A STUDYING ABOUT SOME CHARACTERIZATION OF FINITE MATROID GROUPS

Submited on 09/02/2020– Accepted on 10/11/2020

Abstract

In this work, we show that a very large class of matroid groups possesses the basis property. Moreover, we show that this class behaves like vector spaces in terms of basis. Applications include new proofs for the characterization of finite matroid groups. Moreover, we show that every group possesses BEP, also possesses the span property and in the definition of matroid group, the extension property can be replaced by BEP. The fact that BEP always correct in vector spaces, but the situation is different in groups was showed. In the end, we show that each base and maximal independent subset are equivalent in any group with embedding property.

Keywords: *Matroid group, basis property,basis exchange property, extension property*

NADER TAFFACH

Department of Mathematics, Faculty of Science, Idlib University, Syria.

ntaffash77@windowslive.com

I- INTRODUCTION

Matroid theory contributes in several fields of sciences such as Coding Theory, Electronics and Computer Science [1]. The word ”matroid” came first from ”matrix”, and then it has its own structure.

Recently the notion of matroid group was introduced by several mathematicians. They studied the structure of such groups [2], [3].

II. PROBLEM STATEMENT AND FUNDAMENTAL CONCEPTS

Definition 1 : [4]**.**A group G is called a group with basis property if there exists a basis (minimal generating set) for every subgroup H of G and every two bases are equivalent.

A group G is called a group with exchange property, if $x \notin \langle X \rangle \wedge x \in \langle X \cup \{y\} \rangle$, then $y \in \langle X \cup \{x\} \rangle$, for all $x, y \in G$ and for every subset $X \subseteq G$.

Definition 2: A generating set X is said to be minimal if it has no proper subset which forms a generating set. The subset X of a group G is called independent, if for all $x \in X \wedge x \notin \langle X \setminus \{x\} \rangle$. Independent set X is called a basis subgroup $\langle X \rangle$.

Example 1: Let (Z; +) be an additive abelian group, then we can write $Z = \langle 1 \rangle = \langle 2,3 \rangle$ even though $2 \notin \langle 3 \rangle$ and $3 \notin \langle 2 \rangle$. Thus Z does not have the basis property. Hence free groups do not have the basis property.

Definition 3: A matroid M is an ordered pair (E, Ω) consisting of a finite set E and a nonempty subset Ω of the power set (E) such that ;

(a) If $I \in \Omega$ and $I_0 \subseteq I$ then $I_0 \subseteq \Omega$. (Hereditary Property).

(b) If $I_1, I_2 \in \Omega$ and $1 + |I_1| = |I_2|$, then there exists an element $e \in I_2 - I_1$ satisfying $I_1 \cup \{e\} \in \Omega$ (Extension Property).

The elements of Ω are called independent where the elements of $(E) \setminus \Omega$ are called dependent. Matroid basis are defined to be the maximal elements of Ω .

The concepts of independence and basis should be clarified before we go on. The condition (a) is satisfied for each group G when we assume that the elements of Ω are the independent subsets of G . This is obvious since if the elements $x_1, ..., x_r$ are independent in the sense that non of them can be written in terms of the others, then any subset of $\{x_1, ..., x_r\}$ is independent. It should be pointed out that, in groups, each base is a maximal independent element of Ω , but the converse is not true. Here is an examples.

Example 2: In A_4 , the subset $\{(12)(34), (13)(24)\}$ is independent and maximal, but certainly is not a base.

Definition 4: A group is satisfying the ”embedding property” if each independent subset can be embedded in a base.

From this definition, one deduces that, base and maximal independent subset are equivalent in any group with embedding property.

Definition 5: A group G is said to be matroid if it satisfies

(a_1) the empedding

(b_1) extension properties

Example5: A typical example of such groups is the finite elementary Abelian groups as they can be viewed as vector spaces over the finite Galios field $GF(p)$. But not all groups are matroid, for if we consider D_4, the dihedral group $\langle x, y\ ; x^2 = y^4 = 1,\ x^{-1}yx = y^{-1}\rangle$, the $X = \{x, y^2\}$ is independent but cannot be embedded in any base.

For non-Abelian case, one may take S_3 to see that it is a matroid group.

III. MATROID GROUPS AND BASISPROPERTY

Remember that we say a group G has the "span property" if for any two bases X, Y for G then $|X| = |Y|$ If in addition, the same thing is true for all subgroups of G, then G is said to have the "Basis Property". In other words, G has the basis property if all its subgroups have the span property [5], [6].

Proposition 1: Matroid groups possess the span property.

Proof. Let B_1, B_2 be two bases of a matroid group, and assume that $|B_1| < |B_2|$, so there exists an independent subset $B \subseteq B_2$ such that $|B| = |B_1| + 1$, and thus there exists an element $x \in B - B_1$ such that $B_1 \cup \{x\}$ is independent according to (b_1). But B_1 is a base of the group, so it is maximal independent subset. Therefore, $B_1 \cup \{x\}$ is dependent. This contradicts what we just stated.

Proposition 2: Matroid groups possess the basis property.

Proof. Let H be a proper subgroup of a matroid group G. Consider the two bases of H, $X = \{x_1, ..., x_r\}, Y = \{y_1, ..., y_l\}$. By (a_1), both bases can be extended to bases for G. This means there exist elements s_i such that $\{x_1, ..., x_r, s_1, ..., s_k\}$ is a base of G. By Proposition 1, any base of G contains exactly $r + k$ elements. Now, it is clear that $H \subseteq \{y_1, ..., y_l, s_1, ..., s_k\}$, and also any element of $G - H$ can be expressed in terms of x_is and s_is , but any x_i can be expressed in terms of $y_i s$,thus any element of G can be written in terms of $y_i s$ and $s_i s$ .Therefore $\langle y_1, ..., y_l, s_1, ..., s_k\rangle = G$ .This implies that $r + k \le l + k$ or $r \le l$. We may switch X with Y in the above argument to see that $r \ge l$. Hence $r = l$, and G has the basis property.

This leads to a notion similar to the dimension in vector spaces.

In matroid groups, the number of elements in any base is called the "rank" for the matroid group G , and it is denoted by $\delta(G)$.

Proposition 3: For a matroid group G . If H is a proper subgroup of G , then $\delta(H) \le \delta(G)$.

Proof: Let B be a base of H . So, B contains independent elements, and by (a_1), B can be embedded in a base X for G containing B with $|B| < |X|$ or $\delta(H) \le \delta(G)$.

IV. MATROID GROUPS AND BASIS EXCHANGEPROPERTY

Definition 6: A group G is said to have the basis exchange property (BEP) if for any two bases B_1, B_2 for G , if there exists an element $x \in B_1 - B_2$, then there exists an element $y \in B_2 - B_1$ such that $(B_1 - \{x\}) \cup \{y\}$ is a base for G .

This special property is always correct in vector spaces, but the situation is different in groups. To demonstrate this point, let us focus on the following example.

Example 6: In S_9, let $a = (123)(456)(789)$, $b = (147)(258)(369)$ $c = (24)(37)(68)$. The calculations show that $(ac)^3 = (16)(29)(57)$.

we consider the group $G = \langle a, c\rangle$,and let $x = (ac)^2$, $y = (ac)^3$ and $z = yc$.

We easily find the two bases $B_1 = \{ac, b\}$, $B_2 = \{x, y, z\}$. Replacing z by ac gives the subset $\{x, y, ac\}$ which generates only $\langle ac\rangle \ne G$ .The subset

$\{x, y, b\}$ is dependent since $x \in \langle y, b \rangle$ Hence G does not possess the BEP. One notices that G does not possess the span property either. This example is revealing, and we state this proposition.

Proposition 4: If a group G possesses the BEP. Then it satisfies the span property.

Proof: Assume the contrary. That is G has two bases B_1, B_2 with $|B_1| < |B_2|$. Let us choose these two bases such that $|B_1 - B_2|$ is the least possible difference. Obviously, $B_2 - B_1 \neq \phi$, since otherwise B_1 would not be maximal. Now, let $x \in B_2 - B_1$. By BEP, there exists $y \in B_1 - B_2$ such that $(B_2 - \{x\}) \cup \{y\}$ is a base. But $|(B_2 - \{x\}) \cup \{y\} - B_1| < |B_2 - B_1|$. This contradicts the minimality of $|B_2 - B_1|$, and hence leads to $|B_1| = |B_2|$.

Proposition 5: Matroid groups have the BEP.

Proof: Let B_1, B_2 be two bases of a matroid group G. Let $x \in B_1 - B_2$. Proposition 1 shows that $|B_1| = |B_2|$, and we know that both $B_1 - \{x\}$ and B_2 have independent elements. Obviously, $|B_2| = |B_1 - \{x\}| + 1$, so there exists $y \in B_2 - (B_1 - \{x\})$ such that $(B_1 - \{x\}) \cup \{y\}$ is independent. By the extension property, it can be extended a base. But since $|(B_1 - \{x\}) \cup \{y\}| = |B_1|$, then $(B_1 - \{x\}) \cup \{y\}$ is a base itself.

In the definition of matroid group, the extension property can be replaced by BEP.

Proposition 6: Let G be a group with the embedding property. Then the following properties are equivalent.

(i) Extension property.

(ii) Basis exchange property.

Proof: $(i) \Rightarrow (ii)$. Let G be satisfying the extension property. Since G has the embedding property. So G is matroid. According to the previous proposition, G has the basis exchange property.

$(ii) \Rightarrow (i)$ Assume that G has the BEP and G dose not satisfy the extension property. Thus, there are two independent sets I_1, I_2 where $|I_2| = |I_1| + 1$ and for all $e \in I_2 - I_1$ the set $I_1 \cup \{e\}$ is dependent. Embedding property leads to existence of two bases B_1, B_2 such that $I_1 \subseteq B_1$, $I_2 \subseteq B_2$. Choose B_1, B_2 such that $|B_2 - (I_2 \cup B_1)|$ is minimal. Notice that $I_2 - B_1 = I_2 - I_1$, because $(I_2 - I_1) \cap B_1 = \phi$ due to adding any element of $I_2 - I_1$ to I_1 would make the set B_1 dependent. Now $B_2 - (I_2 \cup B_1) = \phi$ for otherwise, one can choose $x \in B_2 - (I_2 \cup B_1)$ and by BEP, there exists $y \in B_1 - B_2$ with $(B_1 - \{x\}) \cup \{y\}$ is a base. But $|(B_2 - \{x\}) \cup \{y\} - (I_2 \cup B_1)| < |B_2 - (I_2 \cup B_1)|$ which contradicts our choice of B_2. So, $B_2 - B_1 = I_2 - B_1$ and hence $B_2 - B_1 = I_2 - I_1$. Moreover, $B_1 - (I_1 \cup B_2) = \phi$ for otherwise, there will be an element $x \in B_1 - (I_1 \cup B_2)$, and therefore, there exists $y \in B_2 - B_1$ such that $(B_1 - \{x\}) \cup \{y\}$ is a base for G. Now $I_1 \cup \{y\} \subseteq (B_1 - \{x\}) \cup \{y\}$, so $I_1 \cup \{y\}$ is independent, and since $y \in B_2 - B_1 = I_2 - I_1$ we reach a contradiction with our assumption. Thus, $B_1 - B_2 = I_1 - B_2 \subseteq I_1 - I_2$. But $|B_1| = |B_2|$ this means that $|B_1 - B_2| = |B_2 - B_1|$ and we may deduce that $|I_2 - I_1| \leq |I_1 - I_2|$ or $|I_2| \leq |I_1|$ which is a contradiction.

From this statement, one may define the matroid group to be any finite group that satisfying embedding property and the BEP.

5. THE CHARACTERIZATION OF MATROID GROUPS

A subset X of a finite group G is called independent, respectively Frattini-independent, if there is no proper subset $Y \subset X$ such that $\langle X \rangle = \langle Y \rangle$, respectively $\langle X \cup \phi(G) \rangle = \langle Y \cup \phi(G) \rangle$. The group G is called a matroid group if G has property B and every Frattini-independent subset of G can be extended to a minimal generating set of G. Alternatively, G is a matroid group if $H = G / \phi(G)$ is a Frattini-free B− group and every independent subset of H can be extended to an minimal generating set. The definition of a matroid group given here is the one used in [3]. We obtain a small variation of the characterization of matroid groups in [3].

Theorem 1: Let G be a finite group. Then G is a Frattini-free B− group if and only if one of the following holds:

(1) G is an elementary abelian $p-$group for some prime p ;

(2) $G=P\times Q$, where P is an elementary abelian $p-$group and Q is a non- trivial cyclic $q-$group, for distinct primes $p\neq q$ such that Q acts faithfully on P and the F_pQ-module P is a direct sum of isomorphic copies of one simple module.

Remark1: This means that there are no Frattini-free finite $\mathrm{B}-$groups beyond the examples constructed in [7]. Indeed, the groups listed in (2) of Theorem1.3can be concretely realized as semi direct products via multiplication in finite fields of characteristic p : the simple module in question is of the form $F_p(\zeta)$, the additive group of a finite field generated by a q^k throot of unity ζ over F_p, with a generator z of Q acting on $F_p(\zeta)$ as multiplication by ζ .

Theorem 2 :[3]. Let G be a finite group and let $H=G/\phi(G)$ .The group G is a matroid group if and only if one of the following holds:

(1) G is a $p-$group for some prime p ,

(2) $H=P\times Q$, where $P\cong F_p^d$ and Q is cyclic of order q , for primes p,q such that $q/p-1$, and $Q\to F_p^{\times}$ acts on P via field multiplication.

Proof: By the Burnside basis theorem every finite group of prime-power order is a matroid group. From now suppose that G does not have prime-power order.

First suppose that G is a matroid group. Then, by Theorem1 and Remark1 , the Frattini quotient H is a matroid group of the form $H=P\times Q$, where P is an elementary abelian $p-$ group and Q is a non-trivial cyclic group of order q^k , for distinct primes $p\neq q$, such that $Q\to F^{\times}$ acts faithfully on $P\cong F^d$ via multiplication in a finite field F .Here F is obtained from F_p by adjoining a primitive $q^k th$ root of unity and we set $r=\left[F:F_p\right]$. We observe that the common size of all minimal generating sets of G is $d+1$.

Being isomorphic to an F_P -vector space of dimension rd , the subgroup P contains an independent subset of size rd . This subset extends to a minimal generating set of H . We deduce that $rd\leq d$, thus $r=1$. Let z be a generator of Q and assume for a contradiction that $k\geq 2$. Choose a minimal generating set X for P as an F_pQ- module. Then $X\cup\{z^q\}$ is an independent set of size $d+1$ that does not generate H and does not extend to a minimal generating set of H . This implies that H is not a matroid group in contradiction to our assumptions. Hence, $k=1$, i.e., Q is cyclic of order q . From $Q\to F_p^{\times}$ we obtain $q/p-1$.

Conversely, suppose that $H=P\times Q$, where $P\cong F_p^d$ and $Q=\langle z\rangle$ is cyclic of order q , for primes q,p such that $q/p-1$, and $Q\to F_p^{\times}$ acts on P via field multiplication. By Theorem 1 the group H has property B and it suffices to show that every independent subset of H extends to a minimal generating set. Let $X=\{x_1,...,x_m\}\subseteq H$ be an independent subset of size m .If $X\subseteq P$ then, regarding P as an F_p -vector space, we extend X to a minimal generating set of P and add the generator z of Q to obtain a minimal generating set of H . Now suppose that $X\not\subseteq P$ .Since H does not contain any element of order pq , we may assume without loss of generality that $x_1=z$. Then $X=\{z,v_2z^{j_2},...,v_mz^{j_m}\}$ where $\{v_2,...,v_m\}\subseteq P$ is an independent subset of size $m-1$ and $j_2,...,j_m$ are integers.

We extend $\{v_2,...,v_m\}$ to a minimal generating set $\{v_2,...,v_d\}$ of P . Then $X\cup\{v_{m+1},...,v_d\}$ is a minimal generating set of H .

Using Theorem 1.5 we obtain the following consequence.

Corollary 1: Let G be a finite group. Then G is a matroid group if and only if one of the following holds:

(1) G is a $p-$group for some prime p ,

(2) $G=P\times Q$, where P is a $p-$group, Q is a cyclic $q-$group for primes q,p such that $q/p-1$, $Q/C_Q(P)$ has order q and acts on $P/\phi(P)$ fixed-point-freely.

REFERENCES

[1] R. J. Wilson, "An Introduction to Matroid Theory," Amer. Math. Monthly, 5, pp. 500-525, 1973.

[2] R. Scapellato, and L. Verardi, "Sur les ensembles generateurs minimaux d'un groupe fini," Ann. Sci. Univ.

B. Pascal, Clermont II, Ser. Mat., no. 26, pp. 51-60, 1990. (French).

[3] R. Scapellato, and L. Verardi, "Groupes finis qui jouissent d'une propriete analogue au theoreme des bases de Burnside," Boll. Un. Mat. It.,vol. 7, no. 5-A, pp. 187-194, 1991. (French)

[4] P. Jones, "Basis properties for inverse semigroups," J. Algebra, Vol. 50 (1978), 135-152.

[5] A. Aljouiee, "Basis property conditions on some groups," Int. J. of Math. & Comp. Sci.,vol. 3, pp. 102-112, 2008.

[6] A. Alkhalaf, "Finite groups with bassically property," Dokl. Akad. Nauk. BSSR, no. 11, pp. 47-56, 1989. (Russian).

[7] J. McDougall-Bagnall, and M. Quick, "Groups with the basis property," J. Algebra,vol. 346, pp. 332–339, 2011.