Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
32 (2016), 33–37
www.emis.de/journals
ISSN 1786-0091

ON DEDEKIND SUBRINGS

JANUSZ ZIELIŃSKI

Abstract. We present an elementary proof of a theorem of Zaks concerning Dedekind subrings of polynomial rings over an infinite field.

1. Introduction

Let k be an infinite field. The following theorem first appeared in Zaks [7].

Theorem 1.1. *Let $k \subset R \subset k[x_1, \ldots, x_n]$. If R is a Dedekind domain, then it is a polynomial ring in one variable.*

Zaks' theorem is also valid for finite fields, but the proof (see [7]) is slightly different. The case of infinite fields has numerous applications. It plays notably important role in differential algebra. For instance, it follows from it that the ring of constants of a non-zero derivation (or a family of derivations) of the polynomial ring in two variables over the field of characteristic zero is isomorphic to the polynomial ring in one variable. It was proved by Nagata and Nowicki in [5]. Zaks' theorem was also used in [6] for the description of the centralizer. For more results that are consequences of Theorem 1.1 we refer the reader to [4].

In the proof of Proposition 4 in [7] it states: "Since $k[u] \subset R$ and $R \subset k(u)$, R is a localization of k[u]. As $R \subset k[x]$, the invertible elements of R are the (non-zero) elements of k thus $R = k[u]$." This is not clear why there do not exist other rings between $k[u]$ and $k(u)$. No references nor arguments are given. Also the latter sentence is not obvious. Nevertheless Zaks' approach is correct. The aim of this paper is to complete his proof. One possible way is theory of Prüfer domains, namely so-called *domains with QR-property* (see [3]). However, we give a completely elementary proof.

Recall that a Dedekind domain is a Noetherian domain that is normal (i.e., integrally closed in its field of fractions) and its Krull dimension equals 1 (i.e., its non-zero prime ideals are maximal). Note that our proof does not

---

2010 *Mathematics Subject Classification.* Primary 13N15; Secondary 13F05, 13G05, 12H05, 16U10.

Key words and phrases. Dedekind domain, derivation, ring of constants.

exploit Noetherianity. Basic examples of Dedekind domains are principal ideal domains. In that case an analogous theorem was known earlier (see [2]). An alternative proof of Theorem 1.1 was given by Eakin [1].

2. Auxiliary lemmas

In the following two lemmas k is an arbitrary field. If R is a domain, then we denote by R_0 the field of fractions of R.

Lemma 2.1. *Let $R \subset k[x]$ be a subring containing k. If $R_0 = k(w)$ for some $w \in R$, then $R = k[w]$.*

Proof. Obviously $k[w] \subset R$. Suppose that there exists a polynomial $f \in R \setminus k[w]$. Let $n = \deg w$. We show that there exists $g \in R \setminus k[w]$ such that $\deg g$ is not divisible by n. If $n \nmid \deg f$, then we take $g = f$. If $\deg f = mn$ for some natural m, then subtracting from f the polynomial w^m with the suitable coefficient from k we obtain a polynomial $f_1 \in R$ of the degree $< mn$. If $f_1 \in k[w]$, then $f \in k[w]$, which is a contradiction. Thus $f_1 \in R \setminus k[w]$. If $n \nmid \deg f_1$, we take $g = f_1$. If $n \mid \deg f_1$, then analogously as above we find a polynomial f_2. By recursion we obtain the sequence (f_r) of polynomials not belonging to $k[w]$ with decreasing degrees. Because each polynomial of degree < 1 belongs to $k[w]$ (since $k \subset k[w]$), the procedure stops at some polynomial f_s. Then $n \nmid \deg f_s$ and we take $g = f_s$.

Since $R_0 = k(w)$, there exist univariate polynomials F and G with coefficients in k such that

$$\frac{g}{1} = \frac{F(w)}{G(w)}.$$

Thus $g \cdot G(w) = F(w)$. This is a contradiction, because $n \mid \deg F(w)$ and $n \nmid \deg(g \cdot G(w))$. □

Lemma 2.2. *Let R be a ring such that $k \subset R \subset k[x]$. If $R_0 \cap k[x] = R$, then $R = k[u]$ for some $u \in R$.*

Proof. If $\deg_x r < 1$ for every $r \in R$, then $R \subset k$. Consequently, $R = k = k[1]$. Assume then that R contains a polynomial of positive degree. Let $u(x) \in R$ be a polynomial of smallest positive degree in R (obviously $u(x)$ is not uniquely determined). Let $m = \deg_x u(x)$. Consider the polynomial ring $R_0[z]$, where z is a new independent variable.

We show that the polynomial $u(z) - u(x)$ is irreducible in $R_0[z]$. Suppose it is reducible. Let

$$u(z) - u(x) = p_1(x, z) \cdot p_2(x, z), \tag{2.1}$$

where $p_1(x, z), p_2(x, z) \in R_0[z]$. We write the variable x in the polynomials p_1 and p_2 for the technical reason. Formally it is the factorization of polynomials in the variable z. Nevertheless, the coefficients of these polynomials belong to R_0 and hence are rational functions in variable x. It will be useful in the proof to consider x as well. We aim to have the variable x in p_1 and p_2 in the polynomial form (it is not guaranteed yet). The coefficient of the highest power of z on the left-hand side of (2.1) belongs to the field k. Without loss of generality we can assume that the coefficients of the highest powers of z in p_1 and p_2 also belong to k (we may multiply one of these polynomials, and divide the other, by a suitable element from R_0). We show that then the polynomials $p_1(x,z)$ and $p_2(x,z)$ belong to $k[x,z]$.

Consider (2.1) as an equality in the ring $k(x)[z]$. Let $r = \deg_z p_1$ and $s = \deg_z p_2$. Let $h_r(x) \in k[x]$ be the least common denominator of the coefficients of the polynomial $p_1 \in R_0[z]$ and let $f_s(x) \in k[x]$ be the least common denominator of the coefficients of the polynomial $p_2 \in R_0[z]$. Then we can write:

$$p_1(x,z) = \frac{1}{h_r(x)}\left(h_0(x) + h_1(x)z + \cdots + ch_r(x)z^r\right), \tag{2.2}$$

$$p_2(x,z) = \frac{1}{f_s(x)}\left(f_0(x) + f_1(x)z + \cdots + df_s(x)z^s\right), \tag{2.3}$$

where $h_0, \ldots, h_r, f_0, \ldots, f_s \in k[x]$, $\gcd(h_0, \ldots, h_r) = 1$, $\gcd(f_0, \ldots, f_s) = 1$ and $c, d \in k$. Then

$$h_r(x)f_s(x)\left(u(z) - u(x)\right) = \left(h_0(x) + \cdots + ch_r(x)z^r\right)\left(f_0(x) + \cdots + df_s(x)z^s\right).$$

Since both factors of the right-hand side of the last equation are primitive polynomials, it follows from Gauss's lemma that the left-hand side of the equation is a primitive polynomial. In particular, $h_r(x), f_s(x) \in k$, and consequently (2.2) and (2.3) imply $p_1(x,z), p_2(x,z) \in k[x,z]$. Thus, we established that the coefficients of the polynomials $p_1, p_2 \in R_0[z]$ belong to $k[x]$, and hence to $R_0 \cap k[x] = R$.

Temporarily consider p_1 and p_2 as polynomials in $k[x,z]$. Let (i_1, j_1), (i_2, j_2) be the respective grades of these polynomials in the lexicographic order. Then i_1 is the highest exponent of x in p_1 and j_1 is the highest exponent of z among terms of p_1 divisible by x^{i_1}. Then the grade of $p_1(x,z) \cdot p_2(x,z)$ equals $(i_1 + i_2, j_1 + j_2)$. However that grade is equal to the grade of $u(z) - u(x)$, that is to $(m, 0)$. Therefore $j_1 = 0$ and $j_2 = 0$. We examine what polynomial in the variable x is the coefficient of z^0 in p_1. The grade of $p_1(x,z)$ is $(i_1, 0)$, then the expansion of $p_1(x,z)$ contains the term $a_{i_1}x^{i_1}$ for a non-zero $a_{i_1} \in k$. Thus the coefficient of z^0 is equal to $a_{i_1}x^{i_1} + \cdots + a_1x + a_0$. Because we showed that the coefficients of p_1 belong to R, we obtain that R contains a polynomial of degree (with respect to x) i_1. Since $i_1 \geqslant 0$, $i_2 \geqslant 0$ and $i_1 + i_2 = m$, the minimality of m implies that $i_1 = 0$ or $i_1 = m$. In the latter case we have $i_2 = 0$, hence the grade of one of the polynomials $p_1(x,z)$, $p_2(x,z)$ equals $(0,0)$. Therefore one of these polynomials belong to the field k. This proves the irreducibility of $u(z) - u(x)$ in $R_0[z]$.

Since x is a root of an irreducible (over R_0) polynomial $u(z) - u(x)$, it follows that $[R_0(x) : R_0] = m$. Since $k \subset R \subset k[x]$, we have $R_0(x) = k(x)$, thus $[k(x) : R_0] = m$. An element x is also a root of $u(y) - u(x) \in k(u)[y]$, and then $[k(x) : k(u)] \leqslant m$, where similarly to above we make use of the formula $(k(u))(x) = k(x)$. Since $u \in R \subset R_0$, we have $k(u) \subset R_0 \subset k(x)$, hence

$$[k(x) : k(u)] = [k(x) : R_0] \cdot [R_0 : k(u)].$$

Therefore $m \geqslant m \cdot [R_0 : k(u)]$, and thus $1 \geqslant [R_0 : k(u)]$, because m is positive. Consequently $[R_0 : k(u)] = 1$, and finally $R_0 = k(u)$. Then Lemma 2.1 implies $R = k[u]$. □

From now on, we assume that k is an infinite field. The proof of the next lemma is based on the proof of Lemma 1 in [7]. Zaks proves that the transcendence degree of R_0 over k equals 1. We can also easily deduce it from the following lemma, however the weakened assertion of Lemma 2.3 suffices to prove the main theorem.

Lemma 2.3. *Let R be a ring such that $k \subset R \subset k[x_1, \ldots, x_n]$. If the Krull dimension of R equals 1, then R is a subring of the polynomial ring in one variable.*

Proof. Let m be the smallest positive integer such that R is a subring of the polynomial ring in m variables $k[y_1, \ldots, y_m]$. If $m = 1$, the assertion follows. Suppose then that $m > 1$.

Let a be an arbitrary element of k. Consider the homomorphism

$$f_a \colon R \longrightarrow k[y_1, \ldots, y_m]$$

defined by $f_a(r) = r(y_1, \ldots, y_{m-1}, a)$ for $r(y_1, \ldots, y_m) \in R$. The kernel of a homomorphism is a prime ideal and the Krull dimension of R equals 1, then either $\ker f_a = 0$, or $\ker f_a$ is a maximal ideal in R. In the former case, we obtain an inclusion of R into the ring $k[y_1, \ldots, y_{m-1}]$, which is a contradiction to the minimality of m. In the latter case, the quotient ring $R/\ker f_a$ is a field. It is isomorphic to the image of R under f_a. Hence every non-zero element in the image is invertible. The only invertible elements in $k[y_1, \ldots, y_{m-1}]$ are non-zero elements of k. Thus $r(y_1, \ldots, y_{m-1}, a) \in k$ for all $r \in R$ and $a \in k$.

Since m is minimal and greater than 1, the inclusion $R \subset k[y_m]$ is impossible. Then there exists $r \in R \setminus k[y_m]$. Let

$$r = \sum b_{i_1 \ldots i_m} y_1^{i_1} \cdots y_m^{i_m} = \sum \left(\sum b_{i_1 \ldots i_m} y_m^{i_m} \right) y_1^{i_1} \cdots y_{m-1}^{i_{m-1}},$$

where every $b_{i_1 \ldots i_m}$ belongs to k. If all elements of the form $\sum b_{i_1 \ldots i_m} y_m^{i_m}$ are zero polynomials, then $r = 0$, contrary to $r \notin k[y_m]$. Furthermore, if only $\sum b_{0 \ldots 0 i_m} y_m^{i_m}$ is a non-zero polynomial, then $r = \sum b_{0 \ldots 0 i_m} y_m^{i_m} \in k[y_m]$. Hence, there exist integers $j_1, \ldots, j_{m-1}$, not all equal to zero, such that the polynomial $\sum b_{j_1 \ldots j_{m-1} i_m} y_m^{i_m}$ is non-zero. Denote this polynomial by $b(y_m)$. Since it is non-zero, it has finitely many roots. The field k is infinite, then there exists $a \in k$ such that $b(a) \neq 0$. Thus $r(y_1, \ldots, y_{m-1}, a) \notin k$, because in that evaluation the coefficient of the monomial $y_1^{j_1} \cdots y_{m-1}^{j_{m-1}}$ is a non-zero element of k. This is a contradiction with the fact we obtained above, and this proves that $m = 1$. □

3. Proof of Zaks' theorem

Proof. In view of Lemma 2.3 we may assume that $R \subset k[x]$. Let $S = R_0 \cap k[x]$. Then S is a ring, as an intersection of rings. Since $R \subset R_0$ and $R \subset k[x]$, we have $R \subset S$. Then $R_0 \subset S_0$. Moreover, $S \subset R_0$ and R_0 is a field, then we have $S_0 \subset R_0$ and consequently $S_0 = R_0$. Because k is included in both $k[x]$ and R_0, we deduce that $k \subset S \subset k[x]$. Furthermore, $S_0 = R_0$ implies $S = S_0 \cap k[x]$. By Lemma 2.2, $S = k[v]$ for some $v \in S$.

Thus $R \subset k[v]$ and $R_0 = S_0 = k(v)$. In particular, $v = \frac{r}{s}$ for $r, s \in R$. Therefore $vs - r = 0$. Since $s \in R \subset k[v]$, it follows that $s = f(v)$, where f is a univariate polynomial over k. Then v is a root of the polynomial $xf(x) - r \in R[x]$. The leading coefficient of the latter polynomial belongs to k and hence is invertible in R. Consequently, the element v is integral over R. Since $v \in R_0$ and the ring R is normal, we have $v \in R$. Finally, $R = k[v]$. $\square$

References

[1] P. Eakin. A note on finite dimensional subrings of polynomial rings. *Proc. Amer. Math. Soc.*, 31:75–80, 1972.

[2] A. Evyatar and A. Zaks. Rings of polynomials. *Proc. Amer. Math. Soc.*, 25:559–562, 1970.

[3] R. Gilmer. *Multiplicative ideal theory*. Marcel Dekker, Inc., New York, 1972. Pure and Applied Mathematics, No. 12.

[4] A. Nowicki. *Polynomial derivations and their rings of constants*. Uniwersytet Mikołaja Kopernika, Toruń, 1994.

[5] A. Nowicki and M. Nagata. Rings of constants for k-derivations in $k[x_1, \cdots, x_n]$. *J. Math. Kyoto Univ.*, 28(1):111–118, 1988.

[6] I. P. Shestakov and U. U. Umirbaev. Poisson brackets and two-generated subalgebras of rings of polynomials. *J. Amer. Math. Soc.*, 17(1):181–196 (electronic), 2004.

[7] A. Zaks. Dedekind subrings of $k[x_1, \cdots, x_n]$ are rings of polynomials. *Israel J. Math.*, 9:285–289, 1971.

Received March 16, 2014.

Faculty of Mathematics and Computer Science,
N. Copernicus University,
ul. Chopina 12/18,
87-100 Toruń, Poland
E-mail address: ubukrool@mat.uni.torun.pl