Journal of Algebra 664 (2025) 631–654

Contents lists available at ScienceDirect

Journal of Algebra

journal homepage: www.elsevier.com/locate/jalgebra

Research Paper

A parametrization of nonassociative cyclic algebras of prime degree

Monica Nevins [a,1], Susanne Pumplün [b,*]

[a] *Department of Mathematics and Statistics, University of Ottawa, Ottawa, K1N 6N5, Canada*
[b] *School of Mathematical Sciences, University of Nottingham, Nottingham NG7 2RD, United Kingdom*

ARTICLE INFO

Article history:
Received 24 June 2024
Available online 24 October 2024
Communicated by Alberto Elduque

MSC:
17A35
17A99

Keywords:
Nonassociative division algebras
Nonassociative cyclic algebras

ABSTRACT

We determine and explicitly parametrize the isomorphism classes of nonassociative quaternion algebras over a field of characteristic different from two, as well as the isomorphism classes of nonassociative cyclic algebras of odd prime degree m when the base field contains a primitive mth root of unity. In the course of doing so, we prove that any two such algebras can be isomorphic only if the cyclic field extension and the chosen generator of the Galois group are the same. As an application, we give a parametrization of nonassociative cyclic algebras of prime degree over a local nonarchimedean field F, which is entirely explicit under mild hypotheses on the residual characteristic. In particular, this gives a rich understanding of the important class of nonassociative quaternion algebras up to isomorphism over nonarchimedean local fields.

* Corresponding author.
E-mail addresses: mnevins@uottawa.ca (M. Nevins), Susanne.Pumpluen@nottingham.ac.uk (S. Pumplün).

[1] The first author's research is supported NSERC Discovery Grant RGPIN-2020-05020.

https://doi.org/10.1016/j.jalgebra.2024.10.021

1. Introduction

The general study of the classification and construction of nonassociative algebras is a classical subject, dating back to pioneering works of [1,2,7]. It is a rich area, including such important examples as Jordan algebras which go back to [12], and semifields (*i.e.*, nonassociative division algebras over finite fields).

In this paper, we give a parametrization of the isomorphism classes of a particular class of nonassociative algebras first defined (slightly more generally) as Sandler semifields in [27], and later studied over any base field (*e.g.* in [30]): nonassociative cyclic algebras of degree m (Definition 2.1). They are defined by a cyclic Galois field extension K/F of degree m, a generator σ of $\mathrm{Gal}(K/F)$, and an element $a \in K \setminus F$, and are denoted $(K/F, \sigma, a)$. In particular, when the degree m is prime, and F contains a primitive mth root of unity, a nonassociative cyclic algebra of degree m over F is necessarily a division algebra [30]. These algebras are a direct generalization of associative cyclic algebras which, over local and global fields F, generate the Brauer group of (associative) central simple algebras over F. Associative central simple algebras similarly arise as the key objects in the theorems of Merkurjev and Suslin on the m-torsion of Brauer groups over arbitrary fields.

After deriving our explicit parametrizations (in the quadratic case in Theorem 4.2 and in the case of extensions of odd prime degree m, assuming F contains a primitive mth root of unity in Theorem 5.5), we go on to apply our parametrization to nonassociative cyclic algebras over local nonarchimedean fields F. These are the finite algebraic extensions of the p-adic numbers $\mathbb{Q}_p$, together with Laurent series over a finite field. Local nonarchimedean fields lie at the intersection of real and finite fields: they are complete locally compact fields that are suitable for use in analysis, but retain abundant number-theoretic properties related to their finite residue fields. We exploit these features to give a classification that is elegant and completely explicit under mild hypotheses on the field: for nonassociative quaternion algebras, the relevant results are Theorems 4.4, 4.5 and 4.6; for higher prime degree, our general result follows from Proposition 5.6 and we present in detail the case of $m = 3$ in Theorem 5.7.

In the course of deriving our results, we also prove the following counterintuitive result (Theorem 5.1), valid for nonassociative cyclic algebras of arbitrary degree (and in direct contrast with the associative case).

Theorem. *Let F be an arbitrary field and let $m \geq 3$ be the degree of a cyclic Galois extension K/F. For any two distinct generators $\sigma_1 \neq \sigma_2$ of the Galois group* $\mathrm{Gal}(K/F)$*, and for any $a_1, a_2 \in K \setminus F$, we have*

$$(K/F, \sigma_1, a_1) \ncong (K/F, \sigma_2, a_2).$$

Given the importance of associative cyclic algebras in the Brauer group of F, it is natural to expect that nonassociative cyclic algebras (which are pivotal examples of

semiassociative algebras) will play a similarly central role in the recently defined semiassociative Brauer monoid [4,23]. Nonassociative cyclic algebras also recently appeared as first examples of residue m-hyperrings [26, Example 4.10 (i), Remark 4.11].

Furthermore, in the special case that m is equal to 2, the nonassociative cyclic algebras over F are exactly all the four-dimensional unital algebras over F which have a separable quadratic field extension of F contained in their nucleus [31]. They are also identical to the nonassociative quaternion (division) algebras that are obtained by a generalized Cayley-Dickson doubling [3].

In general, the classification of n-dimensional nonassociative algebras is a wild problem. Rough classifications up to the derivation types of the algebras, or up to their automorphism groups, are more tractable, and are possible for small dimensions, fixed base fields, or certain families of nonassociative algebras. Classifications up to isotopy, or even up to isomorphism, are often difficult even for small dimensions and special base fields. Investigations of special classes of small dimensional algebras usually involve structure constants. For a comprehensive recent literature review, see [13, Section 2.1].

Three- and four-dimensional nonassociative division algebras over a p-adic field were roughly classified up to isotopy in [6] and Limburg [17] by studying the determinant of the matrix of their left multiplication and classifying it up to isometry. Unfortunately, this classification does not reveal the algebraic structure for some of the classes of algebras listed.

To our knowledge, ours are some of the first known parametrizations of a large class of nonassociative division algebras over nonarchimedean local fields F, and our work invites several interesting next directions.

For one, there should be a relationship between the nonassociative cyclic algebras arising from unramified extensions and those arising from the corresponding extensions of the finite residue field, through localization. Note that nonassociative cyclic algebras are special cases of Petit algebras [19,20,16], and over finite base fields isotopic to Jha-Johnson semifields [11], which form one of the largest known classes of semifields. However, it is evident from examples that this localization depends on the parameters in ways that are not evident from the high-level theory.

We also believe that the explicit nature of our parameterization will help in tackling concrete open problems in the new theory of semiassociative algebras. We note that nonassociative cyclic algebras are also employed in the construction of space-time codes which are used in digital data transmission, and in linear code constructions; see, for example, [22,24,25]. It would be very interesting to explore how to exploit the essentially binary nature of nonassociative cyclic algebras over $\mathbb{F}_2(\!(t)\!)$, for example, to the development of more efficient linear codes.

The paper is organized as follows. We set our notation and collect some main results on nonassociative cyclic algebras and nonarchimedean local fields in Sections 2 and 3. In Section 4 we prove our parametrization (a classification up to isomorphism) of nonassociative quaternion algebras, first over general fields of characteristic different from 2 (Theorem 4.2), and then specialized to nonarchimedean local fields, including the

characteristic 2 case, which has a very different flavor (Theorem 4.6). In particular, we have thus achieved full parametrizations of exactly all four-dimensional unital algebras over F which have a separable quadratic field extension of F contained in their nucleus.

Section 5 contains the two main results of this paper (Theorems 5.1 and 5.5). We then derive the parametrization over local nonarchimedean fields of residual characteristic different from m (and containing μ_m) employing Lemma 5.6 and in particular for degree three in Section 5.4. We conclude in Section 6 with a short exploration of the case of degree 4 nonassociative cyclic algebras over a local nonarchimedean field such that $p \neq 2$.

2. Notation and background

We use $R^\times$ to denote the group of invertible elements of a unital associative ring R, and denote by $(R^\times)^n$ the subgroup $\{x^n \mid x \in R^\times\}$. Let F be a field and let μ_m be the group of mth roots of unity in a fixed algebraic closure of F, when the characteristic of F does not divide m.

2.1. Nonassociative algebras

An F-vector space A is an *algebra* over F if there exists an F-bilinear map $A \times A \to A$, $(x, y) \mapsto x \cdot y$. We denote this *multiplication* in A simply by the juxtaposition xy. An algebra A is called *unital* if there is an element in A, denoted by 1, such that $1x = x1 = x$ for all $x \in A$. We will only consider unital finite-dimensional nonzero algebras.

Define the *associator* of A by $[x, y, z] = (xy)z - x(yz)$. The *left, middle and right nucleus* of A are defined as $\mathrm{Nuc}_l(A) = \{x \in A \,|\, [x, A, A] = 0\}$, $\mathrm{Nuc}_m(A) = \{x \in A \,|\, [A, x, A] = 0\}$ and $\mathrm{Nuc}_r(A) = \{x \in A \,|\, [A, A, x] = 0\}$, respectively. These are associative subalgebras of A and their intersection $\mathrm{Nuc}(A) = \{x \in A \,|\, [x, A, A] = [A, x, A] = [A, A, x] = 0\}$ is the *nucleus* of A. The *center* of A is $\mathrm{C}(A) = \{x \in A \,|\, x \in \mathrm{Nuc}(A) \text{ and } xy = yx \text{ for all } y \in A\}$.

An algebra $A \neq 0$ is called a *division algebra* if for any $a \in A$, $a \neq 0$, the left multiplication with a, $L_a(x) = ax$, and the right multiplication with a, $R_a(x) = xa$, are bijective. If A has finite dimension over F, A is a division algebra if and only if A has no zero divisors [28, pp. 15, 16].

2.2. Nonassociative cyclic algebras

We now define our principal objects of study; we adapt the definition from [30], where the opposite algebras were considered instead.

Definition 2.1. Let K/F be a cyclic Galois field extension of degree m and let σ be a generator of $\mathrm{Gal}(K/F)$. Then for any $a \in K^\times$, the *nonassociative cyclic algebra* $(K/F, \sigma, a)$ *of degree* m is the unital algebra of dimension m^2 defined by

$$(K/F,\sigma,a)=\bigoplus_{s=0}^{m-1}Kt^s$$

with F-bilinear multiplication defined for $0\leq s,s'<m$ and $k,k'\in K$ by

$$(kt^s)(k't^{s'})=\begin{cases}k\sigma^s(k')t^{s+s'} & \text{if } s+s'<m;\\ k\sigma^s(k')at^{s+s'-m} & \text{if } s+s'\geq m.\end{cases} \tag{2.1}$$

In particular, $t^m=a$.

Note that for all $a\in K\setminus F$ the algebra $(K/F,\sigma,a)$ is not associative, not even power-associative, since for example $t(t^m)=ta=\sigma(a)t$ but $(t^m)t=at$. If we instead choose $a\in F^\times$, then the definition above yields the classical central simple associative cyclic algebra $(K/F,\sigma,a)$ of degree m [10, §1.4]. In the following, we call a nonassociative cyclic algebra $(K/F,\sigma,a)$ that is not associative (*i.e.* $a\in K\setminus F$) sometimes also a *proper* nonassociative cyclic algebra.

An equivalent way to define $(K/F,\sigma,a)$ involves twisted polynomials: Let $f(t)=t^m-d\in R=K[t;\sigma]$. Then $R_m=\{g\in K[t;\sigma]\,|\,\deg(g)<m\}$ together with the usual addition and the multiplication defined via $g\circ h=gh \bmod_r f$, where the right hand side is simply the remainder of gh after division by f of the right, is the nonassociative cyclic algebra $(K/F,\sigma,a)$, also denoted by $R/R(t^m-a)$ as it is a special case of a Petit algebra [19]. Note that when $\deg(g)+\deg(h)<m$, the multiplication in $(K/F,\sigma,a)$ is the same as the multiplication in R. If $a\in F^\times$ then $(K/F,\sigma,a)$ is the classical central simple associative cyclic algebra $(K/F,\sigma,a)$ which can also be written as the quotient algebra $K[t;\sigma]/(f)$ [19, (7), (9), (10)], [10, p. 19]. This justifies the notation R/Rf introduced by Petit.

We record some quick properties.

Lemma 2.2. *[19] Let $A=(K/F,\sigma,a)$ with $a\in K\setminus F$. Then $C(A)=F$, $\mathrm{Nuc}_l(A)=\mathrm{Nuc}_m(A)=K$ and $\mathrm{Nuc}_r(A)=\{g\in R/Rf\,|\,fg\in Rf\}$.*

Note that $\{g\in R/Rf\,|\,fg\in Rf\}$ can be identified as the 0-eigenspace of the right multiplication operator R_f, also called the *eigenspace of f* [19].

In particular when m is prime we must have $\mathrm{Nuc}_r((K/F,\sigma,a))=K$. We also know that $(K/F,\sigma,a)$ is a division algebra if and only if $\mathrm{Nuc}_r((K/F,\sigma,a))$ is a division algebra, *e.g.* see [9, Proposition 4].

Nonassociative cyclic algebras of degree 2 are also called *nonassociative quaternion algebras*, and were first described by Dickson [7]. They can also be constructed by a generalized Cayley-Dickson process $\mathrm{Cay}(K,a)$ [3, Lemma 1], as it coincides with the specialization to $m=2$ of Definition 2.1.

2.3. Properties and isomorphisms

Let us now summarize some needed results from the literature.

Theorem 2.3. *[19] Suppose either that $m = 2$ or 3, or that $m \geq 5$ is a prime such that F contains a primitive mth root of unity. Let $a \in K \setminus F$. Then $(K/F, \sigma, a)$ is a division algebra.*

The case $m = 2$ is distinguished: nonassociative quaternion algebras are, up to isomorphism, the only four-dimensional unital division algebras over a field F that have a quadratic field extension K/F in their nucleus, and which are not associative [31, Theorem 1]. We thus put a special emphasis on them in this paper.

When m is not prime, we have the following statement.

Theorem 2.4. *[30, Theorem 4.4, Corollary 4.5] Suppose that $(K/F, \sigma, a)$ is a nonassociative cyclic algebra where K/F is of degree m. If a does not lie in a proper subfield of K/F, then $(K/F, \sigma, a)$ is a division algebra.*

Proof. If $1, a, \cdots, a^{m-1}$ are linearly independent over F, then $(K/F, \sigma, a)$ is a division algebra [30, Theorem 4.4]. The elements $1, a, \cdots, a^{m-1}$ are linearly independent over F if and only if the minimal polynomial of a over F has degree at least m, whence $F(a)/F$ has degree at least m. Thus this condition is equivalent to having $K = F(a)$ and thus that a lies in no proper subfield of K. □

We now turn to the question of when two such algebras are isomorphic.

Lemma 2.5. *Suppose K, K' are two distinct cyclic Galois extensions of a field F. Then for any generators σ, σ' of their respective Galois groups, and any $a \in K \setminus F$, $a' \in K' \setminus F$, we have*

$$(K/F, \sigma, a) \ncong (K'/F, \sigma', a').$$

The proof is immediate, since isomorphic algebras will have the same left nuclei. In the rest of the paper, we will rely on the following strong classification theorem [5, Corollary 32].

Theorem 2.6. *Let K be a cyclic Galois extension of F and let σ be a generator of $\mathrm{Gal}(K/F)$. For $a, b \in K \setminus F$ we have that $(K/F, \sigma, a) \cong (K/F, \sigma, b)$ if and only if there exists some $\tau \in \mathrm{Gal}(K/F)$ such that*

$$a \in \tau(b) N_{K/F}(K^\times). \tag{2.2}$$

For each such extension K, we denote by $\sim$ the equivalence relation on $K \setminus F$ induced by (2.2), that is, $a \sim b$ if and only if there is some power $i \in \mathbb{Z}$ such that $a \in \sigma^i(b)N_{K/F}(K^\times)$.

3. Background on p-adic fields

A local nonarchimedean field is a locally compact, nondiscrete field equipped with an ultrametric norm $|\cdot|$. For each prime number p, there are precisely two kinds: the finite algebraic extensions of the p-adic numbers $\mathbb{Q}_p$, which are the completion of a number field with respect to the p-adic norm; and the fields $\mathbb{F}_q(\!(t)\!)$ of Laurent series over a finite field of order $q = p^n$ for some $n \geq 1$, with $|t| < 1$. The former are called p-adic fields, and have characteristic zero. An excellent resource for the summary given here is [14, Chapter II]; for examples, see [18].

Let F be a local nonarchimedean field. Its integer ring is its maximal compact open subring $\mathcal{R} = \{x \in F : |x| \leq 1\}$. This ring is local, with unique maximal ideal $\mathcal{P} = \{x \in F : |x| < 1\}$. Its unit subgroup of invertible elements is then $\mathcal{R}^\times = \mathcal{R} \setminus \mathcal{P}$. The quotient $\kappa := \mathcal{R}/\mathcal{P}$, called the *residue field* of F, is a finite field of order $q = p^n$ for some $n \in \mathbb{N}$ and prime p (called the *residual characteristic* of F).

Example 3.1. If $F = \mathbb{F}_q(\!(t)\!)$ then $\mathcal{R} = \mathbb{F}_q[\![t]\!]$, $\mathcal{P} = (t)$, and $\kappa = \mathbb{F}_q$. Similarly, if $F = \mathbb{Q}_p$ then we have

$$\mathbb{Q}_p^\times = \{a = \sum_{i=N}^{\infty} a_i p^i : N \in \mathbb{N}, a_i \in \{0, 1, \ldots, p-1\}\}$$

with addition and multiplication computed "with carrying" as one would for finite sums. Here the least i such that $a_i \neq 0$ is the p-adic valuation of a, and in this case $|a| = p^{-i}$. The p-adic integers $\mathcal{R} = \mathbb{Z}_p$ is the set of all elements of valuation at least 0.

More generally, we define the valuation of $a \in F^\times$ by $v(a) = \min\{n \in \mathbb{Z} : a \in \mathcal{P}^n\}$ and scale the norm so that $|a| = q^{-v(a)}$. We fix a generator ϖ of $\mathcal{P}$ for once and for all; it satisfies $v(\varpi) = 1$.

The fundamental relationship between F and κ is captured by Hensel's Lemma. The following general version is adapted from [8, Thm 7.3].

Lemma 3.2 *(Hensel's Lemma). Let $f(x) \in \mathcal{R}[x]$ be a polynomial and $f'(x)$ its formal derivative. If $a \in \mathcal{R}$ satisfies*

$$f(a) \equiv 0 \mod f'(a)^2\mathcal{P},$$

then there exists a unique $b \in \mathcal{R}$ satisfying

$$f(b) = 0 \quad \textit{and} \quad b \equiv a \mod f'(a)\mathcal{P}.$$

Example 3.3. The elements of $\kappa^\times$ are the roots of $f(x) = x^{q-1} - 1$. For each $\overline{a} \in \kappa^\times$, choose $a \in \mathcal{R}$ to be some preimage. Since $f(a) \equiv 0 \mod \mathcal{P}$ and $f'(a) = (q-1)a^{q-2} \in \mathcal{R}^\times$, Hensel's Lemma implies that there exists a unique $b \in \mathcal{R}$ satisfying $b^{q-1} = 1$ and such that $b \in a + \mathcal{P}$. The set of all such b (sometimes called Teichmüller lifts of elements of $\kappa^\times$) are distinct and form the group of $(q-1)$th roots of unity μ_{q-1} in F. Note that we similarly recover $\mu_n \cap F$ for any n not divisible by p, and this group will have order n exactly when $n|(q-1)$.

It is sometimes convenient to decompose $F^\times$ as the direct product of groups

$$F^\times \cong \mu_{q-1} \times (1 + \mathcal{P}) \times \mathbb{Z} \tag{3.1}$$

via the map that associates to a triple (b, u, n) the element $bu\varpi^n$.

Finite algebraic extensions of F are again local nonarchimedean fields and they come in two forms. There is a unique (Galois) *unramified extension* of each degree n, which is the splitting field of $x^{q^n} - x$. We often denote it L_n. Its residue field is $\kappa_{L_n} \cong \mathbb{F}_{q^n}$ and its maximal ideal $\mathcal{P}_{L_n}$ is generated over $\mathcal{R}_{L_n}$ by ϖ.

At the other extreme are the totally ramified extensions K of F of degree n, of which there are usually several (in fact, infinitely many if the characteristic of F is $p = n$), and not all of which are Galois. They each have the property that their residue field satisfies $\kappa_K \cong \kappa$ and ϖ generates $\mathcal{P}_K^n$.

A general finite algebraic extension K of F can be uniquely factored as an unramified extension L/F of degree f followed by a totally ramified extension K/L of degree e, the *ramification index*. We say K/F is *tamely ramified* if $(e, p) = 1$ and *wildly ramified* if not. The totally and tamely ramified extensions of degree e are all obtained by adjoining to F a root of $x^n - u\varpi$, for some choice of $u \in \mathcal{R}^\times/(\mathcal{R}^\times)^e$; these are Galois only if F contains a primitive eth root of unity.

By local class field theory [14, XI §4], the Galois extensions of degree n of F are in one-to-one correspondence with the subgroups of index n of $F^\times$, via the map that assigns K/F to the subgroup $N_{K/F}(K^\times)$, which is the image of the norm map. In particular, this implies that $F^\times/N_{K/F}(K^\times)$ is a finite group of order n equal to the degree of the extension.

For example, if $K = L_n$ is an unramified extension, then upon restriction to the integer ring, the norm map $N_{K/F} : \mathcal{R}_K^\times \to \mathcal{R}^\times$ is surjective, and the group $F^\times/N_{K/F}(K^\times)$ is represented by the elements

$$\{1, \varpi, \varpi^2, \cdots, \varpi^{n-1}\}.$$

On the other hand, for a totally and tamely ramified extension, $F^\times/N_{K/F}(K^\times) \cong \mathcal{R}^\times/(\mathcal{R}^\times)^n$ and Hensel's Lemma identifies this group with $\kappa^\times/(\kappa^\times)^n$.

These features make the explicit classification of nonassociative cyclic algebras over F quite tractable.

4. Nonassociative quaternion algebras

In this section, we first derive some general results about nonassociative quaternion algebras and then apply these to the case of local nonarchimedean fields. As noted, these algebras exhaust the four-dimensional unital nonassociative division algebras that contain a quadratic field extension in their nucleus.

4.1. Isomorphism classes of nonassociative quaternion algebras in odd characteristic

Throughout this section, let F denote an arbitrary field of characteristic different from two.

Lemma 4.1. *If A is a proper nonassociative quaternion algebra over F, then there exists a* unique *(nontrivial) coset $c(F^\times)^2 \in F^\times/(F^\times)^2$ and an element $a \in F(\sqrt{c}) \setminus F$ such that*

$$A \cong (F(\sqrt{c})/F, \sigma, a),$$

where $\sigma \in \mathrm{Gal}(F(\sqrt{c})/F)$ denotes the unique nontrivial element of the Galois group of this quadratic extension.

Proof. Since the characteristic of F is odd, or zero, the distinct quadratic field extensions of F are given by $F(\sqrt{c})$ as c runs over the distinct nontrivial classes in $F^\times/(F^\times)^2$. Applying Lemma 2.5 then yields the assertion. □

We now refine this to an explicit classification of these nonassociative cyclic algebras.

Theorem 4.2. *Suppose K is a separable quadratic extension of a field F of the form $K = F(\sqrt{c})$, for some $c \in F^\times \setminus (F^\times)^2$ and let $\sigma \in \mathrm{Gal}(K/F)$ be nontrivial. Let $\mathcal{C}_K$ denote a set of coset representatives of $F^\times/N_{K/F}(K^\times)$. Then the distinct isomorphism classes of the nonassociative quaternion algebras with left nucleus K are represented by $(K/F, \sigma, a)$ where a is chosen from the set $\mathcal{S}(K)$ given by*

$$\mathcal{S}(K) = \begin{cases} \{r\sqrt{c}, r + s\sqrt{c} \mid r \in \mathcal{C}_K, s \in F^\times/\{\pm 1\}\} & \text{if } -1 \in N_{K/F}(K^\times) \\ \{r'\sqrt{c} \mid r' \in \mathcal{C}_K/\{\pm 1\}\} & \\ \quad \cup \{r + s\sqrt{c} \mid r \in \mathcal{C}_K, s \in F^\times/\{\pm 1\}\} & \text{if } -1 \notin N_{K/F}(K^\times). \end{cases}$$

Proof. We begin by noting that if $-1 \notin N_{K/F}(K^\times)$, then the quotient group $F^\times/N_{K/F}(K^\times)$ contains a class represented by -1, whence the normal subgroup we denote $\{\pm 1\}$; this defines the expression $\mathcal{C}_K/\{\pm 1\}$.

Since $S \subset K \setminus F$, each $a \in S$ defines a nonassociative cyclic algebra $(K/F, \sigma, a)$ with left nucleus K. By Theorem 2.6, two nonassociative cyclic algebras $(K/F, \sigma, a)$ and $(K/F, \sigma, b)$ are isomorphic if and only if $a \sim b$, that is, if

$$a \in bN_{K/F}(K^\times) \cup \sigma(b)N_{K/F}(K^\times).$$

What we will show is that for every $b \in K \setminus F$, there exists a unique choice of $a \in \mathcal{S}(K)$ such that either $b \in aN_{K/F}(K^\times)$ or $\sigma(b) \in aN_{K/F}(K^\times)$. We begin with existence.

Let $b \in K \setminus F$. Then there exist $b_0 \in F, b_1 \in F^\times$ such that $b = b_0 + b_1\sqrt{c}$.

If $b_0 = 0$, then since $b_1 \in F^\times$, we may write $b_1 = rn$ for a unique choice of $r \in \mathcal{C}_K$ and $n \in N_{K/F}(K^\times)$, whence $b \in r\sqrt{c}N_{K/F}(K^\times)$.

If $b_0 \in F^\times$, then there exists a unique $r \in \mathcal{C}_K$ and $n \in N_{K/F}(K^\times)$ such that $b_0 = rn$. Setting $s = b_1 n^{-1}$, we have

$$b = (r + s\sqrt{c})n \in (r + s\sqrt{c})N_{K/F}(K^\times).$$

Since $\sigma(r + s\sqrt{c}) = r - s\sqrt{c}$, the elements $r \pm s\sqrt{c}$ always represent the same isomorphism class of an algebra. On the other hand, since $\sigma(r\sqrt{c}) = -r\sqrt{c}$, σ preserves the class $r\sqrt{c}N_{K/F}(K^\times)$ if and only if $-1 \in N_{K/F}(K^\times)$, in which case each of these elements represent pairwise nonisomorphic algebras. If $-1 \notin N_{K/F}(K^\times)$, then instead only the elements $r'\sqrt{c}$, for $r' \in \mathcal{C}_K/\{\pm 1\}$, are pairwise nonisomorphic. □

For use in practice, we briefly offer an alternative parametrization of these nonassociative quaternion algebras.

Corollary 4.3. *In the setting of Theorem 4.2, we may alternatively parametrize the distinct isomorphism classes of nonassociative quaternion algebras with left nucleus K by elements of the set $\mathcal{S}'(K)$, where*

$$\mathcal{S}'(K) = \begin{cases} \{t + r\sqrt{c} \mid r \in \mathcal{C}_K, t \in \{0\} \cup F^\times/\{\pm 1\}\} & \text{if } -1 \in N_{K/F}(K^\times); \\ \{t + r\sqrt{c},\ r'\sqrt{c} \mid r \in \mathcal{C}_K, r' \in \mathcal{C}_K/\{\pm 1\}, t \in F^\times/\{\pm 1\}\} & \text{if } -1 \notin N_{K/F}(K^\times). \end{cases}$$

Proof. The elements of the form $r\sqrt{c}$ in $\mathcal{S}(K)$ and $\mathcal{S}'(K)$ are in bijection. Suppose $r + s\sqrt{c} \in \mathcal{S}(K)$. Then $s = r'n$ for a unique $r' \in \mathcal{C}_K$ and $n \in N_{K/F}(K^\times)$. Therefore with $t = rn^{-1}$ we have

$$r + s\sqrt{c} = (rn^{-1} + r'\sqrt{c})n \in (t + r'\sqrt{c})N_{K/F}(K^\times).$$

Since s was only defined as an element of $F^\times/\{\pm 1\}$, the same is true of t, whence the bijection. □

4.2. Case of local nonarchimedean fields of odd residual characteristic

In this section, let F be a nonarchimedean local field of residual characteristic $p \neq 2$; that is, we exclude the finite algebraic extensions of $\mathbb{Q}_2$ and of $\mathbb{F}_2(\!(t)\!)$. We provide a fully explicit parametrization of the nonassociative quaternion algebras in this case, based on Theorem 4.2.

First note that the square classes in $F^\times$ are represented by

$$F^\times/(F^\times)^2 = \{1, \varepsilon, \varpi, \varepsilon\varpi\}$$

where $\varepsilon \in \mathcal{R}^\times \setminus (\mathcal{R}^\times)^2$ is a fixed nonsquare element of valuation zero, which may be thought of as a lift to $\mathcal{R}^\times$ of a nonsquare element of the residue field via Hensel's Lemma 3.2. Therefore there are exactly three distinct quadratic extensions of F in this case:

- $L_2 = F(\sqrt{\varepsilon})$, the unique unramified quadratic extension;
- $K_\varpi = F(\sqrt{\varpi})$, a ramified extension;
- $K_{\varepsilon\varpi} = F(\sqrt{\varepsilon\varpi})$, a second ramified extension.

Secondly, note that local class field theory gives $F^\times/N_{K/F}(K^\times) \cong \mathrm{Gal}(K/F)$. Explicitly, when K/F is quadratic, this means we may take our set of representatives to be

$$\mathcal{C}_K = \begin{cases} \{1, \varpi\} & \text{if } K = L_2 \text{ is unramified over } F; \\ \{1, \varepsilon\} & \text{if } K/F \text{ is ramified.} \end{cases}$$

Thirdly: when $K = L_2$ is unramified, $-1 \in \mathcal{R}^\times \subset N_{K/F}(K^\times)$, independent of $p > 2$. When K/F is ramified, however, then $-1 \in N_{K/F}(K^\times)$ if and only if $-1 \in (F^\times)^2$. Since $p \neq 2$, Hensel's Lemma 3.2 implies this occurs if and only if -1 is a square in the residue field $\mathbb{F}_q$. Since $\mathbb{F}_q^\times$ is a cyclic group of order $q-1$, we infer directly that -1 is a square if and only if $q \equiv 1 \mod 4$.

Finally, note that when $p \neq 2$, we choose a set of representatives for $F^\times/\{\pm 1\}$ via a choice of representatives of $\kappa^\times/\{\pm 1\}$. Let S_κ be such a set; then via the isomorphism $\kappa^\times \cong \mu_{q-1} \subset \mathcal{R}^\times$ of Example 3.3 we can lift this to a subset of $\mathcal{R}^\times$ contained in the subgroup μ_{q-1}. Then using (3.1) we may take

$$F^\times/\{\pm 1\} = \{s u_1 \varpi^n \mid s \in S_\kappa, u_1 \in 1 + \mathcal{P}, n \in \mathbb{Z}\} \cong (\mu_{p-1}/\mu_2) \times (1 + \mathcal{P}) \times \mathbb{Z}.$$

Putting these together gives the following satisfyingly explicit and simple statement.

Theorem 4.4. *Let F be a local nonarchimedean field of odd residual characteristic, and suppose its residue field κ has q elements. Let K be a quadratic extension of F. Then the distinct isomorphism classes of nonassociative quaternion algebras with left nucleus K are given by $(K/F, \sigma, a)$ where $\sigma \in \mathrm{Gal}(K/F)$ is the nontrivial element and $a \in \mathcal{S}(K)$, where $\mathcal{S}(K)$ is given as follows:*

(1) *If $K = F(\sqrt{\varepsilon})$ is unramified, then*

$$\mathcal{S}(K) = \{\sqrt{\varepsilon},\ \varpi\sqrt{\varepsilon},\ 1 + s\sqrt{\varepsilon},\ \varpi + s\sqrt{\varepsilon} \mid s \in F^\times/\{\pm 1\}\}.$$

(2) *If* $K = F(\sqrt{\alpha})$ *is ramified, where* $\alpha \in \{\varpi, \varepsilon\varpi\}$, *then*
(a) *If* $q \equiv 1 \mod 4$ *then*

$$\mathcal{S}(K) = \{\sqrt{\alpha},\ \varepsilon\sqrt{\alpha},\ 1 + s\sqrt{\alpha},\ \varepsilon + s\sqrt{\alpha} \mid s \in F^\times/\{\pm 1\}\}.$$

(b) *If* $q \equiv 3 \mod 4$ *then*

$$\mathcal{S}(K) = \{\sqrt{\alpha},\ \pm 1 + s\sqrt{\alpha} \mid s \in F^\times/\{\pm 1\}\}.$$

Proof. We apply Theorem 4.2. If K/F is unramified, then $\mathcal{C}_K = \{1, \varpi\}$ and $-1 \in N_{K/F}(K^\times)$, yielding the first case. If it is ramified, then $\mathcal{C}_K = \{1, \varepsilon\}$. By the preceding, if $q \equiv 1 \mod 4$ then $-1 \in (F^\times)^2 \subset N_{K/F}(K^\times)$, and this yields the second case. In the last case, we have $-1 \notin (F^\times)^2$, which implies we may without loss of generality choose $\varepsilon = -1$. Thus $\mathcal{C}_K = \{\pm 1\}$, giving the desired result. □

Note that for p-adic fields F, $p \neq 2$, these algebras lie in class one or two, or are new examples for class three or four in [17], since proper nonassociative quaternion algebras are not isotopic to twisted fields.

4.3. Case of 2-adic fields

The classification of nonassociative quaternion algebras given in Theorem 4.2 applies also to the quadratic extensions of 2-adic fields (meaning, finite algebraic extensions of $\mathbb{Q}_2$), since these have characteristic zero. There are two differences.

For one, when F has residual characteristic 2, we have

$$|F^\times/(F^\times)^2| = 2^{e+2}$$

were e is the ramification degree of F over $\mathbb{Q}_2$. That is, the number of distinct quadratic extensions of F increases exponentially with its absolute ramification index. As these give the distinct choices for the left nucleus of a nonassociative quaternion algebra, the number of isomorphism classes of nonassociative quaternion algebras increases exponentially in the ramification index as well. Nonetheless, for any given choice of F, we can generate an explicit list of representatives of $\mathcal{R}^\times/(\mathcal{R}^\times)^2$ using Hensel's Lemma 3.2, and then the distinct quadratic extensions are obtained as $F(\sqrt{c})$ as c varies over the nontrivial elements of the product

$$\{1, \varpi\} \times \mathcal{R}^\times/(\mathcal{R}^\times)^2.$$

For another, while local class field theory implies that $|\mathcal{C}_K| = |F^\times/N_{K/F}(K^\times)| = 2$, it can be nontrivial to generate an explicit representative, such as would be obtained from the Artin reciprocity map. Of course, in degree two this is simply equivalent to identifying an element of $F^\times$ that is not in the image of the norm map.

To give a flavor of the parametrization of isomorphism classes of nonassociative quaternion algebras in this case, we present the example of $F = \mathbb{Q}_2$ in detail.

Theorem 4.5. *Let $F = \mathbb{Q}_2$. Then F has seven distinct quadratic extensions K, enumerated in Table 1. The isomorphism classes of nonassociative quaternion algebras with left nucleus K are represented by $(K/F, \sigma, a)$ where $\sigma \in \mathrm{Gal}(K/F)$ is the nontrivial element and $a \in \mathcal{S}(K)$, where $\mathcal{S}(K)$ is given as follows:*

(a) *If $K = \mathbb{Q}_2(\sqrt{-3})$, then this extension is unramified and*

$$\mathcal{S}(K) = \{\sqrt{-3},\ 2\sqrt{-3},\ 1 + s\sqrt{-3},\ 2 + s\sqrt{-3} \mid s \in \mathbb{Q}_2^\times/\{\pm 1\}\}.$$

(b) *If $K = \mathbb{Q}_2(\sqrt{\alpha})$ with $\alpha \in \{2, -6\}$, then this extension is ramified and $-1 \in N_{K/F}(K^\times)$. We have*

$$\mathcal{S}(K) = \{\sqrt{\alpha},\ 3\sqrt{\alpha},\ 1 + s\sqrt{\alpha},\ 3 + s\sqrt{\alpha} \mid s \in \mathbb{Q}_2^\times/\{\pm 1\}\}.$$

(c) *If $K = \mathbb{Q}_2(\sqrt{\alpha})$ with $\alpha \in \{-1, -2, 3, 6\}$, then this extension is ramified and $-1 \notin N_{K/F}(K^\times)$. We have*

$$\mathcal{S}(K) = \{\sqrt{\alpha},\ \pm 1 + s\sqrt{\alpha} \mid s \in F^\times/\{\pm 1\}\}.$$

Proof. We record in Table 1 several facts about the quadratic extensions of $\mathbb{Q}_2$, as follows. Using Hensel's Lemma, we deduce that there are no solutions to $x^2 = \alpha$ for $\alpha \in \{-1, -3, 3\}$ but that every element of $1 + 4\mathbb{Z}_2$ is a square; moreover, no element of valuation equal to 1 may have a square root in F. We deduce that $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 = \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Thus the first column lists the distinct quadratic extensions of $\mathbb{Q}_2$, with the unramified extension (the one containing the cube roots of unity) being listed first. The second column is taken from [29, p. 34] where the image of the norm map was computed explicitly on a case-by-case basis. In the third column we record a convenient choice of element γ such that $\mathcal{C}_K = F^\times/N_{K/F}(K^\times) = \{1, \gamma\}$.

The theorem is now a direct application of Theorem 4.2. To specify the cases of that theorem that apply, we explicitly record in the fourth column of Table 1 whether or not -1 is in the image of the norm map, and in the final column put a label to the corresponding case of the statement of Theorem 4.5. □

4.4. Case of Laurent series over a finite field of characteristic two

Suppose now that we are in the last remaining case, that of characteristic two.

Note first that extensions of the form $F(\sqrt{c})$ for any $c \notin (F^\times)^2$ are (purely) inseparable. Instead, the distinct Galois quadratic extensions over a field F of characteristic 2 are obtained, by the Artin–Schreier Theorem [15, Ch VI Thm 6.4, 8.3], as

Table 1
The distinct quadratic extensions of $\mathbb{Q}_2$.

$K = F(\sqrt{c})$	$N_{K/F}(K^\times)/(F^\times)^2$	$\mathcal{C}_K$	$-1 \in N_{K/F}(K^\times)$?	Case
$\mathbb{Q}_2(\sqrt{-3})$	$\{\pm 1, \pm 3\}$	$\{1, 2\}$	yes	(a)
$\mathbb{Q}_2(\sqrt{-6})$	$\{\pm 2, \pm 6\}$	$\{1, 3\}$	yes	(b)
$\mathbb{Q}_2(\sqrt{2})$	$\{\pm 1, \pm 2\}$	$\{1, 3\}$	yes	(b)
$\mathbb{Q}_2(\sqrt{-1})$	$\{1, -2, -3, 6\}$	$\{\pm 1\}$	no	(c)
$\mathbb{Q}_2(\sqrt{-2})$	$\{1, 2, 3, 6\}$	$\{\pm 1\}$	no	(c)
$\mathbb{Q}_2(\sqrt{3})$	$\{1, -2-, 3, 6\}$	$\{\pm 1\}$	no	(c)
$\mathbb{Q}_2(\sqrt{6})$	$\{1, -2, 3, -6\}$	$\{\pm 1\}$	no	(c)

$$K = F(x)/(x^2 + x + c)$$

where $c \in F$ ranges over the nontrivial cosets of the additive subgroup $\mathfrak{P}_2 = \{z^2 + z \mid z \in F\}$. Note that if $\alpha \in K$ is a root of $x^2 + x + c$ then so is $\alpha + 1$, so $K = F(\alpha)$.

In this section, we let F be a local nonarchimedean field of characteristic two. Then we have $F = \mathbb{F}_{2^f}(\!(t)\!)$, for some $f \in \mathbb{N}$.

While F admits a unique quadratic unramified Galois extension, it has infinitely many distinct ramified Galois quadratic extensions. For example, since each element of $\mathfrak{P}_2 \smallsetminus \mathcal{R}$ must have *even* valuation, it follows that the elements of $\{t^{-2k-1} : k \in \mathbb{N}\}$, whose distinct differences have odd valuation, represent infinitely many distinct cosets of $\mathfrak{P}_2$.

The classification of the distinct nonassociative quaternion algebras over F correspondingly assumes a different flavor. For one, there will be infinitely many distinct choices for the left nucleus, corresponding to these various distinct quadratic Galois extensions. On the other hand, the parametrization of the isomorphism classes corresponding to a fixed quadratic extension admits a simpler description, as follows.

Theorem 4.6. *Suppose $K = F(\alpha)$ is a separable quadratic extension of a local field F of characteristic 2. Let γ be a nontrivial element of $F^\times/N_{K/F}(K^\times)$ and σ the element of $\mathrm{Gal}(K/F)$ such that $\sigma(\alpha) = \alpha + 1$. The distinct isomorphism classes of nonassociative quaternion algebras with left nucleus K are represented by $(K/F, \sigma, a)$ where a is chosen from the set $\mathcal{S}(K)$ given by*

$$\mathcal{S}(K) = \{s + \alpha, \gamma(s + \alpha) \mid s \in F/\{0, 1\}\}$$

where $F/\{0, 1\}$ denotes the quotient of the additive group of F by the two-element prime field $\mathbb{F}_2$.

Proof. Let $m(x) = x^2 + x + c$ be the minimal polynomial of α. Its other root is $\alpha + 1$, and these are linearly independent over F. Thus

$$\{\alpha, \alpha + 1\}$$

forms a basis for K/F. Let us evaluate the equivalence relation $\sim$ arising from Theorem 2.6 on $K \smallsetminus F$. Write $a = a_0 + a_1\alpha$; then $a_1 \neq 0$ since $a \notin F$. Thus there exists a

unique $r \in \{1, \gamma\}$ and $n \in N_{K/F}(K^\times)$ such that $a_1 = rn$. Setting $s = a_0 n^{-1}$, it follows that $a \in (s + r\alpha)N_{K/F}(K^\times)$.

Since $\sigma(s+\alpha) = (s+1)+\alpha$ and $\sigma(s+\gamma\alpha) = (s+\gamma)+\gamma\alpha$, and since the characteristic of F is 2, it follows that the distinct isomorphism classes are parametrized by the set

$$\{s_1 + \alpha, s_\gamma + \gamma\alpha \mid s_1 \in F/\{0,1\}, s_\gamma \in F/\{0,\gamma\}\}.$$

As the map sending $a \in F$ to $a\gamma \in F$ is an additive group automorphism sending $\{0,1\}$ to $\{0,\gamma\}$, we deduce the final form of the parameter set $\mathcal{S}(K)$. □

5. Nonassociative cyclic algebras of degree $m > 2$

In this section, we begin with some results for nonassociative cyclic algebras of degree $m > 2$, before specializing to the case that m is prime (and F contains a primitive mth root of unity), concluding with an application to the case of local nonarchimedean fields.

5.1. *Different generators of* $\mathrm{Gal}(K/F)$ *give nonisomorphic algebras*

Let F be an arbitrary field such that F admits a cyclic Galois extension K of degree $m > 2$. By Lemma 2.5, the choice of field K is an invariant of the isomorphism class.

In the case of *associative* cyclic algebras, that is, when $a \in F^\times$, one has $(K/F, \sigma, a) \cong (K/F, \sigma^k, a^k)$ [21, 15.1 Corollary a], that is, different choices of generator of the Galois group yield isomorphic algebras.

We show that, in stark contrast, nonassociative cyclic algebras corresponding to distinct choices of generator $\sigma \in \mathrm{Gal}(K/F)$ are *never* isomorphic.

Theorem 5.1. *Let F be an arbitrary field and let $m \geq 3$ be the degree of a cyclic Galois extension K/F. For any two distinct generators $\sigma_1 \neq \sigma_2$ of the Galois group $\mathrm{Gal}(K/F)$, and for any $a_1, a_2 \in K \setminus F$, we have*

$$(K/F, \sigma_1, a_1) \ncong (K/F, \sigma_2, a_2).$$

Proof. Suppose to the contrary that there exists an isomorphism $\varphi\colon (K/F, \sigma_1, a_1) \to (K/F, \sigma_2, a_2)$; this is an isomorphism of F-vector spaces satisfying $\varphi(uv) = \varphi(u)\varphi(v)$ for all $u, v \in (K/F, \sigma_1, a_1)$. In particular, φ restricts to a field automorphism of K; since the Galois group is cyclic, and thus abelian, this implies φ commutes with σ_i on K, for $i \in \{1, 2\}$.

By Definition 2.1, $(K/F, \sigma_i, a_i) = \bigoplus_{s=0}^{m-1} K t_i^s$ with an F-bilinear multiplication defined for $0 \leq s, s' < m$ and $k, k' \in K$ by

$$(kt_i^s)(k't_i^{s'}) = \begin{cases} k\sigma_i^s(k')t_i^{s+s'} & \text{if } s + s' < m; \\ k\sigma_i^s(k')a_i t_i^{s+s'-m} & \text{if } s + s' \geq m. \end{cases}$$

In particular, we infer that the left K-submodule Kt_i^s can be characterized as

$$Kt_i^s = \{u \in (K/F, \sigma_i, a_i) \mid \forall k \in K, uk = \sigma_i^s(k)u\}.$$

Since σ_1, σ_2 both generate $\mathrm{Gal}(K/F)$, there is some $1 < j < m$, with $(j, m) = 1$, such that $\sigma_1 = \sigma_2^j$. It follows that $\varphi(t_1) = kt_2^j$ for some $k \in K$.

Let ℓ be the least positive integer such that $\ell j > m$; since $\sigma_1 \neq \sigma_2$, we have $\ell < m$. For any index $s \geq 1$, set $\gamma_s(k) = k\sigma_2^j(k)\sigma_2^{2j}(k)\cdots\sigma_2^{(s-1)j}(k)$. Then one can show by induction that

$$\varphi(t_1^s) = \begin{cases} \gamma_s(k)t_2^{sj} & \text{if } 1 \leq s < \ell; \\ \gamma_\ell(k)a_2t_2^{\ell j - m} & \text{if } s = \ell. \end{cases}$$

Since $1 \leq \ell < m$, we have

$$t_1 \cdot t_1^\ell = t_1^\ell \cdot t_1 = \begin{cases} t_1^{\ell+1} & \text{if } \ell + 1 < m; \\ a_1 & \text{if } \ell + 1 = m. \end{cases}$$

However, we have

$$\varphi(t_1^\ell)\varphi(t_1) = \gamma_\ell(k)a_2t_2^{\ell j - m} \cdot kt_2^j = \begin{cases} \gamma_{\ell+1}(k)a_2t_2^{\ell j + j - m} & \text{if } (\ell+1)j < 2m; \\ \gamma_{\ell+1}(k)a_2^2t_2^{\ell j + j - 2m} & \text{if } 2m \leq (\ell+1)j \end{cases}$$

whereas

$$\varphi(t_1)\varphi(t_1^\ell) = kt_2^j \cdot \gamma_\ell(k)a_2t_2^{\ell j - m} = \begin{cases} \gamma_{\ell+1}(k)\sigma_2^j(a_2)t_2^{\ell j + j - m} & \text{if } (\ell+1)j < 2m; \\ \gamma_{\ell+1}(k)\sigma_2^j(a_2)a_2t_2^{\ell j + j - 2m} & \text{if } 2m \leq (\ell+1)j. \end{cases}$$

It follows that φ is well-defined only if $\sigma_1(a_2) = \sigma_2^j(a_2) = a_2$, meaning that a_2 lies in the fixed field of σ_1. But this is impossible: σ_1 generates the cyclic Galois group, and $a_2 \notin F$, by construction. □

5.2. An explicit parametrization of isomorphism classes

Now suppose that m is an odd prime and that F contains a primitive mth root of unity. If F has prime characteristic p then this condition implies that $gcd(m, p) = 1$. Kummer theory [15, Ch VI Thm 6.2, 8.2] ensures that the Galois extensions of F of degree m are in bijection with the subgroups of $F^\times/(F^\times)^m$ of order m.

By Theorem 5.1, we may fix a choice of cyclic field extension K/F of degree m and a choice of generator σ of $\mathrm{Gal}(K/F)$. We wish to classify the algebras $(K/F, \sigma, a)$, as a runs over $K \setminus F$, up to isomorphism.

Let $\zeta \in F$ be a primitive mth root of unity. By Kummer theory, K is the splitting field of some polynomial $x^m - b$, with $b \notin (F^\times)^m$. Thus we may choose $\beta \in K$ to be a root of $x^m - b$ for which $\sigma(\beta) = \zeta\beta$. Then

$$\{1, \beta, \beta^2, \dots, \beta^{m-1}\}$$

is an F-basis for K with the property that $\sigma(\beta^k) = \zeta^k\beta^k$ for all $0 \leq k < m$.

We first prove that the isomorphism classes of cyclic algebras $(K/F, \sigma, a)$ admit a coarse partition into 2^{m-1} subsets with respect to this choice of basis, inspired by the classification of quaternion algebras in Theorem 4.2.

Definition 5.2. Let $\mathcal{I} = \mathcal{P}(\{0, 1, \dots, m-1\}) \setminus \{\{0\}, \emptyset\}$ be the set of nonempty subsets of $\{0, 1, \dots, m-1\}$, excluding the set $\{0\}$. For each $I \in \mathcal{I}$, define

$$K(I) = \{\sum_{i=0}^{m-1} a_i\beta^i \mid \forall i \in I, a_i \in F^\times, \forall i \notin I, a_i = 0\} \subset K \setminus F.$$

Thus for example if $m = 3$, $K(\{1, 2\}) = \{a_1\beta + a_2\beta^2 \mid a_1, a_2 \in F^\times\}$. It follows directly that

$$K \setminus F = \bigcup_{I \in \mathcal{I}} K(I),$$

and that these sets $K(I)$ are invariant both under the action of σ, and under multiplication by elements of $F^\times$. Applying Theorem 2.6 gives the following lemma.

Lemma 5.3. *Suppose $I, J \in \mathcal{I}$ are distinct. Then for any $a \in K(I)$, $b \in K(J)$, we have*

$$(K/F, \sigma, a) \ncong (K/F, \sigma, b).$$

To further refine these partitions, we require the following definition.

Definition 5.4. Let $I \in \mathcal{I}$ be such that $|I| = k + 1 \geq 2$. Write $F^{[\times k]}$ for the k-fold direct product $F^\times \times F^\times \times \cdots \times F^\times$. If the elements of I are $i_0 < i_1 < \cdots < i_k$ then let

$$\Delta_I = \{(\zeta^{s(i_1 - i_0)}, \zeta^{s(i_2 - i_0)}, \dots, \zeta^{s(i_k - i_0)}) \in F^{[\times k]} \mid 1 \leq s \leq m\}$$

where ζ is any primitive mth root of unity. Write $F^{[\times k]}/\Delta_I$ for any fixed choice of representatives for these cosets. For any fixed choice of $a_{i_0} \in F^\times$, define

$$K(I; a_{i_0}) = \{a_{i_0}\beta^{i_0} + \sum_{j=1}^{k} a_{i_j}\beta^{i_j} \mid (a_{i_1}, a_{i_2}, \dots, a_{i_k}) \in F^{[\times k]}/\Delta_I\}.$$

Finally, set $K(I; a_{i_0}) = \{a_{i_0}\beta^{i_0}\}$ when $I = \{i_0\} \in \mathcal{I}$.

We may now state our main classification theorem for cyclic extensions of odd prime degree.

Theorem 5.5. *Suppose m is an odd prime and F contains a primitive mth root of unity ζ. Then the distinct isomorphism classes of nonassociative cyclic algebras of degree m over F are represented by*

$$(K/F, \sigma, a)$$

where:

- *K is one of the distinct cyclic Galois field extensions of F of degree m, and $\mathcal{C}_K$ denotes a set of representatives of $F^\times/N_{K/F}(K^\times)$;*
- *σ is a generator of $\mathrm{Gal}(K/F)$; and*
- *$a \in \mathcal{S}(K) \subset K \setminus F$*

where $\mathcal{S}(K)$ is defined as follows.

If $\zeta \in N_{K/F}(K^\times)$, then we take

$$\mathcal{S}(K) = \bigcup_{I\in\mathcal{I}, a_{i_0}\in\mathcal{C}_K} K(I; a_{i_0}),$$

whereas otherwise, we may take $\mathcal{C}_K = \mu_m$ and then

$$\mathcal{S}(K) = \bigcup_{I\in\mathcal{I}: i_0=0, a_0\in\mu_m} K(I; a_0) \cup \bigcup_{I\in\mathcal{I}: i_0>0} \{1 + \sum_{j=1}^{|I|-1} a_{i_j}\beta^{i_j} \mid \forall j, a_{i_j} \in F^\times\}.$$

Proof. By Theorem 5.1 and Lemma 5.3, it suffices to partition $K(I)$ into equivalence classes under $\sim$ for each fixed K/F, σ and $I \subset \mathcal{I}$.

Let $\mathcal{C}_K$ be a fixed set of representatives for $F^\times/N_{K/F}(K^\times)$. When $\zeta \notin N_{K/F}(K^\times)$, it follows that $\mu_m \cap N_{K/F}(K^\times) = \{1\}$ and thus this m-element group must represent the quotient, allowing us to set $\mathcal{C}_K = \mu_m$.

Let $a \in K(I)$ and let $i_0 < i_1 < \cdots < i_k$ be the distinct elements of I. Then $a_{i_0} = cn$ for some unique $c \in \mathcal{C}_K$ and some $n \in N_{K/F}(K^\times)$. Consequently, scaling a by n^{-1} gives

$$a \sim c\beta^{i_0} + \sum_{j=1}^{k} a_{i_j}\beta^{i_j}$$

for some $a_{i_j} \in F^\times$ and $c \in \mathcal{C}_K$. Furthermore, for any $s \in \mathbb{Z}$, we have

$$\sigma^s\left(c\beta^{i_0} + \sum_{j=1}^{k} a_{i_j}\beta^{i_j}\right) = c\zeta^{si_0}\beta^{i_0} + \sum_{j=1}^{k} a_{i_j}\zeta^{si_j}\beta^{i_j}. \tag{5.1}$$

If $\zeta \in N_{K/F}(K^\times)$, then we may scale this expression by $\zeta^{-si_0} \in N_{K/F}(K^\times)$ to produce an equivalent element of $K(I)$. It follows that the equivalence classes are parametrized by

$$\{c\beta^{i_0} + \sum_{j=1}^{k} a_{i_j}\beta^{i_j} \mid (a_{i_1}, \dots, a_{i_k}) \in F^{[\times k]}/\Delta_I\} = K(I; c),$$

as c varies over $\mathcal{C}_K$, as required.

If instead we have $\mathcal{C}_K = \mu_m$, then there are two cases. If $i_0 = 0$, then the relations induced by (5.1) imply directly, as above, that every element $a \in K(I)$ is equivalent to a unique element of the set $K(I; c)$. However, if $i_0 > 0$, then as s varies over $\{1, 2, \cdots, m\}$, the coefficient of β^{i_0} in (5.1) varies over $\mathcal{C}_K$. Consequently, every $a \in K(I)$ is equivalent to one for which the first nonzero coefficient c is equal to 1, and no two distinct elements of this form will be equivalent. Taken together, this gives the set $\mathcal{S}(K)$ in this second case. □

5.3. Application to local nonarchimedean fields

From now on, let F be again a local nonarchimedean field of residual characteristic p and residue field of order q. Let m be an odd prime distinct from p; then all extensions of degree m of F are tamely ramified. Let us furthermore assume that F contains a primitive mth root of unity, or equivalently, that $m|(q-1)$, where $q = |\kappa|$ is the order of the residue field of F.

Since $F^\times/(F^\times)^m \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, Kummer theory implies that we have precisely $m+1$ distinct Galois extensions of degree m, corresponding to all order-m subgroups, and consequently $m+1$ collections of isomorphism classes, one for each such extension.

We now make the parametrization given in Theorem 5.5 wholly explicit in this setting, by defining a set $\mathcal{C}_K$ of representatives of $F^\times/N_{K/F}(K^\times)$ for each degree m extension of F, and determining the conditions under which $\mu_m \subset N_{K/F}(K^\times)$.

Proposition 5.6. *Let K be a cyclic Galois field extension of degree m of a local nonarchimedean field F, such that $\mu_m \subset F$ and $m \neq p$. Let q denote the order of the residue field κ of F. Then $F^\times/N_{K/F}(K^\times)$ is represented by*

$$\mathcal{C}_K = \begin{cases} \{1, \varpi, \varpi^2, \cdots, \varpi^{m-1}\} & \text{if } K/F \text{ is unramified;} \\ \mu_m(F) & \text{if } K/F \text{ is ramified and } m^2 \nmid (q-1); \\ \{1, \xi, \xi^2, \cdots, \xi^{m-1}\} & \text{if } K/F \text{ is ramified and } m^2|(q-1), \end{cases}$$

where $\xi \in \mu_{q-1}(F)$ is any choice of primitive $(q-1)$th root of unity in F.

Proof. Since $m \neq p$, Hensel's Lemma implies that the map $x \mapsto x^m$ is a bijection on $1 + \mathcal{P}$, and that $\mu_{q-1}(F) \cong \kappa^\times$ as in Example 3.3.

Thus via the map sending a pair $(\overline{a}, \ell) \in \kappa^\times \times \mathbb{Z}$ to $a\varpi^\ell$, we have $\kappa^\times/(\kappa^\times)^m \times \mathbb{Z}/m\mathbb{Z} \cong F^\times/(F^\times)^m$. Now $(F^\times)^m \subset N_{K/F}(K^\times) \subset F^\times$ and $|F^\times/N_{K/F}(K^\times)| = m$ by local class field theory. When K/F is unramified, the norm map surjects onto $\mathcal{R}^\times$, so we may take our representatives $\mathcal{C}_K$ from powers of ϖ. When K/F is (totally) ramified, we instead have $N_{K/F}(K^\times) \cap \mathcal{R}^\times = (\mathcal{R}^\times)^m$ so it suffices to identify a set of representatives from among the Teichmüller lifts of elements of $\kappa^\times/(\kappa^\times)^m$.

If $m^2 \nmid (q-1)$, then no primitive mth root of unity can be an mth power, and thus we may take $\mathcal{C}_K = \mu_m$ as a preferred set of representatives. Otherwise, one may take the first m powers of any primitive element of $\mu_{q-1}(F) \cong \kappa^\times$ (or indeed, of any element whose order k satisfies $mk \nmid (q-1)$). □

5.4. An explicit example: nonassociative cyclic algebras of degree 3

In this section, we specialize the results of the preceding section to degree 3, to better illustrate the combinatorial and explicit nature of the parametrization.

Theorem 5.7. *Let F be a local nonarchimedean field of residual characteristic different from* 3 *such that F contains a primitive cube root of unity ζ. Write $\mu_3 = \langle\zeta\rangle$ and set $\Delta_3 = \{(a, a^{-1}) \in F^\times \times F^\times | a \in \mu_3\}$. Then the distinct isomorphism classes of nonassociative cyclic algebras of degree* 3 *over F are represented by $(K/F, \sigma, a)$ where σ is a nontrivial element of* $\mathrm{Gal}(K/F)$ *and K and $a \in \mathcal{S}(K)$ are determined as follows:*

(a) *$K = L_3$ is the unique unramified extension of F and*

$$\mathcal{S}(K) = \{r\beta, r\beta^2, r\beta + s\beta^2, r + s\beta, r + s\beta^2, r + s_1\beta + s_2\beta^2 \mid r \in \{1, \varpi, \varpi^2\}, s \in F^\times/\mu_3, (s_1, s_2) \in (F^\times \times F^\times)/\Delta_3\}.$$

(b) *$K = F(\beta)$ is one of the three ramified extensions, where $\beta^3 = u\varpi$ for some $u \in \mathcal{R}^\times/(\mathcal{R}^\times)^3$, and*
   (a) *if $q \not\equiv 1 \mod 9$, then*

$$\mathcal{S}(K) = \{r + s_1\beta + s_2\beta^2, \beta + s\beta^2, \beta^2 | r \in \mu_3, s \in F, (s_1, s_2) \in (F^\times \times F^\times)/\Delta_3\};$$

   (b) *if $q \equiv 1 \mod 9$, then let $F^\times/N_{K/F}(K^\times) = \mathcal{R}^\times/(\mathcal{R}^\times)^3 = \{1, \gamma, \gamma^2\}$ and set*

$$\mathcal{S}(K) = \{r\beta, r\beta^2, r\beta + s\beta^2, r + s\beta, r + s\beta^2, r + s_1\beta + s_2\beta^2 \mid r \in \{1, \gamma, \gamma^2\}, s \in F^\times/\mu_3, (s_1, s_2) \in (F^\times \times F^\times)/\Delta_3\}.$$

Proof. Note that $\mu_3 \subset \mathcal{R}^\times$ implies that 3 divides $q-1$ or $q \equiv 1 \mod 3$, where q is the order of the residue field of F. Similarly, ζ is itself a cube if and only if $F^\times$ contains a primitive 9th root of unity, which is the condition that $9|(q-1)$. Here, $\mathcal{I} = \{\{1\}, \{2\}, \{0,1\}, \{1,2\}, \{0,2\}, \{0,1,2\}\}$. When $I = \{i\} \in \mathcal{I}$, we have $K(I, r) = \{r\beta^i\}$;

when $I = \{i_0 < i_1\} \in \mathfrak{I}$, we have $K(I,r) = \{r\beta^{i_0} + s\beta^{i_1} : s \in F^\times/\mu_3\}$; and when $I = \{0,1,2\}$, we have $K(I,r) = \{r + s_1\beta + s_2\beta^2 : (s_1,s_2) \in \Delta_{\{0,1,2\}} = \Delta_3\}$. The statement now from Theorem 5.5. □

6. Nonassociative cyclic algebras of degree four

When the degree of the nonassociative cyclic algebra is not prime, its structure becomes more interesting. Let K/F be a cyclic Galois field extension of degree m with Galois group $G = \mathrm{Gal}(K/F) = \langle\sigma\rangle$ and $a \in K \setminus F$.

When m is not prime, then there is a nonassociative subalgebra of $(K/F,\sigma,a)$ associated to each $1 < s < m$ such that $(s,m) \neq 1$. Namely, set $E = \mathrm{Fix}(\sigma^s)$ to be the subfield of K fixed by σ^s; then $(K/E,\sigma^s,a)$ is a cyclic algebra over E, that is nonassociative if $a \notin E$, and that is an F-subalgebra of $(K/F,\sigma,a)$.

In particular, if we let $H = \{\tau \in G \,|\, \tau(a) = a\}$ be the subgroup of the (cyclic) Galois group fixing a, and let $E = \mathrm{Fix}(H)$, then $H = \sigma^s$ for some divisor s of m and by [23, Theorem 1] we have

$$\mathrm{Nuc}_r((K/F,\sigma,a)) = (K/E,\sigma^s,a),$$

where this latter is now an associative cyclic algebra of degree r over $E = \mathrm{Fix}(\sigma^s)$ (and hence independent of the choice of generator σ^s).

We briefly discuss the degree four case.

We first consider F an arbitrary field of characteristic different from 2. Let K/F be a cyclic Galois field extension of degree four with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Then K has exactly one quadratic subfield $E = \mathrm{Fix}(\sigma^2)$.

Let $a \in K \setminus F$ and consider $(K/F,\sigma,a)$. This is a 16-dimensional algebra over F. We know by Theorem 2.4 that if $a \notin E$ then $(K/F,\sigma,a)$ is a division algebra.

Using Definition 2.1 or the general results mentioned above, the nonassociative cyclic E-algebra $B = (K/E,\sigma^2,a)$ can be embedded as the F-subalgebra generated by 1 and t^2 in $(K/F,\sigma,a)$; it is 8-dimensional over F.

Lemma 6.1.

(a) *If $a \notin E$, then B is a proper nonassociative quaternion division algebra over E, hence also a nonassociative division algebra over F.*

(b) *If $a \in E$, then B is the right nucleus of A. In this case, it is an associative quaternion algebra over E, which is a division algebra if and only if $a \notin N_{K/F}(K^\times)$. Furthermore, then B is a division algebra if and only if $(K/F,\sigma,a)$ is a division algebra.*

We give an explicit, but coarse, classification of these algebras in the case of local nonarchimedean fields as follows (note that these may not all be division algebras).

Proposition 6.2. *Let F be a local nonarchimedean field of residual characteristic different from 2. Then every nonassociative cyclic algebra of degree four over F is of one of the following types, and moreover, algebras corresponding to distinct field extensions and distinct generators of the Galois group are nonisomorphic:*

(1) $(L_4/F, \sigma, a)$, *corresponding to the unique unramified extension of degree 4. Here* $B = (L_4/F(\sqrt{\varepsilon}), \sigma^2, a)$.
(2) $(K_0/F, \sigma, a)$, *corresponding to the extension* $K_0 = E(\sqrt{\varepsilon_E \varpi})$ *where* $E = F(\sqrt{\varepsilon})$ *and* ε_E *is a nonsquare of* $\mathcal{R}_E^\times \setminus \mathcal{R}^\times$. *Here* $B = (K_0/E, \sigma^2, a)$.
(3) *If* $-1 \in (F^\times)^2$*: for* $i \in \{1, 2, 3, 4\}$, $(K_i/F, \sigma, a)$, *corresponding to the extension* $K_i = F(\sqrt[4]{\varepsilon^i \varpi})$. *The intermediate subfield is* $E = F(\sqrt{\varpi})$ *if* i *is even and* $E = F(\sqrt{\varepsilon\varpi})$ *if* i *is odd. Here* $B = (K_i/E, \sigma^2, a)$.

Proof. Let A be a nonassociative cyclic algebra of degree four over F. Since the left nucleus of A is invariant under isomorphism, it suffices to generate a list of distinct cyclic Galois extensions K of F of degree 4. Moreover, by Theorem 5.1, we know that for the two distinct choices of generator σ of $\mathrm{Gal}(K/F)$ the resulting algebras will be nonisomorphic.

It can be shown that F admits 6 cyclic Galois extensions of degree four if $-1 \in (F^\times)^2$ and only two otherwise. The first of these is the unique unramified extension L_4, with intermediate subfield $E = L_2$. The second is a partially ramified extension K_0, obtained as the quadratic extension of $E = L_2$ by an element of the form $u\varpi$, where u is chosen as a nonsquare of $\mathcal{R}_{L_2}^\times$ that does not lie in $\mathcal{R}^\times$.

When $-1 \in (F^\times)^2$, then F contains a primitive 4th root of unity, and there are correspondingly four additional Galois totally ramified extensions, given as $K_i = F(\sqrt[4]{\varepsilon^i \varpi})$. Their unique intermediate subfield is $E = F(\sqrt{\varpi})$ if i is even and $E = F(\sqrt{\varepsilon\varpi})$ if i is odd. □

Thus we count four different types for each such field F if $-1 \notin (F^\times)^2$ and twelve if $-1 \in (F^\times)^2$.

While in the associative case, all cyclic algebras of degree m over F are isomorphic to an algebra of the type $(L_m/F, \sigma, a)$ for some $a \in F^\times$, this proposition shows once again that the situation in the nonassociative setting is more varied.

Acknowledgment

This paper was written while the second author was a visitor at the University of Ottawa in the spring of 2024. She would like to thank the Department of Mathematics and Statistics for its hospitality and congenial atmosphere.

Data availability

No data was used for the research described in the article.

References

[1] A.A. Albert, Non-associative algebras: I. Fundamental concepts and isotopy, Ann. Math. 43 (4) (1942) 685–707.
[2] A.A. Albert, Non-associative algebras: II. New simple algebras, Ann. Math. 43 (4) (1942) 708–723.
[3] V. Astier, S. Pumplün, Nonassociative quaternion algebras over rings, Isr. J. Math. 155 (2006) 125–147.
[4] G. Blachar, D. Haile, E. Matzri, E. Rein, U. Vishne, Semiassociative algebras over a field, J. Algebra 649 (1) (July 2024) 35–84, https://doi.org/10.1016/j.jalgebra.2024.03.006.
[5] C. Brown, S. Pumplün, The automorphisms of Petit's algebras, Commun. Algebra 46 (2) (2018) 834–849.
[6] A. Deajim, D. Grant, On the classification of 3-dimensional non-associative division algebras over p-adic fields, J. Théor. Nr. Bordx. 2 (2011) 329–346.
[7] L.E. Dickson, Linear algebras with associativity not assumed, Duke Math. J. 1 (1935) 113–125.
[8] D. Eisenbud, Commutative Algebra, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry.
[9] J. Gòmez-Torrecillas, Basic module theory over non-commutative rings with computational aspects of operator algebras, With an appendix by V. Levandovskyy, in: Algebraic and Algorithmic Aspects of Differential and Integral Operators, in: Lecture Notes in Comput. Sci., vol. 8372, Springer, Heidelberg, 2014, pp. 23–82.
[10] N. Jacobson, Finite-Dimensional Division Algebras over Fields, Springer Verlag, Berlin-Heidelberg-New York, 1996.
[11] V. Jha, N.L. Johnson, An analog of the Albert-Knuth theorem on the orders of finite semifields, and a complete solution to Cofman's subplane problem, Algebras Groups Geom. 6 (1) (1989) 1–35.
[12] P. Jordan, Über Verallgemeinerungsmöglichkeiten des Formalismus der Quantenmechanik, Nachr. Akad. Wiss. Gött. Math.-Phys. Kl., I 41 (1933) 209–217.
[13] I. Kaygorodov, Non-associative algebraic structures: classification and structure, Commun. Math. 32 (3) (2024) 1–62.
[14] S. Lang, Algebraic Number Theory, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994.
[15] S. Lang, Algebra, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.
[16] M. Lavrauw, J. Sheekey, Semifields from skew-polynomial rings, Adv. Geom. 13 (4) (2013) 583–604.
[17] S. Limburg, Space-time codes, nonassociative division algebras and elliptic curves, PhD thesis, Oregon State University, 2006.
[18] The LMFDB Collaboration, The L-functions and modular forms database, https://www.lmfdb.org, 2024. (Accessed 5 June 2024), Online.
[19] J.-C. Petit, Sur certains quasi-corps généralisant un type d'anneau-quotient, in: Séminaire Dubriel, in: Algèbre et Théorie des Nombres, vol. 20–1966–1967, pp. 1–18.
[20] J.-C. Petit, Sur les quasi-corps distributifs à base monogène, C. R. Acad. Sci. Paris, Sér. A 266 (1968) 402–404.
[21] R.S. Pierce, Associative Algebras, Studies in the History of Modern Science, vol. 9, Springer-Verlag, New York-Berlin, 1982. Graduate Texts in Mathematics, 88.
[22] S. Pumplün, Tensor products of nonassociative cyclic algebras, J. Algebra 451 (2016) 145–165.
[23] S. Pumplün, Nonassociative cyclic algebras and the semiassociative Brauer monoid, Rend. Circ. Mat. Palermo 2 (2024), https://link.springer.com/article/10.1007/s12215-024-01105-4.
[24] S. Pumplün, A. Steele, Fast-decodable MIDO codes from nonassociative algebras, Int. J. Inf. Coding Theory 3 (1) (2015) 15–38.
[25] S. Pumplün, A. Steele, The nonassociative algebras used to build fast-decodable space-time block codes, Adv. Math. Commun. 9 (4) (2015) 449–469.
[26] L.H. Rowen, Residue structures, Preprint, online at https://arxiv.org/pdf/2403.09467.pdf, 2024.
[27] R. Sandler, Autotopism groups of some finite non-associative algebras, Am. J. Math. 84 (1962) 239–264.

[28] R.D. Schafer, An Introduction to Nonassociative Algebras, Dover Publ., Inc., New York, 1995.
[29] G. Shimura, Arithmetic of Quadratic Forms, Springer Monographs in Mathematics, Springer, New York, 2010.
[30] A. Steele, Nonassociative cyclic algebras, Isr. J. Math. 200 (1) (2014) 361–387.
[31] W.C. Waterhouse, Nonassociative quaternion algebras, Algebras Groups Geom. 4 (1987) 365–378.