DIFFERENTIAL BASIS,\( p \)-BASIS, AND SMOOTHNESS IN CHARACTERISTIC \( p > 0 \)

ANDRZEJ TYC

(Communicated by William C. Waterhouse)

ABSTRACT. It is shown that every differential basis of a Noetherian ring \( R \) of prime characteristic \( p \) over an arbitrary subring \( k \) is a \( p \)-basis of \( R \) over \( k \). Moreover, if \( k \) is a field, then \( R \) is smooth over \( k \), provided \( R \) has a differential basis over \( k \) and the ring \( R \otimes_k k^{p^{-1}} \) is reduced.

I. Introduction. Let \( R \) be a commutative ring of prime characteristic \( p \) and let \( k \) be a subring of \( R \). A subset \( \Gamma \) of \( R \) is called a differential basis of \( R \) over \( k \) if the \( k \)-module of Kähler differentials \( \Omega_k(R) \) is free and \( \{dy, y \in \Gamma\} \) is a basis of \( \Omega_k(R) \), or equivalently, if for any \( R \)-module \( M \) and any function \( s: \Gamma \rightarrow M \) there exists a unique \( k \)-derivation \( d: R \rightarrow M \) such that \( d|_{\Gamma} = s \). It is well known (and easily seen) that each \( p \)-basis of \( R \) over \( k \) is a differential basis of \( R \) over \( k \). Matsumura proved in [6] that the converse is true under the assumption that \( R \) is a local ring and \( R \) is a finite \( k \)-module. In [4] Kimura and Niitsuma established that the converse is true in the case where \( R \) is a regular local ring and \( k = R^p \). Our first aim in this paper is to prove that if \( R \) is a Noetherian ring and \( k \) is an arbitrary subring of \( R \), then every differential basis of \( R \) over \( k \) is a \( p \)-basis of \( R \) over \( k \). Our next aim is to indicate some connection between the notions of smoothness and that of differential basis. More precisely, we show that a Noetherian ring \( R \) is smooth over a subfield \( k \), whenever \( R \) possesses a differential basis over \( k \) and the ring \( R \otimes_k k^{p^{-1}} \) is reduced.

II. Preliminaries. In this paper all rings are commutative (with identity) and have prime characteristic \( p \). A local ring is assumed to be Noetherian. A ring \( R \) is said to be regular if all the localizations of \( R \) at prime ideals are regular local rings. \( R \) is said to be reduced if it has no nonzero nilpotent elements. Let \( k \) be a subring of a ring \( R \). A subset \( \Gamma \) of \( R \) is called \( p \)-independent over \( k \) if the monomials \( y_1^{s_1} \cdots y_n^{s_n} \), where \( y_1, \ldots, y_n \) are distinct elements in \( \Gamma \) and \( 0 \leq s_i < p \), are linearly independent over \( k[R^p] \) \( (R^p = \{r^p, r \in R\}) \). \( \Gamma \) is called a \( p \)-basis of \( R \) over \( k \) if it is \( p \)-independent over \( k \) and \( R = k[R^p, \Gamma] \). Given \( R \) and \( k \) as above, \( \Omega_k(R) \) will denote the \( k \)-module of Kähler differentials and \( d: R \rightarrow \Omega_k(R) \) will denote the canonical \( k \)-derivation. Now let \( t \) be a ring. Recall that a \( t \)-algebra \( A \) is said to be smooth if for any \( t \)-algebra \( B \), a nilpotent ideal \( N \) in \( B \), and a homomorphism of \( t \)-algebras \( f: A \rightarrow B/N \) there exists a homomorphism of \( t \)-algebras \( g: A \rightarrow B \) such that \( f(a) = g(a) + N \) for all \( a \in A \). If \( A \) is a local \( t \)-algebra with the unique maximal ideal \( m \), then \( A \) is said to be formally smooth if the above condition holds for those homomorphisms \( f: A \rightarrow B/N \) which vanish on some power of \( m \) (for
smoothness and formal smoothness, see [2 and 6]). Recall also that if \( t \) is a field, then a \( t \)-algebra \( B \) is called geometrically regular (resp. separable) if for any finite field extension \( L/t \), the ring \( B \otimes_t L \) is regular (resp. reduced). Finally, for later use recall the following result due to Fogarty.

**Proposition 1** [3, Proposition 1]. Let \( R \) be a Noetherian ring and let \( k \) be a subring of \( R \). Then \( R \) is a finite \( k[R^p] \)-module if and only if \( \Omega_k(R) \) is a finite \( R \)-module.

### III. Results.

**Theorem 1.** Let \( R \) be a Noetherian ring and let \( k \) be a subring of \( R \). Then each differential basis of \( R \) over \( k \) is a \( p \)-basis of \( R \) over \( k \).

**Proof.** Let \( \Gamma \) be a differential basis of \( R \) over \( k \). Since \( \Omega_k(R) = \Omega_{k[R^p]}(R) \), then replacing \( k \) with \( k[R^p] \) we may assume that \( k \) contains the subring \( R^p \). It is known (and easy to see) that the set \( \Gamma \) is \( p \)-independent over \( k \). So it remains to prove that \( k[\Gamma] = R \). First suppose that \( R \) is a local ring with the maximal ideal \( m \) and put \( L = R/m, L^+ = k/k \cap m \). Then clearly \( L^+ \) is a subfield of \( L \) containing \( L^p \). Furthermore, as the natural map \( \Omega_k(R) \to \Omega_{L^+}(L) \) is surjective, there is a subset \( S \) of \( \Gamma \) such that \( S = \{ s + m, s \in S \} \subset L \) is a \( p \)-basis of \( L \) over \( L^+ \). Let \( R' = k[S] \). One readily checks that \( \Gamma - S \) is a differential basis of \( R \) over \( R' \). On the other hand, by \( [2, \text{Satz} 1, (b)] \), there exists an exact sequence of \( L \)-modules and \( L \)-linear maps of the form

\[
0 \to m/(m^2 + m'R) \to \Omega_{R'}(R) \otimes_R L \to \Omega_{L^+}(L) \to 0,
\]

where \( m' = m \cap R', L' = R'/m' \subset L \) (\( R' = R'[R^p]! \)). Hence \( \Omega_{R'}(R) \otimes_R L \simeq m/(m^2 + m'R) \) as \( L \)-modules, because \( L' = L^+ [S] = L \). It follows that

\[
|\Gamma - S| = \text{rank} \Omega_{R'}(R) = \text{dim}_L(\Omega_{R'}(R) \otimes_R L)
\]

\[
= \text{dim}_L(m/(m^2 + m'R)) \leq \text{dim}_L(m/m^2) < \infty,
\]

which means that \( \Omega_{R'}(R) \) is a finite \( R \)-module. According to Proposition 1 this implies that \( R \) is a finite \( R' \)-module. This in turn implies that \( \Gamma - S \) is a \( p \)-basis of \( R \) over \( R' \), by the already mentioned Matsumura result [6, §38, Proposition]. Consequently, \( R = R'[\Gamma - S] = k[S][\Gamma - S] = k[\Gamma] \), and thus Theorem 1 has been shown in the case where \( R \) is a local ring.

Now suppose that \( R \) is an arbitrary Noetherian ring. Then for any prime ideal \( P \) in \( R \) the set \( \Gamma_P = \{ y/1 \in R_P, y \in \Gamma \} \) is a differential basis of \( R_P \) over \( k_q \), where \( q = P \cap k \). Therefore, by the first part of the proof, \( \Gamma_P \) is a \( p \)-basis of \( R_P \) over \( k_q \). In particular, given an \( r \in R \), there is a \( z_q \in k - q \) such that \( z_q r \in k[\Gamma] \). Since this holds for any \( P \in \text{Spec} R \) and any prime ideal \( q' \) in \( k \) of the form \( P' \cap k \), where \( P' = \{ x \in R, x^p \in q' \} \subset \text{Spec} R \), we see that \( r \in k[\Gamma] \). The conclusion is that \( R = k[\Gamma] \), as was to be shown.

**Corollary.** If \( R \) is a local ring and \( \Omega_k(R) \) is a free \( R \)-module of finite rank, then \( R \) possesses a \( p \)-basis over \( k \).

**Remark.** The proof of Theorem 1 is in part patterned upon the proof of the theorem in [4].

From now on, \( k \) denotes a fixed field.
THEOREM 2. Let $R$ be a Noetherian $k$-algebra satisfying the following conditions:
(1) $R$ has a differential basis over $k$, (2) the ring $R \otimes_k k^{p-1}$ is reduced. Then $R$ is a smooth $k$-algebra.

The lemmas below will be employed in the proof.

**LEMMA 1.** In the situation of Theorem 2, $R$ is a regular ring.

**PROOF.** It is easy to see that we may assume $R$ is a local ring. Then, thanks to the Kunz Theorem (cf. [6, Theorem 107]), it suffices to show that $R$ is a free $k^p$-module. By Theorem 1, $R$ is a free $k[R^p]$-module. So we will be done, if we prove that $k[R^p]$ is a free $k^p$-module. Let $S$ be a $p$-basis of $k$ over $k^p$. Our claim is that $S$ is a basis of $k[R^p]$ over $R^p$. Obviously, $S$ is a set of generators of $k[R^p]$ over $R^p$. Let $s_1,...,s_n \in S$ and $s_i \in R$. Then $s_i = y_i^p$ for certain $y_i \in k[R^p]$, and we have $0 = \sum r_i \otimes s_i = (\sum r_i \otimes y_i)^p$ in $R \otimes_k k^{p-1}$. Hence $0 = \sum r_i \otimes y_i$, because the ring $R \otimes_k k^{p-1}$ is reduced. But, as $s_1,...,s_n$ are linearly independent over $k^p$, $y_1,...,y_n$ are linearly independent over $k$. Consequently, $r_1 = \cdots = r_n = 0$, which means that $S$ is a basis of $k[R^p]$ over $R^p$. The lemma follows.

**REMARK 1.** Suppose that $R$ is a reduced local ring and $k$ is the prime field contained in $R$. From Lemma 1 it results that if $R$ has a differential basis over $k$ (or, what is the same, over $R^p = k[R^p]$), then $R$ is a regular local ring. The converse turns out to be false. To see this take $R = K[X]$, where $K$ is a field with $[K : K^p] = \infty$, and observe that, in view of [5, Example 3.8] and Theorem 1, $R$ has no differential basis over $k$.

**LEMMA 2.** Let $A$ be an integral domain containing the field $k$ and such that the ring $A \otimes_k k^{p-1}$ is reduced. Then the localization $A_S$ is a separable $k$-algebra for any multiplicative subset $S$ of $A$.

**PROOF.** It is clearly sufficient to show that the quotient field $A_0$ is a separable $k$-algebra. For this purpose we need only verify that the ring $A_0 \otimes_k k^{p-1}$ is reduced, see [6, (27.F) Lemma 3]. The latter follows easily from the assumption.

**LEMMA 3.** Suppose $R$ is a local $k$-algebra satisfying conditions (1) and (2) of Theorem 2. Then $R$ is a formally smooth $k$-algebra.

**PROOF.** In virtue of [6, Theorem 93] formal smoothness is equivalent to geometric regularity. Therefore, it is enough to show that $R \otimes_k L$ is a regular ring for any finite field extension $L/k$. Let $L/k$ be such an extension. By Lemma 1, the ring $A = R \otimes_k L$ is regular, whenever the $L$-algebra $A$ satisfies conditions (1) and (2) of Theorem 2. Since $\Omega_L(A) = \Omega_k(R) \otimes_R A$ and $R$ has a differential basis over $k$, $A$ has a differential basis over $L$. As for condition (2), Lemma 1 implies that $R$ is a regular local ring, so in particular, $R$ is an integral domain. By Lemma 2, it follows that $R$ is a separable $k$-algebra, whence $A \otimes_L L^{p-1} = R \otimes_k L \otimes_L L^{p-1} = R \otimes_k L^{p-1}$ is a reduced ring. The lemma is proved.

The next lemma is known.

**LEMMA 4.** Let $R$ be a Noetherian $k$-algebra such that
(a) $\Omega_k(R)$ is a projective $R$-module,
(b) $R_P$ is a formally smooth $k$-algebra for all $P \in \text{Spec } R$.
Then $R$ is a smooth $k$-algebra.
PROOF. In view of [1, p. 223, Proposition 17, p. 222, Definition 14] smoothness of $R$ amounts to $H^1(k, R, M) = 0$ for all $R$-modules $M$ (for the cohomology groups $H^1(k, R, M)$ and the homology groups $H_1(k, R, M)$ that we will use below, see [1]). Suppose for the moment that $H_1(k, R, M) = 0$ for all $R$-modules $M$. Then Lemma 19 in [1, p. 41] applied to $A = k$, $B = C = R$ and the assumption (a) give

$$H^1(k, R, M) = \text{Ext}_R^1(H_0(k, R, R), M) = \text{Ext}_R^1(\Omega_k(R), M) = 0$$

$$H_0(k, R, R) = \Omega_k(R).$$

So the proof reduces to showing that $H_1(k, R, M) = 0$ for all $M$. This condition, however, is equivalent to our assumption (b), by [1, p. 331, Theorem 30].

COROLLARY. Suppose $H$ is a commutative Hopf algebra over $k$ such that $H \otimes_k k^{p\mathbb{Z}}$ is a reduced ring and $H$ is finitely generated as a $k$-algebra. Then $H$ is a smooth $k$-algebra.

PROOF. Thanks to [7, §11.3, Theorem] and to the assumption we know that $\Omega_k(H)$ is a finite free $H$-module. It results that $\Omega_k(H_P)$ is a finite free $H_P$-module for any $P \in \text{Spec } H$. Hence, making use of Lemma 3, one obtains that $H_P$ is a formally smooth $k$-algebra for all $P$. Consequently, $H$ is a smooth $k$-algebra, by Lemma 4.

We are now in position to give the

PROOF OF THEOREM 2. As it was already noticed each localization of $R$ at a prime ideal satisfies conditions (1) and (2) of Theorem 2. Therefore, by Lemma 3, $R_P$ is a formally smooth $k$-algebra for any $P \in \text{Spec } R$. Moreover, $\Omega_k(R)$ is a free $R$-module, by condition (1). The conclusion now follows, using Lemma 4.

Let $R$ be a smooth $k$-algebra. It is not difficult to show that the ring $R \otimes_k k^{p\mathbb{Z}}$ is reduced. It turns out, however, that $R$ need not have a differential basis over $k$ (i.e. conditions (1) and (2) of Theorem 2 are essentially stronger then smoothness of $R$). To see this assume that $p = \text{char}(k) \neq 2$ and set $R = k[x, y]/(x^2 + y^2 - 1)$. Further, let $\Delta: R \rightarrow R \otimes_k R$, $S: R \rightarrow R$, and $\varepsilon: R \rightarrow k$ be the morphisms of $k$-algebras determined by

$$\Delta(x) = x \otimes x - y \otimes y, \quad \Delta(y) = x \otimes y + y \otimes x,$$

$$S(x) = x, \quad S(y) = -y,$$

$$\varepsilon(x) = 1, \quad \varepsilon(y) = 0,$$

where $x, y$ are the residues of $X, Y$. Then one readily checks (cf. [7, §1.6, Example 11(c)]) that $(R, \Delta, S, \varepsilon)$ is a Hopf algebra over $k$. By the corollary from Lemma 4, it results that $R$ is a smooth $k$-algebra. On the other hand we have

PROPOSITION. The following conditions are equivalent:

(a) $R$ has a differential basis over $k$,

(b) $-1$ is a square in $k$.

In particular, if $k = F_p$, then $R$ has a differential basis over $k$ if and only if $p \equiv 1 \mod 4$.

PROOF. Let $w = xdy - ydx$. From [7, §11] one knows that $w$ is a basis of $\Omega_k(R)$. So we have to prove that $\Omega_k(R) = Rdz$ with some $z \in R$ if and only if
$-1$ is a square in $k$. Denote by $\bar{k}$ an algebraic closure of $k$ and choose $i \in \bar{k}$ with $i^2 = -1$. Then

$$R' = k(i)[X, Y]/(X^2 + Y^2 - 1) = k(i)[U, V]/(UV - 1) \simeq k(i)[U]_U,$$

where $U = X + iY$, $V = X - iY$. Hence $\Omega_k(R') = R'dU$, which proves the implication (b) $\Rightarrow$ (a). Now suppose that $\Omega_k(R) = R'dU$ with some $z \in R$. Then $w = udz$ for some unit $u \in R$. Furthermore, it is easy to see that $w = i(dU/U)$ in $\Omega_k(R')$ and that the differential $dU/U$ is not exact (i.e. $dU/U \not\in d(R')$). This implies that the unit $u$ cannot be in $k$. Thus, all that remains to be proved is the following.

**Lemma 5.** If $u$ is a unit in $R$ and $u \notin k$, then $i \in k$.

**Proof of the Lemma.** Since every unit in $R'$ is of the form $aU^n$, where $a \in k(i)$ and $n$ is a rational integer, $u = a(x + iy)^n$ for some $a \in k(i)$ and $n \neq 0$. First consider the case in which $n > 0$. Then, by the equality $y^2 = 1 - x^2$, we have

$$u = a \cdot \sum_{m=0}^{n} \binom{n}{m} x^{n-m}(iy)^m = af(x) + aig(x)y,$$

where

$$f(x) = \sum_{j=0}^{n'} (-1)^j \binom{n}{2j} x^{n-2j}(1 - x^2)^j,$$

$$g(x) = \sum_{j=0}^{n''} (-1)^j \binom{n}{2j + 1} x^{n-2j-1}(1 - x^2)^j,$$

and $n'$, $n''$ are the integral parts of $n/2$, $(n - 1)/2$, respectively. It follows that the polynomials $af(x)$ and $aig(x)$ are in $k[x]$, because $R'$ (resp. $R$) is a free $k(i)[x]$-module (resp. a free $k[x]$-module) with 1, $y$ as a basis. Moreover, the coefficient at $x^n$ in the polynomial $af(x)$ is equal to $a \cdot \sum_{j=0}^{n'} \binom{n}{2j} = a2^{n-1}$ and the coefficient at $x^{n-1}$ in $aig(x)$ is equal to $a_i \cdot \sum_{j=0}^{n''} \binom{n}{2j + 1} = ai2^{n-1}$. Hence we conclude that $i \in k$ (char$(k) \neq 2$).

In the case where $n < 0$ we have $u = a(x + iy)^n = a(x - iy)^{-n}$, and exactly the same arguments as above show that $i \in k$. The lemma is proved.

**Acknowledgment.** The above proposition and the sketch of its proof is due to the referee. The author would like to thank the referee for his kind permission to use it in this paper.

**References**


INSTITUTE OF MATHEMATICS, POLISH ACADEMY OF SCIENCES, UL. CHOPINA 12/18, 87-100 TORUŃ, POLAND