LE MATEMATICHE
Vol. XLVIII (1993) – Fasc. II, pp. 203-212

SUBRING OF CONSTANTS OF A RING OF CHARACTERISTIC $p > 0$

MARILENA CRUPI

Let A be a local ring of characteristic $p > 0$ which has a p-basis over a subring C, and B be the subring of constants of A for a derivation (or derivations) of A over C.
We give a sufficient condition for B to have a p-basis over C. We add some examples.

Introduction.

Let (A, m) be a local ring of prime characteristic p and let B be an intermediate local ring between A and A^p. It is interesting to deduce theoretic properties of B from theoretic properties of A.
In this direction there are several results when B is the subring of constants of A for derivations of A ([10]).
For example if A is a complete regular local ring and the derivations satisfy certain conditions, B is a complete regular local ring too ([10]). On the other hand we know that if R is a regular local ring of characteristic $p > 0$ and R is a finite R^p-module, R has a p-basis over R^p ([2]).
Hence it is interesting to study when if A has a p-basis over A^p, B has a p-basis over A^p too.

Entrato in Redazione il 20 settembre 1993.

Partially supported by M.U.R.S.T. (60%) and a member of C.N.R. - G.N.S.A.G.A.

The purpose of this paper is to study when if A is a ring of prime characteristic p with a p-basis over a subring C, the subring of constants of A for a finite number of derivations of A over C, has a p-basis over C too.
We prove the following result:

Let (A, m) be a local ring of characteristic $p > 0$ and of dimension n and let k be a subfield of A.
Suppose that

i) *$A \otimes_k k^{p^{-1}}$ is reduced*
ii) *A/m is a separable extension of k*
iii) *there exist $x_1 \dots, x_r \in m$ and $D_1 \dots, D_r \in \mathrm{Der}_k(A)$ such that*

$$D_i x_j = \delta_{ij} \qquad [D_i, D_j] = 0 \qquad D_i^p = 0\,.$$

Then if A has a finite p-basis over k, the subring of constants of A for $D_1 \dots, D_r$ has a finite p-basis over k too.

The author would like to express her hearty thanks to Professor H. Matsumura for his encouragement and helpful suggestions.

1. Preliminaries.

In this paper, p is always a prime number and all rings are assumed to be commutative, noetherian with a unit element.
Let A be a ring of characteristic p and A^p denote the subring of A $\{x^p : x \in A\}$. Let B a subring of A. A subset Γ of A is said to be p-independent over B, if the monomials $x_1^{e_1} \dots x_n^{e_n}$, where $x_1, \dots, x_n$ are distinct elements of Γ and $0 \leq e_i < p$, are linearly independent over $A^p[B]$. Γ is called a p-basis of A over B if it is p-independent over B and $A^p[B, \Gamma] = A$.

We denote the differential module of A over B by $\Omega_B(A)$ and the differentiation of A over B by d. For definition and elementary properties, refer to [6].

Now let A be a ring. The set of all derivations of A into itself is an A-module and is denoted by $\mathrm{Der}\,(A)$.

If B is a subring of A, the submodule consisting of the derivations which vanish on B will be denoted by $\mathrm{Der}_B(A)$.

If $D_1, \dots, D_n \in \mathrm{Der}_B(A)$, the subring

$$A_0 = \{a \in A : D_i(A) = 0, \quad i = 1, \dots, n\}$$

is called the subring of constants of A over B for $D_1, \dots, D_r$.

Finally, for later use recall the following result:

Proposition 1. ([8], 38. Proposition) *Let (R, m_R) be a local ring of characteristic p, and S be a subring of R containing R^p such that R is finite over S. Put $m_S = m_R \cap S$, $k = R/m_r$ and $k' = S/m_s$. If $\Omega_S(R)$ is a free R-module with $dx_1, \dots, dx_r (x_i \in R)$ as a basis, then $x_1, \dots, x_r$ form a p-basis of R over S.*

2. Results.

Theorem 1. *Let (A, m) be a local ring of characteristic $p > 0$ and of dimension n. Let $x_1, \dots, x_r \in m$ and $D_1, \dots, D_r \in \mathrm{Der}(A)$ be such that*

$$D_i x_j = \delta_{ij} \qquad [D_i, D_j] = 0 \qquad D_i^p = 0$$

and put

$$A_0 = \{a \in A : D_i(A) = 0,\ i = 1, \dots, r\}.$$

Then we have

1) *$\{x_1, \dots, x_r\}$ is a p-basis of A over A_0.*
2) *Let $I = x_1 A + \cdots + x_r A$, $I_0 = x_1^p A_0 + \cdots + x_r^p A_0$. Then $I \cap A_0 = I_0$ and $A/I \simeq A_0/I_0$.*
3) *A_0 is a local ring of dimension n with the same residue field as A.*
4) *Put $m_0 = m \cap A_0$ and let $y_1, \dots, y_s \in m_0$ be such that their images in A_0/I_0 form a minimal set of generators of m_0/I_0. Then $\{x_1, \dots, x_r, y_1, \dots, y_s\}$ is a minimal set of generators of A. If A is regular then A_0 is also regular, $r + s = n$ and $\{x_1^p, \dots, x_r^p, y_1 \dots, y_s\}$ is a regular system of parameters of A_0.*

Proof. 1) We proceeded by induction on r.

For $r = 1$, see [9], Ex. 25.5 or Theorem 27.3.

Now let $r > 1$ and put $A_1 = \{a \in A : D_1(A) = 0\}$. A_1 is a local ring with maximal ideal $m' = m \cap A_1$.
Moreover $\{x_2, \dots, x_r\} \subset m'(D_i(x_i) = 0,\ i = 2, \dots, r)$.
Now let $\bar{D}_2, \dots, \bar{D}_r$ be the restriction of $D_2, \dots, D_r$ to A_1. By virtue of the assumptions $[D_1, D_i] = 0$, each $\bar{D}_j$ maps A_1 into itself.
Hence we can apply the induction hypothesis to A_1 and $\{x_1, \dots, x_r\}$ will be a p-basis of A over A_0.

2), 3), 4): see [10], Theorem 5.

Remark 1. A can be non regular even if we assume that A_0 is regular.
For example if $A = k[[X, Y]]/(X^p)$, $D = \partial/\partial x$.
But if we assume that A_0 is regular and $\{x_1^p, \dots, x_r^p,\ y_1, \dots, y_s\}$ is a regular system of parameters then A is regular.

Remark 2. Under the same hypotheses of Theorem 1, if A is a regular local ring that is a finite A^p-module, A_0 has a p-basis over A^p and over A_0^p.
In fact if A is regular and is a finite A^p-module, by [3], Lemma 4, A_0 is regular and has a p-basis over A^p.
Moreover since A_0 is an intermediate local ring between A and A^p and since A^p is a noetherian ring, A_0 is a finite A^p-module. Hence A_0 is a finite A_0^p-module and by [2], Cor. 3.2, A_0 has a p-basis over A_0^p.

Lemma 1. *Let (A, m) be a local ring and let k be a subfield of A of characteristic $p > 0$. Suppose*

i) *A has a p-basis over k;*
ii) *$A \otimes_k k^{p^{-1}}$ is reduced.*

Then A is a regular local ring.

Proof. See [11], Lemma 1.

Now we are ready to prove the main theorem.

Theorem 2. *Let (A, m) be a local ring of characteristic $p > 0$ and of A dimension n and let k be a subfield of A. Suppose that*

i) *$A \otimes_k k^{p^{-1}}$ is reduced;*
ii) *A/m is a separable extension of k;*
iii) *there exist $x_1, \dots, x_r \in m$ and $D_1, \dots, D_r \in \mathrm{Der}_k(A)$ such that*

$$D_i x_j = \delta_{ij} \qquad [D_i, D_j] = 0 \qquad D_i^p = 0\,.$$

Put

$$A_0 = \{a \in A : D_i(A) = 0,\ i = 1, \dots, r\}.$$

If A has a finite p-basis over k, A_0 has a finite p-basis over k too.

Proof. First of all we observe that by i) A is a regular local ring (Lemma 1), hence A_0 is a regular local ring too (Theorem 1) with regular system of parameters $\{x_1^p, \dots, x_r^p, x_{r+1}, \dots, x_n\}$, and $\{x_1, \dots, x_r, x_{r+1}, \dots, x_n\}$ is a regular system of parameters of A.
By hypothesis A is a finite $k[A^p]$-module and then since A is a noetherian ring, $k[A^p]$ is a noetherian ring too ([9], Th. 3.7).
Since $k[A^p]$ is a noetherian ring the $k[A^p]$-submodule of A, A_0 is a finite $k[A^p]$-module too.
On the other hand A has a finite p-basis over A_0 (Theorem 1) and so A is a finite A_0-module too. Hence A^p is a finite A_0^p-module and so $k[A^p]$ is a finite $k[A_0^p]$-module too.

Finally A_0 is a finite $k[A_0^p]$-module $\left(k[A_0^p] \subset k[A^p] \subset A_0\right)$.
Hence in order to prove that A_0 has a finite p-basis over k, it sufficies to show that $\Omega_k(A_0)$ is a free A_0-module (Proposition 1).

From Theorem 1, $\Gamma = \{x_1, \dots, x_r\}$ is a p-basis of A over A_0, i.e.

$$A = A_0[x_1, \dots, x_r].$$

Then

$$A \simeq A_0[X_1, \dots, X_r]/I$$

where $I = (X_1^p - x_1^p, \dots, X_r^p - x_r^p)$ and $X_1, \dots, X_r$ are indeterminates over A_0.

Thanks to [8], Theorem 58, the inclusions

$$k \subset A_0 \subset A$$

induce the following isomorphism of A-modules

$$\phi : (\Omega_k(A_0) \otimes_{A_0} A / \sum_{i=1}^{r} A_0 dx_i^p \otimes_{A_0} A) \oplus AdX_1 \oplus \dots \oplus AdX_r \to \Omega_k(A)$$

where AdX_i' s are free A-modules generated by symbols dX_i's and $\phi(dX_j) = d'x_j$, $i = 1, \dots, r$, d is the universal k-derivation of A_0 and d' is the universal k-derivation of A.
Since A has a finite p-basis over k, $\Omega_k(A)$ is a free A-module of finite rank.
Put $M = \Omega_k(A_0)/\sum_{i=1}^{r} A_0 dx_i^p$. Then $M \otimes_{A_0} A$ is a free A-module of finite rank.
Then we can easily show that M is a finite free A_0-module and so

$$\Omega_k(A_0) \simeq M \oplus \sum_{i=1}^{r} A_0 dx_i^p .$$

Therefore to prove that $\Omega_k(A_0)$ is a free A_0-module it sufficies to show that $\sum_{i=1}^{r} A_0 dx_i^p$ is a free A_0-module.
We have to prove that $dx_1^p, \dots, dx_r^p$ are linearly independent over A_0.

Suppose that

$$(*) \qquad \sum_{i=1}^{r} a_i dx_i^p = 0, \quad a_i \in A_0.$$

By the meaning of $(\Omega_k(A_0), d)$, for every A_0-module L and every $\delta \in \mathrm{Der}_k(A_0, L)$ there is a unique A-linear map f from $\Omega_k(A_0)$ to L such that $f \circ d = \delta$.
Then $(*)$ is equivalent to saying

$$\sum_{i=1}^{r} a_i \delta x_i^p = 0$$

for every $\delta \in \mathrm{Der}_k(A_0, L)$.
Since A_0 is a regular local ring with $\{x_1^p, \ldots, x_r^p, x_{r+1}, \ldots, x_n\}$ as a system of parameters, by ii) there exists a coefficient field K_0 of $\hat{A}_0$ containing k and

$$\hat{A}_0 = K_0[[x_1^p, \ldots, x_r^p, x_{r+1}, \ldots, x_n]]$$

where $K_0 = A_0/m_0 = A/m, m_0 = m \cap A_0$ is the maximal ideal of A_0 (Theorem 1).

Then there exist K_0-derivations $\bar{D}_1, \ldots, \bar{D}_r : A_0 \to \hat{A}_0$ such that $\bar{D}_i x_j^p = \delta_{ij}, i, j = 1, \ldots, r$, since $x_1^p, \ldots, x_r^p, x_{r+1}, \ldots, x_n$ are analytically independent over K_0.
Therefore

$$\sum_{i=1}^{r} a_i \bar{D}_j x_i^p = 0$$

implicates that

$$\sum_{i=1}^{r} a_i \delta_{ji} = 0$$

and we get the stated result.

Corollary 1. *Let (A, m) be a local ring of characteristic $p > 0$ and of dimension n and let k be a subfield of A. Let B be a subring of A containing $k[A^p]$. Suppose that*

i) *$A \otimes_k k^{p^{-1}}$ is reduced;*
ii) *A/m is a separable extension of k;*
iii) *A has a finite p-basis over k.*

Then B has a finite p-basis over k if and only if B is a regular ring.

Proof. If B has a finite p-basis over k, since $B \otimes_k k^{p^{-1}}$ is reduced, B is a regular local ring (Lemma 1).

Now let B be a regular local ring.
A is a regular local ring that is a finite $k[A^p]$-module (Lemma 1 and iii)). Moreover since $k[A^p] \subset B$, A is also a finite B-module.
Then thanks to [3], Theorem, A has a finite p-basis over B.

Let $\Gamma = \{y_1, \dots, y_s\}$ be a p-basis of A over B.
Then there exist s B derivations $D_1, \dots, D_s$ such that $D_i y_j = \delta_{ij}$, $i, j = 1, \dots, s$. (It sufficies to take $D_i = \dfrac{\partial}{\partial y_i}$).
It follows that $[D_i, D_j] = 0$ and $D_i^p = 0$ and so from Theorem 2 B has a finite p-basis over k.

Now we give some examples in which we construct the subring of constants of local rings A of prime characteristic p with p-basis over A^p, with respect to certain derivations.
Moreover we determine, when it is possible, the p-basis of this subring.

Example 1. Let A be a local ring of characteristic $p = 3$ and let $\{e_1, e_2\}$ be a 3-basis of A over A^3.
Then A is a free A^3-module with $\{1, e_1, e_2, e_1^2, e_2^2, e_1e_2, e_1e_2^2, e_1^2e_2, e_1^2e_2^2\}$ as a basis.
Let $D : A \to A$ be the A^3-derivation of A defined by

$$D = e_2 \frac{\partial}{\partial e_1} - e_1 \frac{\partial}{\partial e_2}$$

and put

$$A_0 = \{a \in A : D(A) = 0\}.$$

Then we want to determine the elements of A_0. We observe that

$$e_1^2 + e_2^2 \in A_0 \big(D(e_1^2 + e_2^2) = 2e_1e_2 - 2e_1e_2 = 0 \big).$$

Let $a \in A_0$. Since $a \in A$ and $\{e_1, e_2\}$ is a 3-basis of A over A^3 we have

$$(1) \qquad a = \sum_{i,j} a_{ij} e_1^i e_2^j \qquad 0 \le i, j < 3, a_{ij} \in A^3.$$

But a is an element of A_0 and then

$$0 = D(a) = a_{10}e_2 + 2a_{20}e_1e_2 - a_{01}e_1 + a_{11}(-e_1^2 + e_2^2) + a_{21}(-e_1^3 + 2e_1e_2^2) - \\ - 2a_{02}e_1e_2 + a_{12}(-2e_1^2e_2 + e_2^3) + a_{22}(-2e_1^3e_2 + 2e_1e_2^3)$$

hence

$$(2) \qquad (-a_{12}e_2^3 - a_{21}e_1^3) + (-a_{01} + 2a_{22}e_2^3)e_1 + (a_{10} - 2e_1^3a_{22})e_2 + \\ + (2a_{20} - 2a_{02})e_1e_2 + a_{11}(-e_1^2 + e_2^2) + 2a_{21}e_1e_2^2 - 2a_{12}e_1^2e_2 = 0.$$

Since $1, e_1, e_2, -e_1^2 + e_2^2, e_1e_2, e_1e_2^2, e_1^2e_2$ are linearly independent over A^3 and the coefficients of (2) are elements of A^3, we obtain

$$a_{11} = a_{21} = a_{12} = 0,\ a_{20} = a_{02}, a_{01} = 2a_{22}e_2^3, a_{10} = 2e_1^3a_{22}.$$

If we put these values in (1) we obtain

$$a = a_{00} + a_{20}(e_1^2 + e_2^2) + a_{22}(2e_1^4 + 2e_2^4 + e_1^2e_2^2).$$

Therefore

$$A_0 = \left\{\lambda_1 + \lambda_2(e_1^2 + e_2^2) + \lambda_3(2e_1^4 + 2e_2^4 + e_1^2e_2^2), \lambda_i \in A^3\right\}.$$

Now it is easy to see that $1, e_1^2 + e_2^2, 2e_1^4 + 2e_2^4 + e_1^2e_2^2$ are linearly independent over A^3.
Hence A_0 is a free module with basis $\{1, e_1^2 + e_2^2, 2e_1^4 + 2e_2^4 + e_1^2e_2^2\}$ over A^3. But $2e_1^4 + 2e_2^4 + e_1^2e_2^2 = \frac{1}{2}(e_1^2 + e_2^2)^2$ and then A_0 is a free A^3-module with $\left\{1, e_1^2 + e_2^2, (e_1^2 + e_2^2)^2\right\}$ as basis. Hence $\left\{e_1^2 + e_2^2\right\}$ is a 3-basis of A_0 over A^3. Note that A_0 is not regular if e_1, e_2 are in the maximal ideal of A.

Example 2. Let A be a local ring of characteristic $p = 3$ and let $\{e_1, e_2\}$ be a 3-basis of A over A^3.
Let $D : A \to A$ be the A^3-derivation of A defined by

$$D = \frac{\partial}{\partial e_1} + e_1\frac{\partial}{\partial e_2}$$

and put

$$A_0 = \left\{a \in A : D(A) = 0\right\}.$$

By direct calculation as in the preceding example, we find that $A_0 = A^3[e_1^2 + e_2]$, and $\left\{e_1^2 + e_2\right\}$ is a 3-basis of A_0 over A^3. We have $A = A_0[e_1]$, and $\{e_1\}$ is a 3-basis of A over A_0. Hence A_0 is regular if A is so.

Example 3. Let A be a local ring of characteristic $p = 3$ and let $\{e_1, e_2\}$ be a 3-basis of A over A^3.
Let $D : A \to A$ be the A^3-derivation of A defined by

$$D = e_1\frac{\partial}{\partial e_2} + (e_1 + e_2)\frac{\partial}{\partial e_1}.$$

By direct calculation we can easly prove that $A_0 = A^3$.

Remark 3. In [7], there is the following result:
Let E be a field of characteristic $p > 0$, F a subfield such that (1) $[E : F] < \infty$ *and* (2) *E is purely inseparable of exponent one over F (i.e. $E^p \subseteq F$).*
Then $\mathrm{Der}_F(E)$ *is a p-Lie algebra such that $p^n = [E : F]$, where n is the dimension of* $\mathrm{Der}_F(E)$ *as vector space over E.*
Conversely if $\bar{D}$ is a p-Lie algebra of derivations of E (i.e. $\bar{D}$ is an E-module of derivations of E into itself such that $d \in \bar{D}$ implies $d^p \in D$, and $d, d' \in \bar{D}$ implies $[d, d'] = dd' - d'd \in \bar{D}$) such that $[D : E] < \infty$ and if F is the set of $\bar{D}$-constants of E, then $[E : F] < \infty$ and E is purely inseparable of exponent one over F, and $\bar{D} = \mathrm{Der}_F(E)$. Moreover, if $\{D_1, \ldots, D_n\}$ is a basis for $\bar{D}$ over E, then the set of monomials $\{D_1^{k_1} \ldots D_n^{k_n},\ 0 \le k_i < p\}$ form a basis for $\mathrm{End}_F(E)$ *regarded as vector space over E.*

It follows from this theorem that, if we consider an integral domain A of characteristic p and a derivation $D : A \to A$ and its ring of constants $A^D = \{a \in A : D(a) = 0\}$, we should look at the quotient field K of A, and the unique extension of D to a derivation of K (which we shall denote by the same letter D). The K-module $\bar{D}$ generated by $D, D^p, D^{p^2}, \ldots$ is a p-Lie algebra of derivations of K, and of course we have $K^D = K^{\bar{D}}$ and $A^D = A \cap K^D$.
Therefore if $[\bar{D} : K] = r$, then $[K : K^D] = p^r$.
In Ex. 3, we have

$$D^3 = -e_2\frac{\partial}{\partial e_1} + (-e_1 + e_2)\frac{\partial}{\partial e_2}$$

and $D^9 = D$. Hence $[\bar{D} : K] = 2$ and $K^D = K^3$, $A^D = A \cap K^3 = A^3$. (Since A is flat over A^3, A is a regular local ring by a theorem of Kunz and so $A^3 (\simeq A)$ is also regular. Therefore A^3 is integrally closed in K^3 and we have $A \cap k^3 = A^3$).
In Ex. 1,2 we have $D^p = D^3 = aD$ for some $a \in A$, and so $[\bar{D} : K] = 1$ and so we know $A^D \neq A^3$.

Example 4. Let k be a field of characteristic $p = 2$ and let $A = k[[X, Y, Z]]$ a regular local ring of dimension 3. For simplicity let us assume that k is perfect. Then $A^2 = k[[X^2, Y^2, Z^2]]$ and $\{X, Y, Z\}$ is a 2-basis of A over A^2. Let

$$D = X\frac{\partial}{\partial X} + Y\frac{\partial}{\partial Y} + Z\frac{\partial}{\partial Z}.$$

Then we can check that $D^2 = D$, $A_0 \coloneqq \{a \in A : D(a) = 0\} = k[[X^2, Y^2, Z^2, XY, YZ, XZ]]$, which has no 2-basis over A^2.

REFERENCES

[1] L. Chiantini, *p-basi e basi differenziali di un anello,* Rend. Sem. Mat. Univ. Politecn. Torino, 37 (1979), pp. 103–121.

[2] T. Kimura - H. Niitsuma, *Regular local ring of characteristic $p > 0$ and p-basis,* J. Math. Soc. Japan, 32 No 2 (1980), pp. 363–371.

[3] T. Kimura - H. Niitsuma, *On Kunz's conjecture,* J. Math. Soc. Japan, 34 (1982), pp. 371–378.

[4] T. Kimura - H. Niitsuma, *Differential basis and p-basis of a regular local ring,* Proc. Am. Math. Soc., 92 (1984), pp. 335–338.

[5] E. Kunz, *Characterizations of regular local rings of characteristic $p > 0$,* Am. J. Math., 91 (1969), pp. 772–784.

[6] E. Kunz, *Kahler Differentials,* Viehweg & Sohn, Braunschweig, 1986.

[7] N. Jacobson, *Lectures in Abstract Algebra III. Theory of Fields and Galois Theory,* Van Nostrand, 1964.

[8] H. Matsumura, *Commutative Algebra,* 2nd ed., Benjamin Inc., New York, 1980.

[9] H. Matsumura, *Commutative Ring Theory,* Cambridge Univ. Press, 1986.

[10] G. Restuccia - H. Matsumura, *Integrable derivation II,* Acc. Pel. dei Pericolanti di Messina, 70 (1992), pp. 153–172.

[11] A. Tyc, *p-basis and smoothness in characteristic $p > 0$,* Proc. Am. Math. Soc., 103 (1988), pp. 389–394.

Dipartimento di Matematica,
Università di Messina,
Contrada Papardo, Salita Sperone 31,
98166 Messina (Italy)