Ideals in the Integral Octaves

Daniel Allcock*

12 March 1998, revised 9 May 1998

allcock@math.utah.edu

web page: *http://www.math.utah.edu/∼allcock*

Department of Mathematics

University of Utah

Salt Lake City, UT 84112.

Abstract.

We study the nonassociative ring of integral octaves (or Cayley numbers or octonions) discovered independently by Dickson and Coxeter. We prove that every one-sided ideal is in fact two-sided, principal, and generated by a rational integer.

1 Introduction

The nonassociative ring $\mathcal{K}$ of integral octaves is a discrete subring of the nonassociative field $\mathbb{O}$ of octaves—it is the natural analogue of the the rational integers in $\mathbb{Z}$. Dickson introduced $\mathcal{K}$ in [4]; one can use $\mathcal{K}$ to construct the finite simple groups now called $G_2(p)$ for p a prime number. Much later, Coxeter [3] rediscovered the ring and obtained a number of new results concerning it. The purpose of this note is to obtain a complete description of the ideals in $\mathcal{K}$: every one-sided ideal is actually two-sided and generated by a rational integer. This substantially improves a result of Mahler [5], who proved that any one-sided ideal is generated by a rational integer multiple of an element of one of three possible norms. Our arguments rely on geometric properties of the E_8 lattice and its automorphism group, rather than the sort of explicit computation that Mahler used.

Our definitions of $\mathbb{O}$ and $\mathcal{K}$ are those of [1, p. 85]. The nonassociative field $\mathbb{O}$ of octaves is an 8-dimensional algebra over the real numbers $\mathbb{R}$, with basis $e_\infty = 1$, $e_0, \ldots, e_6$. Multiplication is defined by the relations that for each $n = 0, \ldots, 6$, $e_n^2 = -1$ and the span of e_∞, e_n, e_{n+1} and e_{n+3} is a copy of the the (associative) field of quaternions, with $e_n e_{n+1} e_{n+3} = -1$. Here the subscripts should be read modulo 7. If $x = x_\infty e_\infty + x_0 e_0 + \cdots + x_6 e_6$ with each $x_n \in \mathbb{R}$ then the conjugate of x is $\bar{x} = x_\infty e_\infty - x_0 e_0 - \cdots - x_6 e_6$. The absolute value $|x|$ of x is $\sqrt{x\bar{x}}$, which is a nonnegative real number; $|x| = 0$ just if $x = 0$. The identity $|xy| = |x|\,|y|$ (for any $x, y \in \mathbb{O}$) is important for the proof of theorem 1.1. The real part of x is x_∞; if this vanishes then we say that x is imaginary.

* Supported by an NSF postdoctoral fellowship.

The integral octaves $\mathcal{K}$ are the discrete subring of $\mathbb{O}$ consisting of those $x = \sum x_n e_n$ satisfying $x_n \in \frac{1}{2}\mathbb{Z}$ for all $n = \infty, 0, \ldots, 6$ and that the set of n for which $x_n \notin \mathbb{Z}$ is one of

$$\{0124\}, \quad \{0235\}, \quad \{0346\}, \quad \{0156\},$$
$$\{\infty 013\}, \quad \{\infty 026\}, \quad \{\infty 045\}, \quad \{\infty 0123456\},$$

or the complement of one of these. One may check [3] that $\mathcal{K}$ is closed under addition and multiplication. Furthermore, if $x \in \mathcal{K}$ then $|x|^2 \in \mathbb{Z}$, and under the metric on $\mathcal{K}$ induced by the absolute value function, $\mathcal{K}$ is a scaled copy of the E_8 lattice [2, ch. 4, §8.1]. In particular, the minimal distance between elements of $\mathcal{K}$ is 1 and the covering radius of $\mathcal{K}$ is $1/\sqrt{2}$. (This means that every element of $\mathbb{O}$ lies within $1/\sqrt{2}$ of $\mathcal{K}$ and that $1/\sqrt{2}$ is the smallest number for which this holds.) There are 240 elements of $\mathcal{K}$ of absolute value 1, which are the units of $\mathcal{K}$. We denote the set of these by $\mathcal{K}^\times$.

The first step in applying the geometry of the E_8 lattice to the study of ideals in $\mathcal{K}$ is the following theorem and its corollary.

Theorem 1.1 [3] [5]. *The function $x \mapsto |x|^2$ is a Euclidean norm on $\mathcal{K}$.*

Remark: By this we mean that for all $x, m \in \mathcal{K}$ there are $q, r \in \mathcal{K}$ such that $x = qm + r$ with $|r|^2 < |m|^2$, and that there are also $q', r' \in \mathcal{K}$ such that $x = mq' + r'$ with $|r'|^2 < |m|^2$.

Proof: In the notation of the remark, let $q \in \mathcal{K}$ by such that qm is an element of $\mathcal{K}m$ nearest x, and let $r = x - qm$. The right-multiplication map of m increases distances by a factor of $|m|$, so $\mathcal{K}m$ has covering radius $|m|/\sqrt{2}$. Therefore $|r| \leq |m|/\sqrt{2}$. A similar argument applied to $m\mathcal{K}$ completes the proof. □

Corrollary 1.2. *Any left (resp. right) ideal in $\mathcal{K}$ has the form $\mathcal{K}m$ (resp. $m\mathcal{K}$) for some $m \in \mathcal{K}$.*

Proof: This follows from the usual argument that a Euclidean domain is a principal ideal domain. □

Of course, since $\mathcal{K}$ is not associative, if m is a random integral octave then $\mathcal{K}m$ and $m\mathcal{K}$ might fail to be ideals. Our main theorem is essentially the assertion that $\mathcal{K}m$ or $m\mathcal{K}$ is an ideal if and only if m is a product of a rational integer and a unit of $\mathcal{K}$:

Theorem 3.1. *Any one-sided ideal $\mathcal{I}$ in $\mathcal{K}$ is two-sided, principal, and has the form $\mathcal{K}n = n\mathcal{K}$ for some rational integer n.*

In order to prove the theorem we need to identify the group generated by the left (or right)

multiplication maps of units of $\mathcal{K}$. We do this in the next section, and prove the theorem in section 3.

2. Triality

The best way to understand the group generated by the left (or right) multiplication maps of units of $\mathcal{K}$ is by considering the "isotopy" group of $\mathcal{K}$ and its "triality" automorphism. An isotopy is a triple (A, B, C) of $\mathbb{Z}$-linear maps of $\mathcal{K}$ such that for all $x, y, z \in \mathcal{K}$, the equation $xyz = 1$ holds just if $A(x)B(y)C(z) = 1$ holds. These equations make sense because if either $xy \cdot z = 1$ or $x \cdot yz = 1$ then x, y and z all lie in an associative algebra, so that xyz is unambiguously defined and equal to 1. The product of two isotopies is defined by

$$(A, B, C)(A', B', C') = (A \circ A', B \circ B', C \circ C').$$

By [1, p. 85], the group of isotopies is isomorphic to an extension 2^2G of the simple group $G = O_8^+(2)$. Furthermore, 2^2G is generated by the triples (L_u, R_u, B_u) for $u \in \mathcal{K}^\times$, where L_u (resp. R_u) is the map given by left (resp. right) multiplication by u, and B_u is the "bimultiplication" map $x \mapsto u^{-1}xu^{-1}$. The fact that (L_u, R_u, B_u) is an isotopy follows from the Moufang identity: $u(xy)u = (ux)(yu)$ for all $u, x, y \in \mathbb{O}$. For each $u \in \mathbb{O} \setminus \{0\}$ the maps L_u, R_u and B_u are orientation-preserving maps of $\mathbb{O}$, since this is obviously true for $u = 1$ and $\mathbb{O} \setminus \{0\}$ is connected. This implies that there are three different maps π_0, π_1 and π_2 from 2^2G to the rotation group of $\mathcal{K}$; these carry (A, B, C) to A, B and C, respectively. By the rotation group of $\mathcal{K}$ we mean the full group of orientation-preserving isometries of $\mathcal{K}$; this is the commutator subgroup of the E_8 Weyl group. It is a central extension $2G$ of $O_8^+(2)$. Finally, the description of 2^2G in terms of isotopies makes visible the "triality" automorphism $\tau : (A, B, C) \mapsto (B, C, A)$. It is obvious that $\pi_m \circ \tau^n = \pi_{m+n}$, where the subscripts should be read modulo 3.

We define H to be the subgroup of 2^2G generated by those triples (L_u, R_u, B_u) with $u \in \operatorname{Im}\mathcal{K}^\times$, and we set $H_\ell = \pi_0(H)$, $H_r = \pi_1(H)$ and $H_b = \pi_2(H)$. That is, H_ℓ, H_r and H_b are respectively the subgroups of $2G$ generated by the left, right and bimultiplication maps of elements of $\operatorname{Im}\mathcal{K}^\times$.

Lemma 2.1. *H_b is a maximal subgroup of $2G$ and preserves $\{\pm 1\}$.*

Proof: For $u \in \operatorname{Im}\mathcal{K}^\times$ it is easy to check that B_u negates 1 and u and fixes $u^\perp \cap \operatorname{Im}\mathbb{O}$ pointwise. (This uses the fact that orthogonal imaginary octaves anticommute.) Therefore H_b acts on $\operatorname{Im}\mathcal{K}$ as the E_7 Weyl group, since $\operatorname{Im}\mathcal{K}$ is a copy of the E_7 lattice, being the orthogonal complement of a minimal vector in a copy of the E_8 lattice. Furthermore, an element of H_b exchanges 1 and -1

just if it reverses orientation on $\mathrm{Im}\,\mathbb{O}$. Therefore H_b is isomorphic to the E_7 Weyl group, and a computation reveals that $|2G|/|H_b| = 120$. The maximality follows because by [1, p. 85], G has no proper subgroups of index < 120. □

Lemma 2.2. *The maps L_u (or alternately, the R_u or the B_u), for $u \in \mathcal{K}^\times$, generate all of $2G$.*

Proof: By lemma 2.1, H_b is a maximal subgroup of $2G$. Since there are $u \in \mathcal{K}^\times$ such that $B_u(1) \notin \{\pm 1\}$, the group generated by all the B_u is all of $2G$. This is just the assertion that $\pi_2(2^2G) = 2G$. By triality, we see that each of $\pi_0(2^2G)$ and $\pi_1(2^2G)$ is also all of $2G$. The lemma follows. □

We remark the the groups 2^2G and H are respectively $\mathrm{Spin}_8^+(\mathbb{F}_2)$, the universal central extension of $O_8^+(2)$, and $\mathrm{Pin}_7(\mathbb{F}_2)$, the direct product of $\mathbb{Z}/2$ and the universal central extension of $O_7(2)$. Furthermore, the groups H_b, H_ℓ and H_r are isomorphic to $2 \times O_7(2)$, $\mathrm{Spin}_7(\mathbb{F}_2)$ and $\mathrm{Spin}_7(\mathbb{F}_2)$. One may also consider the isotopy group of $\mathbb{O}$ and the obvious analogues of H, H_b, H_ℓ and H_r. These five groups (after discarding Euclidean factors) are respectively isomorphic to $\mathrm{Spin}_8(\mathbb{R})$, $\mathrm{Pin}_7(\mathbb{R})$, $O_7(\mathbb{R})$, $\mathrm{Spin}_7(\mathbb{R})$ and $\mathrm{Spin}_7(\mathbb{R})$. It is remarkable that the exceptional phenomena (triality, etc.) arising in the $\mathbb{F}_2$-versions of these groups can be "embedded" in the real versions. In particular, the triality automorphism τ acts in both cases as the order-three automorphism of the Dynkin diagram D_4, the Dynkin diagram of an orthogonal group in 8 dimensions.

3. The main theorem

The proof of our main theorem is now quite short. We continue using the notation of section 2.

Theorem 3.1. *Any one-sided ideal $\mathcal{I}$ in $\mathcal{K}$ is two-sided, principal, and has the form $\mathcal{K}n = n\mathcal{K}$ for some rational integer n.*

Proof: The result for right ideals follows formally from that for left ideals, since the identity $\overline{xy} = \bar{y}\bar{x}$ (for any $x, y \in \mathbb{O}$) implies that the conjugate of a right ideal is a left ideal. So suppose $\mathcal{I}$ is a nonzero left ideal. By corollary 1.2 we have $\mathcal{I} = \mathcal{K}m$ where m is some minimal (nonzero) element of $\mathcal{I}$. Since $\mathcal{I}$ is a left ideal it is preserved by the group generated by the maps L_u for $u \in \mathcal{K}^\times$. If $\mathcal{K}$ were associative then this group would have order 240. But $\mathcal{K}$ is not, and by lemma 2.2, the group is the full rotation group $2G$ of $\mathcal{K}$. Observe that $\mathcal{I}$ has 240 minimal vectors, namely the vectors um for $u \in \mathcal{K}^\times$. It is obvious that group generated by the L_u acts transitively on these, so the subgroup preserving m has index 240 and order 1,451,520. The only elements of the E_8 lattice with a stabilizer this large are the rational integral multiples of minimal lattice vectors. One

sees this by considering the full isometry group of $\mathcal{K}$, the E_8 Weyl group. The stabilizer of any vector is (conjugate to) a Weyl group corresponding to a subdiagram of the E_8 Dynkin diagram. The only subdiagram whose associated Weyl group is large enough is the (unique) E_7 subdiagram. The conjugates of this subgroup are just the stabilizers of the various minimal vectors u of the lattice. For each such u, the only vectors stabilized by the stabilizer of u are the real multiples of u. Therefore $m = un$ for some $u \in \mathcal{K}^\times$, $n \in \mathbb{Z}$. Then $\mathcal{I} = \mathcal{K}m = \mathcal{K} \cdot un = \mathcal{K}n$ and the proof is complete. □

References

[1] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *ATLAS of Finite Groups*. Oxford, 1985.

[2] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices, and Groups*. Springer-Verlag, 1988.

[3] H. S. M. Coxeter. Integral Cayley numbers. *Duke Math. J.*, 13:561–78, 1946.

[4] L. E. Dickson. A new simple theory of hypercomplex integers. *Journal de Mathématiques Pures et Appliquées*, 2:281–326, 1923.

[5] K. Mahler. On ideals in the Cayley-Dickson algebra. *Proc. Roy. Irish Acad.*, 48:123–133, 1943.