Mathematisches
Forschungsinstitut
Oberwolfach

Member of the Leibniz Association

Oberwolfach Preprints

OWP 2020 - 21

ADAM CHAPMAN

Octonion Polynomials with Values in a Subalgebra

Mathematisches Forschungsinstitut Oberwolfach gGmbH
Oberwolfach Preprints (OWP) ISSN 1864-7596

Oberwolfach Preprints (OWP)

The MFO publishes a preprint series **Oberwolfach Preprints (OWP)**, ISSN 1864-7596, which mainly contains research results related to a longer stay in Oberwolfach, as a documentation of the research work done at the MFO. In particular, this concerns the Research in Pairs-Programme (RiP) and the Oberwolfach-Leibniz-Fellows (OWLF), but this can also include an Oberwolfach Lecture, for example.

A preprint can have a size from 1 - 200 pages, and the MFO will publish it on its website as well as by hard copy. Every RiP group or Oberwolfach-Leibniz-Fellow may receive on request 20 free hard copies (DIN A4, black and white copy) by surface mail.

The full copyright is left to the authors. With the submission of a manuscript, the authors warrant that they are the creators of the work, including all graphics. The authors grant the MFO a perpetual, irrevocable, non-exclusive right to publish it on the MFO's institutional repository.

In case of interest, please send a **pdf file** of your preprint by email to *rip@mfo.de* or *owlf@mfo.de*, respectively. The file should be sent to the MFO within 12 months after your stay as RiP or OWLF at the MFO.

There are no requirements for the format of the preprint, except that the introduction should contain a short appreciation and that the paper size (respectively format) should be DIN A4, "letter" or "article".

On the front page of the hard copies, which contains the logo of the MFO, title and authors, we shall add a running number (20XX – XX). Additionally, each preprint will get a Digital Object Identifier (DOI).

We cordially invite the researchers within the RiP or OWLF programme to make use of this offer and would like to thank you in advance for your cooperation.

Imprint:

Mathematisches Forschungsinstitut Oberwolfach gGmbH (MFO)
Schwarzwaldstrasse 9-11
77709 Oberwolfach-Walke
Germany

Tel	+49 7834 979 50
Fax	+49 7834 979 55
Email	admin@mfo.de
URL	www.mfo.de

The Oberwolfach Preprints (OWP, ISSN 1864-7596) are published by the MFO.

DOI	10.14760/OWP-2020-21

Octonion Polynomials with Values in a Subalgebra

Adam Chapman

Department of Computer Science, Academic College of Tel-Aviv-Yaffo, Rabenu Yeruham St., P.O.B 8401 Yaffo, 6818211, Israel

Abstract

In this paper, we prove that given an octonion algebra A over a field F, a subring $E \subseteq F$ and an octonion E-algebra R inside A, the set S of polynomials $f(x) \in A[x]$ satisfying $f(R) \subseteq R$ is an octonion $(S \cap F[x])$-algebra, under the assumption that either $\frac{1}{2} \in R$ or $\mathrm{char}(F) \neq 0$, and R contains the standard generators of A and their inverses. The project was inspired by a question raised by Werner on whether integer-valued octonion polynomials over the reals form a nonassociative ring. We also prove that the polynomials $\frac{1}{p}(x^{p^2} - x)(x^p - x)$ for prime p are integer-valued in the ring of polynomials $A[x]$ over any real nonsplit Cayley-Dickson algebra A.

Keywords: Alternative Algebras, Octonion Algebras, Ring of Polynomials, Integer-Valued Polynomials, Cayley-Dickson Algebras
2010 MSC: primary 17A75; secondary 17A45, 17A35, 17D05

1. Introduction

Integer-valued polynomials have been the subject of research for a long time. Polya studied polynomials $f(x)$ in $\mathbb{Q}[x]$ satisfying $f(\mathbb{Z}) \subseteq \mathbb{Z}$ and provided a generating set for their ring ([4]).

In [7], Werner addressed the situation of polynomials $f(x) \in \mathbb{H}[x]$ satisfying $f(R) \subseteq R$ where R is a subring of $\mathbb{H}$ containing $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}ij$, and proved that they form a subring of $\mathbb{H}[x]$. In [8], Werner raised the question of whether the set of polynomials $f(x) \in \mathbb{O}[x]$ satisfying $f(R) \subseteq R$ where $R = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}(ij) \oplus \mathbb{Z}\ell \oplus \mathbb{Z}i\ell \oplus \mathbb{Z}j\ell \oplus \mathbb{Z}(ij)\ell$ is closed under multiplication.

We rephrase Werner's question in a more general setting, with a more specified structure: given a field F, a subring E, an octonion F-algebra A, and an octonion E-algebra R inside A, write $\mathrm{Sub}_R(A[x])$ for the set of polynomials $f(x) \in A[x]$

Email address: adam1chapman@yahoo.com (Adam Chapman)

satisfying $f(R) \subseteq R$. Is $\mathrm{Sub}_R(A[x])$ an octonion algebra over $\mathrm{Sub}_R(A[x]) \cap F[x]$? We answer this question affirmatively, under the assumption that either $\frac{1}{2} \in R$ or $\mathrm{char}(F) \neq 0$, and R contains the standard generators of A and their inverses. We also prove that for any prime integer p, the polynomial $\frac{1}{p}(x^{p^2} - x)(x^p - x)$ is in $\mathrm{Sub}_R(\mathbb{O}[x])$ where R is the octonion $\mathbb{Z}$-algebra inside $\mathbb{O}$ generated by the standard generators i, j, ℓ of $\mathbb{O}$. This is in fact proven in a more general setting that addresses the entire family of real nonsplit Cayley-Dickson algebras.

2. Preliminaries

Given a field F of $\mathrm{char}(F) \neq 2$, an octonion algebra A over F is an algebra admitting the structure $A = Q \oplus Q\ell$ where Q is a quaternion F-algebra, and

$$(q + r\ell)(s + t\ell) = qs + \bar{t}r\gamma + (r\bar{s} + tq)\ell$$

for any $q, r, s, t \in Q$ and a fixed $\gamma \in F^\times$ and $\bar{z} \mapsto z$ is the canonical (symplectic) involution on Q. The quaternion algebra Q in turn is of the form

$$Q = F\langle i, j : i^2 = \alpha, j^2 = \beta, ij + ji = 0\rangle,$$

for some $\alpha, \beta \in F^\times$. The canonical involution on Q maps $a + bi + cj + dij$ to $a - bi - cj - dij$. This involution extends to A by $\overline{r + s\ell} = \bar{r} - s\ell$. The trace map $\mathrm{Tr} : A \to F$ mapping z to $z + \bar{z}$ is linear, and the norm map $\mathrm{Norm} : A \to F$ mapping z to $z \cdot \bar{z}$ is quadratic. Each $z \in A$ then satisfies $z^2 - \mathrm{Tr}(z)z + \mathrm{Norm}(z) = 0$. The algebra A is a composition algebra, which means that the norm map is multiplicative, i.e., $\mathrm{Norm}(z_1 z_2) = \mathrm{Norm}(z_1) \cdot \mathrm{Norm}(z_2)$. The algebra A is a division algebra if and only if its norm map is anisotropic, i.e., for each nonzero element $z \in A$, $\mathrm{Norm}(z) \neq 0$.

The ring of (central) polynomials $A[x]$ is defined to be $A \otimes_F F[x]$, which means that the indeterminate x is in the center. Despite this fact, a polynomial $f(x) = c_n x^n + \cdots + c_1 x + c_0 \in A[x]$ decomposes as $f(x) = g(x)(x - \lambda)$ if and if $c_n \lambda^n + \cdots + c_1 \lambda + c_0 = 0$, and thus we define the substitution map $S_\lambda : A[x] \to A$ by $c_n x^n + \cdots + c_1 x + c_0 \mapsto c_n \lambda^n + \cdots + c_1 \lambda + c_0$. This is why these polynomials are often called "left polynomials". The canonical involution extends from A to $A[x]$ by setting $\bar{x} = x$, and thus $A[x]$ is an octonion $F[x]$-algebra.

The notion of octonion algebras extends to algebras over rings ([3, Section 4]): a non-associative algebra A over a commutative ring R is an octonion algebra if it is finitely generated projective of rank 8 as an R-module, contains an identity element and admits a norm, i.e., a quadratic form $\mathrm{Norm} : A \to R$ uniquely determined by the following two conditions:

(i) Norm is non-singular, so its induced symmetric bilinear form $B(x, y) = \mathrm{Norm}(x + y) - \mathrm{Norm}(x) - \mathrm{Norm}(y)$ defines a linear isomorphism from the R-module A onto its dual A^* by the assignment $x \mapsto B(x, —)$.

(ii) Norm permits composition, i.e., $\mathrm{Norm}(xy) = \mathrm{Norm}(x) \cdot \mathrm{Norm}(y)$.

For further reading on octonion algebras over fields and rings see also [9], [2], [6].

3. General Fields and fields of characteristic not 2

Lemma 3.1. *Let F be a field, E a subring of F, A an octonion F-algebra and R an octonion E-algebra inside A. Let $f(x) \in \mathrm{Sub}_R(A[x])$ and let u be a unit in R of* $\mathrm{Tr}(u) = 0$*. Then the polynomial $h(x) = f(x) \cdot u$ satisfies $h(\lambda) = f(u\lambda u^{-1})u$ for any $\lambda \in A$, and thus $h \in \mathrm{Sub}_R(A[x])$ as well.*

Proof. Write $f(x) = \sum_{k=0}^{n} a_n x^n$. Then $h(x) = \sum_{k=0}^{n} a_n u x^n$. Let $\lambda \in A$. Since $\mathrm{Tr}(u) = 0$, we have $u^2 \in F^\times$, and thus the Moufang identity gives $((au)b)u^{-1} = a(ubu^{-1})$ for any $a, b \in A$. So $h(\lambda)u^{-1} = (\sum_{k=0}^{n}(a_n u)\lambda^n)u^{-1} = \sum_{k=0}^{n} a_n(u\lambda^n u^{-1}) = \sum_{k=0}^{n} a_n(u\lambda u^{-1})^n = f(u\lambda u^{-1})$. Therefore, if $\lambda \in R$, then since u and u^{-1} are in R and given that $f(R) \subseteq R$, we get $h(R) \subseteq R$. □

Corollary 3.2. *As an immediate result of Lemma 3.1 we conclude that if we assume in addition that R contains the standard generators of A and their inverses, then* $\mathrm{Sub}_R(A[x])$ *is a right R-module.*

Proposition 3.3. *Let F be a field of* $\mathrm{char}(F) \neq 2$*, E a subring of F, A an octonion F-algebra and R an octonion E-algebra inside A containing the standard generators i, j, ℓ of A, their inverses, and $\frac{1}{2}$. Then every polynomial $f(x) \in \mathrm{Sub}_R(A[x])$ decomposes as $f(x) = f_0(x)+f_1(x)i+f_2(x)j+f_3(x)ij+f_4(x)\ell+f_5(x)(i\ell)+f_6(x)(j\ell)+f_7((ij)\ell)$ where $f_0(x), \dots, f_7(x)$ are polynomials in* $\mathrm{Sub}_R(A[x]) \cap F[x]$*.*

Proof. The decomposition is obvious. It is left to explain why $f_m(x)(R) \subseteq R$ for $m = 0, \dots, 7$. By Lemma 3.1, $g(x) = ((f(x)i)j)(ij)^{-1}$ satisfies $g(R) \subseteq R$, and so does $h(x) = \frac{1}{2}(g(x) + f(x))$, which is equal to $f_0(x) + f_1(x)i + f_2(x)j + f_3(x)(ij)$. Now, $\varphi(x) = \frac{1}{2}(h(x) + ((h(x)i)\ell)(i\ell)^{-1}) = f_0(x) + f_1(x)i$ satisfies $\varphi(R) \subseteq R$ too. Finally $\frac{1}{2}(\varphi(x) + ((\varphi(x)j)\ell)(j\ell)^{-1}) = f_0(x)$ satisfies $f_0(R) \subseteq R$, and so also $f_1(x) = (\varphi(x) - f_0(x))i^{-1}$ satisfies $f_1(R) \subseteq R$. A similar argument applies for the rest of the polynomials in the decomposition. □

Remark 3.4. Note that Proposition 3.3 is false without assuming $\frac{1}{2} \in R$. Take for example $F = \mathbb{R}$, $E = \mathbb{Z}$, $A = \mathbb{O}$ and R the octonion $\mathbb{Z}$-algebra inside $\mathbb{O}$ generated by i, j, ℓ. Then by [8, Lemma 31], $f(x) = \frac{1}{2}(1 + i + j + ij + \ell + i\ell + j\ell + (ij)\ell)(x^2 - x) \in \mathrm{Sub}_R(\mathbb{O}[x])$. However, $f_0(x) = \frac{1}{2}(x^2 - x)$ is not in $\mathrm{Sub}_R(\mathbb{O}[x])$ for $\frac{1}{2}(i^2 - i) = -\frac{1}{2}(1+i)$.

Lemma 3.5. *Let F be a field, E a subring of F, A an octonion F-algebra and R an octonion E-algebra inside A. Let $f(x) \in \mathrm{Sub}_R(A[x])$ and $g(x) \in \mathrm{Sub}_R(A[x]) \cap F[x]$. Then $f(x) \cdot g(x) \in \mathrm{Sub}_R(A[x])$. Moreover, if $f(x)$ is also in $F[x]$, then $f(x) \cdot g(x) \in$* $\mathrm{Sub}_R(A[x]) \cap F[x]$*, and as a result,* $\mathrm{Sub}_R(A[x]) \cap F[x]$ *is a commutative ring.*

Proof. Write $f(x) = a_n x^n + \cdots + a_0$ and $g(x) = b_m x^m + \cdots + b_0$, and $h(x) = f(x)g(x)$. Then $h(\lambda) = \sum_{k=0}^{n} \sum_{r=0}^{m} (a_k b_r)\lambda^{k+\ell}$ for $\lambda \in A$, but since the b_r's are central and for each k, the elements a_k and λ live in an associative subalgebra of A, we have $h(\lambda) = \sum_{k=0}^{n} a_k g(\lambda)\lambda^k = f(\lambda)g(\lambda)$. Therefore, $h(R) \subseteq R$, because $f(R), g(R) \subseteq R$. Hence, $f(x) \cdot g(x) \in \mathrm{Sub}_R(A[x])$. If we assume in addition that $f(x) \in F[x]$, then all the coefficients of $f(x) \in g(x)$ are in $F[x]$, and thus $f(x) \cdot g(x) \in \mathrm{Sub}_R(A[x]) \cap F[x]$. As a result, $\mathrm{Sub}_R(A[x]) \cap F[x]$ is closed under multiplication, and since it is commutative and clearly closed under addition, it is a commutative ring. □

Theorem 3.6. *Let F be a field of* $\mathrm{char}(F) \neq 2$, *E a subring of F, A an octonion F-algebra and R an octonion E-algebra inside A containing the standard generators i, j, ℓ of A, their inverses, and $\frac{1}{2}$. Write $S = \mathrm{Sub}_R(A[x])$ and $C = S \cap F[x]$. Then S is an octonion C-algebra.*

Proof. It is a free C-module of rank 8 (hence, projective) by Proposition 3.3:

$$S = C \oplus Ci \oplus Cj \oplus Cij \oplus C\ell \oplus Ci\ell \oplus Cj\ell \oplus C(ij)\ell.$$

The set S is clearly closed under addition. Consider two polynomials $f(x)$ and $g(x)$ in the set. Then $g(x) = g_0(x) + \cdots + g_7(x)((ij)\ell)$ as in Proposition 3.3. Now, $f(x)g(x) = f(x)g_0(x) + \cdots + f(x)((ij)\ell)g_7(x)$. Since the polynomials $f(x)i, \ldots, f(x)((ij)\ell)$ are in S by Lemma 3.1, and multiplying a polynomial from S by a polynomial from S with central coefficients is in S by Lemma 3.5, we conclude that $f(x)g(x) \in S$, i.e., S is closed under multiplication.

Now, since in the decomposition $f(x) = f_0(x) + \cdots + f_7(x)(ij)\ell$, the polynomials $f_0(x), \ldots, f_7(x)$ are in C, and S is closed under multiplication, we conclude that $\overline{f(x)} = f_0(x) - \cdots - f_7(x)(ij)\ell$ is also in S, i.e., S is closed under the canonical involution of $A[x]$. Moreover, $\mathrm{Norm}(f(x)) = f(x) \cdot \overline{f(x)}$ is thus in S, and since its coefficients live in F, $\mathrm{Norm}(f(x)) \in C$. Therefore S has a norm form $\mathrm{Norm} : S \to C$ mapping $f(x) \mapsto \mathrm{Norm}(f(x)) = f(x) \cdot \overline{f(x)}$, which allows composition by the embedding of S into $A \otimes F(x)$. The underlying symmetric bilinear form $B(x, y) = \mathrm{Norm}(x + y) - \mathrm{Norm}(x) - \mathrm{Norm}(y)$ gives rise to the linear transformation from S to S^* by the assignment $x \mapsto B(x, —)$, whose inverse maps each $\varphi \in S^*$ to

$$\frac{1}{2}\varphi(1) \cdot 1 - \frac{1}{2\alpha}\varphi(i) \cdot i - \frac{1}{2\beta}\varphi(j) \cdot j + \frac{1}{2\alpha\beta}\varphi(ij) \cdot ij - \frac{1}{2\gamma}\varphi(\ell) \cdot \ell + \frac{1}{2\alpha\gamma}\varphi(i\ell) \cdot i\ell + \frac{1}{2\beta\gamma}\varphi(j\ell) \cdot j\ell - \frac{1}{2\alpha\beta\gamma}\varphi((ij)\ell) \cdot (ij)\ell,$$

and so S is an octonion C-algebra. □

Corollary 3.7. *Let F be a field of* $\mathrm{char}(F) = p \geq 3$, *$E$ a subring of F, A an octonion F-algebra and R an octonion E-algebra inside A containing the standard* *generators i, j, ℓ of A and their inverses. Write $S = \mathrm{Sub}_R(A[x])$ and $C = S \cap F[x]$. Then S is an octonion C-algebra, and a free C-module or rank* 8.

Proof. One only needs to stress that R contains the inverse of 2 in this case, because R is unital and thus $\mathbb{F}_p \subseteq R$, and $\mathbb{F}_p$ contains the inverse of 2. □

4. Fields of characteristic 2

If we want to include the possibility of $\mathrm{char}(F) = 2$, the quaternion algebra presentation takes a different form

$$Q = F\langle i, j : i^2 + i = \alpha, j^2 = \beta, ij + ji = j\rangle$$

for some $\alpha \in F$ and $\beta \in F^\times$. The canonical involution now maps $a + bi + cj + dij$ to $a + b + bi + cj + dij$. The octonion algebra is again defined as $A = Q \oplus Q\ell$ with $(q + r\ell)(s + t\ell) = qs + \bar{t}r\gamma + (r\bar{s} + tq)\ell$ for any $q, r, s, t \in Q$ and a fixed $\gamma \in F^\times$. This involution extends to A by $\overline{r + s\ell} = \bar{r} + s\ell$, giving rise to the trace and norm maps, which satisfy the same properties as before. Note that Lemmas 3.1 and 3.5 hold true in any characteristic.

Proposition 4.1. *Let F be a field of $\mathrm{char}(F) = 2$, E a subring of F, A an octonion F-algebra and R an octonion E-algebra inside A containing the standard generators i, j, ℓ of A and their inverses. Then every polynomial $f(x) \in \mathrm{Sub}_R(A[x])$ decomposes as $f(x) = f_0(x)+f_1(x)i+f_2(x)j+f_3(x)ij+f_4(x)\ell+f_5(x)(i\ell)+f_6(x)(j\ell)+f_7((ij)\ell)$ where $f_0(x), \dots, f_7(x)$ are polynomials in $\mathrm{Sub}_R(A[x]) \cap F[x]$.*

Proof. The decomposition is obvious. It is left to explain why $f_m(x)(R) \subseteq R$ for $m = 0, \dots, 7$. By Lemma 3.1, $g(x) = ((f(x)j)\ell)(j\ell)^{-1}$ satisfies $g(R) \subseteq R$, and so does $h(x) = g(x) + f(x)$, which is equal to $f_1(x) + f_3(x)j + f_5(x)\ell + f_7(x)j\ell$. Now, $\varphi(x) = h(x) + ((h(x)(ij))\ell)((ij)\ell)^{-1} = f_3(x) + f_7(x)\ell$ satisfies $\varphi(R) \subseteq R$ too. Finally $\varphi(x)+((\varphi(x)j)(i\ell))(j(i\ell))^{-1}) = f_7(x)$ satisfies $f_7(R) \subseteq R$. A similar argument applies for the rest of the polynomials in the decomposition. □

Then the following analogue of Theorem 3.6 holds true with the same proof:

Theorem 4.2. *Let F be a field of $\mathrm{char}(F) = 2$, E a subring of F, A an octonion F-algebra and R an octonion E-algebra inside A containing the standard generators i, j, ℓ of A and their inverses. Write $S = \mathrm{Sub}_R(A[x])$ and $C = S \cap F[x]$. Then S is an octonion C-algebra.*

5. Examples

- When $F = \mathbb{F}_p(r,s,t)$ is the function field in three algebraically independent variables over $\mathbb{F}_p$ for a prime integer p, $E = \mathbb{F}_p(s,t)[r]$, $A = Q \oplus Q\ell$ where $\ell^2 = t$ and Q is generated over F by i and j where $j^2 = s$ and $\mathbb{F}_p(i)/\mathbb{F}_p$ is the unique quadratic field extension of $\mathbb{F}_p$, and R is the octonion E-algebra generated by i, j, ℓ, the set $S = \mathrm{Sub}_R(A[x])$ is an octonion $(S \cap F[x])$-algebra.

- When $F = \mathbb{Q}_p(s,t)$ is the function field in two algebraically independent variables over $\mathbb{Q}_p$ for an odd prime p, $E = \mathbb{Z}_p(s,t)$, $A = Q \oplus Q\ell$ where $\ell^2 = t$ and Q is generated over F by i and j where $j^2 = s$ and $\mathbb{Q}_p(i)/\mathbb{Q}_p$ is the unique quadratic field extension of $\mathbb{Q}_p$ which is unramified with respect to the p-adic valuation, and R is the octonion E-algebra generated by i, j, ℓ, the set $S = \mathrm{Sub}_R(A[x])$ is an octonion $(S \cap F[x])$-algebra. Note that 2 is invertible in R in this case, and therefore Theorem 3.6 applies.

- When $F = \mathbb{Q}$, $E = \mathbb{Z}[\frac{1}{2}]$, $A = \mathbb{O}$ and R is the octonion E-algebra generated by the standard generators of $\mathbb{O}$, $S = \mathrm{Sub}_R(A[x])$ is an octonion $(S \cap F[x])$-algebra.

6. Cayley-Dickson Algebras

Given a field F, an F-algebra A with involution σ and an element $\delta \in F^\times$, the Cayley-Dickson doubling (A, σ, δ) gives an algebra $B = A \oplus A\ell$ whose dimension over F is twice the dimension of A, and its multiplication is defined by

$$(q + r\ell)(s + t\ell) = qs + \sigma(t)r\delta + (r\sigma(s) + tq)\ell$$

for any $q, r, s, t \in A$. The involution σ extends to B by $\sigma(q + r\ell) = \sigma(q) - r\ell$.

Starting with a separable quadratic extension K/F with the nontrivial automorphism as the involution, one step would give rise to a quaternion algebra, and another step would give an octonion algebra. Algebras that are obtained by this process are called Cayley-Dickson algebras. In particular, such algebras are power-associative (see [5]). Moreover, every element λ in a Cayley-Dickson algebra A with involution σ over F satisfies $\lambda^2 - \mathrm{Tr}(\lambda) \cdot \lambda + \mathrm{Norm}(\lambda) = 0$ where $\mathrm{Tr}(\lambda) = \lambda + \sigma(\lambda) \in F$ and $\mathrm{Norm}(\lambda) = \lambda \cdot \sigma(\lambda) \in F$.

In this section we focus on the Cayley-Dickson algebras obtained by repeating those steps with δ always being -1, starting with the quadratic extension $\mathbb{C}/\mathbb{R}$. We call these algebras “the real nonsplit Cayley-Dickson algebras”, because their norm forms are the nonsplit quadratic Pfisre forms. The algebras $\mathbb{H}$ and $\mathbb{O}$ are among those algebras.

In what follows, let A be a real nonsplit Cayley-Dickson algebra. This algebra has a natural $\mathbb{R}$-basis provided by the process. Let R be the free $\mathbb{Z}$-module spanned by that basis. By the multiplication law, it is clear that R is closed under multiplication. Our aim in this section is to prove that for any $\lambda \in R$, also $\frac{1}{p}(\lambda^{p^2}-\lambda)(\lambda^p-\lambda)$ is in R, thus extending this result from [7] that was stated for $\mathbb{H}$ only. The congruence $\alpha \equiv \beta \pmod{p}$ means that $\alpha - \beta \in p \cdot R$.

Lemma 6.1. *Let $\lambda \in R$. Write $\lambda = y+z$ where $y \in \mathbb{Z}$ and $\mathrm{Tr}(z) = 0$. Then $\lambda^p \equiv y+z^p \pmod{p}$ for any prime integer p.*

Proof. Since y commutes with z, we have $(y+z)^p = \sum_{n=0}^{p} \binom{p}{n} y^n z^{p-n}$. Since all the coefficients, except for the initial and final coefficients, are multiples of p, we have $\lambda^p \equiv y^p + z^p \pmod{p}$. Now, $y^p \equiv y \pmod{p}$ by Fermat's little theorem, and so $\lambda^p \equiv y + z^p \pmod{p}$. □

Corollary 6.2. *For any odd prime p, positive integer n and $\lambda = y+z \in R$ where $y \in \mathbb{Z}$ and $\mathrm{Tr}(z) = 0$, $\lambda^{p^n} \equiv y + z^{p^n} \pmod{p}$.*

Proof. By induction on n. Since p is odd, $z^{p^n} = (-\mathrm{Norm}(z))^{\frac{p^n-1}{2}} z$, which means $\mathrm{Tr}(z^{p^n}) = 0$, and so $(y+z^{p^n})^p \equiv y + z^{p^{n+1}} \pmod{p}$. □

Theorem 6.3. *Let p be an odd prime integer. Then $(\lambda^{p^2}-\lambda)(\lambda^p-\lambda) \in p \cdot R$ for any $\lambda \in R$.*

Proof. Write $\lambda = y+z$ where $y \in \mathbb{Z}$ and $\mathrm{Tr}(z) = 0$. Then $\lambda^p \equiv y+z^p \pmod{d}$. By the previous corollary, $\lambda^{p^2} - \lambda \equiv z^{p^2} - z \pmod{p}$. If $p \nmid \mathrm{Norm}(z)$, then $z^{p^2} - z = z \cdot (((-\mathrm{Norm}(z))^{\frac{p+1}{2}})^{p-1} - 1)$. Since $\mathrm{Norm}(z)^{\frac{p+1}{2}} \in \mathbb{Z} \setminus p\mathbb{Z}$, by Fermat's little theorem we conclude that $((-\mathrm{Norm}(z))^{\frac{p+1}{2}})^{p-1} - 1 \equiv 0 \pmod{p}$, and so $\lambda^{p^2} - \lambda \equiv 0 \pmod{p}$. Suppose now that $p \mid \mathrm{Norm}(z)$. Then $(\lambda^{p^2}-\lambda)(\lambda^p-\lambda) \equiv (z^{p^2}-z)(z^p-z) = z^{p^2+p} - z^{p^2+1} - z^{p+1} + z^2$. Since the powers $p^2+p, p^2+1, p+1$ and 2 are all even integers, the latter is an integer multiple of $\mathrm{Norm}(z)$, and therefore a multiple of p. Consequently, $(\lambda^{p^2}-\lambda)(\lambda^p-\lambda) \equiv 0 \pmod{p}$ in all cases. □

Theorem 6.4. *For any $\lambda \in R$, we have $(\lambda^4-\lambda)(\lambda^2-\lambda) \in 2 \cdot R$.*

Proof. Write $\lambda = y+z$ where $y \in \mathbb{Z}$ and $\mathrm{Tr}(z) = 0$. Then $\lambda^2 \equiv y+z^2 \pmod{2}$. Since z^2 is also in $\mathbb{Z}$, we have $(y+z^2)^2 \equiv y^2+z^4 \pmod{2}$. The latter is congruent to $y+z^2 \pmod{2}$. Hence, $\lambda^4 \equiv y+z^2 \equiv \lambda^2 \pmod{2}$. Now $(\lambda^4-\lambda)(\lambda^2-\lambda) = \lambda^6-\lambda^5-\lambda^3+\lambda^2$, and $\lambda^6 = \lambda^2 \cdot \lambda^4 \equiv \lambda^2 \cdot \lambda^2 = \lambda^4 \equiv \lambda^2 \pmod{2}$ and $\lambda^5 = \lambda \cdot \lambda^4 \equiv \lambda \cdot \lambda^2 = \lambda^3$, and so $\lambda^6 - \lambda^5 - \lambda^3 + \lambda^2 \equiv 2\lambda^2 - 2\lambda^3 \equiv 0 \pmod{2}$. Consequently, $(\lambda^4-\lambda)(\lambda^2-\lambda) \equiv 0 \pmod{2}$. □

Corollary 6.5. *Setting $R = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}ij \oplus \mathbb{Z}\ell \oplus \mathbb{Z}i\ell \oplus \mathbb{Z}j\ell \oplus \mathbb{Z}(ij)\ell$, for any prime integer p, the polynomial $\frac{1}{p}(x^{p^2} - x)(x^p - x)$ is in* $\mathrm{Sub}_R(\mathbb{O}[x])$.

As already mentioned, in addition to the polynomials of the form $\frac{1}{p}(x^{p^2} - x)(x^p - x)$, by [8, Lemma 31], we also have $\frac{1}{2}(1 + i + j + ij + \ell + i\ell + j\ell + (ij)\ell)(x^2 - x)$ in $\mathrm{Sub}_R(\mathbb{O}[x])$. Apparently, this extends to arbitrary Cayley-Dickson algebras too.

Theorem 6.6. *Let A be a real nonsplit Cayley-Dickson algebra of degree 2^n, $\{s_m : 1 \leq m \leq 2^n\}$ its natural $\mathbb{R}$-basis, and $R = \oplus_{m=1}^{2^n} \mathbb{Z}s_m$. Then for any $\lambda \in R$, we have $(\sum_{m=1}^{2^n} s_m)(\lambda^2 - \lambda) \in 2 \cdot R$.*

Proof. The set $Q_n = \{s_m, -s_m : 1 \leq m \leq 2^n\}$ studied in [1] forms a loop, and right-multiplication by any basis element induces a permutation on Q_n. Consequently, right-multiplication by a basis element acts transitively on the mod 2 classes of Q_n, and therefore

$$(\sum_{m=1}^{2^n} s_m)s_t \equiv \sum_{m=1}^{2^n} s_m \pmod 2, \quad \text{for any } t \in \{1, \ldots, 2^n\}. \tag{1}$$

Moreover, $(\sum_{m=1}^{2^n} a_m s_m)^2 = a_1^2 + \sum_{m=2}^{2^n}(a_m^2 s_m^2 + 2a_1 a_m s_m)$, for $s_1 = 1$ and all the other basis elements anti-commute in pairs, and so $(\sum_{m=1}^{2^n} a_m s_m)^2 \equiv \sum_{m=1}^{2^n} a_m^2 s_m^2 \equiv \sum_{m=1}^{2^n} a_m^2 \equiv \sum_{m=1}^{2^n} a_m \pmod 2$. Write $\lambda = \sum_{m=1}^{2^n} a_m s_m$. Then $\lambda^2 \equiv \sum_{m=1}^{2^n} a_m \pmod 2$, and so $(\sum_{m=1}^{2^n} s_n)\lambda^2 \equiv \sum_{m=1}^{2^n}(\sum_{t=1}^{2^n} a_t)s_m \pmod 2$. By (1) we conclude that $(\sum_{m=1}^{2^n} s_m)\lambda \equiv \sum_{m=1}^{2^m}(\sum_{t=1}^{2^n} s_t)a_m \equiv (\sum_{m=1}^{2^n} s_m)\lambda^2 \pmod 2$. Therefore, $(\sum_{m=1}^{2^n} s_n)(\lambda^2 - \lambda) \equiv 0 \pmod 2$. ◻

7. Acknowledgements

This research was supported through the program “Research in Pairs” by the Mathematisches Forschungsinstitut Oberwolfach in 2020 (fellowship 2039q). The author thanks Nicholas J. Werner and Jean-Pierre Tignol for their comments in the early stages of this project. The author also thanks Alon Nishry for referring the author’s attention to Werner’s work.

References

[1] J. Kirshtein. Multiplication groups and inner mapping groups of Cayley-Dickson loops. *J. Algebra Appl.*, 13(1):1350078, 26, 2014.

[2] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol. *The book of involutions*, volume 44 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1998. With a preface in French by J. Tits.

[3] O. Loos, H. P. Petersson, and M. L. Racine. Inner derivations of alternative algebras over commutative rings. *Algebra Number Theory*, 2(8):927–968, 2008.

[4] G. Pólya. Über ganzwertige ganze Funktionen. *Rend. Circ. Mat. Palermo*, 40:1–16, 1915.

[5] R. D. Schafer. On the algebras formed by the Cayley-Dickson process. *Amer. J. Math.*, 76:435–446, 1954.

[6] T. A. Springer and F. D. Veldkamp. *Octonions, Jordan algebras and exceptional groups*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.

[7] N. J. Werner. Integer-valued polynomials over quaternion rings. *J. Algebra*, 324(7):1754–1769, 2010.

[8] N. J. Werner. Integer-valued polynomials on algebras: a survey of recent results and open questions. In *Rings, polynomials, and modules*, pages 353–375. Springer, Cham, 2017.

[9] K. A. Zhevlakov, A. M. Slin'ko, I. P. Shestakov, and A. I. Shirshov. *Rings that are nearly associative*, volume 104 of *Pure and Applied Mathematics*. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], New York-London, 1982. Translated from the Russian by Harry F. Smith.