Matematisk seminar
Universitetet i Oslo

No 7 - 1969

FORMAL EMBEDDING THEOREMS OVER FINITE FIELDS

by

A. Holme

In [2], we proved a <u>formal embedding</u> theorem closely related to the classical result that a smooth projective variety over an infinite field k of dimension n can be embedded in $\mathbb{P}^{2n+1}_k$, (see f.inst. [5].)

Namely, let k be an infinite field, and

$\underline{O} = k[[X_1,\ldots,X_N]]/I = k[[\xi_1,\ldots,\xi_N]]$, and let $0 \leq h \leq n = \dim(\underline{O})$. Further, put $\delta = \max\{rk_{k(x)}\hat{\Omega}^1_{\underline{O}/k}(x) \mid x \in PN(\underline{O})\}$. For the definition of $\hat{\Omega}^1_{O/k}$, see [13]. $PN(\underline{O})$ denotes the open subscheme of $Spec(\underline{O})$ obtained by deleting the closed point. Then there are $h + \delta$ linear combinations in $\xi_1,\ldots\xi_N$, $\zeta_1,\ldots,\zeta_{h+\delta}$ such that the inclusion $Q = k[[\zeta_1,\ldots\zeta_{h+\delta}]] \hookrightarrow \underline{O}$ makes $\underline{O}$ to a finite Q-module and induces a morphism $f_h: PN(\underline{O}) \to PN(\underline{Q})$ for which $\dim B(f_h) \leq \max\{-1, n-h-2\}$ and $\dim C(f_h) \leq n-h-1$, where $B(f_h)$ denotes the (closed) set of points in $PN(\underline{O})$ at which f_h is ramified, and $C(f_h)$ is the (closed) set of points in $PN(\underline{Q})$ where f_h is not an isomorphism. (A morphism $f: X \to Y$ is said to be an isomorphism at y provided there exists an open subscheme U of Y containing y such that $f^{-1}(U) \to U$ is an isomorphism.)

In [2] we also proved a refinement of the above: If the non-smooth locus $S(X)$ of $X = PN(\underline{O})$ is of dimension less than n, then δ may be replaced by $\delta' = \max\{n, \delta-1\}$*)

The aim of this note is to prove a weaker result for <u>finite</u> fields k. To be precise, we prove the theorems referred to above with "linear combinations" replaced by "polynomials".

---

*) Chopping up $s(X)$ according to the size of $\hat{\Omega}^1_{O/k}(x)$, one can push this refinement somewhat further, see [3].

The necessity of introducing polynomials (which may not, in general, even be assumed to be homogenous of the same degree) reflects the fact that over a finite field, the classical embedding theorem referred to above fails to be true, see for example [4]. This condition is not necessary, however, for the existence of some embedding $X \hookrightarrow \mathbb{P}^{N-1}_k$, see [3].

So the aim of this note is to prove the following.

Theorem. Let k be a finite field of characteristic p, and let $\underline{O} = k[[X_1,\ldots,X_N]]/I = k[[\xi_1,\ldots,\xi_N]]$. With δ as before, and $0 \leq h \leq n = \dim(\underline{O})$, there exists $\delta+h$ polynomials $\zeta_1,\ldots, \zeta_{\delta+h}$ in $\xi_1,\ldots, \xi_N$ with coefficients from k, such that the inclusion $\underline{Q} = k[[\zeta_1,\ldots, \zeta_{\delta+h}]] \longrightarrow \underline{O}$ makes $\underline{O}$ to a finite $\underline{Q}$-module and such that the canonical morphism $f_h : PN(\underline{O}) \to PN(\underline{Q})$ satisfies

$$\dim(B(f_h)) \leq \max\{-1,\ n-h-2\}$$

and

$$\dim(C(f_h)) \leq n - h - 1 .$$

Proof: In order to apply the techniques of [2], we need the following

Lemma 1. Let $x_1,\ldots x_h$ and $y_1,\ldots, y_t$ be points of $PN(\underline{O})$, and let V_i be a proper $k(x_i)$-subspace of $\hat{\Omega}^1_{\underline{O}/k}(x_i)$ for all $i = 1,\ldots, h$. Then there exists a polynomial ζ in $\xi_1,\ldots, \xi_N$ with coefficients from k, such that $\zeta \in \underline{m} = \max(\underline{O})$,

(1.1) $\zeta \notin \underline{p}(x)$ for all $x \in \{x_1,\ldots, x_h, y_1,\ldots, y_t\}$

and

(1.2) $d\zeta(x_i) \notin V_i$ for all $i = 1,\ldots, h$.

<u>Remark (1.3).</u> (i). Suppose that ζ' satisfies Lemma 1 for the points $x_1,\ldots, x_h, y_1,\ldots, y_{t-1}$, and the subspaces $V_1\ldots,V_h$. Pick a polynomial ξ in $\xi_1,\ldots,\xi_N$, such that $\xi \in \underline{m} = \max(\underline{O})$ but $\xi \notin \underline{p}(y_t)$. (For example, we may take $\xi = \xi_{i_o}$ for some i_o.) Then there exists a finite set J_1 of positive integers such that if $m \notin J_1$, then $\zeta = \zeta' + \xi^{pm}$ satisfies Lemma 1 for the points $x_1,\ldots, x_h, y_1,\ldots, y_t$ and the subspaces $V_1,\ldots, V_h$.

(ii). Assume that ζ' satisfies Lemma 1 for the points $x_1,\ldots, x_{h-1}, y_1,\ldots, y_t$ and the subspaces $V_1,\ldots,V_{h-1}$. Using (i) we may assume that $\zeta' \notin p(x_h)$, if necessary by replacing ζ' by $\zeta' + (\xi_{i_1})^{m_1}$ for suitable i_1 and m_1. Suppose that ζ' does not satisfy Lemma 1. Pick a polynomial ξ in $\xi_1,\ldots,\xi_N$ with coefficients from k such that $\xi \in \underline{m}$ and $d\xi(x_h) \notin V_h$. (Again we can take $\xi = \xi_{i_o}$ for some i_o.) Then there exists a finite set J_2 of positive integers such that if $m \notin J_2$ and $p \nmid m$, then $\zeta = (\zeta')^m + \xi$ satisfies Lemma 1 for the points $x_1,\ldots, x_h, y_1,\ldots, y_t$ and the subspaces $V_1,\ldots, V_h$.

<u>Proof</u>. If $h = 0$, $t = 1$ or if $h = 1$, $t = 0$, the lemma is obvious. We proceed by induction on $h+t$, and it suffices to show (1.3).

To prove (i), let $x \in \{x_1,\ldots, x_h, y_1,\ldots, y_t\}$. If $\xi \in \underline{p}(x)$ then $x \neq y_t$, so $\zeta = \zeta' + \xi^{pm} \notin \underline{p}(x)$ for all m. If on the other hand $\xi \notin \underline{p}(x)$, then there is at most one positive integer m such that $\zeta' + \xi^{pm} \in \underline{p}(x)$: Indeed, suppose that $\zeta' + \xi^{pm_1}$ and $\zeta' + \xi^{pm_2}$ are in $\underline{p}(x)$ for $m_1 > m_2$. Then $\xi^{pm_2}(\xi^{p(m_1-m_2)} - 1) \in \underline{p}(x)$, thus $\xi \in \underline{p}(x)$ since $\xi^{p(m_1-m_2)} - 1$ is a unit in $\underline{O}$, a contradiction. Since $d\zeta = d\zeta'$, we may take J_1 to be the set of all positive integers m such that $\zeta' + \xi^{pm} \in \underline{p}(x)$ for some $x \in \{x_1,\ldots, x_h, y_1,\ldots,y_t\}$.

To prove (ii), we note first that

(1.4) $(m_1(\zeta')^{m_1-1} - m_2(\zeta')^{m_2-1})(x_i) \neq 0$ for all $i = 1,\ldots,h,$

and all positive integers $m_1 > m_2$ such that $p \nmid m_2$.

In fact, suppose that $m_1(\zeta')^{m_1-1} - m_2(\zeta')^{m_2-1} \in \underline{p}(x_i)$ for some i and some integers $m_1 > m_2$ where $p \nmid m_2$. Then

$$(\zeta')^{m_2-1}(m_1(\zeta')^{m_1-m_2} - m_2) \in \underline{p}(x_i) ,$$

and since $\zeta' \notin \underline{p}(x_i)$, we get $m_1(\zeta')^{m_1-m_2} - m_2 \in \underline{p}(x_i)$, contradicting $p \nmid m_2$.

By assumption $d\zeta'(x_i) \in V_h$. Thus for all m we get $d((\zeta')^m + \xi)(x_h) \notin V_h$. Moreover, if $d\xi(x_i) \in V_i$, then $d((\zeta')^m + \xi)(x_i) \notin V_i$ for all m not divisible by p. Finally if for some $i < h$ $d\xi(x_i) \notin V_i$ then $d((\zeta')^m + \xi)(x_i) \in V_i$ for at most one positive integer m not divisible by p. If namely $m_1 > m_2$ are positive integers, not divisible by p, such that $d((\zeta')^{m_j} + \xi)(x_i) \in V_i$ for $j = 1, 2$, then

$$(m_1(\zeta')^{m_1-1} - m_2(\zeta')^{m_2-1})(x_i)(d\zeta'(x_i)) \in V_i$$

which contradicts $d\zeta'(x_i) \notin V_i$, because of (1.4). Now the proof is complete once we show that there is a finite set J_2 of positive integers such that if $m \notin J_2$, then $(\zeta')^m + \xi \notin \underline{p}(x)$ for all $x \in \{x_1, \dots, x_h, y_1, \dots, y_t\}$. This is clear: If $\xi \in \underline{p}(x)$, then $(\zeta')^m + \xi \notin \underline{p}(x)$ for all m, and if $\xi \notin \underline{p}(x)$, then there is at most one integer m such that $(\zeta')^m + \xi \in \underline{p}(x)$. If namely this holds for the integers $m_1 > m_2$, then $(\zeta')^{m_2}((\zeta')^{m_1-m_2} - 1) \in \underline{p}(x)$, and hence $\zeta' \in \underline{p}(x)$, a contradiction.

This completes the proof of Lemma 1.

Next, we prove a modification of Proposition (1.2) in [2]: Let $X_0, \dots, X_p$ be any collection of closed irreducible subsets of $X = PN(\underline{O})$. For all $j \le p$ and all integers d, put

$$X_{j,d} = \{x \in X_j \mid \mathrm{rk}_{k(x)} \hat{\Omega}^1_{\underline{O}/k}(x) \geq d\} .$$

We denote the irreducible components of $X_{j,d}$ by

$$Y_s, \ s \in I(j,d) = \{(j,d,1),\ldots,(j,d,\gamma(j,d))\}.$$

Lemma 2. Let F_s be a closed subset of Y_s , and assume that the elements $\zeta_1,\ldots, \zeta_\lambda$ in the maximal ideal $\underline{m}$ of $\underline{O}$ satisfy $\mathrm{rk}_{k(x)}(\hat{\Omega}^1_{\underline{O}/k}/(d\zeta_1,\ldots, d\zeta_\lambda))(x) = d-\lambda$ for all $x \in Y_s - F_s$, for all j, d and $s \in I(j,d)$. Let m be an integer.

Moreover, let $x_1,\ldots, x_h$, $y_1,\ldots, y_t$ and $V_1,\ldots V_h$ be as in Lemma 1.

Then there is a linear combination in $\xi_1,\ldots, \xi_N$ with coefficients from k, $\zeta_{\lambda+1} = a_1\xi_1 +\ldots+ a_N\xi_N$ such that for all j, $d \geq \lambda+m$ and $s \in I(j,d)$, there exists a closed subset F_s' of Y_s, of codimension $\geq m$ in Y_s , such that $\mathrm{rk}_{k(x)}(\hat{\Omega}^1_{\underline{O}/k}/(d\zeta_1,\ldots, d\zeta_{\lambda+1}))(x) = d-(\lambda+1)$ for all $x \in Y_s-(F_s \cup F_s')$, and such that the conclusion of Lemma 1 holds.

Proof. The proof follows closely that of Proposition (1.2) in [2], to which we shall make frequent references in the following.

First, for $m = 0$, the claim follows by Lemma 1 taking $F_s' = Y_s$ for all s. We proceed by induction on m. So assume $m > 0$ and that Lemma 2 holds for $m-1$.

We get a polynomial u_1 by the induction assumption, such that there exists a closed subset G_s of Y_s of codimension $\geq m-1$ for which (1.2.4) in the proof of Proposition (1.2)) holds for all $s \in I(j,d)$ where $\lambda + (m-1) \leq d$, in particular for $\lambda+m \leq d$. Moreover, in the present case we may also assume that u_1 satisfies the conclusion of Lemma 1 for the points $x_1,\ldots, x_h$, $y_1,\ldots, y_t$ and the subspaces $V_1,\ldots, V_h$.

Define L_s and G_s' as in the proof of Proposition (1.2). G_s' is of codimension $\geq m-1$ in Y_s, and (2.1.4) holds if G_s is replaced by G_s'. Define $G_{s,1},\ldots, G_{s,r(s)}$, $y_{s,1},\ldots,y_{s,r(s)}$, A and $V(x)$ as in the proof of Proposition (1.2).

We now apply the induction assumption to the elements $\zeta_1,\ldots, \zeta_\lambda$ and u_1, the subsets $F_s \subseteq Y_s$ and to the points and subspaces $x_1,\ldots,x_h$, $y_{s,1},\ldots,y_{s,r(s)}$, $y_1,\ldots,y_t$, $V_1,\ldots, V_h$, $V(y_{s,1}),\ldots, V(y_{s,r(s)})$ for all $s \in I(j,d)$ where $(\lambda+1)+(m-1) \leq d$. We get a polynomial u_2 in $\xi_1,\ldots, \xi_N$ such that there exist closed subsets $H_s \subseteq Y_s$, of codimension $\geq m-1$ in Y_s, for which (1.2.7) holds, and such that

$$u_2 \notin \underline{p}(x) \quad \text{for all} \quad x \in A \cup \{x_1,\ldots, x_h, y_1,\ldots, y_t\}$$

(2.1) and

$$du_2(x) \notin V(x) \quad \text{for all} \quad x \in A, \; du_2(x) \notin V_i \text{ for all } i = 1,\ldots,h$$

We may assume that H_s is contained in the (closed) set of points x in Y_s for which $rk_{k(x)}(\hat{\Omega}^1_{\underline{O}/k}/(d\zeta_1,\ldots,d\zeta_\lambda,du_1,du_2))(x) \geq d-\lambda-1$.

Now define $H_{s,1},\ldots, H_{s,q(s)}$, $z_{s,1},\ldots, z_{s,q(s)}$, B and $V(x)$ as in the proof of Proposition (1.2). By remark (1.3), (i), we may assume that $u_2 \notin \underline{p}(x)$ for all $x \in A \cup B \cup \{x_1,\ldots,x_h, y_1,\ldots,y_t\}$. We prove:

(2.2) There exists an integer M such that if $v = (u_1)^M + u_2$, then $v \notin \underline{p}(x)$ for all $x \in \{x_1,\ldots,x_h, y_1,\ldots,y_t\}$, and $dv(x_i) \notin V_i$ for all $i = 1,\ldots,h$ and $dv(x) \notin V(x)$ for all $x \in A \cup B$.

In fact, by (2.1) we have $du_2(x) \notin V(x)$ for all $x \in A$ and $du_2(x_i) \in V_i$ for all $i = 1,\ldots,h$. Since u_1 satisfies (1.2.4) for G_s' and $z_{s,1},\ldots,z_{s,q(s)}$ are not in $G_s' \cup F_s$, $du_1(x) \notin V(x)$ for all $x \in B$. Let $B' \subseteq B$ be the set of points in B such that $du_2(x) \in V(x)$ for all $x \in B'$. By Remark (1.3), (ii), there is a finite set $J(x)$ of positive integers for all $x \in B'$, such that if $m' \notin J(x)$ and m' is not divisible by p, then $d((u_2)^{m'}+u_1)(x_i) \notin V(y)$ for all y in $A \cup (B-B') \cup \{x\}, d((u_2)^{m'}+u_1) \notin V_i$ for all $i = 1,\ldots,h$, and finally $(u_2)^{m'} + u_1 \notin \underline{p}(y)$ for y in $A \cup B \cup \{x_1,\ldots,x_h, y_1,\ldots y_t\}$. Pick M not divisible by p outside $\bigcup_{x \in B'} J(x)$, and (2.2) follows.

Take $v = \zeta_{\lambda+1}$, and define $K_s, K_{s,1},\ldots, K_{s,p(s)}$ as in the proof of Proposition (1.2). To prove that $\zeta_{\lambda+1}$ and $F_s' = K_{s,1} \cup \ldots \cup K_{s,p(s)}$ satisfies the conclusion of Lemma 2, it remains to show that F_s' is of codimension $\geq m$ in Y_s, i.e. that each $K_{s,i}$ is of codimension $\geq m$.

First, $K_s \subseteq F_s \cup H_s$: In fact, assume that $x \in K_s$ but $x \notin F_s$ and $x \notin H_s$. Then

$$\mathrm{rk}_{k(x)}(\hat{\Omega}^1_{\underline{O}/k}/(d\zeta_1,\ldots,d\zeta_{\lambda+1}))(x) \geq d-\lambda$$

$$\mathrm{rk}_{k(x)}(\hat{\Omega}^1_{\underline{O}/k}/(d\zeta_1,\ldots,d\zeta_{\lambda}))(x) = d-\lambda$$

$$\mathrm{rk}_{k(x)}(\hat{\Omega}^1_{\underline{O}/k}/(d\zeta_1,\ldots,d\zeta_{\lambda},du_1,du_2))(x) = d-\lambda-2,$$

i.e., $d\zeta_1,\ldots,d\zeta_\lambda$, du_1, du_2 are linearly independent at x, and $d\zeta_{\lambda+1}(x) = Mu_1(x)^{M-1}du_1(x) + du_2(x) \in (d\zeta_1(x),\ldots,d\zeta_\lambda(x))$, a contradiction. Thus $K_{s,i} \subseteq H_s$ for all s and i.

Now (2.2) shows that $\zeta_1,\ldots,\zeta_{\lambda+1}$ satisfy (1.2.8), and the rest of the proof is identical to that of Proposition (1.2).

Lemma 3. There exist δ polynomials $\zeta_1,\ldots, \zeta_\delta$ in $\zeta_1,\ldots,\zeta_N$ with coefficients from k, such that $\underline{O}$ is finite over the subring $k[[\zeta_1,\ldots,\zeta_\delta]]$ and such that for all $j = 0,\ldots,p$ the closed subsets of X,

$$E(X_j,\delta,i) = \{x \in X_j \mid \mathrm{rk}_{k(x)}(\hat{\Omega}^1_{\underline{O}/k}/(d\zeta_1,\ldots,d\zeta_\delta))(x) \geq i\},$$

are of dimension $\leq \max\{\dim(X_j) - i, -1\}$ for all $i = 1,\ldots,\delta$.

The proof of Lemma 3 is identical to that of Lemma (2.1.3) in [2], using Lemma 2 instead of the combination of Proposition (1.2) and Lemma (1.2.5).

Lemma 4. Assume that $\underline{O} = k[[\xi_1,\ldots,\xi_N]]$ is finite over the subring $Q = k[[\zeta_1,\ldots\zeta_m]]$, where $\zeta_1,\ldots,\zeta_m \in (\xi_1,\ldots,\xi_N)\underline{O}$. Then $\underline{O} = \underline{Q}\,[\xi_1,\ldots,\xi_N]$.

Moreover, let $f : \mathrm{Spec}(\underline{O}) \longrightarrow \mathrm{Spec}(\underline{Q})$ be the induced morphism, and let $p_1,\ldots,p_a$ be points of $\mathrm{PN}(\underline{O})$ such that

(4.1) $k(p_i)$ is a (finite) separable extension of $k(f(p_i))$ for all $i = 1,\ldots, a$.

Moreover, let $x_1,\ldots,x_h$ be points of $\mathrm{PN}(\underline{O})$ and V_i be a proper subspace of $\hat{\Omega}^1_{\underline{O}/k}(x_i)$ for all $i = 1,\ldots,h$.

Then there exists a polynomial ζ in $\xi_1,\ldots,\xi_N$ and $\zeta_1,\ldots,\zeta_m$ which satisfies the following three conditions:

(4.1) $d\zeta(x_i) \notin V_i$ for all $i = 1,\ldots,h$.

(4.2) The image of ζ in $k(p_i)$ generates $k(p_i)$ over $k(f(p_i))$ for all $i = 1,\ldots,a$,

and

(4.3) if $f' : \mathrm{Spec}(\underline{O}) \longrightarrow \mathrm{Spec}(Q[\zeta])$ is the morphism induced by the inclusion, then $f'^{-1}(f'(p_i)) = \{p_i\}$ for all $i = 1,\ldots,a$.

Proof. $\underline{O} = Q[\xi_1,\ldots,\xi_N]$ is obvious.

Let $P_{i,\alpha}$, $\alpha = 1,\ldots, \alpha(i)$ be the finite number of points in $\mathrm{PN}(\underline{O})$ such that $f(P_{i,\alpha}) = f(p_i)$. Let $J \subseteq \{1,\ldots,s\}$ be a set of indicies such that $f(p_i) \neq f(p_j)$ if $i \neq j$ are indicies from J, and such that $\{f(p_i)|i\in J\} = \{f(p_i)|i = 1,\ldots,s\}$.

For each i in J there is a finite, normal extension K_i of $k_i = k(f(p_i))$ such that for each $\alpha = 1,\ldots,a(i)$

there is at least one k_i-embedding $k(P_{i,\alpha}) \longrightarrow K_i$. We denote the finite number of such embeddings by

$$\pi(i,\alpha,\beta) : k(P_{i,\alpha}) \longrightarrow K_i, \ \beta = 1,\dots,\beta(i,\alpha).$$

Let $\theta(i,\alpha,\beta) : \underline{O} \longrightarrow K_i$ be the composition of $\pi(i,\alpha,\beta)$ with the canonical $\sigma(i,\alpha) : \underline{O} \longrightarrow k(P_{i,\alpha})$. For $\alpha \neq \alpha'$, define a k-subspace of $\underline{m}$ by

$$W(i,\alpha,\alpha',\beta,\beta') = \{\lambda \in \underline{m} \mid \theta(i,\alpha,\beta)(\lambda) = \theta(i,\alpha',\beta')(\lambda)\}.$$

For all i, $\alpha \neq \alpha'$, β and β', not all $\xi_1,\dots,\xi_N$ are in $W(i,\alpha,\alpha',\beta,\beta')$. In fact, choose $\lambda \in \underline{p}(P_{i,\alpha})$, $\lambda \notin \underline{p}(P_{i,\alpha'})$. Then $\lambda = F(\xi_1,\dots,\xi_N)$, where $F \in \underline{Q}[X_1,\dots,X_N]$. Thus, if $\theta(F)$ denotes the polynomial over $k(P_{i,\alpha})$ whose coefficients are the images of the corresponding ones of F,

$$\theta(\lambda) = \theta(F)(\theta(\xi_1),\dots,\theta(\xi_N)), \text{ where } \theta = \theta(i,\alpha,\beta),$$

$$\theta'(\lambda) = \theta'(F)(\theta'(\xi_1),\dots,\theta'(\xi_N)), \text{ where } \theta' = \theta(i,\alpha',\beta').$$

Since θ and θ' coincide on $\underline{Q}$, $\theta(F) = \theta'(F)$. But $\theta(\lambda) \neq \theta'(\lambda)$, and therefore $\theta(\xi_{i_o}) \neq \theta'(\xi_{i_o})$ for some i_o, i.e. $\xi_{i_o} \notin W(i,\alpha,\alpha',\beta,\beta')$.

We note that

$$(4.4) \quad \left[\begin{array}{l} \zeta \notin \cup W(i,\alpha,\alpha',\beta,\beta'), \text{ where} \\ \text{the union is taken over all} \\ \alpha \neq \alpha',\ \beta \text{ and } \beta'. \end{array}\right] \Longrightarrow \left[\begin{array}{l} \zeta \text{ satisfies } (2.1.4.4) \\ \text{for all } j \text{ such that} \\ f(p_j) = f(p_i). \end{array}\right]$$

This is shown in the same way as (2.1.4.5) in the proof of Lemma (2.1.4) in [2].

Now put $\underline{q}(x) = \underline{p}(x) \cap k[\zeta_1,\dots,\zeta_m]$ and $L(x) = k[\zeta_1,\dots,\zeta_m]/q(x)$. Let $\{x_1,\dots,x_h, p_1,\dots,p_s\} = \{y_1,\dots,y_r\}$.

If $y_j = p_i$ for some i in J, let $W_{j,1},\dots,W_{j,t(j)}$ be the collection of the subspace $W(i,\alpha,\alpha',\beta,\beta')$ of $\underline{m}$. Denote the two homomorphisms which define $W_{j,t}$ by $\theta_{j,t}$ and

$\theta'_{j,t}$. Put

$$F_j(X_1,\dots,X_N)=\prod_{t=1}^{t(j)}[X_1(\theta_{j,t}(\xi_1)-\theta'_{j,t}(\xi_1))+\dots+X_N(\theta_{j,t}(\xi_N)-\theta'_{j,t}(\xi_N))]$$

Since for all $t = 1,\dots,t(j)$ there is i_o such that $\xi_{i_o} \notin W_{j,t}$, we conclude that $F_j(X_1,\dots,X_N)$ is a non zero polynomial. Furthermore, the images $\overline{\xi}_1,\dots,\overline{\xi}_N$ of $\xi_1,\dots,\xi_N$ in $k(y_j)$ generate $k(y_j)$ over $k(f(y_j))$, so we get a non zero polynomial $G_j(X_1,\dots,X_N) \in k(y_j)[X_1,\dots,X_N]$ such that if $G_j(\alpha_1,\dots,\alpha_N) \neq 0$ for some $\alpha_1,\dots,\alpha_N$ in $k(y_j)$, then $\alpha_1\overline{\xi}_1 +\dots+ \alpha_N\overline{\xi}_N$ generate $k(y_j)$ over $k(f(y_j))$. Now put $H_j = F_jG_j$.

The polynomials H_j are such that whenever $a_1,\dots,a_N$ are elements of $\underline{Q}$ such that the images $\overline{a}_1,\dots,\overline{a}_N$ in $k(f(y_j))$ satisfy $H_j(\overline{a}_1,\dots,\overline{a}_N) \neq 0$, then (4.2) and (4.3) hold for $\zeta = a_1\xi_1 +\dots+ a_N\xi_N$: In fact, by the choice of G_j (4.2) holds, and since $\overline{a}_1\theta_{j,t}(\xi_1)+\dots+\overline{a}_N\theta_{j,t}(\xi_N)\neq \overline{a}_1\theta'_{j,t}(\xi_1)+\dots+\overline{a}_N\theta'_{j,t}(\xi_N)$ for all $t = 1,\dots,t(j)$, we get $\theta_{j,t}(\zeta) \neq \theta'_{j,t}(\zeta)$ for all $t = 1,\dots,t(j)$. Thus (4.3) follows by (4.4).

Now suppose that $y_j = x_i$ for some i. Then there is a non zero polynomial $H_j \in k(y_j)[X_1,\dots,X_N]$ such that if $\alpha_1,\dots\alpha_N$ are elements of $k(y_j)$ for which $H_j(\alpha_1,\dots,\alpha_N) \neq 0$, then $\alpha_1 d\xi_1(y_j) +\dots+ \alpha_N d\xi_N(y_j) \notin V_i$. Put $f_j(X_1,\dots,X_N) = H_j((X_1)^p,\dots,(X_N)^p)$ for all $j = 1,\dots,r$. Since f_j is a non zero polynomial, the set A_j of all α in $L(y_j)$ for which $f_j(\alpha,X_2,\dots,X_N)$ is the zero polynomial is finite.

We show that there exists $a_1 \in k[\zeta_1,\dots,\zeta_m]$ such that for all j the image $\overline{a}_1$ of a_1 in $k(y_j)$ is not in A_j. Indeed, this follows once we show that $k[\zeta_1,\dots,\zeta_m]$ is not covered by a finite number of subsets of the form $g+\underline{p}$, where $g \in k[\zeta_1,\dots,\zeta_m]$ and $\underline{p}$ is a prime, properly contained in the maximal ideal $\underline{m}_o = (\zeta_1,\dots,\zeta_m)k[\zeta_1,\dots,\zeta_m]$. Assume that

$k[\zeta_1,\ldots,\zeta_m] = g_1+\underline{p}_1) \cup \ldots \cup (g_a+\underline{p}_a)$. In particular $\underline{m}_o \subseteq (g_1+\underline{p}_1) \cup \ldots \cup (g_a+\underline{p}_a)$. Deleting some of the sets, we may assume that all $g_h+\underline{p}_h$ have at least one element in common with $\underline{m}_o$, i.e. $g_h+f_h \in \underline{m}_o$ for some $f_h \in \underline{p}_h$. Thus $g_h \in \underline{m}_o$, and $\underline{m}_o = (g_1+\underline{p}_1) \cup \ldots \cup (g_a+\underline{p}_a)$. Choose $g \in \underline{m}_o$ such that $g \in \underline{p}_1 \cup \ldots \cup \underline{p}_a$. Then $g^b - g_h \in \underline{p}_h$ for at most one integer b. Thus choosing b large enough, we get $g^b \notin (g_1+\underline{p}_1) \cup \ldots \cup (g_a+\underline{p}_a)$, a contradiction.

Repeating this, we get $a_1,\ldots,a_N$ in $k[\zeta_1,\ldots,\zeta_m]$ such that $f_j(\bar{a}_1,\ldots,\bar{a}_N) \neq 0$ for all $j = 1,\ldots,r$.

Since $d[(a_1)^p\xi_1 +\ldots+ (a_N)^p\xi_N] = (a_1)^p d\xi_1 +\ldots+ (a_N)^p d\xi_N$, $\zeta = (a_1)^p\xi_1 +\ldots+ (a_N)^p\xi_N$ gives what we want.

This completes the proof of Lemma 4.

Lemma 5. Let $X_o,\ldots,X_p$ be a collection of distinct closed irreducible subsets of $X = PN(\underline{O})$, including the irreducible components of X. Then for all integers $1 \leq h \leq n = \dim(O)$ there are $\delta+h$ polynomials $\zeta_1,\ldots,\zeta_{\delta+h}$ with coefficients from k, such that if

$$f : PN(\underline{O}) \to PN(k[[\zeta_1,\ldots,\zeta_{\delta+h}]])$$

is the morphism induced from the inclusion, then $\dim(f^{-1}(C(f)) \cap X_j) \leq \dim(X_j) - h$ for all $j = 0,\ldots,p$, and the closed subset $E_{i,j}$ of X_j consisting of the points x for which $rk_{k(x)}(\hat{\Omega}^1_{\underline{O}/k}/(d\zeta_1,\ldots,d\zeta_{\delta+1})(x)) \geq \dot{1}$, is of dimension $\subseteq \max\{\dim(X_j)-i-h, -1\}$ for all j and all $i = 1,\ldots,\delta$.

Proof. The proof follows that of Proposition (2.1.8), of [2] using Lemma 3 instead of Lemma (2.1.3), using Lemma 2 instead of Proposition (1.2) and Lemma (1.2.5), and finally using Lemma 4 instead of Lemma (2.1.4).

Lemma 5 now immediately implies the theorem.

References.

[1] Grothendieck, A., "Elementes de Geometric Algebrique", Publ. Math. de L'Institut des Hautes Etudes Scientifiques.

[2] Holme, A., "Formal embedding and projection theorems". To appeare. Preprints available from Department of Mathematics, University of Oslo, Norway.

[3] Holme, A., "On a general embedding theorem in formal geometry". Forthcoming.

[4] Holme, A., "Embedding theorems for projective varieties over finite fields". Forthcoming.

[5] Lluis, E.. "Sur l'immersion des varietes algebriques". Ann. of Math. 62 (1955) 120-127.

[6] Serre, I.P. "Modules projectifs et espaces fibres a fibre vectorielle". Seminaire Dubreil-Puissot Faculté de Sciences de Paris (1957-58).