LMS J. Comput. Math. 19 (Special issue A) (2016) 178–195 © 2016 Authors
doi:10.1112/S1461157016000310

Division algebras and maximal orders for given invariants

Gebhard Böckle and Damián Gvirtz

Abstract

Brauer classes of a global field can be represented by cyclic algebras. Effective constructions of such algebras and a maximal order therein are given for $\mathbb{F}_q(t)$, excluding cases of wild ramification. As part of the construction, we also obtain a new description of subfields of cyclotomic function fields.

1. *Introduction*

Let F be a global function field and S a finite set of places of F. For each $v \in S$ let $s_v = n_v/r_v$ be a reduced fraction in $\mathbb{Q}$ such that for their classes in $\mathbb{Q}/\mathbb{Z}$ we have

$$\sum_{v \in S} s_v \equiv 0 \mod \mathbb{Z}. \tag{1.1}$$

We extend $(s_v)_v$ to a sequence of invariants ranging over all places of F, by setting $s_v = 0/1$ whenever v does not lie in S.

Denote by $\mathrm{Br}(K)$ the Brauer group of a field K; see [**13**, Theorem 28.2]. For any place v of F, denote by F_v the completion of F at v. Then as a consequence of Hasse's main theorem on the theory of algebras (cf. [**13**, Remarks 32.12]), one has a short exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{Br}(F) \arrow[r, "{[A]\mapsto[A\otimes_F F_v]_v}"] & \coprod_v \mathrm{Br}(F_v) \arrow[r, "{(\alpha_v)\mapsto\sum_v \mathrm{inv}_v}"] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0, \end{tikzcd} \tag{1.2}$$

for suitably defined local isomorphisms $\mathrm{inv}_v \colon \mathrm{Br}(F_v) \to \mathbb{Q}/\mathbb{Z}$. Hence, given any sequence $(s_v)_v$ as in the previous paragraph, there exists a unique class in $\mathrm{Br}(F)$ with this set of invariants, that is, up to isomorphism, a unique division algebra D with this set of invariants. Moreover, the Grunwald–Wang theorem implies that D can be written in the form of a cyclic algebra.

For the rest of this paper, let F be the field $\mathbb{F}_q(t)$ where $\mathbb{F}_q$ denotes the finite field of q elements and q is a power of a prime p. The aim of this paper is to effectively construct a cyclic algebra, starting only with its invariants (with the restriction that $s_\infty = 0$), and once this has been achieved, to find a maximal $\mathbb{F}_q[t]$-order in it. Our approach will work whenever q is prime to the denominators of any invariant. For division quaternion algebras and q odd, [**2**, § 4] gives a different algorithm. We note that in our setting there is a unique maximal order up to conjugation; see Theorem 9. Besides, we also provide a Kummer theory way of calculating a subfield of a cyclotomic function field, which to our knowledge is new and computationally performs better than more naive approaches.

Our method can be adapted to $F = \mathbb{Q}$, as we have checked, and with some refinements probably also to all global function fields (and any fixed place ∞). This would make $s_\infty = 0$

Received 21 February 2016.

Contributed to the Twelfth Algorithmic Number Theory Symposium (ANTS-XII), Kaiserslautern, Germany, 29 August–2 September 2016.

GB was supported by the DFG within the SPP1489 and the FG1920. DG was supported by a Gerhard C. Starck Scholarship.

superfluous when constructing D; the condition $s_\infty = 0$ is needed to have a maximal $\mathbb{F}_q[t]$-order. We focus on $F = \mathbb{F}_q(t)$ for two reasons. First, our interest in having access to explicit models of maximal $\mathbb{F}_q[t]$-orders Λ for a fixed set of invariants stems from planned experimental investigations of certain function field automorphic forms for $F = \mathbb{F}_q(t)$, namely harmonic cochains on Bruhat–Tits buildings that are equivariant for a suitable action of Λ. Second, we wish to focus on the division algebra aspect and not aspects related to Dedekind domains for general global function fields.

Our algorithm to find D cannot be extended to the case where p divides some r_v. The general case can be split into the case we treat, the *tame case*, and the *wild case*: one can write each s_v as a sum $s_{v,p} + s_v^p$ where the denominator of the first is a power of p and that of the second is prime to p. We provide a solution D^p for the sequence (s_v^p). If one has an algorithm that gives D_p as a cyclic algebra for sequences $(s_{v,p})$, the general solution arises via $D_p \otimes_F D^p$. An algorithm for the latter case requires one to consider extensions L/F that have wild ramification at all $v \in S$. We have not worked out details. Once D_p has been constructed, further methods are required to find a maximal order in it. Similar complications arise over $F = \mathbb{Q}$ when Hasse invariants contain powers of 2 in the denominator.

Magma code for all constructions is available from https://github.com/dgvirtz/divalg.

2. *Central simple algebras*

This section reviews well-known basic results on central simple algebras. Basic references are [8, 13].

2.1. *Cyclic algebras*

Let K be a field and L/K be a Galois extension with cyclic Galois group of order d with a chosen generator σ. Pick an element $a \in K^*$.

Definition 1. The (non-commutative) cyclic algebra attached to L/K, σ and a is

$$(L/K, \sigma, a) := L[\tau, \tau^{-1}]/(\tau^d - a)L[\tau, \tau^{-1}],$$

where multiplication in the Laurent polynomial ring $L[\tau, \tau^{-1}] = \bigoplus_{n\in\mathbb{Z}} L\tau^n$ is defined by

$$\alpha\tau^n \cdot \beta\tau^m = \alpha\sigma^n(\beta)\tau^{n+m} \quad \text{for } \alpha, \beta \in L,\ n, m \in \mathbb{Z}.$$

It is an L-vector space with basis $\{\tau^i \mid i = 0, \ldots, d-1\}$. It is also a K-algebra, by identifying K with the central subfield $K\tau^0$. From [13, Theorems 30.3 and 29.6] we infer that $(L/K, \sigma, a)$ is a central simple algebra over K, and that $\{\alpha_i\tau^j \mid i, j = 0, \ldots, d-1\}$ is a K-basis for every K-basis $\alpha_0, \ldots, \alpha_{d-1}$ of L.

We recall some basic properties of cyclic algebras for K and L fixed.

Theorem 2 [13, Theorem 30.4]. *The following hold:*

(i) $(L/K, \sigma, a) \cong (L/K, \sigma^s, a^s)$ *for any* $s \in \mathbb{Z}$ *with* $\gcd(s, d) = 1$*;*
(ii) $(L/K, \sigma, a) \cong M_n(K)$ *if and only if* $a \in \mathrm{Norm}_{L/K}(L^*)$*.*

The following result is useful, for instance, when passing from K to its completion.

Theorem 3 [13, Theorem 30.8]. *Let* $K' \supset K$ *be any field extension; denote by* L' *a splitting field over* K' *of the minimal polynomial over* K *of any primitive element for* L/K*, so that* $H := \mathrm{Gal}(L'/K')$ *is naturally a subgroup of* $\mathrm{Gal}(L/K)$*. Let* $k = \min\{n \in \mathbb{N}_{>0} \mid \sigma^n \in H\}$*. Then*

$$K' \otimes_K (L/K, \sigma, a) \sim (L'/K', \sigma^k, a).$$

In particular, $L \otimes_K (L/K, \sigma, a)$ *is trivial in* $\mathrm{Br}(L)$*.*

https://doi.org/10.1112/S1461157016000310 Published online by Cambridge University Press

2.2. *The Hasse invariant of a local algebra*

In this subsection, K denotes a complete discrete-valued field with respect to a valuation $v = v_K$, with ring of integers $\mathcal{O}$ and finite residue field k. By π we denote a uniformizer. For an unramified extension W/K of finite degree with residue field k', the Frobenius automorphism $\sigma \in \operatorname{Gal}(W/K)$ is the unique automorphism whose restriction to $\operatorname{Gal}(k'/k)$ is given by $x \mapsto x^{\#k}$. For the definition of the Hasse invariant, consult [13, Theorems 14.3, 14.5 and footnote p. 148].

THEOREM 4 [13, Theorem 31.5]. *Let W and W' be unramified extensions of K of degrees d and d'. Denote by σ, σ' the respective Frobenius automorphisms, and let s, s' be in $\mathbb{Z}$ such that $s/d = s'/d'$. Then*

$$(W/K, \sigma, \pi^s) \sim (W'/K, \sigma', \pi^{s'}).$$

The following result is basic to determine the invariant of a cyclic algebra over a local field.

THEOREM 5. *Let W/K be an unramified extension of degree d. Denote by $\sigma \in \operatorname{Gal}(W/K)$ the Frobenius automorphism. Let a be in K^* and let D be the division algebra equivalent to $(W/K, \sigma, a)$ in $\operatorname{Br}(K)$. Then the Hasse invariant satisfies*

$$\operatorname{inv}_K D = \frac{v_K(a)}{d}.$$

Proof. We indicate how to deduce this standard fact (for example, [11, 31.4]) from the definition of the Hasse invariant given in [13]. There $\operatorname{inv}_K D$ is defined in [13, footnote p. 148] as r/d provided that $\pi_D \omega \pi_D^{-1} = \omega^{q^{r'}}$ for some r' with $rr' \equiv 1 \pmod{d}$, where ω is a primitive $(q^d - 1)$th root of unity in D and $\pi_D \in D$ with π_D^d a uniformizer of $K \subset D$.

Define $d'' := \gcd(v_K(a), d)$ and $d' := d/d''$, and denote by W' the unique subfield of W with degree d' over K, and by $\sigma' \in \operatorname{Gal}(W'/K)$ the Frobenius automorphism on W'. Then by Theorems 2, 4 and $N_{W/K}(W^*) \subset \mathcal{O}_K$, we have $(W/K, \sigma, a) \sim (W'/K, \sigma', \pi^{v_K(a)/d''})$, and $D := (W'/K, \sigma', \pi^{v_K(a)/d''})$ is a division algebra over K of degree d'. Because $v_K(a)/d = (v_K(a)/d'')/d'$, we shall assume from now on that $a = \pi^r$ for some $r \in \mathbb{Z}$ prime to d, so that, in particular, $(W/K, \sigma, a)$ is a division algebra.

Choose integers r', n such that $rr' + nd = 1$, and define $\pi_D := \tau^{r'} \pi^n$. Observe that $\sigma(\pi) = \pi$ since $\pi \in K$, so that τ and π commute. From the choices of r', n we thus see that $\pi_D^d = \pi$. Now let $q := \#k$ and denote by ω a primitive $(q^d - 1)$th root of unity in W. Then

$$\pi_D \omega \pi_D^{-1} = \tau^{r'} \pi^n \omega \pi^{-n} \tau^{-r'} = \sigma^{r'}(\omega) = \omega^{q^{r'}},$$

where for the last equality we note that σ acts on roots of unity of order prime to p in the same way as on their reduction mod π. Since $rr' \equiv 1 \pmod{d}$, we compute $\operatorname{inv}_K D = r/d = v_K(a)/d$. □

2.3. *Discriminants*

Suppose that K is a global field that is the quotient field of a Dedekind domain A, and that a lies A. Then $\mathcal{O}_L[\tau, \tau^{-1}]/(\tau^d - a)$ is an A-order of $L[\tau, \tau^{-1}]/(\tau^d - a)$. The main purpose of this subsection is the computation of the discriminant of this order.

LEMMA 6. *Let D be the cyclic algebra $(L/K, \sigma, a)$. Denote by $\operatorname{Tr}_{D/K}$ the reduced trace of D over K and by $\operatorname{Tr}_{L/K}$ the trace of L over K. Then for $x = \sum_{i=0}^{d-1} \alpha_i \tau^i \in D$ one has*

$$\operatorname{Tr}_{D/K}(x) = \operatorname{Tr}_{L/K}(\alpha_0).$$

https://doi.org/10.1112/S1461157016000310 Published online by Cambridge University Press

Proof. The reduced trace of x is the trace of left multiplication by x on D, considered as a right L-vector space[†]. A basis of this vector space is given by $\{\tau^i\}_{i=0,\ldots,d-1}$. On this

$$x\tau^i = \tau^i\sigma^{-i}(\alpha_0) + \text{terms in } \tau^j, \quad j \neq i.$$

Hence $\mathrm{Tr}_{D/K}(x) = \sum_{i=0,\ldots,d-1}\sigma^{-i}(\alpha_0) = \mathrm{Tr}_{L/K}(\alpha_0)$. □

COROLLARY 7. *Let $\mathcal{O}_L$ denote the maximal order of L over A, that is, the integral closure of A in L. Denote by Λ the A-order $\sum \mathcal{O}_L\tau^i$ of $D = (L/K, \sigma, a)$. Then the discriminant of Λ is given by*

$$\mathrm{disc}(\Lambda) = a^{d(d-1)}\,\mathrm{disc}(L/K)^d.$$

Proof. Since the formation of the discriminant commutes with localization, it suffices to prove the asserted formula after localizing A at sufficiently many $b \in A\backslash\{0\}$ such that $\mathrm{Spec}\,A = \bigcup_b \mathrm{Spec}\,A[1/b]$. Since A arises from a global field, one can find b such that the rings $A[1/b]$ are principal ideal domains. Thus it suffices to prove the corollary in the case where $\mathcal{O}_L$ possesses an A-basis $b_0, \ldots, b_{d-1}$. Then an A-basis of Λ is given by $b_i\tau^j$, where i, j range over $0, \ldots, d-1$. Now we compute

$$\mathrm{Tr}_{D/K}(b_i\tau^j b_{i'}\tau^{j'}) = \mathrm{Tr}_{D/K}(b_i\sigma^j(b_{i'})\tau^{j+j'}) = \begin{cases} 0 & \text{if } j+j' \neq 0, d, \\ \mathrm{Tr}_{L/K}(b_i\sigma^j(b_{i'})) & \text{if } j+j' = 0, \\ a\,\mathrm{Tr}_{L/K}(b_i\sigma^j(b_{i'})) & \text{if } j+j' = d. \end{cases}$$

Thus the discriminant of Λ is given by

$$\det(\mathrm{Tr}_{L/K}(b_i\sigma^0(b_{i'})))_{i,i'}\prod_{j=1}^{d-1}\det(a\,\mathrm{Tr}_{L/K}(b_i\sigma^j(b_{i'})))_{i,i'} = a^{d(d-1)}\,\mathrm{disc}(L/K)^d. \qquad \square$$

REMARK 8. We warn the reader that for D fixed the discriminant of the order $\Lambda = \sum \mathcal{O}_L\tau^i$ depends on the choice of the generator σ, since changing σ will change the choice of a.

2.4. *Maximal orders*

Suppose that K is a global function field that is the quotient field of a Dedekind domain A. Let D be a central division algebra over K of finite dimension.

THEOREM 9. *If A has trivial class group and if there is a place v of K not corresponding to a prime of A with $\mathrm{inv}_v\,D = 0$, then all maximal A-orders Λ in D are conjugate under D^*.*

Proof. Lacking a direct reference, we indicate a proof. For global function fields, the hypothesis on v in the theorem means that D is Eichler over A; see [13, Definition 34.3]. Let $\Lambda \subset D$ be any maximal order. Then by [13, Theorem 35.14] due to Swan, the class number of Λ is 1 because this holds for A. Now [4, VI.8.2] implies that the type number of D is 1, and this means that for any two maximal orders Λ, Λ' there exists $c \in D^*$ such that $c\Lambda c^{-1} = \Lambda'$. □

3. *Cyclic extensions of the field F*

In this section we recall parts of the theory of abelian extensions for the field $F = \mathbb{F}_q(t)$. References are [6, Chapter 3] and [14, Chapter 12]. By ∞ we denote the place of vanishing of $1/t$.

[†] This can be seen via the explicit isomorphism $D \otimes_K L \to \mathrm{End}_L(D), a \otimes \lambda \mapsto (z \mapsto az\lambda)$.

https://doi.org/10.1112/S1461157016000310 Published online by Cambridge University Press

3.1. *Tamely ramified abelian extensions of $\mathbb{F}_q(t)$*

Denote by A the ring $\mathbb{F}_q[t]$. The Carlitz module is the unique ring homomorphism

$$\phi\colon A \to A[\tau] : a \mapsto \phi_a,$$

characterized by $\phi_\alpha = \alpha$, for $\alpha \in \mathbb{F}_q$, and $t \mapsto \phi_t = t + \tau$, and where $\tau a = a^q\tau$ in $A[\tau]$ for $a \in A$. Substituting τ^i by x^{q^i} for $i \geqslant 0$ provides one with a polynomial $\phi_a(x) \in A[x]$.

For any $a \in A\backslash\mathbb{F}_q$ we denote by $\lambda_a \in \overline{F}$ a primitive a-torsion point of ϕ, that is, $\phi_a(\lambda_a) = 0$ and ϕ_a is completely split over $F(\lambda_a)$. If $v(a) = 0$, we also write λ_a for its image in $\overline{F_v}$.

The field $F(\lambda_a)$ is an abelian extension of F with Galois group isomorphic to $(A/a)^*$, and an isomorphism is given by

$$(A/a)^* \longrightarrow \mathrm{Gal}(F(\lambda_a)/F), \bar{b} \longmapsto (\sigma_b\colon \lambda_a \mapsto \phi_b(\lambda_a)). \tag{3.1}$$

It is ramified exactly at those finite places of F defined by the finite prime divisors of a. A function field analogue of the Kronecker–Weber theorem states that any finite abelian extension of F which is totally split above ∞, except for an initial tamely ramified extension of degree dividing $q-1$, is contained in $F(\lambda_a)$ for some $a \in A\backslash\mathbb{F}_q$.

It will be useful to gather information about the fields $F_v(\lambda_a)$. Let v be a finite place of F. Denote by $h_v \in \mathbb{F}_q[t]$ the *monic* irreducible polynomial with $v(h_v) = 1$.

Theorem 10. *The extension $F_v(\lambda_a)/F_v$ is unramified if and only if $h_v \nmid a$. In this situation, $[F_v(\lambda_a) : F_v] = \mathrm{ord}_{(A/a)^*}(h_v)$.*

We can also describe the ramification above ∞ of the fields $F(\lambda_a)$.

Theorem 11 ([14, Theorem 12.14], [5, Lemma 1.4]). *For any monic $a \in A\backslash\mathbb{F}_q$ we have:*

(i) *the polynomial $\phi_a(x)/x$ splits over F_∞ into $(q^{\deg a} - 1)/(q-1)$ irreducible factors of degree $q-1$;*

(ii) *for any root λ_a of $\phi_a(x)/x$ in a finite extension of F_∞, the extension $F_\infty(\lambda_a)/F_\infty$ is totally tamely ramified of degree $q-1$;*

(iii) *supposing a is irreducible, then for any extension of F_∞ as in* (b),

$$\mathrm{Norm}_{F_\infty(\lambda_a)/F_\infty}(F_\infty(\lambda_a)^*) = t^{\mathbb{Z}}\left(1 + \frac{1}{t}\mathbb{F}_q\left[\left[\frac{1}{t}\right]\right]\right).$$

3.2. *Subfields of a cyclotomic extension*

The last theme we wish to cover in this subsection is that of primitive elements of the rings of integers of subfields of a cyclotomic field, a problem that is computationally considerably harder than the number field analogue by Leopoldt and Lettl, for example [10]. Let $k = \mathbb{F}_q$ and $E = F(\lambda_a)$ be the cyclotomic extension for an irreducible polynomial $a \in k[t]$ of degree d. We follow the Kummer-theoretical approach of [3] to find a primitive element of the subfield L of E of degree r over F for any divisor r of $q^d - 1$.

Let $k' = \mathbb{F}_{q^d}$. The polynomial a splits completely in $k'[t]$, and we write $a = \prod_{i=1}^d a_i$ as a product of distinct linear factors where we regard the indices as elements in $\mathbb{Z}/(d)$. We order the a_i so that under the natural action of $\mathrm{Gal}(k'/k) = \mathrm{Gal}(k'(t)/k(t))$ on $k'(t) = k'F$, the Frobenius automorphism $\mathcal{F}\colon x \mapsto x^q$ maps each a_i to a_{i+1}. Let $u_1, \ldots, u_d$ be rth roots of $-a_1, \ldots, -a_d$ and set $L' = k'F[u_1, \ldots, u_d]$. Because L/F is cyclic of degree r and k' contains all rth roots of unity, by Kummer theory the field $k'L$ is contained in L'. We display the

https://doi.org/10.1112/S1461157016000310 Published online by Cambridge University Press

relevant fields in the following diagram:

$$\begin{tikzcd}
L' \arrow[r, dash] & k'L \arrow[dr, dash] & & \\
k'F \arrow[ur, dash] \arrow[dr, dash] & & L \arrow[r, dash] & E \\
& F = k(t) \arrow[ur, dash] & &
\end{tikzcd}$$

Writing U_r for the rth roots of unity in k', we have an isomorphism

$$(U_r)^d \xrightarrow{\simeq} \mathrm{Gal}(L'/k'F)$$

from Kummer theory, defined by having $\bar{\alpha} = (\alpha_i)_i \in (U_r)^d$ act on $u = (u_i)_{i=1,\dots,d}$ via

$$\bar{\alpha}(u) = (\alpha_i u_i)_{i=1,\dots,d}.$$

Furthermore, the Frobenius automorphism $\mathcal{F}$ can be extended to $\Phi \in \mathrm{Gal}(L'/F)$ via $u_i \mapsto u_{i+1}$, to yield an automorphism of order d. For $j \in \mathbb{Z}/(d)$ one computes

$$\bar{\alpha}(\Phi^j(u_i)) = \bar{\alpha}(u_{i+j}) = \alpha_{i+j} u_{i+j}.$$

Thus $\bar{\alpha}\Phi^j = \bar{\alpha}'\Phi^{j'}$ only if $j = j', \bar{\alpha} = \bar{\alpha}'$. It follows by a size argument that the set of $d \cdot r^d$ automorphisms $\bar{\alpha}\Phi^j$ forms the Galois group $\mathrm{Gal}(L'/F)$. More precisely, $\mathrm{Gal}(L'/F) = (U_r)^d \rtimes \mathbb{Z}/(d)$, where the generator Φ of the right factor sends $\bar{\alpha}$ in the left factor to $(\mathcal{F}\alpha_1, \dots, \mathcal{F}\alpha_d)$.

Define $\delta_i = \prod_{j=0}^{d-1} u_{i+j}^{q^{d-1-j}}$ for $i \in \mathbb{Z}/(d)$. Then

$$\Phi(\delta_i) = \prod_{j=0}^{d-1} u_{i+j+1}^{q^{d-1-j}} = \delta_{i+1}, \quad \bar{\alpha}(\delta_i) = \prod_{j=0}^{d-1} (\alpha_{i+j} u_{i+j})^{q^{d-1-j}} = \hat{\alpha}_i \delta_i,$$

where $\hat{\alpha}_i = \prod_{j=0}^{d-1} \alpha_{i+j}^{q^{d-1-j}}$.

Setting $v_\beta = \sum_{i=0}^{d-1} \beta^{q^i} \delta_i$ for $\beta \in k'^*$, we want to compute $\mathrm{Gal}(L'/F(v_\beta))$. It follows from $\hat{\alpha}_i^q = \hat{\alpha}_{i+1}$ that

$$\Phi(v_\beta) = \sum_{i=0}^{d-1} \Phi(\beta^{q^i}\delta_i) = \sum_{i=0}^{d-1} \beta^{q^{i+1}} \delta_{i+1} = v_\beta, \quad \bar{\alpha}(v_\beta) = \sum_{i=0}^{d-1} \hat{\alpha}_i \beta^{q^i} \delta_i = \sum_{i=0}^{d-1} \hat{\alpha}_0^{q^i} \beta^{q^i} \delta_i = v_{\hat{\alpha}_0 \beta}.$$

An automorphism $\bar{\alpha}\Phi$ leaves $F(v_\beta)$ fixed if and only if $\hat{\alpha}_0 = 1$. Hence for such an $\bar{\alpha}\Phi$, the first $d-1$ components of $\bar{\alpha}$ determine the last. This means that $\#\,\mathrm{Gal}(L'/F(v_\beta)) = d \cdot r^{d-1}$ and

$$\#\,\mathrm{Gal}(F(v_\beta)/F) = r.$$

LEMMA 12. *One has $F(v_\beta) = L$.*

Proof. We write $a_i = (t - \beta_i)$ for suitable $\beta_i \in k'$ with $\beta_i^q = \beta_{i+1}$. Define $u'_1, \dots, u'_d$ as (q^d-1)th roots of $-a_1, \dots, -a_d$. With $E' = k'F[u'_1, \dots, u'_d]$ we can analogously define Φ', δ'_i and v'_β and get $\mathrm{Gal}(E'/F) = (k'^*)^d \rtimes \mathbb{Z}/(d)$. The restriction $\mathrm{Gal}(E'/F) \to \mathrm{Gal}(L'/F)$ is given by

$$(\alpha_0, \dots, \alpha_{d-1})\Phi'^j \longmapsto (\alpha_0^{r'}, \dots, \alpha_{d-1}^{r'})\Phi^j, \tag{3.2}$$

where $r' = (q^d-1)/r$. We define $\bar{\alpha}' = (\alpha_0^{r'}, \dots, \alpha_{d-1}^{r'})$.

A direct computation found in [3, Step 1 in proof of Theorem 4] reveals that $\phi_t(v'_\beta) = {v'_\beta}^q + Tv'_\beta = v'_{\beta_{-1}\beta}$. Inductively this gives $\phi_f(v'_\beta) = v'_{f(\beta_{-1})\beta}$. Therefore $\phi_h(v'_\beta) = 0$ and

https://doi.org/10.1112/S1461157016000310 Published online by Cambridge University Press

because the v'_β are distinct, they have to be exactly the h-torsion points of the Carlitz module. One concludes $F(v'_\beta) = E$.

As in the preceding construction, we know that

$$\mathrm{Gal}(E'/E) = \{\bar{\alpha}\Phi^j \in \mathrm{Gal}(E'/F) \mid \hat{\alpha}_0 = 1\}.$$

Using the restriction formula (3.2), we deduce from the previous paragraph

$$\mathrm{Gal}(E'/F(v_\beta)) = \{\bar{\alpha}\Phi^j \in \mathrm{Gal}(E'/F) \mid \hat{\alpha}'_0 = 1\}.$$

Obviously $\hat{\alpha}_0 = 1$ implies $\hat{\alpha}'_0 = 1$, so $\mathrm{Gal}(E'/E) \subset \mathrm{Gal}(E'/F(v_\beta))$ or equivalently $E \supset F(v_\beta)$. From $[L : F] = [F(v_\beta) : F] = r$ we find $L = F(v_\beta)$. □

LEMMA 13. *Keeping the above notation, the local Frobenius at an unramified prime $g \in k[t]$ of degree e, with g monic, is given by $v_\beta \mapsto v_{x\beta}$ where $x = (g(\beta_{e-1}))^{r'q^{d-e}}$.*

Proof. Split g into linear factors $g = (t - b_0)\ldots(t - b_{e-1})$ with $b_i^q = b_{i+1}$. The Frobenius is given by taking the q^eth power modulo (g). One computes

$$\delta_i^q = a_i^{r'}\delta_{i+1}, \quad \delta_i^{q^e} = (a_{i+e-1}a_{i+e-2}^q \cdots a_i^{q^{e-1}})^{r'}\delta_{i+e}.$$

Reducing modulo g by substituting $t \mapsto b_0$, the base term can be simplified:

$$\begin{aligned}(a_{i+e-1}a_{i+e-2}^q \cdots a_i^{q^{e-1}}) &= (\beta_{i+e-1} - t)(\beta_{i+e-1} - t^q)\ldots(\beta_{i+e-1} - t^{q^{e-1}})\\ &\equiv (\beta_{i+e-1} - b_0)(\beta_{i+e-1} - b_1)\ldots(\beta_{i+e-1} - b_{e-1}) \pmod{g}\\ &= g(\beta_{i+e-1}) = g(\beta_{e-1})^{q^i}.\end{aligned}$$

Finally, we can compute

$$v_\beta^{q^e} \equiv \sum_{i=0}^{d-1}\beta^{q^{i+e}}(g(\beta_{e-1}))^{r'q^i}\delta_{i+e} \pmod{g} = \sum_{i=0}^{d-1}(\beta(g(\beta_{e-1}))^{r'q^{d-e}})^{q^{i+e}}\delta_{i+e} = v_{x\beta}.$$ □

REMARK 14. Of course, there are other approaches to get a primitive element of L: in [1, Theorem 2.5], a normal integral basis of $\mathcal{O}_L$ is given in terms of universal Gauss–Thakur sums. Alternatively the norm of a primitive h-torsion element can be taken [7, Theorem 4.3].

Implementations of all three constructions by the authors in Magma, tested on many examples, confirm the better performance of the approach introduced here. For instance, for $q = 5$ and h_w of degree 4, our approach took 0.170 s to compute a primitive element of the subfield of degree $r = 6$ and its minimal polynomial, while the norm and the Gauss–Thakur sum approaches took 12.160 and 13.600 s. We have no complete understanding of this.

The approaches in [1, 7] rely on computations in the field E, ours on computations in $L'/k'F$. In all three cases the coefficients of a minimal polynomial of a generator of L/F are computed. This requires multiplications in E and L' respectively, and thus in each case a reduction of elements to standard representatives. In our tests this step appears time-consuming in E and rapid in L'. Therefore we expect that the simple structure of the multi-Kummer extension $L'/k'F$, that is, $L' = k'F[X_1, \ldots, X_d]/(X_i^r + a_i, i = 1, \ldots, d)$, if compared with the cyclotomic extension E/F, where $E = F[X]/(\phi_a(X)/X)$, is responsible for the better performance.

4. *The basic algorithm*

Let S be a finite set of finite places of F, and for each $v \in S$, let $s_v = n_v/r_v$ be a reduced fraction, and define $r = \mathrm{lcm}(r_v : v \in S)$. Then the Grunwald–Wang theorem (for example, [13, Theorem 32.20]) guarantees the existence of a cyclic field L/F of degree r and of a cyclic algebra of the form $D=(L/F,\bar{\sigma},a)$, for some generator $\bar{\sigma}$ of $\mathrm{Gal}(L/F)$ and some $a\in K$, whose local invariant satisfy $\mathrm{inv}_v\, D=s_v$.

For the simple algorithm below, we shall make the following further restriction:

Assumption 15. None of the r_v is divisible by p, and $\infty\notin S$.

More concretely, the simple algorithm wishes to find a subextension L of $E=F(\lambda_w)$ for a place w of F, that is, L/F is of prime conductor, such that:

(1) $r=[L:F]$; and
(2) for all $v\in S$ we have $r_v|[L_v:F_v]=:d_v$.

We fix a generator σ of $G:=\mathrm{Gal}(E/F)$ and denote by $H\leqslant G$ the subgroup corresponding to L. We set $q_w=q^{\deg(w)}$. We display the situation in the following diagram:

$$\begin{tikzcd}
E \arrow[d, dash, "H=\langle\sigma^r\rangle"] \arrow[dd, dash, bend right, "{G=(A/h_w)^*\cong\mathbb{Z}/(q_w-1)}"'] & & E_v \arrow[d, dash, "H_v=\langle\sigma_v^{d_v}\rangle"] \arrow[dd, dash, bend right, "G_v\cong\mathbb{Z}/(f_v)"'] \\
L \arrow[d, dash, "\overline{G}=\langle\bar{\sigma}\rangle\cong\mathbb{Z}/(r)"] & & L_v \arrow[d, dash, "\overline{G}_v=\langle\bar{\sigma}_v\rangle\cong\mathbb{Z}/(d_v)"] \\
F & & F_v,
\end{tikzcd}$$

where σ_v denotes the Frobenius endomorphism at v. A bar on top of an endomorphism is used to denote the restriction of the endomorphism to the intermediate field L or L_v.

4.1. *Global conditions*

The global condition is $r|q_w-1$, that is, that $q^{\deg(w)}\equiv 1\pmod{r}$. Recall that we assume that p does not divide r here, so that q is a unit in $\mathbb{Z}/(r)$.

4.2. *Local conditions*

For the local degree $f_v(w):=[E_v:F_v]$ of E_v/F_v (this depends on v and w, so we include both parameters in our notation) we have

$$f_v(w)=\mathrm{ord}_{(A/w)^*}(h_v).$$

Hence the local decomposition group is

$$G_v=\langle\sigma^{(q_w-1)/f_v(w)}\rangle=\langle\sigma_v\rangle.$$

The decomposition group of L_v/F_v is now given by HG_v/H. Since everything takes place inside the cyclic group G, the subgroup HG_v is cyclic, and for the order d_v of the quotient HG_v/H we deduce

$$d_v=\mathrm{lcm}\left(\frac{q_w-1}{r},f_v(w)\right)\Big/\frac{q_w-1}{r}=f_v(w)/\gcd\left(\frac{q_w-1}{r},f_v(w)\right).$$

The condition we require is $r_v|d_v$.

4.3. *Statement of the algorithm*

After a number of simple manipulations we obtain the following algorithm.

Algorithm 16. **Input:** an integer $m\geqslant 2$, monic irreducible elements $\{h_v\}_{v\in S}$ with $v(h_v)=1$, reduced fractions $s_v=n_v/r_v$ for $v\in S$ with $\sum_v s_v\equiv 0\mod\mathbb{Z}$.
Output: a monic irreducible polynomial h_w.

https://doi.org/10.1112/S1461157016000310 Published online by Cambridge University Press

(i) Compute $r = \operatorname{lcm}(r_v : v \in S)$. If $p|r$, then stop.
(ii) Compute $d_0 = \operatorname{ord}_{(\mathbb{Z}/(r))^*}(q)$.
(iii) Start for loop over $j = 1, 2, 3, \ldots$.
(iv) Start for loop over all monic irreducible polynomials h_w of degree $d_0 j$.
(v) If $h \in S$, then go to next irreducible. If all irreducibles of degree $d_0 j$ are tested, increase j.
(vi) Compute for $v \in S$ the quantity $f_v(w) = \operatorname{ord}_{(A/w)*}(h_v)$ and check if it is divisible by r_v. If not, go to next irreducible. If all irreducibles of degree $d_0 j$ are tested, increase j.
(vii) Check for $v \in S$ whether $\gcd(q_w - 1/r, f_v(w))$ divides $f_v(w)/r_v$. If not, go to next irreducible. If all irreducibles of degree $d_0 j$ are tested, increase j.
(viii) Return h_w and end the loops.

While the algorithm provides a cyclotomic extension which is sufficient to construct a cyclic algebra with the required invariants, the later explicit construction of a maximal $\mathbb{F}_q[t]$-order will need to replace the condition $r_v|d_v$ by the stronger condition of equality $r_v = d_v$. This amounts to changing the divisibility checks (vii) in the algorithm by tests for equality. We will refer to this altered algorithm as Algorithm 16 with *strong conditions* while the original algorithm will be referred to as Algorithm 16 with *weak conditions*.

4.4. *Construction of L, $\bar{\sigma}$ and a*

We now assume that the search for w was successful and set $L = E^{\langle \sigma^r \rangle}$, so that $\bar{\sigma} = \sigma|_L$ is a generator of $\operatorname{Gal}(L/F)$.

Then $u_v := r/d_v$ is the smallest positive integer such that $\bar{\sigma}^{u_v} \in \overline{G}_v$. In particular, both $\bar{\sigma}^{u_v}$ and the Frobenius automorphism $\bar{\sigma}_v$ at v are generators of $\overline{G}_v \cong \mathbb{Z}/(d_v)$. Therefore the following definition makes sense.

Definition 17. Define $u'_v \in (\mathbb{Z}/d_v\mathbb{Z})^*$ such that $\bar{\sigma}^{u_v} = \bar{\sigma}_v^{u'_v}$.

This means that $\bar{\sigma}^{u_v}$ acts on the residue field at v as $\alpha \mapsto \alpha^{q_v^{u'_v}}$.

Let $u''_v \in \mathbb{Z}$ an inverse to u'_v modulo d_v. Then for $a \in F$ we have

$$(L/F, \bar{\sigma}, a) \otimes_F F_v \overset{\text{Theorem 3}}{=} (L_v/F_v, \bar{\sigma}_v^{u'_v}, a) \overset{\text{Theorem 2(a)}}{\sim} (L_v/F_v, \bar{\sigma}_v, a^{u''_v}).$$

In particular,

$$\operatorname{inv}_v(L/F, \bar{\sigma}, a) \equiv \frac{u''_v v(a)}{d_v} \pmod{\mathbb{Z}}.$$

Locally at v we want $\operatorname{inv}_v D = n_v/r_v$, that is, $n_v/r_v \equiv u''_v v(a)/d_v \pmod{\mathbb{Z}}$. Since d_v is a multiple of r_v, we obtain

$$n_v \frac{d_v}{r_v} \equiv u''_v v(a) \pmod{d_v}.$$

Solving for $v(a)$ yields

$$v(a) \equiv u'_v n_v \frac{d_v}{r_v} \pmod{d_v}. \tag{4.1}$$

The above argument holds for all finite places. We define g_v to be the integer such that

$$g_v \equiv u'_v n_v \pmod{r_v} \quad \text{and} \quad 0 \leqslant g_v \leqslant r_v - 1. \tag{4.2}$$

We define $a = \prod_v h_v^{g_v d_v / r_v}$.

Theorem 18. *With notation as above, $D = (L/F, \bar{\sigma}, a)$ is a central division algebra over F with $\operatorname{inv}_v D = s_v$ for all places v of F.*

Proof. The statement is clear for the invariants at all finite places different from w. Because $\sum s_v = 0$, it remains to show $s_\infty = 0$. By Theorem 3, we have

$$(L/F, \bar{\sigma}, a) \otimes_F F_\infty = (L_\infty/F_\infty, \bar{\sigma}^k, a),$$

where $k > 0$ is the smallest integer such that $\bar{\sigma}^k$ lies in $\mathrm{Gal}(L_\infty/F_\infty)$. But now observe that a is a norm from $F_\infty(\lambda_w)^*$ to F_∞^* by definition of a_∞ and Theorem 11(c), because $t^{-\deg a}a$ is a 1-unit in F_∞ and hence a is a norm from $F_\infty(\lambda_w)^*$. □

4.5. *A simple construction in special cases*

We would like to mention a natural construction under special conditions on the sequence $(s_v)_{v\in S}$ which appears in forthcoming work of M. Papikian on Drinfeld–Stuhler modules. Namely, suppose that r_v divides $d_v = r/\mathrm{gcd}(r, \deg v)$ for all $v \in S$. It is not required that r is relatively prime to p. Let L be the constant field extension of F of degree r. Let $\sigma \in \mathrm{Gal}(L/F)$ be the automorphism induced from the Frobenius automorphism of $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ and let $a \in F^*$. Then by [6, Theorem 4.12.4] one has

$$\mathrm{inv}_v(L/F, \sigma, a) = \frac{v_{F_v}(a) \cdot \deg v}{r}$$

in $\mathbb{Q}/\mathbb{Z}$. Define $a = \prod_{v\in S} h_v^{e_v d_v/r_v}$ for $e_v \in \{1, \ldots, r_v - 1\}$ such that $e_v(\deg v/(\mathrm{gcd}(\deg v, r))) \equiv n_v \pmod{r_v}$. Then $D = (L/F, \sigma, a)$ has invariant s_v for $v \in S$ and 0 for $v \notin S$. Let us also mention that under the further condition $d_v = r_v$ for all $v \in S$ the procedure explained in § 6 will yield a maximal A-order in D.

5. *Termination of the algorithm*

THEOREM 19. *Algorithm 16 terminates with weak and strong conditions.*

We shall prove the theorem, by showing that the set of primes w for which the algorithm terminates is a Čebotarev set of positive density.

5.1. *Weak conditions*

We introduce notation for the prime factorization of r, namely we denote it by $r = \prod_i p_i^{e_i}$ for pairwise distinct prime numbers p_i and integer exponents $e_i \geqslant 1$.

The conditions on the w that we seek are then as follows.

(a) $w \notin S$;

(b) $\mathrm{ord}_{\mathbb{Z}/(r)^*}(q) | \deg(w)$;

(c) $f_v(w) = \mathrm{ord}_{A/(w)^*}(h_v)$ is a multiple of r_v, or, in other words,

$$\forall i : \mathrm{ord}_{p_i}(r_v) \leqslant \mathrm{ord}_{p_i}(f_v(w)).$$

(d) $\forall v \in S, \forall p_i$: $\min(\mathrm{ord}_{p_i}(q_w - 1/r), \mathrm{ord}_{p_i}(f_v(w))) \leqslant \mathrm{ord}_{p_i}(f_v(w)) - \mathrm{ord}_{p_i}(r_v)$. This in turn is equivalent to

$$\forall v \in S,\ \forall p_i : \text{if } p_i | r_v \text{ then } \mathrm{ord}_{p_i}(q_w - 1) - \mathrm{ord}_{p_i}(r/r_v) \leqslant \mathrm{ord}_{p_i}(f_v(w)).$$

LEMMA 20. *Suppose condition* (a) *holds. Then condition* (b) *is equivalent to* $\mathrm{Frob}_w = 1$ *in* $\mathrm{Gal}(F(\zeta_r)/F)$ *for* ζ_r *a primitive* r*th root of unity.*

Proof. Using that w should not ramify in $F(\zeta_r)$ and the Frobenius generates the local Galois group, one gets a chain of equivalences

$$\mathrm{Frob}_w = 1 \in \mathrm{Gal}(F(\zeta_r)_w/F_w) \Leftrightarrow [F(\zeta_r)_w : F_w] = 1 \Leftrightarrow [\mathbb{F}_w(\zeta_r) : \mathbb{F}_w] = 1 \Leftrightarrow r | q_w - 1,$$

where $\mathbb{F}_w$ denotes the residue class field of F at w. □

https://doi.org/10.1112/S1461157016000310 Published online by Cambridge University Press

Moreover, under (d), condition (c) is superfluous, that is, the join of the two becomes:

(e) $\forall v \in S, \forall p_i$: if $p_i | r_v$ then $\operatorname{ord}_{p_i}(q_w - 1) - \operatorname{ord}_{p_i}(r/r_v) \leqslant \operatorname{ord}_{p_i}(f_v(w))$.

We define $e_{i,v} := \operatorname{ord}_{p_i}(r/r_v) + 1$ whenever $p_i | r_v$, and note that under this condition we have $e_{i,v} \leqslant e_i$ since $\operatorname{ord}_{p_i}(r_v) \geqslant 1$.

LEMMA 21. *Let $\mathbb{F}_w$ denote the residue field of $F(\zeta_r)$ at w and $\overline{h}_v$ the reduction of h_v in that field. Assuming that* $\operatorname{Frob}_w = 1$ *in* $\operatorname{Gal}(F(\zeta_r)/F)$ *and* $0 \leqslant e_{i,v} \leqslant e_i$*, the following assertions are equivalent:*

(i) $\operatorname{Frob}_w = 1$ *in* $\operatorname{Gal}(F(\zeta_r, \sqrt[p_i^{e_{i,v}}]{h_v})/F)$;

(ii) $\sqrt[p_i^{e_{i,v}}]{\overline{h}_v} \in \mathbb{F}_w^*$;

(iii) $\operatorname{ord}_{p_i}(f_v(w)) \leqslant \operatorname{ord}_{p_i}(q_w - 1) - e_{i,v}$.

Note that adjoining any $p_i^{e_{i,v}}$th root of unity is a Kummer extension of $F(\zeta_r)$ since $p_i^{e_i}$ divides r.

Proof. As in the proof of the previous lemma

$$\begin{aligned}&\operatorname{Frob}_w = 1 \in \operatorname{Gal}(F(\zeta_r, \sqrt[p_i^{e_{i,v}}]{h_v})/F)\\ \Leftrightarrow\ &\operatorname{Frob}_w = 1 \in \operatorname{Gal}(F(\zeta_r, \sqrt[p_i^{e_{i,v}}]{h_v})/F(\zeta_r)) \Leftrightarrow \sqrt[p_i^{e_{i,v}}]{\overline{h}_v} \in \mathbb{F}_w^*\end{aligned}$$

where the first equivalence uses that $\operatorname{Frob}_w = 1$ in $\operatorname{Gal}(F(\zeta_r)/F)$.

For (ii) ⇒ (iii), let $\overline{h}_v = x^{p_i^{e_{i,v}}} \in \mathbb{F}_w^*$. Then $\operatorname{ord}_{\mathbb{F}_w^*} x | q_w - 1$, so

$$\operatorname{ord}_{p_i}(f_v(w)) = \operatorname{ord}_{p_i}(\operatorname{ord}_{\mathbb{F}_w^*}(x^{p_i^{e_{i,v}}})) = e_{i,v} + \operatorname{ord}_{p_i}(\operatorname{ord}_{\mathbb{F}_w^*} x) \leqslant e_{i,v} + \operatorname{ord}_{p_i}(q_w - 1).$$

For (iii) ⇒ (ii), let x be a generator of $\mathbb{F}_w^*$ and $x^s = \overline{h}_v$. Then because

$$\operatorname{ord}_{p_i}(\operatorname{ord}_{\mathbb{F}_w^*} h_v) = \operatorname{ord}_{p_i}(f_v(w)) \leqslant \operatorname{ord}_{p_i}(q_w - 1) - e_{i,v}$$

we know that $\operatorname{ord}_{p_i}(s) \geqslant e_{i,v}$, hence $p_i^{e_{i,v}} | s$ and $\sqrt[p_i^{e_{i,v}}]{\overline{h}_v}$ is given by $x^{s/p_i^{e_{i,v}}}$. □

We deduce the following result, of which Theorem 19 with weak conditions is an immediate corollary.

PROPOSITION 22. *The density of primes w in F satisfying* (*a*)–(*d*) *is*

$$\frac{1}{\phi(r)} \cdot \prod_{j=1}^{m} \prod_{i:p_i|r_{v_j}} \left(1 - \frac{1}{p_i^{e_{i,v_j}}}\right).$$

Proof. Define $E_v := \prod_{i:p_i|r_v} p_i^{e_{i,v}}$ for all $v \in S$ and consider the tower of fields

$$F'' := F(\zeta_r)(h_{v_1}^{1/E_{v_1}}, \ldots, h_{v_m}^{1/E_{v_m}}) \supset F' := F(\zeta_r) \supset F.$$

Then (1) $\operatorname{Gal}(F'/F) = \mathbb{Z}/\phi(r)\mathbb{Z}$, (2) the extension F'/F is unramified, (3) the extensions $F_j' := F'(h_{v_j}^{1/E_{v_j}})/F'$ are proper, linearly disjoint and ramified precisely at v_j and totally ramified at v_j, (4) F''/F' is abelian with Galois group $\operatorname{Gal}(F''/F') \cong \prod_{j=1}^{m} \mathbb{Z}/E_{v_j}\mathbb{Z}$, (5) the extension F''/F is Galois and its group is a semidirect product $\operatorname{Gal}(F''/F') \rtimes \operatorname{Gal}(F'/F)$.

To see properness in (3), note in the function field case that F'/F is unramified but F_j'/F ramifies at h_{v_j}; because p is not allowed to divide r_v, the extension F'/F is Galois. Linear disjointness follows because the extensions have distinct ramification places.

https://doi.org/10.1112/S1461157016000310 Published online by Cambridge University Press

It follows that w is a place satisfying conditions (a)–(d) if and only if Frob_w is trivial in $\mathrm{Gal}(F'/F)$ and Frob_w is non-trivial in all primary factors of $\mathrm{Gal}(F'(h_{v_j}^{1/E_{v_j}})/F')$. From the Čebotarev density theorem (for example, [12, § VII.13]) we get the required density. □

5.2. *Strong conditions*

We have to replace the first inequality in condition (d) with equality and call this (d′). As above we make (c) superfluous and set $e_{i,v} := \mathrm{ord}_{p_i}(r/r_v) + 1$ for $p_i|r_v$. Using Lemma 21, we restate (d′).

(e′) If $p_i|r_v$, then

$$\mathrm{Frob}_w = 1 \in \mathrm{Gal}(F(\zeta_r, \sqrt[p_i^{e_{i,v}-1}]{h_v})/F) \wedge \mathrm{Frob}_w \neq 1 \in \mathrm{Gal}(F(\zeta_r, \sqrt[p_i^{e_{i,v}}]{h_v})/F).$$

(e″) If $p_i \nmid r_v$, then $\mathrm{Frob}_w = 1 \in \mathrm{Gal}(F(\zeta_r, \sqrt[p_i^{e_i}]{h_v})/F)$.

The factors in Theorem 22 change to $(p_i-1)/p_i^{e_{i,v}}$ for $p_i|r_v$ and $1/p_i^{e_i}$ for $p_i \nmid r_v$. We deduce the following result, of which Theorem 19 with strong conditions is an immediate corollary.

Proposition 23. *The density of primes w in F satisfying the strong conditions is*

$$\frac{1}{\phi(r)} \cdot \prod_{j=1}^{m} \frac{r_{v_j}}{r} \prod_{i:p_i|r_{v_j}} \left(1 - \frac{1}{p_i}\right).$$

6. *Constructing a maximal $\mathbb{F}_q[t]$-order*

The present section describes how to obtain a maximal order for $D = (L/F, \sigma, a)$ constructed by the algorithm with strong conditions, that is, in the case where $r_v = d_v$ for all $v \in S$; in this section σ denotes a generator of $\mathrm{Gal}(L/F)$, for example the $\bar{\sigma}$ from § 4.4, and by order we will always mean $\mathbb{F}_q[t]$-order. Because $\mathbb{F}_q[t]$ is a principal ideal domain and $s_\infty = 0$, Theorem 9 shows that all maximal orders are conjugate.

First, observe that we are dealing with a local question.

Theorem 24 [13, 11.6]. *An order Λ is maximal if and only if for all places $v \neq \infty$ of F the completion Λ_v is maximal in D_v.*

We will describe how to maximize the order $\Lambda = \bigoplus_{i=0}^{r-1} \mathcal{O}_L \tau^i$ at the different places of F. The globally maximal order is the linear hull of all the locally maximized orders.

6.1. *The discriminant of a maximal order*

An important tool to decide whether an order is maximal inside a central simple algebra is its discriminant. Here we collect the relevant facts needed for the construction of a maximal order in D starting with $\Lambda = \bigoplus_{i=0}^{r-1} \mathcal{O}_L \tau^i$.

The following result is immediate from [13, Theorem 32.1].

Proposition 25. *Suppose D has local invariants s_v/r_v at the finite set of places S of F with corresponding primes h_v, and set $r = \mathrm{lcm}(r_v : v \in S)$. Then for a maximal order Λ of D one has* $\mathrm{disc}(\Lambda) = (\prod_{v \in S} h_v^{r-r/r_v})^r$.

Corollary 26. *Let D be as in Theorem 18 and let Λ be the order $\bigoplus_{i=0}^{r-1} \mathcal{O}_L \tau^i$. Then:*

(i) *the order Λ is maximal at all places outside $S \cup \{w\}$;*

(ii) *the discriminant of Λ at w is* $\mathrm{disc}(L/K)^r = p^{r(r-1)}$ *or* $\mathrm{disc}(L/K)^r = h_w^{r(r-1)}$*;*

https://doi.org/10.1112/S1461157016000310 Published online by Cambridge University Press

(iii) *the discriminant of* Λ *is* $h_v^{r(r-1)\cdot g_v d_v/r_v}$ *at* $v \in S$*;*
(iv) *the order* Λ *is maximal at* $v \in S$ *if and only if* $r_v = d_v = r$ *and* $g_v = 1$.

Proof. The first three parts are immediate from the computation of $\operatorname{disc}(\Lambda)$ in Corollary 7 and the standard formula for discriminants of abelian extensions of $\mathbb{F}_q(t)$ in terms of conductors of the defining characters; see [15].

For the last part we need to compare (iii) with the formula in Proposition 25. This gives the condition $h_v^{g_v d_v/r_v \cdot r(r-1)} \overset{!}{=} (h_v^{r-r/r_v})^r$. It is equivalent to $g_v(d_v/r_v)(1-1/r) = 1-1/r_v$. From this (iv) is immediate. □

6.2. *The ramified place* w

L/F is totally ramified at w and we can write $D_w = (L_w/F_w, \sigma, a)$, where, in an abuse of notation, σ denotes the unique extension of σ onto L_w. Because $\operatorname{inv}_w D = 0$ we know that an isomorphism $D_w \cong M_r(F_w)$ exists. Moreover, this isomorphism can be described explicitly in two steps.

Theorem 27 [13, Proof of Theorem 30.4].
(i) *There exists an element* $f \in \mathcal{O}_{L_w}^*$ *such that* $\operatorname{Norm}_{L_w/F_w} f = a$*. It induces an isomorphism* $(L_w/F_w, \sigma, 1) \to (L_w/F_w, \sigma, a)$ *by letting* L_w *be fixed and* $\tau \mapsto (f\tau)$*. In fact, the existence of a solution to the norm equation is equivalent to* $(L_w/F_w, \sigma, 1) \cong (L_w/F_w, \sigma, a)$*.*
(ii) *An isomorphism* $(L_w/F_w, \sigma, 1) \to \operatorname{End}_{F_w}(L_w) \cong M_r(F_w)$ *is given by* $\tau \mapsto \sigma$*,* $x \mapsto x_{L_w}$ *for* $x \in L_w$*, where* x_{L_w} *denotes multiplication by* x*. After choosing a basis* $e = (e_1, \ldots, e_r)$ *of* $\mathcal{O}_{L_w}$ *over* $\mathcal{O}_w$*, and writing* $x_{L_w} e = eT_x$*,* $\sigma e = eP$ *for unique matrices* T_x, P *in* $M_r(F_w)$*, the isomorphism* $(L_w/F_w, \sigma, 1) \to M_r(F_w)$ *is given by* $\tau \mapsto P$*,* $x \mapsto T_x$*.*

In general, $M_r(F_w)$ has many maximal orders, namely $M_r(\mathcal{O}_w)$ and all its conjugates [13, 17.3]. Luckily, under the above isomorphism we have $\Lambda_w \subset M_r(\mathcal{O}_w)$. To see this, first note that Λ_w remains unchanged under the first isomorphism as $f \in \mathcal{O}_{L_w}^*$. Under the second isomorphism the action of Λ_w on L_w lies in the stabilizer of $\mathcal{O}_{L_w}$ which is equal to $M_r(\mathcal{O}_w)$ with the choice of an integral basis.

6.2.1. *Solving the norm equation.* We now describe how to find the solution f of the norm equation by a limit procedure. Choose a uniformizer π at w, so that $\mathfrak{p} = \mathcal{O}_{L_w}\pi$ is the maximal ideal of $\mathcal{O}_{L_w}$. The unit group $U_{L_w} = \mathcal{O}_{L_w} - \mathfrak{p}_w$ has the filtration $U_{L_w}^0 = U_{L_w}$, $U_{L_w}^i = 1 + \mathfrak{p}^i, i \geqslant 1$. We recall that $U_{L_w}^0/U_{L_w}^1 \cong \mathbb{F}_w^*$ and $U_{L_w}^i/U_{L_w}^{i+1} \cong \mathfrak{p}_w^i/\mathfrak{p}_w^{i+1} \cong \mathbb{F}_w$, where the second isomorphism depends on π. The same definitions can be made for F_w.

The higher ramification groups G_i of $G_w = \operatorname{Gal}(L_w/F_w)$ form a decreasing sequence of normal subgroups for $i \geqslant -1$. As proven in [17, Corollary IV.2.2,3], the higher quotients G_i/G_{i+1} vanish for $p \nmid r$ (being direct products of groups of order p). Thus $G_w = G_0, G_i = 1, i \geqslant 1$ and with $\psi(n) = rn$ we get the following theorem.

Theorem 28 [17, Proposition V.6.8, Corollary V.6.2].
(i) *For every integer* $n \geqslant 0$ *one has*

$$N(U_{L_w}^{\psi(n)}) \subset U_{K_w}^n, \quad N(U_{L_w}^{\psi(n)+1}) \subset U_{K_w}^{n+1},$$

where $N = \operatorname{Norm}_{L_w/F_w}$*. By passing to the quotients this yields*

$$N_0 : \mathbb{F}_w^* \to \mathbb{F}_w^*, \quad N_n : \mathbb{F}_w \to \mathbb{F}_w \quad \text{for } n \geqslant 1.$$

(ii) *The map* N_0 *is given by* $\xi \mapsto \xi^r$*.*
(iii) *The map* N_n *is surjective and given by* $\xi \mapsto \beta_n \xi$ *for some* $\beta_n \in \mathbb{F}_w^*$*.*

https://doi.org/10.1112/S1461157016000310 Published online by Cambridge University Press

Using this description of the norm (β_n can be determined experimentally) we can construct $f_n = \sum_{k=0}^{n} a_k \pi^{rk}$ that approximate a solution f up to order rn for all $n \geqslant 0$.

6.2.2. *Necessary precision.* Let Λ'_w be the maximal order $M_r(\mathcal{O}_w)$, so that $\Lambda_w \subset \Lambda'_w$. Since both are finitely generated $\mathcal{O}_w$ modules of the same rank, there exists an integer $s \geqslant 0$ such that $\pi^s \Lambda'_w \subset \Lambda_w$.

In terms of bases $(e'_1, \ldots, e'_{r^2})$ and $(e_1, \ldots, e_{r^2})$ of Λ'_w and Λ_w, we write $e'_i = \pi^{-s}(\sum_j \alpha_{ij} e_j)$ for suitable $\alpha_{ij} \in \mathcal{O}_w$. Now suppose $\hat{a}_{ij} \equiv a_{ij} \pmod{\pi^s}$; then defining $\hat{e}'_i := \pi^{-s}(\sum_j \hat{\alpha}_{ij} e_j)$, a set of generators of Λ'_w is given by $\{\hat{e}'_1, \ldots, \hat{e}'_{r^2}, e_1, \ldots, e_{r^2}\}$. One concludes that it is enough to solve the norm equation up to order $s - 1$.

THEOREM 29. *The integer s can be chosen as r.*

Proof. Consider the $r \times r$ Vandermonde matrix with columns $(\pi^i, \sigma(\pi^i), \ldots, \sigma^{r-1}(\pi^i))^t$ for $i = 0, \ldots, r-1$. Acting from the right on $(\lambda_1, \ldots, \lambda_r) \in F_w^r$, it gives the image of $(\pi^0, \pi^1, \ldots, \pi^{r-1})$ under $\sum_i \lambda_i \tau^i$. The condition $\Lambda'_w \subset \pi^{-r}\Lambda_w$ is equivalent to showing that all $\sum_i \lambda_i \tau^i$ that send $(\pi^0, \pi^1, \ldots, \pi^{r-1})$ to $\mathcal{O}_{L_w}^r$ lie in $\pi^{-r}\Lambda_w$, that is, the inverse V^{-1} sends $\mathcal{O}_{L_w}$ to $\pi^{-r}\mathcal{O}_{L_w}$.

Thus, we only need to know the denominators of the inverse of a Vandermonde matrix. According to [9, Exercise 40], they are given by $\sigma^i(\pi)\prod_{1 \leqslant k \leqslant r, k \neq i}(\sigma^i(\pi) - \sigma^k(\pi))$. Because of $G_0 = G_w, G_1 = 1$, all factors have valuation 1 and the total valuation is r. □

LEMMA 30. *It suffices to solve the norm equation up to order* 0.

Proof. Recall that the solution f was constructed in order jumps of size r. □

6.2.3. *Fixing the denominator.* The approximated generators $\hat{e}'_1, \ldots, \hat{e}'_{r^2}$ may have denominators at places different from w. To make sure that we still have a multiplicatively closed order, multiply the generators with the prime-to-w part, so that the order Λ'' they generate still equals Λ'_w at w but is contained in the original order Λ_v at all $v \neq w$.

Because this inclusion in Λ_v may be proper, the global order sought (which is maximal at w but Λ_v at other places v) is the linear hull of Λ'' and Λ.

6.3. *Unramified places $v \in S$*

For convenience, fix the notation $d := d_v$, $u := r/d$ throughout this section and assume $d = r_v$ (*strong conditions*). Fix prolongations $w_0, \ldots, w_{u-1}$ of v to L such that σ acts on the w_i by sending each to the next one and w_{u-1} to w_0. In other words, σ sends each component of $M := L \otimes F_v = \bigoplus_{i=0}^{u-1} L_i$ to the next one, where $L_i := L_{w_i}$. We construct an order maximal at v containing $\Lambda = \bigoplus_{i=0}^{r-1} \mathcal{O}_L \tau^i$.

Locally, D is given as

$$D \otimes F_v = M[\tau]/(\tau^r - a) = \left(\bigoplus_{i=0}^{u-1} L_i\right)[\tau]/(\tau^r - a) = \bigoplus_{i,j=0}^{u-1} (L_i[\tau^u]/((\tau^u)^d - a))\tau^j.$$

Defining $D_i := L_i[\tau^u]/((\tau^u)^d - a)$, one knows that $D_i \cong D_j$ for all $0 \leqslant i, j \leqslant u-1$ and $D \otimes F_v \cong M_u(D_0)$ (especially the D_i have the same local invariant). Multiplication of elements in the right-hand side of the above equation works via

$$\sigma : D_i \to D_{i+1}, b(\tau^u)^s \mapsto \sigma(b)(\tau^u)^s, \quad \alpha\beta = \begin{cases} 0 & i \neq j, \\ \alpha \cdot_{D_i} \beta & i = j, \end{cases} \tag{6.1}$$

for $b \in L_i, \alpha \in D_i, \beta \in D_j$.

https://doi.org/10.1112/S1461157016000310 Published online by Cambridge University Press

For $d = r_v$ (*strong conditions*) the algebra D_j actually is a skewfield; cf. [**13**, 31.6]. As seen in [**13**, 12.6 and 12.8], the valuation v can be uniquely extended to a discrete valuation on D_j, which we denote by v as well. It is given for $x \in D_j$ as

$$v(x) := \frac{1}{[K(x) : K]} v(\mathrm{Norm}_{K[x]/K}(x)).$$

Theorem 31 [**13**, 13.3]. *Let $x \in D_j$ have valuation $1/d$. Then $\Lambda'_v = \bigoplus_{i=0}^{d-1} \mathcal{O}_{L_j} x^i$ is a maximal order in D_j.*

Now $v(\tau^u) = v((\tau^u)^d)/d = v(a)/d$, hence for a uniformizer h of v in F_v,

$$v(h^m(\tau^u)^n) = m + nv(a)/d.$$

Since $(v(a), d) = 1$ the extended Euclidean algorithm yields $m, n \in \mathbb{Z}$ with $md + nv(a) = 1$, and $h^m(\tau^u)^n$ is the required element. Hence, in D_j we get the maximal order:

$$\mathcal{O}_{D_j} := \mathcal{O}_{L_j}[h^m(\tau^u)^n].$$

Next, we will give an explicit description of a maximal order in $(M/F_v, \sigma, a)$ as stabilizer of a suitable lattice.

Lemma 32. *$V := \bigoplus_{i=0}^{u-1} D_i\tau^i$ is a left $(M/F_v, \sigma, a)$-submodule of $(M/F_v, \sigma, a)$.*

Proof. V is obviously closed under addition. It remains to show that left multiplication with ‘scalars’ sends V to V. So let

$$a = \sum_{i,j=0}^{u-1} \alpha_i\tau^j \in (M/F_v, \sigma, a), \qquad x = \sum_{i=0}^{u-1} \beta_i\tau^i \in V.$$

Then a straightforward calculation shows

$$a \cdot x = \sum_{i,j=0}^{u-1} \alpha_i\tau^j \sum_{k=0}^{u-1} \beta_k\tau^k = \sum_{i,j,k=0}^{u-1} \alpha_i\sigma^j(\beta_k)\tau^{j+k} \overset{(6.1)}{=} \sum_{i,j,k=0, j+k=i}^{u-1} \alpha_i\sigma^j(\beta_k)\tau^i \in V. \qquad \square$$

We now define a maximal lattice in V by $\Lambda_V := \bigoplus_{i=0}^{u-1} \mathcal{O}_{D_i}\tau^i$.
Furthermore, define three lattices in $M[\tau]/(\tau^r - a)$:

$$R_0 := \bigoplus_{i=0}^{u-1} \bigoplus_{j=i-u+1}^{i} \mathcal{O}_{D_i}\tau^j \subseteq R_1 := \bigoplus_{i=0}^{u-1}\bigoplus_{j=0}^{u-1} \mathcal{O}_{D_i}\tau^j \subseteq R_2 := \bigoplus_{i=0}^{u-1}\bigoplus_{j=0}^{u-1} \mathcal{O}_{L_i}[\tau^u]\tau^j.$$

Note that R_1 is the v-adic closure of $\mathcal{O}_L[\tau, h^m(\tau^u)^n]$ and R_2 the v-adic closure of $\mathcal{O}_L[\tau]$.

Theorem 33. *R_0 equals the stabilizer of Λ_V (and is therefore a maximal order).*

Proof. Let i, k run from 0 to $u - 1$ and j from $i - u + 1$ to i. Note first that $\mathcal{O}_{D_i}\tau^j\mathcal{O}_{D_k}\tau^k = \mathcal{O}_{D_i}\sigma^j(\mathcal{O}_{D_k})\tau^{j+k} = \mathcal{O}_{D_i}\mathcal{O}_{D_{j+k}}\tau^{j+k}$. By (6.1) the last term is non-zero only if $i = j + k$, in which case it lies in Λ_V. This proves ‘$\subseteq$’.

We now show the converse inclusion ‘$\supseteq$’. Let $\alpha = \sum_{i,j} \alpha_{ij}\tau^j$ with $\alpha_{ij} \in D_i$ for all $i = 0, \ldots, u - 1$. If α lies in the stabilizer, then it maps test elements $x = \beta_k\tau^k$ with $\beta_k \in \mathcal{O}_{D_k}$ to Λ_V:

$$\alpha x = \sum_i \alpha_{i,i-k}\sigma^{i-k}(\beta_k)\tau^i \overset{!}{\in} \Lambda_V.$$

From this we deduce that $\alpha_{i,i-k} \in \mathcal{O}_{D_i}$ for all $k = 0, \ldots, u - 1$. Therefore $\alpha \in R_0$. $\square$

The explicit description of the maximal order R_0 can be lifted to that of a global order maximal at v. Before stating this result, we need a short lemma.

LEMMA 34. *Choose integers e_t for $t = 0, \ldots, u-1$ such that*

$$\mathcal{O}_{D_i} = \mathcal{O}_{L_i}[h^m(\tau^u)^n] = \bigoplus_{t=0}^{d-1} \mathcal{O}_{L_i} h^{e_t}(\tau^u)^t.$$

Furthermore, set $e_d := -v(a)$, so that $\mathcal{O}_{D_i} = \bigoplus_{t=1}^{d} \mathcal{O}_{L_i} h^{e_t}(\tau^u)^t$. Then $e_{t-1} - e_t \in \{0,1\}$ for all $0 < t \leqslant d$.

Proof. $h^{e_t}(\tau^u)^t$ has valuation between 0 and $1 - 1/d$, so

$$1 > |v(h^{e_{t-1}}(\tau^u)^{t-1}) - v(h^{e_t}(\tau^u)^t)| = |e_{t-1} - e_t - v(\tau^u)|.$$

Noting that $0 \leqslant v(\tau^u) = v(a)/d \overset{(4.2)}{=} (g_i d/r_i)/d = g_i/r_i < 1$, the claim follows. □

We now rewrite the maximal order R_0:

$$\begin{aligned} R_0 &= \bigoplus_{i=0}^{u-1} \bigoplus_{j=i-u+1}^{i} \bigoplus_{s=0}^{d-1} \mathcal{O}_{L_i} h^{e_s}(\tau^u)^s \tau^j = R_1 + \bigoplus_{i=0}^{u-1} \bigoplus_{j=i+1}^{u-1} \bigoplus_{s=0}^{d-1} \mathcal{O}_{L_i} h^{e_s}(\tau^u)^s \tau^{j-u} \\ &= R_1 + \bigoplus_{i=0}^{u-1} \bigoplus_{j=i+1}^{u-1} \bigoplus_{s=0}^{d-1} \mathcal{O}_{L_i} h^{e_s}(\tau^u)^{s-1} \tau^j = R_1 + \bigoplus_{i=0}^{u-1} \bigoplus_{j=i+1}^{u-1} \bigoplus_{s=0}^{d-1} \mathcal{O}_{L_i} h^{e_{s+1}}(\tau^u)^s \tau^j. \end{aligned}$$

Let $(\bar{b}_{ij})_{j=0,\ldots,d-1}$ be a basis of k_i/k (the residue field of L_i over that of F_v) for all $i = 0, \ldots, u-1$. Choose lifts $\tilde{b}_{ij}$ to $\mathcal{O}_{L_i}$ and b_{ij} to $\mathcal{O}_L$. Note that $\mathcal{O}_L/(h) = \bigoplus_i \mathcal{O}_{L_i}/(h)$, so that b_{ij} can be thought of as a first-order approximation of the tuple $(0, \ldots, 0, \tilde{b}_{ij}, 0, \ldots, 0)$. Then

$$R_0 = R_1 + \sum_{i=0}^{u-1} \sum_{j=i+1}^{u-1} \sum_{s=0}^{d-1} \sum_{t=0}^{d-1} A_v \tilde{b}_{it} h^{e_{s+1}}(\tau^u)^s \tau^j = R_1 + \sum_{i=0}^{u-1} \sum_{j=i+1}^{u-1} \sum_{s=0}^{d-1} \sum_{t=0}^{d-1} A_v b_{it} h^{e_{s+1}}(\tau^u)^s \tau^j.$$

The last equation follows because

$$A_v(\tilde{b}_{it} - b_{it}) h^{e_{s+1}}(\tau^u)^s \tau^j \subset \bigoplus \mathcal{O}_{L_i} h^{e_{s+1}+1}(\tau^u)^s \tau^j \overset{\text{Lemma 34}}{\subset} \bigoplus \mathcal{O}_{L_i} h^{e_s}(\tau^u)^s \tau^j \subset R_1.$$

The above formula for R_0 provides a global lift of R_0. It is the order

$$\mathcal{O}_L[\tau, h^m(\tau^u)^n] + \sum_{i=0}^{u-1} \sum_{j=i+1}^{u-1} \sum_{s=0}^{d-1} \sum_{t=0}^{d-1} A b_{it} h^{e_{s+1}}(\tau^u)^s \tau^j.$$

Fixing the denominator at other places is not necessary.

6.4. *Unramified places $v \notin S$*

For these places, any order containing $\Lambda = \mathcal{O}_L[\tau]$ will be maximal since the discriminant commutes with localization and $\operatorname{disc}(\Lambda) = a^{d(d-1)} \operatorname{disc}(L/K)$ is a local unit.

7. *Example*

The following results were obtained by the authors using their Magma implementation of the described algorithms. Even for the small example chosen, performance was considerably better (0.130 s) compared to Magma's generic built-in function for maximal orders in associative structure constant algebras (104.600 s).

https://doi.org/10.1112/S1461157016000310 Published online by Cambridge University Press

Here, $q = 5$ and the chosen invariants are $1/2$, $1/4$ and $1/4$ at the places $h_1 = t$, $h_2 = t^2+t+1$ and $h_3 = t^3 + t^2 + 1$, respectively. Then the algorithm finds a suitable ramification place w with $h_w = t^2 + 3t + 4$. The cyclic algebra is computed as $(L/F, \sigma, a) = L[\tau]/(\tau^4 - a)$, where L has primitive element α with minimal polynomial

$$T^4 - (t + 4)^4 h_w,$$

the chosen generator of $\mathrm{Gal}(L/F)$ is

$$\sigma : \alpha \to 2\alpha$$

and

$$a = t(t^2 + t + 1)(t^3 + t^2 + 1)^3.$$

Defining $\beta = \alpha/(t + 4)$, we get

$$\mathcal{O}_L = A[\beta].$$

An A-basis of the computed maximal order is given by the following 16 elements:

$$\begin{gathered}
\tau^0, \quad \frac{1}{h_w}\beta\tau^0 + \frac{4t+2}{h_w}\beta\tau^1 + \frac{4t+1}{h_w h_3}\beta\tau^2 + \frac{t+3}{h_w h_1 h_3^2}\beta\tau^3 + \frac{4}{h_1 h_3^2}\beta^3\tau^3, \\
\frac{1}{h_w}\beta^2\tau^0 + \frac{2t+3}{h_w h_3}\beta^2\tau^2 + \frac{2t}{h_w h_3^2}\beta^2\tau^3, \quad \frac{1}{h_w}\beta^3\tau^0 + \frac{4t}{h_w h_3^2}\beta^3\tau^3, \\
\tau^1, \quad \beta\tau^1, \quad \frac{1}{h_w}\beta^2\tau^1 + \frac{3t+3}{h_w h_3}\beta^2\tau^2 + \frac{3t+4}{h_w h_3^2}\beta^2\tau^3, \quad \frac{1}{h_w}\beta^3\tau^1 + \frac{4t+2}{h_w h_3^2}\beta^3\tau^3, \\
\frac{1}{h_3}\tau^2, \quad \frac{1}{h_3}\beta\tau^2, \quad \frac{1}{h_3}\beta^2\tau^2, \quad \frac{1}{h_w h_3}\beta^3\tau^2 + \frac{2t+2}{h_w h_3^2}\beta^3\tau^3, \\
\frac{1}{h_1 h_3^2}\tau^3 + \frac{2}{h_1 h_3^2}\beta^2\tau^3, \quad \frac{1}{h_1 h_3^2}\beta\tau^3 + \frac{2}{h_1 h_3^2}\beta^3\tau^3, \quad \frac{1}{h_3^2}\beta^2\tau^3, \quad \frac{1}{h_3^2}\beta^3\tau^3.
\end{gathered}$$

Note that h_2 does not appear in the denominators because the order $\mathcal{O}_L[\tau]$ we started with was already maximal at this place, as can be checked with the discriminant.

Acknowledgements. We thank Nils Schwinning for formulating the basis of this paper in his master's thesis [16]. There he implemented an algorithm for computing a cyclic algebra from given invariants in the number field case that was suggested by G. B., as was the analysis of the effectiveness of the algorithm. Both authors thank the referees for helpful remarks and for suggesting Theorem 9.

References

1. B. Anglès, 'Bases normales relatives en caractéristique positive', *J. Théor. Nombres Bordeaux* 14 (2002) no. 1, 1–17.
2. G. Böckle and R. Butenuth, 'On computing quaternion quotient graphs for function fields', *J. Théor. Nombres Bordeaux* 24 (2012) no. 1, 73–99.
3. R. J. Chapman, 'Carlitz modules and normal integral bases', *J. Lond. Math. Soc.* (2) 44 (1991) no. 2, 250–260.
4. M. Deuring, *Algebren*, 2nd edn, Ergebnisse der Mathematik und ihrer Grenzgebiete 41 (Springer, Berlin, 1968).
5. S. Galovich and M. Rosen, 'Units and class groups in cyclotomic function fields', *J. Number Theory* 14 (1982) no. 2, 156–184.
6. D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 35 (Springer, Berlin, 1996).
7. V. Guruswami, 'Cyclotomic function fields, Artin–Frobenius automorphisms, and list error correction with optimal rate', *Algebra Number Theory* 4 (2010) no. 4, 433–463.
8. J. C. Jantzen and J. Schwermer, *Algebra* (Springer, Berlin, 2006).

https://doi.org/10.1112/S1461157016000310 Published online by Cambridge University Press

9. D. E. Knuth, *The art of computer programming, Vol. 1: Fundamental algorithms*, 3rd edn (Addison-Wesley, Reading, MA, 1997).

10. G. Lettl, 'The ring of integers of an abelian number field', *J. reine angew. Math.* 404 (1990) 162–170.

11. F. Lorenz, 'Fields with structure, algebras and advanced topics', *Algebra, Vol. II*, Universitext (Springer, New York, 2008). Translated from the German by Silvio Levy, with the collaboration of Levy.

12. J. Neukirch, *Algebraische Zahlentheorie*, 1st edn (Springer, Berlin, 1992).

13. I. Reiner, *Maximal orders* (Academic Press, London, 1975).

14. M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics 210 (Springer, New York, 2002).

15. M. Rzedowski-Calderón and G. Villa-Salvador, 'Conductor-discriminant formula for global function fields', *Int. J. Algebra* 5 (2011) no. 29–32, 1557–1565.

16. N. Schwinning, 'Ein Algorithmus zur Berechnung von Divisionsalgebren über $\mathbb{Q}$ zu vorgegebenen Invarianten', Diplomarbeit, Universität Duisburg-Essen, Germany, 2011.

17. J.-P. Serre, *Local fields*, Graduate Texts in Mathematics 67 (Springer, New York, 1979). Translated from the French by Marvin Jay Greenberg.

Gebhard Böckle
Universität Heidelberg
Interdisziplinäres Zentrum für wissenschaftliches Rechnen (IWR)
Im Neuenheimer Feld 368
69120 Heidelberg
Germany

gebhard.boeckle@iwr.uni-heidelberg.de

Damián Gvirtz
The London School of Geometry and Number Theory
Department of Mathematics
University College London
Gower Street
London WC1E 6BT
United Kingdom

damian.gvirtz.15@ucl.ac.uk

https://doi.org/10.1112/S1461157016000310 Published online by Cambridge University Press