Contemporary Mathematics

Applications of Local-Global Principles to Arithmetic and Geometry

Laurent Moret-Bailly

Abstract. We review existing local-global principles over "big" rings of integers in the algebraic closure of a global field, with some applications to geometry (construction of curves over number fields) and number theory (construction of Galois extensions of number fields).

Introduction

This is a survey paper on Rumely's local-global principle, some of its variants and generalisations, and some applications.

Rumely's theorem (Theorem 1 of [**Ru1**], see 1.3 and 1.7 below) is a very powerful existence theorem for solutions of Diophantine systems over (in particular) the ring $\widetilde{\mathbb{Z}}$ of algebraic integers. A consequence which motivates the interest of model theorists is the decidability of $\widetilde{\mathbb{Z}}$ (see [**D**] for details). Rumely's theorem was later generalised to provide existence criteria for solutions satisfying local rationality conditions at finitely many places ([**MB3**], see Section 2 below).

The paper is organised as follows.

In Section 1 we explain the general problem and discuss Rumely's original theorem.

In Section 2 we introduce local splitting conditions and explain the corresponding generalisations of Rumely's theorem; we also give some immediate applications to the geometry and algebra of "totally Σ-adic fields".

In Section 3, we apply the previous results to the problem of constructing varieties over global fields with prescribed local properties. We concentrate on the case of curves, the idea being to explain the difficulties involved and motivate the generalisation of local-global principles given in [**MB5**].

In Section 4, we apply our local-global principles to the construction of Galois extensions of global fields with given group and given local behaviour at some places.

The following topics are *not* discussed in this paper:

1991 *Mathematics Subject Classification.* 14G25, 14D20, 11R04, 11G35.

The author is a member of the TMR network "Arithmetic algebraic geometry" (network contract ERB FMRX 960006).

- Rumely's capacity theory [**Ru2**], which he used to prove his local-global principle but in fact gives more precise information;
- applications to model theory, especially decidability results (see [**D**]);
- deeper applications to field theory, such as Pop's structure theorem for certain absolute Galois groups (see [**P**]).

Conventions. All rings are commutative with unit. We use the language of schemes throughout; the hostile reader may generally read "variety" when we work over a field, and "system of polynomial equations" (at the minor cost of restricting to the affine case) over a ring.

1. The general problem and Rumely's theorem

1.1. Notations. K denotes a global field, i.e., either a number field or a one-variable function field over a finite field (which we shall denote by k when necessary).

M_K is the set of places (or absolute values) of K.

R is a subring of K which is:

- in the number field case, the ring of "S-integers" of K, where S is a finite set of finite places of K (that is, the subring of K consisting of elements integral at all places *not* in S);
- in the function field case, the ring of some affine open subset of the projective smooth k-curve with function field K.

So, in both cases, R is a Dedekind domain with fraction field K. We put $B = \operatorname{Spec} R$ (in the function field case, this is a smooth affine curve over k).

We identify, as usual, the set M_R of height one prime ideals of R (= closed points of B) with the corresponding proper subset of M_K.

Observe that, given R, we have two ways of constructing other rings R' of the same type:

- *extension*: take a finite extension L of K, and define R' as the integral closure of R in L;
- *localisation*: take a finite subset Σ of M_R, and define R' as the affine ring of $U := B \setminus \Sigma$.[1]

We denote by $\widetilde{K}$ a fixed algebraic closure of K, and by $\widetilde{R}$ the integral closure of R in $\widetilde{K}$.

For $v \in \mathrm{M}_K$, we denote by K_v (resp. R_v) either the completion or the henselisation of K (resp. R) at v; "either" means that the reader may choose. (If $v \notin \mathrm{M}_R$, R_v is just K_v; in the archimedean case, the henselisation may be defined as the algebraic closure of K in the corresponding completion). For each v, we fix an algebraic closure $\widetilde{K}_v$ of K_v, and denote by $\widetilde{R}_v$ the integral closure of R_v in $\widetilde{K}_v$.

1.2. Integral points. We are interested in solving, in $\widetilde{R}$, finite systems of polynomial equations with coefficients in $\widetilde{R}$; more precisely, we look for *existence* criteria for solutions of such systems.

[1] To see that U is indeed affine, observe that $U \hookrightarrow B$ is an affine morphism because this is a local condition and Σ is locally defined by one equation. Explicitly, one can define R' as follows: if $I \subset R$ is the ideal of Σ, put $R' = (\bigoplus_{n\in\mathbb{N}} I^{-n}T^n)/(T-1)$. This works for an arbitrary Dedekind domain; in our case, however, one can simply note that I^n is principal for some $n > 0$, take a generator a, and put $R' = R[1/a]$.

Without loss of generality we may assume that the coefficients are in R (by extending R if necessary).[2]

Such a system

$$F_i(T_1, \dots, T_n) = 0, \quad i = 1, \dots, s \tag{1.2.1}$$

(with all F_i in $R[T_1, \dots, T_n]$) defines an R-algebra of finite type

$$A = R[T_1, \dots, T_n]/(F_1, \dots, F_s), \tag{1.2.2}$$

with the property that if S is any R-algebra, solutions $(t_1, \dots, t_n) \in S^n$ of (1.2.1) correspond bijectively to R-algebra homomorphisms from A to S. Of course, any R-algebra of finite type can be thought of as classifying in this way a system of equations. A similar correspondence also holds if one replaces R by $\widetilde{R}$, but if one insists on studying only finite systems, one should replace "finite type" by "finite presentation" in the above discussion.

The basic geometric object attached to (1.2.1) is the R-scheme of finite type

$$f : X = \operatorname{Spec} A \longrightarrow B = \operatorname{Spec} R. \tag{1.2.3}$$

In the function field case, this f is a morphism of affine varieties (not necessarily reduced or irreducible) over the finite field k, B being a smooth affine curve. In general, solutions of (1.2.1) in $\widetilde{R}$ correspond to B-morphisms $\widetilde{B} = \operatorname{Spec} \widetilde{R} \to X$ ("$\widetilde{B}$-valued points of X"). We see in particular an obvious necessary existence condition: since $\widetilde{B} \to B$ is surjective, f must also be surjective. In terms of (1.2.1) this just means that for every prime $\mathfrak{p}$ of R, (1.2.1) should have a solution in an algebraic closure $\widetilde{\kappa(\mathfrak{p})}$ of the residue field of $\mathfrak{p}$. This condition, of course, is not sufficient: take, for $R = \mathbb{Z}$ and $n = 1$, the system $2(2T_1 - 1) = T_1(2T_1 - 1) = 0$, where X is isomorphic to the disjoint union of the point $\operatorname{Spec} \mathbb{F}_2$ and its open complement in B (equivalently, A is isomorphic to $\mathbb{F}_2 \times \mathbb{Z}[1/2]$).

So we have to refine the above necessary condition. Geometrically, one can observe that since $\widetilde{R}$ is a domain, every $\widetilde{B}$-valued point of X must factor through some irreducible component X_0 of X, hence $X_0 \to B$ must also be surjective. In algebraic terms: an R-morphism $A \to \widetilde{R}$ must factor through some quotient $A/\mathfrak{Q}$, for some minimal prime $\mathfrak{Q}$ of A, so the enlarged system defined by this $\mathfrak{Q}$ must also have a solution in $\widetilde{\kappa(\mathfrak{p})}$, for all $\mathfrak{p}$.

In other words, we are reduced to considering the case when X is irreducible and f is surjective. But here is a slightly less trivial example: take $R = \mathbb{Z}$ and $X = \operatorname{Spec} \mathbb{Z}[T_1, T_2]/(T_1^2 + 1, T_2(T_1 - 2) - 1)$. Now, a $\widetilde{B}$-valued point of X would be an algebraic integer t (the value of T_1) such that $t^2 = -1$ and $t - 2$ is invertible in $\widetilde{\mathbb{Z}}$, an obvious impossibility. However, X is irreducible and surjective over $\operatorname{Spec} \mathbb{Z}$: geometrically, it is obtained from the spectrum of the ring $\mathbb{Z}[i]$ of Gaussian integers (a ramified double cover of $\operatorname{Spec} \mathbb{Z}$) by removing one point, corresponding to one of the two primes of characteristic 5. (And, algebraically, A is isomorphic to the subring $\mathbb{Z}[i, (i-2)^{-1}]$ of $\mathbb{C}$).

What happens here can be "explained" by extending the ground field from $\mathbb{Q}$ to $L = \mathbb{Q}(i)$, with integers $R' = \mathbb{Z}[i]$: the scheme $X_{R'}$ now has *two* irreducible components, corresponding to the ideals $(T_1 - i)$ and $(T_1 + i)$, none of which is surjective over $\operatorname{Spec} R'$: they are isomorphic to $\operatorname{Spec} R'[1/(i-2)]$ and $\operatorname{Spec} R'[1/(-i-2)]$, respectively.

[2] Note that since $\widetilde{R}$ is not Noetherian, finiteness of the system is essential for this argument.

The easiest way to avoid this kind of problem is by requiring the generic fibre X_K to be geometrically irreducible over K (in other words, $X_{\widetilde{K}}$ should be irreducible). Starting from an arbitrary X, this condition can be achieved by replacing R by its integral closure R' in a finite extension L of K such that all components of $X_{\widetilde{K}}$ are defined over L, and by working with all components of $X_{R'}$ individually. Now we can state:

1.3. Theorem (Rumely). *With $B = \operatorname{Spec} R$ as above, let $f : X \to B$ be an R-scheme of finite type. Assume that X is irreducible, X_K is geometrically irreducible over K, and f is surjective. Then X has an $\widetilde{R}$-valued point.*

1.4. History. The first historical appearance of "Rumely-like" theorems is in Skolem's paper [**S**], which contains many special cases such as this: If f is a primitive polynomial (i.e., not divisible by any prime number) in $\mathbb{Z}[T_1, \dots, T_n]$, there exist algebraic integers $t_1, \dots, t_n$ such that $f(t_1, \dots, t_n)$ is an algebraic *unit*. This is the special case of 1.3 obtained by taking $X = \operatorname{Spec}(\mathbb{Z}[T_1, \dots, T_n, Y]/(Yf - 1))$. Geometrically, X is the open complement, in the affine n-space $\mathbb{A}^n_{\mathbb{Z}}$, of the hypersurface defined by f; the primitivity condition is equivalent to the surjectivity of X over $\operatorname{Spec} \mathbb{Z}$.

Theorem 1.3 itself was proved in [**Ru1**], as an application of Rumely's "capacity theory" (exposed in [**Ru2**]) which in fact contains much more information when the underlying variety X_K is a curve. Another, more geometric, proof due to Szpiro and myself was later given in [**MB2**].

1.5. Remarks.

1.5.1. The case when X_K is an *affine curve* in in fact the key case, in the sense that all known proofs of Rumely's theorem (and variants) proceed by first reducing to this case by some hyperplane section argument.

1.5.2. On the other hand, the "opposite" case when X is *proper* (e.g. projective) over B is trivial: there is a finite extension K' of K such that X has a K'-valued point, which by the valuative criterion of properness extends to an R'-valued point, where R' is the integral closure of R in K'.

1.5.3. In Theorem 1.3, and all subsequent similar results, we are only interested in solutions of polynomial systems with coordinates in rings which are domains. Therefore, if we start, say, from a system (1.2.1), corresponding to a ring A as in (1.2.2), we can replace A by the quotient A_{red} of A by its radical. More generally, in 1.3, we may assume the scheme X to be *reduced*.

1.6. Other rings. It is easy to extend Rumely's theorem to base rings which are *arbitrary localisations* of our R. The extreme case is the ring K itself, for which the result is just Hilbert's Nullstellensatz; but apart from this, even the case of the localisation of R at one finite prime isn't obvious at all.

In fact, the general discussion of 1.2 is of course valid over much more general rings than those considered here; however, the validity of Rumely's theorem is a very special (and, in my opinion, very surprising) property of these particular rings. For instance, it is easy to see that if the analogue of Rumely's theorem is true for, say, a Dedekind domain D, then the ideal class group of D must be a torsion group, and the same property also holds for the integral closure of D in any finite extension of its fraction field. This rules out rings as innocent-looking as $\mathbb{Q}[T]$. Much more

strikingly, Rumely's theorem is false for discrete valuation rings such as $\mathbb{Q}[T]_{(T)}$! (See [**MB1**]).

Rumely's theorem is often presented in the following form:

1.7. Corollary ("Rumely's local-global principle"). *With $B = \operatorname{Spec} R$ as before, let $f : X \to B$ be an R-scheme of finite type. Assume that X_K is geometrically irreducible over K. Then X has an $\widetilde{R}$-valued point if and only if it has an $\widetilde{R}_v$-valued point for every $v \in \mathrm{M}_R$.*[3]

Proof. The "only if" part is trivial. Conversely, assume $X(\widetilde{R}_v) \neq \emptyset$ for every $v \in \mathrm{M}_R$. Let X_0 be the Zariski closure of X_K in X (with, for instance, its reduced subscheme structure, but this does not matter). Obviously, X_0 is irreducible and $(X_0)_K = (X_K)_{\mathrm{red}}$ is geometrically irreducible over K. Moreover, if R_1 is any overdomain of R, we have $X(R_1) = X_0(R_1)$. In particular, $X_0(\widetilde{R}_v) \neq \emptyset$ for every $v \in \mathrm{M}_R$, and it follows that $X_0 \to B$ is surjective. So by 1.3, $X_0(\widetilde{R}) = X(\widetilde{R})$ is not empty.[4] □

1.8. Remark. Conversely, it is not very difficult to deduce 1.3 from 1.7.

1.9. Density. In [**Ru1**], Rumely proves the following more precise result. Let Σ be a finite set of places of K, with the "incompleteness" property that at least one place of K belongs neither to Σ nor to M_R. Then $X(\widetilde{R})$ has a dense image in $\prod_{v\in\Sigma} X(\widetilde{R}_v)$, where the right-hand side is given the product of the v-adic topologies.

When Σ consists of finite places only, this can in fact be deduced from the "crude" form 1.3; this is done in [**MB2**]. This just doesn't seem to work for archimedean places: in this respect, Rumely's density theorem is stronger than the existence theorem.

Without the incompleteness property above, and if X_K is a curve, see Rumely's book [**Ru2**] on capacity theory.

1.10. Effectivity. It is of course natural to ask for more information on the $\widetilde{R}$-valued points obtained by 1.3. The most obvious question is to give bounds for the degree of a field of rationality. Answers to this question, in special cases, are given in [**M**] and [**E**].

2. Local rationality (or splitting) conditions

2.1. Notations. We keep the notations and assumptions of 1.1. In addition, we fix a finite subset Σ of M_K. We shall assume the following condition, already encountered in 1.9 above:

Incompleteness condition. *There exists a place of K which is neither in Σ nor in M_R.*

We denote by $K^\Sigma \subset \widetilde{K}$ the maximal extension of K which is totally split at each $v \in \Sigma$. (For instance, if $K = \mathbb{Q}$ and Σ is the archimedean place, then K^Σ is

[3] Or, equivalently, for every $v \in \mathrm{M}_K$: recall that if $v \notin \mathrm{M}_R$ then $\widetilde{R}_v = \widetilde{K}_v$.

[4] The reader unfamiliar with the language may find it easier to follow the argument in the affine case: if X is as in (1.2.3), assumed reduced, then $X_0 = \operatorname{Spec} A_0$ where A_0 is the image of the ring A of (1.2.2) into $K \otimes_R A$, i.e. $A_0 = A/(R\text{-torsion})$. Then our assumptions imply that $K \otimes_R A$ is a domain, hence so is A_0.

the field $\mathbb{Q}^{\mathrm{tr}}$ of totally real numbers.) R^Σ will denote the integral closure of R in K^Σ; in other words, $R^\Sigma = \widetilde{R} \cap K^\Sigma$. Note that K^Σ is a Galois extension of K.[5]

For each $v \in \Sigma$ we have a natural metric *topology* on K_v, deduced from the absolute value v. From this it is easy to define a topology on $X(K_v)$ for any K_v-scheme X of finite type: for affine X, it is the topology induced by any embedding of X in an affine space $\mathbb{A}^n_{K_v}$ (where we identify $\mathbb{A}^n_{K_v}(K_v)$ with K_v^n and give the latter the product topology). Note that if X is an R_v-scheme of finite type, (the image of) $X(R_v)$ is *open* in $X(K_v)$ (essentially because R_v is open in K_v).[6]

For $v \in \Sigma$, there are many K-embeddings of K^Σ in K_v; they correspond bijectively to the absolute values of K^Σ extending v, and they are all conjugate under $\mathrm{Gal}\,(K^\Sigma/K)$. Thus, if X is a K-scheme of finite type and $x \in X(K^\Sigma)$, we can define the *orbit* of x in $X(K_v)$ as the set of all images of x obtained via all K-embeddings of K^Σ into K_v. Because of the conjugacy property above, this orbit can be seen as a Galois orbit, or "set of conjugates of x".

2.2. Theorem (refined Rumely's theorem). *With notations and assumptions as in* 2.1*, let $f : X \to B$ be a B-scheme of finite type. Assume that X is irreducible, X_K is geometrically irreducible over K, and f is surjective.*

For each $v \in \Sigma$, fix a subset Ω_v of $X(R_v)$, which is open (in the v-topology) and contains nonsingular points.

Then there exists $x \in X(R^\Sigma)$ such that, for each $v \in \Sigma$, the orbit of x in $X(K_v)$ is contained in Ω_v.

2.3. Remark. By a "nonsingular point of $X(R_v)$", we mean here a point whose canonical image in $X(K_v)$ is in the nonsingular (or smooth) locus of the generic fibre X_K. In the case of a system such as (1.2.1), this means that some Jacobian determinant is nonzero, *not* that it is invertible in R_v, which would be a stronger condition.

The conditions on Ω_v can be rephrased as "Ω_v is open for the v-topology, and dense in X_{K_v} for the Zariski topology".

2.4. The incompleteness condition of 2.1 is essential: if we take $R = \mathbb{Z}$, $\Sigma = \{\infty\}$ (the archimedean place of $\mathbb{Q}$), $X =$ the affine line $\mathrm{Spec}\,\mathbb{Z}[T]$, and $\Omega_\infty =]0,1[\subset X(\mathbb{R}) = \mathbb{R}$, an x as in the theorem would be an algebraic integer with all conjugates in $]0,1[$, an impossibility.

2.5. Remark. For concreteness' sake, let us make the meaning more explicit in the "affine" case when X is described by a system of polynomial equations (1.2.1). In each Ω_v we have a "local" solution $\underline{t}^{(v)} = (t_1^{(v)}, \dots, t_n^{(v)})$ of our system, with each $t_i^{(v)}$ in R_v, and $\underline{t}^{(v)}$ a nonsingular point of $X(K_v)$. Without loss of generality, we may assume that Ω_v is a "ball" defined as the set of solutions $(u_1^{(v)}, \dots, u_n^{(v)}) \in R_v^n$ of (1.2.1) satisfying $|u_i^{(v)} - t_i^{(v)}|_v < \varepsilon_v$ for each i, for some positive ε_v. In this case, the theorem says that there exists a solution $\underline{x} = (x_1, \dots, x_n) \in \widetilde{K}^n$ such that each x_i is in R^Σ (i.e. integral over R and totally split at each $v \in \Sigma$) and $\underline{x}$ is "close" to

[5] With one stupid exception: if $\Sigma = \emptyset$, then $K^\Sigma = \widetilde{K}$ which is not separable over K in the geometric case.

[6] For the experts: we have not assumed X to be separated, so we cannot in general identify $X(R_v)$ with a subset of $X(K_v)$. If this causes trouble, just assume X separated—which is done in [**MB2**] and [**MB3**] anyway; but in fact this is unnecessary.

each $\underline{t}^{(v)}$ in the sense that we have $|x_i - t_i^{(v)}|_w < \varepsilon_v$ for each i and each place w of $\widetilde{K}$ inducing a $v \in \Sigma$.

2.6. History. The first proof of a special case of 2.2 is due to Cantor and Roquette [**C-R**]: they proved the theorem under the assumption that X_K is a K-unirational variety (i.e., dominated by an open subset of an affine K-space).

The general case was then proved in [**MB3**]. A proof in a more valuation-theoretic language was later given in [**G-P-R**].

Taking $\Omega_v = X(R_v)$ in 2.2, we obtain the following "local-to-global" version:

2.7. Corollary (refined local-global principle). *With notations and assumptions as in* 2.1*, let $f : X \to B$ be a B-scheme of finite type. Assume that X_K is geometrically irreducible over K, and that*

- *for all $v \in \mathrm{M}_R$, $X(\widetilde{R}_v) \neq \emptyset$;*
- *for all $v \in \Sigma$, $X(R_v)$ contains a nonsingular point (in the sense of* 2.3*).*

Then $X(R^\Sigma) \neq \emptyset$. □

2.8. Variants.

2.8.1. Just as in the case of 1.3, this theorem readily extends to arbitrary localisations of R (this was already noticed in [**MB3**], 1.7). But in contrast with 1.3, even the case $R = K$ is a nontrivial fact, for which a simplified proof is given in [**P**].

2.8.2. Theorem 2.2 is stated in [**MB3**] using local conditions which are more general than those defined above. Namely, for each $v \in \Sigma$ one fixes a finite Galois extension L_v of K_v, and takes Ω_v to be a Galois-invariant open subset of $X(L_v)$, containing smooth points. There is a maximal extension, say N, of K in $\widetilde{K}$, with the property that, for each $w \in \mathrm{M}_N$ above $v \in \Sigma$, we have $N_w \subset L_v$. If $x \in X(N)$ we can define, as before, the orbit of x as a subset of $X(L_v)$, so it makes sense to say that this orbit is in Ω_v. Theorem 2.2 generalises to this situation, but in fact this can be deduced from the seemingly weaker form presented here, which is also easier to state.

2.8.3. Theorems 1.3 and 2.2 are formulated here in terms of a given ground ring R. But they can also be seen as properties of "big" rings such as $\widetilde{R}$ or R^Σ; this is, for instance, the point of view taken in [**D**]. It is in a sense more natural; on the other hand proofs are carried out using R (or finite extensions of it) because these are Noetherian rings, over which algebraic geometry looks less exotic.

For example, we have the following "Hasse principle" for algebraic extensions of K^Σ:

2.9. Theorem. *Let $L \subset \widetilde{K}$ be an extension of K^Σ. Let V be a smooth geometrically connected variety over L. Then V has an L-rational point if and only if it has an L_w-rational point for every place w of L (resp. for every place w of L extending a place in Σ).*

Proof. The "only if" part is trivial, and the two variants are clearly equivalent because if the restriction of w to K is not in Σ, then L_w is separably closed.

For every extension $M \subset \widetilde{K}$ of K, let us denote by Σ_M the set of places of M extending places in Σ. This Σ_M has a natural compact Hausdorff topology: it is the projective limit of the finite sets $\Sigma_{K'}$, where K' runs through finite extensions

of K contained in M. Observe that in this inverse system, the transition maps are surjective.[7]

Now, assume $V(L_w) \neq \emptyset$ for all $w \in \Sigma_L$, and let us prove that $V(L) \neq \emptyset$.

First, let us assume $L = K^\Sigma$. Then the result is a mere rephrasing of (a special case of) 2.2. Indeed, V is defined over some finite extension $K' \subset L$ of K, which must be split over Σ since it is contained in L. So let us fix a "K'-model" of V, i.e., a K'-variety X' plus an isomorphism $L \otimes_{K'} X' \xrightarrow{\sim} V$. If $v \in \Sigma_{K'}$, then v extends to some $w \in \Sigma_L$, and $K'_v \xrightarrow{\sim} L_w$, which implies that $X'(K'_v) \neq \emptyset$. Now just apply 2.2, where R is replaced by K', Σ by $\Sigma_{K'}$, and Ω_v is defined as $X'(K'_v)$ (note that $(K')^{\Sigma_{K'}} = K^\Sigma = L$).

The case when L is finite over K^Σ follows easily: apply the previous case to the Weil restriction of V to K^Σ.

In the general case, V is defined over a finite extension L_0 of K^Σ contained in L. Fixing L_0 and an L_0-model V_0 of V, consider, for every intermediate field $L_0 \subset M \subset L$, finite over L_0, the set

$$F_M := \{v \in \Sigma_M \mid V_0(M_v) = \emptyset\}.$$

It is easy to see that F_M is closed in Σ_M, and that F_L is the inverse limit of all F_M's for M finite over L_0. But, by assumption, F_L is empty, so by compactness F_M must be empty for some finite M, over which the previous case applies. □

2.10. Field-theoretic consequences. Pop observed in [**P**] that results such as 2.9 gave a wealth of new examples of fields with nice field-theoretic properties. For instance, taking $K = \mathbb{Q}$ and $\Sigma = \{\infty\}$ in 2.9 leads to the conclusion that $\mathbb{Q}^{\mathrm{tr}}$ is a pseudo-real closed (PRC) field, and that $\mathbb{Q}^{\mathrm{tr}}[\sqrt{-1}]$ is pseudo-algebraically closed (PAC). Let me just recall that a field k is PAC if every (geometrically irreducible) k-variety has a k-rational point.

More generally, all K^Σ's are examples of *large fields*, a notion first introduced by Pop in [**P**] (and an example of a good notion with a poor name).

In the same circle of ideas, 2.9 immediately implies the following:

2.11. Corollary. *Let $L \subset \widetilde{K}$ be an extension of K^Σ. Assume that for every place w of L above Σ, the field L_w is algebraically closed. Then L is PAC.*

For instance, let Σ_1 and Σ_2 be two disjoint finite sets of places of K. Then the composite extension $K^{\Sigma_1} K^{\Sigma_2}$ is a PAC field. □

2.11.1. *Remark.* Of course, one coud replace "algebraically closed" by "PAC" in the statement of the corollary; however, as the referee has pointed out to me, this would not be much of an improvement (at least in the number field case) since Frey and Prestel have shown (see for instance [**F-J**], Thm. 10.14) that every Henselian valued field which is PAC is separably closed.

3. Application: constructing varieties

One of the first types of applications of Rumely-like theorems that comes to mind (at least to a geometer's mind) is this: these results provide existence theorems for very general systems of equations over, say, $\widetilde{\mathbb{Z}}$. But solutions of some systems are known to parametrise geometric objects such as varieties — this is the general

[7] If $\widehat{K}$ denotes the K-algebra $\prod_{v\in\Sigma} K_v$, then one can also identify Σ_M with $\mathrm{Spec}\,(\widehat{K} \otimes_K M)$, with the Zariski topology.

idea of "moduli spaces". So, we should be able to deduce from our theorems the existence of *varieties over number fields with prescribed behaviour over the integers.*

3.1. Notations. To illustrate these ideas, we shall from now on take the case of curves. We fix an integer $g \geq 1$. By a *curve* over a field K we shall mean, in this section:

- either a projective, smooth, geometrically connected K-curve of genus g,
- or, in case $g = 1$, an elliptic curve, i.e. a K-curve of genus 1 plus a rational point, called the "base point".

(In the first case we do not exclude $g = 1$). "Either" means that the following discussion will be valid for each of the above definitions of a curve. Occasionally we shall have to distinguish between three cases: the case $g \geq 2$ and the two $g = 1$ cases (with and without base point).

There is a corresponding notion over any base scheme S: an *S-curve* will be an S-scheme $\varphi : C \to S$, with φ projective and smooth, such that for every point $s \in S$ the fibre C_s is a $\kappa(s)$-curve in the above sense (as usual, $\kappa(s)$ denotes the residue field of s). In the "elliptic curve" variant, the curve (of genus 1) should be provided with a section $\varepsilon : S \to C$ of φ, still called the base point.

These S-curves form a category $\mathcal{M}(S)$, where morphisms are just isomorphisms of S-schemes (respecting the base point, in the elliptic case). We denote by $M(S)$ the set of (S-)isomorphism classes of S-curves. Note that for every morphism $S' \to S$ we have a base change functor $\mathcal{M}(S) \to \mathcal{M}(S')$ and a corresponding map $M(S) \to M(S')$, so that M is a contravariant functor from schemes to sets.

Now, one can fairly easily deduce from Rumely's theorem 1.3 the following result (recall that from now on the meaning of "curve" is restricted to one of the above):

3.2. Theorem. *There exists a number field L, with ring of integers O_L, and a curve $C \to \operatorname{Spec} O_L$ in the above sense. In other words, there exists a curve over* $\operatorname{Spec} \widetilde{\mathbb{Z}}$.

In more classical terms: there exists a number field L and an L-curve with good reduction at each finite place of L.

3.3. Local conditions. Before I explain how one can prove this, let us try to go further and guess what a version "with splitting conditions" should look like. So, let us fix, say, K, R and Σ as in 2.1. First, there certainly exist curves over any field (in particular over each K_v), so if we believe in an analogue of 2.2 we should expect the existence of a curve $C \to \operatorname{Spec} R^\Sigma$. Moreover, as examples of "local approximation" conditions, one could fix, for instance:

- for each finite place $v \in \Sigma$, a curve Γ_v over the residue field $\kappa(v)$ of v,
- for each real place $v \in \Sigma$, a curve Γ_v over $K_v = \mathbb{R}$,

and require our curve C to satisfy, for each $v \in \Sigma$, the following condition:

Condition (Cond_v):

- *If v is finite, C has reduction isomorphic to Γ_v*[8] *at each place of K^Σ above v* (this makes sense since the residue fields are the same).

[8] Of course, this contains the assumption that the curve C_{K^Σ} has good reduction at all places above v; this is automatic if $v \in \mathrm{M}_R$, and in this case the condition means that the $\kappa(v)$-curve deduced from C by any R-morphism $R^\Sigma \to \kappa(v)$ is isomorphic to Γ_v.

- *If v is real, for every place w of K^Σ above v, the curve C_w over $K_w^\Sigma \cong \mathbb{R}$ deduced from C has the same number of real connected components as Γ_v.*

And, as we whall see, we have in fact the following:

3.4. Theorem. *With data as in* 3.3*, there exists a curve $C \to \operatorname{Spec} R^\Sigma$ satisfying condition* (Cond_v)*, for each $v \in \Sigma$.*

3.5. The natural strategy. Let us pretend, temporarily, that the functor M of 3.1 is *representable*: that is, there is a scheme $\underline{M}$ (a "fine moduli scheme for curves") and, for every scheme S, a bijection between $M(S)$ and the set $\underline{M}(S)$ of morphisms from S to $\underline{M}$, this bijection being functorial in S. (Intuitively, such an $\underline{M}$ should be thought of as a "parameter space for all curves").

Assume, moreover, that this $\underline{M}$, as a scheme over $\operatorname{Spec}\mathbb{Z}$, satisfies our usual assumptions: namely, that it is irreducible, of finite type, and that its generic fibre $\underline{M}_{\mathbb{Q}}$ is geometrically irreducible. (Note that it is automatically surjective since there are curves over any field). From this we would immediately deduce Theorem 3.2, simply by applying Rumely's theorem 1.3 to $\underline{M}$!

Next, to prove the refined version 3.4, define Ω_v, for $v \in \Sigma$, as the set of $x \in \underline{M}(R_v)$ such that the corresponding curve over K_v satisfies (Cond_v). Now I claim that Ω_v is automatically open in $x \in \underline{M}(K_v)$, for the v-adic topology. Unraveling the definitions, this boils down to the following fact, which is not hard to prove: Let $C \to S$ be any S-curve, where S is a K_v-scheme of finite type. Then the set $\{x \in S(K_v) \mid \text{ the curve } C_x \text{ satisfies } (\mathrm{Cond}_v)\}$ is v-adically open.

So, to conclude by applying 2.2, we only need some smoothness property for $\underline{M}$ (recall that in 2.2, the Ω_v's are assumed to contain nonsingular points). But we shall come back to this later and stop dreaming for now, because

3.6. The strategy fails. Indeed, the functor M is *not* representable. This is in fact easy to see: if k' is an extension of a field k, the natural map $M(k) \to M(k')$ is in general not injective, which it would be if M were representable.

To overcome this, there are two possible approaches:

- *The ad hoc way:* Try to replace the moduli functor M by something else that is a scheme to which our theorems apply, and is still related to curves.
- *The ambitious way:* Try to generalise Theorems 1.3 and 2.2 so that they apply not only to schemes but to moduli problems such as M.

In fact, as I shall now explain, both approaches work.

3.7. The ad hoc way, I. This method will be enough to prove Theorem 3.2. It is known that there is a "coarse moduli scheme for curves": a scheme M' of finite type over $\mathbb{Z}$, plus, for every scheme S, a map $h(S) : M(S) \to M'(S)$, functorial in S, which is in a sense a "best approximation of M from the right by a representable functor". In fact, this M' is quite familiar if $g = 1$ (with or without marked point): it is the affine line $\operatorname{Spec}\mathbb{Z}[T]$, and the map h associates to a genus 1 curve its modular j-invariant.[9] (The existence of M' is much harder to prove if $g \geq 2$).

The map $h(S)$ is in general neither injective nor surjective (even for elliptic curves); however it is bijective when $S = \operatorname{Spec} k$ where k is an algebraically closed

[9] Observe, however, that Theorem 3.2 is rather trivial if $g = 1$: just take a curve with integral j-invariant! We could make it more interesting by imposing some further condition on the invariant $j(C)$, such as "$P(j(C))$ is invertible in $\widetilde{\mathbb{Z}}$", for some specified primitive polynomial $P \in \mathbb{Z}[T]$.

field, or, more generally, an integrally closed domain with algebraically closed fraction field, such as $\widetilde{\mathbb{Z}}$. So, Theorem 3.2 will be proved if we show that $M'(\widetilde{\mathbb{Z}}) \neq \emptyset$. To get this we can now apply 1.3, or more simply its local-global version 1.7: it is obvious that $M'(\widetilde{\mathbb{Z}}_p) \neq \emptyset$ for every prime p (in fact $M'(\mathbb{Z}_p) \neq \emptyset$, since there are $\mathbb{Z}_p$-curves), and the geometric irreduciblity of $M'_{\mathbb{Q}}$ is equivalent to the irreducibility of $M'_{\mathbb{C}}$ which is a (deep) classical fact[10]. Theorem 3.2 now follows.

3.8. The ad hoc way, II. The above method fails for the problem with local conditions of 3.3, because, with our notations, the map $h(\operatorname{Spec} R^{\Sigma})$ is not surjective in general. In other words, even if we can produce a finite extension R' of R, contained in R^{Σ}, and an element of $M'(R')$, we can associate it to a curve only over some further finite extension of R', which is hard to control (and in particular may not be contained in R^{Σ}). Another difficulty is that M' is in general singular, so we may have trouble finding smooth points in our Ω_v's.

3.8.1. But, instead of approximating M from the right (by a map $M \to M'$), we may try to approach it from the left, i.e., find a scheme H and a morphism of functors $H \to M$ with nice properties. Note that, just by general nonsense, such a map is nothing else than an (isomorphism class of) H-curve. So, forgetting (temporarily) about moduli spaces, our problem is this: find a scheme $H \to B$ satisfying the assumptions for X in Theorem 2.2, and an H-curve $C \to H$ with the property that, for each $v \in \Sigma$, there is at least a smooth point $x_v \in H(R_v)$ such that the fibre C_x satisfies (Cond_v). (As we remarked in 3.5, the set Ω_v of these points is open in $H(K_v)$).

The latter condition will of course be satisfied if *every* curve, over any field k, occurs as the fibre of $C \to H$ at some point $x \in X(k)$. We shall in fact obtain this stronger condition, except for curves of genus 1 without marked point.

So now let's distinguish between our three cases. The respective H's will be denoted by H_{ell} and H_g; moreover we shall construct them for $R = \mathbb{Z}$, to simplify notations; over a general R, just make a base change, i.e. use the fibre product $H \times_{\operatorname{Spec} \mathbb{Z}} B$.

3.8.2. *Elliptic curves.* In this case, the solution is in fact much simpler than the method of 3.7. The key fact is that any elliptic curve (over a field, say) is embeddable as a cubic in $\mathbb{P}^2$. If we denote the homogeneous coordinates by Z_0, Z_1, Z_2, we can choose the embedding so as to map the origin to a specified point, say the traditional (0:1:0), and, to normalise things further, we can impose the line $Z_2 = 0$ as an inflection tangent at that point. Such a cubic has a unique homogeneous equation F satisfying $F(Z_0, Z_1, 0) = Z_0^3$.

Conversely, a form of degree 3 in Z_0, Z_1, Z_2 with this property is the normalised equation of a cubic, nonsingular iff the discriminant of the form is nonzero. Such forms are parametrised by an affine space $Q \cong \mathbb{A}^6_{\mathbb{Z}}$, with the 6 remaining coefficients $T_1, \ldots, T_6$ as coordinates. Singular cubics correspond to the hypersurface Δ defined by the vanishing of the discriminant, a polynomial $D \in \mathbb{Z}[T_1, \ldots, T_6]$ which must be primitive since there exist normalised cubics over any field.

Now, if we put

$$H_{\mathrm{ell}} = Q \setminus \Delta = \operatorname{Spec}(\mathbb{Z}[T_1, \ldots, T_6, D^{-1}]),$$

[10] If $g \geq 2$, the topological space $M'_g(\mathbb{C})$ can be constructed as a quotient of the "Teichmüller space" which is homeomorphic to $\mathbb{R}^{6g-6}$.

we have a canonical H_{ell}-cubic $C_{\mathrm{ell}} \subset H_{\mathrm{ell}} \times \mathbb{P}^2$ (given by the obvious cubic form with coefficients T_i), with a section given by (0:1:0). Every elliptic curve (E, ε) over a field k occurs as a fibre of that family: embed E into $\mathbb{P}^2_k$, in the normalised way above, and take the point of $H_{\mathrm{ell}}(k)$ corresponding to the normalised equation of E.

Since H_{ell} is obviously smooth over $\operatorname{Spec} \mathbb{Z}$, with geometrically irreducible fibres (it is an open subset of an affine space, and D is primitive), we can apply Theorem 2.2 to it, and we are done.

3.8.3. *Genus $g \geq 2$: discussion.* To explain the next construction, let us first examine *how* an elliptic curve (E, ε) over a field is embedded into $\mathbb{P}^2$. The trick is to consider ε as a divisor on E, and to consider the linear system $|3\varepsilon|$: using Riemann-Roch, one proves that this is a projective plane, and that the canonical rational map from E to this space is an embedding. To actually embed the curve in $\mathbb{P}^2$, all we need is choose a projective basis of $|3\varepsilon|$, e.g. a basis of the vector space $\mathcal{L}(3\varepsilon)$ of functions on E with at most a triple pole at ε.[11]

So the key to our construction was the existence of a "natural" divisor (or invertible sheaf) giving rise to a projective embedding of the curve.

Now if C is a curve of genus $g \geq 2$ over a field k, we still have such an object: it is the "tricanonical system", given by the sheaf $\Omega^{\otimes 3}_{C/k}$ of triple differentials. Its space of global sections (the k-vector space of regular triple differentials on C) has dimension $5g - 5$ by Riemann-Roch, so if we choose a basis of this space we get an embedding of C into $\mathbb{P}^{5g-6}_k$.

But, contrary to the case of elliptic curves, we don't know in general what the equations of the curve so embedded may look like, so we cannot construct a parameter space explicitly, as we did in 3.8.2 using cubics. However, in the elliptic case we could have defined H_{ell} by the functor that it represents; for instance, if k is a field, $H_{\mathrm{ell}}(k)$ is in canonical 1-1 correspondence with the set of isomorphism classes of triples $(E, \varepsilon, \mathcal{B})$ where (E, ε) is an elliptic curve over k and $\mathcal{B}$ is a basis of $\mathcal{L}(3\varepsilon)$, suitably normalised. This description of $H_{\mathrm{ell}}(k)$ can be extended to arbitrary schemes (instead of $\operatorname{Spec} k$), and has an analogue H_g for genus $g \geq 2$ which we can now describe:

3.8.4. *Genus $g \geq 2$: construction of H_g.* For every scheme S, let us put

$$H_g(S) \quad = \quad \text{set of isomorphism classes of pairs } (C \xrightarrow{\varphi} S, \mathcal{B}), \text{ where:}$$
$$\bullet\ C \xrightarrow{\varphi} S \text{ is an } S\text{-curve, and}$$
$$\bullet\ \mathcal{B} \text{ is a basis oftriple differentials}^{12} \text{ of } C \text{ on } S.$$

Now it is a standard fact that this H_g is representable by a scheme of finite type over $\mathbb{Z}$. One shows this by noting, as before, that an element $(C \xrightarrow{\varphi} S, \mathcal{B})$ canonically determines an embedding of C into $\mathbb{P}^{5g-6}_S$, so that one can also view $H_g(S)$ as a set of S-curves *embedded into a fixed projective space over S*, and there are powerful standard tools to treat such objects.

If we still denote by H_g the scheme representing H_g, we have, by general nonsense, an H_g-curve $\mathcal{C}_g \to H_g$ (with a basis of triple differentials). If k is a field and C is a k-curve, then any choice of basis of triple differentials on C determines an

[11] The normalisation conditions on the embedding are easily expressed in terms of the chosen basis of $\mathcal{L}(3\varepsilon)$.

[12] By this we mean, in fancy terms, a basis of the sheaf $\varphi_*(\Omega^{\otimes 3}_{C/S})$, which is locally free of rank $5g - 5$ and replaces the space of triple differentials of the preceding discussion.

element of $H_g(k)$, i.e., a k-point of H_g, the fiber of $\mathcal{C}_g$ at that point being isomorphic to C. Next:

3.8.5. *Genus ≥ 2: H_g is smooth over* $\operatorname{Spec}\mathbb{Z}$. To prove this, there is a powerful criterion due to Grothendieck: H_g is smooth if and ony if, whenever A is a ring and I an ideal of A with square zero, the natural map $H_g(A) \to H_g(A/I)$ is surjective. Plugging the definition of H_g into this, we just have to check that:

- every A/I-curve lifts to an A-curve, and
- for an A-curve C, every basis of triple differentials over A/I lifts to a basis over A.

The first point follows from deformation theory (basically, there is an obstruction to lifting which lives in an H^2, which for a curve is zero). The second boils down to the following completely elementary fact: if F is a locally free A-module of finite type, every A/I-basis of F/IF lifts to a basis of F.

3.8.6. *Genus ≥ 2: $H_{g,\mathbb{Q}}$ is geometrically irreducible.* We have a morphism h from H_g to the coarse moduli scheme M' sending $(C \to S, \mathcal{B})$ to the element of $M'(S)$ corresponding to the S-curve C. Since we know that $M'_{\mathbb{C}}$ is irreducible, it is enough to show that h has geometrically irreducible fibres. But if C is a curve over an algebraically closed field k, and $[C] \in M'(k)$ corresponds to C, then $h^{-1}([C])$ is isomorphic to the variety of bases of triple differentials on C, modulo the natural action of $\operatorname{Aut} C$. Since the variety of bases is isomorphic to $\mathrm{GL}_{5g-5,k}$, this is obviously irreducible.[13]

3.8.7. *Genus ≥ 2: conclusion.* We can now apply Theorem 2.2 to the scheme $H_g \times_{\operatorname{Spec}\mathbb{Z}} B$ with the local data explained in 3.8.1. This proves Theorem 3.4 (and, of course, reproves 3.2).

3.8.8. *Genus 1.* For curves of genus 1, the method of 3.8.2 doesn't work because there is no ε we can use; the method of 3.8.3 also fails because the canonical sheaf of a curve of genus 1 is trivial (at least locally on the base), so it cannot be used to get a projective embedding.

In fact, of course, a given curve of genus 1 (say, over a field) can be embedded into a projective space, but there is no uniform bound (valid for all curves) for the degree of the embedding. So, there is no hope of finding (as we did in previous cases) a scheme H_1 of finite type over $\mathbb{Z}$ and an H_1-curve of genus 1 including, as fibers, *all* curves of genus 1 over fields[14].

Fortunately, we only "need" finitely many such curves: for every $v \in \Sigma$, choose an R_v-curve C_v satisfying (Cond_v), and then fix an integer $d \geq 3$ such that each C_v has a divisor of degree d over K_v. Now, for a scheme S, define $H_1(S)$ as the set of isomorphism classes of triples $(C \xrightarrow{\varphi} S, \mathcal{L}, \mathcal{B})$ where $C \to S$ has genus 1, $\mathcal{L}$ is an invertible sheaf of degree d on C, and $\mathcal{B}$ is a basis of $\varphi_*\mathcal{L}$. Again, for such a triple, we have a canonical embedding of C into $\mathbb{P}^d_S$, and H_1 is representable, smooth over $\mathbb{Z}$, with geometrically irreducible fibres; moreover our choice of d ensures that each of our curves C_v corresponds to (many) points of $H_1(K_v)$, so conditions (Cond_v) define nonempty open subsets of $H_1(K_v)$, and we can apply Theorem 2.2.

[13] More precisely, there is a natural action of the $\mathbb{Z}$-group scheme GL_{5g-5} on H_g, corresponding to "changing the basis", and M' can be defined as the quotient scheme.

[14] Not even if we fix the field and the j-invariant of the curve!

3.9. The ambitious way: algebraic stacks. In a sense, the failure of the strategy 3.5 can be blamed on curves with nontrivial automorphisms: for instance, the non-injectivity of $M(k) \to M(k')$ for a field extension is due to the existence of "twisted forms" of curves; for $g \geq 2$, the non-smoothness of the coarse moduli scheme M' is due to the fact that GL_{5g-5} does not act freely at points of H_g corresponding to curves with automorphisms.[15]

But a more sound mathematical attitude would be to say: "Automorphisms are a fact of nature; perhaps they are not troublesome by themselves, but *we* are in trouble because we sinfully persist in ignoring them by only considering sets of isomorphism classes."

In other words, if we want to classify curves over a scheme S, the natural object to look at is not the set $M(S)$ defined above but the *category* $\mathcal{M}(S)$ of S-curves. Accordingly, the functor M is to be replaced by the assignment to each S of the category $\mathcal{M}(S)$, together with base change *functors* $\mathcal{M}(S) \to \mathcal{M}(S')$ associated to morphisms $S' \to S$.

Such an assignment (satisfying some quite natural conditions) is called a *fibred category* over the category $\underline{\mathrm{Sch}}$ of schemes. Note that, if X is any scheme, we can trivially associate to X the fibred category $S \mapsto X(S) = \mathrm{Hom}_{\underline{\mathrm{Sch}}}(S, X)$ (a set being identified with a category where the only morphisms are identities). In this way we can view a scheme as a (very) special case of fibred category. These fibred categories will here be called *representable*.

Now certain fibred categories, called *algebraic stacks* (and including our $\mathcal{M}$), are so close to being representable that many notions and constructions can be generalised to them: it makes sense to say that an algebraic stack is connected, or irreducible, or normal, or Noetherian, or smooth over another.

For instance, the stack $\mathcal{M}$ is smooth over $\mathrm{Spec}\,\mathbb{Z}$, contrary to the scheme M'; this is just the deformation-theoretic argument of 3.8.5. Furthermore, the scheme H_g defined in 3.8.4 is provided with a natural "forgetful" morphism $\pi : H_g \to \mathcal{M}$ sending $(C, \mathcal{B})$ to C (which can also be seen as the classifying morphism for the H_g-curve $\mathcal{C}_g$ of 3.8.4). Now π is smooth (this is the "basis lifting property" of 3.8.5), and in a precise sense π makes H_g into a principal GL_{5g-5}-bundle over $\mathcal{M}$.

The definition of an algebraic stack is beyond the scope of this paper (see [**L-MB**]).[16] Suffice it to say that the word "stack" refers to good properties with respect to étale descent (of which Galois descent is a special case), while "algebraic" reflects, among other things, the existence of a "nice covering" by a scheme. For instance, in 3.8 we constructed (in various ways) a curve C over a "parameter scheme" H, which we used as a substitute for a moduli scheme for curves. Now we can view this $C \in \mathcal{M}(H)$ as a morphism $H \to \mathcal{M}$, which happens to be such a "nice covering".

We have seen in 3.5 an example of how some natural notions for schemes (or varieties) can be generalised to stacks, when we explained why our Ω_v's are open. More generally, if F is, say, a local field, and $\mathcal{X}$ is an algebraic F-stack of finite

[15] And, in fact, one can define a subfunctor of M by restricting to curves without nontrivial automorphisms; this turns out to be representable and to provide another proof of 3.4, if $g \geq 3$ (if $g \leq 2$ this functor is empty).

[16] Historically, the general notion of stack (the French word is "champ") is due to Grothendieck, and is studied in detail in [**G**]. Algebraic stacks were first introduced in [**D-M**] for the study of the moduli of curves; the definition was then modified by Artin [**A**] to include more general objects. The definition adopted in [**L-MB**] is slightly less general than Artin's.

type, an *open subset* Ω of $\mathcal{X}(F)$ is a set of isomorphism classes of objects of $\mathcal{X}(F)$ with the following property: for every F-scheme S of finite type and every object C of $\mathcal{X}(S)$, the set of points $x \in S(F)$ such that the object C_x of $\mathcal{X}(F)$ (obtained from C by the base change $x : \operatorname{Spec} F \to S$) belongs to Ω, is open in $S(F)$ for the metric topology.

Now, it simply turns out that Theorem 2.2 is still true if one replaces the B-scheme X by an algebraic B-stack with the same assumptions. This is proved in [**MB5**], and immediately implies 3.4 as a special case.

3.10. Refinements. In [**MB5**], we refine Theorem 2.2 in other ways. First, we also treat the case when X_K is not necessarily geometrically irreducible (in concrete cases this may prove more convenient than trying to reduce to that case by some extension of K).

More importantly, it is shown in [**MB5**] that the incompleteness condition of 2.1 can be omitted in some cases, including Theorem 3.4 when $g \geq 3$.

4. Application to Galois groups

4.1. Preliminaries on Galois algebras. Let G be a finite group. For a ring A, a *G-Galois A-algebra* is an A-algebra A' with an action of G on the left by A-automorphisms, such that A' is a locally free A-module of rank $|G|$, and $A' \otimes_A A'$ (with G acting, say, on the right factor) is isomorphic to the permutation algebra $A'^{|G|}$ as an A'-algebra with G-action.

If A and A' are fields, this is just the usual notion of a Galois extension with group G; but if A'' is another extension field of A, then $A'' \otimes_A A'$ is still a G-Galois A''-algebra, even if it is not a field.

These notions generalise to schemes in an obvious way, via the notion of *G-torsor:* a G-torsor over a scheme Y may be defined as a Y-scheme $\pi : X \to Y$, plus a free action of G on X such that π induces an isomorphism $X/G \xrightarrow{\sim} Y$.

There is an obvious "induction" procedure: if H is a subgroup of G, and A_1 is an H-Galois A-algebra, then A_1 maps H-equivariantly into a G-Galois A-algebra $\operatorname{Ind}_H^G A_1$, which is universal in an obvious sense, and can be defined as the A-algebra of H-equivariant maps from G to A_1, with the left G-action deduced from the right action of G on itself by translation. As an A-algebra, it is isomorphic to the product of $(G : H)$ copies of A_1.

If k is a field, every G-Galois k-algebra k' is obtained in this way from a subgroup H of G and a Galois *extension* of k with group H; this H is unique up to conjugacy in G, and deserves the name of *decomposition group* of k' over k. Obviously, if k_1 is another extension of k, the decomposition group of $k_1 \otimes_k k'$ over k_1 is contained in H. Moreover, of course, k' is a field if and only if $H = G$. From this we deduce:

4.1.1. Lemma. *Let k be a field and let k' be a G-Galois k-algebra. Assume that for every cyclic subgroup C of G, there is an extension k_C of k such that the decomposition group of $k_C \otimes_k k'$ over k_C contains C. Then k' is a field.*

Proof. This follows from the preceding remarks and the following well-known fact: if G is a finite group and H is a subgroup of G, meeting every conjugacy class of G, then $H = G$. (Idea of proof: observe that if e is the unit element of G, then $G \setminus \{e\}$ is the union of all conjugates of $H \setminus \{e\}$, and then count). □

Now let us go back to local-global principles.

4.2. Notations. We fix a finite group G. The symbols K, M_K, $\widetilde{K}$, K_v (resp. Σ and K^Σ) have the same meaning as in 1.1 (resp. 2.1). We shall apply the results of sections 1 and 2 for $R = K$ (in particular the incompleteness condition is trivially satisfied).

4.3. Theorem. *With notations as above, fix for each $v \in \Sigma$ a G-Galois K_v-algebra L_v. Then there exist:*

- *a finite extension E of K, contained in K^Σ (i.e., split over Σ), and*
- *a Galois extension F of E, with group G,*

such that for each $v \in \Sigma$ and each K-embedding $\sigma : E \to K_v$, the G-Galois K_v-algebra $K_v \otimes_{\sigma,E} F$ is isomorphic to L_v.

4.4. Proof of 4.3: first reduction. Assume that we can prove (for every choice of data) the weaker version of Theorem 4.3 where F is only required to be a G-Galois E-algebra, not necessarily a field. Then we can argue as follows: for every (conjugacy class of) cyclic subgroup C of G, pick a finite place v_C of K (with all the v_C's distinct and not in Σ), and a C-Galois extension N_C of K_{v_C}. (These things exist!) Now enlarge Σ by adjoining all v_C's, put $L_{v_C} = \mathrm{Ind}_C^G N_C$ for each C, andapply the weak version of the theorem to these data. We obtain an extension E of K and a G-Galois E-algebra F, which satisfies our local requirements above the original Σ, and must be a field by Lemma 4.1.1.

So we are reduced to proving the weak version of 4.3 explained above. This can be rephrased as follows: with the same data as in 4.3, there exists a G-Galois algebra M over K^Σ, with local structure specified by L_v at places over v, for each $v \in \Sigma$. This looks very much like a "local-to-global" problem, and in fact we can repeat the discussion of 3.5 and 3.6, replacing curves by G-torsors throughout. And, as before, we have two ways out:

4.5. The ambitious way. If we associate to each K-scheme S the category of G-torsors over S, we obviously get a fibred category (see 3.9) over the category of K-schemes. Just as $\mathcal{M}$ in 3.9, this turns out to be an algebraic stack of finite type over K, sometimes called the *classifying K-stack* of G, and denoted by $\mathrm{B}(G/K)$.[17]

In a sense, $\mathrm{B}(G/K)$ has only one point, because any G-torsor becomes trivial after some finite étale base change. This can be made precise: the trivial G-torsor over $\operatorname{Spec} K$ defines a morphism $\operatorname{Spec} K \to \mathrm{B}(G/K)$, which is étale and surjective (strange as it may sound, since it is also a section of the structural morphism $\mathrm{B}(G/K) \to \operatorname{Spec} K$!). Consequently, $\mathrm{B}(G/K)$ is smooth and geometrically irreducible over K.

Now for the v-adic topologies: assume S is a K_v-scheme of finite type, for some $v \in \Sigma$, and $\pi : S' \to S$ is a G-torsor. Then the set of $x \in S(K_v)$ such that the G-torsor $\pi^{-1}(x)$ over K_v is isomorphic to $\operatorname{Spec} L_v$, is v-adically open: this is easily deduced from the fact that K_v is Henselian. In other words, the "set" Ω_v of G-torsors over K_v isomorphic to L_v is open (and nonempty!) in $\mathrm{B}(G/K)(K_v)$, in

[17] This type of stack, already discussed in [**D-M**], is the simplest example of an algebraic stack which is not a scheme. In this respect it is one of the basic examples to keep in mind when one wants to learn how to use stacks; simple as it is, it shows many of the counter-intuitive phenomena that may confuse beginners.

the sense defined in 3.9. So, just as we did there, we can apply the main result of [**MB5**], generalising 2.2 to stacks. This proves Theorem 4.3.

4.6. The ad hoc way. There is, trivially, a coarse moduli space for $\mathrm{B}(G/K)$, which is just the point $\operatorname{Spec} K$ and doesn't help a bit, for the same reasons as explained at the beginning of 3.8.

But we have a morphism $X \to \mathrm{B}(G/K)$ which can play the same role as $H \to \mathcal{M}$ in 3.8, and is in fact well known in inverse Galois circles since it is the key to "Noether's method".

So let's forget about $\mathrm{B}(G/K)$ and consider the natural permutation action of G on the affine space $\mathbb{A}_K^{|G|}$, and denote by U the open subset where "all coordinates are distinct", i.e., the largest open subset where G acts freely. Now put $X = U/G$: the natural map $\pi : U \to X$ defines a G-torsor over X. Obviously, X is smooth and geometrically irreducible over K.

Next, I claim that for every extension E of K, every G-Galois E-algebra F "occurs in π" i.e., there is a point of $X(E)$ whose fibre under π is G-isomorphic to $\operatorname{Spec} F$. Indeed, the E-algebra F is generated by one element $x \in F$ (recall that K is infinite); one then gets a point of $U(F) \subset F^{|G|}$ with coordinates gx ($g \in G$), and one then checks that the image of that point in $X(F)$ is in fact E-rational and satisfies our requirements.[18]

In particular, for each $v \in \Sigma$, the set Ω_v of points $x \in X(K_v)$ such that $\pi^{-1}(x) \cong \operatorname{Spec} L_v$ is nonempty (and open, as we have seen in 4.5). So all conditions of Theorem 2.2 are satisfied, and again Theorem 4.3 is proved.

4.7. Remark. Theorem 4.3 was proved in [**MB4**], where the author also takes unnecessary care to ensure that, in addition, the extension F/E is unramified outside Σ. This can easily be achieved by enlarging E to "kill ramification".

Observe that, to obtain 4.3 by Noether's method (4.6) we need Theorem 2.2 only for a unirational variety, i.e., in the form proved in [**C-R**].

4.8. Corollary. *If Σ contains a finite place, then G is a Galois group over K^Σ.*

Proof. Since $[K^\Sigma : K] = \infty$, we may, by replacing K by a finite extension, assume that Σ contains as many finite places as we need. Then choose finite places v_C and extensions N_C just as in 4.4, except that we take the v_C's in Σ, and apply 4.3, to get an extension F/E: again it follows from Lemma 4.1.1 that the G-Galois K^Σ-algebra $K^\Sigma \otimes_E F$ is in fact a field. □

4.9. Remark. The proof of 4.8 actually shows more: there exists a Galois extension of K^Σ, with group G, and prescribed local structure over every place of Σ except one fixed finite place.

4.10. Remark. In [**P**], Pop gives a precise structure theorem for the absolute Galois group of K^Σ, which immediately implies 4.8, but is also harder to prove.

When Σ is a (nonempty) set of *real* places, Pop's theorem implies that every finite group *generated by involutions* is a Galois group over K^Σ. (The special case where $K^\Sigma = \mathbb{Q}^{\mathrm{tr}}$ was proved earlier in [**F-H-V**]). I have not been able to give a

[18] In fact, we have a nice description of the functor represented by X in terms of G-torsors: for every K-scheme S, $X(S)$ can be identified with the set of isomorphism classes of pairs $(S' \to S, j)$ where $S' \to S$ is a G-torsor and j is an S-embedding $S' \hookrightarrow \mathbb{A}^1_S$. Compare with 3.8, where our problem was solved, essentially, by considering *embedded* curves.

proof of this along the lines of 4.8: the argument breaks down when one tries to use 4.1.1.

References

[A] M. Artin, *Versal Deformations and Algebraic Stacks*, Invent. Math. 27 (1974), 65–189.

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

[D] L. Darnière, *Decidability and Local-Global Principles*, this volume.

[D-M] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. 36 (1969), 75–110.

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

[F-H-V] M. Fried, D. Haran and H. Völklein, *Absolute Galois group of the totally real numbers*, C. R. Acad. Sci. Paris Sér. I Math. 317 (1993), 995–999.

[F-J] M. Fried and M. Jarden, *Field Arithmetic*, Ergeb. Math. Grenzgeb. (3), Volume 11, Springer (1986).

[G] J. Giraud, *Cohomologie non abélienne*, Grundlehren Math. Wiss. 179, Springer (1971).

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

[L-MB] G. Laumon and L. Moret-Bailly, *Champs algébriques*, Ergeb. Math. Grenzgeb. (3), Volume 39, Springer (1999).

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

[MB1] L. Moret-Bailly, *Points entiers des variétés arithmétiques*, Séminaire de Théorie des Nombres, Paris 1985-86, Progress in Math. Volume 71, Birkhäuser (1988).

[MB2] L. Moret-Bailly, *Groupes de Picard et problèmes de Skolem I*, Ann. Sci. École Norm. Sup. (4) 22 (1989), 161–179.

[MB3] L. Moret-Bailly, *Groupes de Picard et problèmes de Skolem II*, Ann. Sci. École Norm. Sup. (4) 22 (1989), 181–194.

[MB4] L. Moret-Bailly, *Extensions de corps globaux à ramification et groupe de Galois donnés*, C. R. Acad. Sci. Paris Sér. I Math. 311 (1990), 273–276.

[MB5] L. Moret-Bailly, *Problèmes de Skolem sur les champs algébriques*, Compositio Math. (to appear).

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

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

[Ru2] R. Rumely, *Capacity Theory on Algebraic Curves*, Lecture Notes in Math. 1378, Springer (1989).

[S] T. Skolem, *Lösung gewisser Gleichungen in ganzen algebraischen Zahlen, insbesondere in Einheiten*, Skrifter Norske Videnskaps-Akademi i Oslo, Mat. Naturv Kl. 10 (1934).

IRMAR, Université de Rennes 1, Campus de Beaulieu, F-35040 Rennes Cedex
E-mail address: moret@univ-rennes1.fr
URL: www.maths.univ-rennes1.fr/~moret/