



RELATION BETWEEN GROUPS WITH BASIS PROPERTY AND GROUPS WITH EXCHANGE PROPERTY

A.Al Khalaf, M. Alkadhi

Abstract

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 $X \subseteq G$.

In this research, we proved the following: Every polycyclic group satisfies the basis property. Every element in a group with the exchange property has a prime order. Every p -group satisfies the exchange property if and only if it is an elementary abelian p -group. Finally, we found necessary and sufficient condition for every group to satisfy the exchange property, based on a group with the basis property.

1 Introduction

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 $x \in X$, $x \notin \langle X \setminus \{x\} \rangle$. Independent set X is called a basis subgroup $\langle X \rangle$. In 1978 Jones [5] introduced an initial study of semigroups with the basis property. Jones [5] states that if G is an inverse semigroup and $U \leq V \leq G$ then a U -basis for V is a subset X of V which is minimal such that $\langle U \cup X \rangle = G$.

Key Words: Groups, Basis property, Exchange property.
2010 Mathematics Subject Classification: Primary 20D25; Secondary 20D10.
Received: 31.07.2014
Accepted: 20.02.2015

So a minimal generating set for V is a \emptyset -basis. A basis property of universal algebra A means that every two minimal (with respect to inclusion) generating set (basis) of an arbitrary subalgebra of A have the same cardinality [1].

2 Basis property

Definition 2.1 A group G is called a group with basis property if there exists a basis minimal (irreducible) generating sets (with respect to inclusion) for every subgroup H of G and every two bases are equivalent (i.e. they have the same cardinality) [1].

Notice that finitely generated vector spaces have the property that all minimal generating sets have the same cardinality. Jones [5] introduce another concept which is state for inverse semigroup.

Definition 2.2 An inverse semigroup S has the strong basis property if for any inverse subsemigroup V of S and inverse subsemigroup U of V any two U -bases for V have the same cardinality.

Let $(\mathbb{Z}, +)$ be an additive abelian group, then we can write $\mathbb{Z} = \langle 1 \rangle = \langle 2, 3 \rangle$ even though $2 \notin \langle 3 \rangle$ and $3 \notin \langle 2 \rangle$. Thus \mathbb{Z} does not have the basis property. Hence free groups do not have the basis property. The first results on the basis property of groups was in [6]. The author proved that a group with basis property is periodic, all elements of such a group have prime power order, and solvable. Therefore by [1] every finite p -group has a basis property, and the homomorphic image of every finite group with basis property is again a group with basis property, but in case of infinite group we have the following:

Remark 2.3 Let $G = \sum_{i=1}^{\infty} \mathbb{Z}_{p^i}$ be a direct sum of a cyclic p -group P , then one of homomorphic image is a quasicyclic group $K = \mathbb{Z}_{p^\infty}$, which is not a group with basis property, but the group G is a group with basis property.

Lemma 2.4 Let G be a group in which every element has prime power order, let $x \in G$ such that $|x| = p^c$ and $y \in G$ such that $|y| = q^b$, $p \neq q$ are primes. Then $xy \neq yx$.

Proof. Suppose that $xy = yx$, then xy is an element of order $p^c q^b$, hence xy has a composite order in G . This is contradiction with basis property[1], so $xy \neq yx$. □

Proposition 2.5 Let G be a finite nilpotent group. Then G is a group with basis property if and only if G is a primary group.

Proof. Suppose that G is a finite nilpotent group with basis property. From [11] every finite nilpotent group is decomposable in a direct product of Sylow

subgroups. Then

$$G = G_1 \times G_2 \times \cdots \times G_m,$$

such that G_i is a p_i -group for some primes p_i , $p_i \neq p_j$ if $i \neq j$. If $m > 1$, then in G there exists two commute elements with a prime power order. Hence we have a contradiction with lemma(2-4). Thus G is a primary group.

Conversely, if G is a primary group, then G is a group with basis property [5]. \square

A classification of group with the basis property was announced by Dickson and Jones in [5], but as far as we can see this has yet to be published. However a classification of finite groups with the basis property was given by Al Khalaf [1] exploiting Higman's result, this classification requires a technical condition on the p -group and he proved the following theorem:

Theorem 2.6 [1]. Let a finite group G be a semidirect product of a p -group $P = Fit(G)$ (Fitting subgroup) of G by a cyclic q -group $\langle y \rangle$, of order q^b , where $p \neq q$ (p and q are primes), $b \in \mathbb{N}$. Then the group G has basis property if and only if for any element $y \in \langle y \rangle$, $y \neq e$ and for any invariant subgroup H of P the automorphism φ_u must define an isotopic representation on every quotient Frattini subgroup of H .

In [4], the author used some common results from both group and module theory using Maschke, Clifford and Krull-Schmidt, to classify the group with basis property.

Finally Jones [7] studied basis property from the point of view exchange properties.

Theorem 2.7 [3] Let G be a semidirect product of abelian p -group P by a cyclic q -group $\langle y \rangle$, of order q^b , where $p \neq q$ (p and q are primes), $b \in \mathbb{N}$, which is defined automorphism φ of order q^b and P has an exponent p^c , $c \in \mathbb{N}$. Then the group G has basis property if and only if there exists a polynomial $g(x) \in \mathbb{Z}[x]$ such that satisfy the following conditions:

1. The polynomial $f(x) = \bar{\theta}(g(x))$ is irreducible over the field $GF(p)$,
 $f(x) \mid x^{q^b} - 1$ and $f(x) \nmid x^{q^{b-1}} - 1$.
2. $g^m(\varphi) = 0$.

In this research we study special group with the basis property. The concept of exchange property and continued results as shown in [7] and [8].

Theorem 2.8 Let G be a finite polycyclic group such that G has a presentation [9]:

$$G = \langle x, y : x^{p^c} = y^{q^b} = 1, y^{-1}xy = x^r \rangle, \quad (2-1)$$

such that $p \neq q$ (p and q are primes) $b, c, r \in \mathbb{Z}^+$, $(p, r-1) = 1$ and

$$r^{q^b} \equiv 1 \pmod{p^c}, r \not\equiv 1 \pmod{p}, 0 \leq r \leq p^c. \quad (2-2)$$

Then G is a group with the basis property if and only if it satisfies the following conditions:

$$p \equiv 1 \pmod{q^b}, \quad (2-3)$$

$$r^{q^{b-1}} \not\equiv 1 \pmod{p}. \quad (2-4)$$

Proof. Suppose that G is a group with the basis property. From (2-1) we have that G is a semidirect product of cyclic p -group $\langle x \rangle$, $|\langle x \rangle| = p^c$ by a cyclic q -group $|\langle y \rangle| = q^b$, where $p \neq q$ (p and q are primes) $b, c \in \mathbb{Z}^+$. Then from [1] G is a Frobenius group with kernel $\langle x \rangle$ and complement $\langle y \rangle$. Thus by [3] we see that $p \equiv 1 \pmod{q^b}$. Thus (2-3) holds.

Assume that

$$r^{q^{b-1}} \equiv 1 \pmod{p}. \quad (2-5)$$

Then $r^{q^{b-1}} = 1 + mp$ for some $m \in \mathbb{Z}^+$. Considering the non trivial elements $x^{p^{c-1}}, y^{q^{b-1}}$ and using (2-1) and (2-5) then we have:

$$\begin{aligned} y^{-q^{b-1}} x^{p^{c-1}} y^{q^{b-1}} &= \left(y^{-q^{b-1}} x y^{q^{b-1}} \right)^{p^{c-1}} = \left(y^{-q^{b-1}-1} (y^{-1} x y) y^{q^{b-1}-1} \right)^{p^{c-1}} \\ &= \left(y^{-q^{b-1}-1} x^r y^{q^{b-1}-1} \right)^{p^{c-1}} = \dots = \left(x^{r^{q^{b-1}}} \right)^{p^{c-1}} = x^{p^{c-1}(1+mp)} = \\ &= x^{p^{c-1}} (x^{p^c})^m = x^{p^{c-1}}. \end{aligned}$$

Hence the p -element $x^{p^{c-1}}$ commutes with the q -element in G , so we have a contradiction with lemma (2-4). Thus (2-4) holds.

Conversely, let G be a polycyclic group satisfying conditions (2-3), and (2-4). Then from [9] we see that G is an extension of cyclic p -group $\langle x \rangle$ of order p^c by cyclic q -group $\langle y \rangle$ of order q^b , $p \neq q$ (p and q are primes) $b, c \in \mathbb{Z}^+$. Thus $(|\langle x \rangle|, |\langle y \rangle|) = 1$ and $|G| = |\langle x \rangle| |\langle y \rangle|$, then $\langle x \rangle \cap \langle y \rangle = \{1\}$ and $G = \langle x \rangle \langle y \rangle$,

so $G = \langle x \rangle \rtimes \langle y \rangle$. Since $\langle x \rangle \trianglelefteq G$ and $\langle x \rangle$ is an abelian p -group, then by using theorem (2-7) we prove that G is a group with the basis property.

Now consider the polynomial $g(x) = x - r$ over the ring \mathbb{Z} . Denote that $f(x) = \bar{\theta}(g(x))$. Then the polynomial $f(x)$ is an irreducible over the field $GF(p)$ and has \bar{r} zeros. Thus by (2-2), and (2-4) we have $\bar{r}^{q^b} = 1$, $\bar{r}^{q^{b-1}} \neq 1$, hence by Bezout theorem the polynomial $f(x)$ is divides $x^{q^b} - 1$ and not divides $x^{q^{b-1}} - 1$, i.e. the condition 1) in theorem(2-7) holds for $g(x)$. Now consider the automorphism φ , which defines a semidirect product $\langle x \rangle \rtimes \langle y \rangle$ and induced by y element, i.e.

$$\varphi : a \rightarrow y^{-1}ay, \quad \forall a \in \langle x \rangle.$$

From (2-1) we get

$$\varphi(a) = a^r, \quad \forall a \in \langle x \rangle.$$

Using additive form in $\langle x \rangle$, then we have $g(\varphi) = 0$. Thus the condition 2) of theorem(2-7) for $g(x)$ holds too. Hence G is a group with the basis property. \square

3 Exchange property

The fundamental property of generating operator φ of subspace of the vector space V over the field F that this operator satisfies exchange property.

Definition 3.1 Let V be a vector space, then $\forall x, y \in V$ and for every subset $X \subseteq V$ if $x \notin \varphi(X)$ and if $x \in \varphi(X \cup \{y\})$, then $y \in \varphi(X \cup \{x\})$.

Theorem 3.2 Let G be a group with the exchange property, i.e. $\forall x, y \in G$ and for every subset $X \subseteq G$,

$$\text{if } x \notin \langle X \rangle \wedge x \in \langle X \cup \{y\} \rangle, \text{ then } y \in \langle X \cup \{x\} \rangle. \quad (3-1)$$

Then the order of every element $a \in G$, $a \neq 1$ is a prime.

Proof. First, we prove that every cyclic subgroup of G is simple, i.e. every cyclic subgroup does not contain non trivial normal subgroup.

Suppose that $\{1\} \leq \langle x \rangle \leq \langle y \rangle$ for $x, y \in G$. Then $x \notin \{1\}$ and $x \in \langle \{1\} \cup \{y\} \rangle$ such that substituting $X = \{1\}$ in (3-1) we find $y \in \langle \{1\} \cup \{x\} \rangle = \langle x \rangle$ and we get a contradiction with our assumption. Thus $O(x) \in \{p, q\}$, $\forall x \in G \setminus \{1\}$.

Theorem 3.3 Let G be a p -group such that p is a prime. Then G is a group with the exchange property if and only if G is elementary abelian p -group.

Proof. Suppose that G is a p -group with the exchange property. Then by theorem (3-2)

$$x^p = 1, \forall x \in G, \quad (3-2)$$

hence $G^p = \{1\}$ and by [10] $\Phi(G) = G^p G'$. Since G is a p -group, then

$$\Phi(G) = G', \quad \Phi^2(G) = G'', \dots$$

If $G' = \{1\}$, then G is an elementary abelian group.

Suppose that $G' \neq \{1\}$. Then there exist elements $a, b, c \in G$ such that

$$[a, b] = a^{-1}b^{-1}ab = c \neq 1. \quad (3-3)$$

Now assume that $c \in \langle a \rangle$, then $a \in \langle c \rangle$. Let consider the subgroup, which is generated by two elements a, b , i.e. $\langle a, b \rangle$. If $\langle a, b \rangle$ is a cyclic group, then it is commutative and we have a contradiction with (3-3), then $a \notin \langle b \rangle$ and $b \notin \langle a \rangle$. Hence the set $\{a, b\}$ forms a basis of group $\langle a, b \rangle$. Since $\langle a \rangle = \langle c \rangle$, so $\langle a, b \rangle = \langle c, b \rangle$ and by the basis property of G [6]. Thus we have that the set $\{c, b\}$ forms a basis of G and this is a contradiction with properties of the Frattini subgroup, i.e. $c \in \Phi(G)$.

Hence $c \notin \langle a \rangle$ and $c \in \langle a, b \rangle$, and by the exchange property we have $b \in \langle a, c \rangle$. But then $\langle a, b \rangle = \langle a, c \rangle$. So by the basis property for G and since $a \notin \langle b \rangle$, $b \notin \langle a \rangle$ we conclude that the set $\{a, c\}$ forms a basis for G . Hence this is a contradiction with properties of the the Frattini subgroup $\Phi(G)$, i.e. $c \in \Phi(G)$. Thus $[a, b] = 1$ and the group G is an elementary abelian p -group.

Conversely, suppose that a group G is an elementary abelian p -group, then we consider G as an additive group of a vector space over the field $GF(p)$.

Hence the exchange property is satisfied for a group G .

4 Intersection between the basis property and the exchange property

Example 4.1 Let S be the semilattice $\{a, b, 0\}$, where a, b are incomparable and $ab = 0$. Then S has unique basis, so S has basis property. But $0 \in \langle \langle a \rangle \cup \{b\} \rangle$ and $0 \notin \langle \langle a \rangle \rangle$, $b \notin \langle \langle a \rangle \cup \{0\} \rangle$. Hence S does not satisfy the exchange property.

Example 4.2 Let $G = \langle a \rangle$ be a cyclic group such that $|G| = p^2$, p is a prime. Then G is a group with the basis property, because it is a p -group, but it does not satisfy the exchange property.

Theorem 4.3 Let G be a finite group. Then G is a group with the exchange property if and only if one of the following conditions hold:

1. G is an elementary abelian p -group, p is a prime.
2. G is a semidirect product of an elementary abelian p -group P by a cyclic q -group $\langle y \rangle$, of order q , where $p \neq q$ (p and q are primes). Therefore G must satisfy the following relations:

$$\begin{aligned} p &\equiv 1 \pmod{q}, & y^{-1}ay &= a^r, & r &\in \mathbb{Z}^+, \\ r &\not\equiv 1 \pmod{p}, & r^q &\equiv 1 \pmod{p}. \end{aligned}$$

Proof. Suppose that G is a group with the exchange property. Then we consider two cases:

Firstly, if G is a primary group (p -group), p is a prime, then by theorem(3-3) G is an elementary abelian p -group for a prime p .

Secondly, if G is not primary group, then from the basis property in theorem(2-6), we see that G is a semidirect product (i.e. $G = P \rtimes \langle y \rangle$) of p -group P by a cyclic q -group $\langle y \rangle$, where $p \neq q$ (p and q are primes). Since P is a group with the exchange property, then by theorem(3-3) P is an elementary abelian p -group. Therefore by theorem(3-1) the group $\langle y \rangle$ has order q , q is a prime.

Suppose that $|P| = p^s$, $s \in \mathbb{Z}^+$. Since the element y is regular operator on P , i.e. the operator φ inducing by element y is a regular, then

$$p^s \equiv 1 \pmod{q}.$$

Assume that $a \in P$, $a \neq 1$. Consider the element $b = y^{-1}ay$, since the operator φ induced by element y is regular, then $b \neq a$. Assume that $b \in \langle a \rangle$, hence $b = a^r$, $r \not\equiv 1 \pmod{p}$. From $y^q = 1$ we have $a^{r^q} = 1$, i.e. $r^q \equiv 1 \pmod{p}$.

Now let $b \notin \langle a \rangle$, so by the exchange property if $b \in \langle y, a \rangle$, then $y \in \langle a, b \rangle \leq P$. We get a contradiction with $y \notin P$. Thus the automorphism $\varphi_y : P \rightarrow P$ is regular and act on a group $\langle a \rangle$ of order p , hence $p \equiv 1 \pmod{q}$ and $p > q$. Since G is a group with the basis property, then by theorem(2-6) the representation $y \rightarrow \varphi_y$ is an isotopic with dimension 1, i.e. the matrix A of linear operator φ_y in some basis of vector space P which contains s elements has the following form:

$$A = \begin{pmatrix} \bar{r} & 0 \dots & 0 \\ 0 & \bar{r} \dots & 0 \\ 0 & 0 & \bar{r} \end{pmatrix},$$

such that \bar{r} is an image of the element r under the conical homomorphism $\bar{\theta}: \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$, then

$$r \not\equiv 1 \pmod{p}, \text{ and} \\ r^q \equiv 1 \pmod{p}.$$

Conversely, If G is an elementary abelian p -group for a prime p , then G is a group with basis property. Using theorem(3-3), then it remains to prove that if P is an elementary abelian, and $\langle y \rangle$ has order q , where $p \neq q$ (p and q are primes), and if the following conditions hold

$$y^{-1}xy = x^r, \forall x \in P, \\ p \equiv 1 \pmod{q}, \\ r \not\equiv 1 \pmod{p}, \\ r^q \equiv 1 \pmod{p}. \quad (4-1)$$

Then G is a group with the exchange property. Suppose that the set $X \subseteq G$ and $a, b \in G$ such that $a \notin \langle X \rangle$ and $a \in \langle X \cup \{b\} \rangle$. Now we prove that $b \in \langle X \cup \{a\} \rangle$.

Let $G_1 = \langle X \cup \{b\} \rangle$ and we study the following cases:

If $\langle X \cup \{b\} \rangle \leq P$, then $G_1 \leq P$, G_1 satisfies the exchange property, because it is an elementary abelian p -group (by theorem(3-3)), hence $b \in \langle X \cup \{a\} \rangle$.

If $\langle X \cup \{b\} \rangle \not\leq P$, then suppose that the set $X \cup \{b\}$ contains element of order q . Now if X contains elements of order q , and since G is a semidirect product of p -group by cyclic $\langle y \rangle$. Then we can prove that the set X contains only one element of order q , (because if there exist two elements as $y^{s_1}a_1$, $y^{s_2}a_2$ in X of order q , then for some $w \in \mathbb{Z}$ there exists $c \in P$ such that

$$y^{s_2}a_2 = (y^{s_1}a_1)^w c.$$

Then $\langle y^{s_1}a_1, c \rangle = \langle y^{s_1}a_1, y^{s_2}a_2 \rangle$, hence we consider element $y^{s_2}a_2$ as $c \in P$. Now suppose that the set $X = \{x_1, x_2, \dots, x_n\}$ such that $x_2, \dots, x_n \in P$, $x_1 \notin P$. Then the Fitting subgroup $F(\langle X \rangle)$ of group $\langle X \rangle$ is generated by the set $\{x_2, \dots, x_n\}$ and the image of this set under the automorphism $\varphi_{x_1}^m$, $m \in \mathbb{Z}$.

Since the group P is an abelian group, then the Fitting subgroup $F(\langle X \rangle)$ is generated by the set $\{x_2, \dots, x_n\}$ and the image of this set under the automorphism φ_y^m and by (4-1) this is the power of the same elements x_2, \dots, x_n . In another words, the group $F(\langle X \rangle)$ is generated by x_2, \dots, x_n if these elements are exists. So by our assumption $a \in \langle X \cup \{b\} \rangle$. Then there exists a word $u(x_1, x_2, \dots, x_n)$ such that $a = u(x_1, x_2, \dots, x_n, b)$ and by (4-1) we have

$$a = v(x_1, x_2, \dots, x_n)b^w, \quad (4-2)$$

such that $v(x_1, x_2, \dots, x_n)$ is a word. If $b^w = e$, then by (4-2) we have

$$a = v(x_1, x_2, \dots, x_n) \in \langle X \rangle .$$

Thus we get a contradiction with our assumption for a , so we assume that $b^w \neq e$. Since a group P is an elementary abelian p -group, then $\langle b^w \rangle = \langle b \rangle$, so by (4-2) we have

$$b \in \langle b^w \rangle = \langle v(x_1, x_2, \dots, x_n)^{-1} a \rangle \subseteq \langle X \cup \{a\} \rangle .$$

Finally, let $X \subseteq P$. Since $X \cup \{b\} \not\subseteq P$, then b is element of order q . Suppose that $G_1 = \langle X \cup \{b\} \rangle$ is a semidirect product of a group $\langle X \rangle$ by $\langle b \rangle$. Then from $a \in \langle X \cup \{b\} \rangle$ we have the following for $w \in \mathbb{Z}$ and $c \in \langle X \rangle$

$$a = b^w c. \quad (4-3)$$

If an element a is a q -element, then $b^w \neq e$ and since $\langle b \rangle = \langle b^w \rangle$ we get

$$b \in \langle b^w \rangle = \langle c^{-1} a \rangle \subseteq \langle X \cup \{a\} \rangle .$$

If a is p -element, then by (4-3) we have $b^w = e$ and $a = c \in \langle X \rangle$ which is a contradiction with $a \notin \langle X \rangle$. Thus we study all cases. Hence G is a group with change property.

5 Acknowledgements

The authors gratefully acknowledge the partial financial support from the Deanship of Academic Research (Project No.331201) at Al Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia.

References

- [1] A. Al Khalaf, Finite group with basis property, Dok. Acad. Nauk BSSR, n. 11, 1989 (Russian)
- [2] M. Alkadhi, A. Al Khalaf and M. Quick, The Nilpotency Class of Fitting Subgroups of Groups with Basis Property. International Journal of Algebra, Vol. 6, 2012, no. 14, 697 - 704.
- [3] A. Aljouiee, Basis Property Conditions on Some Groups, International Journal of Mathematics and Computer Science, 3, No3, 1-11, (2008), Lebanon.

- [4] Jonathan McDougall-Bagnall, Martyn Quick, Groups with the basis property, *Journal of Algebra* 346 (2011) 332-339.
- [5] P. R. Jones, A basis theorem for free inverse Semigroup, *J. Algebra*, v. 49, 1977. p.172-190.
- [6] P. R. Jones, Basis properties for inverse Semigroups, *J. Algebra*, v. 50, 1978. p.135-152.
- [7] P. R. Jones, Basis properties, exchange properties and embeddings in idempotent-free semigroups, *Semigroups and their applications*, 69-82, Reidel, Dordrecht, 1987.
- [8] P. R. Jones, Exchange properties and basis properties for closure operators, *Colloq. Math.* 57(1989), no. 1, 29-33.
- [9] M. Hall, *The Theory of Groups*, Macmillan, 1959.
- [10] B. Huppert, *Endliche Gruppen*, Springer-Verlag, 1967.
- [11] D. Robinson, *A Course in the Theory of Groups*, Second Edition. Springer-Verlag New York, Inc. (1996)

Al Khalaf Ahmad,
Department of Mathematics, College of Sciences
Al-Imam Mohammad Ibn Saud Islamic University
P.O. Box 90950, Riyadh, Saudi Arabia.
Email: akhalaf59@gmail.com

Alkadhi Mohammed
Department of Mathematics, College of Sciences
Al-Imam Mohammad Ibn Saud Islamic University
P.O. Box 90950, Riyadh, Saudi Arabia.
Email: malki2@yahoo.com