# DEDEKIND SUBRINGS OF $k[x_1,\cdots,x_n]$ ARE RINGS OF POLYNOMIALS*

BY
ABRAHAM ZAKS

ABSTRACT

The purpose of this note is to prove that a Dedekind domain R which contains a field k, and which is a subring of $k[x_1,\ldots,x_n]$ is a ring of polynomials. This generalizes similar results of A. Evyatar and A. Zaks on principal ideal domains, and of P. M. Cohn for the case $n = 1$. Our methods and proofs differ from those introduced previously.

Let $k$ be a field of characteristic $p$. Let $R$ be a $k$-subalgebra of $k[x_1,\cdots,x_n]$. Let $K$ be the field of quotients of $R$. Let Krull-dim $R = 1$.

An element $r$ in $R$ is irreducible if whenever there exist elements $s$ and $t$ in $R$ such that $r = st$ then either $s$ is invertible, or else $t$ is invertible.

An element $r$ in $R$ is prime if the ideal $Rr$ is a prime ideal.

We shall provide proofs only for the case $p \neq 0$. The proofs for the case $p = 0$ are essentially the same as those for the case $p \neq 0$, except that some parts of the proofs become superfluous, since $k$ is then necessarily an infinite field, and every extension of $k$ is a separable extension.

LEMMA 1. tr.deg $K/k = 1$.

PROOF. Let $n$ be the smallest possible integer for which $R$ is isomorphic to a $k$-subalgebra of $F[x_1,\cdots,x_n]$, where $F$ is a finite algebraic extension** of $k$. If $n = 1$ we are done. So let $n > 1$. We shall derive a contradiction as follows: Evaluating $x_n = a$ for some $a$ in an algebraic extension of $F$ induces a homomorphism $f_a$ from $R$ into the domain $F(a)\ [x_1,\cdots,x_{n-1}]$. As Krull-dim $R = 1$

* This research was partially supported by the National Science Foundation, Grant GP-23861.

** If $k$ is an infinite field we may take $F = k$.

I wish to thank Professor S. A. Amitsur and Professor M. Nagata for their helpful comments and suggestions during the preparation of this paper.

Received June 29, 1970 and in revised form September 20, 1970

either $\ker f_a = 0$ or else $\ker f_a$ is a maximal ideal in $R$, say $M_a$, in which case $R/M_a$ is a field between $F$ and $F(a)$. By the minimality hypothesis on $n$, we necessarily have $\ker f_a \neq 0$. Since $n > 1$, and since $n$ is minimal, then there exists an element $r$ in $R$ that is not an element of $F[x_n]$. So let

$$r = \sum b_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n} = \sum \left(\sum b_{i_1 \dots i_n} x_n^{i_n}\right) x_1^{i_1} \cdots x_{n-1}^{i_{n-1}}.$$

Then there exists integers $j_1, \cdots, j_{n-1}$ so that $b(x_n) = \sum b_{j_1 \dots j_{n-1} i_n} x_n^{i_n}$ is not identically zero.

In particular, there exists an element $a$ in an algebraic extension* of $F$ so that $b(a) \neq 0$ and this is a contradiction, since for this $a$, $R/M_a$ is a field between $F$ and $F(a)$, but $f_a(r) \notin F(a)$.

This contradiction implies that $n = 1$, and since $F$ is an algebraic extension of $k$, then $\operatorname{tr.deg} K/k = 1$.

Since in the infinite case we may take $F = k$ we have:

LEMMA 2. *If $k$ is an infinite field then $R$ is a $k$-subalgebra of $k[x]$.*

By Igusa's generalization of Lüroth's theorem we have:

COROLLARY 3. *$K$ is a field of rational functions in one variable over $k$.*

We proceed first with the case of $k$ being an infinite field. As by Lemma 2 $R \subset k[x]$, our next object is to have a criterion on a subring $R$ of $k[x]$ that suffices to imply that $R$ is a ring of polynomials (see also [2]).

PROPOSITION 4. *Let $k$ be any field, let $R$ be a ring, $k \subset R \subset k[x]$, with quotient field $K$. If $K \cap k[x] = R$, then $R$ is a ring of polynomials.*

PROOF. The condition $K \cap k[x] = R$ states that if $u = sv$ in $k[x]$, while $u, v \in R$, then $s \in R$. Let $\| w \|$ denote the degree of $w$, for every $w$ in $k[x]$. Let $u(x)$ be an element in $R$ of smallest possible positive degree, say $\| u(x) \| = m$. Let $z$ be a variable over $k(x)$, and assume that $u(z) - u(x)$ decomposes in $K[z]$, say $u(z) - u(x) = p_1(x,z)p_2(x,z)$. As the highest term coefficient on the left hand side is an element of $k$, we may assume that such are the highest term coefficients in $p_1(x,z)$ and in $p_2(x,z)$. We consider now the last decomposition in $k(x)[z]$. It follows that $p_1(x,z)$, $p_2(x,z) \in k[x,z]$. In particular, the coefficients of $p_1(x,z)$ and $p_2(x,z)$ lie all in $K \cap k[x]$, thus in $R$. Let $(i_1, j_1)$ and $(i_2, j_2)$ be the grade of $p_1(x,z)$ and $p_2(x,z)$ in the lexicographical order (taking $x$ first). Then the grade of $p_1(x,z) \cdot p_2(x,z)$ is $(i_1 + i_2, j_1 + j_2)$. But the grade of

* If $k$ is an infinite field this element may be chosen from $k$.

$p_1(x,z)p_2(x,z) = u(z) - u(x)$ is exactly $(m,0)$. Thus by the minimality of $m$, we have to say $i_1 = 0$, $i_2 = m$ and $j_1 = j_2 = 0$. Therefore, the grade of $p_1(x,z)$ is $(0,0)$, whence $p_1(x,z) \in k$, and therefore $u(z) - u(x)$ is indecomposable over $K$. In particular $[k(x): K] = m$. As $[k(x): k(u)] = m$ it follows that $K = k(u)$. 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 $R = k[u]$.

We are now ready for the main theorem, under the restriction of $k$ being an infinite field.

THEOREM 5. *If $k$ is an infinite field, and if $R$ is a Dedekind domain, then $R$ is a ring of polynomials.*

PROOF. By Lemma 2 we may assume that $R \subset k[x]$.

Set $S = K \cap k[x]$, then $S$ is an overring of $R$ within $K$, whence $S$ is a Dedekind domain. By Proposition 4 $S = k[v]$ for some $v$ in $S$. Therefore, $R \subset k[v]$ and $K = k(v)$. In particular $v = r/s$ for some $r$ and $s$ in $R$. Since $s \in k[v]$ and $r \in R$, $vs = r$ yields an integral equation for $v$ over $R$, hence $v \in R$ and thus $R = k[v]$.

The next lemma is obvious in case $k$ is an infinite field in view of Theorem 5, but it is needed in order to complete the study of the case of $k$ being a finite field.

LEMMA 6. *Let $y$ be a variable over $k(x_1, \cdots, x_n)$, then $k(y)R$ is a ring of polynomials in one variable over $k(y)$, whenever $R$ is a Dedekind domain.*

PROOF. By Lemma 1, $\text{tr.deg}\, K/k = 1$, whence $\text{tr.deg}\, K(y)/k(y) = 1$, and $K(y)$ is the field of quotients of $k(y)R$. Since $k(y)$ is an infinite field, and since $k(y) \subset k(y)R \subset k(y)[x_1, \cdots, x_n]$, it suffices to prove that $k(y)R$ is a Dedekind domain. Since $\text{tr.deg}\, K(y)/k(y) = 1$, it suffices to show that $k(y)R$ is a Krull domain (e.g. [3]). However, $k(y)R$ is the localization of $k[y]R$ at the multiplicative set $k[y] - 0$. Since $R$ is a Krull domain such are $k[y]R$ and its localization $k(y)R$, and this completes the proof.

From Theorem 5 and Lemma 6 we deduce (see also [3]):

COROLLARY 7. *If $R$ is a principal ideal domain then $R$ is a ring of polynomials.*

PROOF. By Lemma 6 $k(y)R$ is a ring of polynomials over $k(y)$, say $k(y)R = k(y)[u]$. Without loss of generality we may assume that $u \in k[y]R$, and that no polynomial in $y$ is a factor of $u$ (in $k(y, x_1, \cdots, x_n]$). Furthermore, since for some integer $i, x_i$ properly appear in $u$, we may also assume that $u(x_1, \cdots, x_n, 0) \notin k$. Then for every element $r$ in $R$ there exist polynomials $p(y)$, $p_0(y), \cdots, p_m(y)$ in $k[y]$ so that $p(y)r = p_0(y) + \cdots + p_m(y)u^m$. Let $p(y)$ be of the smallest possible degree. Since $u(x_1, \cdots, x_n, 0) \notin k$ it follows that if $p(0) = 0$ then $p_0(0) = \cdots = p_m(0) = 0$, because $u(x_1, \cdots, x_n, 0)$ is a transcendental element over $k$. Thus, if $p(0) = 0$ a contradiction to the minimality of $p(y)$ results. Consequently, $p(0) \neq 0$ and $r = p(0)^{-1}p_0(0) + \cdots + p(0)^{-1}p_m(0)u^m(x_1, \cdots, x_n, 0)$. Since $u(x_1, \cdots, x_n, 0) \in R$ it follows that $R = k[u(x_1, \cdots, x_n, 0)]$.

THEOREM 8. *If $R$ is a Dedekind domain, then $R$ is a ring of polynomials over $k$.*

PROOF. By Lemma 6 we have $k(y)R = k(y)[u]$ for some variable $y$ over $k(x_1, \cdots, x_n)$. Let $r$ be any irreducible element in $R$, then we claim that $r$ is a prime element in $k(y)R$. As $k(y)R$ is a principal ideal domain, if $r$ is not a prime element in $k(y)R$, then $r = v_1 \cdot v_2$, $v_i \in k(y)R$ for $i = 1,2$. As $y$ is a variable over $k(x_1, \cdots, x_n)$, and as $R \subset k[x_1, \cdots, x_n]$, we may assume that $v_1$ and $v_2$ are elements in $k[y, x_1, \cdots, x_n]$. As $y$ does not appear in $r$, it cannot appear in $v_1$ nor in $v_2$, whence $v_1$ and $v_2$ are elements of $k[x_1, \cdots, x_n]$. Thus necessarily $v_1$ and $v_2$ are elements of $R$. This is impossible, as $r$ was chosen to be irreducible, unless $v_1$ (or $v_2$) is invertible in $R$. Hence $r$ is a prime element in $k(y)R$. From the unique factorization property of $k[y, x_1, \cdots, x_n]$ it easily follows that $k(y)Rr \cap R = Rr$. In particular this implies that $r$ is a prime element in $R$. Because let $a$ and $b$ be elements in $R$ so that $ab \in Rr (\subset k(y)Rr)$, then $a$ (or $b$) belongs to $k(y)Rr \cap R = Rr$. Since $R$ is a Dedekind domain, and since irreducible elements are prime, $R$ is a principal ideal domain. From Corollary 7 it now follows that $R$ is a ring of polynomials over $k$.

Observe that in the proof we used only that $R$ is an integrally closed domain of Krull dimension one. However, such a ring is necessarily Noetherian in view of Lemma 1 and [1]:

LEMMA 9. *A $k$-subalgebra $R$ of $k[x_1, \cdots, x_n]$ is Noetherian whenever* $\mathrm{tr.deg.}\, K/k = 1$.

PROOF. Let $r \in R$ be an element of $R$, transcendental over $k$, and let $K^*$ be the field of quotients of $k[r]$. Let $S = K^* \cap R$ and let $T$ be a finitely generated extension of $S$ such that $K$ is the field of quotients of $T$, which is possible in this case. Consequently $R$ is an overring of $T$. The Krull-dimension of all the rings involved is one [3], and $T$ is a finitely generated extension of $S$. The result now follows by applying [1] to the extensions $S$ (of $k[r]$), and $R$ (of $T$).

In particular, in the case of $n = 1$, integral closure for $R$ is the sole condition required (see [2]).

Remark that the same line of argument yields:

LEMMA 10. *A k-algebra R is Noetherian whenever* $\text{tr.deg}\, K/k = 1$ *and K is a finitely generated field over k.*

## REFERENCES

1. I. S. Cohen, *Commutative rings with restricted minimum condition*, Duke Math. J. **17** (1950), 27–42.

2. P. M. Cohn, *Subalgebras of free associative algebras*, Proc. London Math. Soc. **14** (1964), 618–632.

3. A. Evyatar and A. Zaks, *Rings of polynomials*, Proc. Amer. Math. Soc., **22** (1969) 582–586.

4. J. Igusa, *On a theorem of Lueroth*, Mem. Coll. Sci. Univ. Kyoto Ser. A Math. **26** (1951), 251–253.

NORTHWESTERN UNIVERSITY, EVANSTON, ILLINOIS
TECHNION — ISRAEL INSTITUTE OF TECHNOLOGY, HAIFA