Article:

Manoharmayum, J. (2020) A note on the structure of complete alternative local algebras. Communications in Algebra, 48 (12). pp. 5511-5516. ISSN 0092-7872

https://doi.org/10.1080/00927872.2020.1791150

A NOTE ON THE STRUCTURE OF COMPLETE ALTERNATIVE LOCAL ALGEBRAS

JAYANTA MANOHARMAYUM

Abstract. Let $(A, \mathfrak{m})$ be an alternative algebra with maximal ideal $\mathfrak{m}$ which is complete and separated for the $\mathfrak{m}$-adic topology. Assuming that $A/\mathfrak{m} := \boldsymbol{k}$ is a perfect field of positive characteristic and that the associated graded algebra is a $\boldsymbol{k}$-algebra, we show that the reduction map $W(\boldsymbol{k}) \to \boldsymbol{k}$ from the Witt ring $W(\boldsymbol{k})$ lifts canonically to a morphism $W(\boldsymbol{k}) \to A$ thereby giving A the structure of a unital $W(\boldsymbol{k})$-algebra.

1. Introduction

The structure theorem for commutative complete local rings (see Theorem 29.2 of [3]) tells us that any such ring with perfect residue field is naturally an algebra over the Witt ring of its residue field. In this note, we establish an analogous result for complete local alternative algebras: we show, under natural conditions, our alternative algebras are unital and have a natural structure of an algebra over the corresponding Witt rings.

We now outline an introduction to our objects of interest; for further details, see [2], [4], [5], [9]. As we are going to be dealing with potentially non-unital multiplicative structures, we shall use the term algebra to mean a $\mathbb{Z}$-algebra; by contrast, rings are always assumed to be unital. Ideals, unless indicated otherwise, are always assumed to be two sided.

Recall that an algebra A is an *alternative algebra* if multiplication in A satisfies

$$x^2y = x(xy) \text{ and } xy^2 = (xy)y$$

for all $x, y \in A$. Equivalently, the algebra A is alternative if and only if the associativity condition $(xy)z = x(yz)$ holds whenever $\{x, y, z\} \subseteq A$ has cardinality at most 2. Alternative algebras, in a sense, are not too far off being associative: by a theorem of Artin, an alternative algebra is an algebra in which any two elements generate an associative subalgebra. In fact, in an alternative algebra, any three elements that associate with each other generate an associative subalgebra. (See [8], Theorem 1.)

Products of ideals in an alternative algebra can be formed just as in the associative setting: if I and J are ideals in the alternative algebra A, then the additive subgroup IJ consisting of all finite sums $\sum xy$ with $x \in I, y \in J$ is in fact an ideal of A. By the *full n-th power* I^n of the ideal I, we mean the ideal generated by all possible products of n arbitrary elements of I. The full n-th power I^n is in fact the $\mathbb{Z}$-submodule of R generated by all possible products of n arbitrary elements of I, and we have the recurrence

$$I^n = II^{n-1} + \cdots + I^{n-1}I \quad \text{for } n \geq 2.$$

2010 *Mathematics Subject Classification.* Primary: 17D05; Secondary: 17A60, 17A75.

By a *complete alternative local algebra* $(A, \mathfrak{m})$, we mean an alternative algebra A together a maximal ideal $\mathfrak{m}$ such that A is complete and separated under the $\mathfrak{m}$-adic topology i.e. the topology with a base of open neighbourhoods of 0 given by the filtration of full powers $\mathfrak{m} \supseteq \mathfrak{m}^2 \supset \ldots$. The natural map

$$A \to \varprojlim A/\mathfrak{m}^n$$

is then an isomorphism of topological algebras (with each factor in the product having the discrete topology). The same filtration also allows us to construct the *associated graded algebra*

$$\mathrm{gr}(A) \;:=\; \frac{A}{\mathfrak{m}} \oplus \frac{\mathfrak{m}}{\mathfrak{m}^2} \oplus \frac{\mathfrak{m}^2}{\mathfrak{m}^3} \oplus \ldots.$$

While the associated graded algebra $\mathrm{gr}(A)$ is always an alternative algebra, there is no reason to expect $\mathrm{gr}(A)$ to acquire additional $A/\mathfrak{m}$-algebra structure when the residue $A/\mathfrak{m}$ is a field (so commutative and associative). But if it does, then we have the following consequence for the original alternative algebra; and, this forms the main result of our note.

Theorem 1.1. *Let $(A, \mathfrak{m})$ be a complete alternative local algebra. Assume that the residue algebra $A/\mathfrak{m} := \boldsymbol{k}$ is a perfect field of positive characteristic, and that $gr(A)$ is a $\boldsymbol{k}$-algebra. Then A is unital. Furthermore, the reduction map $W(\boldsymbol{k}) \to \boldsymbol{k}$ from the Witt ring $W(\boldsymbol{k})$ lifts canonically to a ring homomorphism $W(\boldsymbol{k}) \to A$ thereby giving A the structure of a unital $W(\boldsymbol{k})$-algebra.*

Our motivation for the above result is from Number Theory, particularly in relation to completions of orders in Cayley's octonions[1], and also construction of central elements in completed group algebras. Note that if A is an alternative ring (i.e. unital alternative algebra) and $B \subseteq A$ is a commutative associative subring, then A is a B-algebra precisely when B is in the centre of A. (See Section 2.1 for the definition of the centre of an alternative algebra.) Thus Theorem 1.1 shows that a complete local algebra has enough elements in its centre provided its associated graded ring has an algebra structure over a field. Also, while we do not state this explicitly, it is clear that the hypothesis is necessary for the conclusions of Theorem 1.1 to hold. As in the case of commutative local rings, we show that we can construct 'Teichmüller lifts' of the residue field and then verify that these are central elements in the alternative algebra. (For the commutative case, see §5 and §6 of Chapter II in [6].)

2. A structural characteristic of complete alternative local rings: proof of Theorem 1.1

2.1. **Generalities.** We begin by recalling some definitions. Let A be an algebra. We write $(x, y, z) := (xy)z - x(yz)$ for the *associator* of $x, y, z \in A$, and write $[x, y] := xy - yx$ for the *commutator* of $x, y \in A$. An element $x \in A$ is *central* if it commutes and associates with all other elements of A i.e.

$$[x, y] = (x, y, z) = (y, x, z) = (y, z, x) = 0$$

for all $y, z \in A$. The set of all central elements of A is the *centre* $Z(A)$ of A; it is a sub-algebra of A.

[1] Although John Graves had discovered them earlier; see the introduction in [1].

We will need to use the following two properties of the associator on an alternative algebra. So let A be an alternative algebra. Firstly, the associator is an alternating form on A, and therefore the identities

$$(x, y, z) = (y, z, x) = (z, x, y) = -(y, x, z) = -(z, y, x) = -(x, z, y) \tag{2.1}$$

hold for all $x, y, z \in A$. Secondly, we can factor out terms from associators: if $x, y, z \in A$, then

$$(x, yx, z) = x(x, y, z) \quad \text{and} \quad (x, xy, z) = (x, y, z)x. \tag{2.2}$$

(See Chapter 2 Section 3 of [9]; Section 1 of [10]; or, Section 2 of [7].)

The following running assumption will now be in place for the remainder of this note.

Assumption 2.1. *From here on:*

- $\boldsymbol{k}$ *is a perfect field of characteristic* $p > 0$*;*
- $(A, \mathfrak{m})$ *is a complete alternative ring with residue field* $A/\mathfrak{m} := \boldsymbol{k}$*, and the associated graded ring* $gr(A)$ *is a* $\boldsymbol{k}$*-algebra.*

We record some consequences of Assumption 2.1. Firstly, the $\boldsymbol{k}$-algebra structure on $\mathrm{gr}(A)$ implies the following statements hold in A.

(A1) If $x \in \mathfrak{m}^n$ then $px \in \mathfrak{m}^{n+1}$.
(A2) If $x \in A$ and $y \in \mathfrak{m}^n$, then the commutator $[x, y] \in \mathfrak{m}^{n+1}$.
(A3) If $x, y \in A$ and $z \in \mathfrak{m}^n$, then the associator $(x, y, z) \in \mathfrak{m}^{n+1}$.

The next consequence comes from the topology on A. For $y, z \in A$, the sets $\{ x \in A \mid [x, y] = 0\}$ and $\{ x \in A \mid (x, y, z) = 0\}$ are closed in A (since multiplication is continuous and $\{0\}$ is closed in A); taking the intersection of these sets, we obtain the following consequence for the centre.

(A4) The centre $Z(A)$ is a topologically closed subalgebra of A.

2.2. **Multiplicative system of representatives and proof of Theorem 1.1.** Let $(A, \mathfrak{m})$ be a complete local alternative algebra as in Assumption 2.1. We say that a subset $X \subseteq A$ is *a multiplicative system of representatives* if it is multiplicatively closed and the reduction map $X \to A/\mathfrak{m}$ is a bijection compatible with multiplication.

The following proposition guarantees the existence of a system of representatives.

Proposition 2.2. *Let* $(A, \mathfrak{m})$ *be as in Assumption 2.1. Then:*

(i) A has a unique multiplicative system of representatives X*.*
(ii) The elements in X *are central elements of* A*.*

We shall now deduce Theorem 1.1 from the above proposition, and leave the proof of Proposition 2.2 to the next section. Before moving on to the deduction, we recall that the Witt ring $W(\boldsymbol{k})$ is an initial object in the category of commutative complete local rings with residue field $\boldsymbol{k}$. If $\boldsymbol{k}$ is a finite field of cardinality q then $W(\boldsymbol{k})$ can be identified with the p-adic completion of the ring $\mathbb{Z}[\zeta]$ where ζ is a primitive $(q-1)$-th root of unity; and, the multiplicative system of representatives is given by $\{0, \zeta, \ldots, \zeta^{q-1}\}$.

Proof of Theorem 1.1 assuming Proposition 2.2. Let $e \in X$ be the representative for $1 \in \boldsymbol{k}$. We will show that e is the multiplicative identity of A. Now e is an idempotent: as $e^2 \in X$ and $e^2 \pmod{\mathfrak{m}} = 1$, we have $e^2 = e$. Also, left multiplication by e is an injective map (because $x \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}$ implies $ex \notin \mathfrak{m}^{n+1}$ from the $\boldsymbol{k}$-algebra structure on $\mathrm{gr}(A)$). Now, if $x \in A$ then

$$e(ex - x) = e(ex) - ex = (e^2)x - ex = 0,$$

and we obtain $ex = x$. Similarly $xe = x$, and A is unital.

Finally, using (A4), we see that $Z(A)$ is a commutative associative complete local ring with maximal ideal $Z(A) \cap \mathfrak{m}$ and residue field $\boldsymbol{k}$. The section map $\boldsymbol{k} \to X$ therefore induces a canonical morphism $W(\boldsymbol{k}) \to Z(A) \subseteq A$ of local rings, and this completes the proof of Theorem 1.1. □

2.3. **Proof of Proposition 2.2.** As in the commutative associative case, we construct the multiplicative system of representatives by taking limits of compatible p-powers of elements in the residue field. In our setting, the role of commutativity and associativity will be replaced by the weaker conditions (A2), (A3), and completeness; and, the following lemma will allow us to carry this out.

Lemma 2.3. *With $(A, \mathfrak{m})$ as in Assumption 2.1, let $x, y \in A$ and let k be a positive integer. Then the following statements hold.*

(i) If $y \in \mathfrak{m}^k$ then $(x+y)^p \equiv x^p + y^p \pmod{\mathfrak{m}^{k+1}}$.
(ii) If $[x, y] \in \mathfrak{m}^k$ then $[x, y^p] \in \mathfrak{m}^{k+1}$.
(iii) If $x \equiv y \pmod{\mathfrak{m}^k}$ then $x^p \equiv y^p \pmod{\mathfrak{m}^{k+1}}$.
(iv) $(xy)^{p^k} \equiv x^{p^k} y^{p^k} \pmod{\mathfrak{m}^k}$.

Proof. Note that, in what follows, all algebraic manipulations work inside the associative subalgebra of A generated by x and y.

If $y \in \mathfrak{m}^k$ then the usual binomial expansion holds modulo $\mathfrak{m}^{k+1}$ by (A2) i.e.

$$(x+y)^n \equiv x^n + nx^{n-1}y + \cdots + nxy^{n-1} + y^n \pmod{\mathfrak{m}^{k+1}}.$$

Part (i) of the lemma follows since $\boldsymbol{k}$ has characteristic p. Part (iii) is similar: start with $x = y + m$ where $m \in \mathfrak{m}^k$, and then expand out $(y+m)^p$.

For part (ii), write $xy = yx + m$ with $m \in \mathfrak{m}^k$. A straightforward induction then shows

$$xy^n \equiv y^n x + nmy^{n-1} \pmod{\mathfrak{m}^{k+1}}$$

holds for all $n \in \mathbb{N}$, and (ii) follows.

We use induction for part (iv) as well. If $(xy)^{p^n} \equiv x^{p^n} y^{p^n} \pmod{\mathfrak{m}^n}$ then

$$(xy)^{p^{n+1}} \equiv \left(x^{p^n} y^{p^n}\right)^p \pmod{\mathfrak{m}^{n+1}}$$

by part (iii). Part (iv) now follows since $x^{p^n} y^{p^n} \equiv y^{p^n} x^{p^n} \pmod{\mathfrak{m}^n}$ by (ii). □

As we will see when we turn to the proof of Proposition 2.2, the preceding lemma will give elements in the commutative centre of A. If the characteristic p is different from 3, then the commutative centre is inside the centre $Z(A)$ (see Chapter 7 Corollary 1 of [9]) and no further work is needed. To cover all characteristics, we will need the following lemma.

Lemma 2.4. *With $(A, \mathfrak{m})$ as in Assumption 2.1, let $k \geq 0$ be an integer and let $x, y, z \in R$. If both (x, y, z) and $[x, y]$ are in $\mathfrak{m}^k$, then $(x^p, y, z) \in \mathfrak{m}^{k+1}$.*

Proof. We prove by induction that if n is a positive integer, then

$$(x, y, z), [x, y] \in \mathfrak{m}^k \implies (x^n, y, z) \equiv nx^{n-1}(x, y, z) \pmod{\mathfrak{m}^{k+1}}$$

for all $x, y, z \in A$.

The case $n = 1$ is trivially true. For the inductive step, first note that

$$(x^{n+1}, y, z) = (x^n, xy, z) + x^n(x, y, z). \tag{2.3}$$

Now, using (2.2), we see that

$$(x, xy, z) = (x, [x, y], z) + (x, yx, z) = (x, [x, y], z) + x(x, y, z)$$

and $[x, xy] = x^2y - xyx = x[x, y]$. Thus both $(x, xy, z), [x, xy] \in \mathfrak{m}^k$. Furthermore, since $(x, [x, y], z) \in \mathfrak{m}^{k+1}$ by (A3), we have $(x, xy, z) \equiv x(x, y, z) \pmod{\mathfrak{m}^{k+1}}$. So assuming the claim for n, we obtain

$$(x^n, xy, z) \equiv nx^{n-1}(x, xy, z) \equiv nx^n(x, y, z) \pmod{\mathfrak{m}^{k+1}},$$

and the assertion follows from (2.3). $\square$

Proof of Proposition 2.2. Let $a \in \boldsymbol{k}$. For each positive integer n, choose an element $a_n \in A$ such that

$$a_n \pmod{\mathfrak{m}} = a^{p^{-n}}.$$

We call $({a_n}^{p^n})$ a sequence of p-power roots of a. Since $a_{n+1}^p \equiv a_n \pmod{\mathfrak{m}}$, Lemma 2.3(iii) implies that

$${a_{n+1}}^{p^{n+1}} \equiv {a_n}^{p^n} \pmod{\mathfrak{m}^{n+1}}.$$

The sequence $({a_n}^{p^n})$ therefore converges in A. The limit is independent of the choice of lifts: if $({a'_n}^{p^n})$ was another sequence of p-power roots of a then, for the same reason,

$${a_n}^{p^n} \equiv {a'_n}^{p^n} \pmod{\mathfrak{m}^{n+1}}.$$

We call this limit the *Teichmüller lift* of a and denote it by $\omega(a)$; thus

$$\omega(a) := \lim_{n\to\infty} {a_n}^{p^n}.$$

Note that if X is a multiplicative system of representatives and $x \in X$ reduces to a modulo $\mathfrak{m}$, then the constant sequence $x, x, \dots$ is a sequence of p-power roots of a and so $x = \omega(a)$. Hence a multiplicative system of representatives, if it exists, is unique and consists of Teichmüller lifts.

To show that Teichmüller lifts are central, consider a sequence $({a_n}^{p^n})$ of p-power roots of a, and let $x, y \in A$. Now, both $[a_n, x]$ and (a_n, x, y) are in the maximal ideal $\mathfrak{m}$. Using Lemma 2.3(ii) and Lemma 2.4, we conclude that

$$[{a_n}^{p^n}, x] \in \mathfrak{m}^{n+1} \quad \text{and} \quad (a_n^{p^n}, x, y) \in \mathfrak{m}^{n+1}.$$

Hence $[\omega(a), x] = (\omega(a), x, y) = 0$, and therefore the Teichmüller lift $\omega(a) \in Z(A)$.

We will now verify that the set of Teichmüller lifts is a multiplicative system of representatives: i.e. *if* $a, b \in \boldsymbol{k}$ *then* $\omega(ab) = \omega(a)\omega(b)$. To see this, let $({a_n}^{p^n})$ and $({b_n}^{p^n})$ be sequences of p-power roots of a and b respectively, and let $c_n := a_nb_n$. Then

$${c_n}^{p^n} = (a_nb_n)^{p^n} \equiv {a_n}^{p^n}{b_n}^{p^n} \pmod{\mathfrak{m}^n}$$

by Lemma 2.3(iv), and so $({c_n}^{p^n})$ is a sequences of p-power roots of ab. Hence $\omega(ab) = \omega(a)\omega(b)$, and we have completed the proofs of parts (i) and (ii). $\square$

Remark 2.5. We could have set our discussion in the context of filtrations on alternative algebras. More precisely, let R be an alternative algebra together with a separated and complete filtration $R =: I_0 \supseteq I_1 \supseteq I_2 \supseteq \dots$ of ideals (that is, the ideals I_n have trivial intersection and the natural map $R \to \varprojlim R/I_n$ is an isomorphism), satisfying the following conditions:

- $R/I_1; = \boldsymbol{k}$ is a perfect field of positive characteristic;
- $I_m I_n \subseteq I_{m+n}$ for $m, n \geq 0$, and the associated graded algebra is a $\boldsymbol{k}$-algebra.

The conclusions of Proposition 2.2 and Theorem 1.1 then hold for R. (The proof involves simply replacing each ideal $\mathfrak{m}^n$ by $I(n)$ in the preceding arguments.)

References

[1] J. C. Baez. *The octonions.* Bull. Amer. Math. Soc. (N.S.) Vol 39 (2002), No. 2, pages 145–205
[2] Y. A. Bakhturin, A. M. Slin'ko, and I. P. Shestakov. *Nonassociative rings.* J. Math. Sci. 18 (1982), pages 169–211.
(Translated from Itogi Naukii Tekhniki, Seriya Algebra, Topologiya, Geometriya, Vol. 18, pp. 3-72, 1981.)
[3] H. Matsumura. *Commutative ring theory.* Cambridge Studies in Advanced Mathematics, 8. Cambridge University Press, Cambridge, 1989.
[4] K. McCrimmon. *A taste of Jordan algebras.* Universitext. Springer-Verlag, New York, 2004.
[5] R. D. Schafer. *An introduction to non-associative algebras.* Pure and Applied Mathematics, Vol. 22 Academic Press, New York-London, 1966.
[6] J.-P. Serre. *Local Fields.* Graduate Text in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.
[7] M. Slater. *Nucleus and center in alternative rings.* J. Algebra 7 (1967), 372–388.
[8] M. F. Smiley. *The radical of an alternative ring.* Ann. of Math. (2), Vol. 49, No. 3 (1948), pp. 702-709
[9] K. A. Zhevlakov, A. M. Slin'ko, I. P. Shestakov, and A. I. Shirshov. *Rings that are nearly associative.* Pure and Applied Mathematics, 104. Academic Press, New York-London, 1982.
[10] M. Zorn. *Alternative rings and related questions I: existence of the radical.* Ann. of Math. (2), Vol 42, No. 3 (1941), pages 676–686.

School of Mathematics and Statistics, University of Sheffield, Sheffield S3 7RH, U.K.

Email address: J.Manoharmayum@sheffield.ac.uk