1. Introduction

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: