The University of British Columbia

Faculty of Graduate Studies

PROGRAMME OF THE

FINAL ORAL EXAMINATION

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

of

BOMSHIK CHANG

B. A., Seoul University, 1954
M. A., Seoul University, 1956

IN ROOM 207, ARTS BUILDING

WEDNESDAY, APRIL 29, 1959 AT 11:30 A. M.

COMMITTEE IN CHARGE

DEAN W. H. GAGE: Chairman

G. O. B. DAVIES	F. A. KAEMPFFER
R. P. DORE	B. N. MOYLS
R. D. JAMES	D. C. MURDOCH
S. A. JENNINGS	A. STROLL

External Examiner: PHILLIP HALL, M. A., F. R. S.
Sadleirian Professor of Mathematics
Cambridge University

ON ENGEL RINGS OF EXPONENT p-1 OVER GF(p)

ABSTRACT

It is well known that the restricted Burnside problem for a prime exponent p can be rephrased in terms of the nilpotence of finitely generated Engel rings over GF(p), with exponent p-1. We study these rings with the object of extending our knowledge of the Burnside groups.

Let E^q be the Lie ring over GF(p) generated by $e_1, \ldots, e_q$, where the elements of E^q are restricted by the Engel condition $[fg^{p-1}] = 0$ for all $f, g \in E^q$. If L^q is the free Lie ring over GF(p) generated by $a_1, \ldots, a_q$, and if I^q is the ideal of L^q generated by $[xy^{p-1}]$ for all $x, y \in L^q$, then $E^q \simeq L^q / I^q$. We study E^q by investigation of I^q in L^q.

Let I^q_n be the submodule of I^q consisting of linear combinations of monomials in $a_1, \ldots, a_q$ of degree n, and let $I^q(n_1, \ldots, n_q)$ be the submodule of I^q_n consisting of linear combinations of degree n_1 in a_1, n_2 in a_2, $\ldots$, n_q in a_q, $n_1 + \ldots + n_q = n$. The ranks of I^q_n and $I^q(n_1, \ldots, n_q)$ are denoted respectively by i^q_n and $i^q(n_1, \ldots, n_q)$.

We prove first that I^q is the module spanned by all elements of the form $[uxy^{p-1}]$, and obtain upper bounds for i^q_n and $j^q(n_1, \ldots, n_q)$ which may be most conveniently expressed as coefficients of certain formal power series.

Further results are obtained by giving another set of elements which spans I^2. This enables us to find upper bounds for $i^2(m, n)$ by an inductive method. In particular, we prove

$$i^2(p+r-n, n) \leq \frac{r^{n-1}}{(n-1)!} + K,$$

where K is a polynomial in r of degree at most n-2.

Using the above formula, we prove that, if the Engel ring E^2 were nilpotent with class c_p, then c_p / p would not be bounded.

Finally, we give a new proof of the relation between the Burnside groups and the Engel rings by studying the free restricted Lie rings and Zassenhaus' representation of the free groups.

PUBLICATIONS

B. Chang, S. A. Jennings, and R. Ree, **On certain pairs of matrices which generate free groups.** Can. J. Math. **10** 279-284 (1958).

GRADUATE STUDIES

Field of Study: Abstract Algebra and Group Theory

Modern Algebra	B. N. Moyls
Theory of Functions	W. H. Simons
Functional Analysis	R. R. Christian

Other Studies:

Symbolic Logic	A. Stroll
Electricity and Magnetism	W. Opechowski
Theoretical Mechanics	F. A. Kaempffer

ON ENGEL RINGS OF EXPONENT p-1 OVER GF(p)

by

BOMSHIK CHANG

M. A., Seoul University, 1956

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
in the Department
of
MATHEMATICS

We accept this thesis as conforming to the
standard required from candidates for the
degree of Doctor of Philosophy:

THE UNIVERSITY OF BRITISH COLUMBIA

April, 1959

ABSTRACT

It is well-known that the restricted Burnside problem for a prime exponent p can be rephrased in terms of the nilpotence of finitely generated Engel rings over GF(p) with the exponent p-1. In this thesis we study these rings with the object of extending our knowledge of the Burnside groups.

Let $\mathcal{E}^q$ be the Lie ring over GF(p) generated by $e_1, e_2, \ldots, e_q$, where the elements of $\mathcal{E}^q$ are restricted by the Engel condition $[fg^{p-1}] = 0$ for all $f, g \in \mathcal{E}^q$. If $\mathcal{L}^q$ is the free Lie ring over GF(p) generated by $a_1, a_2, \ldots, a_q$, and if $\mathcal{J}^q$ is the ideal of $\mathcal{L}^q$ generated by $[xy^{p-1}]$ for all $x, y \in \mathcal{L}^q$, then $\mathcal{E}^q \cong \mathcal{L}^q/\mathcal{J}^q$. We study $\mathcal{E}^q$ by investigation of $\mathcal{J}^q$ in $\mathcal{L}^q$.

Let $\mathcal{J}_n^q$ be the submodule of $\mathcal{J}^q$ consisting of linear combinations of monomials in $a_1, a_2, \ldots, a_q$ of degree n, and let $\mathcal{J}^q(n_1, n_2, \ldots, n_q)$ be the submodule of $\mathcal{J}_n^q$ consisting of linear combinations of degree n_1 in a_1, n_2 in $a_2, \ldots,$ n_q in a_q, $n_1 + n_2 + \ldots + n_q = n$. The ranks of $\mathcal{J}_n^q$ and $\mathcal{J}^q(n_1, n_2, \ldots, n_q)$ are denoted respectively by i_n^q and $i^q(n_1, n_2, \ldots, n_q)$.

We prove first that $\mathcal{J}^q$ is the module spanned by all elements of the form $[xy^{p-1}]$, and obtain upper bounds for i_n^q and $i^q(n_1, n_2, \ldots, n_n)$ in

terms of well defined integers j_n^q and $j^q(n_1,n_2,\ldots,n_q)$ which may be most conveniently expressed as coefficients of certain formal power series.

Further results are obtained by giving another set of elements which spans $\mathcal{J}^2$. This enables us to find upper bounds for $i^2(m,n)$ by an inductive method. In particular, we prove

$$i^2(p+r-n,n) \leq \frac{r^{n-1}}{(n-1)!} + K,$$

where K is a polynomial in r of degree at most n-2.

Using the above formula, we prove that, if the Engel ring $\mathcal{E}^2$ were nilpotent with class c_p, then c_p/p would not be bounded.

We give another proof of well-known fact about the relation between the Burnside groups and the Engel rings by studying the free restricted Lie rings and Zassenhaus' representation of the free groups.

The University of British Columbia

Faculty of Graduate Studies

PROGRAMME OF THE

FINAL ORAL EXAMINATION

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

of

BOMSHIK CHANG

B. A., Seoul University, 1954
M. A., Seoul University, 1956

IN ROOM 207, ARTS BUILDING

WEDNESDAY, APRIL 29, 1959 AT 11:30 A. M.

COMMITTEE IN CHARGE

DEAN W. H. GAGE: Chairman

G. O. B. DAVIES	F. A. KAEMPFFER
R. P. DORE	B. N. MOYLS
R. D. JAMES	D. C. MURDOCH
S. A. JENNINGS	A. STROLL

External Examiner: PHILLIP HALL, M. A., F. R. S.
Sadleirian Professor of Mathematics
Cambridge University

ON ENGEL RINGS OF EXPONENT p-1 OVER GF(p)

ABSTRACT

It is well known that the restricted Burnside problem for a prime exponent p can be rephrased in terms of the nilpotence of finitely generated Engel rings over GF(p) with exponent p-1. We study these rings with the object of extending our knowledge of the Burnside groups.

Let E^q be the Lie ring over GF(p) generated by $e_1, \ldots, e_q$, where the elements of E^q are restricted by the Engel condition $[fg^{p-1}] = 0$ for all $f, g \in E^q$. If L^q is the free Lie ring over GF(p) generated by $a_1, \ldots, a_q$, and if I^q is the ideal of L^q generated by $[xy^{p-1}]$ for all $x, y \in L^q$, then $E^q \simeq L^q/I^q$. We study E^q by investigation of I^q in L^q.

Let I^q_n be the submodule of I^q consisting of linear combinations of monomials in $a_1, \ldots, a_q$ of degree n, and let $I^q(n_1, \ldots, n_q)$ be the submodule of I^q_n consisting of linear combinations of degree n_1 in a_1, n_2 in a_2, ..., n_q in a_q, $n_1 + \ldots + n_q = n$. The ranks of I^q_n and $I^q(n_1, \ldots, n_q)$ are denoted respectively by i^q_n and $i^q(n_1, \ldots, n_q)$.

We prove first that I^q is the module spanned by all elements of the form $[xy^{p-1}]$, and obtain upper bounds for i^q_n and $j^q(n_1, \ldots, n_q)$ which may be most conveniently expressed as coefficients of certain formal power series.

Further results are obtained by giving another set of elements which spans I^2. This enables us to find upper bounds for $i^2(m, n)$ by an inductive method. In particular, we prove

$$i^2(p+r-n, n) \leq \frac{r^{n-1}}{(n-1)!} + K,$$

where K is a polynomial in r of degree at most n-2.

Using the above formula, we prove that, if the Engel ring E^2 were nilpotent with class c_p, then c_p / p would not be bounded.

Finally, we give a new proof of the relation between the Burnside groups and the Engel rings by studying the free restricted Lie rings and Zassenhaus' representation of the free groups.

PUBLICATIONS

B. Chang, S. A. Jennings, and R. Ree, **On certain pairs of matrices which generate free groups.** Can. J. Math. **10** 279-284 (1958).

GRADUATE STUDIES

Field of Study: Abstract Algebra and Group Theory

Modern Algebra	B. N. Moyls
Theory of Functions	W. H. Simons
Functional Analysis	R. R. Christian

Other Studies:

Symbolic Logic	A. Stroll
Electricity and Magnetism	W. Opechowski
Theoretical Mechanics	F. A. Kaempffer

In presenting this thesis in partial fulfilment of the requirements for an advanced degree at the University of British Columbia, I agree that the Library shall make it freely available for reference and study. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by the Head of my Department or by his representatives. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Department of Mathematics

The University of British Columbia,
Vancouver 8, Canada.

Date April 4, 1958

TABLE OF CONTENTS

Introduction. Let Φ be either the ring of integers, or a field. A Lie ring $\mathfrak{L}$ over Φ is a Φ-module in which the Lie product xy for each ordered pair of elements x and y of $\mathfrak{L}$ is defined, and the following postulates are fulfilled:

(0.1) $\lambda(xy) = (\lambda x)y = x(\lambda y)$ $(\lambda \in \Phi,\ x, y \in \mathfrak{L})$,

(0.2) $(x + y)z = xz + yz$,

$x(y + z) = xy + xz$ $(x, y, z \in \mathfrak{L})$,

(0.3) (Anticommutative law)

$xx = 0$ $(x \in \mathfrak{L})$.

As a consequence of the above postulates, we have

(0.3)' $xy = -yx$ $(x, y \in \mathfrak{L})$,

(0.4) (Jacobi's identity)

$(xy)z + (yz)x + (zx)y = 0$ $(x, y, z \in \mathfrak{L})$,

A Φ-submodule $\mathfrak{L}'$ of $\mathfrak{L}$ is called a Lie subring, if $xy \in \mathfrak{L}'$ for any pair of elements x, y of $\mathfrak{L}'$, and $\mathfrak{L}'$ is called a Lie ideal, or simply an ideal, if $xy \in \mathfrak{L}'$ for any elements $x \in \mathfrak{L}'$ and $y \in \mathfrak{L}$. (If $xy \in \mathfrak{L}'$ then by (0.3)' $yx \in \mathfrak{L}'$ also. Thus any Lie ideal is a two-sided ideal.)

For any Lie ring $\mathfrak{L}$ we may form the lower central series:

(0.5) $\mathfrak{L} = \mathfrak{L}_{(1)} \supseteq \mathfrak{L}_{(2)} \supseteq \mathfrak{L}_{(3)} \supseteq \cdots$,

where

(0.6) $\mathfrak{L}_{(i+1)} = \mathfrak{L}\mathfrak{L}_{(i)}$ $(i = 1, 2, \ldots)$.

A Lie ring $\mathfrak{L}$ is said to be nilpotent of class n, if

(0.7) $\mathfrak{L}_{(n+1)} = 0, \quad \mathfrak{L}_{(n)} \neq 0.$

We may also form the derived series of $\mathfrak{L}$:

$$\mathfrak{L} = \mathfrak{L}^{(1)} \supseteq \mathfrak{L}^{(2)} \supseteq \mathfrak{L}^{(3)} \supseteq \dots , \tag{0.8}$$

where

$$\mathfrak{L}^{(i+1)} = \mathfrak{L}^{(i)}\mathfrak{L}^{(i)} \qquad (i = 1, 2, \dots), \tag{0.9}$$

and a Lie ring $\mathfrak{L}$ is said to be solvable if

$$\mathfrak{L}^{(n)} = 0 \tag{0.10}$$

for some n.

A Lie ring $\mathfrak{L}$ is called an Engel ring, or is said to satisfy the Engel condition if for any elements x, y of $\mathfrak{L}$ there exists a positive integer n, which may depend on x and y, such that

$$((\dots((xy\overbrace{)y)\dots)y}^{n})y = 0. \tag{0.11}$$

In particular, if n is independent of x, y then $\mathfrak{L}$ is called an Engel ring of exponent n, or $\mathfrak{L}$ is said to satisfy the nth Engel condition.

A well-known theorem (Engel's theorem) says that if $\mathfrak{L}$ is a Φ-module of finite rank over a field Φ and if $\mathfrak{L}$ satisfies the nth Engel condition then $\mathfrak{L}$ is nilpotent. Zorn [30] has shown that if $\mathfrak{L}$ satisfies the maximum condition for subrings, and if $\mathfrak{L}$ satisfies the Engel condition then $\mathfrak{L}$ is nilpotent. Higgins [8] has shown that a solvable Engel ring of exponent n over a ring or a field of characteristic prime to n! is nilpotent. The question as to whether a finitely generated Engel ring of exponent n is nilpotent is, however, still open.

The main purpose of this thesis is to study a special class of Engel rings, namely, free Engel rings over GF(p), of exponent p-1. Rings of this type have important applications in connection with the celebrated Burnside problem. We may indicate this connection, somewhat intuitively, as follows. To a given group we associate a ring in such a way that the product and the commutator of group elements correspond to the sum and the Lie product of Lie elements respectively (Lazard [13], Magnus [18]). If the given group is of exponent p (i.e. $g^p = 1$ for every element g of the group) then the associated Lie ring satisfies the (p-1)st Engel condition (Higman [9], Sanov [26]). Hence the nilpotence of the "free" Engel ring $\mathcal{E}^q$ with q generators implies the proposition R'_p (cf. Section 6). Indeed, the solution of the problem for p = 5 (Higman [9], Kostrikin [12]) is based on this fact. Moreover, for i = 1, 2, ... , 2p-2, the orders of the factor rings $\mathcal{E}^q_{(i)} / \mathcal{E}^q_{(i+1)}$ are equal respectively to the orders of the factor groups $\mathcal{B}_i / \mathcal{B}_{i+1}$, where $\mathcal{E}^q_{(n)}$ and $\mathcal{B}_n$ denote the nth term of the lower central series of $\mathcal{E}^q$ and the Burnside group $\mathcal{B}$.

In section 1, we introduce some notations and review some concepts concerning the free Lie ring over GF(p) and its derivation ring, which are used in later sections.

In section 2, we consider the derivation

ring and introduce Jacobson's [10] notation:

$$\left\{ \begin{matrix} X_1 & X_2 & \dots & X_n \\ 1 & 1 & \dots & 1 \end{matrix} \right\} = \sum X_{i_1} X_{i_2} \dots X_{i_n} ,$$

where the X_i are noncommutative but associative indeterminates and the summation is taken over all permutations $i_1, i_2, \dots, i_n$ of $1, 2, \dots, n$ which may be called the symmetric sum of $X_1, X_2, \dots, X_n$. We list some properties of these symmetric sums most of which were obtained by Jacobson. It is well-known that,

$$(X + Y)^p - X^p - Y^p = \Lambda(X,Y) \qquad (\text{mod } p)$$

is a Lie element (cf. Section 1.2) in X and Y (Jacobson [11], Zassenhaus [28]), which implies that, in general, the symmetric sum $\{X_1 X_2 \dots X_p / 1\ 1 \dots 1\}$ (mod p) is a Lie element in $X_1, X_2, \dots, X_p$. For example, $(X + Y)^2 - X^2 - Y^2 = XY + YX = XY - YX = [XY]$ (mod 2). We prove that,

$$[X_1 \{X_2 \dots X_p / 1\ 1 \dots 1\}] = \sum [\dots[[X_1 X_{i_2}] X_{i_3}] \dots X_{i_p}],$$

where again the summation is taken over all permutations $i_1, i_2, \dots, i_p$ of $2, 3, \dots, p$, is actually the symmetric sum $\{X_1 X_2 \dots X_p / 1\ 1 \dots 1\}$. This fact plays a most important role throughout this thesis.

In section 3, we define the Engel ideal $\mathcal{J}$ of the free Lie ring $\mathcal{L}$ over GF(p) to be the ideal of $\mathcal{L}$ generated by all elements of the form $((\dots(\overbrace{xy)\dots)y)}^{p-1}y$, $x, y \in \mathcal{L}$, and prove that the Engel ideal is the module generated by all elements $((\dots(\overbrace{xy)\dots)y)}^{p-1}y$, i.e. the set of all linear combinations of such elements

(Theorem 3.1). Using this theorem we obtain upper bounds for the ranks of the module $\mathcal{J}_i/\mathcal{J}_{i+1}$ which will give lower bounds for the ranks of the abelian factor groups $\mathcal{B}_i/\mathcal{B}_{i+1}$ for i = 1, 2, ..., 2p-2.

In section 4, we restrict ourselves to a consideration of the Engel ideal $\mathcal{J}^2$ of the free Lie ring $\mathcal{L}^2$ with two generators. We choose, first, a special type of basis (a <u>normal basis</u>) for $\mathcal{L}^2$. Using this set of basis elements we obtain a subset of elements of $\mathcal{L}^2$ such that any element of $\mathcal{J}^2$ may be written as a linear combination of elements of this set (Theorem 4.2). As an application of this theorem we shall obtain another expression for the upper bounds of the ranks of the submodules $\mathcal{J}(m,n)$ of $\mathcal{J}^2$ consisting of all homogeneous elements with degree m in one generator and n in the other.

In section 5, using the upper bounds for the ranks for $\mathcal{J}(m,n)$ obtained in section 4 together with well-known Witt's formula we prove that the class of nilpotence of Engel ring of exponent p-1 with more than one generator cannot be expressed as a linear function of p in general (Theorem 5.1).

In section 6, we discuss the connection between the preceding results and the Burnside groups.

We list some open question in connection with this thesis in the last section 7.

1. Free Lie ring $\mathcal{L}^q$ over GF(p). In what follows we denote the free Lie ring over GF(p) with q generators $a_1, a_2, \ldots, a_q$ by $\mathcal{L}^q$, or simply by $\mathcal{L}$. We shall denote elements of $\mathcal{L}$ by small Latin letters. The Lie product of elements x and y in $\mathcal{L}$ will be denoted by xy. An element of the form $(\ldots((x_1x_2)x_3)\ldots)x_n$ will be called a (right) normal product in $x_1, x_2, \ldots, x_n$, and will be denoted by $x_1x_2x_3\ldots x_n$. A normal product of the form $xy\overbrace{\ldots}^{i}y\overbrace{z\ldots z}^{j}\ldots\overbrace{u\ldots u}^{k}$ will be written as $xy^iz^j\ldots u^k$. We have

$$x(yz) = xyz - xzy. \tag{1.1}$$

This identity enables us to write every element of $\mathcal{L}$ as a linear combination of (right) normal products in the generators $a_1, a_2, \ldots, a_q$.

The submodule of $\mathcal{L}^q$ consisting of all linear combinations of homogeneous monomials of degree n in the generators will be denoted by $\mathcal{L}_n^q$, or if no confusion arises, by $\mathcal{L}_n$. Similarly, $\mathcal{L}(n_1, n_2, \ldots, n_q)$ will denote the submodule of $\mathcal{L}_n^q$ consisting of all linear combinations of homogeneous monomials in each generator with degree n_1 in a_1, n_2 in $a_2, \ldots$, and n_q in a_q, where $n_1 + n_2 + \ldots + n_q = n$. The ranks of the modules $\mathcal{L}_n^q$ and $\mathcal{L}(n_1, n_2, \ldots, n_q)$ will be denoted by f_n^q and $f(n_1, n_2, \ldots, n_q)$ respectively. Expressions for f_n^q and $f(n_1, n_2, \ldots, n_q)$ have been given by Witt [27], viz

$$f_n^q = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d}, \tag{1.2}$$

$$(1.3)\qquad f(n_1, n_2, \ldots, n_q) = \frac{1}{n} \sum_{d \mid n_i} \frac{\mu(d)\ \frac{n}{d}!}{\frac{n_1}{d}!\ \frac{n_2}{d}!\ \cdots\ \frac{n_q}{d}!}$$

$$(n_1 + n_2 + \ldots + n_q = n),$$

where $\mu(d)$ is the Moebius function.

1.2. The free associative ring $\mathfrak{A}^q$ over GF(p). An inner derivation Y of $\mathfrak{L}$ is a mapping of $\mathfrak{L}$ into $\mathfrak{L}$ itself defined by Y: $x \longrightarrow xy$ for all $x \in \mathfrak{L}$, where y is a fixed element of $\mathfrak{L}$. Throughout, we denote inner derivations by the same capital letter as is used for the fixed element of $\mathfrak{L}$ defining the inner derivation; for example Y_i will denote the mapping $x \longrightarrow xy_i$ for all $x \in \mathfrak{L}$. The inner derivation defined by yz, i.e. the mapping $x \longrightarrow x(yz)$ will be denoted by [YZ]. By (1.1) we have

$$(1.2.1)\qquad [YZ] = YZ - ZY.$$

Again, for brevity, we will write

$$(1.2.2)\qquad [\ldots[[X_1X_2]X_3]\ldots X_n] = [X_1X_2X_3\ldots X_n],$$

$$(1.2.3)\qquad [XY\overbrace{\ldots}^{i}YZ\overbrace{\ldots}^{j}Z\ldots U\overbrace{\ldots}^{k}U] = [XY^iZ^j\ldots U^k].$$

The associative ring over GF(p) generated by the inner derivations A_i: $x \longrightarrow xa_i$, $i = 1, 2, \ldots, q$, will be denoted by $\mathfrak{A}^q$ or $\mathfrak{A}$. It is known that $\mathfrak{A}$ is a free ring with generators $A_1, A_2, \ldots, A_q$ (Witt [27]). The elements of $\mathfrak{A}$ which are themselves inner derivations of $\mathfrak{L}$ form a Lie ring if the Lie product of X and Y,

where X and Y are inner derivations, is defined by $[XY] = XY - YX$. This Lie ring will be denoted by $\mathfrak{D}^q$ or simply by $\mathfrak{D}$. The mapping $x \longrightarrow X$, $y \longrightarrow Y$ and $xy \longrightarrow [XY]$ is an isomorphic mapping of $\mathfrak{L}$ onto $\mathfrak{D}$ ([27]). We shall call the elements of $\mathfrak{D}$ the Lie elements of $\mathfrak{A}$: for example $A_1, \ldots, A_q$, $[A_1A_2] = A_1A_2 - A_2A_1, \ldots$ are Lie elements of $\mathfrak{A}$. We prefer not to consider as a restricted Lie algebra ([10],[11]) so that an element of $\mathfrak{A}$ of the form X^p, $X \in \mathfrak{D}$, will not be called a Lie element of $\mathfrak{A}$.

The identity mapping of $\mathfrak{L}$ defined by $x \longrightarrow x$ for all $x \in \mathfrak{L}$, will be denoted by E. Note that E is not an element of $\mathfrak{A}$, but, for convenience in the following sections we will consider E adjoined to $\mathfrak{A}$. We shall use the following convenient natations:

(1.2.4)
$$x = xE,$$
$$xy = xY,$$
$$x(yz) = x[YZ],$$
$$xyz = xYZ, \quad \text{ect.}$$

2. Some identities in $\mathfrak{A}$. In this section we list certain identities among the elements of $\mathfrak{A}$ which will be used in later sections. We shall not give proofs for well-known formulas.

Let $X_1, X_2, \ldots, X_n, X, Y$ be elements of $\mathfrak{A}$. Using Jacobson's [10] notation the symbol

$$\begin{Bmatrix} X_1 & X_2 & \ldots & X_n \\ i_1 & i_2 & \ldots & i_n \end{Bmatrix} \quad (\text{or } \{X_1\ X_2 \ldots X_n / i_1\ i_2 \ldots i_n\})$$

where $i_1, i_2, \ldots, i_n$ are non-negative integers smaller than p, will denote the sum of all products of i_1 of X_1, i_2 of $X_2, \ldots,$ i_n of X_n in every possible order. In particular, $\begin{Bmatrix} X_1 & X_2 & \ldots & X_n \\ 1 & 1 & \ldots & 1 \end{Bmatrix}$ (or $\{X_1\ X_2 \ldots X_n / 1\ 1 \ldots 1\}$) denotes the sum of n! terms $X_{i_1} X_{i_2} \ldots X_{i_n}$, where $i_1, i_2, \ldots, i_n$ are taken over all permutations of $1, 2, \ldots, n$.

Consider $\{Y_1\ Y_2 \ldots Y_m / 1\ 1 \ldots 1\}$, $(m = i_1 + i_2 + \ldots + i_n)$, and replace each of the first i_1 of the Y_k by X_1, each of the next i_2 of the Y_k by $X_2, \ldots,$ and each of the last i_n of the Y_k by X_n. Then we have

$$(2.1) \qquad \begin{Bmatrix} X_1 & \ldots & X_1 & X_2 & \ldots & X_2 & \ldots & X_n & \ldots & X_n \\ 1 & \ldots & 1 & 1 & \ldots & 1 & \ldots & 1 & \ldots & 1 \end{Bmatrix}$$

$$= i_1! i_2! \ldots i_n! \begin{Bmatrix} X_1 & X_2 & \ldots & X_n \\ i_1 & i_2 & \ldots & i_n \end{Bmatrix}$$

Another rather simple but useful identity is

$$(2.2)\qquad \begin{Bmatrix} X_1 & X_2 & \dots & X_n \\ i_1 & i_2 & \dots & i_n \end{Bmatrix}$$

$$= X_1 \begin{Bmatrix} X_1 & X & \dots & X_n \\ i_1-1 & i_2 & \dots & i_n \end{Bmatrix} + X_2 \begin{Bmatrix} X_1 & X_2 & \dots & X_n \\ i_1 & i_2-1 & \dots & i_n \end{Bmatrix}$$

$$+ \dots + X_n \begin{Bmatrix} X_1 & X_2 & \dots & X_n \\ i_1 & i_2 & \dots & i_n-1 \end{Bmatrix}$$

$$= \begin{Bmatrix} X_1 & X_2 & \dots & X_n \\ i_1-1 & i_2 & \dots & i_n \end{Bmatrix} X_1 + \begin{Bmatrix} X_1 & X_2 & \dots & X_n \\ i_1 & i_2-1 & \dots & i_n \end{Bmatrix} X_2$$

$$+ \dots + \begin{Bmatrix} X_1 & X_2 & \dots & X_n \\ i_1 & i_2 & & i_n-1 \end{Bmatrix} X_n \ .$$

The following two identities are well-known([10]).

$$(2.3)\qquad \begin{Bmatrix} X_1 & X_2 & \dots & X_n \\ 1 & 1 & \dots & 1 \end{Bmatrix}$$

$$= (X_1 + X_2 + \dots + X_n)^n - \sum_c (X_1 + X_2 + \dots + X_{n-1})^n$$

$$+ \sum_c (X_1 + X_2 + \dots + X_{n-2})^n - \dots + (-1)^{n-1} \sum_c X_1^n \ .$$

Here $\sum_c (X_1 + X_2 + \dots + X_{n-i})^n$ denotes the sum of the $\binom{n}{n-i}$ terms $(X_{j_1} + X_{j_2} + \dots + X_{j_{n-i}})^n$ where $j_1, j_2, \dots, j_{n-i}$ runs over all combinations of 1, 2,..., n taken n-i at a time.

$$(2.4)\qquad \begin{Bmatrix} X_1 + X_2 + \dots + X_n & X \\ & 1 \end{Bmatrix} - \sum_c \begin{Bmatrix} X_1 + X_2 + \dots + X_{n-1} & X \\ & 1 \end{Bmatrix}$$

$$+ \dots + (-1)^{n-1} \sum_c \begin{Bmatrix} X_1 & X \\ n & 1 \end{Bmatrix}$$

$$= \begin{Bmatrix} X_1 & X_2 & \dots & X_n & X \\ 1 & 1 & \dots & 1 & 1 \end{Bmatrix} ,$$

where $\sum_c$ has the same significance as in (2.3). (The

identities (2.3) and (2.4) hold in any associative ring.)

In the rest of this section X, X_i, Y, Y_i are assumed to be elements of $\mathfrak{I}$. The following two identities are also well-known. (cf. (1.2.3) for the notations.)

$$(2.5) \qquad [XY^p] = XY^p - Y^pX.$$

$$(2.6) \qquad [XY^{p-1}] = \sum_{i=0}^{p-1} Y^i XY^{p-i-1} = \left\{ \begin{matrix} X & Y \\ 1 & p-1 \end{matrix} \right\}.$$

A generalization of (2.6) is the identity:

$$(2.7) \qquad \left[X \left\{ \begin{matrix} X_1 & X_2 & \cdots & X_{p-1} \\ 1 & 1 & \cdots & 1 \end{matrix} \right\} \right] = \left\{ \begin{matrix} X & X_1 & X_2 & \cdots & X_{p-1} \\ 1 & 1 & 1 & \cdots & 1 \end{matrix} \right\}.$$

(For clarity we stress again our convention (1.2.2), so that the left-hand side denotes $\sum [XX_{i_1} X_{i_2} \ldots X_{i_{p-1}}]$, where the summation is taken over all permutations $i_1, i_2, \ldots, i_{p-1}$ of $1, 2, \ldots, p-1$.)

Proof of (2.7). By (2.3), we have

$$\begin{aligned}
&\left[X \left\{ \begin{matrix} X_1 & X_2 & \cdots & X_{p-1} \\ 1 & 1 & \cdots & 1 \end{matrix} \right\} \right] \\
&= [X(X_1 + X_2 + \ldots + X_{p-1})^{p-1}] \\
&- \sum_c [X(X_1 + X_2 + \ldots + X_{p-2})^{p-1}] \\
&\quad \cdots\cdots \\
&+ (-1)^{p-1} \sum_c [XX_1^{p-1}] \\
&= \left\{ \begin{matrix} X & X_1 + X_2 + \ldots + X_{p-1} \\ 1 & p-1 \end{matrix} \right\} \\
&- \sum_c \left\{ \begin{matrix} X & X_1 + X_2 + \ldots + X_{p-2} \\ 1 & p-1 \end{matrix} \right\} \\
&\quad \cdots\cdots
\end{aligned}$$

$$+ (-1)^{p-1}\sum_{c}\left\{\begin{matrix} X & X_1 \\ 1 & p-1 \end{matrix}\right\} \qquad \text{(by (2.6))}$$

$$= \left\{\begin{matrix} X & X_1 & X_2 & \dots & X_{p-1} \\ 1 & 1 & 1 & \dots & 1 \end{matrix}\right\} \qquad \text{(by (2.4))}.$$

This identity gives another proof of the well-known formula (Zassenhaus [28]):

$$(X + Y)^p = X^p + Y^p + \Lambda(X,Y),$$

where X, Y are elements of an associative ring over a field of characteristic $p > 0$, and $\Lambda(X,Y)$ is a sum of Lie products in X and Y. Indeed,

$$(2.8) \qquad (X + Y)^p = X^p + Y^p + \sum_{n=1}^{p-1}\left\{\begin{matrix} X & Y \\ n & p-n \end{matrix}\right\},$$

and

$$\Lambda(X,Y) = \sum_{n=1}^{p-1}\left\{\begin{matrix} X & Y \\ n & p-n \end{matrix}\right\} = \sum_{n=1}^{p-1}\left[X\left\{\begin{matrix} X & Y \\ n-1 & p-n \end{matrix}\right\}\right].$$

A similar argument establishes the identity:

$$(2.9) \qquad (X_1 + X_2 + \dots + X_k)^p$$

$$= X_1^p + X_2^p + \dots + X_k^p + \Lambda(X_1, X_2, \dots, X_k),$$

where

$$\Lambda(X_1, X_2, \dots, X_k) = \sum\left\{\begin{matrix} X_1 & X_2 & \dots & X_j & \dots & X_k \\ i_1 & i_2 & \dots & i_j & \dots & i_k \end{matrix}\right\}$$

$$= \sum\left[X_j\left\{\begin{matrix} X_1 & X_2 & \dots & X_j & \dots & X_k \\ i_1 & i_2 & \dots & i_j-1 & \dots & i_k \end{matrix}\right\}\right]$$

$$(i_j \neq 0,\ i_1 + i_2 + \dots + i_k = p).$$

The following important relations in the free Lie ring $\mathcal{L}$ are implied by (2.7):

$$(2.10) \qquad x_1\left\{\begin{matrix} x_2 & \dots & x_i & \dots & x_p \\ 1 & \dots & 1 & \dots & 1 \end{matrix}\right\} = x_i\left\{\begin{matrix} x_2 & \dots & x_1 & \dots & x_p \\ 1 & \dots & 1 & \dots & 1 \end{matrix}\right\}.$$

(2.11) $$y\left\{\begin{matrix} x_1 & x_2 & \dots & x_p \\ 1 & 1 & \dots & 1 \end{matrix}\right\} = -x_1\left\{\begin{matrix} x_2 & \dots & x_p \\ 1 & \dots & 1 \end{matrix}\right\}y \quad .$$

(Again $x_1\left\{\begin{matrix} x_2 & \dots & x_i & \dots & x_p \\ 1 & \dots & 1 & \dots & 1 \end{matrix}\right\}$ denotes $\sum x_1 x_{j_2} \dots x_{j_i} \dots x_{j_p}$

where the summation is taken over all permutations

$j_2, \dots, j_i, \dots, j_p$ of $2, \dots, i, \dots, p$ and $x_1\left\{\begin{matrix} x_2 & \dots & x_p \\ 1 & \dots & 1 \end{matrix}\right\}y$

denotes $\sum x_1 x_{j_2} \dots x_{j_p} y$ with the same convention on $\sum$

as above.)

Proof of (2.11).

$$y\left\{\begin{matrix} x_1 & x_2 & \dots & x_p \\ 1 & 1 & \dots & 1 \end{matrix}\right\} = y\left\{\begin{matrix} X_1 & X_2 & \dots & X_p \\ 1 & 1 & \dots & 1 \end{matrix}\right\}$$

$$= y\left[X_1\left\{\begin{matrix} X_2 & \dots & X_p \\ 1 & \dots & 1 \end{matrix}\right\}\right] = y\left(x_1\left\{\begin{matrix} x_2 & \dots & x_p \\ 1 & \dots & 1 \end{matrix}\right\}\right)$$

$$= -x_1\left\{\begin{matrix} x_2 & \dots & x_p \\ 1 & \dots & 1 \end{matrix}\right\}y \quad .$$

Again in $\mathfrak{V}$, using the following identity:

(2.12) $$Y_1Y_2\dots Y_nZ - ZY_1Y_2\dots Y_n$$

$$= [Y_1Z]Y_2\dots Y_n + Y_1[Y_2Z]\dots Y_n + \dots$$

$$+ Y_1Y_2\dots[Y_nZ],$$

we can establish

(2.13) $$\left\{\begin{matrix} Y_1 & Y_2 & \dots & Y_n \\ 1 & 1 & \dots & 1 \end{matrix}\right\}Z - Z\left\{\begin{matrix} Y_1 & Y_2 & \dots & Y_n \\ 1 & 1 & \dots & 1 \end{matrix}\right\}$$

$$= \left\{\begin{matrix} [Y_1Z] & Y_2 & \dots & Y_n \\ 1 & 1 & \dots & 1 \end{matrix}\right\} + \left\{\begin{matrix} Y_1 & [Y_2Z] & \dots & Y_n \\ 1 & 1 & \dots & 1 \end{matrix}\right\}$$

$$+ \dots + \left\{\begin{matrix} Y_1 & Y_2 & \dots & [Y_nZ] \\ 1 & 1 & \dots & 1 \end{matrix}\right\} .$$

3. The Engel ideal $\mathcal{J}^q$. The Lie ideal in $\mathcal{L}^q$ generated by all elements of the form xy^{p-1} will be called the Engel ideal of $\mathcal{L}^q$ of exponent p-1 or simply the Engel ideal of $\mathcal{L}^q$, since we shall be dealing with only fixed exponent p-1, and will be denoted by $\mathcal{J}^q$ or $\mathcal{J}$.

In order to avoid confusion, we shall say that a module is spanned by a subset of elements of a ring if every elements of the module can be written as a (finite) linear combination of elements of the subset.

Let $\mathcal{R}$ denote the submodule of $\mathcal{A}$ spanned by all elements of the form Y^{p-1}, $Y \in \mathcal{D}$. Then using the notations defined in (1.2.4), $\mathcal{J}$ is the ideal of $\mathcal{L}$ generated by all elements of the form xZ, $x \in \mathcal{L}$, $Z \in \mathcal{R}$, or $\mathcal{J}$ is the submodule of $\mathcal{L}$ spanned by all elements of the form xZD, $x \in \mathcal{L}$, $Z \in \mathcal{R}$, and D is either the identity mapping E or an element of $\mathcal{A}$.

By (2.3) if $Y_1, Y_2, \ldots, Y_{p-1} \in \mathcal{D}$, then $\{Y_1 Y_2 \ldots Y_{p-1}/1\ 1 \ldots 1\} \in \mathcal{R}$. Using this fact, we shall prove the following theorem.

Theorem 3.1. The ideal $\mathcal{J}$ is the submodule of $\mathcal{L}$ spanned by all elements of the form xy^{p-1}.

Proof. Consider an element $xy^{p-1}z \in \mathcal{J}$. Then

$$xy^{p-1}z = -z(xy^{p-1}) = -z[XY^{p-1}]$$

$$= -z\begin{Bmatrix} X & Y \\ 1 & p-1 \end{Bmatrix} \qquad \text{(by (2.6))}$$

$$= -zXY^{p-1} - zY\begin{Bmatrix} X & Y \\ 1 & p-2 \end{Bmatrix} \qquad \text{(by (2.2))}$$

$$= -(zx)Y^{p-1} - (zy)\begin{Bmatrix} X & Y \\ 1 & p-2 \end{Bmatrix}.$$

But $Y^{p-1} \in \mathfrak{K}$ and $\begin{Bmatrix} X & Y \\ 1 & p-2 \end{Bmatrix} \in \mathfrak{K}$, so that $xy^{p-1}z$ is a linear combination of elements of the form uv^{p-1}, $u, v \in \mathcal{L}$.

In the proof of this theorem, we have used only the fact that $\mathcal{L}$ is a Lie ring over a field of characteristic p and the exponent of Engel ideal is p-1. In other words, the proof shows that if $\mathcal{L}$ is any Lie ring over a field of characteristic p then the ideal generated by all elements xy^{p-1}, $x, y \in \mathcal{L}$ is the module spanned by all elements xy^{p-1}. However, this is not true in general. (A counter example is easily constructed.)

3.2. The upper bounds j_n^q and $j(n_1, n_2, \ldots, n_q)$. Theorem 3.1 and formula (2.3) show that the ideal $\mathcal{J}$ is the module spanned by all elements of the form $x_1\begin{Bmatrix} x_2 & \cdots & x_p \\ 1 & \cdots & 1 \end{Bmatrix}$, $x_i \in \mathcal{L}$. Since $x_1\begin{Bmatrix} x_2 & \cdots & x_p \\ 1 & \cdots & 1 \end{Bmatrix}$ is a linear form in each component x_i, $i = 1, 2, \ldots, p$, i.e.,

$$x_1\begin{Bmatrix} x_2 & \cdots & x_i + x_i' & \cdots & x_p \\ 1 & \cdots & 1 & \cdots & 1 \end{Bmatrix} = x_1\begin{Bmatrix} x_2 & \cdots & x_i & \cdots & x_p \\ 1 & \cdots & 1 & \cdots & 1 \end{Bmatrix} + x_1\begin{Bmatrix} x_2 & \cdots & x_i' & \cdots & x_p \\ 1 & \cdots & 1 & \cdots & 1 \end{Bmatrix},$$

$\mathcal{J}$ may be spanned by all elements of the form $x_1\begin{Bmatrix} x_2 & \cdots & x_p \\ 1 & \cdots & 1 \end{Bmatrix}$ where each x_i is basis element of $\mathcal{L}$.

Let $\mathcal{J}_n^q = \mathcal{J}^q \cap \mathcal{L}_n^q$ and $\mathcal{J}(n_1, n_2, \ldots, n_q) = \mathcal{J}^q \cap \mathcal{L}(n_1, n_2, \ldots, n_q)$. The ranks of the modules $\mathcal{J}_n^q$ and $\mathcal{J}(n_1, n_2, \ldots, n_q)$ will be denoted by i_n^q and $i(n_1, n_2, \ldots, n_q)$ respectively. We give upper bounds of i_n^q and $i(n_1, n_2, \ldots, n_q)$ as follows.

It is known (cf. M. Hall [5]) a basis of exists such that every basis element is a homogeneous expression in the generators $a_1, a_2, \ldots, a_q$ of $\mathcal{L}$. Let $u_1, u_2, \ldots$ be such a basis, and let $x_1, x_2, \ldots, x_p$ be selected from among these basis elements (repetitions allowed) such that the sum of the degrees of $x_1, x_2, \ldots, x_p$ in the generators $a_1, a_2, \ldots, a_q$ is equal to n. Denote by j_n^q the number of ways in which such a selection

may be made. Then by the above argument and (2.10), $\mathfrak{J}_n^q$ is spanned by j_n^q elements of the form $x_1\left\{\begin{matrix} x_2 & \dots & x_p \\ 1 & \dots & 1 \end{matrix}\right\}$, and hence

$$i_n^q \leq j_n^q$$

for all n.

Using Witt's formula (1.2), j_n^q may be given as follows. Let

$$T = \prod_{\nu=1}^{\infty} (1 - t_\nu)^{-f_\nu^q}, \tag{3.2.1}$$

where $t_1, t_2, \dots$ are commutative indeterminates. Then j_n^q is the sum of the coefficients of all terms $t_{\nu_1}^{\lambda_1} t_{\nu_2}^{\lambda_2} \dots t_{\nu_k}^{\lambda_k}$ in the formal expression of T as a power series, such that

$$\lambda_1 + \lambda_2 + \dots + \lambda_k = p,$$

$$\nu_1\lambda_1 + \nu_2\lambda_2 + \dots + \nu_k\lambda_k = n.$$

In particular,

$$i_n^q = j_n^q = 0 \qquad (1 \leq n \leq p-1). \tag{3.2.2}$$

In case $n = p$, j_n^q is the number of combinations of the generators of $\mathfrak{L}^q$; $a_1, a_2, \dots, a_q$ taken p at a time allowing repetitions. Among these combinations there are q which involve just one generator a_i taken p times, $i = 1, 2, \dots, q$, these correspond to the elements $a_i\{a_i\ a_i \dots a_i / 1\ 1 \dots 1\} = 0$. On the other hand, each of the remaining combinations corresponds to an element $a_{i_1}\{a_{i_2}\ a_{i_3} \dots a_{i_p} / 1\ 1 \dots 1\} \neq 0$ and and each submodule $\mathfrak{J}(n_1, n_2, \dots, n_q)$, $n_1 + n_2 + \dots + n_q = p$,

of $\mathcal{J}_p^q$ is spanned by one and only one of these elements. Therefore they are linearly independent and we have

$$(3.2.3)_0 \qquad i_p^q = j_p^q - q = \binom{f_1^q+p-1}{p} - q = \binom{q+p-1}{p} - q.$$

This gives an explicit expression of the rank of $\mathcal{J}_p^q$.

We may easily evaluate the next few j_{p+i}^q. In case n = p+1, there is only one choice of the term $t_{\nu_1}^{\lambda_1} t_{\nu_2}^{\lambda_2} \cdots t_{\nu_\kappa}^{\lambda_\kappa} = t_2 t_1^{p-1}$, and we have

$$(3.2.3)_1 \qquad j_{p+1}^q = f_2^q \binom{f_1^q+p-2}{p-1} = \frac{1}{2}(q^2-q)\binom{q+p-2}{p-1}.$$

In case n = p+2, there are two terms; $t_3 t_1^{p-1}$ and $t_2^2 t_1^{p-2}$ which satisfy the required condition, and

$$(3.2.3)_2 \qquad j_{p+2}^q = f_3^q \binom{f_1^q+p-2}{p-1} + \binom{f_2^q+1}{2}\binom{f_1^q+p-3}{p-2}$$

$$= \frac{1}{3}(q^3-q)\binom{q+p-2}{p-1} + \frac{1}{8}(q^2-q)(q^2-q+2)\binom{q+p-3}{p-2}.$$

Similarly, j_{p+3}^q is the sum of the coefficients of the terms $t_4 t_1^{p-1}$, $t_3 t_2 t_1^{p-2}$ and $t_2^3 t_1^{p-3}$. Thus we obtain

$$(3.2.3)_3 \qquad j_{p+3}^q = f_4^q \binom{f_1^q+p-2}{p-1} + f_3^q f_2^q \binom{f_1^q+p-3}{p-2} + \binom{f_2^q+1}{3}\binom{f_1^q+p-4}{p-3}$$

$$= \frac{1}{4}(q^4-q^2)\binom{q+p-2}{p-1} + \frac{1}{6}(q^3-q)(q^2-q)\binom{q+p-3}{p-2}$$

$$+ \frac{1}{48}(q^2-q)(q^2-q+2)(q^2-q+4)\binom{q+p-4}{p-3}$$

Next, j_{p+4}^q is the sum of the coefficients of the terms $t_5 t_1^{p-1}$, $t_4 t_2 t_1^{p-2}$, $t_3^2 t_1^{p-2}$, $t_3 t_2^2 t_1^{p-3}$ and $t_2^4 t_1^{p-4}$, and we have

$$(3.2.3)_4 \quad j^q_{p+4} = f^q_5\binom{f^q_1+p-2}{p-1} + f^q_4 f^q_2\binom{f^q_1+p-3}{p-2} + \binom{f^q_3+1}{2}\binom{f^q_1+p-3}{p-2}$$

$$+ f^q_3\binom{f^q_2+1}{2}\binom{f^q_1+p-4}{p-3} + \binom{f^q_2+3}{4}\binom{f^q_1+p-5}{p-4}$$

$$= \frac{1}{5}(q^5-q)\binom{q+p-2}{p-1} + \frac{1}{8}(q^4-q^2)(q^2-q)\binom{q+p-3}{p-2}$$

$$+ \frac{1}{18}(q^3-q)(q^3-q+3)\binom{q+p-3}{p-2}$$

$$+ \frac{1}{24}(q^3-q)(q^2-q)(q^2-q+2)\binom{q+p-4}{p-3}$$

$$+ \frac{1}{384}(q^2-q)(q^2-q+2)(q^2-q+4)(q^2-q+6)\binom{q+p-5}{p-4}.$$

An upper bound $j(n_1,n_2,\ldots,n_q)$ for $i(n_1,n_2,\ldots,n_q)$ may be obtained by a similar method. Let

$$(3.2.4) \quad T' = \prod(1 - t(\nu_1,\nu_2,\ldots,\nu_q))^{-f(\nu_1,\nu_2,\ldots,\nu_q)},$$

where $t(\nu_1,\nu_2,\ldots,\nu_q)$ are commutative indeterminates and the product is taken over all q-tuples of non-negative integers $\nu_1, \nu_2,\ldots, \nu_q$. Define $j(n_1,n_2,\ldots,n_q)$ to be the sum of the coefficients of all terms $t(\nu_{11},\nu_{12},\ldots,\nu_{1q})^{\lambda_1}\ldots t(\nu_{k1},\nu_{k2},\ldots,\nu_{kq})^{\lambda_k}$ of T' such that

$$\lambda_1 + \lambda_2 + \ldots + \lambda_k = p,$$

$$\lambda_1\nu_{11} + \lambda_2\nu_{21} + \ldots + \lambda_k\nu_{k1} = n_1,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\lambda_1\nu_{1q} + \lambda_2\nu_{2q} + \ldots + \lambda_k\nu_{kq} = n_k,$$

then we have

(3.2.5) $\quad i(n_1,n_2,\ldots,n_q) \leq j(n_1,n_2,\ldots,n_q).$

It is noteworthy that, if $r > p-1$, then

(3.2.6) $\quad j(r+p-2,2,0,\ldots,0) > f(r+p-2,2,0,\ldots,0).$

By the definition, $j(r+p-2,2,0,\ldots,0)$ is the number of elements which are either of the form $x_1\begin{Bmatrix} x_2 & a_1 & \cdots & a_1 \\ 1 & 1 & \cdots & 1 \end{Bmatrix}$ or of the form $x_3\begin{Bmatrix} a_1 & a_1 & \cdots & a_1 \\ 1 & 1 & \cdots & 1 \end{Bmatrix}$, where x_1 and x_2 are basis elements of $\mathfrak{L}(m_1,1,0,\ldots,0)$ and $\mathfrak{L}(m_2,1,0,\ldots,0)$ respectively and $m_1 + m_2 = r$, and x_3 is a basis element of $\mathfrak{L}(r-1,2,0,\ldots,0)$. The number of elements of the first form is $[\frac{r+2}{2}]$ (the number of partitions of r into not more than two parts), and the number of elements of the second form is $f(r-1,2,0,\ldots,0) = [\frac{r}{2}]$. Hence

$$j(r+p-2,2,0,\ldots,0) = [\tfrac{r+2}{2}] + [\tfrac{r}{2}]$$

$$= r + 1 \quad \text{or} \quad r,$$

according as $r \equiv 0$ or $1 \pmod 2$. On the other hand,

$$f(r+p-2,2,0,\ldots,0) = [\tfrac{r+p-1}{2}] .$$

Thus we have proved (3.2.6).

Since $i(n_1,n_2,\ldots,n_q) \leq f(n_1,n_2,\ldots,n_q)$, we have

$$i(r+p-2,2,0,\ldots,0) < j(r+p-2,2,0,\ldots,0)$$

if $r \geq p-1$. This relation implies

(3.2.7) $\quad i_n^q < j_n^q \qquad (n \geq 2p-1)$

4. The ideal $\mathcal{J}^2$. In this section we shall be dealing with only $\mathcal{L}^2$, $\mathcal{J}^2$, and $\mathcal{E}^2$. The generators of $\mathcal{L}^2$ will be denoted by a and b. Thus $\mathcal{L}(m,n)$ will denote the submodule of $\mathcal{L}^2$ consisting of all linear combinations of homogeneous monomials in a and in b with degree m in a and n in b. Similarly $\mathcal{J}(m,n) = \mathcal{L}(m,n) \cap \mathcal{J}^2$, and f(m,n) and i(m,n) will be the ranks of $\mathcal{L}(m,n)$ and $\mathcal{J}(m,n)$ respectively.

4.1. Normal basis of $\mathcal{L}(m,n)$. By (1.1) every element of $\mathcal{L}(m,n)$ may be written as a linear combination of normal products in a and b, and the $\binom{m+n}{n}$ normal products consisting of m a and n b multiplied together in all possible orders span the module $\mathcal{L}(m,n)$. We introduce a linear order in this set of normal products as follows:

(4.1.1) $$xaD < ybD,$$

for any x, y and D, where D is either E or any product of the inner derivations A and B. for example, $ba < ab$, $babab < ba^2b^2$. This is a lexicographic ordering from right to left.

Let

(4.1.2) $$x_1 < x_2 < \ldots < x_i$$

be all the elements of the $\binom{m+n}{n}$ normal products, with the order defined as above, in ascending order. Let i_1 be the smallest integer such that x_{i_1} is a non-zero element in (4.1.2), and i_2 be the smallest integer

such that x_{i_2} does not depend linearly on x_{i_1}. (Clearly $i_1 < i_2$.) In general, let $i_1, i_2, \ldots, i_k$ be such that $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$ are linearly independent elements and every x_k, $i_h \leq j < i_{h+1} \leq i_k$, is linearly dependent on $x_{i_1}, \ldots, x_{i_k}$. Then we define i_{k+1} to be the smallest integer such that $x_{i_{k+1}}$ does not depend linearly on $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$. It is clear that i_{k+1} is defined uniquely by the ordering (4.1.1) in the sequence (4.1.2) in each step. There will be $f(m,n)$ of x_{i_k} which form a basis of the module $\mathfrak{L}(m,n)$. We shall call these basis elements x_{i_k} the normal basis of $\mathfrak{L}(m,n)$, and the expression for an element x of $\mathfrak{L}^2$ as a linear combination of normal basis elements will be called the normal form of x.

Lemma 4.1. Let $y_1 < y_2 < \ldots < y_s$, $s = f(m-1,n)$, and $z_1 < z_2 < \ldots < z_t$, $t = f(m,n-1)$, be normal bases of $\mathfrak{L}(m-1,n)$ and $\mathfrak{L}(m,n-1)$ respectively. Then the elements $y_1a < y_2a < \ldots < y_sa$ are the first $f(m-1,n)$ elements of the normal basis of $\mathfrak{L}(m,n)$. The rest of the normal basis of $\mathfrak{L}(m,n)$ consists of elements of the form $z_1'b < z_2'b < \ldots < z_r'b$ where $r = f(m,n) - f(m-1,n)$ and the sequence $z_1' < z_2' < \ldots < z_r'$ is a subsequence of $z_1 < z_2 < \ldots < z_t$.

Proof. A normal basis element of $\mathfrak{L}(m,n)$ has either the form ya or the form zb. We will show first that $y_1a, y_2a, \ldots, y_sa$ comprise all the normal

basis elements of $\mathcal{L}(m,n)$ of the form ya. For if y'a is a normal basis element of $\mathcal{L}(m,n)$ then $y' = y_i$ for some i, $1 \leq i \leq s$, since otherwise $y' = \sum y_j$ where $y_j < y'$ and therefore $y'a = \sum y_j a$ and $y_j a < y'a$ which says that y'a cannot be a normal basis element. Moreover, $y_1 a, y_2 a, \ldots, y_s a$ are linearly independent, because otherwise we could have a relation,

$$\lambda_1 y_1 a + \lambda_2 y_2 a + \ldots + \lambda_s y_s a = 0 \qquad (\lambda_i \varepsilon GF(p)),$$

or,

$$(\lambda_1 y_1 + \lambda_2 y_2 + \ldots + \lambda_s y_s)a = 0.$$

This implies that $\lambda_1 y_1 + \lambda_2 y_2 + \ldots + \lambda_s y_s$ is either zero or a, both of which contradict the assumption.

Similarly, we may show that a normal basis element of the form zb is of the form $z_i b$ for some i, $1 \leq i \leq t$.

We shall denote the set of all the normal basis elements of $\mathcal{L}(m,n)$ by U(m,n) and the set of all normal basis elements of $\mathcal{L}(m,n)$ of the form zb by V(m,n). The number of elements of the set V(m,n) is f(m,n) - f(m-1,n) and will be denoted by $\varphi(m,n)$.

Obviously, the normal bases of $\mathcal{L}(1,0)$, $\mathcal{L}(0,1)$, $\mathcal{L}(1,1)$, $\mathcal{L}(2,1)$ and $\mathcal{L}(1,2)$ consist of the single element a, b, ba, ba^2 and bab respectively. We may give explicit forms for the elements of U(k,1), U(k,2) and U(k,3) for all k.

Obviously U(k,1) consists of one element ba^k. By formula (1.3),

$$\varphi(k,2) = f(k,2) - f(k-1,2) = 0 \qquad k \equiv 0 \pmod 2,$$

$$\varphi(k,2) = 1 \qquad k \equiv 0 \pmod 2,$$

$V(k,2)$ is vacuous if k is even and $V(k,2)$ consists of one element ba^kb if k is odd. Therefore $U(k,2)$ consists of the $[\frac{k+1}{2}]$ elements of the form ba^jba^{k-j}, $j = 1, 3, \ldots$.

Indeed, we may prove that ba^jba^{k-j}, where j is even, is linearly dependent on smaller elements. For

$$\begin{aligned} 0 &= ba^n(ba^n) \\ &= ba^n[BA^n] \\ &= ba^nBA^n - \binom{n}{1}ba^nABA^{n-1} + \ldots + (-1)^n ba^nA^nB \\ &= ba^nba^n - \binom{n}{1}ba^{n+1}ba^{n-1} + \ldots + (-1)^n ba^{2n}b. \end{aligned}$$

or,

$$ba^{2n}b = \binom{n}{1}ba^{2n-1}ba - \ldots + (-1)^{n-1}ba^nba^n,$$

and all the elements on the right are smaller, in the ordering (4.1.1), than the element on the left.

Again, by (1.3), we have $\varphi(k,3) = [\frac{k+2}{3}]$. We shall show that $V(k,3)$ consists of the first $\varphi(k,3)$ elements in the ordered set of elements y_jb, $y_j \in U(k,2)$.

Consider the $[\frac{k+2}{3}] + 1$ st element of $U(k,2)$. It has the form ba^mba^n where $m = 2[\frac{k+2}{3}] + 1$, $n = k - m$ and $m \geq 2n+3$, for $m - 2n - 3 = 6([\frac{k+2}{3}] - \frac{k}{3}) \geq 0$. Therefore every element of the ordered set $U(k,2)$ which is greater than the $[\frac{k+2}{3}]$th element has the form ba^mba^n, $m \geq 2n+3$. Now for an element ba^mba^nb, $m \geq 2n+3$, let $m = n+1+r$, $r > n+1$, and consider the relation:

$$ba^r(ba^{n+1})(ba^n) = -ba^n((ba^r)(ba^{n+1})).$$

We may rewrite this in the form

$$ba^r[BA^{n+1}][BA^n] = -ba^n[BA^r][BA^{n+1}] + ba^n[BA^{n+1}][BA^r].$$

and if we again write this last identity in terms of normal products in a and b, the largest element of the left side is $(-1)^{2n+1}ba^mba^nb$ and all the elements on the right are smaller than ba^mba^nb. Therefore we have shown that ba^mba^nb, $m \geq 2n+3$ is linearly dependent on smaller elements, i.e., ba^mba^nb, $m \geq 2n+3$ is not contained in $V(k,3)$. Therefore $U(k,3)$ consists of elements of the form $ba^mba^nba^r$ where m is odd, $m < 2n+3$ and $m+n+r = k$.

It is rather an unfortunate fact that we cannot continue this method of constructing $V(k,h)$ by taking the first $\varphi(k,h)$ elements from y_jb, $y_j \in U(k,h-1)$. The first and the simplest counter example occurs in the construction of $V(10,4)$ where $baba^8bab > ba^5ba^3ba^2b$ but $ba^5ba^3ba^2b \notin V(10,4)$ and yet $baba^8bab \in V(10,4)$.

4.2. The set Γ. For a given set Σ of elements of a (Lie or associative) ring, the symbol $M(\Sigma)$ will denote the submodule of the ring spanned by Σ. In order to avoid confusion, we shall use the symbol $\varepsilon(x_i)$ for the set consisting of the elements x_i, instead of more usual notation $\{x_i\}$.

In the previous section we have shown that $\mathcal{J}^2 = M(\Lambda)$, $\Lambda = \varepsilon\left(x_1\left\{\begin{matrix} x_2 & \cdots & x_p \\ 1 & \cdots & 1 \end{matrix}\right)\right| x_i \in U(m_i,n_i)$ for some m_i and n_i). We have used theorem 3.1, which

asserts that an element of the form $y_1\{y_2 \dots y_p/1 \dots 1\}z$ may always be written as a sum of elements of the form $x_1\{x_2 \dots x_p/1 \dots 1\}$. The main purpose of this section is to establish another set Γ such that $M(\Gamma) = \mathcal{J}^2$ by using a method which could be described as "opposite" to the earlier one.

Theorem 4.2. Let $\Gamma = \varepsilon\left(x_1\begin{Bmatrix} x_2 & \dots & x_p \\ 1 & \dots & 1 \end{Bmatrix}^D\right)$

where

(i) each x_i is either the generator a or b of $\mathcal{L}^2$ or a normal basis element of $\mathcal{L}^2$ of the form xb, i.e. an element of the set $V(m_i,n_i)$ for some m_i and n_i,

(ii) if $x_1\{x_2 \dots x_p/1 \dots 1\} = b\{a \dots a/1 \dots 1\}$ then either D = E or a product in A and B, while if $x_1\{x_2 \dots x_p/1 \dots 1\} \neq b\{a \dots a/1 \dots 1\}$ then either D = E or D = BD', where, again, D' = E or a product in A and B.

Then $M(\Gamma) = \mathcal{J}^2$.

The proof of the theorem will be divided into two parts. In part I, we shall prove that the set $\Gamma' = \varepsilon(x_1\{x_2 \dots x_p/1 \dots 1\}D)$ spans $\mathcal{J}^2$, where the x_i satisfy condition (i) and D = E or D is a product in A and B. For convenience, we shall denote the set consisting of E and products in A and B by Ω. Thus $D \in \Omega$. In part II, we shall prove that $M(\Gamma') \subseteq M(\Gamma)$, i.e., $M(\Gamma') = M(\Gamma)$.

Proof, Part I. Let $\Gamma^* = \varepsilon\left(x_1\left\{\begin{matrix} x_2 & \cdots & x_p \\ 1 & \cdots & 1 \end{matrix}\right\}D\right)$ where each x_i is a normal basis element of $\mathcal{L}^2$ and $D \varepsilon \Omega$. Obviously $M(\Gamma^*) = \mathfrak{J}^2$.

Suppose that the set of p elements $x_1, x_2, \ldots, x_p$ consists of i_1 elements y_1, i_2 elements y_2, ..., i_k elements y_k, $i_1 + i_2 + \ldots + i_k = p$, then

$$(4.2.1) \qquad x_1\left\{\begin{matrix} x_2 & \cdots & x_p \\ 1 & \cdots & 1 \end{matrix}\right\} = \lambda y_1\left\{\begin{matrix} y_1 & y_2 & \cdots & y_k \\ i_1-1 & i_2 & \cdots & i_k \end{matrix}\right\},$$

$$(\lambda \varepsilon GF(p),\ \lambda \neq 0),$$

by (2.10) and (2.1). We shall say the elements

$x_1\left\{\begin{matrix} x_2 & \cdots & x_p \\ 1 & \cdots & 1 \end{matrix}\right\}$ and $y_1\left\{\begin{matrix} y_1 & y_2 & \cdots & y_k \\ i_1-1 & i_2 & \cdots & i_k \end{matrix}\right\}$ are <u>equivalent</u>.

Thus by (4.2.1) if $\sum$ is a set of elements of the form $x_1\{x_2 \ldots x_p/1 \ldots 1\}D$ and $\sum'$ is a set obtained by replacing any element of $\sum$ by an equivalent one then $M(\sum) = M(\sum')$. In what follows, therefore, we may replace an element $x_1\{x_2 \ldots x_p/1 \ldots 1\}D$ of Γ^* by an equivalent element $y_1\left\{\begin{matrix} y_1 & y_2 & \cdots & y_k \\ i_1-1 & i_2 & \cdots & i_k \end{matrix}\right\}D$ without loss of generality.

We shall divide Γ^* into subsets $\Gamma(i,j;m,n)$ defined as follows:

$$\Gamma(i,j;m,n) = \varepsilon\left(y_1 a\left\{\begin{matrix} y_2 a & \cdots & y_i a & z_1 b & \cdots & z_j b & a & b \\ 1 & \cdots & 1 & 1 & \cdots & 1 & m & n \end{matrix}\right\}D\right)$$

$$(i \geq 1),$$

$$\Gamma(0,j;m,n) = \varepsilon\left(z_1 b\left\{\begin{matrix} z_2 b & \cdots & z_j b & a & b \\ 1 & \cdots & 1 & m & n \end{matrix}\right\}D\right) \qquad (j \geq 1),$$

$$\Gamma(0,0;m,n) = \varepsilon\left(a\left\{\begin{matrix} a & b \\ m-1 & n \end{matrix}\right\}^D\right) = \varepsilon\left(b\left\{\begin{matrix} a & b \\ m & n-1 \end{matrix}\right\}^D\right) \quad (m,\ n \geq 1),$$

$$\Gamma(0,0;0,p) = \Gamma(0,0;p,0).$$

Then we have

$$\Gamma^* = \bigcup_{i,j,m,n} \Gamma(i,j;m,n),$$

where $\bigcup_{i,j,m,n}$ denotes the union taken for all non-negative integers i, j, m and n with the relation $i + j + m + n = p$. Define

$$\Gamma' = \bigcup_{j,m,n} \Gamma'(0,j;m,n).$$

We shall now prove that,

(4.2.2) $$M(\Gamma^*) = M(\Gamma').$$

Consider a typical element of $\Gamma(i,j;m,n)$;

$$y_1 a\left\{\begin{matrix} y_2 a & \cdots & y_i a & z_1 b & \cdots & z_j b & a & b \\ 1 & \cdots & 1 & 1 & \cdots & 1 & m & n \end{matrix}\right\}^D \qquad (i \geq 1).$$

Then by (2.2)

(4.2.3)
$$y_1 a\left\{\begin{matrix} y_2 a & \cdots & y_i a & z_1 b & \cdots & z_j b & a & b \\ 1 & \cdots & 1 & 1 & \cdots & 1 & m & n \end{matrix}\right\}$$

$$= y_1\left\{\begin{matrix} y_2 a & \cdots & y_i a & z_1 b & \cdots & z_j b & a & b \\ 1 & \cdots & 1 & 1 & \cdots & 1 & m+1 & n \end{matrix}\right\}$$

$$- y_1(y_2 a)\left\{\begin{matrix} y_2 a & \cdots & y_i a & z_1 b & \cdots & z_j b & a & b \\ 0 & \cdots & 1 & 1 & \cdots & 1 & m+1 & n \end{matrix}\right\}$$

. . . . .

$$- y_1(y_i a)\left\{\begin{matrix} y_2 a & \cdots & y_i a & z_1 b & \cdots & z_j b & a & b \\ 1 & \cdots & 0 & 1 & \cdots & 1 & m+1 & n \end{matrix}\right\}$$

$$- y_1(z_1 b)\left\{\begin{matrix} y_2 a & \cdots & y_i a & z_1 b & \cdots & z_j b & a & b \\ 1 & \cdots & 1 & 0 & \cdots & 1 & m+1 & n \end{matrix}\right\}$$

. . . . .

$$- y_1(z_j b)\begin{Bmatrix} y_2 a & \dots & y_i a & z_1 b & \dots & z_j b & a & b \\ 1 & \dots & 1 & 1 & \dots & 0 & m+1 & n \end{Bmatrix}$$

$$- y_1 b\begin{Bmatrix} y_2 a & \dots & y_i a & z_1 b & \dots & z_j b & a & b \\ 1 & \dots & 1 & 1 & \dots & 1 & m+1 & n-1 \end{Bmatrix}.$$

Using (2.11), the first element on the right may be written as follows:

(4.2.4)
$$y_1\begin{Bmatrix} y_2 a & \dots & y_i a & z_1 b & \dots & z_j b & a & b \\ 1 & \dots & 1 & 1 & \dots & 1 & m+1 & n \end{Bmatrix}$$

$$= -a\begin{Bmatrix} y_2 a & \dots & y_i a & z_1 b & \dots & z_j b & a & b \\ 1 & \dots & 1 & 1 & \dots & 1 & m & n \end{Bmatrix} Y_1$$

$$\varepsilon\ M(\Gamma(i-1,j;m+1,n)).$$

Writing the elements $y_1(y_2 a),\dots, y_1(y_i a)$, $y_1(z_1 b),\dots, y_1(z_j b)$, $y_1 b$ which appear on the right of (4.2.3) in normal form it may be seen that,

(4.2.5)
$$y_1(y_2 a)\begin{Bmatrix} y_2 a & \dots & y_i a & z_1 b & \dots & z_j b & a & b \\ 0 & \dots & 1 & 1 & \dots & 1 & m+1 & n \end{Bmatrix}$$

$$\varepsilon\ M(\Gamma(i-1,j;m+1,n)) + M(\Gamma(i-2,j+1;m+1,n)),$$

(4.2.6)
$$y_1(z_1 b)\begin{Bmatrix} y_2 a & \dots & y_i a & z_1 b & \dots & z_j b & a & b \\ 1 & \dots & 1 & 0 & \dots & 1 & m+1 & n \end{Bmatrix}$$

$$\varepsilon\ M(\Gamma(i,j-1;m+1,n)) + M(\Gamma(i-1,j;m+1,n)),$$

(4.2.7)
$$y_1 b\begin{Bmatrix} y_2 a & \dots & y_i a & z_1 b & \dots & z_j b & a & b \\ 1 & \dots & 1 & 1 & \dots & 1 & m+1 & n-1 \end{Bmatrix}$$

$$\varepsilon\ M(\Gamma(i,j;m+1,n-1)) + M(\Gamma(i-1,j+1;m+1,n-1)).$$

Hence, we have

(4.2.8)
$$M(\Gamma(i,j;m,n))$$

$$M(\Gamma(i,j-1;m+1,n)) + M(\Gamma(i,j;m+1,n-1))$$

$$+ M(\Gamma(i-1,j;m+1,n)) + M(\Gamma(i-1,j+1;m+1,n-1))$$

$$+ M(\Gamma(i-2,j+1;m+1,n)).$$

In particular,

$$(4.2.9)\quad M(\Gamma(i,0;m,n)) \leq M(\Gamma(i,0;m+1,n-1)) + M(\Gamma(i-1,0;m+1,n)) + M(\Gamma(i-1,1;m+1,n-1)) + M(\Gamma(i-2,1;m+1,n)) \qquad (n \geq 1),$$

$$(4.2.10)\quad M(\Gamma(i,j;m,0)) \leq M(\Gamma(i,j-1;m+1,0)) + M(\Gamma(i-1,j;m+1,0)) + M(\Gamma(i-2,j+1;m+1,0)) \qquad (j \geq 1);$$

$$(4.2.11)\quad M(\Gamma(i,0;m,0)) \leq M(\Gamma(i-1,0;m+1,0)) + M(\Gamma(i-2,1;m+1,0)) \qquad (i \geq 2),$$

and when $i = 1$,

$$(4.2.12)\quad M(\Gamma(1,0;p-1,0)) \leq M(\Gamma(0,1;p-1,0)) + M(\Gamma(0,0;p-1,1)).$$

To establish (4.2.12), we note that if $x = yba^m$, then

$$xa\begin{Bmatrix} a \\ p-1 \end{Bmatrix} = yb\begin{Bmatrix} a \\ p-1 \end{Bmatrix}a^m \in \Gamma(0,1;p-1,0),$$

and if $x = ba^m$, then

$$xa\begin{Bmatrix} a \\ p-1 \end{Bmatrix} = b\begin{Bmatrix} a \\ p-1 \end{Bmatrix}a^m \in \Gamma(0,0;p-1,1).$$

Now suppose $i \geq 1$. Applying (4.2.8) a finite number of times, we obtain

$$(4.2.13)\quad M(\Gamma(i,j;m,n)) \leq \sum_{m',n'} M(\Gamma(i,0;m',n')) + \sum_{j',m'} M(\Gamma(i,j';m',0)) + \sum_{\substack{i'<i \\ j',m',n'}} M(\Gamma(i',j';m',n')).$$

Again applying (4.2.9) for each term $M(\Gamma(i,0;m',n'))$ in the first summation of (4.2.13) if $n' \geq 1$ and applying (4.2.10) for each $M(\Gamma(i,j';m',0))$ of the

second summation, we obtain, in a finite number of steps,

$$(4.2.14)\quad M(\Gamma(i,j;m,n)) \subseteq \sum_{m'} M(\Gamma(i,0;m',0)) + \sum_{\substack{i'<i \\ j';m';n'}} M(\Gamma(i',j';m',n')).$$

Again by (4.2.11) we obtain

$$(4.2.15)\quad M(\Gamma(i,j;m,n)) \subseteq \sum_{\substack{i'<i \\ j';m';n'}} M(\Gamma(i',j';m',n')).$$

These show that

$$M(\Gamma(i,j;m,n)) \subseteq \sum_{j';m';n'} M(\Gamma(0,j';m',n')).$$

Hence we have proved (4.2.2).

Proof, Part II. We shall divide the set

$$\Gamma' = \varepsilon\left(x_1\begin{Bmatrix} x_2 & \dots & x_p \\ 1 & \dots & 1 \end{Bmatrix} D \,\middle|\, \begin{array}{l} x_i = a,\ x_i = b \text{ or } x_i \in V(m_i,n_i), \\ D \in \Omega. \end{array}\right)$$

into subsets according to the degrees of elements in a and b. Let

$$\Gamma(m,n) = \Gamma' \cap \mathfrak{J}(m,n),$$

and define

$$\Gamma(m,n)D = \varepsilon(xD \mid x \in \Gamma(m,n)),$$

where $D \in \Omega$.

By this definition,

$$\Gamma(m-1,n)A \cup \Gamma(m,n-1)B \subseteq \Gamma(m,n).$$

However $\Gamma(m,n)$ may contain elements not belonging to either $\Gamma(m-1,n)A$ or $\Gamma(m,n-1)B$, namely elements of the form $x_1\{x_2 \dots x_p/1 \dots 1\}E$. We shall denote the subset of $\Gamma(m,n)$ of elements of the form $x_1\{x_2 \dots x_p/1 \dots 1\}E$ by $\Delta(m,n)$. Now we have a decomposition of $\Gamma(m,n)$ into mutually disjoint subsets, viz:

$$(4.2.16)\quad \Gamma(m,n) = \Gamma(m-1,n)A \cup \Gamma(m,n-1)B \cup \Delta(m,n).$$

Similarly,

(4.2.17) $$\Gamma(m-1,n)A$$
$$= \Gamma(m-2,n)A^2 \cup \Gamma(m-1,n-1)BA \cup \Delta(m-1,n)A.$$

We shall prove, when $n > 2$, that

(4.2.18) $$M(\Delta(m-1,n)A)$$
$$\subseteq M(\Gamma(m-2,n)A^2 \cup \Gamma(m-1,n-1)BA \cup \Delta(m,n-1)B)$$
$$= M(\Gamma(m-1,n)A \cup \Gamma(m,n-1)B - \Delta(m-1,n)A).$$

We have the following three types of elements of $\Delta(m-1,n)A$:

Type I. $$x_1\begin{Bmatrix} x_2 & \cdots & x_i & a & b \\ 1 & \cdots & 1 & h & k \end{Bmatrix}A,$$

where $x_1, x_2, \ldots, x_i$ are of degree greater than one in a and b, and $i \geq 1$, $h < p-1$.

Type II. $$b\begin{Bmatrix} a & & b \\ m-1 & & n-1 \end{Bmatrix}A \quad (\varepsilon J_{p+1}^2) \qquad (m < p).$$

Type III. $$xa^{p-1}A = yba^p.$$

Using (2.2) we have the following relation, for an element of Type I,

(4.2.19) $$x_1\begin{Bmatrix} x_2 & \cdots & x_i & a & b \\ 1 & \cdots & 1 & h & k \end{Bmatrix}A$$
$$= x_1\begin{Bmatrix} x_2 & \cdots & x_i & a & b \\ 1 & \cdots & 1 & h+1 & k \end{Bmatrix}$$
$$- x_1\begin{Bmatrix} x_2 & \cdots & x_i & a & b \\ 0 & \cdots & 1 & h+1 & k \end{Bmatrix}X_2$$
$$\cdots\cdots$$
$$- x_1\begin{Bmatrix} x_2 & \cdots & x_i & a & b \\ 1 & \cdots & 0 & h+1 & k \end{Bmatrix}X_i$$
$$- x_1\begin{Bmatrix} x_2 & \cdots & x_i & a & b \\ 1 & \cdots & 1 & h+1 & k-1 \end{Bmatrix}B.$$

Moreover, by (2.11), we have, if $i \geq 2$,

$$(4.2.20)\qquad x_1\left\{\begin{matrix} x_2 & \cdots & x_i & a & b \\ 1 & \cdots & 1 & h+1 & k \end{matrix}\right\} = x_2\left\{\begin{matrix} x_3 & \cdots & x_i & a & b \\ 1 & \cdots & 1 & h+1 & k \end{matrix}\right\}X_1 ,$$

and if $i = 1$,

$$(4.2.21)\qquad x_1\left\{\begin{matrix} a & b \\ h+1 & k \end{matrix}\right\} = b\left\{\begin{matrix} a & b \\ h+1 & k-1 \end{matrix}\right\}X_1 .$$

By writing each of $X_1, X_2, \ldots, X_i$ as a linear combination of products in A and B, we can see that every element in the right of (4.2.19) is contained in $M(\Gamma(m-2,n)A^2 \cup \Gamma(m-1,n-1)BA \cup \Gamma(m,n-1)B)$, for $X_j \neq A$, $j = 1, 2, \ldots, i$.

For an element of Type II, we have,

$$b\left\{\begin{matrix} a & b \\ m-1 & n-1 \end{matrix}\right\}a = b\left\{\begin{matrix} a & b \\ m & n-1 \end{matrix}\right\} - b\left\{\begin{matrix} a & b \\ m & n-2 \end{matrix}\right\}b$$

$$= b\left(b\left\{\begin{matrix} a & b \\ m & n-2 \end{matrix}\right\}\right) - b\left\{\begin{matrix} a & b \\ m & n-2 \end{matrix}\right\}b$$

$$= -2b\left\{\begin{matrix} a & b \\ m & n-2 \end{matrix}\right\},$$

and an element of Type III may be written

$$yba^p = y(ba^p) - ya^pb = -ba^py - ya^pb.$$

Thus we have proved (4.2.18).

Using induction on both m and n, we may readily show that

$$M(\Gamma(m,n)) \subseteq M(\Gamma)$$

for all m and n, which implies that

$$M(\Gamma') \subseteq M(\Gamma).$$

This completes the proof of Theorem 4.2.

4.3. The upper bounds $k(m,n)$. Let $k(m,n)$ be the number of elements of $\Gamma(m,n)$. Then by Theorem 4.2,

$$i(m,n) \leq k(m,n). \tag{4.3.1}$$

Now, by (4.2.16), (4.2.17) and (4.2.18), we have

$$\Gamma(m,n) = \Gamma(m-2,n)A^2 \cup \Gamma(m-1,n-1)BA \cup \Gamma(m,n-1)B \cup \Delta(m,n) \qquad (n \geq 2), \tag{4.3.2}$$

which at once implies that,

$$\Gamma(m,n) = \bigcup_{j=0}^{j=m} \Gamma(m-j,n-1)BA^j \cup \Delta(m,n). \tag{4.3.3}$$

Let $h(m,n)$ denote the number of elements of $\Delta(m,n)$. Since the sets $\Gamma(m-j,n-1)BA^j$, $j = 0, 1, \ldots, m$, and $\Delta(m,n)$ are mutually disjoint, we have

$$k(m,n) = \sum_{j=0}^{m} k(m-j,n-1) + h(m,n) \qquad (n \geq 2). \tag{4.3.4}$$

Thus if we know $k(m',n-1)$ for all $m' < m$, the problem of finding $k(m,n)$ will be reduced to that of finding $h(m,n)$.

Since $k(m,n) = 0$ when $m + n \leq p$, we may write (4.3.4) as follows:

$$k(r+p-n,n) = \sum_{j=0}^{r-1} k(j+p-n+1,n-1) + h(r+p-n,n) \qquad (n \geq 2). \tag{4.3.5}$$

In order to find $h(r+p-n,n)$, we shall first consider subsets of $\Delta(r+p-n,n)$ defined as follows. Let $i_1, i_2, \ldots, i_k$, where $i_1 + i_2 + \ldots + i_k = n$ and $i_1 \geq i_2 \geq \ldots \geq i_k \geq 1$ be a partition of n into $k \leq p$ parts, and define

$$\Delta_r(i_1, i_2, \ldots, i_k)$$

$$= \varepsilon\left(x_1\begin{Bmatrix} x_2 & \cdots & x_k & a \\ 1 & \cdots & 1 & p-k \end{Bmatrix} \middle| x_j \in V(m_j,n_j) \text{ for some } m_j\right)$$

$$\subseteq \Delta(r+p-n,n).$$

Note that $i_1, i_2, \ldots, i_k$ denote the degrees of $x_1, x_2, \ldots, x_k$ in b respectively. There is no restriction on the degree of each of the x_j in a except that the sum of degrees of $x_1, x_2, \ldots, x_k$ in a is $r - (i_1 + i_2 + \ldots + i_k) + k = r - n + k$. For a given integer n, the number of different subsets $\Delta_r(i_1,i_2,\ldots,i_k)$ is the number $\pi(n,p)$ of partitions of n into not more than p parts, and therefore does not depend on r. The number $\pi(n,p)$ is well-known and is usually given by the following generating function:

$$(4.3.6) \qquad \sum_{n=0}^{\infty} \pi(n,p)t^n = \prod_{i=1}^{p}(1 - t^i)^{-1}.$$

Denote the number of elements of the set $\Delta_r(i_1,i_2,\ldots,i_k)$ by $h_r(i_1,i_2,\ldots,i_k)$.

Lemma 4.3.1. For $i_k \geq 2$ and $j \leq p - k$,

$$h_r(i_1,i_2,\ldots,i_k,\overbrace{1,1,\ldots,1}^{j})$$

$$= h_r(i_1,i_2,\ldots,i_k).$$

Proof. The mapping of $\Delta_r(i_1,i_2,\ldots,i_k,\overbrace{1,\ldots,1}^{j})$ onto $\Delta_r(i_1,i_2,\ldots,i_k)$ defined by

$$x_1\begin{Bmatrix} x_2 & \cdots & x_k & b & a \\ 1 & \cdots & 1 & j & p-k-j \end{Bmatrix} \longleftrightarrow x_1\begin{Bmatrix} x_2 & \cdots & x_k & a \\ 1 & \cdots & 1 & p-k \end{Bmatrix}$$

gives the required one-to-one correspondence.

Thus the problem of finding $h_r(i_1,i_2,\ldots,i_k)$

with $i_k \geq 1$ is reduced to that of $h_r(i_1,i_2,\ldots,i_k)$ with $i_k \geq 2$. We shall now use a similar method to the one we used for j_n^q and $j(n_1,n_2,\ldots,n_q)$ in section 3, to obtain an expression for $h_r(i_1,i_2,\ldots,i_k)$. Let

$$T'' = \prod_{m,n} (1 - t(m,n))^{-\binom{m,n}{}}, \tag{4.3.7}$$

where the $t(m,n)$ are commutative indeterminates, m is taken over all positive integers and n is taken over all integers greater than 1. Then $h_r(i_1,i_2,\ldots,i_k)$ is the sum of the coefficients of all terms $t(m_1,i_1)t(m_2,i_2)\ldots t(m_k,i_k)$ in the formal power series expansion of T'', such that $m_1+m_2+\ldots+m_k = r-n+k$.

We shall evaluate $k(r+p-n,n)$, $n = 2, 3, 4$. It is clear that,

$$\begin{aligned} \mathcal{J}(r+p-1,1) &= M(\Gamma(r+p-1,1)) \\ &= M(ba^{r+p-1}), \end{aligned}$$

and therefore.

$$i(r+p-1,1) = k(r+p-1,1) = 1. \tag{4.3.8}$$

Similarly,

$$\begin{aligned} \mathcal{J}(p-n,n) &= M(\Gamma(p-n,n)) \\ &= M\left(b \left\{ \begin{matrix} a & b \\ p-n & n-1 \end{matrix} \right\}\right) \qquad (1 \leq n < p), \end{aligned}$$

and we have

$$i(p-n,n) = k(p-n,n) = 1 \qquad (1 \leq n < p). \tag{4.3.9}$$

By (4.3.5) and (4.3.8), we have

$$\begin{aligned} k(r+p-2,2) &= \sum_{j=0}^{r-1} k(j+p-1,1) + h(r+p-2,2) \\ &= r + h(r+p-2,2). \end{aligned}$$

On the otherhand,

$$\Delta(r+p-2,2) = \Delta_r(2) = \varepsilon(xa^{p-1} \mid x \in V(r-1,2)),$$

and therefore,

$$h(r+p-2,2) = h_r(2) = \varphi(r-1,2)$$

$$= 1 \text{ or } 0,$$

according as $r \equiv 0$ or $1 \pmod 2$. Hence,

(4.3.10) $$k(r+p-2,2) = r+1 \quad \text{or} \quad r,$$

according as $r \equiv 0$ or $1 \pmod 2$.

Putting $r = p-3$ we have

(4.3.11) $$k(2p-5,2) = f(2p-5,2) = p - 2.$$

We shall show that

(4.3.12) $$k(r+p-2,2) = i(r+p-2,2) \qquad (0 \leq r \leq p-2),$$

which together with (4.3.11) implies that

$$\mathcal{J}(2p-5,2) = \mathcal{L}(2p-5,2).$$

The proof of (4.3.12) uses the explicit form of normal basis elements of $\mathcal{L}(r+p-2,2)$ obtained in section 4.2. Suppose that r is even. Then $U(r+p-2,2)$ consists of the following elements:

$$baba^{r+p-3} < ba^3ba^{r+p-5} < \ldots < ba^{r+p-2}b.$$

The first $r/2$ elements and the last $r/2$ elements in the sequence are of the form xa^p and ba^py respectively and therefore they are contained in $\mathcal{J}(r+p-2,2)$. Moreover, $\mathcal{J}(r+p-2,2)$ contains the element

$$b\begin{Bmatrix} a & b \\ p-2 & 1 \end{Bmatrix}a^r = ba^{p-2}ba^r + b\begin{Bmatrix} a & b \\ p-3 & 1 \end{Bmatrix}a^{r+1}$$

which does not depend linearly on the r elements of $\mathcal{J}(r+p-2,2)$ obtained previously. Therefore $\mathcal{J}(r+p-2,2)$

contains at least r+1 linearly independent elements of $\mathfrak{L}(r+p-2,2)$, in other words,

$$i(r+p-2,2) \geq r+1,$$

which together with (4.3.1) and (4.3.10) proves (4.3.12). By a similar method we can prove (4.3.12) in case of r is odd.

By (4.3.10), we have

$$\sum_{j=0}^{r-1} k(j+p-2,2) = \frac{r^2}{2} + \alpha_1,$$

where $\alpha_1 = 0$ or $\frac{1}{2}$ according as $r \equiv 0$ or $1 \pmod 2$. The set $\Delta(r+p-3,3)$ consists of the sets $\Delta_r(2,1)$ and $\Delta_r(3)$ and

$$h(r+p-3,3) = h_r(2,1) + h_r(3)$$

$$= h_r(2) + h_r(3).$$

Now,

$$h_r(2) = 1, \quad 0,$$

according as $r \equiv 0, 1 \pmod 2$ and since $\Delta_r(3)$ $= \varepsilon(xa^{p-1} \mid x \in V(r-2,3))$,

$$h(3) = \varphi(r-2,3) = \frac{r}{3} + \alpha_2,$$

where $\alpha_2 = 0, -\frac{1}{3}, -\frac{2}{3}$, according as $r \equiv 0, 1, 2 \pmod 3$. Altogether, by (4.3.5), we have

$$k(r+p-3,3) = \frac{1}{6}(3r^2 + 2r + \alpha), \tag{4.3.13}$$

where $\alpha = 6, 1, 2, 3, 4, -1$ according as $r \equiv 0, 1, 2, 3, 4, 5 \pmod 6$.

This expression (4.3.13) was obtained by Meier-Wunderli [22] in his study on the structure of

the Burnside groups. As we shall see later (Section 6) his result implies that

$$k(r+p-3,3) = i(r+p-3,3) \qquad (r \leq 2p-5),$$

that is, $k(r+p-3,3)$ is not only an upper bound for $i(p+r-3,3)$ but actually equality holds for $r \leq 2p-5$. The author has verified that, for $p = 7$, $i(12,3) = f(12,3) - 1, i(13,3) = f(13,3)$, and for $p > 7$, $i(3p-9,3) = f(3p-9,3)$.

Again, by (4.3.13), we have

$$\sum_{j=0}^{r-1} k(j+p-3,3) = \frac{r^3}{6} - \frac{r^2}{12} + \frac{r}{3} + \frac{\alpha_1}{12},$$

where $\alpha_1 = 0, 7, 4, 3, 4, 7$ according as $r \equiv 0, 1, 2, 3, 4, 5 \pmod 6$. The set $\Delta(r+p-4,4)$ consists of $\Delta_r(2,1,1)$, $\Delta_r(3,1)$, $\Delta_r(4)$ and $\Delta_r(2,2)$, so that

$$h(r+p-4,4) = h_r(2,1,1) + h_r(3,1) + h_r(4) + h_r(2,2)$$
$$= h_r(2) + h_r(3) + h_r(4) + h_r(2,2).$$

Now, $\Delta_r(4) = \varepsilon(xa^{p-1} \mid x \in V(r-3,4))$ and therefore

$$h_r(4) = \varphi(r-3,4) = \frac{r^2}{8} + \beta_2 r + \alpha_2,$$

where $\beta_2 = -\frac{1}{4}$ or $-\frac{1}{2}$, $\alpha_2 = 0$ or $\frac{3}{8}$ according as $r \equiv 0$ or $1 \pmod 2$. Again, $\Delta_r(2,2)$

$$= \varepsilon\left(x_1 \left\{ \begin{matrix} x_2 & a \\ 1 & p-2 \end{matrix} \right\} \;\middle|\; x_1 \in V(m_1,2),\ x_2 \in V(m_2,2),\ m_1 + m_2 = r-2 \right)$$

and therefore,

$$h_r(2,2) = \frac{r}{4}, \ 0, \ \frac{r}{4} - \frac{1}{2}, \ 0,$$

according as $r \equiv 0, 1, 2, 3 \pmod 4$. Altogether, we obtain

$$(4.3.14) \qquad k(r+p-4,4) = \frac{1}{24}(4r^3 + r^2 + \alpha r + \beta),$$

where $\alpha = 16$ or 4 according as $r \equiv 0$ or $1 \pmod 2$,

$\beta = 24, 15, 4, 15, 24, 7, 12, 15, 16, 15, 12, 7$

according as $r \equiv 0, 1, 2, \ldots, 11 \pmod{12}$.

4.4. The upper bound k_r. Let $k_r = \sum_{m+n=r} k(m,n)$. Then k_r is an upper bound for i_r^2. We shall evaluate k_{p+r} for $r = 0, 1, \ldots, 5$ and shall show that for these values of r the upper bounds k_{p+r} are equal respectively to the upper bound j_{p+r}^2 obtained earlier. The author has been unable to prove that $j_{p+r}^2 = k_{p+r}$ in general, although it seems to be true.

First, we note

Lemma 4.4.1.

$$h(p,r) = h(p-1,r+1) = \ldots = h(r,p) \qquad (1 \leq r \leq p-1).$$

Proof. Consider the subset $\Delta_r(i_1, i_2, \ldots, i_k, \overbrace{1,1,\ldots,1}^{j})$, where $i_k \geq 2$, $i_1 + i_2 + \ldots + i_k + j = r + n$, of the set $\Delta(p-n, r+n)$. We shall show that $j \geq n$. Every element of the subset has total degree in a and b at least

$$(i_1+1) + (i_2+1) + \ldots + (i_k+1) + j + (p-k-j) = p+r+n-j$$

for is a non-zero element has the degree $i > 1$ in b then it has total degree at least $i+1$ in a and b. therefore

$$p+r+n-j \leq p+r$$

and thus we have $j \geq n$. This fact shows that $\Delta(p-n,r+n)$ contains only those subsets $\Delta_r(i_1,i_2,\ldots,i_k,1,1,\ldots,1)$ where the number of ones is always not less than n. On the other hand, by Lemma 4.3.1, we have

$$(4.4.1) \qquad h_r(i_1,i_2,\ldots,i_k,\overbrace{1,1,\ldots,1}^{n+n'}) = h_r(i_1,i_2,\ldots,i_k,\overbrace{1,1,\ldots,1}^{n'}),$$

where the right hand side is the number of elements of the subset $\Delta_r(i_1,i_2,\ldots,i_k,\overbrace{1,1,\ldots,1}^{n'})$ of $\Delta(p,r)$. Applying this argument to each subset $\Delta_r(i_1,i_2,\ldots,i_j)$ of $\Delta(p-n,r+n)$, we obtain

$$h(p-n,r+n) = h(p,r).$$

Thus the lemma has been proved.

Lemma 4.4.1, together with the fact $k(p-n,n) = 1$ and the identity (4.3.5), implies

Lemma 4.4.2.

$$k(p,r) = k(p-1,r+1) = \ldots = k(r,p) \qquad (1 \leq r \leq p-1).$$

Using this lemma we can evaluate certain k_{p+r} readily. Let $\delta(k_{p+r})$ denote the sequence

$$k(p+r-1,1),\ k(p+r-2,2),\ \ldots\ ,\ k(1,p+r-1).$$

We know,

$$(4.4.2) \qquad \delta(k_p) = 1,\ 1,\ \ldots,\ 1.$$

$$(4.4.2)' \qquad k_p = p - 1,$$

while $k(p,1) = 1$ implies,

$$(4.4.3) \qquad \delta(k_{p+1}) = 1,\ 1,\ \ldots,\ 1,$$

(4.4.3)' $k_{p+1} = p.$

Again $k(p+1,1) = 1$ and $k(p,2) = 3$ (cf. (4.3.10)) imply,

(4.4.4) $\delta(k_{p+2}) = 1, 3, 3, \ldots, 3, 1,$

(4.4.4)' $k_{p+2} = 3p - 1.$

Similarly, by (4.3.9), (4.3.10) and (4.3.13),

(4.4.5) $\delta(k_{p+3}) = 1, 3, 6, 6, \ldots, 6, 3, 1,$

(4.4.5)' $k_{p+3} = 6p - 4.$

Again, by (4.3.9), (4.3.10), (4.3.13) and (4.3.14),

(4.4.6) $\delta(k_{p+4}) = 1,5,10,15,15,\ldots,15,10,5,1,$

(4.4.6)' $k_{p+4} = 15p - 13.$

Now $\Delta(p,5)$ consists of $\Delta_5(5)$, $\Delta_5(4,1)$, $\Delta_5(3,2)$, $\Delta_5(3,1,1)$, $\Delta_5(2,2,1)$ and $\Delta_5(2,1,1,1)$. Therefore

$$\begin{aligned} h(p,5) &= h_5(5) + h_5(4,1) + h_5(3,2) \\ &\quad + h_5(3,1,1) + h_5(2,2,1) + h_5(2,1,1,1) \\ &= h_5(5) + h_5(4) + h_5(3,2) \\ &\quad + h_5(3) + h_5(2,2) + h_5(2) \\ &= \varphi(1,5) + \varphi(2,4) + \varphi(1,3)\varphi(1,2) \\ &\quad + \varphi(3,3) + \varphi(2,2)\varphi(1,2) + \varphi(4,2) \\ &= 1 + 1 + 1 + 1 + 0 + 0 = 4, \end{aligned}$$

$$k(p,5) = \sum_{j=0}^{4} k(j+p-4,4) + h(p,5) = 30.$$

Thus we have

(4.4.7) $\delta(k_{p+5}) = 1,5,14,23,30,30,\ldots,30,23,14,5,1,$

(4.4.7)' $k_{p+5} = 30p - 34.$

5. Lower bounds for the class of $\mathcal{E}^q$. Let $\mathcal{E}^q$ be the Lie quotient ring $\mathcal{L}^q/\mathcal{J}^q$, i.e. $\mathcal{E}^q$ is isomorphic to the Lie ring over GF(p) generated by $e_1, e_2, \ldots, e_q$ in which the identical relation $xy^{p-1} = 0$ holds for any pair of elements x, y of the ring. If it is necessary to specify the exponent p-1, we shall write $\mathcal{E}^q = \mathcal{E}^q(p)$. The question as to whether or not a finitely generated Engel ring is nilpotent is a well-known unsolved problem, related to the restricted Burnside problem.

The nilpotence of an Engel ring with exponent 1 or 2 is trivial. For the case of exponent 4, Kostrikin [12] proved that $\mathcal{E}^2(5)$ is nilpotent of class 13 and gave a basis of the ring. Higman [9] proved that any finitely generated Engel ring of exponent 4 over a ring of characteristic prime to 6 is nilpotent, but he did not determine the class of nilpotence. Recently, Meier-Wunderli [22] has shown that the Burnside group with prime exponent $p > 3$ cannot be nilpotent of class less than 2p-1, which implies that $\mathcal{E}^q(p)$ cannot be nilpotent of class less than 2p-1. (See also Green [3].) The main purpose of this section is to prove the following

Theorem 5.1. For any positive integer d there exists a positive integer m such that if p is a prime greater than m, then the Engel ring $\mathcal{E}^2(p)$ cannot be nilpotent of class less than dp.

Let $e(r,n) = f(r,n) - i(r,n)$. Then by (4.3.1), $e(r,n) \geq f(r,n) - k(r,n)$. We shall prove

Theorem 5.1 by showing that, for some n, $f(dp-n,n) > k(dp-n,n)$ so that $e(dp-n,n) > 0$.

By Witt's formula (1.3) we may easily establish

Lemma 5.2. For a given integer $n \geq 2$ there exists a polynomial $F_n(r)$ of degree at most n-2 in r such that

$$f(r,n) \geq \frac{1}{n!} r^{n-1} + F_n(r) \tag{5.1}$$

for all positive integers r, and there exists another polynomial $\Phi_n(r)$ of degree at most n-2 in r with non-negative coefficients such that

$$\varphi(r,n) \leq \Phi_n(r) \tag{5.2}$$

for all positive integers r.

Since $\Phi_n(r)$ has non-negative coefficients, it is clear that

$$\Phi_n(r) \leq \Phi_n(r+1). \tag{5.3}$$

Using (5.2) and (5.3) we shall prove

Lemma 5.3. For a given integer $n \geq 2$ there exists a polynomial $H_n(r)$ of degree at most n-2 in r such that

$$h(r+p-n,n) \leq H_n(r) \tag{5.4}$$

for all positive integers r and primes p.

Proof. Let $\pi(n)$ be the number of partitions of n, so that

$$\sum_{n=0}^{\infty} \pi(n)t^n = \prod_{i=1}^{\infty} (1 - t^i)^{-1}. \tag{5.5}$$

Clearly $\pi(n) \geq \pi(n,p)$ for all p, which implies that the number of subsets $\Delta_r(i_1, i_2, \ldots, i_r)$, $i_1 + i_2$

$+ \ldots + i_k = n$, $k < p$, of $\Delta(r+p-n,n)$ is not greater than $\pi(n)$ for any prime p. (cf. Section 4.3.) Therefore to prove Lemma 5.3, it is enough to show that for each partition $i_1 \geq i_2 \geq \ldots \geq i_k$ of n there exists a polynomial $H_r(i_1,i_2,\ldots,i_k)$ of degree at most n-2 in r such that

$$h_r(i_1,i_2,\ldots,i_k) \leq H_r(i_1,i_2,\ldots,i_k) \tag{5.6}$$

for all r.

If $k = 1$, $i_1 = n$, then

$$\Delta_r(n) = \varepsilon(xa^{p-1} \mid x \in V(r-n+1,n)),$$

therefore by (5.2)

$$h_r(n) = \varphi(r-n+1,n) \leq \Phi_n(r-n+1). \tag{5.7}$$

If $k \geq 2$ and $i_k \geq 2$, then

$$\Delta_r(i_1,i_2,\ldots,i_k)$$

$$= \varepsilon\left(x_1\begin{Bmatrix} x_2 & \ldots & x_k & a \\ 1 & \ldots & 1 & p-k \end{Bmatrix} \;\middle|\; x_j \in V(m_j,n_j),\ 1 \leq m_j \leq r-n+1\right)$$

However, noting that the maximum of each m_j (the degree of x_j in a) is r-n+1, it follows that the number of all possible choicesoof each $x_j \in V(m_j,n_j)$ in $\Delta_r(i_1,i_2,\ldots,i_k)$ is not greater than

$$\varphi(1,i_j) + \varphi(2,i_j) + \ldots + \varphi(r-n+1,i_j)$$

$$\leq (r-n+1)\Phi_{i_j}(r-n+1) \qquad \text{(by (5.3))}.$$

Therefore if $i_k \geq 2$, then

$$h_r(i_1,i_2,\ldots,i_k) \tag{5.8}$$

$$\leq (r-n+1)^k \Phi_{i_1}(r-n+1)\Phi_{i_2}(r-n+1)\ldots\Phi_{i_k}(r-n+1).$$

Now, the degree in r of the polynomial on the right is

$$k + (i_1-2) + (i_2-2) + \ldots + (i_k-2) = n - k.$$

Finally, if $i_1 \geq \ldots \geq i_j > i_{j+1} = \ldots = i_k = 1$, then by (4.4.1) and above argument,

$$(5.9) \qquad h_r(i_1,i_2,\ldots,i_k) = h_r(i_1,i_2,\ldots,i_k)$$
$$\leq (r-n'+1)^j \Phi_{i_1}(r-n'+1)\Phi_{i_2}(r-n'+1)\ldots\Phi_{i_j}(r-n'+1),$$

where $n' = i_1 + i_2 + \ldots + i_j$ and the degree in r of the polynomial on the right is $j + (i_1-2) + (i_2-2) + \ldots + (i_j-2) = n - k$.

Thus we have obtained the required polynomials $H_r(i_1,i_2,\ldots,i_k)$ and Lemma 5.3 has proved.

Proof of Theorem 5.1. We shall show first, by induction, that for a given integer n there exists a polynomial $K_n(r)$ of degree in r not greater than n-1 such that

$$(5.10) \qquad k(r+p-n,n) \leq \frac{r^{n-1}}{(n-1)!} + K_n(r)$$

for all positive integers r and primes p.

We have already verified (5.10) for n = 1, 2, 3 and 4. Suppose (5.10) holds for all positive integers less than n. Then by (4.3.5) and Lemma 5.3,

$$k(r+p-n,n) = \sum_{j=0}^{r-1} k(j+p-n+1,n-1) + h(r+p-n,n)$$
$$\leq \sum_{j=0}^{r-1} \left(\frac{j^{n-2}}{(n-2)!} + K_{n-1}(j)\right) + H_n(r)$$

$$= \frac{r^{n-1}}{(n-1)!} + K_n'(r) + \sum K_{n-1}(j) + H_n(r).$$

Clearly, $K_n'(r) + \sum K_{n-1}(j) + H_n(r)$ is a polynomial of degree in r not greater than n-2, which completes the induction.

Now, by (5.1) and (5.10)

$$e(r+p-n,n) \geq \frac{1}{n!}(r+p-n)^{n-1} + F_n(r)$$

$$- \frac{1}{(n-1)!} r^{n-1} - K_n(r),$$

Let $r = (d-1)p$, then

$$e(dp-n,n) \geq \frac{1}{n!}(dp-n)^{n-1} + F_n((d-1)p)$$

$$- \frac{1}{(n-1)!}((d-1)p)^{n-1} - K_n((d-1)p)$$

$$= \frac{(d-1)^{n-1}}{n!}((\frac{d}{d-1})^{n-1} - n)p^{n-1} + E_n(p),$$

where $E_n(p)$ is a polynomial of degree in p less than n-1.

For a given integer $d \geq 2$, we may always find an integer n such that

$$(\frac{d}{d-1})^{n-1} - n > 0,$$

and having chosen n satisfying this condition, we may find m such that for any prime $p > m$

$$e(dp-n,n) \geq \frac{(d-1)^{n-1}}{n!}((\frac{d}{d-1})^{n-1} - n)p^{n-1} + E_n(p) > 0.$$

This completes the proof of Theorem 5.1.

6. Burnside's groups. Let $\mathfrak{F}^q$, or simply $\mathfrak{F}$, denote the free group with q generators and let $\mathfrak{F}^q(n)$ or $\mathfrak{F}(n)$ denote the subgroup of $\mathfrak{F}^q$ generated by all elements g^n, $g \in \mathfrak{F}^q$. The subgroup $\mathfrak{F}^q(n)$ is normal and the factor group $\mathfrak{F}^q/\mathfrak{F}^q(n)$ will be called, as usual, the Burnside group of exponent n with q generators, or simply the Burnside group, which we will denote by $\mathfrak{B}^q(n)$, $\mathfrak{B}(n)$ or $\mathfrak{B}$.

Burnside's problem [2] it to prove or disprove the following conjecture:

B_n: Any finitely generated group of exponent n, in the sense that every element g of the group satisfies the relation $g^n = 1$, is finite.

This may be rephrased as:

B_n': $\mathfrak{B}^q(n)$ is a finite group.

The weaker proposition R_n known as the restricted Burnside conjecture is as follows:

R_n: For each q and each n, there exists an upper bound for the orders of all finite groups of exponent n that can be generated by q elements.

When n is a prime p, the proposition R_p can be rephrased in terms of the Burnside group $\mathfrak{B}(p)$. (cf. Baer [1], Hall and Higman [7], Higman [9]) Let $\mathfrak{B}_i$ be the ith term of the lower central series of $\mathfrak{B}(p)$ and $\mathfrak{B}_\infty = \bigcap_{i=1}^{\infty} \mathfrak{B}_i$. When p is a prime, a group satisfying the hypothesis in the proposition R_p is a finite p-group and, as it is well-known,

nilpotent. Therefore such a group is a factor group of $\mathfrak{B}(p)/\mathfrak{B}_r$ for some r, and so of $\mathfrak{B}(p)/\mathfrak{B}_\infty$. Thus we may rephrase R_p as follows:

R_p': $\mathfrak{B}(p)/\mathfrak{B}_\infty$ is a finite group.

If $\mathfrak{B}(p)/\mathfrak{B}_\infty$ is nilpotent, that is, if $\mathfrak{B}_r = \mathfrak{B}_{r+1} = \ldots = \mathfrak{B}_\infty$, for some r, then $\mathfrak{B}(p)/\mathfrak{B}_\infty = \mathfrak{B}(p)/\mathfrak{B}_r$. Since $\mathfrak{B}(p)/\mathfrak{B}_i$ is known to be finite for any i, the nilpotence of $\mathfrak{B}(p)/\mathfrak{B}_\infty$ implies R_p'.

So far, the known results concerning this problem are the following:

B_2 is trivially true. For, a group of exponent 2 is abelian and therefore the order of the group $\mathfrak{B}^q(2)$ is 2^q.

B_3 has been proved by Levi and Van der Waerden [14]. The order of $\mathfrak{B}^q(3)$ is shown to be $3^{\binom{q}{1}+\binom{q}{2}+\binom{q}{3}}$.

B_4 has been proved by Sanov [23].

R_5 has been proved by Kostrikin [12] for $q = 2$ and by Higman [9] for any finite q. However, B_5 is still undecided.

There are also important results of P. Hall and G. Higman [9] on the following still weaker proposition:

S_n: For each q and each n there exists an upper bound for the orders of all solvable groups of exponent n that can be generated by q elements.

It is not our intention to prove or disprove the above propositions, but rather to apply our results on Engel rings to the Burnside groups.

6.1. Connection between the Burnside groups and the Engel rings. We shall briefly review well-known facts about the connection between the factor groups $\mathfrak{B}_n/\mathfrak{B}_{n+1}$ and the submodules $\mathcal{E}_n$ of the Engel ring $\mathcal{E}$. To begin with, we recall Magnus' [16], [17], [18] representation of the free group by formal power series.

Let $\overline{\mathfrak{A}}^q$ (or simply $\overline{\mathfrak{A}}$) be the free associative ring over the ring of integers generated by $\overline{A}_1, \overline{A}_2, \ldots, \overline{A}_q$, and let $\overline{\mathfrak{L}}^q$ (or $\overline{\mathfrak{L}}$) be the free Lie ring over the same ring generated by $\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_q$. As in section 1, $\overline{\mathfrak{J}}^q$ (or $\overline{\mathfrak{J}}$) will denote the Lie ring (over the ring of integers) consisting of linear combinations of the elements $\overline{A}_i$, $i = 1, 2, \ldots, q$, and their Lie products, defined successively by $[XY] = XY - YX$, $X \in \overline{\mathfrak{J}}$, $Y \in \overline{\mathfrak{J}}$. Again, as is well-known [27], $\overline{\mathfrak{L}} \cong \overline{\mathfrak{J}}$, by the mapping $\overline{\delta}$: $\overline{a}_i \longrightarrow \overline{A}_i$ and $xy \longrightarrow [XY]$, where $x \longrightarrow X$, $y \longrightarrow Y$. The symbols $\overline{\mathfrak{A}}_n^q$, $\overline{\mathfrak{L}}_n^q$ and $\overline{\mathfrak{J}}_n^q$ (or simply $\overline{\mathfrak{A}}_n$, $\overline{\mathfrak{L}}_n$ and $\overline{\mathfrak{J}}_n$) denote the submodules of $\overline{\mathfrak{A}}^q$, $\overline{\mathfrak{L}}^q$ and $\overline{\mathfrak{J}}^q$ respectively, consisting of homogeneous elements of degree n in the generators.

Magnus [16] has shown that the formal power series:

$$g_i = 1 + \overline{A}_i,$$

$$g_i^{-1} = 1 - \overline{A}_i + \overline{A}_i^2 - \dots , \qquad (i = 1, \dots, q),$$

generate the free group with q generators. In this section 6.1, we use $\mathfrak{F}^q$ or $\mathfrak{F}$ to denote the free group represented in this way. Each element $G \in \mathfrak{F}$ has the form

$$G = 1 + D_n + D_{n+1} + \dots ,$$

where $D_n \in \overline{\mathfrak{o}}_n$, $D_{n+i} \in \mathfrak{A}_{n+i}$ $i = 1, 2, \dots$, for some n. The nth dimensional subgroup consisting of all elements $1 + D_n + D_{n+1} + \dots , D_n \in \overline{\mathfrak{o}}_n$, is the nth term $\mathfrak{F}_n$ of the lower central series of $\mathfrak{F}$ ([17]). Moreover, the mapping:

$$\psi: \quad G = 1 + D_n + D_{n+1} + \dots \longrightarrow D_n ,$$

$$GG' = (1 + D_n + D_{n+1} + \dots)(1 + D_n' + D_{n+1}' + \dots)$$

$$= 1 + (D_n + D_n') + \dots \longrightarrow D_n + D_n' ,$$

gives a homomorphism of the multiplicative group $\mathfrak{F}_n$ on to the module $\overline{\mathfrak{o}}_n$ where the kernel is $\mathfrak{F}_{n+1}$, i.e.

$$\mathfrak{F}_n / \mathfrak{F}_{n+1} \cong \overline{\mathfrak{o}}_n \cong \overline{\mathfrak{L}}_n . \tag{6.1.1}$$

Now, consider the factor group $\mathfrak{B}_n / \mathfrak{B}_{n+1}$ (cf, [17], [18], [26]), Since,

$$\mathfrak{B}_n / \mathfrak{B}_{n+1} \cong \mathfrak{F}_n / \mathfrak{F}_{n+1} (\mathfrak{F}_n \cap \mathfrak{F}(p)) \tag{6.1.2}$$

$$\cong \mathfrak{F}_n / \mathfrak{F}_{n+1} / \mathfrak{F}_{n+1} (\mathfrak{F}_n \cap \mathfrak{F}(p)) / \mathfrak{F}_{n+1},$$

the abelian group $\mathfrak{B}_n / \mathfrak{B}_{n+1}$ is a homomorphic image

of $\overline{\mathfrak{L}}_n$. Let $\overline{\mathfrak{P}}_n$ be the kernel, i.e.

$$\mathfrak{B}_n/\mathfrak{B}_{n+1} \cong \overline{\mathfrak{L}}_n - \overline{\mathfrak{P}}_n. \tag{6.1.3}$$

(We shall use the symbol "-" instead of " / " to denote a quotient module.) It is easy to see that $\overline{\mathfrak{P}}_n$ contains all the elements of $p\overline{\mathfrak{L}}_n = \varepsilon(px \mid x \in \overline{\mathfrak{L}}_n)$, for if an element of $\mathfrak{F}_n$ has the form:

$$G = 1 + pD_n + D_{n+1} + \dots ,$$

then there exists an element $G' \in \mathfrak{F}_n$ such that

$$G' = 1 + D_n + D'_{n+1} + \dots ,$$

and

$$G(G'^{-1})^p = (1 + pD_n + \dots)(1 - D'_n + \dots)^p$$

$$= 1 + D''_{n+1} + \dots \in \mathfrak{F}_{n+1}$$

or

$$G \in \mathfrak{F}_{n+1}(\mathfrak{F}_n \cap \mathfrak{F}(p)).$$

Thus, $\mathfrak{B}_n/\mathfrak{B}_{n+1}$ is not only a homomorphic image of $\overline{\mathfrak{L}}_n$ but also of the submodule $\mathfrak{L}_n$ of the free Lie ring $\mathfrak{L}$ over GF(p). Therefore,

$$\mathfrak{B}_n/\mathfrak{B}_{n+1} \cong \mathfrak{L}_n - \mathfrak{P}_n, \tag{6.1.4}$$

for some submodule $\mathfrak{P}_n$ of $\mathfrak{L}_n$.

The direct sum $\mathfrak{P} = \mathfrak{P}_1 \dotplus \mathfrak{P}_2 \dotplus \dots$ is known to be an ideal of $\mathfrak{L}$ (Magnus [18]) and contains the Engel ideal $\mathfrak{J}$ (Sanov [26], Higman [9]),

$$\mathfrak{P}_n \supseteq \mathfrak{J}_n \qquad n = 1, 2, \dots . \tag{6.1.5}$$

Consequently,

(6.1.6) $$\mathfrak{B}_n/\mathfrak{B}_{n+1} \cong \mathfrak{L}_n - \mathfrak{P}_n \subseteq \mathfrak{L}_n - \mathfrak{J}_n = \mathfrak{E}_n.$$

Whether or not $\mathfrak{P} = \mathfrak{J}$ is not known, except for Sanov's result:

(6.1.7) $$\mathfrak{P}_n = \mathfrak{J}_n \qquad (n \leq 2p - 2),$$

which implies

(6.1.8) $$\mathfrak{B}_n/\mathfrak{B}_{n+1} \cong \mathfrak{E}_n \qquad (n \leq 2p - 2).$$

Sanov's proof of (6.1.5) uses the fact that $e^{x_1}, e^{x_2}, \ldots, e^{x_q}$ generate a free group (Magnus [18], [19]), together with the Baker-Hausdorff formula. Higman's proof is based on Hall's [6] well-known commutator collection process. In section 6.3, we give another proof of (6.1.5) using Zassenhaus' representation of the free groups by formal power series of elements in the free associative ring over GF(p).

Now, by (6.1.6), if the Engel ring $\mathfrak{E}$ is nilpotent, i.e. $\mathfrak{E}_n = \mathfrak{E}_{n+1} = \ldots = 0$ for some n, then $\mathfrak{B}_n = \mathfrak{B}_{n+1} = \ldots = \mathfrak{B}_\infty$ and consequently $\mathfrak{B}/\mathfrak{B}_\alpha$ is also nilpotent and finite. Thus the nilpotence of the Engel ring $\mathfrak{E}$ implies the proposition R_p'. The question of whether or not R_p' implies B_p' is still open.(cf. [1]).

A few results are known about the subgroups $\mathfrak{B}_n/\mathfrak{B}_{n+1}$ for general exponent p. By combining Sanov's result (6.1.8) and our previous ones, we have

$$(6.1.9) \qquad \operatorname{rank}(\mathfrak{B}_n / \mathfrak{B}_{n+1}) \geq f_n^q - j_n^q \qquad (1 \leq n \leq 2p-2).$$

Lyndon [15], using the Fox free differential calculus, obtained the following results:

$$\operatorname{rank}(\mathfrak{B}_p / \mathfrak{B}_{p+1}) = f_p^q - \binom{q+p-1}{p} + q,$$

$$\operatorname{rank}(\mathfrak{B}_{p+1} / \mathfrak{B}_{p+2}) = f_{p+1}^q - \binom{q}{2}\binom{q+p-2}{p-1},$$

$$\operatorname{rank}(\mathfrak{B}_{p+2} / \mathfrak{B}_{p+3}) = f_{p+2}^2 - 3p + 1 \qquad (p > 3,\ q = 2),$$

$$\operatorname{rank}(\mathfrak{B}_{p+3} / \mathfrak{B}_{p+4}) = f_{p+3}^2 - 6p + 4 \qquad (p > 5,\ q = 2),$$

which coincide with our lower bounds.

The results of Meier-Wunderli [20] also coincide with our lower bounds for the ranks of $\mathfrak{E}(r+p-3,3)$ for $r \leq p - 2$.

Using (6.1.9) we may obtain a lower bound 7^{408} for the order of the Burnside group of exponent 7 with two generators. This is, however, not the best possible result by any means.

6.2. The free restricted Lie ring $\mathfrak{J}^*$. In order to give, in section 6.4, our new proof of (6.1.5), we introduce, in this section, the notion of the "free" restricted Lie ring, and in section 6.3, recall some properties of Zassenhaus' dimensional subgroups of a free group. (cf. [10], [11], [28], [29].)

The Lie ring $\mathfrak{J}$, as defined in section 1.2, consists of elements δx, $x \in \mathfrak{L}$, where δ is the isomorphism of $\mathfrak{L}$ onto $\mathfrak{J}$ defined by,

$$\delta a_i = A_i,$$
$$\delta(y + z) = \delta y + \delta z = Y + Z,$$
$$\delta(yz) = [(\delta y)(\delta z)] = [YZ] = YZ - ZY.$$

Thus, $\mathfrak{J}$ does not contain elements like X^p, $X \in \mathfrak{J}$, even though these elements enjoy the property

$$[Y\overbrace{XX\ldots X}^{p}] = [YX^p] = YX^p - X^pY,$$

analogous to $[YZ] = YZ - ZY$ with $Z = X^p$. We shall now define a new Lie ring $\mathfrak{J}^*$ which does contain $\mathfrak{J}$ and all X^p, $X \in \mathfrak{J}^*$.

Let $\mathfrak{J}^{[p^e]}$ be the module spanned by all elements X^{p^e}, $X \in \mathfrak{J}$, and $\mathfrak{J}^*$ be the module sum $\mathfrak{J} + \mathfrak{J}^{[p]} + \mathfrak{J}^{[p^2]} + \ldots$. (Ofcourse, this sum is not direct sum.) In this module $\mathfrak{J}^*$ we define two operations, namely Lie multiplication, and following Zassenhaus, the π-operation, as follows:

(6.2.1) $$[XY] = XY - YX,$$

(6.2.2) $$X^{\pi} = X^{p}.$$

By (2.5) we have immediately

(6.2.3) $$[XY^{\pi}] = [Y^{\pi}X] = [XY^{p}].$$

We prove that $\mathfrak{I}^{*}$ is closed under these two operations. It is obvious that $[XY]$, $X^{\pi} \in \mathfrak{I}^{*}$ when $X, Y \in \mathfrak{I}$, so that, in order to prove $[XY] \in \mathfrak{I}^{*}$ for any $X, Y \in \mathfrak{I}^{*}$, it suffices to show that $[X'Y'] \in \mathfrak{I}^{*}$ if $X' = X_1^{p^e}$, $Y' = Y_1^{p^f}$ and $X_1, Y_1 \in \mathfrak{I}$. But, using (2.5) we may show that

(6.2.4) $$[X'Y'] = -[Y_1 X_1^{p^e} Y_1^{p^f-1}] \in \mathfrak{I}.$$

Thus we have seen that $\mathfrak{I}^{*}$ is closed under Lie multiplication. Next, we use induction on e to prove that $X^{\pi} \in \mathfrak{I}^{*}$ for $X \in \mathfrak{I} + \mathfrak{I}^{[p]} + \ldots + \mathfrak{I}^{[p^e]}$. Let

$$X = X_0 + X_1^{p^e} + \ldots + X_n^{p^e},$$

where

$$X_0 \in \mathfrak{I} + \mathfrak{I}^{[p]} + \ldots + \mathfrak{I}^{[p^{e-1}]},$$

$$X_1, \ldots, X_n \in \mathfrak{I}.$$

Then by (2.9)

(6.2.5) $$X^{\pi} = X_0^{p} + X_1^{p^{e+1}} + \ldots + X_n^{p^{e+1}} + \Lambda(X_0, X_1^{p^e}, \ldots, X_n^{p^e}).$$

By induction hypothesis $X_0^{p} = X_0^{\pi} \in \mathfrak{I}^{*}$ and by (6.2.4) $\Lambda(X_0, X_1^{p^e}, \ldots, X_n^{p^e}) \in \mathfrak{I}$, thus $X^{\pi} \in \mathfrak{I}^{*}$.

The Lie ring $\mathfrak{I}^{*}$ with the π-operation thus defined will be called <u>the free restricted Lie ring of characteristic</u> p (<u>with</u> q <u>generators</u>).

By the above argument it may be seen that

$\mathfrak{J}^*$ is the module spanned by all elements $U_i^{p^e}$, where the U_i are basis elements of $\mathfrak{J}$ and $e = 0, 1, 2, \ldots$. We shall show in section 6.5, that these elements $U_i^{p^e}$ actually form a basis of $\mathfrak{J}^*$.

Assume for the moment that the set $\varepsilon(U_i^{p^e})$ form a basis for $\mathfrak{J}^*$. Let $\mathfrak{K}^*$ denote the submodule of $\mathfrak{J}^*$ spanned by all elements of the set $\varepsilon(U_i^{p^e} \mid e \geq 1)$. Then we have a direct decomposition of the module

$$\mathfrak{J}^* = \mathfrak{J} + \mathfrak{K}^*. \tag{6.2.6}$$

Note that $\mathfrak{J}$ is closed under Lie multiplication but not under the π-operation, and $\mathfrak{K}^*$ is not closed under either of these operations.

Let $\mathfrak{H}$ denote the Engel ideal of $\mathfrak{J}$, that is, the image of the Engel ideal $\mathcal{I}$ of $\mathcal{L}$ under the isomorphism $\delta: \mathcal{L} \longrightarrow \mathfrak{J}$, or, alternatively, the module spanned by all elements $[XY^{p-1}]$, $X, Y \in \mathfrak{J}$. By (2.8) $\mathfrak{H}$ may considered to be the module spanned by all elements $(X + Y)^p - X^p - Y^p = \Lambda(X,Y)$, $X, Y \in \mathfrak{J}$. We now define an ideal of $\mathfrak{J}^*$, which we may call the Engel ideal of $\mathfrak{J}^*$. Let $\mathfrak{H}^*$ be the submodule of $\mathfrak{J}^*$ consisting of all linear combinations of elements X^p, $X \in \mathfrak{J}^*$. Using the same method as in the proof of Theorem 3.1 and the method in the earlier part of this section 6.3, it may be shown that $\mathfrak{H}^*$ is an ideal of $\mathfrak{J}^*$, in the sense that, $X \in \mathfrak{H}^*$ and $Y \in \mathfrak{J}^*$ implies $[XY] \in \mathfrak{J}^*$, and $\mathfrak{H}^*$ is closed under the π-operation (cf. [11]). Moreover, it is clear that $\mathfrak{K}^* \subseteq \mathfrak{H}^*$ and

we have the direct decomposition of the module

(6.2.7) $$\mathfrak{H}^* = \mathfrak{H} + \mathfrak{K}^*.$$

By (6.2.6) and (6.2.7), we have

(6.2.8) $$\mathfrak{I}^* - \mathfrak{H}^* \cong \mathfrak{I} - \mathfrak{H}.$$

Let $\mathcal{E}^*$ be the quotient module $\mathfrak{I}^* - \mathfrak{H}^*$ (in fact, $\mathfrak{I}^* - \mathfrak{H}^*$ is a quotient ring, for $\mathfrak{H}^*$ is an ideal of $\mathfrak{I}^*$) and $\mathcal{E}' = \mathfrak{I} - \mathfrak{H}$, so that $\mathcal{E}'$ is the image of the Engel ring $\mathcal{E}$ of $\mathcal{L}$ under the isomorphism $\delta: \mathcal{L} \longrightarrow \mathfrak{I}$. Then (6.2.8) may be written as,

(6.2.9) $$\mathcal{E}^* \cong \mathcal{E}',$$

in other words, the two Engel rings $\mathcal{E}'$ and $\mathcal{E}^*$, the one obtained from $\mathfrak{I}$ and the other obtained from $\mathfrak{I}^*$, are isomorphic.

In the following, we shall use symbols like $\mathfrak{I}_n^*$, $\mathfrak{H}_n^*$ or $\mathfrak{H}_n$ to denote the submodule of the corresponding module without the subscript, which consists of all homogeneous elements of degree n in the generators, as we have done earlier.

6.3. The Zassenhaus dimensional subgroups.

Zassenhaus [29] has shown that the formal power series:

$$g_i = 1 + A_i,\ g_i^{-1} = 1 - A_i + A_i^2 - \ldots,\ (i = 1,2,\ldots,q),$$

(where A_i are the generators of the free associative ring $\mathfrak{A}^q$ over GF(p),) generate the free group with q generators. We shall again use $\mathfrak{F}^q$ or $\mathfrak{F}$ to denote this group in sections 6.3 and 6.4 below. Let $\mathfrak{F}_n^*$ denote the nth "dimensional subgroup" of $\mathfrak{F}$, consisting of all elements

of the form

$$G = 1 + D_n + D_{n+1} + \cdots \qquad (D_i \in \mathfrak{o}_i).$$

The main results of Zassenhaus on these dimensional subgroups are the following:

6.3.1. If $G = 1 + D_n + D_{n+1} + \cdots \in \mathfrak{F}_n^*$ then $D_n \in \mathfrak{d}_n^*$.

6.3.2. $\mathfrak{F}_n^* / \mathfrak{F}_{n+1}^* \cong \mathfrak{d}_n^*$.

More precisely, the mapping:

$$\psi^*: \quad G = 1 + D_n + \cdots \longrightarrow D_n$$

$$GG' = (1 + D_n + \cdots)(1 + D_n' + \cdots)$$

$$= 1 + (D_n + D_n') + \cdots \longrightarrow D_n + D_n',$$

gives a homomorphism of $\mathfrak{F}_n^*$ onto $\mathfrak{d}_n^*$ and the kernel is $\mathfrak{F}_{n+1}^*$.

6.3.3. $\mathfrak{F}_n^* = \{\mathfrak{F}_i(p^j)\} \qquad (ip^j \geq n)$,

where $\{\mathfrak{F}_i(p^j)\}$ denotes the group generated by all the $p^j$the powers of elements of $\mathfrak{F}_i$, the ith term of the lower central series of $\mathfrak{F}$.

6.3.4. $\mathfrak{F}_n^* \cap \mathfrak{F}_m = \{\mathfrak{F}_i(p^j)\} \quad (ip^j \geq n,\ i \geq m)$.

Because of these properties, we have the following isomorphism relations:

(6.3.5) $\mathfrak{B}_n \cong \mathfrak{F}_n^* / \mathfrak{F}_n^* \cap \mathfrak{F}(p)$,

(6.3.6) $\mathfrak{B}_n / \mathfrak{B}_{n+1} \cong \mathfrak{F}_n^* / \mathfrak{F}_{n+1}^* (\mathfrak{F}_n^* \cap \mathfrak{F}(p))$,

and the following homomorphism relation:

(6.3.7) $\mathfrak{d}_n^* \sim \mathfrak{F}_n^* / \mathfrak{F}_{n+1}^* (\mathfrak{F}_n^* \cap \mathfrak{F}(p)) \cong \mathfrak{B}_n / \mathfrak{B}_{n+1}$,

or

(6.3.8) $$\mathfrak{B}_n/\mathfrak{B}_{n+1} \cong \mathfrak{I}_n^* - \mathfrak{P}_n^*,$$

where the submodule $\mathfrak{P}_n^*$ of $\mathfrak{I}_n^*$ is the kernel of this homomorphism.

6.4. Connection between $\mathfrak{P}_n^*$ and $\mathfrak{H}_n^*$.

We show, in this section 6.4, that

(6.4.1) $$\mathfrak{P}_n^* \supseteq \mathfrak{H}_n^*,$$

which will give another proof of (6.1.5).

To prove (6.4.1) it is enough to show that if D_n is a monomial of $\mathfrak{H}_n^*$ and if $G = 1 + D_n + \ldots \in \mathfrak{F}_n^*$, then $G \in \mathfrak{F}_{n+1}^*(\mathfrak{F}_n^* \cap \mathfrak{F}(p))$. As we have seen in 6.2, every monomial of $\mathfrak{H}_n^*$ is either of the form $U^{p^j} \in \mathfrak{K}_n^*$, $ip^j = n$, $j \geq 1$, or $\{U_1 U_2 \ldots U_p/1\ 1 \ldots 1\} \in \mathfrak{H}_n$, where the U_k are basis elements of $\mathfrak{I}$. If $D_n = U^{p^j}$ then it is clear that $G \in \mathfrak{F}_{n+1}^*(\mathfrak{F}_n^* \cap \mathfrak{F}(p))$. Now consider the following, (which may be regarded as a generalization of Jacobson's identity (2.3)).

Let $X_1, X_2, \ldots, X_p$ be elements of a free associative ring over GF(p) and let $\mathfrak{G}$ be the free group generated by formal power series $H_i = 1 + X_i$, $H_i^{-1} = 1 - X_i + X_i^2 - \ldots$, $i = 1, 2, \ldots, p$. Let

$$W_0 = W_0(H_1, H_2, \ldots, H_p) = (H_1 H_2 \ldots H_p)^p;$$

then

$$W_0 = 1 + (X_1 + X_2 + \ldots + X_p)^p + \ldots,$$

where each of the remaining terms is of degree at least p+1 in the X_i. Let

$$W_0 = 1 + w_1 + w_1',$$

where w_1 is the power series consisting of all terms, each of which does not contain X_1 and w_1' consisting of the remaining terms, i.e. every term of w_1' contains X_1. Then it is clear that

$$1 + w_1 = W_0(1, H_2, \ldots, H_p),$$

and

$$W_0(1, H_2, \ldots, H_p)^{-1} = 1 - w_1 + w_1^2 - \ldots .$$

Let

$$W_1 = W_1(H_1, H_2, \ldots, H_p) = W_0(H_1, H_2, \ldots, H_p) W_0(1, H_2, \ldots, H_p)^{-1}$$
$$= 1 + w_1' + w_1'(-w_1 + w_1^2 - \ldots).$$

Note that every term of the power series for W_1 contains X_1 and $(X_1 + X_2 + \ldots + X_p)^p - (X_2 + X_3 + \ldots + X_p)^p$ is the term of lowest degree. Again, let

$$W_1 = 1 + w_2 + w_2' ,$$

where w_2 is the power series consisting of all the terms which do not contain X_2, and w_2' consists of the remaining terms. Clearly, every term of w_2' contains both X_1 and X_2. Once again,

$$1 + w_2 = W_1(H_1, 1, H_3, \ldots, H_p).$$

Now let

$$W_2 = W_2(H_1, H_2, \ldots, H_p) = W_1(H_1, H_2, \ldots, H_p) W_1(H_1, 1, \ldots, H_p)^{-1}$$
$$= 1 + w_2' + w_2'(-w_2 + w_2^2 - \ldots).$$

Every term of the power series for W_2 contains both X_1 and X_2, and the term of lowest degree is

$$(X_1 + X_2 + \ldots + X_p)^p - (X_2 + X_3 + \ldots + X_p)^p$$
$$- (X_1 + X_3 + \ldots + X_p)^p + (X_3 + X_4 + \ldots + X_p)^p.$$

Repeating this process, that is, defining

$$W_{i+1} = W_{i+1}(H_1, H_2, \ldots, H_p)$$

$$= W_i(H_1, H_2, \ldots, H_i, \ldots, H_p) W_i(H_1, H_2, \ldots, 1, \ldots, H_p)^{-1},$$

inductively, we finally see that

$$W_p = W_p(H_1, H_2, \ldots, H_p)$$

$$= 1 + (X_1 + X_2 + \ldots + X_p)^p - \sum_c (X_1 + X_2 + \ldots + X_{p-1})^p$$

$$+ \sum_c (X_1 + X_2 + \ldots + X_{p-2})^p - \ldots + \sum_c X_1^p + V,$$

or using (2.3),

$$W_p = 1 + \begin{Bmatrix} X_1 & X_2 & \ldots & X_p \\ 1 & 1 & \ldots & 1 \end{Bmatrix} + V, \tag{6.4.2}$$

where every term in the power series V is of degree at least p+1 in the X_i and moreover every term contains all of $X_1, X_2, \ldots, X_p$ among its factors.

Suppose, now, in the previous free group $\mathfrak{F}$,

$$G = 1 + \begin{Bmatrix} U_1 & U_2 & \ldots & U_p \\ 1 & 1 & \ldots & 1 \end{Bmatrix} + \ldots \varepsilon \mathfrak{F}_n^* ,$$

where each U_k is a basis element of $\mathfrak{I}_{i_k}$ and $i_1 + i_2 + \ldots + i_p = n$. Then, let

$$G_k = 1 + U_k + \ldots \varepsilon \mathfrak{F}_{i_k}^* \qquad (k = 1, 2, \ldots, p),$$

and consider $W_p(G_1, G_2, \ldots, G_p)$. By (6.4.2) we have

$$W_p(G_1, G_2, \ldots, G_p) = 1 + \begin{Bmatrix} U_1 & U_2 & \ldots & U_p \\ 1 & 1 & \ldots & 1 \end{Bmatrix} + \ldots$$

where each of the remaining terms is of degree greater than n in the generators of $\mathfrak{A}$, or

$$W_p(G_1, G_2, \ldots, G_p) \varepsilon \mathfrak{F}_n^* \cap \mathfrak{F}(p),$$

therefore,

$$GW_p(G_1, G_2, \ldots, G_p)^{-1} \varepsilon \mathfrak{F}_{n+1}^* ,$$

or

$$(6.4.3) \qquad G \in \mathfrak{F}^*_{n+1}(\mathfrak{F}^*_n \cap \mathfrak{F}(p))$$

and we have completed the proof of (6.4.1).

The above argument enables us to generalize the following well-known formula (Grün [4]):

$$\prod [H_1 H_{i_2} H_{i_3} \ldots H_{i_p}] \equiv 1 \pmod{\mathfrak{F}(p)\mathfrak{F}_{p+1}},$$

where $[H_1 H_{i_2} H_{i_3} \ldots H_{i_p}]$ denotes the group commutator $[[\ldots[[H_1, H_{i_2}], H_{i_3}], \ldots], H_{i_p}]$ and the product is taken over all permutations $i_2, i_3, \ldots, i_p$ of $2, 3, \ldots, p$, and the H_i are generators of the free group $\mathfrak{F}$. In particular

$$[H_1 \overbrace{H_2 H_2 \ldots H_2}^{p-1}] \equiv 1 \pmod{\mathfrak{F}(p)\mathfrak{F}_{p+1}}.$$

Let $G_1, G_2, \ldots, G_p$ be elements of $\mathfrak{F}$ such that

$$G_k = 1 + D_k + \ldots \in \mathfrak{F}_{n_k} \qquad (k = 1, 2, \ldots, p).$$

Then it may easily be seen that

$$\prod [G_1 G_{i_2} G_{i_3} \ldots G_{i_p}] = 1 + \left[D_1 \begin{Bmatrix} D_2 & \ldots & D_p \\ 1 & \ldots & 1 \end{Bmatrix} \right] + \ldots$$

$$= 1 + \begin{Bmatrix} D_1 & D_2 & \ldots & D_p \\ 1 & 1 & \ldots & 1 \end{Bmatrix} + \ldots \in \mathfrak{F}^*_n,$$

where $n = n_1 + n_2 + \ldots n_p$. On the other hand

$$W_p(G_1, G_2, \ldots, G_p) = 1 + \begin{Bmatrix} D_1 & D_2 & \ldots & D_p \\ 1 & 1 & \ldots & 1 \end{Bmatrix} + \ldots \in \mathfrak{F}^*_n$$

Therefore,

$$\prod [G_1 G_{i_2} G_{i_3} \ldots G_{i_p}] W_p(G_1, G_2, \ldots, G_p)^{-1} \in \mathfrak{F}^*_{n+1},$$

or

$$\prod [G_1 G_{i_2} G_{i_3} \ldots G_{i_p}] \equiv 1 \pmod{\mathfrak{F}_{n+1}\mathfrak{F}(p)}.$$

6.5. A basis for $\mathfrak{J}^*$. We prove now that the set $\varepsilon(U_i^{p^e})$, where the U_i are basis elements of $\mathfrak{J}$ and $e = 0, 1, 2, \ldots$, form a basis for $\mathfrak{J}^*$. Since we have already seen that $\mathfrak{J}^*$ is spanned by the elements of $\varepsilon(U_i^{p^e})$, it remains only to prove that these elements are linearly independent.

Certainly the U_i are linearly independent. We use induction on e, and assume that the elements $U_i^{p^f}$, $f = 0, 1, \ldots, e-1$, are linearly independent. Suppose we had

$$U = \sum \lambda_{0i} U_i + \sum \lambda_{1i} U_i^{p} + \ldots + \sum \lambda_{ei} U_i^{p^e} = 0, \tag{6.5.1}$$

$$\lambda_{ki} \in GF(p).$$

Since $U_i^{p^k}$ are elements of a free associative ring we may assume, without loss of generality, that U is a homogeneous expression in each generator of $\mathfrak{A}^q$, in other words, we may assume that for some fixed $n_1, n_2, \ldots, n_q$, $U_i^{p^k} \in \mathfrak{A}(n_1^{p^e}, n_2^{p^e}, \ldots, n_q^{p^e})$ for all U_i. Let

$$W = (\sum \lambda_{1i} U_i + \ldots + \sum \lambda_{ei} U_i^{p^{e-1}})^p - (\sum \lambda_{1i} U_i^p + \ldots + \sum \lambda_{ei} U_i^{p^e}).$$

Then by (2.9) and (6.2.4),

$$W \in \mathfrak{J}.$$

Again, let

$$V = \sum \lambda_{1i} U_i + \ldots + \sum \lambda_{ei} U_i^{p^{e-1}},$$

then

$$V \in \mathfrak{A}(n_1^{p^{e-1}}, n_2^{p^{e-1}}, \ldots, n_q^{p^{e-1}}),$$

and

$$U = \sum \lambda_{0i} U_i - W + V^p .$$

We have therefore

$$0 = [UV] = [(\sum \lambda_{0i} U_i - W)V] \in \mathfrak{I} ,$$

or

$$0 = (\sum \lambda_{0i} u_i - w)V \in \mathfrak{L} .$$

Since $\sum \lambda_{0i} U_i - W$ and V have different degrees in the generators, $\sum \lambda_{0i} U_i - W \neq V$ and hence $\sum \lambda_{0i} U_i - W = 0$ or $V = 0$. If $\sum \lambda_{0i} U_i - W = 0$ then $U = V^p = 0$ and $V = 0$. By induction hypothesis, $V = 0$ implies that all the $\lambda_{1i}, \ldots, \lambda_{ei}$ are zero and also $W = 0$. Therefore $\lambda_{0i} = 0$. Thus $U_i, U_i^p, \ldots, U_i^{p^e}$ are linearly independent and we have completed induction.

This fact enables us to determine the ranks of submodules $\mathfrak{I}_n^*$ of the free restricted Lie ring. Let f_n^{q*} be the rank of $\mathfrak{I}_n^*$ (with q generators). Then

$$(6.5.2) \qquad f_n^{q*} = \sum_{p^k | n} f_{n/p^k}^q .$$

Similarly, let $f^*(n_1, n_2, \ldots, n_q)$ be the rank of the submodule $\mathfrak{I}^*(n_1, n_2, \ldots, n_q)$ of $\mathfrak{I}^*$ consisting of homogeneous elements of degree n_1 in A_1, n_2 in A_2, ..., n_q in A_q. Then

$$(6.5.3) \qquad f^*(n_1, n_2, \ldots, n_q)$$

$$= \sum_{p^k | n_i} f(n_1/p^k, n_2/p^k, \ldots, n_q/p^k) .$$

7. Unsettled problems. The following questions, which the author has been unable to answer, arise naturally in connection with the above.

7.1. We have seen that the upper bounds $j(n_1,n_2,\ldots,n_q)$ for $i(n_1,n_2,\ldots,n_q)$ are actually equal to $i(n_1,n_2,\ldots,n_q)$ for the special cases previously calculated by Lyndon and Meier-Wunderli. Is it true that

$$j(n_1,n_2,\ldots,n_q) = i(n_1,n_2,\ldots,n_q),$$

for $n_1 + n_2 + \ldots + n_q \leq 2p - 2$?

Similarly, is it true that

$$k(m,n) = i(m,n),$$

for $m + n \leq 2p - 2$?

7.2. We have verified that

$$j(m,n) = k(m,n),$$

for $m + n \leq p + 4$. It may also be easily seen that

$$j(r+p-n,n) = k(r+p-n,n),$$

for $n = 1, 2, 3, 4$. Is it, in general, true that

$$j(m,n) = k(m,n)?$$

7.3. As a generalization of Sanov's theorem, is it true that

$$\mathfrak{F} = \mathfrak{H} \quad ?$$

7.4. The analogue of Theorem 5.1 for the Burnside groups:

For a given positive integer d, is it always possible to find a prime such that the class of nilpotence of the Burnside group $\mathfrak{F}/\mathfrak{F}(p)$ with

two generators is greater than dp?

Certainly if 7.3 were true, 7.4 would be also true, but not necessarily conversely.

7.5. It seems to be difficult to determine explicit forms for the normal basis elements of $\mathfrak{L}^2$. However, we may raise the following question:

Let $\bar{\mathfrak{L}}^2$ be the free Lie ring over the ring of integers generated by $\bar{a}$ and $\bar{b}$. For a given normal product $x = ba^{m_1}b^{n_1}\ldots a^{m_\kappa}b^{n_\kappa}$ of $\mathfrak{L}^2$, the free Lie ring over GF(p) generated by a and b, let $\bar{x}$ denote the element $\bar{b}\bar{a}^{m_1}\bar{b}^{n_1}\ldots\bar{a}^{m_\kappa}\bar{b}^{n_\kappa}$ in $\bar{\mathfrak{L}}^2$. Then is it true that, if $\varepsilon(u_i)$ is the normal basis for $\mathfrak{L}^2$, then $\varepsilon(\bar{u}_i)$ is a basis for $\bar{\mathfrak{L}}^2$?

This proposition is true, as we have seen for submodules $\mathfrak{L}(m,n)$, when n = 1, 2 and 3.

BIBLIOGRAPHY

1. R. Baer, The higher commutator subgroups of a group, Bull. Amer. Math. Soc. vol. 50 (1944) pp. 143-160.

2. W. Burnside, On an unsettled question in the theory of discontinuous groups, Quart. J. Math. vol. 33 (1902) pp. 230-238.

3. J. A. Green, On groups with odd prime-power exponent, J. London Math. Soc. vol. 27 (1952) pp. 476-485.

4. O. Grün, Zusammenhang zwischen Potenzbildung und Kommutatorbildung, J. Reine Angew. Math. vol. 182 (1940) pp. 158-177.

5. M. Hall, A basis for free Lie rings and higher commutators in free groups, Proc. Amer. Math. Soc. vol. 1 (1950) pp. 575-581.

6. P. Hall, A contribution to the theory of groups of prime power order, Proc. London Math. Soc. (2) vol. 36 (1934) pp. 29-95.

7. P. Hall and G. Higman, The p-length of a p-soluble groups and reduction theorems for Burnside's problem, Proc. London Math. Soc. (3) vol. 7 (1956) pp. 1-42.

8. P. J. Higgins, Lie rings satisfying the Engel condition, Proc. Camb. Phil. Soc. vol. 50 (1954) pp. 8-15.

9. G. Higman, On finite groups of exponent five, Proc. Camb. Phil. Soc. vol. 51 (1955) pp. 381-390.

10. N. Jacobson, Abstract derivation and Lie algebras, Trans. Amer. Math. Soc. vol. 42 (1937) pp. 206-224.

11. ———————, Restricted Lie algebras of characteristic p, Trans. Amer. Math. Soc. vol. 50 (1941) pp. 15-25.

12. A. I. Kostrikin, Solution of the restricted Burnside problem for exponent five. Izvestiya Akad. Nauk SSSR Ser. Mat. vol. 19 (1955) pp. 233-244.

13. M. Lazard, Sur les groupes nilpotents et les anneaux de Lie, Ann. Sci. Éc. Norm. Sup. Paris (3) vol. 71 (1954) pp. 101-190.

14. F. Levi und B. L. van der Waerden, Über eine besondere Klasse von Gruppen, Abhand. Math. Sem. Hamburg Univ. vol. 9 (1932) pp. 154-158.

15. R. C. Lyndon, On Burnside's problem, Trans. Amer. Math. Soc. vol. 77 (1954) pp. 202-215, II, ibid. vol. 78 (1955) pp. 329-332.

16. W. Magnus, Beziechungen zwischen Gruppen und Idealen in einem speziellen Ring, Math. Ann. vol. 111 (1935) pp. 259-280.

17. ———————, Über Beziechungen zwischen höheren Kommutatoren, J. Reine Angew. Math. vol. 177 (1937) pp. 105-115.

18. W. Magnus, Über Gruppen und zugeordnete Liesche Ringe, J. Reine Angew. Math. vol. 182 (1940) pp. 142-149.

19. ———, A connection between the Baker-Hausdorff formula and a problem of Burnside, Annals of Math. vol. 52 (1950) pp. 111-126.

20. H. Meier-Wunderli, Über endliche p-Gruppen, deren Elemente der Gleichung $x^p = 1$ genügen, Comment. Math. Helv. vol. 24 (1950) pp. 18-45.

21. ———, Note on a basis of P. Hall for the higher commutators in free groups, Comment. Math. Helv. vol. 25 (1952) pp. 1-5.

22. ———, Über die Struktur der Brunsidegruppen mit zwei Erzeugenden und vom Primzahlexponenten $p > 3$, Comment. Math. Helv. vol. 30 (1956) pp. 144-174.

23. I. N. Sanov, Solution of the Burnside problem for the exponent 4, Ucenye Zapiski Leningrad Univ. vol. 55 (1940) pp. 166-170.

24. ———, On the Burnside problem, Doklady Akad. Nauk SSSR vol. 57 (1947) pp. 759-761.

25. ———, On a system of relations in periodic groups with prime power periods, Izvestiya Akad. Nauk SSSR Ser. Mat. vol. 15 (1951) pp. 477-502.

26. ———, The connection between periodic groups and Lie rings, Izvestiya Akad. Nauk SSSR Ser. Mat. vol. 16 (1952) pp. 23-58.

27. E. Witt, True Darstellung Liesche Ringe, J. Reine Angew. Math. vol. 177 (1937) pp. 152-160.

28. H. Zassenhaus, Über Lie'sche Ringe mit Primzahlcharakteristik, Abhand. Math. Sem. Hamburg Univ. vol. 13 (1940) pp. 1-100.

29. ———————, Ein Verfahren, jeder endlichen p-Gruppe einen Lie-Ring mit der Charakteristik p zuzuordnen, Abhand. Math. Sem. Hamburg Univ. vol. 13 (1940) pp. 200-207.

30. M. Zorn, On a theorem of Engel, Bull. Amer. Math. Soc. vol. 43 (1937) pp. 401-404.