3. Proof of main results

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **13.09.2024**

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 $X_0,\dots,X_d$ 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 $N(t,X_1,\dots,X_d) - X_0^d f(t)$ we find a nontrivial zero with $X_i = x_i(t) \in \overline{\mathbf{Q}}[t]$. Suppose $x_0(t) = 0$. Then $N(t,x_1(t),\dots,x_d(t)) = 0$. But this cannot happen unless $x_i(t) = 0$ for all $i > 0$. In fact, $\omega_1,\dots,\omega_d$ 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 $\le D$, then a solution may be found where the unknowns have degree $\le \max(0, D-d+1)$. 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 $A(O,h) = \bigcup_{p \in \mathcal{P}(h)} \{x \in \mathbf{Q} : \mathrm{ord}_p(x - r_1) = 1\}$ 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*

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

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

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

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

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

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 **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

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

where $L(z) = \sum^*{}_{d \le z} \prod_{p|d} (\frac{1-\nu_p}{\nu_p})$ 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 $\le x$ 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

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

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

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

Also, $L(z) \ge \sum^{**} \frac{1}{\tau(d)d^s} - \sum^{**}{}_{d>z} \frac{1}{\tau(d)d^s} \ge \sum^{**} \frac{1}{\tau(d)d^s} + O(1)$. 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 $\ge \gamma \log \frac{1}{s-1}$ 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 $\sum m_iG_i$ 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 $\sum m_iG_i$ 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 $\mathbf{Q}_v(P_s)$.

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

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 $N(r, x_1, \dots, x_d)$ 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.