Nonassociative algebras obtained from skew polynomial rings and their applications

S. Pumplün

2017

Content:

I. Skew-polynomial rings

Let D be a unital associative division ring, σ a ring endomorphism of D, $\delta : D \to D$ a *left σ-derivation* of D, i.e. an additive map such that

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

for all $a, b \in D$. The *skew-polynomial ring* $R = D[t; \sigma, \delta]$ is the set of polynomials

$$f(t) = a_n t^n + \cdots + a_1 t + a_0 \quad (a_i \in D)$$

where addition is defined term-wise and multiplication by the rule

$$ta = \sigma(a)t + \delta(a) \text{ for all } a \in D.$$

Example: $D[t] = D[t; id, 0]$ is the ring of left polynomials, with the "usual" multiplication

$$(\sum_{i=1}^{s} a_i t^i)(\sum_{i=1}^{t} b_i t^i) = \sum_{i,j} a_i b_j t^{i+j}.$$

• For $f(t) = a_n t^n + \cdots + a_1 t + a_0 \in R$ with $a_n \neq 0$ define the *degree* of f as

$$\deg(f) = n \text{ and } \deg(0) = -\infty.$$

Then $\deg(fg) = \deg(f) + \deg(g)$.

• $f(t) \in R = D[t; \sigma, \delta]$ is *irreducible* in R if $f(t)$ is no unit and it has no proper factors, i.e if there do not exist $g(t), h(t) \in R$ with $\deg(g), \deg(h) < \deg(f)$ such that $f(t) = g(t)h(t)$.

• There is a *right-division algorithm* in $R = D[t;\sigma,\delta]$: for all $f(t), g(t) \in R$, $f(t) \neq 0$, there exist unique $r(t), q(t) \in R$, deg$(r) <$ deg(f), such that

$$g(t) = q(t)f(t) + r(t).$$

II. Nonassociative algebras

Let F be a field. An *algebra* A over F is an F-vector space together with a bilinear map $A \times A \to A$, $(x,y) \to x \cdot y$, the *multiplication* of A.

A is *unital* $\Leftrightarrow \exists\ e \in A$: $e \cdot x = x \cdot e = x$ for all $x \in A$.

A is a *division algebra* over F, if $A \neq 0$ and if left and right multiplication $L_a, R_a : A \to A$, $L_a(x) = a \cdot x$, $R_a(x) = x \cdot a$, are bijective for all $a \in A$, $a \neq 0$.

For $\dim_F A < \infty$, this implies: A division algebra $\Leftrightarrow$ A has no zero divisors (so $uv = 0$ means $u = 0$ or $v = 0$).

• The associator $[x, y, z] = (xy)z - x(yz)$ measures the associativity of A:

• $\mathrm{Nuc}_l(A) = \{x \in A \,|\, [x, A, A] = 0\}$ is the *left nucleus*,

• $\mathrm{Nuc}_m(A) = \{x \in A \,|\, [A, x, A] = 0\}$ the *middle nucleus*,

• $\mathrm{Nuc}_r(A) = \{x \in A \,|\, [A, A, x] = 0\}$ the *right nucleus*,

• $\mathrm{Nuc}(A) = \mathrm{Nuc}_l(A) \cap \mathrm{Nuc}_m(A) \cap \mathrm{Nuc}_r(A)$ is the *nucleus* of A.

• $\mathrm{C}(A) = \{x \in A \,|\, x \in \mathrm{Nuc}(A)$ and $xy = yx$ for all $y \in A\}$ is the *center* of A.

III. How to construct nonassociative algebras from skew-polynomial rings

Let $f(t) \in R = D[t;\sigma,\delta]$ have degree m.

• If $Rf(t)$ is a two-sided ideal, $R/Rf(t)$ is a quotient ring.

> ...but what if $Rf(t)$ is not a two-sided ideal?

• Then $R/Rf(t)$ is a left R-module...but also has a nonassociative ring structure!

Theorem (Petit, 1966) Let $\mathrm{mod}_r f$ denote the remainder of right division by f. Then

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

together with the usual addition and the multiplication

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

is a unital nonassociative ring S_f which is an algebra over

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

F_0 is a subfield of D. S_f is also denoted by $R/Rf(t)$.

- S_f is associative iff $Rf(t)$ is a two-sided ideal.

In that case, $S_f = R/Rf(t)$ is the classical quotient algebra obtained by factoring out a two-sided ideal.

Example Let $^-$ be complex conjugation, then

$$\mathbb{C}[t;^-]/\mathbb{C}[t;^-](t^2+1) \cong \mathbb{H} = (-1,-1)_{\mathbb{R}},$$

while

$$\mathbb{C}[t;^-]/\mathbb{C}[t;^-](t^2+i)$$

is a *nonassociative quaternion division algebra* over $\mathbb{R}$ with nucleus $\mathbb{C}$ (Dickson '35).

Are these algebras actually useful for anything?

• Yes: in space-time block coding (Adv. Math. Comm. 2015 (joint with Steele), J. Algebra 2016);

in particular to build fast-decodable space-time codes for less receive than transmit antennas, like the iterated codes constructed by Markin, Oggier and Srinath, Rajan (both in IEEE Trans. Inf. Theory, 2013).

• Over finite fields they yield Jha-Johnson semifields, i.e., certain finite-dimensional division algebras (Lavrauw-Sheekey, Adv. Geom. 2013).

• They are the algebras behind linear (f, σ, δ)-codes, e.g. skew-cyclic codes (to appear in Adv. Math. Comm.).

• They can be seen as generalizations of classical central simple algebras (csa's)... some of them will only have inner automorphisms, as it is the case for the classical associative csa's.

IV. Some structure theory

Let $f(t) \in R = D[t;\sigma,\delta]$ have degree ≥ 2.

Theorem (Petit, '67)
(i) If $f(t) \in D[t;\sigma,\delta]$ is irreducible, then right multiplication with a is bijective for all non-zero $a \in S_f$, hence S_f is a *right division algebra*: each non-zero element in S_f has a left inverse.

(ii) If $f(t)$ is irreducible and S_f is a finite-dimensional F_0-vector space, then S_f is a division algebra.

(iii) S_f has no zero divisors iff $f(t) \in D[t;\sigma,\delta]$ is irreducible.

Theorem (Petit, '66)
(i) If S_f is not associative then $\text{Nuc}_l(S_f) = \text{Nuc}_m(S_f) = D$, and

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

(ii) If $f(t) \in D[t;\sigma,\delta]$ is irreducible then $\text{Nuc}_r(S_f)$ is an associative division algebra.

IV. Algebras whose right nucleus is a central simple algebra

$\boxed{char(F) = 0\text{:}}$ Let K/F be a field extension such that F is algebraically closed in K. Let $K[t;\delta] = K[t;id,\delta]$, $\text{Const}(\delta) = \{a \in K \mid \delta(a) = 0\} = F$.

Theorem (Amitsur '54) If A is a central simple algebra over F of degree m that is split by K, then

$$A \cong \mathrm{Nuc}_r(S_f)$$

for some $f(t) \in K[t;\delta]$ of degree m.

Theorem For every csa A over F of degree m, there is a field extension K splitting A, where F is algebraically closed in K, and a differential polynomial $f(t) \in K[t;\delta]$ of degree m, such that

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

is an infinite-dimensional algebra over F with

$$\mathrm{Nuc}_r(S_f) \cong A$$

and $\mathrm{Nuc}_l(S_f) = \mathrm{Nuc}_m(S_f) \cong K$.

Example Let $F = \mathbb{R}$, $A = (-1,-1)_{\mathbb{R}}$, and K be the function field of the projective real conic $x^2+y^2+z^2=0$. K splits $(-1,-1)_{\mathbb{R}}$. Take a derivation δ on K with $\mathbb{R} = \mathrm{Const}(\delta)$. Then there is $f(t) \in K[t;\delta]$ of degree 2, such that

$$S_f = K[t;\delta]/K[t;\delta]f(t) = K \oplus Kt$$

is an infinite-dimensional unital algebra over $\mathbb{R}$ with $\mathrm{Nuc}_r(S_f) \cong (-1,-1)_{\mathbb{R}}$ and $\mathrm{Nuc}_l(S_f) = \mathrm{Nuc}_m(S_f) \cong K$.

$\boxed{char(F) = p\text{:}}$ Let A be a p-algebra of degree m over F which is split by a purely inseparable extension K of exponent one (i.e. $[K : F] = p^e$, A has exponent p). Define a derivation δ on K with Const$(\delta) = F$.

Theorem (Amitsur '54) If $m \leq [K : F]$ then $A \cong \text{Nuc}_r(S_f)$ for some $f \in K[t;\delta]$ of degree m.

Theorem Suppose A is a division algebra. Then $m \leq [K : F]$ and:
(i) If $m = [K : F]$ then $A \cong S_f$ with $f \in K[t;\delta]$ two-sided and irreducible of degree m.
(ii) If $m < [K : F] = p^e$ then there exists an irreducible $f \in K[t;\delta]$ of degree m such that S_f is a division algebra of dimension mp^e over F. S_f has right nucleus A and left and middle nucleus K.

Remark To find an algebra S_f of smallest possible dimension which contains a given csa A of degree m as a right nucleus is equivalent to finding a purely inseparable extension K of exponent one and smallest possible degree $m < [K : F] = p^e$ splitting A. This is connected to the question how many cyclic algebras are needed such that A is similar to a product of cyclic algebras of degree p in the Brauer group $Br(F)$.

Theorem Let A be a p-algebra over F of degree m, index $d = p^n$ and exponent p, such that $m = r^2 p^n < p^{d-1}$. Then there is a purely inseparable extension K of exponent one with $[K : F] = p^{d-1}$, and $f(t) \in K[t;\delta]$ of degree m such that

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

is an algebra over F of dimension mp^{d-1} with right nucleus A.

VI. The multiplicative loops of the algebras S_f.

Let $F = \mathbb{F}_q$, $K = \mathbb{F}_{q^n}$ and Gal$(K/F) = \langle\sigma\rangle$. If $S_f = K[t;\sigma]/K[t;\sigma]f(t)$ is a division algebra (a *semifield*), then its invertible elements form a finite multiplicative loop.

There are less than $r\sqrt{log_2(r)}$ non-isotopic semifields S_f of order r (Kantor), so there are less than $r\sqrt{log_2(r)}$ non-isotopic loops of order $r-1$ which can be obtained as their multiplicative loops.

Let S_f be a proper semifield and $L_f = S_f \setminus \{0\}$ be its multiplicative loop. Then

$$|L_f| = q^{mn} - 1, \quad \text{Nuc}_l(L_f) = \text{Nuc}_m(L_f) = \mathbb{F}_{q^n}^{\times}$$

and $\text{Nuc}_r(L_f) \cong \mathbb{F}_{q^m}^{\times}$, $C(L_f) = \mathbb{F}_q^{\times}$.

Proposition Suppose $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in F[t] \subset K[t;\sigma]$ is irreducible and not invariant.
(i) $\text{Aut}(L_f)$ contains a cyclic subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z}$.
(ii) Suppose $a_{m-1} \in F^{\times}$. Then $\text{Aut}(K)$ is isomorphic to a subgroup of $\text{Aut}(L_f)$.
(iii) The powers of t form a multiplicative group of order m in L_f.

Proposition For every prime number m there is a loop L of order $q^{m^2}-1$ with center $\mathbb{F}_q^\times$, $\text{Nuc}_l(L) = \text{Nuc}_m(L) = \text{Nuc}_r(L) = \mathbb{F}_{q^m}^\times$ and a non-trivial automorphism group, which contains a cyclic subgroup of inner automorphisms of order $(q^m-1)/(q-1)$.

VII. Other applications.

• The algebras S_f can be defined using skew polynomial rings $D[t;\sigma,\delta]$, when D is not a division ring, if $f(t)$ has an invertible leading coefficient. We thus can construct new nonassociative unital algebras on subsets of quantum planes, Weyl algebras etc.

• Applications to (f, σ, δ)-codes; e.g. in coset coding, or to generalize the classical Construction A for lattices from linear codes, to canonically construct lattices from cyclic (f, σ, δ)-codes over finite rings.

• We can calculate the automorphism groups of certain Jha-Johnson semifields (P.-Brown, 2017).

• We can generalize other classical concepts originally introduced by Jacobson, Albert and Amitsur for central simple algebras in the 50s, and construct for instance nonassociative differential algebras (Results in Math. 2017).

• We can obtain results on solvable crossed product algebras (P.-Brown, 2017).