Tomáš Kepka; Markku Niemenmaa
On splitting k-systems

Acta Universitatis Carolinae. Mathematica et Physica, Vol. 27 (1986), No. 2, 3--10

Persistent URL: `http://dml.cz/dmlcz/142568`

On Splitting k-Systems

T. KEPKA
Department of Mathematics, Charles University, Prague

M. NIEMENMAA
Department of Mathematics, University of Oulu

Received 15 November, 1985

A connection between groups and certain groupoids is investigated.

Vyšetřuje se souvislost mezi grupami a jistými grupoidy.

Изучается связь групп и некоторых группоидов.

1. Introduction

Generalizations of the notion of the arithmetic mean value have been considered e.g. in [2] and [5]. If $(G, +, \cdot)$ is an algebra where $(G, +)$ is a uniquely $2-$divisible abelian group and the multiplication is the usual arithmetic mean value, then $x + yz = xy + xz$. The aim of the present paper is to study algebraic systems satisfying identities of a similar type.

Let k be an integer. An algebra $(G, +, \cdot)$ with two binary operations is called a k-system if $(G, +)$ is a group (possibly non-commutative) and the following identity holds:

(1) $$x + k(yx) = xy + xz .$$

Let $G = (G, +, \cdot)$ be a k-system. We denote by $Z(G)$ the centre of the group $(G, +)$. If $a \in G$ then we have four transformations L_a, R_a, L_a^+ and R_a^+ of G defined by $L_a(b) = ab$, $R_a(b) = ba$, $L_a^+(b) = a + b$ and $R_a^+(b) = b + a$. Obviously, both L_a^+ and R_a^+ are permutations. Further, we define five transformations d, e, f, g and h of G by $d(a) = aa$, $e(a) = (2 - k)\, a$, $f(a) = ka$, $g(a) = (k - 1)\, a$ and $h(a) = 2a$ for every $a \in G$.

In the sequel we shall need the following simple result.

1.1. Lemma. Let $k \neq 0$ be an integer and $(G, +)$ a 2-divisible group such that $ka = 0$ for every $a \in G$. Then $(G, +)$ is uniquely 2-divisible.

*) 186 00 Praha, Sokolovská 83, Czechoslovakia
**) 90570 Oulu, Finland

1.2. Example. Let $(G, +)$ be a 2-divisible group and let t be any transformation of G such that $2\,t(a) = a$ for every $a \in G$. Put $ab = t(a)$ for all $a, b \in G$. Then $(G, +, \cdot)$ is a 0-system.

1.3. Example Let $(G, +)$ be a 2-divisible abelian group and let t be any transformation of G such that $2\,t(a) = a$ for every $a \in G$. Put $ab = t(a) + t(b)$ for all $a, b \in G$. Then $(G, +, \cdot)$ is a 1-system.

1.4. Example. Let k be an integer and $(G, +)$ a group such that $ka = 0$ for every $a \in G$. Suppose further that the group $(G, +)$ is uniquely 2-divisible (e.g. k is odd or $k \neq 0$ and $(G, +)$ 2-divisible – see 1.1) and put $ab = a/2$ for all $a, b \in G$. Then $(G, +, \cdot)$ is a k-system.

The k-systems constructed in 1.4 will be called k-systems of type one.

1.5. Example. Let k be an integer and $(G, +)$ an abelian group such that $(k - 1)\,a = 0$ for every $a \in G$. Suppose further that the group $(G, +)$ is uniquely 2-divisible (e.g. k even or $k \neq 1$ and $(G, +)$ 2-divisible – see 1.1) and put $ab = a/2 + b/2$ for all $a, b \in G$. Then $(G, +, \cdot)$ is a k-system.

The k-systems constructed in 1.5 will be called k-systems of type two.

1.6. Example. Let k be an integer and $(G, +)$ a group such that $k(k - 1)\,a = 0$ and $ka \in Z(G)$ for every $a \in G$. Suppose further that the group $(G, +)$ is uniquely 2-divisible (e.g. $k \neq 0, 1$ and $(G, +)$ 2-divisible – see 1.1) and put $ab = a/2 + kb/2$ for all $a, b \in G$. Then $(G, +, \cdot)$ is a k-system.

A k-system G is said to be splitting if it is isomorphic to the direct sum of a k-system of type one and a k-system of type two.

Finally, the reader should consult [1] and [4] for definions, notation etc.

2. Basic properties of k-systems

In this section let G be a k-system.

2.1. Lemma. For all $a, b \in G$: (2) $a = (2 - k)(aa)$, (3) $(k - 1)(ab) = -a + aa = (k - 1)(aa)$, (4) $2(ab) + (2 - 2k)(bb) = a + b$, (5) $2(ab) = a + k(bb)$.

These equalities are easy consequences of (1).

2.2. Lemma. $k(k - 1)\,a = 0$ for every $a \in G$.

Proof. We have $k(k - 1)(aa) = (k - 1)(0 + k)(aa)) = (k - 1)\,2(0a) = 2(k - 1)(0a) = 2(00)$ by (3) and (5). Hence, by (2), $k(k - 1)\,a = k(k - 1)\,.\,(2 - k)(aa) = 2(2 - k)(00) = 0$.

2.3. Lemma. (i) $ed = \mathrm{id}_G$, (ii) gL_a is constant for every $a \in G$, (iii) $R_a^+ = R^+_{-hgd(a)}hR_a$ and $R^+_{k(aa)} = hR_a$ for every $a \in G$, (iv) $L_a^+ fL_b = L_{ab}L_a$ for all $a, b \in G$, (v) $L_a^+ fR_b = R_{ab}^+ L_a$ for all $a, b \in G$.

Proof. (i) follows from (2), (ii) from (3), (iii) from (4) and finally (iv) and (v) follow from (1).

2.4. Lemma. The transformation e is surjective, d is injective, h is surjective and R_a is injective for every $a \in G$.

Proof. Use 2.3.

2.5. Corollary. (i) The group $(G, +)$ is 2-divisible and $(k - 2)$-divisible, (ii) The group $(G, +)$ is uniquely 2-divisible provided that $k \neq 0, 1$, (iii) Let $k \neq 0, 1$ and $k(k - 1) = 2^i j$, $i \geqq 0$, j odd. Then $ja = 0$ for every $a \in G$. (iv) The groupoid $(G, \cdot)$ is right cancellative.

2.6. Proposition. The following conditions are equivalent:

(i) The groupoid $(G, \cdot)$ is right divisible.
(ii) The groupoid $(G, \cdot)$ is a right quasigroup.
(iii) The group $(G, +)$ is uniquely 2-divisible.

Furthermore, these conditions are satisfied if $k \neq 0, 1$.

Proof. See 2.3 (iii) and 2.5.

Now k-systems satisfying the equivalent conditions of 2.6 are said to be regular.

2.7. Lemma. Let $a, b, c \in G$ be such that $ab = ac$. Then $fL_b = fL_c$, $fR_b = fR_c$ and $f(bb) = f(cc)$.

Proof. By 2.3 (iv), $L_a^+ fL_b = L_{ab}^+ L_a = L_{ac}^+ L_a f L_c$, so that $fL_b = fL_c$. Similarly $fR_b = fR_c$. Combining the two equations we get $f(bb) = f(cc)$.

2.8. Lemma. For all $a, b \in G$: (i) $k(aa) = ka$ and (ii) $2(ab) = a + kb$.

Proof. (i) We have $ka = k(2 - k)(aa) = (2 - k) k(aa) = 2k(aa) - k^2(aa)$. By 2.2, $k^2(aa) = k(aa)$ and hence $ka = k(aa)$.

(ii) This follows from (i) and (5).

2.9. Lemma. $2(00) = 0$ and if $k = 0$, then $00 = 0$.

Proof. By 2.8 (ii), $2(00) = 0$. If $k \neq 0, 1$ then $(G, +)$ is uniquely 2-divisible and $00 = 0$. If $k = 1$, then $00 = 0$ by (2).

2.10. Lemma. Let G be regular. Then kc and $kc/2$ are elements of $Z(G)$ for every $c \in G$.

Proof. Put $q = h^{-1}$. By 2.8 (ii), $ab = q(a + kb)$ for all $a, b \in G$. Let $c \in G$. Now the equation (1) can be written in the form:

$$a + kq(b + kc) = q(a + kb) + q(a + kc).$$

For $a = 0$ we have

$$kq(b + kc) = q(kb) + q(kc),$$

so that

$$a + q(kb) + q(kc) = q(a + kb) + q(a + kc).$$

From this, for $c = 0$, we see that

$$a + q(kb) = q(a + kb) + q(a),$$

hence

$$a + q(kb) - q(a) = q(a + kb),$$

and therefore

$$a + q(kb) + q(kc) = a + q(kb) - q(a) + a + q(kc) - q(a).$$

Consequently,

$$q(kc) = q(a) + q(kc) - q(a),$$

so that $q(kc) \in Z(G)$.

3. 0-systems

3.1. Proposition. Let G be a 0-system. Then there exists a transformation t of G such that $2\,t(a) = a$ and $ab = t(a)$ for all $a, b \in G$.

Proof. It is enough to put $t(a) = aa$ for every $a \in G$. Now the result follows from (2) and (3).

4. 1-systems

In this section let G be a 1-system.

4.1. Lemma. (i) $a = aa$ and $2(ab) = a + b$ for all $a, b \in G$. (ii) $f = \mathrm{id}_G$. (iii) $L_a^+ L_b = L_{ab}^+ L_a$ for all $a, b \in G$. (iv) $L_a^+ R_b = R_{ab}^+ L_a$ for all $a, b \in G$. (v) $L_0 = R_0$. (vi) $L_{a0}^+ L_a = R_{a0}^+ L_a$ for every $a \in G$.

Proof. (i) follows from (2) and (5), (ii) is obvious, (iii) follows from 2.3 (iv) and (iv) from 2.3 (v). To prove (v) notice that we have $L_0 = R_0^+ L_0 = R_{00}^+ L_0 = L_0^+ R_0 = R_0$. Finally (vi) is clear from (iii), (iv) and (v).

4.2. Lemma. Let $a \in G$ such that $0a \in Z(G)$. Then $L_a = R_a$.

Proof. By 4.1 (iii) and (iv), $L_a = L_{0a}^+ L_0 = R_{0a}^+ L_0 = R_a$.

4.3. Lemma. $a\,0 \in Z(G)$ for every $a \in G$.

Proof. By 4.1 (vi), $a\,0 + a\,b = ab + a0$ for each $b \in G$. Hence, by 4.1 (i), $a\,0 + a + b = a\,0 + 2(ab) = 2(ab) + a\,0 = b + a\,0$.

4.4. Lemma. Both the group $(G, +)$ and the groupoid $(G, \cdot)$ are commutative.

Proof. By 4.1 (v) and 4.3, $a\,0 = 0a \in Z(G)$ for every $a \in G$. Now $(G, \cdot)$ is commutative by 4.2 and $(G, +)$ by 4.1 (i).

4.5. Proposition. $(G, +)$ is an abelian group and there exists a transformation t of G such that $2\,t(a) = a$, $t(0)$ and $ab = t(a) + t(b)$ for all $a, b \in G$.

Proof. Put $t(a) = a\,0$. Then $2\,t(a) = a$ by 4.1 (i), $t(0) = 0$ by 4.1 (i) and $t(a) + t(b) = 0a + 0b = 0 + ab = ab$.

5. k-systems of type 1

5.1. Proposition. The following conditions are equivalent for a k-system G:
(i) $ka = 0$ for every $a \in G$.
(ii) $ab = ac$ for all $a, b, c \in G$.
(iii) Either $k = 0$ or G is of type 1.

Proof. (i) implies (ii): This follows immediately from (3). (ii) implies (i): This follows easily from 2.8 (ii). (i) implies (iii): Suppose that $k \neq 0$. Then $(G, +)$ is uniquely 2-divisible and $ab = a/2$ by 2.8 (ii). Thus G is of type one. (iii) implies (i): This is trivial.

5.2. Proposition. Now a 0-system is of type one iff it is regular.

Proof. Use 3.1.

5.3. Lemma. Let $k = \pm 2^i$, $i \geqq 0$. Then every k-system of type one is trivial (i.e. a one-element set).

Proof. Obvious.

6. k-systems of type 2

6.1. Proposition. The following conditions are equivalent for a k-system G:
(i) $(k - 1)\,a = 0$ for every $a \in G$.
(ii) The groupoid $(G, \cdot)$ is idempotent.
(iii) The groupoid $(G, \cdot)$ is commutative.
(iv) Either $k = 1$ or G is of type 2.

Proof. (i) is equivalent to (ii): This is clear from (2). (i) implies (iv): suppose that $k \neq 1$. Then G is regular and $(G, +)$ is abelian by 2.10. Now $ab = a/2 + b/2$ by 2.8 (ii), so that G is of type 2. (iv) implies (iii): This is obvious. (iii) implies (i): By 2.8 (ii), $a + kb = 2(ab) = 2(ba) = b + ka$ for all $a, b \in G$. Thus for $b = 0$ we have $(k - 1)\,a = 0$.

6.2. Proposition. Now a 1-system is of type 2 iff it is regular.

Proof. Use 4.5.

6.3. Lemma. Let $k = \pm 2^i$, $i \geqq 0$. Then every k-system of type 2 is trivial.

Proof. Obvious.

7. Several consequences

7.1. Proposition. Let G be a k-system. Then $ka \in Z(G)$ for every $a \in G$. Moreover, if G is regular then $ka/2 \in Z(G)$.

Proof. The assertion is trivial for $k = 0$ and it follows from 4.5 for $k = 1$. If $k \neq 0, 1$ then G is regular and 2.10 can be applied.

7.2. Theorem. Let G be a regular k-system. Then $ab = a/2 + kb/2$ for all $a, b \in G$.

Proof. The statement follows easily from 2.8 (ii) and 7.1.

7.3. Proposition. Let G be a k-system and $H = \{a \in G: (k-1)\, a = 0\}$. Then:
(i) $(H, +)$ is a normal subgroup of $(G, +)$, $H \subseteq Z(G)$ and $ka \in H$ for every $a \in G$.
(ii) H is a subsystem of the k-system G and H is a k-system of type 2 provided that either $k \neq 1$ or G is regular.

Proof. If $k = 0, 1$ then the situation is clear. Now assume that $k \neq 0, 1$. By 7.1 and 2.2, $H \subseteq Z(G)$ and $ka \in H$ for every $a \in G$. Thus $(H, +)$ is a normal subgroup of $(G, +)$. By 1.1, the group $(G, +)/(H, +)$ is uniquely 2-divisible and we see that $a/2 \in H$ for every $a \in H$. The rest is clear from 7.2.

7.4. Proposition. Let $k \neq 0$ and let G be a k-system. Then: (i) $Z(G)$ is a subsystem of G. (ii) $Z(G)$ is an abelian k-system.

Proof. We can proceed similarly as in the proof of 7.3.

7.5. Proposition. Let G be a k-system. Define a relation r on G by $(a, b) \in r$ iff $a - b \in H$. Then

(i) r is a congruence of the k-system G.
(ii) H is one of the blocks of G.
(iii) The factor system G/r is a k-system of type one provided $k \neq 0$.

Proof. We can assume that $k \neq 0, 1$. Now let $a, b, c \in G$ with $(b, c) \in r$. Then $b - c \in H$ and $ab - ac = a/2 + kb/2 - kc/2 - a/2 = kb/2 - kc/2$. Further, $(k-1)(kb/2 - kc/2) = 0$. We see that $ab - ac \in H$, so that $(ab, ac) \in r$. Similarly, $ba - ca = b/2 - c/2 = (b - c)/2 + c/2 - c/2 = (b - c)/2$. Thus $ba - ca \in H$ and $(ba, ca) \in r$. We conclude that r is a congruence of the k-system G. The rest is clear.

7.6. Proposition. Let G be a regular k-system. Then the groupoid $(G, \cdot)$ is medial (i.e. satisfies the identity $xy\,.\,uv = xu\,.\,yv$).

Proof. Apply 7.1 and 7.2.

8. Some k-systems

8.1. Proposition. (i) Every 2-system is trivial.
(ii) Let $i \geqq 1$. Then every $\pm 2^i$-system is of type 2.
(iii) Le: $i \geqq 1$ and $k = \pm 2^i + 1$. Then every k-system is of type 1.

Proof (i): This is clear from (2). (ii): Let G be a $\pm 2^i$-system. Consider the congruence r of G by 7.5. From 5.3 and 7.5 (ii) it follows that $r = G \times G$, i.e. $H = G$ and G is of type 2. (iii): Using 6.3, we can proceed in the same way as in the proof of (ii).

9. Splitting k-systems

In this section, let $k \neq 0, 1$ and let G be a k-system. Put $K = \{a \in G: ka = 0\}$ and define a relation s on G by $(a, b) \in s$ iff $a - b \in K$.

9.1. Lemma. (i) $(k - 1)\, a \in K$ for every $a \in G$.

(ii) $H \cap K = 0$, $H + K = G$ and each element g of G has a unique expression of the form $g = h + x$, where $h \in H$ and $x \in K$.

(iii) s is reflexive and symmetric.

(i3) $r \cap s = \mathrm{id}_G$.

Proof. Now (i), (iii) and (iv) are clearly true. As for (ii), it is easy to see that $H \cap K = 0$ and $H + K = G$. Let $g = h_1 + x_1 = h_2 + x_4$, where $h_i \in H$ and $x_i \in K$ $(i = 1, 2)$. Then $h_1 - h_4 = x_2 - x_1 \in H \subseteq Z(G)$. Thus $2(x_4 - x_1) = (x_2 - x_1) + (x_2 - x_1) = x_2 + (x_2 - x_1) - x_1 = 2x_2 - 2x_1$. By induction, $k(x_2 - x_1) = kx_4$ W $kx_1 = 0$, hence $x_2 - x_1 \in K$. Now $x_2 - x_1 \in H \cap K = 0$, so that $x_2 = x_1$ and $h_1 = h_2$ yeilding the uniqueness of the expression.

9.2. Theorem. If G is a k-system, then it is splitting.

Proof. Define a mapping $m: G \to H \oplus G/H$ (direct sum) by $m(g) = (h, x + H)$, where g has the unique expression $g = h + x(h \in H, x \in K)$. This mapping is a group homomorphism with $\mathrm{Ker}\,(m) = 0$ and $\mathrm{Im}\,(m) = H \oplus G/H$. Hence

$$(G, +) \cong (H, +) \oplus (G, +)/(H, +)$$

and now it is clear that G is splitting by 7.3 and 7.5.

9.3. Corollary. If G is a k-system, then

(i) $(K, +)$ is a normal subgroup of $(G, +)$.

(ii) The transformation f is an endomorphism of $(G, +)$.

(iii) s is a congruence of the k-system G.

Proof. Now (i) and (ii) follow from 9.2 and (iii) is a consequence of 7.2.

10. Finite k-systems

10.1. Proposition. Let G be a finite k-system of order n. Then n is odd and G is splitting.

Proof. Use 2.6 and 9.3 (the cases $k = 0, 1$ are trivial).

Now let G be a finite 1-system of odd order n. By 4.4 it is easy to see that $(G, \cdot)$ is a commutative quasigroup. Thus the transformations $L_a = R_a$ $(a \in G)$ are permutations of G and they generate the multiplication group of $(G, \cdot)$ which we denote by $M(G, \cdot)$.

Denote by t the mapping $x \to ((n + 1)/2)\, x$. Clearly, t is an automorphism of $(G, +)$. Now we prove

10.2. Proposition. Let G be a finite 1-system with odd order $n = p_1^{a_1} \dots p_n^{a_n}$ (the primary decomposition of n, n odd.). Then $M(G, \cdot)$ is the group theoretical splitting extension of $(G, \cdot)$ by $\langle t \rangle$. Furthermore,

$$o(t) \mid 1\ \mathrm{cm}\, .\, (p_1^{a_1} - p_1^{a_1 - 1}, \dots, p_n^{a_n} - p_n^{a_n - 1})\, .$$

Proof. The first part of the proposition follows from lemma 2.2 in [3]. Since $(n + 1)/2$ is a unit in z_n and n is odd, the well-known properties of the group of units of z_n imply the second past.

References

[1] BRUCK, R. H.: A survey of binary systems (Springer, Berlin 1971).

[2] JEŽEK, J., KEPKA, T., NĚMEC, P.: Distributive groupoids. Rozpravy Československé Akademie Ved 91/3 (Piaha, 1981).

[3] KEPKA, T.: Multiplication groups of some quasigroups. Universal Algebra (Proc. Conf. Esztergom, 1977). Colloq. Math. Soc. Janos Bolyai 29 (North-Holland, Amsterdam 1982), 459—465.

[4] ROSE, J.: A course in group theory (Cambridge University Press, Cambridge 1978).

[5] SOUBLIN, J. P.: Etude algébrique de la notion de moyenne. J. Math. Pures et Appl. 50 (1971), 53—264.