NONASSOCIATIVE DIFFERENTIAL EXTENSIONS OF CHARACTERISTIC p

S. PUMPLÜN

Abstract. Let F be a field of characteristic p. We define and investigate nonassociative differential extensions of F and of a central simple division algebra over F and give a criterium for these algebras to be division. As special cases, we obtain classical results for associative algebras by Amitsur and Jacobson. We construct families of nonassociative division algebras which can be viewed as generalizations of associative cyclic extensions of a purely inseparable field extension of exponent one or a central division algebra. Division algebras which are nonassociative cyclic extensions of a purely inseparable field extension of exponent one are particularly easy to obtain.

Introduction

Differential polynomial rings $D[t;\delta]$, where D is a division algebra over a field F and δ a derivation on D, have been used successfully to construct associative central simple algebras. These appear either as a quotient algebra $D[t;\delta]/(f)$ when factoring out a two-sided ideal generated by a differential polynomial $f \in D[t;\delta]$, cf. [2], [4], [5, Sections 1.5, 1.8, 1.9], or as the eigenring of a differential polynomial f, e.g. see [1], [9]. We can put these constructions into a nonassociative context as follows:

Given $f \in D[t;\delta]$ of degree m, the set of all differential polynomials of degree less than m can be canonically equipped with a nonassociative ring structure, using right division by f to define the multiplication $g \circ h = gh \bmod_r f$. The resulting nonassociative unital ring S_f is an algebra over the field $F_0 = C(D) \cap \mathrm{Const}(\delta)$ (Petit [10]). If f is not two-sided (i.e., does not generate a two-sided ideal in $D[t;\delta]$) and δ not trivial, then the S_f are algebras whose nuclei are larger than their center F_0. In particular, their right nucleus is the eigenring of f employed in [1] and [9], whereas if f generates a two-sided ideal, then S_f is the (associative) quotient algebra employed in [2] and [5], each time for well considered choices of f and $D[t;\delta]$.

Let F be a field of characteristic $p > 0$. We study the algebras S_f containing a purely inseparable field extension K/F of exponent one or a central division algebra D over F as left nucleus. As a special case we reprove the classical results on differential extensions by Jacobson [5] and Amitsur's results on noncommutative cyclic extensions of degree p [2].

The paper is organized as follows: we introduce the basic terminology in Section 1. In Section 2 we focus on the case that δ is a quasi-algebraic derivation with minimal polynomial

Date: 20.6.2016.

1991 *Mathematics Subject Classification.* Primary: 17A35; Secondary: 17A60, 17A36.

Key words and phrases. Differential polynomial ring, skew polynomial, differential polynomial, differential operator, differential algebra, nonassociative division algebra.

g and therefore S_f an algebra of finite dimension over $F = \mathrm{Const}(\delta)$. In particular, for $f(t) = g(t) - d \in D[t;\delta]$ where g is the minimum polynomial of $\delta|_{C(D)}$, the set of all logarithmic derivatives $\{\delta(c)/c \,|\, c \in C(D)\}$ turns out to be a subgroup of the automorphism group of S_f. We follow up on this observation and define nonassociative differential extensions of a field in Section 3 and nonassociative differential extensions of a central simple division algebra in Section 4, generalizing classical constructions by Amitsur and Jacobson, by choosing $f(t) = g(t) - d \in D[t;\delta]$ to be a p-polynomial of a certain type.

In particular, when K is a purely inseparable extension of F of exponent one with derivation δ such that δ has minimum polynomial $g(t) = t^p - t \in F[t]$ and $f(t) = t^p - t - d \in K[t;\delta]$, $S_f = (K, \delta, d)$ is a unital nonassociative division algebra over $F = \mathrm{Const}(\delta)$ of dimension p^2 for all $d \in K \setminus F$. Its automorphism group contains a cyclic subgroup of order p which leaves K invariant (Theorem 14). This canonically generalizes Amitsur's associative cyclic extensions of degree p. Thus $(K(x), \delta, h(x))$ is a division algebra over $F(x)$ of dimension p^2 for all $h(x) \in K(x) \setminus F(x)$, and so a nonassociative cyclic extension of $K(x)$ (Example 15). This generalizes [5, Proposition 1.9.10]. Analogously, Theorem 20 in Section 4 generalizes the result on associative cyclic extensions of D, cf. [5, Theorem 1.3.27].

In Section 5 we construct tensor products of a central simple division algebra and a nonassociative cyclic extension, generalizing another classical result by Jacobson [5, Theorem 1.9.13] in Theorem 25. As an application, we show that $(K(x), \delta, h(x)) \otimes_{F(x)} D_{F(x)}$ with $h(x) \in K(x) \setminus F(x)$ is a division algebra if and only if $h(x) \neq (t-z)^p - t^p - z$ for all $z \in D_{K(x)}$ in Example 26, provided that δ has minimum polynomial $g(t) = t^p - t$ and that $D \otimes_F K$ is a division algebra. This algebra is a nonassociative cyclic extension of $D_{K(x)}$ if it is division. This generalizes [5, Theorem 1.9.11], where $h(x) = x$ in which case the algebra is division.

The theory presented in this paper can be extended to nonassociative cyclic extensions of degree any prime power if desired, along the lines presented here. It complements the theory of nonassociative cyclic algebras $(K/F, \sigma, d)$ which are constructed out of twisted polynomial rings $K[t;\sigma]$ and $f(t) = t^m - d \in K[t;\sigma]$, where K/F is a cyclic Galois extension of degree m, $\mathrm{Gal}(K/F) = <\sigma>$ and F has characteristic zero or p, but now with p coprime to m, cf. [17], and the theory of nonassociative generalized cyclic algebras (D, σ, d) which are constructed out of twisted polynomial rings $D[t;\sigma]$ and $f(t) = t^m - d \in D[t;\sigma]$, where D is a cyclic division algebra of degree m, $f(t) = t^m - d \in D[t;\sigma]$, and σ chosen suitably, cf. [12], [15].

1. Preliminaries

1.1. **Nonassociative algebras.** Let F be a field and let A be an F-vector space. A is an *algebra* over F if there exists an F-bilinear map $A \times A \to A$, $(x, y) \mapsto x \cdot y$, denoted simply by juxtaposition xy, the *multiplication* of A. 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 algebras from now on without explicitly saying so.

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 [16, pp. 15, 16].

Associativity in A is measured by the *associator* $[x, y, z] = (xy)z - x(yz)$. The *left nucleus* of A is defined as $\mathrm{Nuc}_l(A) = \{x \in A \,|\, [x, A, A] = 0\}$, the *middle nucleus* of A is $\mathrm{Nuc}_m(A) = \{x \in A \,|\, [A, x, A] = 0\}$ and the *right nucleus* of A is $\mathrm{Nuc}_r(A) = \{x \in A \,|\, [A, A, x] = 0\}$. $\mathrm{Nuc}_l(A)$, $\mathrm{Nuc}_m(A)$, and $\mathrm{Nuc}_r(A)$ are associative subalgebras of A. Their intersection $\mathrm{Nuc}(A) = \{x \in A \,|\, [x, A, A] = [A, x, A] = [A, A, x] = 0\}$ is the *nucleus* of A. $\mathrm{Nuc}(A)$ is an associative subalgebra of A containing $F1$ and $x(yz) = (xy)z$ whenever one of the elements x, y, z is in $\mathrm{Nuc}(A)$. The *center* of A is $\mathrm{C}(A) = \{x \in A \,|\, x \in \mathrm{Nuc}(A)$ and $xy = yx$ for all $y \in A\}$.

1.2. **Differential polynomial rings.** Let D be an associative division ring and $\delta : K \to K$ a *derivation*, i.e. an additive map such that

$$\delta(ab) = a\delta(b) + \delta(a)b$$

for all $a, b \in K$. The *differential polynomial ring* $D[t; \delta]$ is the set of polynomials

$$a_0 + a_1 t + \cdots + a_n t^n$$

with $a_i \in D$, where addition is defined term-wise and multiplication by

$$ta = at + \delta(a) \quad (a \in K).$$

For $f = a_0 + a_1 t + \cdots + a_n t^n$ with $a_n \neq 0$ define $\deg(f) = n$ and $\deg(0) = -\infty$. Then $\deg(fg) = \deg(f) + \deg(g)$. An element $f \in R$ is *irreducible* in R if it is no unit and it has no proper factors, i.e if there do not exist $g, h \in R$ with $\deg(g), \deg(h) < \deg(f)$ such that $f = gh$.

$R = D[t; \delta]$ is a left and right principal ideal domain and there is a right division algorithm in R: for all $g, f \in R$, $g \neq 0$, there exist unique $r, q \in R$ with $\deg(r) < \deg(f)$, such that

$$g = qf + r.$$

There is also a left division algorithm in R [5, p. 3 and Prop. 1.1.14]. (Our terminology is the one used by Petit [10]; it is opposite to Jacobson's.)

We know that

$$G_{\tau,a}(\sum_{i=0}^{n} a_i t^i) = \sum_{i=0}^{n} \tau(a_i)(t + a)^i$$

is an automorphism of $R = D[t; \delta]$ if and only if τ is an automorphism of D and

$$\delta(\tau(z)) - \tau(\delta(z)) = a\tau(z) - \tau(z)a$$

for all $z \in D$ [7].

1.3. **Nonassociative algebras obtained from differential polynomial rings.** Let $f \in R = D[t;\delta]$ of degree m. Let $\text{mod}_r f$ denote the remainder of right division by f. Define $F = \text{Cent}(\delta) = \{a \in D \,|\, \delta(a) = 0\}$.

Definition 1. (cf. [10, (7)]) The vector space

$$R_m = \{g \in D[t;\delta] \,|\, \deg(g) < m\}$$

together with the multiplication

$$g \circ h = gh \text{ mod}_r f$$

is a unital nonassociative algebra $S_f = (R_m, \circ)$ over

$$F_0 = \{a \in D \,|\, ah = ha \text{ for all } h \in S_f\}.$$

F_0 is a commutative subring of D [10, (7)] and it is easy to check that $F_0 = \text{Cent}(\delta) \cap C(D)$. The algebra S_f is also denoted by R/Rf [10, 11] if we want to make clear which ring R is involved in the construction. In the following, we call the algebras S_f *Petit algebras* and denote their multiplication simply by juxtaposition.

Using left division by f and the remainder $\text{mod}_l f$ of left division by f, we can define a second unital nonassociative algebra structure on R_m over F, called ${}_fS$ or R/fR.

It suffices to consider the Petit algebras S_f, however, since every algebra ${}_fS$ is the opposite algebra of some Petit algebra (cf. [10, (1)]).

We call $f \in R$ a *(right) semi-invariant* polynomial if for every $a \in D$ there is $b \in D$ such that $f(t)a = bf(t)$. If also $f(t)t = (ct + d)f(t)$ for some $c, d \in D$ then f is called *(right) invariant*. The invariant polynomials are also called *two-sided*, as the ideals they generate are left and right ideals.

Theorem 1. *(cf.* [10, (2), p. 13-03, (5), (6), (7), (9)]*) Let $f(t) \in R = D[t;\delta]$.*
(i) If S_f is not associative then $\text{Nuc}_l(S_f) = \text{Nuc}_m(S_f) = D$ and

$$\text{Nuc}_r(S_f) = \{g \in R \,|\, fg \in Rf\}.$$

(ii) The powers of t are associative if and only if $t^m t = t t^m$ if and only if $t \in \text{Nuc}_r(S_f)$ if and only if $ft \in Rf$.
(iii) If f is irreducible then $\text{Nuc}_r(S_f)$ is an associative division algebra.
(iv) Let $f \in R$ be irreducible and S_f a finite-dimensional F-vector space or free of finite rank as a right $\text{Nuc}_r(S_f)$-module. Then S_f is a division algebra.
Conversely, if S_f is a division algebra then f is irreducible.
(v) S_f is associative if and only if f is a two-sided element. In that case, S_f is the usual quotient algebra $D[t;\delta]/(f)$.

Proposition 2. *Let $R = D[t;\delta]$ and $F_0 = F \cap C(D)$. For all $f \in F_0[t;\delta] = F_0[t]$,*

$$F_0[t]/(f) \cong F_0 \oplus F_0 t \oplus \cdots \oplus F_0 t^{m-1}$$

is a commutative subring of S_f which is an algebraic field extension of F_0 if $f(t) \in F_0[t]$ is irreducible, and

$$F_0[t]/(f) = F_0 \oplus F_0 t \oplus \cdots \oplus F_0 t^{m-1} \subset \text{Nuc}_r(S_f).$$

Proof. Since $f \in F_0[t;\delta] = F_0[t]$, S_f contains the commutative subring $F_0[t]/(f)$. This subring is isomorphic to the ring consisting of the elements $\sum_{i=0}^{m-1} a_i t^i$ with $a_i \in F_0$. In particular, we know that the powers of t are associative. By Theorem 1 (ii), this implies that $t \in \mathrm{Nuc}_r(S_f)$. Clearly $F_0 \subset \mathrm{Nuc}_r(S_f)$, so if $t \in \mathrm{Nuc}_r(S_f)$ then $F_0 \oplus F_0 t \oplus \cdots \oplus F_0 t^{m-1} \subset \mathrm{Nuc}_r(S_f)$, hence we obtain the assertion. If f is irreducible in $F_0[t]$, this is an algebraic field extension of F_0. □

Proposition 3. *Let $f \in R$ be of degree $m \geq 2$. Then f is a semi-invariant polynomial if and only if*

$$D \subset \mathrm{Nuc}_r(S_f).$$

Proof. If $f \in R$ is a semi-invariant polynomial then for every $a \in D$ there is $b \in D$ such that $f(t)a = bf(t) \in Rf$ and hence $D \subset \{g \in R_m \,|\, fg \in Rf\} = \mathrm{Nuc}_r(S_f)$.

Conversely, if $D \subset \mathrm{Nuc}_r(S_f)$ then for all $a \in D$ there is $g(t) \in R$ such that $f(t)a = g(t)f(t)$. Comparing degrees, this means $g(t) \in D$, so that for all $a \in D$ there is $b \in D$ such that $f(t)a = bf(t)$. □

Corollary 4. *Let $R = D[t;\delta]$. If R is simple then there are no non-associative algebras S_f such that $D \subset \mathrm{Nuc}_r(S_f)$.*

Proof. If $R = D[t;\delta]$, R is not simple if and only if there is a non-constant semi-invariant $f \in R$ [8]. The assertion now follows from Proposition 3. □

We will assume throughout the paper that $f(t) \in D[t;\delta]$ has $\deg(f(t)) = m \geq 2$ (if f has degree $m = 1$ then $S_f \cong D$) and that $\delta \neq 0$. Without loss of generality, we only only look at monic $f(t)$.

1.4. **The characteristic** $p > 0$ **case.** For a division ring D of characteristic p and $R = D[t;\delta]$,

$$(t-b)^p = t^p - V_p(b), \quad V_p(b) = b^p + \delta^{p-1}(b) + *$$

for all $b \in D$, with $*$ a sum of commutators of $b, \delta(b), \ldots, \delta^{p-2}(b)$. If D is commutative, or if b commutes with all its derivatives, then the sum $*$ is 0 and the formula simplifies to

$$V_p(b) = b^p + \delta^{p-1}(b)$$

[5, p. 17ff]. An iteration yields

$$(t-b)^{p^e} = t^{p^e} - V_{p^e}(b)$$

for all $b \in D$ [5, 1.3.22] with $V_{p^e}(b) = V_p^e(b) = V_p(\ldots(V_p(b))\ldots)$. For any p-polynomial

$$f(t) = a_0 t^{p^e} + a_1 t^{p^{e-1}} + \cdots + a_e t + d \in D[t;\delta]$$

we thus have

$$f(t) - f(t-b) = a_0 V_{p^e}(b) + a_1 V_{p^{e-1}}(b) + \cdots + a_e b$$

for all $b \in D$ and define

$$V_f(b) = a_0 V_{p^e}(b) + a_1 V_{p^{e-1}}(b) + \cdots + a_e b.$$

Lemma 5. *(i)* [2, Lemmata 4] *$t^p - t - a \in D[t;\delta]$ is either irreducible or a product of commutative linear factors.*
(ii) [2, Lemmata 6] *$f(t) = t^p - t - d \in D[t;\delta]$ is irreducible if and only if $V_f(z) \neq 0$ for all $z \in D$ which is equivalent to*

$$V_p(z) - z \neq d$$

for all $z \in D$.
(iii) [3] *In characteristic 3, $f(t) = t^3 - ct - d \in D[t;\delta]$ is irreducible if and only if*

$$V_3(z) - cz \neq d \text{ and } V_3(z) - zc + \delta(c) \neq d$$

for all $z \in D$.

Proof. (iii) f is irreducible if and only if it neither right nor left divisible by some linear factor $t - z$, $z \in D$. Now $f(t) \neq g(t)(t - z)$ for all $z \in D$ is equivalent to $V_f(z) \neq 0$ for all $z \in D$ [5] (i.e. to $V_3(z) - cz \neq d$), and $f(t) \neq (t - z)h(t)$ for all $z \in D$ is equivalent to $V_3(z) - zc - d + \delta(c) \neq 0$ for all $z \in D$ by a straightforward calculation. □

2. Petit's algebras from algebraic derivations

Let C be a field of characteristic p and D a central division algebra over C of degree n (we allow $D = C$ here). Let δ be a derivation of D, such that $\delta|_C$ is algebraic with minimum polynomial

$$g(t) = t^{p^e} + a_1 t^{p^{e-1}} + \cdots + a_e t \in F[t]$$

of degree p^e, where $F = \mathrm{Const}(\delta)$. Then $g(\delta) = id_{d_0}$ is an inner derivation of D and we choose $d_0 \in F$ so that $\delta(d_0) = 0$ [5, Lemma 1.5.3]. The center of $R = D[t;\delta]$ is $F[z]$ with $z = g(t) - d_0$ and the two-sided $f \in D[t;\delta]$ are of the form $f(t) = uh(t)$ with $u \in D$ and $h(t) \in C(R)$ [5, Theorem 1.1.32]. For all $a \in C$, define

$$V(a) = V_g(a) = V_{p^e}(a) + a_1 V_{p^{e-1}}(a) + \cdots + a_e a.$$

Then $V(a) \in F$ [6] and $V : C \longrightarrow F$ is a homomorphism of the additive groups C and F. Moreover,

$$V(a) = 0 \text{ if and only if } a = \delta(c)/c$$

for some $c \in C$ ([6], cf. also [4, p. 2]. V can be seen as an additive analogue to the norm of a cyclic separable field extension.

In particular, δ is a quasi-algebraic derivation on D in the sense of [8] and so $R = D[t;\delta]$ is not simple. Theorem 1 together with Proposition 2 and Corollary 4 yields:

Theorem 6. *Let $f \in D[t;\delta]$ have degree m.*
(i) S_f is a unital algebra over F of dimension mn^2p^e and if f is irreducible then S_f is a division algebra over F. If f is not two-sided then its left and middle nucleus are D. D is not contained in the right nucleus.
(ii) If $f \in F[t]$ then $\mathrm{Nuc}_r(S_f)$ contains the subring

$$F[t]/(f) \cong F \oplus Ft \oplus \cdots \oplus Ft^{m-1}$$

which is a subfield of degree mp^e over F whenever $f(t) \in F[t]$ is irreducible.
(iii) If $f(t) \in C[t;\delta]$, then S_f contains $C[t;\delta]/C[t;\delta]f$ as a subalgebra of dimension mp^e over F.

When S_f is not associative, any automorphism of S_f extends an automorphism of D since the left nucleus of an algebra is left invariant under automorphisms.

Let $H : D[t;\delta] \longrightarrow D[t;\delta]$ be any F-automorphism of $R = D[t;\delta]$. Then H canonically induces an isomorphism of F-algebras

$$S_f \cong S_{H(f)}.$$

This leads us to:

Proposition 7. *Let $f(t) = a_0 t^{p^e} + a_1 t^{p^{e-1}} + \cdots + a_e t + d \in D[t;\delta]$ be a p-polynomial of degree p^e.*
(i) $S_f \cong S_h$ for all $h(t) = f(t) - V_f(a)$, $a \in C$.
(ii) The map $G_{id,-a}$ defined via $G|_D = id_D$ and $G(t) = t - a$ is an automorphism of S_f for all $a \in C$ such that $V_f(a) = 0$.

Proof. We know that $G = G_{id,-a}$ is an automorphism of R if and only if $a \in C(D) = C$. G is F-linear. Since $f(t) - f(t-a) = V_f(a)$ for all $a \in C$, $G(f(t)) = f(t-a) = f(t) - V_f(a)$, so that $G(f(t)) = f(t)$ for all $a \in C$ with $V_f(a) = 0$ implying (ii). □

We conclude:

Proposition 8. *For $f(t) = g(t) - d \in D[t;\delta]$,*

$$\ker(V) = \{a \in C \,|\, V(a) = 0\} = \{\delta(c)/c \,|\, c \in C\}$$

is isomorphic to the subgroup $\{G_{id,-a} \,|\, a \in C$ with $V(a) = 0\}$ of $\mathrm{Aut}_F(S_f)$.

Proof. There is a one-one correspondence between the sets $\ker(V)$ and $\{G_{id,-a} \,|\, a \in C, V(a) = 0\}$ of $\mathrm{Aut}_F(S_f)$ given by $a \mapsto G_{id,-a}$ which yields the assertion. □

For $f(t) = t^p - t - d$ we have in particular $G(f(t)) = f(t)$ for all $a \in C(D)$ with $\delta^{p-1}(a) + a^p - a = 0$.

Lemma 9. *For $f(t) = t^p - t - d \in D[t;\delta]$, $G_{id,-1} \in \mathrm{Aut}(S_f)$ has order p.*

Proof. $G = G_{id,-1}$ is an automorphism of R of order p [2]. For $f(t) = t^p - t - d$ we have $G(f(t)) = f(t)$ since $\delta^{p-1}(1) + 1^p - 1 = 0$. Thus $G_{id,-1}$ induces an automorphism of S_f, it is easy to see it has order p. □

3. Nonassociative differential extensions of a field

Let K be a field of characteristic p together with a derivation $\delta : K \to K$ and $F = \mathrm{Const}(\delta)$. Put $R = K[t;\delta]$. We assume that δ is an algebraic derivation of K of degree p^e with minimum polynomial

$$g(t) = t^{p^e} + c_1 t^{p^{e-1}} + \cdots + c_e t \in F[t]$$

of degree p^e. Then K is a purely inseparable extension of F of exponent one, and $K^p \subset F \subset K$. More precisely, $K = F(u_1, \dots, u_e) = F(u_1) \otimes_F \dots \otimes_F F(u_e)$, $u_i^p = a_i \in F$, and $[K : F] = p^e$. The center of R is $F[z]$ with $z = g(t) - d_0$, $d_0 \in F$.

Theorem 6 becomes:

Theorem 10. *Let $f \in K[t; \delta]$ have degree m. Then S_f is an algebra over F of dimension mp^e and if $f(t)$ is irreducible then S_f is a division algebra. If f is not two-sided then S_f has left and middle nucleus K and K is not contained in the right nucleus.*
In particular, if $f(t) \in F[t]$ then $\mathrm{Nuc}_r(S_f)$ contains the subring

$$F[t]/(f) \cong F \oplus Ft \oplus \dots \oplus Ft^{m-1}$$

which is a subfield of degree m over F whenever $f(t)$ is irreducible in $F[t]$.

We will investigate the following special case:

Definition 2. Let $f(t) = g(t) - d \in K[t; \delta]$. Then the F-algebra

$$(K, \delta, d) = S_f = K[t; \delta]/K[t; \delta]f(t)$$

is called a *(nonassociative) differential extension* of K.

(K, δ, d) has dimension p^{2e}, is free of dimension p as a K-vector space, and contains K as a subfield. (K, δ, d) is associative if and only if $d \in F$ and a division algebra if and only if $f(t)$ is irreducible. For $d \in K \setminus F$ it has left and middle nucleus K.

Proposition 11. *(i) For $d \in K \setminus F$, the right nucleus of (K, δ, d) contains K, thus*

$$\mathrm{Nuc}((K, \delta, d)) = K.$$

The powers of t are not associative in (K, δ, d).
(ii) For all $a, d \in K$, $(K, \delta, d) \cong (K, \delta, d - V(a))$.

Proof. (i) Since g is semi-invariant and monic of minimal degree, we have $g(t)a = ag(t)$ for all $a \in K$ [8, (2.1), p. 3], i.e. $f(t)a = af(t)$ for all $a \in K$ and so f is semi-invariant, too, and hence the right nucleus of (K, δ, d) contains K by Proposition 3. By [8], f is two-sided iff f is semi-invariant and $ft \in Rf$. Here, f is not two-sided, therefore $ft \notin Rf$, which implies that the powers of t are not associative in (K, δ, d) by Theorem 1.
(ii) For $a, d \in K$ and $G = G_{id,-a}$ we have $G(f(t)) = f(t) - V(a)$ and $S_f \cong S_{G(f)}$. □

In fact, for $f(t) = g(t) - d \in F[t]$ (i.e. here $f(t)$ is two-sided),

$$(K, \delta, d) = K[t; \delta]/K[t; \delta]f(t)$$

is an associative central simple F-algebra called a *differential extension of* K and treated in [5, p. 23]. Then K is a maximal subfield of (K, δ, d). Note that (K, δ, d) contains the subring $F[t]/(f(t))$, which is a field extension of F of degree p^e whenever $f(t)$ is irreducible in $F[t]$ (thus a maximal subfield of (K, δ, d)).

Remark 12. In the special case where $g(t) = t^p - t$ and $f(t) = t^p - t - d \in F[t]$, the automorphism group of (K, δ, d) has a cyclic subgroup of order p generated by $G_{id,-1}$ which leaves K invariant. If $f(t) = t^p - t - d$ is irreducible then the division algebra (K, δ, d) is called a *cyclic extension of* K of degree p by Amitsur, as it can be seen as a noncommutative generalization of a cyclic field extension of K: it has dimension p as a K-vector space and the automorphism group of (K,δ,d) has a cyclic subgroup of order p. All cyclic extensions of K of degree p are of this form [2]. Note that they always contain the cyclic separable field extension $F[t]/(t^p-t-d)$ of degree p.

When $g(t)=t^p-t\in F[t]$ and $f(t)=t^p-t-d\in K[t;\delta]$, $d\in K\setminus F$ is irreducible, the nonassociative division algebra (K,δ,d) is a canonical, nonassociative, generalization of a cyclic extension:

Theorem 13. *Let δ be of degree p with minimum polynomial $g(t)=t^p-t\in F[t]$. Let $f(t)=t^p-t-d\in K[t;\delta]$. Then*

$$(K,\delta,d)=K[t;\delta]/K[t;\delta]f(t)$$

is a nonassociative algebra over F of dimension p^2, and is a division algebra if and only if

$$V_p(z)-z\neq d$$

for all $z\in K$, if and only if

$$z^p+\delta^{p-1}(z)-z\neq d$$

for all $z\in K$. $\mathrm{Aut}_F(S_f)$ has a cyclic subgroup of order p generated by $G=G_{id,-1}$, i.e. $G|_K=id_K$.

Proof. Here $f(t)=t^p-t-d\in K[t;\delta]$ is irreducible if and only if for all $z\in K$, $V_p(z)-z\neq d$ by Lemma 5 (ii). Since K is commutative, the second equivalence is clear. The remaining assertion follows from Lemma 9. □

If $d\in F$ then $S_f=(K,\delta,d)$ is the cyclic extension of F of degree p in Remark 12. As a corollary of Theorem 13 we obtain a canonical construction method for *nonassociative cyclic extensions* of K, if we define these algebras as division algebras containing K which are K-vector spaces of dimension p and whose automorphism group contains a cyclic subgroup of order p which leaves K invariant:

Theorem 14. *Let δ be of degree p with minimum polynomial $g(t)=t^p-t\in F[t]$. For all $f(t)=t^p-t-d\in K[t;\delta]$ with $d\in K\setminus F$, (K,δ,d) is a unital nonassociative division algebra over F of dimension p^2. Its left and middle nucleus is K, its right nucleus contains K, and its automorphism group contains a cyclic subgroup of order p which leaves K invariant.*

Proof. Suppose there is $z\in K$ such that $z^p+\delta^{p-1}(z)-z=d$. Apply δ to both sides to obtain $\delta(z^p)+\delta^p(z)-\delta(z)=\delta(d)$, which means $\delta(z^p)=\delta(d)$ since $\delta^p=\delta$ here. Now $\delta^p(z)=pz^{p-1}\delta(z)=0$ implies that $\delta(d)=0$ and hence the first assertion since $d\notin F$ by Lemma 5 (ii). The right nucleus contains K by Proposition 11 and the remaining assertion follows from Theorem 13. □

Example 15. Let δ have minimum polynomial $g(t)=t^p-t\in F[t]$. Let x be an indeterminate and δ be the extension of δ to $K(x)$ via $\delta(x)=0$. Clearly $\mathrm{Const}(\delta)=F(x)$ and

$g(t) = t^p - t \in F(x)[t]$ is the minimal polynomial of the extended derivation δ. Then for all $h(x) \in K(x) \setminus F(x)$, $f(t) = t^p - t - h(x)$ is irreducible and hence

$$(K(x), \delta, h(x))$$

is a unital nonassociative division algebra over $F(x)$ of dimension p^2, and a nonassociative cyclic extension of $K(x)$. This generalized [5, Proposition 1.9.10].

When F has characteristic 3, using Lemma 5 and Proposition 8 we can generalize Theorem 14 slightly:

Theorem 16. *Let F have characteristic 3 and δ be of degree 3 with minimum polynomial $g(t) = t^p - ct \in F[t]$. For all $f(t) = t^p - ct - d \in K[t;\delta]$ with $d \in K \setminus F$, (K, δ, d) is a nine-dimensional unital nonassociative division algebra over F. Its left and middle nucleus is K, its right nucleus contains K and $\{\delta(c)/c \,|\, c \in K\}$ is isomorphic to the subgroup $\{G_{id,-a} \,|\, a \in C \text{ with } V(a) = 0\}$ of $\mathrm{Aut}_F((K, \delta, d))$.*

Proof. Suppose there is $z \in K$ such that $z^3 + \delta^2(z) - cz = d$. Apply δ to both sides to obtain $\delta(z^3) + \delta^p(z) - c\delta(z) = \delta(d)$. Now $\delta^3(z) = 0$ and $\delta^3 = c\delta$ implies that $0 = \delta(d)$, a contradiction. Next assume that that there is $z \in K$ such that $z^3 + \delta^2(z) - cz + \delta(c) = d$. Apply δ to both sides to obtain $\delta(z^3)+\delta^p(z)-c\delta(z)++\delta^2(c) = \delta(d)$, i.e. again that $0 = \delta(d)$, a contradiction. Thus f is irreducible by Lemma 5 (iii). The right nucleus contains K by Proposition 11 and the assertion follows. □

Example 17. Let F have characteristic 3 and δ be of degree 3 with minimum polynomial $g(t) = t^3 - ct \in F[t]$. Let x be an indeterminate and δ be the extension of δ to $K(x)$ via $\delta(x) = 0$. Clearly $\mathrm{Const}(\delta) = F(x)$ and $g(t) = t^3 - ct \in F(x)[t]$ is the minimal polynomial of the extended derivation δ. Then for all $h(x) \in K(x) \setminus F(x)$, $f(t) = t^3 - ct - h(x)$ is irreducible and so

$$(K(x), \delta, h(x))$$

is a unital nine-dimensional nonassociative division algebra over $F(x)$. This again generalizes [5, Proposition 1.9.10].

4. Nonassociative differential extensions of a division algebra

4.1. Let C be a field of characteristic p and D a central division algebra over C of degree n. Let δ be a derivation of D, such that $\delta|_C$ is algebraic with minimum polynomial

$$g(t) = t^{p^e} + c_1 t^{p^{e-1}} + \cdots + c_e t \in F[t]$$

of degree p^e and $F = \mathrm{Const}(\delta)$ as in Section 2.

Definition 3. For all $f(t) = g(t) - d \in D[t;\delta]$, the F-algebra

$$(D, \delta, d) = S_f = D[t;\delta]/D[t;\delta]f(t)$$

is called a *(nonassociative) generalized differential algebra.*

(D, δ, d) is a unital nonassociative algebra over F of dimension $p^{2e}n^2$ and free of rank p^e as a left D-module, and contains D as a subalgebra. For $d \in D \setminus F$ it has left and middle nucleus D.

Lemma 18. *For $d \in D \setminus F$, the right nucleus of (D, δ, d) does not contain D, thus* $\mathrm{Nuc}((D, \delta, d))$ *is properly contained in D.*
If $d \in C \setminus F$, then $(C, \delta|_C, d)$ is a subalgebra of (D, δ, d) and the right nucleus of (D, δ, d) contains C, thus $C \subset \mathrm{Nuc}((D, \delta, d))$.

Proof. Since g is semi-invariant and monic of minimal degree, we have $g(t)a = ag(t)$ for all $a \in D$ [8, (2.1), p. 3], i.e. $f(t)a = ag(t) - da$ for all $a \in D$ and so f is not semi-invariant, since this would mean that $da = ad$ for all $a \in D$ and we assumed $d \in D \setminus F$. Hence the right nucleus of (K, δ, d) does not contain D by Proposition 3.

If $d \in C \setminus F$, then $f \in C[t, \delta] = C[t; \delta|_C]$ is semi-invariant in $C[t, \delta]$ and $\delta|_C$ is an algebraic derivation on C with minimum polynomial $g(t)$ of degree p^e. Since $d \in C$, f is semi-algebraic in $C[t, \delta]$, see the proof of Lemma 11. Thus for every $a \in C$ we have $f(t)a \in C[t; \delta]f \subset Rf$ and hence $C \subset \mathrm{Nuc}_r((D, \delta, d))$. □

Proposition 19. *For all $d \in D$ and $a \in C$,*

$$(D, \delta, d) \cong (D, \delta, d - V(a)).$$

Proof. The proof is analogous to the one of Proposition 11 (ii). □

(D, δ, d) is associative if and only if $d \in F$ and a division algebra if and only if $f(t)$ is irreducible. For $f(t) = g(t) - d \in F[t]$, the associative F-algebra

$$(D, \delta, d) = S_f = D[t; \delta]/D[t; \delta]f(t)$$

is a central simple algebra over F and called a *generalized differential extension of* D in [5, p. 23]. The defining relations characterizing the associative algebra (D, δ, d) are given by

$$ta = at + \delta(a) \text{ and } t^{p^e} + c_1 t^{p^{e-1}} + \cdots + c_e t = d$$

for all $a \in D$ [5, p. 23]. Moreover, the central simple algebra (D, δ, d) contains D as the centralizer of C [4, Theorem 3.1] and Proposition 19 for $d \in F$ was proved in [4, Theorem 3.2].

In the special case where $g(t) = t^p - t$ and hence $f(t) = t^p - t - d \in F[t]$, the automorphism group of the central simple algebra (D, δ, d) of degree n^2p^2 has a cyclic subgroup of order p generated by $G_{id,-1}$ which leaves D invariant. If f is irreducible then the division algebra (D, δ, d_0) is also called a *cyclic extension of* D of degree p by Amitsur, as it is also free of rank p as a right D-module and thus can be seen as canonical generalization of a cyclic field extension. All cyclic extensions of D of degree p are of this form [2].

Note that if $f(t) = t^p - t - d \in F[t]$ is irreducible, then (D, δ, d) also contains the cyclic field extension $F[t]/(t^p - t - d)$ of dimension p over F as a subfield.

Theorem 20. *Let δ have minimum polynomial*

$$g(t) = t^p - t \in F[t].$$

Then for all $f(t) = t^p - t - d \in D[t; \delta]$,

$$(D, \delta, d) = D[t; \delta]/D[t; \delta]f(t)$$

is a nonassociative algebra over F of dimension n^2p^2 and a division algebra if and only if

$$d \neq V_p(z) - z$$

for all $z \in D$, if and only if

$$d \neq (t-z)^p - t^p - z$$

for all $z \in D$. (D, δ, d) is associative if and only if $d \in F$.

$\mathrm{Aut}_F((D, \delta, d))$ *has a cyclic subgroup of order p generated by $G = G_{id,-1}$, i.e. $G|_D = id_D$.*

Proof. We know that $S_f = (D, \delta, d) = D[t; \delta]/D[t; \delta]f(t)$ with $f(t) = t^p - t - d$ is a division algebra if and only if $d \neq V_p(z) - z$ for all $z \in D$ by Lemma 5 (ii). The remaining assertion follows from Lemma 9. □

This nicely generalizes [5, Theorem 1.3.27] on cyclic extensions of D whenever f is irreducible. We thus call unital nonassociative division algebras which contain D as a subalgebra, are free of rank p as a left D-module and have a cyclic subgroup of automorphisms of order p which restrict to id_D on D, *nonassociative cyclic extensions of D of degree p.*

In particular, if $f(t) \in C[t; \delta]$ in Theorem 20, then (D, δ, d) contains the nonassociative cyclic extension $(C, \delta, d) = C[t; \delta]/C[t; \delta]f$ of C treated in Theorem 13 as a subalgebra of dimension p^2 over F. This is a division subalgebra whenever $d \in C \setminus F$ by Theorem 14.

Note also that for $f(t) = t^p - t - d \in D[t; \delta]$ and all $a \in C$ we have

$$(D, \delta, d) \cong (D, \delta, d + \delta^{p-1}(a) + a^p - a) = (D, \delta, d + V_p(a) - a).$$

Remark 21. Petit's construction of nonassociative algebras S_f can be generalized to the setting where $f \in S[t; \delta]$ is a monic polynomial and S any unital associative ring [14]. Therefore some of the results above also hold for nonassociative algebras obtained by employing $f(t) = t^p - t - d \in S[t; \delta]$ if δ satisfies the polynomial identity $\delta^p = \delta$ as before. I.e., we can construct algebras which are free of rank p as left S-modules whose automorphism group contains a cyclic subgroup of order p. Amitsur's method of determining the (associative) cyclic extensions of division rings D was extended to simple rings S already in [7].

When F has characteristic 3, we can generalize Theorem 20 slightly, employing Lemma 5 and and Proposition 8:

Theorem 22. *Let δ have minimum polynomial*

$$g(t) = t^3 - ct \in F[t].$$

Then for all $f(t) = t^3 - ct - d \in D[t; \delta]$,

$$(D, \delta, d) = D[t; \delta]/D[t; \delta]f(t)$$

is a nonassociative unital algebra over F of dimension $9n^2$ and a division algebra if and only if

$$V_3(z) - cz \neq d \text{ and } V_3(z) - zc - d + \delta(c) \neq 0$$

for all $z \in D$. (D, δ, d) is associative if and only if $d \in F$. $\mathrm{Aut}_F((D, \delta, d))$ has a subgroup isomorphic to $\{\delta(c)/c \,|\, c \in K\}$.

4.2. Let D be a central division algebra over C of degree $[D : F] = n$ and let C have characteristic p. As a consequence of [10, (3)] we obtain the following partial generalization of [2, Theorem 3] which states when a nonassociative cyclic extension S of D of degree p has the form discussed in Theorem 20:

Theorem 23. *Let S be a division ring with multiplication $\circ$, which is not associative, such that*
(1) S has D as subring, is a free left D-module of rank p, and there is $t \in S$ such that $t^0, t, t^2, \dots, t^{p-1}$ is a basis of S over D, when defining $t^{i+1} = t \circ t^i$, $t^0 = 1$, for $0 \leq i < p$;
(2) for all $a \in D$, $a \neq 0$, there is $a' \in D^\times$ such that $t \circ a = a \circ t + a'$;
(3) for all $a, b, c \in D$, $i + j < p$, $k < p$, we have

$$[a \circ t^i, b \circ t^j, c \circ t^k] = 0,$$

(4) $t^p = t + d$ for some $d \in D^\times$ with $t^p = t \circ t^{p-1}$ as above. Then

$$\delta(a) = a' = t \circ a - a \circ t \quad (a \in D)$$

is a derivation on D and

$$S \cong S_f$$

with $f(t) = t^p - t - d \in D[t; \delta]$ irreducible. For any $H \in \mathrm{Aut}_F(S_f)$, $H|_D \in \mathrm{Aut}_F(D)$.
If, in particular, $\delta|_C$ is algebraic with minimal polynomial $g(t) = t^p - t$ and $F = \mathrm{Const}(\delta)$ then S is a nonassociative cyclic extension of D of dimension $p^2[D : F]$ over F.

Remark 24. Conditions (1), (2), (3) are equivalent to conditions (1), (2), (5), (6), (7) with
(5) $D \subset \mathrm{Nuc}_l(S) \cap \mathrm{Nuc}_m(S)$;
(6) $t^i \circ b = t \circ (t^{i-1} \circ b)$ for all $b \in D$, $0 \leq i < p$,
(7) for $0 \leq i, j, k < p$ and $i + j < p$, $k < p$, we have $[t^i, t^j, t^k] = 0$ [10, (3)].

An analogous result holds when $D = K$ is a field of characteristic p and we consider the setup as in Section 3.

5. Some tensor product constructions

Let E/F be a finite dimensional purely inseparable extension of exponent one and characteristic p and δ a derivation on E such that $F = \mathrm{Const}(\delta)$. Then δ is an algebraic derivation of degree p^e with minimum polynomial

$$g(t) = t^{p^e} + c_1 t^{p^{e-1}} + \dots + c_e t \in F[t]$$

of degree p^e, and $[E : F] = p^e$.

Let D be an (associative) central division algebra over F such that $D_E = D \otimes_F E$ is a division algebra and let δ be the extension of δ to D_E such that $\delta|_D = 0$. Suppose that

$$S_f = E[t; \delta]/E[t; \delta]f(t)$$

with $f(t) \in E[t; \delta]$ of degree m, is a division algebra of dimension mp^e over $F = \mathrm{Const}(\delta)$ (i.e., that $f(t) \in E[t; \delta]$ is irreducible). Then the tensor product

$$S_f \otimes_F D = E[t; \delta]/E[t; \delta]f(t) \otimes_F D \cong D_E[t; \delta]/D_E[t; \delta]f(t)$$

is a nonassociative algebra over F of dimension $mp^e[D:F]$ and a division algebra if and only if $f(t)$ is irreducible in $D_E[t;\delta]$. We consider the following special case:

Theorem 25. *If $g(t)=t^p-t\in F[t]$ is the minimal polynomial of δ and $f(t)=t^p-t-d\in E[t;\delta]$, then*

$$(E,\delta,d)\otimes_F D\cong D_E[t;\delta]/D_E[t;\delta]f(t)$$

and

$$(E/F,\delta,c)\otimes_F D$$

is a nonassociative division algebra over F of dimension $p^2[D:F]$ if and only if

$$d\neq V_p(z)-z$$

for all $z\in D_E$, if and only if

$$d\neq (t-z)^p-t^p-z$$

for all $z\in D_E$.

$\mathrm{Aut}_F((E/F,\delta,c)\otimes_F D)$ has a cyclic subgroup of order p generated by $G=G_{id,-1}$, i.e. $G|_D=id_D$.

Proof. $f(t)=t^p-t-d$ is irreducible if and only if $d\neq V_p(z)-z$ for all $z\in D_E$ by Lemma 5 (ii). This is equivalent to $d\neq t^p-(t-z)^p-z$ for all $z\in D_E$ by [5, (1.3.19)]. The remaining assertion follows from Lemma 9. □

This generalizes [5, Theorem 1.9.13] which appears as the case $d\in F$.

Example 26. Let δ be of degree p with minimum polynomial $g(t)=t^p-t\in F[t]$. Let x be an indeterminate and δ be the extension of δ to $K(x)$ via $\delta(x)=0$, where $\mathrm{Const}(\delta)=F(x)$. For all $f(t)=t^p-t-h(x)$ with $h(x)\in K(x)\setminus F(x)$, $(K(x),\delta,h(x))$ is a unital nonassociative division algebra over $F(x)$ of dimension p^2, and a nonassociative cyclic extension of $K(x)$, see Example 15.

Let D be a central division algebra over F of degree n such that $D\otimes_F K$ is a division algebra. Then

$$(K(x),\delta,h(x))\otimes_{F(x)} D_{F(x)}\cong D_{K(x)}[t;\delta]/D_{K(x)}[t;\delta]f(t)$$

is a nonassociative unital algebra over $F(x)$ of dimension p^2n^2 and a division algebra if and only if

$$h(x)\neq V_p(z)-z$$

for all $z\in D_{K(x)}$, if and only if

$$h(x)\neq (t-z)^p-t^p-z$$

for all $z\in D_{K(x)}$.

Its automorphism group has a cyclic subgroup of order p generated by $G=G_{id,-1}$, so that the algebra is a nonassociative cyclic extension of $D_{K(x)}$ if it is division.

This can be seen as a generalization of [5, Theorem 1.9.11], where $h(x)=x$ in which case the algebra is division.

References

[1] A. S. Amitsur, *Differential Polynomials and Division Algebras.* Annals of Mathematics, Vol. 59 (2) (1954) 245-278.

[2] A. S. Amitsur, *Non-commutative cyclic fields.* Duke Math. J. 21 (1954), 87105.

[3] C. Brown, PhD Thesis University of Nottingham, in preparation.

[4] Hoechsmann, Klaus, *Simple algebras and derivations.* Trans. Amer. Math. Soc. 108 (1963), 1-12.

[5] N. Jacobson, "Finite-dimensional division algebras over fields." Springer Verlag, Berlin-Heidelberg-New York, 1996.

[6] N. Jacobson, *Abstract derivation and Lie algebras.* Trans. Amer. Math. Soc. 42 (2) (1937), 206-224.

[7] K. Kishimoto, *On cyclic extensions of simple rings.* J. Fac. Sci. Hokkaido Univ. Ser. I 19 (1966), 74-85.

[8] T. Y. Lam, K. H. Leung, A. Leroy, J. Matczuk, *Invariant and semi-invariant polynomials in skew polynomial rings.* Ring theory 1989 (Ramat Gan and Jerusalem, 1988/1989), 247-261, Israel Math. Conf. Proc., 1, Weizmann, Jerusalem, 1989.

[9] O. Ore, *Formale Theorie der linearen Differentialgleichungen. (Zweiter Teil).* (German) J. Reine Angew. Math. 168 (1932), 233-252.

[10] J.-C. Petit, *Sur certains quasi-corps généralisant un type d'anneau-quotient.* Séminaire Dubriel. Algèbre et théorie des nombres 20 (1966 - 67), 1-18.

[11] J.-C. Petit, *Sur les quasi-corps distributifes à base momogène.* C. R. Acad. Sc. Paris 266 (1968), Série A, 402-404.

[12] S. Pumplün, *Nonassociative generalized cyclic algebras.* Preprint.

[13] S. Pumplün, *Algebras with a central simple algebra as right nucleus.* Preprint.

[14] S. Pumplün, *Finite nonassociative algebras obtained from skew polynomials and possible applications to (f, σ, δ)-codes* online at arXiv:1507.01491[cs.IT]

[15] S. Pumplün, A. Steele, *Fast-decodable MIDO codes from nonassociative algebras.* Int. J. of Information and Coding Theory (IJICOT) 3 (1) 2015, 15-38.

[16] R. D. Schafer, "An Introduction to Nonassociative Algebras." Dover Publ. Inc., New York, 1995.

[17] A. Steele, *Nonassociative cyclic algebras.* Israel Journal of Mathematics 200 (1) (2014), 361-387.

E-mail address: susanne.pumpluen@nottingham.ac.uk

School of Mathematical Sciences, University of Nottingham, University Park, Nottingham NG7 2RD, United Kingdom