polynomial functions vs polynomials

Canonical name	PolynomialFunctionsVsPolynomials
Date of creation	2013-03-22 19:18:03
Last modified on	2013-03-22 19:18:03
Owner	joking (16130)
Last modified by	joking (16130)
Numerical id	4
Author	joking (16130)
Entry type	Theorem
Classification	msc 13A99

Let k be a field. Recall that a function

$$f : k \to k$$

is called polynomial function, iff there are $a_0, \dots, a_n \in k$ such that

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

for any $x \in k$.

The ring of all polynomial functions (together with obvious addition and multiplication) we denote by $k\{x\}$. Also denote by $k[x]$ the ring of polynomials (see `http://planetmath.org/PolynomialRing`this entry for details).

There is a canonical function $T : k[x] \to k\{x\}$ such that for any polynomial

$$W = \sum_{i=1}^{n} a_i \cdot x^i$$

we have that $T(W)$ is a polynomial function given by

$$T(W)(x) = \sum_{i=1}^{n} a_i \cdot x^i.$$

(Although we use the same notation for polynomials and polynomial functions these concepts are not the same). This function is called the **evaluation map**. As a simple exercise we leave the following to the reader:

Proposition 1. The evaluation map T is a ring homomorphisms which is ,,onto".

The question is: when T is ,,1-1"?

Proposition 2. T is ,,1-1" if and only if k is an infinite field.

Proof. ,,$\Rightarrow$" Assume that $k = \{a_1, \dots, a_n\}$ is a finite field. Put

$$W = (x - a_1) \cdots (x - a_n).$$

Then for any $x \in k$ we have that $x = a_i$ for some i and

$$T(W)(x) = (x - a_1) \cdots (x - a_n) = (a_i - a_1) \cdots (a_i - a_i) \cdots (a_i - a_n) = 0$$

which shows that $W \in \mathrm{Ker} T$ although W is nonzero. Thus T is not ,,1-1".

,,$\Leftarrow$" Assume, that

$$W = \sum_{i=1}^{n} a_i \cdot x^i$$

is a polynomial with positive degree, i.e. $n \geqslant 1$ and $a_n \neq 0$ such that $T(W)$ is a zero function. It follows from the Bezout's theorem that W has at most n roots (in fact this is true over any integral domain). Thus since k is an infinite field, then there exists $a \in k$ which is not a root of W. In particular

$$T(W)(a) \neq 0.$$

Contradiction, since $T(W)$ is a zero function. Thus T is ,,1-1", which completes the proof. □

This shows that the evaluation map T is an isomorphism only when k is infinite. So the interesting question is what is a kernel of T, when k is a finite field?

Proposition 3. Assume that $k = \{a_1, \ldots, a_n\}$ is a finite field and

$$W = (x - a_1) \cdots (x - a_n).$$

Then $T(W) = 0$ and if $T(U) = 0$ for some polynomial U, then W divides U. In particular

$$\mathrm{Ker} T = (W).$$

Proof. In the proof of proposition 2 we've shown that $T(W) = 0$. Now if $T(U) = 0$, then every a_i is a root of U. It follows from the Bezout's theorem that $(x - a_i)$ must divide U for any i. In particular W divides U. This (together with the fact that $T(W) = 0$) shows that the ideal $\mathrm{Ker} T$ is generated by W. □.

Corollary 4. If k is a finite field of order $q > 1$, then $k\{x\}$ has exactly q^q elements.

Proof. Let $k = \{a_1, \ldots, a_q\}$ and

$$W = (x - a_1) \cdots (x - a_q).$$

By propositions 1 and 3 (and due to First Isomorphism Theorem for rings) we have that

$$k\{x\} \simeq k[x]/(W).$$

But the degree of W is equal to q. It follows that dimension of $k[x]/(W)$ (as a vector space over k) is equal to

$$\dim_k k[x]/(W) = q.$$

Thus $k\{x\}$ is isomorphic to q copies of k as a vector space

$$k\{x\} \simeq k \times \cdots \times k.$$

This completes the proof, since k has q elements. $\square$

Remark. Also all of this hold, if we replace k with an integral domain (we can always pass to its field of fractions). However this is not really interesting, since finite integral domains are exactly fields (Wedderburn's little theorem).