

# 6. Effectiveness

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **25.07.2024**

## **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

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.

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  $\psi_\sigma$ , as in (2) above. Now we can construct, as in the proof, the rational functions  $R_\sigma$ . 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  $R_\sigma$  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  $\xi: G \rightarrow k^*$ .

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  $\xi$ , when it exists.

Suppose that such a function  $\xi$  exists. First, since the  $\zeta_{\sigma,\tau}$  are roots of unity, the divisor  $D_\sigma$  of  $\xi_\sigma$  satisfies  $\partial(D_\sigma) = 0$ . The group of divisors of  $k$  is however a permutation module for the action of  $G = \text{Gal}(k/\mathbf{Q})$ , 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  $\xi_\sigma$  with  $\xi_\sigma \sigma(y)/y$  we may thus assume that the divisor of  $\xi_\sigma$  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  $z_\sigma$  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.