Annals of Mathematics, **104** (1976), 203-233

Solving diophantine problems over all residue class fields of a number field and all finite fields

By M. FRIED[1] and G. SACERDOTE[2]

Table of Contents

0. Introduction

A. History and explanation of the problem

Let K be a number field with ring of integers $\mathcal{O}_K$. Let L_K be the first order language of the theory of fields. For the sake of definiteness, L_K has: countably many variables $x_1, x_2, \cdots$; a prescribed list of constants; the operation symbols $+$ and $\cdot$; the predicate $=$; and the sentential connectives $\&$, $\vee$, $\sim$, $\exists$, and $\forall$. From elementary logic (see § 0. B) each sentence of L_K is equivalent to a sentence of the form

$$(Q_1\underset{\sim}{x}_1)\cdots(Q_n\underset{\sim}{x}_n)(B(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n)) \tag{0.1}$$

where the $\underset{\sim}{x}_i$ are finite sequences of distinct variables, the Q_i are alternately the quantifiers $\forall$ and $\exists$, and $B(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n)$ is a Boolean combination of polynomial equations over $\mathcal{O}_K$. Without loss of generality we may replace $B(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n)$ by a *constructible set* (union of locally closed subschemes; see § 1. A) in affine space with coordinates obtained by juxtaposing the coordinates of

[1] Partially supported by the Sloan Foundation, a grant from the Institute for Advanced Study (Spring 1972), and NSF grants.

[2] Partially supported by a grant from the Institute for Advanced Study.

$\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n$ in order. We denote this affine space by $\mathbf{A}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n)$. For most of this paper $\mathbf{A}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n)$ and its subschemes are to be regarded as schemes over $\mathcal{O}_K$ (over the prime ideal spectrum Spec $(\mathcal{O}_K)$ of the ring $\mathcal{O}_K$). This use of the language of schemes facilitates the statements and proofs of the most technical parts of this paper.

In any case, expression (0.1) may be written as

$$(0.2) \qquad (Q_1\underset{\sim}{x}_1)\cdots(Q_n\underset{\sim}{x}_n)[(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n) \in A]$$

where A is a union of locally closed subschemes of $\mathbf{A}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n)$.

For a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ we may interpret a sentence of L_K in $\mathcal{O}_K/\mathfrak{p}$ by interpreting the constants as their images in $\mathcal{O}_K/\mathfrak{p}$. The main result of this paper is the *description of an algorithm which determines those sentences φ of L_K which are true in $\mathcal{O}_K/\mathfrak{p}$ for all but finitely many $\mathfrak{p}$* (i.e. almost all primes $\mathfrak{p}$) *and which also computes for each such φ the finite list of exceptional primes.*

If $A_\mathfrak{p}$ is the reduction of A modulo the prime $\mathfrak{p}$ of $\mathcal{O}_K$ (A as above) this result may be rephrased as a *primitive recursive procedure* for deciding the problem:

$$(\mathrm{P})_\varphi \qquad \text{Is } (Q_1\underset{\sim}{x}_1^0)\cdots(Q_n\underset{\sim}{x}_n^0)[(\underset{\sim}{x}_1^0, \cdots, \underset{\sim}{x}_n^0) \in A_\mathfrak{p}] \text{ true in } \mathcal{O}_K/\mathfrak{p}$$
$$\text{for almost all primes } \mathfrak{p} \text{ of } \mathcal{O}_K\,?$$

We use the phrase "$(\mathrm{P})_\varphi$ is true in $\mathcal{O}_K/\mathfrak{p}$" to express that, for the prime $\mathfrak{p}$ $(Q_1\underset{\sim}{x}_1^0)\cdots(Q_n\underset{\sim}{x}_n^0)[(\underset{\sim}{x}_1^0, \cdots, \underset{\sim}{x}_n^0) \in A_\mathfrak{p}]$ is true.

J. Ax [A 1, 2] has obtained a general recursive algorithm for this problem through model theoretic means. We give a layman's distinction between a general recursive and a primitive recursive procedure by noting that (theoretically) our procedure can be put in a computer program (call this *I*) which itself is preceded by another computer program (call this *II*) such that: the length of running time of *II* depends only on the magnitudes of the conjugates (over $\mathbf{Q}$) of the non-zero coefficients of the polynomials describing the locally closed subschemes that appear in A; *II* produces the running time of *I*; after *I* has run we are presented with a yes or no to question $(\mathrm{P})_\varphi$ and if the answer is yes, *I* also produces the list of primes $\mathfrak{p}$ for which $(Q_1\underset{\sim}{x}_1^0)\cdots(Q_n\underset{\sim}{x}_n^0)[(\underset{\sim}{x}_1^0, \cdots, \underset{\sim}{x}_n^0) \in A_\mathfrak{p}]$ is *not* true.

An analogue of the algorithm allows us to determine for a fixed prime $\mathfrak{p}$ those sentences of L_K which are true in all but finitely many finite extensions of $\mathcal{O}_K/\mathfrak{p}$. Combining these two results we obtain a primitive recursive algorithm which determines those sentences that are true for all but finitely many field extensions of residue class fields of $\mathcal{O}_K$ (and which computes the finite list of exceptional fields). The method demonstrates anew Ax's strik-

ing result that a sentence of L_K is true for *all residue class fields* of $\mathcal{O}_K$ if and only if it is true for *all finite extensions* of residue class fields of $\mathcal{O}_K$.

Our algorithm uses the method of *quantifier elimination*, but not in an entirely straightforward way. A straightforward quantifier elimination (if it existed) would produce from the problem $(\mathrm{P})_\varphi$ (as above) a new problem:

$$(\mathrm{P}')_{\varphi'} \qquad \text{Is } (Q_1 \underset{\sim}{x}_1^0) \cdots (Q_{n-1} \underset{\sim}{x}_{n-1}^0)[(\underset{\sim}{x}_1^0, \cdots, \underset{\sim}{x}_{n-1}^0) \in A'_{\mathfrak{p}}] \text{ true in } \mathcal{O}_K/\mathfrak{p}\,?$$

where A' is a constructible subscheme of $\mathbf{A}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_{n-1})$, and, excluding a finite (computable) set of primes $\mathfrak{p}$, $(\mathrm{P}')_{\varphi'}$ is true in $\mathcal{O}_K/\mathfrak{p}$ if and only if $(\mathrm{P})_\varphi$ is true in $\mathcal{O}_K/\mathfrak{p}$. In this way we would *eliminate one block of varibles at a time* until we would be left with a *quantifier-free statement*. We give a simple example to illustrate how ludicrous this would be.

Consider the case where: $\mathcal{O}_K = \mathbf{Z}$, $f(x) \in \mathbf{Z}[x]$ is an irreducible polynomial in one variable of degree at least 2 over $\mathbf{Q}$ and the problem $(\mathrm{P})_\varphi$ is given by:

$$(\mathrm{P})_\varphi \qquad \text{Is } (\exists x^0)[f(x^0) = 0] \text{ true in } \mathbf{Z}/(p)\,?$$

In this case $n = 1$ and A is a 0-dimensional subscheme of affine 1-space over Spec $(\mathbf{Z})$. The elimination of the variable x would leave us with a quantifier-free statement concerning a constructible subset of 0-dimensional affine space (a "point") over Spec $(\mathbf{Z})$. Thus we would conclude that either $(\mathrm{P})_\varphi$ is true in $\mathbf{Z}/(p)$ for almost all primes p or $(\mathrm{P})_\varphi$ is false in $\mathbf{Z}/(p)$ for almost all primes p (excluding a finite set of primes p). Of course, one consequence of the Čebotarev density theorem is that $(\mathrm{P})_\varphi$ is *true* for *infinitely* many primes p and *false* for *infinitely* many primes p.

In order to obtain an elimination of quantifiers we must create statements more general than those of the language L_K, statements which may still be interpreted modulo $\mathfrak{p}$ for the prime ideals $\mathfrak{p}$ of the ring $\mathcal{O}_K$. The concept that allows the expeditious creation of these more general statements is that of a *Galois Stratification* (see § 1. C for the precise definition).

Roughly speaking, a Galois stratification $\mathfrak{U}$ consists of a constructible set A in $\mathbf{A}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n)$, a stratification $\mathfrak{S}(A)$ of A such that for each $X \in \mathfrak{S}(A)$, X is a locally closed subscheme of $\mathbf{A}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n)$, and for each $X \in \mathfrak{S}(A)$, an étale Galois cover $C(X) \xrightarrow{\varphi(X)} X$ along with a union of conjugacy classes, $\mathrm{Con}(X)$, of the Galois group of $C(X)/X$. We call the set $A \overset{\text{def}}{=} A(\mathfrak{U})$ the *underlying space* of $\mathfrak{U}$. Statements of the type $(\mathrm{P})_\varphi$ are replaced by

$$(\bar{\mathrm{P}})_{\bar{\varphi}} \qquad (Q_1 \underset{\sim}{x}_1^0) \cdots (Q_n \underset{\sim}{x}_n^0)[\mathrm{Fr}\,(\underset{\sim}{x}_1^0, \cdots, \underset{\sim}{x}_n^0) \in \bigcup_{X \in \mathfrak{S}(A)} \mathrm{Con}\,(X)]$$

where: $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$; $(\underset{\sim}{x}_1^0, \cdots, \underset{\sim}{x}_n^0)$ is a rational point of $\mathbf{A}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n)_{\mathfrak{p}}$ contained in $X_{\mathfrak{p}}$ for some $X \in \mathfrak{S}(A)$; $\mathrm{Fr}\,(\underset{\sim}{x}_1^0, \cdots, \underset{\sim}{x}_n^0)$ is the conjugacy class

of the Frobenius element of a place of $C(X)_{\mathfrak{p}}$ lying over the place $(\underset{\sim}{x}_1^0, \cdots, \underset{\sim}{x}_n^0) \in X_{\mathfrak{p}}$.

We call such a statement an *elementary Frobenius statement* (for the Galois stratification $\mathfrak{U}$). In this context there is an elimination of quantifiers whereby through a primitive recursive procedure we construct a new Galois stratification $\mathrm{pr}(\mathfrak{U})$ (with underlying space $A(\mathrm{pr}(\mathfrak{U}))$; $\mathrm{pr}(A)$ by abuse), and a new elementary statement:

$$(\overline{\mathrm{P}}')_{\bar{\varphi}'} \qquad (Q_1 \underset{\sim}{x}_1^0) \cdots (Q_{n-1} \underset{\sim}{x}_{n-1}^0)[\mathrm{Fr}(\underset{\sim}{x}_1^0, \cdots, \underset{\sim}{x}_{n-1}^0) \in \bigcup_{(Y \in \mathfrak{S}(\mathrm{pr}(A)))} \mathrm{Con}(Y)] .$$

Most importantly, excluding a finite computable set of primes $\mathfrak{p}$, $(\overline{\mathrm{P}}')_{\bar{\varphi}'}$ is true in $\mathcal{O}_K/\mathfrak{p}$ if an only if $(\overline{\mathrm{P}})_{\bar{\varphi}}$ is true in $\mathcal{O}_K/\mathfrak{p}$.

Thus, by induction, there is a quantifier-free elementary Frobenius statement $(\overline{\mathrm{P}}'')_{\bar{\varphi}''}$ such that (excluding a finite set of computable primes $\mathfrak{p}$) $(\overline{\mathrm{P}}'')_{\bar{\varphi}''}$ is true in $\mathcal{O}_K/\mathfrak{p}$ if and only if $(\overline{\mathrm{P}})_{\bar{\varphi}}$ is true in $\mathcal{O}_K/\mathfrak{p}$. A quantifier-free elementary Frobenius statement consists of a finite Galois extension M of K; an element $a \in \mathcal{O}_K$ such that $\mathrm{Spec}(\mathcal{O}_M[1/a]) \to \mathrm{Spec}(\mathcal{O}_K[1/a])$ is a Galois cover, with group G; a collection $\mathrm{Con}(X)$ $(X = \mathrm{Spec}(\mathcal{O}_K[1/a]))$ of conjugacy classes in G; and for each of the finite set of primes $\mathfrak{p}$ of $\mathcal{O}_K$ dividing a, a finite extension $k_{\mathfrak{p}}$ of $\mathcal{O}_K/\mathfrak{p}$ and a collection of elements of $G(k_{\mathfrak{p}}/(\mathcal{O}_K/\mathfrak{p}))$. The statement $(\overline{\mathrm{P}}'')_{\bar{\varphi}''}$ is true in $\mathcal{O}_K/\mathfrak{p}$ for almost all primes $\mathfrak{p}$ if and only if the Frobenius conjugacy class is in $\mathrm{Con}(X)$ for almost all primes $\mathfrak{p}$. By the Čebotarev density theorem this is true if and only if $\mathrm{Con}(X)$ contains *all conjugacy classes of* G. Since it can be checked in a primitive recursive manner as to whether or not $\mathrm{Con}(X) = G$, this concludes the algorithm for deciding if $(\overline{\mathrm{P}})_{\bar{\varphi}}$ is true in $\mathcal{O}_K/\mathfrak{p}$ for almost all primes $\mathfrak{p}$.

Observe that in order to apply these considerations to our original problem $(\mathrm{P})_{\varphi}$ we have merely to regard $A \subseteq \mathbf{A}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n)$ as a Galois stratification. Indeed, let $\mathfrak{S}(A)$ be any stratification of A so that for $X \in \mathfrak{S}(A)$, X is a locally closed subscheme of $\mathbf{A}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n)$; for each $X \in \mathfrak{S}(A)$, $C(X) = X$; and for each $X \in \mathfrak{S}(A)$, $\mathrm{Con}(X)$ is the identity element in the "trivial" covering group of $C(X)/X$.

In the main algorithm of this paper we have chosen to do our elimination of quantifiers in blocks (where the quantifiers $\forall$ and $\exists$ alternate, as above). The procedure works (theoretically) just as well by elimination of exactly one quantifier at a time. In addition, the technical work utilizing the *Intersection-Union Process* and the generalization of the Bertini and Noether theorems is somewhat simplified by elimination of one quantifier at a time. Nevertheless, several serious applications of the methods of this paper suggest that it is worth the extra effort to eliminate the quantifiers

in blocks. We explain this in more detail in relationship to finding the "exceptional primes" in the Artin conjecture solved by Ax and Kochen [AK1, 2, 3].

In a later paper we will consider the problem of finding a primitive recursive algorithm to decide if (0.1) is true in the $\mathfrak{p}$-adic completion of $\mathcal{O}_K$ for all but finitely many primes $\mathfrak{p}$ of $\mathcal{O}_K$. An appropriate generalization of Hensel's lemma and of the non-regular analogue of the Čebotarev density theorem (see § 4) are among the tools that complement the techniques of the present paper. P. Cohen [C] has shown (by use of entirely different methods, i.e., p-adic analysis) that a primitive recursive algorithm for deciding if (0.1) is true in $\mathcal{O}_K/\mathfrak{p}$ for all but finitely many $\mathfrak{p}$ can be extended to a primitive recursive algorithm for deciding if (0.1) is true for the $\mathfrak{p}$-adic completions of $\mathcal{O}_K$ for all but finitely many primes $\mathfrak{p}$. Still, no one has yet (in general) described the finite set of primes p for which there exists a form of degree d in d^2+1 variables over $\mathbf{Q}_p$ (p-adic numbers) which does *not* have a (non-trivial) rational solution (i.e., the primes for which the Artin conjecture does not hold). This is a problem that has two blocks of quantifiers. Let I be the least set of integer-valued functions on $\mathbf{Z}$ having the property that if $f \in I$ and $g \in I$, then f^g (exponentiation), $f \cdot g$ (multiplication) and $f+g$ (addition) are also in I. Then we might ask if there exists $f \in I$ such that the exceptional primes p for the integer d in the Artin conjecture are all less than $f(d)$. We might hope that our techniques would shed light on this problem (and its generalizations to an arbitrary statement such as (0.1)).

There is another context in which our procedure works almost immediately. Let $\bar{\mathbf{Q}}$ be a fixed algebraic closure $\mathbf{Q}$, let $\sigma_1, \cdots, \sigma_r \in G(\bar{\mathbf{Q}}/\mathbf{Q})$, and let $\bar{\mathbf{Q}}(\underset{\sim}{\sigma})$ be the fixed field of the group generated by $\sigma_1, \cdots, \sigma_r$ in $\bar{\mathbf{Q}}$. Then (modulo the action of $\sigma_1, \cdots, \sigma_r$ explicitly on the elements of $\bar{\mathbf{Q}}$) there is a primitive recursive procedure for deciding the truth of an elementary statement over the field $\bar{\mathbf{Q}}(\underset{\sim}{\sigma})$, for *almost all* r-tuples of elements of $G(\bar{\mathbf{Q}}/\mathbf{Q})$. The term *almost all* is used here (as in [J]) to mean in the Haar-measure sense. Indeed, for the case $r=1$ this is an exercise in the methods of this paper combined with the technique of Jarden's paper. Jarden was the first to show that there are proper subfields of $\bar{\mathbf{Q}}$ which are *pseudo-algebraically closed* (PAC; every absolutely irreducible variety over a PAC field has a rational point). In fact, he showed that the fields $\bar{\mathbf{Q}}(\underset{\sim}{\sigma})$ have this property for almost all $\underset{\sim}{\sigma}$. From the technique of Jarden's paper for $r=1$, we can easily show that for almost all $\sigma \in G(\bar{\mathbf{Q}}/\mathbf{Q})$ the fields $\bar{\mathbf{Q}}(\sigma)$ have the *Čebotarev property*. That is, if $C(X) \xrightarrow{\varphi(X)} X$ is a *cyclic* (Galois) étale cover of absolutely irreducible affine varieties defined over $\bar{\mathbf{Q}}(\sigma)$, then there exists a prime p of

the function field of $C(X)$ lying over $\mathfrak{p}$, a degree 1 closed point of the function field of X (i.e. $\mathfrak{p}$ is $\bar{\mathbf{Q}}(\sigma)$-rational), and the degree of the residue class field of p over the residue class field of $\mathfrak{p}$ is equal to deg $(\varphi(X))$. Following this the techniques of this paper apply directly to the field $\bar{\mathbf{Q}}(\sigma)$.

The fields $\bar{\mathbf{Q}}(\sigma)$ occurred earlier in [A, 1, 2] as the absolute constants of non-trivial ultraproducts of the residue class fields of prime ideals of $\mathbf{Z}$. We do not know if there is primitive recursive procedure for deciding the truth of an elementary statement (or more generally, an elementary Frobenius statement) over *each* of the fields $\bar{\mathbf{Q}}(\sigma)$ for *every* $\sigma \in G(\bar{\mathbf{Q}}/\mathbf{Q})$.

In order to aid the reader there is a *very* simple example at the end of Section 4 illustrating the ingredients of the algorithm.

B. Background from logic and elimination theory

The set of primitive recursive functions (see [P]) is the least class of functions on $\mathbf{N}$ (the positive integers) closed under composition and primitive recursion, and containing the constant functions, the projection functions and the successor function.

We give a heuristic description of the use of *Gödel numbers*. Suppose we are given a class of algebraic objects (e.g., the collection of subfields $\mathfrak{L}$ of a given field K separable over another field L) and an algebraic operation from which we derive a third object of the class from two other objects of the class (e.g., composition of subfields of K). Suppose also that we are given a computable subset S (i.e. defined by primitive recursive functions) of $\mathbf{N}^{(\mathbf{N})}$ (sequences of elements of $\mathbf{N}$, almost all of which are zero), and a map from S to the elements of $\mathfrak{L}$. To continue the discussion explicitly, in the example of fields in $\mathfrak{L}$ our computable subset S of $\mathbf{N}^{(\mathbf{N})}$ might be chosen so that each element of S corresponds to an element of K. Map S to the element of $\mathfrak{L}$ (call this map ψ) so that if $s \in S$ corresponds to $\alpha \in K$, then $\psi(s)$ is the field generated by α over L. Notice that the map from S to $\mathfrak{L}$ is not assumed to be one-one. We call s a Gödel number for the field $L(\alpha)$. We say that the algebraic operation from $\mathfrak{L} \times \mathfrak{L} \to \mathfrak{L}$ (e.g., composition of fields) is primitive recursive with respect to the Gödel numbering S if there exists a primitive recursive function $S \times S \xrightarrow{\gamma} S$ such that for $(s_1, s_2) \in S \times S$, $\psi(\gamma(s_1, s_2)) = \gamma(\psi(s_1), \psi(s_2))$. We say that the algebraic operation is *primitive recursive* if there exists a Gödel numbering S (of $\mathfrak{L}$) such that the algebraic operation is primitive recursive with respect to S.

First we give some remarks on fields. All the fields we use are finitely generated extensions of their prime subfields. By the phrase "given a finitely generated field K" we mean that we are given a pure transcendental field

extension T of the prime field of K of finite transcendence degree; the maximal finite separable extension M of T in K and a Gödel number for the minimal polynomials of a generator of M over T (primitive generator); and Gödel numbers for the minimal polynomials of a finite set of generators of K over M. From this we may compute a primitive recursive encoding of the elements of K. Inseparable field extensions do not occur in our computations until Section 5.

Similarly, "given an algebraic set defined over K" means we are given a Gödel number for its defining Boolean combination of polynomials with coefficients in the field K. Similarly, "given a group" means we are given a Gödel number for its elements as disjoint cycles in some symmetric group (so that group multiplication and taking the inverse are primitive recursive).

Also, a number of computations in the theory of polynomial rings and in Galois theory are primitive recursive. The ones listed below will be used without further comment.

(i) Kronecker's method for factoring a polynomial (defined over a field) into irreducible factors [W; pp. 77-78].

(ii) Given a finite collection of fields of the same characteristic: to compute a field which contains them all [W; p. 127].

(iii) Given a field K, let the symbols $\alpha_1, \cdots, \alpha_n$ be the roots of an irreducible polynomial $f(x)$ over K, to compute the Galois group of the splitting field of $f(x)$ over K as a set of permutations of $\alpha_1, \cdots, \alpha_n$ [W; § 6 1].

(iv) Given a field K and a finite Galois extension K_1 of K; to compute the Galois group $G(K_1/K)$ [W; § 6 1].

(v) Given a Galois extension K_1 of K and $\sigma \in G(K_1/K)$, to compute the fixed field of σ [W; § 6 1].

(vi) Given a field K_1 and K as in (v) and an algebraic set W defined over K_1 and $\sigma \in G(K_1/K)$, to compute the transform of W under σ, ${}^{\sigma}W$.

(vii) Given $W \to V$ a morphism of algebraic varieties where W is reduced (see § 1. A. for the definition of reduced), to compute the ideal of the image of W ([He] and [S]).

(viii) Given a field K and an algebraic set W defined over K, to compute a finite extension $K_1 \supseteq K$ and a sequence $U_1, \cdots, U_n$ of absolutely irreducible varieties defined over K_1 such that $W = U_1 \cup \cdots \cup U_n$ ([He] and [S]).

(ix) Same as (viii) but write $W = U_1 \cup \cdots \cup U_n$ where $U_1, \cdots, U_n$ are irreducible varieties defined over K.

(x) Determine the function field of a K-irreducible variety V.

We would like to thank Moshe Jarden and William Messing for their helpful comments concerning the arrangements of parts of this paper.

1. Generalizing the quantifier elimination problem

A. Notations and terminology

We let $\mathbf{A}^n = \mathbf{A}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n)$ denote affine space with the coordinates $\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n$ (as in § 0). Let R be an integral domain and let $\mathbf{A}^n(R)$ be Spec $(R[\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n])$, a scheme over Spec (R). We borrow, for our purposes, some of the definitions from [Gr]. By a *closed subscheme* A of $\mathbf{A}^n(R)$ we mean a scheme $A = \text{Spec}\,(R[\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n]/I)$ where I is an ideal in $R[\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n]$ ([Gr; § 4]). We say A is *dominant* over Spec (R) if the canonical morphism $A \to \text{Spec}(R)$ (written $A \to R$, by abuse of notation, when no confusion will occur) is generically surjective. A ringed space $(Y, \mathcal{O}_Y)$ is a *locally closed subscheme* of $\mathbf{A}^n(R)$ if there exists an open subset V of $\mathbf{A}^n(R)$ such that Y is contained in V and $(Y \cap V, \mathcal{O}_Y|_V)$ is a closed subscheme of V. If $A \to B$ is a morphism of varieties where A is a union of locally closed subschemes of $\mathbf{A}^n$, then the image of A is a union of locally closed subschemes of B [M 1; Corollary 2, p. 97]. For the purposes of this paper we will present locally closed subschemes Y of $\mathbf{A}^n(R)$ very explicitly. In fact, a locally closed subscheme will be given as a union of Spec $(R(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n, 1/f_i]/I_i)$, with $I_i = (g_{i,1}, \cdots, g_{i,s(i)})$ an ideal of $R[\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n]$, $i = 1, \cdots, r$. We refer to the collection $f_1, \cdots, f_r, g_{1,1}, \cdots, g_{r,s(r)}$ as the *polynomials* of Y.

If $(Y, \mathcal{O}_Y)$ is a locally closed subscheme of $\mathbf{A}^n(R)$, then there is a sheaf $\mathfrak{N}$ of $\mathcal{O}_X$-ideals such that for $y \in Y$, $\mathfrak{N}_Y = \{\alpha \in (\mathcal{O}_Y)_y | \alpha^t = 0$ for some integer $t\}$; $\mathfrak{N}_y$ is the *nilradical* of $(\mathcal{O}_Y)_y$ [Gr, § 5]. We call $(Y, \mathcal{O}_Y/\mathfrak{N})$ the *reduced scheme with underlying space* Y, and we denote this by Y_{red}. In the case that $Y = \text{Spec}(R[\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}, 1/f]/I)$, $Y_{\text{red}} = \text{Spec}(B/N)$ where $B = R[\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n, 1/f]/I$ and N is the nilradical of B. From [Gr; Prop, 5. 2. 1], Y_{red} is the unique reduced locally closed subscheme of $\mathbf{A}^n(R)$ having Y as its underlying space.

Throughout this paper we freely replace a locally closed subscheme Y of $\mathbf{A}^n(R)$ by Y_{red}. We may do this because our concern is with diophantine problems, where we deal with the rational points on the underlying space of Y.

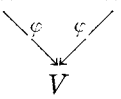
For much of this paper R will be the ring $\mathcal{O}_K[1/a]$ where K is a number field, $\mathcal{O}_K$ is the ring of integers of K, and a is an element of $\mathcal{O}_K$. Let A be a locally closed subscheme of $\mathbf{A}^n(\mathcal{O}_K)$, and let $\mathfrak{p}$ be a maximal prime ideal of $\mathcal{O}_K$. Then we denote by $A_\mathfrak{p}$ the fiber of A over $\mathfrak{p}$ (i. e. over Spec $(\mathcal{O}_K/\mathfrak{p})$).

Naively this is obtained by reducing the coefficients of the polynomials of A modulo $\mathfrak{p}$.

One of the essential tools in our algorithm is a free use of finite étale Galois covers of a morphism $V \to \mathbf{A}^n(\mathcal{O}_K)$. Let $W \xrightarrow{\varphi} V$ be a morphism between affine algebraic sets so $W = \mathrm{Spec}(B)$ and $V = \mathrm{Spec}(A)$ where B is an A-algebra. The reader will have no trouble generalizing this discussion to the case where V is a locally closed subscheme of $\mathbf{A}^n(\mathcal{O}_K)$. Then φ is a *finite morphism* if B is a finite dimensional module over A. We say that the finite morphism φ is a *cover* if φ is surjective and flat ([M 1; p. 424]). Every morphism $W \xrightarrow{\varphi} V$ is flat over a Zariski open subset of V ([D; p. 48]) by the theorem of *generic flatness*. The finite morphisms that occur in our algorithm are presented explicitly as follows: $W = \mathrm{Spec}(A[y]/(f(y)))$ (reduced as on page 9; i. e., $f(y)$ is a product of relatively prime irreducible factors to the first power) with $f(y)$ a monic polynomial in $A[y]$. In this case, φ is automatically flat and $A[y]/(f(y))$ is a free A-module. Hence, by [M 1, p. 432] φ is finite, and surjective. If W is given this way, and $P_1, \cdots, P_m$ are the polynomials of V, we say that the collection $\{P_1, \cdots, P_m; f\}$ consists of the *polynomials of the cover* $W \xrightarrow{\varphi} V$. The degree of $f(y)$ is denoted $\deg(W/V)$.

We say that the explicitly presented cover $W \xrightarrow{\varphi} V$ is *étale* if the discriminant of $f(y)$ (denoted D; see [M 1, p. 435]) is invertible in A.

Let $W \xrightarrow{\varphi} V$ be a cover and let $\mathrm{Aut}(W/V)$ be the set of automorphisms β of W such that β: $W \longrightarrow W$ is a commutative diagram. We say that



$W \xrightarrow{\varphi} V$ is a *Galois cover* if $|\mathrm{Aut}(W/V)| = \deg(W/V)$.

Let V be an irreducible algebraic set defined over K. We denote the field of rational functions on V defined over K by $K(V)$. Let $W \xrightarrow{\varphi} V$ be a Galois cover with W, φ, and V defined over K (φ has an affine structure as a cycle on $W \times V$), and assume that W is irreducible, and that $W \xrightarrow{\varphi} V$ is étale. Then $\mathrm{Aut}(W/V)$ is (non-canonically) isomorphic to the Galois group $G(K(W)/K(V))$. By an abuse of language we denote $\mathrm{Aut}(W/V)$ by $G(W/V)$ if $W \xrightarrow{\varphi} V$ is a Galois cover. *For the remainder of this paper the word cover refers to Galois, étale covers.*

We remark on the process by which covers arise in the course of our algorithm. We start with the following ingredients: an irreducible affine variety V' embedded as a locally closed subscheme of $\mathbf{A}^n(\mathcal{O}_K)$ (by an abuse

of terminology we write $V' \to \mathrm{Spec}(\mathcal{O}_K)$), and a finite Galois field extension $L/K(V')$ with an explicit set of generators. By taking a linear combination (with coefficients in $\mathbf{Q}$) of the generators of $L/K(V')$ and then multiplying by an element of $K(V')$ as in [W; p. 168] we can find an explicit generator (primitive element) for $L/K(V')$ such that $L \simeq K(V')[y]/(f(y))$ where $f(y) \in K(V')[y]$ is a monic polynomial with coefficients which are regular on V'. If we let $\mathcal{O}_K[V']$ denote the functions which are regular on V', then we obtain a morphism

$$\mathrm{Spec}\,(\mathcal{O}_K[V'][y]/(f(y))) \to V'. \tag{1.1}$$

In our terminology, (1.1) is not a cover because it is not étale. There is a Zariski open subset of V' over which the discriminant of $f(y)$ is invertible. This set is $\mathrm{Spec}\,(\mathcal{O}_K[V', 1/D_f])$, where D_f is the discriminant of f. We denote $\mathrm{Spec}\,(\mathcal{O}_K[V', 1/D_f])$ by V, and the pullback over V of $\mathrm{Spec}\,(\mathcal{O}_K[V'][y]/f(y))$ by $C(V)$. Thus we obtain an étale cover $C(V) \to V$.

Whenever we are given two connected covers $C_1(V) \to V$ and $C_2(V) \to V$ we shall usually (for simplicity's sake) *amalgamate* them: the two covers correspond, respectively, to Galois field extensions $K_1(V)$ and $K_2(V)$ of $K(V)$. Therefore the composite $K_1(V) \cdot K_2(V)$ is a Galois field extension of $K(V)$ whose group is a subgroup of $G(K_1(V)/K(V)) \times G(K_2(V)/K(V))$. Amalgamation consists of forming a cover corresponding to the field $K_1(V) \cdot K_2(V)$. Actually, this is easily seen to be the same cover as is obtained by taking a connected component of the fibered product $C_1(V) \times_V C_2(V)$ ([M 1; p. 61]).

B. The Frobenius symbol

Let $C(V) \xrightarrow{\varphi} V \to \mathcal{O}_K$ be a connected cover (étale and Galois by the assumptions of § 1. A). Let $w \in C(V)$, $v \in V$ be closed points (i.e., correspond to maximal ideals of the respective coordinate rings of $C(V)$ and V) with $\varphi(w) = v$ and let $\mathfrak{p}$ be the prime ideal of $\mathcal{O}_K$ corresponding to the image of v. Let S (respectively R) be the functions regular on $C(V)$ (respectively V) and let $\mathfrak{p}(w)$ (respectively $\mathfrak{p}(v)$) be the prime ideal of S (respectively R) corresponding to w (respectively v). Then $S/\mathfrak{p}(w)$ is a finite extension of $R/\mathfrak{p}(v)$ which in turn is a finite extension of the residue class field of the prime $\mathfrak{p}$ (because $\mathfrak{p}$ is not the 0-ideal). The group $G((S/\mathfrak{p}(w))/(R/\mathfrak{p}(v)))$ has a special generator Fr (the Frobenius element) obtained by putting the elements of $S/\mathfrak{p}(w)$ to the q-th power where $R/\mathfrak{p}(v)$ has order q. For $\alpha \in G(C(V)/V)$ there is induced a unique automorphism $\alpha^*: S \to S$ which is the identity on R, obtained by pullback of functions. If α^* maps $\mathfrak{p}(w)$ into $\mathfrak{p}(w)$ then α^* induces an automorphism of $S/\mathfrak{p}(w)$.

The *Frobenius element associated* to w, $\mathrm{Fr}(w)$, is the unique element of $G(C(V)/V)$ (unique because $C(V)/V$ is étale) such that $\mathrm{Fr}(w)^*$ induces the element Fr in $G((S/\mathfrak{p}(w))/(R/\mathfrak{p}(v)))$. If w' also lies over v then $\mathrm{Fr}(w)$ is conjugate to $\mathrm{Fr}(w')$ in $G(C(V)/V)$ ([CF; p. 14]). The *Frobenius class associated* to v, denoted $\mathrm{Fr}(v)$, is the conjugacy class in $G(C(V)/V)$ of $\mathrm{Fr}(w)$. We denote by $\deg(v)$ the degree of the residue class field of $\mathfrak{p}(v)$ over the residue class field of $\mathfrak{p}$.

We must make a remark relating our notation to standard notation in the special case $V = \mathrm{Spec}(\mathcal{O}_K[1/a])$. In this case our cover $C(V)$ is associated to a Galois extension M/K. As an element of $G(M/K)$, the Frobenius class associated to the prime ideal $\mathfrak{p}$ is usually denoted $\left(\frac{M/K}{\mathfrak{p}}\right)$, a notation we continue to use when it is appropriate.

Let M/K be a Galois extension of K. If $W \to \mathbf{A}^n(\mathcal{O}_M)$ is an affine algebraic variety defined over M, then for $\beta \in G(M/K)$ we have the *conjugate* ${}^{\beta}W \to \mathbf{A}^n(\mathcal{O}_M)$ of W by β, obtained by applying β to the coefficients of the polynomials describing W as a locally closed subscheme of $\mathbf{A}^n(\mathcal{O}_M)$.

We have need to consider a further concept regarding covers. Let $C(W) \to W$ will be an irreducible cover of T-schemes where T is any field. Let X be an irreducible subvariety of W, defined over T. We denote by $C(W)|_X$ the fibered product $C(W) \times_W X$ (pullback of $C(W)$ over X). Let C and C' be T-irreducible components of $C(W)|_X$ regarded as covers $C \to X$, and $C' \to X$. We remind the reader again that we use the word cover to designate that $C(W)$ is Galois and étale over W. We identify $G(C/X)$ with the subgroup of $G(C(W)/W)$ consisting of those automorphisms whose restriction to $C(W)|_X$ leaves C fixed. Also, the groups $G(C/X)$ and $G(C'/X)$ are *conjugate* subgroups in $G(C(W)/W)$. We refer to a representative of this conjugacy class of subgroups *as a decomposition group* of X.

C. Galois stratification and generalization of the diophantine problem

Let $A \to \mathbf{A}^n(\mathcal{O}_K)$ be a constructible subset (finite union of locally closed subschemes) of $\mathbf{A}^n$ defined over K. Suppose that all of the following structures are also defined over K:

(1.2) (a) a stratification $\mathfrak{S}(A)$ of A (that is, a decomposition of A into finitely many disjoint algebraic sets $A = \bigcup_{X \in \mathfrak{S}(A)} X$ where X is a locally closed subscheme of $\mathbf{A}^n$;

(b) for each $X \in \mathfrak{S}(A)$ a cover $C(X) \xrightarrow{\varphi(X)} X$;

(c) for each $X \in \mathfrak{S}(A)$ a union of conjugacy classes $\mathrm{Con}(X)$ in $G(C(X)/X)$, and;

(d) an element $\alpha(\mathfrak{A}) \in \mathcal{O}_K$ such that $A \to \mathcal{O}_K$ factors through $\mathrm{Spec}\,(\mathcal{O}_K[1/\alpha(\mathfrak{A})])$ (i. e. for $\mathfrak{p}$ dividing $\alpha(\mathfrak{A})$, the fiber $A_\mathfrak{p}$ is empty).

The morphism $\varphi(X)$ in (b) may be called $\varphi(X, C(X))$ when the context demands it. We call this collection a *Galois stratification of* A. Sometimes A will be referred to as the *underlying space* of the stratification. Galois stratifications will be denoted by Gothic letters $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\cdots$.

Let $\mathfrak{A}$ and $\mathfrak{A}'$ be two Galois stratifications. We say that $\mathfrak{A}'$ is *finer* than $\mathfrak{A}$ if $\alpha(\mathfrak{A})|\alpha(\mathfrak{A}')$; $A|_{\mathcal{O}_K[1/\alpha(\mathfrak{A}')]}$ (A pulled back over $\mathrm{Spec}\,(\mathcal{O}_K[1/\alpha(\mathfrak{A}')])$) is equal to A'; for each $X \in \mathbb{S}(A)$, $X|_{\mathcal{O}_K[1/\alpha(\mathfrak{A}')]}$ is a union of elements X' with $X' \in \mathbb{S}(A')$;

$$\begin{array}{ccc} C(X)|_{X'} & \xleftarrow{\ \psi\ } & C(X') \\ & {\scriptstyle \varphi(X, C(X))|_{X'}} \searrow \quad \swarrow {\scriptstyle \varphi(X', C(X'))} & \\ & X' & \end{array}$$

is a commutative triangle for some morphism ψ (necessarily a cover); and in this triangle $\mathrm{Con}\,(X')$ consists of all elements of $G(C(X')/X')$ whose restrictions (images under ψ) to $C(X)|_{X'}$ are in $\mathrm{Con}\,(X)|_{X'}$. We shall feel free, throughout this paper, to replace any Galois stratification by a finer Galois stratification whenever this does not affect the consideration of our basic problem (e. g., as in the diophantine problems discussed below).

Similarly for any ring R we may define the notion of a Galois stratification of a locally closed subscheme $A \to \mathbf{A}^n(R)$ (denoted $\mathfrak{A} \to R$ by abuse of notation). We define a *full Galois stratification* over K to consist of a Galois stratification $\mathfrak{A} \to \mathcal{O}_K$ (or we might write this as $\mathfrak{A} \to \mathcal{O}_K[1/\alpha(\mathfrak{A})]$) together with a collection of Galois stratifications $\mathfrak{B}_\mathfrak{p} \to \mathcal{O}_K/\mathfrak{p}$ where $\mathfrak{p}$ runs over the primes dividing $\alpha(\mathfrak{A})$. We do not ask that the $\mathfrak{B}_\mathfrak{p}$'s be related to each other for different values of $\mathfrak{p}$; in particular we may have $\mathfrak{B}_\mathfrak{p}$ empty.

For $\mathfrak{p}$ a prime of $\mathcal{O}_K$ we let $C(X_\mathfrak{p}) \to X_\mathfrak{p}$ be the reductions (as in § 1. A) modulo $\mathfrak{p}$, of the members of the stratification $\mathbb{S}(A)$. Note that from our étaleness assumption $G(C(X_\mathfrak{p})/X_\mathfrak{p})$ is identified canonically with a conjugacy class of subgroups of $G(C(X)/X)$. If $v \in X$ lies over the point of $\mathrm{Spec}\,(\mathcal{O}_K)$ associated to $\mathfrak{p}$, and if $\deg(v) = 1$, then v modulo $\mathfrak{p}$ is an $\mathcal{O}_K/\mathfrak{p}$-valued point $(\underset{\sim}{x}_1^0, \cdots, \underset{\sim}{x}_n^0) \in X_\mathfrak{p}$. When no confusion occurs, we make one last abuse of notation and we write Fr_v as $\mathrm{Fr}\,(\underset{\sim}{x}_1^0, \cdots, \underset{\sim}{x}_n^0; \mathfrak{p})$ (or $\mathrm{Fr}\,(\underset{\sim}{x}_1^0, \cdots, \underset{\sim}{x}_n^0)$). By the notation

$$\mathrm{Fr}\,(\underset{\sim}{x}_1^0, \cdots, \underset{\sim}{x}_n^0) \in \bigcup_{X \in \mathbb{S}(A)} \mathrm{Con}\,(X)\,, \tag{1.3}$$

we mean: $(\underset{\sim}{x}_1^0, \cdots, \underset{\sim}{x}_n^0) \in X_\mathfrak{p}$ for some $X \in \mathbb{S}(A)$, and; $\mathrm{Fr}\,(\underset{\sim}{x}_1^0, \cdots, \underset{\sim}{x}_n^0) \in \mathrm{Con}\,(X)$.

Let $\mathfrak{A}$ be a full Galois stratification with underlying space A. As in

Section 0.A we may consider (problem $(\bar{P})_{\bar{\varphi}}$ of the introduction)

$$(P) \qquad (Q_1\underset{\sim}{x}_1)\cdots(Q_n\underset{\sim}{x}_n)[\mathrm{Fr}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n) \in \bigcup_{X\in\mathfrak{S}(A)} \mathrm{Con}(X)] .$$

In Section 4 we give our algorithm for deciding if (P) is true for all primes $\mathfrak{p}$ (or almost all primes $\mathfrak{p}$ of $\mathcal{O}_K$) where, for $\mathfrak{p}$ dividing $\alpha(\mathfrak{A})$, (P) must be interpreted as being given by the Galois stratification $\mathfrak{B}_{\mathfrak{p}} \to \mathcal{O}_K/\mathfrak{p}$.

Now, suppose we are given a Galois stratification $\mathfrak{A} \to \mathbf{A}^n(\mathcal{O}_K)$. We denote by $\mathbf{A}^{n-1}$ the affine space with coordinates $\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_{n-1}$. In Section 4 we give a primitive recursive algorithm to calculate a new Galois stratification $\mathrm{pr}(\mathfrak{A}) \to \mathbf{A}^{n-1}(\mathcal{O}_K)$ having the following property. Let B be the underlying space of $\mathrm{pr}(\mathfrak{A})$. Then for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K[1/\alpha(\mathrm{pr}(\mathfrak{A}))]$,

$$(Q_n\underset{\sim}{x}_n)[\mathrm{Fr}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n) \in \bigcup_{X\in\mathfrak{S}(A)} \mathrm{Con}(X)]$$

is equivalent to

$$[\mathrm{Fr}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_{n-1}) \in \bigcup_{Y\in\mathfrak{S}(B)} \mathrm{Con}(Y)] .$$

Then we answer the question "Is (P) true in $\mathcal{O}_K/\mathfrak{p}$ for all (or almost all) primes $\mathfrak{p}$?" by the procedure of Section 0.A. The Galois stratification $\mathrm{pr}(\mathfrak{A})$ depends on Q_n. Also, $\alpha(\mathrm{pr}(\mathfrak{A}))$ depends on the degrees of the polynomials defining A and B (as in § 1. A) as well as on $\underset{\sim}{n}$. The source of this dependency is the fact we can guarantee that an absolutely irreducible projective variety over a finite field has rational points only if the order of the finite field is larger than an explicitly computable quantity which is a function of the degree and dimension of the variety. This fact (a consequence of the Riemann hypothesis for *curves* over finite fields, see [LW]) appears in somewhat disguised form in our use of the non-regular analogue of the Čebotarev density theorem (§ 4 and [F]).

2. The intersection-union process

A. The intersection-union process over a finite field

Let k be a finite field. Let W be a locally closed subscheme of $\mathbf{A}^n(k)$, and let $IU(W, k)$ be $\{X | X$ is a maximal absolutely irreducible subset of W defined over $k\}$. N. Greenleaf ([G]) defined and gave a procedure for calculating $IU(W, k)$.

LEMMA 2.1. *There is a primitive recursive function $g(W, k)$ which for a given (code number for) set W computes (the code number for) a finite sequence of algebraic set $\langle U_1, \cdots, U_n\rangle$ which are the elements of $IU(W, k)$.*

Proof. We first give an informal algorithm to compute $IU(W, k)$. Then we will convert this informal algorithm into an explicit calculation of a

primitive recursive function which computes $IU(W, k)$.

Write W as a union of absolutely irreducible varieties $W = W_1 \cup \cdots \cup W_l$ where $W_1, \cdots, W_l$ (the first stage varieties) are defined over a finite Galois extension k_v ($[k_v: k] = v$). Let $\sigma \in G(k_v/k)$ be the Frobenius generator (q^{th} power map on k_v where $q = |k|$). We let $v = v(1)$. Then σ permutes the W_i among each other. We form $\bigcap_{r=0}^{v-1} {}^{\sigma^r}W_i$ ($i = 1, \cdots, l$), which is an algebraic set defined over k.

Let $W_{i1} \cup \cdots \cup W_{il(i)}$ be the absolutely irreducible varieties in $\bigcap_{r=0}^{v-1} {}^{\sigma^r}W_i$ (*these are the 2nd stage varieties*). Assume that $W_{i1}, \cdots, W_{il(i)}$ are all defined over $k_{v(2)}$. We continue with the W_{ij}'s forming $k_{v(3)}$ and $\bigcap_{r=0}^{v(2)-1} {}^{\sigma^r}W_{ij} = W_{ij1} \cup \cdots \cup W_{ijl(ij)}$ a union of absolute irreducible varieties defined over $k_{v(3)}$. Continue, stage by stage. We say the *process stops at the t^{th} stage* if the t^{th} stage varieties are exactly the same as the $(t+1)^{\text{th}}$ stage varieties. This is equivalent to the statement: the t^{th} stage varieties are all absolutely irreducible subvarieties of W, *defined over* k. Note that every element of $IU(W, k)$ is a member of the last stage. If, at the i^{th} stage, a variety V appears which is not defined over k, then at the $i+1^{\text{th}}$ stage, V is replaced by a finite collection of varieties of dimension less than the dimension of V. Therefore, the process stops at the t^{th} stage where t is at most the dimension of W plus 1.

We now give the formal calculation of a primitive recursive function to compute $IU(W, k)$. Let $|k| = q$. Then $|k|$ is computable from k by a primitive recursive function. We simplify notation by writing k_i in place of $k_{v(i)}$. Let $g_0(W, k) = (k_1, \langle W_1, \cdots, W_l\rangle)$, where k_1 is a finite Galois extension of k, $\langle W_1, \cdots, W_l\rangle$ is (the code number for) a finite sequence of absolutely irreducible algebraic sets defined over k_1, and $W = W_1 \cup \cdots \cup W_l$. The function g_0 is primitive recursive as was noted in the introduction. Let $g_1(W, k, k_1)$ be defined for k_1, a finite Galois extension of k of degree $v(1)$ and W is defined over k, by the function $g_1(W, k, k_1) = \bigcap_{r=0}^{v-1} {}^{\sigma^r}W$, where σ is the automorphism of k_1/k given by $\sigma(x) = x^q$. The function g_1 is primitive recursive since $[k_1: k]$ is, and so is the function which computes ${}^{\sigma^r}W$ for each r. If

$$g_0(W_i, k_1) = \langle k(i), \langle W_{i1}, \cdots, W_{il(i)}\rangle\rangle ,$$

let

$$g_2(\langle W_1, \cdots, W_l\rangle, k) = \langle k_1, \langle g_1(W_{11}, k, k_2), \cdots, g_1(W_{ij}, k, k_2) \cdots\rangle\rangle$$

where $k_2 = k(1) \cdots k(l)$. Then the function g_2 is primitive recursive since it is the composition of primitive recursive functions. We now define a function $g_3(\langle W_1, \cdots, W_l\rangle, k, n)$ by induction on n. Let

$$g_3(\langle W_1, \cdots, W_l\rangle, k, 0) = \langle k, \langle W_1, \cdots, W_l\rangle\rangle ,$$

and inductively

$$g_3(\langle W_1, \cdots, W_l\rangle, k, n+1) = g_2(g_3(\langle W_1, \cdots, W_l\rangle, k, n)) .$$

The desired function $g(W, k)$ is $\pi_2(g_3(\langle W\rangle, k, m))$ where π_2 is projection onto the second component, and $m = 1 + \dim W$. This will be a sequence of absolutely irreducible algebraic sets. These sets are defined over k. In fact, if one of the algebraic sets U computed in $g_3(\langle W\rangle, k, n)$ were not defined over k, then at the $n+1^{\text{th}}$ stage U would be replaced by a union of algebraic sets of lower dimension of the function g_2. Thus $IU(W, k)$ is the sequence of sets produced by the primitive recursive function $g(W, k)$.

Let $C(W) \to W$ be a cover, which we may assume is connected. If $X \in IU(W, k)$ we consider the pullback

$$\begin{array}{ccc} C(W)|_X & \hookrightarrow & C(W) \\ \downarrow & & \downarrow \\ X & \hookrightarrow & W . \end{array}$$

Then, as a locally closed subscheme of $\mathbf{A}^n(k)$, X has a closure $\bar{X}$ in $\mathbf{A}^n$. We define $\deg(\bar{X} - X)$ (resp. $\dim(\bar{X} - X)$) to be the collection of degrees (resp. dimensions) of the k-irreducible components of $\bar{X} - X$. All the connected components of $C(W)|_X$ are isomorphic and each has Galois group $H(C, X)$ (as a cover of X) isomorphic to a subgroup of $G(C(W)/W)$ as in Section 1. B. Let $k(C)$ be the field of k-rational functions on C. Let $\hat{k}$ be the algebraic closure of k in $k(C)$, and let $\hat{H}(C, X)$ be the subset of elements which induce the Frobenius element on $\hat{k}$.

Definition 2.1. The *type* of $IU(W, k)$ is the finite sequence of 6-tuples

$$\{(\deg X, \dim X, \deg(\bar{X} - X), \dim(\bar{X} - X), H(C, X), \hat{H}(C, X))\}$$

for all $X \in IU(W, k)$.

B. The intersection-union process over a perfect field

We generalize the intersection-union process to define $IU(W, T)$ where T is any perfect field with $W \subseteq \mathbf{A}^n(T)$ a locally closed subscheme defined over T. We define $IU(W, T)$ to be the collection of pairs (U, σ) computed by the following algorithm:

Stage 1: Write $W = W_1 \cup \cdots \cup W_l$ where $W_1, \cdots, W_l$ (the *first stage varieties*) are absolutely irreducible varieties defined over $T(1)$ where $T(1)$ is a Galois extension of T. For each $\sigma(1) \in G(T(1)/T)$ and each integer i ($|\sigma(i)|$ denotes the order of $\sigma(i)$), we form

$$\bigcap_{r=0}^{|\sigma(1)|-1} \sigma(1)^r W_i = W_{\sigma(1);i1} \cup \cdots \cup W_{\sigma(1);il(i)}$$

where the absolutely irreducible varieties $W_{\sigma(1);i1}, \cdots, W_{\sigma(1);il(i)}$ are the *second stage varieties*. There is a Galois extension $T(2)/T$ such that all the second stage varieties are defined over $T(2)$ and $T(2) \supset T(1)$. For each pair $(\sigma(1), \sigma(2))$ where $\sigma(2) \in G(T(2)/T)$ and $\sigma(1)$ is the restriction of $\sigma(2)$ to $T(1)$ we consider

$$\bigcap_{r=0}^{|\sigma(2)|-1} \sigma(2)^r W_{\sigma(1);ij} = W_{\sigma(2);ij1} \cup \cdots \cup W_{\sigma(2);ijl(ij)}$$

(absolutely irreducible varieties, the 3rd stage varieties). *Inductively*, we form:

$$W_{\sigma(u-1);\underset{\sim}{i}1} \cup \cdots \cup W_{\sigma(u-1);\underset{\sim}{i}l(\underset{\sim}{i})} \text{ and } T(u)$$

where $\underset{\sim}{i}$ is a $(u-1)$-tuple of integers, and; $T(u)$ is a Galois extension of $T(u-1)$ such that all the u^{th} stage varieties are defined over $T(u)$. Then, for $\sigma(u) \in G(T(u)/T)$ such that $\sigma(u)|_{T(i)} = \sigma(i)$ we form the $(u+1)^{\text{th}}$ stage varieties from the formula:

$$W_{\sigma(u);\underset{\sim}{\bar{i}}1} \cup \cdots \cup W_{\sigma(u);\underset{\sim}{\bar{i}}l(\underset{\sim}{\bar{i}})} \text{ is equal to } \bigcap_{v=0}^{|\sigma(u)|-1} \sigma(u)^r W_{\sigma(u-1);\underset{\sim}{\bar{i}}_u}$$

where $\underset{\sim}{\bar{i}}_u$ is a u-tuple of positive integers. As in the previous intersection-union process, this "*stops*" at a stage prior to the $\dim(W) + 2$nd stage where "stops" means that from some point on we get the same varieties. For simplicity we assume that the intersection union process stops at the $(\dim(W) + 1)^{\text{th}}$ stage (if it stops before, just continue until this stage). We let $T^* = T^*(IU(W, T))$ be the last stage field. For each $\sigma \in G(T^*/T)$ we have the last stage varieties corresponding to the chain of restrictions of σ to $T(i)$ (denoted $\sigma(i)$). We denote the collection of last stage varieties by $IU(W, T, \sigma)$. The verification that this calculation is primitive recursive is very similar to the previous verfication with the addition of the primitive recursive calculation involving the elements of $G(T^*/T)$.

Given a cover $C(W) \to W$ we let $H(C(W), X)$ be the subgroup of $G(C(W)/W)$ obtained from a connected component of $C(W)|_X \to X$, as above.

Definition 2.2. The *type* of $IU(W, T)$ (where W is equipped with a cover $C(W) \to W$, also defined over T) is defined to be the collection of types

$$\{(\deg X, \dim X, \deg(\bar{X} - X), \dim(\bar{X} - X), H(C(W), X))\}$$

where the collection is indexed by the pairs (σ, X) with $\sigma \in G(T(IU(W, T))/T)$ and $X \in IU(W, T, \sigma)$ (see Definition 2.1.)

Let W be a variety defined over T. Assume that W is equipped with a stratification $\mathcal{S}(W)$ such that for $Y \in \mathcal{S}(W)$, Y is equipped with a cover $C(Y) \to Y$ defined over T. In this case we define the *type of* $IU(W, T)$ *to be*

the union of the types of $IU(Y, T)$ *for* $Y \in \mathbb{S}(W)$. From the methods of the proof of Lemma 2.1 we have

LEMMA 2.2. $IU(W, T)$, $IU(W, T, \sigma)$, T^*, *and the types of* $IU(W, T)$ *are all primitive recursive functions.*

3. A generalization of the theorems of Bertini and Noether

We use the notations from Sections 1 and 2. We make one comment on the degree of an algebraic set. The notion of degree of an algebraic set is most suitable for projective varieties. Therefore, if $A \to \mathbf{A}^n$ is a locally closed subscheme of $\mathbf{A}^n$ (not necessarily irreducible) of dimension r, we define the *degree of* A ($\deg(A)$) to be the degree of the projective variety (intersection multiplicity with $n_1 + n_2 + \cdots + n_n - r$ hyperplane sections) obtained by taking the closure of A in $\mathbf{P}^n$.

Let $W \xrightarrow{\varphi} V$ be a morphism of $\mathcal{O}_K$-schemes which are irreducible as K-schemes such that $W \to V$ and $V \to \mathcal{O}_K$ are dominant (generically surjective; see § 1. A). Let $\tilde{x}^{\text{gen}}$ be a generic point of V. Consider the generic fiber, $W_{\tilde{x}^{\text{gen}}}$, of the morphism φ. We assume that

(3.1) $\qquad W_{\tilde{x}^{\text{gen}}}$ is *absolutely irreducible* over $K(\tilde{x}^{\text{gen}})$

(the field generated by the coordinates of $\tilde{x}^{\text{gen}}$ over K). We explain this further in the case most relevant to our applications by assuming that W and V are affine varieties: $W = \operatorname{Spec}(S)$, $V = \operatorname{Spec}(R)$ where S is an R algebra, and $S = \mathcal{O}_K[\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n]/I$, I an ideal of $\mathcal{O}_K[\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n]$. Then $K(\tilde{x}^{\text{gen}})$ may be identified with the quotient field of R (and in scheme theoretic language it *is indeed* canonically so identified). Consider $\operatorname{Spec}(\bar{M}[\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n]/I)$ where I is regarded as an ideal in $\bar{M}[\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n]$, and $\bar{M}$ is an algebraic closure of the quotient field of R. Condition (3.1) is equivalent to: $\operatorname{Spec}(\bar{M}[\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n]/I)$ is irreducible as an $\bar{M}$-variety. For p a closed point of V we let k_p denote the residue class field of p. The following result is well-known.

LEMMA 3.1 (*Bertini and Noether*). *With notation as above, if condition* (3.1) *holds, then there exists an explicitly computable Zariski open subset* (*non-empty*) U *of* V *such that for each closed point* $p \in U$, W_p *is absolutely irreducible as a variety over* $\operatorname{Spec}(k_p)$.

Comments on the proof (for the convenience of the reader). From [M 1; Corollary 1, p. 96] there is an explicitly computable Zariski open subset $U_1 \subset V$ such that for $p \in U_1$, the components of W_p each have dimension r (where r is the dimension of $W_{\tilde{x}^{\text{gen}}}$). From [M 1; Normalization Lemma on p. 253-255] we may form

$$W' \xhookrightarrow{\varphi} \mathbf{A}^{r+1} \times V \xrightarrow{\mathrm{pr}_1} \mathbf{A}^{r+1}$$
$$\xrightarrow{\mathrm{pr}_2} V,$$

such that for $p \in V$, the fiber W'_p is presented as a hypersurface in $\mathbf{A}^{r+1}$ by the restriction of $\mathrm{pr}_1 \cdot \varphi$ to W'_p, and there exists a Zariski open subset $U_2 \subset U_1$ such that for $p \in U_2$ each component of W'_p is birational to W_p.

From this construction we are reduced to proving the lemma in the case that $W' \to \mathbf{A}^{r+1} \times V$ is a family of hypersurfaces in $\mathbf{A}^{r+1}$. We now give an outline of the proof in this case.

Let $y_1, \cdots, y_{r+1}$ be the variables of $\mathbf{A}^{r+1}$. We are reduced in the above to considering a polynomial $g \in R[y_1, \cdots, y_{r+1}]$; $V = \mathrm{Spec}(R)$ where $R = \mathcal{O}_K[z_1, \cdots, z_t]/J$ and J is an ideal of $\mathcal{O}_K[z_1, \cdots, z_t]$. For p a closed point of V we define g_p to be the polynomial obtained by reduction of the coefficients of g modulo the prime of R corresponding to p. We show that for each integer l with $1 \leqq l \leqq \deg(g) - 1$ there is an open (non-empty) subset $U^{(l)}$ of V such that for p a closed point of $U^{(l)}$, g_p has no divisor of degree l over $\bar{k}_p$ (an algebraic closure of k_p). The open subset $\bigcap_{l=1}^{\deg(g)-1} U^{(l)}$ is the open set satisfying the conclusion of the lemma.

Let f be a polynomial over an algebraically closed field $\bar{F}$ in the variables $y_1, \cdots, y_{r+1}$, where $\deg f = \deg g$. Supposed that f factors into $f_1 = \sum a_{\underset{\sim}{i}} y^{\underset{\sim}{i}}$ and $f_2 = \sum b_{\underset{\sim}{i}} y^{\underset{\sim}{i}}$ with $\deg f_1 = l$. Then, for a fixed collection $\{b_{\underset{\sim}{i}}\}$, the collection $\{a_{\underset{\sim}{i}}\}$ is a solution of a set of linear equations. Thus, from basic linear algebra, $\{b_{\underset{\sim}{i}}\}$ gives a solution of a set of polynomials P which are polynomials in the coefficients of f. From Hilbert's Nullstellensatz, the collection P has this common solution $\{b_{\underset{\sim}{i}}\}$ if and only if another collection of polynomials P', in the coefficients of the polynomials of P, are zero. Thus, there exist universal polynomials P'' in the coefficients of f such that f is reducible if and only if the polynomials of P'' are zero. Suppose that the collection P'' consists of $\bar{t}$ polynomials. Then we obtain a morphism ψ from $V = \mathrm{Spec}(R)$ to $\mathbf{A}^{\bar{t}}(R)$: for $p \in V$,

$$p \xrightarrow{\psi} \{\text{the evaluation of the } \bar{t} \text{ polynomials of } P'' \text{ at the coefficients of } g_p\}.$$

If $\tilde{x}^{\mathrm{gen}}$ is a generic point of V, then the assumptions of the lemma imply that $\psi(\tilde{x}^{\mathrm{gen}})$ is distinct from the origin of $\mathbf{A}^{\bar{t}}$. Therefore, if we let V_0 be the fiber of V over the origin of $\mathbf{A}^{\bar{t}}(R)$ then $V - V_0$ is the set $U^{(0)}$ sought in the paragraph above. With this we conclude the proof of the lemma.

Now we consider the morphism pr_{n-1}: $\mathbf{A}^{\underset{\sim}{n}} \to \mathbf{A}^{\underset{\sim}{n-1}} = \mathbf{A}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_{n-1})$ obtained by projection of $(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n)$ onto the first $(n-1)$-tuples of the

collection of coordinates. Let A be a locally closed subscheme of $\mathbf{A}^n_{\sim}(\mathcal{O}_K)$ (dominant over Spec $(\mathcal{O}_K)$; see § 1. A). Proposition 3.1 shows, roughly, that $\mathrm{pr}_{\underset{\sim}{n-1}}(A)$ may be stratified so that the elements of the stratification indicate the types of the intersection-union process applied to the fibers of $\mathrm{pr}_{\underset{\sim}{n-1}}$. This proposition collects together the technical difficulties of the production of the Galois stratification pr $(\mathfrak{A})$ (as in § 0. A). We retain the name Galois stratification for the objects with underlying space $\mathrm{pr}_{\underset{\sim}{n-1}}(A)$ produced in Proposition 3.1 even though they lack the conjugacy class structure (Con(Y) for $Y \in \mathbb{S}(\mathrm{pr}_{n-1}(A))$). The conjugacy class structure will be added, along with some adjustment, in Section 4. Also, in Proposition 3.1 we consider only locally closed subschemes of $\mathbf{A}^n_{\sim}(\mathcal{O}_K)$ and $\mathbf{A}^{n-1}_{\sim}(\mathcal{O}_K)$ which are dominant over $\mathcal{O}_K$ (see § 1. A).

PROPOSITION 3.1 (*Generalization of Bertini and Noether theorems*).

(a) *Let $A \to \mathcal{O}_K$ be a constructible subscheme of $\mathbf{A}^n_{\sim}(\mathcal{O}_K)$. Then there exists a Galois stratification $\mathbb{S}(\mathrm{pr}_{\underset{\sim}{n-1}}(A))$ of $\mathrm{pr}_{\underset{\sim}{n-1}}(A)$ such that: for each $Y \in (\mathrm{pr}_{\underset{\sim}{n-1}}(A))$ and for each closed point $\underset{\sim}{y}^0 = (\underset{\sim}{y}^0_1, \cdots, \underset{\sim}{y}^0_{n-1}) \in Y$ of degree* 1 (i. e., *$\underset{\sim}{y}^0$ lies over the maximal prime $\mathfrak{p}$ of $\mathcal{O}_K$ and is an $\mathcal{O}_K/\mathfrak{p}$-valued point of $Y_{\mathfrak{p}}$), the type of $IU(A_{\underset{\sim}{y}^0}, \mathcal{O}_K/\mathfrak{p})$ depends only on* Fr $(\underset{\sim}{y}^0_1, \cdots, \underset{\sim}{y}^0_{n-1})$.

(b) *Let $C(A) \to A$ be a K-irreducible cover (Galois and étale, as always) of A, with A a locally closed subscheme of $\mathbf{A}^n_{\sim}(\mathcal{O}_K)$. Then there exists a Galois stratification $\mathbb{S}'(\mathrm{pr}_{\underset{\sim}{n-1}}(A))$ such that: for each $Y \in \mathbb{S}'(\mathrm{pr}_{\underset{\sim}{n-1}}(A))$ and for each closed point $\underset{\sim}{y}^0 \in Y$ of degree* 1, *the type of $IU(A_{\underset{\sim}{y}^0}, \mathcal{O}_K/\mathfrak{p})$ (as in Definition* 2.1) *depends only on* Fr $(\underset{\sim}{y}^0_1, \cdots, \underset{\sim}{y}^0_{n-1})$. (*Here $A_{\underset{\sim}{y}^0}$ is equipped with the cover $C(A)$ restricted to $A_{\underset{\sim}{y}^0}$ as in Definition* 2.2).

Proof. Stratify A into K-irreducible locally closed subschemes, $X \in \mathbb{S}(A)$ of $\mathbf{A}^n_{\sim}(\mathcal{O}_K)$. For each such subscheme X we show that the conclusion of part (a) of the proposition holds for some Galois stratification $\mathbb{S}_X$ with underlying space $\mathrm{pr}_{\underset{\sim}{n-1}}(X)$. We then combine these Galois stratifications into a Galois stratification of $\mathrm{pr}_{\underset{\sim}{n-1}}(A)$ by the following rules. For $Y \in \mathbb{S}(\mathrm{pr}_{\underset{\sim}{n-1}}(A))$ and each $X \in \mathbb{S}(A)$, either $Y \cap \mathrm{pr}_{\underset{\sim}{n-1}}(X) = \varnothing$ or Y is a locally closed K-subscheme of some $Z \in \mathbb{S}_X$. List these Z's as $Z_1, \cdots, Z_t$. Then the cover $C(Y) \to Y$ is obtained as the amalgamation of the covers of Y obtained by the restriction of the covers $C(Z_i) \to Z_i$, $i = 1, \cdots, t$ to Y (as in § 1. A). From this procedure we need only prove Proposition 3.1(a) for the case where A is a K-irreducible locally closed subscheme of $\mathbf{A}^n_{\sim}(\mathcal{O}_K)$.

First we stratify $\mathrm{pr}_{\underset{\sim}{n-1}}(A)$ into K-irreducible, locally closed subschemes of $\mathrm{pr}_{\underset{\sim}{n-1}}(A)$. Denote this stratification by $\mathbb{S}_1(\mathrm{pr}_{\underset{\sim}{n-1}}(A)) = \mathbb{S}_1$. Let $Y \in \mathbb{S}_1$ and

let $K(Y)$ be the field of rational functions on Y. Then $K(Y) = K(\underset{\sim}{y}^{\text{gen}})$ where $\underset{\sim}{y}^{\text{gen}}$ is a generic point on Y and $K(\underset{\sim}{y}^{\text{gen}})$ is the field generated over K by the coordinates of $\underset{\sim}{y}^{\text{gen}}$. Let $A_{\underset{\sim}{y}^{\text{gen}}}$ be the fiber of $A|_Y \to Y$ (notation of §1. B) over the generic point of Y. Let T_Y^* be the field $T^*(IU(A_{\underset{\sim}{y}^{\text{gen}}}, K(Y)))$, the field obtained from the intersection-union process (§ 2. B). Then T_Y^* is a finite Galois extension of $K(Y)$. For each $\sigma \in G(T_Y^*/K(Y))$ the intersection-union process displays a collection of absolutely irreducible subsets of $A_{\underset{\sim}{y}^{\text{gen}}}$ (defined over T_Y^*). Let $W_{\sigma;i_1,\cdots,i_j}$ be one of the j^{th} stage varieties; $W_{\sigma,i_1,\cdots,i_{j+1}}$ (a variety of the $(j+1)^{\text{th}}$ stage) one of the components of the intersection $\bigcap_r {}^{\sigma^r} W_{\sigma;i_1,\cdots,i_j}$.

From $T_Y^*/K(Y)$ we obtain a cover (étale and Galois, as always) $C(Z) \to Z$ of a Zariski K-open subset Z of Y. See the discussion preceding expression (1.1) of §1.A. For $\sigma \in G(C(Z)/Z)$ consider $C(Z) \to C^{(\sigma)}(Z) \to Z$ where $C(Z)/C^{(\sigma)}(Z)$ is a cover with Galois group generated by σ. Let $A|_{C^{(\sigma)}(Z)} \to C^{(\sigma)}(Z)$ be the pullback of A over $C^{(\sigma)}(Z)$, $\underset{\sim}{z}^0$ any degree 1 closed point of Z, $\underset{\sim}{\bar{z}}^0$ a point of $C^{(\sigma)}(Z)$ over $\underset{\sim}{z}^0$, and $\underset{\sim}{\bar{\bar{z}}}^0$ a point of $C(Z)$ over $\underset{\sim}{\bar{z}}^0$. We now show that we can replace Z by a Zariski K-open subset of Z (which we still refer to as Z) so that for $\sigma = \text{Fr}(\underset{\sim}{\bar{\bar{z}}}^0)$ and $\mathfrak{p}$ the prime of $\mathcal{O}_K$ beneath $\underset{\sim}{z}^0$:

$$(IU(A_{\underset{\sim}{y}^{\text{gen}}}, K(Y), \sigma))_{\underset{\sim}{\bar{z}}^0} = IU((A|_{C^{(\sigma)}(Z)})_{\underset{\sim}{\bar{z}}^0}, \mathcal{O}_K/\mathfrak{p}) . \tag{3.1}$$

The left side of expression (3.1) denotes the collection of varieties obtained by specialization of the coefficients of the polynomials defining the varieties of $IU(A_{\underset{\sim}{y}^{\text{gen}}}, K(Y), \sigma)$, at the place corresponding to $\underset{\sim}{\bar{\bar{z}}}^0$. The expression $(A|_{C^{(\sigma)}(Z)})_{\underset{\sim}{\bar{z}}^0}$ is the fiber of $A|_{C^{(\sigma)}(Z)} \to C^{(\sigma)}(Z)$ over the point $\underset{\sim}{\bar{z}}^0$. We note that expression (3.1) implies that:

(3.2) The type of the right side of (3.1) is dependent only on σ (actually on the conjugacy class of σ) for $\underset{\sim}{z}^0 \in Z$.

We abuse notation and let $W_{\sigma, \underset{\sim}{y}^{\text{gen}}}$ be one of the varieties appearing in one of the stages of the construction of $IU(A_{\underset{\sim}{y}^{\text{gen}}}, K(Y), \sigma)$. The coefficients of the polynomials defining $W_{\sigma, \underset{\sim}{y}^{\text{gen}}}$ generate a field M over the field of K-regular functions, $K(C^{(\sigma)}(Z))$, on $C^{(\sigma)}(Z)$. We have $C(Z) \to C' \to C^{(\sigma)}(Z)$ where $K(C')$ is M. We may regard $W_{\sigma, \underset{\sim}{y}^{\text{gen}}}$ as the generic fiber of a morphism $W_\sigma \xrightarrow{\varphi_\sigma} C'$.

In addition to properties (3.1) and (3.2) we construct Z so that for each σ and each W_σ:

(3.3) (a) φ_σ has constant fiber dimensions;

(b) the degrees of the geometric fibers of φ_σ are constant;

(c) for $\underset{\sim}{\bar{z}}' \in C'$ lying over $\underset{\sim}{\bar{z}}^0 \in C^{(\sigma)}(Z)$, the field generated by the coeffici-

ents of the polynomials defining $(W_\sigma)_{\underset{\sim}{z}'}$ (as an extension of $\mathcal{O}_K[C^{(\sigma)}(Z)]/\mathfrak{p}(\underset{\sim}{z}^0)$) is $\mathcal{O}_K[C']/\mathfrak{p}(\underset{\sim}{z}')$ (notation as in § 1. B).

Assume that for each $Y \in \mathcal{S}_1(\mathrm{pr}_{\underset{\sim}{n-1}}(A))$, a (non-empty) Zariski K-open subset Z has been selected so that (3.1) (therefore (3.2)) holds. Then the conclusion of Proposition (3.1) (a) holds for a constructible subset Y' of $\mathrm{pr}_{\underset{\sim}{n-1}}(A)$, where $\mathrm{pr}_{\underset{\sim}{n-1}}(A) - Y'$ is of lower dimension than $\mathrm{pr}_{\underset{\sim}{n-1}}(A)$. Using induction on the dimension of the elements of $\mathcal{S}_1(\mathrm{pr}_{\underset{\sim}{n-1}}(A))$, we may consider the restriction of $A \to \mathrm{pr}_{\underset{\sim}{n-1}}(A)$ to the complement of Y' in $\mathrm{pr}_{\underset{\sim}{n-1}}(A)$ to form a stratification of $\mathrm{pr}_{\underset{\sim}{n-1}}(A)$ which satisfies the conclusion of Proposition (3.1)(a).

From the *theorem of generic flatness* ([M 2; p. 57]) there exists an element $f \in \mathcal{O}_K[Z]$ so that for $Z^* = \mathrm{Spec}\,(\mathcal{O}_K[Z, 1/f])$, $W_\sigma|_{Z^*} \xrightarrow{\varphi_\sigma|_{Z^*}} C'|_{Z^*}$ is flat.

In [M 2] the choice of f can be made primitive recursive (explicit) by the use of the explicitly constructive form of the Noether normalization lemma that appears in [S].

Let $\bar{W}_\sigma|_{Z^*}$ be the closure of W_σ in $P^n_{\sim} \times_{\mathcal{O}_K} (C'|_Z)$. Since $\bar{W}_\sigma|_{Z^*} \to C'|_{Z^*}$ is flat, the conservation of number (see the argument of [M 2; p. 83]) shows that the geometric fibers have constant degree. By replacing Z by Z^* we have shown that Z may be chosen to satisfy (3.3) (a) and (b).

Let $c_1, \cdots, c_l \in \mathcal{O}_K[C']$ be the coefficients of the explicit polynomials representing W_σ. Consider a linear combination $\alpha = \sum_{j=1}^{l} a_j c_j$, of $c_1, \cdots, c_l$, such that: $a_1, \cdots, a_l \in \mathbf{Z}$, and if $c_j^{(1)}, \cdots, c_j^{(n(j))}$ are the conjugates of c_j over $K(C^{(\sigma)}(Z))$, then $\sum_{j=1}^{l} a_j c_j^{(r(j))} \neq \alpha$ for $r(j)$ any integer between 1 and $n(j)$. Kronecker's lemma implies that $K(C^{(\sigma)}(Z), \alpha) = K(C')$. Let $f_\alpha(y) \in \mathcal{O}_K[C^{(\sigma)}(Z)][y]$ be the monic irreducible polynomial for α over $\mathcal{O}_K[C^{(\sigma)}(Z)]$. Then $\mathrm{Spec}\,(\mathcal{O}_K[C^{(\sigma)}(Z)][y]/(f_\alpha(y)))$ is isomorphic to $\mathrm{Spec}\,(\mathcal{O}_K[C'])$ outside of the discriminant locus of $f_\alpha(y)$. Therefore, (3.3) (c) is satisfied if we replace Z by the Zariski K-open subset of Z consisting of the complement in Z of the image of the discriminant locus of $f_\alpha(y)$. With no loss we can now assume that the conditions of (3.3) are satisfied by Z.

From (3.3) the dimensions and degrees of the left side of (3.1) depend only on σ. Therefore, if (3.1) holds, then (3.2) and the conclusion of Proposition (3.1) (a) hold. From Lemma 3.1 we can replace Z by a Zariski K-open subset so that Z satisfies:

(3.4) $(W_\sigma)_{\underset{\sim}{z}'}$ is absolutely irreducible as an affine variety over $\mathcal{O}_K[C']/\mathfrak{p}(\underset{\sim}{z}')$ (notation as in § 1. B) for $\underset{\sim}{z}' \in C'$ lying over $\underset{\sim}{z} \in Z$ of degree 1.

With Z satisfying all these properties we are assured that $(W_\sigma)_{\underset{\sim}{z}'}$ (as in

expression (3.4)) is not defined over a proper subfield of $\mathcal{O}_K[C']/\mathfrak{p}(\underset{\sim}{z}')$. Therefore we easily conclude that (3.1) holds from the definition of the intersection-union process. This concludes the proof of Proposition (3.1) (a).

We retain the notation above. In part (a) we formed a stratification $\mathcal{S}(\mathrm{pr}_{\underset{\sim}{n-1}}(A))$ (with the properties as described in the statement of the proposition). We now show that for each $Y \in \mathcal{S}(\mathrm{pr}_{\underset{\sim}{n-1}}(A))$ (we've chosen our stratifications so that Y is a K-irreducible locally closed subscheme of $\mathbf{A}^{\underset{\sim}{n-1}}(\mathcal{O}_K)$) there exists a Zariski K-open subscheme, Y' of Y and a cover $C(Y') \to Y'$ such that for each closed point $\underset{\sim}{y}^0 \in Y'$ of degree 1, the type of $IU(A_{\underset{\sim}{y}^0}, \mathcal{O}_K/\mathfrak{p})$ equipped with the cover given by restriction of $C(A)$ to the fiber $A_{\underset{\sim}{y}^0}$, depends only on $\mathrm{Fr}(\underset{\sim}{y}^0_1, \cdots, \underset{\sim}{y}^0_{n-1})$. Then we complete the proof of part (b) by an induction on the dimension of $\mathrm{pr}_{\underset{\sim}{n-1}}(A)$ as in part (a).

As in the proof of part (a) let $\underset{\sim}{y}^{\mathrm{gen}}$ be a generic point of Y; let T^*_Y be the field $T^*(IU(A_{\underset{\sim}{y}^{\mathrm{gen}}}, K(Y)))$; let $\sigma \in G(T^*_Y/K(Y))$; let $W_{\sigma, \underset{\sim}{y}^{\mathrm{gen}}}$ be one of the *last stage* varieties in $IU(A_{\underset{\sim}{y}^{\mathrm{gen}}}, K(Y))$; and let $C(W_{\sigma, \underset{\sim}{y}^{\mathrm{gen}}}) \to W_{\sigma, \underset{\sim}{y}^{\mathrm{gen}}}$ be the cover obtained by restriction of $C(A)$ to the subset $W_{\sigma, \underset{\sim}{y}^{\mathrm{gen}}}$ in the fiber $A_{\underset{\sim}{y}^{\mathrm{gen}}}$. Since $W_{\sigma, \underset{\sim}{y}^{\mathrm{gen}}}$ is defined over T^*, each T^*-irreducible component, C^*, of the cover $C(W_{\sigma, \underset{\sim}{y}^{\mathrm{gen}}}) \to W_{\sigma, \underset{\sim}{y}^{\mathrm{gen}}}$ corresponds to a conjugacy class of subgroups of $G(C(A)/A)$ (decomposition groups as in § 1. B).

Let T^{**} be a finite Galois extension of $K(Y)$ containing T^* such that C^* breaks up into absolutely irreducible components $C^{**}_1, \cdots, C^{**}_r$ over T^{**}. We remind the reader that T^{**} depends on $W_{\sigma, \underset{\sim}{y}^{\mathrm{gen}}}$. The remainder of the proof follows from the argument of part (a). From T^{**} we obtain a cover $C(Z') \to Z'$ of a Zariski K-open subset of Y such that the field of K-rational functions on $C(Z')$ is T^{**}. In addition, as was shown in part (a), we may assume that Z' has the following properties: for $\underset{\sim}{z}^0 \in Z'$, a degree 1 closed point of Z' lying over $\mathfrak{p}$ of $\mathcal{O}_K$, the specialization of $\underset{\sim}{y}^{\mathrm{gen}}$ to $\underset{\sim}{z}^0$ leads to the specialization of *all* the last stage varieties $W_{\sigma, \underset{\sim}{y}^{\mathrm{gen}}}$ to the collection of last stage varieties of $IU(A_{\underset{\sim}{z}^0}, \mathcal{O}_K/\mathfrak{p})$ where σ is $\mathrm{Fr}(\underset{\sim}{z}^0_1, \cdots, \underset{\sim}{z}^0_{n-1}) = \mathrm{Fr}(\underset{\sim}{z}^0)$. Let p^{gen} be a point of $C(Z')$ over $\underset{\sim}{y}^{\mathrm{gen}}$. In addition, from Lemma 3.1, we may assume that the specialization of p^{gen} to $p^0 \in C(Z')$ lying over $\underset{\sim}{z}^0$ leads to the specialization of $C^{**}_1, \cdots, C^{**}_r$ to the absolutely irreducible components of the restriction of $C(A)$ to the element of $IU(A_{\underset{\sim}{z}^0}, \mathcal{O}_K/\mathfrak{p})$ corresponding to $W_{\sigma, \underset{\sim}{y}^{\mathrm{gen}}}$ in this specialization. With this, part (b) of the proposition follows.

Applying the procedure at the beginning of the proof of part (a) of the proposition, we have no difficulty extending part (b) to the case where A is equipped with a Galois stratification. Hence, the conclusion of part (b) is:

for each closed point $\underset{\sim}{y}^0 \in Y$ of degree 1 we obtain a Galois stratification of $IU(A_{\underset{\sim}{y}^0}, \mathcal{O}_K/\mathfrak{p})$, and the *type* of this stratification depends only on $\mathrm{Fr}(\underset{\sim}{y}_0^0, \cdots, \underset{\sim}{y}_{n-1}^0)$. We remark that the conjugacy classes in the covers of this stratification are obtained from the intersections of the Galois groups in these covers (regarded as subgroups of the Galois groups in the covers $C(X) \to X$ for $X \in \mathbb{S}(A)$) with the sets $\mathrm{Con}(X)$ for $X \in \mathbb{S}(A)$.

For the results of Section 4 we consider two special cases compatible with the discussion at the beginning of the section. Let $Y \in \mathbb{S}'(\mathrm{pr}_{n-1}(A))$, and let $\sigma \in G(C(Y)/Y)$. We say that the conjugacy class, $\mathrm{Con}(\sigma)$, of σ satisfies the following:

Case 1*: For each degree 1 point $\underset{\sim}{y}^0 \in Y$ with $\mathrm{Fr}(\underset{\sim}{y}^0) = \mathrm{Con}(\sigma)$ we have:
(3.5) (a) $IU(A_{\underset{\sim}{y}^0}, \mathcal{O}_K/\mathfrak{p})$ is non-empty, and

(b) $\mathrm{Con}(M) \cap \hat{G}(C(M)/M)$ is non-empty for *some* element M of the induced Galois stratification on $IU(A_{\underset{\sim}{y}^0}, \mathcal{O}_K/\mathfrak{p})$. The set $\hat{G}(C(M)/M)$ is explained in Definition 2.1 and at the beginning of Section 4.

Similarly we say that $\mathrm{Con}(\sigma)$ satisfies *Case* 2*: For each degree 1 point $\underset{\sim}{y}^0 \in Y$ with $\mathrm{Fr}(\underset{\sim}{y}^0) = \mathrm{Con}(\sigma)$ we have:
(3.6) (a) $IU(A_{\underset{\sim}{y}^0}, \mathcal{O}_K/\mathfrak{p})$ has underlying space isomorphic to $\mathbf{A}(\underset{\sim}{x}_n)$ (i. e. equal to the whole fiber of $\mathbf{A}^n \to \mathbf{A}^{n-1}$ over $\underset{\sim}{y}^0$), and

(b) $\mathrm{Con}(M)$ contains $\hat{G}(C(M)/M)$ for *each* element M of the induced Galois stratification of $IU(\mathbf{A}_{\underset{\sim}{y}^0}, \mathcal{O}_K/\mathfrak{p})$.

Notice that conditions (3.5) and (3.6) are satisfied for *all* $\underset{\sim}{y}^0$ of degree 1 with $\mathrm{Fr}(\underset{\sim}{y}^0) = \mathrm{Con}(\sigma)$ if they are satisfied for one such $\underset{\sim}{y}^0$.

4. Diophantine problems over all residue class fields of a number field

Let W be an absolutely irreducible locally closed subscheme of $\mathbf{A}^n(k)$, where k is a finite field. Let $C(W) \to W$ be a k-irreducible cover (étale and Galois by the assumptions of § 1. A). Let $\hat{k}$ be the algebraic closure of k in $k(C(W))$ (the field of functions on $C(W)$ defined over k). Define $\hat{G}$ to be the subset of $G = G(C(W)/W)$ consisting of $\sigma \in G$ such that: σ^* acting on $k(C(W))$ induces the Frobenius element in its restriction to $\hat{k}$ (§ 1. B). For $\sigma \in G$ we consider the conjugacy class $\mathrm{Con}(\sigma)$ in G. Let $B(\sigma)$ be the number of degree 1 points $\underset{\sim}{x}^0 \in W$ such that $\mathrm{Fr}(\underset{\sim}{x}^0) = \mathrm{Con}(\sigma)$. Notice that if $\sigma \notin \hat{G}$, then $B(\sigma) = 0$. Let $\bar{W}$ be the closure of W in $\mathbf{A}^n(k)$. In the notation above we take $\sigma \in \hat{G}$.

PROPOSITION 4.1 (*non-regular analogue of the Čebotarev density theorem*). *There exists a constant $\bar{C}$, dependent only on the degree and dimension of*

W, $\deg(C(W)/W)$, *and the degree and dimension of the components of* $\bar{W} - W$ *such that*

$$|B(\sigma) - (|\mathrm{Con}(\sigma)|/|\hat{G}|) \cdot |k|^{\dim(W)}| < \bar{C} \cdot |k|^{\dim(W)-1/2}.$$

Proof. The proof of Proposition 2 in [F] suffices to establish Proposition 4.1 in the case where $\dim(W) = 1$. We reduce the general case to the case where $\dim(W) = 1$ by the generic hyperplane section technique of [LW] or [L 2].

Let $\mathfrak{A} \to \mathbf{A}^n(\mathcal{O}_K)$ be a *full Galois stratification* with underlying space A. We consider, as in the introduction and in § 1. C, the statement:

$$(P) \qquad (Q_1 \underset{\sim}{x}_1) \cdots (Q_n \underset{\sim}{x}_n)[\mathrm{Fr}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n) \in \bigcup_{X \in \mathbb{S}(A)} \mathrm{Con}(X)].$$

We now give an explicit (primitive recursive) procedure for deciding if (P) is true modulo $\mathfrak{p}$ for almost all prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$. In addition we obtain a list of the exceptional primes if (P) is, indeed, true for almost all primes $\mathfrak{p}$. We say that (P) is answered affirmatively in this case.

It is an easy observation that if $\mathfrak{A}'$ is a Galois stratification and $\mathfrak{A}'$ is finer than $\mathfrak{A}$, then question (P) is answered affirmatively for $\mathfrak{A}$ if and only if (P) is answered affirmatively for $\mathfrak{A}'$. From the discussion ending § 1. C, in order to eliminate quantifiers in question (P) we have only to find a Galois stratification, say $\mathrm{pr}(\mathfrak{A})$ with underlying space $\mathrm{pr}_{\underset{\sim}{n-1}}(A)$, such that:

$$(4.1) \qquad Q_n \underset{\sim}{x}_n[\mathrm{Fr}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n) \in \bigcup_{X \in \mathbb{S}(A)} \mathrm{Con}(X)]$$
$$\Longleftrightarrow [\mathrm{Fr}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_{n-1}) \in \bigcup_{Y \in \mathbb{S}(\mathrm{pr}_{\underset{\sim}{n-1}}(A))} \mathrm{Con}(Y)],$$

where $(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_{n-1}) \in \mathbf{A}^n(\mathcal{O}_K/\mathfrak{p})$, for *all* prime ideals $\mathfrak{p}$ of $\mathcal{O}_K[1/\alpha(\mathrm{pr}(\mathfrak{A}))]$.

To start with, consider the Galois stratification produced by Proposition 3.1) (b) and the remarks following Proposition 3.1. There are two cases to consider in order to complete the formation of this Galois stratification (denoted $\mathbb{S}'(\mathrm{pr}_{\underset{\sim}{n-1}}(A))$, by abuse of notation).

Case 1. $Q_n = \exists$. For $Y \in \mathbb{S}'(\mathrm{pr}_{\underset{\sim}{n-1}}(A))$ we define $\mathrm{Con}(Y)$ to be the union of the conjugacy classes $\mathrm{Con}(\sigma)$ for $\sigma \in G(C(Y)/Y)$ such that $\mathrm{Con}(\sigma)$ satisfies condition (3.5).

Case 2. $Q_n = \forall$. For $Y \in \mathbb{S}'(\mathrm{pr}_{\underset{\sim}{n-1}}(A))$ we define $\mathrm{Con}(Y)$ to be the conjugacy classes, $\mathrm{Con}(\sigma)$ in $G(C(Y)/Y)$, such that $\mathrm{Con}(\sigma)$ satisfies condition (3.6)

In each of these cases we have now produced a new Galois stratification, denoted $\mathrm{pr}(\mathfrak{A})$. In order for our notation to be compatible with expression (4.1) we indicate the elements of the stratification of the underlying space $\mathrm{pr}_{\underset{\sim}{n-1}}(A)$ as lying in $\mathbb{S}(\mathrm{pr}_{\underset{\sim}{n-1}}(A))$. The only element still missing is the

constant $\alpha(\mathrm{pr}(\mathfrak{A}))$ and this is produced in the proof of

THEOREM 1. *There is a primitive recursive algorithm for deciding if* (P) *is true for almost all prime ideals* $\mathfrak{p}$ *of* $\mathcal{O}_K$. *And, if* (P) *is answered affirmatively, the algorithm lists the exceptional primes.*

Proof. From the comments above we have only to produce a constant $\alpha(\mathrm{pr}(\mathfrak{A}))$ so that expression (4.1) holds for *all* prime ideals $\mathfrak{p}$ of $\mathcal{O}_K[1/\alpha(\mathrm{pr}(\mathfrak{A}))]$. In fact, for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ for which $\mathfrak{p}$ *divides* $\alpha(\mathrm{pr}(\mathfrak{A}))$ we may check the truth of (P) for $\mathcal{O}_K/\mathfrak{p}$ by explicitly testing all the $\mathcal{O}_K/\mathfrak{p}$-valued points in $\mathbf{A}^n_z$.

Consider the 6-tuple

$$(\dim(M), \deg(M), \dim(\bar{M} - M), \deg(\bar{M} - M), H(C, M), \hat{H}(C, M))$$

that occurs in Definition 2.1, where M is one of the elements of the Galois stratification on $IU(A_{y^0}, \mathcal{O}_K/\mathfrak{p})$ discussed in Case 1* and Case 2* at the end of Section 3. From Proposition 4.1 we obtain a constant $\bar{C}(M, \sigma)$. We conclude easily that the expression $B(\sigma)$ in Proposition 4.1 is *positive* if $|k|$ is greater than

$$\left(\frac{\bar{C}(M, \sigma) \cdot |\hat{H}(C, M)|}{|\mathrm{Con}(\sigma)|}\right)^2 = \bar{\bar{C}}(M, \sigma) .$$

Using the notation of the proof of Proposition (3.1) (b) for each $\tau \in G(T^{**}/K(Y))$ and each $Y \in \mathfrak{S}(\mathrm{pr}_{\underset{\sim}{n-1}}(A))$ we choose $C_1(Y, \tau)$ to be larger than $\bar{\bar{C}}(M, \sigma)$ for all $\sigma \in \hat{H}(C, M)$ and all M in the induced Galois stratification on $IU(A_{\underset{\sim}{y}^0}, \mathcal{O}_K/\mathfrak{p})$. Now let C_2 be a constant larger than $C_1(Y, \tau)$ for τ running over all elements of $G(T^{**}/K(Y))$ and Y running over all elements of $\mathfrak{S}(\mathrm{pr}_{\underset{\sim}{n-1}}(A))$. We choose $\alpha(\mathrm{pr}(\mathfrak{A})) \in \mathcal{O}_K$ so that $\alpha(\mathrm{pr}(\mathfrak{A}))$ is divisible by each prime $\mathfrak{p}$ having one of the properties: $|N_{K/Q}(\mathfrak{p})| \leqq C_2$, or $\mathfrak{p}$ is not in the image in $\mathrm{Spec}(\mathcal{O}_K)$ of the morphism $Y \to \mathcal{O}_K$ for at least one element $Y \in \mathfrak{S}(\mathrm{pr}_{n-1}(A))$ (recall that we have already assumed that $Y \to \mathcal{O}_K$ is a dominant morphism).

Now we establish the equivalence of expression (4.1) for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K[1/\alpha(\mathrm{pr}(\mathfrak{A}))]$. Let $(\underset{\sim}{x}^0_1, \cdots, \underset{\sim}{x}^0_{n-1}) = \underset{\sim}{y}^0 \in \mathrm{pr}_{\underset{\sim}{n-1}}(A)$ be a degree 1 point lying over the prime $\mathfrak{p}$. There exists a unique $Y \in \mathfrak{S}(\mathrm{pr}_{\underset{\sim}{n-1}}(A))$ such that $\underset{\sim}{y}^0 \in Y$.

We treat *Case* 1 first. The statement that there exists $\underset{\sim}{x}^0_n$ such that $\mathrm{Fr}(\underset{\sim}{x}^0_1, \cdots, \underset{\sim}{x}^0_n) \in \bigcup_{X \in \mathfrak{S}(A)} \mathrm{Con}(X)$, is equivalent to: for $\mathrm{Con}(\sigma) = \mathrm{Fr}(\underset{\sim}{y}^0)$ (in $G(C(Y)/Y)$), *Case* 1* holds (end of § 3). In fact, we identify $\underset{\sim}{x}^0_n$ with a point on $IU(A_{\underset{\sim}{y}^0}, \mathcal{O}_K/\mathfrak{p})$, say $\underset{\sim}{x}^0_n \in M$, and $\mathrm{Fr}(\underset{\sim}{x}^0_1, \cdots, \underset{\sim}{x}^0_n)$ is identified with a conjugacy class of $\tilde{C}(M)/M$ by restriction of $C(X)$ (for X containing $(\underset{\sim}{x}^0_1, \cdots, \underset{\sim}{x}^0_n)$) to the fiber $A_{\underset{\sim}{y}^0}$. Therefore, in this identification $\mathrm{Fr}(\underset{\sim}{x}^0_1, \cdots, \underset{\sim}{x}^0_n)$ has its restriction

to $C(M) \to M$ contained in the set of expression (3.5) (b). Conversely, Proposition 4.1 guarantees that (since $|\mathcal{O}_K/\mathfrak{p}|$ is large enough) if the set of expression (3.5) (b) is non-empty, then there is a point $\underset{\sim}{x}_n^0 \in M$ such that $\underset{\sim}{x}_n^0$ is an $\mathcal{O}_K/\mathfrak{p}$-valued point, and $\mathrm{Fr}(\underset{\sim}{x}_1^0, \cdots, \underset{\sim}{x}_n^0)$ restricts (as above) to an element of $\mathrm{Con}(M) \cap \hat{G}(C(M)/M)$.

Case 2 is just as easily accomplished, and we leave this to the reader.

The proof of our next theorem is almost exactly the same as the proof of Theorem 1. Let $\mathfrak{A}$ be a full Galois stratification. For $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$, m an integer, let $k(\mathfrak{p}, m)$ be the extension of degree m of $\mathcal{O}_K/\mathfrak{p}$. Consider the statement

$$(\mathrm{P}') \qquad (Q_1 \underset{\sim}{x}_1) \cdots (Q_n \underset{\sim}{x}_n)[\mathrm{Fr}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n) \in \bigcup_{X \in \mathbb{S}(A)} \mathrm{Con}(X)] \quad \text{for } (\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n) \in \mathbf{A}^n(k(\mathfrak{p}, m)) .$$

THEOREM 2. *There is a primitive recursive algorithm for deciding if* (P′) *is true for all pairs* $(\mathfrak{p}, m)$ *excluding a finite number of primes* $\mathfrak{p}$. *In addition the algorithm computes the exceptional primes* $\mathfrak{p}$.

Note. In Section 5 we prove there is an algorithm for deciding if (P′) is true for all pairs $(\mathfrak{p}, m)$ excluding a *finite number of such pairs.*

At the behest of the referee we conclude this section with a *very* simple example that illustrates the procedure of Theorem 1. This example supplements the examples of [F; Section 2] and for explicit treatments of these problems the reader might find it valuable to return to that paper.

Consider: $K = \mathbf{Q}$, and

$$(\mathrm{P}) \qquad (\forall x)(\exists y)[f(x, y) = 0] \text{ where: } f(x, y) \in \mathbf{Z}[x, y] ,$$

and $f(x, y)$ involves both x and y. We wish to apply our procedure to see if (P) is true modulo p for almost all rational primes p. Let pr: $\mathbf{A}^2 \to \mathbf{A}^1$ be projection of pairs (x, y) onto their 1st coordinate (x coordinate). We stratify the constructible subset A described by $f(x, y) = 0$ into K-irreducible locally closed subschemes. Let this stratification be designated by $\mathbb{S}_1(A)$. In accordance with the proof of Proposition 3.1 we may assume that our stratification has been selected so that for $X \in \mathbb{S}_1(A)$, pr: $X \to$ Image of X is a flat morphism. Therefore the elements of $\mathbb{S}_1(A)$ are of two types, dependent on whether $\dim(\mathrm{pr}(X)) = 0$, or $\dim(\mathrm{pr}(X)) = 1$. In addition there are two subtypes in the case that $\dim(\mathrm{pr}(X)) = 0$: $\dim(X) = 0$ or $\dim(X) = 1$. In general, in order to carry out our algorithm it is important to have a convenient labeling for the possible types that arise. In this case we associate to $X \in \mathbb{S}_1(A)$ the 2-tuple $(\dim(X), \dim(\mathrm{pr}(X)))$ which takes on one of the 3 possible values: (1, 1), (1, 0), or (0, 0). We treat each case

separately in order to form our Galois stratification of $\mathrm{pr}(A)$. To simplify the treatment we assume that $\mathcal{S}_1(A)$ has been further stratified so that for $X \in \mathcal{S}_1(A)$ of type (1, 1) the morphism $X \to \mathrm{pr}(X)$ is étale (finite but not necessarily Galois).

As in the proof of Proposition 3.1 we give a stratification $\mathcal{S}_X$ of $\mathrm{pr}(X)$ for each $X \in \mathcal{S}_1(A)$.

Case 1: *X of type* (1, 1). There is an element, $Y = \mathrm{pr}(X)$ in $\mathcal{S}_X$, and $C(Y) \to Y$ is the cover obtained by taking the normalization of the morphism $X \to \mathrm{pr}(X)$ in the field $\widehat{\mathbf{Q}(X)}$ (the Galois closure of the field extension $\mathbf{Q}(X)/\mathbf{Q}(\mathrm{pr}(X))$. The group $G(C(Y)/Y)$ has a natural permutation representation T_Y coming from the right cosets of $G(C(Y)/X)$ (since $C(Y)$ is a cover of X). Note that if $\underset{\sim}{y^0} \in Y$ is a degree 1 point lying over p, then the elements of $\mathrm{Fr}(\underset{\sim}{y^0})$ fix at least one letter in the representation T_Y if and only if the fiber of $X \to \mathrm{pr}(X)$ lying over $\underset{\sim}{y^0}$ contains a degree 1 point of X.

Case 2: *X of type* (1, 0). There is one element $Y = \mathrm{pr}(X)$ in $\mathcal{S}_X$, and $C(Y) \to Y$ is the trivial (degree 1) cover. In order to follow our procedure closely we should be keeping track of the degree of the complement of X in the fiber over (the 0-dimensional $\mathbf{Q}$-irreducible locus) Y. However, this is not essential to understanding at this point.

Case 3: *X of type* (0, 0). There is one element $Y = \mathrm{pr}(X)$ in $\mathcal{S}_X$. In regarding $X \to \mathrm{pr}(X)$ as a morphism, by replacing $\mathcal{S}_X$ by a finer stratification (localizing away from a finite set of primes of $\mathbf{Z}$), we may assume that this morphism is étale. Then the morphism $Y \to \mathbf{Z}$ corresponds to a ring homomorphism $Z[1/a] \to \mathcal{O}_L[1/a]$ where $\mathcal{O}_L$ is the ring of integers of some number field L, and $a \in \mathbf{Z}$ is some non-zero integer. By suitable choice of "a" we may assume that $X \to \mathrm{pr}(X)$ corresponds to the homomorphism $\mathcal{O}_L[1/a] \to \mathcal{O}_M[1/a]$, for M some finite extension of L. Let $\hat{M}$ be the Galois closure of M/L (we may wish to choose $\hat{M}$ to be a Galois extension of $\mathbf{Q}$ in an explicit procedure; the important thing is that it be Galois over L, and contain M). The cover $C(Y) \to Y$ corresponds to the homomorphism $\mathcal{O}_L[1/a] \to \mathcal{O}_{\hat{M}}[1/a]$. Identify $G(C(Y)/Y)$ with $G(\hat{M}/L)$, equipped with the permutation representation T_Y coming from the right cosets of $G(\hat{M}/M)$.

We complete the formation of the Galois stratification $\mathrm{pr}(\mathfrak{A})$ by following the procedure at the beginning of Proposition 3.1. This procedure is most easily effected by making additional assumptions on the stratification $\mathcal{S}_1(A)$: the set $\mathrm{pr}(X)$ is the *same* for all $X \in \mathcal{S}_1(A)$ with X of type (1, 1) and for X not of type (1, 1), $\mathrm{pr}(X)$ is *disjoint* from the image in $\mathbf{A}^1$ of the sets of type (1, 1). From this we have a stratification of $\mathrm{pr}(A)$. Let Y be an

element of this stratification and let $X_1, \cdots, X_t$ run over all elements of $\mathfrak{S}_1(A)$ such that $\mathrm{pr}(X_i) = Y$. Then we *amalgamate* (as in §1. A) all the covers $C(\mathrm{pr}(X_i)) \to \mathrm{pr}(X_i)$ (each of which is equipped with a permutation representation $T_{\mathrm{pr}(X_i)}$, $i = 1, \cdots, t$), to obtain the cover $C(Y) \to Y$ (which is equipped with the permutation representation T that is the product of all the representations $T_{\mathrm{pr}(X_i)}$, $i = 1, \cdots, t$). If we define $\mathrm{Con}(Y)$ to be the elements of $G(C(Y)/Y)$ that fix at least one letter in the representation T, then we have completed the production of the Galois stratification $\mathrm{pr}(\mathfrak{A})$ (excluding our glossing over the production of $\alpha(\mathrm{pr}(\mathfrak{A}))$, which in theory should be no problem).

In order to continue our elimination of quantifiers we must consider

$$(\mathrm{P}') \qquad \forall x\,[\mathrm{Fr}(x) \in \bigcup_{Y \in \mathfrak{S}(\mathrm{pr}(A))} \mathrm{Con}(Y)]\,.$$

Indeed $\mathrm{pr}(A) \subseteq \mathbf{A}^1$, and we must form a Galois stratification $\mathfrak{B}$ of $\mathbf{A}^0(\mathbf{Z}[1/a])$ for some explicit $a \in \mathbf{Z}$ (where $\mathbf{A}^0$ is 0-dimensional affine space) so that for a given prime p, not dividing a, (P′) is true modulo p if and only if the Frobenius element associated to the prime p is in the conjugacy classes associated to the (unique) cover of $\mathbf{A}^0(\mathbf{Z}[1/a])$ in the Galois stratification $\mathfrak{B}$. Thus, allowing ourselves to again be cavalier about the production of the constant "a", we give $\mathfrak{B}$ which amounts to giving a Galois extension $L_{\mathfrak{B}}$ of $\mathbf{Q}$, and a collection $\mathrm{Con}(\mathfrak{B})$ of conjugacy classes of $G(L_{\mathfrak{B}}/\mathbf{Q})$. We conclude our example with the production of $L_{\mathfrak{B}}$ and $\mathrm{Con}(\mathfrak{B})$.

For each $Y \in \mathfrak{S}(\mathrm{pr}(A))$ let $\mathbf{Q}(C(Y))$ be the field of $\mathbf{Q}$-rational functions on $C(Y)$. Let L_Y be the algebraic closure of $\mathbf{Q}$ in $\mathbf{Q}(C(Y))$. Then $L_{\mathfrak{B}}$ is the composite of the fields L_Y as Y runs over $\mathfrak{S}(\mathrm{pr}(A))$. For $\sigma \in G(L_{\mathfrak{B}}/\mathbf{Q})$ and $Y \in \mathfrak{S}(\mathrm{pr}(A))$ we let: $G^{(\sigma)}(C(Y)/Y)$ consist of the elements $\tau \in G(C(Y)/Y)$, such that τ induces τ^* **on** $\mathbf{Q}(C(Y))$ where the restriction of τ^* to L_Y is σ. Then $\sigma \in \mathrm{Con}(\mathfrak{B})$ if and only if $G^{(\sigma)}(C(Y)/Y) \subset \mathrm{Con}(Y)$.

5. Diophantine problems over finite fields

A. Diophantine problems over all extensions of a given finite field

Let $k = \mathbf{F}(q)$ be the finite field with q elements. We discuss first the problem of solving diophantine problems over all finite extensions of k. Let k_m be the field $\mathbf{F}(q^m)$. Let A be a union of locally closed subschemes of $\mathbf{A}^n(k)$, and A_{k_m} the k_m-valued points of A. We consider

$$(\mathrm{P})_m \qquad (Q_1 \underline{x}_1) \cdots (Q_n \underline{x}_n)[(\underline{x}_1, \cdots, \underline{x}_n) \in A_{k_m}]\,.$$

We want to find a procedure for deciding if $(\mathrm{P})_m$ is true for all but finitely many integers m, and if this is so to find an explicit (primitive recursive)

list of the exceptional integers.

The easiest way to extend the methods of the last section is to generalize the notion of Galois stratification. In fact, in the definition of Galois stratification in Section 1. C, instead of demanding that a cover $C(X) \to X$ of k-schemes be étale and Galois we ask that there be finite flat morphisms $C(X) \xrightarrow{\varphi} C'$ and $C' \xrightarrow{\psi} X$ such that φ is purely inseparable and ψ is a cover in our sense (§ 1. A étale and Galois). Since φ is purely inseparable, each k-rational place on C' extends uniquely to a k-rational place of $C(X)$. The conjugacy classes $\mathrm{Con}(X)$ are a subset of the conjugacy classes of $G(C'/X)$.

With these considerations, we replace A by a Galois stratification $\mathfrak{A}$ over k and proceed with the elimination of quantifiers as suggested, say, by expression (4.1). In this case we equip each Galois stratification with an integer $\alpha(\mathfrak{A})$ so that we produce a new Galois stratification $\mathrm{pr}(\mathfrak{A})$ such that if $m > \alpha(\mathfrak{A})$:

$$(5.1) \qquad (Q_n \underset{\sim}{x}_n)[\mathrm{Fr}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n) \in \bigcup_{X \in \mathbb{S}(A)} \mathrm{Con}(X)] \Longleftrightarrow [\mathrm{Fr}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_{n-1}) \in \bigcup_{Y \in \mathbb{S}(\mathrm{pr}_{n-1}(A))} \mathrm{Con}(Y)]$$

where $(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n) \in \mathbf{A}^n(k_m)$.

Exceptional integers m occur in the use of Proposition 4.1 in the same manner as in the proof of Theorem 1. We make some comments on Bertini's theorem in positive characteristic. Our proofs of Lemma 3.1 and Proposition 3.1 are valid with $\mathcal{O}_K$ replaced by k, so long as the obvious allowance for the appearance of inseparable extensions is included. The essential fact for our purposes is MacLane's criterion: The function fields of varieties over finite fields are *separably* generated. This fact is necessary to apply Stolzenberg's results ([S]) as in Section 0. B.

However, there are forms of Bertini's theorem which are not valid in positive characteristic. For example, if $W \to \mathbf{A}^r$ is a dominant morphism with $r \geqq 2$, W nonsingular, and the generic fiber irreducible, in characteristic zero there is a Bertini theorem which says that the general fiber is also nonsingular. This theorem is not true in positive characteristic.

From the discussion above we obtain:

THEOREM 3. *There is a primitive recursive algorithm to decide if* $(\mathrm{P})_m$ *is true for all but finitely many integers* m, *and if this is so, to compute the list of exceptional integers.*

B. Diophantine problems over all finite fields

Let $\mathfrak{A}$ be a full Galois stratification, $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$, m an integer,

and $k(\mathfrak{p}, m)$ the degree m extension of $\mathcal{O}_K/\mathfrak{p}$. Consider

$$(P'') \qquad (Q_1\underset{\sim}{x}_1)\cdots(Q_n\underset{\sim}{x}_n)[\mathrm{Fr}(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n) \in_{X \in \mathfrak{S}(A)} \mathrm{Con}(X)]$$

where A is the underlying space of the Galois stratification $\mathfrak{A}$. We say that (P'') is true in $k(\mathfrak{p}, m)$ if the statement (P'') is true for the variables $(\underset{\sim}{x}_1, \cdots, \underset{\sim}{x}_n)$ running over $\mathbf{A}^n(k(\mathfrak{p}, m))$.

THEOREM 4. *There is a primitive recursive algorithm for deciding if* (P'') *is true in* $k(\mathfrak{p}, m)$ *for all but finitely many pairs* $(\mathfrak{p}, m)$. *If* (P'') *is true in* $k(\mathfrak{p}, m)$ *for all but finitely many pairs* $(\mathfrak{p}, m)$ *then the algorithm also lists the exceptional pairs.*

Proof. From Theorem 2 (§ 4) there is a primitive recursive algorithm to decide if (P'') is true in $k(\mathfrak{p}, m)$, excluding a finite collection of exceptional primes $\mathfrak{p}_1, \cdots, \mathfrak{p}_l$. For each exceptional prime $\mathfrak{p}_i$, the fiber of the full Galois stratification $\mathfrak{A}$ at $\mathfrak{p}_i$ provides us with a list of questions of the form of $(P)_m$, as in § 5. A. Theorem 3 allows us to decide if $(P)_m$ is true for almost all integers m, and if this is so, Theorem 3 provides us with a list of exceptional integers.

UNIVERSITY OF CALIFORNIA, IRVINE
AMHERST COLLEGE, MASSACHUSETTS

REFERENCES

[A] J. AX, Solving diophantine problems modulo every prime, Ann. of Math. **85** (1967), 161-183.

[A 2] ———, The elementary theory of finite fields, Ann. of Math. **88** (1968), 239-271.

[AK 1] J. AX and S. KOCHEN, Diophantine problems over local fields: I, Am. J. Math. **87** (1965), 605-630.

[AK 2] ———, Diophantine problems over local fields: II, A complete set of axioms for p-adic number theory, Am. J. Math. **87** (1965), 631-648.

[AK 3] ———, Diophantine problems over local fields: III, Decidable fields, Ann. of Math. **83** (1966), 437-456.

[CF] J. W. S. CASSELS and A. FROHLICH, *Algebraic Number Theory*, Thompson, Washington, D. C., 1967.

[C] P. COHEN, Decision Procedures for Real and *P*-adic Fields. Prepared for Office of Naval Research, (**79**) (NR-043-317).

[D] J. DIEUDONNÉ, *Fondements de la Géométrie Algébrique Moderne*, Université de Montréal Press, Canada, 1964.

[F] M. FRIED, On Hilbert's irreducibility theorem, J. Number Theory, 374, **6** (1974), 111-133.

[G] N. GREENLEAF, Irreducible subvarieties and rational points, Am. J. Math. **87** (1965), 25-31.

[Gr] A. GROTHENDIECK, *Éléments de Géométrie Algébrique* (en collaboration avec J. Dieudonné), Chapter I, Le Langage des Schémas. Publications Math. I.H.E.S., No. 4, 1960.

[Ha] H. HASSE, Bericht über neuere Untersuchungen und Probleme aus der Theorie der Algebraischen Zahlkörper I, Ia, II, Jahr. der D.M.V. Berlin **35** (1926), 1-55: **36** (1927), 233-311; **6** (1930 A), 1-204.

[He] G. HERMANN, Die Frage der Endlich Vielen Schnitte in der Theorie der Polynomideale, *Math. Annalen* **95** (1925), 736-788.

[J] M. JARDEN, Elementary statements over large algebraic fields, Trans. A.M.S. **164** (1972), 67-91.

[L 1] S. LANG, *Diophantine Geometry*, Interscience Publishers, John Wiley and Sons, 1962.

[L 2] ———, Sur les Séries L d'une variété algébrique, Bull. Soc. Math. France, **84** (1956), 385-407.

[LW] S. LANG and A. WEIL, Number of points of varieties in finite fields, Am. J. Math. **76** (1954), 819-827.

[M 1] D. MUMFORD, *Introduction to Algebraic Geometry*, Harvard University Notes, Cambridge, Mass., 1966.

[M 2] ———, Lectures on curves on an algebraic surface, Annals of Mathematics Studies, **59** (1965).

[P] R. PETER, *Recursive Functions*. Third revised edition, Academic Press, N.Y. 1967.

[S] G. STOLZENBERG, Constructive normalization of an algebraic variety, Bull. A.M.S. (1968), 595-599.

[W] B.L. VAN DER WAERDEN, *Modern Algebra*, Frederick Ungar, N.Y. 1950.

[Z] O. ZARISKI, Pencils on an algebraic variety and a new proof of a theorem of Bertini, Trans. A.M.S. **50** (1941), 48-70.

[ZS] O. ZARISKI and P. SAMUEL, *Commutative Algebra*, Vol. I. Van Nostrand, Princeton, N.J. 1960.

(Received January 8, 1975)
(Revised February 6, 1976)