MATHEMATICS OF COMPUTATION
Volume 65, Number 216
October 1996, Pages 1663–1674

SOLVABILITY OF NORM EQUATIONS OVER CYCLIC NUMBER FIELDS OF PRIME DEGREE

VINCENZO ACCIARO

ABSTRACT. Let $L = \mathbb{Q}[\alpha]$ be an abelian number field of prime degree q, and let a be a nonzero rational number. We describe an algorithm which takes as input a and the minimal polynomial of α over $\mathbb{Q}$, and determines if a is a norm of an element of L. We show that, if we ignore the time needed to obtain a complete factorization of a and a complete factorization of the discriminant of α, then the algorithm runs in time polynomial in the size of the input.

As an application, we give an algorithm to test if a cyclic algebra $A = (E, \sigma, a)$ over $\mathbb{Q}$ is a division algebra.

1. INTRODUCTION

In his survey paper on algorithms in algebraic number theory [8], H. W. Lenstra states 'Among the many other algorithmic questions in algebraic number theory that merit attention we mention (...), problems from class field theory such as the calculation of Artin symbols, (...)'. In this paper we consider the following problem, which belongs naturally to class field theory:

Let $L = \mathbb{Q}[\alpha]$ be an abelian extension of the rationals of prime degree q, and $a \in \mathbb{Q}$, with $a \neq 0$. Does the equation

$$N_{L/\mathbb{Q}}(\lambda) = a \tag{1}$$

admit any solution λ in L?

Note that we are not interested in finding a solution λ, but simply determining whether a solution exists. Without loss of generality we can assume that $\alpha \in \mathcal{O}$, the ring of algebraic integers of L.

If we assume that $a \in \mathbb{Z}$, the rational integers, and we ask for solutions of (1) in the algebraic integers, we can use an algorithm, due to U. Fincke and M. Pohst [12, p. 336], based on methods borrowed from the geometry of numbers, which works for any finite extension of $\mathbb{Q}$. However, even if (1) is not solvable in the algebraic integers, it may still be solvable in $\mathbb{Q}[\alpha]$.

In this paper we give a polynomial-time algorithm to determine if (1) is solvable, based on methods from class field theory. The input to our algorithm consists of a and the minimal polynomial $m_\alpha(x)$ of α over $\mathbb{Q}$. We assume that $m_\alpha(x)$ is given in its dense representation, that is, as an array giving all its coefficients. If we ignore the time needed to obtain a complete factorization of a and a complete factorization of $d_L(\alpha)$, the discriminant of α, then the algorithm runs in time polynomial in the size of the input.

Received by the editor March 30, 1995 and, in revised form, July 14, 1995.
1991 *Mathematics Subject Classification.* Primary 11R37; Secondary 11Y40.

Our algorithm is based on the celebrated Hasse Norm Theorem, which states that, for a cyclic extension K/k, an element $a \in k$ is a norm from K if and only if it is a local norm at every prime of K. As we will show below, it is possible to list a finite set of primes such that these are the only finite primes that must be taken into consideration in applying the Hasse Norm Theorem. Moreover, we will show in §8 that the infinite primes play a role only in the quadratic case. Then, in §9 we present the complete algorithm and discuss its complexity.

As an application, we give in §10 an algorithm to test if a cyclic algebra A of finite dimension n over $\mathbb{Q}$ is a division algebra. We assume that A is presented in the standard form [11, p. 277] as a triple (E, σ, a), where E is a cyclic subfield of A of degree $\sqrt{n}$ over $\mathbb{Q}$, σ is a generator of the Galois group of $E/\mathbb{Q}$, and a is a nonzero element of $\mathbb{Q}$. The field E is given by the minimal polynomial $m_c(x)$ of a primitive element c for E over $\mathbb{Q}$, and the automorphism σ is given as a polynomial $i(x)$ such that $i(c) = \sigma(c)$.

Note 1. Using methods borrowed from noncommutative number theory, L. Rónyai developed an algorithm [13, 4] to test if a central simple algebra A over an algebraic number field K is a division algebra. The input to Rónyai's algorithm consists of a set of structure constants for A, and the algorithm runs in time polynomial in the size of the input, assuming the use of oracles for factoring integers and for factoring polynomials over finite fields. In contrast, we do not need to factor polynomials over finite fields. Rónyai's algorithm is very powerful, since it computes the *index* of A (for the definition of 'index' refer to §10), thus allowing one to gain a lot of information about the structure of the algebra A.

The algorithms described in this paper have been implemented using the number theory package PARI, developed in France by Professor H. Cohen and his collaborators.

For the terminology and the basic concepts of algebraic number theory used in this paper we refer the reader to [5]. For the theory of associative algebras we refer the reader to [11].

2. Notation

If B is a subgroup of a group A, $(A : B)$ will denote the index of B in A, and A^m the subgroup of A generated by the mth powers of the elements of A.

If k is a subfield of a field K, $[K : k]$ will denote the degree of the field extension K/k, and $K^* = K\backslash\{0\}$ will denote the multiplicative group of K.

Let L be an algebraic number field. By a prime of L we mean a class of equivalent valuations of L. Recall that the finite primes are in one-to-one correspondence with the prime ideals of $\mathcal{O}$, and the infinite primes with the embeddings σ of L into $\mathbb{C}$, the field of complex numbers. We will use the same symbol to denote a finite prime of L and the corresponding prime ideal of $\mathcal{O}$.

Let $\mathcal{P}$ be a finite prime of L. If $\beta \in L$ and $\beta \neq 0$, we will denote by $\nu_{\mathcal{P}}(\beta)$ the order of β at $\mathcal{P}$, that is, the power of $\mathcal{P}$ in the factorization of the fractional ideal $\beta\mathcal{O}$. We define $\nu_{\mathcal{P}}(0)$ to be ∞. The symbol $L_{\mathcal{P}}$ will denote the completion of L with respect to the $\mathcal{P}$-adic valuation, and $\mathcal{O}_{\mathcal{P}} = \{x \in L_{\mathcal{P}} \mid \nu_{\mathcal{P}}(x) \geq 0\}$ the ring of $\mathcal{P}$-adic integers.

Let $\mathcal{P}$ be an infinite prime of L, that is, an embedding $\sigma : L \to \mathbb{C}$. The symbol $L_{\mathcal{P}}$ will denote the completion of L with respect to the (Archimedean) valuation $\beta \mapsto |\sigma(\beta)|$.

Let p be a rational prime. If $b \in \mathbb{Q}$ and $b \neq 0$, then $\nu_p(b)$ will denote the order of b at p, that is, the power of the ideal $p\mathbb{Z}$ in the factorization of the fractional ideal $b\mathbb{Z}$. We define $\nu_p(0)$ to be ∞. The symbol $\mathbb{Q}_p$ will denote the field of p-adic numbers, $\mathbb{Z}_p$ the ring of p-adic integers, and U_p the group of units of $\mathbb{Z}_p$. Finally, $\mathbb{F}_p$ will denote the finite field of p elements.

3. Cyclic number fields of prime degree

Fundamental to the entire construction is the following theorem (see [5, p. 156]).

Theorem 1 (Hasse Norm Theorem)**.** *Let K/k be a cyclic extension. An element $a \in k^*$ is a norm from K^* if and only if a is a local norm at every prime (including the infinite primes) of k.*

We will deal with the infinite primes in §8. Until then, all the primes considered will be finite.

The following lemma tells us that the property of being Galois is preserved by the completions at the finite primes. For its proof we refer to [11, p. 347, Corollary c].

Lemma 1. *Let K be a finite Galois extension of an algebraic number field k. Let p be a prime of k and $\mathcal{P}$ be a prime of K lying above p. Then $K_\mathcal{P}/k_p$ is also Galois, and the Galois groups* $\mathrm{Gal}(K_\mathcal{P}/k_p)$ *and* $\mathrm{Gal}(K/K \cap k_p)$ *are isomorphic.*

Throughout the following, L will denote a cyclic extension of prime degree q over $\mathbb{Q}$. Since $L/\mathbb{Q}$ is Galois, all the ideals lying above a rational prime p must have the same ramification index e and the same inertial degree f. Therefore, the degree $[L_\mathcal{P} : \mathbb{Q}_p]$, which is equal to ef, is independent of the prime ideal $\mathcal{P}$ lying above p. Let g be the number of distinct prime ideals lying above p. From the formula $efg = [L : \mathbb{Q}]$ and the primality of q it follows that either $e = 1$ or $e = q$.

Our first task is to recognize the decomposition type of a rational prime p in L. Since we do not wish to involve the cost of computing an integral basis, in the next section we will develop a fast algorithm to accomplish this task when an integral basis for L is not known.

4. Decomposition of primes

In the following lemma we relate the decomposition of the minimal polynomial $m_\alpha(x)$ of α over $\mathbb{Q}_p$ to the decomposition of p in L.

Lemma 2. *Let $L = \mathbb{Q}[\alpha]$ be a cyclic number field of prime degree q, with α an algebraic integer, and let p be a rational prime. If p is inert or totally ramified in L, then $m_\alpha(x)$ is irreducible over $\mathbb{Q}_p$.*

Proof. Let $K = \mathbb{Q}[\beta]$ be an arbitrary number field. It can be shown (see [5, Exercise 1, p. 92]) that if $\mathcal{P}_i$ $(i = 1, \ldots, r)$ are the prime ideals lying above a rational prime p, with inertial degree f_i and ramification index e_i, then $m_\beta(x)$ splits into r factors in $\mathbb{Q}_p$, of degree $e_1 f_1, \ldots, e_r f_r$. In our case we have $r = 1$ and so $m_\alpha(x)$ is irreducible over $\mathbb{Q}_p$. □

The following corollary to Lemma 2 is an easy consequence of Hensel's Lemma.

Corollary 1. *Let $L = \mathbb{Q}[\alpha]$ be a cyclic number field of prime degree q, with α an algebraic integer, and let p be a rational prime. If p does not split in L, then $m_\alpha(x)$ is either irreducible over $\mathbb{F}_p$ or it is the qth power of a linear polynomial over $\mathbb{F}_p$.*

The next lemma exploits the Galois structure of L to obtain more information about the decomposition of the rational primes in L.

Lemma 3. *Let $L = \mathbb{Q}[\alpha]$ be a cyclic number field of prime degree q, with α an algebraic integer, and let p be a rational prime. If p splits completely in L, then $m_\alpha(x)$ splits into (possibly equal) linear factors over $\mathbb{F}_p$. Conversely, if $m_\alpha(x)$ has at least two distinct linear factors over $\mathbb{F}_p$, then p splits completely in L.*

Proof. The first assertion follows easily from the fact that when p splits completely in L, the Frobenius automorphism of p has order one.

To prove the second assertion, assume that p does not split in L and $m_\alpha(x) \equiv g(x)h(x) \pmod p$, with $g(x)$ and $h(x)$ relatively prime. This clearly contradicts Corollary 1. □

The next lemma (see [3, Proposition 5.11, p. 102]) gives us a partial converse of Corollary 1.

Lemma 4. *Let $K = \mathbb{Q}[\beta]$ be an algebraic number field, with β integral over $\mathbb{Z}$, and let p be a rational prime. If the minimal polynomial $m_\beta(x)$ of β over $\mathbb{Q}$ is irreducible over $\mathbb{F}_p$, then p is inert in K.*

Combining the results obtained so far, we obtain the following.

Lemma 5. *Let $L = \mathbb{Q}[\alpha]$ be a cyclic extension of $\mathbb{Q}$ of prime degree q, where α is an algebraic integer. Then its minimal polynomial $m_\alpha(x)$ is either irreducible over $\mathbb{F}_p$ or it splits into linear factors over $\mathbb{F}_p$. If $m_\alpha(x)$ has at least two distinct roots in $\mathbb{F}_p$, then p splits completely in L. If $m_\alpha(x)$ has no roots in $\mathbb{F}_p$, then p is inert in L.*

The value of Lemma 5 lies in the fact that it is possible to check very efficiently whether its hypotheses are fulfilled. For this purpose we compute $l(x) = \gcd(x^p - x, m_\alpha(x))$ over $\mathbb{F}_p$. Then $m_\alpha(x)$ has no roots in $\mathbb{F}_p$ precisely when $\deg l(x) = 0$, and it is a qth power over $\mathbb{F}_p$ precisely when $\deg l(x) = 1$. [In practice we compute $j(x) = x^p \bmod m_\alpha(x)$ over $\mathbb{F}_p$, using the binary powering algorithm (see [2, p. 8]); then $l(x)$ is given by $\gcd(j(x) - x, m_\alpha(x))$.]

Before proving the main theorem of this section, we need a last lemma (see [7, Proposition 11, p. 52]).

Lemma 6. *Let $L = \mathbb{Q}[\alpha]$ be a cyclic number field of prime degree q with $\alpha \in \mathcal{O}$, the ring of integers of L, and let p be a rational prime.*

If p ramifies in L and $\pi \in \mathcal{P}\backslash\mathcal{P}^2$, where $\mathcal{P}$ denotes the unique prime ideal of $\mathcal{O}$ above p, then the minimal polynomial $m_\pi(x)$ of π is Eisenstein at p. Conversely, if the minimal polynomial $m_\pi(x)$ of some $\pi \in \mathcal{O}$ is Eisenstein at p, then p ramifies in L.

Now we can state the main theorem of this section.

Theorem 2. *Let $L = \mathbb{Q}[\alpha]$ be a cyclic number field of prime degree q with $\alpha \in \mathcal{O}$, the ring of integers of L, and let p be a rational prime. Then:*

(i) *If p is inert or totally ramified, then there exist $m, h \in \mathbb{Z}$ such that*

$$\gamma = (\alpha - m)/p^h \in \mathcal{O} \tag{2}$$

but no integers h', m' with $h' > h$ such that

$$\gamma' = (\alpha - m')/p^{h'} \in \mathcal{O}.$$

(ii) *If p is inert in L, then $m_\gamma(x)$ is irreducible over $\mathbb{F}_p$.*
(iii) *If p ramifies in L, then $m_\gamma(x) \equiv (x-c)^q \pmod p$, with $q \nmid r = \nu_p(N_{L/\mathbb{Q}}(\gamma - c))$. Let $s \in \mathbb{N}$ and $l \in \mathbb{Z}$ be such that $rs + ql = 1$. Then $\pi = (\gamma - c)^s p^l$ satisfies an Eisenstein polynomial at p.*

Proof. By assumption, $\alpha \in \mathcal{O} \backslash \mathbb{Z}$. Assertion (i) comes from the fact that when p does not split completely, $\alpha \notin \mathbb{Q}_p$ by Lemma 2, and so we must have $\mathcal{O} \cap \mathbb{Z}_p = \mathbb{Z}$. Note that $L = \mathbb{Q}[\gamma]$.

To prove (ii), assume that p is inert and $m_\gamma(x)$ is not irreducible over $\mathbb{F}_p$. Then, by Corollary 1 we would have $m_\gamma(x) \equiv (x-c)^q \pmod p$ for some $c \in \mathbb{Z}$. Hence $\gamma - c \in p\mathcal{O}$, and so $(\alpha - m - cp^h)/p^{h+1} \in \mathcal{O}$, contradicting the choice of h.

To prove (iii), assume that p ramifies, and so $p\mathcal{O} = \mathcal{P}^q$, where $\mathcal{P}$ denotes the unique prime ideal of $\mathcal{O}$ above p. Since $m_\gamma(x)$ cannot be irreducible over $\mathbb{F}_p$ by Lemma 5, we must have $m_\gamma(x) \equiv (x-c)^q \pmod p$ for some $c \in \mathbb{Z}$. Then $(\gamma - c)^q \in p\mathcal{O}$, and so $\gamma - c \in \mathcal{P}$. We claim that $\gamma - c \notin \mathcal{P}^q$. For otherwise, reasoning as above, we would have $(\alpha - m - cp^h)/p^{h+1} \in \mathcal{O}$, contradicting the choice of h. Therefore $\gamma - c \in \mathcal{P}^r \backslash \mathcal{P}^{r+1}$, with $0 < r < q$. Let $s \in \mathbb{N}$ and $l \in \mathbb{Z}$ be such that $rs + ql = 1$. It can be easily seen that $\pi = (\gamma - c)^s p^l \in \mathcal{P} \backslash \mathcal{P}^2$, and therefore by Lemma 6 the polynomial $m_\pi(x)$ must be Eisenstein at p. □

The next lemma shows that the integer h given by (2) is 'small'.

Lemma 7. *Let us assume the notation of Theorem 2. If p is inert, then $h = \nu_p(d_L(\alpha))/(q(q-1))$. If p is totally ramified, then $h \le \nu_p(d_L(\alpha))/(q(q-1))$.*

Proof. Assume first that p is inert. Let $\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} | \nu_p(x) \ge 0\}$, and let $\mathcal{O}_{(p)}$ denote the integral closure of $\mathbb{Z}_{(p)}$ in L, which is equal to $\{x \in L | \nu_{\mathcal{P}}(x) \ge 0\}$ since $\mathcal{P}$ is the unique prime ideal of $\mathcal{O}$ above p. Since γ is a primitive element for $\mathcal{O}/\mathcal{P}$ over $\mathbb{Z}/p\mathbb{Z}$, the set $\{1, \gamma, \dots, \gamma^{q-1}\}$ is an integral basis for $\mathcal{O}_{(p)}$ over $\mathbb{Z}_{(p)}$ (see [7, Proposition 23, p. 26]), and therefore $\nu_p(d_L(\gamma)) = 0$. Now in general, when $\delta \in \mathcal{O}$ and $b \in \mathbb{Z}$, we have $d_L(p\delta) = p^{q(q-1)} d_L(\delta)$, and $d_L(p\delta + b) = d_L(p\delta)$, and therefore $d_L(\alpha) = p^{q(q-1)h} d_L(\gamma)$, i.e., $\nu_p(d_L(\alpha)) = q(q-1)h$. This proves the first part of the lemma.

Assume next that p ramifies. We have seen that in this case $m_\gamma(x) \equiv (x-c)^q \pmod p$ for some $c \in \mathbb{Z}$, with $\gamma - c \in \mathcal{P}^r \backslash \mathcal{P}^{r+1}$ $(0 < r < q)$. Clearly, $\nu_p(d_L(\gamma - c)) \ge \nu_p(d_L)$. It is known (see [14]) that for odd q we have

$$\nu_p(d_L) = \begin{cases} q-1 & \text{if} \quad p \ne q, \\ 0 \text{ or } 2(q-1) & \text{if} \quad p = q. \end{cases}$$

Moreover, it can be shown (see [2, Proposition 5.1.1, p. 218]) that when $q = 2$, we have

$$\nu_p(d_L) = \begin{cases} 1 & \text{if} \quad p \ne 2, \\ 2 \text{ or } 3 & \text{if} \quad p = 2. \end{cases}$$

The same argument as above shows that $\nu_p(d_L(\alpha)) = q(q-1)h + \nu_p(d_L(\gamma - c))$, and so $\nu_p(d_L(\alpha)) \ge q(q-1)h + \nu_p(d_L)$. It follows that

$$h \le (\nu_p(d_L(\alpha)) - \nu_p(d_L))/(q(q-1)),$$

and hence $h \le \nu_p(d_L(\alpha))/(q(q-1))$. □

```
procedure DECOMPOSE(p, β):
    if p ∤ d_L(β)
        then if m_β(x) has no roots in F_p
            then return INERT
            else return SPLITS
        endif
    endif
    let h = ⌊ν_p(d_L(β))/(q(q − 1))⌋;
    for i = 1 to h do
        if m_β(x) has exactly one root c in F_p
            then let β = (β − c)/p;
                if m_β(x) ∉ Z[x]
                    then let β = pβ;
                    return CONSTRUCT_EISENSTEIN(p, β)
                endif
            else return SPLITS
        endif
    endfor
    if m_β(x) has exactly one root c in F_p
        then let β = β − c
        else if m_β(x) has no roots in F_p
                then return INERT
                else return SPLITS
            endif
    endif
    return CONSTRUCT_EISENSTEIN(p, β)
```

FIGURE 1. The algorithm DECOMPOSE

```
procedure CONSTRUCT_EISENSTEIN(p, β):
    let r = ν_p(N_{L/Q}(β));
    if q | r
        then return SPLITS
    endif
    find s ∈ N and l ∈ Z such that rs + ql = 1;
    let π = (β)^s p^l;
    if m_π(x) is Eisenstein at p
        then return RAMIFIES and π
        else return SPLITS
    endif
```

FIGURE 2. Auxiliary procedure used by DECOMPOSE

Note 2. When p is inert, if $u \in \mathbb{Z}$ and $i < h = \nu_p(d_L(\alpha))/(q(q-1))$, then the minimal polynomial of $(\alpha - u)/p^i$ cannot be irreducible over $\mathbb{F}_p$. In fact, if $\omega = (\alpha - u)/p^i$, with $i < h$ and $u \in \mathbb{Z}$, then the argument used in the proof of Lemma 7 shows that $\nu_p(d_L(\omega)) > 0$. But then the set $\{1, \omega, \dots, \omega^{q-1}\}$ cannot be an integral basis for $\mathcal{O}_{(p)}$ over $\mathbb{Z}_{(p)}$, hence ω cannot be a primitive element for $\mathcal{O}/\mathcal{P}$ over $\mathbb{Z}/p\mathbb{Z}$, and so $m_\omega(x)$ must be a qth power over $\mathbb{F}_p$.

The computation of the algebraic integer γ that satisfies (2) is carried out by p-adic lifting. For this purpose we compute iteratively a sequence of algebraic numbers $\gamma_1, \gamma_2, \dots$ as follows: if $m_{\gamma_{i-1}}(x) \equiv (x - c_i)^q \pmod p$, where $\gamma_0 = \alpha$, then we let $\gamma_i = (\gamma_{i-1} - c_i)/p$. From what has been said in this section it is clear that the process can stop as soon as either one of the following conditions is satisfied:

(i) $i = \nu_p(d_L(\alpha))/(q(q-1))$. By applying Theorem 2 to $\gamma = \gamma_i$ we are able to verify if p ramifies or it is inert in L. If neither cases are true, then p splits completely in L.

(ii) $\gamma_i \notin \mathcal{O}$ for $i < \nu_p(d_L(\alpha))/(q(q-1))$. The note above shows that p cannot be inert, and so we have to check if p is ramified, by applying Theorem 2 to $\gamma = \gamma_{i-1}$. If p is not ramified, then it splits completely.

(iii) The minimal polynomial of γ_i, with $i \leq \nu_p(d_L(\alpha))/(q(q-1))$, has at least two distinct roots in $\mathbb{F}_p$. In this case p splits completely in L.

The algorithm DECOMPOSE, shown in Figure 1, implements the ideas described above. It takes as input p and α, and returns $INERT$ if p is inert in $L = \mathbb{Q}[\alpha]$, $SPLITS$ if it splits, and $RAMIFIES$ plus an Eisenstein element π if p ramifies.

The argument following Lemma 5 shows that it is possible to check if $m_\alpha(x)$ has no roots, at least two distinct roots or just one root in $\mathbb{F}_p$ – and in the last case compute the unique root, which has multiplicity q – in time polynomial in the size of p and in the degree q of $m_\alpha(x)$. Moreover, it is not difficult to show that the size of m_γ is bounded by a polynomial in the size of m_α. Therefore, the algorithm DECOMPOSE runs in time polynomial in the size of the input.

5. The unramified case

In this section we deal with the case $e = 1$, that is, we assume that the prime p is *unramified* in L.

The case when $f = 1$, that is, when p *splits completely* in L, is uninteresting, since we have $L_\mathcal{P} = \mathbb{Q}_p$, and so any $a \in \mathbb{Q}_p^*$ is the norm of itself in the trivial extension of $\mathbb{Q}_p$.

Hence we will restrict our attention to the case $f = q$, that is, when p is *inert* in L. Then $L_\mathcal{P}$ is a nontrivial unramified extension of $\mathbb{Q}_p$ of degree q, so the next theorem characterizes completely the norm group of $L_\mathcal{P}/\mathbb{Q}_p$. For its proof we refer to [1, Theorem 19, p. 141] and to [5, p. 153].

Theorem 3. *Let $L_\mathcal{P}$ be an unramified extension of $\mathbb{Q}_p$ of degree f over $\mathbb{Q}_p$. Let $\beta = p^m u \in \mathbb{Q}_p^*$, with $u \in U_p$, $m \in \mathbb{Z}$. Then $\beta \in N_{L_\mathcal{P}/\mathbb{Q}_p}(L_\mathcal{P}^*)$ if and only if $f \mid m$. In particular, every unit of $\mathbb{Q}_p$ is the norm of a unit in $L_\mathcal{P}$.*

6. The totally ramified case

For the totally ramified extensions of $\mathbb{Q}_p$, the problem of deciding whether an element of $\mathbb{Q}_p^*$ is a local norm is harder. We need a preliminary lemma.

Lemma 8. *Let $u = \sum_{i=0}^{\infty} u_i p^i \in U_p$, with u_i integers, $0 \leq u_i < p$ and $u_0 \neq 0$. If $q \neq p$ is a prime, then $u \in U_p^q$ if and only if u_0 is a qth power modulo p. The index $(U_p : U_p^q)$ is equal to q if $q \mid p-1$, and it is equal to 1 otherwise.*

Proof. Clearly, if u is a qth power in $\mathbb{Q}_p$, then u_0 is a qth power modulo p. Conversely, let $g(x) = x^q - u$. Consider the equation

$$g(x) = 0 \tag{3}$$

in $\mathbb{Q}_p$. Assume that $\hat{x}^q \equiv u_0 \pmod{p}$, where $\hat{x} \not\equiv 0 \pmod{p}$, since $u_0 \not\equiv 0 \pmod{p}$. Now $g'(\hat{x}) = q\hat{x}^{q-1} \not\equiv 0 \pmod{p}$, and therefore, by Hensel's lemma [5, Proposition 3.5, p. 83], we can lift $\hat{x}$ to a solution of the equation (3) in U_p.

If $q \nmid p-1$, then every integer not divisible by p has a qth root (mod p). Therefore, the argument given above shows that every element of U_p has a qth root in U_p, and so $(U_p : U_p^q) = 1$.

If $q \mid p-1$, choose an integer w which is not a qth root (mod p). Since the group of units of $\mathbb{Z}/p\mathbb{Z}$ is cyclic, the first part of the lemma shows that the set $\{1, w, \ldots, w^{q-1}\}$ is a set of coset representatives for U_p^q in U_p, and therefore $(U_p : U_p^q) = q$. □

The next result, known as the *fundamental equality of local class field theory,* is valid for any local field, and hence in particular for any p-adic field (see [7, Corollary, p. 221] and [7, Theorem 3, p. 219]).

Theorem 4. *Let K/k be a cyclic extension of local fields, with ramification index e. Let U_K (resp. U_k) denote the group of units of K (resp. k). Then $(U_k : N_{K/k}(U_K)) = e$ and $(k^* : N_{K/k}(K^*)) = [K : k]$.*

We can now characterize the norm groups of the totally ramified extensions of $\mathbb{Q}_p$ of prime degree.

Theorem 5. *Let $L_{\mathcal{P}}$ be a totally ramified cyclic extension of $\mathbb{Q}_p$, of prime degree q, where $q \mid p-1$. An element $u \in U_p$ is a norm of a unit in $L_{\mathcal{P}}$ if and only if u is a qth power in U_p.*

Proof. Let $U_{\mathcal{P}}$ denote the group of units of $L_{\mathcal{P}}$. It is easy to see that $N_{L_{\mathcal{P}}/\mathbb{Q}_p}(U_{\mathcal{P}}) \supset U_p^q$, since for any $x \in U_p$ we have $N_{L_{\mathcal{P}}/\mathbb{Q}_p}(x) = x^q$. By Lemma 8 the index $(U_p : U_p^q)$ is equal to q. Then Theorem 4, with $K = L_{\mathcal{P}}$, $k = \mathbb{Q}_p$ and $e = q = [L_{\mathcal{P}} : \mathbb{Q}_p]$, gives us the desired equality $N_{L_{\mathcal{P}}/\mathbb{Q}_p}(U_{\mathcal{P}}) = U_p^q$. □

Note 3. The case $p \neq q$ and $q \nmid p-1$, with $L_{\mathcal{P}}$ a totally ramified cyclic extension of $\mathbb{Q}_p$ of degree q, can never happen. Indeed, we certainly have $N_{L_{\mathcal{P}}/\mathbb{Q}_p}(U_{\mathcal{P}}) \supset U_p^q$, and Lemma 8 implies that $U_p = U_p^q$. This contradicts Theorem 4 (for a different proof of this statement, which uses the conductor-discriminant formula, see [14]).

Note 4. The remaining case $p = q$ can be ignored, without incurring the risk of being incomplete. It is in fact true (see [5, p. 190]) that *if $K/\mathbb{Q}$ is abelian and $a \in \mathbb{Q}^*$ is a p-local norm for all the primes p, with the possible exception of one particular prime, then a must be a local norm at that prime also.* Thus, if a is not a local norm at the prime $p = q$, then there is a prime $p' \neq q$ for which a is not a local norm. Hence we can avoid consideration of the case $p = q$.

7. The finite primes: summarizing

Let p be a rational prime and $\mathcal{P}$ be a prime ideal of $\mathcal{O}$ lying above p. We want to determine whether $a \in N_{L_\mathcal{P}/\mathbb{Q}_p}(L_\mathcal{P}^*)$.

If p splits completely in $\mathcal{O}$, then every $a \in \mathbb{Q}_p^*$ is a norm, and so this case is not interesting.

The case where p is inert is also easily dealt with, as it has been shown in §5.

It remains to consider the case where p divides d_L, the discriminant of $L/\mathbb{Q}$, that is, when $L_\mathcal{P}$ is a totally ramified extension of $\mathbb{Q}_p$ of degree q. We have seen that we can ignore the case $p = q$, so suppose $p \neq q$. Assume that we know an element $u_1 \in U_p$ such that

$$pu_1 \in N_{L_\mathcal{P}/\mathbb{Q}_p}(L_\mathcal{P}^*). \tag{4}$$

If $a = p^t u$ with $u \in U_p$, then we can write $a = (pu_1)^t u/u_1^t$ and so $a \in N_{L_\mathcal{P}/\mathbb{Q}_p}(L_\mathcal{P}^*)$ if and only if

$$\frac{u}{u_1^t} \in N_{L_\mathcal{P}/\mathbb{Q}_p}(L_\mathcal{P}^*). \tag{5}$$

Now Theorem 5 tells us that (5) holds precisely when

$$\frac{u}{u_1^t} \in U_p^q. \tag{6}$$

Thus, we want to construct an element $u_1 \in U_p$ which satisfies (4). For this purpose, take any $\pi \in \mathcal{P}\backslash\mathcal{P}^2$. Then $\nu_\mathcal{P}(\pi) = 1$, and $\nu_p(N_{L/\mathbb{Q}}(\pi)) = \nu_\mathcal{P}(\pi) = 1$. Since $[L : \mathbb{Q}] = [L_p : \mathbb{Q}_p] = q$, and q is prime, we have $N_{L_p/\mathbb{Q}_p}(\pi) = N_{L/\mathbb{Q}}(\pi)$. Hence, we can take $u_1 = N_{L_p/\mathbb{Q}_p}(\pi)/p$.

Note 5. In order to decide if (6) is satisfied, we proceed as follows. We know that $u/u_1^t \in \mathbb{Q}^*$ and $\nu_p(u/u_1^t) = 0$ by construction. We write u/u_1^t as j/k with $j, k \in \mathbb{Z}$ and $\gcd(j, k) = 1$, and then we compute $m, n \in \mathbb{Z}$ such that $mk + np = 1$. Now $jm \in \mathbb{Z}$, and it can be shown (see [6, p. 12]) that $\nu_p(u/u_1^t - jm) \geq 1$. Lemma 8 then tells us that u/u_1^t is a qth power in U_p if and only if jm is a qth residue modulo p, and it is well known (see [10, Theorem 2.27, p. 64]) that this holds if and only if

$$(jm)^{(p-1)/\gcd(q,p-1)} \equiv 1 \pmod{p},$$

that is, if and only if

$$(jm)^{(p-1)/q} \equiv 1 \pmod{p}$$

since $q \mid p - 1$.

8. The infinite primes

Since $L = \mathbb{Q}[\alpha]$ is Galois over $\mathbb{Q}$, then either L is *totally real*, that is, all the possible embeddings of L in $\mathbb{C}$ are real, or L is *totally complex*, that is, all the embeddings are nonreal (see [2, Def. 4.1.9]).

Since $[L : \mathbb{Q}] = q$ is a prime number, if $q \neq 2$, then q is odd, and hence L must necessarily be totally real. If $[L : \mathbb{Q}] = 2$, then L is complex precisely when $d_L(\alpha) < 0$.

Given any infinite prime ∞, if L is totally real, then $L_\infty = \mathbb{R}$, and if L is totally complex, then $L_\infty = \mathbb{C}$. The completion of $\mathbb{Q}$ at its unique infinite prime is $\mathbb{R}$.

In the totally real case, any element of $\mathbb{R}$ is the norm of itself in the trivial extension of $\mathbb{R}$. In the totally complex case we have $N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}) = \mathbb{R}^+$, the nonnegative reals. The latter case can only arise when $q = 2$.

9. The test

We now describe an algorithm to decide if $a \in \mathbb{Q}^*$ is a norm in $L/\mathbb{Q}$.

Write a as r/s, with $r \in \mathbb{Z}$, $s \in \mathbb{Z}\backslash\{0\}$, and $\gcd(r, s) = 1$. The considerations in §7 show that the only finite primes that must be taken into account are those which divide r, those which divide s, and those which divide d_L, and that we may ignore the prime q. Recall that $d_L(\alpha)$ can be computed by the formula

$$d_L(\alpha) = (-1)^{q(q-1)/2} N_{L/\mathbb{Q}}(m'_\alpha(\alpha)), \tag{7}$$

where $m'_\alpha(x)$ denotes the formal derivative of $m_\alpha(x)$. Once a complete factorization of $d_L(\alpha)$ is known, we can use the algorithm DECOMPOSE to determine which prime factor p of $d_L(\alpha)$ ramifies in L, and for each ramified prime a corresponding element π whose norm has p-order 1.

The complete algorithm NORM is shown in Figure 3. It takes as input a and $m_\alpha(x)$, and returns $TRUE$ if $a \in N_{L/\mathbb{Q}}(L^*)$, $FALSE$ otherwise.

```
procedure NORM(a, m_α(x)):
    if ([L : ℚ] = 2 and d_L(α) < 0 and a < 0) then
        return FALSE
    endif
    construct the set RP of ramified primes;
    express a as r/s, with r, s ∈ ℤ and gcd(r, s) = 1;
    let NP be the set of positive primes dividing r;
    let DP be the set of positive primes dividing s;
    for all the p in RP ∪ NP ∪ DP, with p ≠ q do
        let t = ν_p(a);
        if p ∉ RP then
            if (p is inert and q ∤ t) then
                return FALSE
            endif
        else
            let π ∈ L be such that ν_p(N_{L/ℚ}(π)) = 1;
            let u = a/(N_{L/ℚ}(π)^t);
            express u as j/k, with j, k ∈ ℤ and gcd(j, k) = 1;
            compute m, n ∈ ℤ such that mk + np = 1;
            let z = (p − 1)/q;
            if (jm)^z ≢ 1 (mod p) then
                return FALSE
            endif
        endif
    endfor
    return TRUE
```

Figure 3. The algorithm NORM

In analyzing the complexity of the algorithm NORM, we will ignore the cost of factoring a and $d_L(\alpha)$. Let us define size(m), for $m \in Z$, to be the number of bits needed to represent m, and size(a) to be size(r) + size(s).

We want to show that the algorithm NORM runs in time polynomial in the size of the input. For this purpose it is enough to show that the size of the primes involved in the test is bounded by size(a) + size$(m_\alpha(x))^{\mathcal{O}(1)}$. Now, Mahler's bound on the discriminant of a polynomial [9, Corollary to Theorem 1, p. 261] implies that size$(d_L(\alpha))$ is bounded by size$(m_\alpha(x))^{\mathcal{O}(1)}$. Since $d_L \mid d_L(\alpha)$, it follows that the size of each prime divisor of d_L is bounded by size$(m_\alpha(x))^{\mathcal{O}(1)}$ as well. Since $d_L(\alpha)$ can have at most $\log |d_L(\alpha)|$ prime divisors, it follows that the size of the list of primes dividing $d_L(\alpha)$ is bounded by size$(m_\alpha(x))^{\mathcal{O}(1)}$.

10. Test of cyclic algebras over $\mathbb{Q}$ for zero divisors

Let A be a central simple algebra of finite dimension n over $\mathbb{Q}$. Recall that the dimension n of a central simple algebra A over the base field is always a square number; the positive integer $d = \sqrt{n}$ is called the *degree* of A.

By the Wedderburn structure theorem, any central simple algebra A over a field F is isomorphic to a full matrix algebra over a, possibly noncommutative, finite extension D of F. The degree of D over F (as an algebra) is called the (*Schur*) *index* of A. Clearly, *A is a division algebra if and only if its index and its degree are the same.*

On the other hand, it is known from Brauer's theory (see [11, p. 260]) that, for some finite number h, the tensor product $A \otimes \cdots \otimes A$ (h times) is isomorphic to a full matrix algebra over F. The smallest such h is called the *exponent* of A.

An important class of central simple algebras is given by the cyclic algebras. They can be defined in a concrete way as follows (see [11, p. 277]):

Definition 1. A finite-dimensional associative algebra A over a field F is called cyclic if it is generated over F by two elements c and b such that:

(i) The subalgebra $F[c]$ of A generated by c is a cyclic extension field E of F of degree d, say;
(ii) b is invertible and $b^{-1}cb = \sigma(c)$, where σ is a generator of the Galois group $\mathrm{Gal}(E/F)$;
(iii) $b^d \in F^*$.

It follows from this characterization that A is a central simple algebra of dimension d^2 over F with basis $\{c^i b^k | 0 \le i, k < d\}$. Let $a = b^d$. We denote the algebra A by (E, σ, a).

Although cyclic algebras have an uncomplicated structure, as the next theorem shows they are quite general (see [11, p. 359] for a proof).

Theorem 6 (Brauer-Hasse-Noether)**.** *Every central simple algebra over an algebraic number field is cyclic, and its index is equal to its exponent.*

In particular, every division algebra over $\mathbb{Q}$ is cyclic. The theorem that follows is basic for our construction – for its proof we refer to [1, p. 98].

Theorem 7 (Albert)**.** *Let E/F be a cyclic extension of commutative fields of degree d. Then the cyclic algebra (E, σ, a) has exponent d if and only if $a \notin N_{L/F}(L^*)$ for each minimal subfield L of E over F.*

Note that in the case F is an algebraic number field, Theorems 6 and 7 give a criterion for (E, σ, a) to be a division algebra.

Given a cyclic algebra $A = (E, \sigma, a)$, we can use the algorithm NORM developed in the previous sections to check if the conditions of Theorem 7 are satisfied.

The minimal subfields of E are in one-to-one correspondence with the maximal subgroups of $\mathrm{Gal}(E/\mathbb{Q})$. For each prime q dividing d, let $H_{d/q} = \langle \sigma^{(q)} \rangle$ denote the unique maximal subgroup of $\mathrm{Gal}(E/\mathbb{Q})$ of order d/q, and let L_q denote the unique minimal subfield of E of degree q corresponding to it. To find L_q, compute

$$h_q(x) = (x - \sigma^q(c))(x - \sigma^{2q}(c)) \cdots (x - \sigma^d(c)). \tag{8}$$

It is a standard fact from Galois theory (see [15, p. 169]) that the coefficients of $h_q(x)$ lie in L_q and they generate L_q over $\mathbb{Q}$. From the minimality of L_q it follows that any coefficient of $h_q(x)$ which does not lie in $\mathbb{Q}$ is a primitive element for L_q over $\mathbb{Q}$. Note that the number of subfields which must be considered is bounded by $\mathrm{size}(d) = \mathrm{size}(n)/2$, since $\lfloor \log d \rfloor$ is an upper bound for the number of prime divisors of d, and $\mathrm{size}(d)$ is equal to $\lfloor \log d \rfloor + 1$.

Acknowledgements

The author is indebted to Professor J.D. Dixon for his invaluable advice and extremely helpful comments. The author also wishes to thank Professor V.L. Plantamura and Professor K.S. Williams for their constant support.

References

1. A.A. Albert, *Structure of algebras,* A.M.S. Colloquium Publications 24, 1961. MR **23:**A912
2. H. Cohen, *A course in computational algebraic number theory,* Springer-Verlag, Berlin, 1993. MR **94i:**11105
3. D.A. Cox, *Primes of the form $x^2 + ny^2$,* John Wiley and Sons, New York, 1989. MR **90m:**11016
4. G. Ivanyos and L. Rónyai, *Finding maximal orders in semisimple algebras over $\mathbb{Q}$,* Comput. Complexity 3 (1993), 245–261. MR **95c:**11154
5. G.J. Janusz, *Algebraic number fields,* Academic Press, London, 1973. MR **51:**3110
6. N. Koblitz, *p-adic Numbers, p-adic Analysis and Zeta Functions,* Springer-Verlag, New York, 1984. MR **86c:**11086
7. S. Lang, *Algebraic number theory,* Addison-Wesley, Reading, Massachusetts, 1970. MR **44:**181
8. H.W. Lenstra, Jr., *Algorithms in algebraic number theory,* Bull. Amer. Math. Soc. 26 (1992), 211-244. MR **93g:**11131
9. K. Mahler, *An inequality for the discriminant of a polynomial,* Michigan Math. J. 11 (1964), 257-262. MR **29:**3465
10. I. Niven and H.S. Zuckerman, *An Introduction to the Theory of Numbers,* John Wiley and Sons, New York, 1980. MR **81g:**10001
11. R.S. Pierce, *Associative Algebras,* Springer-Verlag, Berlin, 1982. MR **84c:**16001
12. M.E. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory,* Cambridge Univ. Press, Cambridge, 1989. MR **92b:**11074
13. L. Rónyai, *Algorithmic properties of maximal orders in simple algebras over $\mathbb{Q}$,* Comput. Complexity 2 (1992), 225–243. MR **94e:**11143
14. B.M. Urazbaev, *On the discriminant of a cyclic field of prime degree,* Izvestiya Akad. Nauk Kazah. SSR 97 (1950), Ser. Math. Meh. 4 (1950), 19-32. MR **15:**403c
15. B.L. van der Waerden, *Algebra, Volume 1,* Springer-Verlag, Berlin, 1991. MR **91h:**00009a

School of Computer Science, Carleton University, Ottawa, Ontario, K1S 5B6, Canada

E-mail address: acciaro@seldi2.uniba.it