LOCAL-GLOBAL PRINCIPLE FOR NORMS FROM CYCLIC EXTENSIONS OF Q(t) (A DIRECT, CONSTRUCTIVE AND QUANTITATIVE APPROACH)

Autor(en): **ZANNIER, Umberto**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **45 (1999)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **19.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-64456

L'Enseignement Mathématique, t. 45 (1999), p. 357–377

A LOCAL-GLOBAL PRINCIPLE FOR NORMS FROM CYCLIC EXTENSIONS OF $\mathbf{Q}(t)$ (A DIRECT, CONSTRUCTIVE AND QUANTITATIVE APPROACH)

by Umberto ZANNIER

ABSTRACT. Let L be a cyclic extension of $\mathbf{Q}(t)$, regular over $\mathbf{Q}$. We are concerned with the representability of a rational function $f \in \mathbf{Q}(t)$ as a norm $N^L_{\mathbf{Q}(t)}(g)$ where $g \in L$. This problem was treated by Davenport-Lewis-Schinzel in the special case $[L : \mathbf{Q}(t)] = 2$. They obtained a kind of local-global principle by proving that f is representable in the required way if, for a suitable set of integers n, $f(n)$ is likewise representable as a value of the norm-form specialized at $t = n$. In case $[L : \mathbf{Q}(t)]$ is arbitrary, it does not seem easy to extend their arguments, but a similar conclusion is a corollary of certain results on specializations of Brauer groups, obtained independently by several authors. Here we treat the general case by means of a direct method, which is self-contained as far as cohomology is concerned. Moreover our arguments are constructive and allow one to decide about the above-mentioned representability and to produce solutions when they exist. As in previous work by Serre, the method yields quantitative estimates, via sieve inequalities. We also discuss several other relevant questions.

1. INTRODUCTION

The well-known Hasse local-global principle for a cyclic extension L/K of number fields (see e.g. [CF, p. 185]) asserts that an element $a \in K^*$ is a norm from L^* (i.e. of the form $N^L_K(b)$ for some $b \in L^*$) if and only if for every place v of K and some (= all) place(s) w of L, with $w|v$, we have $a \in N^{L_w}_{K_v}(L^*_w)$ (where the subscripts denote completions). Actually Hasse's theorem holds more generally when L/K is any cyclic extension of *global fields*; these are either number fields or function fields of curves over finite fields, namely finite extensions of some field $\mathbf{F}_q(t)$.

It seems natural to investigate what happens when L/K is a cyclic extension of function fields of curves over number fields. Let us concentrate on the case when the base is rational, namely $K = k(t)$, where k is a number field.

The *constant extension* case, i.e. the case $L = k_1(t)$, k_1/k cyclic, was treated by Davenport-Lewis-Schinzel for $k = \mathbf{Q}$ [DLS1] (and generalized by Schinzel to general k [Sch1, Thm. 42]). The case of an arbitrary quadratic extension L/K was again considered by Davenport-Lewis-Schinzel. Among others, they proved ([DLS2] or [Sch1, Thm. 37]) the following elegant statement.

Let $A, B \in \mathbf{Q}[t]$ and suppose that every arithmetic progression contains an integer n such that the equation $x^2A(n) + y^2B(n) = z^2$ has a nontrivial solution $(x^*, y^*, z^*) \in \mathbf{Z}^3$. Then the equation $X^2A + Y^2B = Z^2$ has a nontrivial solution $(X^*, Y^*, Z^*) \in \mathbf{Q}[t]^3$.

(For extensions to number fields and several variables see [Sch1], section 24.) To put the statement in the present context one considers the quadratic function field extension $\mathbf{Q}(t, \sqrt{A(t)})/\mathbf{Q}(t)$; the corresponding norm-form is $z^2 - A(t)x^2$ and we want to represent $B(t)$ by this form, with $x, z \in \mathbf{Q}(t)$.

The proof of this *quadratic* theorem used a descent procedure containing some features of Legendre's proof (as presented e.g. in [Se1, p. 74]) of the local-global principle for ternary rational quadratic forms (a particular case of Hasse's theorem). The methods do not seem to extend to a cyclic extension L/K of arbitrary degree.

Now, we recall that the elements in a field which are not norms from a cyclic extension, give rise to nontrivial elements of the *Brauer group* of that field. In fact, let L/K be finite, with cyclic Galois group Γ. Then, by [CF, Thm. 5, p. 108], the cohomology groups $\hat{H}^q(\Gamma, L^*)$ are *periodic* in q, of period 2. In particular, $\hat{H}^0(\Gamma, L^*) \cong \hat{H}^2(\Gamma, L^*)$. Now, on the one hand we have $\hat{H}^0(\Gamma, L^*) = K^*/N_K^L(L^*)$ directly from the definition [CF, Ch. IV]. On the other hand, by [CF, Cor. 1, p. 125], the *inflation* map yields an injection $\hat{H}^2(\Gamma, L^*) \to H^2(\mathrm{Gal}(\bar{K}/K), \bar{K}^*) =: Br(K)$, the Brauer group of K. In conclusion, we get the injection referred to above:

$$K^*/N_K^L(L^*) \to Br(K).$$

This link puts our basic question into the context of *specializations of Brauer groups*, a topic to which a number of papers have been devoted. We mention e.g. [Se3] (considering 2-torsion of the Brauer group) and [FSS]. In the latter paper the concept of *Brauer-Hilbertian field* is introduced and it is proved that global fields are Brauer-Hilbertian. Taking into account the above remarks, this implies in particular (compare with the Theorem below): *if $f(t_0)$ is a norm from the residue field extensions, for almost all $t_0 \in k$, then $f(t)$ is a norm from L.*

(A version by Voronovich [V] involving arithmetic progressions is also quoted in [FSS].) The proofs make use of the Faddeev exact sequence (for a review see [CThSDy]) and of other tools from Galois cohomology.

It is the purpose of the present paper to generalize by a direct method the above-mentioned result in [DLS2], to the case of an arbitrary k-regular (i.e. $L \cap \bar{k} = k$) cyclic extension $L/k(t)$. Our language will avoid any reference to Brauer groups and to the Faddeev sequence; our tools from cohomology will be practically limited to Hilbert 90, recalled below. Therefore the paper will be self-contained in this respect. However we remark that the main ideas are in fact implicitly near to the above quoted concepts.

Our arguments yield a description of the exceptional set of specializations implying a result for arithmetic progressions (as in [DLS1,2]) and quantitative bounds (similarly to [Se3]). In addition, the proofs are constructive and allow one to decide whether a given f is a norm from L and to produce a corresponding representation when it exists. This is carried out in §6. (Though part of our Theorem follows from the quoted results on the Brauer group, effectiveness seems not to have been considered and it is not clear to what extent the quoted proofs on the Brauer group may be made completely effective.)

To simplify the exposition we shall restrict ourselves to the case $k = \mathbf{Q}$. The arguments however work for any number-field k.

To state the results precisely, let L be a cyclic extension of $K = \mathbf{Q}(t)$, of degree d, L regular over $\mathbf{Q}$. Let $\omega_1, \ldots, \omega_d \in L$ be a linear basis for L/K. Even if it does not matter for the results, we shall assume for technical reasons that it is an integral basis for L over $\mathbf{Q}[t]$. We consider, for variables $X_1, \ldots, X_d$, the norm form

$$N(t, X_1, \ldots, X_d) := N_K^L(X_1\omega_1 + \cdots + X_d\omega_d) \in k[t][X_1, \ldots, X_d].$$

Plainly there is a multiplicative identity

$$N(t, X_1, \ldots, X_d)N(t, Y_1, \ldots, Y_d) = N(t, Z_1, \ldots, Z_d)$$

where the Z_i are bilinear functions of the X_i, Y_j with coefficients in $\mathbf{Q}[t]$.

From [Se2, Def. 3.1.1] we recall a definition: *A set of rational numbers is called "thin" if it is contained in a finite union of sets of type $\varphi(X(\mathbf{Q}))$, where $X/\mathbf{Q}$ is a curve and $\varphi\colon X \to \mathbf{P}^1$ is a rational map of degree ≥ 2.*

Also, to simplify the statements it will be convenient to introduce a little more terminology. Let $\mathcal{P}$ be a set of prime numbers, of positive lower Dirichlet

density [1]), and for $p \in \mathcal{P}$ let r_p be an integer. Put

$$A = \bigcup_{p \in \mathcal{P}} \{x \in \mathbf{Q} : \mathrm{ord}_p(x - r_p) = 1\}.$$

Below we shall say that a subset of $\mathbf{Q}$ is *rare* if it is disjoint from a set A obtained in this way.

For a function $f \in \mathbf{Q}(t)$ we define N_f to be the set of rational numbers s such that $f(s)$ is of the form $N(s, x_1, \ldots, x_d)$ for some $x_i \in \mathbf{Q}$. Also, for a set $S \subset \mathbf{Q}$ we define $S(x)$ to be the number of elements of S with height bounded by x.

In the proofs we shall also use an equivalent geometrical language. Namely, L is the function field of a nonsingular absolutely irreducible curve $C/\mathbf{Q}$. The extension L/K corresponds to a morphism $t\colon C \to \mathbf{P}^1$ defined over $\mathbf{Q}$. We may lift the point $s \in \mathbf{P}^1(\mathbf{Q})$ to a point $P_s \in C(\overline{\mathbf{Q}})$ with $t(P_s) = s$. We could replace N_f with the set of $s \in \mathbf{Q}$ such that $f(s)$ is a norm from the residue field extension $\mathbf{Q}(P_s)/\mathbf{Q}$. Such conditions are indeed equivalent if $[\mathbf{Q}(P_s) : \mathbf{Q}] = d = [L : K]$ and actually the proof will use only such values.

THEOREM. *Assume that $f \in \mathbf{Q}(t)^*$ is not in $N_K^L(L^*)$. Then N_f is contained in a union of a thin set and a rare set.*

(We note that it is not true in general that N_f is thin: take e.g. $L = \mathbf{Q}(\sqrt{t})$, $f(t) = -1$. Then N_f consists of the nonzero rational numbers which are sums of two squares, and is not thin [Se2, Ex. 3, p. 20].) In [Se3] the description of the exceptional specializations is somewhat similar, but more precise. As in that paper, the structure of thin sets and a sieve argument imply at once the following corollary.

COROLLARY 1. *Let f be as in the Theorem. Then the complement of N_f in $\mathbf{Q}$ contains an arithmetical progression. Also, we have $N_f(x) \ll x^2/\log^\delta x$ and $(N_f \cap \mathbf{Z})(x) \ll x/\log^\delta x$, where δ is a positive number (which may depend on f).*

(In [Se3], a $\delta \geq 1/2$ is given explicitly.) Combining the Theorem with Hasse's theorem mentioned above we shall obtain another kind of local-global principle, i.e.

---

[1]) i.e. $\liminf_{s \to 1+} \sum_{p \in \mathcal{P}} p^{-s}/\log(\frac{1}{s-1}) > 0$

COROLLARY 2. *Let Σ be a finite subset of places of $\mathbf{Q}$. Assume that*
(a) For all places $v \notin \Sigma$ the function $f \in K$ is a norm from $\mathbf{Q}_v L$ to $\mathbf{Q}_v(t)$.
(b) For all $v \in \Sigma$ there exist $a_v, b_{i,v} \in \mathbf{Q}_v$ with

$$f(a_v) = N(a_v, b_{1,v}, \ldots, b_{d,v}) \in \mathbf{Q}_v^* .$$

Then f is a norm from L.

(In §5 we shall see that (a) is not sufficient in itself.) Colliot-Thélène has shown me a different proof of this corollary using the above-mentioned Faddeev exact sequence, actually removing the regularity assumption. The result reminds one of the work by Pourchet (see [Raj, Lemma 17.4]) and by Colliot-Thélène, Coray, Sansuc [CThCS, Prop. 1.3]. (For instance the last paper contains the proof that a *multiplicative* quadratic form over $k(t)$ represents f over $k(t)$ if and only if it represents f over $k_v(t)$ for all places v of k.)

The paper is organized as follows. In §2 we shall recall a few basics from cohomology. In §3 we shall prove the theorem and its corollaries. In §4 we shall discuss a simple counterexample to an analogous result when $\mathrm{Gal}(L/K)$ is a four-group (similarly to the number-field case). In §5 we shall discuss how the assumptions for Corollary 2 are equivalent for large p both to the solvability of congruences $f \equiv N(g) \pmod{p}$ and to the existence of solutions over the completion of $\mathbf{Q}_p L$ under the Gauss norm. Incidentally, we shall prove that if a representation of f by N exists at all with the $x_i \in k(t)$, then some representation will have the x_i's of degree bounded explicitly only in terms of $\deg f$ and genus and degree of $kL/k(t)$. This seems to have some interest in itself. These observations lead also to the construction of varieties satisfying the usual local-global principle. Finally, in §6 we shall discuss how to find effectively a possible representation of f by N.

2. A COUPLE OF FACTS FROM COHOMOLOGY

Let G be a finite group acting on an abelian group M. For a function $\xi\colon G \to M$, $\sigma \mapsto \xi_\sigma$ we denote (the usual coboundary operator)

$$\partial(\xi_\sigma) = \partial(\xi)\colon G^2 \to M , \qquad (\sigma, \tau) \mapsto \xi_\sigma + \sigma(\xi_\tau) - \xi_{\sigma\tau} .$$

With this notation (but writing M multiplicatively) we now recall Hilbert's Theorem 90:

Let k_1/k be a finite Galois extension with group G and let $\xi: G \to k_1^*$ be a function satisfying $\partial(\xi) = 1$. Then there exists $\alpha \in k_1^*$ such that $\xi_\sigma = \alpha/\sigma(\alpha)$ for all $\sigma \in G$.

The usual proof (see e.g. [CF, Prop. 3, p. 124]) is simple and runs as follows: For $x \in k_1$ form the sum $\alpha = \sum_{\sigma \in G} \xi_\sigma \sigma(x)$. By a well-known elementary result of Artin, we may choose $x \in k_1$ such that $\alpha \neq 0$. A quick computation using the assumption on ξ then shows that α has the stated property.

An easy corollary (the original Hilbert's 90) is that, *if G is cyclic generated by g, then every element $a \in k_1^*$ such that $N_k^{k_1}(a) = 1$ is of the form $b/g(b)$ for some $b \in k_1^*$*. To derive this conclusion it suffices to apply the above statement to the function on G defined by $\xi_{g^m} = \prod_{i=0}^{m-1} g^i(a)$ (which is well defined).

In §6 on effectiveness we shall need a simple result on *permutation modules* for the action of a finite group G. Such a module is simply a free abelian group on which G acts, which moreover has a $\mathbf{Z}$-basis permuted by G. We have:

Let M be a permutation module and let $\xi: G \to M$ satisfy $\partial(\xi) = 0$. Then there exists $m \in M$ such that $\xi_\sigma = m - \sigma(m)$ for all $\sigma \in G$.

We give a short argument for completeness. We may write M as a direct sum of permutation modules, each of which has a $\mathbf{Z}$-basis which is a G-orbit. It suffices to prove the claim for each direct factor. Write the mentioned basis as $\{g(b)\}$ for a certain $b \in M$ and g running through a set of representatives for G/H, H being the stabilizer of b.

We sum the equations $\xi_{\sigma\tau} = \xi_\sigma + \sigma(\xi_\tau)$ over $\tau \in G$. Letting n be the order of G and putting $\mu := \sum_{g \in G} \xi_g \in M$, we get

$$n\xi_\sigma = \mu - \sigma(\mu).$$

Write $\mu = \sum_{g \in G/H} a_g g(b)$ for suitable $a_g \in \mathbf{Z}$. The displayed equation implies $\mu \equiv \sigma(\mu) \pmod{nM}$ for every $\sigma \in G$. This immediately gives the existence of $a \in \mathbf{Z}$ such that $a_g \equiv a \pmod{n}$ for all $g \in G/H$, so we write $a_g = a + nq_g$ where $q_g \in \mathbf{Z}$. Let $m := \sum_{G/H} q_g g(b) \in M$. Then $nm = \mu - a\sum_{G/H} g(b)$, where the last term is invariant by G. Hence $n\xi_\sigma = n(m - \sigma(m))$, whence $\xi_\sigma = m - \sigma(m)$, as required.

3. PROOF OF MAIN RESULTS

To prove the Theorem we start by using the following result of Tsen (see e.g. [Oj, Cor. 3.12, p. 42] or [P, §19.4]): *every homogeneous non-constant form over* $\overline{\mathbf{Q}}(t)$, *of degree* d, *in* $d+1$ *variables* $X_0, \ldots, X_d$ *admits a non-trivial zero in* $\overline{\mathbf{Q}}[t]^{d+1}$. (This is relevant also for the above-mentioned Faddeev sequence.)

Applying this claim to the form $N(t, X_1, \ldots, X_d) - X_0^d f(t)$ we find a nontrivial zero with $X_i = x_i(t) \in \overline{\mathbf{Q}}[t]$. Suppose $x_0(t) = 0$. Then $N(t, x_1(t), \ldots, x_d(t)) = 0$. But this cannot happen unless $x_i(t) = 0$ for all $i > 0$. In fact, $\omega_1, \ldots, \omega_d$ are linearly independent over $\mathbf{Q}(t)$; hence they are linearly independent over $\overline{\mathbf{Q}}(t)$, since $L/\mathbf{Q}$ is regular (we are using [We, Ch. I, Prop. 7]). Therefore $x_0(t)$ is nonzero and dividing everything by x_0^d we see that f is representable by N over $\overline{\mathbf{Q}}(t)$. Let N^* denote the norm from $\overline{\mathbf{Q}}L$ to $\overline{\mathbf{Q}}(t)$. Then there exists $\varphi \in \overline{\mathbf{Q}}L$ such that

$$f = N^*(\varphi). \tag{1}$$

REMARK 1. The proofs of Tsen's result referred to above are quite simple. Moreover they yield the more precise result that, if the relevant form has coefficients in $\overline{\mathbf{Q}}[t]$, of degree $\leq D$, then a solution may be found where the unknowns have degree $\leq \max(0, D - d + 1)$. This bound may be important in effectivity questions (as in §6).

Let $G_{\mathbf{Q}} := \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Then $G_{\mathbf{Q}}$ acts on $\overline{\mathbf{Q}}L/L$. We define, for $\sigma \in G_{\mathbf{Q}}$,

$$\psi_\sigma := \frac{\varphi}{\sigma(\varphi)} \in \overline{\mathbf{Q}}L. \tag{2}$$

It is immediately shown that $f \in N^*(L^*)$ would follow (against the assumption), provided ψ_σ is still of the shape $\varphi'/\sigma(\varphi')$, but with $N^*(\varphi') = 1$ (see the end of the proof). Accordingly, *our aim will be to prove this representation for* ψ_σ, *assuming the conclusion of the Theorem to be false.*

Let k be a number field such that $\varphi \in kL$. Enlarging k we may assume that it is normal over $\mathbf{Q}$ and that all zeros and poles of all the functions $\sigma(\varphi)$ are defined over k. We let $G = \mathrm{Gal}(k/\mathbf{Q})$ and observe that ψ_σ depends only on the image of σ in G. Therefore from now on we let σ run through the finite group G.

Applying σ to (1) we see that $N^*(\psi_\sigma) = 1$. To exploit this fact, let γ be a generator for the Galois group $\Gamma := \mathrm{Gal}(L/K)$. By regularity L and k are

linearly disjoint over $\mathbf{Q}$, so the Galois group of kL over K is isomorphic to $G \times \Gamma$. By Hilbert's theorem 90 for the cyclic extension $kL/k(t)$ (with Galois group isomorphic to Γ) for each ψ_σ there exists $L_\sigma = L_{\psi_\sigma} \in (kL)^*$ such that

$$\psi_\sigma = \frac{L_\sigma}{\gamma(L_\sigma)}\,. \tag{3}$$

Observe that the sets of ψ_σ and L_σ depend only on φ (not on k). Therefore we may assume to have chosen k such that all poles and zeros of the L_σ are defined over k.

Equation (2) yields $\partial\psi_\sigma = 1$. Therefore, by (3) we see that ∂L_σ is invariant by γ, so it lies in $k(t)$. We denote

$$Q_{\sigma,\tau} = \partial L_\sigma = L_\sigma \sigma(L_\tau) L_{\sigma\tau}^{-1} \in k(t)^*\,. \tag{4}$$

To get the alluded representation of ψ_σ, it would be sufficient to prove that L_σ in (4) could actually be chosen in $k(t)^*$. This might not be true, but from $Q_{\sigma,\tau} = \partial L_\sigma$ we find

$$Q_{\sigma,\tau} = Q_{\sigma,\tau\mu}\sigma(Q_{\tau,\mu})(Q_{\sigma\tau,\mu})^{-1}$$

for all $\sigma, \tau, \mu \in G$. Take the product of these equations over $\mu \in G$. Letting n be the order of G and defining $R_\sigma := \prod_{\mu\in G} Q_{\sigma,\mu}$ we obtain

$$Q_{\sigma,\tau}^n = \partial R_\sigma\,, \qquad R_\sigma \in k(t)^*\,. \tag{5}$$

Observe that our choice of k ensures that poles and zeros of all the R_σ lie in $k \cup \infty$. (In cohomological language, $Q_{\sigma,\tau}$ is a 2-cocycle in $k(t)^*$ for the action of G, and is a coboundary in $(kL)^*$, by definition (4). We wish to show that it is a coboundary in $k(t)^*$, which might not be true without further information. Formula (5) shows however that Q^n is indeed of that shape. Our direct calculation reflects the classical fact [CF, Ch. IV] that the order n of the group kills the cohomology groups.)

We now refer to some theory of thin sets, as presented in [Se2]. We may view L as defined over k. Let, as in the introduction, P_s be a point of C above $s \in \mathbf{P}^1$. The set of $s \in k$ such that $\mathrm{Gal}(k(P_s)/k) \neq \Gamma$ is a thin set in k [Se2, Prop. 3.3.1]. By [Se2, Prop. 3.2.1], the intersection of this set with $\mathbf{Q}$ is also thin. Define S to be its complement in $\mathbf{Q}$.

Note that the property $\mathrm{Gal}(k(P_s)/k) = \Gamma$ implies that the fields k and $\mathbf{Q}(P_s)$ are linearly disjoint over $\mathbf{Q}$. Therefore $\mathrm{Gal}(k(P_s)/\mathbf{Q}) = G \times \Gamma$. Frequently in the sequel we shall identify G (resp. Γ) with $G \times \{1\}$ (resp. $\{1\} \times \Gamma$). Finally observe that such properties imply that the action of Γ on $k(C) = kL$ commutes with specialization of rational functions in $k(C)$ at P_s.

In view of these facts it will cause no confusion if we continue to use the notation N^* both for $N_k^{k(P_s)}$ and for $N_{\mathbf{Q}}^{\mathbf{Q}(P_s)}$.

Let $S' = S \cap N_f$. For $s \in S'$ there exists $\alpha(s) \in \mathbf{Q}(P_s)$ such that

$$N^*(\alpha(s)) = f(s).$$

Specializing (1) at P_s we also obtain $N^*(\varphi(P_s)) = f(s)$, whence

$$\varphi(P_s) = \alpha(s)\xi(s), \quad \text{where } \alpha(s) \in \mathbf{Q}(P_s),\ \xi(s) \in k(P_s) \text{ and } N^*(\xi(s)) = 1.$$

By Hilbert's Theorem 90 for the cyclic extension $k(P_s)/k$ we may write

$$\xi(s) = \frac{\rho(s)}{\gamma(\rho(s))}, \qquad \text{where } \rho(s) \in k(P_s). \tag{6}$$

Also, since k and $\mathbf{Q}(P_s)$ are linearly disjoint over $\mathbf{Q}$ we have $\sigma(\alpha(s)) = \alpha(s)$ for all $\sigma \in G$. Therefore specializing (2) at P_s we get

$$\psi_\sigma(P_s) = \frac{\xi(s)}{\sigma(\xi(s))}.$$

(Note that, since $N^*(\xi(s)) = 1$, this equation is the *specialization* of the sought representation for ψ_σ.) Recalling (3) and (6) we get

$$\frac{L_\sigma(P_s)}{\gamma(L_\sigma(P_s))} = \frac{\rho(s)/\sigma(\rho(s))}{\gamma(\rho(s)/\sigma(\rho(s)))},$$

namely

$$L_\sigma(P_s) = \frac{\rho(s)}{\sigma(\rho(s))}\mu_\sigma(s), \quad \text{where } \gamma(\mu_\sigma(s)) = \mu_\sigma(s), \text{ i.e. } \mu_\sigma(s) \in k. \tag{7}$$

(We tacitly disregard all the finitely many $s \in S'$ with the property that some of the finitely many involved functions either vanishes or is not defined at P_s.)

By (4), (5) and (7) we get

$$\partial R_\sigma(P_s) = \partial \mu_\sigma(s)^n.$$

On the other hand $R_\sigma \in k(t)$, so $R_\sigma(P_s) = R_\sigma(s) \in k$. By Hilbert's Theorem 90 for the extension $k/\mathbf{Q}$ we get the existence of $\beta(s) \in k$ such that

$$R_\sigma(s) = \frac{\beta(s)}{\sigma(\beta(s))}\mu_\sigma(s)^n. \tag{8}$$

Our next purpose is to show that, if the sought conclusion is not true, then these numerical equations actually come from an identity (see the lemma below). This will be done by comparison of *functional* and *numerical*

factorizations. To carry out this program, we start by constructing some relevant rare sets. First of all, fix a number p_0 sufficiently large to justify the subsequent arguments. This number is to depend only on the R_σ's, hence only on f.

Consider the set of algebraic numbers r which are zeros or poles of some R_σ. We have assumed that such a set is contained in k, and the same is true of its G-orbit, which we denote by Ω. Naturally Ω is a finite disjoint union of G-orbits of single elements.

For $r \in \Omega$ and for $\sigma \in G$, define $m_\sigma(r)$ as the multiplicity of r in R_σ. Consider a G-orbit $O \subset \Omega$ and select once and for all $r = r_O \in O$, so $O = \{\sigma(r) : \sigma \in G\}$.

Let $h \in G$ satisfy $h(r) = r$. Let $\mathcal{P}(h)$ be the set of prime numbers $p > p_0$ unramified in k and such that the decomposition group of some prime ideal π of k above p is generated by h. By Chebotarev's theorem such a set is infinite and actually the quantitative formulation [Nar, Thm. 7.11 (resp. 7.11*)] asserts that $\mathcal{P}(h)$ has a positive Dirichlet (resp. natural) density.

Let $p \in \mathcal{P}(h)$ and let $v = v_p$ be the order function on k with respect to π. Observe that π lies above a prime of the fixed field of h which has degree 1 over p. Since h fixes r, such a fixed field contains $\mathbf{Q}(r)$. In particular there exists an integer $r_1 \in \mathbf{Z}$ such that $v(r - r_1) \geq 2$. Observe that for a rational number x, we have that $v(x - r_1) = 1$ is equivalent to $v(x - r) = 1$.

We put $A(O, h) = \bigcup_{p \in \mathcal{P}(h)} \{x \in \mathbf{Q} : \operatorname{ord}_p(x - r_1) = 1\}$ and we define $\mathcal{R}(O, h) = \mathbf{Q} \setminus A(O, h)$ to be the corresponding rare set. The kernel of the proof is the following lemma (compare with (8) above).

LEMMA. *Suppose that for each O, h there exists $s \in S'$ which does not lie in the set $\mathcal{R}(O, h)$ just defined. Then there exist rational functions $B, U_\sigma \in k(t)$ such that*

$$R_\sigma = \frac{B}{\sigma(B)} U_\sigma^n \qquad \text{for all } \sigma \in G.$$

Proof of Lemma. With the above notation, define a function $\nu : O \to \mathbf{Z}/(n)$ by

$$\nu(\sigma(r)) :\equiv -m_{\sigma^{-1}}(r) \pmod{n}. \tag{9}$$

We contend that this definition is a good one. To verify this, suppose that $\sigma_1(r) = \sigma_2(r)$. This is equivalent to $\sigma_2 = \sigma_1 h$ where $h(r) = r$. By assumption we may pick $s \in S'$ outside $\mathcal{R}(O, h)$, whence there exists $p \in \mathcal{P}(h)$ such that $v(s - r) = v_p(s - r) = 1$.

By (8) we have $v(R_{\sigma_i^{-1}}(s)) \equiv v(\beta(s)) - v(\sigma_i^{-1}(\beta(s)))$ (mod n) for $i = 1, 2$. Therefore

$$v(R_{\sigma_1^{-1}}(s)) - v(R_{\sigma_2^{-1}}(s)) \equiv -v(\sigma_1^{-1}(\beta(s))) + v(h^{-1}\sigma_1^{-1}(\beta(s))) \pmod{n}.$$

On the other hand, $v = v \circ h^{-1}$, since h^{-1} lies in the decomposition group of π and so

$$v(R_{\sigma_1^{-1}}(s)) \equiv v(R_{\sigma_2^{-1}}(s)) \pmod{n}. \tag{10}$$

Now observe that we can write $R_\sigma(t)$ as the product of a nonzero constant $c_\sigma \in k$ times a product $\prod_{u\in\Omega}(t-u)^{m_\sigma(u)}$, so if we suppose that $p > p_0$ is so large that all c_σ are coprime to p, we have

$$v(R_\sigma(s)) = \sum_{u\in\Omega} m_\sigma(u)v(s-u).$$

Since $v(s-r) = 1$ we see that if p_0 has been chosen large enough, we have $v(s-u) = 0$ for all $u \in \Omega \setminus \{r\}$. In fact, if $p > p_0$ is large we may assume $v(s-u) \geq 0$ for all $u \in \Omega$ and if we had $v(s-u) > 0$ then $v(u-r) > 0$. But if $u \neq r$, $u - r$ has finitely many prime ideal factors. If p is coprime with all of them, the assertion follows.

In conclusion we deduce $v(R_\sigma(s)) = m_\sigma(r)v(s-r) = m_\sigma(r)$ and comparing with (10) we get

$$m_{\sigma_1^{-1}}(r) \equiv m_{\sigma_2^{-1}}(r) \pmod{n},$$

which is precisely what we want, in view of (9).

By equation (5) we have that $\partial R_\sigma = R_\sigma \sigma(R_\tau)R_{\sigma\tau}^{-1} = Q_{\sigma,\tau}^n$ is an n-th power in $k(t)$. Recalling that $m_\sigma(u)$ is the multiplicity of u in R_σ, we see that $m_\tau(\sigma^{-1}u)$ is the multiplicity of u in $\sigma(R_\tau)$. Computing the multiplicity of u in ∂R_σ we then get

$$m_{\sigma\tau}(u) \equiv m_\sigma(u) + m_\tau(\sigma^{-1}u) \pmod{n}.$$

In this congruence replace σ by τ^{-1} and τ by σ. We get, for all $u \in \Omega$,

$$m_{\tau^{-1}\sigma}(u) \equiv m_{\tau^{-1}}(u) + m_\sigma(\tau(u)) \pmod{n}.$$

Putting $u = r$ and using our (good) definition (9) we may rewrite this as

$$\nu(\tau(r)) - \nu(\sigma^{-1}\tau(r)) \equiv m_\sigma(\tau(r)) \pmod{n}. \tag{11}$$

Finally, take any integer representatives (denoted in the same way) for the classes $\nu(\tau(r))$ modulo n, $\tau \in G$, and do this for all G-orbits $O \subset \Omega$. Define

$$B_1(t) = \prod_O \prod_{\tau(r_O)\in O} (t - \tau(r_O))^{\nu(\tau(r_O))} .$$

Congruence (11) shows that $R_\sigma(B_1/\sigma(B_1))^{-1}$ has all its zeros and poles in k, with multiplicity divisible by n, so is of the form $c_\sigma Z_\sigma^n$, where $c_\sigma \in k$ and $Z_\sigma \in k(t)$. Evaluating at some $s' \in S'$ we see from (8) that $c_\sigma = \mu_\sigma^n(\beta/\sigma(\beta))$ for some $\beta, \mu_\sigma \in k$. Now it suffices to define $B := \beta B$, $U_\sigma := \mu_\sigma Z_\sigma$ to obtain the statement of the lemma. □

Under the assumptions of the lemma we get $\partial R_\sigma = \partial U_\sigma^n$ and on the other hand $\partial R_\sigma = Q_{\sigma,\tau}^n = \partial L_\sigma^n$ by (4) and (5). Therefore $\partial(U_\sigma/L_\sigma)^n = 1$. Therefore there exist n-th roots of unity $\zeta_{\sigma,\tau} \in k$ such that

$$\partial(L_\sigma/U_\sigma) = \zeta_{\sigma,\tau} . \tag{12}$$

Specialize this equation at P_s for some fixed $s \in S'$ and use equation (7) to obtain

$$\partial(\mu_\sigma(s)/U_\sigma(s)) = \zeta_{\sigma,\tau} .$$

Observe that $\lambda_\sigma := \mu_\sigma(s)/U_\sigma(s) \in k$. Also, we have

$$\partial(\frac{L_\sigma}{\lambda_\sigma U_\sigma}) = 1 .$$

By Hilbert's Theorem 90 for the extension kL/L we derive the existence of $\phi \in kL$ such that

$$L_\sigma = \lambda_\sigma U_\sigma \frac{\phi}{\sigma(\phi)} .$$

Recall that $\lambda_\sigma U_\sigma \in k(t)$ is invariant by Γ. Therefore by (3) we have

$$\psi_\sigma = \frac{\phi/\gamma(\phi)}{\sigma(\phi/\gamma(\phi))} .$$

Comparing with (2) we see that $\eta := \frac{\varphi}{\phi/\gamma(\phi)}$ is invariant by G, hence lies in L. But $N^*(\eta) = N^*(\varphi) = f$, against the assumptions of the Theorem. Therefore for some O, h as above, the element s in the assumptions of the Lemma cannot exist, proving that $S' \subset \mathcal{R}(O, h)$, as desired. □

Proof of Corollary 1. By [Se2, Thm. 3.5.3] the complement of a thin set in $\mathbf{Q}$ contains an arithmetical progression (see also [Sch2]). Therefore the first assertion follows.

As to the second one, it suffices to prove the stated estimates for N_f replaced both by a thin set and by a rare set. For the first case, see [Se2, Ch. 3] for much sharper estimates. In the case of a rare set, the estimates follow in a rather standard way from sieve inequalities. We outline some

arguments using the large sieve, similarly to [Se3]. We recall from [Se3] the following statement (see the *Théorème* on p. 401), entirely analogous to a corollary of the Davenport-Halberstam Theorem, as discussed e.g. in [Se2, Ch. X].

Let Ω be a subset of $\mathbf{Z}^n$ such that for all primes p its reduction Ω_p modulo p^2 contains at most $\nu_p p^{2n}$ elements. Then, putting $\Omega(x) := \Omega \cap [0,x]^n$, we have

$$\#\Omega(x) \leq (2x)^n / L(\sqrt[4]{x}),$$

where $L(z) = \sum^*_{d \leq z} \prod_{p|d} (\frac{1-\nu_p}{\nu_p})$ and the star means that summation is restricted to square-free positive integers.

We use this result with $n = 1$ to estimate the number of positive integers $\leq x$ in a rare set Ω. (The case of rationals of bounded height in a rare set becomes entirely similar by taking $n = 2$ and associating to a fraction a/b in lowest terms, the point $(a,b) \in \mathbf{Z}^2$.)

Let $\mathcal{P}$ be a set of primes associated to the rare set Ω. By definition the reduction Ω_p modulo p^2 contains at most $p^2 - p + 1$ elements for $p \in \mathcal{P}$. Therefore we may take $\nu_p = 1 - \frac{1}{2p}$ for $p \in \mathcal{P}$ and $\nu_p = 1$ otherwise. We find

$$L(z) \geq \sum_{d \leq z}^{**} \frac{1}{\tau(d)d},$$

where the summation now runs through square-free integers whose prime factors are all in $\mathcal{P}$ and where $\tau(d)$ is the number of divisors of d. For $s > 1$ we have the identity

$$\prod_{p \in \mathcal{P}} (1 + \frac{1}{2p^s}) = \sum^{**} \frac{1}{\tau(d)d^s}.$$

Put $s = 1 + \frac{\log\log z}{\log z} = 1 + \rho$, say. Then

$$\sum_{d>z}^{**} \frac{1}{\tau(d)d^s} \leq \sum_{d>z} d^{-s} \ll \int_z^\infty t^{-s} \mathrm{d}t = \frac{1}{\rho z^\rho} \ll 1.$$

Also, $L(z) \geq \sum^{**} \frac{1}{\tau(d)d^s} - \sum^{**}_{d>z} \frac{1}{\tau(d)d^s} \geq \sum^{**} \frac{1}{\tau(d)d^s} + O(1)$. On the other hand,

$$\log(\sum^{**} \frac{1}{\tau(d)d^s}) = \sum_{p \in \mathcal{P}} \log(1 + \frac{1}{2p^s}) \gg \sum_{p \in \mathcal{P}} p^{-s}.$$

Since $\mathcal{P}$ has positive lower Dirichlet density, for large z the left side is $\geq \gamma \log \frac{1}{s-1}$ where γ is a fixed positive real number. These inequalities imply

$L(z) \geq (\frac{\log z}{\log\log z})^{\gamma} + O(1)$ and an estimate $\Omega(x) \ll \frac{x}{\log^{\delta} x}$ follows, where δ is any positive number $< \gamma$.

Proof of Corollary 2. It suffices to show that the assumptions for Corollary 2 imply that N_f does not satisfy the conclusion of the Theorem.

Assume first that $v \notin \Sigma$. Let $\varphi \in \mathbf{Q}_v(C)$ be such that $N^*(\varphi) = f$. We wish to specialize suitably this equation, but first we may have to modify φ. The divisor $\mathrm{div}(\varphi)$ is rational over $\mathbf{Q}_v$. Let F be a prime divisor of $\mathbf{Q}_v(t)$ which does not appear in f. We may write

$$F = e(G_1 + \cdots + G_r)$$

where the G_i are prime divisors of L, rational over $\mathbf{Q}_v$ and $e = e_F$ is the ramification index. Since F is Γ-invariant, in fact the G_i's constitute just the Γ-orbit of G_1, so we may write $G_i = \gamma^{i-1}(G_1)$. By taking norms we have $dF = er\sum_{\sigma\in\Gamma}\sigma(G_1)$. Let $\sum m_i G_i$ be the part of $\mathrm{div}(\varphi)$ made up with the G_i's. Since $N^*(\varphi) = f$ we have $\sum_i m_i = 0$. Hence we may write $\sum m_i G_i$ as a sum of terms $G_i - G_j$, $i < j$. In turn, $G_i - G_j = \sum_{s=i}^{j-1}(G_s - G_{s+1})$ is of the form $G - \gamma(G)$ for some $\mathbf{Q}_v$-rational divisor G. These arguments prove that we may write the divisor of φ in the form $D_1 + (D - \gamma(D))$, where D_1, D are $\mathbf{Q}_v$-rational and D_1 is made up of zeros or poles of f.

Let now $s \in \mathbf{Q}$ and let P_s be a point of C with $t(P_s) = s$. We assume that $f(s)$ is defined and nonzero. In particular D_1 does not contain any $\tau(P_s)$ for $\tau \in \Gamma$. We also assume that $\mathbf{Q}(P_s)$ has degree d over $\mathbf{Q}$. This holds outside a thin set T_f of $\mathbf{Q}$. We embed $\mathbf{Q}(P_s)$ into a finite extension of $\mathbf{Q}_v$.

Now, there exists a divisor Δ, rational over $\mathbf{Q}_v$, such that $D - \Delta$ does not contain any point $\tau(P_s)$. Let $g \in \mathbf{Q}_v(C)$ be a rational function such that no τP_s appears in $\Delta + \mathrm{div}(g)$. Then, the divisor of $\psi := \varphi g/\gamma(g)$ does not contain any $\tau(P_s)$. Observe that $N^*(\psi) = N^*(\varphi) = f$. On the other hand we may evaluate at P_s each factor appearing in the norm and we find that $f(s)$ is a norm from $\mathbf{Q}_v(P_s)$.[2])

Assume now that $v \in \Sigma$. For $r \in \mathbf{Q}_v$, we have that $N(r, x_1, \ldots, x_d)$ has an image on $\mathbf{Q}_v^d$ which contains some neighborhood of 1 in $\mathbf{Q}_v$, the neighborhood depending only on v. In fact such an image contains the set of d-th powers in $\mathbf{Q}_v$. Now, let a_v be as in (b) and suppose that $r \in \mathbf{Q}_v$ is very near to a_v in the v-adic topology. We have that $f(a_v)$ equals some nonzero value $N(a_v, b_1, \ldots, b_d)$ with $b_i \in \mathbf{Q}_v$. Then $N(r, b_1, \ldots, b_d)$ is very near to $f(r)$, so we may write

---

[2]) This is true even if $[\mathbf{Q}_v(P_s) : \mathbf{Q}_v] < d$. In any case $N^*(\psi(P_s))$ is a product of $\frac{d}{[\mathbf{Q}_v(P_s):\mathbf{Q}_v]}$ factors, each a norm from $\mathbf{Q}_v(P_s)$.

$$N(r, b_1, \ldots, b_d) = f(r)\mu$$

where $\mu \in \mathbf{Q}_v$ is very close to 1; in fact $f(r)$ is near to $f(a_v)$, which is nonzero. By the previous remarks, μ^{-1} is in the image of $N(r, x_1, \ldots, x_d)$ on $\mathbf{Q}_v^d$, hence the same must be true for $f(r)$, by the basic multiplicative identity for N. In particular $f(r)$ will be a norm from $\mathbf{Q}_v(P_r)$ to $\mathbf{Q}_v$.

Let now S consist of the elements of $\mathbf{Q}$ which are not poles or zeros of f, which satisfy $[\mathbf{Q}(P_s) : \mathbf{Q}] = d$ and which are sufficiently close (in the mentioned sense) to a_v, for each $v \in \Sigma$. We have proved that $f(s)$ is a norm from $\mathbf{Q}_v(P_s)$, for all $s \in S$ and for all places v. By Hasse's theorem, $f(s)$ is a norm from $\mathbf{Q}(P_s)$, so $S \subset N_f$. On the other hand $S \cap \mathbf{Z}$ contains the complement of a thin set in an arithmetic progression, whence N_f cannot satisfy the conclusion of the Theorem (or of Corollary 1), as required. □

4. An example for the non-cyclic case

We show that assuming that L/K is cyclic is essential in the Theorem (as in the number-field case, as shown in [CF, Ex. 5]).

To describe a counterexample, define $L = \mathbf{Q}(t, \sqrt{4t+3}, \sqrt{4t+7})$, $f(t) = t^2$. We proceed to show that $\mathbf{N} \subset N_f$. We have to show that for all large integers n, n^2 is a norm from $L(n) := \mathbf{Q}(\sqrt{4n+3}, \sqrt{4n+7})$. By [CF, Ex. 5.1 and 5.2, p. 360] it is sufficient to show that the local degree $[L(n)_w : \mathbf{Q}_p]$ is 4 for some prime p. Observe that the Jacobi symbol $\left(\frac{4n+3}{4n+7}\right) = \left(\frac{-1}{4n+7}\right) = -1$. Hence there exists some prime p dividing $4n+7$ with an odd multiplicity and such that $\left(\frac{4n+3}{p}\right) = -1$. Then p ramifies in $L(n)$ and the residual degree is 2, proving the claim. Observe that the first conclusion of Corollary 1 does not hold for N_f.

On the other hand, t^2 is not a norm from L to K. Otherwise by [CF, Ex. 5.1] we could write t as the product of three norms from the three quadratic subfields of L. In other words we could write nontrivially

$$q^2(t)t = (a_1^2(t) - (4t+3)b_1^2(t))(a_2^2(t) - (4t+7)b_2^2(t))(a_3^2(t) - (4t+3)(4t+7)b_3^2(t)),$$

where $q, a_i, b_j \in \mathbf{Q}[t]$. We may suppose that a_i and b_i are coprime for each i, otherwise we can divide out a common factor. Now, putting $t = 0$ we get a contradiction.

5. Remarks on Corollary 2

Corollary 2 does not remain true if we delete (b). In fact, take e.g. $L = \mathbf{Q}(t, \sqrt{2(t^2-5)})$, $f(t) = 5$ and let $p > 5$. Then 2 is a norm from $\mathbf{Q}_p(\sqrt{5})$ to $\mathbf{Q}_p$, so $2(t^2-5)$ is a norm from $\mathbf{Q}_p(t, \sqrt{5})$ to $\mathbf{Q}_p(t)$, namely we can write

$$a_p(t)^2 - 5b_p(t)^2 = 2(t^2-5)$$

for suitable $a_p, b_p \in \mathbf{Q}_p(t)$. Necessarily b_p is nonzero, so 5 is a norm from $\mathbf{Q}_p L$ to $\mathbf{Q}_p(t)$ for all $p > 5$. On the other hand simple congruence considerations show that this is not true for $p = 5$.

An assumption which may perhaps seem more natural than (a), is that (for $v = p$) f *is a norm from* $\widehat{\mathbf{Q}_p L}$ *to* $\widehat{\mathbf{Q}_p(t)}$, where the *hat* denotes completion with respect to an extension of the Gauss norm on $\mathbf{Q}_p(t)$. This last assumption is directly related to the solvability of a congruence $N(t, x_1, \ldots, x_d) \equiv f \pmod{p}$ with $x_i \in \mathbf{F}_p(t)$. When such a congruence is solvable, Hensel's principle may lead to a solution with $x_i \in \widehat{\mathbf{Q}_p(t)}$, but not perhaps with $x_i \in \mathbf{Q}_p(t)$.

However *a posteriori* the solvability of the above congruence is equivalent with any of the mentioned assumptions, for almost all p. We sketch a proofs of this claim.

Take first p to be a prime not dividing d and such that the cover L/K has good reduction at p. By this we mean that the Gauss norm on $\mathbf{Q}_p(t)$ admits only one extension to $\mathbf{Q}_p L$. Denote by $L(p)$ the residue field of L with respect to this extended valuation. Then $L(p)$ is cyclic of degree d over $\mathbf{F}_p(t)$. Also, it goes back to Deuring that the genus of $L(p)$ does not exceed the genus of L. We remark that it is well known that these properties are satisfied by all but finitely many p. For large p we may also suppose that the reductions of the ω_i's are linearly independent over $\mathbf{F}_p(t)$. In that case to say that f is a norm from $L(p)$ is equivalent to solving (13) with $x_i \in \mathbf{F}_p[t]$.

We now define certain relevant projective varieties. Consider the equation

$$N(t, x_1, \ldots, x_d) = x_0^d f\,, \tag{13}$$

where the x_i's are polynomials of degree $\leq B$. This is equivalent to a certain system of homogeneous equations over $\mathbf{Q}$ (each of degree d) in the coefficients of the x_i's. Such a system defines a variety in $\mathbf{P}^{(d+1)(B+1)-1}$ which we denote by V_B. To find a point of V_B over a field k means to find a nontrivial solution of (13) with $x_i \in k[t]$ of degree $\leq B$. In particular we may then represent f as a norm from kL.

We pause to note a fact not without interest in itself. Let $\mathbf{k}$ be any field and let $\mathbf{L}$ be a cyclic, $\mathbf{k}$-regular separable extension of $\mathbf{k}(t)$ with Galois group Γ of order d. Let g be the genus of $\mathbf{L}$. By $\deg_{\mathbf{L}}$ we shall mean the degree (of a function or divisor) referred to $\mathbf{L}$, while deg will be referred to $\mathbf{k}(t)$. We have

PROPOSITION. *If f is a norm from $\mathbf{L}$ to $\mathbf{k}(t)$, then it is the norm of a function $\psi \in \mathbf{L}$ with $\deg_{\mathbf{L}} \psi \leq \deg f + g + d - 1$.*

To prove this assertion, let $N = N_{\mathbf{k}(t)}^{\mathbf{L}}$ be the mentioned norm and write $f = N(\phi)$. Let F be a prime divisor of $\mathbf{k}(t)$ appearing in f with multiplicity $m = m_F$. We may write, as in the proof of Corollary 2,

$$F = e(G_1 + \cdots + G_r),$$

where the G_i are prime divisors of $\mathbf{L}$, rational over $\mathbf{k}$, $e = e_F$ is the ramification index and $G_i = \gamma^{i-1}(G_1)$. We have $\deg_{\mathbf{L}} F = d \deg F = e r \deg_{\mathbf{L}} G_1$. By taking norms we have $dF = er \sum_{\sigma \in \Gamma} \sigma(G_1)$. Let $\sum m_i G_i$ be the part of $\operatorname{div}(\phi)$ made up with the G_i's. Since $N(\phi) = f$ we have $d(\sum_i m_i) = erm$. Hence $|\sum m_i| \leq |erm/d|$ and we may write $\sum m_i G_i = m' G_1 + \sum m_i' G_i$, where $|m'| \leq |erm/d|$ and $\sum m_i' = 0$. Also, $\sum m_i' G_i$ can be written as a sum of terms $G_i - G_j$, $i < j$. In turn, $G_i - G_j = \sum_{s=i}^{j-1} (G_s - G_{s+1})$ is of the form $G - \gamma(G)$ for some rational divisor G. These arguments prove that we may write the divisor of ϕ in the form $D_+ - D_- + (D - \gamma(D))$, where $D_+ . D_- . D$ are $\mathbf{k}$-rational, $D_+ . D_-$ are positive and

$$\deg_{\mathbf{L}} D_{\pm} \leq \sum_{\pm m_F \geq 0} (\pm m_F) \frac{e\, r}{d} \deg_{\mathbf{L}} G_1 \leq \sum_{\pm m_F \geq 0} m_F \deg F = \deg f .$$

Take now the divisor Z of zeros of the function t, say. This is positive of $\mathbf{L}$-degree d, rational over $\mathbf{k}$ and invariant by Γ. Let h be the least integer such that $\deg D + hd \geq g$. Then $g \leq \deg(D + hZ) \leq g + d - 1$. By Riemann-Roch there exists a function $\xi \in \mathbf{L}$ such that its divisor is of the form $E - D - hZ$, where E is positive. Since D, Z and ξ are rational over $\mathbf{k}$, E is also rational over $\mathbf{k}$. Also, $\deg_{\mathbf{L}} E = \deg_{\mathbf{L}} D + hd \leq g + d - 1$. Put $\psi = \phi \frac{\xi}{\gamma(\xi)}$. Then

$$\begin{aligned} \operatorname{div}(\psi) &= D_+ - D_- + D - \gamma(D) + E - D - hZ - \gamma(E) + \gamma(D) + hZ \\ &= D_+ - D_- + E - \gamma(E) . \end{aligned}$$

Therefore the divisor of zeros of ψ has degree (in $\mathbf{L}$) bounded by $\deg_{\mathbf{L}}(E + D_+) \leq \deg f + g + d - 1$. Also $N(\psi) = N(\phi) = f$. This proves the claim.

COROLLARY. *If f is a norm from kL to $k(t)$, then V_B has a k-point for some B bounded only in terms of* $\deg f$ *and L (but not on k).*

Here k is any field of characteristic zero and $kL := k(t) \otimes_{Q(t)} L$. To prove the assertion, let ψ be as in the Proposition (with $\mathbf{L} = kL$, $\mathbf{k} = k$) and write $\psi = \sum_{i=1}^{d} y_i \omega_i$ with $y_i \in k(t)$. Conjugating the equation over $k(t)$ we obtain a $d \times d$ invertible linear system in the y_i's, namely $\sigma(\psi) = \sum_{i=1}^{d} y_i \sigma(\omega_i)$ for $\sigma \in \Gamma$. We may solve this system for the y_i and express them as linear combinations of the $\sigma(\psi)$ with coefficients depending only on the basis $\{\omega_i\}$. On the other hand the (kL)-degree of $\sigma(\psi)$ is bounded as in the Proposition. Since the degree is subadditive and $\deg y_i = (\deg_{kL} y_i)/d$, we see that $\deg y_i$ is bounded depending only on $\deg f$ and L. Therefore we may write $y_i = x_i/x_0$, where the x_i's are polynomials in $k[t]$ whose degree is likewise bounded, say by $B = B(\deg f, L)$, and the claim follows.

Applying then the Proposition with $\mathbf{L} = L(p)$, $\mathbf{k} = \mathbf{F}_p$ and arguing as in the above Corollary we may assume that the degrees of the x_i's are bounded in terms of $\deg f$ and L only. In turn, this is like finding an $\mathbf{F}_p$-point on the reduction of V_B, provided $B = B(\deg f, L)$ is large enough.

Now we observe the following fact: *Given a projective variety $V/\mathbf{Q}$, for almost all p the existence of a point over $\mathbf{F}_p$ in the reduction of V mod p is equivalent to the existence of a point in $V(\mathbf{Q}_p)$.*
(We tacitly assume to choose a set of defining equations for V and to define the reduction of V by reducing modulo p the equations, for large p.) This claim is most probably well known, but we have no reference. We just sketch a proof of the nontrivial part by induction on $\dim V$. If V is a finite set of points and some such point P reduces in $\mathbf{F}_p$ modulo some prime ideal above p, then $\mathbf{Q}(P)$ may be embedded in $\mathbf{Q}_p$ for large p. Suppose $m = \dim V \geq 1$. We may assume that V is $\mathbf{Q}$-irreducible and express it as a union of absolutely irreducible varieties W_σ defined over a number field k and conjugate over $\mathbf{Q}$. Suppose V has a point over $\mathbf{F}_p$, where p is large. Then there exist some W_σ and a prime π of k, lying above p, such that the reduction of W_σ modulo π has a point over $\mathbf{F}_p$. If such a reduction is defined over $\mathbf{F}_p$ then it contains points over $\mathbf{F}_p$ in any prescribed Zariski open subset; in fact the reduction is absolutely irreducible for large p and we may apply the Lang-Weil theorem [Se2, Thm. 3.6.1, p. 30]. In this case Hensel's principle gives a point of W_σ over $\mathbf{Q}_p$. If the reduction is not defined over $\mathbf{F}_p$, then the mentioned point lies in the intersection with some other conjugate over $\mathbf{F}_p$, i.e. in the reduction of

some intersection $W_\sigma \cap W_\tau$ of distinct conjugates. This has smaller dimension and induction applies.

In conclusion, for large p and B as above we have that the following are equivalent: *(i) f is norm from $\mathbf{Q}_p L$; (ii) V_B has a $\mathbf{Q}_p$-point; (iii) V_B has an $\mathbf{F}_p$-point; (iv) f is a norm from $L(p)$.*

We finally observe that the varieties V_B so defined satisfy the usual local-global principle, in view of the above Corollary 2 (with $\Sigma = \varnothing$) and in view of the Corollary to the Proposition (applied with $\mathbf{k} = \mathbf{Q}$ and $\mathbf{k} = \mathbf{Q}_v$).

REMARK 2. A proof of the equivalence of *(i)* and *(iv)* may also be given by arguments partially analogous to the proof of the Theorem, without invoking the Proposition or the varieties V_B. We start by finding a solution over a finite normal extension k of $\mathbf{Q}$. We embed k in a finite extension k_v of $\mathbf{Q}_p$ and we consider the functions ψ_σ, L_σ, $Q_{\sigma,\tau}$ for $\sigma, \tau \in G' := \mathrm{Gal}(k_v/\mathbf{Q}_p)$; for large p we may reduce everything modulo v, denoting it with a tilde, finding a similar situation over the residue field $\mathbf{F}_v$ of k_v. Also, we may assume that $\mathrm{Gal}(\mathbf{F}_v/\mathbf{F}_p) \cong G'$. By assumption, there exists $\xi \in L(p)$ with norm $\tilde{f}$. Then $\tilde{\varphi}$ and ξ have the same norm, whence $\tilde{\varphi} = \xi(A/\gamma A)$ for some $A \in \mathbf{F}_v L(p)$. This easily leads to $\widetilde{L}_\sigma = (A/\sigma A)\widetilde{B}_\sigma(t)$, where $\widetilde{B}_\sigma \in \mathbf{F}_v(t)$. In turn we find that $\widetilde{Q}_{\sigma,\tau} = \partial(\widetilde{B}_\sigma)$. If p is so large that no two zeros or poles of $Q_{\sigma,\tau}$ may collapse after reduction, then is is easily seen that we may find rational functions $B_\sigma \in k_v(t)$ such that $Q_{\sigma,\tau}/\partial(B_\sigma) \in k_v$, reducing to the case when the $Q_{\sigma,\tau}$ are constant. Actually, by using equations (5), we reduce to the case when they are roots of unity in k_v, in which case the proof is easily completed.

6. EFFECTIVENESS

The problem is the following. How can we decide whether a given f admits a nontrivial representation in the form (13), with $x_i \in \mathbf{Q}[t]$? An answer can be given with the methods at the end of the last section. In fact, we have proved that if some representation exists, then a certain projective variety V (whose equations can be found) has a $\mathbf{Q}$-point and conversely. We have observed that V satisfies the local-global principle. Known methods allow one to decide whether V has points over all $\mathbf{Q}_v$ and this gives an answer to the original question.

Another, more direct, procedure is furnished by the method of proof of the Theorem. This has the advantage of yielding a representation when it exists. We start by finding a solution over $\overline{\mathbf{Q}}$. This can be done by e.g. Remark 1. We may then construct the number field k and the functions ψ_σ, as in (2) above. Now we can construct, as in the proof, the rational functions R_σ. Reversing the arguments in the proof of the Theorem, we see that the main problem may be solved if and only if

(i) the conclusion of the Lemma holds for the R_σ and

(ii) if (i) is in fact true, the function $\zeta_{\sigma,\tau}$ given by (12) is of the form $\partial\xi_\sigma$ for some $\xi: G \to k^*$.

Question (i), as in the proof of the Lemma, amounts to the fact that definition (9) is a good one and that (11) holds. Plainly this can be decided with a finite amount of computation.

As to the second question, it can be decided e.g. by the usual local-global principle for 2-cocycles over number fields or by the following method, which allows even to find a suitable function ξ, when it exists.

Suppose that such a function ξ exists. First, since the $\zeta_{\sigma,\tau}$ are roots of unity, the divisor D_σ of ξ_σ satisfies $\partial(D_\sigma) = 0$. The group of divisors of k is however a permutation module for the action of $G = \mathrm{Gal}(k/\mathbf{Q})$, so, as we have seen in §2, we may write $D_\sigma = D - \sigma(D)$ for some divisor D. Since the class number of k is finite, we may write $D = (y) + R$, where (y) is the principal divisor of $y \in k^*$ and R is in a finite set which can be computed. Replacing ξ_σ with $\xi_\sigma\sigma(y)/y$ we may thus assume that the divisor of ξ_σ belongs to a finite set. Hence we may write $\xi_\sigma = z_\sigma u_\sigma$, where the $z_\sigma \in k^*$ lie in a finite set and $u_\sigma \in k^*$ are units. In particular we may suppose the z_σ to be fixed. Now, the unit group of k is of the form $\mathbf{Z}/(m) \times \mathbf{Z}^s$, for some integers m, s (and we may effectively find corresponding generators). The action of G corresponds to a certain linear action on this product. Our problem is thus easily reduced to a finite system of linear equations and congruences modulo m, to be solved in integers. It is an easy and well-known matter how to decide about the existence of integral solutions. This completes the argument.

ACKNOWLEDGEMENT. I would like to thank Professors J.-L. Colliot-Thélène, A. Schinzel, J.-P. Serre and the Referees for very helpful remarks and references.

REFERENCES

[CF] CASSELS, J.W.S. and A. FRÖHLICH (eds.). *Algebraic Number Theory.* Academic Press, London and New York, 1967.

[CThSDy] COLLIOT-THÉLÈNE, J.-L., and Sir PETER SWINNERTON-DYER. Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties. *J. reine angew. Math. 453* (1994), 49–112.

[CThCS] COLLIOT-THÉLÈNE, J.-L., D. CORAY et J.-J. SANSUC. Descente et principe de Hasse pour certaines variétés rationnelles. *J. reine angew. Math. 320* (1980), 150–191.

[DLS1] DAVENPORT, H., D.J. LEWIS and A. SCHINZEL. Polynomials of certain special types. *Acta Arith. 9* (1964), 107–116.

[DLS2] DAVENPORT, H., D.J. LEWIS and A. SCHINZEL. Quadratic diophantine equations with a parameter. *Acta Arith. 11* (1966), 353–358.

[FSS] FEIN, B., D.J. SALTMAN and M. SCHACHER. Brauer-Hilbertian fields, *Trans. Amer. Math. Soc. 334* (1992), 915–928.

[Nar] NARKIEWICZ, W. *Elementary and Analytic Theory of Algebraic Numbers.* 2nd ed., Polish Scientific Publishers & Springer Verlag, 1990.

[Oj] OJANGUREN, M. *The Witt Group and the Problem of Lüroth.* ETS Ed., Pisa, 1990.

[P] PIERCE, R. *Associative Algebras.* GTM 88, Springer, 1982.

[Raj] RAJWADE, A.R. *Squares.* London Math. Soc. Lecture Note 171. Cambridge Univ. Press, 1993.

[Sch1] SCHINZEL, A. *Selected Topics on Polynomials.* The University of Michigan Press, Ann Arbor, 1982.

[Sch2] —— On Hilbert's irreducibility theorem. *Ann. Polon. Math. 16* (1965), 333–340.

[Se1] SERRE, J.-P. *Cours d'arithmétique.* Presses Universitaires de France, Paris, 1970.

[Se2] —— *Topics in Galois Theory.* Jones and Bartlett, Boston, 1992.

[Se3] —— Spécialisation des éléments de $Br_2(\mathbf{Q}(t_1, \ldots, t_n))$. *C. R. Acad. Sci. Paris, Sér. I, 311* (1990), 397–402.

[V] VORONOVICH, I.I. Linear local-global principles for algebras over rational function fields. *Doklady Akad. Nauk BSSR 31* (1987), 877–880.

[We] WEIL, A. *Foundations of Algebraic Geometry.* A.M.S. Colloquium Publications, vol. 29, repr. 1989.

(Reçu le 5 février 1999)

Umberto Zannier

Istituto Univ. Architettura – D.C.A.
S. Croce, 191
I-30135 Venezia
Italy
e-mail: zannier@brezza.iuav.unive.it

vide-leer-empty