# Unramified Skolem Problems and Unramified Arithmetic Bertini Theorems in Positive Characteristic

Dedicated to Professor Kazuya Kato

on the occasion of his fiftieth birthday

Akio Tamagawa

Received: November 9, 2002
Revised: June 18, 2003

Abstract. In this paper, we prove unramified, positive-characteristic versions of theorems of Rumely and Moret-Bailly that generalized Skolem's classical problems, and unramified, positive-characteristic versions of arithmetic Bertini theorems. We also give several applications of these results.

2000 Mathematics Subject Classification: Primary 11G35; Secondary 11G25, 14G15, 14G25, 14H25
Keywords and Phrases: Skolem's problem, arithmetic Bertini theorem, positive characteristic.

## §0. Introduction.

Let $f : X \to S$ be a morphism between schemes $X$ and $S$. We refer to an $S$-morphism $\sigma : S' \to X$ from an $S$-scheme $S'$ to $X$ as a quasi-section of $f$, if the structure morphism $\pi : S' \to S$ is surjective. Moreover, for each property $\mathcal{P}$ of morphisms of schemes, we say that $\sigma$ is a $\mathcal{P}$ quasi-section, if $\pi$ is $\mathcal{P}$. In this terminology, Rumely's theorem, which generalized Skolem's classical problems and was augmented by the work of Moret-Bailly, can be stated as follows:

Theorem ([Ru1], [Mo2]). *Let $S$ be a non-empty, affine, open subscheme of either the spectrum of the integer ring of an algebraic number field $K$ or a proper, smooth, geometrically connected curve over a finite field with function field $K$. Let $X$ be a scheme and $f : X \to S$ a morphism of schemes, such that $X$ is irreducible, that $X_K \stackrel{\mathrm{def}}{=} X \times_S \mathrm{Spec}(K)$ is geometrically irreducible over $K$, and that $f$ is of finite type and surjective. Then, $f$ admits a finite quasi-section.*

On the other hand, the following is a well-known fact in algebraic geometry:

Theorem ([EGA4], Corollaire (17.16.3)(ii)). *Let $f : X \to S$ be a morphism of schemes (with $S$ arbitrary) which is smooth and surjective. Then, $f$ admits an étale quasi-section.*

In the present paper, we prove, among other things, the following theorem in positive characteristic, which is a sort of mixture of the above two theorems:

Theorem (0.1). (See (3.1).) *Let $S$ be a non-empty, affine, open subscheme of a proper, smooth, geometrically connected curve over a finite field with function field $K$. Let $X$ be a scheme and $f : X \to S$ a morphism of schemes, such that $X_K$ is geometrically irreducible over $K$, and that $f$ is smooth and surjective. Then, $f$ admits a finite étale quasi-section.*

Here, we would like to note that the validity of this theorem is typical of positive characteristic. For example, it is easy to observe that $\mathbf{P}^1_{\mathbb{Z}} - \{0, 1, \infty\} \to \mathrm{Spec}(\mathbb{Z})$ does not admit a finite étale quasi-section.

In the work of Rumely and Moret-Bailly, they also proved certain refined versions of the above theorem, which involve local conditions at a finite number of primes. To state these refined versions, let $S$ and $K$ be as in the theorem of Rumely and Moret-Bailly. Thus, $K$ is either an algebraic number field or an algebraic function field of one variable over a finite field. We denote by $\Sigma_K$ the set of primes of $K$, and we denote by $\Sigma_S$ the set of closed points of $S$, which may be regarded as a subset of $\Sigma_K$. Moreover, let $\Sigma$ be a (an automatically finite) subset of $\Sigma_K - \Sigma_S$, which is not the whole of $\Sigma_K - \Sigma_S$. (This last assumption is referred to as incompleteness hypothesis.) For each $v \in \Sigma$, let $K_v$ denote the $v$-adic completion of $K$, and assume that a normal algebraic extension $L_v/K_v$ (possibly of infinite degree) is given. Let $X$ and $f : X \to S$ be as in the theorem of Rumely and Moret-Bailly, and assume that, for each $v \in \Sigma$, a non-empty, $v$-adically open, $\mathrm{Gal}(K_v^{\mathrm{sep}}/K_v)$-stable subset $\Omega_v$ of $X(L_v)$ is given.

Theorem ([Ru1], [Mo3]). *Notations and assumptions being as above, assume, moreover, either $L_v = \overline{K}_v$ (*[Ru1]*) or $L_v$ is Galois over $K_v$ (*[Mo3]*). Then, there exists a finite quasi-section $S' \to X$ of $f : X \to S$, such that, for each $v \in \Sigma$, $S'_{L_v} \overset{\mathrm{def}}{=} S' \times_S \mathrm{Spec}(L_v)$ is a direct sum of (a finite number of) copies of $\mathrm{Spec}(L_v)$, and the image of $S'_{L_v}$ in $X(L_v) = X_{L_v}(L_v)$ is contained in $\Omega_v$.*

*Remark* (0.2). In fact, Moret-Bailly's version implies Rumely's version. See [Mo3], Remarque 1.6 for this. Indeed, Moret-Bailly's version implies more, namely, that it suffices to assume that $L_v$ is a normal algebraic extension of $K_v$ such that $L_v \cap K_v^{\mathrm{sep}}$ is ($v$-adically) dense in $L_v$. (See the proof of [Mo3], Lemme 1.6.1, case (b).)

*Remark* (0.3). Here is a brief summary of the history (in the modern terminology) of Skolem's problems and its generalizations. Skolem [S] proved the existence of finite quasi-sections for rational varieties. Cantor and Roquette

[CR] proved it for unirational varieties. (A similar result was slightly later obtained in [EG].) Then, Rumely [Ru1] gave the first proof for arbitrary varieties (in the case of rings of algebraic integers). (See also [Ro].) Moret-Bailly (and Szpiro) [Mo2,3] gave an alternative proof of Rumely's result in stronger forms. (Another alternative proof was later given in [GPR].) Moret-Bailly also proved the existence of finite quasi-sections for algebraic stacks ([Mo5]).

We also prove the following refined version in the unramified setting. Unfortunately, in the unramified setting, our version for the present is weaker than Moret-Bailly's version (though it is stronger than Rumely's version). To state this, let $S$ and $K$ be as in (0.1). Thus, $K$ is an algebraic function field of one variable over a finite field. We denote by $\Sigma_K$ the set of primes of $K$, and we denote by $\Sigma_S$ the set of closed points of $S$. Moreover, let $\Sigma$ be a subset of $\Sigma_K - \Sigma_S$, which is not the whole of $\Sigma_K - \Sigma_S$. For each $v \in \Sigma$, let $K_v$ denote the $v$-adic completion of $K$, and assume that a normal algebraic extension $L_v/K_v$ is given. Let $f : X \to S$ be as in (0.1), and assume that, for each $v \in \Sigma$, a non-empty, $v$-adically open, $\mathrm{Gal}(K_v^{\mathrm{sep}}/K_v)$-stable subset $\Omega_v$ of $X(L_v)$ is given.

Theorem (0.4). (See (3.1).) *Notations and assumptions being as above, assume, moreover, that, for each $v \in \Sigma$, $L_v \cap K_v^{\mathrm{sep}}$ is dense in $L_v$, and that the residue field of $L_v$ is infinite. Then, there exists a finite étale quasi-section $S' \to X$ of $f : X \to S$, such that, for each $v \in \Sigma$, $S'_{L_v}$ is a direct sum of copies of* $\mathrm{Spec}(L_v)$*, and the image of $S'_{L_v}$ in $X(L_v) = X_{L_v}(L_v)$ is contained in $\Omega_v$.*

Roughly speaking, the proof of (0.4) goes as follows. Via some reduction steps, we may assume that $X$ is quasi-projective over $S$. Then, by means of a version of arithmetic Bertini theorem, we take hyperplane sections successively to obtain a suitable quasi-section finally. More precisely, we use the following unramified version of arithmetic Bertini theorem, which is another main result of the present paper:

Theorem (0.5). (See (3.2).) *Let $S$, $\Sigma$, $L_v$ be as in* (0.4). *Moreover, let $Y_1, \dots, Y_r$ be irreducible, reduced, closed subschemes of $\mathbf{P}^n_S$. For each $v \in \Sigma$, let $\check{\Omega}_v$ be a non-empty, $v$-adically open,* $\mathrm{Gal}(K_v^{\mathrm{sep}}/K_v)$*-stable subset of $\check{\mathbf{P}}^n_S(L_v)$. Then, there exist a connected, finite, étale covering $S' \to S$ such that, for each $v \in \Sigma$, $S'_{L_v}$ is a direct sum of copies of* $\mathrm{Spec}(L_v)$*, and a hyperplane $H \subset \mathbf{P}^n_{S'}$, such that the following hold:* (a) *for each $i = 1, \dots, r$, each geometric point $\overline{s}$ of $S'$ and each irreducible component $P$ of $Y_{i,\overline{s}}$, we have $P \cap H_{\overline{s}} \subsetneq P$;* (b) *for each $i = 1, \dots, r$, the scheme-theoretic intersection $(Y_i^{\mathrm{sm}})_{S'} \cap H$ (in $\mathbf{P}^n_{S'}$) is smooth over $S'$ (Here, $Y_i^{\mathrm{sm}}$ denotes the set of points of $Y_i$ at which $Y_i \to S$ is smooth. This is an open subset of $Y_i$, and we regard it as an open subscheme of $Y_i$.);* (c) *for each $i = 1, \dots, r$ and each irreducible component $P$ of $Y_{i,\overline{K}}$ (where we identify the algebraic closure of the function field of $S'$ with that of $S$) with* $\dim(P) \geq 2$*, $P \cap H_{\overline{K}}$ is irreducible; and* (d) *for each $v \in \Sigma$, the image of $S'_{L_v}$ in $\check{\mathbf{P}}^n(L_v)$ by the base change to $L_v$ of the classifying morphism $[H] : S' \to \check{\mathbf{P}}^n_S$ over $S$ is contained in $\check{\Omega}_v$.*

There remain, however, the following non-trivial problems. Firstly, a Bertini-type theorem is, after all, to find a (quasi-)section in an open subset of the (dual) projective space, which requires a Rumely-type theorem. Secondly, in the (most essential) case where $X$ is of relative dimension 1 over $S$, the boundary of $X$ (i.e., the closure of $X$ minus $X$ in the projective space) may admit vertical irreducible components (of dimension 1). Since a hyperplane intersects non-trivially with every positive-dimensional irreducible component, the hyperplane section does not yield a finite quasi-section of $X$ (but merely of the closure of $X$).

To overcome the first problem, we have to prove a Rumely-type theorem for projective $n$-spaces directly. It is not difficult to reduce this problem to the case $n = 1$. First, we shall explain the proof of this last case assuming $\Sigma = \emptyset$. So, we have to construct a finite, étale quasi-section in an open subscheme $X$ of $\mathbf{P}^1_S$. Moreover, for simplicity, we assume that $X$ is a complement of the zero locus $W$ of $w(T) \in R[T]$ in $\mathbf{A}^1_S = \mathrm{Spec}(R[T])$, where $R \stackrel{\mathrm{def}}{=} \Gamma(S, \mathcal{O}_S)$. (Since $X$ is assumed to be surjectively mapped onto $S$, $w(T)$ is primitive.) The original theorem of Rumely and Moret-Bailly, together with some arguments from Moret-Bailly's proof, implies that there exists a monic polynomial $g(T) \in R[T]$ of positive degree, such that the zero locus of $g$ in $\mathbf{A}^1_S$ is contained in $X$. Now, if the zero locus of $g$ is étale over $S$, we are done. In general, we shall consider the following polynomial: $F(T) = g(T)^{pm} + w(T)^p T$ for sufficiently large $m > 0$. Then, $F(T)$ is a monic polynomial in $R[T]$, and its zero locus $S'$ gives a closed subscheme of $\mathbf{A}^1_S$ which is finite, flat over $S$. Since $g(T)$ (resp. $w(T)$) is a unit (resp. zero) on $W$, $F(T)$ is a unit on $W$, or, equivalently, $S'$ is contained in $X$. Moreover, since $F'(T) = w(T)^p$, the zero locus of $F'$ coincides with $W$, hence is disjoint from the zero locus $S'$ of $F$. This means that $S'$ is étale over $S$, as desired. (This argument is inspired by an argument of Gabber in [G].) Next, assume $\Sigma \neq \emptyset$. Then, to find a finite, étale quasi-section with prescribed local conditions at $\Sigma$, we need to investigate local behaviors of roots of polynomials like the above $F$. Since it is easy to reduce the problem to the case where the above $w$ is $v$-adically close to 1 (by means of a coordinate change), we see that it is essential to consider local behaviors of roots of polynomials in the form of

$$a_1 T + \sum_{i=0}^{m} a_{ip} T^{ip}$$

with $a_1 \neq 0$. (In the present paper, we refer to a polynomial in this form as a superseparable polynomial.) As a result of this investigation, we see that we can take the above $F$ so that, for each $v \in \Sigma$, every root of $F$ is contained in the given $\Omega_v$. Also, in this investigation, the (hopefully temporary) condition that the residue field of $L_v$ is infinite for each $v \in \Sigma$ arises.

To overcome the second problem, we take a finite, flat quasi-section with local conditions by means of Moret-Bailly's version of Rumely's theorem. Then, by using this (horizontal) divisor, we construct a (new) quasi-projective embedding of $X$. Now, in this projective space, we can construct a finite, étale quasi-section of $X$ as a hyperplane section.

Here is one more ingredient of our proof that we have not yet mentioned:

Theorem (0.6). (See (2.1) and (2.2).) *Let $S$ and $\Sigma$ be as in* (0.4)*. Assume, moreover, that, for each $v \in \Sigma$, a finite Galois extension $L_v/K_v$ is given. Then, there exists a connected, finite, étale, Galois covering $S' \to S$, such that, for each $v \in \Sigma$, $S' \times_S \mathrm{Spec}(K_v)$ is isomorphic to a disjoint sum of copies of* $\mathrm{Spec}(L_v)$ *over $K_v$.*

We use this result in some reduction steps. See §3 for more details.

The author's original motivation to prove results like (0.1) arises from the study of coverings of curves in positive characteristic. For example, in the forthcoming paper, we shall prove the following result as an application of (0.1):

Theorem (0.7). *For each pair of affine, smooth, connected curves $X, Y$ over $\overline{\mathbb{F}}_p$, there exists an affine, smooth, connected curve $Z$ over $\overline{\mathbb{F}}_p$ that admits finite, étale morphisms $Z \to X$ and $Z \to Y$ over $\overline{\mathbb{F}}_p$.*

*In other words, there exists an $\overline{\mathbb{F}}_p$-scheme $H$, such that, for every affine, smooth, connected curve $X$ over $\overline{\mathbb{F}}_p$, the 'pro-finite-étale universal covering' $\tilde{X}$ of $X$ is isomorphic to $H$ over $\overline{\mathbb{F}}_p$.*

For other applications of the above main results, see §4.

Finally, we shall explain the content of each § briefly. In §1, we investigate the above-mentioned class of polynomials in positive characteristic, namely, superseparable polynomials. The aim here is to control how a superseparable polynomial over a complete discrete valuation field in positive characteristic decomposes. Here, (1.18) is a final result, on which the arguments in §2 and §3 are based. In §2, we prove the existence of unramified extensions with prescribed local extensions, such as (0.6) above. The main results are (2.1) and (2.2). In the former, we treat an arbitrary Dedekind domain in positive characteristic, while, in the latter, we only treat a curve over a field of positive characteristic but we can impose (weaker) conditions on all the primes of the function field. The proofs of both results rely on the results of §1. In §3, we prove the main results of the present paper, namely, an unramified version of the theorem of Rumely and Moret-Bailly in positive characteristic (3.1), and an unramified version of the arithmetic Bertini theorem in positive characteristic (3.2). In §4, we give several remarks and applications of the main results. Some of these applications are essentially new features that only arise after our unramified versions.

*Acknowledgment.* Professor Kazuya Kato was the advisor of the author's master's thesis [T] at the University of Tokyo (May 1990 – March 1992). The author would like to express his sincerest gratitude to Professor Kato for having encouraged and stimulated the author constantly since then. Also, the author would like to thank Bjorn Poonen and Pierre Dèbes (resp. Osamu Fujino and Hiromichi Takagi) very much for various helpful information concerning the work of Rumely and Moret-Bailly (resp. [CFHR]). Finally, the author would like to thank one of the referees for a simplification of Step 2 of §3. (See (3.8).)

## §1. Superseparable polynomials.

Throughout this §, we let $K$ denote a field.

Definition. Let $f(T)$ be a polynomial in $K[T]$. We say that $f$ is superseparable, if the derivative $f'(T)$ of $f(T)$ falls in $K[T]^\times = K^\times$.

Lemma (1.1). *For each $f(T) \in K[T]$, the following* (a)–(c) *are equivalent.*
(a) *$f$ is superseparable.*
(b) *The $K$-morphism $\mathbf{A}^1_K \to \mathbf{A}^1_K$ associated to $f$ is étale everywhere.*
(c) *$f$ is in the form of*

$$f(T) = \begin{cases} a_1 T + a_0, & \textit{if } \mathrm{char}(K) = 0, \\ a_1 T + \displaystyle\sum_{i=0}^{m} a_{ip} T^{ip}, & \textit{if } \mathrm{char}(K) = p > 0, \end{cases}$$

*where $a_j \in K$ and $a_1 \neq 0$.*

*Proof.* Immediate. □

*Remark* (1.2). $f$ is separable (i.e., $(f, f') = 1$) if and only if the associated $K$-morphism from $\mathbf{A}^1_{\mathrm{upper},K} \stackrel{\mathrm{def}}{=} \mathbf{A}^1_K$ to $\mathbf{A}^1_{\mathrm{lower},K} \stackrel{\mathrm{def}}{=} \mathbf{A}^1_K$ is étale at $0 \in \mathbf{A}^1_{\mathrm{lower},K}$.

From now on, let $p$ denote a prime number, and we assume that $K$ is of characteristic $p$ and is equipped with a complete discrete valuation $v$, normalized as $v(K^\times) = \mathbb{Z}$. We denote by $R$, $\mathfrak{m}$, $k$, and $t$ the valuation ring of $v$, the maximal ideal of $R$, the residue field $R/\mathfrak{m}$, and a prime element of $R$, respectively. We fix an algebraic closure $\overline{K}$ of $K$, and we denote again by $v$ the unique valuation $\overline{K} \to \mathbb{Q} \cup \{\infty\}$ that extends $v$. Moreover, for each subfield $L$ of $\overline{K}$ containing $K$, we denote by $R_L$, $\mathfrak{m}_L$, and $k_L$ the integral closure of $R$ in $L$, the maximal ideal of $R_L$, and the residue field $R_L/\mathfrak{m}_L$, respectively.

Now, consider a superseparable polynomial

$$f(T) = aT + h(T^p), \tag{1.3}$$

where $a \in K^\times$, $h \in K[T]$, and we put $m \stackrel{\mathrm{def}}{=} \deg(h)$. (We put $m = 0$ if $h = 0$.) The aim of this § is to describe how $f$ decomposes and what is the Galois group associated with $f$.

Definition. (i) We say that a polynomial $g$ in $\overline{K}[T]$ is integral, if all the coefficients of $g$ belong to $R_{\overline{K}}$.

(ii) Let $g$ be a non-zero polynomial in $\overline{K}[T]$. We denote by $\mathrm{roots}(g)$ the set of roots of $g$ in $\overline{K}$. This is a finite subset of $\overline{K}$.
(iii) Let $g$ be a separable polynomial in $K[T]$. Then, we denote by $K_g$ the minimal splitting field of $g$ in $\overline{K}$, i.e., the subfield of $\overline{K}$ generated by $\mathrm{roots}(g)$ over $K$. This is a Galois extension of $K$, and we put $G_g \stackrel{\mathrm{def}}{=} \mathrm{Gal}(K_g/K)$.
(iii) Let $g$ be a polynomial in $\overline{K}[T]$, and $\alpha$ an element of $\mathrm{roots}(g)$. Then, we put

$$\mu(g,\alpha) \stackrel{\mathrm{def}}{=} \max\{v(\alpha'-\alpha) \mid \alpha' \in \mathrm{roots}(g) - \{\alpha\}\}.$$

Here, we put $\max\emptyset \stackrel{\mathrm{def}}{=} -\infty$.

The following is a version of Krasner's lemma.

Lemma (1.4). *Let $f$ be a monic, integral, superseparable polynomial in $K[T]$ as in* (1.3).
(i) *For each $\alpha \in \mathrm{roots}(f)$, we have $\mu(f,\alpha) \leq \frac{1}{p-1}v(a)$.*
(ii) *Let $\epsilon(T) = \displaystyle\sum_{j=0}^{mp}\epsilon_j T^j$ be a polynomial in $K[T]$ (with degree $\leq mp$), such that $v(\epsilon_j) > \frac{p}{p-1}v(a)$ holds for all $j = 0,\dots,mp$. We put $f_1 \stackrel{\mathrm{def}}{=} f+\epsilon$. Then, $f_1$ is separable and we have $K_{f_1} = K_f$.*

*Proof.* (i) Observe the Newton polygon of $f(T+\alpha)$ (which is also a monic, integral, superseparable polynomial).
(ii) For each $\alpha \in \mathrm{roots}(f)$, put $g_\alpha(T) = f_1(T+\alpha)$, which is an integral polynomial in $\overline{K}[T]$. Then, we have $\mathrm{roots}(g_\alpha) = \{\beta-\alpha \mid \beta \in \mathrm{roots}(f_1)\}$. We have $g_\alpha(0) = f_1(\alpha) = \epsilon(\alpha)$ and $g'_\alpha(0) = f'_1(\alpha) = a+\epsilon'(\alpha)$, hence $v(g_\alpha(0)) > \frac{p}{p-1}v(a)$ and $v(g'_\alpha(0)) = v(a)$. Thus, by observing the Newton polygon of $g_\alpha$, we see that there exists a unique $\beta = \beta_\alpha \in \mathrm{roots}(f_1)$, such that $v(\beta-\alpha) > \frac{1}{p-1}v(a)$. The map $\mathrm{roots}(f) \to \mathrm{roots}(f_1)$, $\alpha \mapsto \beta_\alpha$ is clearly $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-equivariant. Moreover, this map is injective, since, for each pair $\alpha,\alpha' \in \mathrm{roots}(f)$ with $\alpha \neq \alpha'$, we have $v(\alpha-\alpha') \leq \frac{1}{p-1}v(a)$ by (i). As $\sharp(\mathrm{roots}(f)) = mp \geq \sharp(\mathrm{roots}(f_1))$, this map must be a bijection. Thus, we obtain a $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-equivariant bijection $\mathrm{roots}(f) \xrightarrow{\sim} \mathrm{roots}(f_1)$, so that $f_1$ is separable and $K_f = K_{f_1}$, as desired. □

Definition. Let $m$ and $n$ be natural numbers.
(i) We put $I_n \stackrel{\mathrm{def}}{=} \{1,\dots,n\}$.
(ii) We denote by $S_n$ the symmetric group on the finite set $I_n$. Moreover, identifying $I_n$ with $\mathbb{Z}/n\mathbb{Z}$ naturally, we define

$$B_n \stackrel{\mathrm{def}}{=} \{\sigma \in S_n \mid \exists a \in (\mathbb{Z}/n\mathbb{Z})^\times,\ \exists b \in \mathbb{Z}/n\mathbb{Z},\ \forall i \in \mathbb{Z}/n\mathbb{Z},\ \sigma(i) = ai+b\}$$

and

$$C_n \stackrel{\mathrm{def}}{=} \{\sigma \in S_n \mid \exists b \in \mathbb{Z}/n\mathbb{Z},\ \forall i \in \mathbb{Z}/n\mathbb{Z},\ \sigma(i) = i+b\}.$$

Thus, $S_n \supset B_n \rhd C_n$, and $B_n$ (resp. $C_n$) can be naturally identified with the semi-direct product $(\mathbb{Z}/n\mathbb{Z})^\times \ltimes (\mathbb{Z}/n\mathbb{Z})$ (resp. the cyclic group $\mathbb{Z}/n\mathbb{Z}$).

(ii) We denote by $S_{m\times n}$ the symmetric group on the finite set $I_m \times I_n$. (Thus, $S_{m\times n} \simeq S_{mn}$.) Let $\mathrm{pr}_1$ denote the first projection $I_m \times I_n \to I_m$. We define

$$S_{m\ltimes n} \stackrel{\text{def}}{=} \{\sigma \in S_{m\times n} \mid \exists \overline{\sigma} \in S_m,\ \forall (i,j) \in I_m \times I_n,\ \mathrm{pr}_1(\sigma((i,j))) = \overline{\sigma}(i)\}.$$

Thus, $S_{m\ltimes n}$ can be naturally identified with the semi-direct product $S_m \ltimes (S_n)^{I_m}$. Here, for a group $G$ and a positive integer $r$, $G^{I_r}$ denotes the direct product $\underbrace{G \times \cdots \times G}_{r \text{ times}}$. We adopt this slightly unusual notation to save the notation $G^r$ for $\{g^r \mid g \in G\}$ (for a commutative group $G$).

The following proposition is a mere exercise in Galois theory over local fields in positive characteristic, but it is the starting point of our proofs of main results in later §§.

Proposition (1.5). *Let $f$ be a superseparable polynomial as in* (1.3) *with $m \geq 1$. Moreover, we assume that* (a) *$h$ is separable, and* (b) *we have $\delta(a,h,\alpha) > \mu(h,\alpha)$ for all $\alpha \in \mathrm{roots}(h)$, where*

$$\delta(a,h,\alpha) \stackrel{\text{def}}{=} \min\left( v(a) - v(h'(\alpha)) + \frac{1}{p}v(\alpha), \frac{p}{p-1}(v(a) - v(h'(\alpha)))\right).$$

*Then, by choosing a suitable bijection between* $\mathrm{roots}(f)$ *and $I_m \times I_p$:*
(i) *The Galois group $G_f$ can be identified with a subgroup of $S_{m\ltimes p}$ ($\subset S_{m\times p}$).*
(ii) $G_f \cap (S_p)^{I_m} \subset (B_p)^{I_m}$.
(iii) *The group filtration*

$$\{1\} \subset G_f \cap (C_p)^{I_m} \subset G_f \cap (S_p)^{I_m} \subset G_f$$

*corresponds via Galois theory to the field filtration*

$$K_f \supset M_f \supset K_h \supset K,$$

*where $M_f$ is the subfield of $\overline{K}$ generated by $\{(-a/h'(\alpha))^{\frac{1}{p-1}} \mid \alpha \in \mathrm{roots}(h)\}$ over $K_h$.*

*Proof.* (i) First, we shall prove the following:

*Claim* (1.6). (i) For each $\alpha \in \mathrm{roots}(h)$, put

$$F_\alpha \stackrel{\text{def}}{=} \{\beta \in \mathrm{roots}(f) \mid v(\beta^p - \alpha) \geq \delta(a,h,\alpha)\}.$$

Then, $F_\alpha$ has cardinality $p$ for each $\alpha \in \mathrm{roots}(h)$.
(ii) For each $\beta \in \mathrm{roots}(f)$, there exists a unique $\alpha = \alpha_\beta \in \mathrm{roots}(h)$, such that $F_\alpha \ni \beta$.

*Proof.* (i) Observe the Newton polygon of $f(T+\alpha^{1/p}) = h(T^p+\alpha)+aT+a\alpha^{1/p}$ by using $\delta(a,h,\alpha) > \mu(h,\alpha)$. Then, we see that $F_\alpha$ has cardinality $p$, as

desired (and that the subset $\{\beta \in \mathrm{roots}(f) \mid v(\beta^p - \alpha) = \delta(a,h,\alpha)\}$ of $F_\alpha$ has cardinality $\geq p-1$).
(ii) First, we shall prove the uniqueness. Suppose that there exist $\alpha_1, \alpha_2 \in \mathrm{roots}(h)$, $\alpha_1 \neq \alpha_2$, such that $v(\beta^p - \alpha_i) \geq \delta(a,h,\alpha_i)$ holds for $i = 1, 2$. Then, we have

$$v(\alpha_1 - \alpha_2) = v((\beta^p - \alpha_2) - (\beta^p - \alpha_1)) \geq \min(\delta(a,h,\alpha_1), \delta(a,h,\alpha_2)),$$

while, by assumption, we have

$$\min(\delta(a,h,\alpha_1), \delta(a,h,\alpha_2)) > \min(\mu(h,\alpha_1), \mu(h,\alpha_2)) \geq v(\alpha_1 - \alpha_2).$$

This is absurd.

By this uniqueness and (i), we have

$$\sharp(\bigcup_{\alpha \in \mathrm{roots}(h)} F_\alpha) = \sum_{\alpha \in \mathrm{roots}(h)} \sharp(F_\alpha) = mp = \sharp(\mathrm{roots}(f)),$$

hence $\bigcup_{\alpha \in \mathrm{roots}(h)} F_\alpha = \mathrm{roots}(f)$. This implies the existence of $\alpha = \alpha_\beta$ for each $\beta \in \mathrm{roots}(f)$. $\square$

By (1.6)(ii), we obtain a well-defined map $\pi : \mathrm{roots}(f) \to \mathrm{roots}(h)$, $\beta \mapsto \alpha_\beta$. By (1.6)(i), $\pi$ is surjective and each fiber of $\pi$ has cardinality $p$. Since $\pi$ is $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-equivariant by definition, this implies (1.5)(i). (We may choose any bijections $\mathrm{roots}(h) \simeq I_m$ and $F_\alpha \simeq I_p$ ($\alpha \in \mathrm{roots}(h)$).)

Note that this construction already shows that the field extension of $K$ corresponding to the subgroup $G_f \cap (S_p)^{I_m} = \mathrm{Ker}(G_f \to S_m)$ coincides with $K_h$.
(ii) We shall start with the following. From now on, for each $x, x' \in \overline{K}^\times$, we write $x \sim x'$ if $x'/x \in 1 + \mathfrak{m}_{\overline{K}}$, or, equivalently, $v(x'-x) > v(x)$.

*Claim* (1.7). (i) Let $\alpha, \alpha' \in \mathrm{roots}(h)$ and $\beta \in F_\alpha$. Assume $\alpha \neq \alpha'$. Then, we have $\beta^p - \alpha' \sim \alpha - \alpha'$. In particular, we have $v(\beta^p - \alpha') = v(\alpha - \alpha')$.
(ii) Let $\alpha, \alpha' \in \mathrm{roots}(h)$, $\beta \in F_\alpha$, and $\beta' \in F_{\alpha'}$. Assume $\beta \neq \beta'$. Then, we have

$$v((\beta')^p - \beta^p) = \begin{cases} v(\alpha' - \alpha) \ (\leq \mu(h,\alpha)), & \text{if } \alpha \neq \alpha', \\ \frac{p}{p-1}(v(a) - v(h'(\alpha))) \ (\geq \delta(a,h,\alpha)), & \text{if } \alpha = \alpha'. \end{cases}$$

*Proof.* (i) $v((\beta^p - \alpha') - (\alpha - \alpha')) = v(\beta^p - \alpha) \geq \delta(a,h,\alpha) > \mu(h,\alpha) \geq v(\alpha - \alpha')$.
(ii) If $\alpha \neq \alpha'$, we have $v((\beta')^p - \beta^p) = v(((\beta')^p - \alpha') - (\beta^p - \alpha')) = v(\beta^p - \alpha')$, since $v((\beta')^p - \alpha') > v(\beta^p - \alpha')$ by the definition of $F_{\alpha'}$. (Recall that $F_\alpha \cap F_{\alpha'} = \emptyset$ holds by (1.6)(ii).) Thus, in this case, $v((\beta')^p - \beta^p) = v(\alpha' - \alpha)$ holds by (i).

By using this and (i), observe the Newton polygon of $f(T+\beta) = h(T^p + \beta^p) + aT + a\beta$ and compare it with the Newton polygon of $f(T + \alpha^{1/p})$. Then, we can read off the value $v(\beta' - \beta)$ for $\alpha = \alpha'$. $\square$

For each $\alpha \in \operatorname{roots}(h)$, the subgroup $\operatorname{Gal}(K_f/K(\alpha))$ of $G_f$ acts on $F_\alpha$. In order to prove (1.5)(ii), it suffices to prove that the image $\operatorname{Gal}(K(\alpha)(F_\alpha)/K(\alpha))$ of this action is contained in $B_p$ ($\subset S_p$), after choosing a suitable bijection $F_\alpha \simeq I_p$.

*Claim* (1.8). Let $\alpha \in \operatorname{roots}(h)$ and $\beta \in F_\alpha$.
(i) We have $K(\alpha)(F_\alpha) = K(\alpha)(\beta)((-a/h'(\alpha))^{1/(p-1)})$.
(ii) Let $\beta' \in F_\alpha$, $\beta' \neq \beta$. Then, we have $(\beta' - \beta)^{p-1} \sim -a/h'(\alpha)$. More precisely, we have

$$\{(\beta' - \beta) \bmod \sim \mid \beta' \in F_\alpha,\, \beta' \neq \beta\} = \{\zeta(-a/h'(\alpha))^{\frac{1}{p-1}} \bmod \sim \mid \zeta \in \mathbb{F}_p^\times\}.$$

*Proof.* As in the proof of (1.7)(ii), observe the Newton polygon of $f(T+\beta) = h(T^p + \beta^p) + aT + a\beta$. Then, observing the coefficients of $T^0, T^1, \dots, T^p$, we see that $K(\alpha)(F_\alpha) = K(\alpha)(\beta)((-a/h'(\beta^p))^{1/(p-1)})$. Now, by (1.7)(i), we obtain $h'(\beta^p) \sim h'(\alpha)$, which implies $K(\alpha)(\beta)((-a/h'(\beta^p))^{1/(p-1)}) = K(\alpha)(\beta)((-a/h'(\alpha))^{1/(p-1)})$. These complete the proof of (i), and also show (ii). $\square$

Lemma (1.9). *Let $G$ be a subgroup of $S_p$, and, for each $i = 1, \dots, p$, we denote by $G_i$ the stabilizer of $i$ in $G$. Moreover, let $\phi : G \to \mathbb{F}_p^\times$ be a homomorphism, such that, for each $i = 1, \dots, p$, there exists an identification $\sigma_i : I_p - \{i\} \xrightarrow{\sim} \mathbb{F}_p^\times$, such that $\sigma_i g_i \sigma_i^{-1}$ coincides with the $\phi(g_i)$-multiplication map on $\mathbb{F}_p^\times$ for each $g_i \in G_i$. Then, we have $G \subset B_p$ via a suitable identification $I_p \simeq \mathbb{F}_p$.*

*Proof.* Put $N \stackrel{\text{def}}{=} \operatorname{Ker}(\phi)$. Then, $N$ is a normal subgroup of $G$. By using the identity $\phi(g_i)\cdot = \sigma_i g_i \sigma_i^{-1}$, we see that $N \cap G_i = \{1\}$ for all $i = 1, \dots, p$. Namely, the action of $N$ on $I_p$ is free. Since $\sharp(I_p) = p$ is a prime number, this implies that either $N = \{1\}$ or $N = C_p$ (via some identification $I_p \simeq \mathbb{F}_p$). In the latter case, we obtain $G \subset B_p$, since the normalizer of $C_p$ in $S_p$ coincides with $B_p$. So, assume $N = \{1\}$. Then, $G = G/N$ is abelian with $\sharp(G) \mid p - 1$.

Let $X$ be any $G$-orbit of $I_p$. Suppose that $X$ is not a one-point set. Then, there exist $i, j \in X$, $i \neq j$. Since $G$ is abelian, this implies $G_i = G_j$. On the other hand, by the identity $\phi(g_i)\cdot = \sigma_i g_i \sigma_i^{-1}$, we see that $G_i \cap G_j = \{1\}$. Thus, we must have $G_i (= G_j) = \{1\}$.

By this consideration, we conclude that $I_p$ is isomorphic as a $G$-set to a disjoint union of copies of $G$ and copies of $G/G$. If a copy of $G/G$ appears, then this means $G = G_i$ for some $i = 1, \dots, p$, and, by using the unique extension of $\sigma_i$ to $I_p \xrightarrow{\sim} \mathbb{F}_p$, we obtain $G \subset \mathbb{F}_p^\times \subset B_p$.

On the other hand, if no copy of $G/G$ appears, we must have $\sharp(G) \mid p$. As $\sharp(G) \mid p - 1$ also holds, we conclude $G = \{1\} \subset B_p$. This completes the proof. $\square$

By (1.8), we may apply (1.9) to $G = \operatorname{Gal}(K(\alpha)(F_\alpha)/K(\alpha))$ and the Kummer character $\phi : G \to \mathbb{F}_p^\times$ defined by $(-a/h'(\alpha))^{1/(p-1)}$, and conclude $G \subset B_p$, as desired.
(iii) This has been already done in the proofs of (i) and (ii). $\square$

COROLLARY (1.10). *Let $m$ be an integer $\geq 1$. Let $R = R^{\mathrm{univ}}$ be the completion of the discrete valuation ring $\mathbb{F}_p[s_0, s_p, s_{2p}, \ldots, s_{(m-1)p}, s_1]_{(s_1)}$ (where $s_i$'s are algebraically independent indeterminates), i.e., $R = \mathbb{F}_p(s_0, s_p, \ldots, s_{(m-1)p})[[s_1]]$, and $K = K^{\mathrm{univ}}$ the field of fractions of $R$. Consider a superseparable polynomial $f(T)$ as in* (1.3)*, where $a = s_1$ and $h(T) = \sum_{i=0}^{m} s_{ip} T^i$ ($s_{mp} \stackrel{\mathrm{def}}{=} 1$). Then:*

(i) *By choosing a suitable bijection between* $\mathrm{roots}(f)$ *and $I_m \times I_p$, the Galois group $G_f$ can be identified with an extension group of $S_m$ by a subgroup $B$ of $(B_p)^{I_m}$. Here, $B$ is an extension of a subgroup $E$ of $(B_p)^{I_m}/(C_p)^{I_m} = (\mathbb{F}_p^\times)^{I_m}$ by $(C_p)^{I_m}$, where $E = (\mathbb{F}_2^\times)^{I_m} = \{1\}$ if $p = 2$,*

$$E = \begin{cases} \mathrm{Ker}((\mathbb{F}_p^\times)^{I_2} \twoheadrightarrow (\mathbb{F}_p^\times/\{\pm 1\})^{I_2}/\Delta(\mathbb{F}_p^\times/\{\pm 1\})), & m = 2, \\ \mathrm{Ker}((\mathbb{F}_p^\times)^{I_m} \twoheadrightarrow \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2), & m \equiv 0 \pmod 2,\ m \neq 2, \\ (\mathbb{F}_p^\times)^{I_m}, & m \not\equiv 0 \pmod 2, \end{cases}$$

*if $p \equiv 1 \pmod 4$, and*

$$E = \begin{cases} \mathrm{Ker}((\mathbb{F}_p^\times)^{I_2} \twoheadrightarrow (\mathbb{F}_p^\times/\{\pm 1\})^{I_2}/\Delta(\mathbb{F}_p^\times/\{\pm 1\})), & m = 2, \\ \mathrm{Ker}((\mathbb{F}_p^\times)^{I_m} \twoheadrightarrow \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2), & m \equiv 0 \pmod 4, \\ (\mathbb{F}_p^\times)^{I_m}, & m \not\equiv 0 \pmod 4,\ m \neq 2, \end{cases}$$

*if $p \equiv 3 \pmod 4$. Here, for a commutative group $G$ and a positive integer $r$, we define subgroups $\Delta(G)$ and $(G^{I_r})^0$ of $G^{I_r}$ by $\Delta(G) = \{(g, \ldots, g) \in G^{I_r} \mid g \in G\}$ and $(G^{I_r})^0 = \mathrm{Ker}(G^{I_r} \to G,\ (g_1, \ldots, g_r) \mapsto g_1 \cdots g_r)$, respectively, and, in the case where either $p \equiv 1 \pmod 4$, $m \equiv 0 \pmod 2$, $m \neq 2$ or $p \equiv 3 \pmod 4$, $m \equiv 0 \pmod 4$ holds, the surjective homomorphism $(\mathbb{F}_p^\times)^{I_m} \twoheadrightarrow \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ is the composite of $(\mathbb{F}_p^\times)^{I_m} \twoheadrightarrow (\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2)^{I_m}$ and $(\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2)^{I_m} \twoheadrightarrow (\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2)^{I_m}/((\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2)^{I_m})^0 = \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$. Moreover, the inertia subgroup of $G_f$ corresponds to $\Delta(\mathbb{F}_p^\times) \ltimes (\mathbb{F}_p)^{I_m}$.*

(ii) *$k_{K_f}$ is generated by $\{(\alpha \bmod \mathfrak{m}_{K_f})^{1/p} \mid \alpha \in \mathrm{roots}(h)\} \cup \{(h'(\alpha)/h'(\alpha'))^{\frac{1}{p-1}} \bmod \mathfrak{m}_{K_f} \mid \alpha, \alpha' \in \mathrm{roots}(h)\}$ over $k$. Moreover, the algebraic closure $\mathbb{F}$ of $\mathbb{F}_p$ in $k_{K_f}$ coincides with $\mathbb{F}_2$ if $p = 2$,*

$$\mathbb{F} = \begin{cases} \mathbb{F}_{p^2}, & m = 2, \\ \mathbb{F}_p, & m \neq 2, \end{cases}$$

*if $p \equiv 1 \pmod 4$, and*

$$\mathbb{F} = \begin{cases} \mathbb{F}_{p^2}, & m \equiv 2 \pmod 4, \\ \mathbb{F}_p, & m \not\equiv 2 \pmod 4, \end{cases}$$

*if $p \equiv 3 \pmod 4$.*

*Proof.* (i) In order to apply (1.5), we have to check that conditions (a) and (b) of (1.5) hold. It is easy to see that (a) holds. Next, since $K_h = \mathbb{F}_p(\alpha_1, \dots, \alpha_m)((s_1))$, where $\mathrm{roots}(h) = \{\alpha_1, \dots, \alpha_m\}$, we have $\mu(h, \alpha) = 0$ for each $\alpha \in \mathrm{roots}(h)$, while $\delta(a, h, \alpha) = v(s_1) = 1$. Thus (b) holds, and we may apply (1.5).

It is easy to see that $K_h/K$ is an unramified $S_m$-extension. Next we have $M_f = K_h((-s_1/h'(\alpha_1))^{1/(p-1)}, \dots, (-s_1/h'(\alpha_m))^{1/(p-1)})$. Since $-1/h'(\alpha_i)$ is a unit of $R_{K_h}$ and $s_1$ is a prime element of $R_{K_h}$, the inertia subgroup of $\mathrm{Gal}(M_f/K_h)$ corresponds to $\Delta(\mathbb{F}_p^\times)$, and the maximal unramified subextension $M_{0,f}/K_h$ in $M_f/K_h$ is $K_h((h'(\alpha_i)/h'(\alpha_j))^{1/(p-1)} \mid i, j = 1, \dots, m) = K_h((h'(\alpha_i)/h'(\alpha_1))^{1/(p-1)} \mid i = 2, \dots, m)$.

Now, observing the subgroup of $K_h^\times/(K_h^\times)^{p-1}$ generated by the classes of $-a/h'(\alpha)$ ($\alpha \in$ roots) by using the divisor group of (the spectrum of) the polynomial ring $\mathbb{F}_p[\alpha_1, \dots, \alpha_m]$ over $\mathbb{F}_p$, we obtain the desired description of $E$. (We leave the details to the readers.)

Finally, by (1.6)(i), $k_{K_f}$ contains $\{(\alpha \bmod \mathfrak{m}_{K_f})^{1/p} \mid \alpha \in \mathrm{roots}(h)\}$. Since $k_{K_h}$ is a purely transcendental extension of $\mathbb{F}_p$ generated by $\alpha \bmod \mathfrak{m}_{K_f}$ and $k_{M_f}$ is separable over $k_{K_h}$, the inseparable degree of the extension $k_{K_f}/k_{M_f}$ is at least $p^m$. Thus, the ramification index of the extension $K_f/M_f$ is at least $p^m$. Therefore, $K_f/M_f$ must be totally ramified with degree $p^m$ and the Galois group $\mathrm{Gal}(K_f/M_f)$ must coincide with the whole of $(C_p)^{I_m}$.

These complete the proof of (i).

(ii) The above proof shows that $k_{K_h} = k(\alpha \bmod \mathfrak{m}_{K_h} \mid \alpha \in \mathrm{roots}(h))$, and that $k_{K_f}$ contains the field $k'_{K_f}$ generated by $\{(\alpha \bmod \mathfrak{m}_{K_f})^{1/p} \mid \alpha \in \mathrm{roots}(h)\} \cup \{(h'(\alpha)/h'(\alpha'))^{\frac{1}{p-1}} \bmod \mathfrak{m}_{K_f} \mid \alpha, \alpha' \in \mathrm{roots}(h)\}$ over $k_{K_h}$ (or, equivalently, over $k$, as $\alpha = (\alpha^{1/p})^p$). Moreover, we can check $[k_{K_f} : k_{K_h}] = [k'_{K_f} : k_{K_h}]$, which implies $k_{K_f} = k'_{K_f}$, as desired.

Finally, $k_{K_h}$ is a purely transcendental extension of $\mathbb{F}_p$ generated by $\{\alpha \bmod \mathfrak{m}_{K_h} \mid \alpha \in \mathrm{roots}(h)\}$. Moreover, observing the subgroup of $(K_h\overline{\mathbb{F}}_p)^\times/((K_h\overline{\mathbb{F}}_p)^\times)^{p-1}$ generated by the classes of $-a/h'(\alpha)$ ($\alpha \in \mathrm{roots}(h)$) by using the divisor group of (the spectrum of) the polynomial ring $\overline{\mathbb{F}}_p[\alpha_1, \dots, \alpha_m]$ over $\overline{\mathbb{F}}_p$, and comparing the result with the above description of the subgroup of $K_h^\times/(K_h^\times)^{p-1}$ generated by the classes of $-a/h'(\alpha)$ ($\alpha \in \mathrm{roots}(h)$), we see that the algebraic closure of $\mathbb{F}_p$ in $k_{K_h}$ is as described in the assertion. Since $k_{K_f}/k_{M_f}$ is purely inseparable, this completes the proof. $\square$

So far, we have only investigated superseparable polynomials over complete discrete valuation fields. Here, we shall introduce the following global situation and study superseparable polynomials in a moduli-theoretic fashion. We put

$$A^{mp}_{\mathrm{upper}} \stackrel{\mathrm{def}}{=} \mathrm{Spec}(\mathbb{F}_p[t_1, \dots, t_{mp}]) \simeq \mathbf{A}^{mp}_{\mathbb{F}_p}$$

and

$$A^{mp}_{\mathrm{lower}} \stackrel{\mathrm{def}}{=} \mathrm{Spec}(\mathbb{F}_p[s_0, \dots, s_{mp-1}]) \simeq \mathbf{A}^{mp}_{\mathbb{F}_p}.$$

Moreover, consider the morphism $E : A^{mp}_{\text{upper}} \to A^{mp}_{\text{lower}}$, defined by

$$\prod_{i=1}^{mp}(T - t_i) = \sum_{i=0}^{mp} s_i T^i,$$

where $s_{mp} \stackrel{\text{def}}{=} 1$. Namely, for $i = 0, \ldots, mp-1$, $s_i$ is $(-1)^{mp-i}$ times the $(mp-i)$-th elementary symmetric polynomial in $t_1, \ldots, t_{mp}$. It is well-known that $E$ is finite flat of degree $(mp)!$, and that, if we delete the discriminant locus $D_{\text{lower}}$ from $A^{mp}_{\text{lower}}$ and the union $D_{\text{upper}}$ of weak diagonals from $A^{mp}_{\text{upper}}$, $E$ gives a finite, étale, Galois covering with Galois group $S_{mp}$.

Let $A^{m+1}_{\text{lower}}$ be the closed subscheme of $A^{mp}_{\text{lower}}$ defined by $s_i = 0$ for all $i$ with $p \nmid i$ and $i \neq 1$. We define a divisor $A^m_{\text{lower}}$ of $A^{m+1}_{\text{lower}}$ by $s_1 = 0$. Observe that $A^m_{\text{lower}}$ coincides with the non-étale locus of $E|_{A^{m+1}_{\text{lower}}}$, and that we have $A^m_{\text{lower}} = A^{m+1}_{\text{lower}} \cap D_{\text{lower}}$ set-theoretically. We also have $A^{m+1}_{\text{lower}} \simeq \mathbf{A}^{m+1}_{\mathbb{F}_p}$ and $A^m_{\text{lower}} \simeq \mathbf{A}^m_{\mathbb{F}_p}$ naturally.

Now, we have the following diagram:

$$\begin{array}{ccc}
A^{mp}_{\text{upper}} - D_{\text{upper}} & \stackrel{E}{\to} & A^{mp}_{\text{lower}} - D_{\text{lower}} \\
\uparrow \text{c.i.} & \square & \uparrow \text{c.i.} \\
U_m & \to & A^{m+1}_{\text{lower}} - A^m_{\text{lower}}
\end{array}$$

where $\square$ means a fiber product diagram, $\stackrel{\text{c.i.}}{\to}$ means a closed immersion, and $U_m \stackrel{\text{def}}{=} A^{mp}_{\text{upper}} \times_{A^{mp}_{\text{lower}}} (A^{m+1}_{\text{lower}} - A^m_{\text{lower}})$.

We shall apply this moduli-theoretic situation to the study of superseparable polynomials over a (an arbitrary) complete discrete valuation field $K$ of characteristic $p > 0$. From now, for each finite subset $S$ of $\overline{K}$, we put $\phi_S(T) \stackrel{\text{def}}{=} \prod_{\alpha \in S}(T - \alpha)$.

Proposition (1.11). *Let $m$ be an integer $\geq 1$. Assume that there exists a finite subset $S$ of $K$ with cardinality $m$, such that $\phi_S$ satisfies*

$$\phi'_S(\gamma)/\phi'_S(\gamma') \in (K^\times)^{p-1} \text{ for all } \gamma, \gamma' \in S. \tag{1.12}$$

*Then, there exists a monic, superseparable polynomial $f(T) \in K[T]$ with $\deg(f) = mp$, such that $f$ is completely splittable in $K$.*

*Proof.* We consider the above moduli-theoretic situation $E : A^{mp}_{\text{upper}} \to A^{mp}_{\text{lower}}$ and $A^m_{\text{lower}} \stackrel{\text{c.i.}}{\to} A^{m+1}_{\text{lower}} \stackrel{\text{c.i.}}{\to} A^{mp}_{\text{lower}}$. We have to show that $U \stackrel{\text{def}}{=} U_m$ admits a $K$-rational point. Recall that $E$ induces a finite, étale (not necessarily connected) $S_{mp}$-Galois covering $U \to A^{m+1}_{\text{lower}} - A^m_{\text{lower}}$. However, first we need to investigate the non-étale loci of $E$.

We put $A^m_{\mathrm{upper}} \stackrel{\mathrm{def}}{=} \mathrm{Spec}(\mathbb{F}_p[u_1, \ldots, u_m]) \simeq \mathbf{A}^m_{\mathbb{F}_p}$, and define a morphism $D : A^m_{\mathrm{upper}} \to A^{mp}_{\mathrm{upper}}$ by

$$(u_1, \ldots, u_m) \mapsto (\underbrace{u_1, \ldots, u_1}_{p \text{ times}}, \ldots, \underbrace{u_m, \ldots, u_m}_{p \text{ times}}),$$

which is clearly a closed immersion. It is easy to see that $E \circ D : A^m_{\mathrm{upper}} \to A^{mp}_{\mathrm{lower}}$ factors through $A^m_{\mathrm{lower}} \stackrel{\text{c.i.}}{\to} A^{mp}_{\mathrm{lower}}$. More explicitly, $E \circ D$ induces a morphism $A^m_{\mathrm{upper}} \to A^m_{\mathrm{lower}}$, $(u_1, \ldots, u_m) \mapsto ((v_1)^p, \ldots, (v_m)^p)$, where $v_i$ is $(-1)^{m-i}$ times the $(m-i)$-th elementary symmetric polynomial in $u_1, \ldots, u_m$.

Now, we obtain the following diagram:

$$\begin{tikzcd}
 & & A^{mp}_{\mathrm{upper}} \arrow[r, "E"] & A^{mp}_{\mathrm{lower}} \\
 & \tilde{X} \arrow[r] & X \arrow[r] \arrow[u, "\text{c.i.}"'] \arrow[ur, phantom, "\square"] & A^{m+1}_{\mathrm{lower}} \arrow[u, "\text{c.i.}"'] \\
 & Z' \arrow[r] \arrow[u, "\text{c.i.}"'] \arrow[ur, phantom, "\square"] & Z \arrow[r] \arrow[u, "\text{c.i.}"'] \arrow[ur, phantom, "\square"] & A^m_{\mathrm{lower}} \arrow[u, "\text{c.i.}"'] \\
\tilde{W} \arrow[r] & W \arrow[r] \arrow[u, "\text{c.i.}"'] & A^m_{\mathrm{upper}}. \arrow[u, "\text{c.i.}"'] &
\end{tikzcd}$$

Here, $X \stackrel{\mathrm{def}}{=} A^{mp}_{\mathrm{upper}} \times_{A^{mp}_{\mathrm{lower}}} A^{m+1}_{\mathrm{lower}}$, $\tilde{X}$ denotes the normalization of $X$ in $U$, $Z \stackrel{\mathrm{def}}{=} X \times_{A^{m+1}_{\mathrm{lower}}} A^m_{\mathrm{lower}}$, $Z' \stackrel{\mathrm{def}}{=} \tilde{X} \times_X Z$, $W$ denotes an irreducible component of $\tilde{X} \times_X A^m_{\mathrm{upper}}$ (regarded as a reduced closed subscheme of $\tilde{X}$) that is surjectively mapped onto $A^m_{\mathrm{upper}}$, and $\tilde{W}$ is the normalization of the integral scheme $W$.

Now, we are in the situation of (1.10). More explicitly, in the notation of (1.10), $K^{\mathrm{univ}}$ is just the field of fractions of the completed local ring of $A^{m+1}_{\mathrm{lower}}$ at the generic point of $A^m_{\mathrm{lower}}$, $k_{K^{\mathrm{univ}}} = \mathbb{F}_p(A^m_{\mathrm{lower}})$, and $k_{K^{\mathrm{univ}}_f} = \mathbb{F}_p(W)$. Moreover, we see that $\mathbb{F}_p(A^m_{\mathrm{upper}}) = K^{\mathrm{univ}}_h((\alpha_1)^{1/p}, \ldots, (\alpha_m)^{1/p})$. Thus, (1.10)(ii) implies that $\mathbb{F}_p(W)$ is generated by $\{(h'(\alpha)/h'(\alpha'))^{1/(p-1)} \mid \alpha, \alpha' \in \mathrm{roots}(h)\}$ over $\mathbb{F}_p(A^m_{\mathrm{upper}})$. Note that $u_i = \alpha_i^{1/p}$ holds for each $i = 1, \ldots, m$. So, if we put $\mathbb{S} \stackrel{\mathrm{def}}{=} \{u_1, \ldots, u_m\}$, we have $\phi'_{\mathbb{S}}(u_i)^p = h'(\alpha_i)$, hence

$$\left( \frac{(h'(\alpha_i)/h'(\alpha_j))^{1/(p-1)}}{(\phi'_{\mathbb{S}}(u_i)/\phi'_{\mathbb{S}}(u_j))} \right)^{p-1} = \phi'_{\mathbb{S}}(u_i)/\phi'_{\mathbb{S}}(u_j).$$

Thus, we see that $\mathbb{F}_p(W)$ is generated by $\{(\phi'_{\mathbb{S}}(u_i)/\phi'_{\mathbb{S}}(u_j))^{1/(p-1)} \mid i, j = 1, \ldots, m\}$ over $\mathbb{F}_p(A^m_{\mathrm{upper}})$.

Let $V$ be the complement of the union of weak diagonals defined by $u_i - u_j = 0$ for $i, j = 1, \dots, m,\ i \neq j$ in $A^m_{\mathrm{upper}}$. Since $\tilde{W}$ coincides with the integral closure of $A^m_{\mathrm{upper}}$ in $\mathbb{F}_p(W)$, we now see that $\tilde{W}_V \stackrel{\mathrm{def}}{=} \tilde{W} \times_{A^m_{\mathrm{upper}}} V$ is finite étale covering generated by $\{(\phi'_{\mathbb{S}}(u_i)/\phi'_{\mathbb{S}}(u_j))^{1/(p-1)} \mid i, j = 1, \dots, m\}$ over $V$.

Now, take a finite set $S$ as in our assumption, and put $S = \mathrm{roots}(\phi_S) = \{\gamma_1, \dots, \gamma_m\}$. Then, $x = (\gamma_1, \dots, \gamma_m)$ gives an element of $V(K) \subset A^m_{\mathrm{upper}}(K)$. Moreover, condition (1.12), together with the above description of $\tilde{W}_V$, implies that the fiber of $\tilde{W}_V \to V$ at $x$ consists of $K$-rational points. In particular, we have $\tilde{W}_V(K) \neq \emptyset$. Note that $\tilde{W}_V$ is smooth over $\mathbb{F}_p$, as being étale over $A^m_{\mathrm{upper}}$. Or, equivalently, $\tilde{W}_V$ is contained in the smooth locus $\tilde{W}^{\mathrm{sm}}$ of $\tilde{W}$. Now, as $K$ is large, we conclude that $\tilde{W}(K)$ is Zariski dense in $\tilde{W}$. (See [Pop] for the definition and properties of large fields.) Accordingly, $W(K)$ is dense in $W$, a fortiori.

On the other hand, since $\tilde{X}$ is normal (and $\mathbb{F}_p$ is perfect), the complement of $\tilde{X}^{\mathrm{sm}}$ is of codimension $\geq 2$ in $\tilde{X}$. It follows from this that $W \cap \tilde{X}^{\mathrm{sm}}$ is non-empty (and open in $W$). Moreover, since $W$ is integral (and $\mathbb{F}_p$ is perfect), we have $W^{\mathrm{sm}}$ is also non-empty and open, hence so is $W' \stackrel{\mathrm{def}}{=} W^{\mathrm{sm}} \cap \tilde{X}^{\mathrm{sm}}$. As we have already seen, $W(K)$ is dense in $W$. Accordingly, we have $W'(K) \neq \emptyset$, hence, a fortiori, $\tilde{X}^{\mathrm{sm}}(K) \neq \emptyset$. As $K$ is large, this implies that there exists a connected (or, equivalently, irreducible) component $Y$ of $\tilde{X}$, such that $Y(K)$ is dense in $Y$. Now, observe that $Y \to A^{m+1}_{\mathrm{lower}}$ is (finite and) surjective. From this, $Y_U \stackrel{\mathrm{def}}{=} Y \times_X U = Y \cap U$ (where the last intersection is taken in $\tilde{X}$) is non-empty (and open in $Y$). Thus, $Y_U(K)$ is non-empty, hence, a fortiori, $U(K)$ is non-empty. This completes the proof. □

Lemma (1.13). *Let $m$ be an integer $\geq 1$. Assume that $(K, m)$ satisfies:*

(1.14) *At least one of the following holds:*
*$K \supset \mathbb{F}_{p^2}$; $p = 2$; $m \equiv \epsilon \pmod{p+1}$ for some $\epsilon \in \{0, \pm 1\}$.*

*Then, there exists a finite subset $S$ of $K$ with cardinality $m$, such that $\phi_S$ satisfies* (1.12).

*Proof.* Let $s$ denote any element of $\mathfrak{m} \cap (K^\times)^{p-1}$ (e.g., $s = t^{p-1}$).

Firstly, assume that either $K \supset \mathbb{F}_{p^2}$ or $p = 2$ holds. In this case, we take any integers $i_1, \dots, i_m$ with $i_1 < \cdots < i_m$ and put $S \stackrel{\mathrm{def}}{=} \{s^{i_k} \mid k = 1, \dots, m\}$. Then, $\sharp(S) = m$ clearly holds. Now, for $\gamma = s^{i_k} \in S$, we have

$$\begin{aligned} \phi'_S(\gamma) &= \prod_{j=1}^{k-1}(s^{i_k} - s^{i_j}) \prod_{j=k+1}^{m}(s^{i_k} - s^{i_j}) \\ &= (-1)^{k-1} s^{i_1 + \cdots + i_{k-1} + (m-k)i_k} \prod_{j \neq k}(1 - s^{|i_k - i_j|}). \end{aligned}$$

Note that we have $-1, s \in (K^\times)^{p-1}$ and $1 + \mathfrak{m} \subset (K^\times)^{p-1}$. (For $-1$, use the assumption that either $K \supset \mathbb{F}_{p^2}$ or $p = 2$ holds.) Thus, (1.12) holds.

Secondly, assume $m \equiv \epsilon \pmod{p+1}$ with $\epsilon \in \{0, \pm 1\}$. We may put $m = (p+1)n + \epsilon$. Moreover, we take any integers $i_1, j_1, i_2, j_2, \dots, i_n, j_n, i_{n+1}$ with $i_1 < j_1 < i_2 < j_2 < \cdots < i_n < j_n < i_{n+1}$. Now, we put $S_\epsilon = \{s^{i_k} \mid k \in I_\epsilon\} \cup \{s^{j_k} + c s^{j_k+1} \mid k = 1, \dots, n,\ c \in \mathbb{F}_p\}$, where

$$I_\epsilon = \begin{cases} \{2, \dots, n\}, & \epsilon = -1, \\ \{1, \dots, n\}, & \epsilon = 0, \\ \{1, \dots, n+1\}, & \epsilon = 1. \end{cases}$$

Then, by using $s \in (K^\times)^{p-1}$, $1 + \mathfrak{m} \subset (K^\times)^{p-1}$, and the fact $\prod_{j \in \mathbb{F}_p^\times} j = -1$, we can elementarily check that $\phi'_{S_\epsilon}(\gamma) \in (K^\times)^{p-1}$ (resp. $\phi'_{S_\epsilon}(\gamma) \in -(K^\times)^{p-1}$) holds for each $\gamma \in S_\epsilon$, if $\epsilon = 0, 1$ (resp. $\epsilon = -1$). Thus, (1.12) holds. □

Definition. Let $f(T) = a_1 T + \sum_{i=0}^{m} a_{ip} T^{ip}$ be a superseparable polynomial (over some field of characteristic $p$).
(i) We say that $f$ is of special type, if $a_{mp} = a_1 = 1,\ a_0 = 0$ holds.
(ii) We put $\operatorname{def}(f) \stackrel{\text{def}}{=} \sup\{r > 0 \mid a_j = 0 \text{ for all } j \text{ with } mp > j > mp - r\}$ and call it the defect of $f$. (Thus, we have $0 < \operatorname{def}(f) \le mp - 1$, unless $m = 0$.)

Corollary (1.15). *Let $m$ be a positive integer.*
(i) *Assume that $(K, m)$ satisfies* (1.14). *Then, there exists a monic, integral, superseparable polynomial $f(T) \in K[T]$ with $f(0) = 0$ and $\deg(f) = mp$, such that $f$ is completely splittable in $K$.*
(ii) *Assume that $(K, m)$ satisfies one of the following: $K \supset \mathbb{F}_{p^2}$ and $(p-1, m-1) = (p+1, m+1) = 1$; $p = 2$; $m \equiv \epsilon \pmod{p+1}$ for some $\epsilon \in \{0, \pm 1\}$ and $(p-1, m-1) = 1$. Then, there exists a superseparable polynomial $f(T) \in K[T]$ of special type with $\deg(f) = mp$, such that $f$ is completely splittable in $K$.*

*Proof.* (i) By (1.11) and (1.13), there exists a monic superseparable polynomial $f(T) \in K[T]$ with $\deg(f) = mp$, such that $f$ is completely splittable in $K$. Replacing $f(T)$ by $f_c(T) \stackrel{\text{def}}{=} c^{mp} f(c^{-1}T)$ with $c \in K^\times$, $v(c) \gg 0$, we may assume that $f$ is integral. (Observe that $\operatorname{roots}(f_c) = c \operatorname{roots}(f)$.) Finally, replacing $f(T)$ by $f(T + \alpha)$, where $\alpha \in \operatorname{roots}(f)$, we may assume $f(0) = 0$.
(ii) We have $K \supset \mathbb{F}_q((t))$ with $q = p^2$ (resp. $q = p$), if $K \supset \mathbb{F}_{p^2}$ (resp. either $p = 2$ or $m \equiv \epsilon \pmod{p+1}$ with $\epsilon \in \{0, \pm 1\}$). Thus, it suffices to prove the assertion in the case $K = \mathbb{F}_q((t))$. So, from now on, we assume that $K = \mathbb{F}_q((t))$.

By (1.11) and (1.13), there exists a monic, superseparable polynomial $f_1(T) \in K[T]$ with $\deg(f_1) = mp$, such that $f_1$ is completely splittable in $K$. Replacing $f_1(T)$ by $f_1(T + \alpha)$, where $\alpha \in \operatorname{roots}(f_1)$, we may assume that $f_1(0) = 0$. Moreover, we may put $f_1(T) = a_1(t) T + \sum_{i=0}^{m} a_{ip}(t) T^{ip}$, where

$a_{ip}(t) \in K = \mathbb{F}_q((t))$, $a_1(t) \in K^\times = \mathbb{F}_q((t))^\times$, and $a_{mp}(t) = 1$, $a_0(t) = 0$. Next, we put $f_2(T) \stackrel{\text{def}}{=} a_1(t^{mp-1})T + \sum_{i=1}^{m} a_{ip}(t^{mp-1})T^{ip}$. Then, $f_2(T)$ is completely splittable in $\mathbb{F}_q((t)) \supset \mathbb{F}_q((t^{mp-1}))$.

Put $a_1(t) = ct^r + \cdots$, where $c \in \mathbb{F}_q^\times$, $r \in \mathbb{Z}$, and $\cdots$' means the higher order terms. Then, we have $a_1(t^{mp-1}) = ct^{r(mp-1)} + \cdots$. Here, observe that $(p-1, m-1) = (p+1, m+1) = 1$ (resp. $(p-1, m-1) = 1$) is equivalent to saying $(q-1, mp-1) = 1$, for $q = p^2$ (resp. $q = p$). So, we have $\mathbb{F}_q^\times = (\mathbb{F}_q^\times)^{mp-1}$. By using this fact (and the fact that $1 + \mathfrak{m} \subset (K^\times)^{mp-1}$ as $p \nmid mp-1$), we see that $a_1(t^{mp-1}) \in (K^\times)^{mp-1}$. So, write $a_1(t^{mp-1}) = b(t)^{mp-1}$. Now, it is easy to check that $f(T) \stackrel{\text{def}}{=} b(t)^{-mp} f_2(b(t)T)$ satisfies the desired conditions. This completes the proof. $\square$

Corollary (1.16). (i) *There exists a positive integer $m_1$ (which depends only on $p$), such that, for each positive integer $m$ with $m_1 \mid m$, there exists a monic, integral, superseparable polynomial $f$ in $K[T]$ with $f(0) = 0$ and $\deg(f) = mp$, such that $f$ is completely splittable in $K$.*
(ii) *There exists a positive integer $m_2$ (which depends only on $p$), such that, for each positive integer $m$ with $m_2 \mid m$, there exists a superseparable polynomial $f$ in $K[T]$ of special type and with $\deg(f) = mp$, such that $f$ is completely splittable in $K$.*

*Proof.* (i) (resp. (ii)) is a direct corollary of (1.15)(i) (resp. (ii)). We can take, for example, $m_1 = p + 1$ (resp. $m_2 = (p+1)(p-1)$). $\square$

Lemma (1.17). *Let $F$ be a field of characteristic $p$, and $L$ a Galois extension of $F$. Let $A$ be an $\mathbb{F}_p[\mathrm{Gal}(L/F)]$-submodule of $L$ with $\dim_{\mathbb{F}_p}(A) = r < \infty$, and put $\phi_A(T) \stackrel{\text{def}}{=} \prod_{\alpha \in A}(T - \alpha)$. Then:*
(i) *$\phi_A(T)$ is a monic superseparable polynomial in $F[T]$.*
(ii) *$F_{\phi_A} = F(A)$.*
(iii) *$\deg(\phi_A) = p^r$ and $\mathrm{def}(\phi_A) \geq p^r - p^{r-1}$.*
(iv) *$\phi'_A(T) = \prod_{\alpha \in A - \{0\}} \alpha$.*
(v) *If, moreover, $F = K$ and $A \subset R_L$, then $\phi_A$ is integral.*

*Proof.* (i) By definition, $\phi_A$ is monic and separable. It is well-known that $\phi_A$ is an additive polynomial, hence a superseparable polynomial. Since $A$ is $\mathrm{Gal}(L/F)$-stable, $\phi_A(T) \in F[T]$.
(ii) Clear.
(iii) The first assertion is clear. The second assertion follows from the fact that $\phi_A$ is an additive polynomial.
(iv) Since $\phi_A$ is monic and superseparable, we obtain

$$\phi'_A(T) = \phi'_A(0) = \prod_{\alpha \in A - \{0\}} (-\alpha) = \prod_{\alpha \in A - \{0\}} \alpha,$$

as desired.
(v) Clear. $\square$

The following corollary is a final result of this §, of which (i) (resp. (ii)) will play a key role in §2 (resp. §3). Note that one of the main differences between (i) and (ii) consists in the fact that, in (ii), the defect of the superseparable polynomial is estimated from below.

Corollary (1.18). (i) *Let $L$ be a finite Galois extension of $K$. Then, there exists a positive integer $m_{L/K}$, such that, for each positive integer $m$ with $m_{L/K} \mid m$, there exists a superseparable polynomial $f(T) \in K[T]$ of special type with* $\deg(f) = mp$ *and* $K_f = L$.
(ii) *We have:*

$\forall n$*: positive integer,*

$\exists m_n$*: positive integer (depending only on $p$ and $n$),*

$\forall m$*: positive integer with $m_{K,n} \mid m$,*

$\exists c = c_{K,n,m}$*: positive real number,*

$\forall L$*: (possibly infinite) Galois extension of $K$,*

$\forall A$*: finite $\mathbb{F}_p[\mathrm{Gal}(L/K)]$-submodule of $R_L$ with $A \cap \mathfrak{m}_L = \{0\}$,*

$\forall r$*: integer $> \dim_{\mathbb{F}_p}(A)$,*

$\forall \nu$*: integer,*

$\exists \delta$*: positive integer with $\delta \leq cmp^{r+1}/\sharp(A)$ and $\delta \equiv \nu \pmod{n}$,*

$\forall a \in K^\times$ *with $v(a) = \delta$,*

$\exists f(T)$*: monic, integral, superseparable polynomial in $K[T]$,*

*s.t.* $\deg(f) = mp^{r+1}$, $\mathrm{def}(f) \geq (p-1)p^r$, $f'(T) = a$ *and* $K_f = K(A) \subset L$.

*Proof.* (i) Since $L/K$ is finite, we see that there exists a finite $\mathbb{F}_p[\mathrm{Gal}(L/K)]$-submodule $A_0 \neq \{0\}$ of $L$, such that $L = K(A_0)$. We put $q \stackrel{\mathrm{def}}{=} \sharp(A_0)$, which is a power of $p$. Then, by (1.17), $\phi_1 \stackrel{\mathrm{def}}{=} \phi_{A_0}$ is a monic, superseparable polynomial in $K[T]$ with $\deg(\phi_1) = q$, $\phi_1(0) = 0$, and $\phi_1'(T) = a_0 \stackrel{\mathrm{def}}{=} \prod_{\alpha \in A_0 - \{0\}} \alpha$, and $L = K_{\phi_1}$. On the other hand, take $m_2$ as in (1.16)(ii). Now, we put $m_{L/K} \stackrel{\mathrm{def}}{=} q(q-1)m_2$.

Let $m$ be any positive integer divisible by $m_{L/K}$, and put $n \stackrel{\mathrm{def}}{=} m/m_{L/K}$. Then, by (1.16)(ii), there exists a superseparable polynomial $f_1(T) \in K[T]$ of special type and with degree $n(q-1)m_2p$, such that $f_1$ is completely splittable in $K$.

For each $b \in K^\times$, we put $f_b(T) \stackrel{\mathrm{def}}{=} b^{n(q-1)m_2p} f_1(b^{-1}T)$ (resp. $\phi_b(T) \stackrel{\mathrm{def}}{=} b^q \phi_1(b^{-1}T)$), so that $f_b$ (resp. $\phi_b$) is a monic, superseparable polynomial with $\deg(f_b) = n(q-1)m_2p$ (resp. $\deg(\phi_b) = q$), $f_b(0) = 0$ (resp. $\phi_b(0) = 0$), and $f_b'(T) = b^{n(q-1)m_2p-1}$ (resp. $\phi_b'(T) = b^{q-1}a_0$).

Now, by (1.4)(ii), every polynomial in $L[T]$ with degree $q$ which is sufficiently close to $\phi_b(T)$ ($b \in K^\times$) is completely splittable in $L$. By using this, we see that $F_{b,b'} \stackrel{\text{def}}{=} f_{b'} \circ \phi_b \in K[T]$ satisfies $K_{F_{b,b'}} = L$ for all $b' \in K^\times$ with $v(b') \geq C(b)$, where $C(b)$ denotes a constant depending on $b$. Observe that $F_{b,b'}$ is a monic, superseparable polynomial with $\deg(F_{b,b'}) = n(q-1)m_2p \times q = mp$, $F_{b,b'}(0) = 0$, and $F'_{b,b'}(T) = (b')^{n(q-1)m_2p-1}b^{q-1}a_0$.

Now, take $b = a_0^{-nm_2p}$ and $b' = a_0 d^{mp-1}$ for any $d \in K^\times$ with $v(d)$ sufficiently large, then $f(T) \stackrel{\text{def}}{=} D^{-mp}F_{b,b'}(DT)$ with $D \stackrel{\text{def}}{=} d^{n(q-1)m_2p-1}$ satisfies all the desired properties.

(ii) Let $m_1$ be as in (1.16)(i), and choose any common multiple $m_n > 1$ of $m_1$, $p-1$, and $n$.

Let $m$ be any positive integer with $m_n \mid m$. Then, by (1.16)(i), there exists a monic, integral, superseparable polynomial $f_1(T) \in K[T]$ with $\deg(f_1) = mp$, $f_1(0) = 0$, and $K_{f_1} = K$. Now, put $f_1'(T) = a_1 \in R$ and $c \stackrel{\text{def}}{=} \max(\frac{v(a_1)}{m}, \frac{np}{p-1})$.

Let $L$ be any Galois extension of $K$, $A$ any finite $\mathbb{F}_p[\mathrm{Gal}(L/K)]$-submodule of $R_L$ with $A \cap \mathfrak{m}_L = \{0\}$, and $r$ any integer $> r_0 \stackrel{\text{def}}{=} \dim_{\mathbb{F}_p}(A)$. Let $\nu$ be any integer. We define $\mu$ to be the unique integer with $0 < \mu \leq n$, such that $\mu \equiv v(a_1) - (r-r_0) - \nu \pmod{n}$. We put $\delta \stackrel{\text{def}}{=} v(a_1) + \mu(mp-1) + \sum_{j=1}^{r-r_0}(mp^{j+1}-1)$.

Then, we have

$$\begin{aligned}
\delta &\leq v(a_1) + \sum_{j=0}^{r-r_0} nmp^{j+1} \\
&= m\left(\frac{v(a_1)}{m} + \frac{np}{p-1}(p^{r-r_0+1}-1)\right) \\
&\leq m(c + c(p^{r-r_0+1}-1)) \\
&= cmp^{r+1}/\sharp(A)
\end{aligned}$$

and

$$\delta \equiv v(a_1) - \mu - (r-r_0) \equiv \nu \pmod{n},$$

as desired.

Let $a$ be any element of $K^\times$ with $v(a) = \delta$. For $j = 0, \dots, r-r_0$, we shall inductively define a monic, integral, superseparable polynomial $f_{2,j}(T)$ with $\deg(f_{2,j}) = mp^{j+1}$, $f_{2,j}(0) = 0$, $f_{2,j}(T) \equiv T^{mp^{j+1}} \pmod{\mathfrak{m}}$, and $K_{f_{2,j}} = K$, as follows. First, for $j = 0$, we put $g_0(T) \stackrel{\text{def}}{=} f_1(T)$ and $f_{2,0}(T) \stackrel{\text{def}}{=} t^{\mu mp}g_0(t^{-\mu}T)$. Next, for $j$ with $0 < j < r-r_0$, we put $g_j \stackrel{\text{def}}{=} f_{2,j-1} \circ \phi_{\mathbb{F}_p}$, where $\phi_{\mathbb{F}_p}(T) = T^p - T$, and $f_{2,j}(T) \stackrel{\text{def}}{=} t^{mp^{j+1}}g_j(t^{-1}T)$. Finally, for $j = r-r_0$, let $u$ and $u'$ be elements of $R^\times$, which we shall fix later, and we put $g_{r-r_0} \stackrel{\text{def}}{=} f_{2,r-r_0-1} \circ \phi_{u\mathbb{F}_p}$, where $\phi_{u\mathbb{F}_p}(T) = T^p - u^{p-1}T$, and $f_{2,r-r_0}(T) \stackrel{\text{def}}{=} (u't)^{mp^{r-r_0+1}}g_{r-r_0}((u't)^{-1}T)$.

We can check inductively that $f_{2,j}(T)$ is a monic, integral, superseparable polynomial with $\deg(f_{2,j}) = mp^{j+1}$, $f_{2,j}(0) = 0$, $f_{2,j}(T) \equiv T^{mp^{j+1}} \pmod{\mathfrak{m}}$, and $K_{f_{2,j}} = K$. Moreover, since $f'_{2,0} = t^{\mu(mp-1)}a_1$, $f'_{2,j} = (-t^{mp^{j+1}-1})f'_{2,j-1}$ $(0 < j < r - r_0)$, and $f'_{2,r-r_0} = (-u^{p-1})(u't)^{mp^{r-r_0+1}-1}$, we obtain

$$\begin{aligned} f'_{2,r-r_0} &= u^{p-1}(u')^{mp^{r-r_0+1}-1}(-1)^{r-r_0}a_1 t^{\mu(mp-1)+\sum_{j=1}^{r-r_0}(mp^{j+1}-1)} \\ &= u^{p-1}(u')^{mp^{r-r_0+1}-1}(-1)^{r-r_0}(a_1/t^{v(a_1)})t^{\delta}. \end{aligned}$$

So, put $u' = (-1)^{r-r_0}(a_1/t^{v(a_1)})(t^\delta/a)w$, where $w \overset{\text{def}}{=} \prod_{\alpha\in A-\{0\}} \alpha \in R^\times$, and $u = (u')^{-\frac{m}{p-1}p^{r-r_0+1}}$, then we have $f'_{2,r-r_0}(T) = aw^{-1}$. Now, we put $f_2 \overset{\text{def}}{=} f_{2,r-r_0}$.

Finally, put $f \overset{\text{def}}{=} f_2 \circ \phi_A$. Then, $f$ is a monic, integral, superseparable polynomial in $K[T]$ with $\deg(f) = \deg(f_2)\deg(\phi_A) = mp^{r-r_0+1}\sharp(A) = mp^{r+1}$, $f' = f'_2\phi'_A = (aw^{-1})w = a$, and $K_f = K(A) \subset L$. Finally, by the above construction, we see that $f$ is in the form of (a superseparable polynomial with degree $mp$) $\circ$ (an additive polynomial with degree $p^r$). As $m \geq m_{K,n} > 1$ and $r > r_0 \geq 0$, this implies $\mathrm{def}(f) \geq p^{r+1} - p^r$. This completes the proof. $\square$

*Remark* (1.19). So far, we have assumed that $K$ is a complete discrete valuation field (of characteristic $p$). However, this assumption is superfluous. More specifically, (1.4), (1.5), (1.11), (1.13), (1.15), (1.16), and (1.18) remain valid if we replace this assumption by the weaker assumption that $K$ is henselian (of characteristic $p$), and (1.10) remains valid if we replace the phrase 'completion' by 'henselization'. Indeed, the proof of the henselian case is just similar to the complete case.

Moreover, among these, (1.11), (1.13), (1.15) (except that we need to delete the phrase 'integral' in (i)), (1.16) (except that we need to delete the phrase 'integral' in (i)), and (1.18)(i) remain valid, if we only assume that $K$ is a large field (of characteristic $p$) in the sense of [Pop]. (In particular, we do not have to assume that $K$ is equipped with a discrete valuation.) Indeed, we see that these statements can be formulated in terms of the existence of $K$-rational points of $K$-varieties. The validity of the complete case implies that these varieties admit $K((t))$-rational points. Now, the large case follows directly from one of the equivalent definitions of large fields (see [Pop], Proposition 1.1, (5)).

## §2. Unramified extensions with prescribed local extensions.

In this §, we use the following new notation. Let $C$ be a noetherian, normal, integral, separated $\mathbb{F}_p$-scheme of dimension 1. We denote by $K$ the rational function field of $C$, and fix an algebraic closure $\overline{K}$ of $K$. We denote by $K^{\mathrm{sep}}$ and $G = G_K$ the separable closure of $K$ in $\overline{K}$ and the absolute Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ of $K$, respectively. Let $\Sigma_C$ be the set of closed points of $C$. For each $v \in \Sigma_C$, we denote by $R_v$ the completion of the local ring $\mathcal{O}_{C,v}$. This is a complete discrete valuation ring. We denote by $K_v$, $\mathfrak{m}_v$ and $k_v$ the field of fractions of $R_v$, the maximal ideal of $R_v$ and the residue field $R_v/\mathfrak{m}_v$ of $R_v$, respectively. We fix an algebraic closure $\overline{K}_v$ of $K_v$, and denote by $K_v^{\mathrm{sep}}$ and $G_v = G_{K_v}$ the separable closure of of $K_v$ in $\overline{K}_v$ and the absolute Galois group $\mathrm{Gal}(K_v^{\mathrm{sep}}/K_v)$, respectively.

Definition. We refer to a tuple $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$ as a base scheme data, if $C$ is as above, $\Sigma$ is a (possibly empty) finite subset of $\Sigma_C$; and, for each $v \in \Sigma$, $L_v$ is a (possibly infinite) normal subextension of $\overline{K}_v$ over $K_v$, such that $L_v \cap K_v^{\mathrm{sep}}$ is $v$-adically dense in $L_v$. (For example, this last condition is satisfied if either $L_v/K_v$ is Galois or $L_v = \overline{K}_v$.)

If, moreover, $C$ is a normal, geometrically integral curve over a field $k$ of characteristic $p$, we refer to $\mathcal{C}$ as a base curve data over $k$.

For a base scheme data $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$, we put $B = B_{\mathcal{C}} \overset{\mathrm{def}}{=} C - \Sigma$. If, moreover, $B$ is affine, then we put $R = R_{\mathcal{C}} \overset{\mathrm{def}}{=} \Gamma(B, \mathcal{O}_B)$, so that $R$ is a Dedekind domain and that $B = \mathrm{Spec}(R)$.

We say that a base scheme data $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$ is finite, if $L_v$ is a finite extension of $K_v$ for each $v \in \Sigma$. (In this case, $L_v$ is automatically Galois over $K_v$.)

Definition. Let $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$ be a base scheme data. Let $K'$ be an extension of $K$ contained in $\overline{K}$. Then, we say that $K'$ is $\mathcal{C}$-distinguished (resp. $\mathcal{C}$-admissible), if the integral closure $C'$ of $C$ in $K'$ is étale over $B$; and, for each $v \in \Sigma$ and each embedding $\iota : \overline{K} \hookrightarrow \overline{K}_v$ over $K$, we have $\iota(K')K_v = L_v$ (resp. $\iota(K')K_v \subset L_v$).

Theorem (2.1). *Let $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$ be a finite base scheme data, and assume that $C$ is affine. Then, there exists a $\mathcal{C}$-distinguished finite Galois extension $K'/K$.*

*Proof.* For each $v \in \Sigma$, take a positive integer $m_{L_v/K_v}$ as in (1.18)(i), and let $m$ be any common multiple of $m_{L_v/K_v}$ ($v \in \Sigma$). Then, for each $v \in \Sigma$, there exists a superseparable polynomial $f_v(T) \in K_v[T]$ of special type and with degree $mp$, such that $L_v = (K_v)_{f_v}$.

Now, observe that $R$ is dense in $\prod_{v\in\Sigma} K_v$. (This follows essentially from the Chinese Remainder Theorem for the Dedekind domain $\Gamma(C, \mathcal{O}_C)$.) From this, we can take a superseparable polynomial $f(T) \in R[T]$ of special type and with degree $mp$, which is arbitrarily close to $f_v$ for each $v \in \Sigma$. Then, we have $(K_v)_f = (K_v)_{f_v} = L_v$. Or, equivalently, $K_f \otimes_K K_v$ is isomorphic to a direct product of copies of $L_v$ over $K_v$. On the other hand, for each $v \in \Sigma_C - \Sigma$, $f \bmod \mathfrak{m}_v$ is a separable polynomial over $k_v$, since $f$ is of special type. From this, we see that $K_f$ is unramified at $v$. Thus, $K' \overset{\mathrm{def}}{=} K_f$ satisfies all the desired properties. $\square$

Definition. Let $F$ be a field. We denote by $F^{\mathrm{sep}}$ and $G_F$ a separable closure of $F$ and the absolute Galois group $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ of $F$, respectively. For each prime number $l$, we define $F(l)$ to be the union of finite Galois extensions $F'$ of

$F$ in $F^{\mathrm{sep}}$ with $\mathrm{Gal}(F'/F) \simeq (\mathbb{Z}/l\mathbb{Z})^n$ for some $n$. Thus, $F(l)$ corresponds via Galois theory to the closed subgroup $G_F(l) \stackrel{\mathrm{def}}{=} \overline{[G_F, G_F](G_F)^l}$ of $G_F$ (which coincides with the kernel of $G_F \twoheadrightarrow G_F^{\mathrm{ab}}/(G_F^{\mathrm{ab}})^l$).

DEFINITION. Let $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$ be a base scheme data and $\Sigma_\infty$ a subset of $\Sigma$. Let $K'$ be an extension of $K$ contained in $\overline{K}$. Then, we say that $K'$ is nearly $\mathcal{C}$-distinguished (resp. nearly $\mathcal{C}$-admissible) with respect to $\Sigma_\infty$, if the integral closure $C'$ of $C$ in $K$ is étale over $B$; for each $v \in \Sigma - \Sigma_\infty$ and each embedding $\iota : \overline{K} \hookrightarrow \overline{K}_v$ over $K$, we have $\iota(K')K_v = L_v$ (resp. $\iota(K')K_v \subset L_v$); and, for each $v \in \Sigma_\infty$ and each embedding $\iota : \overline{K} \hookrightarrow \overline{K}_v$ over $K$, we have $L_v \subset \iota(K')K_v \subset L_v(p)$ (resp. $\iota(K')K_v \subset L_v(p)$).

THEOREM (2.2). *Let $k$ be a field of characteristic $p$, and $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$ a finite base curve data over $k$. Let $\Sigma_\infty$ be a subset of $\Sigma$, and assume that $C - \Sigma_\infty$ is affine. Then, there exists a finite Galois extension $K'/K$ that is nearly $\mathcal{C}$-distinguished with respect to $\Sigma_\infty$.*

*Proof.* Let $C^*$ be the normal, geometrically integral compactification of $C$, and put $\Sigma^* \stackrel{\mathrm{def}}{=} \Sigma \cup (\Sigma_{C^*} - \Sigma_C)$ and $\Sigma^*_\infty \stackrel{\mathrm{def}}{=} \Sigma_\infty \cup (\Sigma_{C^*} - \Sigma_C)$. Moreover, for each $v \in \Sigma_{C^*} - \Sigma_C$, we choose any finite Galois extension $L_v$ of $K_v$ (say, $L_v = K_v$). Then, replacing $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$ by $(C^*, \Sigma^*, \{L_v\}_{v\in\Sigma^*})$ and $\Sigma_\infty$ by $\Sigma^*_\infty$, we may assume that $C$ is proper over $k$. In this case, we have $\Sigma_\infty \neq \emptyset$, since $C - \Sigma_\infty$ is affine.

For each $v \in \Sigma$, take a positive integer $m_{L_v/K_v}$ as in (1.18)(i), and let $m$ be any common multiple of $m_{L_v/K_v}$ ($v \in \Sigma - \Sigma_\infty$), $pm_{L_v/K_v}$ ($v \in \Sigma_\infty$) and 2. Then, for each $v \in \Sigma - \Sigma_\infty$ (resp. $v \in \Sigma_\infty$), there exists a superseparable polynomial $f_v(T) \in K_v[T]$ of special type and with degree $mp$ (resp. $m$), such that $L_v = (K_v)_{f_v}$.

Now, let $v \in \Sigma - \Sigma_\infty$. Then, for each polynomial $f_{1,v}(T) \in K_v[T]$ with degree $mp$ which is sufficiently close to $f_v(T)$, we have $(K_v)_{f_{1,v}} = (K_v)_{f_v} = L_v$. More precisely, we can take (sufficiently small) $n_v \in \mathbb{Z}$ and (sufficiently large) $m_v \in \mathbb{Z}$ with $n_v < m_v$, so that every coefficient of $f_v$ belongs to $\mathfrak{m}_v^{n_v}$, and that, if every coefficient of $f_{1,v} - f_v$ belongs to $\mathfrak{m}_v^{m_v}$, then we have $(K_v)_{f_{1,v}} = (K_v)_{f_v}$.

On the other hand, let $v \in \Sigma_\infty$. Then, similarly as above, we can take (sufficiently small) $n_v \in \mathbb{Z}$ and (sufficiently large) $m_v \in \mathbb{Z}$ with $n_v < m_v$, so that every coefficient of $f_v$ belongs to $\mathfrak{m}_v^{n_v}$, and that, for each polynomial $f_{1,v}(T) \in K_v[T]$ with degree $m$, if every coefficient of $f_{1,v} - f_v$ belongs to $\mathfrak{m}_v^{m_v}$, then we have $(K_v)_{f_{1,v}} = (K_v)_{f_v}$. Moreover, replacing $n_v$ and $m_v$ if necessary, we may assume that, for each monic polynomial $f_{1,v}(T) \in K_v[T]$ with degree $m$ whose constant term is 0, if every coefficient of $f_{1,v} - f_v$ belongs to $\mathfrak{m}_v^{m_v}$, then we have $(K_v)_{f_{1,v}} = (K_v)_{f_v}$ and there exists a bijection $\iota : \mathrm{roots}(f_v) \xrightarrow{\sim} \mathrm{roots}(f_{1,v})$, such that, for each $\alpha \in \mathrm{roots}(f_v)$, $v(\iota\alpha) = v(\alpha)$, $\mu(f_{1,v}, \iota(\alpha)) = \mu(f_v, \alpha)$, and $f'_{1,v}(\iota(\alpha)) \sim f'_v(\alpha) = 1$. (For the notations $\mu(-,-)$ and $\sim$, see §1.) Now, we let $d_v$ denote the minimal non-negative integer satisfying

$$\begin{aligned}\mu(f_v,\alpha) &< \min\left(d_v - v(f_v'(\alpha)) + \frac{1}{p}v(\alpha), \frac{p}{p-1}(d_v - v(f_v'(\alpha)))\right)\\ &= \min\left(d_v + \frac{1}{p}v(\alpha), \frac{p}{p-1}d_v\right)\end{aligned}$$

for all $\alpha \in \mathrm{roots}(f_v)$.

Lemma (2.3). *Let $P_1,\dots,P_r$ be distinct closed points of $C$, and, for each $i = 1,\dots,r$, let $a_i$ and $b_i$ be integers with $a_i \geq b_i$. If $b_1[k_{P_1} : k] + \cdots + b_r[k_{P_r} : k] > 2p_a(C) - 2$, then the natural map $\Gamma(C, \mathcal{O}_C(a_1P_1 + \cdots + a_rP_r)) \to \mathfrak{m}_{P_1}^{-a_1}/\mathfrak{m}_{P_1}^{-b_1} \oplus \cdots \oplus \mathfrak{m}_{P_r}^{-a_r}/\mathfrak{m}_{P_r}^{-b_r}$ is surjective. Here, $p_a(C)$ denotes the arithmetic genus of $C$.*

*Proof.* This follows from [CFHR], Theorem 1.1. $\square$

We fix a sufficiently large integer $N$ satisfying

$$\left(p(p-1)\sum_{v\in\Sigma_\infty}[k_v : k]\right)N - \sum_{v\in\Sigma}[k_v : k]m_v > 2p_a(C) - 2 \tag{2.4}$$

and

$$(mp-1)(p-1)N \geq \max\{d_v \mid v \in \Sigma_\infty\}(\geq 0), \tag{2.5}$$

and, for each $v \in \Sigma_\infty$, choose any $e_v \in K_v$ with $v(e_v) = N$.

Now, put

$$g_v(T) \stackrel{\text{def}}{=} \begin{cases} f_v(T), & v \in \Sigma - \Sigma_\infty,\\ e_v^{-mp(p-1)}f_v(-e_v^{p(p-1)}T^p) + T, & v \in \Sigma_\infty.\end{cases}$$

Then, $g_v(T)$ is a superseparable polynomial in $K_v[T]$ of special type and with degree $mp$. (For $v \in \Sigma_\infty$, use the assumption that $2 \mid m$.) So, by (2.3) and (2.4), we see that there exists a superseparable polynomial $g(T) \in R[T]$ of special type and with degree $mp$, such that every coefficient of $g(T) - g_v(T)$ belongs to $\mathfrak{m}_v^{m_v}$ (resp. $\mathfrak{m}_v^{-p(p-1)N+m_v}$) for $v \in \Sigma - \Sigma_\infty$ (resp. $v \in \Sigma_\infty$).

We put $K' \stackrel{\text{def}}{=} K_g$. Just as in the proof of (2.1), $K'$ satisfies the desired property for $v \in \Sigma - \Sigma_\infty$ and $v \in \Sigma_C - \Sigma$. So, we shall observe what happens at $v \in \Sigma_\infty$. We put $g_{e_v}(T) \stackrel{\text{def}}{=} e_v^{mp(p-1)}g(-e_v^{-(p-1)}T)$. Or, writing $g(T) = T + k(T^p)$, we have $g_{e_v}(T) \stackrel{\text{def}}{=} -e_v^{(mp-1)(p-1)}T + k_v(T^p)$, where $k_v(T) \stackrel{\text{def}}{=} e_v^{mp(p-1)}k(-e_v^{-(p-1)p}T^p)$. By the choice of $g$, every coefficient of $g(T) - g_v(T)$ belongs to $\mathfrak{m}_v^{-p(p-1)N+m_v}$, hence every coefficient of $g_{e_v}(T) - (f_v(T^p) - e_v^{(mp-1)(p-1)}T)$ belongs to $e_v^{p(p-1)}\mathfrak{m}_v^{-p(p-1)N+m_v} = \mathfrak{m}_v^{m_v}$. Or, equivalently, every coefficient of $k_v - f_v$ belongs to $\mathfrak{m}_v^{m_v}$. Thus, we may apply the preceding argument to $f_{1,v}=k_v$. Since, moreover, $v(-e_v^{(mp-1)(p-1)})=(mp-1)(p-1)N\geq d_v$ by (2.5), we may apply (1.5) to $g_{e_v}(T)=-e_v^{(mp-1)(p-1)}T+k_v(T^p)$. Then, firstly, we have $(K_v)_{g_{e_v}}\supset (K_v)_{k_v}=(K_v)_{f_v}=L_v$. Secondly, for each $\alpha_1\in\mathrm{roots}(k_v)$, $(-(-e_v^{(mp-1)(p-1)})/k_v'(\alpha_1))\sim(e_v^{mp-1})^{p-1}$ belongs to $((K_v)_{k_v}^\times)^{p-1}$. Thus, we have $M_{g_{e_v}}=(K_v)_{k_v}$. Thirdly, since $\mathrm{Gal}((K_v)_{g_{e_v}}/M_{g_{e_v}})$ is a subgroup of $(C_p)^{I_m}$, we have $(K_v)_{g_{e_v}}\subset M_{g_{e_v}}(p)$. Combining these, we obtain $L_v\subset(K_v)_{g_{e_v}}\subset L_v(p)$. Finally, since $\mathrm{roots}(g_{e_v})=-e_v^{p-1}\,\mathrm{roots}(g)$, we have $(K_v)_{g_{e_v}}=(K_v)_g$. Thus, $K'=K_g$ satisfies the desired property at $v\in\Sigma_\infty$. This completes the proof. $\square$

## §3. Main results.

In this §, we use the following notation. Let $k$ be an (a possibly infinite) algebraic extension of $\mathbb{F}_p$ and $C$ a smooth, geometrically connected (or, equivalently, normal, geometrically integral) curve over $k$. In particular, $C$ is a noetherian, normal, integral, separated $\mathbb{F}_p$-scheme of dimension 1, and we use the notations introduced at the beginning of §2 for this $C$. Among other things, see §2 for the definition of base curve data.

Definition. (i) We refer to a tuple $\mathcal{S}=(\mathcal{C},f:X\to B,\{\Omega_v\}_{v\in\Sigma})$ as a (smooth) Skolem data, if $\mathcal{C}=(C,\Sigma,\{L_v\}_{v\in\Sigma})$ is a base curve data; $B=B_{\mathcal{C}}$; $f:X\to B$ is a smooth, surjective morphism whose generic fiber $X_K$ is geometrically irreducible; and, for each $v\in\Sigma$, $\Omega_v$ is a non-empty, $v$-adically open, $G_v$-stable subset of $X(L_v)$. (Observe that $X$ is automatically irreducible.)
(ii) We refer to a tuple $\mathcal{B}=(\mathcal{C},Y_1,\dots,Y_r\subset\mathbf{P}(\mathcal{E}),\{\check{\Omega}_v\}_{v\in\Sigma})$ as a Bertini data, if $\mathcal{C}=(C,\Sigma,\{L_v\}_{v\in\Sigma})$ is a base curve data; $\mathcal{E}$ is a locally free sheaf of finite rank $\neq 0$ on $B$; $r\geq 0$; $Y_i$ is an irreducible, reduced, closed subscheme of $\mathbf{P}(\mathcal{E})$; and, for each $v\in\Sigma$, $\check{\Omega}_v$ is a non-empty, $v$-adically open, $G_v$-stable subset of $\mathbf{P}(\check{\mathcal{E}})(L_v)$, where $\check{\mathcal{E}}\stackrel{\mathrm{def}}{=}\mathcal{H}om_{\mathcal{O}_B}(\mathcal{E},\mathcal{O}_B)$.

For a Bertini data $\mathcal{B}=(\mathcal{C},Y_1,\dots,Y_r\subset\mathbf{P}(\mathcal{E}),\{\check{\Omega}_v\}_{v\in\Sigma})$, we define $Y_i^{\mathrm{sm}}$ $(i=1,\dots,r)$ to be the set of points of $Y_i$ at which $Y_i\to B$ is smooth. This is an (a possibly empty) open subset of $Y_i$, and we regard it as an open subscheme of $Y_i$.

Definition. (i) Let $\mathcal{S}=(\mathcal{C},f:X\to B,\{\Omega_v\}_{v\in\Sigma})$ be a Skolem data with $\mathcal{C}=(C,\Sigma,\{L_v\}_{v\in\Sigma})$. Then, an $\mathcal{S}$-admissible quasi-section is a $B$-morphism $s:B'\to X$, where $B'$ is the integral closure of $B$ in a finite, $\mathcal{C}$-admissible extension $K'$ of $K$, such that, for each $v\in\Sigma$, the image of $B'_{L_v}\stackrel{\mathrm{def}}{=}B'\times_B L_v$ in $X_{L_v}\stackrel{\mathrm{def}}{=}X\times_B L_v$ is contained in $\Omega_v$ $(\subset X(L_v)=X_{L_v}(L_v))$.
(ii) Let $\mathcal{B}=(\mathcal{C},Y_1,\dots,Y_r\subset\mathbf{P}(\mathcal{E}),\{\check{\Omega}_v\}_{v\in\Sigma})$ be a Bertini data with $\mathcal{C}=(C,\Sigma,\{L_v\}_{v\in\Sigma})$. Then, a $\mathcal{B}$-admissible quasi-hyperplane is a hyperplane $H$ in $\mathbf{P}(\mathcal{E})_{B'}$, where $B'$ is the integral closure of $B$ in a finite, $\mathcal{C}$-admissible extension $K'$ of $K$, such that (a) for each $i=1,\dots,r$, each geometric point $\overline{b}$ of $B'$ and each irreducible component $P$ of $Y_{i,\overline{b}}$, we have $P\cap H_{\overline{b}}\subsetneq P$; (b) for each $i=1,\dots,r$, the scheme-theoretic intersection $(Y_i^{\mathrm{sm}})_{B'}\cap H$ (in $\mathbf{P}(\mathcal{E})_{B'}$) is smooth over $B'$; (c) for each $i=1,\dots,r$ and each irreducible component $P$

of $Y_{i,\overline{K}}$ with $\dim(P) \geq 2$, $P \cap H_{\overline{K}}$ is irreducible; and (d) for each $v \in \Sigma$, the image of $B'_{L_v}$ in $\mathbf{P}(\check{\mathcal{E}})_{L_v}$ by the base change to $L_v$ of the classifying morphism $[H] : B' \to \mathbf{P}(\check{\mathcal{E}})$ over $B$ is contained in $\check{\Omega}_v$ ($\subset \mathbf{P}(\check{\mathcal{E}})(L_v) = \mathbf{P}(\check{\mathcal{E}})_{L_v}(L_v)$).

Definition. Let $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$ be a base curve data over $k$.
(i) We denote by $R_{L_v}$, $\mathfrak{m}_{L_v}$, and $k_{L_v}$ the integral closure of $R_v$ in $L_v$, the maximal ideal of $R_{L_v}$, and the residue field $R_{L_v}/\mathfrak{m}_{L_v}$, respectively.
(ii) We say that $\mathcal{C}$ satisfies condition (RI), if $[k_{L_v} : \mathbb{F}_p] = \infty$ for all $v \in \Sigma$. (Here, 'RI' means 'residually infinite'.)

Now, the following are the main results of the present paper.

Theorem (3.1). *Let $\mathcal{S} = (\mathcal{C}, f : X \to B, \{\Omega_v\}_{v\in\Sigma})$ be a Skolem data with $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$, and assume that $C$ is affine and that* (RI) *holds. Then, there exists an $\mathcal{S}$-admissible quasi-section.*

Theorem (3.2). *Let $\mathcal{B} = (\mathcal{C}, Y_1, \dots, Y_r \subset \mathbf{P}(\mathcal{E}), \{\check{\Omega}_v\}_{v\in\Sigma})$ be a Bertini data with $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$, and assume that $C$ is affine and that* (RI) *holds. Then, there exists a $\mathcal{B}$-admissible quasi-hyperplane.*

The aim of the rest of this § is to prove these theorems, together and step by step. From now on, we put $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$, $\mathcal{S} = (\mathcal{C}, f : X \to B, \{\Omega_v\}_{v\in\Sigma})$, and $\mathcal{B} = (\mathcal{C}, Y_1, \dots, Y_r \subset \mathbf{P}(\mathcal{E}), \{\check{\Omega}_v\}_{v\in\Sigma})$, and assume always that $C$ is affine and that (RI) holds.

Definition. We say that a Skolem data $\mathcal{S} = (\mathcal{C}, f : X \to B, \{\Omega_v\}_{v\in\Sigma})$ is essentially rational, if $\Omega_v \cap X(K_v) \neq \emptyset$ for each $v \in \Sigma$.

*Step 1.* Assume that $\mathcal{S}$ is essentially rational, and that $X$ is an open subscheme of $\mathbf{P}^1_B$. Then, there exists an $\mathcal{S}$-admissible quasi-section.

*Proof.* We put $W \stackrel{\text{def}}{=} \mathbf{P}^1_B - X$. By shrinking $X$ if necessary, we may assume that $W$ is purely of codimension 1 in $\mathbf{P}^1_B$ and that $W$ contains the infinity section $\infty_B$ of $\mathbf{P}^1_B$. Next, we put $\tilde{R} \stackrel{\text{def}}{=} \Gamma(C, \mathcal{O}_C)$, which is a Dedekind domain contained in $R = \Gamma(B, \mathcal{O}_B)$, such that $C = \operatorname{Spec}(\tilde{R})$.

Since $\operatorname{Pic}(C)$ is a torsion group (cf. [Mo2], 1.9), there exists $n > 0$, such that $(\mathfrak{m}_v \cap \tilde{R})^n$ is a principal ideal of $\tilde{R}$ for each $v \in \Sigma$. In particular, there exists $\varpi \in \tilde{R}$, such that $(\prod_{v\in\Sigma}(\mathfrak{m}_v \cap \tilde{R}))^n = \tilde{R}\varpi$. On the other hand, since $\mathbf{A}^1(R)$ is dense in $\prod_{v\in\Sigma} \mathbf{P}^1(K_v)$, there exists $x \in \mathbf{A}^1(R)(= R)$, such that $x \in \Omega_v \cap X(K_v)$ for each $v \in \Sigma$. (Here, we have used the assumption that $\mathcal{S}$ is essentially rational.) Since $\Omega_v$ is $v$-adically open in $X(L_v)$, there exists $l_v \geq 0$, such that $x + (\mathfrak{m}_v R_{L_v})^{l_v} \subset \Omega_v$. Finally, take a sufficiently large integer $M$, such that $nM \geq l_v$ for each $v \in \Sigma$ and that $nM > v(\omega - x)$ for each $v \in \Sigma$ and each $\omega \in W(\overline{K}_v) - \{\infty\}$.

Now, let $S$ denote the coordinate of $\mathbf{A}^1_B$ that we are using. Since $\varpi \in R^\times$ and $x \in R$, the coordinate change $S \to T \stackrel{\text{def}}{=} (S-x)/\varpi^M$ gives an automorphism of $\mathbf{P}^1_B$ that fixes the infinity section $\infty_B$. (More sophisticatedly, this corresponds to a certain blowing-up(-and-down) process in the fibers of $\mathbf{P}^1_C \to C$ at $\Sigma$.)

From now, we shall use this new coordinate $T$. Then, by the choice of $(\varpi, x, M)$, we have $R_{L_v} = \mathbf{A}^1(R_{L_v}) \subset \Omega_v$ for each $v \in \Sigma$ and $v(\omega) < 0$ for each $v \in \Sigma$ and $\omega \in W(\overline{K}_v) - \{\infty\}$.

We define $\tilde{W}$ to be the closure of $W$ in $\mathbf{P}^1_C$, which contains the infinity section $\infty_C$ of $\mathbf{P}^1_C$. By the above choice of coordinate, we have $\tilde{W} \cap \mathbf{P}^1_{k_v} \subset \infty_{k_v}$ for each $v \in \Sigma$. From now, we regard $\tilde{W}$ as a reduced closed subscheme (or, as a divisor) of $\mathbf{P}^1_C$. By [Mo2], Théorème 1.3, $\mathrm{Pic}(\tilde{W})$ is a torsion group. So, let $s_0$ be the order of the class of the line bundle $\mathcal{O}_{\mathbf{P}^1_C}(1)|_{\tilde{W}}$ on $\tilde{W}$. On the other hand, let $e$ be the degree of $\tilde{W}$ over $C$. Now, choose a positive integer $s$ which is divisible by $s_0$ and greater than $e-2$. As in [Mo2], proof of Théorème 1.7, Étape VIII, consider the exact sequence

$$0 \to \mathcal{O}_{\mathbf{P}^1_C}(s)(-\tilde{W}) \to \mathcal{O}_{\mathbf{P}^1_C}(s) \to \mathcal{O}_{\mathbf{P}^1_C}(s)|_{\tilde{W}} \to 0,$$

which induces the following long exact sequence:

$$\cdots \to H^0(\mathbf{P}^1_C, \mathcal{O}_{\mathbf{P}^1_C}(s)) \to H^0(\tilde{W}, \mathcal{O}_{\mathbf{P}^1_C}(s)|_{\tilde{W}}) \\ \to H^1(\mathbf{P}^1_C, \mathcal{O}_{\mathbf{P}^1_C}(s)(-\tilde{W})) \to \cdots.$$

Since $s_0 \mid s$, we have $\mathcal{O}_{\mathbf{P}^1_C}(s)|_{\tilde{W}} \simeq \mathcal{O}_{\tilde{W}}$, so that there exists an element $g_0 \in H^0(\tilde{W}, \mathcal{O}_{\mathbf{P}^1_C}(s)|_{\tilde{W}})$ which generates $\mathcal{O}_{\mathbf{P}^1_C}(s)|_{\tilde{W}}$. On the other hand, since $s > e-2$, we see that $H^1(\mathbf{P}^1_C, \mathcal{O}_{\mathbf{P}^1_C}(s)(-\tilde{W}))$ (which is the dual of $H^0(\mathbf{P}^1_C, \mathcal{O}_{\mathbf{P}^1_C}(-2-s)(\tilde{W}))$) vanishes. Thus, there exists an element $g \in H^0(\mathbf{P}^1_C, \mathcal{O}_{\mathbf{P}^1_C}(s))$ that maps to $g_0$. Then, we have $\mathrm{Supp}(g) \cap \tilde{W} = \emptyset$. In particular, we have $\mathrm{Supp}(g) \cap \infty_C = \emptyset$.

We may identify $H^0(\mathbf{P}^1_C, \mathcal{O}_{\mathbf{P}^1_C}(s))$ with the set of polynomials in $\tilde{R}[T]$ with degree $\leq s$. Then, since $\mathrm{Supp}(g) \cap \infty_C = \emptyset$, we see that $g$ is strictly of degree $s$ and that the coefficient $u$ of $T^s$ in $g = g(T)$ is an element of $\tilde{R}^\times$. So, replacing $g$ by $u^{-1}g$ (and $g_0$ by $u^{-1}g_0$), we may assume that $g$ is monic.

Next, since $\mathrm{Pic}(\mathbf{A}^1_C) = \mathrm{Pic}(C)$ is a torsion group, there exists an element $w(T) \in \tilde{R}[T]$, such that the zero locus of $w(T)$ in $\mathbf{A}^1_C$ coincides (set-theoretically) with $\tilde{W} \cap \mathbf{A}^1_C$. Recall that, for each $v \in \Sigma$ and each root $\omega$ of $w$ in $\overline{K}_v$, we have $v(\omega) < 0$. From this fact (and the fact that $\tilde{W} \cap \mathbf{A}^1_{k_v} \subsetneq \mathbf{A}^1_{k_v}$), we see that $w(0)$ is a unit in $R_v$ and that $w(T) \equiv w(0) \pmod{\mathfrak{m}_v}$. Moreover, since $k_v^\times$ is a torsion group, we may assume that $w(0) \equiv 1 \pmod{\mathfrak{m}_v}$ for each $v \in \Sigma$, replacing $w$ by a suitable power. Now, we define $d$ to be the degree of $w$.

First, assume $\Sigma \neq \emptyset$, and we shall apply (1.18)(ii) carefully. Let $n$ be as in the beginning of the proof. Then, there exists a positive integer $m_n$. We choose a positive integer $m$ to be a common multiple of $m_n$ and $s$. For this $m$, we obtain a positive real number $c_{K_v,n,m}$. We put $c_m \stackrel{\text{def}}{=} \max\{c_{K_v,n,m} \mid v \in \Sigma\}$.

We put $D \stackrel{\text{def}}{=} \frac{d}{p-1}$ and $E \stackrel{\text{def}}{=} \frac{p}{p-1} c_m mp$. We take a positive integer $t$, such that $p^t > D$. Next, since we are assuming the condition (RI) that $k_{L_v}$ is an infinite algebraic extension of $\mathbb{F}_p$, there exists a finite subfield of $k_{L_v}$ with arbitrarily large cardinality. So, we may take a finite subfield $\mathbb{F}_v$ of $k_{L_v}$, such that $p^{r_v} \stackrel{\text{def}}{=} \sharp(\mathbb{F}_v) > Ep^t$. Since $R_v$ is complete, $\mathbb{F}_v$ admits a canonical lifting in $R_{L_v}$, to which we refer again as $\mathbb{F}_v$. Now, take a positive integer $r > \max\{r_v(v \in \Sigma), t\}$.

Applying (1.18)(ii) to $L = L_v$, $A = \mathbb{F}_v$, $r$ as above, and $\nu = 0$, we see that there exists a positive integer $\delta_v$, such that $\delta_v \leq c_m mp^{r+1}/\sharp(\mathbb{F}_v) = c_m mp^{r-r_v+1}$ and that $\delta_v \equiv 0 \pmod{n}$. Since $\delta_v$ is divisible by $n$, $\mathfrak{a} \stackrel{\text{def}}{=} \prod_{v\in\Sigma}(\mathfrak{m}_v \cap \tilde{R})^{\delta_v}$ is a principal ideal of $\tilde{R}$. So, let $a \in \tilde{R}$ be a generator of $\mathfrak{a}$. Then, $v(a) = \delta_v$ for each $v \in \Sigma$. Now, the conclusion of (1.18)(ii) is that there exists a monic, integral, superseparable polynomial $f_v(T) \in K_v[T]$, such that $\deg(f_v) = mp^{r+1}$, $\operatorname{def}(f_v) \geq (p-1)p^r$, $f_v'(T) = a$ and $(K_v)_{f_v} = K_v\mathbb{F}_v \subset L_v$. Moreover, by using (1.4)(ii) and the Chinese Remainder Theorem (for the Dedekind domain $\tilde{R}$), we may assume that $f_v(T) \in \tilde{R}[T]$ and $f_v(T)$ does not depend on $v$. So, put $f(T) \stackrel{\text{def}}{=} f_v(T)$ for some (or, equivalently, all) $v \in \Sigma$, then, $f$ is monic, superseparable polynomial in $\tilde{R}[T]$, such that $\deg(f) = mp^{r+1}$, $\operatorname{def}(f) \geq (p-1)p^r$, $f'(T) = a$ and $(K_v)_f = K_v\mathbb{F}_v \subset L_v$ for each $v \in \Sigma$.

Next, assume $\Sigma = \emptyset$. In this case, we define $m$ to be any multiple of $s$, put $D \stackrel{\text{def}}{=} \frac{d}{p-1}$, take a positive integer $t$ with $p^t > D$ and a positive integer $r$ with $r > t$, and let $a$ be any element of $\tilde{R}^\times$. Now, we choose a monic superseparable polynomial $f(T) \in \tilde{R}[T] = R[T]$, such that $\deg(f) = mp^{r+1}$, $\operatorname{def}(f) \geq (p-1)p^r$, and $f'(T) = a$. (For example, put $f(T) = T^{mp^{r+1}} + aT$.)

Finally, we put

$$F(T) \stackrel{\text{def}}{=} g(T)^{\frac{m}{s}p^{r+1}} + w(T)^{p^{r-t}}(f(T) - g(T)^{\frac{m}{s}p^{r+1}}) \in \tilde{R}[T].$$

*Claim* (3.3). $F$ is monic of degree $mp^{r+1}$.

*Proof.* $f$ is monic with $\deg(f) = mp^{r+1}$ and $\operatorname{def}(f) \geq (p-1)p^r$. On the other hand, since $g$ is monic of degree $s$, $g^{\frac{m}{s}}$ is monic of degree $m$, hence $g^{\frac{m}{s}p^{r+1}}$ is monic of degree $mp^{r+1}$ and with 'defect' $\geq p^{r+1} \geq (p-1)p^r$. From these, we see that $f - g^{\frac{m}{s}p^{r+1}}$ has degree $\leq mp^{r+1} - (p-1)p^r$. Thus,

$$\begin{aligned}\deg(w^{p^{r-t}}(f - g^{\frac{m}{s}p^{r+1}})) &\leq p^{r-t}d + mp^{r+1} - (p-1)p^r \\ &< p^r dD^{-1} + mp^{r+1} - (p-1)p^r = mp^{r+1}.\end{aligned}$$

Since $g^{\frac{m}{s}p^{r+1}}$ is monic of degree $mp^{r+1}$ as we have already seen, we conclude that $F$ is monic of degree $mp^{r+1}$. $\square$

*Claim* (3.4). For each $v \in \Sigma$, any root $\alpha$ of $F$ in $\overline{K}_v$ is contained in $R_{L_v}$.

*Proof.* Since $w(T) \equiv 1 \pmod{\mathfrak{m}_v}$, we have $w(T)^{p^{r-t}} \equiv 1 \pmod{\mathfrak{m}_v^{p^{r-t}}}$. Thus,

$$F(T) \equiv g(T)^{\frac{m}{s}p^{r+1}} + (f(T) - g(T)^{\frac{m}{s}p^{r+1}}) = f(T) \pmod{\mathfrak{m}_v^{p^{r-t}}}.$$

Now, since $p^{r-t} > Ep^{r-r_v} = \frac{p}{p-1} c_m m p^{r-r_v+1} \geq \frac{p}{p-1}\delta_v$, we have $(K_v)_F = (K_v)_f \subset L_v$ by (1.4)(ii). This implies $\alpha \in L_v$. Since $F(T)$ is a monic polynomial in $\tilde{R}[T] \subset R_v[T]$, we have $\alpha \in R_{L_v}$, as desired. □

Let $\tilde{Z}$ be the zero locus of $F(T)$ in $\mathbf{A}^1_C$. By (3.3), $\tilde{Z}$ is closed in $\mathbf{P}^1_C$. We put $Z \stackrel{\text{def}}{=} \tilde{Z} \cap \mathbf{P}^1_B$.

*Claim* (3.5). (i) $Z \subset X$.
(ii) $Z$ is finite étale over $B$.

*Proof.* (i) On $(W \cap \mathbf{A}^1_B)^{\text{red}}$, we have $F(T) \equiv g(T)^{\frac{m}{s}p^{r+1}}$. Now, since the zero locus of $g$ in $\mathbf{A}^1_B$ is disjoint from $W \cap \mathbf{A}^1_B$, so is that of $F$, as desired.
(ii) By (3.3), $Z = \mathrm{Spec}(R[T]/(F(T)))$ is finite (and flat) over $R$. Since $F' = w^{p^{r-t}} f' = w^{p^{r-t}} a$ and $a \in R^\times$, the zero locus of $F'$ in $\mathbf{A}^1_B$ is (set-theoretically) contained in $W$. This, together with (i), implies that the zero loci of $F$ and $F'$ are disjoint from each other, as desired. □

Take an irreducible (or, equivalently, connected) component $B'$ of $Z$. By (3.5), we have a natural immersion $B' \hookrightarrow X$ over $B$, which we regard as a finite étale quasi-section of $X \to B$. Since $R_{L_v} \subset \Omega_v$, (3.4) implies that this quasi-section is $\mathcal{S}$-admissible. This completes the proof. □

Step 1 is the main step, and, roughly speaking, the rest of proof is only concerning how to reduce general cases to Step 1.

*Step 2.* Assume that $\mathcal{S}$ is essentially rational, and that $X$ is an open subscheme of $\mathbf{P}^n_B$ for some $n \geq 0$. Then, there exists an $\mathcal{S}$-admissible quasi-section.

*Proof.* If $n = 0$, we must have $X = B$, and the assertion clearly holds. So, assume $n \geq 1$.

Let $A$ be a commutative ring. We define $\mathbf{P}^n(A)^0$ to be $(\mathbf{A}^{n+1} - 0)(A)/A^\times$, where 0 denotes the section $(0, \dots, 0)$, regarded as a closed subscheme of $\mathbf{A}^{n+1}$. We define $\mathbf{P}^n(A)^{00}$ to be $\cup_{i=0}^n U_i(A)$, where $U_i(\simeq \mathbf{A}^n)$ is the standard open subset of $\mathbf{P}^n$. Then, we have $\mathbf{P}^n(A)^{00} \subset \mathbf{P}^n(A)^0 \subset \mathbf{P}^n(A)$. If $\mathrm{Pic}(A) = \{0\}$ (resp. $A$ is a local ring), then we have $\mathbf{P}^n(A)^0 = \mathbf{P}^n(A)$ (resp. $\mathbf{P}^n(A)^{00} = \mathbf{P}^n(A)^0 = \mathbf{P}^n(A)$). If $A$ is a Dedekind domain, we see that $\mathbf{P}^n(A)^0$ forms a $GL_{n+1}(A)$-orbit.

Now, observe that $\mathbf{P}^n(R)^{00} \cap X(K)$ is dense in $\prod_{v \in \Sigma} \mathbf{P}^n(K_v)$. ($X(R)$ may be empty, though.) So, there exists $x \in \mathbf{P}^n(R)^0 \cap X(K)$, such that $x \in \Omega_v \cap X(K_v)$ for each $v \in \Sigma$. (Note that $\mathcal{S}$ is essentially rational.) By changing the coordinates via the $GL_{n+1}(R)$-action, we may assume $x = [1 : 0 : \cdots : 0]$ ($\in U_0$).

Let $e_1, \dots, e_{n-1}$ be positive integers, and consider the $B$-morphism $i_{e_1,\dots,e_{n-1}} : \mathbf{A}^1_B \to U_0 = \mathbf{A}^n_B$, $t \mapsto (t^{e_1}, \dots, t^{e_{n-1}}, t)$. It is easy to see that $i_{e_1,\dots,e_{n-1}}$ is a closed immersion.

*Claim* (3.6). For some choice of $e_1, \dots, e_{n-1}$, $(i_{e_1,\dots,e_{n-1}})^{-1}(X)$ surjects onto $B$.

*Proof.* Denote by $T_1, \dots, T_n$ the coordinates of $U_0 = \mathbf{A}^n_B$. Then, there exist a finite number of polynomials $f_1, \dots, f_r \in R[T_1, \dots, T_n]$, such that the closed subset $\mathbf{A}^n_B - X$ of $\mathbf{A}^n_B$ coincides with the common zero locus of $f_1, \dots, f_r$. Since $\mathbf{A}^n_B \cap X$ surjects onto $B$ (as $X$ surjects onto $B$), we see that, for each $b \in B$, there exists $i = i_b \in \{1, \dots, r\}$, such that the image of $f_i$ in $k_b[T_1, \dots, T_r]$ is non-zero.

Lemma (3.7). *Let $S$ be a finite subset of $\mathbb{Z}^n$. Then, there exist positive integers $e_1, \dots, e_{n-1}$, such that the map $S \to \mathbb{Z}$, $(k_1, \dots, k_n) \mapsto e_1 k_1 + \cdots + e_{n-1} k_{n-1} + k_n$ is injective.*

*Proof.* Put $T \stackrel{\text{def}}{=} \{s - s' \mid s, s' \in S, s \neq s'\}$. This is a finite subset of $\mathbb{Z}^n$ that does not contain $0 = (0, \dots, 0)$. For each $t = (l_1, \dots, l_n) \in T$, consider the linear subspace $W_t$ of $\mathbf{A}^n_{\mathbb{Q}}$ defined by $l_1 x_1 + \dots l_n x_n = 0$. On the other hand, consider the hyperplane $H = \{(x_1, \dots, x_n) \mid x_n = 1\}$ of $\mathbf{A}^n_{\mathbb{Q}}$. As $H \not\subset W_t$, $H' \stackrel{\text{def}}{=} H - \cup_{t \in T} W_t$ is a non-empty open subset of $H$. Since the set $\{(e_1, \dots, e_{n-1}, 1) \mid e_1, \dots, e_{n-1} \in \mathbb{Z}_{>0}\}$ is Zariski dense in $H$ (as $\mathbb{Z}_{>0}$ is an infinite set), it must intersect non-trivially with $H'$. Take $(e_1, \dots, e_{n-1}, 1)$ in this intersection, then $e_1, \dots, e_{n-1}$ satisfies the desired property. $\square$

We define $S$ to be the set of elements $(k_1, \dots, k_n) \in (\mathbb{Z}_{\geq 0})^n$ such that the coefficient of $T_1^{k_1} \cdots T_n^{k_n}$ in $f_i$ is non-zero for some $i = 1, \dots, r$. Applying (3.7) to this $S$, we obtain $e_1, \dots, e_{n-1} \in \mathbb{Z}_{>0}$. Then, we see that, for each $b \in B$, there exists $i = i_b \in \{1, \dots, r\}$, such that the image of $f_i(T^{e_1}, \dots, T^{e_{n-1}}, T)$ in $k_b[T]$ is non-zero. This means that $(i_{e_1, \dots, e_{n-1}})^{-1}(X)$ surjects onto $B$, as desired. $\square$

Take $e_1, \dots, e_{n-1}$ as in (3.6), and put $\mathcal{S}' \stackrel{\text{def}}{=} (\mathcal{C}, (i_{e_1, \dots, e_{n-1}})^{-1}(X) \to B, \{(i_{e_1, \dots, e_{n-1}}(L_v))^{-1}(\Omega_v)\})$, where $i_{e_1, \dots, e_{n-1}}(L_v)$ denotes the map $\mathbf{A}^1(L_v) \to U_0(L_v) = \mathbf{A}^n(L_v)$ induced by $i_{e_1, \dots, e_{n-1}}$. Then, $\mathcal{S}'$ is an essentially rational Skolem data. (Observe that $0 \in \mathbf{A}^1(K)$ lies in $(i_{e_1, \dots, e_{n-1}}(L_v))^{-1}(\Omega_v)$.)

Now, by Step 1, there exists an $\mathcal{S}'$-admissible quasi-section. By composing this quasi-section with $i_{e_1, \dots, e_{n-1}}$, we obtain an $\mathcal{S}$-admissible quasi-section. This completes the proof. $\square$

*Remark* (3.8). The above argument that involves rational curves with higher degree was communicated to the author by a referee. The author's original argument, which is slightly more complicated, uses lines over finite extensions.

*Step 3.* Assume that $X$ is an open subscheme of $\mathbf{P}^n_B$ for some $n \geq 0$. Then, there exists an $\mathcal{S}$-admissible quasi-section.

*Proof.* For each $v \in \Sigma$, $\mathbf{P}^n(L_v \cap K_v^{\text{sep}})$ is $v$-adically dense in $\mathbf{P}^n(L_v)$. Accordingly, we have $\Omega_v \cap \mathbf{P}^n(L_v \cap K_v^{\text{sep}}) \neq \emptyset$. So, there exists a finite Galois subextension $M_v/K_v$ of $L_v/K_v$, such that $\Omega_v \cap X(M_v)$ is non-empty. Now, put $\mathcal{C}_1 \stackrel{\text{def}}{=} (C, \Sigma, \{M_v\}_{v \in \Sigma})$, which is a finite base curve data. By (2.1), there exists a $\mathcal{C}_1$-distinguished finite Galois extension $K'$ of $K$. We define $C'$ (resp. $B'$) to be the integral closure of $C$ (resp. $B$) in $K'$, and put $\Sigma' \stackrel{\text{def}}{=} C' - B'$, which is the inverse image of $\Sigma$ in $C'$. Let $v'$ be an element of $\Sigma'$ and $v$ the image of $v'$ in $\Sigma$. Then, we have $(K')_{v'} = M_v \subset L_v$. So, put $\mathcal{C}' \stackrel{\text{def}}{=} (C', \Sigma', \{L_v\}_{v' \in \Sigma'})$ and $\mathcal{S}' \stackrel{\text{def}}{=} (\mathcal{C}', X_{B'} \to B', \{\Omega_v\}_{v' \in \Sigma'})$. Then, $\mathcal{C}'$ is a base curve data (over the algebraic closure of $k$ in $K'$) such that $C'$ is affine and that (RI) holds, and $\mathcal{S}'$ is an essentially rational Skolem data such that $X_{B'}$ is an open subscheme of $\mathbf{P}^n_{B'}$. So, by Step 2, there exists an $\mathcal{S}'$-admissible quasi-section $B'' \to X_{B'}$. Now, the composite of this morphism and the natural projection $X_{B'} \to X$ gives an $\mathcal{S}$-admissible quasi-section. This completes the proof. $\square$

*Step 4.* Assume that $\mathcal{E} \simeq \mathcal{O}_B^{n+1}$, where $n+1$ is the rank of $\mathcal{E}$. Then, there exists a $\mathcal{B}$-admissible quasi-hyperplane.

*Proof.* For simplicity, we put $\mathbf{P} = \mathbf{P}(\mathcal{E})$ and $\check{\mathbf{P}} = \mathbf{P}(\check{\mathcal{E}})$. Let $I$ denote the incidence subscheme of $\mathbf{P} \times_B \check{\mathbf{P}}$, and let $p$ and $\check{p}$ be the natural projections $\mathbf{P} \times_B \check{\mathbf{P}} \to \mathbf{P}$ and $\mathbf{P} \times \check{\mathbf{P}} \to \check{\mathbf{P}}$, respectively. Both $p|_I$ and $\check{p}|_I$ are $\mathbf{P}^{N-1}$-bundles, hence, a fortiori, smooth.

Let $i = 1, \ldots, r$. Since $Y_i$ is an integral scheme and $B$ is a smooth curve, the morphism $Y_i \to B$ is either flat over $B$ or flat over $b_i$ for some closed point $b_i \in B$. We shall refer to the former (resp. latter) case as case 1 (resp. 2).

In case 1, let $\tilde{Y}_i$ be the normalization of $Y_i$ and $B_i$ the integral closure of $B$ in $\tilde{Y}_i$. Then, since the generic fiber of $\tilde{Y}_i \to B_i$ is geometrically irreducible, there exists a non-empty open subset $B_i'$ of $B_i$, such that each fiber of $\tilde{Y}_i \times_{B_i} B_i' \to B_i'$ is geometrically irreducible ([EGA4], Théorème (9.7.7)). We denote by $\Sigma_i$ the image of $B_i - B_i'$ in $B$, which is a finite set. We define $U_{i,1}$ to be the image of $(\tilde{Y}_i \times_{B_i} \check{\mathbf{P}}_{B_i}$ minus the inverse image of $I_{B_i})$ in $\check{\mathbf{P}}_{B_i}$, which is an open subset of $\check{\mathbf{P}}_{B_i}$, and define $U_{i,2}$ to be the complement in $\check{\mathbf{P}}$ of the image of $\check{\mathbf{P}}_{B_i} - U_{i,1}$, which is an open subset of $\check{\mathbf{P}}$. Moreover, for each $b \in \Sigma_i$, fix a geometric point $\bar{b}$ on $b$. Then, for each irreducible component $P$ of $Y_{i,\bar{b}}$, we put $U_{P,1}$ the image of $(P \times_{\bar{b}} \check{\mathbf{P}}_{\bar{b}}$ minus the inverse image of $I_{\bar{b}})$ in $\check{\mathbf{P}}_{\bar{b}}$, and define $T_{P,2}$ to be the image of $\check{\mathbf{P}}_{\bar{b}} - U_{P,1}$ in $\check{\mathbf{P}}_b$, which is a closed subset of $\check{\mathbf{P}}_b$. Now, put $U_i \stackrel{\text{def}}{=} U_{i,2} - \cup_{b \in \Sigma_i} \cup_P T_{P,2}$, which is an open subset of $\check{\mathbf{P}}$. In case 2, for each irreducible component $P$ of $Y_{i,\bar{b}_i}$, we define a closed subset $T_{P,2}$ of $\check{\mathbf{P}}_{b_i}$ just as above, and put $U_i \stackrel{\text{def}}{=} \check{\mathbf{P}} - \cup_P T_{P,2}$.

Now, we put $U \stackrel{\text{def}}{=} \cap_{i=1}^r U_i$. Let $\bar{b}$ be a geometric point on $B$, then, we see that a point of $U_{\bar{b}}$ corresponds to a hyperplane $H_{\bar{b}}$ of $\mathbf{P}_{\bar{b}}$ that satisfies condition (a) in the definition of $\mathcal{B}$-admissible quasi-hyperplane. In particular, $U_b$ is a non-empty open subset of $\check{\mathbf{P}}_b$ for each $b \in B$.

Next, for each $i = 1, \ldots, r$, let $((p|_I)^{-1}(Y_i^{\mathrm{sm}}))^{\text{non-sm}}$ be the set of points of $(p|_I)^{-1}(Y_i^{\mathrm{sm}})$ at which $(p|_I)^{-1}(Y_i^{\mathrm{sm}}) \to \check{\mathbf{P}}$ is not smooth. This is a closed subset of $(p|_I)^{-1}(Y_i^{\mathrm{sm}})$. Let $Z_i$ be the image of $((p|_I)^{-1}(Y_i^{\mathrm{sm}}))^{\text{non-sm}}$ in $\check{\mathbf{P}}$. Chevalley's theorem implies that $Z_i$ is a constructible subset of $\check{\mathbf{P}}$, and the usual Bertini theorem implies that, for each $b \in B$, $\check{\mathbf{P}}_b - Z_i$ contains a non-empty open subset of $\check{\mathbf{P}}_b$. From these, we observe that $V_i \stackrel{\text{def}}{=} \check{\mathbf{P}} - \overline{Z_i}$ satisfies that, for each $b \in B$, $(V_i)_b$ is a non-empty open subset of $\check{\mathbf{P}}_b$. We put $V \stackrel{\text{def}}{=} \cap_{i=1}^r V_i$. Then, for each $b \in B$, $V_b$ is a non-empty open subset of $\check{\mathbf{P}}_b$.

Next, let $P$ be an irreducible component of $Y_{i,\overline{K}}$ with $\dim(P) \geq 2$. Then, by a version of Bertini theorem ([J], Théorème 6.11, 3), there exists a non-empty open subset $W_{P,1}$ of $\check{\mathbf{P}}_{\overline{K}}$, such that, for each hyperplane $H_{\overline{K}}$ corresponding to a point of $W_{P,1}$, $P \cap H_{\overline{K}}$ is irreducible. We define $W_1$ to be the intersection of $W_{P,1}$ for irreducible components $P$ of $Y_{i,\overline{K}}$ with $\dim(P) \geq 2$, which is a non-empty open subset of $\check{\mathbf{P}}_{\overline{K}}$, and $T_2$ the image of $\check{\mathbf{P}}_{\overline{K}} - W_1$ in $\check{\mathbf{P}}_K$, which is a proper closed subset of $\check{\mathbf{P}}_K$. Moreover, we denote by $\overline{T}_2$ the closure of $T_2$ in $\check{\mathbf{P}}$. We see that $(\overline{T}_2)_b$ is a proper closed subset of $\check{\mathbf{P}}_b$ for each $b \in B$. Now, we put $W = \check{\mathbf{P}} - \overline{T}_2$. Then, for each $b \in B$, $W_b$ is a non-empty open subset of $\mathbf{P}_b$.

Now, we put $\check{X} \stackrel{\text{def}}{=} U \cap V \cap W$. This is an open subset of $\check{\mathbf{P}}$ that is surjectively mapped onto $B$. Put $\mathcal{S}' \stackrel{\text{def}}{=} (\mathcal{C}, \check{X} \to B, \{\check{\Omega}_v \cap \check{X}(L_v)\}_{v \in \Sigma})$. Then, $\mathcal{S}'$ is a Skolem data.

So, by Step 3 and the assumption that $\mathcal{E} \simeq \mathcal{O}_B^{n+1}$, there exists an $\mathcal{S}'$-admissible quasi-section $B' \to \check{X}$. By the choice of $\mathcal{S}'$, this section corresponds to a hyperplane $H$ of $\mathbf{P}_{B'}$, which satisfies all the conditions (a)–(d) in the definition of $\mathcal{B}$-admissible quasi-hyperplane. This completes the proof. $\square$

*Step 5.* Assume that $X$ is quasi-projective of relative dimension 1 over $B$. Then, there exists an $\mathcal{S}$-admissible quasi-section.

*Proof.* By assumption, we may assume that $X$ is a subscheme of $\mathbf{P}_B^n$ for some $n \geq 1$. We define $\overline{X}_1$ to be the closure of $X$ in $\mathbf{P}_B^n$, regarded as a reduced scheme. $\overline{X}_1$ is a projective flat integral curve over $B$, and $X$ is an open subscheme of $\overline{X}_1$. It is well-known that, after normalizations and blowing-ups outside $X$, $\overline{X}_1$ can be desingularized. Namely, there exists a birational projective morphism $\pi : \overline{X}_2 \to \overline{X}_1$, where $\overline{X}_2$ is a regular, integral scheme, such that $\pi^{-1}(X) \xrightarrow{\sim} X$. Since $X_{\overline{K}}$ is irreducible, so is $(\overline{X}_2)_{\overline{K}}$. Hence, by [EGA4], Théorème (9.7.7), there exists a non-empty open subset $B_1$ of $B$, such that each fiber of $X_{B_1} \to B_1$ is geometrically irreducible, and, in particular, irreducible. We put $\Sigma_1 \stackrel{\text{def}}{=} B - B_1$, which is a finite set.

Now, we introduce a new base curve data $\mathcal{C}_1 \stackrel{\text{def}}{=} (C, \Sigma \cup \Sigma_1, \{L_v\}_{v \in \Sigma} \cup \{K_v^{\text{ur}}\}_{v \in \Sigma_1})$, where $K_v^{\text{ur}}$ denotes the maximal unramified extension of the complete discrete valuation field $K_v$. Note that $\mathcal{C}_1$ satisfies (RI) and that $C$ is affine. Moreover, we put $\mathcal{S}_1 = \{\mathcal{C}_1, X_{B_1} \to B_1, \{\Omega_v\}_{v \in \Sigma} \cup \{X(R_{K_v^{\text{ur}}})\}_{v \in \Sigma_1}\}$. Since $X \to B$ is smooth surjective, we see that $X(R_{K_v^{\text{ur}}})$ is non-empty. Thus, $\mathcal{S}_1$ becomes a Skolem data. Now, suppose that there exists an $\mathcal{S}_1$-admissible quasi-section $B_1' \to X_{B_1}$. Then, firstly, the integral closure $B'$ of $B$ in $B_1'$ is finite étale over $B$. Secondly, as $\overline{X}_2 \to B$ is proper, $B_1' \to X_{B_1}$ extends to $B' \to \overline{X}_2$. Now, since $B_1' \to X_{B_1}$ is $\mathcal{S}_1$-admissible, we see that the image of $B' \to \overline{X}_2$ must be contained in $X$. Thus, we obtain an $\mathcal{S}$-admissible quasi-section $B' \to X$.

So, replacing $\mathcal{S}$ by $\mathcal{S}_1$, we may assume that each fiber of $\overline{X}_2 \to B$ is geometrically irreducible. Now, we put $\overline{X} \stackrel{\text{def}}{=} \overline{X}_2$.

Lemma (3.9). *Let $F$ be a field and $X$ a projective, geometrically integral $F$-scheme of dimension* 1*. We denote by $X'$ the normalization of $X_{\overline{F}}$, so that we have a natural morphism $\pi : X' \to X$. Then, there exists a natural number $N$, such that each invertible sheaf $L$ on $X$ with* $\deg(L) \geq N$ *is very ample, where* $\deg(L) \stackrel{\text{def}}{=} \deg(\pi^*(L))$.

*Proof.* This follows from [CFHR], Theorem 1.1. (We may take $N = 2p_a(X) + 1$.) $\square$

Now, take a natural number $N$ for $\overline{X}_K$ as in (3.9). We shall choose horizontal divisors $Y_1, Y_2, \dots$ of $\overline{X}$ inductively, as follows. Firstly, by [Mo3], Théorème 1.3, there exists a horizontal divisor $Y_1$ of $\overline{X}$, such that $Y_1$ is contained in $X$ and that, for each $v \in \Sigma$, $Y_1 \times_B \mathrm{Spec}(L_v)$ is a disjoint union of copies of $\mathrm{Spec}(L_v)$ and is contained in $\Omega_v$. Next, assume that we have defined $Y_1, \dots, Y_r$. Then, again by [Mo3], Théorème 1.3, there exists a horizontal divisor $Y_{r+1}$ of $\overline{X}$, such that $Y_{r+1}$ is contained in $X - \cup_{i=1}^r Y_i$ and that, for each $v \in \Sigma$, $Y \times_B \mathrm{Spec}(L_v)$ is a disjoint union of copies of $\mathrm{Spec}(L_v)$ and is contained in $\Omega_v - \cup_{i=1}^r Y_i(L_v)$. By construction, $Y_1, Y_2, \dots$ are disjoint from one another. Now, take $n$ so large that $\deg(Y_{1,K} + \cdots + Y_{n,K}) \geq N$, and we put $Y \stackrel{\text{def}}{=} Y_1 + \cdots + Y_n$. (Note that each $Y_i$ defines an invertible sheaf on $\overline{X}$, since it lies in the smooth locus.) Then, by (3.9), $Y_K$ is very ample. On the other hand, since each fiber of $\overline{X} \to B$ is geometrically irreducible, $Y$ itself is ample (cf. [Mo2], Proposition 4.3), hence there exists a natural number $m$ such that $mY$ is very ample. So, consider an embedding $\overline{X} \hookrightarrow \mathbf{P}^n_B$ with respect to the very ample divisor $mY$.

We put $D \stackrel{\text{def}}{=} \overline{X} - X$. Let $E_1, \dots, E_h$ be the irreducible components of $D$, which must be either an isolated point or a horizontal divisor, as $X \to B$ is surjective and each fiber of $\overline{X} \to B$ is irreducible. Next, for each $v \in \Sigma$, we define $\check{\Omega}'_v$ to be the subset of $\check{\mathbf{P}}^n(L_v)$ consisting of points corresponding to $L_v$-rational hyperplanes $H$ such that $\overline{X}_{L_v} \cap H$ is a disjoint union of $L_v$-rational points in $\Omega_v$ (whose cardinality must coincide with $\deg(mY_K)$). It is easy to show that $\check{\Omega}'_v$ is a $v$-adically open subset of $\check{\mathbf{P}}(L_v)$. Moreover, by using the fact that (not only $mY_K$ but also) $Y_K$ is very ample and that $Y_{L_v}$ is a disjoint union of $L_v$-rational points in $\Omega_v$, we see that $\check{\Omega}'_v$ is non-empty.

Now, we put $\mathcal{B}' \stackrel{\text{def}}{=} (\mathcal{C}, \overline{X}, E_1, \dots, E_h \subset \mathbf{P}^n_B, \{\check{\Omega}'_v\}_{v \in \Sigma})$, which becomes a Bertini data. As $\mathbf{P}^n_B = \mathbf{P}(\mathcal{O}_B^{n+1})$, we may apply Step 4 to this Bertini data $\mathcal{B}'$, to conclude that there exists a $\mathcal{B}'$-admissible quasi-hyperplane $H \subset \mathbf{P}^n_{B'}$. By condition (a), we see that $\overline{X}_{B'} \cap H$ is finite (as proper and quasi-finite) over $B$, and that $E_{i,B'} \cap H = \emptyset$ for each $i = 1, \dots, h$, hence $D_{B'} \cap H = \emptyset$, or, equivalently, $\overline{X}_{B'} \cap H = X_{B'} \cap H$. By condition (b), we see that $X_{B'} \cap H$ is smooth over $B'$. From these, $X_{B'} \cap H$ is finite étale over $B'$, hence over $B$. Moreover, by condition (d), each component of $(\overline{X}_{B'} \cap H)_{L_v}$ is a disjoint union of $L_v$-rational point in $\Omega_v$. Thus, any connected component of $X_{B'} \cap H$ gives an $\mathcal{S}$-admissible quasi-section. This completes the proof. $\square$

*Step 6.* Assume that $X$ is quasi-projective over $B$. Then, there exists an $\mathcal{S}$-admissible quasi-section.

*Proof.* We shall prove this by using induction on the relative dimension $d$ of $X$ over $B$. If $d = 0$, this is clear. If $d = 1$, this is just the content of Step 5. So, assume $d > 1$. Since $X$ is quasi-projective, we may choose an embedding $X \hookrightarrow \mathbf{P}^n_B$. We denote by $\overline{X}$ the closure of $X$ in $\mathbf{P}^n_B$, and put $W \overset{\text{def}}{=} \overline{X} - X$. Next, for each $v \in \Sigma$, we define $\check{\Omega}'_v$ to be the subset of $\check{\mathbf{P}}^n(L_v)$ consisting of points corresponding to $L_v$-rational hyperplanes that meet transversally with a point of $\Omega_v$. Then, it is easy to see that $\check{\Omega}'_v$ is a non-empty, $v$-adically open, $G_v$-stable subset of $\check{\mathbf{P}}^n(L_v)$. Thus, $\mathcal{B}' \overset{\text{def}}{=} (\mathcal{C}, \overline{X}, W \subset \mathbf{P}^n_B, \{\check{\Omega}'_v\}_{v \in \Sigma})$ becomes a Bertini data, and, by Step 4, there exists a $\mathcal{B}'$-admissible quasi-hyperplane $H \subset \mathbf{P}^n_{B'}$, where $B'$ is the integral closure of $B$ in some finite $\mathcal{C}$-admissible extension $K'$ of $K$. By conditions (a) and (b) in the definition of $\mathcal{B}'$-admissibility, we see that $X'_{B'} \overset{\text{def}}{=} X_{B'} \cap H$ is smooth, surjective over $B'$. By condition (c), $X'_{B'} \times_{B'} \overline{K'}$ is irreducible. Moreover, by condition (d), $\Omega'_v \overset{\text{def}}{=} \Omega_v \cap H(L_v)$ is non-empty.

Now, we define $C'$ (resp. $B'$) to be the integral closure of $C$ (resp. $B$) in $K'$, and put $\Sigma' \overset{\text{def}}{=} C' - B'$, which is the inverse image of $\Sigma$ in $C'$. Let $v'$ be an element of $\Sigma'$ and $v$ the image of $v'$ in $\Sigma$. Then, we have $(K')_{v'} \subset L_v$. So, put $\mathcal{C}' \overset{\text{def}}{=} (C', \Sigma', \{L_v\}_{v' \in \Sigma'})$ and $\mathcal{S}' \overset{\text{def}}{=} (\mathcal{C}', X'_{B'} \to B', \{\Omega'_v\}_{v' \in \Sigma'})$. Then, $\mathcal{C}'$ is a base curve data (over the algebraic closure of $k$ in $K'$) such that $C'$ is affine and that (RI) holds, and $\mathcal{S}'$ is a Skolem data such that the relative dimension of $X_{B'}$ over $B'$ is $d-1$. Thus, by the assumption of induction, there exists an $\mathcal{S}'$-admissible quasi-section $B'' \to X'_{B'}$. Composing this quasi-section with the natural map $X'_{B'} \to X$, we obtain an $\mathcal{S}$-admissible quasi-section, as desired. This completes the proof. $\square$

*Step 7.* There exists an $\mathcal{S}$-admissible quasi-section. Namely, (3.1) holds.

*Proof.* Let $X'$ be a non-empty affine open subset of $X$, and let $B'$ denote the image of $X'$ in $B$, which is a non-empty open subset of $B$. Put $\Sigma' \overset{\text{def}}{=} B - B'$. Then, $\mathcal{S}' \overset{\text{def}}{=} (\mathcal{C}', X' \to B', \{\Omega_v \cap X'(L_v)\}_{v \in \Sigma} \cup \{X'(K_v^{\text{ur}}) \cap X(R_{K_v^{\text{ur}}})\}_{v \in \Sigma'})$, where $\mathcal{C}' \overset{\text{def}}{=} (C, \Sigma \cup \Sigma', \{L_v\}_{v \in \Sigma} \cup \{K_v^{\text{ur}}\}_{v \in \Sigma'})$, becomes a Skolem data. Now, just as in the proof of Step 5, an $\mathcal{S}'$-admissible quasi-section (whose existence is assured by Step 6) induces an $\mathcal{S}$-admissible quasi-section. This completes the proof. $\square$

*Step 8.* There exists a $\mathcal{B}$-admissible quasi-hyperplane. Namely, (3.2) holds.

*Proof.* This is just similar to the proof of Step 4, except that we use Step 7 instead of Step 3. $\square$

## §4. Some remarks and applications.

*4.1. On condition* (RI).
It is desirable to remove the disgusting condition (RI) in the main results (3.1) and (3.2). The main (and the only) technical difficulty in doing so appears in Step 1 of §3. More specifically, recall that we have applied (1.18)(ii) in Step 1. However, to apply (1.18)(ii), we need a finite submodule $A$ of $R_{L_v}$ with $A \cap \mathfrak{m}_{L_v} = \{0\}$ and with $\sharp(A)$ sufficiently large, which requires the infiniteness of the residue field of $L_v$. In fact, it is possible to modify (1.18)(ii) to include the case where $A \cap \mathfrak{m}_{L_v} = \{0\}$ does not hold, but then we cannot expect the valuation $\delta$ of $a$ is sufficiently small compared to $\deg(f)$, and the proof of (3.4) fails when we try to apply (1.4)(ii).

*4.2. On the incompleteness hypothesis.*
In the main results (3.1) and (3.2), we have assumed the incompleteness hypothesis that the base curve $C$ is affine. It is impossible to remove this condition entirely, but it is desirable to be able to control the objects at the points at infinity, even in some weaker sense. In this direction, we have a capacity-theoretic approach due to Rumely ([Ru1], [Ru2]) and another approach via small codimension arguments due to Moret-Bailly ([Mo5]). The author hopes for the following third approach (though it is only applicable to positive characteristic). More precisely, let $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$ be a base curve data over an algebraic extension $k$ of $\mathbb{F}_p$ (with $C$ not necessarily affine), and $\Sigma_\infty$ a non-empty subset of $\Sigma$. Then, even if $C$ is proper over $k$, we might expect that the following version of (3.1) and (3.2) hold.

For (3.1), let $\mathcal{S} = (\mathcal{C}, f : X \to B, \{\Omega_v\}_{v\in\Sigma-\Sigma_\infty} \cup \{X(L_v)\}_{v\in\Sigma_\infty})$ be a Skolem data. (Thus, for $v \in \Sigma_\infty$, we just assume $X(L_v) \neq \emptyset$.) Then, we might expect that there exists a quasi-section $s : B' \to X$ of $f : X \to B$ which is nearly $\mathcal{S}$-admissible with respect to $\Sigma_\infty$ in the following sense: $K'$ is a finite extension of $K$ which is nearly $\mathcal{C}$-admissible with respect to $\Sigma_\infty$; $B'$ is the integral closure of $B$ in $K'$; and for each $v \in \Sigma - \Sigma_\infty$, the image of $B'_{L_v} \stackrel{\text{def}}{=} B' \times_B L_v$ in $X_{L_v} \stackrel{\text{def}}{=} X \times_B L_v$ is contained in $\Omega_v$ ($\subset X(L_v) = X_{L_v}(L_v)$). (For $v \in \Sigma_\infty$, the image of $B'_{L_v(p)}$ in $X_{L_v(p)}$ is automatically contained in $X(L_v(p)) = X_{L_v(p)}(L_v(p))$, and we do not impose any more condition.)

For (3.2), let $\mathcal{B} = (\mathcal{C}, Y_1, \dots, Y_r \subset \mathbf{P}(\mathcal{E}), \{\check{\Omega}_v\}_{v\in\Sigma-\Sigma_\infty} \cup \{\mathbf{P}(\check{\mathcal{E}})(L_v)\}_{v\in\Sigma_\infty})$ be a Bertini data. Then, we might expect that there exists a quasi-hyperplane $H \subset \mathbf{P}(\mathcal{E})_{B'}$ which is nearly $\mathcal{B}$-admissible with respect to $\Sigma_\infty$ in the following sense: $K'$ is a finite extension of $K$ which is nearly $\mathcal{C}$-admissible with respect to $\Sigma_\infty$; $B'$ is the integral closure of $B$ in $K'$; (a), (b), (c) as in the definition of $\mathcal{B}$-admissibility; and (d) as in the definition of $\mathcal{B}$-admissibility only for $v \in \Sigma-\Sigma_\infty$. (For $v \in \Sigma_\infty$, the image of $B'_{L_v(p)}$ in $\mathbf{P}(\check{\mathcal{E}})_{L_v(p)}$ is automatically contained in $\mathbf{P}(\check{\mathcal{E}})(L_v(p)) = \mathbf{P}(\check{\mathcal{E}})_{L_v(p)}(L_v(p))$, and we do not impose any more condition.)

We might consider (2.2) as a weak evidence for this expectation.

*4.3. Hopeful generalizations (mild).*
Firstly, it should be possible to generalize the main results (3.1) and (3.2) to the case of algebraic spaces or even algebraic stacks, along the lines of [Mo5].

Secondly, it should be possible to prove qualitative versions of (3.1) and (3.2), in terms of heights (cf. [U], and [A1,2]) and/or degrees (cf. [Mi], [E1,2]). (See also [Poo].)

Thirdly, it is desirable to be able to prove that, in (3.1), we can choose an $\mathcal{S}$-admissible quasi-section $B' \to X$ which is a closed immersion (cf., e.g., [Mo2], Définition 1.4.), and, similarly, that, in (3.2), we can choose a $\mathcal{B}$-admissible quasi-hyperplane $H \subset \mathbf{P}(\mathcal{E})_{B'}$ such that the classifying morphism $[H] : B' \to \mathbf{P}(\check{\mathcal{E}})$ is a closed immersion. This third possible generalization was suggested to the author by the referee. Indeed, this generalization is possible in Steps 1 and 2 of §3. (For Step 2, this is possible by means of the simplification of the proof due to him or her. See (3.8).)

*4.4. Hopeful generalizations (ambitious).*
As we have mentioned in the Introduction, word-for-word translations of the main results (3.1) and (3.2) to the number field case, namely, to the case where $C$ in the base scheme data is (an open subscheme of) the spectrum of the integer ring of an algebraic number field are false. However, it is very interesting (at least to the author) to ask if we might hope for any (modified) unramified versions of (3.1) and (3.2) also in the number field case.

Also, it might be interesting to investigate what happens in the case where $C$ is a higher-dimensional (affine) scheme, even in positive characteristic. One of the main obstacles of this direction consists in the fact that the Picard group of $C$ is no longer a torsion group, and word-for-word translations of (3.1) and (3.2) to the higher-dimensional case are false. However, there might exist some reasonable restrictions on the (Skolem or Bertini) data, with which (3.1) and (3.2) are valid.

*4.5. An application to local-global principle and largeness in field theory.*

Definition. Let $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$ be a base scheme data. Then, we define $K^{\mathcal{C}}$ to be the maximal $\mathcal{C}$-admissible extension of $K$ contained in the algebraic closure $\overline{K}$ of $K$, $C^{\mathcal{C}}$ (resp. $B^{\mathcal{C}}$) the integral closure of $C$ (resp. $B$) in $K^{\mathcal{C}}$, and $\Sigma^{\mathcal{C}}$ to be the inverse image of $\Sigma$ in $C^{\mathcal{C}}$. (Thus, $\Sigma^{\mathcal{C}} = C^{\mathcal{C}} - B^{\mathcal{C}}$.)

As an application of (3.1), we obtain the following local-global principle in field theory (cf. [Mo4]).

Theorem (4.1). *Let $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$ be a base curve data over an algebraic extension of $\mathbb{F}_p$, and assume that $C$ is affine and that* (RI) *holds. Then, $K^{\mathcal{C}}$ satisfies the local-global principle in the sense that, for each smooth, geometrically connected scheme $X$ over $K^{\mathcal{C}}$, $X(K^{\mathcal{C}}) \neq \emptyset$ holds if and only if $X((K^{\mathcal{C}})_w) \neq \emptyset$ holds for every prime $w$ of $K^{\mathcal{C}}$. Here, $(K^{\mathcal{C}})_w$ denotes the algebraic closure of $K_v$ in the completion of $K^{\mathcal{C}}$ at $w$, where $v$ is the prime of $K$ that is below $w$.*

*Proof.* The 'only if' part is trivial. To prove the 'if' part, assume that $X((K^{\mathcal{C}})_w) \neq \emptyset$ holds for every prime $w$ of $K^{\mathcal{C}}$. First, replacing $X$ by any non-empty quasi-compact open subset, we may assume that $X$ is of finite type over $K^{\mathcal{C}}$. (Observe that the image of $X((K^{\mathcal{C}})_w)$ in $X$ is Zariski dense.) Then, replacing $K$ and $\mathcal{C}$ by a suitable finite $\mathcal{C}$-admissible extension and a suitable base curve data, respectively, we may assume that $X$ comes from a (smooth, geometrically connected) $K$-scheme $X_K$. Now, the following (4.2) implies $X(K^{\mathcal{C}}) = X_K(K^{\mathcal{C}}) \neq \emptyset$, as desired. (Put $\Omega_v = X_K(L_v)$.) $\square$

Theorem (4.2). *Notations and assumptions being as in* (4.1)*, let $X_K$ be a smooth, geometrically connected $K$-scheme. Assume that $X_K(K_b^{\mathrm{ur}}) \neq \emptyset$ holds for each closed point $b \in B$, and that a non-empty, $v$-adically open, $G_v$-stable subset $\Omega_v$ of $X_K(L_v)$ is given for each $v \in \Sigma$. Then, there exists a finite $\mathcal{C}$-admissible extension $K'$ of $K$ and $s_K \in X_K(K')$, such that, for each $v \in \Sigma$, the image by $s_K \times_K L_v$ of* $\mathrm{Spec}(K') \times_K L_v$ *in $X_{L_v} \overset{\mathrm{def}}{=} X_K \times_K L_v$ is contained in $\Omega_v$ ($\subset X_K(L_v) = X_{L_v}(L_v)$).*

*Proof.* First, assume that there exist a regular, integral scheme $\overline{X}$ proper, flat over $B$ and an open immersion $X_K \hookrightarrow \overline{X}_K$ over $K$. (We shall refer to such an $\overline{X}$ as a regular, relative compactification over $B$.) Put $W_K \overset{\mathrm{def}}{=} \overline{X}_K - X_K$ and denote by $W$ the closure of $W_K$ in $\overline{X}$. Then, we see easily that $W \cap \overline{X}_K = W_K$ and that the fiber $W_b$ of $W$ at each closed point $b$ of $B$ has dimension strictly smaller than the dimension of the whole fiber $\overline{X}_b$ (which is automatically equidimensional). On the other hand, let $\overline{X}^{\mathrm{sm}}$ denote the set of points of $\overline{X}$ at which $\overline{X} \to B$ is smooth. This is an open subset of $\overline{X}$. Since $\overline{X}$ is regular and $\overline{X}(K_b^{\mathrm{ur}})(\supset X_K(K_b^{\mathrm{ur}})) \neq \emptyset$ for each closed point $b \in B$, we see that $\overline{X}^{\mathrm{sm}} \to B$ is surjective. From these, we conclude that $X \overset{\mathrm{def}}{=} \overline{X}^{\mathrm{sm}} - W$ surjects onto $B$ and that $X \times_B K = X_K$ holds. Now, applying (3.1) to the Skolem data $\mathcal{S} \overset{\mathrm{def}}{=} (\mathcal{C}, X \to B, \{\Omega_v\}_{v \in \Sigma})$, we obtain an $\mathcal{S}$-admissible quasi-section $s : B' \to X$. Then, $s_K \overset{\mathrm{def}}{=} s \times_B K$ satisfies the desired properties.

In general, the above desingularization result may not be available, but we can proceed by using induction on $d \overset{\mathrm{def}}{=} \dim(X_K)$, as follows. The case $d = 0$ is trivial. In the case $d = 1$, the existence of a regular, relative compactification as above is well-known. So, we may assume $d \geq 2$. Replacing $X_K$ by a suitable (say, non-empty and affine) open subset, we may also assume that $X_K$ is quasi-projective over $K$. (Observe that the image of $\Omega_v$ in $X_K$ is Zariski dense.) We choose an embedding $X_K \hookrightarrow \mathbf{P}^n_K$. Then, as in the proof of Step 4 of §3, there exists a non-empty open subset $\check{U}_K$ of the dual projective space $\check{\mathbf{P}}^n_K$, such that, for each hyperplane $H_{\overline{K}}$ that corresponds to a point of $\check{U}_K(\overline{K})$, $X_{\overline{K}} \cap H_{\overline{K}}$ is smooth, (geometrically) connected of dimension $d-1$. Moreover, as in the proof of Step 6 of §3, for each $v \in \Sigma$, we define $\check{\Omega}'_v$ to be the subset of $\check{\mathbf{P}}^n(L_v)$ consisting of points corresponding to $L_v$-rational hyperplanes that meet transversally with a point of $\Omega_v$. Then, it is easy to see that $\check{\Omega}'_v$ is a non-empty, $v$-adically open, $G_v$-stable subset of $\check{\mathbf{P}}^n(L_v)$. Now, since $\check{U}_K$ admits a regular, relative compactification $\check{\mathbf{P}}^n_B$, we may apply the above argument to $(\check{U}_K, \{\Omega'_v \cap \check{U}_K(L_v)\}_{v\in\Sigma})$ to obtain a suitable quasi-section $s'_K$ of $\check{U}_K$. (Note also that $\check{U}_K(K_b^{\mathrm{ur}}) \neq \emptyset$ holds for each closed point $b$ of $B$.) Now, as in the proof of Step 6 of §3, we may reduce the problem to the case $d-1$ by cutting (the base change of) $X_K$ with the quasi-hyperplane corresponding to $s'_K$. Thus, the proof by induction is completed. □

Corollary (4.3). *$K^{\mathcal{C}}$ is large (in the sense of* [Pop]*).* □

*Proof.* Immediate from (4.1). (See [Pop], Proposition 3.1.) □

This corollary gives an interesting new example of large fields. Indeed, as far as the author knows, in all the known examples of large fields which are algebraic extensions of either number fields $K$ or function fields $K$ over finite fields, we can control only finitely many primes of $K$. On the other hand, our $K^{\mathcal{C}}$ is defined by imposing restrictions at almost all primes of $K$.

In this sense, this corollary may be regarded as the first example of large fields which are not so large! (See also (4.11) below.)

*4.6. An application to principal ideal theorem.*
As an application of (3.1), we obtain the following (cf. [Mo1], 3.1):

Theorem (4.4). *Let $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$ be a base curve data over an algebraic extension $k$ of $\mathbb{F}_p$, and assume that $C$ is affine and that* (RI) *holds. Then, we have* $\mathrm{Pic}(C^{\mathcal{C}}) = \{0\}$*. In particular, we have* $\mathrm{Pic}(B^{\mathcal{C}}) = \{0\}$*.*

*Proof.* Let $\mathcal{L}^{\mathcal{C}}$ be any invertible sheaf on $C^{\mathcal{C}}$. Then, there exists a finite subextension $K_1$ of $K^{\mathcal{C}}$ over $K$, such that $\mathcal{L}^{\mathcal{C}} = \mathcal{L}_1 \otimes_{\mathcal{O}_{C_1}} \mathcal{O}_{C^{\mathcal{C}}}$ holds for some invertible sheaf $\mathcal{L}_1$ on $C_1$, where $C_1$ is the integral closure of $C$ in $K_1$. We define $B_1$ and $\Sigma_1$ to be the integral closure of $B$ in $K_1$ and the inverse image of $\Sigma$ in $C_1$, respectively, and, for each $v_1 \in \Sigma_1$, we put $L_{v_1} \stackrel{\text{def}}{=} L_v$, where $v$ is the image of $v_1$ in $\Sigma$. Then, observe that $\mathcal{C}_1 \stackrel{\text{def}}{=} (C_1, \Sigma_1, \{L_{v_1}\}_{v_1\in\Sigma_1})$ becomes a base curve data (over the algebraic closure of $k$ in $K_1$), such that $(C_1)^{\mathcal{C}_1} = C^{\mathcal{C}}$. Now, consider the Skolem data $\mathcal{S}_1 = (\mathcal{C}_1, (\mathbf{V}(\check{\mathcal{L}}_1) - 0_{C_1}) \times_{C_1} B_1 \to B_1, \{(\mathbf{V}(\check{\mathcal{L}}_1) - 0_{C_1})(R_{L_v})\}_{v_1\in\Sigma_1})$ (such that $C_1$ is affine and that (RI) holds), where $\mathbf{V}(\check{\mathcal{L}}_1)$ denotes the (geometric) line bundle on $C_1$ defined by the dual $\check{\mathcal{L}}_1$ of $\mathcal{L}_1$, and $0_{C_1}$ denotes the zero section of $\mathbf{V}(\check{\mathcal{L}}_1)$. Now, by (3.1), there exists an $\mathcal{S}_1$-admissible quasi-section $B' \to (\mathbf{V}(\check{\mathcal{L}}_1) - 0_{C_1}) \times_{C_1} B_1$. By the choice of $\mathcal{S}_1$, this quasi-section extends to a (unique) quasi-section $C' \to \mathbf{V}(\check{\mathcal{L}}_1) - 0_{C_1}$ of $\mathbf{V}(\check{\mathcal{L}}_1) - 0_{C_1} \to C_1$, where $C'$ is the integral closure of $C_1$ in $B'$. This implies that $\mathcal{L}_1$ admits an everywhere non-vanishing section over $C'$, or, equivalently, $\mathcal{L}_1$ becomes trivial after the base change to $C'$. Therefore, $\mathcal{L}^{\mathcal{C}}$ is trivial, a fortiori. This completes the proof of the first assertion.

The second assertion follows from the first, as the natural map $\mathrm{Pic}(C^{\mathcal{C}}) \to \mathrm{Pic}(B^{\mathcal{C}})$ is surjective. □

In the case where $\Sigma = \emptyset$, (4.4) directly follows from the principal ideal theorem in class field theory. In general, however, there exists an invertible sheaf that cannot be trivialized if we only consider abelian $\mathcal{C}$-admissible extensions. (See (4.11) below.) In this sense, we may regard (4.4) as a new (non-abelian) type of principal ideal theorem which cannot be covered by class field theory.

*4.7. An application to torsors.*
More generally than the second assertion of (4.4), we obtain the following:

Theorem (4.5). *Let $\mathcal{C} = (C, \Sigma, \{L_v\}_{v\in\Sigma})$ be a base curve data over an algebraic extension of $\mathbb{F}_p$, and assume that $C$ is affine and that* (RI) *holds. Let $G^{\mathcal{C}}$ be a smooth, separated group scheme of finite type over $B^{\mathcal{C}}$, such that the generic fiber $G^{\mathcal{C}}_{K^{\mathcal{C}}}$ is connected. Then, we have* $\mathrm{Ker}(\check{H}^1_{fpqc}(B^{\mathcal{C}}, G^{\mathcal{C}}) \to \prod_{w\in\Sigma^{\mathcal{C}}} \check{H}^1_{fpqc}(\mathrm{Spec}((K^{\mathcal{C}})_w), G^{\mathcal{C}}))) = \{1\}$.

*Proof.* By [Ra], Théorème XI, 3.1, each class $x$ of $\check{H}^1_{fpqc}(B^{\mathcal{C}}, G^{\mathcal{C}})$ corresponds to a representable $B^{\mathcal{C}}$-torsor $X^{\mathcal{C}}$. If, moreover, $x$ belongs to the kernel in question, $X^{\mathcal{C}}$ admits a $(K^{\mathcal{C}})_w$-rational point for each $w \in \Sigma^{\mathcal{C}}$. Since $X^{\mathcal{C}}$ is of finite presentation over $B^{\mathcal{C}}$, it comes from a scheme over a finite ($\mathcal{C}$-admissible) extension of $B$. Now, as in the proof of (4.4), we can prove that $X^{\mathcal{C}}$ admits a $B^{\mathcal{C}}$-section, by using (3.1). This completes the proof. □

Note that the second assertion of (4.4) is a special case of (4.5), where $G^{\mathcal{C}} = \mathbb{G}_{m,B^{\mathcal{C}}}$. (The first assertion of (4.4) can also be generalized in a suitable sense. We leave it to the readers.)

As an interesting corollary of (4.5), we obtain:

Corollary (4.6). *Let $C$ be an affine, smooth curve over an algebraic extension of $\mathbb{F}_p$, and $K$ the function field of $C$. Let $G$ be a smooth, separated, commutative group scheme of finite type over $C$, such that the generic fiber $G_K$ is connected.*

*Then, we have $H^1_{\text{ét}}(C, G) = H^1(\pi_1(C), G(\tilde{C}))$, where $\tilde{C} \stackrel{\text{def}}{=} B^{\mathcal{C}} (= C^{\mathcal{C}})$ for the base curve data $\mathcal{C} \stackrel{\text{def}}{=} (C, \emptyset, \emptyset)$.*

*Proof.* This follows from (4.5), together with the Hochschild-Serre spectral sequence. □

*4.8. A group-theoretical remark.*
Recall that a quasi-$p$ group (for a prime number $p$) is a finite group that does not admit a non-trivial quotient group of order prime to $p$.

Proposition (4.7). *Let $B$ be a smooth, geometrically connected curve over a finite field $k$ of characteristic $p$. We denote by $B^*$ the smooth compactification of $B$ and put $\Sigma \stackrel{\text{def}}{=} B^* - B$ (which we regard as a reduced closed subscheme of $B^*$). Then, there exists a natural number $N$ (depending only on the genus $g$ of $B^*$ and the cardinality $n$ of $\Sigma(\bar{k})$), such that, for each finite extension $l$ of $k$ with $\sharp(l) \geq N$, there is no non-trivial finite étale covering of $B_l \stackrel{\text{def}}{=} B \times_k l$ at most tamely ramified over $\Sigma_l \stackrel{\text{def}}{=} \Sigma \times_k l$ in which every point of $B(l) = B_l(l)$ splits completely.*

*Proof.* This is a rather well-known application of the Weil bound on the cardinality of rational points over finite fields. More specifically, suppose that $l$ is a finite extension of $k$ with cardinality $q$ and that $B'$ is a connected finite étale covering with degree $d$ of $B_l$ at most tamely ramified over $\Sigma_l$ in which every point of $B(l)$ splits completely. We denote by $l'$ the integral closure of $l$ in $B'$, and define $(B')^*$, $g'$ and $n'$ for $B'$ just similarly to $B^*$, $g$ and $n$, respectively, for $B$. Now, firstly, the tamely ramified condition, together with the Hurwitz' formula, implies

$$2g'-2 \leq d_{\mathrm{geom}}(2g-2)+(d_{\mathrm{geom}}-1)n \leq d(2g-2)+(d-1)n,$$

where $d_{\mathrm{geom}} \stackrel{\mathrm{def}}{=} d/[l':l]$. Secondly, the complete splitting condition, together with the Weil (lower) bound for $B_l$, implies that

$$\sharp(B'(l)) = d\sharp(B_l(l)) \geq d(\sharp((B')^*(l))-n) \geq d(1+q-2g\sqrt{q}-n).$$

Thirdly, the Weil (upper) bound for $B'$ implies

$$\sharp(B'(l)) \leq \sharp((B')^*(l)) \leq 1+q+2g'\sqrt{q}.$$

(Note that this holds (trivially) even if $[l':l]>1$.) Combining these three inequalities together, we obtain

$$d(q-(4g+n-2)\sqrt{q}-(n-1)) \leq q-(n-2)\sqrt{q}+1.$$

From this, we see that $d<2$ (or, equivalently, $d=1$) must hold for sufficiently large $q$, as desired. $\square$

Proposition (4.8). *Let $k$ and $B$ be as in* (4.7). *Then, there exist finite sets $\Sigma_1$ and $\Sigma_2$ of closed points of $B$, disjoint from each other, such that the following holds: For each $v \in \Sigma_1$ (resp. $v \in \Sigma_2$), let $L_v$ be any (possibly infinite) pro-$p$ Galois extension of $K_v$ (resp. Galois extension such that $\mathrm{Gal}(L_v \cap K_v^{\mathrm{ur}}/K_v)$ is a pro-prime-to-$p$ group) and put $\mathcal{C} = (B, \Sigma_1 \cup \Sigma_2, \{L_v\}_{v\in\Sigma_1\cup\Sigma_2})$. Then, for every $\mathcal{C}$-admissible, finite, Galois extension $K'$ of $K$, $\mathrm{Gal}(K'/K)$ is a quasi-$p$ group and the constant field of $K'$ (i.e., the algebraic closure of $k$ in $K'$) coincides with $k$.*

*Proof.* Take a natural number $N$ as in (4.7), and choose two finite extensions $l_1$ and $l_1'$ of $k$ with $\sharp(l_1) \geq N$ and $\sharp(l_1') \geq N$, such that $l_1 \cap l_1' = k$. We define $\Sigma_1$ to be the union of the images of $B(l_1)$ and $B(l_1')$ in $B$. Next, the Weil bound implies that there exists a natural number $N'$, such that, for each finite extension $l$ of $k$ with $\sharp(l) \geq N'$, $(B-\Sigma_1)(l) \neq \emptyset$ holds. (Note that $B-\Sigma_1$ is geometrically connected over $k$.) So, we can choose a finite extension $l_2$ of $k$, such that $(B-\Sigma_1)(l_2) \neq \emptyset$ and that $[l_2:k]$ is not divisible by $p$. We define $\Sigma_2$ to be any non-empty subset of the image of $(B-\Sigma_1)(l_2)$ in $B-\Sigma_1$. Now, for each $v \in \Sigma_1$ (resp. $v \in \Sigma_2$), let $L_v$ be any pro-$p$ Galois extension of $K_v$ (resp.

Galois extension such that $\mathrm{Gal}(L_v \cap K_v^{\mathrm{ur}}/K_v)$ is a pro-prime-to-$p$ group), and put $\mathcal{C} = (B, \Sigma_1 \cup \Sigma_2, \{L_v\}_{v \in \Sigma_1 \cup \Sigma_2})$.

Let $K'$ be any $\mathcal{C}$-admissible finite Galois extension of $K$. We define $\mathrm{Gal}(K'/K)^{p'}$ (resp. $\mathrm{Gal}(K'/K)^p$) to be the maximal quotient group of $\mathrm{Gal}(K'/K)$ with order prime to $p$ (resp. with order a power of $p$), and denote by $M_1$ (resp. $M_2$) the subextension of $K'$ over $K$ that corresponds via Galois theory the kernel of the natural surjective map $\mathrm{Gal}(K'/K) \twoheadrightarrow \mathrm{Gal}(K'/K)^{p'}$ (resp. $\mathrm{Gal}(K'/K) \twoheadrightarrow \mathrm{Gal}(K'/K)^p$). Thus we have $\mathrm{Gal}(M_1/K) = \mathrm{Gal}(K'/K)^{p'}$ (resp. $\mathrm{Gal}(M_2/K) = \mathrm{Gal}(K'/K)^p$) .

We shall first prove that $\mathrm{Gal}(K'/K)$ is a quasi-$p$ group, or, equivalently, that $M_1 = K$ holds. As $K'$ is $\mathcal{C}$-admissible, so is $M_1$. Since, moreover, $\mathrm{Gal}(M_1/K)$ has order prime to $p$ and $\mathrm{Gal}(L_v/K_v)$ is pro-$p$ for each $v \in \Sigma_1$, $M_1/K$ must split completely at each $v \in \Sigma_1$. Now, by (4.7), we obtain $M_1 \subset Kl_1 \cap Kl'_1 = K$, as desired.

Next, we shall prove that the constant field of $K'$ is $k$. Since the Galois group over $k$ of a finite extension of $k$ is cyclic (hence nilpotent, a fortiori), we see that the constant field of $K'$ is the compositum of those of $M_1$ and $M_2$. Since we have already proved $M_1 = K$, it suffices to prove that the constant field of $M_2$ is $k$. As $K'$ is $\mathcal{C}$-admissible, so is $M_2$. Since, moreover, $\mathrm{Gal}(M_2/K)$ has $p$-power order and $\mathrm{Gal}(L_v \cap K_v^{\mathrm{ur}}/K_v)$ is pro-prime-to-$p$ for each $v \in \Sigma_2$, $M_2/K$ does not admit a non-trivial residue field extension over $\Sigma_2$. In particular, the constant field of $M_2$ is contained in the residue field of each $v \in \Sigma_2$, hence in $l_2$ by the choice of $\Sigma_2$. Now, since $\mathrm{Gal}(M_2/K)$ has $p$-power order and $[l_2 : k]$ is prime to $p$, the constant field of $M_2$ must coincide with $k$, as desired.

This completes the proof. □

Proposition (4.9). *Let the notations and the assumptions be as in* (2.2), *and assume, moreover, that $k$ is an algebraic extension of $\mathbb{F}_p$. Then, in the conclusion of* (2.2), *we may assume that* $\mathrm{Gal}(K'/K)$ *is a quasi-$p$ group and that the constant field of $K'$ coincides with $k$.*

*Proof.* We can choose a finite subextension $k_0$ of $\mathbb{F}_p$ in $k$, such that the curve $C$ and the (reduced) closed subscheme $\Sigma$ of $C$ descend to $C_0$ and $\Sigma_0$, respectively. Replacing $k_0$ by a suitable finite extension (in $k$), we may assume $\sharp(\Sigma) = \sharp(\Sigma_0)$. Moreover, again replacing $k_0$ by a suitable finite extension, we may assume that, for each $v \in \Sigma$, the finite Galois extension $L_v/K_v$ descends to a finite Galois extension $L_{0,v_0}/K_{0,v_0}$, where $K_0$ is the function field of $C_0$ and $v_0$ is the image of $v$ in $\Sigma_0$. We define $\Sigma_{0,\infty}$ to be the image of $\Sigma_\infty$ in $\Sigma_0$. We also put $B_0 \stackrel{\mathrm{def}}{=} C_0 - \Sigma_0$.

Now, take finite sets $\Sigma_1$ and $\Sigma_2$ of closed points of $B_0$ as in (4.8), and put $\mathcal{C}_0 \stackrel{\mathrm{def}}{=} (C_0, \Sigma_0 \cup \Sigma_1 \cup \Sigma_2, \{L_{0,v_0}\}_{v_0 \in \Sigma_0} \cup \{K_{0,v_0}\}_{v_0 \in \Sigma_1 \cup \Sigma_2})$. Applying (2.2) to $\mathcal{C}_0$ and $\Sigma_{\infty,0}$, we obtain a finite Galois extension $K'_0$ of $K_0$ that is nearly $\mathcal{C}_0$-distinguished with respect to $\Sigma_{\infty,0}$. By (4.8), $\mathrm{Gal}(K'_0/K_0)$ is a quasi-$p$ group and the constant field of $K'_0$ coincides with $k_0$.

Finally, put $K' \stackrel{\mathrm{def}}{=} K'_0 k$. Then, we easily see that $K'$ is a finite Galois extension of $K = K_0k$ that is nearly $\mathcal{C}$-distinguished with respect to $\Sigma_\infty$, that $\mathrm{Gal}(K'/K)$ is a quasi-$p$ group (as $\mathrm{Gal}(K'/K)\tilde{\to}\mathrm{Gal}(K'_0/K_0)$) and that the constant field of $K'$ coincides with $k$. This completes the proof. $\square$

Proposition (4.10). *In* (3.1) *and* (3.2)*, we may choose $B'$ such that $K'$ is a finite Galois extension of $K$ with quasi-$p$ Galois group and that the constant field of $K'$ coincides with $k$.*

*Proof.* The proof of this fact goes rather similarly as that of (4.9). The main difference between them consists in the fact that, in the proof of (4.9), we can use the trivial extension $K_{0,v_0}/K_{0,v_0}$ for each $v \in \Sigma_1 \cup \Sigma_2$, while, in the proof of (4.10), this is impossible, since we have to require that condition (RI) also holds for the (enlarged) base curve data. Here, however, we may take $K_{0,v_0}\mathbb{F}_p(p^\infty)/K_{0,v_0}$ (resp. $K_{0,v_0}\mathbb{F}_p(p')/K_{0,v_0}$) for $v_0 \in \Sigma_1$ (resp. $v_0 \in \Sigma_2$) instead of $K_{0,v_0}/K_{0,v_0}$, where $\mathbb{F}_p(p^\infty)$ (resp. $\mathbb{F}_p(p')$) denotes the maximal pro-$p$ (resp. pro-prime-to-$p$) extension of $\mathbb{F}_p$. Details are left to the readers. $\square$

*Remark* (4.11). The group-theoretical results of this subsection are also applicable to other results in this section.

For example, (4.8) implies that, for some base curve data $\mathcal{C}$, the field $K^{\mathcal{C}}$ that appears in (4.1) and (4.3) satisfies the following property: $\mathrm{Gal}(K^{\mathcal{C}}/K)$ is pro-quasi-$p$ in the sense that its maximal pro-prime-to-$p$ quotient is trivial.

A similar remark is also applicable to (4.4). Namely, for some base curve data $\mathcal{C}$, $\mathrm{Gal}(K^{\mathcal{C}}/K)(= \mathrm{Aut}(B^{\mathcal{C}}/B))$ is pro-quasi-$p$. In particular, the abelianization $\mathrm{Gal}(K^{\mathcal{C}}/K)^{\mathrm{ab}}$ of $\mathrm{Gal}(K^{\mathcal{C}}/K)$ is a pro-$p$ group, or, equivalently, every finite abelian $\mathcal{C}$-admissible extension of $K$ has $p$-power degree. Accordingly, if, moreover, we start with $\mathcal{C}$ such that $\mathrm{Pic}(C)$ admits a non-trivial torsion element $[L]$ whose order is prime to $p$, then $L$ cannot be trivialized over any finite abelian $\mathcal{C}$-admissible extension, while it can be trivialized over some finite (necessarily non-abelian) $\mathcal{C}$-admissible extension by (4.4).

## References


[A1] P. Autissier, *Points entiers sur les surfaces arithmétiques*, J. Reine Angew. Math. **531** (2001), 201–235.

[A2] ———, *Points entiers et théorèmes de Bertini arithmétiques*, Ann. Inst. Fourier (Grenoble) **51** (2001), 1507–1523; Corrigendum, ibid. **52** (2002), 303–304.

[CR] D. C. Cantor and P. Roquette, *On Diophantine equations over the ring of all algebraic integers*, J. Number Theory **18** (1984), 1–26.

[CFHR] F. Catanese, M. Franciosi, K. Hulek and M. Reid, *Embeddings of curves and surfaces*, Nagoya Math. J. **154** (1999), 185–220.

[EGA4] A. Grothendieck et al, *Éléments de géométrie algébrique IV, Étude locale des schémas et des morphismes de schémas,* Publications Mathématiques, 20, 24, 28, 32, IHES, 1964–1967.

[E1] R. Erné, *The degree of an integral point in* $\mathbf{P}^s$ *minus a hypersurface*, C. R. Acad. Sci. Paris, Sér. I, Math. **324** (1997), 1121–1126.

[E2] ______, *On the degree of integral points of a projective space minus a horizontal hypersurface*, J. Reine Angew. Math. **532** (2001), 151–177.

[EG] D. R. Estes and R. M. Guralnick, *Module equivalences: local to global when primitive polynomials represent units*, J. Algebra **77** (1982), 138–157.

[G] O. Gabber, *On space filling curves and Albanese varieties*, Geom. Funct. Anal. **11** (2001), 1192–1200.

[GPR] B. Green, F. Pop and P. Roquette, *On Rumely's local-global principle*, Jahresber. Deutsch. Math.-Verein. **97** (1995), 43–74.

[J] J.-P. Jouanolou, *Théorèmes de Bertini et applications,* Progress in Mathematics, 42, Birkhäuser Boston, Inc., Boston, 1983.

[Mi] P. Mikkelsen, *Effective bounds for integral points on arithmetic surfaces*, J. Reine Angew. Math. **496** (1998), 55–72.

[Mo1] L. Moret-Bailly, *Points entiers des variétés arithmétiques*, in Séminaire de Théorie des Nombres, Paris 1985–86, Progr. Math., 71, Birkhäuser Boston, Boston, 1987, pp. 147–154.

[Mo2] ______, *Groupes de Picard et problèmes de Skolem, I*, Ann. Sci. École Norm. Sup. (4) **22** (1989), 161–179.

[Mo3] ______, *Groupes de Picard et problèmes de Skolem, II*, Ann. Sci. École Norm. Sup. (4) **22** (1989), 181–194.

[Mo4] ______, *Applications of local-global principles to arithmetic and geometry,* in Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Contemp. Math., 270, Amer. Math. Soc., Providence, 2000, pp. 169–186.

[Mo5] ______, *Problèmes de Skolem sur les champs algébriques*, Compositio Math. **125** (2001), 1–30.

[Poo] B. Poonen, *Bertini theorems over finite fields*, Ann. of Math. (to appear).

[Pop] F. Pop, *Embedding problems over large fields*, Ann. of Math. (2) **144** (1996), 1–34.

[Ra] M. Raynaud, *Faisceaux amples sur les schémas en groupes et les espaces homogènes,* Lecture Notes in Mathematics, 119, Springer-Verlag, Berlin-New York, 1970.

[Ro] P. Roquette, *Solving diophantine equations over the ring of all algebraic integers*, in Atas da 8. Escola de Álgebra (Rio de Janeiro, 1984), 2, Coleção Atas, no. 16, Instituto de Mathemática Pura e Aplicada, 1985, pp. 1–26.

[Ru1] R. S. Rumely, *Arithmetic over the ring of all algebraic integers*, J. Reine Angew. Math. **368** (1986), 127–133.

[Ru2] ______, *Capacity theory on algebraic curves,* Lecture Notes in Mathematics, 1378, Springer-Verlag, Berlin, 1989.

[S] T. Skolem, *Lösung gewisser Gleichungen in ganzen algebraischen Zahlen, insbesondere in Einheiten*, Skr. Norske Vid.-Akad. Oslo I, Mat. Naturv. Kl. (1934), no. 10.

[T] A. Tamagawa, *The Eisenstein quotient of the Jacobian variety of a Drinfeld modular curve*, Publ. Res. Inst. Math. Sci. **31** (1995), 203–246.

[U] E. Ullmo, *Points entiers, points de torsion et amplitude arithmétique*, Amer. J. Math. **117** (1995), 1039-1055.

Akio Tamagawa
Research Institute for
Mathematical Sciences
Kyoto University
Kyoto 606-8502, Japan