Commentationes Mathematicae Universitatis Carolinae

Tomáš Kepka

A note on associative triples of elements in cancellation groupoids

Commentationes Mathematicae Universitatis Carolinae, Vol. 21 (1980), No. 3, 479--487

Persistent URL: http://dml.cz/dmlcz/106014

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE

21,3 (1980)

A NOTE ON ASSOCIATIVE TRIPLES OF ELEMENTS IN CANCELLATION GROUPOIDS

Tomáš KEPKA

Abstract: A cancellation groupoid G is a semigroup iff $x.yz = xy.z$ for all $x,y,z \in G$, $y \neq x \neq z$.

Key words: Associative triple of elements, cancellation groupoid.

Classification: 20N99

A division groupoid G is a group iff the associative law holds for any three distinct elements of G (see [1] and [2]). In the present note, similar results are proved for cancellation groupoids. It is shown that a cancellation groupoid G is a semigroup iff $x.yz = xy.z$ for all $x,y,z \in G$, $y \neq x \neq z$. On the other hand, an example of a cancellation groupoid G is constructed such that G is not associative and $x.yz = xy.z$ for all $x,y,z \in G$, $x \neq y \neq z$.

1. A groupoid G is said to be a cancellation groupoid if $b = c$, whenever $b,c \in G$ and either $ab = ac$ or $ba = ca$ for some $a \in G$. A congruence r of a groupoid G is called cancellative if G/r is a cancellation groupoid.

In the following seven lemmas, let G be a cancellation groupoid such that $x.yz = xy.z$ for all $x,y,z \in G$, $x \neq y \neq z$ and $x \neq z$.

1.1. <u>Lemma</u>. Let $a,b,c \in G$ be such that $a \neq b,c,ab,ba,ac$ and $b \neq c,ac$ and $c \neq ab,ba$. Then $a.ba = ab.a$.

Proof. We have $(a.ba)c = a(ba.c) = a(b.ac) = ab.ac = (ab.a)c$ and consequently $a.ba = ab.a$.

1.2. <u>Lemma</u>. Suppose that G contains at least seven elements. Let $a,b \in G$ be such that $a \neq b,ab.ba$. Then $a.ba = ab.a$.

Proof. According to the hypothesis, there exists $c \in G$ such that $c \neq a,b,ab,ba$ and $a \neq ac \neq b$. Then $a.ba = ab.a$ by 1.1.

1.3. <u>Lemma</u>. Let $a = ab$ for some $a,b \in G$, $a \neq b$. Then b is a left unit of G and $a.ba = aa = ab.a$.

Proof. If $c \in G$, $a \neq c \neq b$, then $a.bc = ab.c = ac$ and $bc = c$. Assume $ba \neq a$. Since G is a cancellation groupoid and $bc = c$ for every $a \neq c \neq b$, we must have $ba = b$ and $bb = a$. Hence $bb = a = ab$, $b = a$, a contradiction. Thus $ba = a$, $bb = b$, b is a left unit and $a.ba = aa = ab.a$.

1.4. <u>Lemma</u>. Let $a = ba$ for some $a,b \in G$, $a \neq b$. Then b is a right unit of G and $a.ba = aa = ab.a$.

Proof. Dual to that of 1.3.

1.5. <u>Lemma</u>. Suppose that G is a quasigroup. Then $a.aa = aa.a$ for every $a \in G$.

Proof. G is a loop by 1.3 and 1.4. Let $a \in G$. If $aa = 1$ then $a.aa = a = aa.\ a$. If $aa = a$ then $a = 1$ and $a.aa = 1 = aa.a$. Assume $1 \neq aa \neq a$. There are $b,c \in G$ such that $ab = 1 = ca$. If $b \neq c$ then $c = c1 = c.ab = ca.b = 1b = b$, a contradiction. Hence $b = c$. Put $f(x) = a.bx$ for every $x \in G$. Then f is a permutation and f(d) = a.bd = ab.d = d for $d \neq a,b$. Further, f(a) = a.ba = a, and therefore f(b) = b. Thus a.bx = x for every $x \in G$. Similarly, b.ax = xa.b = xb.a = = x. Now, if aa = b, then a.aa = 1 = aa.a. If $aa \neq b$ then a.aa = ((a.aa)b)a = (a(aa.b))a = aa.a, since aa.b = a.

1.6. <u>Lemma</u>. Suppose that G is a quasigroup. Then a.ba = ab.a, a.bb = ab.b and bb.a = b.ba for all $a,b \in G$.

Proof. With respect to 1.5, we can assume that $a \neq b$. If ab = a (ab = b) then b(a) is a left unit by 1.3 (1.4). Since G is a loop, b(a) is a unit and the result follows easily. Assume $a \neq ab \neq b$ and put f(x) = ax, g(x) = bx and $h(x) = g^{-1}f^{-1}(ab.x)$ for every $x \in G$. Then h is a permutation and h(c) = c for every $a \neq c \neq b$. If h(a) = a then h(b) = = b and a.ba = ab.a, a.bb = ab.b. Let $h(a) \neq a$. Then h(a) = = b, h(b) = a, ab.a = a.bb and ab.b = a.ba. If b = bb then b is a unit and a = ab, a contradiction. If a = bb then ab.a = a.bb = aa yields a = ab, a contradiction. Thus $a \neq$ $\neq bb \neq b$ and we have (ab.a)b = (a.bb)b = a(bb.b) = a(b.bb)= = ab.bb = (ab.b)b = (a.ba)b, ab.a = a.ba and h(a) = a = b, a contradiction. We have proved that a.ba = ab.a and a.bb= = ab.b. Similarly the rest.

1.7. <u>Lemma</u>. a.ba = ab.a for all $a,b \in G$, $a \neq b$.

Proof. With respect to 1.2, 1.3 and 1.4, we can assume that G contains at most six elements. Then G is a quasigroup and the result follows from 1.6.

In the next five lemmas, let G be a cancellation groupoid such that x.yz = xy.z for all $x,y,z \in G$ with $y \neq x \neq z$.

1.8. <u>Lemma</u>. Let $a,b,c \in G$ be such that $a \neq b,c,ab,ca$ and

$b \neq ca$ and $c \neq aa, ab$. Then $a.ab = aa.b$.

Proof. We have $c(a.ab) = ca.ab = (ca.a)b = (c.aa)b =$ $= c(aa.b)$ (apply 1.7 if $b = c$), and so $a.ab = aa.b$.

1.9. <u>Lemma</u>. Suppose that G contains at least six elements. Let $a,b \in G$ be such that $a \neq b, ab$. Then $a.ab = aa.b$.

Proof. Use 1.8.

1.10. <u>Lemma</u>. Let $a = ab$ for some $a,b \in G$, $a \neq b$. Then $a.ab = aa.b$.

Proof. By 1.3, b is a left unit of G. If $b \neq aa$ then $(aa.b)a = aa.ba = aa.a$ and $aa.b = aa = a.ab$ (use 1.7). If $b = aa$ then $aa.b = bb = b = aa = a.ab$.

1.11. <u>Lemma</u>. $a.ab = aa.b$ for all $a,b \in G$, $a \neq b$.

Proof. This is an easy consequence of 1.9, 1.10 and 1.6.

1.12. <u>Lemma</u>. $a.aa = aa.a$ for every $a \in G$.

Proof. According to 1.5, we can assume that G contains at least three elements. Then $a \neq b, ab$ for some $b \in G$. If $a =$ $= aa$ then $a.aa = a = aa.a$. If $a \neq aa$ then $(a.aa)b = a(aa.b) =$ $= a(a.ab) = aa.ab = (aa.a)b$ (use 1.7, 1.11) and $a.aa = aa.a$.

1.13. <u>Theorem</u>. A cancellation groupoid G is a semigroup, provided at least one of the following two conditions is true:

(i) $x.yz = xy.z$ for all $x,y,z \in G$ such that $y \neq x \neq z$.

(ii) $x.yz = xy.z$ for all $x,y,z \in G$ such that $y \neq z \neq x$.

Proof. (i) Apply 1.7,1.11 and 1.12.

(ii) Dual to (i).

2. Let W be an absolutely free groupoid over a non-empty set X (elements of W are called terms). For every $a \in W$,

we define two transformations L_a and R_a of W by $L_a(b) = ab$ and $R_a(b) = ba$.

Let r be a reflexive and symmetric relation defined on W. Define three relations o(r), p(r) and q(r) as follows: $(a,b) \in o(r)$ iff there are $n \geq 2$ and $a_1,\dots,a_n \in W$ such that $a = a_1$, $b = a_n$ and $(a_1,a_2),(a_2,a_3),\dots,(a_{n-1},a_n) \in r$; $(a,b) \in p(r)$ iff there are $n \geq 0$, $S^{(1)},\dots,S^{(n)} \in \{L,R\}$ and $e_1,\dots,e_n,c,d \in W$ such that $(c,d) \in r$ and $a = S^{(1)}_{e_1}\dots S^{(n)}_{e_n}(c)$, $b = S^{(1)}_{e_1}\dots S^{(n)}_{e_n}(d)$; $(a,b) \in q(r)$ iff there are $n \geq 0$, $S^{(1)},\dots$ $\dots,S^{(n)} \in \{L,R\}$ and $c_1,\dots,c_n \in W$ such that $(S^{(1)}_{c_1}\dots S^{(n)}_{c_n}(a), S^{(1)}_{c_1}\dots S^{(n)}_{c_n}(b)) \in r$. Put $t(r) = r \cup o(r) \cup po(r) \cup qpo(r) \cup$ $\cup\, oqpo(r) \cup \dots$.

2.1. __Lemma__. t(r) is a cancellative congruence of W.

Proof. Easy.

Now, suppose that r satisfies the following two conditions:

(1) If $(a,b) \in r$ then every $x \in X$ has the same number of occurrences in both a and b.

(2) If $(a,b) \in r$ and $x \in X$ then the term xx has the same number of occurrences in both a and b.

2.2. __Lemma__. o(r), p(r) and q(r) satisfy (1) and (2).

Proof. Easy.

2.3. __Lemma__. t(r) satisfies (1) and (2).

Proof. This follows from 2.2.

2.4. __Example__. Define r as follows: $(a,b) \in r$ iff either $a = b$ or there are $c,d,e \in W$ such that $c \neq d \neq e$ and $\{a,b\} =$ $= \{c.de,\ cd.e\}$. Evidently, r is reflexive and symmetric.

Moreover, r satisfies (1) and (2). By 2.1 and 2.3, $w = t(r)$ is a cancellative congruence satisfying (1) and (2). Put $G = W/w$. One may check easily that G possesses the following properties:

(i) G is a cancellation groupoid.

(ii) $x.yz = xy.z$ for all $x,y,z \in G$ such that either $x \neq y \neq z$ or $x = y = z$.

(iii) G is not a semigroup.

3. For a groupoid G, let $A(G) = \{(a,b,c) \mid a,b,c \in G, a.bc = ab.c\}$ and $B(G) = G^3 \setminus A(G)$.

3.1. <u>Lemma</u>. Let G be a cancellation groupoid and $a,b,c,d \in G$ such that $(a,bc,d),(b,c,d),(a,b,cd),(ab,c,d) \in A(G)$. Then $(a,b,c) \in A(G)$.

Proof. We have $(a.bc)d = a(bc.d) = a(b.cd) = ab.cd = (ab.c)d$, and therefore $a.bc = ab.c$.

3.2. <u>Proposition</u>. Let G be a non-associative cancellation groupoid containing at least seven elements. Then $\operatorname{card} G \leq \operatorname{card} B(G)$.

Proof. For all $a,b,c,d \in G$, let $B(a,b,c,d) = \{(a,bc,d), (b,c,d),(a,b,cd),(ab,c,d)\}$. The rest of the proof will be divided into four parts.

(i) Let $a,b,c,d,e \in G$ be such that $d \neq e$ and $B(a,b,c,d) \cap B(a,b,c,e) \neq \emptyset$. Then either $a = b = c$ or $a = ab$, $b = c$ or $b = bc$.

(ii) Suppose that there is $(a,b,c) \in B(G)$ with $bc \neq b \neq c$. By 3.1, $B(a,b,c,d) \cap B(G) \neq \emptyset$ for every $d \in G$. Now, taking into account (i), we see that $\operatorname{card} G \leq \operatorname{card} B(G)$.

(iii) Suppose that either $y = yz$ or $y = z$ for all $(x,y,z) \in$ $\in B(G)$. Since G is not a semigroup, B(G) is non-empty. Let $(a,b,c) \in B(G)$ and $d \in G$. With respect to 3.1, at least one of the following equalities is true: $c = d$, $b = cd$, $bc = d$, $c = cd$, $b.cd = b$, $bc = bc.d$. Using this, it is easy to conclude that card $G \leq 6$, a contradiction.

(ib) By (ii) and (iii), card $G \leq$ card B(G).

3.3. <u>Corollary</u>. Let G be an infinite non-associative cancellation groupoid. Then card G = card B(G).

3.4. <u>Example</u>. Let G be an infinite set. Then there is an injective mapping $f:G^2 \longrightarrow G$. The corresponding groupoid $G = G(f)$ is a cancellation groupoid and $B(G) = G^3$.

Let Q be a quasigroup. For every $a \in Q$, there exist uniquely determined elements e(a) and f(a) such that $f(a)a =$ $= a = ae(a)$. We obtain thus two transformations e and f of the set Q.

3.5. <u>Lemma</u>. Let Q be a quasigroup and $a,b,c \in Q$. Then $(a,b,c) \in A(Q)$, provided at least one of the following conditions is satisfied:

(i) $f(b) = a$ and $e(b) = c$.

(ii) $e(ab) = c = e(b)$.

(iii) $f(bc) = a = f(b)$.

(iv) $e(a) = b = f(c)$.

Proof. Obvious.

3.6. <u>Corollary</u>. card $Q \leq$ card A(Q) for any quasigroup Q.

3.7. <u>Corollary</u>. Let Q be an infinite non-associative quasigroup. Then card $A(Q)$ = card Q = card $B(Q)$.

3.8. Lemma. Let Q be a quasigroup such that $ab = b = bc$ for all $(a,b,c) \in A(Q)$. Then:

(i) The transformations e and f are injective.

(ii) Every element of $e(Q) \cap f(Q)$ is idempotent.

(iii) If both e and f are surjective then Q is idempotent.

Proof. (i) Let $a,b,c,d \in Q$, $e(a) = c = e(b)$ and $a = db$. Then $(d,b,c) \in A(Q)$, and so $a = db = b$. We have proved that e is injective. Similarly for f.

(ii) Let $a,b,c \in Q$ and $e(b) = a = f(c)$. Then $(b,a,c) \in A(Q)$, $b = ba = a = ac = c$ and $a = aa$.

(iii) This is an immediate consequence of (ii).

3.9. Proposition. Let Q be a finite quasigroup such that card Q = card $A(Q)$. Then Q is idempotent.

Proof. By 3.5 (i) and the hypothesis, $A(Q) = \{(f(a), a, e(a)) \mid a \in Q\}$. By 3.8 (i), e and f are injective. Since Q is finite, e and f are permutations and Q is idempotent by 3.8 (iii).

It seems to be an open problem whether there exists a non-trivial (finite) quasigroup Q with $A(Q) = \{(f(a),a,e(a)) \mid a \in Q\}$.

3.10. Lemma. Let Q be a finite idempotent quasigroup of order n such that Q is isotopic to a group. Then $n^2 \leq$ card $A(Q)$.

Proof. Let $a \in Q$, $h(x) = xa$, $g(x) = ax$ and $x + y = h^{-1}(x)g^{-1}(y)$ for all $x,y \in Q$. Then $Q(+)$ is a group, a is its unit, $h(a) = a = g(a)$ and $xy = h(x) + g(y)$ for all $x,y \in Q$. We have $x = xx = h(x) + g(x)$, and so $g(x) = -h(x) + x$.

Now, let $b \in Q$. There is $c \in Q$ such that $-h^2(b) + h(b) =$ $= hg(c)$. Then $b.ac = h(b) + g^2(c) = h^2(b) + hg(c) + g^2(c) =$ $= h^2(b) + g(c) = ba.c$. Hence $(b,a,c) \in A(Q)$. The rest is clear.

3.11. Proposition. Let Q be a finite non-trivial quasigroup isotopic to a group. Then card $Q <$ card $A(Q)$.

Proof. The statement follows from 3.9 and 3.10.

R e f e r e n c e s

[1] D.A. NORTON: A note on associativity, Pacific J. Math. 10(1960), 591-595.

[2] A. WAGNER: On the associative law of groups, Rend. Mat. e Appl. 21(1962), 60-76.

Matematicko-fyzikální fakulta
Universita Karlova
Sokolovská 83, 18600 Praha 8
Československo

(Oblatum 19.3. 1980)