stichting mathematisch centrum



AFDELING ZUIVERE WISKUNDE

ZW 17/73

DECEMBER

J.M. GEIJSEL SCHNEIDER'S METHOD IN FIELDS OF CHARACTERISTIC p \neq 0

2e boerhaavestraat 49 amsterdam

Sthiotherk
Coultrasvoy Wishands en Informatics
Amsterdam

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.

Schneider's method in fields of characteristic $p \neq 0$

bу

J.M. Geijsel

Abstract

In this report two theorems on transcendental elements of fields of characteristic p > 0, namely L.I. Wade's result on the analogue of the Gelfond-Schneider theorem for fields of characteristic p (see Duke Math. J. $\underline{13}$ (1946), 79-85), and my result on the trancendency of certain values of the Carlitz-Bessel functions (see Math. Centre Report ZW 2/71, Amsterdam) are generalized for a wider class of so called E-functions.

Let \mathbb{F}_q be a finite field of characteristic $p \neq 0$ with $p = q^0$ elements. We denote by $\mathbb{F}_q[x]$ the ring of polynomials with coefficients in \mathbb{F}_q and by $\mathbb{F}_q[x]$ its quotientfield.

For $0 \neq E \in \mathbb{F}_q[x]$ we define the (logarithmic) valuation

dg E = degree of E and dg $0 = -\infty$.

For
$$Q \in \mathbb{F}_q\{x\}$$
 where $Q = \frac{E}{F}$ with $E, F \in \mathbb{F}_q[x]$ and $F \neq 0$ we define $dg \ Q = dg \ E - dg \ F$.

The completion of $\mathbb{F}_q\{x\}$ with respect to the valuation is denoted by F and the completion of the algebraic closure of F by Φ . The valuation dg on $\mathbb{F}_q\{x\}$ can be extended to Φ in a unique way and also will be denoted by dg.

A function $f : \Phi \rightarrow \Phi$ given by a power series

$$f(t) = \sum_{i=0}^{\infty} a_i t^i \quad \text{with } a_i \in \Phi,$$

which converges for all t with dg t < R is called linear if

$$\begin{cases} f(t+u) = f(t) + f(u) & \forall t, u \in \Phi \text{ with dg } t < R, \text{ dg } u < R, \\ f(ct) = cf(t) & \forall t \in \Phi \text{ with dg } t < R \text{ and } c \in \mathbb{F}_q. \end{cases}$$

For linear functions we define for all t for which the involving series converge the operators Δ^{r} (r=1,2,...) by

$$\Delta f(t) = f(xt) - x f(t),$$

$$\Delta^{r} f(t) = \Delta^{r-1} f(xt) - x^{q^{r-1}} \Delta^{r-1} f(t), \qquad r \ge 2.$$

For purpose of notation we define $\Delta^0 f(t) = f(t)$.

A function $f: \Phi \to \Phi$ is said to be *entire* if f can be written as a power series with coefficients in Φ , which converges for all $t \in \Phi$.

For entire linear functions f we have an "expansion formula" (see [1], or [2] lemma 2.1), namely:

for every M $\in \mathbb{F}_q[x]$ we have

$$f(Mt) = \int_{v=0}^{dg} \frac{\psi_{v}(M)}{F_{v}} \Delta^{v} f(t),$$
where
$$F_{v} := (x^{q^{v}} - x)(x^{q^{v}} - x^{q}) \dots (x^{q^{v}} - x^{q^{v}}), \quad v \ge 1$$

$$F_{0} := 1$$

$$\psi_{v}(t) := \prod_{\substack{dg \ E < v \\ E \in \mathbb{F}_{q}[x]}} (t - E).$$

Now we introduce a special class of linear functions.

Definition. A linear function $f : \Phi \rightarrow \Phi$ given by

$$f(t) = \sum_{k=0}^{\infty} a_k \frac{t^{q^k}}{F_k}$$

is called an E-function if there exists a finite separable algebraic extension K of F of degree h such that:

(1)
$$a_k \in K$$
, $k = 0, 1, ...$

(2)
$$\exists c \in \mathbb{R}, c > 0 \text{ such that dg } a_k < cq^k$$

(3) $\forall k \in \mathbb{N} \cup \{0\} \quad \exists Q_k \in \mathbb{F}_q[x] \text{ of minimal degree such that}$ $Q_k^a_0, Q_k^a_1, \dots, Q_k^a_k \text{ are integers in } K \text{ and}$ $\deg Q_k = O(kq^k), k \to \infty.$

Remarks

- (i) From (1) and (2) we have that every E-function is entire.
- (ii) The functions $\psi(t)$ and $J_n(t)$ (see [3]) are E-functions.
- (iii) Linear polynomials with separable algebraic coefficients in Φ are E-functions.
 - (iv) If f and g are E-functions then $\Delta^{\mathbf{r}} \mathbf{f}$ (r\ge 1), $\mathbf{f}^{\mathbf{q}}$, f + g are E-functions.
 - (v) If P is a linear polynomial with separable algebraic coefficients in Φ and Φ and Φ and Φ are Φ -function, then Φ

<u>Lemma 1.</u> Let K be a separable finite algebraic extension of $\mathbb{F}\{x\}$ of degree h. Let r, $s \in \mathbb{N}$ with 0 < r < s. Then the system of linear equations

$$\sum_{i=1}^{s} \alpha_{ki} X_{i} = 0 \qquad (k=1,\ldots,r),$$

where α_{ki} are algebraic integers in K and

$$a = \max_{k,i} (dg \alpha_{ki}, 0)$$

has a non-trivial solution $\{X_i\}_{i=1}^s$ with

$$X_{i} \in \mathbb{F}_{q}[x]$$

such that

$$dg X_{i} < \frac{cs + ar}{s - r} \qquad (i=1,...,s),$$

where c is a positive constant only depending on the field K.

Proof. We use the following lemma which will be proved in an appendix.

<u>Lemma</u>: Let K be a separable finite algebraic extension of $\mathbb{F}_q\{x\}$ of degree h. Then there exists a basis β_1 ,..., β_h of algebraic integers of K such that every algebraic integer ξ ϵ K can be written uniquely as

$$\xi = \sum_{i=1}^{h} A_i \beta_i$$
 with $A_i \in \mathbb{F}_q[x]$.

Further we use the methods of lemma 4.2 in [3]. [

Now we can formulate the main result of this paper.

Theorem 1. Let $f_1(t)$, ..., $f_n(t)$ be E-functions, not all polynomials. Suppose

$$\Delta^{r} f_{v}(t) = R_{vr}(f_{1}(t), ..., f_{n}(t))$$
, $r = 0, 1, ...; v = 1, ..., n$

where R are n-linear polynomials of n variables f₁,..., f_n of total degree $< q^r$ with coefficients in $\mathbb{F}_q[x]$ of degree $< q^r$.

Let $\alpha \neq 0$, $\beta \notin \mathbb{F}_q\{x\}$ and $f_{\nu}(t) \not\equiv 0$. Then at least one of the elements

$$\{\beta, f_1(\alpha), \dots, f_n(\alpha), f_1(\alpha\beta), \dots, f_n(\alpha\beta)\}$$

is transcendental over $\mathbb{F}_{q}\{x\}$.

Corollary 1.

- a) With the choice $f_1(t) = \psi(t)$, $\alpha = \lambda(\alpha^*)$, where α^* is not a zero of $\lambda(t)$, and $\beta \notin \mathbb{F}_q\{x\}$ we get the analogue of the theorem of Gelfond-Schneider: at least one of the elements $\{\beta, \alpha^* = \psi(\lambda(\alpha^*)), \psi(\beta\lambda(\alpha^*))\}$ is transcendental over $\mathbb{F}_q\{x\}$. This result was proved by Wade in [5].
- b) With $f_1(t) = J_n(t)$, $f_2(t) = \Delta J_n(t)$ and $\alpha \neq 0$, $\beta \notin \mathbb{F}_q\{x\}$ we get: at least one of the elements

$$\{\beta, J_n(\alpha), \Delta J_n(\alpha), J_n(\alpha\beta), \Delta J_n(\alpha\beta)\}$$

is transcendental over $\mathbb{F}_q\{x\}$. This result was essentially proved in [3], where the theorem said under the same conditions for α and β : at least one element of the set $V=\{\alpha,\beta,J_n(\alpha),\Delta J_n(\alpha),J_n(\alpha\beta),\Delta J_n(\alpha\beta)\}$ is transcendental over $\mathbb{F}_q\{x\}$. At the begin of the proof in [3] we supposed α to be algebraic over $\mathbb{F}_q\{x\}$ but we didn't use this fact, hence α can be omitted in V.

Corollary 2. If we choose $f_1(t) = \psi(\alpha_1^*t), \ldots, f_n(t) = \psi(\alpha_n^*t)$, where $\alpha_{\nu}^* \neq 0$, $\nu=1,\ldots,n$, and if $\alpha=1$, $\beta \notin \mathbb{F}_q\{x\}$ then at least one of the elements $\{\beta, \psi(\alpha_1^*), \ldots, \psi(\alpha_n^*), \psi(\alpha_1^*\beta), \ldots, \psi(\alpha_n^*\beta)\}$ is transcendental over $\mathbb{F}_q\{x\}$.

If now α_i is not a zero of $\lambda(t)$, $i=1,\ldots,n$, and $\alpha_i^*:=\lambda(\alpha_i)$, then at least one of the elements of the set $\{\beta,\alpha_1,\ldots,\alpha_n,\psi(\beta\lambda(\alpha_1)),\ldots,\psi(\beta\lambda(\alpha_n))\}$ is transcendental over $\mathbb{F}_q\{x\}$. For n=1 we have the result of corollary 1a.

For $\beta \notin \mathbb{F}_q^{\{x\}}$, α algebraic and $\lambda(\alpha) \neq 0$ we have: at least one of the elements $\{\beta, \psi(\beta\lambda(\alpha)), \psi(\beta\lambda(\alpha^q), \ldots, \psi(\beta\lambda(\alpha^q^n))\}$, $n \geq 1$, is transcendental over $\mathbb{F}_q^{\{x\}}$. Equivalent with this last result is: at least one of the

elements $\{\beta, \psi(\lambda(\alpha)), \psi(\beta\lambda(x\alpha)), \ldots, \psi(\beta\lambda(x^n\alpha))\}, n \ge 1$, is transcendental over $\mathbb{F}_q\{x\}$, since $\Delta\lambda(t) = \lambda(xt) - x\lambda(t) = \lambda(t^q)$.

Proof of theorem 1. Suppose β , $f_1(\alpha), \ldots, f_n(\alpha), f_1(\alpha\beta), \ldots, f_n(\alpha\beta)$ are algebraic over $\mathbb{F}_q\{x\}$, then, for some $e \in \mathbb{N}$, β^q , $f_1^q(\alpha), \ldots, f_n^q(\alpha)$, $f_1^q(\alpha\beta), \ldots, f_n^q(\alpha\beta)$ are separable over $\mathbb{F}_q\{x\}$ and they generate a separable extension K of $\mathbb{F}_q\{x\}$ of degree h.

Let $\Gamma \in \mathbb{F}_q[x]$ be such that $\Gamma \beta^q$, $\Gamma f_{\nu}^q(\alpha)$, $\Gamma f_{\nu}^q(\alpha \beta)$, $\nu=1,\ldots,n$, are algebraic integers of K.

The natural numbers k, ℓ with k < $\frac{1}{3}\ell$ will be chosen later. Define

$$L(t) := \sum_{v=1}^{n} \sum_{j=0}^{q^{2k}-1} \sum_{i=0}^{q^{2k}-1} X_{ijv} t^{jq^{e}} f_{v}^{iq^{e}}(\alpha t),$$

where the polynomials X_{ijv} will be determined by the following:

$$L(A+\beta B) = 0$$
 for all $A, B \in \mathbb{F}_q[x]$ with dg $A < m$, dg $B < m$, where $m := k + \ell - 1$.

Since $\beta \notin \mathbb{F}_q\{x\}$ we get a linear system of at most q^{2m} equations in $nq^{2k+2\ell}$ variables $X_{ij\nu}$ with algebraic coefficients:

(1)
$$L(A+\beta B) = \sum_{\nu=1}^{n} \sum_{j=0}^{q^{2k}-1} \sum_{i=0}^{q^{2k}-1} X_{ij\nu} (A+\beta B)^{jq} f_{\nu}^{iq} (\alpha(A+\beta B)) = 0,$$

$$dg A < m, dg B < m.$$

 $f_i(\alpha A + \alpha \beta B) = f_i(\alpha A) + f_i(\alpha \beta B)$ since f_i is linear. Since

with A $i\mu j_1 \cdots j_n \in \mathbb{F}_q[x]$ and dg A $i\mu j_1 \cdots j_n < q^\mu$, the expansion formula gives:

$$f_{\mathbf{i}}(\alpha A) = \sum_{\mu=0}^{\operatorname{dg}} \frac{A}{F_{\mu}} \underbrace{\int_{\mathbf{j}_{1}+\ldots+\mathbf{j}_{n}\leq\mu}}_{\mathbf{j}_{1}+\ldots+\mathbf{j}_{n}\leq\mu} A_{\mathbf{i}\mu\mathbf{j}_{1}\cdots\mathbf{j}_{n}} f_{1}^{q}(\alpha) \ldots f_{n}^{q}(\alpha).$$

Since
$$dg \frac{\psi_{\mu}(A)}{F_{\mu}} \le \max_{0 \le \mu \le dg} A dg \frac{\psi_{\mu}(A)}{F_{\mu}} = \max_{0 \le \mu \le dg} (q^{\mu}dg A - \mu q^{\mu}) \le dg A \cdot q^{dg} A$$
,

$$dg f_{i}(\alpha A) \leq mq^{m} + q^{m} + q^{m} \max\{dg f_{i}(\alpha), ..., dg f_{n}(\alpha), 0\}.$$

Since $f_{i}^{q}(\alpha A)$ resp. $f_{i}^{q}(\alpha \beta A)$ is a polynomial in $f_{v}^{q}(\alpha)$ resp. $f_{v}^{q}(\alpha \beta)$, i,v ϵ (1,...,n), of degree $\leq q^{m}$ with coefficients in $\mathbb{F}_{q}\{x\}$, the coefficients of X_{ijv} in (1) are polynomials in

$$\beta^{q^e}$$
 of degree $\leq q^{2k} - 1$
 $f_{\nu}^{q}(\alpha)$, $f_{\nu}^{q}(\alpha\beta)$ of degree $\leq (q^{2k}-1)q^m$

with coefficients in $\mathbb{F}_{q}\{x\}$.

Since $q^{2k}-1+2n(q^{2k}-1)q^m< q^{2k+2n}$ we can get a system of equations with integral algebraic coefficients in K by multiplying each equation with the factor

$$\Gamma^{q^{2l+2n}} (F_m^q)^{q^{2k-1}}.$$

This gives the system of equations:

$$\Gamma^{q^{2l+2n}} (F_m^q)^{q^{2k}-1} L(A+\beta B) = 0 \qquad \text{for dg A,dg B < m; A,B } \in \mathbb{F}_q[x]$$

which we denote by

(2)
$$\sum_{v=1}^{n} \sum_{j=0}^{2^{k}-1} q^{2k} - 1$$

$$\sum_{v=1}^{n} \sum_{j=0}^{n} \sum_{i=0}^{n} X_{ijv} D_{ijv} = 0 \quad \text{for A,B } \in \mathbb{F}_{q}[x]; \text{ dg A,dg B < m.}$$

Since m = k + ℓ - 1 the number of equations, q^{2m} , is less than the number of variables n $q^{2k+2\ell}$. Furthermore

$$dg D_{ij} \leq q^{2l+2n} dg \Gamma + mq^{m+2k+e} + q^{2l+e}(m+c_1) + q^{2k+e}(mq^m+q^m+q^mc_0)$$

where $c_1 = \max(dg\beta,0)$; $c_0 = \max(dg f_{\nu}(\alpha); dg f_{\nu}(\alpha\beta), (\nu=1,...,n); 0)$, which gives (since $k < \frac{1}{3}\ell$):

dg
$$D_{ijv} \le (3m+c_2)q^{2l+e}$$
 where $c_2 \ge 0$.

According to lemma 1 with $r=q^{2m}$, $s=nq^{2k+2\ell}$ and $a=\max(\deg D_{ij\nu},0)$ i,j, ν we have that there exist polynomials $X_{ij\nu}\in \mathbb{F}_q[x]$, not all zero, such that (1) is satisfied and

(3) dg
$$X_{ijv} \le (3m+c_3)q^{2l+e}$$
 where $c_3 \ge 0$.

Now we shall prove that, for all A , $B\in \mathbb{F}_q[x],\ L(A+\beta B)$ = 0. Let $\mu\geq m$ and η = μ - k + 1, then $\eta\geq \ell$. Furthermore let

$$\mathcal{B}(\mu)$$
 = {A + βB | dg A < μ , dg B < μ , A and B not both 0}.

Suppose L(t) = 0 for all t \in B(μ). Let $\xi \in$ B(μ +1) \ B(μ), then dg ξ = μ + g with g \geq 0. We choose ℓ such that m + g < 2m. By assumption

is an entire function since L(t) is entire. According to the maximum-modu-lus-principle

$$\label{eq:dg_def} dg\left(\frac{L(\xi)}{\Pi\left(\xi-A-\beta B\right)}\right) \leq \max_{\substack{dg \ t=2\mu}} \ dg \ \left(\frac{L(t)}{\Pi\left(t-A-\beta B\right)}\right).$$

Hence

$$dg L(\xi) \leq \max_{\substack{dg \ t = 2\mu}} dg L(t) - 2\mu(q^{2\mu}-1) + (\mu+g)(q^{2\mu}-1).$$

From the definition of L(t) we get

max dg L(t)
$$\leq$$
 max dg X_{ijv} + $2\mu q^{2k+e}$ + q^{2k+e} max dg f_v(α t). dg t = 2μ

Since $f_{,,}$ is an E-function we have

$$f_{v}(t) = \sum_{k=0}^{\infty} a_{vk} \frac{t^{q^k}}{F_k}, \quad v = 1,...,n,$$

where $\exists c > 0$ such that $dg \ a_{\nu k} < cq^k$ for $k > k_0$ and $\nu = 1, \dots, n$. Hence

$$\max_{\mbox{dg $t=2$$}\mu} \mbox{dg f}_{\mbox{ν}}(\alpha t) \leq \max_{\mbox{$k \geq 0$}} \mbox{$(dg$ a}_{\mbox{ν}k} + 2\mu q^k - kq^k + q^k dg \ \alpha) < \\ < \max_{\mbox{$k \geq 0$}} \mbox{$(c+2\mu-k+dg$ $\alpha)$} q^k \leq c_4^2 q^{2\mu}$$

where c_{Λ} > 0 and μ ≥ m. This gives

$$\label{eq:dg_L(x)} \text{dg} \ \text{L}(\xi) \ \le \ (3\text{m+c}_3) \, q^{2\ell+e} \ + \ 2\mu q^{2\ell+e} \ + \ c_4 q^{2\mu+2k+e} \ - \ (\mu-g) \, q^{2\mu}.$$

Since $\mu \ge m$, $\eta \ge \ell$ and $\mu = \eta + k - 1$ we get

(4) dg
$$L(\xi) \le q^{2\eta+e} (5\mu+c_5q^{4k}-(\mu-g)q^{2k-e}).$$

L(ξ) is a polynomial in β^q of degree $q^{2k}-1$ and in each of the $f_{\nu}^q(\alpha)$, $f_{\nu}^q(\alpha\beta)$ of degree $(q^{2k}-1)q^{\mu}$, hence L(ξ) is algebraic; since

$$q^{2l} + 2nq^{2k+\mu} < q^{2\eta+2n}$$
,

$$N(F_{\mu}^{q})$$
 $\Gamma^{q^{2\eta+2\eta}}$ $L(\xi)) \in \mathbb{F}_{q}[x]$

and

$$\begin{array}{lll} \text{dg N}(F_{\mu}^{q} & \Gamma^{q^{2\eta+2e}} & \text{L}(\xi)) \leq \\ \\ \leq h [\mu q^{2k+e+\mu} + q^{2\eta+2n} \text{ dg } \Gamma + q^{2\eta+e} & (5\mu+c_{5}q^{4k} - (\mu-g)q^{2k-e})] \leq \\ \\ \leq h q^{2\eta+e} [(6\mu+c_{6}q^{4k}) - (\mu-g)q^{2k-e}], \end{array}$$

which is negative for sufficiently large k and £. Now choose k and £ such that dg N(F $_{\mu}^{q}$ Γ^{q} L(ξ)) is negative. Hence L(ξ) = 0.

In the following k and ℓ are fixed. Since $\beta \notin \mathbb{F}_q\{x\}$ all A + βB are different and L(t) has an infinite number of zero's. Since L(t) is entire and not a polynomial L(t) is a transcendental function (see [4] or [2]).

Let N be the set of zero's \neq 0 of L(t), then N is countable and for any $\nu \in {\rm I\! N}$

$$L(t) = \gamma_0 \quad t^{\rho} \quad \prod_{\xi \in \mathcal{B}(\nu)} (1 - \frac{t}{\xi}) \quad \prod_{\xi \notin \mathcal{B}(\nu)} (1 - \frac{t}{\xi}) \quad \text{with } \rho \ge 0 \text{ and } \gamma_0 \in \Phi.$$

Let v_0 be the minimum of the degrees of the zero's $\neq 0$ of L(t), then

$$\max_{\text{dgt} = 2\nu} \deg \prod_{\xi \in \mathcal{N} \setminus \mathcal{B}(\nu)} (1 - \frac{t}{\xi}) \ge \max_{\text{dgt} = \frac{\nu_0}{2}} \deg \prod_{\xi \in \mathcal{N} \setminus \mathcal{B}(\nu)} (1 - \frac{t}{\xi}) = 0.$$

Furthermore

$$\Pi_{\xi \in \mathcal{B}(\nu)} (1 - \frac{t}{\xi}) = \frac{\Pi_{(\lambda + \beta B - t)}}{\Pi_{(\lambda + \beta B)}},$$

$$\mathcal{B}(\nu)$$

hence

max dg L(t)
$$\geq c_7 + 2\nu\rho + 2\nu(q^{2\nu}-1) - (\nu+g)(q^{2\nu}-1)$$
, dg t = 2ν

where c_7 is a constant only depending on L(t). This gives

(5)
$$\max_{\text{dg t} = 2v} \text{dg L(t)} \ge (c_8 v + c_9) q^{2v} \text{ with } c_8 > 0.$$

On the other hand we have proved

(6)
$$\max_{\text{dg t} = 2v} \text{dg L(t)} \le (3m+c_3)q^{2l+e} + 2vq^{2l+e} + c_4q^{2v+2k+e}$$
.

For ν large enough (5) and (6) are contradictory, which completes the proof of the theorem. \square

Remark. The theorem is also true for systems $\{f_1, \ldots, f_n\}$ for which the following relation is true:

$$\Delta^2 f_{v}(t) = R_{vr}(f_1(t), ..., f_n(t)), r=0,1,...; v=1,2,...,n,$$

where

$$R_{vr}(f_1(t),...,f_n(t)) = \sum_{j_1+...+j_n \le r} Q_{vrj_1...j_r} f_1^{q}(t)...f_n^{q}(t)$$

with $Q_{\nu r j_1 \cdots j_r} \in \mathbb{F}_q\{x\}$, such that for all $r \ge 0$ there exists a polynomial A_r such that $Q_{\nu \rho j_1 \cdots j_r} A_r \in \mathbb{F}_q[x]$ for $\rho = 0, 1, \ldots, r; 1 \le \nu \le n;$ $j_1 + \ldots + j_n \le r$ and dg $A_r < q^r$.

References

- [1] L. Carlitz On certain functions connected with polynomials in a Galoisfield, Duke Math. J. 1 (1935), 137-168.
- [2] J.M. Geijsel Speciale funkties over lichamen van karakteristiek p,
 Math. Centre Report ZN 35/70, Amsterdam, 1970.
- [3] J.M. Geijsel Transcendence properties of the Carlitz-Besselfunctions,
 Math. Centre Report ZW 2/71, Amsterdam, 1971.
- [4] W. Schöbe Beiträge zur Funktionentheorie in nichtarchimedisch bewerteten Körpern, Thesis, Helios, Münster, 1930.
- [5] L.I. Wade Transcendence properties of the Garlitz ψ -functions, Duke Math. J. 13 (1946), 79-85.

APPENDIX

<u>Lemma</u>. Let K be a separable finite algebraic extension of $\mathbb{F}_q\{x\}$ of degree h. Then there exists a basis β_1 , ..., β_h of algebraic integers of K such that every algebraic integer $\xi \in K$ can be written uniquely as

$$\xi = \sum_{i=1}^{h} A_i \beta_i \text{ with } A_i \in \mathbb{F}_q[x].$$

<u>Proof.</u> According to the theorem of the primitive element [*], since K is a separable finite extension of $\mathbb{F}_q\{x\}$ of degree h there exists an element $\theta \in K$ such that $K = \mathbb{F}_q\{x\}(\theta)$. θ is a separable algebraic element of K, hence there is a polynomial P in $\mathbb{F}_q[x]$ such that P θ is an algebraic integer of K. Denote P θ again by θ . Let $\theta_1 = \theta$, θ_2 , ..., θ_h be the conjugate elements of the algebraic integer θ . The discriminant $\Delta(1,\theta,\ldots,\theta^{h-1})$ of the basis $1,\theta,\ldots,\theta^{h-1}$ of K / $\mathbb{F}_q\{x\}$ is a Van der Monde determinant and since θ is separable, $\theta_1 \neq \theta_1$ ($i \neq j$); hence $\Delta(1,\theta,\ldots,\theta^{h-1}) \neq 0$. Furthermore is

$$\Delta(1,\theta,\ldots,\theta^{h-1}) = \prod_{1 \le i < j \le h} (\theta_i - \theta_j)^2$$

a symmetric polynomial in the conjugate elements of θ and can be expressed as a polynomial in the coefficients of the minimal polynomial of θ ; hence $\Delta(1,\theta,\ldots,\theta^{h-1})\in\mathbb{F}_{\sigma}[x]$.

For every base $\{\mathbf{w_l}, \dots \mathbf{w_h}\}$ of K / $\mathbb{F}_q\{\mathbf{x}\}$ with $\mathbf{w_i}$ algebraic integer in K we have

$$\Delta(w_1, \dots, w_h) = (\det(a_{ij}))^2 \cdot \Delta(1, \theta, \dots, \theta^{h-1})$$

where $w_i = a_{i1} + a_{i2}\theta + \dots + a_{ih}\theta^{h-1}$ (i=1,...,h) with $a_{ij} \in \mathbb{F}_q\{x\}$, and det $a_{ij} \neq 0$. On the other hand as a symmetric polynomial in the algebraic integers w_1 ,..., w_h and its conjugates $\Delta(w_1,\ldots,w_h) \in \mathbb{F}_q[x]$. Consider all bases $\{w_1,\ldots,w_h\}$ for K / $\mathbb{F}_q\{x\}$ with algebraic integers w_1 ,..., w_h . Then dg $\Delta(w_1,\ldots,w_h) \in \mathbb{N} + \{0\}$, hence there exists a basis $\{\beta_1,\ldots,\beta_h\}$ with dg $\Delta(\beta_1,\ldots,\beta_h)$ minimal and β_1 ,..., β_h algebraic integers. We shall prove that this basis $\{\beta_1,\ldots,\beta_h\}$ is a basis for the ring of algebraic

integers in K over $\mathbb{F}_{q}[x]$.

Suppose $\{\beta_1,\dots,\beta_h\}$ is not a basis for the integers in K over $\mathbb{F}_q[x]$, then there exists an algebraic integer $\xi\in K$ such that $\xi=a_1\beta_1+\dots+a_h\beta_h$ with $a_i\in\mathbb{F}_q[x]$ and not all $a_i\in\mathbb{F}_q[x]$. Suppose $a_1\notin\mathbb{F}_q[x]$. $a_1=A+r$ with $A\in\mathbb{F}_q[x]$ and $r\in\mathbb{F}_q[x]\setminus\mathbb{F}_q[x]$, dg r<0 and $r\neq0$. Now define

$$\beta_1^* = \xi - A\beta_1 = (a_1 - a)\beta_1 + a_2\beta_2 + \dots + a_h\beta_h$$

 $\beta_i^* = \beta_i$, $i = 2, \dots, h$.

The system $\{\beta_1^*,\ldots,\beta_h^*\}$ is a basis for K / $\mathbb{F}_q\{x\}$ and β_i^* (i=1,...,h) are algebraic integers.

$$\Delta(\beta_{1}^{*},...,\beta_{h}^{*}) = \det \begin{pmatrix} a_{1} - a & a_{2} & a_{3} & ... & a_{h} \\ 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 1 & ... & 0 \\ ... & ... & ... & ... & ... \\ 0 & 0 & 0 & 1 \end{pmatrix} \Delta(\beta_{1},...,\beta_{h})$$

$$= r^{2} \Delta(\beta_{1},...,\beta_{h}).$$

$$dg \ \Delta(\beta_1^*, \ldots, \beta_h^*) = 2 \ dg \ r + dg \ \Delta(\beta_1, \ldots, \beta_h) < dg \ (\beta_1, \ldots, \beta_h).$$

This contradicts the minimality of dg $\Delta(\beta_1,\dots,\beta_h)$ and proves the lemma. \Box

[*] B.L. van der Waerden, Algebra I, §43.

