i(m) = \frac{m}{1}$.

Proposition 3. *If $f\colon R \to M$ is a C-function of degree n then the only n-derivation $f_S\colon R_S \to M_S$ satisfying the condition $f_S(i(r)) = i(f(r))$ for all $r \in R$ (Proposition 1) is a C-function of degree n.*

Proof. First let $n = 2^l$. Observe that $f_S(-1) = \frac{f(-1)}{1}$ and

$$p\left(\frac{a}{s}, \frac{b}{s}\right) = \sum_{k=1}^{n-1} \frac{1}{2}\binom{n}{k}\left(\frac{a}{s}\right)^{n-k}\left(\frac{b}{s}\right)^{k} = \frac{p(a,b)}{s^n}.$$

Then using Proposition 1 we compute that

$$(\mathrm{C}'_n) \quad (\varDelta^2 f_S)\left(\frac{a}{s}, \frac{b}{s}\right) = \frac{(\varDelta^2 f)(a,b)}{s^n} = \frac{p(a,b)f(-1)}{s^n} = p\left(\frac{a}{s}, \frac{b}{s}\right) f_S(-1).$$

Let now $n = 3$. We will prove that f_S satisfies $(\mathrm{C}1'), (\mathrm{C}2), (\mathrm{C}3')$. Let $\frac{a}{t}, \frac{b}{t}, \frac{c}{t}, \frac{r}{t}, \frac{s}{t}$ be arbitrary elements of R_S.

(C1′) It follows from Lemma 1(ix) and Proposition 1 that

$$\begin{aligned}3\tilde{f}_S\left(\frac{r}{t}, \frac{s}{t}\right) &= 3\frac{1}{t^4}\tilde{f}_S\left(\frac{r}{1}, \frac{s}{1}\right) = 3\frac{\tilde{f}(r,s)}{t^4} \\ &= \frac{(r-s)(\varDelta^2 f)(r,s)}{t^4} = \left(\frac{r}{t} - \frac{s}{t}\right)(\varDelta^2 f_S)\left(\frac{r}{t}, \frac{s}{t}\right).\end{aligned}$$

(C2) Using Proposition 1 and Lemma 3(ii) we obtain

$$\begin{aligned}&(\varDelta^2 f_S)\left(\frac{a}{t}\left(\frac{r}{t}\right)^3, \frac{b}{t}\left(\frac{s}{t}\right)^3\right) - (\varDelta^2 f_S)\left(\frac{a}{t}\frac{r}{t}, \frac{b}{t}\frac{s}{t}\right) \\ &\quad = \frac{(\varDelta^2 f)(ar^3, bs^3)}{t^{12}} - \frac{(\varDelta^2 f)(ar, bs)}{t^6} \\ &\quad = \frac{(\varDelta^2 f)(ar^3, bs^3) - (\varDelta^2 f)(ar, bs)}{t^{12}} - \frac{(t^9 - t^3)(\varDelta^2 f)(ar, bs)}{t^{15}} \\ &\quad = \frac{3a^2bt^3 f(r^2 s) + 3ab^2t^3 f(rs^2)}{t^{15}} - \frac{(3(ar)^2bs + 3ar(bs^2))f(t^3)}{t^{15}} \\ &\quad = 3\frac{a^2b}{t^3}\,\frac{t^3 f(r^2 s) - r^2 s f(t^3)}{t^{12}} + 3\frac{ab^2}{t^3}\,\frac{t^3 f(rs^2) - rs^2 f(t^3)}{t^{12}} \\ &\quad = 3\frac{a^2b}{t^3} f_S\left(\frac{r^2 s}{t^3}\right) + 3\frac{ab^2}{t^3} f_S\left(\frac{rs^2}{t^3}\right) \\ &\quad = 3\left(\frac{a}{t}\right)^2\frac{b}{t} f_S\left(\left(\frac{r}{t}\right)^2\frac{s}{t}\right) + 3\frac{a}{t}\left(\frac{b}{t}\right)^2 f_S\left(\frac{r}{t}\left(\frac{s}{t}\right)^2\right).\end{aligned}$$

(C3′) Since $f_S(\frac{2}{1}) = \frac{f(2)}{1}$, it follows from Proposition 1 that

$$(\varDelta^3 f_S)\left(\frac{a}{t}, \frac{b}{t}, \frac{c}{t}\right) = \frac{(\varDelta^3 f)(a,b,c)}{t^3} = \frac{abcf(2)}{t^3} = \frac{a}{t}\,\frac{b}{t}\,\frac{c}{t}\,\frac{f(2)}{1}. \quad \blacksquare$$

As in Section 2, we deduce

Proposition 4. *There exists an R_S-isomorphism $C(R)_S \approx C(R_S)$ such that $\frac{[r]}{s} \leftrightarrow \frac{1}{s}\left[\frac{r}{1}\right]$.*

Proof. Replace $\langle r\rangle$ by $[r]$ in the proof of Proposition 2. ∎

6. The main lemmas. Let $n = 2^l$ or $n = 3$. We consider the kernel of the R-homomorphism $P\colon C(R) \to I_n(R)$, $P([r]) = r^n - r$ for $r \in R$.

Lemma 4. $I_n(R)\,\mathrm{Ker}(P) = 0$.

Proof. Let $x = \sum_i a_i[r_i] \in \mathrm{Ker}(P)$, that is, $\sum_i a_i(r_i^n - r_i) = 0$. Then (D) shows that

$$(r^n - r)x = \sum_i a_i(r^n - r)[r_i] = \sum_i a_i(r_i^n - r_i)[r] = 0[r] = 0. \ ∎$$

Let $n = 2^l$. Lemmas 2(ii) and 1(vii) give the following formulas:

$$\Big[\sum_{i=1}^k r_i\Big] = \sum_{i=1}^k [r_i] + p(r_1,\ldots,r_k)[-1], \tag{6}$$

$$[r^n] = [r^{2^l}] = ((r^{2^{l-1}})^n + r^{2^{l-1}})((r^{2^{l-2}})^n + r^{2^{l-2}})\ldots(r^n + r)[r]. \tag{7}$$

Lemma 5. *Let $n = 2^l$ and $x = \sum_{i=1}^k a_i[r_i] \in \mathrm{Ker}(P)$, where one of the r_i is -1. If all a_i belong to $I_n(R)^m$ for some $m \ge 0$ then $x = \sum_{i=1}^k b_i[r_i]$ where all b_i belong to $I_n(R)^{nm+1}$.*

Proof. By the assumption, $\sum_{i=1}^k a_i r_i^n = \sum_{i=1}^k a_i r_i$. Using (6) we obtain

$$\Big[\sum_{i=1}^k a_i r_i\Big] = \sum_{i=1}^k [a_i r_i] + p[-1] = \sum_{i=1}^k a_i[r_i] + \sum_{i=1}^k r_i^n[a_i] + p[-1],$$

$$\Big[\sum_{i=1}^k a_i r_i^n\Big] = \sum_{i=1}^k [a_i r_i^n] + q[-1] = \sum_{i=1}^k a_i^n[r_i^n] + \sum_{i=1}^k r_i^n[a_i] + q[-1],$$

where

$$p = p(a_1r_1,\ldots,a_kr_k) = \sum \frac{1}{2}(i_1,\ldots,i_k)a_1^{i_1}\ldots a_k^{i_k} r_1^{i_1}\ldots r_k^{i_k},$$

$$q = p(a_1r_1^n,\ldots,a_kr_k^n) = \sum \frac{1}{2}(i_1,\ldots,i_k)a_1^{i_1}\ldots a_k^{i_k}(r_1^{i_1}\ldots r_k^{i_k})^n,$$

and the sums are over all systems of non-negative integers $i_1,\ldots,i_k$ such that $i_1 + \cdots + i_k = n$ and at least two i_j are non-zero. Since

$$\sum_{i=1}^k a_i[r_i] + \sum_{i=1}^k r_i^n[a_i] + p[-1] = \sum_{i=1}^k a_i^n[r_i^n] + \sum_{i=1}^k r_i^n[a_i] + q[-1],$$

we obtain

$$x = \sum_{i=1}^{k} a_i[r_i] = \sum_{i=1}^{k} a_i^n[r_i^n] + (q-p)[-1]$$
$$= \sum_{i=1}^{k} a_i^n((r_i^{2^{l-1}})^n + r_i^{2^{l-1}})((r_i^{2^{l-2}})^n + r_i^{2^{l-2}}) \dots$$
$$\dots (r_i^n + r_i)[r_i] + (q-p)[-1]$$

by (7). Since $a_i \in I_n(R)^m$ it follows that $a_i^n \in I_n(R)^{nm}$ and $r_i^n + r_i = (-r_i)^n - (-r_i) \in I_n(R)$, since n is even. Hence

$$a_i^n((r_i^{2^{m-1}})^n + r_i^{2^{m-1}})((r_i^{2^{m-2}})^n + r_i^{2^{m-2}}) \dots (r_i^n + r_i) \in I_n(R)^{nm+1}.$$

Moreover, $a_1^{i_1} \dots a_k^{i_k} \in I_n(R)^{nm}$ since $a_i \in I_n(R)^m$ and $i_1 + \dots + i_k = n$, and $(r_1^{i_1} \dots r_k^{i_k})^n - r_1^{i_1} \dots r_k^{i_k} \in I_n(R)$. Hence

$$q - p = \sum \frac{1}{2}(i_1, \dots, i_k) a_1^{i_1} \dots a_k^{i_k}((r_1^{i_1} \dots r_k^{i_k})^n - r_1^{i_1} \dots r_k^{i_k}) \in I_n(R)^{nm+1}.$$

This completes the proof. ∎

The above lemma gives immediately

Corollary 3. *Let $n = 2^l$ and $x = \sum_{i=1}^{k} a_i[r_i] \in \operatorname{Ker}(P)$. Let M denote the submodule of $C(R)$ generated by $[r_1], \dots, [r_k]$ and $[-1]$. Then*

$$x \in \bigcap_{m=0}^{\infty} I_n(R)^m M.$$

Let now $n = 3$. Lemmas 3(iv) and 1(vi) give the formulas

$$\Big[\sum_i r_i\Big] = \sum_i [r_i] + \sum_{i<j} [r_i, r_j] + \sum_{i<j<k} r_i r_j r_k [2] \tag{8}$$

for any finite set of elements $r_i \in R$, and

$$[r^3] = (r^6 + r^4 + r^2)[r], \qquad r \in R. \tag{9}$$

Lemma 6. *Let $n = 3$ and $x = \sum_i a_i[r_i] \in \operatorname{Ker}(P)$ where one of the r_i is equal to 2. If all a_i belong to $I_3(R)^m$ for some $m \geq 0$ and one of the following conditions is satisfied:*

(1) *all r_i belong to $I_3(R)$, or*
(2) *$3 \in I_3(R)$,*

then $x = \sum_i b_i[r_i]$ where all b_i belong to $I_3(R)^{3m+1}$.

Proof. By the assumption, $\sum_i a_i r_i^3 = \sum_i a_i r_i$. Using (8), (9) and (D) we obtain

$$\begin{aligned}\Big[\sum_i a_i r_i\Big] &= \sum_i [a_i r_i] + \sum_{i<j}[a_i r_i, a_j r_j] + \sum_{i<j<k} a_i r_i a_j r_j a_k r_k[2] \\ &= \sum_i a_i[r_i] + \sum_i r_i^3[a_i] + \sum_{i<j}[a_i r_i, a_j r_j] + \sum_{i<j<k} a_i r_i a_j r_j a_k r_k[2]\end{aligned}$$

and

$$\begin{aligned}\Big[\sum_i a_i r_i^3\Big] &= \sum_i [a_i r_i^3] + \sum_{i<j}[a_i r_i^3, a_j r_j^3] + \sum_{i<j<k} a_i r_i^3 a_j r_j^3 a_k r_k^3[2] \\ &= \sum_i a_i^3[r_i^3] + \sum_i r_i^3[a_i] + \sum_{i<j}[a_i r_i^3, a_j r_j^3] + \sum_{i<j<k} a_i r_i^3 a_j r_j^3 a_k r_k^3[2] \\ &= \sum_i a_i^3(r_i^6 + r_i^4 + r_i^2)[r_i] + \sum_i r_i^3[a_i] + \sum_{i<j}[a_i r_i^3, a_j r_j^3] \\ &\quad + \sum_{i<j<k} a_i r_i^3 a_j r_j^3 a_k r_k^3[2].\end{aligned}$$

Since the left hand sides above are equal, (C2) and Lemma 1(v) give

$$\begin{aligned}x &= \sum_i a_i[r_i] \\ &= \sum_i a_i^3(r_i^6 + r_i^4 + r_i^2)[r_i] + \sum_{i<j}[a_i r_i^3, a_j r_j^3] - \sum_{i<j}[a_i r_i, a_j r_j] \\ &\quad + \sum_{i<j<k} a_i r_i^3 a_j r_j^3 a_k r_k^3[2] - \sum_{i<j<k} a_i r_i a_j r_j a_k r_k[2] \\ &= \sum_i a_i^3(r_i^6 + r_i^4 + r_i^2)[r_i] + \sum_{i<j} 3a_i^2 a_j[r_i^2 r_j] + \sum_{i<j} 3a_i a_j^2[r_i r_j^2] \\ &\quad + \sum_{i<j<k} a_i a_j a_k(r_i^3 r_j^3 r_k^3 - r_i r_j r_k)[2] \\ &= \sum_i a_i^3((r_i^2)^3 - r_i^2 + r_i(r_i^3 - r_i) + 3r_i^2)[r_i] \\ &\quad + \sum_{i<j} 3a_i^2 a_j(r_i^6[r_j] + r_i^3 r_j[r_i] + r_i r_j[r_i]) \\ &\quad + \sum_{i<j} 3a_i a_j^2(r_j^6[r_i] + r_i r_j^3[r_j] + r_i r_j[r_j]) \\ &\quad + \sum_{i<j<k} a_i a_j a_k((r_i r_j r_k)^3 - r_i r_j r_k)[2].\end{aligned}$$

Observe that $(r_i^2)^3 - r_i^2$, $r_i^3 - r_i$, $(r_i r_j r_k)^3 - r_i r_j r_k \in I_3(R)$; hence the summands not multiplied by 3 belong to $I_3(R)^{3m+1}$. If all r_i belong to $I_3(R)$, or

$3 \in I_3(R)$, the remaining summands also belong to $I_3(R)^{3m+1}$. This means that in both cases all coefficients in the above sums belong to $I_3(R)^{3m+1}$. ∎

COROLLARY 4. *Let $n = 3$ and $x = \sum_i a_i[r_i] \in \mathrm{Ker}(P)$. Let M denote the submodule of $C(R)$ generated by all $[r_i]$ and $[2]$. If one of the following conditions is satisfied:*

(1) *all r_i and 2 belong to $I_3(R)$, or*
(2) $3 \in I_3(R)$,

then $x \in \bigcap_{m=0}^{\infty} I_3(R)^m M$.

7. The main theorem. Proving the following fact is the purpose of this paper:

THEOREM 1. *Let $C(R) = C^{(n)}(R)$ where $n = 2^l$, $l = 1, 2, \ldots$ or $n = 3$. Then $P\colon C(R) \to I_n(R)$, $P([r]) = r^n - r$ for $r \in R$, is an R-isomorphism. In other words, if $n = 2^l$, $l = 1, 2, \ldots$, then the following are generating relations between the generators $[r] = r^n - r$ of $I_n(R)$:*

(D) $$[rs] = r^n[s] + s[r], \qquad r, s \in R,$$

(C) $$[r + s] = [r] + [s] + p(r, s)[-1], \qquad r, s \in R,$$

where
$$p(r, s) = \sum_{k=1}^{n-1} \frac{1}{2}\binom{n}{k} r^{n-k}s^k;$$

and if $n = 3$ then the following are generating relations between the generators $[r] = r^3 - r$ of $I_3(R)$:

(D) $[rs] = r^3[s] + s[r], \qquad r, s \in R,$

(C1) $3s[r] - 3r[s] = (r - s)[r, s], \qquad r, s \in R,$

(C2) $[ar^3, bs^3] - [ar, bs] = 3a^2b[r^2s] + 3ab^2[rs^2], \qquad a, b, r, s \in R,$

(C3) $[r + s, t] = [r, t] + [s, t] + rst[2], \qquad r, s, t \in R,$

where $[r, s] = [r + s] - [r] - [s] = (\Delta^2[\ ])(r, s)$.

Proof. Our goal is to prove that $\mathrm{Ker}(P) = 0$.

Noetherian case. Assume that R is noetherian. By Proposition 4 we can assume that R is local and noetherian with quotient field K. Then $I_n(R)$ is the maximal ideal if $|K| - 1 \mid n - 1$, and $I_n(R) = R$ otherwise (see Introduction).

If $I_n(R) = R$ then Lemma 4 shows that $\mathrm{Ker}(P) = 0$, as we want. So let $I_n(R)$ be the maximal ideal of R.

Assume first that $n = 2^l$. Let $x \in \mathrm{Ker}(P)$. Define the submodule M as in Corollary 3 and observe that it is finitely generated over a local noetherian ring. Then the intersection in the corollary is zero by the Krull intersection theorem, and hence $x = 0$. This proves that $\mathrm{Ker}(P) = 0$.

Let now $n = 3$. Then $|K| = 2$ or 3.

CASE 1: $|K| = 3$. Then $3 \in I_3(R)$. Let $x \in \mathrm{Ker}(P)$. Define M as in Corollary 4 and observe that condition (2) of the corollary holds. As before, $x = 0$ by the Krull intersection theorem, and so $\mathrm{Ker}(P) = 0$.

CASE 2: $|K| = 2$. Then $2 \in I_3(R)$ and $K = \{I_3(R), 1 + I_3(R)\}$. Hence the set of units of R is $1 + I_3(R)$. Condition (C1) for $s = 1$ gives

$$3[r] - 3r[1] = (r-1)([r+1] - [r] - [1]),$$

and since $[1] = 0$ this shows that $(r+2)[r] = (r-1)[r+1]$. So if r is invertible then so is $r + 2$, and

$$[r] = \frac{r-1}{r+2}[r+1]$$

where $r + 1$ is non-invertible. Let $x = \sum_i a_i[r_i] \in \mathrm{Ker}(P)$. If one of r_i is invertible then using the above formula we can replace $[r_i]$ by $\frac{r_i-1}{r_i+2}[r_i+1]$. So we can assume that all r_i above are non-invertible, that is, belong to $I_3(R)$. Since $2 \in I_3(R)$, condition (1) of Corollary 4 holds, and as before we find that $x = 0$, and finally $\mathrm{Ker}(P) = 0$.

General case. Let $x = \sum_i a_i[r_i] \in \mathrm{Ker}(P)$. Define S to be the subring of R generated by all a_i and r_i. Since S is a finitely generated ring, and hence noetherian, the previous part of the proof shows that $P\colon C(S) \to S$ is injective. Let $i\colon S \to R$ 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 II*, in preparation.

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

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

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

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

[6] A. Prószyński, *Relations between elements* $r^2 - r$, Bull. Polish Acad. Sci. Math. 55 (2007), 317–323.

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

Received April 9, 2014;
received in final form June 6, 2014 (7967)