

**Zeitschrift:** L'Enseignement Mathématique  
**Band:** 45 (1999)  
**Heft:** 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

**Artikel:** LOCAL-GLOBAL PRINCIPLE FOR NORMS FROM CYCLIC EXTENSIONS OF  $\mathbb{Q}(t)$  (A DIRECT, CONSTRUCTIVE AND QUANTITATIVE APPROACH)  
**Kapitel:** 5. Remarks on Corollary 2  
**Autor:** ZANNIER, Umberto  
**DOI:** <https://doi.org/10.5169/seals-64456>

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

**Download PDF:** 07.10.2024

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

## 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  $N(t, x_1, \dots, x_d) \equiv f \pmod{p}$  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  $\omega_i$ '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

$$(13) \quad N(t, x_1, \dots, x_d) = x_0^d f,$$

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  $\Gamma$  of order  $d$ . Let  $g$  be the genus of  $\mathbf{L}$ . By  $\text{deg}_{\mathbf{L}}$  we shall mean the degree (of a function or divisor) referred to  $\mathbf{L}$ , while  $\text{deg}$  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  $\text{deg}_{\mathbf{L}} \psi \leq \text{deg} f + g + d - 1$ .*

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  $\text{deg}_{\mathbf{L}} F = d \text{deg} F = er \text{deg}_{\mathbf{L}} G_1$ . By taking norms we have  $dF = er \sum_{\sigma \in \Gamma} \sigma(G_1)$ . Let  $\sum m_i G_i$  be the part of  $\text{div}(\phi)$  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  $\phi$  in the form  $D_+ - D_- + (D - \gamma(D))$ , where  $D_+, D_-, D$  are  $\mathbf{k}$ -rational,  $D_+, D_-$  are positive and

$$\text{deg}_{\mathbf{L}} D_{\pm} \leq \sum_{\pm m_F \geq 0} (\pm m_F) \frac{er}{d} \text{deg}_{\mathbf{L}} G_1 \leq \sum_{\pm m_F \geq 0} m_F \text{deg} F = \text{deg} f.$$

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  $\Gamma$ . Let  $h$  be the least integer such that  $\text{deg} D + hd \geq g$ . Then  $g \leq \text{deg}(D + hZ) \leq g + d - 1$ . 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  $\xi$  are rational over  $\mathbf{k}$ ,  $E$  is also rational over  $\mathbf{k}$ . Also,  $\text{deg}_{\mathbf{L}} E = \text{deg}_{\mathbf{L}} D + hd \leq g + d - 1$ . Put  $\psi = \phi \frac{\xi}{\gamma(\xi)}$ . Then

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

Therefore the divisor of zeros of  $\psi$  has degree (in  $\mathbf{L}$ ) bounded by  $\text{deg}_{\mathbf{L}}(E + D_+) \leq \text{deg} f + g + d - 1$ . 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  $\psi$  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  $W_\sigma$  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  $W_\sigma$  and a prime  $\pi$  of  $k$ , lying above  $p$ , such that the reduction of  $W_\sigma$  modulo  $\pi$  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  $W_\sigma$  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  $\Sigma = \emptyset$ ) 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  $\psi_\sigma, L_\sigma, Q_{\sigma,\tau}$  for  $\sigma, \tau \in G' := \text{Gal}(k_v/\mathbf{Q}_p)$ ; 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  $\text{Gal}(\mathbf{F}_v/\mathbf{F}_p) \cong G'$ . By assumption, there exists  $\xi \in L(p)$  with norm  $\tilde{f}$ . Then  $\tilde{\varphi}$  and  $\xi$  have the same norm, whence  $\tilde{\varphi} = \xi(A/\gamma A)$  for some  $A \in \mathbf{F}_v L(p)$ . This easily leads to  $\tilde{L}_\sigma = (A/\sigma A)\tilde{B}_\sigma(t)$ , where  $\tilde{B}_\sigma \in \mathbf{F}_v(t)$ . In turn we find that  $\tilde{Q}_{\sigma,\tau} = \partial(\tilde{B}_\sigma)$ . If  $p$  is so large that no two zeros or poles of  $Q_{\sigma,\tau}$  may collapse after reduction, then it 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.