Год. збор. Матем. фак.
33-34 (99-103) 1982—1983

SOME EXISTENCE CONDITIONS FOR VECTOR VALUED GROUPS

Dončo Dimovski

ABSTRACT

The main results in this paper are the following theorems:

Theorem 1. Let A [ ] be an $(n+1, n)$-group, $n > 2$ and $1 < |A| < \infty$. Then each prime divisor p of $n\ (n+1)$ is also a divisor of $|A|$.

Theorem 2. If A [ ] is a commutative $(n+1,\ n)$-group, $n > 2$, then $|A| = 1$.

These results give partial answers to the questions, asked by Ǵ. Čupona, about the existence of finite (n, m)-grups and about embedda-Billity of commutative, cancellative $(n,\ m)$-semigroups in commutative (n, m)-groups, when m is not a divisor of n.

In [1], (n, m)-groups are defined. We state here the definition.

An (n, m)*-semigroup* $(k = n - m > 0)$ A [ ] is an associative mapping [ ]: $A^n \to A^m$, denoted by

[ ]: $(x_1, x_2, \dots, x_n) \mapsto [x_1 x_2 \dots x_n]$, which satisfies

$$[[x_1 \dots x_n] x_{n+1} \dots x_{2k+m}] = [x_1 \dots x_i [x_{i+1} \dots x_{i+n}] x_{i+n+1} \dots x_{2k+m}]$$

for each $i \in \{1, 2, \dots, k\}$. In this case we write

$[x_1 \dots x_{2k+m}]$ for $[[x_1 \dots x_n] x_{n+1} \dots x_{2k+m}]$.

An (n, m)-semigroup A [ ] is called *cancellative* if it satisfies the following condition: For each $\mathbf{a} \in A^k$, $\mathbf{x}, \mathbf{y} \in A^m$,

$$[\mathbf{a}\, \mathbf{x}] = [\mathbf{a}\, \mathbf{y}] \text{ or } [\mathbf{x}\, \mathbf{a}] = [\mathbf{y}\, \mathbf{a}], \text{ implies } \mathbf{x} = \mathbf{y}.$$

An (n, m)-semigroup is called *commutative* if the following identity is satisfied:

$$[x_1 \dots x_n] = [x_{i_1} x_{i_2} \dots x_{i_n}], \text{ for any permutation}$$

$$j \mapsto i_j \text{ of } \{1, 2, \dots, n\}.$$

An (n, m)-semigroup $A[\ ]$ is called an *(n, m)-group* if for each $\mathbf{a} \in A^k$, $\mathbf{b} \in A^m$, there exist $\mathbf{x}, \mathbf{y} \in A^m$ such that $[\mathbf{a}\,\mathbf{x}] = \mathbf{b} = [\mathbf{y}\,\mathbf{a}]$.

Theorem 1 says that there exist finite sets which do not admit an $(n+1, n)$-group structure. This theorem gives a partial answer to a question about the existence of finite vector valued groups, asked by Ǧ. Čupona in the Seminar of the Institute for Algebra and Geometry at the Mathematical Faculty in Skopje. Also this question can be found (not exactly in this form) in the list of prblems from [1].

Theorem 2 gives a partial answer to Problem 5.4. from [1] which is: Is it true that any commutative, cancellative (n, m)-semigroup is an (n, m)-subsemigroup of a commutative (n, m)-group?

In the following, $A[\ ]$ will be an $(n+1, n)$-group.

Proposition 1. (See [1, 3.2. (d)]) A^n with the operation

$$\mathbf{a}\,\mathbf{b} = [\mathbf{a}\,\mathbf{b}] \text{ is a group.}$$

Proof. (i) The multiplication in A^n is well defined because $[\dots[[a_1 \dots a_n\, b_1]\, b_2] \dots b_n]$ is well defined in an $(n+1, n)$-semigroup.

(ii) The multiplication in A^n is associative because

$$\mathbf{a}\,(\mathbf{b}\,\mathbf{c}) = \mathbf{a}\,[\mathbf{b}\,\mathbf{c}] = [\mathbf{a}\,[\mathbf{b}\,\mathbf{c}]] = [[\mathbf{a}\,\mathbf{b}]\,\mathbf{c}] = [\mathbf{a}\,\mathbf{b}]\,\mathbf{c} = (\mathbf{a}\,\mathbf{b})\,\mathbf{c}.$$

(iii) Let $\mathbf{a} = (a_1, \dots, a_n) \in A^n$, and $\mathbf{b} \in A^n$. For a_1 and $\mathbf{b}$ there exists $\mathbf{z}_1 \in A^n$ such that $[a_1 \mathbf{z}_1] = \mathbf{b}$ (since $A[\ ]$ is an $(n+1, n)$-group). For a_1 and $\mathbf{z}_1$ there exists $\mathbf{z}_2 \in A^n$ such that $[a_2 \mathbf{z}_2] = \mathbf{z}_1$. After n steps we will find $z_n = \mathbf{x} \in A^n$ such that $[a_1 a_2 \dots a_n\, \mathbf{x}] = [\mathbf{a}\,\mathbf{x}] = \mathbf{b}$. Hence, for each $\mathbf{a}, \mathbf{b} \in A^n$ there exists $\mathbf{x} \in A^n$ such that $\mathbf{a}\,\mathbf{x} = b$. Similarly, for each $\mathbf{a}, \mathbf{b} \in A^n$ there exists $\mathbf{y} \in A^n$ such that $\mathbf{y}\,\mathbf{a} = \mathbf{b}$. (i), (ii) and (iii) imply that A^n is a group. ∎

Proposition 2. Let $a \in A$, and $\mathbf{b}, \mathbf{c} \in A^n$. If $[a\,\mathbf{b}] = [a\,\mathbf{c}]$ then $\mathbf{b} = \mathbf{c}$. If $[\mathbf{b}, a] = [\mathbf{c}, a]$ then $\mathbf{b} = \mathbf{c}$. ($A[\ ]$ is a cancellative $(n+1, n)$-semigroup.)

Proof. Let $\mathbf{e} = (e_1, e_2, \dots, e_n)$ be the identity in the group A^n, and let $[a\,\mathbf{b}] = [a\,\mathbf{c}]$. Then.

$[\mathbf{e}\,a]\,\mathbf{b} = \mathbf{e}\,[a\,\mathbf{b}] = [a\,\mathbf{b}] = [a\,\mathbf{c}] = \mathbf{e}\,[a\,\mathbf{c}] = [\mathbf{e}\,a]\,\mathbf{c}$, which implies that $\mathbf{b} = \mathbf{c}$, because this is an equation in the group A^n. ∎

Proposition 3. The identity $\mathbf{e}$ in A^n is equal to $\underbrace{(e, e, \dots, e, e)}_{n}$ for an element $e \in A$.

Proof. Let $\mathbf{e} = (e_1, \dots, e_n)$. We will show that $e_1 = e_2 \dots = e_n = e$ For each $x \in A$,

$$[e_1 \dots e_n\, e_1 \dots e_{n-1}\, x] = (e_1, \dots, e_{n-1}, x) = [e_1 \dots e_{n-1}\, x e_1 \dots e_n],$$

which implies, by Proposition 2, that for each $x \in A$, $(e_n\, e_1 \ldots e_{n-1}\, x] = [xe_1 \ldots \ldots e_n]$. Now for $x \in A$ and $\mathbf{y} \in A^n$ $(e_n, e_1, \ldots, e_{n-1})\,[x\,\mathbf{y}] = [e_n\, e_1 \ldots e_{n-1}\, x\mathbf{y}] = [xe_1 \ldots e_n\, \mathbf{y}] = [x\,[e_1 \ldots e_n\, \mathbf{y}]] = [x\,\mathbf{y}] = \mathbf{e}\,[x\,\mathbf{y}]$. Now we can cancell by $[x\,\mathbf{y}]$ and get that $(e_n, e_1, \ldots, e_{n-1}) = (e_1, e_2, \ldots, e_n)$, which implies that $e_1 = e_2 = \ldots = e_n$ ∎.

The element $(x, x, \ldots, x, x) \in A^i$ will be denoted by x^i or (x^i).

Proposition 4. Let $i \in \{1, \ldots, n-1\}$. If $[\mathbf{e}\, e^i] = \mathbf{e}$, then $|\mathrm{A}| = 1$.

Proof. $[\mathbf{e}\, e^i] = \mathbf{e}$ implies that $[e^i\, \mathbf{e}] = \mathbf{e}$. Let $x \in A$. Then $(e^{n-1}, x) = \mathbf{e}\,(e^{n-1}, x) = [\mathbf{e}\, e^{n-1}\, x] = [\mathbf{e}\, e^i\, e^{n-1} x] = [e^{n+i-1}\, x]$, and $(e^{n-1}, x) = (e^{n-1}, x) = [e^{n-1}\, x\, \mathbf{e}] = [e^{n-1}\, x\, e^i\, \mathbf{e}] = [e^{n-1}\, x\, e^i]$. So, for each $x \in A$, $[e^i\, e^{n-i-1}\, x\, e^i] = [e^{n-1}\, x\, e^i] = [e^{n+i-1}\, x] = [e^i\, e^{n-1}\, x]$, which implies, by Proposition 2,. that $(e^{n-i-1}, x, e^i) = (e^{n-1}, x)$. Hence, for each $x \in A$, $x = e$, i.e. $|A| = 1$. ∎

Proposition 5. Let $1 < |A| < \infty$. Then n is a divisor of $|A|^n$.

Proof. We will show that $[e^{n+1}] \in A^n$ has order n, and because A^n is a finite group it will imply that n is a divisor of $|A|$.

$$[e^{n+1}]^n = [e^{n(n+1)}] = [e^{nn+n}] = [e^{nn}\, \mathbf{e}] = [e^{nn}] = \mathbf{e}^n = \mathbf{e}.$$

Let $i \in \{1, 2, \ldots, n-1\}$ and let $[e^{n+1}]^i = \mathbf{e}$. Then $\mathbf{e} = [e^{ni+i}] = [(e^n)^i\, e^i] = [\mathbf{e}\, e^i]$, which together with $1 < |A|$ contradicts Proposition 4. Hence, $[e^{n+1}]$ has order n. ∎

Proposition 6. If $[x_1\, x_2 \ldots x_{n+1}] = \mathbf{e}$, then for each $1 \leqslant i \leqslant n+1$, $[x_i\, x_{i+1} \ldots x_{n+1}\, x_1 \ldots x_{i-1}] = \mathbf{e}$.

Proof. $[x_1\, x_2 \ldots x_{n+1}] = \mathbf{e}$ implies that $(x_1, \ldots, x_n)\,[x_{n+1}\, \mathbf{e}] = \mathbf{e} = [x_{n+1}\, \mathbf{e}]\,(x_1, \ldots, x_n) = [x_{n+1}\, \mathbf{e}\, x_1 \ldots x_n] = [x_{n+1}\, x_1 \ldots x_n]$. ∎

Proposition 7. If $[x_1 x_2 \ldots x_{n+1}] = \mathbf{e}$, then there is a positive integer m, such that $n + 1 = mr$; for each $1 \leqslant i < m$, $x_i = x_{i+m} = \ldots = x_{i+(r-1)m}$; and $|\{x_1, x_2, \ldots, x_m\}| = m$.

Proof. Let $[x_1 x_2 \ldots x_{n+1}] = \mathbf{e}$. If $x_i \neq x_j$ for $i \neq \mathrm{j}$, then $m = n + 1$, and $|\{x_1, x_2, \ldots, x_{n+1}\}| = n + 1$. Suppose that $x_i = x_j$ for some $i \neq j$. Then Propositions 2 and 6 imply that $x_1 = x_k$ for some $k \neq 1$. Let s be the smallest integrer such that $x_1 = x_s$, and let $m = s - 1$. Then from the equation

$$[x_1 x_2 \ldots x_m\, x_1 x_{m+2} \ldots x_{2m}\, x_{2m+1} \ldots x_{3m}\, x_{3m+1} \ldots x_{n+1}] =$$

$= [x_1\, x_{m+2} \ldots x_{2m}\, x_{2m+1} \ldots x_{3m}\, x_{3m+1} \ldots x_{n+1}\, x_1\, x_2 \ldots x_m]$ we get that $x_m = x_{2m} = x_{3m} = \ldots x_{rm}$, $n + 1 = rm$; and for each $1 \leqslant i < m$, $x_i = x_{m+i} = x_{2m+i} = \ldots = x_{(r-1)\, m+i}$. ∎

Let $x \in A$. Then $[x\,\mathbf{e}] \in A^n$, and there is an element $(x_1, x_2, \ldots, x_n) \in$ $\in A^n$, such that $[x\,\mathbf{e}]\,(x_1, x_2, \ldots, x_n) = \mathbf{e}$. This implies that $[xx_1x_2 \ldots x_n] = \mathbf{e}$. For $x \in A$, let B_x be the set $\{x, x_2, x_3, \ldots, x_m\}$ such that $[(xx_2x_3 \ldots x_m)^r] = \mathbf{e}$, for some r with $mr = n + 1$. Propositions 2 and 7, show that B_x is uniquelly and well determined by x.

Proposition 8. $B_x \cap B_y \neq \emptyset$ implies $B_x = B_y$.

Proof. Let $B_x = \{x_1, x_2, \ldots, x_m\}$, $B_y = \{y_1, y_2, \ldots, y_k\}$, $x = x_1$, $y =$ $= y_1$, $mr = n + 1 = ks$, and $[(x_1x_2 \ldots x_m)^r] = \mathbf{e} = [(y_1y_2 \ldots y_k)^s]$. Let $B_x \cap B_y \neq \emptyset$. Then there are i and j such that $x_i = y_j$, and

$$[(y_j\, y_{j+1} \ldots y_k\, y_1 \ldots y_{j-1})^s] = \mathbf{e} = [(x_i\, x_{i+1} \ldots x_m\, x_1 \ldots x_{i-1})^r].$$

Now, Proposition 2 implies that $r = s$, $m = k$ and $B_x = B_y$. ∎

Proposition 9. Let $B_x = \{x_1, x_2, \ldots, x_m\}$ for $x = x_1$ and $n + 1 =$ $= mr$. If $|A| \neq 1$, then $[\mathbf{e}x_1x_2 \ldots x_m]$ has ordder r in the group A^n.

Proof. $[\mathbf{e}\,x_1 \ldots x_m]^r = [(x_1 \ldots x_m)^r] = \mathbf{e}$. Let $i \in \{1, 2, \ldots, r-1\}$ and let $[\mathbf{e}\,x_1x_2 \ldots x_m]^i = \mathbf{e} = [\mathbf{e}\,(x_1 \ldots x_m)^i]$. Let $n + 1 = mi + t$ where $t \geqslant m$. Then $[e^{n-t}\,(x_1 \ldots x_m)^i\, e^t] = \mathbf{e} = [e^{n-t+1}\,(x_1 \ldots x_m)^i\, e^{t-1}]$, which implies, by Proposition 2, that $((x_1, \ldots, x_m)^i, e^{t-1}) = (e, (x_1, \ldots, x_m)^i, e^{t-2})$. This equation implies that $x_1 = x_2 = \ldots = x_m = e$, which contradicts Proposition 4, because

$$\mathbf{e} = [(x_1x_2 \ldots x_m)^r] = [e^{n+1}] = [\mathbf{e}\, e]. \; ∎$$

Proof of Theorem 1. Let p be a prime divisor of n. Then p is a divisor of $|A|^n$ by Proposition 5, which implies that p is a divisor of $|A|$.

Proposition 8 tells us that we can write A as a disjoint union of the sets B_x. Let $A = (\cup B_x^1) \cup (\cup B_x^2) \cup \ldots\ldots \cup (\cup B_x^r)$, where B_x^i are the sets B_x that have r_i elements, $n + 1 = p_1 > p_2 > \ldots\ldots > p_t = 1$, and $n + 1 = p_i\, r_i$ for each i. Let d be the greatest common divisor for $p_1, p_2,$ $\ldots, p_t$. Since $A = \cup B_x$, it follows that d is a divisor of $|A|$. Let p be a prime divisor of $n + 1$. If p is a divisor of each p_i then p is a divisor of d, and so is a divisor of $|A|$. If there is i such that p is not a divisor of p_i, then p is a divisor of r_i (because $n + 1 = p_i\, r_i$). By Proposition 9, r_i is a divisor of $|A|^n$, and so p is a divisor of $|A|$. ∎

Corollary 1. Let $A[\;]$ be an $(n+1, n)$-group, and $1 < |A| < \infty$ Then $|A|$ is even.

Proof. For each n, 2 is a divisor of $n\,(n + 1)$. ∎

Theorem 3. Let $A[\;]$ be an $(n + 1, n)$-group, $n \geqslant 2$ and $1 < |A| < \infty$. Then, for each divisor $m \neq 1$ of n, each prime divisor p of $m + 1$ is also a divisor of $|A|$.

Proof. Since $A[\ ]$ is an $(n+1, n)$-group, it can be made into an $(n+t, n)$-group for each $t \geqslant 1$. (See [1, 3.2. (*c*)]). Let $n = ms$, for $m \neq 1$. Then we have an $(n+m, n)$ i.e. $((m+1)s, ms)$ — group structure on A. This structure gives us an $(m+1, m)$-group structure on A^s. Now we apply Theorem 1. ■

Corollary 2. Let $A[\ ]$ be an (n,m)-group, $m \geqslant 2$, $n = (r+1)s$, $m = rs$ and $1 < |A| < \infty$. Then, for each divisor h of r, each prime divisor p of $(h+1)\,n\,(n+1)$ is a divisor of $|A|$. ■

Proof of *Theorem* 2. Let $A[\ ]$ be a commutative $(n+1, n)$-group, $n \geqslant 2$ and let $\mathbf{e} = (e, e, \ldots, e)$ be the identity in the group A (Proposition 3). Commutativity implies that $[\mathbf{e}\,x] = [e^{n-1}\,xe]$ for each $x \in A$. After cancelling we get that $x = e$, for each $x \in A$. Here we use the fact that $n \geqslant 2$. Hence $|A| = 1$. ■

Corollary 3. If $S[\ ]$ is a nontrivial ($|S| \neq 1$) cancellative, commutative $(n+1, n)$ — semigroup, $n \geqslant 2$, then $S[\ ]$ is not an $(n+1, n)$-subsemigroup of a commutative $(n+1, n)$-group. ■

REFERENCES

[1] Čupona, Ġ.: Vector valued semigroups, Semigroup Forum Vol. 26 (1983) 65-74.

Резиме

НЕКОИ УСЛОВИ ЗА ПОСТОЕЊЕ НА ВЕКТОРСКО ВРЕДНОСНИ ГРУПИ

Дончо Димовски

Главните резултати во оваа работа се следните теореми:

Теорема 1. Нека $A[\ ]$ е $(n+1, n)$-група, $n > 2$ и $1 < |A| < \infty$. Тогаш секој прост делител p на $n(n+1)$ е исто така и делител на $|A|$. ■

Теорема 2. Ако $[\ ]$ е комутативна $(n+1, n)$-група, $n > 2$, тогаш $|A| = 1$.

Овие резултати даваат делумни одговори на прашањата, поставени од Ѓ. Чупона, за постоење на конечни (n, m)-групи и за сместување на комутативни (n, m)-полугрупи со кратење во комутативни (n, m)-групи, кога m не е делител на n.