CYCLES IN ALGEBRAIC SYSTEMS

D. A. NORTON AND SHERMAN K. STEIN

1. **Introduction.** The object of this work is to generalize the definition of cycle [1] to an arbitrary Latin square, exhibit the relation of cycles to sequences of inverses, commutativity, the law of keys, Steiner triples and consider some problems which they suggest. It is essentially independent of [1]; the relation of cycles to local homology plays no role here.

2. **Cycles and their terminology.** Let L be an $n \times n$ Latin square or, alternatively, let Q be a quasigroup of order n. Let M be the set of n^2 ordered triplets ijk, where k is the entry in the ith row and jth column of L. If S is the set of n^2 ordered pairs ij, and if $\pi_i: M \to S$ is the projection parallel to the ith coordinate (for example, $\pi_2(ijk) = ik$), then for each i, $1 \leqq i \leqq 3$, π_i is onto S (or equivalently is one-one). There is clearly a one-one correspondence between Latin squares L of order n and sets M of n^2 ordered triplets for which the π_i are all onto S. Let $T: S \to S$ be the involution defined by $T(ij) = (ji)$ and $P_i: M \to M$ be $\pi_i^{-1} T \pi_i$. For each i, $1 \leqq i \leqq n$, let $M_i \subset M$ be the set of triplets which contain i. Each $t \in M_i$, with leading element i, generates what we shall call a *cycle on i* in the following manner. If $\theta: M_i \to M_i$ denotes $P_2P_1P_3$, the cycle beginning with t shall consist of the triplets

$$t,\ P_3t,\ P_1P_3t\theta t,\ P_3\theta t,\ P_1P_3\theta t,\ \theta^2 t,\ \cdots,\ P_1P_3\theta^{n-1}t$$

where n is the smallest positive integer such that $\theta^n t = t$. The *length* of the cycle is the integer n. The *number, k, of elements* in a cycle C is the number of i, $1 \leqq i \leqq n$, which appear in at least one triplet of the cycle; C will be called a *cycle with k elements.*

If M contains the n triplets (iii), $1 \leqq i \leqq n$, M will be called *idempotent.* A triplet (iii), or the cycle of length one containing (iii), will also be called an idempotent triplet or idempotent cycle respectively.

3. **Relation of cycles to sequences of inverses.** Let Q be a loop, that is, a quasigroup with unit element 1. For $x \in Q$ distinct elements $x, x_1, x_2, \cdots, x_{n-1}$ of Q, defined inductively by

$$x_1 x = 1, \qquad x_2 x_1 = 1, \qquad x_3 x_2 = 1, \cdots$$

and satisfying $x x_{n-1} = 1$, form a sequence of left inverses on x [2,

Received by the editors December 27, 1955.

p. 448]. Two sets of left inverses are either identical or disjoint. Thus, Q is partitioned into sets of left inverses.

THEOREM 3.1. *There is a one-one correspondence between sets of left inverses in Q and cycles on* 1.

PROOF. Let $x, x_1, x_2, \cdots, x_{n-1}$ be a sequence of left inverses and $x_n = x$. Associate with this sequence the following cycle on 1:

$$(1xx),\ P_3(1xx),\ P_1P_3(1xx),\ \theta(1xx),\ P_3\theta(1xx),\ P_1P_3\theta(1xx),\ \cdots,\ P_1P_3\theta^{n-1}(1xx).$$

(Explicitly

$$(1xx),\ (x1x),\ (x_1x1),\ (1x_1x_1),\ (x_11x_1),\ (x_2x_11),\ \cdots,\ (xx_{n-1}1).)$$

Conversely such a cycle on 1 determines a set of left inverses.

4. Cycles of length one. The following theorems illustrate how restrictions on the cycles influence L (or Q).

THEOREM 4.1. *The following conditions are equivalent*:
(α) *M is idempotent and each cycle is of length one*;
(β) *Q satisfies the identities*:

$$(1)\ a^2 = a, \qquad (2)\ ab \cdot ba = a, \qquad \text{all } a, b \in Q.$$

PROOF. Assume (α). Since M is idempotent (1) is valid in Q and (2) is valid if $a = b$. If "a" is not equal to "b" consider the cycle on "a" containing the triplet (abc). This cycle, consisting of three elements, must be of the form (abc), (bad), (cda), i.e. $c = ab$, $d = ba$, $a = cd$. This establishes (β). The converse is proved similarly.

THEOREM 4.2. *The order, n, of a quasigroup Q satisfying* (1) *and* (2) *above is congruent to* 0 *or* 1 (mod 4).

PROOF. Consider the set C of $n(n-1)/2$ unordered pairs $\{a, b\}$ $a \neq b$, $a, b \in Q$. Define $\phi: C \to C$ by $\phi\{a, b\} = \{ab, ba\}$. Because of (1) and (2) ϕ^2 is the identity mapping of C, and ϕ has no fixed elements. Thus, ϕ induces a pairing of the elements of C. Hence $n(n-1)/2$ is even and the theorem is proved. (*Alternate proof.* In the notation of [1], $Z \equiv (n)(n-1)/2$ (mod 2), coupled with $Z = n(n-1)$, implies the theorem.)

Since conditions (1) and (2) are preserved under direct products of quasigroups, the set of integers $\{n\}$ for which there exists Q of order n satisfying (1) and (2) is closed under multiplication. For $n = 4$ the following Q satisfies (1) and (2), and is in fact unique up to an isomorphism:

	a	b	c	d
a	a	c	d	b
b	d	b	a	c
c	b	d	c	a
d	c	a	b	d

Thus for $n=4^k$, $k=0, 1, 2, \cdots$ there exists Q of order n satisfying (1) and (2). A brief enumeration of cases shows, however, that there is none of order 5. Bruck[1] has established the existence of such Q for $n=2^k$, $k\geqq 2$, without the use of direct products.

Equations (1) and (2) suggest the equations:

$$(1)\ a^2 = a, \qquad (2')\ ab\cdot ba = b.$$

It should be noted that (2') is not easily translatable into the notation of cycles.

The first proof of Theorem 3 goes through unchanged to show that the order of Q satisfying (1) and (2') must be congruent to 0 or 1 (mod 4). A brief enumeration shows that there is none of order 4 and that the following two are, up to isomorphism, the only Q of order 5 satisfying (1) and (2'):

	a	b	c	d	e
a	a	c	b	e	d
b	d	b	e	a	c
c	e	d	c	b	a
d	c	e	a	d	b
e	b	a	d	c	e

	a	b	c	d	e
a	a	c	d	e	b
b	d	b	e	c	a
c	e	a	c	d	b
d	b	e	a	d	c
e	c	d	b	a	e

Bruck[1] has shown that if all the prime factors of n are congruent to 1 (mod 4) then there exists a Q satisfying (1) and (2'). It is inviting to conjecture that there exists Q of order n satisfying (1) and (2) if and only if $n=1$, or is of the form $4k$; similarly that there exists Q of order n satisfying (1) and (2') if and only if n is of the form $4k+1$.

5. **Cycles with three distinct elements where Q is idempotent.** In this section a natural correspondence between sets of "Steiner's Triples" [4, p. 204] and idempotent algebraic systems satisfying the "bilateral law of keys" [3, p. 420] is used to establish an existence theorem. A cycle containing at most three distinct elements is either

[1] In a letter to the authors.

of length two or idempotent. If not idempotent it takes the form

(3) $(abc), (bac), (bca), (acb), (cab), (cba).$

THEOREM 5.1. *Every cycle of Q is idempotent or contains exactly three distinct elements if and only if Q satisfies the bilateral law of keys $ab\cdot b=b\cdot ba=a$.*

PROOF. If every cycle of Q is idempotent or of type (3) above then $ab\cdot b=cb=a$ and $b\cdot ba=b\cdot c=a$ so Q satisfies the bilateral law of keys. Conversely assume that Q satisfies the bilateral law of keys. If (abc), $(bad)\in M$ then the bilateral law of keys implies (acb) and $(bda)\in M$. The cycle on "a" beginning with (abc) must be (abc), (bad), (bda), (acb), (cae), (cea) $\cdots$. But $(abc)\in M$ implies $(cba)\in M$ so $e=b$ and the cycle is of the form (abc), (bad), (bda), (acb), (cab), (cba). Furthermore, (cba), $(bad)\in M$ imply respectively (cab), $(dab)\in M$ so that $c=d$. The cycle is thus of the form (3). Observe that the bilateral law of keys, therefore, implies commutativity [3, p. 420].

THEOREM 5.2. *An idempotent quasigroup Q of order n, the cycles of which contain at most three distinct elements, exists if and only if* $n\equiv 1, 3 \pmod 6$.

PROOF. Each cycle of the form (3) containing three distinct elements is completely determined by these three elements. Let λ be the mapping which assigns to each of these cycles, C, the unordered triplet, λC, consisting of its three elements. If Q is idempotent, there are n idempotent triplets. If, furthermore, the cycles of Q contain at most three distinct elements, the set of all unordered triplets λC is a set of $n(n-1)/6$ Steiner's Triples, (i.e., a set of unordered triples on n elements which contain every unordered pair i, j, $i\neq j$ exactly once), which exist if and only if $n\equiv 1, 3 \pmod{(6)}$ [4, p. 204].

The triplets of cycle (3) are the set of all possible permutations of three distinct elements. The converse of Theorem 5 follows immediately. To a Steiner's Triple, associate the six ordered permutations of its elements. Adjoin to this set the triplets (iii), $1\leqq i\leqq n$. This total set of triplets defines a quasigroup Q, where the triplet (abc) defines the binary operation $a\cdot b=c$ in Q.

Combining Theorems 5.1 and 5.2 we have

COROLLARY 5.3. *An idempotent quasigroup of order n satisfying the bilateral law of keys exists if and only if* $n\equiv 1, 3 \pmod 6$.

6. Other cycles of length one or two. The most general type of cycle of length two on "a" is

(4) $(abc), (bad), (eda), (afe), (fag), (cga).$

A cycle of length two contains at most seven distinct elements. The following theorem is obvious from (4).

THEOREM 6.1. *If Q is a system in which every cycle is of length one or two, then for $a, b, f \in Q$, if $(af)(ba) = a$ then $(ab)(fa) = a$.*

THEOREM 6.2. *If Q is commutative, every cycle of Q is of length one or two.*

PROOF. Because of commutativity, a cycle on "a," starting with the triplet (abc), proceeds

$$(abc), (bac), (dca), (aed), (ead), (fda) \cdots . \tag{5}$$

But since $(dca) \in M$, commutativity yields $(cda) \in M$. This fact, coupled with $(fda) \in M$, imply $c = f$ so cycle (5) closes.

Of the other possible systems with cycles of length equal to one or two, this paper will consider only two types of cycles which give rise to familiar algebraic systems:

(A) $(abc), (bad), (eda), (ade), (dab), (cba)$;

(B) $(abc), (bad), (bda), (acb), (cae), (cea)$;

where b, c, d, e are not necessarily distinct.

THEOREM 6.3. *A quasigroup Q satisfies the right law of keys $ab \cdot b = a$,* [3, p. 420] *if and only if every cycle is idempotent or of type* (A).

PROOF. It is easy to check that if every cycle of Q is idempotent or type (A) then Q satisfies the right law of keys. Conversely if Q satisfies the right law of keys, $(abc), (bad), (eda) \in M$ imply respectively $(cba), (dab), (ade) \in M$ so a cycle on "a" beginning with (abc) becomes

$$(abc), (bad), (eda), (ade), (dab), (cba)$$

which is (A).

THEOREM 6.4. *For every integer n there exists a quasigroup of order n satisfying the right law of keys.*

PROOF. This will be proved by construction of a quasigroup satisfying the theorem. Let $G(\cdot)$ be an abelian group of order n and binary operation $(\cdot)$. Let $Q(\circ)$ be a quasigroup of order n on the same elements as G but with the binary operation $(\circ)$ defined by $x \circ y = x^{-1} \cdot y^k$, $x, y \in G$, where "k" is any nonzero integer. If $k = 1$, Q is clearly a quasigroup in which $(x \circ y) \circ y = x$. Furthermore, Q has a left identity, namely the identity of G.

If $k = 2$, the elements of Q satisfy the identity $x \circ x = x$ and $Q(\circ)$

is diagonal but not necessarily a quasigroup. Clearly $x \circ y = z \circ y$ implies $x = z$. However, $x \circ y = x \circ z$ implies

$$y \cdot y = z \cdot z. \tag{6}$$

If n is even, G always has distinct elements y and z satisfying (6). If n is odd, G may be chosen as the cyclic group of order n in which the identity (6) implies $x = z$. In this latter case Q is a quasigroup. We have also proved:

COROLLARY 6.5. *For every odd integer n there exists an idempotent quasigroup Q of order n satisfying the right law of keys.*

Theorem 6.7, to follow, implies that if n is even there is no such Q.

Clearly by an identical proof we have

THEOREM 6.6. *A quasigroup Q satisfies the left law of keys $b \cdot ba = a$ if and only if every cycle is of length one or of type* (B).

Similarly Theorem 6.4 and its corollary have immediate duals with "right law of keys" replaced by "left law of keys."

THEOREM 6.7. *If Q is an idempotent quasigroup in which each cycle is either idempotent or of length two, then the order of Q is odd. Moreover, such a Q exists for each odd order.*

PROOF. Select $a \in Q$. Define $\phi: Q - \{a\} \to Q - \{a\}$ in the following manner. If $b \in Q - \{a\}$, let $\phi(b)$ be the solution, f, to $(ab)(fa) = a$. By Theorem 6.1, ϕ^2 is the identity. Moreover, as is clear from the proof of Theorem 3.1, ϕ has no fixed elements. Thus $Q - \{a\}$ must contain an even number of elements. The second example of Theorem 6.4 establishes the existence of such Q of each odd order.

Theorem 6.7 generalizes the fact that there is no symmetric diagonalized Latin square of even order. Also, it is interesting to note that Theorem 6.7 implies that the construction used in the proof of Theorem 6.4 must break down if n is even and thus proves that an abelian group must have a subgroup of order two.

REFERENCES

1. D. A. Norton and Sherman K. Stein, *An integer associated with Latin squares*, Proc. Amer. Math. Soc. vol. 7 (1956) pp. 331–334.

2. Rafael Artzy, *On loops with a special property*, Proc. Amer. Math. Soc. vol. 6 (1955) pp. 448–453.

3. Albert Sade, *Contributions à la théorie des quasi-groupes*, C. R. Acad. Sci. Paris vol. 237 (1953) pp. 420–422.

4. Eugene Netto, *Lehrbuch der Combinatorik*, 2d ed., Leipsig-Berlin, Teubner, 1927.

UNIVERSITY OF CALIFORNIA, DAVIS