Nonassociative Algebras Obtained from Skew Polynomial Rings

Christian Brown

University of Nottingham

Christian.Brown@nottingham.ac.uk

13th June, 2017

Overview

Nonassociative Algebras

- Let F be a field. An **algebra** A is an F-vector space together with a bilinear map $A \times A \to A, (x, y) \mapsto xy$ which we call the **multiplication** of A. We assume that our algebras are **unital**, i.e. they contain a multiplicative identity 1.

Nonassociative Algebras

- Let F be a field. An **algebra** A is an F-vector space together with a bilinear map $A \times A \to A, (x, y) \mapsto xy$ which we call the **multiplication** of A. We assume that our algebras are **unital**, i.e. they contain a multiplicative identity 1.
- The **associator** of three elements of an algebra A is defined as $[x, y, z] = (xy)z - x(yz)$.

Nonassociative Algebras

- Let F be a field. An **algebra** A is an F-vector space together with a bilinear map $A \times A \to A, (x, y) \mapsto xy$ which we call the **multiplication** of A. We assume that our algebras are **unital**, i.e. they contain a multiplicative identity 1.
- The **associator** of three elements of an algebra A is defined as $[x, y, z] = (xy)z - x(yz)$.
- We define the **left nucleus, middle nucleus** and **right nucleus** as

$$\mathrm{Nuc}_l(A) = \{x \in A : [x, A, A] = 0\}$$

$$\mathrm{Nuc}_m(A) = \{x \in A : [A, x, A] = 0\}$$

$$\mathrm{Nuc}_r(A) = \{x \in A : [A, A, x] = 0\}$$

The **nucleus** of A is their intersection.

- We say an algebra $0 \neq A$ is **left division** (resp. **right division**) if left multiplication $L_a : x \mapsto ax$ (resp. right multiplication $R_a : x \mapsto xa$) are bijective for all $0 \neq a \in A$.

- We say an algebra $0 \neq A$ is **left division** (resp. **right division**) if left multiplication $L_a : x \mapsto ax$ (resp. right multiplication $R_a : x \mapsto xa$) are bijective for all $0 \neq a \in A$.
- A is a **division algebra** if it is both left and right division.

Skew Polynomial Rings (Ore, 1933)

Let D be an associative division ring, σ an endomorphism of D and let δ be a **left σ-derivation** of D. i.e., $\delta : D \to D$ is an additive map and satisfies

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

for all $a, b \in D$.

Skew Polynomial Rings (Ore, 1933)

Let D be an associative division ring, σ an endomorphism of D and let δ be a **left** σ**-derivation** of D. i.e., $\delta : D \to D$ is an additive map and satisfies

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

for all $a, b \in D$.

Definition

The **skew polynomial ring** $R = D[t; \sigma, \delta]$ is the set of left polynomials

$$a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n \ , \ a_i \in D$$

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

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

- $D[t;\sigma] = D[t;\sigma,0]$ is called a **twisted polynomial ring**

- $D[t;\sigma] = D[t;\sigma,0]$ is called a **twisted polynomial ring**
- $D[t;1,\delta] = D[t;\delta]$ is called a **differential polynomial ring**.

- $D[t;\sigma] = D[t;\sigma,0]$ is called a **twisted polynomial ring**
- $D[t;1,\delta] = D[t;\delta]$ is called a **differential polynomial ring**.
- $D[t;id,0]$ is the usual left polynomial ring.

- $D[t;\sigma] = D[t;\sigma,0]$ is called a **twisted polynomial ring**
- $D[t;1,\delta] = D[t;\delta]$ is called a **differential polynomial ring**.
- $D[t;id,0]$ is the usual left polynomial ring.
- We define the **degree** of a polynomial $f(t) = a_n t^n + \ldots + a_1 t + a_0$, $a_n \neq 0$ to be $\deg(f) = n$ and $\deg(0) = -\infty$.

- $D[t;\sigma] = D[t;\sigma,0]$ is called a **twisted polynomial ring**
- $D[t;1,\delta] = D[t;\delta]$ is called a **differential polynomial ring**.
- $D[t;id,0]$ is the usual left polynomial ring.
- We define the **degree** of a polynomial $f(t) = a_n t^n + \ldots + a_1 t + a_0$, $a_n \neq 0$ to be $\deg(f) = n$ and $\deg(0) = -\infty$.
- We say that a polynomial $f \in R = D[t;\sigma,\delta]$ is **irreducible** if it is not a unit and has no proper factors. i.e there do not exist $g(t), h(t) \in R$ with $\deg(g(t)), \deg(h(t)) < \deg(f(t))$ such that $f(t) = g(t)h(t)$.

- $D[t;\sigma] = D[t;\sigma, 0]$ is called a **twisted polynomial ring**
- $D[t;1,\delta] = D[t;\delta]$ is called a **differential polynomial ring**.
- $D[t;id,0]$ is the usual left polynomial ring.
- We define the **degree** of a polynomial $f(t) = a_n t^n + \ldots + a_1 t + a_0$, $a_n \neq 0$ to be $\deg(f) = n$ and $\deg(0) = -\infty$.
- We say that a polynomial $f \in R = D[t;\sigma,\delta]$ is **irreducible** if it is not a unit and has no proper factors. i.e there do not exist $g(t), h(t) \in R$ with $\deg(g(t)), \deg(h(t)) < \deg(f(t))$ such that $f(t) = g(t)h(t)$.
- R is a left principal ideal domain and there exists a right division algorithm in R: for all $f, g \in R$, $f \neq 0$ there exists unique $r, q \in R$, $\deg(r) < \deg(f)$ such that

$$g = qf + r.$$

How to construct nonassociative algebras using skew polynomial rings

Definition (Petit (1966))

Let $f(t) \in R = D[t;\sigma,\delta]$ be of degree m and let $\mathrm{mod}_r f$ denote the remainder of right division by $f(t)$.

$$R_m = \{g \in D[t;\sigma,\delta] \mid \deg(g) < m\}, \;\; g \circ h = gh \;\mathrm{mod}_r f$$

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

$$F = \{a \in D \mid ah = ha \text{ for all } h \in S_f\}.$$

S_f is also denoted R/Rf.

How to construct nonassociative algebras using skew polynomial rings

Definition (Petit (1966))

Let $f(t) \in R = D[t;\sigma,\delta]$ be of degree m and let $\mathrm{mod}_r f$ denote the remainder of right division by $f(t)$.

$$R_m = \{g \in D[t;\sigma,\delta] \mid \deg(g) < m\}, \;\; g \circ h = gh \,\mathrm{mod}_r f$$

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

$$F = \{a \in D \mid ah = ha \text{ for all } h \in S_f\}.$$

S_f is also denoted R/Rf.

Hamilton's quaternion algebra is the algebra S_f for $f(t) = t^2 + 1 \in \mathbb{C}[t;\sigma]$ where σ denotes complex conjugation.

Properties of the algebras S_f

Theorem (Petit (1966))

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

(i) *If S_f is not associative then*

$$Nuc_l(S_f) = Nuc_m(S_f) = D$$

and

$$Nuc_r(S_f) = \{u \in R_m : fu \in Rf\}.$$

(ii) *S_f is associative iff $f(t)$ is right invariant iff Rf is a two-sided ideal of R.*

Properties of the algebras S_f

Theorem (Petit (1966))

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

(i) *If S_f is not associative then*

$$Nuc_l(S_f) = Nuc_m(S_f) = D$$

and

$$Nuc_r(S_f) = \{u \in R_m : fu \in Rf\}.$$

(ii) *S_f is associative iff $f(t)$ is right invariant iff Rf is a two-sided ideal of R.*

- If Rf is a two-sided ideal then $S_f = {}^{R}\!/_{Rf}$ is the classical quotient ring.

Properties of the algebras S_f

Theorem (Petit (1966))

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

(i) *If S_f is not associative then*

$$Nuc_l(S_f) = Nuc_m(S_f) = D$$

and

$$Nuc_r(S_f) = \{u \in R_m : fu \in Rf\}.$$

(ii) *S_f is associative iff $f(t)$ is right invariant iff Rf is a two-sided ideal of R.*

- If Rf is a two-sided ideal then $S_f = {}^{R}\!/_{Rf}$ is the classical quotient ring.
- If Rf is not two-sided then S_f is central. That is, $\text{Cent}(S_f) = \text{Comm}(S_f) \cap \text{Nuc}(S_f) = F_0$.

Theorem

Let $f(t) \in D[t;\sigma,\delta]$.

(i) $f(t)$ *is irreducible iff* S_f *is a right division algebra.*

Theorem

Let $f(t) \in D[t;\sigma,\delta]$.

(i) $f(t)$ *is irreducible iff* S_f *is a right division algebra.*

(ii) *(Petit, 1966). Suppose* S_f *is a finite-dimensional* F_0*-vector space or a finite-dimensional right* $Nuc_r(S_f)$*-module. Then* S_f *is division iff* $f(t)$ *is irreducible.*

Theorem

Let $f(t) \in D[t;\sigma,\delta]$.

(i) $f(t)$ *is irreducible iff* S_f *is a right division algebra.*

(ii) *(Petit, 1966). Suppose* S_f *is a finite-dimensional* F_0*-vector space or a finite-dimensional right* $Nuc_r(S_f)$*-module. Then* S_f *is division iff* $f(t)$ *is irreducible.*

(iii) *Suppose* S_f *is associative. Then* $f(t)$ *is irreducible iff* S_f *is a division algebra.*

Let F be a field and A be a central simple algebra over F of degree n. A is called a G-**crossed product algebra** if it contains a field extension M/F which is Galois of degree n with Galois group $G = \mathrm{Gal}(M/F)$.

Let F be a field and A be a central simple algebra over F of degree n. A is called a G-**crossed product algebra** if it contains a field extension M/F which is Galois of degree n with Galois group $G = \mathrm{Gal}(M/F)$.

Suppose G is a finite solvable group, then there exists a chain of subgroups

$$\{1\} = G_0 < G_1 < \ldots < G_k = G,$$

such that G_j is normal in G_{j+1} and G_{j+1}/G_j is cyclic of prime order q_j for all $j \in \{0, \ldots, k-1\}$.

Theorem (Petit (1966), B.-Pumplün (2017))

Let M/F *be a field extension of degree* n *with non-trivial* $G = \mathrm{Aut}_F(M)$*, and* A *be a central simple algebra of degree* n *over* F *containing* M*. Then* G *is solvable if there exists a chain of subalgebras*

$$M = A_0 \subset A_1 \subset \ldots \subset A_k \subseteq A,$$

of A *which all have maximal subfield* M*, where* A_k *is a* G*-crossed product algebra over* $\mathrm{Fix}(G)$*, and where*

$$A_{i+1} \cong A_i[t_i;\tau_i]/A_i[t_i;\tau_i](t_i^{q_i} - c_i),$$

for all $i \in \{0, \ldots, k-1\}$*, such that*

- q_i *is the prime order of the factor group* G_{i+1}/G_i *in the chain of normal subgroups,*
- τ_i *is an* F*-automorphism of* A_i *of inner order* q_i *which restricts to* $\sigma_{i+1} \in G_{i+1}$ *which generates* G_{i+1}/G_i*, and*
- $c_i \in \mathrm{Fix}(\tau_i)$ *is invertible.*

If A is a crossed product algebra then $A_k = A$.

Theorem (B.-Pumplün (2017))

Let A be a central division algebra of degree n over F with maximal subfield M and non-trivial $\sigma \in \mathrm{Aut}_F(M)$ of order h. Then A contains a cyclic division algebra

$$(M/\mathrm{Fix}(\sigma), \sigma, c) \cong M[t;\sigma]/M[t;\sigma](t^h - c)$$

of degree h over $\mathrm{Fix}(\sigma)$ as a subalgebra.

It is well known that a central division algebra of prime degree over F is a cyclic algebra iff it contains a cyclic subalgebra of prime degree (though not necessarily with center F). This yields the following:

Corollary

Let A be a central division algebra over F of prime degree p. Then either A is a cyclic algebra or each of its maximal subfields M has trivial automorphism group $\mathrm{Aut}_F(M)$.

The End