Notes on vanishing polynomials

By MIKLÓS HOSSZÚ in Miskolc

To Professor László Rédei on his 60th birthday

It is known that there exist rings R in which a polynomial function

$$f_n(x)=a_nx^n+\cdots+a_1x+a_0$$

can vanish identically even if not all coefficients a_k are equal to 0.[1])

Example 1. Let R_n be the ring of a complete residue system of integer numbers modulo n. Then we have

$$\prod_{k=1}^{n}(x-k)=a_nx^n+\cdots+a_0\equiv 0 \pmod n$$

for all $x\in R_n$, however, $a_n=1\neq 0$. Observe that $nx\equiv 0 \pmod n$ is true for all $x\in R_n$.

Example 2. Let R_6 be the ring of a complete residue system of integer numbers modulo 6. Then we have

$$x(x-1)(x-2)(x-3)(x-5)\equiv x^5+x^4-x^3-x^2\equiv 0 \pmod 6$$

for all $x\in R_6$. This is evident for $x=0, 1, 2, 3, 5$ and also for $x=4$ since we have

$$(4-2)(4-1)=6\equiv 0 \pmod 6.$$

Observe that R_6 contains non zero elements of order 2 resp. 3 for which $2a\equiv 0$ resp $3a\equiv 0 \pmod 6$ holds such that $a\not\equiv 0 \pmod 6$.

There arises the problem[2]) to give conditions necessary and sufficient in order that in a ring R an identity

$$a_nx^n+\cdots+a_1x+a_0=b_nx^n+\cdots+b_1x+b_0$$

[1]) Here $x\in R$, further, a_k is taken either from R or if $k\geqq 1$ from the integer numbers; e. g. $x^3-x^2+2x+a_0$ is a polynomial. In the notation we shall take no distinction between the integer 0 and the zero element of R; this leads no to misunderstanding.

[2]) Cf. J. Aczél, Über die Gleichheit der Polynomfunktionen auf Ringen, *Acta Sci. Math.*, **21** (1960), 105—107. See also: Collected Math. Problems of the Inst. of Math. of Kossuth L. Univ. in Debrecen.

implies that the respective coefficients of the polynomials are equal: $a_k = b_k$ $(k = 0, 1, \ldots, n)$. It is clear that this is equivalent with the uniqueness of the identically vanishing polynomial on R. The main result of the present paper is:

Theorem. *Let R be a ring in which (1) R^+ does not contain any element of order $r \leqq n$ (up to 0). Then R has a unique identically vanishing polynomial of degree n if and only if (2) the set of elements of the form x^k $(x \in R)$ possesses a unique left anullator for every fixed $k = 1, \ldots, n$.*

Proof. The necessity of (2) is evident. On the other hand, in order to prove the sufficiency, let us suppose (2) on a ring R satisfying (1) and introduce the difference operator Δ_z^k by

$$\Delta_z^k = \Delta_z^{k-1} \Delta_z, \quad \Delta_z^1 f(x) = f(x+z) - f(x); \qquad x, y \in R.$$

Then

$$f_n(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0$$

implies

$$\Delta_z^n f_n(x) = n!\, a_n z^n \equiv 0.$$

Thus, by (2), we have $n!\, a_n z^n = 0$. But (1) involves the cancellability by $n, n-1, \ldots, 2$ and so we have $a_n = 0$. Now, applying the operator Δ_z^{n-1} for the identically vanishing polynomial $f_n(x) - a_n x^n$, in a similar way we get $a_{n-1} = 0$ and, successively, $a_{n-2} = \cdots = a_1 = 0$. Finally, by putting $x = 0$ into $f_n(x)$, we obtain also $a_0 = 0$.

The present proof makes use of the obvious fact that $\Delta_z^k x^k = k!\, z^k$ is true in an arbitrary ring R.

Remarks. **1.** Examples 1 and 2 show that without supposing (1) our theorem does not hold in general.

2. Since the order of an element is a divisor of the order of R, we have proved the

Corollary. *Let d denote the smallest prime divisor of n. Then R_n (see example 1) has exactly one identically vanishing polynomial of degree less than d.*

3. The condition (1) in our theorem can be replaced by the following one:

(1′) *For every $a \neq 0$ element in R and for arbitrary $i < k = 2, \ldots, n$ there exists at least one integer q such that for $p = q^k - q^i$ we have $pa \neq 0$.*

Then the sufficiency of (2) can be proved by successive application of the operator

$$\sigma_q^k f(x) = f(qx) - q^k f(x)$$

for

$$f_n(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0.$$

In fact, then we have

$$g_0(x) = f_n(x) - f_n(0) = a_n x^n + \cdots + a_1 x \equiv 0,$$
$$g_1(x) = \sigma_{q_1}^1 g_0(x) = (q_1^n - q_1) a_n x^n + \cdots + (q_1^2 - q_1) a_2 x^2 \equiv 0,$$
$$\cdots$$
$$g_{n-1}(x) = \sigma_{q_{n-1}}^{n-1} g_{n-2}(x) = (q_1^n - q_1)(q_2^n - q_2^2) \ldots a_n x^n \equiv 0$$

for all $x \in R$ and for every integer q_i. But this implies that $a_n x^n \equiv 0$ and, consequently, $a_n = 0$, further similarly, $a_{n-1} = \cdots = a_1 = 0$ are true.

Here (1′), i. e., the cancellability of $pa = 0$ by $p = q^k - q^i = q^i(q^{k-i} - 1)$ was used at least for one $p = p(a)$. Observe that this condition (1′) is fulfilled e. g. if the cancellability by 2 and by $2^k - 1$ $(k = 2, \ldots, n-1)$ is supposed on R.

4. Problem. Give necessary and sufficient conditions under which a ring R possesses a unique identically (for all $x \in R$) vanishing polynomial of the form

$$f_n(x) = \sum_{k=1}^{n} (a_k x^k + x^k b_k)$$

resp.

$$g_n(x) = \sum_{k=1}^{n} \prod_{i=0}^{2k} z_{ik}(x)$$

of degree n, where a_k, b_k are fixed elements in R [3]) and

$$z_{ik}(x) = \begin{cases} a_{ik} \in R \text{ (constant), if } i \text{ is even,} \\ x \in R, \text{ otherwise.} \end{cases}$$

(Received August 27, 1959)

---

[3]) Or, more generally, it may be allowed that some of a_k, b_k, a_{ik} are integer numbers.