66–10,185

MONZINGO, Montie Gene, 1940–
SOME GENERALIZATIONS OF KUMMER'S
THEOREM (HILBERT'S THEOREM 90).

The University of Oklahoma, Ph.D., 1966
Mathematics

THE UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

SOME GENERALIZATIONS OF KUMMER'S THEOREM
(HILBERT'S THEOREM 90)

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

degree of

DOCTOR OF PHILOSOPHY

BY

MONTIE GENE MONZINGO

Norman, Oklahoma

1966

SOME GENERALIZATIONS OF KUMMER'S THEOREM

(HILBERT'S THEOREM 90)

APPROVED BY

Gene Levy

John C. Brixey

A S Davis

George M. Ewing

Robert M. St. John

DISSERTATION COMMITTEE

ACKNOWLEDGMENT

I wish to express my deep appreciation to Dr. Gene Levy for his guidance and assistance in the preparation of this thesis, and to the members of the Thesis Committee for their suggestions and criticisms.

TABLE OF CONTENTS

SOME GENERALIZATIONS OF KUMMER'S THEOREM

(HILBERT'S THEOREM 90)

CHAPTER I

INTRODUCTION

In the study of fields, two subjects for study are the relationships between a field and its extensions and the relationships between a field and its subfields. One topic for investigation which is common to both is the group of automorphisms of some field E which leave fixed the elements of F, a subfield of E. If a field F is extended to a field E, one considers the group G of all automorphisms of E which leave fixed the elements of F. One may also start with a field E and the group $\mathfrak{G}$ of all automorphisms of E, then consider the subfield F of all elements of E left fixed by a subgroup G of $\mathfrak{G}$.

In this paper "group" will always mean "finite group". The following definition is from [1] page 92.

Definition 1.1: G is the group of E/F (read E over F) means that G is the group of all automorphisms of the field E which leave fixed the elements of F, a subfield of E.

Notation: If G is the group of E/F, $b \in E$, $b \neq 0$, and $\sigma \in G$, then, as in [1], by definition

$$b^{I-\sigma} = b\sigma(b^{-1}).$$

The following definition is from [1], page 128.

Definition 1.2: Let G be the group of E/F,

$G = \{\sigma_1, \ldots, \sigma_n\}$, and $a \varepsilon E$, then the norm of a, N(a), is defined by $N(a) = \sigma_1(a) \cdots \sigma_n(a)$.

The following question arises. Which elements x of E satisfy $N(x) = 1$, the multiplicative identity of E?

In the following theorem, which is sometimes called Hilbert's Theorem 90, Kummer answered this question for the case in which G is cyclic [1], page 129.

Theorem 1.1 (Kummer): If the group G of E/F is cyclic with generator σ, then the elements a in E with norm 1 are precisely those which can be written in the form $a = b^{I-\sigma}$, I the identity of G.

Kummer's Theorem discloses a great deal about the relationship between the structures of E and F. In fact, Kummer's Theorem is useful in proving the following structure theorem from [1], page 135.

Theorem 1.2: Let F be a field containing a primitive n-th root of unity, then E is a field extension of F such that the group G of E/F is cyclic of order n if and only if E is the extension of F by means of a single adjunction.

On page 130 of [1] it is stated that it is extremely useful to know the set of elements a for which $N(a) = 1$ and that though many attempts have been made to generalize Kummer's Theorem to arbitrary groups, no answer to the problem has been provided.

The literature has been searched for generalizations of Kummer's Theorem, and there seems to be nothing on the subject. As far as the author knows, all the concepts and results in this paper are new with the exception of the definitions, lemmas, and theorems which have references cited.

This paper will be concerned with a characterization of the elements of E of norm 1 for the case in which G is commutative, and with other generalizations.

In Chapter II, with G arbitrary, there is a characterization of the elements a of E for which $a = b^{I-\sigma}$, for some $b \in E$ and $\sigma \in G$, and a characterization of the elements a of E with norm 1, both in terms of subgroups of G.

In Chapter III, with G solvable, a necessary condition for $a \in E$ to be of norm 1 will be proved. Since commutative groups are solvable, this result will be applicable to commutative groups. The concept of a pseudo-decomposable group will be introduced. Then, the necessary condition proven for solvable groups will be shown to be sufficient for some cases with G pseudo-decomposable. In particular, the condition is both necessary and sufficient with G commutative. It is then shown that Kummer's Theorem is a special case of Theorems 3.1 and 3.2.

In Chapter IV the concept of a factorable group will be introduced. With G factorable a necessary condition for $a \in E$ to be of norm 1 will be proved. This necessary condition will be shown to be sufficient for some cases with G factorable. Then, the necessary condition will be strengthened.

CHAPTER II

THE GROUP G OF E/F ARBITRARY

Kummer's Theorem gives a necessary and sufficient condition for $a \varepsilon E$ to be of norm 1 for the case in which G is cyclic. It is proved that $N(a) = 1$ if and only if $a = b^{I-\sigma}$ for some $b \varepsilon E$ and σ a generator of G. Theorem 2.1, a generalization of Kummer's Theorem, deals with an arbitrary group G. A necessary and sufficient condition is given to guarantee that $N(a) = 1$. It happens that $a = b^{I-\sigma}$ for some $b \varepsilon E$ and $\sigma \varepsilon G$ for special cases with G arbitrary.

Definition 2.1: If G is the group of E/F and H is a subgroup of G, $H = \{I, \sigma_1, \ldots, \sigma_k\}$, then

$$N_H(x) = x\,\sigma_1(x) \cdots \sigma_k(x), \text{ for } x \varepsilon E.$$

Lemma 2.1: If H is a subgroup of G and $x, y \varepsilon E$, then $N_H(xy) = N_H(x)\, N_H(y)$.

Proof:
$$\begin{aligned} N_H(xy) &= xy\,\sigma_1(xy) \cdots \sigma_k(xy) \\ &= xy\,\sigma_1(x)\,\sigma_1(y) \cdots \sigma_k(x)\,\sigma_k(y) \\ &= [x\,\sigma_1(x) \cdots \sigma_k(x)]\,[y\,\sigma_1(y) \cdots \sigma_k(y)] \\ &= N_H(x)\,N_H(y). \end{aligned}$$

Lemma 2.2: If H is a subgroup of G, $\sigma \varepsilon H$, and $x \varepsilon E$, then $N_H[\sigma(x)] = N_H(x)$.

Proof: Since $\sigma \varepsilon H$, $H\sigma = H$. Then,

$$\begin{aligned} N_H[\sigma(x)] &= \sigma(x)\sigma_1[\sigma(x)] \cdots \sigma_k[\sigma(x)] \\ &= x\sigma_1(x) \cdots \sigma_k(x) \\ &= N_H(x). \end{aligned}$$

Lemma 2.3: If H is a subgroup of G and $x \in E$, $x \neq 0$, then $N_H\left[(x^{-1})\right] = \left[N_H(x)\right]^{-1}$.

Proof:
$$\begin{aligned} N_H(x^{-1}) &= x^{-1}\,\sigma_1(x^{-1})\cdots\sigma_k(x^{-1}) \\ &= x^{-1}\,[\sigma_1(x)]^{-1}\cdots[\sigma_k(x)]^{-1} \\ &= [x\,\sigma_1(x)\cdots\sigma_k(x)]^{-1} \\ &= [N_H(x)]^{-1}\ . \end{aligned}$$

The following lemma is known as the Fundamental Theorem of Galois Theory, and appears as Corollary 2 on page 92 of [1].

Lemma 2.4: If G is the group of E/F, then there is a one-to-one correspondence between the subgroups of G and the subfields of E which contain F; S is a subgroup of G if and only if there exists a subfield F' of E such that $F \subset F' \subset E$ and S is the group of E/F'.

Theorem 2.1: Let G be the group of E/F. If $a \in E$, then $N(a) = 1$ if and only if there exists a subgroup H of G such that $N_H(a) = 1$. Also, there exist $b \in E$ and $\sigma \in G$ such that $a = b^{I-\sigma}$ if and only if there exists a cyclic subgroup H of G, generated by σ, such that $N_H(a) = 1$.

Proof: If $N(a) = 1$, then G is a subgroup of G such that $N_G(a) = N(a) = 1$.

Suppose that there is a subgroup $H = \{I, \sigma_1, \ldots, \sigma_k\}$ of G such that $N_H(a) = 1$. Let $J_1, \ldots, J_m$ denote the left cosets of H in G; then $J_1, \ldots, J_m$ is a partition of G. For every i, $1 \leq i \leq m$, there is a $\tau_i \in G$ such that
$J_i = \{\tau_i, \tau_i\sigma_1, \ldots, \tau_i\sigma_k\}$.

Now,

$$1 = \tau_i(1) = \tau_i\left[N_H(a)\right] = \tau_i(a)\cdot\tau_i\sigma_1(a)\cdots\tau_i\sigma_k(a)\ , \text{ and}$$

$$N(a) = \prod_{i=1}^{m}\tau_i\left[N_H(a)\right] = 1.$$

Suppose that there exists $b \varepsilon E$ and $\sigma \varepsilon G$ such that $a = b^{I-\sigma}$. Let H be the cyclic subgroup of G generated by σ, then $\sigma \varepsilon H$, and by the preceding lemmas,

$$N_H(a) = N_H\left[b^{I-\sigma}\right] = N_H\left[b\sigma(b^{-1})\right] = N_H(b)\cdot\left[N_H(b)\right]^{-1} = 1.$$

Suppose that there exists a cyclic subgroup H of G, with generator σ, such that $N_H(a) = 1$. To H corresponds a subfield F' of E such that $F \subset F' \subset E$ and H is the group of E/F'. By Kummer's Theorem, $N_H(a) = 1$ implies that there exists $b \varepsilon E$ such that $a = b^{I-\sigma}$.

Although Theorem 2.1 characterizes the elements of E of norm 1, these characterizations may only be in terms of subgroups of G. It would be preferable to characterize the elements $a \varepsilon E$ of norm 1 in terms of elements of E so that an explicit relation satisfied by a could be obtained.

There appears to be a possibility that a characterization of the elements of norm 1 in terms of elements of E has been achieved. That is, if for each $a \varepsilon E$ of norm 1 there is a cyclic subgroup H of G, generated by σ, such that $N_H(a) = 1$, then all the elements of E of norm 1 would be of the form $b^{I-\sigma}$, for some $b \varepsilon E$ and $\sigma \varepsilon G$. The following example shows that this is not the case.

Let R be the rational numbers, and $R(\sqrt{2},\sqrt{3})$ be the field of rational numbers extended by $\sqrt{2}$ and $\sqrt{3}$, that is, the set of real numbers of the form

$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, a,b,c,d rational numbers. The group of $R(\sqrt{2},\sqrt{3})/R$ is $\{I,\sigma_1,\sigma_2,\sigma_3\}$ where the σ_i are given by:

	I	σ_1	σ_2	σ_3
$\sqrt{2} \rightarrow$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$\sqrt{3} \rightarrow$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$

The element $1 + \sqrt{2}$ of $R(\sqrt{2},\sqrt{3})$ is of norm 1, but for no cyclic subgroup H of G is $N_H(1 + \sqrt{2}) = 1$.

CHAPTER III

THE GROUP G OF E/F SOLVABLE

In this chapter the group G of E/F will be assumed to be solvable. The reason for the assumption of solvability will be fully understood following Lemma 3.1. With G solvable the norm N can be expressed in terms of N_1 and N_2 , norms with respect to cyclic groups H_1 and H_2, respectively. After Lemma 3.1, it will be seen that with G solvable, $N(x) = N_1[N_2(x)]$ for $x \varepsilon E$. If $a \varepsilon E$ is of norm 1, then $N_1[N_2(a)] = 1$, and by Theorem 2.1, $N_2(a) = b_1^{I-\sigma_1}$ for some $b_1 \varepsilon E$ and σ_1 a generator of H_1. The problem is then to "remove" N_2 and obtain an expression for a. Since $b_1^{I-\sigma_1}$ need not be 1, Theorem 2.1 does not apply. Following Theorem 3.1, it will be seen that $a^{k_2} = b_1^{I-\sigma_1} b_2^{I-\sigma_2}$, $b_i \varepsilon E$, where σ_i is a generator of H_i, and k_2 is the order of H_2.

<u>Definition 3.1</u>: A group G is solvable if and only if there exists a sequence of subgroups of G $G = G_1 \supset G_2 \supset \cdots \supset G_n \supset G_{n+1} = I$ such that G_{i+1} is normal in G_i, and G_i/G_{i+1} is cyclic of order h_i, $1 \leq i \leq n$.

A solvable group G is sometimes defined as above with the exception that G_i/G_{i+1} need only be commutative. Also, a solvable group G is sometimes defined such that the h_i are prime. As stated on page 15 of [2], if G is finite, then these definitions are equivalent. It then follows that Definition 3.1 is equivalent to the usual definitions of solvability. After Theorem 3.1, it will be seen that it is advantageous not to require that the h_i be prime.

If the group G of E/F is solvable with the sequence of subgroups $G = G_1 \supset G_2 \supset \cdots \supset G_n \supset G_{n+1} = I$, then there is a sequence of subfields of E,
$F = F_1 \subset F_2 \subset \cdots \subset F_n \subset F_{n+1} = E$, such that F_i is the subfield of E with the property that G_i is the group of E/F_i. Let Q_i denote the group of F_{i+1}/F_i; Q_i consists of the restrictions of the elements of G_i to F_{i+1}. Also, as proved on page 30 of [3], the group Q_i of F_{i+1}/F_i is isomorphic to G_i/G_{i+1}, and, hence, is cyclic.

The following result is obtained from a more general result appearing on page 66 of [3].

Let G be the group of E/F and G_1 a normal subgroup of G, then there is a subfield F_1 such that $F \subset F_1 \subset E$ and G_1 is the group of E/F_1. Also, the group Q_1 of F_1/F is isomorphic to G/G_1. Then, for $a \in E$,

$N(a) = N_{E/F}(a) = N_{F_1/F}\left[N_{E/F_1}(a)\right]$, where

$N_{E/F_1}(x) = \prod_{\sigma_i \in G_1} \sigma_i(x)$ for $x \in E$, and

$N_{F_1/F}(y) = \prod_{\tau_i \in Q_1} \tau_i(y)$ for $y \in F_1$.

The following lemma is a generalization of the above.

<u>Lemma 3.1</u>: If the group G of E/F is solvable with the sequence of subgroups $G = G_1 \subset G_2 \subset \cdots \subset G_n \subset G_{n+1} = I$, and F_i is the subfield of E corresponding to G_i, then for $a \in E$,

$$N(a) = N_{E/F}(a) = N_{F_2/F_1}\left[N_{F_3/F_2}\left\{\cdots N_{F_n/F_{n-1}}\left(N_{E/F_n}(a)\right)\right\}\right].$$

Notation: In the remaining work N_{F_{i+1}/F_i} will be denoted by N_i , $1 \leq i \leq n$. Also, where there is no ambiguity, the parentheses, braces, and brackets will be omitted.

Proof: Let $a \in E$; then $N_{E/F_{n-1}}(a) = N_{n-1}\left[N_n(a)\right]$. Suppose that for i, $1 \leq i \leq n-1$,

$N_{E/F_{n-i}}(a) = N_{n-i}\left[\cdots N_n(a)\right]$. Then,

$$\begin{aligned} N_{E/F_{n-i-1}}(a) &= N_{n-i-1}\left[N_{E/F_{n-i}}(a)\right] \\ &= N_{n-i-1}\left[N_{n-i}\left\{\cdots N_n(a)\right\}\right]. \end{aligned}$$

The conclusion follows by induction.

In the following two lemmas G, E, and F will again be arbitrary. Lemma 3.2 is from page 128 of [1].

Lemma 3.2: If G is the group of E/F and $a \in E$, then $N(a) \in F$.

In particular, with G solvable

$N_{E/F_i}(a) = N_i\left[N_{i+1}\cdots N_n(a)\right] \in F_i$.

The following lemma is obtained by applying a more general result from page 66 of [3] to the fact that $N(a) \in F$.

Lemma 3.3: If the group G of E/F is of order k and $a \in E$, then $N\left[N(a)\right] = \left[N(a)\right]^k$.

The following theorem gives a necessary condition for $a \in E$ to be of norm 1 for the case in which G is solvable.

Theorem 3.1: Let the group G of E/F be solvable with the sequence of subgroups

$G = G_1 \supset G_2 \supset \cdots \supset G_n \supset G_{n+1} = I$, G_{i+1} normal in G_i, $1 \leq i \leq n$. Let F_i be the subfield of E corresponding to G_i. If $a \in E$ is of norm 1, then

$$a^{g/h_1} = \prod_{i=1}^{n} b_i^{I-\sigma_i}\ ,\ \text{where}\ \prod_{i=1}^{m} b_i^{I-\sigma_i} \in F_{m+1},\ 1 \leq m \leq n,\ \sigma_i \text{ is a}$$

generator of Q_i, the group of F_{i+1}/F_i, h_i is the order of Q_i, and $g = h_1\ h_2 \cdots h_n$ is the order of G.

<u>Proof</u>: The proof will be an induction on n.

For the case in which $n = 1$, $g = h_1$, and the exponent of a is 1. Also, Q_1 is G so that σ_1 is a generator of G. Hence, the theorem reduces to Kummer's Theorem.

Suppose that for $n = k-1$, $1 \leq k-1$, $N_1 \cdots N_{k-1}(a) = 1$ implies that

$$a^{h_1 \cdots h_{k-1}/h_1} = \prod_{i=1}^{k-1} b_i^{I-\sigma_i}\ ,\ \text{where}\ \prod_{i=1}^{m} b_i^{I-\sigma_i} \in F_{m+1},\ 1 \leq m \leq k-1.$$

If $N_1 \cdots N_k(a) = 1$, then $N_1 \cdots N_{k-1}\left[N_k(a)\right] = 1$, and by the induction hypothesis

$$N_k(a)^{\ h_1 \cdots h_{k-1}/h_1} = \prod_{i=1}^{k-1} b_i^{I-\sigma_i}\ ,\ \text{where}\ \prod_{i=1}^{m} b_i^{I-\sigma_i} \in F_{m+1},$$

$1 \leq m \leq k-1$. Let $z \in F_{k+1}$ be such that

$$a^{h_1 \cdots h_{k-1} h_k/h_1} = z \prod_{i=1}^{k-1} b_i^{I-\sigma_i}\ .\ \text{Then,}$$

$$\begin{aligned} N_k(a)^{\ h_1 \cdots h_{k-1} h_k/h_1} &= N_k(z)\ N_k\left[\prod_{i=1}^{k-1} b_i^{I-\sigma_i}\right] \\ &= N_k(z)\ N_k\left[N_k(a)^{\ h_1 \cdots h_{k-1}/h_1}\right] \\ &= N_k(z)\ \ N_k(a)^{\ h_1 \cdots h_{k-1} h_k/h_1}\ ,\ \text{by} \end{aligned}$$

Lemmas 3.2 and 3.3. This implies that $N_k(z) = 1$, and since the group Q_k of F_{k+1}/F_k is cyclic, there is a $b_k \varepsilon F_{k+1}$ such that $z = b_k^{I-\sigma_k}$, σ_k a generator of Q_k. Hence,

$a^{h_1 \cdots h_{k-1} h_k / h_1} = \prod_{i=1}^{k} b_i^{I-\sigma_i}$. $\prod_{i=1}^{k-1} b_i^{I-\sigma_i} \varepsilon F_k \subset F_{k+1}$, and $z = b_k^{I-\sigma_k} \varepsilon F_{k+1}$, so that $\prod_{i=1}^{k} b_i^{I-\sigma_i} \varepsilon F_{k+1}$. The conclusion follows by induction.

It should be noted that if $n > 1$, then the exponent of a is $h_2 \cdots h_n$. Since h_1 does not appear, it is advantageous to have h_1 as large as possible. Hence, the requirement that the h_i be prime was deleted.

If G is cyclic, then G has a sequence of subgroups $G = G_1 \supset G_2 = I$, with G_2 normal in G_1. Then, $n = 1$, and Theorem 3.1 reduces to Kummer's Theorem.

Corollary 3.1: If m is the least positive integer for which $N(a) = 1$ implies that $a^m = \prod_{i=1}^{n} b_i^{I-\sigma_i}$, then m divides g/h_1.

Proof: Let $g/h_1 = h$, and let r be the integer such that $h = sm + r$, $0 \leqslant r < m$. If $N(a) = 1$, then

$a^h = \prod_{i=1}^{n} b_i^{I-\sigma_i}$ and $a^m = \prod_{i=1}^{n} c_i^{I-\sigma_i}$. Also,

$a^{-sm} = \prod_{i=1}^{n} (c_i^{-s})^{I-\sigma_i}$. Hence, $a^r = a^{h-sm} = \prod_{i=1}^{n} (b_i c_i^{-s})^{I-\sigma_i}$.

Since $r < m$, and r satisfies the same condition as m, then $r = 0$. The conclusion follows.

The following corollary is a partial converse to

Theorem 3.1.

Corollary 3.2: If $a \in E$ is such that $a^{g/h_1} = \prod_{i=1}^{n} b_i^{I-\sigma_i}$, then $[N(a)]^{g/h_1} = 1$ and $N[N(a)] = 1$.

Proof: Q_i consists of the distinct restrictions to F_{i+1} of the elements of G_i. Since $b_i \in F_{i+1}$, $\sigma_i(b_i)$ may be considered as an element of G applied to an element of E. The fact that $N(b_i^{I-\sigma_i}) = 1$ then follows by applying Lemmas 2.1, 2.2, and 2.3 with $H = G$. Then,

$$[N(a)]^{g/h_1} = N(a^{g/h_1}) = N\left[\prod_{i=1}^{n} b_i^{I-\sigma_i}\right] = \prod_{i=1}^{n} N(b_i^{I-\sigma_i}) = 1.$$

Also, if $z \in F$, then $N(z) = z^g$. Since $N(a) \in F$, $N[N(a)] = [N(a)]^g = [N(a)^{g/h_1}]^{h_1} = 1^{h_1} = 1.$

The following indicates the need for restrictions on the h_i in order to guarantee the converse of Theorem 3.1.

Let the group G of E/F be such that G_2 is a normal cyclic subgroup of G of order h_2 for which G/G_2 is cyclic of order h_1. Then, G is solvable with the sequence of subgroups $G = G_1 \supset G_2 \supset G_3 = I$. Corresponding to this sequence of groups is the sequence of fields $F = F_1 \subset F_2 \subset F_3 = E$. If $a \in E$ is of norm 1, then, by Theorem 3.1,
$a^{h_2} = b_1^{I-\sigma_1} b_2^{I-\sigma_2}$, where $b_1^{I-\sigma_1} \in F_2$, σ_1 a generator of Q_1, the group of F_{i+1}/F_i. Suppose that $a^{h_2} = b_1^{I-\sigma_1} b_2^{I-\sigma_2}$, $b_1^{I-\sigma_1} \in F_2$, then
$N_2(a)^{h_2} = N_2(a^{h_2}) = N_2(b_1^{I-\sigma_1}) N_2(b_2^{I-\sigma_2}) = (b_1^{I-\sigma_1})^{h_2}$. Hence, $N_2(a) = c\, b_1^{I-\sigma_1}$, where $c \in F_2$ and $c^{h_2} = 1$. Then,
$N(a) = N_1[N_2(a)] = N_1(b_1^{I-\sigma_1}) N_1(c) = N_1(c)$. If $c \in F$, then $N_1(c) = c^{h_1}$. In this case, $N(a) = c^{h_1}$. If h_2 does not

divide h_1, then c^{h_1} need not be 1. For this reason, restrictions will be placed on the h_i.

Since commutative groups are solvable, page 14 of [2], Theorem 3.1 will apply to the case in which G is commutative. Commutative groups satisfy more properties than solvability. With some of these properties, soon to be enumerated, it will be shown that not only is the converse of Theorem 3.1 true, but also, the exponent of a in Theorem 3.1 can be reduced to a lowest value.

The following lemmas are from [2], pages 12 and 13. In these lemmas and in all the following work, the notion of a direct product is that which some authors refer to as an internal direct product. Here, products of elements of the group are involved. In what is termed an external direct product, one deals with m-tuples of elements of the group.

Lemma 3.4: Every commutative group G is the direct product $G_1 \times G_2 \times \cdots \times G_m$ of subgroups G_i, $1 \leq i \leq m$, such that each G_i is an indecomposable cyclic group of prime power order $p_i^{a_i}$, $a_i > 0$.

The collection of orders $\{p_1^{a_1}, p_2^{a_2}, \ldots, p_m^{a_m}\}$ constitute the elementary divisors of G. They are uniquely determined by G, i.e. independent of the choice or arrangement of the G_i. The prime p_i need not be distinct as seen in the following lemma.

Lemma 3.5: A direct product $H_1 \times \cdots \times H_r$ of cyclic groups H_i whose orders h_i are powers of distinct primes is cyclic. Conversely, any cyclic group is so expressible.

As previously mentioned, the reduction of the exponent of a depends on having the highest possible factor appear with N_1. The following lemma guarantees a decomposition of a commutative group G in such a way that the highest possible factor will appear with N_1. Also, with this decomposition the converse of Theorem 3.1 will be shown to be true. This lemma appears on page 12 of [2] as Theorem 4.5. It should be noted that the arrangement of the H_i in Lemma 3.6 is the reverse of the arrangement of the H_i as they appear in Theorem 4.5.

Lemma 3.6: Every commutative group G is the direct product $H_1 \times \cdots \times H_n$ of cyclic subgroups H_i whose orders k_i have the property that k_{i+1} divides k_i, for all i, $1 \leq i \leq n-1$.

The k_i are sometimes called the invariants of G.

The following is an outline of the proof of Theorem 4.5 in [2]. It is reproduced here in order to illustrate the fact that there is no factorization of G in terms of cyclic subgroups, $J_1 \times \cdots \times J_s$, such that the order of J_1 exceeds k_1.

Start with the decomposition as in Lemma 3.4. For each p_i dividing the order of G, let $p_i^{a_i}$ be the highest power of p_i which occurs among the elementary divisors of G. Then, for each i, some one of the groups G has order $p_i^{a_i}$, say, the group G_{m_i}. Set $H_1 = \prod_i G_{m_i}$. By Lemma 3.5,

H_1 is cyclic of order $\prod_i p_{m_i}^{a_{m_i}}$. Apply the same construction to the remaining G_{m_i}, obtaining a cyclic factor H_2 of order k_2, with $k_2 | k_1$. Continuing in this way, the decomposition of Lemma 3.6 is obtained. It then follows that k_1 is the least common multiple of the elementary divisors. Also, k_2 is the least common multiple of the remaining elementary divisors after the highest power of each prime is removed, and so on. Hence, H_1 has the highest possible order.

Let G be a commutative group and $H_1 \times \cdots \times H_n$ the decomposition guaranteed by Lemma 3.6. This decomposition gives rise to the following sequence of subgroups,

$G = H_1 \times \cdots \times H_n \supset H_2 \times \cdots \times H_n \supset H_3 \times \cdots \times H_n \supset \cdots \supset H_n \supset H_{n+1} = I$

such that $H_{i+1} \times \cdots \times H_n$ is normal in $H_i \times \cdots \times H_n$ and $(H_i \times \cdots \times H_n)/(H_{i+1} \times \cdots \times H_n)$ is cyclic of order k_i, for all i, $1 \leq i \leq n$.

Corresponding to this sequence of subgroups of G is the following sequence of subfields of E,

$F = F_1 \subset F_2 \subset \cdots \subset F_n \subset F_{n+1} = E$, where the group Q_i of F_{i+1} / F_i is isomorphic to $(H_i \times \cdots \times H_n)/(H_{i+1} \times \cdots \times H_n)$.

From the preceding work, it is apparent that Theorem 3.1 will apply.

In Theorem 3.1 factors $b_i^{I-\sigma_i}$ appear, where σ_i is a generator of Q_i. The following lemma shows that in using the decomposition of a commutative group, the σ_i appearing in Theorem 3.1 are specific elements in G, namely, generators of the H_i.

As a matter of fact, there are non-commutative groups having essentially this same property. These groups will be illustrated in the following definition and the example preceding Lemma 3.7.

<u>Definition 3.2</u>: A solvable group G is said to be pseudo-decomposable if and only if there are cyclic subgroups H_i, $1 \leq i \leq n$, of G such that every $\sigma \in G$ is uniquely expressible as a product $\sigma_1 \cdots \sigma_n$, with $\sigma_i \in H_i$. This will be denoted by $G = H_1 H_2 \cdots H_n$. Further, for all i, $1 \leq i \leq n$, $H_{i+1} \cdots H_n$ is a normal subgroup of $H_i \cdots H_n$, where $H_{n+1} = I$.

Hence, a pseudo-decomposable group G gives rise to the following sequence of subgroups,

(1) $G = H_1 \cdots H_n \supset H_2 \cdots H_n \supset \cdots \supset H_n \supset H_{n+1} = I$, where each subgroup is normal in the preceding subgroup. Corresponding to this sequence of subgroups is the sequence of subfields of E,

(2) $F = F_1 \subset \cdots \subset F_n \subset F_{n+1} = E$.

Non-commutative pseudo-decomposable groups exist; the following is an example.

Let $H = \{I, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$, $H_1 = \{I, \tau\}$, and $H_2 = \{I, \sigma, \sigma^2, \sigma^3\}$. Hence, $H = H_1 H_2$. The mixed products are given by the rules $\tau\sigma = \sigma^3\tau$, $\tau\sigma^2 = \sigma^2\tau$, and $\tau\sigma^3 = \sigma\tau$. These rules show that H is not commutative. But, H_2 is a normal subgroup of H, and so H gives rise to the sequence of subgroups $H \supset H_2 \supset I$, each subgroup normal in the preceding subgroup.

Note: There is no loss in generality in assuming that $H_{j+1}\cdots H_n$ is a normal subgroup of $H_j\cdots H_n$, as opposed to the assumption that $H_j\cdots H_{s-1}H_{s+1}\cdots H_n$, $s \neq j$, is a normal subgroup of $H_j\cdots H_n$.

If $H_j\cdots H_{s-1}H_{s+1}\cdots H_n$ is a normal subgroup of $H_j\cdots H_n$, then $H_s\ H_j\cdots H_{s-1}H_{s+1}\cdots H_n \subset H_j\cdots H_n$. Equality will be proved if it can be shown that there are as many elements in $H_sH_j\cdots H_{s-1}H_{s+1}\cdots H_n$ as in $H_j\cdots H_n$. This is equivalent to the showing that the representations of the elements of $H_sH_j\cdots H_{s-1}H_{s+1}\cdots H_n$ are unique. Suppose that

$\sigma_s'\sigma_j'\cdots\sigma_{s-1}'\ \sigma_{s+1}'\cdots\sigma_n' = \sigma_s\ \sigma_j\cdots\sigma_{s-1}\ \sigma_{s+1}\cdots\sigma_n$, where σ_i , $\sigma_i'\in H_i$. Then,

$$\sigma_s^{-1}\sigma_s' = (\sigma_j\cdots\sigma_{s-1}\sigma_{s+1}\cdots\sigma_n)\ (\sigma_j'\cdots\sigma_{s-1}'\sigma_{s+1}'\cdots\sigma_n')^{-1}.$$

Since $H_j\cdots H_{s-1}H_{s+1}\cdots H_n$ is a subgroup, the right side of the equality is in $H_j\cdots H_{s-1}H_{s+1}\cdots H_n$. But, $\sigma_s^{-1}\cdot\sigma_s'\in H_s$, so that this contradicts the uniqueness of the representations in G, unless $\sigma_s^{-1}\cdot\sigma_s' = I$. In this case, $\sigma_s' = \sigma_s$, and

$\sigma_j'\cdots\sigma_{s-1}'\ \sigma_{s+1}'\cdots\sigma_n' = \sigma_j\cdots\sigma_{s-1}\ \sigma_{s+1}\cdots\sigma_n$. Hence,

$\sigma_j' = \sigma_j$,..., $\sigma_{s-1}' = \sigma_{s-1}$, $\sigma_{s+1}' = \sigma_{s+1}$,..., and $\sigma_n' = \sigma_n$.

The conclusion follows by rearranging and renumbering the H_i.

Lemma 3.7: If G is pseudo-decomposable, giving rise to the sequences (1) and (2), then the group Q_i of F_{i+1}/F_i is H_i, $1 \leq i \leq n$.

Proof: It is known that Q_i, the group of F_{i+1}/F_i, is the restriction of $G_i = H_i\cdots H_n$ to F_{i+1} . The elements of F_{i+1} are invariant under the elements of $G_{i+1} = H_{i+1}\cdots H_n$.

Let $x\in F_{i+1}$ and $\sigma\in H_i\cdots H_n$; then $\sigma = \tau_i\ \tau_{i+1}\cdots\tau_n$,

$\tau_j \varepsilon H_j$, $i \leq j \leq n$, and

$\sigma(x) = \tau_i \tau_{i+1} \cdots \tau_n(x) = \tau_i[\tau_{i+1} \cdots \tau_n(x)] = \tau_i(x)$.

Hence, to each $\sigma \varepsilon Q_i$, there corresponds a $\tau_i \varepsilon H_i$. Conversely, to each $\tau_i \varepsilon H_i$, there corresponds a $\sigma \varepsilon Q_i$. Suppose for $\tau_i', \tau_i \varepsilon H_i$, $\tau_i'(x) = \tau_i(x)$, for all $x \varepsilon F_{i+1}$. Then, $\tau_i^{-1} \tau_i'(x) = x$, for all $x \varepsilon F_{i+1}$, and so, $\tau_i^{-1}\tau_i' \varepsilon G_{i+1} = H_{i+1} \cdots H_n$. But, $\tau_i^{-1} \tau_i' \varepsilon H_i$; hence, $\tau_i^{-1} \tau_i' = I$, and $\tau_i' = \tau_i$. Thus, the distinct restrictions of $G_i = H_i \cdots H_n$ to F_{i+1} are precisely the elements of H_i.

The following Lemma 3.8 will not be used, although a portion of the proof will be used in the proof of Lemma 3.9. Lemma 3.8 could well be called a theorem since it of interest in its own right. In this paper it only serves as a step toward the proof of a partial converse of Theorem 3.1; hence, it will be called a lemma.

Lemma 3.8: If t, d, and m are positive integers such that $t^d \equiv 1 (\mathrm{mod}\ m)$ and $d|m$, then $d|t^{d-1} + t^{d-2} + \cdots + t + 1$.

Proof: If $t^d \equiv 1 (\mathrm{mod}\ m)$ and $d|m$, then $t^d \equiv 1 (\mathrm{mod}\ d)$. Hence, $d|(t-1)(t^{d-1} + t^{d-2} + \cdots + t + 1)$. Let $d = p_1^{x_1} \cdots p_v^{x_v}$, where the p_i are distinct primes. If $(p_i, t-1) = 1$, then $p_i^{x_i}|t^{d-1} + t^{d-2} + \cdots + t + 1$, since $p_i^{x_i}|(t-1)(t^{d-1} + \cdots + t + 1)$.

Suppose that $(p_i, t-1) \neq 1$; then $p_i|(t-1)$. Hence, $t = 1 + sp_i$, for some integer s. Then,

$$\begin{aligned}
1 &= 1 \\
t &= 1 + (sp_i) \\
t^2 &= 1 + 2(sp_i) + (sp_i)^2 \\
&\vdots \\
t^{d-1} &= 1 + (d-1)(sp_i) + \cdots + (sp_i)^{d-1}.
\end{aligned}$$

The coefficient of $(sp_i)^{n-1}$ in $t^{d-1} + \cdots + t + 1$ is $\sum_{k=n-1}^{d-1} \binom{k}{n-1}$.

Using the identity $\binom{b+1}{a} = \binom{b}{a} + \binom{b}{a-1}$, rewritten as $\binom{b}{a-1} = \binom{b+1}{a} - \binom{b}{a}$; then,

$$\begin{aligned}
\sum_{k=n-1}^{d-1} \binom{k}{n-1} &= \sum_{k=n-1}^{d-1} \binom{k+1}{n} - \sum_{k=n-1}^{d-1} \binom{k}{n} \\
&= \binom{d}{n} + \sum_{k=n-1}^{d-2} \binom{k+1}{n} - \sum_{k=n}^{d-1} \binom{k}{n} - \binom{n-1}{n} \\
&= \binom{d}{n} + \sum_{k=n}^{d-1} \binom{k}{n} - \sum_{k=n}^{d-1} \binom{k}{n} - 0 \\
&= \binom{d}{n}.
\end{aligned}$$

Hence, the n-th term of $t^{d-1} + \cdots + t + 1$ expressed as a polynomial in (sp_i) is $\binom{d}{n}(sp_i)^{n-1}$. Let the integer $r = \binom{d-1}{n-1}$. Then, then n-th term may be written as $(dr)/n \; (sp_i)^{n-1}$, with $(dr)/n$ integral.

If $(p_i, n) = 1$, then $p_i^{x_i} \mid (dr)/n \; (sp_i)^{n-1}$. If $(p_i, n) \neq 1$, then $n = p_i^m g$, where $p_i \nmid g$.

To show that $m \leq n-1$, suppose to the contrary that $m > n-1$. Then, $m \geq n$. Since $p_i > 1$; $p_i^m > m$. Hence, $p_i^m > m \geq n$, a contradiction. Thus, $m \leq n-1$, and $(dr)/n\ (sp_i)^{n-1} = (dr)/g\ s^{n-1}p_i^{n-m-1}$, where p_i^{n-m-1} is integral. Since $p_i \nmid g$, $p_i^{x_i} \mid (dr)/g\ s^{n-1}p_i^{n-m-1}$. Hence, $p_i^{x_i}$, $1 \leq i \leq m$, divides each term of $t^{d-1} + \cdots + t + 1$ expressed as a polynomial in (sp_i). The conclusion follows.

The following lemma will be the key step in the proof of the converse of Theorem 3.1 for the case in which G is commutative. This lemma will apply to certain other cases with G solvable but not commutative. According to Theorem 2.1, if H is a subgroup of G and $N_H(a) = 1$, then $N(a) = 1$. If H is a Sylow subgroup of G, then H is of prime order p^s. It is known that if H is a group of prime power order p^s, then H is solvable with a sequence of subgroups $H = H_1 \supset H_2 \supset \cdots \supset H_s \supset H_{s+1} = I$ such that H_i/H_{i+1} is cyclic of prime order p, $1 \leq i \leq s$. Hence, if $a \in E$ is of norm 1 such that $N_H(a) = 1$ where H is a Sylow subgroup, then the following lemma will apply. It will also apply to groups G of prime power order.

Lemma 3.9: Let the group G of E/F be solvable with the sequence of subgroups $G = G_1 \supset \cdots \supset G_n \supset G_{n+1} = I$, each subgroup normal in the preceding subgroup. Let F_i denote the subfield corresponding to G_i. Let Q_i, the group of F_{i+1}/F_i, be of order h_i, $1 \leq i \leq n$, such that $h_{i+1} \mid h_i$. If c is a h_{i+1}-th root of 1 in F_{i+1}, then $N_i(c) = 1$.

Proof: If $c = 1$, then $N_i(c) = 1$. Suppose that $c \neq 1$. Let σ_i be a generator of Q_i, and suppose that c is a primitive m-th root of 1. Then, $m | h_{i+1}$. Let $\sigma_i(c) = x$; then, $x^m = \sigma_i(c^m) = \sigma_i(1) = 1$. Hence, x is an m-th root of 1, and $\sigma_i(c) = c^t$. Suppose that $(t,m) = s \neq 1$; then, there are positive integers u and v such that $um = tv$, with $v < m$. Then, $\sigma_i(c^v) = c^{tv} = c^{mu} = 1$, and so $c^v = 1$. This contradicts the assumption that c is a primitive m-th root of 1. Hence, $(t,m) = 1$. Furthermore,

$$\sigma_i^2(c) = c^{t^2}, \ldots, \sigma_i^j(c) = c^{t^j}, \ldots, \text{ and } \sigma_i^{h_i}(c) = I(c) = c.$$

Let d be the least positive integer for which

$c^{t^d} = c$; then $t^d \equiv 1 (\text{mod } m)$.

If $t = 1$, then $\sigma_i(c) = c$ and $c \in F_i$. Since $m | h_{i+1}$ and $h_{i+1} | h_i$, $N_i(c) = c^{h_i} = 1$.

Suppose that $t \neq 1$; then t belongs to the exponent d modulo m. If $t^k \equiv 1 (\text{mod } m)$, then $d | k$. Hence, $d | h_i$. Let $h_i = p_1^{a_1} \ldots p_s^{a_s}$, and $h_{i+1} = p_1^{b_1} \cdots p_s^{b_s}$, where the p_j are distinct primes; then $a_i \geq b_i$, $1 \leq i \leq s$. Since $d | h_i$, $d = p_1^{x_1} \ldots p_s^{x_s}$, $0 \leq x_i \leq a_i$, $1 \leq i \leq s$. Since $m | h_{i+1}$, $m = p_1^{y_1} \ldots p_s^{y_s}$, $0 \leq y_i \leq b_i$, $1 \leq i \leq s$. Now,

$$\begin{aligned} N_i(c) &= \left[c \cdot c^t \cdot c^{t^2} \cdots c^{t^{d-1}}\right]^{h_i/d} \\ &= \left[c^{1+t+t^2+\cdots+t^{d-1}}\right]^{\prod_{i=1}^{s} p^{a_i - x_i}} \end{aligned}$$

Since $t^d - 1 \equiv 0 (\text{mod } m)$, $p_j^{y_j} | (t-1)(t^{d-1} + \cdots + t + 1)$, for all j, $1 \leq j \leq s$.

The conclusion, $N_i(c) = 1$, will follow if it can be shown that

$p_j^{a_j} \mid (t^{d-1}+\cdots+t+1)\prod_{i=1}^{s} p_i^{a_i-x_i}$, for all j, $1 \leq j \leq s$.

If $(p_j, t-1) = 1$, then $p_j^{x_j} \mid (t^{d-1}+\cdots+t+1)$. Suppose then that $p_j \mid (t-1)$. From the proof of Lemma 3.8, $p_j^{x_j} \mid (t^{d-1}+\cdots+t+1)$. Hence, for all j, $1 \leq j \leq s$, $p_j^{a_j} \mid (t^{d-1}+\cdots+t+1)\prod_{i=1}^{s} p_i^{a_i-x_i}$. Since $a_j \geq y_j$, the conclusion follows.

The following theorem is a partial converse of Theorem 3.1.

Theorem 3.2: Let the group G of E/F be solvable with the sequence of subgroups $G = G_1 \supset \cdots \supset G_n \supset G_{n+1} = I$, each subgroup normal in the preceding subgroup. Let F_i be the subfield of E corresponding to G_i, and let Q_i , the group of F_{i+1}/F_i, be of order h_i such that $h_{i+1} \mid h_i$.
If $a^{g/h_1} = \prod_{i=1}^{n} b_i^{I-\sigma_i}$, where $\prod_{i=1}^{m} b_i^{I-\sigma_i} \in F_{m+1}$, $1 \leq m \leq n$, σ_i is a generator of Q_i, and g is the order of G, then $N(a) = 1$.

Proof: The proof will be an induction on n.

For the case in which $n = 1$, $g = h_1$, and the exponent of a is 1. Also, Q_1 is G so that σ_1 is a generator of G. Hence, the theorem reduces to Kummer's Theorem.
Suppose that for $n = k-1$, $1 \leq k-1$,
$a^{h_1 \cdots h_{k-1}/h_1} = \prod_{i=1}^{k-1} b_i^{I-\sigma_i}$, where $\prod_{i=1}^{m} b_i^{I-\sigma_i} \in F_{m+1}$, $1 \leq m \leq k-1$,
implies that $N_1 \cdots N_{k+1}(a) = 1$.

Let $a^{h_1 \cdots h_{k-1} h_k/h_1} = \prod_{i=1}^{k} b_i^{I-\sigma_i}$, where $\prod_{i=1}^{m} b_i^{I-\sigma_i} \in F_{m+1}$, $1 \leq m \leq k$. Then,

$$N_k(a)^{h_1 \cdots h_{k-1} h_k/h_1} = N_k\left(\prod_{i=1}^{k} b_i^{I-\sigma_i}\right) = \left(\prod_{i=1}^{k-1} b_i^{I-\sigma_i}\right)^{h_k}.$$

Thus, $N_k(a)^{h_1 \cdots h_{k-1}/h_1} = \left(\prod_{i=1}^{k-1} b_i^{I-\sigma_i}\right)c$, where c is a k-th root of 1 in F_k. By Lemma 3.9, $N_{k-1}(c) = 1$; hence, $c = d_{k-1}^{I-\sigma_{k-1}}$ for some $d_{k-1} \varepsilon F_k$. Then, $N_k(a)^{h_1 \cdots h_{k-1}/h_1} = \prod_{i=1}^{k-1} d_i'^{I-\sigma_i}$, where $\prod_{i=1}^{m} d_i'^{I-\sigma_i} \varepsilon F_{m+1}$, $1 \leq m \leq k-1$. By the induction hypothesis, $N_1 \cdots N_{k-1} N_k(a) = 1$. The conclusion follows by induction.

The following is an example of a non-commutative solvable group for which Theorem 3.2 applies.

Let G be the quaternion group; then there are fields E and F such that G is the group of E/F. G is generated by σ and τ, which are subject to the relations $\sigma^4 = I$, $\sigma^2 = \tau^2$, and $\tau\sigma = \sigma^3\tau$. Let $G_2 = \{I, \sigma^2\}$. Then, G gives rise to the sequence of subgroups $G = G_1 \supset G_2 \supset G_3 = I$, each subgroup normal in the preceding subgroup. Let F_i be the subfield of E corresponding to G_i. Q_1, the group of F_2/F_1, is of order 4. Q_2, the group of F_3/F_2, is of order 2. If $a \varepsilon E$ is of norm 1, then Theorem 3.1 guarantees that $a^2 = b_1^{I-\sigma_1} b_2^{I-\sigma_2}$, $b_1^{I-\sigma_1} \varepsilon F_2$, and σ_i a generator of Q_i. Since $h_2 | h_1$, Theorem 3.2 guarantees that every $a \varepsilon E$ satisfying the above form is of norm 1.

With G commutative and $a \varepsilon E$ of norm 1, a case in which the exponent of a is 1 may arise. The following corollary examines this case and shows precisely when it will occur.

<u>Corollary 3.3</u>: If G is commutative, then the exponent of a guaranteed by Theorem 3.1 is equal to 1 if and

only if G is cyclic.

Proof: The exponent of a guaranteed by Theorem 3.1 is g/h_1. This exponent is equal to 1 if and only if $g = h_1$. This is the case if and only if $G = H_1$. Since H_1 is cyclic, the conclusion follows.

The following question arises. For the case in which G is commutative but not cyclic, is $a = \prod_{i=1}^{n} c_i^{I-\sigma_i}$? The following example shows that in general this is not the case.

In the example on page 6 of Chapter II, it was mentioned that $N(1 + \sqrt{2}) = 1$. Since $G = \{I,\sigma_1\} \times \{I,\sigma_2\}$, Theorem 3.1 implies that $(1 + \sqrt{2})^2 = b_1^{I-\sigma_1} b_2^{I-\sigma_2}$. It can be shown that $(1 + \sqrt{2}) \neq c_1^{I-\sigma_1} c_2^{I-\sigma_2}$, for all nonzero $c_1, c_2 \varepsilon R(\sqrt{2},\sqrt{3})$. This can be shown by assuming to the contrary that for some nonzero $c_1, c_2 \varepsilon R(\sqrt{2},\sqrt{3})$, $(1 + \sqrt{2}) = c_1^{I-\sigma_1} c_2^{I-\sigma_2}$. Let N_1 denote the norm with respect to the subgroup $\{I,\sigma_1\}$. Then, $-1 = N_1(1 + \sqrt{2}) = N_1(c_2^{I-\sigma_2})$. Let $c_2 = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, with $a,b,c,d \varepsilon R$. Compute $N_1(c_2^{I-\sigma_2})$ in terms of a, b, c, and d. By equating this to -1, the equation $a^2 + 3c^2 - 2b^2 - 6d^2 = 0$ is obtained. It can be shown that this equation has only the solution $a = b = c = d = 0$. But, this is a contradiction since $c_2^{I-\sigma_2}$ is not defined.

CHAPTER IV

THE GROUP G OF E/F FACTORABLE

In Chapter III with G solvable it was shown that if $N(a) = 1$, then some power of a is expressible as a product of elements of E. The purpose of this chapter is to obtain a possible reduction in this exponent. This exponent might be reducible if G has another sequence of subgroups $G = G_1' \supset \cdots \supset G_n' \supset G_{n+1}' = I$, each subgroup normal in the preceding subgroup with G_i'/G_{i+1}' cyclic of order g_i, $1 \leqq i \leqq n$. If $g_1 > h_1$, then by applying Theorem 3.1 to G using this sequence of subgroups the exponent of a is reduced. But, one could as well assume that the sequence of subgroups of G used in Theorem 3.1 is such that the order h_1 of G_1/G_2 is the largest possible. For this reason, one is lead to examine the case in which G is pseudo-decomposable. As seen in Theorem 3.1, the order of first subgroup does not appear in the exponent of a in this case. But, one could as well assume that the pseudo-decomposition of G is such that the order of the first subgroup is the largest possible. This is the case with G commutative; as mentioned, the decomposition of G guaranteed by Lemma 3.5 is such that the exponent of a in Theorem 3.1 can not be reduced by any other decomposition of G. Hence, one is lead to consider a fixed pseudo-decomposition of G and to attempt to reduce the exponent of a by working only with this pseudo-decomposition.

If $G = H_1 \cdots H_n$ and for some permutation P of n symbols, $G = H_{P(1)} \cdots H_{P(n)}$, then possibly a reduction of the exponent of a may be obtained by applying Theorem 3.1 to $H_{P(1)} \cdots H_{P(n)}$. A problem may arise. The pseudo-decomposition $H_1 \cdots H_n$ gives rise to the sequence of subgroups $G = H_1 \cdots H_n \supset H_2 \cdots H_n \supset \cdots \supset H_n \supset H_{n+1} = I$. It may be that even though $G = H_{P(1)} \cdots H_{P(n)}$, $H_{P(2)} \cdots H_{P(n)}$ is not a subgroup of G. If this is the case, then Theorem 3.1 will not apply. For this reason Theorem 4.1 will be proved without the use of solvability. This first requires that the restriction in Definition 3.2 pertaining to the sequence of subgroups be removed.

Definition 4.1: A group G is factorable if and only if there are cyclic subgroups H_i, $1 \leq i \leq n$, of G such that every $\sigma \in G$ is uniquely expressible as a product $\sigma_1 \cdots \sigma_n$, $\sigma_i \in H_i$. This will be denoted by $G = H_1 \cdots H_n$.

Lemma 4.1: Let G be the group of E/F. If $G = H_1 \cdots H_n$, then

$$N(x) = N_{H_1}\left[N_{H_2}\left\{\cdots N_{H_{n-1}}\left(N_{H_n}(x)\right)\right\}\right], \text{ for every } x \in E.$$

Notation: In all the following work, N_{H_i} will be denoted by N_i, $1 \leq i \leq n$, and, where there is no ambiguity, the parentheses, braces, and brackets will be omitted.

Proof: Let $x \in E$; then

$$N(x) = \prod_{\sigma \in G} \sigma(x) = \prod_{\substack{\sigma_i \in H_i \\ 1 \leq i \leq n}} \sigma_1 \cdots \sigma_n(x).$$

But, this is equal to
$\prod_{\tau_1 \in H_1} \tau_1 \left[\prod_{\tau_2 \in H_2} \tau_2 \left\{ \cdots \left(\prod_{\tau_n \in H_n} \tau_n(x) \right) \right\} \right]$. The conclusion follows.

In all the following work F_i will denote the subfield of E corresponding to H_i.

<u>Lemma 4.2</u>: If $a \in E$, then $N_i \cdots N_n(a) \in F_i$.

<u>Proof</u>: $N_{i+1} \cdots N_n(a) \in E$ and H_i is the group of E/F_i; hence, by Lemma 3.2, $N_i \cdots N_n(a) \in F_i$.

<u>Theorem 4.1</u>: Let G be the group of E/F and $a \in E$ have norm 1. If $G = H_1 \cdots H_n$, then $a^{g/h_1} = \prod_{i=1}^{n} b_i^{I-\sigma_i}$, where $\prod_{i=1}^{m} b_i^{I-\sigma_i} \in F_{m+1}$, $1 \leq m \leq n$, $F_{n+1} = E$, σ_i is a generator of H_i, h_i is the order of H_i, and $g = h_1 \cdots h_n$ is the order of G.

<u>Proof</u>: The proof of Theorem 3.2, page 10, makes use of Kummer's Theorem. This proof will apply to the proof of Theorem 4.1 if Kummer's Theorem is replaced by Theorem 2.1, page 5.

The following example illustrates the use of Theorem 4.1.

Let G be the dihedral group. G is generated by σ and τ, subject to the relations $\sigma^4 = \tau^2 = I$ and $\tau\sigma = \sigma^3\tau$. Now, let $H_1 = \{I, \sigma^2\}$, $H_2 = \{I, \tau\}$, and $H_3 = \{I, \sigma\tau\}$. $G = H_{P(1)}H_{P(2)}H_{P(3)}$ for every permutation P of three symbols, but neither H_2H_3 nor H_3H_2 is a subgroup of G. Hence, neither $H_1H_2H_3$ nor $H_1H_3H_2$ is a pseudo-decomposition of G. Therefore, Theorem 3.1 does not apply. Theorem 4.1 applies in both of the above cases.

While it might appear that Theorem 3.1 is a special case of Theorem 4.1, such is not the case. The quaternion group is an example of a group to which Theorem 3.1 applies but Theorem 4.1 does not apply.

A necessary condition for elements to have norm 1 has been obtained for the case in which G is factorable. It is worthwhile to digress from the course of this chapter in the interest of obtaining a partial converse of Theorem 4.1.

<u>Lemma 4.3</u>: Let $G = H_1 \cdots H_n$, where H_i is of order h_i such that $h_{i+1} | h_i$, $1 \leq i \leq n-1$. If c is an h_{i+1}-th root of 1 in E, then $N_i(c) = 1$.

<u>Proof</u>: The proof of Lemma 3.9 on page 21 will apply.

The following is a partial converse of Theorem 4.1.

<u>Theorem 4.2</u>: Let $G = H_1 \cdots H_n$ be the group of E/F, where H_i is of order h_i such that $h_{i+1} | h_i$, $1 \leq i \leq n-1$. If $a^{g/h_1} = \prod_{i=1}^{n} b_i^{I-\sigma_i}$, where $\prod_{i=1}^{m} b_i^{I-\sigma_i} \varepsilon F_{m+1}$, $1 \leq m \leq n$, $F_{n+1} = E$, σ_i a generator of H_i, and $g = h_1 \cdots h_n$ the order of G, then $N(a) = 1$.

<u>Proof</u>: The proof of Theorem 3.2 on page 23 will apply.

<u>Corollary 4.1</u>: If $G = H_1 \cdots H_n$ and a is of norm 1, then $a^{h_{P(2)} \cdots h_{P(n)}} = \prod_{i=1}^{n} c_i^{I-\sigma_i}$ for every permutation P for which $H_{P(1)} \cdots H_{P(n)} = H_1 \cdots H_n$.

<u>Notation:</u> In this corollary and in all the following work the exponent of a guaranteed by Theorem 4.1 will be written as $h_2 \cdots h_n$. If $n = 1$, the exponent of a

in Theorem 4.1 is already 1. Hence, there is no need in attempting a reduction in the exponent of a.

Proof: In applying Theorem 4.1 to $G = H_{P(1)}\cdots H_{P(n)}$, the result is $a^{h_{P(2)}\cdots h_{P(n)}} = \prod_{i=1}^{n} c_{P(i)}^{I-\sigma_{P(i)}}$. Since P is a permutation of n symbols,
$\prod_{i=1}^{n} c_{P(i)}^{I-\sigma_{P(i)}} = \prod_{i=1}^{n} c_i^{I-\sigma_i}$. The conclusion follows.

If $n \geq 2$, then there exists at least one non-identity permutation P of n symbols for which
$H_1\cdots H_n = H_{P(1)}\cdots H_{P(n)}$. The mapping $x \longrightarrow x^{-1}$, $x \in G$, gives a one-to-one correspondence from G to G. Since
$(\tau_1\cdots\tau_n)^{-1} = \tau_1^{-1}\cdots\tau_n^{-1}$, $G = H_n H_{n-1}\cdots H_1$.

The exponent of a might be reduced by some other arrangement of the H_i as in Corollary 4.1. Even more can be done. The next lemma will be useful in showing that a with exponent the greatest common divisor of the exponents obtained from Corollary 4.1 is also of the form
$\prod_{i=1}^{n} c_i^{I-\sigma_i}$, $c_i \in E$.

Lemma 4.4: If $x_j = \prod_{i=1}^{n} b_{ij}^{I-\sigma_i}$, $1 \leq j \leq m$, $b_{ij} \in E$, and s_j are integers, then there are $b_i \in E$ such that
$\prod_{j=1}^{m} x_j^{s_j} = \prod_{i=1}^{n} b_i^{I-\sigma_i}$.

Proof:
$$\prod_{j=1}^{m} x_j^{s_j} = \prod_{j=1}^{m}\left[\prod_{i=1}^{n} b_{ij}^{I-\sigma_i}\right]^{s_j}$$
$$= \prod_{i=1}^{n}\left[\prod_{j=1}^{m}\left(b_{ij}^{I-\sigma_i}\right)^{s_j}\right]$$
$$= \prod_{i=1}^{n}\left[\prod_{j=1}^{m}\left(b_{ij}^{s_j}\right)^{I-\sigma_i}\right]$$
$$= \prod_{i=1}^{n}\left[\prod_{j=1}^{m} b_{ij}^{s_j}\right]^{I-\sigma_i}.$$ Let $b_i = \prod_{j=1}^{m} b_{ij}^{s_j}$.

Corollary 4.2: If G is factorable and $a \in E$ if of norm 1, then $a^d = \prod_{i=1}^{n} b_i^{I-\sigma_i}$, where d is the greatest common divisor of the positive integers in

$\{h_{P(2)}\cdots h_{P(n)} \mid$ P a permutation of n symbols such that $H_1\cdots H_n = H_{P(1)}\cdots H_{P(n)}\}$.

Proof: Apply Lemma 4.4 to Corollary 4.1 with $x_j = a^{h_{P_j(2)}\cdots h_{P_j(n)}}$, $1 \leq j \leq m$, m the number of distinct P_j satisfying $H_1\cdots H_n = H_{P_j(1)}\cdots H_{P_j(n)}$, and s_j, $1 \leq j \leq m$, satisfying $d = \sum_{j=1}^{m} s_j \cdot h_{P_j(2)}\cdots h_{P_j(n)}$.

Corollary 4.3: If m is the least positive integer for which $N(a) = 1$ implies that $a^m = \prod_{i=1}^{n} b_i^{I-\sigma_i}$, then $m \mid d$.

Proof: The proof of Corollary 3.1, page 12, will apply.

Corollary 4.4: If $a^d = \prod_{i=1}^{n} b_i^{I-\sigma_i}$, $b_i \in E$, then $[N(a)]^d = 1$ and $N[N(a)] = 1$.

Proof: The proof of Corollary 3.2, page 13, will apply.

Of course, if G is such that $d = 1$, then this corollary serves as the converse of Theorem 4.1.

As seen by Corollary 3.3, page 24, for the case in which G is commutative, the exponent of a is 1 if and only if G is cyclic. The following example shows that this is not the case with G factorable but non-commutative.

Let $G = \{I, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$, where the mixed products are given by $\sigma^3 = \tau^2 = I$, $\sigma\tau = \tau\sigma^2$, and $\tau\sigma = \sigma^2\tau$. Hence, G is not cyclic. But, $G = H_1H_2 = H_2H_1$, where $H_1 = \{I, \sigma, \sigma^2\}$ and $H_2 = \{I, \tau\}$. For fields E and F for which G is the group of E/F and $a \in E$ of norm 1, Corollary 4.2

guarantees that $a = b_1^{I-\sigma} b_2^{I-\tau}$, $b_i \varepsilon E$.

The following work demonstrates that if G satisfies the hypothesis of Theorem 3.2 and is pseudo-decomposable, then Corollary 4.2 does not reduce the exponent of a.

If G is such that $h_{i+1} \mid h_i$, $1 \leq i \leq n-1$, then $h_i \mid h_1$, for all i, $1 \leq i \leq n$. Theorem 3.1 guarantees that a of norm 1 satisfies $a^{h_2 \cdots h_n} = \prod_{i=1}^{n} b_i^{I-\sigma_i}$, $b_i \varepsilon E$. Corollary 4.2 asserts that this same a satisfies $a^d = \prod_{i=1}^{n} c_i^{I-\sigma_i}$, $c_i \varepsilon E$, where d is the greatest common divisor of the positive integers of $S = \left\{ h_{P(2)} \cdots h_{P(n)} \mid H_1 \cdots H_n = H_{P(1)} \cdots H_{P(n)} \right\}$. Since $h_2 \cdots h_n \varepsilon S$, $d \mid h_2 \cdots h_n$. Let $h_{P(2)} \cdots h_{P(n)} \varepsilon S$. Either $h_{P(2)} \cdots h_{P(n)} = h_2 \cdots h_n$, or $h_{P(2)} \cdots h_{P(n)} = h_1 \cdots h_{i-1} h_{i+1} \cdots h_n$. In the former, $h_2 \cdots h_n \mid h_{P(2)} \cdots h_{P(n)}$. In the latter, all the factors of $h_2 \cdots h_n$ and $h_{P(2)} \cdots h_{P(n)}$ are the same with the exception of h_i in the first and h_1 in the second. But, $h_i \mid h_1$, and so $h_2 \cdots h_n \mid h_{P(2)} \cdots h_{P(n)}$. Hence, $h_2 \cdots h_n \mid d$, and $d = h_2 \cdots h_n$. Thus, Corollary 4.2 does not reduce the exponent of a.

As a matter of fact, in the case in which G is commutative, the decomposition of G, $G = G_1 X \cdots X G_n$, in Lemma 3.3 could have been used in Theorem 4.1. Moreover, $G_{P(1)} X \cdots X G_{P(n)} = G_1 X \cdots X G_n$ for all P. In applying Corollary 4.2, d turns out to be nothing more than $h_2 \cdots h_n$, the exponent obtained by the use of the decomposition of G in Lemma 3.6.

Examples have been given to indicate differences in applications of Theorems 3.1 and 4.1. But, for G pseudo-decomposable both of these theorems may be applied. It might appear that the results would be identical. Also, with G pseudo-decomposable it might appear that applications of both Theorems 3.2 and 4.2 would lead to the same results. With G pseudo-decomposable and $n > 1$, the following diagrams illustrate the differences in the above pairs of theorems.

$$\begin{tikzcd}
G = G_1 \arrow[r, phantom, "="] \arrow[d, dash] & H_1 \cdots H_n \arrow[r] & F_1 = F \arrow[d, dash] \\
G_2 \arrow[r, phantom, "="] \arrow[d, dash] & H_2 \cdots H_n \arrow[r] & F_2 \arrow[d, dash] \\
G_3 \arrow[r, phantom, "="] & H_3 \cdots H_n \arrow[r] & F_3 \\
\vdots & \vdots & \vdots \\
G_n \arrow[r, phantom, "="] \arrow[d, dash] & H_n \arrow[r] & F_n \arrow[d, dash] \\
G_{n+1} \arrow[r, phantom, "="] & I \arrow[r] & F_{n+1} = E
\end{tikzcd}$$

PSEUDO-DECOMPOSABLE GROUPS

$\prod_{i=1}^{m} b_i^{I-\sigma_i} \in F_{m+1}$, $1 \leq m \leq n$, if and only if $\prod_{i=1}^{m} b_i^{I-\sigma_i}$ is invariant under every element of $H_{m+1} \cdots H_n$.

FACTORABLE GROUPS

$$\begin{tikzcd}
 & & G = H_1 \cdots H_n \arrow[rrrrrr] \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[drr, dash] & & & & & & F \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[drr, dash] & & \\
H_1 \arrow[drr, dash] & H_2 \arrow[dr, dash] & H_3 \arrow[d, dash] & \cdots & H_n \arrow[dll, dash] & & F_1 \arrow[drr, dash] & F_2 \arrow[dr, dash] & F_3 \arrow[d, dash] & \cdots & F_n \arrow[dll, dash] \\
 & & I & & & H_i \rightarrow F_i & & & E & &
\end{tikzcd}$$

$\prod_{i=1}^{m} b_i^{I-\sigma_i} \in F_{m+1}$, $1 \leq m \leq n$, if and only if $\prod_{i=1}^{m} b_i^{I-\sigma_i}$ is invariant under every element of H_{m+1}.

As a final note, it should be observed that the generality of the preceding results may be extended somewhat. In all of the preceding work, conditions were placed on the group G. In some cases these conditions may be removed from G and placed on a proper subgroup of G. In the light of Theorem 2.1, with a of norm 1, there may be a proper subgroup H of G for which $N_H(a) = 1$. If H satisfies the conditions assumed of G in the preceding work, then the appropriate theorems will apply to a and H.

LIST OF REFERENCES

1. E. Artin, Modern Higher Algebra, Galois Theory, New York, 1947.

2. Curtis and Reiner, Representation Theory of Finite Groups and Associative Algebras, New York, 1962.

3. N. Jacobson, Lectures in Abstract Algebra, vol. III, New Jersey, 1964.