SOME PROPERTIES OF HALL SUBGROUP

Muthana Abdul-Wahed Mahmoud
University of Anbar - College of Education for Pure Sciences

Abstract: In the present paper, the order and index of the normal abelian Hall subgroups have been studied through using of some functions defined on group rings. Also, some properties of homomorphism have been studied.

Key Words: finite group, Hall subgroup.

Introduction: Let $G$ a group and $H, K$ subgroups of finite index in a group $G$. Also $S$ a subset of group $G$, then $|S|$ will denote the order of $S$, and $|G:H|$ will denote the index of $H$ in group $G$, and $H$ is Hall subgroup if $G$ is a finite group and $|G:H|$ is relatively prime to $|H|$.

We prove in this paper the following corollary: (Let $G$ be a group containing a normal abelian Hall subgroup $A$ of order $m$ and index $n$ in $G$. Then there exists a subgroup $U$ of order $n$ in $G$ it follows that $G = U A$ and $U \cap A = 1$).

Definition 1: [1]
If $H$ is a subgroup of finite index in a group $G$, and $K$ is a subgroup of $G$ containing $H$, then $K$ is of finite index in $G$, and

$$|G:H| = |G:H| \left\| K:H \right\|.$$

Definition 2: [1]
Let $A$ and $B$ be subgroups of group $G$. If $B$ is of of finite index in $G$, then $A \cap B$ is a subgroup of finite index in $A$, and

$$|A : A \cap B| \leq |G : B|.$$

Equality holds if and only if $G = A B$.

In particular, if $|G : A|$ is also finite, then

$$|G : A \cap B| \leq |G : A| \left\| G : B \right\|$$

with equality if and only if $G = A B$.

Definition 3: [1]
If $N$ and $K$ are subgroups of group $G$, and $N$ is normal in $G$, then $N K$ is a subgroup of $G$, and

$$N K / N \cong K / (N \cap K).$$

Proposition (1): [1]
If $A$ and $B$ are subgroups of finite index in a group $G$, and $|G : A|$ and $|G : B|$ are relatively prime, then $G = A B$.

Proof: By (Definition 1), $|A : A \cap B|$ is divisible by both $|G : A|$ and $|G : B|$, and so by their least common multiple. Since $|G : A|$ and $|G : B|$ are relatively prime, their least common multiple is $|G : A| \left\| G : B \right\|$, and so this is at most $|G : A \cap B|$. The result now follows from (Definition 2).

Proposition (2): [2]
If $A, B$ and $C$ are subgroups of group $G$, and $A \subseteq C$, then

$$AB \cap C = A \left( B \cap C \right).$$

Note: $AB$ is not necessarily a subgroup of $G$.
Prove: Let $a \in A \left( B \cap C \right)$, where $a \in A$, and $c \in \left( B \cap C \right)$. Then $a c \in A B$, and $a c \in a C = C$.

Therefore $A \left( B \cap C \right) \subseteq A B \cap C$.

On the other hand, if $a b \in A B \cap C$, where $a \in A$ and $b \in B$, then $b \in a^{-1} C = C$, and so $a b \in A \left( B \cap C \right)$.

Thus $A B \cap C \subseteq A \left( B \cap C \right)$, and the result follows.

Definition 4: [2]

Let $G$ be an arbitrary group, and let $\Omega$ be a set for which, for each $\alpha \in \Omega$ and each $x \in G$, we have defined an element $\alpha^x \in \Omega$ with the properties:

(a) The mapping $\alpha : \alpha \rightarrow \alpha^x$ is a permutation of the set $\Omega$ for each $x \in G$;

and

(b) $x y = y x$ for all $x, y \in G$.

Then for each $\alpha \in \Omega$ the set $\alpha^G = \{ \alpha^x | x \in G \} \subseteq \Omega$ is called the orbit (or transitivity set) of $\alpha$, and the number of letters which $\alpha^G$ contains is the length of the orbit.

The set $G_\alpha = \{ x \in G | \alpha^x = \alpha \} \subseteq G$ is called the stabilizer (or stability subgroup) of $\alpha$.

Proposition (3): [3]

The mapping $x \rightarrow \alpha^x : \{ x \in G \}$, where $\alpha$ is defined in Definition 2 (a) above defines a homomorphism of $G$ into $S_\Omega$. The kernel of the homomorphism is $\bigcap_{\alpha \in \Omega} G_\alpha$.

Prove: The mapping is into $S_\Omega$ by Definition (2) (a), and a homomorphism is $\{ x \in G | a^x = a \text{ for all } a \in \Omega \} = \bigcap_{\alpha \in \Omega} G_\alpha$.

Proposition (4): [2]

Let $H$ be a subgroup of a group $G$. We define $\Omega$ to be the set of all right cosets $H a \left( a \in G \right)$, and define $(H a)^x = H a x \left( H a, H a x \in \Omega; x \in G \right)$.

Then the stabilizer of $H a$ is $a^{-1} H a$, and the kernel $K$ of the homomorphism defined in Proposition (3) is $\bigcap_{a \in G} a^{-1} H a$, which is the largest subgroup of $H$ normal in $G$.

Prove: The stabilizer of $H a$ is $\{ y \in G | H a y = H a \} = \{ y \in G | y a^{-1} H a \} = a^{-1} H a$.

Hence, by Proposition (3) the kernel of the homomorphism is as described. If $N \subseteq H$, and $N$ is a normal subgroup of $G$, then $N = a^{-1} N a \subseteq a^{-1} H a$ for all $a \in G$, and so $N \subseteq K$ as required.

Proposition (5): [2]

If $G$ is a finite group, and $n$ is a positive integer relatively prime to the order of $G$, then for each $x \in G$, there is a unique $y \in G$ such that $y^n = x$.

In particular, if $y^n = z^n$ for two elements $y$ and $x$ in $G$, then $y = z$.

Prove: We first show that, if $y, z \in G$ and $y^n = z^n$ then $y = z$.

Let $m = |G|$ since $m$ and $n$ are relatively prime, there exist integers $s$ and $t$ such that $ms + nt = 1$. Then $y^m = y^{ms + nt} = y^{nt} = z^{nt} = z^m = z$.

because the order of $y$ and $z$ both divide $m$.

It now follows that the set $\{ y^n | y \in G \}$ contains $|G|$ distinct elements of $G$, and so comprises the whole of $G$. Thus $x = y^n$ for some unique $y$ in $G$.

Let $C$ denote the field of complex numbers. Let $G$ be a group, and consider the
set \( R_G \) of all formal sums: \( \sum_{x \in G} \alpha_x x (\alpha_x \in C) \) in which all but a finite number of coefficients \( \alpha_x \) are zero. We define addition and multiplication in \( R_G \) by

\[
\left( \sum_{x \in G} \alpha_x x \right) + \left( \sum_{x \in G} \beta_x x \right) = \sum_{x \in G} (\alpha_x + \beta_x) x
\]

And

\[
\left( \sum_{x \in G} \alpha_x x \right) \left( \sum_{x \in G} \beta_x x \right) = \sum_{x \in G} \gamma_x x ,
\]

where \( \gamma_x = \sum_{z \in G} \alpha_{x^{-1}z} \beta_z \).

(Note that \( \gamma_x \) is a finite sum of elements in \( C \) because \( \beta_z \) is zero for all but a finite number of \( z \in G \).)

**Definition 5:** [3]

An element \( \sum_{x \in G} \alpha_x x \) in \( R_G \), which for some \( u \in G \), has \( \alpha_u = 1 \) and \( \alpha_x = 0 \) for \( x \neq u \), is written as \( u \) and is said to be an element of \( R_G \) lying in \( G \). It is readily shown that \( R_G \) is an associative ring with unity element 1 (the identity of \( G \)), and that \( R_G \) is commutative if and only if \( G \) is abelian.

We call \( R_G \) the group ring of \( G \) (over \( C \)).

**Proposition 6:** [5]

Let \( G \) be a finite group of order \( mn \), where \( m \) is relatively prime to \( n \). Let \( A \) be normal abelian subgroup of order \( m \), and let \( H \) and \( K \) be subgroups of order \( n \) in \( G \). Then there is an isomorphism \( \theta \) of \( H \) onto \( K \) such that:

\[
A x = A x^0 \left( x \in H ; x^0 \in K \right).
\]

Moreover, for some \( c \in A \),

\[
c x c^{-1} = x^0 \text{ for all } x \in H.\]

Thus, \( H \) is conjugate to \( K \) in \( G \).

**Proof:** Since \( m \) is relatively prime to \( n \), \( G = AH = AK \) by (Proposition 1) and:

\[
A \cap H = A \cap K = 1.
\]

Thus \( H \) and \( K \) are each complete sets of coset representatives for \( A \) in \( G \). Therefore we can define a one-to-one mapping \( \theta \) of \( H \) onto \( K \) by the condition

\[
A x = A x^0 \left( x \in H ; x^0 \in K \right).
\]

Since

\[
A(x y)^0 = A x y = (A x)(A y) = (A x^0)(A y^0) = A(x^0 y^0)
\]

for any \( x, y \in H \), it follows that \( \theta \) is an isomorphism of \( H \) onto \( K \).

We now construct \( c \). Since \( u^0 u^{-1} \in A \) for all \( u \in H \), and \( A \) is abelian, we can define \( b \in A \) by

\[
b = \prod_{u \in H} u^0 u^{-1}.
\]

For all \( x \in H \), we have

\[
x b x^{-1} = \prod_{u \in H} \left\{ x (x^0)^{-1} (x u)^0 (x u^{-1}) \right\} = \prod_{u \in H} \left( (x u)^0 (x u^{-1}) \right) = \prod_{u \in H} b.
\]

Because \( m \) is relatively prime to \( n \), we can use (Proposition 5) to find \( c \in A \) such that \( b = c^n \). Then

\[
\left( x c x^{-1} \right)^n = x c^n x^{-1} = x \left( \left( x^0 \right)^{-1} c \right)^n.
\]

Thus by (Proposition 5),

\[
x c x^{-1} = x \left( x^0 \right)^{-1} c ; \text{ that is,}
\]

\[
x^0 = c x c^{-1}.
\]

In particular,

\[
K = c H c^{-1}.
\]

**Definition 6:** [4]

The set \( M(n, G) \) of all \( n \times n \) monomial matrices over \( G \) is a group in which \( D(n, G) \) is a normal subgroup. Moreover,

\[
M(n, G) = S(n) \cap \left\{ D(n, G) \right\}
\]

and

\[
S(n) \cap \left\{ D(n, G) \right\} = 1.
\]

**Definition 7:** [2]

Let \( G \) be a group with a subgroup \( H \) of finite index \( n \) in \( G \). Let \( \theta \) be a
homomorphism of $H$ into a group $S$.

Then we define $\tilde{\theta}$ as a function of $G$ into the group ring of $S$ by:

$$\tilde{\theta}(x) = \begin{cases} \theta(x) & \text{if } x \in H \\ 0 & \text{otherwise} \end{cases}$$

**Definition 8:**

$$\theta^G(x) = \begin{bmatrix} \tilde{\theta}(r_1^{-1}x r_j) & \tilde{\theta}(r_1^{-1}x r_2) & \cdots & \tilde{\theta}(r_1^{-1}x r_n) \\ \tilde{\theta}(r_2^{-1}x r_j) & \tilde{\theta}(r_2^{-1}x r_2) & \cdots & \tilde{\theta}(r_2^{-1}x r_n) \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{\theta}(r_n^{-1}x r_j) & \tilde{\theta}(r_n^{-1}x r_2) & \cdots & \tilde{\theta}(r_n^{-1}x r_n) \end{bmatrix}$$

$$= \left[ \tilde{\theta}(r_i^{-1}x r_j) \right] \quad \ldots \ldots (\ast)$$

The matrix $\theta^G(x)$ lies in $M(n, S)$.

**Proposition (7):** [4]

Let $\theta^G(x)$ be the function of the group $G$ into $M(n, S)$ as defined by (\ast). Then $\theta^G(x)$ is a homomorphism of $G$ into $M(n, S)$. If the kernel of $\theta$ is $N$, then the kernel of $\theta^G$ is $\bigcap_{x \in G} x^{-1}Nx$.

**Proof:** For any $x, y \in G$, we have

$$\theta^G(x) \theta^G(y) = \left[ \tilde{\theta}(r_i^{-1}x r_j) \right] \left[ \tilde{\theta}(r_i^{-1}y r_j) \right] = \sum_{k=1}^{n} \tilde{\theta}(r_i^{-1}x r_k) \tilde{\theta}(r_i^{-1}y r_j)$$

But $\tilde{\theta}(r_i^{-1}x r_k) \tilde{\theta}(r_i^{-1}y r_j)$ is nonzero only if we have both $(r_i^{-1}x r_k)$ and $(r_i^{-1}y r_j)$ lying in $H$ which is, both $(x^{-1}r_i)$ and $(y r_j)$ lying in the same coset $r_kH$.

For given $i$ and $j$ there is at most one such $k$. There is such a $k$ exactly when

$$(x^{-1}r_i)^{-1}(y r_j) = r_i^{-1}x y r_j$$

lies in $H$. Thus

$$\sum_{k=1}^{n} \tilde{\theta}(r_i^{-1}x r_k) \tilde{\theta}(r_i^{-1}y r_j) = \tilde{\theta}(r_i^{-1}x y r_k).$$

Hence

$$\theta^G(x) \theta^G(y) = \theta^G(x y)$$

for all $x, y \in G$, and so $\theta^G(x)$ is a homomorphism. Finally,

$$\theta^G(x) = \text{diag}(1, 1, \ldots, 1)$$

if and only if $(r_i^{-1}x r_j) \in N$ for each $i$. Thus the kernel of $\theta^G$ is

$$\bigcap_{i=1}^{n} r_i N r_i^{-1} = \bigcap_{x \in G} x^{-1}N x$$

**Definition 9:** [4]

Let $G$ be a group, $H$ a subgroup of $G$, and $S$ a subset of $G$. Then $|S|$ will denote the order of $S$, and $|G:H|$ will denote the index of $H$ in $G$. If $G$ is a finite group, then $H$ is a Hall subgroup of $G$ if $|G:H|$ is relatively prime to $|H|$.

**Proposition (8):** [5]

Let $G$ be a group possessing a normal abelian Hall subgroup $A$ of order $m$ and index $n$ in $G$. If $H$ is a Hall subgroup of order $n$ in $G$, and $K$ is a subgroup of $G$ such that $n$ divides $|K|$, then for some $x \in G$, $x^{-1}H x \subseteq K$.

**Proof:** The subgroup $N = K \cap A$ is normalized by both $A$ and $K$, and so it is a normal subgroup of $G = KA$. The
group $G \div N$ contains two Hall subgroup $K \div N$ and $H \div N \div N$ of order $n$, using (Definition (3)), and an abelian normal subgroup $A \div N$ of index $n$. Therefore, by (Proposition (6)), there is $x \in G$ such that

$$x^{-1} H x \subseteq x^{-1} H N x = K$$

Corollary:

Let $G$ be a group containing a normal abelian Hall subgroup $A$ of order $m$ and index $n$ in $G$. Then there exists a subgroup $U$ of order $n$ in $G$ such that $A U \subseteq G$ and $1 = A U \cap G$.

Proof: Let $\theta$ be the identity homomorphism of $A$ onto itself; that is $\theta (a) = a$ for all $a \in A$. Writing $G^* = \theta G (G)$ and $A^* = \theta G(A)$, we have $G^* \cong G$ and $A^* \cong A$, by (Proposition (7)). Now

$$P = S (n) \cap G^* D (n, A)$$

is a group of permutation matrices, and

$$P D (n, A) = \left\{ S (n) \cap G^* D (n, A) \right\} D (n, A) = S (n) D (n, A) \cap G^* D (n, A) = G^* D (n, A)$$

Using (Proposition (2)) and (Definition (6)). Therefore

$$|P| = |P : P \cap D (n, A)| =$$

$$= |P D (n, A) : D (n, A)| =$$

$$= |G^* : G^* \cap D (n, A)| =$$

$$= |G^* : A^*| = n$$

Thus $P$ is a Hall subgroup of $P D (n, A)$. Since $D (n, A)$ is abelian and of order $|A|^n$, and $n$ divides $|G^*|$, it follows from (Proposition (8)) that $G^*$ contains a subgroup of order $n$ conjugate to $P$ in $G^* D (n, A)$.

Thus $G$, which is isomorphic to $G^*$, has a subgroup of order $n$ as asserted.

References:


3- Rotman J. J. Theory of groups, Boston, Allyn and Bacon 1965.
