A remark on polynomial functions over finite commutative rings with identity

Günther Eigenthaler and Winfried B. Müller

Abstract. In the present paper, the degree of polynomial functions on a finite commutative ring R with identity is investigated. An upper bound for the degree is given (Theorem 3) with the help of a reduction formula for powers (Theorem 1).

1. Let R be a *commutative ring with identity*, $R[x_1,\dots,x_k]$ the *polynomial ring in k indeterminates* $x_1,\dots,x_k$ *over* R, $F_k(R)$ the *full k-place function ring over* R and $P_k(R)$ the *ring of k-place polynomial functions on* R. (For the basic notions and results of algebra used here and in the following see e.g. Lausch-Nöbauer (1973) and Atiyah-Macdonald (1969).

There exists a surjective homomorphism σ from $R[x_1,\dots,x_k]$ onto $P_k(R)$, which assigns to each polynomial

$$f = \Sigma a_{i_1\dots i_k} x_1^{i_1} \dots x_k^{i_k} \in R[x_1,\dots,x_k]$$

a polynomial function $\sigma f \in P_k(R)$ defined by

$$(\sigma f)(b_1,\dots,b_k) = \Sigma a_{i_1\dots i_k} b_1^{i_1} \dots b_k^{i_k},\ (b_1,\dots,b_k) \in R^k.$$

(See Lausch-Nöbauer (1973), ch. 1, § 6.) For $\psi \in P_k(R)$ let the *degree* $\|\psi\|$ of ψ be the minimum of the degrees of the polynomials $f \in R[x_1,\dots,x_k]$ with $\sigma f = \psi$.

R is said to be *primary* if every zero divisor of R is nilpotent. Every finite commutative ring R with identity is (unique up to isomorphism) a finite direct sum of finite primary rings (cf. Atiyah-Macdonald (1969), ch. 8, Th.8.7).

2. Now we prove the reduction formula for powers. For a finite group G, exp G denotes the *exponent of* G, i.e. the least common multiple of the orders of the elements of G. $U(R)$ denotes the group of units of R. Furthermore, we shall write $|M|$ for the cardinality of a set M, and $[r_1,\dots,r_n]$ for the least cammom multiple of the integers $r_1,\dots,r_n$.

Recebido em agosto de 1978

Theorem 1. *Let the finite commutative ring R with identity be the direct sum $R_1 \oplus \ldots \oplus R_s$ of the primary rings R_i, $n(R_i)$ be the least positive integer e such that $a_i^e = 0$ for all $a_i \in R_i - U(R_i)$ and $n(R) = \max(n(R_1), \ldots, n(R_s))$. Then for any positive integer m, the equation*

$$a^{m+n(R)} = a^{n(R)}$$

holds in R iff $\exp U(R) = [\exp U(R_1), \ldots, \exp U(R_s)]$ divides m.

Proof. i) Suppose that $\exp U(R)$ divides m and let $a = a_1 + \ldots + a_s \in R$ where $a_i \in R_i$. If $a_i \in U(R_i)$, then $a_i^{\exp U(R)} = 1$ and, therefore, $a_i^m = 1$. If $a_i \in R_i - U(R_i)$, then $a_i^{n(R)} = 0$. Thus, in both cases $a_i^{m+n(R)} = a_i^{n(R)}$ showing that $a^{m+n(R)} = a^{n(R)}$.

ii) Suppose that $a^{m+n(R)} = a^{n(R)}$ for all $a \in R$, then $a^m = 1$ for all $a \in U(R)$, which implies that $\exp U(R)$ divides m.

Lemma 2. *Let R be a commutative ring with identity which is a finite direct sum, say $R = R_1 \oplus \ldots \oplus R_s$, and for every $i = 1, \ldots, s$ let J_i be a set of k-tuples of non-negative integers such that for every $\psi \in P_k(R_i)$ there exists a polynomial $f \in R_i[x_1, \ldots, x_k]$ with*

$$f = \sum_{(i_0, \ldots, i_k) \in J_i} a_{i_1 \ldots i_k} x_1^{i_1} \ldots x_k^{i_k}$$

and $\sigma f = \psi$. Then for every $\psi \in P_k(R)$ there exists an $f \in R[x_1, \ldots, x_k]$ with

$$f = \sum_{(i_1, \ldots, i_k) \in J_1 \cup \ldots \cup J_s} a_{i_1 \ldots i_k} x_1^{i_1} \ldots x_k^{i_k} \text{ and } \sigma f = \psi.$$

Proof. Straightforward (cf. also Lausch-Nöbauer (1973), ch.3, Th.3.61).

If R_i is primary, by Theorem 1 we can take in Lemma 2 $J_i = \{0, 1, \ldots, n(R_i) + \exp U(R_i) - 1\}^k$. Therefore, we get the following.

Theorem 3. *Let R be as in Theorem 1, then for every $\psi \in P_k(R)$ there exists an $f \in R[x_1, \ldots, x_k]$ with*

$$f = \sum_{(i_1, \ldots, i_k) \in J} a_{i_1 \ldots i_1} x_1^{i_1} \ldots x_k^{i_k} \text{ and } \sigma f = \psi, \text{ where}$$

$$J = \{0, 1, \ldots, \max_i (n(R_i) + \exp U(R_i)) - 1\}^k.$$

Thus $\| \psi \| \leq k(\max_i (n(R_i) + \exp U(R_i)) - 1)$ for all $\psi \in P_k(R)$.

Furthermore, we get from Theorem 3 and the fact that $P_k(R_1 \oplus \ldots \oplus R_s)$ is isomorphic to $P_k(R_1) \oplus \ldots \oplus P_k(R_s)$ (see Lausch-Nobauer (1973), ch.3, Th.3.61) the following.

Corollary 4. *Let R be as in Theorem 1, then*

$$|P_k(R)| \leq |R_1|^{(n(R_1) + \exp U(R_1))^k} \cdot \ldots \cdot |R_s|^{(n(R_s) + \exp U(R_s))^k}$$

Remark. In case that $|R|^{(\max_j (n(R_j) + \exp U(R_j)))^k} > |R_1|^{(n(R_1) + \exp U(R_1))^k} \cdot \ldots \cdot |R_s|^{(n(R_s) + \exp U(R_s))^k}$ (under the assumption that $|R_i| > 1$ for all i, this holds iff $\max_j (n(R_j) + \exp U(R_j)) > \min_j (n(R_j) + \exp U(R_j))$) the representation of the functions $\psi \in P_k(R)$ by polynomials with the form given in Theorem 3 is not unique, as is easily seen. The converse does not hold (an example is given by $R = Z_9$, the residue class ring of the integers modulo 9; see later).

3. We apply the above results to the case $R = Z_n$, the residue class ring of the ring Z of integers modulo n with $n > 1$. Let $n = p_1^{e_1} \cdot \ldots \cdot p_s^{e_s}$ be the canonical decomposition of n, then Z_n is isomorphic to $Z_{p_1^{e_1}} \oplus \ldots \oplus Z_{p_s^{e_s}}$, and the $Z_{p_i^{e_i}}$ are primary. For a positive prime p and a positive integer e, let

$$m(p^e) = \begin{cases} \frac{1}{2} \varphi(p^e), & \text{if } p = 2 \text{ and } e \geq 3 \\ \varphi(p^e), & \text{otherwise} \end{cases}$$

where φ is the Euler φ-function. Then $m(p^e) = \exp U(Z_{p^e})$ and furthermore $n(Z_{p^e}) = e$. Let n be as above, then $\exp U(Z_n)$ is the least common multiple of the $m(p_i^{e_j})$ and $n(Z_n) = \max(e_1, \ldots, e_s)$. Since, for any positive integers m, e

$$p_i^{m+e} \equiv p_i^e \bmod n$$

implies that $e_i \leq e$, we get from Theorem 1 the following result, which is contained in Singmaster (1966) and is a generalization of Nöbauer (1954) (§1):

Corollary 5. *Let n be as above, then for any positive integers m, e*

$$a^{m+e} \equiv a^e \bmod n$$

holds for all $a \in Z$ iff $[m(p_1^{e_1}), \ldots, m(p_s^{e_s})]$ divides m and $\max(e_1, \ldots, e_s) \leq e$.

In a similar way, Theorem 3 can be specialized for $R = Z_n$ (cf. also Nöbauer (1955), Hilfssatz 7).

For $n = 9$ and $k = 1$, by Hilfssatz 7 of Nöbauer (1955) $|P_k(Z_n)| = 3^9$. whereas the number of polynomials with the form given in Theorem 3 is equal to 3^{16}. This yields the example announced in the Remark after Corollary 4 (other examples are given by $R = Z_4$ and $R = Z_8$).

For another application of Theorem 1 take $R_i = GF(p_i^{e_i})$, the Galois field of order $p_i^{e_i}$ (p_i is a prime). Then $\exp U(R_i) = p_i^{e_i} - 1$ and $n(R_i) = 1$. This yields the following result of Mrkwiczka (1973) (§7):

Corollary 6. $a^{m+1} = a$ *for all* $a \in GF(p_1^{e_1}) \oplus \ldots \oplus GF(p_s^{e_s})$ *iff* $[p_1^{e_1} - 1, \ldots, p_s^{e_s} - 1]$ *divides* m.

References

[1] M. F. Atiyah – I. G. Macdonald (1969), *Introduction to Commutative Algebra* (Addison--Welsley Publ. Comp., Reading (Massachusetts) – London, 1969).

[2] H. Lausch – W. Nöbauer (1973), *Algebra of Polynomials* (North Holland Publ. Comp., Amsterdam-London, 1973).

[3] G. Mrkwiczka (1973), *Über Gruppen von durch Potenzen oder durch Formenvektoren erzeugten Polynompermutationen*, Diss. Univ Wien, 1973.

[4] W. Nöbauer (1954), *Über eine Gruppe der Zahlentheorie*, Monatsh. Math. 58, 181-192.

[5] W. Nöbauer (1955), *Gruppen von Restklassen nach Restpolynomidealen in mehreren Unbestimmten*, Monatsh. Math. 59, 118-145.

[6] D. Singmaster (1966), *A maximal generalization of Fermat's theorem*, Math. Mag. 39, 103-107.

Günther Eigenthaler
Institut für Algebra
u. Math. Strukturtheorie
Technische Universität Wien
Karlsplatz 13
A-1040 Wien
Austria

Winfried B. Müller
Institut für Mathematik
Universität für Bildungs-
wissenschaften
Universitätsstr. 65
A-9010 Klagenfurt
Austria