G. ČUPONA, D. DIMOVSKI, A. SAMARDŽISKI

FULLY COMMUTATIVE VECTOR VALUED GROUPS

Abstract: In this paper we introduce the notion of fully commutative vector valued i.e. (n, m)-groups. A pair (Q, f), where Q is a nonempty set, is said to be a fully commutative (n, m)-group, $n-m=k\geqslant 1$, if f is an associative mapping from $Q^{(n)}$ into $Q^{(m)}$, such that for each $a\in Q^{(k)}$, $b\in Q^{(m)}$, the equation $f(ax)=b$ has a solution $x\in Q^{(m)}$. Here, $Q^{(p)}$, for p a positive integer, is the subset $\{a_1\ldots a_p \mid a_i\in Q\}$ of the free commutative semigroup $Q^{(+)}$ generated by Q. We show that a nonempty set Q is a carrier of a fully commutative (n, m)-group for $m\geqslant 2$, if and only if $|Q|\leqslant 2$ or Q is infinite, and give a complete description of the fully commutative (n, m)-groups with two elements, for $m\geqslant 2$.

§ 0. INTRODUCTION

In [1] and [2] the notions of vector valued (v.v.) groupoids, semigroups and groups are introduced, generalizing the notions of (usual, binary) groupoids, semigroups and groups, and also of n-groupoids, n-semigroups and n-groups. The notions of fully commutative (f.c.) v.v. groupoids and quasigroups are introduced in [3]. Here we introduce and examine the notion of f.c. v.v. groups, generalizing the notion of commutative groups.

In § 1 we give a brief review of the notions and some known results about v.v. groups. The definitions and the basic results about f.c. v.v. groupoids and semigroups are given in § 2. In § 3 we introduce the notion of f.c. v.v. groups, and show (via universal coverings) that they are in fact a special class of (binary) commutative groups. § 4 is concerned with finite f.c. v.v. groups, where we show that a finite set Q is a carrier of a f.c. (n, m)-group, $m\geqslant 2$, if and only if $|Q|\leqslant 2$, and give a complete characterisation of f.c. (n, m)-groups $(m\geqslant 2)$ with two elements. The fact that every infinite set is a carrier of a f.c. (n, m)-group $(m\geqslant 2)$ is given in § 5, via a specific combinatorial construction.

§ 1. VECTOR VALUED SEMIGROUPS AND GROUPS

Let Q be a nonempty set.

For a positive integer p, Q^p denotes the p-th cartesian power of Q. Instead of writing $(a_1, \ldots, a_p)$ for an element of Q^p, we will use the notations a_1^p and $a_1 \ldots a_p$. With this notation, we can identify Q^p with the subset $\{a_1 \ldots a_p \mid a_i \in Q\}$ of the free semigroup Q^+ generated by Q. (Here, $a_1 \ldots a_p$ denotes the product of $a_1, \ldots, a_p$ in Q^+.)

Let m and n be positive integers with $n-m=k \geqslant 1$. A map $f: Q^n \to Q^m$ is called (n, m)-operation, and (Q, f) is called (n, m)-groupoid. We say that an (n, m)-groupoid is commutative, if

$$f(a_1^n) = f(b_1^n) \tag{1.1}$$

for every $a_1^n \in Q^n$, and every permutation b_1^n of a_1^n. An (n, m)-groupoid is called (n, m)-semigroup, if for every $1 \leqslant i \leqslant k$, and every $x_1^{n+k} \in Q^{n+k}$,

$$f(x_1^i f(x_{i+1}^{i+n}) x_{i+n+1}^{n+k}) = f(f(x_1^n) x_{n+1}^{n+k}). \tag{1.2}$$

An (n, m)-semigroup is called (n, m)-group, if for each $a \in Q^k$, $b \in Q^m$, the equations

$$f(ax) = b = f(ya) \tag{1.3}$$

have solutions $x, y \in Q^m$.

It is clear that the notions of $(n,1)$-groupoids, semigroups and groups, are the same as the notions of n-groupoids, n-semigroups and n-groups, and specially for $n=2$, are the same as the notions of groupoids, semigroups and groups. So, from now on, we consider (n, m)-operations, groupoids, semigroups and groups, only for $n-m=k \geqslant 1$, $m \geqslant 2$, and call them vector valued (abbreviated v.v.) operations, groupoids, semigroups and groups.

In [4] it is proved that if (Q, f) is a commutative v.v. group, then $|Q|=1$. In [5] is proved that if (Q, f) is an $(m+1, m)$-group $(m \geqslant 2)$, and Q is a finite set, then $|Q| = 1$, and that every infinite set is a carrier of an (n, m)-group for each n, m $(m \geqslant 2)$. If m is a divisor of n, then every set is a carrier of an (n, m)-group [2]. The generalization of the associative law for the binary operations is formulated in the following:

Theorem 1.1. (The general associative law: GAL, [4].) Let (Q, f) be an (n, m)-semigroup, and let a collection of v.v. operations f^s, $s \geqslant 1$, $f^s : Q^{m+sk} \to Q^m$ on Q be defined by:

$$f^1 = f;\ f^{s+1}(x_1^{m+sk} y_1^k) = f(f^s(x_1^{m+sk}) y_1^k). \tag{1.4}$$

Then:

(i) For every $a_\nu, b_\nu \in Q$, $s, t \geqslant 1$, $0 \leqslant j \leqslant sk$,
$$f^s(b_1^j f^t(a_1^{m+tk}) b_{j+1}^{sk}) = f^{s+t}(b_1^j a_1^{m+tk} b_{j+1}^{sk}); \tag{1.5}$$

(ii) (Q, f^s) is an $(m+sk, m)$-semigroup

for every $s \geqslant 1$; and

(iii) If (Q, f) is commutative, then (Q, f^s) is commutative as well, for every $s \geqslant 1$. ■

§ 2. FULLY COMMUTATIVE V.V. SEMIGROUPS

Let Q be a nonempty set. Denote by $Q^{(+)}$ the free abelian semigroup generated by Q. If p is a positive integer, let $Q^{(p)}$ be the subset $\{a_1 \ldots a_p \mid a_i \in Q\}$ of $Q^{(+)}$, where $a_1 \ldots a_p$ is the product of $a_1, \ldots, a_p$ in $Q^{(+)}$. As in § 1 we will use the notation a_1^p instead of $a_1 \ldots a_p$, keeping in mind that $a_1^p = b_1^p$ in $Q^{(p)}$, for $a_i, b_i \in Q$ if and only if $b_1, \ldots, b_p$ is a permutation of $a_1, \ldots, a_p$. Considering Q^p as a subset of Q^+ (see § 1), let $\pi_p : Q^p \to Q^{(p)}$ be the natural projection. Note, that $\pi_p(a_1^p) = \pi_p(b_1^p)$ if and only if $b_1, \ldots, b_p$ is a permutation of $a_1, \ldots, a_p$ i. e. $a_1^p = b_1^p$ in $Q^{(+)}$.

Let n, m be positive integers such that $n - m = k \geqslant 1$. A map $f : Q^{(n)} \to Q^{(m)}$ is called fully commutative (abbreviated f.c.) (n, m)-operation on Q, and (Q, f) is called f. c. (n, m)-groupoid (see [3]). We say that a f. c. (n, m)-groupoid (Q, f) is induced by an (n, m)-groupoid (Q, g) if the following diagram commutes:

$$\begin{array}{ccc} Q^n & \xrightarrow{\quad g \quad} & Q^m \\ \pi_n \Big\downarrow & & \Big\downarrow \pi_m \\ Q^{(n)} & \xrightarrow{\quad f \quad} & Q^{(m)} . \end{array} \tag{2.1}$$

An (n, m)-groupoid which induces a f.c. (n, m)-groupoid is called weakly commutative (n, m)-groupoid. A commutative (n, m)-groupoid is weakly commutative, but the converse is not true in general. In [3] it is shown that each f.c. (n, m)-groupoid is induced by a set of weakly commutative (n, m)-groupoids. some of which are commutative.

A f.c. (n, m)-groupoid (Q, f) is called f.c. (n, m)-semigroup, if for each $1 \leqslant i \leqslant k$, and each $x_1^{n+k} \in Q^{(n+k)}$,

$$f\,(f(x_1^n)\; x_{n+1}^{n+k}) = f\,(x_1^i\; f\,(x_{i+1}^{i+n})\; x_{i+n+1}^{n+k}). \tag{2.2}$$

It is easy to check that: a f.c. (n, m)-groupoid is a f.c. (n, m)-semigroup if and only if for each $x_1^{n+k} \in Q^{(n+k)}$,

$$f\,(f\,(x_1^n)\; x_{n+1}^{n+k}) = f\,(f\,(x_2^{n+1}) x_{n+2}^{n+k} x_1); \tag{2.2'}$$

and a f.c. (n, m)-groupoid induced by a commutative (n, m)-semigroup is a f.c. (n, m)-semigroup.

If (Q, f) is a f.c. (n, m)-semigroup, and for each $a \in Q^{(p)}$ we choose only one element $\bar{a} \in Q^p$ such that $\pi_p(\bar{a}) = a$, then a straightforward computation shows that (Q, g), where $g(a) = \overline{f(a)}$, is a commutative (n, m)-semigroup, inducing (Q, f). Using this, and T. 1.1. (GAL), we obtain:

Theorem 2.1. (The general f.c. associative law: GALFC.) Let (Q, f) be a f.c. (n, m)-semigroup induced by an (n, m)-semigroup (Q, g), $n-m=k\geqslant 1$, and for each $s \geqslant 1$, $f^{(s)}: Q^{(m+sk)} \to Q^{(m)}$ be defined by

$$f^{(1)} = f;\ f^{(s+1)}(a_1^{m+sk}b_1^k) = f(f^{(s)}(a_1^{m+sk})b_1^k). \qquad (2.3)$$

Then:

(i) For each $s \geqslant 1$, $(Q, f^{(s)})$ is a f.c. $(m+sk, m)$-semigroup induced by (Q, g^s); and

(ii) For each $s, t \geqslant 1$, $a_\nu, b_\nu \in Q$,

$$f^{(t)}(f^{(s)}(a_1^{m+sk})b_1^{tk}) = f^{(s+t)}(a_1^{m+sk}b_1^{tk}). \ ∎ \qquad (2.4)$$

If (Q,f) is a f.c. (n, m)-semigroup, then we say that the f.c. $(m+sk, m)$-semigroup $(Q, f^{(s)})$ is *derived* from (Q,f).

Because of the GALFC, we use the notation $[\ \ ]: Q^{(n)} \to Q^{(m)}$, instead of $f: Q^{(n)} \to Q^{(m)}$, and $[a_1^{m+sk}]$ instead of $[\ \ ]^{(s)}(x_1^{m+sk})$.

As an application of: the fact that every f.c. (n, m)-semigroup is induced by a commutative (n, m)-semigroup; T.2.1; and Post Theorem for commutative v.v. semigroups [6]; we obtain the following corresponding Post Theorem for f.c. v.v. semigroups.

Theorem 2.2. If $(Q, [\ \ ])$ is a f.c. $(m+sk, m)$-semigroup, then there exists a f.c. $(m+k, m)$-semigroup $(P, [\ \ ]')$, such that $Q \subseteq P$, and for every $x_1^{m+sk} \in Q^{(m+sk)}$,

$$[x_1^{m+sk}] = [x_1^{m+sk}]'. \ ∎$$

Cancellative f.c. v.v. semigroups are a special subclass of f.c. v.v. semigroups. Namely, a f.c. (n, m)-semigroup $(Q, [\ \ ])$ is said to be *cancellative* if for each $a \in Q^{(k)}$, $b,c \in Q^{(m)}$

$$[ab] = [ac] \Rightarrow b = c.$$

We say that a f.c. (n, m)-semigroup $(Q, [\ ])$ is a f.c. ***(n, m)-group***, if for each $a \in Q^{(k)}$, $b \in Q^{(m)}$, the equation $[ax] = b$ has a solution in $Q^{(m)}$.

Since f.c. $(n, 1)$-groups are commutative $(n, 1)$-groups, further on, we will always assume that $m \geqslant 2$, and by a f.c. v.v. group we will mean a f.c. (n, m)-group, for $m \geqslant 2$.

Using GALFC similarly as in (T.5.b), [6]) we obtain the following:

Proposition 2.3. If $(Q, [\ \ ])$ is a f.c. (n, m)-semigroup, $n-m=k \geqslant 1$, then the following statements are equivalent.

(i) $(Q, [\ \ ])$ is a f.c. (n, m)-group;

(ii) $(Q, [\ \ ])$ is a f.c. $(m+sk, m)$-group for some $s \geqslant 1$; and

(iii) $(Q, [\ \ ])$ is a f.c. $(m+sk, m)$-group for each $s \geqslant 1$. ∎

(We note that a corresponding statement for cancellative f.c. v.v. semigroups holds, as well. Compare with [4]).

§ 3. UNIVERSAL COVERING ABELIAN GROUPS

In this section we assume that $(Q, [\ ])$ is a given f.c. (n, m)-group, $n-m=k \geqslant 1$, and p is the least non negative integer, such that $m+p \equiv 0 \pmod{k}$.

For an arbitrary $c \in Q^{(p)}$ we define an operation $*$ (which depends on c) on $Q^{(m)}$ by:

$$a * b = [acb], \tag{3.1}$$

and for $p = 0$

$$a * b = [ab]. \tag{3.2}$$

P.2.3. implies the following:

Proposition 3.1. $(Q,*)$ is a commutative group. ∎

As a corollary of P.3.1. we obtain the following:

Proposition 3.2. $(Q, [\ ])$ is cancellative. ∎

If $x \in Q^{(\alpha)} \subseteq Q^{(+)}$, we say that dimension of x is α, and write $\dim x = \alpha$. Define a relation $\simeq$ on $Q^{(+)}$ by:

$$u \simeq v \Leftrightarrow (\exists a \in Q^{(+)})\ [au] = [av]. \tag{3.3}$$

As a direct consequence of the definition of $\simeq$, we have the following:

Proposition 3.3. (i) $u \simeq v \Rightarrow \dim u \equiv \dim v \pmod{k}$.

(ii) $\simeq$ is a congruence on the free commutative semigroup $Q^{(+)}$, and $Q^{(+)}/\simeq$ is a commutative group, denoted by $Q^{(v)}$ (i.e. $Q^{(v)} = Q^{(+)}/\simeq$). ∎

The following statements can be easely proved.

Proposition 3.4.

(i) $\dim u = \dim v \leqslant m \Rightarrow (u \simeq v \Rightarrow u = v)$;

(ii) $\dim u \leqslant \dim v < \dim u + k \Rightarrow (u \simeq v \Rightarrow \dim u = \dim v)$;

(iii) If $\alpha \geqslant 1$ and j is the smallest non negative integer such that $\alpha \equiv m+j \pmod{k}$, then for each $u \in Q^{(\alpha)}$, $v \in Q^{(j)}$ there exists a unique $w \in Q^{(m)}$ such that $u \simeq vw$. (In the case $j=0$, v is the "empty symbol", i.e. $u \simeq w$.);

(iv) $Q_{m+p} = Q^{(m+p)}/\simeq$ is a subgroup of $Q^{(v)}$. ∎

We say that $Q^{(v)}$ is a universal covering group for $(Q, [\ ])$. Next, we will give more convenient description of $Q^{(v)}$. For this we need the following notations. Let $(G, \cdot)$ be a multiplicatively denoted commutative group, and $Q \subseteq G$ a nonempty subset. We define a family $\{Q_\alpha \mid \alpha \geqslant 1\}$ of subsets of G by:

$$Q_1 = Q,\ Q_{\alpha+1} = Q_\alpha \cdot Q, \tag{3.4}$$

where $M \cdot N = \{xy \mid x \in M, y \in N\}$ for $M, N \subseteq G$. For t, a positive integer, we denote by τ_t the canonical map $Q^{(t)} \to Q_t$ defined by:

$$\tau_t(a_1^t) = a_1 \cdot a_2 \cdot \ldots \cdot a_{t-1} \cdot a_t. \tag{3.5}$$

Theorem 3.5. Let $(G, \cdot)$ be a commutative group, and Q be a nonempty subset of G such that the following conditions are satisfied:

(a) The map $\tau_m : Q^{(m)} \to Q_m$ is bijective;

(b) For each $x \in Q_k$, $Q_m = x \cdot Q_m (= \{x\} Q_m)$;

(c) If $0 \leqslant i \leqslant j < k$ and $Q_{m+i} \cap Q_{m+j} \neq \emptyset$, then $i = j$;

(d) $G = \bigcup_{\alpha \geq 1} Q_\alpha$.

Then, $(Q, [\;])$, where

$$[a_1^n] = b_1^m \Leftrightarrow \tau_n(a_1^n) = \tau_m(b_1^m), \tag{3.6}$$

is a f.c. (n, m)-group. Moreover, $Q^{(\nu)}$ is isomorphic to G.

Proof. (b) implies that for each $t \geqslant 0$, $Q_m = Q_{m+tk}$, and (3.5) implies that, if $\tau_n(a_1^n) = \tau_m(b_1^m)$ and $\tau_n(b_1^m a_{n+1}^{n+k}) = \tau_m(c_1^m)$, then $\tau_{n+k}(a_1^{n+k}) = \tau_m(c_1^m)$. This, together with (a) and the fact that $(G, \cdot)$ is a commutative group, implies that $(Q, [\;])$ is a f.c. (n, m)-group.

Next, we show that the following generalization of (c), holds.

(c′) $Q_\alpha \cap Q_\beta \neq \emptyset \Rightarrow \alpha \equiv \beta \pmod{k}$.

For $\alpha \geqslant m$, $\beta \geqslant m$, (c′) follows from (c) and (b).

Without loss of generality, we may assume that $\alpha < \beta$. Let $\alpha < m$. If $c \in Q^{(m-\alpha)}$, then $Q_\alpha \cap Q_\beta \neq \emptyset$ implies that $\tau_{m-\alpha}(c) \cdot Q_\alpha \cap \tau_{m-\alpha}(c) \cdot Q_\beta \neq \emptyset$, which by (a) implies that $Q_m \cap Q_{m+\beta-\alpha} \neq \emptyset$. Now (c′) for $\alpha = m$, $\beta \geqslant m$ implies that $\beta - \alpha \equiv 0 \pmod{k}$ i.e. $\alpha \equiv \beta \pmod{k}$.

Next, we show that G and $Q^{(\nu)}$ are isomorphic. Denote by τ the canonical map from $Q^{(+)}$ into G, defined by

$$\tau(a_1^t) = \tau_t(a_1^t), \text{ for } t \geqslant 1. \tag{3.7}$$

Now, (3.7) and (d) imply that τ is a surjective homomorphism. To show that $\xi : Q^{(\nu)} \to G$ defined by $\xi(u^{\cong}) = \tau(u)$, for $u^{\cong} = \{v \mid v \in Q^{(t)}, u \cong v\}$, is an isomorphism, we need to show that:

$$u \cong v \Leftrightarrow \tau(u) = \tau(v). \tag{3.8}$$

If $u \cong v$, then there exists $w \in Q^{(+)}$ such that $[uw] = [vw]$, i.e. $\tau(uw) = \tau(vw)$, which implies that $\tau(u) \cdot \tau(w) = \tau(v) \cdot \tau(w)$. Since $(G, \cdot)$ is a group, it follows that $\tau(u) = \tau(v)$. For the converse, let $u \in Q^{(\alpha)}$, $v \in Q^{(\beta)}$, and $\tau(u) = \tau(v)$. Then $Q_\alpha \cap Q_\beta \neq \emptyset$, and (c′) implies that $\alpha \equiv \beta \pmod{k}$, i.e. there exists $\gamma \geqslant 1$, such that $\alpha+\gamma=m+rk$, $\beta+\gamma=m+sk$, for some $r, s \geqslant 1$. Let $w \in Q^{(\gamma)}$ be an arbitrary element. Then, $\tau(uw)=\tau(vw)$, implies that $\tau([uw])=\tau([vw])$, which by (a) implies that $[uw]=[vw]$, i.e. $u \cong v$. ∎

If $(Q, [\ ])$ is a f.c. (n, m)-group, then directly from (3.3) and the definition of $Q^{(v)}$, it follows that $Q^{(v)}$ and $Q \equiv \{a^{\cong} \mid a \in Q\} \subseteq Q^{(v)}$ satisfy the assumptions from T. 3.5, and the f.c. (n, m)-group defined in T.3.5, coincides with the given one. Because of this, further on we will not distinguish $Q^{(v)}$ and G, for any G satisfying the assumptions of T.3.5.

Assuming that G is a universal covering group for a given f.c. (n, m)-group $(Q, [\ ])$, where, $n-m=k$ and $m+p \equiv 0 \pmod k$ are as above, P.3.3, P.3.4, and T.3.5 imply the following:

Proposition 3.6.

(i) Q_{m+p} is a subgroup of G, and $G/Q_{m+p}=\{Q_m, Q_{m+1}, \ldots, Q_{n-1}\}$ is a cyclic group, with a generator Q_{m+p+1}, and order k.

(ii) For $\alpha \geqslant 1$ let j be the smallest non-negative integer such that $\alpha \equiv m+j \pmod k$. Then, for every, $u \in Q_j$, $Q_\alpha = uQ_m$ ($Q_o=\{1\}$ where 1 is the neutral element of G).

(iii) If $a \in Q$, then $Q^{(v)}=Q_m \cup aQ_m \cup a^2Q_m \cup \ldots \cup a^{k-1}Q_m$, where a^t denotes the element $\underbrace{a \ldots a}_{t} \in Q^{(t)}$.

(iv) For every $1 \leqslant i \leqslant m$, the canonical map $\tau_i: Q^{(i)} \to Q_i$ is bijective.

(v) $Q \subseteq Q_{m+p+1}$, $Q^{-1} \subseteq Q_{m+p-1}$, (for p = 0, $Q^{-1} \subseteq Q_{n-1}$) and $QQ^{-1} \subseteq Q_{m+p}$, where $Q^{-1}=\{a^{-1} \mid a \in Q$, a^{-1} is the inverse of a in $G\}$. ∎

§ 4. FINITE F.C. V.V. GROUPS

In this section we give a complete description of finite f.c. v.v. groups.

Theorem 4.1. If $(Q, [\ \ ])$ is a f.c. v.v. group, and Q is finite set i.e. $|Q|<\infty$, then $|Q| \leqslant 2$.

Proof. Let $(Q, [\ \ ])$ be a f.c. (n, m)-group, and $|Q|=q+1$. (Note that we consider only $m \geqslant 2$). Let $Q^{(v)}=G$, $\tau: Q^{(t)} \to G$ and $m+p \equiv 0 \pmod k$ be as in § 3. We note that for every $r \geqslant 1$,

$$|Q^{(r)}|=\binom{q+r}{r}\left(=\frac{(q+r)!}{q!\,r!}\right). \tag{4.1}$$

Thus, P.3.6, implies that

$$|Q_r|=\binom{q+r}{r}; \quad |Q_s|=|Q_m|=\binom{q+m}{m}, \tag{4.2}$$

for every $1 \leqslant r \leqslant m$, $m \leqslant s \leqslant n-1$.

Consider the following subsets H, K, L of G:

$$H=\{a^{-1}\cdot\tau(a_1^{m-1}) \mid a \in Q,\ a_1^{m-1} \in Q^{(m-1)}\}$$

$$K = \{a^{-1} \cdot \tau(a_1^{m-1}) \mid a \in Q,\ a_1^{m-1} \in Q^{(m-1)},\ a \notin \{a_1, \ldots, a_{m-1}\}\}, \quad (4.3)$$

$$L = \{\tau(a_1^{m-2}) \mid a_1^{m-2} \in Q^{(m-2)}\} = Q_{(m-2)}.$$

It is clear that $K \cup L = H$. We will show that $K \cap L = \emptyset$. Suppose the converse, i.e. $a^{-1} \cdot \tau(a_1^{m-1}) = \tau(b_1^{m-2})$ for some $a \in Q$, $a_1^{m-1} \in Q^{(m-1)}$, $b_1^{m-2} \in Q^{(m-2)}$ and $a \notin \{a_1, \ldots, a_{m-1}\}$. Then, $\tau(a_1^{m-1}) = a \cdot \tau(b_1^{m-2}) = \tau(ab_1^{m-2})$. Since, τ_{m-1} is bijective (P.3.6 (iv)) it follows that $a_1^{m-1} = ab_1^{m-2}$ in $Q^{(m-1)}$ which implies that $a \in \{a_1, \ldots, a_{m-1}\}$. Contradiction.

Now, $K \cup L = H$ and $K \cap L = \emptyset$ imply:

$$|K| + |L| = |H|. \quad (4.4)$$

P.3.6. (v), i.e. $Q^{-1} \cdot Q \subseteq Q_{m+p}$, implies that $H \subseteq Q_{m+p+m-2}$.

Then, (4.2) implies that

$$|H| \leqslant \binom{q+m}{m},\ |L| = \binom{q+m-2}{m-2},\ |K| = (q+1)\binom{q+m-2}{m-1}. \quad (4,5)$$

Now (4.4) and (4.5) imply that

$$\binom{q+m-2}{m-2} + (q+1)\binom{q+m-2}{m-1} \leqslant \binom{q+m}{m},$$

which implies that $mq \leqslant q + m - 1$, i.e. $q \leqslant 1$. Hence $|Q| \leqslant 2$. ∎

The next example shows that f.c. (n, m)-groups $(Q, [\ \ ])$ with $|Q| = 2$, do exist.

Example 4.2. Let $Q = \{a, b\}$, $a \neq b$. Let, $Z_{m+1} = \{0, 1, \ldots, m-1, m\}$ be the cyclic additive group of integers mod $(m+1)$, with the addition denoted by $\oplus$. For a fixed $e \in Z_{m+1}$, define $[\ \ ]$ on Q by:

$$[a^\alpha b^{n-\alpha}] = a^{\alpha \oplus e} b^{m-(\alpha \oplus e)}, \quad (4.6)$$

for every $0 \leqslant \alpha \leqslant n$.

It can be easily proved that $(Q, [\ \ ])$ is a f.c. (n, m)-group. We denote this f.c. (n, m)-group by $A(m, k; e)$ where $k = n - m$.

Thus, there exist f.c. (n, m)-groups with two elements.

We note that an analogous result to the fact that every f.c. (n, m)-semigroup is induced by a semigroup, does not hold for f.c. (n, m)-groups and cancellative f.c. (n, m)-semigroups. It is known that finite $(m+1, m)$-groups (with more than one element) do not exist, and the finite cancellative $(m+1, m)$-semigroups are $(m+1, m)$-groups, while finite f.c. $(m+1, m)$-groups with two elements do exist.

Proposition 4.3. If $(Q, [\ \ ])$ is a f.c. (n, m)-group with $Q = \{a, b\}$, $a \neq b$, then there exists an element $e \in Z_{m+1}$, such that $(Q, [\ \ ]) = A(m, k; e)$.

Proof. Consider the universal commutative group $Q^{(\mathrm{v})}$, where the operation is denoted additively. P.3.6. (iii) and (iv), and (4.2) imply that $|Q^{(\mathrm{v})}| = k(m+1)$, and

$$Q^{(\mathrm{v})} = \{ja + \alpha a + (m-\alpha)b \mid 0 \leqslant \alpha \leqslant m,\ 0 \leqslant j \leqslant k\} = \{ja + \alpha(a-b) \mid 0 \leqslant \alpha \leqslant m,\ 0 \leqslant j \leqslant k\}, \quad (4.7)$$

where $a - b = a + (-b)$ for $(-b)$ the inverse of b in $Q^{(\mathrm{v})}$.

P.3.6. (v) implies that $a - b \in Q_{m+p}$, where $m + p \equiv 0 \pmod{k}$ is as in § 3. Now, (4.7) implies that $Q_{m+p} = \{pa + mb + \alpha(a - b) \mid 0 \leqslant \alpha \leqslant m\}$, i.e. Q_{m+p} is a cyclic group of order $m + 1$, with a generator $a - b$. For $0 \leqslant \alpha \leqslant n$, let $[a^{\alpha}b^{(n-\alpha)}] = a^{\beta}b^{m-\beta}$, for some $0 \leqslant \beta \leqslant m$. Then, in $Q^{(\nu)}$, $\alpha a + (m + k - \alpha) b = \beta a + (m - \beta) b$, i.e. $kb = (\beta \ominus \alpha) \cdot (a - b) = e(a - b)$, where $e = \beta \ominus \alpha \in Z_{m+1}$. Therefore, $[a^{\alpha}b^{(n-\alpha)}] = a^{\alpha \oplus e}b^{m-(\alpha \oplus e)}$, i.e. $(Q, [\ ]) = A(m, k; e)$.

From the definition of $A(m, k; e)$, it follows that:

$$[a^{\alpha}b^{m+sk-\alpha}] = a^{\beta}b^{m-\beta} \Leftrightarrow \beta = \alpha \oplus se, \tag{4.8}$$

(where $se = \underbrace{e \oplus \ldots \oplus e}_{s}$) which implies the following:

Proposition 4.4. (i) $A(m, k; d)$ is derived from $A(m, k; e)$ if and only if $se = d$ in Z_{m+1}.

(ii) For every $d \in Z_{m+1}$ there exists $e \in Z_{m+1}$, such that $A(m, ks; d)$ is derived from $A(m, k; e)$ if and only if s and $m+1$ are relatively prime. i.e. $(s, m + 1) = 1$. ∎

P.4.3. implies that there are $m + 1$ f.c. (n, m)-groups on $Q = \{a, b\}$. To find the maximal number μ of non isomorphic f.c. (n, m)-group on $Q = \{a, b\}$ we need the following:

Proposition 4.5. $A(m, k; e)$ is isomorphic to $A(m, k; d)$ if and only if $e = d$ or $k \oplus e \oplus d = 0$. (The notions of homomorphisms and isomorphisms of f.c. v.v. groups have the usual meanings; see [3].)

Proof. $A(m, k; e)$ is isomorphic to $A(m, k; d)$ if and only if there exists a bijection $f: \{a, b\} \to \{a, b\}$ such that for every $0 \leqslant \alpha \leqslant n$: (i) $a^{\alpha \oplus e}b^{m-\alpha \oplus e} = a^{\alpha \oplus d}b^{m-\alpha \oplus d}$, or (ii) $a^{m-\alpha \oplus e}b^{\alpha \oplus e} = a^{(n-\alpha) \oplus d}b^{m-(n-\alpha) \oplus d}$, which is equivalent to: (i) $e = d$, or (ii) $k \oplus e \oplus d = 0$. ∎

To find the number μ we consider the equation $2x \oplus k = 0$ in Z_{m+1}. Namely, if $2e \oplus k = 0$, then $f(a) = b$, $f(b) = a$ is an automorphism of $A(m, k; e)$. Now, it is clear that:

(I) If $m + 1$ is odd, then $2x \oplus k = 0$ has a unique solution, and thus,

$$\mu = \frac{m}{2} + 1 = \left[\frac{m}{2}\right] + 1. \tag{4.9}$$

(II) If $m + 1$ is even, and k is odd, then $2x \oplus k = 0$ does not have solutions in Z_{m+1}, and thus

$$\mu = \frac{m+1}{2} = \left[\frac{m}{2}\right] + 1. \tag{4.10}$$

(III) If $m+1$ and k are even, then $2x \oplus k = 0$ has two solutions in Z_{m+1}, and thus,

$$\mu = \frac{m-1}{2} + 2 = \frac{m+1}{2} + 1 = \frac{m+3}{2} = \left[\frac{m}{2}\right] + 2. \tag{4.11}$$

At the end of this section we give several examples.

Examples 4.6. (1) A (2,1; 0) and A (2,1; 2) are isomorphic, and $f : a \mapsto b$, $b \mapsto a$, is an automorphism of A (2, 1; 1).

(2) A (2, 2; 0) and A (2, 2; 1) are isomorphic, and f is an automorphism of A (2, 2; 2). A (2, 2; 0), A (2, 2; 1), A (2, 2; 2) are derived from A (2, 1; 0), A (2, 1; 2), A (2, 1; 1) respectively.

(3) A (2, 3; 0) is derived from each of A (2, 1; 0), A (2, 1; 1) and A (2, 1; 2). Thus, neither of A (2, 3; 1), A (2, 3; 2) is derived from a f.c. (3, 2)-semigroup. Moreover, A (2, 3; 1) is isomorphic to A (2, 3; 2), and f is an automorphism of A (2, 3; 0).

(4) A (3, 2; 0) and A (3, 2; 2) are isomorphic and f is an automorphism of A (3, 2; 1) and of A (3, 2; 3).

§ 5. EXISTENCE OF INFINITE F.C. V.V. GROUPS

The following result will be shown in this section.

Theorem 5.1. If Q is an infinite set, and n, k arbitrary positive integers, $(m \geqslant 2)$ then there exists a f.c. $(m+k, m)$-structure on Q.

The proof of this theorem is via a special combinatorial construction of f.c. $(m+1, m)$-groups, similar to the construction of free $(m+1, m)$-groups, $m \geqslant 2$, explained in [5], which will be in fact the proof of T. 5.1, for $k=1$. Then we apply P.2.3.

Now, we give the construction.

Let B be a set, possibly empty. For each $b \in B$, choose a set $D_b = \{b_1, \ldots, b_m\}$, such that $D_b \cap B = \emptyset$ and $D_b \cap D_c = \emptyset$ for $b, c \in B$, $b \neq c$. Let $B' = B \cup \bigcup_{b \in B} D_b$. Note, that $B = \emptyset$ implies $B' = \emptyset$. Let $e_1, \ldots, e_m$ be new, not necessarily different elements, let E be the set of all the distinct e_ν, and $E \cap B' = \emptyset$. Now we will define by induction a sequence of sets $\{B_\alpha, \alpha \geqslant 0\}$. First, $B_0 = B' \cup E$.

Suppose that B_α is well defined. Let $C_\alpha \subseteq \bigcup_{t \geqslant m+1} B_\alpha^{(t)} = B'_\alpha$ be the set of all the elements from B'_α, which do not have any one of the following forms:

(a.1) $e_1^m d_1^s$, where $d_\nu \in B_\alpha$, $s \geqslant m$;

(a.2) $b b_1^m d_1^s$, where $d_\nu \in B_\alpha$, $b \in B$;

(a.3) $(1, x)\,(2, x) \ldots (m, x)\, d_1^s$, where $d_\nu \in B_\alpha$ and $x \in B'_{\alpha-1}$.

Set, $B_{\alpha+1} = B_\alpha \cup N_m \times C_\alpha$,

where $N_m = \{1, 2, 3, \ldots, m\}$.

By choosing different notations for the elements of B_0, if necessary, we can obtain: $(B_{\alpha+1} \setminus B_\alpha) \cap (B_{\beta+1} \setminus B_\beta) = \emptyset$ for $\alpha \neq \beta$.

Let $Q = \bigcup_{\alpha \geqslant 0} B_\alpha$.

Define a norm $|\ \ |$ on the elements of $Q^{(+)}$ by induction as follows:

$|x| = 1$ for $x \in B_0$.

If $|\ \ |$ is defined on B_α, and $x = (1, u_1^s) \in B_{\alpha+1} \setminus B_\alpha$, then $|x| = |u_1| + \ldots + |u_s|$.

Next, we define a map $f: Q^{(+)} \to Q^{(+)}$ by induction on the norm, as follows:

(b.1) If u has the form (a.1), then $f(u) = f(d_1^s)$;

(b.2) If u has the form (a.2) then $f(u) = f(e_1^m d_1^s)$;

(b.3) If u has the form (a.3), then $f(u) = f(x d_1^s)$; and

(b.4) If u does not have any one of the forms (a.1), (a.2), (a.3), then $f(u) = u$.

Using the fact that $B' \cap E = \emptyset$, and $(B_{\alpha+1} \setminus B_\alpha) \cap (B_{\beta+1} \setminus B_\beta) = \emptyset$ for $\alpha \neq \beta$, it can be checked by a straightforward inductive proof that:

(c.1) f is well defined;

(c.2) $f(u) \neq u$ if and only if $|f(u)| < |u|$;

(c.3) $f(f(u)) = f(u)$;

(c.4) If, $\dim u \geqslant m$, then $\dim f(u) \geqslant m$;

(c.5) If, $\dim u < m$, then $f(u) = u$; and

(c.6) $f(uv) = f(f(u)\, v)$.

Define $[\ \ ] : Q^{(m+1)} \to Q^{(m)}$, by;

$$[u_1^{m+1}] = (1,\ f(u_1^{n+1})) \ldots (m,\ f(u_1^{m+1})), \tag{5.1}$$

where $(1,\ v_1^m) \ldots (m, v_1^m)$ is only a notation for v_1^m in $Q^{(m)}$.

Using (b.3) and (c.6), for $u, v \in Q$, $x \in Q^{(m-1)}$, we have:

$$[[ux]v] = [(1, f(ux)) \ldots (m,\ f(ux))\ v] = (1,\ f((1, f(ux)) \ldots (m, f(ux))\ v)) \ldots$$
$$\ldots (m, f((1, f(ux)) \ldots (m,\ f(ux))\ v\ )) = (1, f(f(ux), v)) \ldots$$
$$\ldots (m, f(f(ux)(v) = (1, f(uxv\ )) \ldots (m, f(uxv)) = (1, f(xvu)) \ldots$$
$$\ldots (m,\ f(xuv)) = [\ [xv]\,u] = [[vx]\ u] = [u[vx]] = [u\ [xv]\ ].$$

Hence, $(Q, [\ \ ])$ is a f.c. $(m+1, m)$-semigroup.

By induction on the norm, we define a map $g : Q \to Q^{(+)}$ as follows:

(d.1) $g(e_i) = e_1^m e^{i-1} e_{i+1}^m$, for $e_i \in E$;

(d.2) $g(b) = b_1^m$, for $b \in B$;

(d.3) $g(b_i) = bb_1^{i-1}b_{i+1}^m$, for $b \in B$.

(d.4) $g(i, w_1^t) = (1, w_1^t) \dots (i-1, w_1^t)(i+1, w_1^t) \dots (m, w_1^t)\, g(w_1) \dots g(w_t)$.

By an easy inductive proof, it can be shown that for each $u \in Q$,

$$f(ug(u)) = e_1^m. \tag{5.2}$$

Now, let $u \in Q$ and $x \in Q^{(m)}$. Then, $f(ug(u)\,x) = f(f(ug(u))\,x) = f(e_1^m x) = f(x)$. If x does not have the form (a.3), then $f(x) = x$, and so $[u[g(u)\,x]]] = x$. If $x = (1, y) \dots (m, y)$, then $f(x) = f(y) = y$, since y does not have any one of the forms (a.1), (a.2) and (a.3). Then $[ug(u)x] = (1, f(ug(u)\,x)) \dots (m, f(ug(u)\,x)) = (1, y) \dots (m, y) = x$. Hence, for every $u \in Q$, $w \in Q^{(m)}$, the equation $[ux] = w$, has a solution, which shows that $(Q, [\ ])$ is a f.c. $(m+1, m)$-group.

We note, that if $e_1 = e_2 = \dots = e_m$, then $g(e_i) = g(e) = e^{m-1}$, for every i.

From the construction of Q it is clear that if B is an infinite set, then $|B| = |Q|$, i.e. $|B|$ and $|Q|$ have the same cardinality.

This completes the proof of T.5.1. ∎

The f.c. $(m+1, m)$-group $(Q, [\ ])$ constructed above for $|E| = m$, is generated by B, and for each f.c. $(m+1, m)$-group $(H, [\ ])'$ and a map $g: B \to H$, there exists a homomorphism $\bar{g}: (Q, [\ ]) \to (H, [\ ]')$ which is an extension of g. But $\bar{g}$ is not unique with these properties, in fact there are infinitely many such extsnsions. So, we can say that $(Q; [\ ])$ is a free $(m+1, m)$-group.

Recently, K. Trenčevski obtained the following set of f.c. v.v. groups.

Example 5.2. Let F be an algebraically closed field and let $[\ ] = F^{(m+1)} \to F^{(m)}$ be defined by: $[x_0^m] = y_1^m$ if and only if

$$(t - x_0)(t - x_1) \dots (t - x_m) = t^{m+1} + a_1 t^m + \dots + a_m t + a_{m+1}$$

$$(t - y_1)(t - y_2) \dots (t - y_m) = t^m + a_1 t^{m-1} + \dots + a_{m-1} t + a_m.$$

Then, $(F; [\ ])$ is a f.c. $(m+1, m)$-group.

REFERENCES

[1] Б. Трпеновски, Ѓ. Чупона, *[m, n]-групоиди*, Билтен, Друштво матем. физ. СРМ, 21, Скопје, 1970, 19—29,

[2] G. Čupona, *Vector Valued Semigroups*, Semigroup Forum, Vol. 26 (1983), 65—74.

[3] G. Čupona, A. Samardžiski, N. Celakoski, *Fully commutative Vector Valued Quasigroups*, Proc. of Conf. "Algebra and Logic", Sarajevo 1987, (preprint).

[4] G. Čupona, N. Celakoski, S. Markovski, D. Dimovski, *Vector Valued Semigroups and Groups*, Vector Valued Semigroups and Groups, MANU, 1988, 1—78.

[5] D. Dimovski, *Free* $(n+1,\ n)$*-groups*, Vector Valued Semigroups and Groups, MANU, 1988, 103—122.

[6] C. Čupona, S. Markovski, D. Dimovski, B. Janeva, *A Combinatorial Theory of Vector Valued Semigroups*, Vector Valued Semigroups and Groups, MANU, 1988, 141—183.

Ѓ. ЧУПОНА, Д. ДИМОВСКИ, А. САМАРЏИСКИ

ПОТПОЛНО КОМУТАТИВНИ ВЕКТОРСКО ВРЕДНОСНИ ГРУПИ

(Резиме)

Во работата се воведува поимот за потполно комутативни $(m+k,\ m)$-групи, каде што m и k се позитивни цели броеви. Бидејќи потполно комутативни $(1+k,\ 1)$-групи се обични комутативни $k+1$-групи, во текот на работата се претпоставува дека $m \geqslant 2$, и во тој случај се вели дека се работи за потполно комутативни векторско вредносни (п. к. в. в.) групи. Во работата се покажува дека едно непразно множество Q е носител на п. к. в. в. група ако и само ако $|Q| = 2$ или Q е бесконечно. Притоа се дава комплетен опис на п. к. в. в. групи со 2 елементи.

University of Skopje,
Faculty of Sciences,
P.O.B. 162
91000 Skopje, Yugoslavia.