A NOTE ON CAYLEY LOOPS

A. GINZBURG

Introduction. In § 1 the existence of two non-isotopic loops satisfying the same system of relations is proved: C_1 is isomorphic to the well-known *Cayley loop* (see **1** or **6**); C_2 seems not to have been mentioned in the literature. In § 2 a characterization of the second type is given in terms of Tamari's *generalized normal multiplication table* (**7**; **8**) as a *complete symmetric quasi-regular partition*, i.e., a *quasi-associative loop* (**4**, **5**), or a so-called *near-group* (**9**). In § 3 these distinctions are followed by comparing the corresponding algebras.

1. The Cayley numbers can be written in the form $x = a + be$, where a and b are real quaternions and e is an indeterminate (**3**, p. 237). These numbers are combined according to the rules:

$$(a + be) + (c + de) = a + c + (b + d)e, \tag{1}$$

$$(a + be)(c + de) = ac - \bar{d}b + (da + b\bar{c})e. \tag{2}$$

Here $\bar{a}$ denotes the conjugate of the quaternion a.

The 16 elements

$$\{\pm 1, \pm i, \pm j, \pm k, \pm e, \pm ie, \pm je, \pm ke\} \tag{3}$$

form, by (2), a multiplicative loop, called in (**6**) the Cayley loop. This loop is diassociative (i.e. every two of its elements generate a subgroup) and has three generators x_1, x_2, x_3 (e.g., ie, je, ke), which satisfy (**6**; **1**, p. 88):

$$\begin{cases} x_\alpha{}^4 = 1, \quad x_\alpha{}^2 = x_\beta{}^2 \neq 1, \quad x_\alpha x_\beta = x_\beta{}^3 x_\alpha \quad (\alpha \neq \beta), \\ x_\alpha x_\beta \cdot x_\gamma = x_\alpha{}^3 \cdot x_\beta x_\gamma \quad (\alpha, \beta, \gamma = 1, 2, 3 \text{ all different}). \end{cases} \tag{4}$$

We shall refer to a diassociative loop of order 16 generated by three elements satisfying (4) as a C-loop.

PROPOSITION 1. *There exist two non-isotopic C-loops, which will be denoted by C_1 and C_2. Every C-loop is isomorphic either to C_1 or to C_2.*

Proof. The above-mentioned C-loop will be denoted by C_1. As a subloop of the multiplicative loop of non-zero Cayley numbers, which constitute an alternative algebra (i.e. an algebra in which for any two elements a, b the equalities $(aa)b = a(ab)$ and $(ba)a = b(aa)$ hold), C_1 satisfies the Moufang identity $(xy)(zx) = [x(yz)]x$ (**2**, Lemma 2.2).

Received November 6, 1962. The author expresses his thanks to the referees for their remarks.

We consider now a modification of (2) given by

$$(a + be)(c + de) = ac - b\bar{d} + (ad + \bar{c}b)e. \tag{5}$$

The three elements ie, je, ke multiplied according to (5) satisfy the conditions (4) and generate a diassociative loop C_2, consisting of the same 16 elements (3) as C_1. This can be verified by direct inspection.

The loop C_2 does not satisfy Moufang's identity, since, for example,

$$(i\cdot j)(e\cdot i) = k(-ie) = -je \qquad \text{and} \qquad [i(j\cdot e)]i = (i\cdot je)i = ke\cdot i = je.$$

Every loop isotopic to a Moufang loop is Moufang (**1**, p. 58); hence C_1 and C_2 are not isotopic.

Now using (4) one can construct the C-loops by building their multiplication tables. The whole construction is unique, except for one step, where two possibilities arise: one leading to a loop isomorphic to C_1, the other to one isomorphic to C_2. (I wish to thank Professor R. Artzy, who presented me with the multiplication table of this loop.)

Indeed, let ie, je, ke be chosen as generators. Denote $(me)^{-1} = -me$ and $(me)^2 = -1$ $(m = i, j, k)$. Then (by diassociativity and (4)) $(-1)^2 = 1$, $(me)(-1) = (-1)(me) = -me$ and $(-1)(-me) = (-me)(-1) = me$. Putting $ie\cdot je$ (or $ie\cdot ke$, etc.) equal to one of the already introduced elements leads to a contradiction. Denote $ie\cdot je = k$, $ie\cdot ke = -j$, $ie(-je) = -k$, $ie(-ke) = j$. Now $je\cdot ke$ cannot equal one of the above 12 elements. Denote it by i and $je(-ke)$ by $-i$. Using the diassociativity and (4) one can proceed to fill up the multiplication table, but for $k\cdot ke$ one must set a new symbol, say $-e$. Denote also $k(-ke) = e$ and proceed as above. All products except the 24 of the form mn, where $m, n = \pm i, \pm j, \pm k$, and $m \neq \pm n$, are now uniquely defined. The multiplication table must be a latin square; consequently ki, for example, can equal j or $-j$ only. On the other hand $ki = (ie\cdot je)(je\cdot ke)$ and the parentheses cannot be eliminated; (4) does not provide such a situation and diassociativity cannot be used, because there are three different generators in this product. Both decisions $ki = j$ or $ki = -j$ are allowed and result immediately in a complete filling of the multiplication table.

PROPOSITION 2. *A C-loop is isomorphic to C_1 if and only if its generators x_1, x_2, x_3 satisfy:*

$$(x_\alpha x_\beta)(x_\beta x_\gamma) = x_\alpha x_\gamma. \tag{6}$$

It is isomorphic to C_2 if and only if its generators satisfy

$$(x_\alpha x_\beta)(x_\beta x_\gamma) = x_\gamma x_\alpha. \tag{7}$$

Proof. When multiplied according to (2), the generators ie, je, ke satisfy (6), but not (7), and when multiplied according to (5), they satisfy (7), but not (6). This fact, together with the previous proposition, proves the present one.

2. Together with the ordinary multiplication tables, also the so-called generalized normal multiplication tables (g.n.m.t.) **(7; 8)** can be used to describe multiplicative systems.

For example, the quaternion group with the elements $\{\pm 1, \pm i, \pm j, \pm k\}$ is represented by the g.n.m.t. shown in Table I **(4)**. Such a table represents

TABLE I

5	$-k$	k	$-j$	j	1
4	$-i$	i	-1	1	$-j$
3	i	$-i$	1	-1	j
2	-1	1	i	$-i$	$-k$
1	1	-1	$-i$	i	k
	1	2	3	4	5

a family $R = \{r_\alpha, r_\beta, \ldots\}$ of binary relations over a set N (here $N = \{1, 2, 3, 4, 5\}$), being in one-to-one correspondence with the elements of the multiplicative system. The relations are combined by so-called generalized multiplication:

$$r_\alpha \cdot r_\beta = r_\gamma \Leftrightarrow r_\gamma \supset r_\alpha r_\beta \neq \emptyset \qquad \textbf{(7; 8)}.$$

Accordingly, the multiplication in the table is performed using the rule $a_{mn}a_{np} = a_{mp}$, where a_{mn} is the element on the intersection of the mth column (from left to right) and the nth row (upwards). Note, that there are products, such as $i \cdot i$, $i \cdot (-1)$, and others, which can be found in the table more than once. Nevertheless, this table has only 25 entries, while the ordinary multiplication table of this group has 64 entries.

The just given g.n.m.t. has the following three special properties:

(a) Any two elements appearing in it can be multiplied. In other words, it describes a groupoid in the sense used in **(1**, p. 1**)**.

(b) $a_{m_1n_1} = a_{m_2n_2} \Rightarrow a_{n_1m_1} = a_{n_2m_2}$.

(c) Each place in the table is occupied.

A g.n.m.t. satisfying (a), (b), and (c) is called a complete symmetric quasi-regular partition **(4; 5)** and is denoted by P_{sc}.

The groupoid represented by a P_{sc} is an IP-loop (i.e. a loop with the inverse property). On the other hand, not every IP-loop can be represented by a P_{sc}. An IP-loop for which this can be done is called a QA-loop (quasi-associative loop **(4; 5)** or near-group **(9)**). Thus every group is a QA-loop.

PROPOSITION 3. *C_2 is a* QA-*loop, but C_1 is not a* QA-*loop.*

Proof. The P_{sc} shown in Table II is a g.n.m.t. of C_2. Hence C_2 is a QA-loop.

https://doi.org/10.4153/CJM-1964-007-1 Published online by Cambridge University Press

TABLE II

$-ke$	ke	$-je$	je	ie	$-ie$	$-e$	e	1
$-k$	k	$-j$	j	i	$-i$	-1	1	$-e$
k	$-k$	j	$-j$	$-i$	i	1	-1	e
$-j$	j	k	$-k$	-1	1	$-i$	i	ie
j	$-j$	$-k$	k	1	-1	i	$-i$	$-ie$
$-i$	i	-1	1	$-k$	k	j	$-j$	$-je$
i	$-i$	1	-1	k	$-k$	$-j$	j	je
-1	1	i	$-i$	j	$-j$	k	$-k$	$-ke$
1	-1	$-i$	i	$-j$	j	$-k$	k	ke

Now the elements ie and je of C_1 generate a subgroup H of order 8 and $(ie \cdot je)b \neq ie(je \cdot b)$ for any $b \in C_1$ which is not in this subgroup.

Suppose that there exists a P_{sc} representing C_1. $ie \cdot je$ have to be multiplied in it; hence there are $m, n, p \in N$ such that $a_{mn} = ie$ and $a_{np} = je$. But $(a_{mn}a_{np})a_{pq} = a_{mn}(a_{np}a_{pq})$ (both products equal to a_{mq}); hence the whole p column in the above P_{sc} must be occupied by elements $b \in C_1$ such that $(ie \cdot je)b = ie(je \cdot b)$, i.e. by elements of H. This implies that any element in the P_{sc} belongs to H and it cannot represent C_1, which, thus, is not a QA-loop. |

3. The set $A = \{x \mid x = a + be\}$ (a and b real quaternions and e an indeterminate) with the addition (1) and multiplication (5) forms clearly an algebra of order 8 over the field of the real numbers.

Write $\bar{x} = \overline{a + be} = \bar{a} - be$. Then

(a) $\overline{xy} = \bar{y}\bar{x}$,

(b) $N(x) = x\bar{x} = \bar{x}x = a\bar{a} + b\bar{b}$ is a positive number for any $x \neq 0$.

These properties are common to A and to the algebra of Cayley numbers. However, in A, we have in general $N(xy) \neq N(x)N(y)$: if

$$x = a + be = a_0 + ia_1 + ja_2 + ka_3 + (b_0 + ib_1 + jb_2 + kb_3)e,$$
$$y = c + de = c_0 + ic_1 + jc_2 + kc_3 + (d_0 + id_1 + jd_2 + kd_3)e,$$

and if $d\bar{b}$ is denoted by $u_0 + iu_1 + ju_2 + ku_3$, then

$$N(xy) = N(x)N(y) - 4 \begin{vmatrix} a_1 & a_2 & a_3 \\ u_1 & u_2 & u_3 \\ c_1 & c_2 & c_3 \end{vmatrix}.$$

The equality $N(yx) = N(xy)$ is satisfied in A.

https://doi.org/10.4153/CJM-1964-007-1 Published online by Cambridge University Press

A is simple, flexible (i.e. $(ab)a = a(ba)$ for every $a, b \in A$) and power-associative (i.e. every $a \in A$ generates an associative subalgebra), as can be checked directly, but A is not alternative (otherwise C_2 would be a Moufang loop).

By the generalization of (5) to

$$(a + be)(c + de) = ac + \mu b\bar{d} + (ad + \bar{c}b)e,$$

where μ is real, a class of flexible power-associative algebras is obtained.

References

1. R. H. Bruck, *A survey of binary systems* (Göttingen, 1958).
2. R. H. Bruck and E. Kleinfeld, *The structure of alternative division rings*, Proc. Amer. Math. Soc., *2* (1951), 878–890.
3. L. E. Dickson, *Algebras and their arithmetics* (New York, 1938).
4. A. Ginzburg, *Multiplicative systems as homomorphic images of square sets* (Thesis, Haifa, 1959).
5. ——— *Systèmes multiplicatifs de relations. Boucles quasi-associatives*, C.R. Acad. Sci. Paris, *250* (1960), 1413–1416.
6. D. A. Norton, *Hamiltonian loops*, Proc. Amer. Math. Soc., *3* (1952), 56–65.
7. D. Tamari, *Les images homomorphes des groupoïdes de Brandt et l'immersion des semi-groupes*, C. R. Acad. Sci. Paris, *229* (1949), 1291–1293.
8. ——— *Représentations isomorphes par des systèmes de relations. Systèmes associatifs*, C. R. Acad. Sci. Paris, *232* (1951), 1332–1334.
9. ——— *"Near-groups" as generalized normal multiplication tables*, Notices Amer. Math. Soc., *7* (1960), 77.

Technion, Israel Institute of Technology
Haifa, Israel