THE FACTORIZATION THRESHOLD IN CAYLEY–DICKSON INTEGER ALGEBRAS

GIOVANNI LEVRATTI

ABSTRACT. We establish the precise threshold at which the arithmetic of Cayley–Dickson integer algebras breaks down. Let $S_n = \bigoplus_{v \in \mathbb{F}_2^n} \mathbb{Z} \cdot e_v \subset \mathcal{A}_n$ be the canonical integer subalgebra of the n-th Cayley–Dickson algebra over $\mathbb{R}$. We prove that S_n is an integral domain if and only if $n \leq 3$, and that S_n is a UFD if and only if $n \leq 1$. The two thresholds are distinct: S_2 and S_3 are domains that fail UFD, with exactly $2^n - 1$ pairwise inequivalent factorisations of 2 in S_n for $n \in \{2, 3\}$ (and at least $2^n - 1$ for all $n \geq 4$). The count $2^n - 1 = |PG(n-1, \mathbb{F}_2)|$ connects the arithmetic failure to the same finite-geometric structure that governs the zero-divisor count $|ZD(n)| = 336 \cdot \binom{n-1}{3}_2$. For $n \geq 4$ the failure manifests in two complementary ways: the $\{0, 4, 8\}$ Trichotomy shows that no product of two norm-2 elements of S_n can be a nonzero norm-2 element; at the same time, the right annihilator $\mathrm{rann}_{S_n}(a)$ of every ZD-active $a \in C^*(n)$ is non-trivial — it contains non-units of norm 2 — an identity that cannot occur in any integral domain. The threshold $n = 4$ coincides with the endpoint of the classical chain of composition identities for sums of 2^n squares (Hurwitz 1898) and with the failure of norm-multiplicativity. The proofs depend on the counting formula $|\mathrm{ZD}(n)| = 336 \cdot \binom{n-1}{3}_2$, the $\{0, 4, 8\}$ Trichotomy, and the WRAP identity, all established in [4].

CONTENTS

Date: May 29, 2026.

2020 *Mathematics Subject Classification.* 17A35, 17A45, 11E25, 16U30.

Key words and phrases. Cayley–Dickson algebras, zero divisors, unique factorization, Hurwitz integers, integral domain threshold, composition identities, WRAP identity, norm redistribution.

1. Introduction

The Cayley–Dickson construction produces an infinite tower of real algebras:

$$\mathcal{A}_0 = \mathbb{R} \subset \mathcal{A}_1 = \mathbb{C} \subset \mathcal{A}_2 = \mathbb{H} \subset \mathcal{A}_3 = \mathbb{O} \subset \mathcal{A}_4 = \mathbb{S} \subset \cdots$$

in which each doubling step eliminates one algebraic property. Hurwitz [3] identified the first four algebras as the only normed division algebras over $\mathbb{R}$; at $\mathcal{A}_4$ (the sedenions, dimension 16) the multiplicative norm and zero-divisor freeness are simultaneously lost.

The arithmetic question. Each algebra $\mathcal{A}_n$ contains a natural integer subalgebra S_n, the $\mathbb{Z}$-span of its canonical basis. The tower $S_0 = \mathbb{Z} \subset S_1 = \mathbb{Z}[i] \subset S_2 \subset S_3 \subset S_4 \subset \cdots$ is a sequence of non-commutative (and eventually non-associative) rings. Where does the arithmetic of S_n break down irreparably?

Main results. We prove two thresholds for the tower $S_0 \subset S_1 \subset \cdots$:

- *Domain threshold* (Theorem 3.1): S_n is an integral domain $\Leftrightarrow n \leq 3$.
- *UFD threshold* (Corollary 3.3): S_n is a UFD $\Leftrightarrow n \leq 1$.

The two thresholds are strictly separated by the gap $n \in \{2, 3\}$, where S_n is a domain but not a UFD. For $n \geq 4$, Proposition 3.5 quantifies the failure: for $n \in \{2, 3\}$, S_n admits exactly $2^n - 1$ pairwise inequivalent factorisations of 2 (all of the form $(1 + e_k)(1 - e_k)$); for $n \geq 4$, at least $2^n - 1$ such factorisations exist. The count $2^n - 1 = |PG(n - 1, \mathbb{F}_2)|$ is the same finite-geometric quantity governing the zero-divisor structure of $\mathcal{A}_n$. For $n \geq 4$, Section 5 characterises the domain failure precisely: ZD-active elements of norm 2 have non-trivial right annihilators in S_n (Theorem 5.8) and cannot arise as products of two norm-2 non-units (Lemma 5.2).

The norm gap. For any zero-divisor pair $(a, b) \in \mathrm{ZD}(n)$, both elements have norm $N(a) = N(b) = 2$ (established in [4]), yet $N(ab) = 0$. The gap $N(a)N(b) - N(ab) = 4$ (Theorem 3.8) is the quantitative signature of the breakdown, and it connects directly to the classical chain of composition identities: the identities for $1, 2, 4, 8$ squares exist precisely for $n = 0, 1, 2, 3$, and Hurwitz [3] proved no such identity exists for $n \geq 4$.

Relation to existing work. The present paper is a companion to [4], which establishes the full classification of zero-divisors in $\mathcal{A}_n$ via the Sign-Parity framework and proves the counting formula $|\mathrm{ZD}(n)| = 336 \cdot \binom{n-1}{3}_2$. All results labeled [4, Thm X] are proved unconditionally there. Classical references for the integer algebras are Hurwitz [2, 3], Conway–Smith [1], and Schafer [5].

Organisation. Section 2 establishes the setup and locates S_n in the classical hierarchy. Section 3 proves both the domain threshold and the complete UFD threshold for the tower. Section 4 connects to norm-multiplicativity and sum-of-squares identities. Section 5 develops the factorization structure for $n \geq 4$. Section 6 gives an explicit example in S_4. Section 7 states open problems.

2. Setup: the Canonical Integer Subalgebra

Definition 2.1 (Cayley–Dickson algebras)**.** Let $\mathcal{A}_0 = \mathbb{R}$. For $n \geq 0$, $\mathcal{A}_{n+1}$ consists of pairs (a, b) with $a, b \in \mathcal{A}_n$, equipped with

$$(a, b)(c, d) = (ac - \bar{d}b,\ da + b\bar{c}), \qquad \overline{(a, b)} = (\bar{a}, -b).$$

The canonical basis $\mathcal{B}_n = \{e_0, e_1, \dots, e_{2^n-1}\}$ satisfies $N(e_i) = 1$ and $e_0 = 1$. By the XOR Index Theorem [4, Thm 3.1]:

$$e_\alpha \cdot e_\beta = \varepsilon(\alpha, \beta)\, e_{\alpha\oplus\beta}, \qquad \varepsilon(\alpha, \beta) \in \{+1, -1\}.$$

Definition 2.2 (Canonical integer subalgebra)**.** The *canonical integer subalgebra* of $\mathcal{A}_n$ is

$$S_n \;=\; \bigoplus_{v\in\mathbb{F}_2^n} \mathbb{Z}\cdot e_v \;\subset\; \mathcal{A}_n.$$

This is the $\mathbb{Z}$-span of $\mathcal{B}_n$, closed under the Cayley–Dickson product. S_n is a $\mathbb{Z}$-algebra of rank 2^n. The norm is $N(\sum_v a_v e_v) = \sum_v a_v^2$. *Units* of S_n are elements with $N = 1$, namely $\{\pm e_v : v \in \mathbb{F}_2^n\}$; there are 2^{n+1} of them.

Remark 2.3 (Position in the classical hierarchy). Table 1 records the status of each S_n in the first few steps of the tower.

Table 1. The integer subalgebra tower.

n	S_n	Classical name	Domain?	UFD?
0	$\mathbb{Z}$	Rational integers	✓	✓ PID
1	$\mathbb{Z}[i]$	Gaussian integers	✓	✓ PID
2	$L_\mathbb{Z}$	Lipschitz quaternion integers	✓	×
3	$G_\mathbb{Z}$	Gravesian octonion integers	✓	× (see Rem. 2.4)
≥4	—	—	×	×

Remark 2.4 (UFD failure in $G_\mathbb{Z}$). By Proposition 3.5 (with $n = 3$), the element $2 \in G_\mathbb{Z}$ admits exactly $2^3 - 1 = 7$ pairwise inequivalent factorisations

$$2 = (1 + e_k)(1 - e_k), \qquad k = 1, \dots, 7.$$

The additional Coxeter–Dickson units (e.g., $\frac{1+e_1+e_2+e_4}{2}$) that would identify these factorisations lie in the maximal order $O_\mathbb{Z} \supsetneq G_\mathbb{Z}$; $O_\mathbb{Z}$ admits a non-associative analogue of unique factorization [1].

Remark 2.5 (Maximal orders). $S_2 = L_\mathbb{Z}$ is a *strict* subring of the Hurwitz integers $H_\mathbb{Z}$ (the maximal order in $\mathbb{H}$). $H_\mathbb{Z}$ is a UFD [2]; $L_\mathbb{Z}$ is not (Example 3.7). Similarly, $S_3 = G_\mathbb{Z}$ is a strict subring of the Coxeter–Dickson maximal order $O_\mathbb{Z}$, and fails UFD for the same structural reason (Remark 2.4). We work with S_n throughout because it is the natural output of the Cayley–Dickson construction over $\mathbb{Z}$, not with maximal orders.

3. The Integral Domain Threshold

Theorem 3.1 (Integral domain threshold)**.** *S_n is an integral domain if and only if $n \le 3$.*

Proof. **($n \le 3$, S_n is a domain.)** For $n \le 3$ the algebra $\mathcal{A}_n$ is one of $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$, the four normed division algebras over $\mathbb{R}$ [3]. In a normed division algebra, $N(xy) = N(x)N(y)$ for all x, y and N is positive definite. Since $S_n \subset \mathcal{A}_n$ is a subring and N is the restriction of the norm of $\mathcal{A}_n$, the identity $N(ab) = N(a)N(b)$ holds in S_n as well. For $a, b \in S_n$ both non-zero: writing $a = \sum_v a_v e_v$ with $a_v \in \mathbb{Z}$, at least one $a_v \neq 0$, so $N(a) = \sum_v a_v^2 \ge 1$; likewise $N(b) \ge 1$. Hence $N(ab) = N(a)N(b) \ge 1 > 0$, giving $ab \neq 0$.

($n \geq 4$, S_n is not a domain.) By [4, Thm 7.16]:

$$|\mathrm{ZD}(n)| = 336 \cdot \binom{n-1}{3}_2 > 0 \qquad \text{for all } n \geq 4.$$

Hence there exists $(a,b) \in \mathrm{ZD}(n)$ with $a, b \in C^*(n)$, $a \neq 0$, $b \neq 0$, and $ab = 0$. Every element of $C^*(n)$ belongs to S_n (it is the $\mathbb{Z}$-span of two basis elements). □

Corollary 3.2. *For $n \geq 4$, S_n cannot be a UFD.*

Proof. A UFD is an integral domain by definition. □

Corollary 3.3 (UFD threshold)**.** *S_n is a UFD if and only if $n \leq 1$.*

Proof. We verify each case.

- $n = 0$: $S_0 = \mathbb{Z}$ is a PID, hence a UFD.
- $n = 1$: $S_1 = \mathbb{Z}[i]$ is a PID, hence a UFD.
- $n = 2$: $S_2 = L_{\mathbb{Z}}$ is not a UFD: Proposition 3.5 gives $2^2 - 1 = 3$ inequivalent factorisations of 2.
- $n = 3$: $S_3 = G_{\mathbb{Z}}$ is not a UFD: Proposition 3.5 gives $2^3 - 1 = 7$ inequivalent factorisations of 2.
- $n \geq 4$: S_n is not a UFD (Corollary 3.2). □

Remark 3.4. The two thresholds for the tower are therefore distinct:

$$\underbrace{n \leq 1}_{\text{UFD}} \subsetneq \underbrace{n \leq 3}_{\text{domain}} \subsetneq \quad \underbrace{n \geq 4}_{\text{not a domain}} .$$

In the gap $n \in \{2, 3\}$, S_n is an integral domain — norm-positive, zero-divisor free — yet admits non-unique factorisation. The precise obstruction in both cases is the absence of enough units: the missing Hurwitz unit $\frac{1+e_1+e_2+e_3}{2}$ for $n = 2$, and the missing Coxeter–Dickson units for $n = 3$, lie in the respective maximal orders $H_{\mathbb{Z}}$ and $O_{\mathbb{Z}}$ but not in S_n.

Proposition 3.5 (Factorisations of 2 in S_n)**.** *For every $n \geq 2$, the $2^n - 1$ factorisations*

$$2 = (1 + e_k)(1 - e_k), \qquad k = 1, \ldots, 2^n - 1,$$

are pairwise inequivalent in S_n under the unit group $\{\pm e_v : v \in \mathbb{F}_2^n\}$.

Moreover:

(i) For $2 \leq n \leq 3$: these are exactly *all essentially distinct non-trivial factorisations of 2 in S_n.*

(ii) For $n \geq 4$: there are at least *$2^n - 1$ such inequivalent factorisations; additional factorisations with factors of norms other than 2 exist. Computational verification for $n = 4$ (see Remark 7.1) finds non-trivial factorisations with $N(\alpha) = 4$, $N(\beta) = 2$.*

Proof. **Pairwise inequivalence (all $n \geq 2$).** We show no unit sends $1 + e_k$ to $1 + e_l$ for $k \neq l$.

Left multiplication by $\pm e_v$. If $v = 0$: $\pm e_0(1 + e_k) = \pm(1 + e_k)$, giving only $k = l$ (positive sign) or real part -1 (negative sign); neither yields $1 + e_l$ with $l \neq k$. If $v \geq 1$ and $v \neq k$: both e_v and $e_v e_k = \varepsilon(v,k) e_{v \oplus k}$ are index-pure with indices ≥ 1, so $\mathrm{Re}(e_v(1 + e_k)) = 0 \neq 1$. If $v = k$: $e_k(1 + e_k) = e_k + e_k^2 = e_k - e_0$, so $\mathrm{Re}(e_k(1 + e_k)) = -1 \neq 1$. In all cases with $v \geq 1$ the real part differs from $\mathrm{Re}(1 + e_l) = 1$, ruling out left-associates.

Right multiplication by $\pm e_v$. For $v \neq k$: $(1+e_k)e_v = e_v + e_k e_v$. By anti-commutativity [4, Lem 4.1], $e_k e_v = -e_v e_k$, so $(1+e_k)e_v = e_v - e_v e_k$; the real-part argument is the same as for left multiplication. For $v = k$: $(1+e_k)e_k = e_k + e_k^2 = e_k - e_0$, giving real part $-1 \neq 1$.

Hence the $2^n - 1$ elements $\{1+e_k\}_{k=1}^{2^n-1}$ are pairwise non-associate, and all $2^n - 1$ factorisations of 2 are inequivalent.

Completeness for $n \leq 3$ (part (i)). Since S_n is a domain with $N(ab) = N(a)N(b)$ for $n \leq 3$ (Theorem 3.1 and Hurwitz [3]), any non-trivial factorisation $2 = \alpha\beta$ (neither factor a unit) satisfies $N(\alpha)N(\beta) = N(2) = 4$, forcing $N(\alpha) = N(\beta) = 2$.

Write $\alpha = \sum_v \alpha_v e_v$ with $\sum_v \alpha_v^2 = 2$, so exactly two coordinates are ± 1. The real part of $\alpha\beta$ is $\mathrm{Re}(\alpha\beta) = \alpha_0\beta_0 - \sum_{k\geq 1} \alpha_k \beta_k$ (using $e_0 e_0 = e_0$ and $e_k e_k = -e_0$ for $k \geq 1$).

Case $\alpha_0 = 0$ (both indices ≥ 1): Write $\alpha = \alpha_{k_1} e_{k_1} + \alpha_{k_2} e_{k_2}$ with $k_1 \neq k_2$, both ≥ 1, and $\alpha_{k_i} = \pm 1$. From $\mathrm{Re}(\alpha\beta) = -\alpha_{k_1}\beta_{k_1} - \alpha_{k_2}\beta_{k_2} = 2$ and $|\alpha_{k_i}| = |\beta_{k_i}| = 1$, we get $\beta_{k_i} = -\alpha_{k_i}$ for both i. Since $N(\beta) = \beta_{k_1}^2 + \beta_{k_2}^2 = 2$, all other components of β vanish, so $\beta = -\alpha$ and indeed $\alpha\beta = \alpha(-\alpha) = -\alpha^2$. By anti-commutativity [4, Lem 4.1]: $e_{k_i} e_{k_j} = -e_{k_j} e_{k_i}$ for $k_i \neq k_j$, so the cross terms in α^2 cancel:

$$\alpha^2 = \alpha_{k_1}^2 e_{k_1}^2 + \alpha_{k_2}^2 e_{k_2}^2 + \alpha_{k_1}\alpha_{k_2} \underbrace{(e_{k_1} e_{k_2} + e_{k_2} e_{k_1})}_{=0} = -N(\alpha) e_0 = -2e_0.$$

Hence $\alpha\beta = -\alpha^2 = 2e_0 = 2$: *such a factorisation exists.* However, it is left-associate to a Case $\alpha_0 \neq 0$ factorisation. Namely, the unit $u = -e_{k_1}$ satisfies:

$$u\alpha = (-e_{k_1})(\alpha_{k_1} e_{k_1} + \alpha_{k_2} e_{k_2}) = \alpha_{k_1} e_0 - \alpha_{k_2} \varepsilon(k_1, k_2)\, e_{k_1 \oplus k_2},$$

which has real part $\alpha_{k_1} = \pm 1 \neq 0$. Setting $m := k_1 \oplus k_2 \geq 1$ and $\sigma := -\alpha_{k_1}\alpha_{k_2}\varepsilon(k_1, k_2)$: $u\alpha = \alpha_{k_1}(e_0 + \sigma e_m)$, so α is left-associate to $\pm(e_0 + \sigma e_m)$, which is a Case $\alpha_0 \neq 0$ element indexed by m. Hence every Case $\alpha_0 = 0$ factorisation belongs to the same equivalence class as some $(1+e_m)(1-e_m)$, and generates no new class.

Case $\alpha_0 \neq 0$ (i.e., $\alpha_0 = \pm 1$): $\alpha = \pm e_0 + a e_j$ for some $j \geq 1$, $a = \pm 1$. Then $\beta = \bar{\alpha} = \pm e_0 - a e_j$ (the CD conjugate), and $\alpha\beta = \alpha\bar{\alpha} = N(\alpha) e_0 = 2e_0$. ✓

Up to unit equivalence ($\alpha \mapsto -\alpha$ gives the same unordered factorisation), the distinct factorisations are indexed by $j = 1, \ldots, 2^n - 1$, giving exactly $2^n - 1$. □

Remark 3.6 (Connection to finite geometry). The count $2^n - 1$ equals $|\mathbb{F}_2^n \setminus \{0\}|$, the number of nonzero vectors in $\mathbb{F}_2^n$, equivalently the number of points in the projective space $PG(n-1, \mathbb{F}_2)$. For $n = 2$: 3 points (projective line); for $n = 3$: 7 points (the Fano plane $PG(2, \mathbb{F}_2)$). This is the same count that appears in the zero-divisor formula $|ZD(n)| = 336 \cdot \binom{n-1}{3}_2$ via the Fano plane structure established in [4]: both the UFD failure witness (factorisations of 2) and the zero-divisor count share the same finite-geometric origin.

Example 3.7 (UFD failure at $n = 2$, in S_2)**.** The $2^2 - 1 = 3$ factorisations of Proposition 3.5 give:

$$2 = (1+e_1)(1-e_1) = (1+e_2)(1-e_2) = (1+e_3)(1-e_3).$$

Each factor has norm 2 and is irreducible in $L_{\mathbb{Z}}$. The missing Hurwitz unit $\frac{1+e_1+e_2+e_3}{2} \notin S_2$ is what prevents uniqueness; in $H_{\mathbb{Z}}$ it is available and uniqueness is restored [2].

This shows that the *UFD threshold* ($n = 2$ within S_n) is strictly earlier than the *domain threshold* ($n = 4$); see Corollary 3.3 for the complete picture.

Theorem 3.8 (Norm-multiplicativity threshold). *$N(ab) = N(a)N(b)$ for all $a, b \in S_n$ if and only if $n \leq 3$. For $n \geq 4$ and any $(a, b) \in \mathrm{ZD}(n)$:*

$$N(a)N(b) - N(ab) = 4.$$

Proof. The direction $n \leq 3$ is Hurwitz [3]. For $n \geq 4$: by [4, Cor 3.4] every $(a, b) \in \mathrm{ZD}(n)$ satisfies $N(a) = N(b) = 2$, and $N(ab) = 0$ by definition, giving the gap 4. □

4. Norm-Multiplicativity and the Sum-of-Squares Chain

Theorem 4.1 (Sum-of-squares chain). *The following are equivalent for each $n \in \{0, 1, 2, 3\}$:*

(i) $\mathcal{A}_n$ is a normed division algebra;
(ii) $N(ab) = N(a)N(b)$ for all $a, b \in \mathcal{A}_n$;
(iii) there exists a bilinear composition identity $\left(\sum_{k=1}^{2^n} x_k^2\right)\left(\sum_{k=1}^{2^n} y_k^2\right) = \sum_{k=1}^{2^n} z_k^2$, where each z_k is bilinear in $(x_1, \ldots)$ and $(y_1, \ldots)$.

For $n \geq 4$, none of (i)–(iii) *holds.*

Proof. The equivalence of (i) and (ii) is standard. The equivalence of (ii) and (iii), and the impossibility for $n \geq 4$, is Hurwitz's 1898 theorem [3]. □

Table 2 records the four classical identities and their arithmetic consequences.

Table 2. The sum-of-squares chain and its number-theoretic content.

n	Identity	Source	Arithmetic consequence
0	$a^2 \cdot b^2 = (ab)^2$	trivial	$\mathbb{Z}$ is a PID
1	$\left(\sum_2 x_i^2\right)\left(\sum_2 y_i^2\right) = \sum_2 z_i^2$	Brahmagupta–Fibonacci	Fermat two-square theorem
2	$\left(\sum_4 x_i^2\right)\left(\sum_4 y_i^2\right) = \sum_4 z_i^2$	Euler (1748)	Lagrange four-square theorem
3	$\left(\sum_8 x_i^2\right)\left(\sum_8 y_i^2\right) = \sum_8 z_i^2$	Degen–Graves–Cayley	Degen eight-square identity
≥ 4	*does not exist*	Hurwitz (1898)	domain property fails

Remark 4.2 (Born Rule restatement). By [4, Thm 10.2], N is the unique function $\mathcal{A}_n \to \mathbb{R}_{\geq 0}$ satisfying multiplicativity (M), positivity (D), and orthogonal additivity (OA) for $n \leq 3$; no such function exists for $n \geq 4$.

Corollary 4.3 (Behaviour of rational primes). *The factorisation of a rational prime p in S_n is governed by the corresponding composition identity:*

(i) $n = 1$: p splits in $S_1 = \mathbb{Z}[i]$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$ (Fermat–Euler).
(ii) $n = 2$: p is a sum of four squares for all p (Lagrange), giving Hurwitz primes of norm p in $H_{\mathbb{Z}} \supset S_2$.

(iii) $n = 3$*: the Degen–Graves–Cayley eight-square identity is a* composition *result — the product of two sums of* 8 *squares is again a sum of* 8 *squares — implying that the set of norms of elements of* S_3 *is closed under multiplication. The factorisation of* p *in the maximal Coxeter–Dickson order* $O_{\mathbb{Z}}$ *uses this structure, but is more subtle than the* $n = 1, 2$ *cases; see* [1] *and Problem 7.6.*

(iv) $n \geq 4$*: no norm-based factorisation of rational primes in* S_n *is consistent with the zero-divisor structure.*

Remark 4.4. Every positive integer is a sum of 8 squares (since it is a sum of 4 squares by Lagrange, and one can append four zeros); this is a trivial consequence of Lagrange's theorem and is independent of the eight-square identity. The identity's content is *closure*: if x and y are norms of octonion integers, so is xy.

5. Arithmetic Structure of ZD-Active Elements in S_n, $n \geq 4$

We investigate what products can and cannot involve ZD-active elements, and what the right annihilator structure reveals about the domain failure. The results fall into two groups: a norm-level obstruction showing what products *cannot* occur (Lemma 5.2), and an annihilator witness showing the precise shape of the failure (Theorem 5.8).

Throughout this section: $n \geq 4$, $a = e_i + \sigma e_j \in C^*(n)$ with $(a, b) \in \mathrm{ZD}(n)$, and $v_0 = i \oplus j$ (the common XOR value of both pairs, using [4, Thm 3.6]).

5.1. **The Norm-2 Product Obstruction.**

Lemma 5.1 (Norm formula for a weight-2 left factor)**.** *For* $a = e_i + \sigma e_j \in C(n)$ *and any* $\beta \in S_n$*:*

$$N(a\beta) \;=\; 2N(\beta) + 2\sigma\,\langle e_i\beta,\, e_j\beta\rangle,$$

where $\langle x,\, y\rangle = \mathrm{Re}(\bar{x}y)$*.*

Proof. The inner product $\langle x,\, y\rangle = \mathrm{Re}(\bar{x}y) = \sum_v x_v y_v$ is symmetric: using $\overline{ab} = \bar{b}\bar{a}$ and $\bar{\bar{x}} = x$,

$$\mathrm{Re}(\bar{x}y) = \tfrac{1}{2}\big(\bar{x}y + \overline{\bar{x}y}\big) = \tfrac{1}{2}\big(\bar{x}y + \bar{y}x\big) = \mathrm{Re}(\bar{y}x),$$

so $\langle x,\, y\rangle = \langle y,\, x\rangle$ for all $x, y \in \mathcal{A}_n$. Consequently the polarization identity for $N = \sum_v (\cdot)_v^2$ gives a symmetric cross term:

$$\begin{aligned} N(e_i\beta + \sigma e_j\beta) &= N(e_i\beta) + N(\sigma e_j\beta) + \langle e_i\beta,\, \sigma e_j\beta\rangle + \langle \sigma e_j\beta,\, e_i\beta\rangle \\ &= N(e_i\beta) + N(e_j\beta) + 2\sigma\langle e_i\beta,\, e_j\beta\rangle. \end{aligned}$$

By the Isometry Lemma [4, Thm 3.3]: $N(e_k x) = N(x)$ for all $x \in \mathcal{A}_n$, $e_k \in \mathcal{B}_n$. Hence both norms equal $N(\beta)$. □

Lemma 5.2 (Norm-2 product obstruction)**.** *For any* $\alpha, \beta \in C(n)$ *(both of norm* 2*):*

$$N(\alpha\beta) \in \{0,\, 4,\, 8\}.$$

In particular, if $\alpha\beta \neq 0$ *then* $N(\alpha\beta) \geq 4$*; no product of two norm-*2 *elements can be a nonzero norm-*2 *element.*

Proof. Write $\alpha = e_i + \sigma e_j$, $\beta = e_k + \tau e_l$. By the $\{0, 4, 8\}$ Trichotomy [4, Thm 3.6]: $N(\alpha\beta) \in \{0, 4, 8\}$. Since $N(c) = 2$ for every $c \in C(n)$ and $2 \notin \{0, 4, 8\}$, no product of two elements of $C(n)$ lies in $C(n)$. □

Corollary 5.3. *Let* $a \in C^*(n)$ *be ZD-active and* $(a, b) \in \mathrm{ZD}(n)$*. There is no factorization* $a = \alpha\beta$ *with* $\alpha, \beta \in C(n)$*.*

5.2. Inner Product Parity.

Lemma 5.4 (Parity of the inner product). *For any $\beta \in S_n$, the inner product $\langle e_i\beta,\, e_j\beta\rangle$ is always an even integer. Consequently:*

$$N(a\beta) \;\equiv\; 2N(\beta) \pmod 4.$$

In particular, for $N(a\beta) = 2$ it is necessary that $N(\beta)$ be odd.

Proof. Write $\beta = \sum_u \beta_u e_u$. Expanding the inner product:

$$\langle e_i\beta,\, e_j\beta\rangle = \sum_u \beta_u\, \beta_{u\oplus v_0} \cdot \varepsilon(i,u)\, \varepsilon(j, u\oplus v_0).$$

We reorganise this sum by grouping indices into unordered pairs $\{u,\, u \oplus v_0\}$ (noting $v_0 \neq 0$ since $i \neq j$, so $u \neq u \oplus v_0$). For each such pair, the two terms in the sum are:

$$\begin{aligned} &\text{at } u\colon \quad \beta_u\, \beta_{u\oplus v_0} \cdot \varepsilon(i,u)\varepsilon(j,u\oplus v_0),\\ &\text{at } u\oplus v_0\colon \quad \beta_{u\oplus v_0}\, \beta_u \cdot \varepsilon(i,u\oplus v_0)\varepsilon(j,u). \end{aligned}$$

Their sum is $\beta_u\beta_{u\oplus v_0} \cdot d_u$, where

$$d_u := \varepsilon(i,u)\varepsilon(j,u\oplus v_0) + \varepsilon(i,u\oplus v_0)\varepsilon(j,u) \;\in\; \{-2,\, 0,\, +2\}$$

is the spectral coefficient of $S_{ij} := L_{e_i}L_{e_j} + L_{e_j}L_{e_i}$ on the pair $\{u, u\oplus v_0\}$ (see [4, Lem 5.15]). Summing over all unordered pairs gives:

$$\langle e_i\beta,\, e_j\beta\rangle = \sum_{\{u,\, u\oplus v_0\}} \beta_u\, \beta_{u\oplus v_0} \cdot d_u.$$

Each term is an integer ($\beta_u, \beta_{u\oplus v_0} \in \mathbb{Z}$) times an element of $\{-2, 0, +2\}$, hence even. The total is therefore an even integer. The parity of $N(a\beta)$ follows from Lemma 5.1. ☐

Corollary 5.5. *For $\beta \in C(n)$ (norm 2, hence even): $N(a\beta) = 2$ is impossible. This recovers Corollary 5.3 by a different route.*

5.3. The WRAP-Based Computation and ZD Self-Factorization.

Lemma 5.6 (Product $a(a\gamma)$ via WRAP). *For $a = e_i + \sigma e_j \in C^*(n)$ and any $\gamma \in S_n$:*

$$a(a\gamma) \;=\; -2\gamma + \sigma\, S_{ij}(\gamma),$$

where $S_{ij} = L_{e_i}L_{e_j} + L_{e_j}L_{e_i}$.

Proof. Expand by bilinearity:

$$a(a\gamma) = (e_i + \sigma e_j)(e_i\gamma + \sigma e_j\gamma) = e_i(e_i\gamma) + \sigma e_j(e_i\gamma) + \sigma e_i(e_j\gamma) + e_j(e_j\gamma).$$

By the WRAP identity [4, Thm 4.5]: $e_k(e_k x) = -x$ for all $x \in \mathcal{A}_n$ and all $k \geq 1$. Hence $e_i(e_i\gamma) = e_j(e_j\gamma) = -\gamma$. The remaining two terms combine to $\sigma(L_{e_j}L_{e_i} + L_{e_i}L_{e_j})(\gamma) = \sigma S_{ij}(\gamma)$. ☐

Remark 5.7 (The associator). Since $a \in C^*(n)$ has $i, j \geq 1$, its real part $a_0 = 0$ (purely imaginary), so $a^2 = -N(a)e_0 = -2e_0$. Lemma 5.6 then immediately yields the associator:

$$[a,a,\gamma] = (a^2)\gamma - a(a\gamma) = -2\gamma - \big(-2\gamma + \sigma S_{ij}(\gamma)\big) = -\sigma\, S_{ij}(\gamma).$$

This is generally nonzero in S_n ($n \geq 4$) since S_{ij} has non-trivial active eigenspaces [4, Thm 5.16]. In particular, the naive step "$(a^2)\gamma = a(a\gamma)$" requires $[a,a,\gamma] = 0$ and is *invalid* in S_n for $n \geq 4$ without further hypotheses.

Theorem 5.8 (Non-unit right annihilator complement)**.** *Let $n \geq 4$ and $(a,b) \in \mathrm{ZD}(n)$. Set $\gamma_b := e_0 + b \in S_n$. Then:*

(i) $N(\gamma_b) = 3$ (non-unit)*;*
(ii) $a \cdot \gamma_b = a$*, equivalently* $b \in \mathrm{rann}_{S_n}(a)$*;*
(iii) $\mathrm{rann}_{S_n}(a) \neq \{0\}$*: the right annihilator of a in S_n contains elements of norm 2. In any integral domain,* $\mathrm{rann}_R(a) = \{0\}$ *for all $a \neq 0$.*

Proof. (i) Since $b \in C^*(n)$ is index-pure ($b_0 = 0$): $N(e_0 + b) = N(e_0) + N(b) = 1 + 2 = 3$. Neither a (norm 2) nor γ_b (norm 3) is a unit.

(ii) By bilinearity (no associativity required): $a(e_0 + b) = ae_0 + ab = a + 0 = a$. The identity $a\gamma_b = a$ is equivalent to $ab = 0$, which is exactly the statement $b \in \mathrm{rann}_{S_n}(a)$.

(iii) $b \in \mathrm{rann}_{S_n}(a)$ by definition of $\mathrm{ZD}(n)$, and $N(b) = 2$ by [4, Cor 3.4], so b is a non-unit in $\mathrm{rann}_{S_n}(a)$. The domain comparison is immediate: in a domain, $ax = 0$ forces $x = 0$ since $a \neq 0$. □

Remark 5.9 (Structure of the right annihilator)*.* The identity $a\gamma_b = a$ is not a factorization of a in the arithmetic sense: it is a consequence of the ZD relation $ab = 0$ via distributivity, and says precisely that $\gamma_b - e_0 = b \in \mathrm{rann}_{S_n}(a)$. The content of Theorem 5.8 is therefore an *annihilator statement*: the right annihilator of a in S_n is non-trivial, containing non-units of norm 2. This is a direct and elementary witness to the failure of the domain property, entirely independent of any notion of irreducibility (which is ill-defined for zero-divisors).

Corollary 5.10 (Zero-divisors preclude classical primality)**.** *In S_n ($n \geq 4$), every ZD-active element $a \in C^*(n)$ is a* zero-divisor*: $\exists\, b \neq 0$ with $ab = 0$. In ring theory, prime elements are regular (non-zero-divisors) in any domain; since a is a zero-divisor, no notion of "prime element" in the classical domain-theoretic sense applies to a.*

5.4. **Summary of Arithmetic Structure.** Table 3 summarises the results of this section.

Table 3. Arithmetic properties of ZD-active elements $a \in C^*(n)$ for $n \geq 4$.

Property	Status	Key tool
a is a zero-divisor	✓ Proved	Def. + [4, Thm 7.16]
$\mathrm{rann}_{S_n}(a) \neq \{0\}$	✓ Proved (Thm 5.8)	$b \in \mathrm{rann}_{S_n}(a)$, $N(b) = 2$
$a = \alpha\beta$, $\alpha, \beta \in C(n)$	× Impossible (Lem. 5.2)	$\{0, 4, 8\}$ Trichotomy
$b \in aS_n$	**Open** (Prob. 7.3)	Parity: $N(c)$ odd ≥ 3
a prime (classical sense)	× Not applicable	Cor. 5.10

6. Explicit Example in S_4

We verify the main results of Section 5 for a concrete pair in S_4.

Setup. In $\mathcal{A}_4$ (sedenions, dimension 16), take:

$$a = e_1 + e_{10}, \qquad b = e_4 - e_7.$$

The pair $(a, b) \in \mathrm{ZD}(4)$ is confirmed by the explicit classification of [4, §14].

Norms. $N(a) = 1+1 = 2, \quad N(b) = 1+1 = 2, \quad N(ab) = 0$. Norm gap: $N(a)N(b) - N(ab) = 4$. ✓

Norm-2 product obstruction (Lemma 5.2). Since $N(a) = N(b) = 2$, neither can arise as a product of two elements of $C(4)$. ✓

Right annihilator witness (Theorem 5.8).

$$\gamma_b = e_0 + e_4 - e_7, \qquad N(\gamma_b) = 1 + 1 + 1 = 3.$$

By bilinearity and $ab = 0$: $a \cdot \gamma_b = a(e_0 + b) = a + ab = a$. Hence $b = \gamma_b - e_0 \in \mathrm{rann}_{S_4}(a)$, $N(b) = 2$, non-unit. ✓

WRAP computation (Lemma 5.6). For $\gamma = e_0$ (identity):

$$a^2 = a(a \cdot e_0) = -2e_0 + S_{1,10}(e_0).$$

Since $e_0 = 1$: $L_{e_1}(e_0) = e_1$, $L_{e_{10}}(e_1) = \varepsilon(10, 1)e_{11}$; and $L_{e_{10}}(e_0) = e_{10}$, $L_{e_1}(e_{10}) = \varepsilon(1, 10)e_{11}$. By anti-commutativity $\varepsilon(10, 1) = -\varepsilon(1, 10)$: $S_{1,10}(e_0) = [\varepsilon(1, 10) + \varepsilon(10, 1)]e_{11} = 0$. Hence $a^2 = -2e_0$, consistent with the general formula $a^2 = -N(a)e_0$ for purely imaginary a. ✓

Parity check (Lemma 5.4). $N(\gamma_b) = 3$ is odd, consistent with the necessary condition for $N(a\gamma_b) = 2$. ✓

7. Open Problems

Remark 7.1 (Computational verification for $n = 4$). An exhaustive search over all $\alpha, \beta \in S_4$ with $2 \leq N(\alpha) \leq 4$ (29 152 candidates for $N = 4$, verified against all solutions via left-multiplication matrices) confirms the following. The factorisation $2 = \alpha\beta$ in S_4 with neither factor a unit occurs in exactly two norm-types:

(i) $N(\alpha) = N(\beta) = 2$: 480 ordered pairs, $15 = 2^4 - 1$ equivalence classes under the unit group $\{\pm e_v\}$. All are associate to the standard family $(1 + e_k)(1 - e_k)$, $k = 1, \ldots, 15$.
(ii) $N(\alpha) = 4$, $N(\beta) = 2$: 118 ordered pairs, 35 equivalence classes under $\{\pm e_v\}$. In every case both α and β are index-pure (no e_0-component) [VERIFIED computationally], and β is a ZD-active element of $C^*(4)$. These factorisations do not arise for $n \leq 3$, where norm-multiplicativity forces $N(\alpha) = N(\beta) = 2$.

No factorisations with $N(\alpha) = N(\beta) = 4$, $N(\alpha) = 3$, or $N \geq 5$ were found. The $N = (2, 2)$ family gives exactly 15 equivalence classes, consistent with Proposition 3.5(i) at $n = 4$. The 35 additional classes from $N = (4, 2)$ show that the total count of equivalence classes for $n = 4$ is at least 50, confirming that Proposition 3.5(ii) cannot be upgraded to "exactly".

Problem 7.2 (Structure of $N = (4, 2)$ factorisations for $n \geq 4$)**.** The data in Remark 7.1 shows 118 ordered factorisations $2 = \alpha\beta$ in S_4 with $N(\alpha) = 4$, $N(\beta) = 2$ (ZD-active). Two questions remain open:

(i) How many equivalence classes (under the unit group) do these $N = (4, 2)$ factorisations form, and what is the complete structure of the index-pure α of norm 4?
(ii) For $n \geq 5$: do $N = (4, 2)$ factorisations persist, and are there new norm-types? The search bound $N(\alpha) \leq 4$ used here does not cover $n \geq 5$ exhaustively.

Problem 7.3 (Left-divisibility in ZD pairs)**.** Given $(a, b) \in \mathrm{ZD}(n)$: does there exist $c \in S_n$ with $b = ac$? By Lemma 5.4, any such c must have odd norm $N(c)$. The case $N(c) = 3$ requires $\sigma\langle e_i c, e_j c\rangle = 1 - N(c) = -2$, which forces $\langle e_i c, e_j c\rangle = \mp 2$. A complete answer requires explicit analysis of the linear system $(e_i + \sigma e_j)c = e_k + \tau e_l$ over $\mathbb{Z}$ with $N(c) = 3$.

Problem 7.4 (Higher-weight elements of S_4)**.** Theorem 5.8 characterises factorizations of ZD-active elements (norm 2). Elements of S_4 with $N \geq 4$ are not ZD-active (by [4, Cor 3.4]). What is their factorization structure? In particular, are elements of the form $e_0 + a$ (norm 3, with a ZD-active) atoms in S_4?

Problem 7.5 (Multiplicative forms)**.** By Hurwitz [3], no bilinear composition identity $(\sum_{16} x_i^2)(\sum_{16} y_i^2) = \sum_{16} z_i^2$ exists. Is there a non-bilinear multiplicative form $f : S_4 \to \mathbb{Z}$ with $f(ab) = f(a)f(b)$ for all a, b where neither a nor b is ZD-active?

Problem 7.6 (Rational primes in S_4/pS_4)**.** For a rational prime p, what is the structure of the image of ZD(4) in S_4/pS_4? Does the factorisation depend on $p \pmod 8$ or $p \pmod 7$, in analogy with the $p \pmod 4$ dependence in $\mathbb{Z}[i]$?

Problem 7.7 (Maximal order for $n = 4$)**.** The Gravesian integers S_3 are a strict subring of the Coxeter–Dickson maximal order $O_{\mathbb{Z}}$, analogously to $L_{\mathbb{Z}} \subsetneq H_{\mathbb{Z}}$. Does any maximal order in $\mathcal{A}_4$ remain an integral domain? Theorem 3.1 implies the answer is no (the domain property is an intrinsic property of $\mathcal{A}_4$, independent of the chosen order), but the explicit obstruction at the maximal-order level deserves a formal statement.

Acknowledgements

The author thanks Claude (Anthropic) for assistance with algebraic verification, proof development, and LaTeX editing.

References

[1] J. H. Conway and D. A. Smith. *On Quaternions and Octonions.* A K Peters, Natick, MA, 2003.

[2] A. Hurwitz. Ueber die Zahlentheorie der Quaternionen. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen*, pages 313–340, 1896.

[3] A. Hurwitz. Ueber die Composition der quadratischen Formen von beliebig vielen Variabeln. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen*, pages 309–316, 1898.

[4] G. Levratti. Sign-Parity Classification of Zero Divisors in Cayley–Dickson Algebras. Zenodo preprint (2026), doi:10.5281/zenodo.20315751.

[5] R. D. Schafer. *An Introduction to Nonassociative Algebras.* Academic Press, New York, 1966.

Independent Researcher, Modena, Italy
Email address: giovanni.levratti.research@gmail.com