Reprinted from JOURNAL OF ALGEBRA
Vol. 146, No. 1, February 15, 1992
Printed in Belgium


# Groups with Unique Product Structures

DONČO DIMOVSKI*

*University of Skopje, Yugoslavia*

*Communicated by Walter Feit*

Received March 12, 1990

We say that a group $G$ has a unique $m$-element product structure where $m$ is a positive integer, if there is a subset $S \subseteq G$, such that the product map $\varphi: S^m \to G$, defined by $\varphi(x_1, x_2, ..., x_m) = x_1 x_2 \cdots x_m$, is a bijection. We show that the only finite groups with unique $m$-element product structures for $m > 1$ are the trivial ones, and give examples of such groups which are infinite. © 1992 Academic Press, Inc.

The notion of $(n, m)$-groups was introduced in [Č]. In [D1] it was shown that the number of elements in a finite nontrivial (i.e., with more than one element) $(3, 2)$-group is divisible by 6. The existence of a nontrivial $(3, 2)$-group is equivalent to the existence of a nontrivial group $G$ together with a subset $S \subseteq G$, such that each element of $G$ is a unique product of two elements from $S$, i.e., the product map $S \times S \to G$ defined by $(x, y) \to xy$ is a bijection. The question about the existence of such finite groups (in a slightly different form, using permutation groups), came to John Thompson (thanks to R. Geoghegan and J. Keesling). John Thompson kindly provided me with a proof that the only such groups which are finite are the trivial ones (Corollary 1). The proofs of Theorem 1 and Theorem 2 were inspired by and are based on his proof, and his proof is in fact the special case of the proof of Theorem 1 (for $m = 1$) or Theorem 2 (for $m = 2$).

DEFINITION. We say that a group $G$ has a *unique $m$-element product* structure, where $m$ is a positive integer, if there is a subset $S \subseteq G$, such that the product map $\varphi: S^m \to G$, defined by $\varphi(x_1, x_2, ..., x_m) = x_1 x_2 \cdots x_m$, is a bijection. It is obvious that every group has a unique 1-element product structure, so we say that a group $G$ has a *unique product structure* if it has a unique $m$-element product structure for some $m > 1$.

In terms of this definition, the existence of nontrivial finite $(m+1, m)$-groups $(m > 1)$ is equivalent to the existence of nontrivial finite groups with

* Supported in part by a grant from the Research Council of Makedonija.



0021-8693/92 $3.00

unique $m$-element product structures. Professor John Thompson proved that the only finite groups with unique 2-element product structures are the trivial ones.

We show in Theorem 2 that a finite group with unique $m$-element product structure, for $m>1$, must be the trivial one. In [D2], a combinatorial description of free $(m+1, m)$-groups, $m>1$, is given, which implies that they are nontrivial and infinite, and in fact, shows that nontrivial groups with unique product structure do exist. In this paper we will give only a construction of a nontrivial group with unique 2-element product structure, which in fact, gives a construction of a free (3, 2)-group generated by the empty set.

THEOREM 1. *Let $G$ be a finite group, and $S \subseteq G$. If the product map $\varphi$: $S \times S \to G$ is $m$-to-1, for $m \geqslant 1$ (which means that the number of elements of $\varphi^{-1}(g)$ is $m$, i.e., $|\varphi^{-1}(g)| = m$, for every $g \in G$), then $S = G$.*

*Proof.* (a) Since $\varphi$ is $m$-to-1, and $\varphi^{-1}(g) \cap \varphi^{-1}(h) = \varnothing$ if and only if $g = h$, $g$, $h \in G$, it follows that $|S|^2 = \sum_{g \in G} |\varphi^{-1}(g)| = nm$, where $n = |G|$. Because $|S| \leqslant |G|$, it follows that $m \leqslant |S|$.

(b) Let $R = \mathbb{C}[G]$ be the group algebra of $G$ over the field of complex numbers $\mathbb{C}$. Then $R$ is a semi-simple ring and by Wedderburn's theorem (see [H]), $R$ is the direct sum $R = R_1 + R_2 + \cdots + R_s$, of simple rings which are unique apart from the order, and in fact they are two-sided principal ideals in $R$ of idempotents $e_1, e_2, ..., e_s$ in the center of $R$, such that $e_i e_j = 0$ for $i \neq j$, and such that $1 = e_1 + e_2 + \cdots + e_s$. We choose $e_1$ to be the idempotent $(1/n)(\sum_{g \in G} g)$. Moreover, each $R_i$ is the complete matrix ring $L_{f_i}(\mathbb{C})$ of $f_i \times f_i$ matrices over $\mathbb{C}$ (see [H]), where $f_1^2 + f_2^2 + \cdots + f_s^2 = n$. By the choice of $e_1$, we have $f_1 = 1$. We note that the addition and multiplication in $R$ is componentwise, i.e., $(A_1 + A_2 + \cdots + A_s) + (B_1 + B_2 + \cdots + B_s) = (A_1 + B_1) + (A_2 + B_2) + \cdots + (A_s + B_s)$; $(A_1 + A_2 + \cdots + A_s)(B_1 + B_2 + \cdots + B_s) = A_1 B_1 + A_2 B_2 + \cdots + A_s B_s$.

(c) Let $\rho$: $G \to L_n(\mathbb{C})$ be the right regular representation of $G$, which is defined by $\rho(g)(x) = xg$, for each $g \in G$ and $x \in R$, where we think of $R$ as a vector space over $\mathbb{C}$ of dimension $n$. We extend $\rho$ linearly over $R$, i.e., $\rho(\sum_{g \in G} \alpha_g g) = \sum_{g \in G} \alpha_g \rho(g)$. Taking $g_1$, $g_2$, ..., $g_n$ (where $G = \{g_1, g_2, ..., g_n\}$) as a basis for $R$, $\rho(x)$ is a matrix $(x_{ij})$, which is defined by the equations $g_i x = \sum_{j=1}^{n} x_{ij} g_j$, for $x \in R$ and $i = 1, 2, ..., n$. The character $\chi$ of $\rho$ is defined by $\chi(x) = \text{trace}(\rho(x))$, for $x \in R$. For $g \in G$, $\rho(g) = (x_{ij})$, where $x_{ij} = 1$ if $g_i g = g_j$, and $x_{ij} = 0$ otherwise. This implies that $\chi(g) = n$ for $g = 1$, and $\chi(g) = 0$ for $g \neq 1$, where 1 is the neutral element in $G$.

(d) Using a different basis for $R$, obtained via its decomposition as the direct sum $R_1 + R_2 + \cdots + R_s$, for $x = A_1 + A_2 + \cdots + A_s \in R$,

$$\rho(x) = \begin{pmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \cdots & 0 \\ 0 & \cdots & \cdots & 0 \\ 0 & 0 & \cdots & B_s \end{pmatrix}, \quad \text{where} \quad B_i = \underbrace{\begin{pmatrix} A_i & 0 & \cdots & 0 \\ 0 & A_i & \cdots & 0 \\ 0 & \cdots & \cdots & 0 \\ 0 & 0 & \cdots & A_i \end{pmatrix}}_{f_i}, \; i = 1, \ldots, s.$$

Since the character is invariant under the change of basis [H], it follows that $\chi(x) = \operatorname{trace}(\rho(x)) = \sum_{i=1}^{n} f_i \cdot \operatorname{trace}(A_i)$.

(e) Let $[S] = \sum_{g \in S} g = A_1 + A_2 + \cdots + A_s \in R$, $A_i \in R_i$. Then, by the assumption in the theorem, we have $[S] \cdot [S] = m \sum_{g \in S} g = m \cdot n \cdot e_1 = m \cdot n + 0 + 0 + \cdots + 0 = m \cdot n$. This implies that $A_1^2 = m \cdot n$, and for $i \geqslant 2$, $A_i^2 = 0$, i.e., for each $i \geqslant 2$, $A_i$ is a nilpotent matrix. Using the fact that the trace of a nilpotent matrix is 0, we have that $\chi([S]) = A_1$. On the other hand, $\chi([S]) = \sum_{g \in S} \chi(g)$. If $1 \notin S$, then $\chi([S]) = 0$, which is impossible, since $A_1^2 = 0^2 \neq m \cdot n = A_1^2$. Hence, $1 \in S$, and $\chi([S]) = n = A_1$. Now, $m \cdot n = A_1^2 = n^2$ implies that $m = n$. Since $S \subseteq G$, we have that $|S| \leqslant n$. This, together with $n = m \leqslant |S|$ (see (a)), implies that $S = G$. ∎

As a corollary of Theorem 1, we have:

COROLLARY 1. *Let $G$ be a finite group with unique 2-element product structure. Then $|G| = 1$.*

*Proof.* Let $S \subseteq G$ be such that the product map $\varphi\colon S \times S \to G$ is a bijection. Then $\varphi$ is a 1-to-1 map, and by Theorem 1, $S = G$. Let $x \in G$, and let $1 \in G$ be the neutral element in $G$. Since $S = G$, it follows that $\varphi(1, x) = x = \varphi(x, 1)$, which, together with the fact that $\varphi$ is a bijection, implies that $x = 1$. Hence, $|G| = 1$. ∎

THEOREM 2. *Let $G$ be a finite group with a unique $m$-element product structure, for $m \geqslant 2$. Then $|G| = 1$.*

*Proof.* Let $S \subseteq G$ be such that the product map $\varphi\colon S^m \to G$ is a bijection. We will consider two cases: $m$-even and $m$-odd.

*Case* I. Let $m = 2r$, where $r \geqslant 1$. Denote by $L$ the subset $S \cdot \cdots \cdot S$, $r$ times, of $G$, i.e., $L = \{x_1 \cdots x_r \mid x \in S\} \subseteq G$. It is obvious that the product map $\psi\colon S^r \to L$ is a surjection, and since the map $\varphi$ is a bijection, it follows that $\psi$ is a bijection. Similarly, it follows that the product map $\varphi'\colon L^2 \to G$ is a bijection, i.e., 1-to-1. Now, Theorem 1 implies that $L = G$. Using the

facts that $|S|^r = |L| = |G| = |S|^{2r}$, and $r \geqslant 1$, we have that $|S| = 1$, i.e., $|L| = |G| = 1$.

*Case* II. Let $m = 2r + 1$, where $r \geqslant 1$. Denote by $L$ the subset $S \cdot \cdots \cdot S$, $(r+1)$ times, of $G$, i.e., $L = \{x_1 \cdots x_{r+1} \mid x \in S\} \subseteq G$. We need the following fact.

*Fact.* The product map $\psi\colon L^2 \to G$ is $|S|$-to-1.

*Proof.* Because $\varphi\colon S^m \to G$ is a bijection, it follows that for each $g \in G$, $|\varphi^{-1}(g)| = 1$. Let $g \in G$. For each $s \in S$, $\varphi^{-1}(gs^{-1}) \in S^m$, and so $(\varphi^{-1}(gs^{-1}), s) \in S^{m+1} = L^2$. Then, $\psi(\varphi^{-1}(gs^{-1}), s) = (gs^{-1})s = g$, which implies that $\psi$ is a surjection, and $\psi^{-1}(g) \supseteq \{(\varphi^{-1}(gs^{-1}), s) \mid s \in S\}$. Since $|\varphi^{-1}(gs^{-1})| = 1$, it follows that $|\{(\varphi^{-1}(gs^{-1}), s) \mid s \in S\}| = |S|$. This, together with the fact that $|G| = |S|^m = |S|^{2r+1}$, implies that $|\psi^{-1}(g)| = |S|$, for each $g \in G$. Hence, $\psi$ is $|S|$-to-1. ∎

Now, Theorem 1 together with the fact imply that $L = G$, i.e., $|L| = |G|$. Then, $|S|^{r+1} = |L| = |G| = |S|^m = |S|^{2r+1}$ implies that $|S|^r = 1$. Since $r \geqslant 1$, it follows that $|S| = |G| = 1$. ∎

In the next example we will construct a group with unique 2-element product structure. This construction is in fact a variation of the constructions of free (3, 2)-groups generated by the empty set, given in [D1, D2] and later in [DIJ].

EXAMPLE. By induction we will construct a chain of groups $G_0 \leqslant G_1 \leqslant G_2 \leqslant \cdots \leqslant G_i \leqslant \cdots$ and a chain of sets $S_0 \subseteq S_1 \subseteq S_2 \subseteq \cdots \subseteq S_i \subseteq \cdots$, such that $S_i \subseteq G_i$ and the product map $\varphi_i\colon S_i^2 \to G_i$ is injective for each $i \geqslant 0$, and $G_{i-1} \subseteq \varphi_i(S_i^2)$ for each $i \geqslant 1$.

*Step* 0. Let $B_0 = \{e\}$ be a one-element set. Let $G_0$ be the group with the presentation $\langle B_0 \mid R_0 \rangle$, where $R_0$ is the set of relations $\{e^2 = 1\}$. Let $S_0 = B_0$. It is obvious that $G_0 = \langle e \mid e^2 = 1 \rangle = \{1, e\}$, and so, the product map $\varphi\colon S_0^2 \to G_0$ is injective.

*Step* 1. Let $C_1 = G_0 \setminus \varphi_0(S_0^2)$, $S_1 = S_0 \cup (\{1, 2\} \times C_1)$, $B_1 = G_0 \cup (\{1, 2\} \times C_1)$, $R_1 = \{xy = x \circ y \mid x, y \in G_0\} \cup \{(1, x)(2, x) = x \mid x \in C_1\}$ where $x \circ y$ denotes the product of $x$ and $y$ in $G_0$, and $G_1 = \langle B_1 \mid R_1 \rangle$. It is easy to check that $S_1 \subseteq G_1$, $G_0 \leqslant G_1$, and $S_0 \subseteq S_1$. It can be shown, by an explicit construction of a reduction ([D1, D2, DIJ] or [MKS]), that the elements of $G_1$ have canonical reduced form. Using the canonical reduced form, it can be shown that the product map $\varphi_1\colon S_1^2 \to G_1$ is injective [DIJ]. The definition of $G_1$ and $S_1$ implies that $G_0 \subseteq \varphi_1(S_1^2)$.

*Step* $n$. Suppose that we have constructed a chain of groups $G_0 \leqslant G_1 \leqslant G_2 \leqslant \cdots \leqslant G_n$ and a chain of sets $S_0 \subseteq S_1 \subseteq S_2 \subseteq \cdots \subseteq S_n$ such that $S_i \subseteq G_i$

and the product map $\varphi_i: S_i^2 \to G_i$ is injective for each $0 \leqslant i \leqslant n$, and $G_{i-1} \subseteq \varphi_i(S_i^2)$ for each $1 \leqslant i \leqslant n$.

*Step* $n+1$. Let $C_{n+1} = G_n \setminus \varphi_n(S_n^2)$, $S_{n+1} = S_n \cup (\{1, 2\} \times C_{n+1})$, $B_{n+1} = G_n \cup (\{1, 2\} \times C_{n+1})$, $R_{n+1} = \{xy = x \circ y \mid x, y \in G_n\} \cup \{(1, x)(2, x) = x \mid x \in C_{n+1}\}$ where $x \circ y$ denotes the product of $x$ and $y$ in $G_n$, and $G_{n+1} = \langle B_{n+1} \mid R_{n+1} \rangle$. Now, like in Step 2, it can be checked that: $S_{n+1} \subseteq G_{n+1}$, $G_n \leqslant G_{n+1}$, $S_n \subseteq S_{n+1}$, the elements of $G_{n+1}$ have canonical reduced form, and using the canonical reduced form, it can be shown that the product map $\varphi_{n+1}: S_{n+1}^2 \to G_{n+1}$ is injective. At the end, the definition of $G_{n+1}$ and $S_{n+1}$ implies that $G_n \subseteq \varphi_{n+1}(S_{n+1}^2)$.

*Step* $\infty$. Let $G = \bigcup_{i=0}^{\infty} G_i$ and $S = \bigcup_{i=0}^{\infty} S_i$. The properties of the groups $G_i$, the subsets $S_i$, and the product maps $\varphi_i$ imply that $G$ is a group such that the product map $\varphi: S^2 \to G$ is a bijection. Hence, the group $G$ has a unique 2-element product structure. ∎

## References


[Č] G. Čupona, Vector valued semigroups, *Semigroup Forum* **26** (1983), 65–74.

[D1] D. Dimovski, On (3, 2)-groups, *in* "Proc. Conf. Alg. and Logic, Cetinje, 1985," pp. 55–62.

[D2] D. Dimovski, Free $(n+1, n)$-groups, *in* "Vector Valued Semigroups and Groups," pp. 103–122, MANU Skopje, 1988.

[MKS] W. Magnus, A. Karrass, and D. Solitar, "Combinatorial Group Theory," Dover, New York, 1976.

[H] M. Hall, Jr., "The Theory of Groups," Chelsea, New York, 1976.

[DIJ] D. Dimovski, S. Ilić, and B. Janeva, Free vector valued groups, *Comm. Algebra* **19** (1991), 965–979.


Printed by Catherine Press, Ltd., Tempelhof 41, B-8000 Brugge, Belgium