BULL. AUSTRAL. MATH. SOC. 11Y40, 11R20
VOL. 52 (1995) [331–340]

FINDING EISENSTEIN ELEMENTS IN CYCLIC NUMBER FIELDS OF ODD PRIME DEGREE

VINCENZO ACCIARO

Let $L = \mathbf{Q}[\alpha]$ be a cyclic number field of odd prime degree q over the field $\mathbf{Q}$ of rationals. In this paper we give an algorithm to compute the discriminant of $L/\mathbf{Q}$, which relies upon a fast method to find Eisenstein elements in L. The algorithm accepts as input the minimal polynomial of α over $\mathbf{Q}$ and a complete factorisation of the discriminant of α, and computes, in time polynomial in the size of the input, a list consisting of all the ramified primes with corresponding Eisenstein elements.

1. INTRODUCTION

Let L be a normal extension of degree q over the rational field $\mathbf{Q}$, where q is an odd prime. Without loss of generality assume that $L = \mathbf{Q}[\alpha]$, where α is an algebraic integer which is given by its minimal polynomial $m_\alpha(x)$ over $\mathbf{Q}$. Clearly the Galois group $Gal(L/\mathbf{Q})$ of L over $\mathbf{Q}$ is cyclic.

In [**1**] we describe an algorithm to determine if a given $a \in \mathbf{Q}$ is the norm of some x in L. The algorithm requires one to know (i) the rational primes $p \neq q$ which ramify in L; (ii) for each ramified prime $p \neq q$ a generator π of the value group of the (unique) valuation that extends the p-adic valuation from $\mathbf{Q}$ to L. Such a π is sometimes called a *prime element* or a *local uniformiser*.

To find the ramified primes, we need the discriminant $D_{L/\mathbf{Q}}$ of the extension $L/\mathbf{Q}$. The discriminant can be computed using a very general algorithm due to Pohst and Zassenhaus [**6**, **9**, **2**, p.297]: this algorithm indeed computes an integral basis $\mathcal{B} = \{\omega_1, \dots, \omega_q\}$ for the extension $L/\mathbf{Q}$, and the discriminant $D_{L/\mathbf{Q}}$.

We show in [**1**] that, if p is a ramified prime not equal to q, then a corresponding local uniformiser π can be found in the set $\{Tr_{L/\mathbf{Q}}(\omega_i) - q\omega_i \mid i = 1 \dots, q\}$, where $Tr_{L/\mathbf{Q}}$ denotes the trace from L to $\mathbf{Q}$.

In this paper we show that, if we do not need an integral basis for $L/\mathbf{Q}$ for other reasons, then the full power of the Pohst-Zassenhaus' algorithm is not required. Indeed, we give an algorithm which takes as input $m_\alpha(x)$ and a complete factorisation of the discriminant $D_{L/\mathbf{Q}}(\alpha)$ of α, and computes in time polynomial in the sise of the input a list consisting of all the ramified primes p with corresponding local uniformisers π.

Received 5th January, 1995
The author wishes to thank Prof. J.D. Dixon for his invaluable advice and extremely helpful comments, and Prof. V.L. Plantamura for his constant support.

1.1 NOTATION.

Let $\mathcal{P}$ be a prime ideal of the ring of algebraic integers $\mathcal{O}$ of L, and let p be a rational prime.

If $a \in L$ and $a \neq 0$, we shall denote by $\nu_{\mathcal{P}}(a)$ the order of a at $\mathcal{P}$, that is, the power of $\mathcal{P}$ in the factorisation of the fractional ideal $a\mathcal{O}$. We define $\nu_{\mathcal{P}}(0)$ to be ∞.

If $a \in \mathbf{Q}$ and $a \neq 0$, then $\nu_p(a)$ will denote the order of a at p, that is, the power of the ideal $p\mathbf{Z}$ in the factorisation of the fractional ideal $a\mathbf{Z}$. We define $\nu_p(0)$ to be ∞.

$\mathbf{Q}_p$ will denote the field of p-adic numbers, and $L_{\mathcal{P}}$ will denote the completion of L with respect to the valuation determined by $\mathcal{P}$. Then $\mathbf{Z}_p$ will denote the ring of p-adic integers, that is $\{x \in \mathbf{Q}_p \mid \nu_p(x) \geqslant 0\}$, and $\mathcal{O}_{\mathcal{P}}$ the ring of $\mathcal{P}$-adic integers, that is $\{x \in L_{\mathcal{P}} \mid \nu_{\mathcal{P}}(x) \geqslant 0\}$.

Finally, $\mathbf{F}_p$ will denote the finite field of p elements, and $\mathbf{F}_p^*$ its multiplicative group.

2. THE METHOD

Cyclic extension of the rationals of prime power degree have been intensively studied by B.M. Urazbaev. In [7] he proved the following:

LEMMA 1. *The discriminant $D_{L/\mathbf{Q}}$ of a cyclic extension $L/\mathbf{Q}$ of odd prime degree q has the form:*

$$D_{L/\mathbf{Q}} = q^a \prod p_i^{q-1}$$

where the p_i are distinct rational primes of the form $nq+1$, and $a = 0$ or $a = 2(q-1)$.

Clearly, $D_{L/\mathbf{Q}} \mid D_{L/\mathbf{Q}}(\alpha)$. Now, let

$$D_{L/\mathbf{Q}}(\alpha) = q^a \prod_{p_i \in S} p_i^{k_i}$$

be a complete factorisation of $D_{L/\mathbf{Q}}(\alpha)$ into primes, with $p_i \neq p_j$ for $i \neq j$, and $a \geqslant 0$. For each $p_i \in S$ we have to decide if p_i ramifies in L, that is, if $p_i \mid D_{L/\mathbf{Q}}$.

Firstly, by Urazbaev's criterion, we can ignore those primes $p_i \in S$ for which either $p_i \not\equiv 1 \pmod q$ or $k_i < q-1$.

Secondly, we take into account the fact that $L/\mathbf{Q}$ is Galois. This implies that all the ideals of $\mathcal{O}$ lying above $p\mathbf{Z}$ (where p is a rational prime) are conjugate under $Gal(L/\mathbf{Q})$ and so they have the same ramification index e and the same inertial degree f. Let g be the number of distinct prime ideals lying above $p\mathbf{Z}$. From the formula $efg = [L : \mathbf{Q}] = q$ and the primality of q, it follows that, either p *splits completely in* L $(e = 1,\ f = 1$ and $g = q)$, or p *is inert in* L $(e = 1,\ f = q$ and $g = 1)$, or p

https://doi.org/10.1017/S0004972700014763 Published online by Cambridge University Press

is totally ramified in L $(e = q,\ \ f = 1$ and $g = 1)$. In this section we show how to recognise when p is inert.

By assumption $\alpha \in \mathcal{O}$, and therefore the coefficients of $m_\alpha(x)$ lie in $\mathbf{Z}$. The next lemma relates the decomposition of a prime p in L to the factorisation of $m_\alpha(x)$ over $\mathbf{F}_p$.

LEMMA 2. *Let* L *be a cyclic extension of* $\mathbf{Q}$*, of odd prime degree* q*. Let* p *be a rational prime, and* α *be an algebraic integer in* $L \backslash \mathbf{Z}$*. If* p *ramifies in* L*, then the minimal polynomial* $m_\alpha(x)$ *of* α *over* $\mathbf{Q}$ *splits into the product of* q *identical linear factors over* $\mathbf{F}_p$*.*

PROOF: Let us assume that p ramifies in L. Then $m_\alpha(x)$ is irreducible over $\mathbf{Q}_p$ (see [**4**, Theorem 5.1.5, p.75]), and therefore by Hensel's Lemma it is either irreducible or a q^{th} power over $\mathbf{F}_p$. However, it can be shown that if $m_\alpha(x)$ is irreducible over $\mathbf{F}_p$ then p must be inert (see [**3**, Proposition 5.11, p.102]). Hence $m_\alpha(x)$ must split into the product of q identical linear factors over $\mathbf{F}_p$. ∎

To apply Lemma 2, we compute $l(x) = GCD(x^p - x, m_\alpha(x))$ over $\mathbf{F}_p$. Then $m_\alpha(x)$ is a q^{th} power over $\mathbf{F}_p$ precisely when $\deg l(x) = 1$ and $l(x)^q \equiv m_\alpha(x) \pmod p$. In practice we compute $j(x) = x^p \bmod m_\alpha(x)$ in $\mathbf{F}_p$, using the binary powering algorithm [**2**, p.8]. Then $l(x)$ is given by $GCD(j(x) - x, m_\alpha(x))$.

Unfortunately, the previous lemma gives only a necessary condition for a prime p to ramify in L. In the next section we shall develop some some necessary and sufficient conditions.

3. EISENSTEIN POLYNOMIALS

Let us assume that p is totally ramified, and let $\mathcal{P}$ be the unique prime ideal lying above $p\mathbf{Z}$. Since there is only one extension of the p-adic valuation from $\mathbf{Q}$ to L, if $\theta \in L$ we must have [**8**, Corollary 2.5.8, p.68]

$$\nu_{\mathcal{P}}(\theta) = \nu_p\Big(N_{L/\mathbf{Q}}(\theta)\Big). \tag{1}$$

We shall use this fact often in the following.

In particular, if $\theta \in \mathcal{P} \backslash \mathcal{P}^2$, then $\nu_p\Big(N_{L/\mathbf{Q}}(\theta)\Big) = \nu_{\mathcal{P}}(\theta) = 1$. This shows that if p is ramified, then $\mathcal{O}$ contains elements whose norms have p-order equal to 1. On the other hand

LEMMA 3. *If a rational prime* p *is inert in* L *then there is no* $\theta \in \mathcal{O} \backslash \mathbf{Z}$ *whose norm has* p*-order 1.*

PROOF: Assume that $\theta \in \mathcal{O} \backslash \mathbf{Z}$ is an element whose norm has p-order 1. If $\theta_1, \theta_2, \dots, \theta_q$ denote the conjugates of θ, with $\theta = \theta_1$ say, then $N_{L/\mathbf{Q}}(\theta) = \theta_1 \theta_2 \cdots \theta_q$.

Since p is inert, $p\mathcal{O}$ is the only prime ideal of $\mathcal{O}$ lying above $p\mathbf{Z}$. By assumption $\theta_1\theta_2\cdots\theta_q \in p\mathbf{Z} \subset p\mathcal{O}$, and hence, since $p\mathcal{O}$ is a prime ideal, some conjugate of θ must lie in $p\mathcal{O}$. But then, since $p\mathcal{O}$ is σ-invariant, all the conjugates of θ must lie in $p\mathcal{O}$, and therefore $N_{L/\mathbf{Q}}(\theta) \in p^q\mathcal{O} \cap \mathbf{Z} = p^q\mathbf{Z}$, against our assumption. ∎

Theorem 1. *Let p be a rational prime. Assume that there is an element $\theta \in \mathcal{O}\backslash\mathbf{Z}$ whose norm has p-order 1. Then p ramifies in L if and only if $m_\theta(x)$ is Eisenstein at p.*

Proof: By Lemma 3, the existence of $\theta \in \mathcal{O}\backslash\mathbf{Z}$ whose norm has p-order 1 implies that p cannot be inert.

Assume first that $m_\theta(x)$ is Eisenstein at p. Then $m_\theta(x)$ is irreducible in $\mathbf{Q}_p[x]$, and θ generates a totally ramified extension of $\mathbf{Q}_p$ of degree q, that is, p is totally ramified (see [**5**, Proposition 11, p.52]).

Conversely, assume that p ramifies in L. Then $\nu_{\mathcal{P}}(\theta) = \nu_p\Big(N_{L/\mathbf{Q}}(\theta)\Big) = 1$. Since $Gal(L/\mathbf{Q})$ permutes the prime ideals lying above $p\mathbf{Z}$ transitively, and there is only one prime ideal $\mathcal{P}$ above $p\mathbf{Z}$, it follows that $\nu_{\mathcal{P}}(\sigma(\theta)) = 1$ for all $\sigma \in Gal(L/\mathbf{Q})$. Let

$$m_\theta(x) = x^q + b_{q-1}x^{q-1} + \ldots + b_1x + b_0.$$

Then each b_i lies in $\mathbf{Z}$ and is an elementary symmetric function of the set $\{\theta, \sigma(\theta), \ldots, \sigma^{q-1}(\theta)\}$, where σ is any generator of $Gal(L/\mathbf{Q})$. Hence $b_i \in \mathcal{P} \cap \mathbf{Z} = p\mathbf{Z}$. Moreover

$$\nu_p(b_0) = \nu_p\big(\theta\sigma(\theta)\cdots\sigma^{q-1}(\theta)\big) = 1,$$

which shows that $m_\theta(x)$ is Eisenstein at p. ∎

In order to apply Theorem 1, we need an efficient algorithm to solve the following problem: *find an element of $\mathcal{O}$ whose norm has p-order 1.* The next lemma shows that it is enough to find any algebraic integer whose norm has p-order not divisible by q.

Lemma 4. *Let p be a ramified prime. Given $\gamma' \in \mathcal{O}$ with $q \nmid \nu_p\Big(N_{L/\mathbf{Q}}(\gamma')\Big)$, we can construct an element $\gamma \in \mathcal{O}$ with $\nu_p\Big(N_{L/\mathbf{Q}}(\gamma)\Big) = 1$.*

Proof: Let $r = \nu_p\Big(N_{L/\mathbf{Q}}(\gamma')\Big)$. Since $N_{L/\mathbf{Q}}(p) = p^q$, and the norm elements form a multiplicative group, we can find an $s \in \mathbf{N}$ which acts as a multiplicative inverse of $r \pmod q$, that is, such that $rs = 1 + ql$ $(l \in \mathbf{N})$. Let $\gamma = (\gamma')^s/p^l$. Clearly

$$\nu_p\Big(N_{L/\mathbf{Q}}(\gamma)\Big) = s\ \nu_p\Big(N_{L/\mathbf{Q}}(\gamma')\Big) - lq\ \nu_p(p) = 1$$

and therefore $\nu_{\mathcal{P}}(\gamma) = 1$. It is left to prove that $\gamma \in \mathcal{O}$. Clearly, $(\gamma')^s \in \mathcal{O}$. Let $\mathcal{P}$ be the unique prime ideal of $\mathcal{O}$ lying above $p\mathbf{Z}$. Now, $\nu_{\mathcal{P}}\big((\gamma')^s/p^l\big) = 1$, and $\nu_{\mathcal{Q}}\big((\gamma')^s/p^l\big) = \nu_{\mathcal{Q}}\big((\gamma')^s\big) \geqslant 0$ for any prime ideal $\mathcal{Q}$ of $\mathcal{O}$ not equal to $\mathcal{P}$. Therefore $(\gamma')^s/p^l \in \mathcal{O}$ (see [**8**, Corollary 4.1.8, p.125]). ∎

4. Finding Eisenstein elements

We shall continue to assume that p is ramified. The inertia group $I_{\mathcal{P}}$ of $\mathcal{P}$ has order $e = q$ (see [4, Corollary 5.4.5, p.83]), and so it must be equal to $Gal(L/\mathbf{Q})$. Thus, if $\sigma \in Gal(L/\mathbf{Q})$ and $\beta \in \mathcal{O}$, we must have $\sigma(\beta) - \beta \in \mathcal{P}$. We shall use this fact often, in the following.

Let us consider the embedding $\mathcal{O} \hookrightarrow \mathcal{O}_{\mathcal{P}}$. For this purpose, we fix, *once for all,* an element $\pi \in \mathcal{P} \setminus \mathcal{P}^2$, and we take $R = \{0, 1, \dots, p-1\}$ to be a set of representatives of $\mathcal{O}/\mathcal{P}$ in $\mathcal{O}$. Every $\beta \in \mathcal{O}_{\mathcal{P}}$ can be written as a convergent series (in the $\mathcal{P}$-adic metric)

$$\beta = \sum_{i=0}^{\infty} \sum_{j=0}^{q-1} a_{i,j} p^i \pi^j \qquad (a_{i,j} \in R)$$

where the coefficients $a_{i,j}$ are uniquely determined by β.

Moreover, if $\beta \in \mathcal{O} \setminus \mathbf{Z}$, then for some $h, k \in \mathbf{N}$, with $0 < k < q$ we must have

(i) $a_{h,k} \neq 0$; and

(ii) $a_{i,j} = 0$ whenever ($i < h$ and $0 < j < q$) or ($i = h$ and $0 < j < k$).

for otherwise, using the fact that $ef = [L_{\mathcal{P}} : \mathbf{Q}_p] = q = [L : \mathbf{Q}]$, the element β would be a p-adic integer in $\mathcal{O}$, and therefore an element of $\mathbf{Z}$.

We define now a function $\Lambda : \mathcal{O} \to \mathcal{O}$ as follows: if β, h, k are as above, then

$$\Lambda(\beta) = \sum_{j=k}^{q-1} a_{h,j} p^h \pi^j + \sum_{i=h+1}^{\infty} \sum_{j=0}^{q-1} a_{i,j} p^i \pi^j.$$

Since σ fixes p and any element of R, clearly we have

Lemma 5. *Let $\beta \in \mathcal{O}$. If $\sigma \in Gal(L/\mathbf{Q})$ then $\sigma(\beta) - \beta = \sigma(\Lambda(\beta)) - \Lambda(\beta)$.*

4.1 p is totally and tamely ramified.

In this section we assume that p is ramified and $p \neq q$, and we let $\mathcal{P}$ denote the unique ideal of $\mathcal{O}$ above $p\mathbf{Z}$.

Lemma 6. *Let σ be a generator of $Gal(L/\mathbf{Q})$. Then $\nu_{\mathcal{P}}(\sigma(\pi) - \pi) = 1$.*

Proof: Since $\{1, \pi, \dots, \pi^{q-1}\}$ is a local basis at p, we must have (see [8, Proposition 4.8.18, p.164])

$$\nu_{\mathcal{P}}\Big(D_{L/\mathbf{Q}}(\pi)\Big) = \nu_{\mathcal{P}}\Big(D_{L/\mathbf{Q}}\Big) = q - 1.$$

But $D_{L/\mathbf{Q}}(\pi) = N_{L/\mathbf{Q}}(m'_\pi(\pi))$, and

$$\nu_{\mathcal{P}}\Big(N_{L/\mathbf{Q}}(m'_\pi(\pi))\Big) = \nu_{\mathcal{P}}(m'_\pi(\pi)) = \nu_{\mathcal{P}}\big((\sigma(\pi) - \pi) \cdots (\sigma^{q-1}(\pi) - \pi)\big).$$

https://doi.org/10.1017/S0004972700014763 Published online by Cambridge University Press

Each factor on the right hand side has $\mathcal{P}$-order greater than zero, there are $q-1$ factors, and so by the pigeon hole principle $\nu_{\mathcal{P}}(\sigma(\pi)-\pi)$ must be 1. ∎

Lemma 7. *Let σ be a generator of $Gal(L/\mathbf{Q})$. If $0<r<q$ then $\nu_{\mathcal{P}}(\sigma(\pi^r)-\pi^r) = r$.*

Proof: Since $\mathcal{P}$ and all its powers are σ-invariant, it follows that $\sigma(\pi) \equiv a\pi \pmod{\mathcal{P}^2}$, with $0<a<p$. Then $\sigma^2(\pi) \equiv a\sigma(\pi) \pmod{\mathcal{P}^2}$, that is, $\sigma^2(\pi) \equiv a^2\pi \pmod{\mathcal{P}^2}$, and more generally $\sigma^i(\pi) \equiv a^i\pi \pmod{\mathcal{P}^2}$. But $\sigma^q(\pi)=\pi$, and so $a^q \equiv 1 \pmod{p}$. Therefore the order of a in $\mathbf{F}_p^*$ must divide q. Since q is prime and $a \not\equiv 1 \pmod{p}$ by Lemma 6, the order of a in $\mathbf{F}_p^*$ must be equal to q. If $0<r<q$, then

$$\sigma(\pi^r)-\pi^r = \sigma(\pi)^r - \pi^r \equiv a^r\pi^r - \pi^r \pmod{\mathcal{P}^{r+1}}$$

with $a^r \not\equiv 1 \pmod{p}$, which proves the assertion. ∎

Corollary 1. *Let σ be a generator of $Gal(L/\mathbf{Q})$. If $\beta \in \mathcal{O}\backslash\mathbf{Z}$, then*

$$\nu_{\mathcal{P}}(\sigma(\Lambda(\beta))-\Lambda(\beta)) = \nu_{\mathcal{P}}(\Lambda(\beta)).$$

In particular, $q \nmid \nu_{\mathcal{P}}(\sigma(\Lambda(\beta))-\Lambda(\beta))$.

Proof: Define a function $F: L \to L$ by $F(x)=\sigma(x)-x$. Since F is $\mathbf{Z}$-linear, we have

$$\begin{aligned} F(\Lambda(\beta)) &= F\left(\sum_{j=k}^{q-1} a_{h,j}p^h\pi^j + \sum_{i=h+1}^{\infty}\sum_{j=0}^{q-1} a_{i,j}p^i\pi^j\right) \\ &= \sum_{j=k}^{q-1} F\big(a_{h,j}p^h\pi^j\big) + F\left(\sum_{i=h+1}^{\infty}\sum_{j=0}^{q-1} a_{i,j}p^i\pi^j\right) \\ &= \sum_{j=k}^{q-1} F\big(a_{h,j}p^h\pi^j\big) + F(t) \end{aligned}$$

with $t = \sum_{i=h+1}^{\infty}\sum_{j=0}^{q-1} a_{i,j}p^i\pi^j$. Now, $\nu_{\mathcal{P}}(t) \geqslant (h+1)q$, and so $\nu_{\mathcal{P}}(F(t)) \geqslant (h+1)q$.

Note that $\nu_{\mathcal{P}}\big(F\big(a_{h,j}p^h\pi^j\big)\big) = qh+j$ $(j=k,\dots,q-1)$ if $0<a_{h,j}<p$, and $\nu_{\mathcal{P}}\big(F\big(a_{h,j}p^h\pi^j\big)\big) = \infty$ if $a_{h,j}=0$. Clearly $0<a_{h,k}<p$, by the definition of the function Λ, and so $\nu_{\mathcal{P}}\left(\sum_{j=k}^{q-1} F\big(a_{h,j}p^h\pi^j\big)\right) = hq+k$. Therefore $\nu_{\mathcal{P}}(F(\Lambda(\beta))) = hq+k = \nu_{\mathcal{P}}(\Lambda(\beta))$. ∎

Theorem 2. *If $\beta \in \mathcal{O}\backslash \mathbf{Z}$ then $q \nmid \nu_{\mathcal{P}}\left(m'_\beta(\beta)\right)$.*

Proof: By Lemma 5, if σ denotes a generator of $Gal(L/\mathbf{Q})$, we have

$$\begin{aligned} m'_\beta(\beta) &= (\sigma(\beta)-\beta)\cdots(\sigma^{q-1}(\beta)-\beta) \\ &= (\sigma(\Lambda(\beta))-\Lambda(\beta))\cdots(\sigma^{q-1}(\Lambda(\beta))-\Lambda(\beta)) \end{aligned}$$

By Corollary 1, then $\nu_{\mathcal{P}}\left(m'_\beta(\beta)\right) = (q-1)\nu_{\mathcal{P}}(\Lambda(\beta))$. Since $q \nmid \nu_{\mathcal{P}}(\Lambda(\beta))$, it follows that $q \nmid \nu_{\mathcal{P}}\left(m'_\beta(\beta)\right)$. ∎

4.2 p IS TOTALLY AND WILDLY RAMIFIED.

In this section we assume that p is ramified and $p = q$, and we let $\mathcal{P}$ denote the unique ideal of $\mathcal{O}$ above $q\mathbf{Z}$. Define a function $G : L \to L$ by $G(x) = Tr_{L/\mathbf{Q}}(x) - qx$. Clearly, G is $\mathbf{Z}$-linear and it vanishes on $\mathbf{Q}$.

Lemma 8. *Let $0 < r < q$. Then $G(\pi^r) \equiv aq - q\pi^r \pmod{\mathcal{P}^{2q}}$, with $0 \leqslant a < q$.*

Proof: Since $Tr_{L/\mathbf{Q}}(\pi^r) \in q\mathbf{Z}$, we can write $Tr_{L/\mathbf{Q}}(\pi^r) \equiv aq \pmod{q^2}$, with $0 \leqslant a < q$. This proves the assertion. ∎

Theorem 3. *If $\beta \in \mathcal{O}\backslash \mathbf{Z}$, then $G(\beta) = G(\Lambda(\beta))$ and*

$$G(\beta) \equiv bq^{h+1} - cq^{h+1}\pi^k \pmod{\mathcal{P}^{(h+1)q+k+1}}$$

with $0 \leqslant b < q$ and $0 < c < q$.

Proof: Since the function G is $\mathbf{Z}$-linear, and it vanishes on $\mathbf{Q}$, we have

$$\begin{aligned} G(\beta) &= G(\Lambda(\beta)) \\ &= G\left(\sum_{j=k}^{q-1} a_{h,j}q^h\pi^j + \sum_{i=h+1}^{\infty}\sum_{j=0}^{q-1} a_{i,j}q^i\pi^j\right) \\ &= \sum_{j=k}^{q-1} G\left(a_{h,j}q^h\pi^j\right) + G\left(\sum_{i=h+1}^{\infty}\sum_{j=0}^{q-1} a_{i,j}q^i\pi^j\right) \\ &= \sum_{j=k}^{q-1} G\left(a_{h,j}q^h\pi^j\right) + \sum_{j=0}^{q-1} G\left(a_{h+1,j}q^{h+1}\pi^j\right) + G(t) \end{aligned}$$

with $t = \sum_{i=h+2}^{\infty}\sum_{j=0}^{q-1} a_{i,j}q^i\pi^j$. Now, $\nu_{\mathcal{P}}(t) \geqslant (h+2)q$, and so $\nu_{\mathcal{P}}(G(t)) \geqslant (h+2)q$. Also, by Lemma 8, $\nu_{\mathcal{P}}\left(G\left(a_{h+1,j}q^{h+1}\pi^j\right)\right) \geqslant q(h+2)$ $(j = 0, \dots, q-1)$, and

$$G\left(a_{h,k}q^h\pi^k\right) \equiv b_k q^{h+1} - c_k q^{h+1}\pi^k \pmod{\mathcal{P}^{(h+2)q}}$$

https://doi.org/10.1017/S0004972700014763 Published online by Cambridge University Press

with $c_k \not\equiv 0 \pmod q$, since $a_{h,k} \not\equiv 0 \pmod q$ by the definition of the function Λ. Moreover, if $a_{h,s} \not\equiv 0 \pmod q$ $(s = k+1, \dots, q-1)$ then

$$G(a_{h,s}q^h\pi^s) \equiv b_s q^{h+1} - c_s q^{h+1}\pi^s \quad \left(\mathrm{mod}\ \mathcal{P}^{(h+2)q}\right).$$

This shows that

$$G(\beta) \equiv q^{h+1}\left(\sum_{i=k}^{q-1} b_i\right) - q^{h+1}c_k\pi^k \quad \left(\mathrm{mod}\ \mathcal{P}^{(h+1)q+k+1}\right)$$

with $c_k \not\equiv 0 \pmod q$. To prove our assertion, let $b = \sum_{i=k}^{q-1} b_i \bmod q$, and $c = c_k$. □

We show next how Theorem 3 can be used to obtain an algebraic integer whose norm has q-order not divisible by q. Let $w = \nu_q\left(N_{L/\mathbf{Q}}(G(\beta))\right)/q$.

If $w \notin \mathbf{Z}$ then $b \equiv 0 \pmod q$, and $G(\beta)$ is the desired element.

Otherwise, $w = h+1$, and $G(\beta)/q^w \equiv b - c\pi^k \left(\mathrm{mod}\ \mathcal{P}^{k+1}\right)$. Note that $G(\beta)/q^w \in \mathcal{O}$, since $\nu_{\mathcal{P}}(G(\beta)/q^w) = 0$ and $\nu_{\mathcal{Q}}(G(\beta)/q^w) = \nu_{\mathcal{Q}}(G(\beta)) \geqslant 0$, when $\mathcal{Q}$ is any prime ideal of $\mathcal{O}$ not equal to $\mathcal{P}$ (use again [**8**, Corollary 4.1.8, p.125]). Let $\rho = G(\beta)/q^w$. It is easily seen that, if

$$m_{G(\beta)}(x) = x^q + b_{q-1}x^{q-1} + \dots + b_1 x + b_0$$

then

$$m_\rho(x) = x^q + (b_{q-1}/q^w)x^{q-1} + \dots + \left(b_1/q^{w(q-1)}\right)x + (b_0/q^{wq})$$

Since q is assumed to be ramified, $m_\rho(x) \equiv (x - \widehat{s})^q \pmod q$. Let s be a representative of the residue class of $\widehat{s}$. Then $\rho - s \equiv -c\pi^k \left(\mathrm{mod}\ \mathcal{P}^{k+1}\right)$, and so $\rho - s$ is the desired element.

The pseudo code for the algorithm is sketched in Figures 1 and 2. The algorithm EISENSTEIN takes as input $m_\alpha(x)$ and returns a list consisting of the ramified primes and corresponding local uniformisers. If the factorisation of $D_{L/\mathbf{Q}}(\alpha)$ is given as part the input, the entire algorithm runs in polynomial time.

```
procedure CONSTRUCT(γ, p):
    let r = ν_p(N_{L/Q}(γ));
    find l, s ∈ N such that rs = 1 + ql;
    let ε = (γ)^s / p^l;
    if m_ε(x) is Eisenstein at p then return(ε); endif;
    return(0);
```

Figure 1: Pseudo Code for the Algorithm CONSTRUCT.

https://doi.org/10.1017/S0004972700014763 Published online by Cambridge University Press

```
procedure EISENSTEIN(m_α(x)):
    let List = ∅;
    let D_{L/Q}(α) = q^a ∏_{p_i∈S} p_i^{k_i};
    for all the p ∈ S do
        if (p_i ≡ 1 (mod q) and k_i ≥ q − 1
          and m_α(x) is a q^th power over F_p) then
          let γ = m'_α(α);
          let π = CONSTRUCT(γ, p);
          if π ≠ 0 then add {p, π} to List; endif;
        endif;
    endfor;
    if a < 2(q − 1) then return(List); endif;
    if m_α(x) is not a q^th power over F_q then return(List); endif;
    let δ = Tr_{L/Q}(α) − qα;
    let w = ν_q(N_{L/Q}(δ))/q;
    if w ∉ Z then
        let γ = δ;
    else
        let ρ = δ/q^w, and compute m_ρ(x);
        if m_ρ(x) ∉ Z[x] then return(List); endif;
        compute c(x) = GCD(x^q − x, m_ρ(x)) over F_q.
        if c(x) ≠ x − s then return(List); endif;
        let γ = ρ − s;
        if q | ν_q(N_{L/Q}(γ)) then return(List); endif;
    endif;
    let π = CONSTRUCT(γ, q);
    if π ≠ 0 then add {q, π} to List; endif;
    return(List);
```

Figure 2: Pseudo Code for the Algorithm EISENSTEIN.

References

[1] V. Acciaro, 'Solvability of norm equations over Abelian number fields of prime degree", (manuscript, 1994).

[2] H. Cohen, *A course in computational algebraic number theory* (Springer-Verlag, Berlin, Heidelberg, New York, 1993).

[3] D.A. Cox, *Primes of the form* $x^2 + ny^2$ (John Wiley and Sons, New York, 1989).

[4] L.J. Goldstein, *Analytic number theory* (Prentice-Hall, Englewood Cliffs, New Jersey, 1971).

[5] S. Lang, *Algebraic number theory* (Addison-Wesley, Reading, Massachusetts, 1970).

[6] M.E. Pohst, 'Three principal tasks of computational algebraic number theory', in *Number*

https://doi.org/10.1017/S0004972700014763 Published online by Cambridge University Press

theory and applications, Proc. NATO Advanced Study Inst. (Kluwer Academic Publisher, 1989), pp. 123–133.

[7] B.M. Urazbaev, 'On the discriminant of a cyclic field of prime degree', *Izv. Akad. Nauk Kazah. SSR Math. Meh.* 4 (1950), 19–32.

[8] E. Weiss, *Algebraic number theory* (McGraw-Hill, New York, 1963).

[9] H. Zassenhaus, 'Ein Algorithmus zur Berechnung einer Minimalbasis über gegebener Ordnung', *Funktsional Anal.* (1967), 90–103.

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