Elementary proof of finitely generateness of a subring of $\mathbf{k}[t]$

Marek Karaś

IMUJ Preprint 1999/05

Abstract

In this note we present elementary proof of known fact that any subring $R \subset \mathbf{k}[t]$ which contains a field $\mathbf{k}$, where $\mathbf{k}[t]$ is the ring of polynomials in one variable, is finitely generated $\mathbf{k}-$algebra. In our proof only Chinese Remainder Theorem is used.

1 Introductions

By $\mathbb{N}, \mathbb{Z}$ we denote sets of natural and integer numbers, respectively. We assume that $0 \in \mathbb{N}$. By $\mathbf{k}$, $\mathbf{k}[t]$, $\mathbf{k}[X_1, \ldots, X_n]$ and $\mathbf{k}(X_1, \ldots, X_n)$ we denote a field, ring of polynomials in one variable, ring of polynomials in n variables and field of rational functions in n variables, respectively.

The fourteenth problem of Hilbert is the following question:

1 *Let $L \subset \mathbf{k}(X_1, \ldots, X_n)$ be arbitrary subfield such that $\mathbf{k} \subset L$. Whether $L \cap \mathbf{k}[X_1, \ldots, X_n]$ is a finitely generated $\mathbf{k}-$algebra.*

More general quastion is the following:

2 *Let $R \subset \mathbf{k}[X_1,\ldots,X_n]$ be arbitrary subring such that $\mathbf{k} \subset R$. Whether R is a finitely generated $\mathbf{k}-$algebra.*

For $n > 1$ answer to the second quastion is, in general, negative. For some more details see e.g. [1]. For $n = 1$ answer is given by the following known

Theorem 1 *If R is a subring of $\mathbf{k}[t]$ such that $\mathbf{k} \subset R$ then R is a finitely generated $\mathbf{k}-$algebra.*

In this note an elementary proof of the above Theorem is given. In our proof we use only Chinese Remainder Theorem and linear algebra.

2 Numerical Lemma

If $k, l \in \mathbb{Z}$ and $k = l \cdot m$ for some $m \in \mathbb{Z}$ then we will write $l|k$. If $k, l, m \in \mathbb{Z}$ and $m|(k-l)$ then we will write $k \equiv l \,(\mathrm{mod}\, m)$. For any $m_1,\ldots,m_n \in \mathbb{Z}$ by $\mathrm{GCD}(m_1,\ldots,m_n)$ we denote the greatest common divisor of numbers $m_1,\ldots,m_n$ and assume that $\mathrm{GCD}(m_1,\ldots,m_n) \in \mathbb{N}$.

Lemma 2 *Let $n \in \mathbb{N}$, $m_1,\ldots,m_n \in \mathbb{N}$ and $\mathrm{GCD}(m_1,\ldots,m_n) = d$. There exists $l_0 \in \mathbb{N}$ such that if $l \geq l_0$ and $d|l$ then there exist $l_1,\ldots,l_n \in \mathbb{N}$ such that*

$$l = l_1 m_1 + \ldots + l_n m_n.$$

Proof: Let

$$\varepsilon_j = jd \qquad \text{for} \quad j = 0,1,\ldots,u = \frac{m_1}{d} - 1.$$

By Chinese Remainder Theorem there exist $l_{j,1},\ldots,l_{j,n} \in \mathbb{Z}$, $j = 0,1,\ldots,u$, such that

$$\varepsilon_j = l_{j,1} m_1 + \ldots + l_{j,n} m_n.$$

Let

$$I_j = \{i \in \{1,\ldots,n\} \,:\, l_{j,i} < 0\}, \qquad j = 0,1,\ldots,u.$$

For

$$\tilde{\varepsilon}_j = \varepsilon_j + \Sigma_{i \in I_j}(|l_{j,i}| m_1) m_i,$$

we have

$$\tilde{\varepsilon}_j \equiv \varepsilon_j (\bmod m_1)$$

and

$$\tilde{\varepsilon}_j = \Sigma_{i \notin I_j} l_{j,i} m_i + \Sigma_{i \in I_j} (l_{j,i} + |l_{j,i}| m_1) m_i, \qquad \text{for } j = 0, 1, \ldots, u.$$

Thus $\tilde{\varepsilon}_0, \ldots, \tilde{\varepsilon}_u$ can be written as linear combinations of $m_1, \ldots, m_n$ with coefficients from $\mathbb{N}$.

For any $l \geq l_0 = \max\{\tilde{\varepsilon}_0, \ldots, \tilde{\varepsilon}_u\}$ such that $d|l$ there exists $j \in \{0, 1, \ldots, u\}$ such that

$$l \equiv \varepsilon_j (\bmod m_1).$$

Thus

$$l = \tilde{\varepsilon}_j + \tilde{l} m_1$$

for some $\tilde{l} \in \mathbb{N}$, and so l can be written as a linear combination of $m_1, \ldots, m_n$ with coefficients from $\mathbb{N}$. $\square$

3 Proof of the Theorem

We can assume that $\mathbf{k} \neq R$. Let

$$R_p = \{f \in R : \deg f \leq p\} \qquad \text{for } p \in \mathbb{N}.$$

The set R_p, for any $p \in \mathbb{N}$, is a finite dimensional linear space over $\mathbf{k}$.

Let

$$M = \{\deg f : f \in R \backslash \mathbf{k}\}.$$

We have

$$M = \{m_1, m_2, \ldots\},$$

where $m_1, m_2, \ldots \in \mathbb{N}$. Let

$$\mu_1 = m_1,\ \mu_2 = \mathrm{GCD}(m_1, m_2), \ldots, \mu_n = \mathrm{GCD}(m_1, \ldots, m_n), \ldots$$

We have

$$\mu_n \geq \mu_{n+1} \quad \text{and} \quad \mu_n \in \mathbb{N} \qquad \text{for} \quad n \in \mathbb{N}.$$

Thus there exists $n_0 \in \mathbb{N}$ such that

$$\mu_{n_0} = \mu_{n_0+k} \qquad \text{for} \quad k \in \mathbb{N}.$$

We put $\mu = \mu_{n_0}$.

Let $f_1, \ldots, f_{n_0} \in R$ be such that

$$\deg\, f_i = m_i \qquad \text{for} \quad i = 1, \ldots, n_0$$

and $g_1, \ldots, g_s$ be any basis of the $\mathbf{k}-$linear space R_{l_0}, where l_0 is from Lemma 2 (for numbers $m_1, \ldots, m_{n_0}$).

Let $f \in R$ be arbitrary. If $\deg\, f \leq l_0$ then

$$f = a_1 g_1 + \ldots + a_s g_s$$

for some $a_1, \ldots, a_s \in \mathbf{k}$. If $\deg\, f > l_0$ then $\mu | \deg\, f$ and by Lemma 2 there exist $l_1, \ldots, l_{n_0} \in \mathbb{N}$ such that

$$\deg\, f = l_1 \deg\, f_1 + \ldots + l_{n_0} \deg\, f_{n_0}.$$

Then there exists $a \in \mathbf{k}$ such that

$$\deg\, (f - a f_1^{l_1} \cdot \ldots \cdot f_{n_0}^{l_{n_0}}) < \deg\, f.$$

By repeating of the above operation we can construct $\tilde{f} \in \mathbf{k}[f_1, \ldots, f_{n_0}]$ such that

$$\deg\, (f - \tilde{f}) \leq l_0.$$

The above inequality means that $f - \tilde{f} \in R_{l_0}$, and finally we get that

$$f \in \mathbf{k}[g_1, \ldots, g_s, f_1, \ldots, f_{n_0}].$$

□

References

[1] A. Nowicki, *Przykład Freudenburga do czternastego problemu Hilberta,* Materiały na XX konf. szkol. z Geom. Anal. i Alg. Zespolonej, Łódż 1999