Canonical-p-bases[*]

Martin Ziegler

14.3.2003

The purpose of this note is to give a proof of a remark[1] in [1]:

Theorem 1. *Every ω–saturated strict $\mathcal{D}$–field has a canonical p–basis.*

I will use the definitions and notation of [1]. As there, all fields have characteristic p. We start the proof with a couple of Lemmas.

In our application the following lemma, except of its last sentence, can be replaced by Lemma 3.

Lemma 2. *Let K be a field, $d_1, \ldots, d_e$ be a sequence of commuting derivations of K, and $C = C_1 \cap \cdots \cap C_e$, where C_i is the field of constants of d_i. Assume that*

a) $d_i^p = 0$ *for* $i = 1, \ldots, e$

b) $(K : C) = p^e$

Then there are elements $b_1, \ldots, b_e$ such that $d_i(b_j) = \delta_{i,j}$. Each such sequence generates K over C.

Proof. The proof of [1, Lemma 2.1] shows that, for every i, C is a proper subfield of $F_i = \bigcap_{j \neq i} C_j$, which is closed under d_i. Choose $b_i \in F_i$ with $d_i(b_i) = 1$. Consider the sequence

$$K = B_0 \supset B_1 \supset \cdots \supset B_e = C,$$

where $B_i = C_1 \cap \cdots \cap C_i$. b_i generates B_{i-1} over B_i, so $C(b_1, \ldots, b_e) = K$. □

Note that $K^p \subset C$. If $C = K^p$, the b_i form a p–basis of K.

Lemma 3. *Let K and $d_1, \ldots, d_e$ as in Lemma 2. For any sequence $x_1, \ldots, x_e$ of elements of K the following are equivalent:*

1. *There is a $y \in K$ such that $d_i(y) = x_i$ for $i = 1, \ldots, e$.*

[*] *Revision* : 1.3
[1] After Lemma 4.1

2. a) $d_i^{p-1}(x_i) = 0$ *for all* i.

b) $d_i(x_j) = d_j(x_i)$ *for all* i, j.

Proof. That 1 implies 2 is clear. We prove the converse by induction on e.

Case $e = 1$:
$d = d_1$ is a C-linear map, its kernel has dimension 1. This implies that the dimension of $d(K)$ is $p-1$ and the dimension of $\ker d^{p-1}$ at most $p-1$. Since $d(K) \subset \ker d^{p-1}$, we have $d(K) = \ker d^{p-1}$.

Case $e > 1$:
Since $(K : C_e) = p$, we can apply the first case to obtain an element $z \in K$ with $d_e(z) = x_e$. Set $x'_i = x_i - d_i(z)$. The x'_i again satisfy our assumption. They belong to C_e, since $d_e(x'_i) = d_i(x'_e) = d_i(0) = 0$. We apply the induction hypothesis to C_e, with derivations $d_1, \ldots, d_{e-1}$, and $x'_1, \ldots, x'_{e-1}$. This gives us a $y' \in C_e$ such that $d_i(y') = x'_i$ for $i = 1, \ldots, e-1$. Finally we set $y = y' + z$. □

Lemma 4. *Let* K *be a strict* $\mathcal{D}$*–field and* $n > 0$. *Assume that we have an element* a *such that for all* $m < n$

$$\mathbf{D}_{i,p^n}\mathbf{D}_{j,p^m}(a) = 0 \tag{1}$$

for all i, j. *Then there is an* a' *in* K *such that for all* j $\mathbf{D}_{j,p^n}(a') = 0$ *and*

$$\mathbf{D}_{j,p^m}(a') = \mathbf{D}_{j,p^m}(a)$$

for all $m < n$.

Proof. Set $x_i = \mathbf{D}_{i,p^n}(a)$. If we can find a y in

$$F = \{z \in K \mid D_{j,p^m}(z) = 0, \text{ for all } j \text{ and all } m < n\} = K^{p^n}$$

such that $\mathbf{D}_{i,p^n}(y) = x_i$ for all i, $a' = a - y$ will do the job.

We observe first, that the x_i belong to F, because for all j and $m < n$

$$\mathbf{D}_{j,p^m} x_i = \mathbf{D}_{j,p^m}\mathbf{D}_{i,p^n}(a) = \mathbf{D}_{i,p^n}\mathbf{D}_{j,p^m}(a) = 0.$$

The field F together with the derivations $\mathbf{D}_{i,p^n}$ satisfies the conditions of Lemma 3. So it remains only to check the conditions on the x_i:

$$\mathbf{D}_{i,p^n}^{p-1}(x_i) = \mathbf{D}_{i,p^n}^{p}(a) = 0$$
$$\mathbf{D}_{i,p^n}(x_j) = \mathbf{D}_{i,p^n}\mathbf{D}_{j,p^n}(a) = \mathbf{D}_{j,p^n}\mathbf{D}_{i,p^n}(a) = \mathbf{D}_{j,p^n}(x_i)$$

□

Proof of Theorem 1: Let K be a strict $\mathcal{D}$–field and n a natural number. Choose a p–basis $b_1, \ldots, b_e$ by Lemma 2 such that $\mathbf{D}_{i,1}(b_j) = \delta_{i,j}$. Now for every i, if we start with $a = b_i$ and apply Lemma 4 n-times, we get an element

b'_i such that for all $0 < m \leq n$ $\mathbf{D}_{j,p^m}(b'_i) = 0$ and $\mathbf{D}_{j,1}(b'_i) = \mathbf{D}_{j,1}(b_i)$ for all j. (Note that (1) holds trivially, since all $\mathbf{D}_{j,p^m}(a)$ are 0 or 1.)

The b'_i form a canonical p–basis "of depth p^{n+1}", i.e. we have for all $0 < m < p^{n+1}$

$$\mathbf{D}_{i,m}(b'_j) = \begin{cases} 1 & \text{if } m = 1 \text{ and } i = j \\ 0 & \text{otherwise} \end{cases}.$$

References

[1] Martin Ziegler. Separably closed fields with Hasse derivations. *J. Symbolic Logic*, 68:311–318, December 2003.