Studies in Mathematical Sciences **ISSN 1923-8444 [Print]**
Vol. 1, No. 1, 2010, pp. 52-60 **ISSN 1923-8452 [Online]**
www.cscanada.org **www.cscanada.net**

On the Construction of Normal Subgroups

ZENG Li-Jiang[1,*]

Abstract: Introduced extension of a group and other concepts, several of lemmas and theorems on the construction of normal subgroups were proved to use the theory of group characters, and then shows that the construction of normal subgroups of a finite group G.

Key Words: Normal Subgroup; Irreducible Character; Semi-direct Product; Regular Representation; p-Sylow Subgroup

The construction of normal subgroups of a finite group G is one of important problems in group theory. A theorem in the article enables us, under certain conditions, to show the existence of a normal subgroup with preassigned factor group. In this article we shall give theorems on the construction of normal subgroups, the proofs of which will use the theory of group characters.

Let us make preparation for our proof as the following:

Lemma 1 Let $H \lhd G$, and set $i=[G:H]$, $j=[H:1]$. If i and j are relatively prime, show that H is the only subgroup of G of order j.

Proof. Let S be a subgroup of G of order j. Then HS/H is a subgroup of G/H whose order divides i. Also $HS/H \cong S/(S \cap H)$ implies that the order of HS/H divides j. Therefore $HS=H$. The lemma is proved.

Definition 1 A group U is called an extension of a group G by a group H if there exists a homomorphism φ of U onto G with kernel H. the extension is called a split extension if there exists a homomorphism ψ of G into U such that $\varphi\psi=1$.

The example of the generalized quaternion groups shows that even when G and H are commutative, not every extension of G by H need be a split extension. However, there is one important case in which we know that an extension must split. We state without proof.

Lemma 2 (Schur) Let $H \lhd G$, $i=[G: H]$, $j=[H: 1]$, and assume that i and j are relatively prime. Then G contains a subgroup S of order i , and G is a semi-direct product of S and H.

For the proof the reader may consult Reference [1], [2], or [3].

Definition 2 Let the KG-module M afford a matrix representation T, and set $\mu(x)=tr(T(x))$, $x \in KG$. The map μ: $KG \to K$ given by $x \to \mu(x)$ is called the character of M (or of T), and we say that M (or T) affords the character μ. Obviously $\mu(1)=(M: K)$. where l is the unity element of KG. Furthermore we have

(1) $\mu(x+y)=\mu(x)+\mu(y)$, $\mu(\alpha x)=\alpha\mu(x)$, $x, y \in KG$, $\alpha \in K$.

---

[1]Department of mathematics, Zunyi Normal College, No. 830 Shanghai Road, Zunyi 563002, Guizhou Province, China.
*Corresponding author. E-mail address: zlj4383@sina.com.
†Received 10 Semptember 2010; accepted 30 Semptember 2010.

By a group character we mean the restriction of μ to G. A character μ is completely determined by its restriction to G, as is evident from (1). We shall use repeatedly

(2) Each group character μ is a class function on G; that is for $g\in G$ the value $\mu(g)$ depends only upon the conjugate class to which g belongs.

(3) Let

$$M=M_k \supset M_{k-1} \supset \cdots \supset M_1 \supset M_0=(0),$$

be a chain of KG-modules, and let μ_i be the character afforded by the factor module M_i/M_{i-1}, $1 \leqq i \leqq k$. Then we claim that M affords the character $\mu_1+\cdots+\mu_k$. For we may adapt a K-basis of M to the above chain of submodules. The matrix representation afforded by M takes the form

$$x \to T(x) = \begin{pmatrix} T_1(x) & * & \cdots & * \\ 0 & T_2(x) & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & T_k(x) \end{pmatrix},$$

where T_i is the representation afforded by M_i/M_{i-1}, $1\le i\le k$. Therefore,

$$trT(x)=\mu_1(x)+\cdots+\mu_k(x),\ \ x\in KG.$$

As a consequence of Schur's Lemma 2 above, we obtain the fundamental result:

Lemma 3 The functions $\zeta^{(1)}, \cdots, \zeta^{(s)}$ are linearly independent over K under either of the following hypotheses:

(i)K is a splitting field for G,

(ii) *char* K=0.

The proof of Lemma 3 can be found in Reference [4].

Let G be a finite group whose irreducible characters in the complex field K are $\zeta^{(1)}, \cdots, \zeta^{(s)}$,where $\zeta^{(1)}$ is the l-character. By a class function on G is meant a map ψ: $G\to K$ such that $\psi(g)$ depends only upon the conjugate class of g. Since there are s classes, the set of all class functions on G forms an s-dimensional vector space over K. By (2) and Lemma 3, $\zeta^{(1)}, \cdots, \zeta^{(s)}$ are class functions which are linearly independent over K, and thus constitute a K-basis for this vector space.

For and subset S of G, let G-S denote the set of elements in G which are not in S. Further define

$$t^s = s^{-1}ts \qquad t, s \in G.$$

We may now state theorem 1 of this article.

Theorem 1 Let H be a subgroup of G such that

(4) $H\cap H^t=1$ for all $t\in G\text{-}H$.

Set

(5) $G^*=G-\bigcup_{s\in G}(H-1)^s$,

Then $G^* \lhd G$, and we have

(6) $H\cap G^*=1$, $HG^*=G$, $G/G^*\cong H$.

Remark 1 The first two relations in (6) obviously imply the third. The formulas (6) assert that G is the semi-direct product [5] of G^* and H.

We shall prove here the following generalization.

Theorem 2 Let $H^* \lhd H \subset G$ be groups such that

(7) $H \cap H^t \subset H^*$ for all $t \in G\text{-}H$.

Then there is a unique solution G^* of the equations

(8) $G^* \lhd G$, $H \cap G^* = H^*$, $HG^* = G$.

Indeed G^* coincides with the subset of G given by

(9) $S = G - \bigcup_{g \in G} (H - H^*)^g$.

We begin the proof with a pair of lemmas. Throughout this article, "character" will mean "character of a representation [6] by matrices over K".

Lemma 4 Let $H^* \lhd H \subset C$ be groups such that (8) holds for some G^*. Then we have

(i) $G/G^* \cong H/H^*$.

(ii) Every character of H which is constant on H^* can be extended to a character of G constant on G^*.

(iii) If F is a group such that $H \subset F \subset G$, then there exists a subgroup $F^* \lhd F$ such that $H \cap F^* = H^*$, $HF^* = F$.

Proof. The homomorphism theorems [7] easily imply (i). Now let T be a representation of H (by matrices over K) with character τ , and let $\tau(h) = \tau(1)$for $h \in H^*$. Then $T(h) = T(1)$ for all $h \in H^*$, by (3). Extend T to a representation of G by setting

$$T(g) = T(h), \quad g \in G, h \in H,$$

Where gG^* and hH^* correspond to each other in the isomorphism (i). Then the character of T on G is the desired extension of τ . Finally we set $F^* = G^* \cap F$ and easily verify (iii).

A partial converse of the first lemma is the following:

Lemma 5 Let $H^* \lhd H \subset G$ be groups, and S any subset of G containing 1. suppose that every irreducible character ψ of H which is constant on H^* can be extended to a character of G constant on S [8]. Then there exists a subgroup $G^* \lhd G$ such that

$$G^* \supset S, \quad H \cap G^* = H^* .$$

Remark 2 However, $HG^* = G$ need not hold, as may be seen from the example [9] where G is cyclic of order p^2 (p a prime), H is its subgroup of order p, and $H^* = S = (1)$.

Proof The irreducible characters [10] ψ of H which are constant on H^* are in one-to-one correspondence with the irreducible characters $\tilde{\psi}$ of H/H^*, according to the rule

$$\Psi(h) = \tilde{\psi}(hH^*), \quad h \in H.$$

The character $\tilde{\chi}$ of the regular representation [11] of H/H^* can be expressed as a sum of irreducible characters $\tilde{\psi}_i$, say

$$\tilde{\chi} = a_1 \tilde{\psi}_1 + \cdots + a_r \tilde{\psi}_r ,$$

Then

$$\chi = a_1\psi_1 + \cdots + a_r\psi_r ,$$

is a character of a representation of H which is constant on H^* by (3). By the hypothesis, each ψ_i can be extended to a character ψ_i' of G which is constant on $S\cup H^*$. Let T be the representation of G whose character is $a_1\psi_1' + \cdots + a_r\psi_r'$. Then T is constant on $S\cup H^*$ by (3), and for $h\in H$, $T(h)=I$ implies $h\in H^*$, since $\tilde{\chi}$ is the character of a faithful representation of H/H^*. Now define $G^*=\{ g\in G \mid T(g)=I \}$.Then $G^* \lhd G$, $H\cap G^*=H^*$, and $S\subset G^*$. This proves the lemma.

Now let us start the proof of theorem 2. We are given groups $H^* \lhd H\subset G$ for which (7) holds. The theorem is trivially true for the case $H^*=H$ since then G^* must be G. For the remainder of the proof, we may assume that H^* is a proper subgroup of H. We show first the uniqueness of the solution G^*, if there is a solution. For suppose G^* satisfies (8); then on the one hand $H\cap G^*=H^*$ implies that $(H-H^*)\cap G^*$ is empty, whence also

$$(H-H^*)^g \cap G^*,$$

is empty for each $g\in G$, and so $G^*\subset S$. On the other hand, we note that from (7) we may deduce that

$$(H-H^*)^x,\ \ (H-H^*)^y,$$

either are disjoint or coincide, according to whether or not $y\in Hx$. Hence the number of elements in S is $[G: 1]-[G: H]([H: 1]-[H^*: 1])$; that is, S contains $[G: H][H^*: 1]$ elements. But $G/G^*\cong H/H^*$ shows that $[G: H][H^*: 1]=[G^*: 1]$, so S contains$[G^*:1]$elements, and thus $G^*=S$.

Second, we turn to the more difficult "existence" part of the theorem, and shall show that every irreducible character ψ of H constant on H^* may be extended to a character of G constant on S. The result is clear when ψ is the l-character $\psi^{(1)}$, so we exclude this case hereafter. Let χ be a (complex-valued) class function on G which extends ψ and which is constant on S. Then necessarily,

$$\chi(g) = \begin{cases} \psi(1), & g \in S, \\ \psi(g^{x^{-1}}), & g \in (H-H^*)^x. \end{cases}$$

Conversely the above serves to define a class function on G which is constant on S and extends ψ . We wish to show that χ is indeed a character of G, and to do this we shall make use of the orthogonality relations. Set

$$\omega = \chi - t, \qquad \text{t=} t = \chi(1) = \psi(1),$$

so that ω is also a class function, and is given by

$$\omega(g) = \begin{cases} 0, & g \in S, \\ \psi(g^{x^{-1}}) - t, & g \in (H-H^*)^x. \end{cases}$$

Now we may write ω as a K-linear combination of the irreducible characters $\zeta^{(1)}, \cdots, \zeta^{(s)}$ of G, say

$$\omega=a_1\zeta^{(1)}+\cdots+a_s\zeta^{(s)}, \quad a_i \in K.$$

The orthogonality relations yield

$$a_i = [G:1]^{-1}\sum_{g\in G} \omega(g)\overline{\zeta^{(i)}(g)} .$$

Since ω vanishes on S and is class function, we have

$$a_i = [G:1]^{-1} \sum_{g\in G-S} \omega(g)\overline{\zeta^{(i)}(g)}$$
$$= [G:1]^{-1} \sum_{\substack{x\in G \\ x \bmod H}} \sum_{g\in(H-H^*)^x} \omega(g)\overline{\zeta^{(i)}(g)}$$
$$= [G:1]^{-1}[G:H] \sum_{g\in H-H^*} \omega(g)\overline{\zeta^{(i)}(g)},$$

so that

$$a_i = [H:1]^{-1} \sum_{g\in H} \omega(g)\overline{\zeta^{(i)}(g)} \qquad 1\le i\le s.$$

In particular

$$a_1 = [H:1]^{-1} \sum_{g\in H} (\psi(g)-t) = -t,$$

since ψ is not the l-character of H.

From the orthogonality relations on H and the fact that $\omega|H$ and $\zeta^{(i)}|H$ are Z-linear combinations of characters of H, it follows that all the coefficients $a_i \in Z$. Further, from $\omega = \sum a_i\zeta^{(i)}$, we have

$$\sum_{i=1}^{s} a_i^2 = [G:1]^{-1} \sum_{g\in G} |\omega(g)|^2 = [H:1]^{-1} \sum_{h\in H} |\omega(h)|^2 = t^2+1,$$

the second equality holding because ω vanishes outside H, and the last equality following from the fact that

$$\omega|H = \psi - t \bullet \psi^{(1)}.$$

However, we know that a_1=-t and that $\sum a_i^2 = t^2+1$, and so, for $i > 1$, all but one a_i=0, and that exceptional a_i is ±1. Hence

$$\omega = \pm\zeta - t\zeta^{(1)},$$

where ζ is an irreducible character of G, $\zeta \neq \zeta^{(1)}$ and so $\chi = \pm\zeta$. Since $\chi(1)=t>0$, we conclude that $\chi = \zeta$ and we have shown that χ is a character of G.

The above discussion has shown that every irreducible character of H which is constant on H^* may be extended to a character of G constant on Lemma 5, it follows that there exists a subgroup $G^* \lhd G$ such that

$$G^* \supset S, \quad H \cap G^* = H^*.$$

To complete the proof, we need show only that $HG^*=G$. But

$$[HG^*:1] = \frac{[H:1][G^*:1]}{[H^*:1]} \ge \frac{[H:1][S:1]}{[H^*:1]}$$
$$= \frac{[H:1][G:H][H^*:1]}{[H^*:1]} = [G:1],$$

where [S: 1]=number of elements in S. Thus $HG^*=G$. and theorem 2 is proved.

It is easy to prove the deduction of the following formulation of the theorem above in terms of permutation groups (The detail of proof can be found in Reference [5]):

Corollary, let G be a transitive permutation group on the symbols $x_1,\cdots,x_n$. and let

$$H=\{g\in G \mid gx_1=x_1\},$$

and

$$V=\{g\in H \mid gx_i=x_i \text{ for at least one } i>1\},$$

and suppose that V generates the subgroup H^* of H. Then G contains exactly one transitive normal subgroup G^* such that $G^*\cap H=H^*$.

Let us observe now that if $H\neq N_G(H)$, the normalizer of H in G, we may choose $t\in N_G(H)$ such that $t \in G\text{-}H$. For this t, we have

$$H\cap H^t=H,$$

and so (7) can only hold when $H^*=H$. Thus the only time the theorem 2 can be used is when H coincides with its own normalizer. We shall generalize Theorem 2 still further so as to be able to obtain non-trivial results even when $H\neq N_G(H)$.

Theorem 3 Let $H^*\lhd H\subset G$ be groups, and set $F=N_G(H)$. Assume that

$$([F: H], [H: H^*])=1,$$

and that

$$H\cap H^t\subset H^* \quad \text{for all } t \in G\text{-}F.$$

Then there is at most one solution G^* of

(10) $G^*\lhd G,\ H\cap G^*=H^*, HG^*=G$.

Such a solution exists if and only if there is a solution F^* of

(11) $H^*\subset F^*\lhd F,\ \ [F: F^*]=[H: H^*]$.

This latter set of equations has at most one solution. From a solution F^* of (11) one obtains a solution G^* of (10) by setting

(12) $G^*=G-\bigcup\limits_{x\in G}(F-F^*)^x$,

Proof. If F^* satisfies (11), then $[F: HF^*]$ divides both$[F: F^*]$ and$[F: H]$; hence$[F: HF^*]=1$. But then, $[H: H\cap F^*]=[HF^*: F^*]=[F: F^*]=[H: H^*]$.

And since $H^*\subset H\cap F^*$, we conclude that

$$H \cap F^*=H^*,$$

and therefore $H^*\lhd F$. In that case we may form the factor group F/H^*, and notice that F^*/H^* is a normal subgroup of F/H^*, whose index $[F:F^*]$(=$[H: H^*]$) and order $[F^*: H^*]$(=$[F: H]$)are relatively prime. It then follows (see Lemma 1)that the subgroup F^*/H^* is uniquely determined in F/H^*, and so there is at most one F^* satisfying (11).

Suppose now that F^* is a solution of (11), and let us show that

$$F\cap F^t\subset F^* \quad \textit{for all } t\in G\text{-}F,$$

For let $t\in G\text{-}F$, $x\in F\cap F^t$, and set

$$i=[F: H], j=[H: H^*]=[F: F^*].$$

Since $x\in F$ we have $x^i\in H$; likewise $x^i\in H^t$, and so $x^i\in H\cap H^t\subset H^*\subset F^*$. On the other hand $x^j\in F^*$. Thus also $x\in F^*$, since $[F: H]$ and $[H: H^*]$ are relatively prime.

We may therefore apply Theorem 2 to deduce the existence of a subgroup G^* of G satisfying

$$G^*\lhd G,\ F\cap G^*=F^*, FG^*=G,$$

and G^* is given by (12). We find readily that G^* satisfies (10).

Finally we must show that there is at most one solution G^* of (10). For let G^* be any such solution and set $F^*=F\cap G^*$. We have $H^*\subset H\subset F$, $H^*\subset G^*$,

So

$$H^*\subset F\cap G^*=F^*,$$

Certainly, $H^*\lhd F^*$. Finally,

$$G=HG^*\subset FG^*\subset G,$$

so that $FG^*=G$, and we have $[F: F^*]=[G: G^*]=[H: H^*]$. Thus F^* is the unique solution of (11), and so G^* must be given by (12). This completes the proof.

As an application of this result, let us consider the problem of determining the number of solutions of $x^n=1$, $x\in G$, where n is some fixed divisor of $[G: 1]$.

Theorem 4 Let $H^*\lhd H$,G be groups such that

$$H\cap H^g\subset H^* \text{ for all } g\in G\text{-}N_G(H).$$

Set $[H: H^*]=j$, $[G: 1]=mj$, and assume that $(m, j)=1$. If the equation

$$x^m=1,\quad x\in G,$$

has precisely m solutions, these solutions form a characteristic subgroup G^* of G, and we have

$$H\cap G^*=H^*,\ HG^*=G.$$

Proof. Set $F=N_G(H)$, $i=[F: H]$, $s=[H^*: 1]$,and let $M=\{x\in G\,|\,x^m=1\}$, $M_0=\{x\in F\,|\,x^m=1\}$. We note that $H^*\lhd H$ and $s|m$, so that H^* is a normal subgroup of H whose index j is relatively prime to its order s. By Lemma 1, it follows that H^* is the only subgroup of H of order s, and consequently $H^*\lhd F$. there fore we may form F/H^*, and we observe that

$$H/H^*\lhd F/H^*.$$

Now H/H^* has order j, and index i (in F/H^*) which is relatively prime to j. by Lemma 2, we may conclude that F/H^* contains a subgroup F^*/H^* of order i , where F^* is some subgroup of F. We have

$$H^*\subset F^*\subset F,\ [F^*: H^*]=i=[F: H],\ [F: F^*]=[H: H^*]=j.$$

In order to apply Theorem 3, we must verify that $F^*\lhd F$, and this we do by proving that $F^*=M_0$. Since F^* has order $i\cdot s$ which divides m, it is clear that $F^*\subset M_0$. We are now going to show that M_0 contains $i\cdot s$ elements, and we already know (since $F^*\subset M_0$) that M_0 contains at least $i\cdot s$ elements. Note that F contains ijs elements, so that the number of elements in F-M_0 is at most ijs-is.

Suppose next that $y\in G$-M; the order of y cannot divide m, and so there exists a prime p such that $p|j$ and $p|$ order of y. Hence some power of y, call it u, has order p, and $u=u^y$. Now u lies in some p-Sylow subgroup P_0 of G; since $p\dagger[G: H]$, we see that any p-Sylow subgroup P of H is also a p-Sylow group of G, and so we may write $P_0=P^t$ for some $t\in G$. Then $u^y\in P^{ty}$, and hence

$$u \in P^t \cap p^{ty} = (P \cap P^{tyt^{-1}})^t \,,$$

If $tyt^{-1} \in G\text{-}F$, then

$$P \cap P^{tyt^{-1}} \subset H \cap H^{tyt^{-1}} \subset H^* \,,$$

which is impossible because the order of H^* is relatively prime to p, whereas u has order p. This shows that $tyt^{-1} \in F$; that is , y lies in some conjugate of F. Consequently

$$G\text{-}M = \bigcup_{t \in G} (F - M_0)^t \,.$$

The number of distinct conjugates of F is at most $[G: F]$, and the number of elements in $F\text{-}M_0$ is at most $ijs\text{-}is$, so the number of elements in $G\text{-}M$ is at most

$[G: F](ifs\text{-}is)=[G:1]\text{-}m$

Since $G\text{-}M$ contains exactly $[G: 1]\text{-}m$ elements by hypothesis, this shows that $F\text{-}M_0$ contains exactly $ijs\text{-}is$ elements, and so M_0 contains $i{\cdot}s$ elements. Therefore $F^*=M_0$ as stated above, which implies that $F^* \lhd F$

Now we use Theorem 3 to deduce the existence of a normal subgroup G^* in G such that

$$H \cap G^* = H^*,\ HG^* = G,$$

Then we find at once that

$$[G^*: 1] = \frac{[G:1]}{[H:H^*]} = m.$$

So, every element of G^* satisfies $x^m=1$. The hypothesis implies that G^* coincides with $\{x \in G |\ x^m=1\}$,and the theorem is proved.

References

[1] Hall, M. (1959). *The theory of groups*. New York: Macmillan, p.224.

[2] Kurosh, A. G. (1955). *Theory of groups*. New York: Chelsea, 201-202.

[3] Zassenhaus, H. (1938). Neuer beweis der endlichkeit der klassenzahl bei unimodularer aquivalenz endlicher ganzzahliger substitutionsgruppen. *Hamb. Abh., 12*, 276-288.

[4] Mackey, G.W. (1951). On induced representations of groups. *Amer. J. Math., 73*, 576-592.

[5] Robinson, D. J. S. (2003). *A course in the theory of Groups* (2nd ed.). Beijing: World Publishing Corp- oration, 298-326.

[6] Ren X. M., & Shum K. P. (2004). The structure of superabundant semigroups. *Sci China Ser A-Math., 47* , 756-771.

[7] Anderson F. W., & Fuller K. R. (2004). *Rings and categories of modules* (2nd ed.). New York: Springer-Verlag, 233-250.

[8] Li Y., Wang Y., & Wey H. (2003). The influence of π-quasinormality of some subgroups of a finite gro- up. *Arch. Math. (Basel), 81*, 245-252.

[9] Alperin J. L., & Rowen B. B (1997). *Groups and Representations.* New York : Springer-Verlag, 137-164.

[10] Huang J., & Guo W. (2007) . S-conditionally permutable subgroups of finite groups (in Chinese). *Chin. Ann. Math. Ser. A, 28*, 17-26.

[11] Dempwolff U (2001). Primitive rank 3 groups on symmetric designs. *Designs, Codes, and Cryptography, 22*, 191- 207.