ARITHMETICS IN CAYLEY'S ALGEBRA

by P. J. C. LAMONT

(Received 15 October, 1962)

1. Introduction. Let C denote Cayley's algebra defined over the field of rational numbers. This paper contains a simple characterization of arithmetics of C in terms of a given basis $i_0 = 1, i_1, i_2, \ldots, i_7$. We deduce that certain of the arithmetics of C are isomorphic. The result that the maximal arithmetics are isomorphic is also contained in the work of van der Blij and Springer [2].

A general element $\xi = \sum_{s=0}^{7} x_s i_s$ of C with rational components x_s has norm $N\xi = \sum_{s=0}^{7} x_s^2$. Also $i_s^2 = -1$ $(1 \leqq s \leqq 7)$ and, for each of seven *proper associative triads* (u, v, w) consisting of three different basic units, we have $uv = w = -vu$ and $w(uv) = -1 = (wu)v$. Any other triad of different basic units of C not containing 1 is non-associative. $R(\xi) = x_0$ is called the real part and $\bar{\xi} = 2x_0 - \xi$ the conjugate of ξ. Hence any element ξ of C satisfies the rank equation

$$\xi^2 - 2R(\xi)\xi + N\xi = 0. \tag{1.1}$$

Let (u, v, w) be any proper associative triad of basic units of C. Then there exists a basic unit t of C, different from 1, u, v and w and called the *unit assigned to* (u, v, w), such that ut, vt and wt are basic units of C.

u	v	w	t
i_6	i_5	i_3	i_1
i_1	i_7	i_6	i_2
i_7	i_2	i_5	i_3
i_1	i_2	i_3	i_4
i_6	i_2	i_4	i_5
i_7	i_3	i_4	i_6
i_1	i_4	i_5	i_7

For any elements ξ and η of C we have $\xi = \xi_0 + \xi_1 t$ and $\eta = \eta_0 + \eta_1 t$, where ξ_r and η_r $(r = 0, 1)$ are linear combinations of 1, u, v and w. An element such as ξ_0 is called a *quasi-quaternion in* (u, v, w). Hence, following Dickson [8], we have

$$\xi\eta = \xi_0\eta_0 - \bar{\eta}_1\xi_1 + (\eta_1\xi_0 + \xi_1\bar{\eta}_0)t. \tag{1.2}$$

C is a division algebra. To every non-zero element α of C there corresponds a unique inverse $\alpha^{-1} = (N\alpha)^{-1}\bar{\alpha}$. Also for any elements α and β of C

$$(\alpha\alpha)\beta = \alpha(\alpha\beta) \quad \text{and} \quad (\beta\alpha)\alpha = \beta(\alpha\alpha). \tag{1.3}$$

https://doi.org/10.1017/S2040618500034808 Published online by Cambridge University Press

(1.3) shows that C is what Zorn [18] called an alternative ring. We can then deduce the important identity

$$(\delta\alpha)(\beta\delta) = \delta\{(\alpha\beta)\delta\} = \{\delta(\alpha\beta)\}\delta \tag{1.4}$$

due to Moufang [17].

2. Automorphisms. A bijective mapping θ of C onto itself is defined to be an automorphism if

$$\theta(\xi \pm \eta) = \theta(\xi) \pm \theta(\eta) \tag{2.1}$$

and

$$\theta(\xi\eta) = \theta(\xi) \,.\, \theta(\eta) \tag{2.2}$$

for any elements ξ and η of C. If we also demand that

$$\theta(u) = v, \tag{2.3}$$

where u is any unit of C and v a corresponding unit of C, it is well known that there are 168 automorphisms of C which give different permutations of the basic units. This set of 168 automorphisms written as a set of permutations on the suffixes of the basic units of C forms the simple 168 group generated by the permutations (12)(47) and (2143576). Suitable sign changes must of course be applied to the units when necessary [7].

Let ζ be an arbitrary element of C. An element ρ of C is said to induce an automorphism of C if

$$\zeta \to \rho\zeta\rho^{-1}$$

defines an automorphism of C satisfying (2.1) and (2.2).

THEOREM 2.1. *A non-rational Cayley number ρ induces an automorphism of C if and only if*

$$4R^2(\rho) = N\rho.$$

Proof. From (1.4) we have, for any non-zero elements ρ, ξ and η of C,

$$(\rho\xi\rho^{-1})(\rho\eta\rho^2) = \rho\{(\xi\rho^{-1})(\rho\eta\rho)\}\rho$$

and

$$\overline{\rho\eta\rho} = \{\bar{\rho}(\bar{\eta}\bar{\xi}^{-1})\}(\bar{\xi}\bar{\rho}).$$

Thus

$$(\rho\xi\rho^{-1})(\rho\eta\rho^2) = \rho(\xi\eta)\rho^2$$

and the theorem follows by (1.1), since ρ^3 must be a scalar.

3. Non-maximal arithmetics in C. A set of elements of C is called an *arithmetic* of C if the set has the following three properties:

(i) For any element of the set the coefficients of the rank equation (1.1) are rational integers.

(ii) The set is closed under addition, subtraction and multiplication.

(iii) The set contains 1.

An arithmetic is called *maximal* if

https://doi.org/10.1017/S2040618500034808 Published online by Cambridge University Press

(iv) it is not contained in any larger arithmetic of C. This definition was stated by Dickson [11].

Let Q be the quaternion subalgebra of C all of whose elements are linear combinations of $1, i_1, i_2$ and i_3. The set of all elements of Q with rational integral components is denoted by H_0. Clearly H_0 is an arithmetic of Q. Hurwitz [13] defined an integral quaternion to be a quaternion with components either all integers or all half odd integers. Denote the set of all Hurwitz integral quaternions in Q by H. Then H is the unique maximal arithmetic of Q.

We define J_0 to be the set of all elements of C with rational integral components. Then J_0 is an arithmetic of C. We find eight further non-maximal arithmetics of C containing J_0, seven of which are shown to be isomorphic. Suppose that J is an arithmetic of C which contains J_0. Let α be an element of J. By property (i) above, if any one component of α is half an odd rational integer, then four or eight components of α are half odd rational integers. Otherwise all the components of α are rational integers. Now the units of C are elements of J, and J is closed under addition and subtraction. Thus we need only consider which elements ξ of the form

$$\xi = \tfrac{1}{2} \sum_{r=1}^{4} w_r , \tag{3.1}$$

where w_1, w_2, w_3 and w_4 are distinct basic units of C, belong to J and whether the element

$$\eta = \tfrac{1}{2} \sum_{s=0}^{7} i_s \tag{3.2}$$

belongs to J.

Define, for any ξ of the form (3.1), the *characteristic unit* $\chi(\xi)$ of ξ to be

$$\chi(\xi) = | \, w_1 w_2 w_3 w_4 \, |,$$

where, for any basic unit u of C, $| \pm u | = u$. Then $\chi(\xi)$ is a basic unit of C. We note that for any unit v of C

$$\chi(v\xi) = \chi(\xi).$$

Further, if α is of the form $\alpha_0 + \xi$, where α_0 is an element of J_0 and ξ is of the form (3.1), we define

$$\chi(\alpha_0) = 0$$

and

$$\chi(\alpha_0 + \xi) = \chi(\xi).$$

The following lemmas are easily proved.

LEMMA 3.1. *Any two different proper associative triads of basic units of C have precisely one element in common.*

LEMMA 3.2. *Any basic unit of C other than* 1 *appears in three and only three proper associative triads of basic units of C.*

https://doi.org/10.1017/S2040618500034808 Published online by Cambridge University Press

There are seventy elements ξ of the form (3.1). Now consider

$$\xi_u = \tfrac{1}{2}(1+u_1+u_2+u_3)$$

and

$$\xi_u^* = \xi_u u,$$

where u is the unit assigned to the proper associative triad (u_1, u_2, u_3). There are seven different elements ξ_u and seven corresponding different elements ξ_u^* and each is of the form (3.1). Also

$$\chi(\xi_u) = \chi(\xi_u^*) = 1.$$

Now let

$$\xi_{w,v}^* = \tfrac{1}{2}(w+v_1+v_2+v_3)$$

and

$$\xi_{w,v} = \eta - \xi_{w,v}^*,$$

where w is a basic unit other than 1, (v_1, v_2, v_3) the proper associative triad with assigned unit v not containing w, and η is of the form (3.2). Then

$$\chi(\xi_{w,v}) = \chi(\xi_{w,v}^*) = w.$$

By Lemma 3.2, to each value of w there correspond four proper associative triads not containing w. Therefore there are 28 different elements of the form $\xi_{w,v}^*$ and 28 different elements of the form $\xi_{w,v}$, all of which are of the form (3.1). It is to be noted that all sums of the form $\xi_u+\xi_u^*$ equal η, and that ξ_u occurs in an arithmetic of C if and only if ξ_u^* occurs in that arithmetic. The statement also applies to $\xi_{w,v}$ and $\xi_{w,v}^*$.

Let J_s be the set of all elements α of C that can be written in the form

$$\alpha = \alpha_0 + \delta_1 \xi_{i_s} + \delta_2 \xi_{i_s}^*,$$

where s is an integer $(1 \leqq s \leqq 7)$, α_0 belongs to J_0 and $\delta_1, \delta_2 = 0$ or 1. Then, from the definition of the Hurwitz quaternion arithmetic and from (1.2) with $t = i_s$, we see that J_s is closed under multiplication and, in fact, forms an arithmetic of C. Clearly the existence of the automorphism of C associated with the permutation (2143576) on the suffixes of the units of C shows that the arithmetics J_s are isomorphic.

Define the intersection of the seven arithmetics J_s to be J^*. It is easy to see that the intersection of any set of arithmetics is itself an arithmetic. Thus J^* is a non-maximal arithmetic of C.

4. Maximal arithmetics in C. To find further arithmetics of C we first prove

LEMMA 4.1. *Any sum $\xi_u+\xi_v$ satisfies condition* (i) *for an element of an arithmetic of C and* $\chi(\xi_u+\xi_v) = 1$ $(u \neq v)$.

Proof. By Lemma 3.1 we assume without loss of generality that $u_1 = v_1$. Then

$$\xi_u+\xi_v = 1+u_1+\tfrac{1}{2}(u_2+u_3+v_2+v_3).$$

Thus

$$\chi(\xi_u+\xi_v) = |\, u_1 v_1 \,| = 1.$$

https://doi.org/10.1017/S2040618500034808 Published online by Cambridge University Press

LEMMA 4.2. *Any product $\xi_u\xi_v$ satisfies condition* (i) *for an element of an arithmetic of C. $\chi(\xi_u\xi_v)$ equals the basic unit that triads (u_1, u_2, u_3) and (v_1, v_2, v_3) have in common.*

Proof. Again suppose that $u_1 = v_1$. Then, by straightforward multiplication,

$$\xi_u\xi_v = \tfrac{1}{2}(u_1+u_2+v_3+u_2v_3).$$

Hence $\chi(\xi_u\xi_v)$ is defined and equals u_1. The lemma is thus proved. We note that $\xi_u\xi_v = \xi^*_{u_1, x}$, where x is the basic unit assigned to the triad (u_2, v_3, u_2v_3), provided that $|u_2v_3| = u_2v_3$.

LEMMA 4.3. *Two elements $\xi_{w,v}$, $\xi_{w',v'}$ of C cannot both be contained in the same arithmetic J of C unless $w = w'$.*

Proof. We have

$$\xi_{w,v} = \tfrac{1}{2}(1+|v_1w|+|v_2w|+|v_3w|)$$

and

$$\xi_{w',v'} = \tfrac{1}{2}(1+|v_1'w'|+|v_2'w'|+|v_3'w'|).$$

Again, without loss of generality, we let $v_3 = v_3'$. Then

$$|v_3w|\,\xi_{w,v} = \tfrac{1}{2}(|v_3w|+v_2+v_1+1)+\xi_0$$

and

$$|v_3w'|\,\xi_{w',v'} = \tfrac{1}{2}(|v_3w'|+v_2'+v_1'+1)+\xi_0',$$

where ξ_0 and ξ_0' are elements of J_0. Suppose that $\xi_{w,v}$ and $\xi_{w',v'}$ belong to J. Then $|v_3w|\,\xi_{w,v}$ and $|v_3w'|\,\xi_{w',v'}$ also belong to J. Hence

$$\begin{aligned}\alpha &= |v_3w|\,\xi_{w,v} - |v_3w'|\,\xi_{w',v'}\\ &= \tfrac{1}{2}(|v_3w|-|v_3w'|)+\tfrac{1}{2}(v_1+v_2-v_1'-v_2')+\alpha_0\end{aligned}$$

must be an element of J. Now α must satisfy condition (i) for an element of an arithmetic of C. But (v_1, v_2) and (v_1', v_2') have either two elements in common or no element in common. Hence we must have $|v_3w| = |v_3w'|$; therefore $w = w'$. Thus Lemma 4.3 has been established.

Now any element of C for which a characteristic unit is defined has characteristic unit equal to 0, 1 or w, where w is a basic unit of C other than 1. Hence we see at once from Lemma 4.3 that the following lemma holds.

LEMMA 4.4. *All elements of any given arithmetic of C with characteristic units different from* 0 *or* 1 *have equal characteristic units.*

We now prove

LEMMA 4.5. *$\xi_u+\xi_{w,v}$ satisfies the condition* (i) *for an element of an arithmetic J of C if and only if w is an element of the triad (u_1, u_2, u_3) with assigned unit u. If this condition holds,*

$$\chi(\xi_u+\xi_{w,v}) = w.$$

Proof. We have

$$\xi_u+\xi_{w,v} = 1+\tfrac{1}{2}(u_1+u_2+u_3+|v_1w|+|v_2w|+|v_3w|).$$

https://doi.org/10.1017/S2040618500034808 Published online by Cambridge University Press

Clearly (u_1, u_2, u_3) and $(|v_1w|, |v_2w|, |v_3w|)$ cannot have three elements in common. If the triads have an even number of elements in common, $N(\xi_u+\xi_{w,v})$ is not a rational integer and $\xi_u+\xi_{w,v}$ is therefore not contained in J. Assume that $\xi_u+\xi_{w,v}$ is an element of J. Then the triads must have precisely one element in common. Also, by Lemma 3.1, we may take $u_3 = v_3$. Then if $|v_1w|$ belongs to the triad (u_1, u_2, u_3), we have $|v_1w| = u_s$ ($s = 1, 2$ or 3). Now $|v_1w| = u_3$ implies that $|v_2w| = |v_3v_1w| = |u_3u_3| = 1$, which is not so. $|v_1w| = u_s$ ($s = 1$ or 2) implies that $|v_2w| = |v_3v_1w| = |u_3u_s| = u_r$ ($r = 1$ or 2) and then (u_1, u_2, u_3) and $(|v_1w|, |v_2w|, |v_3w|)$ have two elements in common; this cannot hold. Similarly, we cannot have $|v_2w| = u_s$ for $s = 1$, 2 or 3. Hence we must have $|v_3w| = u_s$ for some s ($1 \leqq s \leqq 3$). But since $|v_3w| = |u_3w|$, we have $w = |u_3u_s|$. Now $w \neq 1$ and therefore $u_3 \neq u_s$. Hence, since $u_1(u_2u_3) = -1$, we have $w = u_r$ for some r ($1 \leqq r \leqq 3$); i.e. w belongs to the triad (u_1, u_2, u_3) with assigned unit u.

To complete the proof we suppose without loss of generality that $w = u_2$. Then, since $v_3 = u_3$, we can write

$$\xi_u+\xi_{w,v} = 1+u_1+\tfrac{1}{2}(u_2+u_3+|v_1u_2|+|v_2u_2|).$$

Thus

$$\chi(\xi_u+\xi_{w,v}) = |u_2u_3v_1u_2v_2u_2| = |u_1v_3| = w.$$

This completes the proof of the lemma.

For products of the form $\xi_{w,v}\xi_{w',v'}$ it follows from Lemma 4.4 that we need only consider the case when $w = w'$. It is easy to prove by direct multiplication that the following lemma holds.

LEMMA 4.6. *The product of two elements $\xi_{w,v}$ and $\xi_{w,v'}$ of C satisfies the condition* (i) *for an element of an arithmetic of C, and $\chi(\xi_{w,v}\xi_{w,v'})$ equals w.*

In the same way the following lemma can be simplified for the present argument.

LEMMA 4.7. *The product of two elements ξ_u and $\xi_{w,v}$ belongs to an arithmetic of C if w is an element of the triad (u_1, u_2, u_3).*

In fact to complete our argument we see from Lemma 4.5 that we need only consider products $\xi_u\xi_{w,v}$ for which $w = u_s$ for some s ($1 \leqq s \leqq 3$). The details of the proof involving straightforward multiplication of a quasiquaternion and $\xi_{w,v}$ are omitted. For such products $\xi_u\xi_{w,v} = \xi_x^*+\alpha_0$, where x is the unit assigned to a triad containing w and α_0 is in J_0.

Suppose that J is an arithmetic of C containing the quasiquaternions ξ_u, ξ_v. Let the proper associative triads with assigned units u, v ($u \neq v$) have unit w in common. Then, by Lemma 4.2, J contains an element with characteristic unit w. Also, from the result and proof of Lemma 4.1, it follows that J contains the third quasiquaternion of the form (3.1) with corresponding associative triad containing w.

Now suppose that J contains a quasiquaternion

$$\xi_{u'} = \tfrac{1}{2}(1+u_1'+u_2'+u_3')$$

of the form (3.1) for which $u_s' \neq w$ ($1 \leqq s \leqq 3$); i.e. (u_1', u_2', u_3') is one of the four proper associative triads of basic units not containing w. Then from Lemma 4.2 it follows that

https://doi.org/10.1017/S2040618500034808 Published online by Cambridge University Press

$\chi(\xi_u\xi_{u'})$ is equal to a basic unit of C other than 1 or w. Therefore, by Lemma 4.4, $\xi_u\xi_{u'}$ cannot be an element of J. Hence J cannot contain $\xi_{u'}$. For each basic unit w of C other than 1 we define J_w to be the set of all elements $\alpha_{(w)}$ of C of the form

$$\alpha_{(w)} = \alpha_0 + \delta_1\xi_{(w)} + \delta_2\eta, \tag{4.1}$$

where α_0 is contained in J_0, δ_1, $\delta_2 = 0$ or 1, and $\xi_{(w)} = \xi_u$ where $w = u_s$ for some s $(1 \leqq s \leqq 3)$ or $\xi_{(w)} = \xi_{w,v}$ and $\eta = \frac{1}{2}\sum_{s=0}^{7} i_s$. We have proved in the above lemmas that, for w any basic unit of C other than 1, J_w is a maximal arithmetic of C.

It follows from Lemma 3.2 that each maximal arithmetic J_w of C contains three distinct non-maximal arithmetics J_r, J_s, J_t $(1 \leqq r, s, t \leqq 7)$. The basic units i_r, i_s, i_t are those assigned to the proper associative triads of basic units containing w.

The permutation (2143576), as explained in § 2, when applied to the suffixes of the basic units of C, gives an automorphism of C for suitable sign changes on the units. Thus the seven maximal arithmetics are isomorphic. The permutation (123)(567) was in effect used by Dickson [12] in finding three of the maximal arithmetics of C, namely J_{i_1}, J_{i_2} and J_{i_3}.

In order to treat the same subject Kirmse [15] defined a *module* in Cayley's algebra to be a set of Cayley numbers with rational coefficients closed under subtraction and containing eight linearly independent members. A module is called an *integral domain* if it is closed under multiplication. For example, the module J_0 consisting of all Cayley numbers with rational integral coefficients is an integral domain. Kirmse then defined a *maximal* integral domain to be an extension of J_0 which cannot be further extended without ceasing to be an integral domain. Kirmse's maximal integral domains, if correctly derived, are the same as the seven maximal arithmetics obtained.

Given any element α of C which satisfies condition (i) for an element of an arithmetic of C, we can immediately see to which of the maximal arithmetics J_w it belongs. Any such element α can be written in the form (4.1) for some basic unit w. Clearly, if δ_1, δ_2 are both zero, then α belongs to J_0, while if $\delta_1 = 0$ and $\delta_2 \neq 0$, α is contained in J^*. If $\delta_1 \neq 0$, then α is an element of one or three of the maximal arithmetics J_w. For example, if

$$\xi_{(w)} = \tfrac{1}{2}(1 + i_1 + i_2 + i_3),$$

we have $\xi_{(w)} = \xi_{i_4}$, since $\chi(\xi_{(w)}) = 1$. Thus α is an element of J_{i_1}, J_{i_2} and J_{i_3}. However, if

$$\xi_{(w)} = \tfrac{1}{2}(1 + i_5 + i_6 + i_7),$$

then $\chi(\xi_{(w)}) = i_4$. Thus we see that α is only contained in J_{i_4}.

It is now easy to write down the set of 240 elements of norm 1 of any maximal arithmetic J_w of C. There are 16 units of C, 48 quasiquaternions involving linear combinations of the proper associative triads containing $\pm w$ and the 48 elements obtained from the quasiquaternions by multiplying by the corresponding assigned units. Also there are 64 elements of the form

$$\tfrac{1}{2}(\pm 1 \pm u_1 w \pm u_2 w \pm u_3 w)$$

and 64 elements of the form

$$\tfrac{1}{2}(\pm w \pm u_1 \pm u_2 \pm u_3)$$

where (u_1, u_2, u_3) is a proper associative triad of basic units of C not involving w.

I wish to thank Professor R. A. Rankin who supervised me in a course of research at Glasgow University.

REFERENCES

1. A. A. Albert, On a certain algebra of quantum mechanics, *Ann. of Math.* (2) **35** (1934), 65–73.

2. F. van der Blij and T. A. Springer, The arithmetic of the octaves and of G_2, *Nederl. Akad. Wetensch. Indag. Math.* **21** (1959), 406–418.

3. F. van der Blij, History of the octaves, *Simon Stevin* **34**, III (1961), 106–125.

4. H. Brandt, Zur Zahlentheorie der Quaternionen, *Jber. Deutsch. Math. Verein.* **53** (1943), 23–57.

5. A. Cayley, Note on a system of imaginaries, *Collected Mathematical Papers*, vol. I, 127 – *Phil. Mag.* (3) **26** (1845), 210.

6. A. Cayley, On the eight-square imaginaries, *Collected Mathematical Papers*, vol. II, 368–371 – *Amer. J. Math.* **4** (1881), 293–296.

7. H. S. M. Coxeter, Integral Cayley Numbers, *Duke Math. J.* **13** (1946), 561–578.

8. L. E. Dickson, *Linear Algebras* (Cambridge Tracts in Mathematics, No. 16, 1914).

9. L. E. Dickson, On quaternions and their generalization and the history of the eight square theorem, *Ann. of Math.* (2) **20** (1919), 155–171, 297.

10. L. E. Dickson, Arithmetic of quaternions, *Proc. London Math. Soc.* (2) **20** (1921), 225–232.

11. L. E. Dickson, *Algebras and their arithmetics* (Chicago, 1923).

12. L. E. Dickson, A new simple theory of hypercomplex integers, *J. Math. Pures Appl.* (9) **2** (1923) 281–326.

13. A. Hurwitz, Über die Zahlentheorie der Quaternionen, *Nachr. Akad. Wiss. Göttingen* (1896), 313–340.

14. A. Hurwitz, *Vorlesungen über die Zahlentheorie der Quaternionen* (Berlin, 1919).

15. J. Kirmse, Über die Darstellbarkeit natürlicher ganzer Zahlen als Summen von acht Quadraten und über ein mit diesem Problem zusammenhängendes nichtkommutatives und nichtassociatives Zahlensystem, *Ber. Verh. Sächs. Akad. Wiss. Leipzig* **76** (1924), 63–82.

16. J. Kirmse, Zur Darstellbarkeit natürlicher ganzer Zahlen als Summen von acht Quadraten, *Ber. Verh. Sächs. Akad. Wiss. Leipzig* **80** (1928), 33–34.

17. R. Moufang, Zur Struktur von Alternativkörpern, *Math. Ann.* **110** (1934), 416–430.

18. M. Zorn, Theorie der alternativen Ringen, *Abh. Math. Sem. Univ. Hamburg* **8** (1931), 123–147.

ROYAL COLLEGE OF SCIENCE AND TECHNOLOGY
GLASGOW