JOURNAL OF ALGEBRA 43, 699–708 (1976)

Lüroth's Problem for Rings

S. GLAZ[1], J. D. SALLY,[2,*] AND W. V. VASCONCELOS[1,*]

[1] *Department of Mathematics, Rutgers University, New Brunswick, New Jersey 08903*
[2] *Department of Mathematics, Northwestern University, Evanston, Illinois 60201*

Communicated by D. Buchsbaum

Received December 8, 1975

INTRODUCTION

The problem we consider here fits into the following class of questions: Let X be an algebraic structure 'generated' by a single element and let Y be a substructure; what relationship should exist between X and Y in order that Y be similarly generated by a single element? Examples are (i) X a cyclic group and Y a subgroup; (ii) X a simple algebraic field extension of a field $\mathbf{k}$, Y an intermediate extension $\mathbf{k} \subset Y \subset X$; (iii) Lüroth's theorem itself; (iv) A theorem of P. M. Cohn [2] stating: If T is an indeterminate over a field $\mathbf{k}$ and B is a ring $\mathbf{k} \subset B \subset \mathbf{k}[T]$, then $B = \mathbf{k}[f(T)]$ provided B is integrally closed.

When we rephrase (i) above in terms of group algebras, say $X' = \mathbb{Z}(X)$ and $Y' = \mathbb{Z}(Y)$, a common feature of these examples is that the larger ring is *flat*—even free—over the subring. In this paper we deal with the problem of describing the A-subalgebras B of $A[T]$ over which $A[T]$ is flat. Under mild regularity conditions B turns out to be an augmented A-algebra with invertible augmentation ideal but may fail to be finitely generated even when $A = \mathbb{Z}$. With $A[T]$ faithfully flat over B—as in the examples above—the situation is more pleasant and B behaves much as a polynomial ring over A, or at least as a symmetric algebra of a projective module. This will be the case whenever A is seminormal but may fail when this condition is lacking.

1. THE AUGMENTATION IDEAL

In this discussion let A be a commutative ring, let T be an indeterminate over A and let B be a subring $A \subset B \subset A[T]$ over which $A[T]$ is flat. We

* The research of the two last named authors was partially supported by the National Science Foundation grants GP-29815 and GP-33133, respectively.

assume that $A \neq B$ and denote by I the ideal of B of all polynomials with constant term 0. It is an augmentation ideal.

We express the fact that $A[T]$ is simply generated over B using an exact sequence

$$0 \to J \to B[X] \to A[T] \to 0 \tag{*}$$

with the indeterminate X mapping into T. We use now the accumulated information known on such J's [7, 9, 12, and 14] to derive properties of B. To insure the finiteness of J we impose a mild regularity condition. Let $\delta(B)$ denote the minimal degree of nonzero polynomials in I. If $\delta(B) = n$, we assume the existence of a polynomial

$$g = a_n T^n + \cdots + a_1 T$$

in I where some a_i is a regular element of A. Notice that this hypothesis forces a_n to be regular element and that for any multiplicative system $S \subset A$, $\delta(B) = \delta(B_S)$.

The reason for using a regular element in I of degree $\delta(B)$ is motivated by the desire to rule out rings of the kind $B = A[LT]$, where L is a pure ideal of A.

The following is essentially the theorem of Cohn mentioned above [2, 18]. It will imply, by a result of Gruson [15], the finiteness of J.

(1.1) Lemma. *If some a_i is a unit of A, then $B = A[g]$.*

Proof. We first assume that a_n is a unit and A is a local ring. $A[T]$ is now a finitely generated flat module over B. As

$$E = A[T] \otimes_B A[T]$$

is a finitely generated flat module over $A[T]$, it follows from [16] that E is $A[T]$-projective; by faithhfully flat descent $A[T]$ is B-projective. Since B has no idempotents $\neq 0, 1$, we conclude that $A[T]$ is B-projective of constant rank, say, r. As $A[T]$ contains a distinguished set of generators $\{1, T, T^2,...\}$ it is easy to see that at each localization at a prime of B the first r of these generators will be part of a minimal generating set. Thus $A[T]$ is B-free on these elements. Let $p[X]$ be the minimal polynomial of T over B. Note that $p(X)$ is the generator of the ideal J in (*). Tensor the exact sequence by $A[T]$ over $B[X]$ to get the inclusion

$$J/XJ \to B[X]/(X) = B.$$

Let J_0 be the image of J: J_0 is generated by the 'constant' term of $p(X)$, say, $h(T)$. We claim first that $J_0 = I$. If $f(T) \in I$, then $f(X) - f(T) \in J$ and thus $f(T) \in J_0$. Conversely, if $q(X) \in J$ it is clear that the constant term of $q(X)$ is divisible by T. In this case we conclude $I = B \cdot h(T)$.

$h(T)$ is a polynomial of the following type

$$b_m T^m + \cdots + b_{r+1} T^{r+1} + b_r T^r + \cdots + b_1 T, \qquad b_i \in A.$$

Since $g(T) = h(T) \cdot f(T)$, reading this equation modulo any prime ideal of A gives that $b_m, \ldots, b_{r+1}$ are nilpotent elements and b_r is an invertible element of A. If b is a nonzero element of A that annihilates the elements $b_m, \ldots, b_{r+1}$ we get a nonzero element in I of degree r—thus $r = n$. The element $f(T)$ is then invertible and $I = B \cdot g(T)$. As $g(T)$ is monic we easily conclude that $B = A[g]$.

Let us go back to our original $g(T)$. If $f(T)$ is an element of B there is by the above a regular element s of A such that $s \cdot f \in A[g]$, say

$$s \cdot f = c_0 + c_1 g + \cdots + c_m g^m.$$

If we reduce this equation modulo s we get an algebraic dependence relation for $\bar{g}(T)$ in $A/(s)[T]$. Since $\bar{g}(T)$ is a nonzero divisor in $A/(s)[T]$ we conclude that each c_i is divisible by s.

Having considered in (1.1) the case when $g(T)$ has a unit as a coefficient, we can now assume that $g(T)$ be just regular. According to [7], [9], and [14] the $B[X]$-ideal J in the sequence (*) has the following properties:

(i) J is an invertible ideal—in particular J is finitely generated;

(ii) J has B-content (1)—that is, the ideal of B generated by the coefficients of the polynomials in J is equal to B. This easily implies the existence of an element in I with A-content A itself.

As indicated earlier the ideal J_0 of B generated by the constant terms of all polynomials in J is then equal to I and invertible. We resume these facts in

(1.2) PROPOSITION. *The augmentation ideal of B is invertible. The ideal of A generated by the coefficients of the elements in I is equal to* (1).

Consider now the sequence

$$0 \to I^2 \to I \to I/I^2 \to 0.$$

I/I^2 is a rank one projective module over A. There is then a section $\mathbf{s}: I/I^2 \to I \subset B$, and consequently a mapping

$$\phi_{\mathbf{s}}: \mathrm{Symm}_A(I/I^2) \to B,$$

where $\mathrm{Symm}_A(-)$ is the symmetric algebra functor. Of course it is unlikely that any section $\mathbf{s}$ will lead to an isomorphism—in fact, an example will show the impossibility of finding a section leading to an isomorphism. Nevertheless, let $\mathrm{gr}(\phi_s)$ be the associated mapping of graded rings

$$\mathrm{gr}(\phi_s): \mathrm{Symm}_A(I/I^2) \to \mathrm{gr}_I(B).$$

Much as in [17] we have:

(1.3) PROPOSITION. $\mathrm{gr}(\phi_s)$ *is an isomorphism.*

Proof. We may assume that A is a local ring—or, using a partition of unity, assume that $P = s(I/I^2)$ is a free A-submodule of I. Note $I = P \oplus I^2$ as A-modules. We claim that, more generally, $I^r = P^r \oplus I^{r+1}$, $r \geqslant 1$. For this it suffices to show that in the sequence of A-modules

$$\begin{array}{ccccccccc} & & & & 0 & & & & \\ & & & & \downarrow & & & & \\ & & & & I^{r+1} & & & & \\ & & & & \downarrow & & & & \\ 0 & \to & P^r & \to & I^r & \xrightarrow{\psi} & I^r/P^r & \to & 0 \end{array}$$

the restriction of ψ to I^{r+1} is an isomorphism. That ψ is a surjection is clear by raising the equation $I = P \oplus I^2$ to the rth power (possibly losing the direct sum decomposition). Suppose $b \in P^r \cap I^{r+1}$. Pass now to the total ring of quotients of A, say K. Since $B_K = B \otimes_A K = K[g]$ we conclude that P is generated by $ug + h$, with u a unit of K (which may be taken equal to 1). But then $P^r = A(g + h)^r$, while $I_K^{r+1} = g^{r+1}K[g]$ and $b = 0$. That $\mathrm{gr}(\phi_s)$ is both surjective and injective follows by localization.

Examples of rings such as B above that are not symmetric algebras can be easily constructed using the Zariski Main Theorem: Let $f(T)$ be a polynomial of $A[T]$, with constant term 0 and of content (1); $A[T]$ is then a quasifinite extension of $B_0 = A[f]$. Let B be the integral closure of B_0 in $A[T]$. By the *ZMT* $A[T]$ is B-flat. For instance, with $A = \mathbb{Z}$ and $f = 2T^2 + T$, a simple calculation will show that the integral closure of $\mathbb{Z}[f]$ is $\mathbb{Z}[2T^2 + T, 2T]$. We do not have to stop with the integral closure, that is, any ring C, $B \subset C \subset A[T]$, will have the property that $A[T]$ is flat over C.

(1.4) EXAMPLE. Let us show the existence of such a ring C which is not finitely generated over $\mathbb{Z}$. It will serve the purpose of dispersing some hope of what might be expected from (1.3).

Let $C = \mathbb{Z}[2T, T(2T + 1),..., T^i(2T + 1),...]$. Note that $2T + 1$ conducts $\mathbb{Z}[T]$ to C; if C is Noetherian $\mathbb{Z}[T]$ will be a finitely generated submodule of $C \cdot (2T + 1)^{-1}$. Thus $\mathbb{Z}[T]$ will be an integral extension of C, which together with being an epimorphic extension makes $C = \mathbb{Z}[T]$. We have then

$$T = f(T) = b_1(2T + 1)^{\alpha_1}T^{\beta_1} + \cdots + b_k(2T + 1)^{\alpha_k}T^{\beta_k}$$

where $b_i \in \mathbb{Z}$, $\beta_i > 0$ and if $\alpha_i = 0$ then $b_i = 2^{\beta_i} a_i$ with $a_i \in \mathbb{Z}$. Setting $T = -1/2$ we get

$$-1/2 = f(-1/2) = a_{i_1} 2^{\beta i_1}(-1/2)^{\beta i_1} + \cdots + a_{i_j} 2^{\beta i_j}(-1/2)^{\beta i_j},$$

which gives the contradiction $-1/2 \in \mathbb{Z}$. Thus C is not a finitely generated $\mathbb{Z}$-algebra.

2. Faithfully Flat Extensions

In this section we assume in addition to the preceding hypotheses that $A[T]$ is faithfully flat over B or B-f.flat for short.

One property of the augmentation ideal listed earlier is that there exists $f \in I$ so that the content of f is (1). Let g be, as before, a regular element in I of degree $\delta(B)$. If K is the total ring of quotients of A we have from (1.1) that $f \in K[g]$. We may then write

$$a \cdot f = g \cdot h,$$

where $h \in A[T]$ (actually in B) for an appropriate regular element $a \in A$. We recall the Dedekind content formula [1, Sect. 3, Prob. 21]: if $m = \deg(h)$,

$$c(gh) \cdot c(g)^m = c(h) \cdot c(g)^{m+1},$$

or, in our case

$$a \cdot c(g)^m = [c(g) \cdot c(h)] \cdot c(g)^m.$$

Let A' be the integral closure of A. Then

$$c(g) \cdot c(h) \cdot A' = aA',$$

and $c(g) \cdot A'$ is an invertible ideal of A'. It is easy to see that we can find an intermediate extension $A \subset A_1 \subset A'$, A_1 finitely generated over A and with $c(g) \cdot A_1$ an invertible A_1-ideal. With this A_1 write $B_1 = A_1 \otimes_A B$, $I_1 = A_1 \otimes_A I =$ augmentation ideal of B_1.

(2.1) Theorem. $B_1 \simeq \mathrm{Symm}_{A_1}(I_1/I_1^2)$.

Proof. We assume the change of rings made. The content L of g is now an invertible ideal of A. Note that $L^{-1}g \subset A[T]$; as $L(L^{-1}g) \subset B$ and $g \in L(L^{-1}g)$, by the faithful flatness of $A[T]$ over B we get $L^{-1}g \subset B$. (Actually only that $A[T]/B$ is torsion free over A was needed.)

Finally we claim $L^{-1}gB = I$. As it suffices to show equality locally in the Zariski topology of A, localization and another application of (1.1) completes the proof.

Let us go back to the original A and observe some consequences on finiteness derived through finite descent as in [5] and [11]. It is immediate that the hypothesis "$A[T]$ is B-f.flat" forces B to be A-f.flat.

(2.2) COROLLARY. *If $A[T]$ is B-flat and $A[T]/B$ is A-flat, then $A[T]$ is B-f.flat.*

Proof. First, the hypothesis makes B A-flat. The passage $A \to A_1$, by the argument above, makes B_1 a symmetric algebra of a rank one projective A_1-module. What is left is to show that $A[T]$ is faithfully over $A[g]$ whenever g is a polynomial in I of content (1). Now invoke [11] to show that $A[T]$ is B-f.flat.

(2.3) COROLLARY. *If $A[T]$ is B-f.flat then B is A-projective.*

Proof. This time we use [5] for the descent of projectivity under a finite injective homomorphism.

(2.4) COROLLARY. *If $A[T]$ is B-f.flat then B is an A-algebra of finite type.*

Proof. B_1 is an A_1-algebra of finite type. Again by [5] we prove the statement.

3. PICARD GROUPS AND DIFFERENTIALS

The proof of (2.1) reveals that whenever B is a symmetric algebra I is an extension of an invertible ideal of A. It is natural then to consider $I \cdot A[T]$ and ask whether this is an extended ideal of A. In the faithfully flat case this reasoning leads to the obstruction to B being a symmetric algebra. Indeed, let $\mathrm{Pic}(A)$ and $\mathrm{Pic}(A[T])$ be the Picard groups of A and $A[T]$ and consider the usual exact sequence

$$1 \to \mathrm{Pic}(A) \to \mathrm{Pic}(A[T]) \to C(A) \to 1.$$

Denote by $\alpha(B)$ the image in $C(A)$ of the class of $I \cdot A[T]$. It is immediate that B is a symmetric algebra if and only if $\alpha(B)$ is the trivial element of $C(A)$.

We recall that there is a large class of Noetherian rings other than integrally closed domains for which $C(A)$ is trivial. They are the so-called seminormal rings [13].

(3.1) COROLLARY. *If A is seminormal and $A[T]$ is B-f.flat, then B is a symmetric algebra over A. In particular if A is a* UFD *then $B = A[f]$ for some polynomial f.*

Now we consider the question on whether B is always a symmetric algebra. In the case of a nonseminormal ring containing a field of prime characteristic it will be 'easy' to find examples with B not a symmetric algebra. The reason for this relative easeness lies in observing the similarities between this problem with questions in cancellation of coefficient rings [3, 6 and 8], and adjusting to our case some examples of noncancellation. Later in this section we discuss the case of $\underset{\sim}{Q}$-algebras.

(3.2) EXAMPLE. We present now an example of a ring B, $A \subset B \subset A[T]$, with $A[T]$ B-f.flat that is not a symmetric algebra over A. It is inspired by the example of noncancellation in polynomial rings described in [6].

Let A be a local domain of characteristic 2 with an element a in the quotient field of A but not in A and with a^2, $a^3 \in A$ (e.g. $A = \mathbb{Z}/(2)[[x^2, x^3]]$). Let $G = aT^2 + T \in K[T]$, K the field of quotients of A. Let $B = A[G^2, aG^2 + G]$; note that $B \subset A[T]$. Let W be an indeterminate over B and let $C = B[W]$. Put also

$$U = G + a(G + aW)^2 = (G + aG^2) + a^3W$$
$$V = W + (G + aW)^2 = W + G^2 + a^2W^2.$$

U and V are elements of $B[W]$ and independent indeterminates over A. Thus $A[U, V] \subset B[W]$. We claim these rings are equal:

$$W = V - (U + aV)^2$$
$$G + aG^2 = U - a^2W^2$$
$$G^2 = W - a^2W$$

are all elements of $A[U, V]$ and thus $C = A[U, V]$. In particular, as C is A-free, B is free over A also.

We claim that $A[T]$ is B-flat: Let $A_1 = A[a]$, and denote by B_1 the image of $B \otimes_A A_1$ in $A_1[T]$. $B_1 = A_1[aG^2 + G, G^2] = A_1[G]$. Since $B \otimes_A A_1$ is A_1-torsion free we conclude that $B \otimes_A A_1 = B_1$. Finally note that $A_1[T] = A[T] \otimes_B B_1$, and by the descent result of [5] we conclude that $A[T]$ is B-f.flat.

Finally we show that B is not a symmetric algebra over A—which here means that $B \neq A[F]$ for any polynomial F. Indeed note

$$a^2G = a^3T^2 + a^2T = a^2(aG^2 + G) - a^3G^2 \in B.$$

If we write a^2G as a polynomial in F (degree $(F) = 2$) we conclude

$$a^2G = cF, \quad F = a_0T + a_1T^2, \quad ca_0 = a^2, \quad ca_1 = a^3.$$

Let now $G^2 = dF + eF^2$; then $c^2F^2 = a^4G^2 = a^4dF + aeF^2$ and thus $c^2 = a^4e$ and $d = 0$. As $G^2 = eF^2$, $1 = ea_0{}^2$ and a_0 is a unit in A. Thus $c = a^2a_0^{-1}$ and $a_1a^2a_0^{-1} = a^3$, which is a contradiction.

Remark. To get an example in char $p > 0$ we can use the argument above taking an element $a \in K \backslash A$, a^p, $a^{p+1} \in A$, $G = aT^p + T$ and $B = A[G^p, aG^p - G]$.

The characteristic zero cases can, possibly, be better handled via the modules of differentials. In the sequence we use [10] systematically and assume that A is a Q-algebra.

Let $\Omega_{B/A}$ denote the module of A-differentials of B (similar notation for any other pair of rings). The change of rings $A \to A_1$ yields the isomorphism

$$\Omega_{B/A} \otimes_A A_1 \simeq \Omega_{B/A} \otimes_B B \simeq \Omega_{B_1/A_1}.$$

As $B_1 \simeq \mathrm{Symm}_{A_1}(I_1/I_1^2)$ by (2.1), we conclude that Ω_{B_1/A_1} is a projective B_1-module of rank one. In fact, for a symmetric algebra S of a projective R-module P, we have the following canonical isomorphism

$$P \otimes_R S \simeq \Omega_{S/R}$$

given $e \otimes b \to b \cdot d(e)$, $e \in P$, $b \in S$. With the finite descent result of [5] again we conclude that $\Omega_{B/A}$ is a projective B-module of rank one.

The sequence (*) and the inclusions $A \subset B \subset A[T]$ give rise to the following exact sequences of modules of differentials:

$$\Omega_{B/A} \otimes_B A[T] \to \Omega_{A[T]/A} \to \Omega_{A[T]/B} \to 0,$$

$$J/J^2 \xrightarrow{\mathbf{d}} \Omega_{B[X]/B} \otimes_{B[X]} A[T] \to \Omega_{A[T]/B} \to 0.$$

As $\Omega_{B/A} \otimes_B A[T]$ and J/J^2 are both projective $A[T]$-modules of rank one and $\Omega_{B[T]/B}$ is a torsion module, the sequences above are exact at the left also. By Schanuel's lemma

$$J/J^2 \oplus A[T] \simeq \Omega_{B/A} \otimes_B A[T] \oplus A[T].$$

The usual device of taking exterior powers finally gives the isomorphism

$$J/J^2 \simeq \Omega_{A/B} \otimes_B A[T].$$

More accurately, $\mathbf{d}$ identifies J/J^2 with the submodule of $\Omega_{A[T]/A} = A[T]dT$ generated by differentials such as

$$(rb(T^{r-1} + \cdots + b_1)\, dT$$

where $b_r X^r + \cdots + b_1 X + b_0$ is an element of J.

Let us examine the case when J/J^2 is $A[T]$-free, say $J/J^2 \simeq A[T]\, hdT$. It is easy to see that h is then a polynomial of degree $n - 1$ and has A-content (1). For the polynomial g of degree n in I we then conclude that

$$g' = a \cdot h.$$

As g and g' have the same content when A is a Q-algebra, we conclude that the content of g is (a). We are now in the position to state

(3.3) COROLLARY. *Let A be a Q-algebra. If $A[T]$ is B-faithfully flat and J/J^2 is $A[T]$-free, then B is a polynomial A-algebra. More generally, if the class of J/J^2 in $C(A)$ is trivial, then B is a symmetric algebra.*

What is not altogether clear is whether $\alpha(B)$ and the class $\beta(B)$ of J/J^2 in $C(A)$ constitute the same obstruction to B being a symmetric algebra.

4. AN OPEN PROBLEM

For several variables the analog of the Lüroth's problem discussed here is much different. Although the similarities between the questions raised at the Introduction are still valid for groups and fields [4], the equivalent of Cohn's theorem involves deeper geometric properties. For instance, what are the $\mathbf{k}$-subalgebras B of $\mathbf{k}[x, y] = C$ over which C is faithfully flat? B is a Noetherian regular ring of dimension at most two. If the dimension of B is less than two, $B = \mathbf{k}[f]$ ([18]). W. Heinzer pointed out that if $\dim(B) = 2$ the Zariski's theorem on the Hilbert 14th. problem implies the finite generation of B. But whether one has to resort to this theorem and how close is B from being a polynomial ring remain unanswered questions.

REFERENCES

1. N. BOURBAKI, "Algèbre Commutative," Chap. 7, Diviseurs, Hermann, Paris, 1965.
2. P. M. COHN, Bezout rings and their subrings, *Proc. Cambridge Phil. Soc.* **64** (1968), 251–264.
3. P. EAKIN AND W. HEINZER, A cancellation problem for commutative rings, *in* "Proc. Kansas Commutative algebra Conference, Lecture Notes in Math.," Vol. 311, pp. 61–67, Springer-Verlag, Berlin, 1973.
4. C. FAITH, Derivations and generations of finite extensions, *Bull. Amer. Math. Soc.* **67** (1961), 550–553.
5. L. GRUSON, Dimension homologique des modules plats sur un anneau commutatif noetherien, *in* "Symposia Mathematica XI," pp. 243–254, Academic Press, London and New York, 1973.
6. E. HAMANN, On the R-invariance of $R[x]$, *J. Algebra* **35** (1975), 1–16.
7. W. HEINZER AND J. OHM, The finiteness of I when $R[x]/I$ is flat (II), *Proc. Amer. Math. Soc.* **35** (1972), 1–8.
8. M. HOCHSTER, Nonuniqueness of coefficient rings in a polynomial ring, *Proc. Amer. Math. Soc.* **34** (1972), 81–82.
9. J. OHM AND D. RUSH, The finiteness of I when $R[x]/I$ is flat, *Trans. Amer. Math. Soc.* **171** (1972), 377–408.

10. M. Raynaud, Anneaux locaux Henseliens, *in* "Lecture Notes in Math.," Vol. 169, Springer–Verlag, Berlin, 1970.
11. M. Raynaud and L. Gruson, Critères de platitude et de projectivité, *Inventiones Math.* 13 (1971), 1–89.
12. J. D. Sally and W. V. Vasconcelos, Flat ideals I, *Commun. in Algebra* 6 (1975), 531–543.
13. C. Traverso, Seminormality and Picard group, *Ann. Scuola Norm. Sup. Pisa* **24** (1970), 585–595.
14. W. V. Vasconcelos, Simple flat extensions II, *Math. Zeitschr.* **129** (1972), 57–61.
15. W. V. Vasconcelos, The λ-dimension of a ring, Proc. Kingston Commutative Algebra Conference, *Queen's Papers in Pure and Applied Math.* **42** (1975), 212–224.
16. W. V. Vasconcelos, On projective modules of finite rank, *Proc. Amer. Math. Soc.* **22** (1969), 430–433.
17. D. L. Wright, Algebras which resemble symmetric algebras, Ph.D. Thesis, Columbia University, 1975.
18. A. Zaks, Dedekind subrings of $k[x_1, \ldots, x_n]$ are rings of polynomials, *Israel J. Math.* **9** (1971), 285–289.