Embedding of pro-p-groups, derivations and cohomology.

D. Gildenhuys.

AN EMBEDDING THEOREM FOR PRO-P-GROUPS, DERIVATIONS OF PRO-P-GROUPS AND APPLICATIONS TO FIELDS AND COHOMOLOGY

by

DION GILDENHUYS

A THESIS SUBMITTED TO THE FACULTY OF GRADUATE STUDIES AND
RESEARCH, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY

McGILL

1966

CONTENTS

ACKNOWLEDGEMENTS

I WOULD LIKE TO EXPRESS MY GRATITUDE TO PROFESSOR W. KUYK, FOR HIS VALUABLE ADVICE AND ENCOURAGEMENT, DURING THE PREPARATION OF THIS THESIS.

INTRODUCTION

The contents of this thesis is divided into two independent parts. Both parts contain some new results about inverse limits of finite p-groups. These inverse limit groups are called pro-p-groups.

In Chapter 1, a pro-p-group is constructed, that satisfies the second axiom of countability, and contains isomorphic copies of all other pro-p-groups, satisfying this axiom (see theorem 1.28). Leading up to this construction, the author investigates the functorial properties of the wreath product of two permutation groups (Chapter 1, §2), and then gives a new proof for an important theorem (theorem 1.24), due to Marc Krasner and Léo Kaloujnine, concerning the embedding of certain groups K in a multiple wreath product of quotients of consecutive terms from a chain of subgroups of K.

Chapter 2 deals with the significance of theorem 1.28, for field theory. It is well-known that the Galois group of a Galois extension of fields, is a profinite group, i.e. an inverse limit of finite groups, and one may ask oneself, which profinite groups and, in particular, which pro-p-groups may occur as the Galois groups of field extensions of certain types of fields. In Chapter 2, the author concerns himself with this problem. Theorem 2.5 may be considered as the main result of the Chapter.

Apart from the well-known, elementary properties of the Wreath product, all the results of Part I are due to the joint efforts of Professor W. Kuyk and the author of this thesis, (unless otherwise indicated in the text). Part I contains a detailed exposition of the research announcement that appeared, under joint authorship, in the Comptes Rendus [5].

In Part II of this thesis, the author develops a method, that enables him to determine the cohomological dimension of certain pro-p-groups, defined by a finite number of generators and relations, in the sense of [18], Chapter I, §4.2 and 4.3. He shows that the derivations $\frac{\partial}{\partial x_i}$, defined by Lyndon (originally by Fox), on the discrete free group L(n), on n generators $x_1, \ldots, x_n$ (see [15]), can be extended to the magnus algebra A(n), in which L(n) is imbedded. The author uses these extended derivations to obtain information about the cohomology of pro-p-groups of finite type, defined by a single relation, in a manner that is similar to the way that Lyndon described the cohomology of <u>discrete</u> groups, defined by a single relation (loc cit). The main results of Chapter 3 are theorems 3.13, 3.18, 3.23 and 3.25. The statement of parts (a) and (b) of theorem 3.11 are not due to the author, but can be found in [20]. The proof of theorem 3.11, and all other theorems of Part II, are due to the author.

Although he has not solved his main problem, suggested to him by Professor W. Kuyk, namely that of determining whether a pro-p-group has cohomological dimension 2, if it can be defined by a single non-trivial relation which is not a p-th power, the author believes that further development of his methods may eventually lead to a complete solution of this problem.

PART I

Chapter I : Properties of the Wreath Product and an Embedding Theorem for Pro-p-groups.

1. Permutation Groups.

One finds in [6] a definition of the Wreath product of two permutation groups. For the purpose of investigating the functorial properties of the wreath product, we proceed with the following definitions.

Definition 1.1:

The category $\mathcal{P}'$ has as its objects all triples (G,S,a), where G is a group, S a non-empty set and $a: G \times S \longrightarrow S$ a mapping, such that

$$a(g_1 \cdot g_2, s) = a(g_1, a(g_2, s)), \quad a(1,s) = s$$

for all $g_1, g_2 \in G$, $s \in S$, the identity element of G being denoted by 1. To simplify the notation, we shall often write (G,S) instead of (G,S,a), and $g(s)$ instead of $a(g,s)$, $(g \in G,\ s \in S)$. The morphisms in the category $\mathcal{P}'$, are pairs of maps $(\alpha,\alpha'): (G_1,S_1) \longrightarrow (G_2,S_2)$, where $\alpha: G_1 \longrightarrow G_2$ denotes a homomorphism of groups and $\alpha': S_2 \longrightarrow S_1$ a mapping of sets, satisfying the following compatibility condition:

$$\alpha'(\alpha(g_1)(s_2)) = g_1(\alpha'(s_2))$$

for all $g_1 \in G_1$, $s_2 \in S_2$. Suppose $(\alpha,\alpha'): (G_1,S_1) \longrightarrow (G_2,S_2)$ and $(\beta,\beta'): (G_2,S_2) \longrightarrow (G_3,S_3)$ are morphisms in $\mathcal{P}'$. Define their composition $(\beta,\beta') \circ (\alpha,\alpha') = (\beta \circ \alpha, \alpha' \circ \beta')$.

We proceed to verify that $(\beta\circ\alpha, \alpha'\circ\beta')$ is again a morphism in $\mathcal{GP}'$:

$$\alpha'\left[\beta'\{\beta(\alpha(g_1))(s_3)\}\right] = \alpha'\left[\alpha(g_1)(\beta'(s_3))\right] = g_1(\alpha'(\beta'(s_3)))$$

for all $g_1 \in G_1$, $s_3 \in S_3$. It is clear that $\mathcal{GP}'$ forms a category.

Definition 1.2:

A *permutation group (G,S,a)* is an object from $\mathcal{GP}'$, satisfying the additional condition that, for every $g \in G$, the mapping: $s \longmapsto a(g,s)$ is a bijection of S onto itself. The class of all permutation groups, with morphisms defined as in definition 1.1, constitutes a *subcategory $\mathcal{GP}$* of $\mathcal{GP}'$.

Definition 1.3:

As an example of a permutation group, we may consider the so-called *regular representation* (G,G,m), (to be denoted, henceforth, by (G,G)), *of a group G*. The action $m: G \times G \longrightarrow G$ is the group operation.

Definition 1.4:

A permutation group (G,S) is said to be *transitive* if the map $\pi_s: G \longrightarrow S$, defined by the formula $\pi_s(g) = g(s)$, is surjective, for every $s \in S$.

Remark 1.5:

By way of an example of an isomorphism in the category $\mathcal{GP}$, we shall prove that if a finite set S is of same cardinality as a group G, and (G,S) is a transitive permutation group, then (G,S) is isomorphic to the regular representation (G,G). For each $s \in S$, the map $\pi_s: G \longrightarrow S$, of definition 1.4, is surjective, hence bijective. Let $s_o \in S$. To each $s \in S$, there corresponds a unique $\theta(s) \in G$, such that $\theta(s)(s_o) = s$. The map $\theta : S \longrightarrow G$, thus defined, has the property that $\theta(1_G(g)(s)) = g.(\theta(s))$, for all $g \in G$, $s \in S$; because $\theta(1_G(g)(s))(s_o) = g(s) = g((\theta(s))(s_o)) = (g.\theta(s))(s_o))$, ($1_G$ = the identity map on G). Thus, $(1_G,\theta): (G,G) \longrightarrow (G,S)$ is a morphism. One has $\theta \circ \theta^{-1} = 1_S$ = the identity element on S, and $\theta^{-1}(1_G(g_1)(g_2)) = \theta^{-1}(g_1.g_2) = g_1(\theta^{-1}(g_2))$ for all g_1, $g_2 \in G$, because $\theta(g_1(\theta^{-1}(g_2)))(s_o) = (g_1.(\theta(\theta^{-1}(g_2)))(s_o) = (g_1.g_2)(s_o) = \theta(\theta^{-1}(g_1.g_2))(s_o)$. It follows that $(1_G,\theta^{-1}): (G,S) \longrightarrow (G,G)$ is a morphism. The equalities $(1_G,\theta)\circ(1_G,\theta^{-1}) = (1_G,1_S)$ and $(1_G,\theta^{-1})\circ(1_G,\theta) = (1_G,1_S)$ imply that (G,S) is isomorphic to (G,G).

Definition 1.6:

A permutation group (G,S) is **faithful** if g = identity, whenever $g(s) = s$ for all $s \in S$.

2. The Permutation Wreath Product and Abstract Wreath Product.

Notation: If X and Y are sets, X^Y denotes the set of all mappings from Y into X. If X is a group, then X^Y denotes the group defined on the set X^Y, by the formula $(\psi_1.\psi_2)(y) = \psi_1(y).\psi_2(y)$ for all $y \in Y$. The identity element of a given group, (all groups will be written multiplicatively), will usually be denoted by the symbol 1, (even in those cases where different groups are involved).

Definition 1.7:

Let (A,S) and (B,T) be two objects from $\mathcal{GP}'$. Define their Wreath product $(A,S)\wr(B,T)$ to be the object $(A\wr_T B, S\times T)$ of $\mathcal{GP}'$, where $A\wr_T B$ denotes the group defined on the set $B\times A^T$, by the formula:

$$(b_1,\psi_1)(b_2,\psi_2) = (b_1\cdot b_2,\psi_1^{b_2}\cdot\psi_2),\quad (b_1,b_2\in B,\ \psi_1,\psi_2\in A^T),$$

$\psi_1^{b_2}$ being defined as the map: $T\longrightarrow A$, given by $\psi_1^{b_2}(t) = \psi_1(b_2(t))$, for all $t\in T$. We have $\psi^{(bb')} = (\psi^b)^{b'}$ for all b, $b'\in B, \psi\in A^T$, and $A\wr_T B$ may also be described as the semi-direct product of A^T and B, corresponding to the anti-homomorphism $u:B\longrightarrow \mathrm{Aut}(A^T)$, defined by the formula $u(b)(\psi) = \psi^b$, for all $\psi\in A^T$, $b\in B$. The action of $A\wr_T B$ on $S\times T$ is given by the formula:

$$(b,\psi)(s,t) = (\psi(t)(s),b(t)),\quad (b\in B,\psi\in A^T).$$

If one denotes by $I\in A^T$ the map defined by the formula $I(t) = 1_A =$ the identity element of A, for all $t\in T$, then $(1_B,I)(s,t) = (s,t)$, for all $s\in S$, $t\in T$. Also,

$$[(b_1,\psi_1)(b_2,\psi_2)](s,t) = (\psi_1(b_2(t))(\psi_2(t)(s)),b_1(b_2(t))) = (b_1,\psi_1)(\psi_2(t)(s),b_2(t)),$$

so that $(A,S)\wr(B,T)$ is indeed an object of $\mathcal{GP}'$.

Furthermore, if (A,S) and (B,T) are permutation groups, then $(A,S)\wr(B,T)$ is again a permutation group. To verify this statement, we suppose that

$$(\psi(t_1)(s_1),b(t_1)) = (\psi(t_2)(s_2),b(t_2)),\quad (b\in B,\psi\in A^T,\ s_1,s_2\in S,\ t_1,t_2\in T).$$

Then $t_1 = t_2$ and $s_1 = s_2$. Given (s,t), $(s',t') \in S \times T$, there exists $b \in B$, such that $b(t) = t'$, and there exists $a \in A$, such that $a(s) = s'$. Let $\psi : T \longrightarrow A$ be any mapping with the property that $\psi(t) = a$. Then

$$(b,\psi)(s,t) = (\psi(t)(s), b(t)) = (a(s), b(t)) = (s',t'),$$

and the verification is complete.

Definition 1.8:

If (A,S) and (B,T) are two permutation groups, then the wreath product, or permutation wreath product of (A,S) and (B,T), is defined to be $(A,S) \wr (B,T)$.

Associated to $(A,S)\wr(B,T)$, there exists a canonical split exact sequence of groups:

$$1 \longrightarrow A^T \xrightarrow{k} A \wr_T B \xrightarrow{p} B \longrightarrow 1,$$

where $k(\psi) = (1,\psi)$, $p(b,\psi) = b$, for all $b \in B, \psi \in A^T$.

Theorem 1.9:

(a) The wreath product can be considered as a functor $\wr : \mathcal{P}' \times \mathcal{P}' \longrightarrow \mathcal{P}'$, associative upto natural isomorphism;

(b) $\mathcal{P} \wr \mathcal{P} \subset \mathcal{P}$

(c) $(A,S)\wr(B,T)$ is transitive whenever (A,S) and (B,T) are both transitive permutation groups, and is faithful, whenever (A,S) and (B,T) are both faithful permutation groups.

Proof:

We have already proved (b).

Proof of (a):

Let $\bar\alpha = (\alpha,\alpha'): (A,S)\longrightarrow(A',S')$, $\bar\beta = (\beta,\beta'): (B,T)\longrightarrow(B',T')$ be two morphisms in $\mathcal{P}'$. Define

$(W(\bar\alpha,\bar\beta),W'(\bar\alpha,\bar\beta)): (A,S)\wr(B,T) \longrightarrow (A',S')\wr(B',T')$,

by the formulas:

$W(\bar\alpha,\bar\beta)(b,\psi) = (\beta(b),\alpha\circ\psi\circ\beta')$, $\quad W'(\bar\alpha,\bar\beta)(s',t') = (\alpha'(s'),\beta'(t'))$

for all $b\in B,\psi\in A^T$, $s'\in S'$, $t'\in T'$.

We proceed to verify that $W(\alpha,\beta)$ is homomorphism of groups:

$W(\bar\alpha,\bar\beta)(b_1b_2,\psi_1^{b_2}\psi_2) = (\beta(b_1)\beta(b_2),\alpha\circ(\psi_1^{b_2}.\psi_2)\circ\beta')$;

$[W(\bar\alpha,\bar\beta)(b_1,\psi_1)].[W(\bar\alpha,\bar\beta)(b_2,\psi_2)] = (\beta(b_1).\beta(b_2),(\alpha\circ\psi_1\circ\beta')^{\beta(b_2)}.(\alpha\circ\psi_2\circ\beta'))$.

Now,

$$(\alpha\circ(\psi_1^{b_2}.\psi_2)\circ\beta')(t') = \alpha(\psi_1^{b_2}(\beta'(t')).\alpha(\psi_2(\beta'(t')))$$
$$= \alpha(\psi_1(b_2(\beta'(t')))).\alpha(\psi_2(\beta'(t'))).$$

On the other hand,

$$[(\alpha\circ\psi_1\circ\beta')^{\beta(b_2)}.(\alpha\circ\psi_2\circ\beta')](t') = \alpha(\psi_1(\beta'(\beta(b_2)(t')))).\alpha(\psi_2(\beta'(t'))).$$

Since $(\beta,\beta'): (B,T)\longrightarrow(B',T')$ is a morphism,

$$\beta'(\beta(b_2)(t')) = b_2(\beta'(t'))$$

and it follows that $W(\bar\alpha,\bar\beta)$ is a homomorphism. We proceed to verify the compatibility condition that would make $(W(\bar\alpha,\bar\beta),W'(\bar\alpha,\bar\beta))$ a morphism in the category $\mathcal{P}'$.

$$W'(\bar\alpha,\bar\beta)(W(\bar\alpha,\bar\beta)(b,\psi)(s',t')) = W'(\bar\alpha,\bar\beta)((\beta(b),\alpha\circ\psi\circ\beta')(s',t'))$$
$$= W'(\bar\alpha,\bar\beta)[(\alpha(\psi(\beta'(t')))(s'),\beta(b)(t')]$$
$$= (\alpha'\{\alpha(\psi(\beta'(t')))(s')\},\beta'(\beta(b)(t')))$$
$$= (\psi(\beta'(t'))(\alpha'(s')),b(\beta'(t'))).$$

On the other hand,

$(b,\psi)(W'(\bar{\alpha},\bar{\beta})(s',t')) = (b,\psi)(\alpha'(s'),\beta'(t')) = (\psi(\beta'(t'))(\alpha'(s')),b(\beta'(t')))$.

It follows that $(W(\bar{\alpha},\bar{\beta}),W'(\bar{\alpha},\bar{\beta}))$ is a morphism.

Let $\bar{\alpha}_1 = (\alpha_1,\alpha_1'): (A',S') \longrightarrow (A'',S'')$ and $\bar{\beta}_1 = (\beta_1,\beta_1'): (B',T') \longrightarrow (B'',T'')$ be two morphisms in $\mathcal{P}'$.

We proceed to show that $W(\bar{\alpha}_1,\bar{\beta}_1)\circ W(\bar{\alpha},\bar{\beta}) = W(\bar{\alpha}_1\circ\bar{\alpha}\ ,\bar{\beta}_1\circ\bar{\beta})$:

$$\begin{aligned}W(\bar{\alpha}_1,\bar{\beta}_1)(W(\bar{\alpha},\bar{\beta}))(b,\psi) &= W(\bar{\alpha}_1,\bar{\beta}_1)(\beta(b),\alpha\circ\psi\circ\beta')\\ &= (\beta_1(\beta(b)),\alpha_1\circ\alpha\circ\psi\circ\beta'\circ\beta_1') = W(\bar{\alpha}_1\circ\bar{\alpha},\bar{\beta}_1\circ\bar{\beta})(b,\psi)\end{aligned}$$

for all $(b,\psi)\in A\wr_T B$. It follows from these calculations that the wreath product is a functor.

We shall now prove that the wreath product is associative upto natural isomorphism. Let

$$p_1: B\times A^T \longrightarrow B \quad\text{and}\quad p_2: B\times A^T \longrightarrow A^T$$

be the two set-theoretical projections. There is a group structure defined on $C\times(B\times A^T)^U$, (A,S), (B,T) and (C,U) being three arbitrary objects of $\mathcal{P}'$, and, by definition, $[(A,S)\wr(B,T)]\wr(C,U)$ consists of this group, together with its action on $(S\times T)\times U$. On the other hand, $(A,S)\wr[(B,T)\wr(C,U)]$ consists of a group structure on the set $(C\times B^U)\times A^{T\times U}$, and the action of this group on $S\times(T\times U)$. Define $\gamma: C\times(B\times A^T)^U \longrightarrow (C\times B^U)\times A^{T\times U}$, by the formula $\gamma(c,\psi) = ((c,\psi_1),\psi_2)$, where $\psi\in(B\times A^T)^U$, and $\psi_1\in B^U$, $\psi_2\in A^{T\times U}$ are defined by $\psi_1(u) = p_1(\psi(u))$, $\psi_2(t,u) = p_2(\psi(u))(t)$ for all $u\in U$ and $t\in T$. Suppose $c'\in C$, $\psi'\in(B\times A^T)^U$. Then $(c,\psi)(c',\psi') = (cc',\psi^{c'}.\psi')$.

Define $\psi_1'(u) = p_1(\psi'(u))$, $\psi_2'(t,u) = p_2(\psi'(u))(t)$ for all $u \in U$ and $t \in T$. One has

$$((c,\psi_1),\psi_2)((c',\psi_1'),\psi_2') = ((c,\psi_1).(c',\psi_1'),\psi_2^{(c',\psi_1')}.\psi_2')$$
$$= ((cc',\psi_1^{c'}.\psi_1'),\psi_2^{(c',\psi_1')}.\psi_2')$$

Now, $\gamma((c,\psi).(c',\psi')) = ((cc',(\psi^{c'}.\psi')_1),(\psi^{c'}.\psi')_2)$, where $(\psi^{c'}.\psi')_1(u)=p_1(\psi(c'u).\psi'(u)) = p_1(\psi(c'u)).p_1(\psi'(u))$, and

$$(\psi^{c'}.\psi')_2(t,u) = p_2(\psi(c'u).\psi'(u))(t)) = p_2(\psi(c'u))^{p_1(\psi'(u))}(t).p_2(\psi'(u))(t)$$
$$= p_2(\psi(c'u))(p_1(\psi'(u))(t)).p_2(\psi'(u))(t) \text{ ---------(1)}$$

One has $\gamma(c,\psi).\gamma(c',\psi') = ((cc',\psi_1^{c'}.\psi_1'),\psi_2^{(c',\psi_1')}.\psi_2')$.

We note that the first elements of the pairs $\gamma((c,\psi).(c',\psi'))$ and $\gamma(c,\psi).\gamma(c',\psi')$ are the same.

$$(\psi_2^{(c',\psi_1')}.\psi_2')(t,u) = \psi_2^{(c',\psi_1')}(t,u).\psi_2'(t,u)$$
$$= \psi_2(\psi_1'(u)(t),c'(u)).\psi_2'(t,u)$$
$$= p_2(\psi(c'(u)))(\psi_1'(u)(t)).p_2(\psi'(u))(t)$$
$$= p_2(\psi(c'(u)))(p_1(\psi'(u))(t)).p_2(\psi'(u))(t).$$

Comparison with (1), gives:

$$\gamma((c,\psi).(c',\psi')) = \gamma(cc',\psi^{c'}.\psi'),$$

so that γ is a homomorphism of groups. We now proceed to verify that, by defining $\gamma'(s,(t,u)) = ((s,t),u)$ for all $s \in S$, $t \in T$ and $u \in U$, we obtain a morphism

$$(\gamma,\gamma'): [(A,S)\wr(B,T)]\wr(C,U) \longrightarrow (A,S)\wr[(B,T)\wr(C,U)]$$

in the category $\mathcal{P}'$:

$$\begin{aligned}\gamma(c,\psi)(s,(t,u)) &= ((c,\psi_1),\psi_2)(s,(t,u)) = (\psi_2(t,u)(s),(c,\psi_1)(t,u))\\ &= (p_2(\psi(u))(t)(s),(\psi_1(u)(t),c(u))\\ &= (p_2(\psi(u))(t)(s),(p_1(\psi(u))(t),c(u))).\end{aligned}$$

On the other hand,

$$\begin{aligned}(c,\psi)((s,t),u) &= (\psi(u)(s,t),c(u)) = ((p_1(\psi(u)),p_2(\psi(u)))(s,t),c(u))\\ &= ((p_2(\psi(u))(t)(s),p_1(\psi(u))(t)),c(u)),\end{aligned}$$

which proves that (γ,γ') is a morphism in the category $\mathcal{P}'$. The mappings γ and γ' are invertible. Indeed, if $((c,\psi_1),\psi_2)\in(C\times B^U)\times A^{T\times U}$, then there exists a unique $\psi\in(B\times A^T)^U$, such that $\psi_1(u) = p_1(\psi(u))$, $\psi_2(t,u) = p_2(\psi(u))(t))$, for all $u\in U$ and $t\in T$; so that the formula $\gamma^{-1}((c,\psi_1),\psi_2) = (c,\psi)$ defines the inverse γ^{-1} of γ.

To prove part (c), let us suppose that (A,S) and (B,T) are transitive permutation groups. Given s_1, $s_2\in S$, t_1, $t_2\in T$, there exists $\beta\in B$, such that $\beta(t_1) = t_2$. Since (A,S) is transitive, there exists $\psi\in A^T$, such that $\psi(t_1)(s_1) = s_2$. Thus,

$$(\beta,\psi)(s_1,t_1) = (\psi(t_1)(s_1),t_2) = (s_2,t_2).$$

This proves that $(A,S)\wr(B,T)$ is transitive.

Now, suppose that (A,S) and (B,T) are two faithful permutation groups, and suppose that $(\beta,\psi)(s,t) = (s,t)$, for all $(s,t)\in S\times T$. Since B is faithful, $\beta = 1$. If we suppose that $\psi(t_1)\neq 1$, for some $t_1\in T$, then there exists an $s\in S$, such that $\psi(t_1)(s)\neq s$, whence $(\beta,\psi)(s,t_1) = (\psi(t_1)(s),t_1)\neq(s,t_1)$, which is a contradiction. It follows that $(A,S)\wr(B,T)$ is faithful.

Definition 1.20:

The abstract wreath product $A\wr B$ of two groups A and B, is the group $A\wr_B B$, belonging to the permutation wreath product $(A,A)\wr(B,B)$.

It is a semi-direct product of A^B and B, and one has a canonical split-exact sequence:

$$1 \longrightarrow A^B \xrightarrow{k} A\wr B \xrightarrow{p} B \longrightarrow 1.$$

One may also define $A\wr B$ as the quotient of the free product $A^B * B$, obtained by identifying the words $u.\psi.b.v$ and $u.b.\psi^b.v$ $(b\in B, \psi\in A^B$, $\psi^b(x) = \psi(bx)$, $u, v\in A^B * B)$. Subject to these identifications, every word can be reduced to the form $b.\psi$, and it now becomes clear that the two definitions are the same (upto natural isomorphism).

To each homomorphism of groups $\alpha: A \longrightarrow A'$, we make correspond a homomorphism $\alpha_*: A\wr B \longrightarrow A'\wr B$, by the formula $\alpha_*(b,\psi) = (b,\alpha\circ\psi)$. The abstract wreath product $A\wr B$ is thus seen to be functorial in A. It is not functorial in B, and we have to be content with the limited result, contained in Proposition 1.21, below. The abstract wreath product is not associative. Indeed if a,b and c are the respective cardinalities of groups A, B, C, then $(A\wr B)\wr C$ has the cardinal number $c.(b.a^b)^c = cb^ca^{bc}$, whereas $A\wr(B\wr C)$ is of cardinality $cb^ca^{cb^c}$.

Proposition 1.21:

Suppose $\beta: B \longrightarrow B'$ is a monomorphism of groups. Then

(a) there exists a mapping of sets $\bar{\beta}: B' \longrightarrow B$, such that

$(\beta,\wp)\colon (B,B) \longrightarrow (B',B')$ is a morphism in $\mathcal{P}$;

(b) if $\alpha\colon A \longrightarrow A'$ is any homomorphism of groups, then there exists a homomorphism $\rho\colon A \wr B \longrightarrow A' \wr B'$, and a homomorphism $\delta\colon A^B \longrightarrow (A')^{B'}$, such that the following diagram commutes:

$$\begin{tikzcd}
1 \arrow[r] & A^B \arrow[r] \arrow[d, "\delta"] & A \wr B \arrow[r, "\pi"] \arrow[d, "\rho"] & B \arrow[r] \arrow[d, "\beta"] & 1 \\
1 \arrow[r] & (A')^{B'} \arrow[r] & A' \wr B' \arrow[r, "\pi'"] & B' \arrow[r] & 1
\end{tikzcd}$$

(c) if α is a monomorphism, ρ may be chosen to be a monomorphism.

<u>Proof:</u>

(a) Choose a system $\{b'_\sigma\}_{\sigma\in S}$ of right coset representatives for $\beta(B)$ in B', i.e. $B' = \bigcup_{\sigma\in S} \beta(B)b'_\sigma$, $\beta(B).b'_\sigma \cap \beta(B).b'_{\sigma_1} = \phi$,for $\sigma \neq \sigma_1$. Define a mapping of sets $\wp\colon B' \longrightarrow B$, by putting

$$\wp(b') = \begin{cases} b_1 \text{ whenever } b' \notin \beta(B) \text{ and } b' = \beta(b_1)b'_\sigma \\ b \text{ if } b' = \beta(b). \end{cases}$$

Then $(\beta,\wp)\colon (B,B) \longrightarrow (B',B')$ is a morphism in the category $\mathcal{P}$. Indeed, $\wp(\beta(b)(b')) = \wp(\beta(b).b') = b.b_2$ if $b' = \beta(b_2)$; if not, then there exist b'_σ and b_1, such that $b' = \beta(b_1).b'_\sigma$ and $\beta(b).b' = \beta(bb_1).b'_\sigma$, so that $\wp(\beta(b).b') = bb_1$. Now, $b(\wp(b')) = bb_2$ if $b' = \beta(b_2)$. If, on the other hand, $b' \notin \beta(B)$ and $b' = \beta(b_1).b'_\sigma$, then $b(\wp(b')) = bb_1$. Thus, it is seen that $\wp(\beta(b)(b')) = b(\wp(b'))$, for all $b \in B$, $b' \in B'$, and, therefore, $(\beta,\wp)\colon (B,B) \longrightarrow (B',B')$ is a morphism in $\mathcal{P}$.

(b) Define $\delta(\psi) = \alpha \circ \psi \circ \wp$; Then $\delta(\psi_1 . \psi_2) = \delta(\psi_1).\delta(\psi_2)$. Define $\rho(b,\psi) = (\beta(b),\delta(\psi))$. The diagram certainly commutes.

$\rho(b_1b_2, \psi_1^{b_2}.\psi_2) = (\beta(b_1)\beta(b_2), [\delta(\psi_1^{b_2}).\delta(\psi_2)])$, and

$\rho(b_1,\psi_1).\rho(b_2,\psi_2) = (\beta(b_1).\beta(b_2), [\delta(\psi_1)^{\beta(b_2)}.\delta(\psi_2)])$.

One has

$\delta(\psi_1^{b_2})(b') = \alpha(\psi_1^{b_2}(\wp(b'))) = \alpha(\psi_1(b_2.\wp(b')))$.

One the other hand,

$(\delta(\psi_1))^{\beta(b_2)}(b') = \delta(\psi_1)(\beta(b_2).b') = \alpha(\psi_1(\wp(\beta(b_2).b')))$.

The compatibility condition for the morphism of part (a), gives $\wp(\beta(b_2).b' = b_2.\wp(b')$, so that $\delta(\psi_1^{b_2})(b') = (\delta(\psi_1))^{\beta(b2)}(b')$, for all $b_2 \in B$, $b' \in B'$. Hence ρ is a homomorphism of groups.

(c) Let ρ be defined as above. Suppose that $\rho(b,\psi) = 1$. Then $\beta(b) = 1$ and $b = 1$. Furthermore, $1 = \delta(\psi) = \alpha \circ \psi \circ \wp$. Since $\wp$ is surjective and α injective, $\psi(b') = 1$, for all $b' \in B$, and this completes the proof.

3. Embedding Theorems.

Theorem 1.22 (Krasner and Kaloujnine)

If $1 \to A \xrightarrow{j} G \xrightarrow{\pi} B \to 1$ is an exact sequence of groups and homomorphisms, then there exists a monomorphism

$(\lambda, I): (G,G) \to (A,A)\wr(B,B)$

in the category $\mathcal{P}$ of permutation groups; $\lambda: G \to A\wr B$ is a monomorphism of groups, and the following diagram, with exact rows, commutes:

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "j"] \arrow[d, "\mu"'] & G \arrow[r, "\pi"] \arrow[d, "\lambda"'] & B \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & A^B \arrow[r, "k"] & A\wr B \arrow[r, "p"] & B \arrow[r] & 1
\end{tikzcd}$$

Here $\mu: A \longrightarrow A^B$ is defined in such a way, that for some system of representatives $\tau: B \dashrightarrow G$, one has

$$j(\mu(a)(b)) = \tau(b^{-1}).j(a).\tau(b) , \quad (a \in A,\ b \in B).$$

Proof:

Without loss in generality, we may identify G with the set $B \times A$, multiplication being defined by means of a normalized 2-cocycle $f: B \times B \longrightarrow A$ and a mapping $v: B \longrightarrow \mathrm{Aut}(A)$, according to the formula:

$$(b_1,a_1)(b_2,a_2) = (b_1b_2, f(b_1,b_2).v(b_2)(a_1).a_2), \quad (b_1,b_2 \in B,\ a_1,a_2 \in A);$$

(see, for instance, [6] ,th. 15.1.1). One has:

$$v(y)(v(x)(a)) = f(x,y)^{-1}.v(xy)(a).f(x,y) \text{ ----------(i)}$$

$$f(xy,z).v(z)(f(x,y)) = f(x,yz).f(y,z) \text{---------------(ii)}$$

$(x,y,z \in B,\ a \in A)$. $\lambda: G \longrightarrow A \wr B$ is now defined, by writing

$$\lambda(b_1,a_1) = (b_1, f(b_1,-).v(-)(a_1)).$$

(We recall that $A \wr B$ is a group defined on the set $B \times A^B$.) The expression $f(b_1,-).v(-)(a_1)$ denotes the mapping: $b \longmapsto f(b_1,b).v(b)(a_1)$.

We now proceed to verify that λ satisfies the conditions of the theorem. Let $b,\ b_1,\ b_2 \in B,\ a_1,\ a_2 \in A$; then $\lambda(b_1,a_1).\lambda(b_2,a_2) = (b_1b_2, \gamma)$, where:

$$\begin{aligned}\gamma(b) &= f(b_1,b_2b).v(b_2b)(a_1).f(b_2,b).v(b)(a_2)\\ &= f(b_1,b_2b).f(b_2,b).v(b)(v(b_2)(a_1)).v(b)(a_2), \text{ (by (i))}\\ &= f(b_1b_2,b).v(b)(f(b_1,b_2)).v(b)(v(b_2)(a_1)).v(b)(a_2), \text{ (by (ii).}\end{aligned}$$

One has

$$\begin{aligned}\lambda((b_1,a_1).(b_2,a_2)) &= \lambda(b_1b_2, f(b_1,b_2).v(b_2)(a_1).a_2)\\ &= (b_1b_2, f(b_1b_2,-).v(-)\{f(b_1,b_2).v(b_2)(a_1).a_2\}).\end{aligned}$$

It follows that

$$\lambda(b_1,a_1).\lambda(b_2,a_2) = \lambda((b_1,a_1).(b_2,a_2)),$$

and λ is a homomorphism of groups.

Suppose $\lambda(b_1,a_1) = 1$. Then $b_1 = 1$ and $f(b_1,x).v(x)(a_1) = 1$, for all $x \in B$. It follows that (b_1,a_1) is the identity element $(1,1)$ of G.

We define $I\colon A \times B \longrightarrow A \times B$ to be the identity map. We have identified G with the set $B \times A$, and the regular representation (G,G) is obtained by letting G act on $A \times B$, according to the formula:
$(b_1,a_1)(a,b) = (f(b_1,b).v(b)(a_1).a,b_1b)$, $(b,\ b_1 \in B,\ a,\ a_1 \in A)$.
We proceed to verify that the pair (λ,I) satifies the compatibility condition:

$$\begin{aligned} I(\lambda(b_1,a_1)(a,b)) &= (b_1,f(b_1,-).v(-).a_1)(a,b) = (f(b_1,b).v(b).a_1.a,b_1b) \\ &= (b_1,a_1)(I(a,b)). \end{aligned}$$

The fact that (λ,I) is a monomorphism in the category $\mathcal{P}$, follows from the following more general statement: if (β,β') is a morphism in $\mathcal{P}$, β a monomorphism of groups and β' an epimorphism of sets, then (β,β') is a monomorphism in $\mathcal{P}$. (Proof: the equality $(\beta,\beta')\circ(\alpha_1,\alpha_1') = (\beta,\beta')\circ(\alpha_2,\alpha_2')$ implies $\beta\circ\alpha_1 = \beta\circ\alpha_2$ and $\alpha_1'\circ\beta' = \alpha_2'\circ\beta'$, whence $\alpha_1 = \alpha_2$ and $\alpha_1' = \alpha_2'$.)

It now only remains to verify the commutativity of the diagram contained in the statement of the theorem. Without loss in generality, we may suppose $\tau(b) = (b,1)$, $j(\mu(a)(b)) = (1,v(b)(a)) = (b,1)^{-1}(1,a)(b,1)$, $j(a) = (1,a)$ and $\pi(b,a) = b$ for all $a \in A$ and $b \in B$ (15.1 of [6]). Now,

$$\begin{aligned} k(\mu(a)) = (1,\mu(a)) \quad \text{and} \quad \lambda(j(a)) &= \lambda(1,a) = (1,f(1,-)v(-)(a)) \\ &= (1,v(-)(a)) = (1,\mu(a)); \end{aligned}$$

so that the square on the left commutes. One also has

$$p(\lambda(b,a)) = p(b,f(b,-).v(-)(a)) = b = \pi(b,a),$$

and this completes the proof.

Definition 1.23:

A generalized Schreier extension is a sequence of groups:

$$G_n \subset G_{n-1} \subset \ldots \subset G_1 \subset G_o = G$$

such that G_{i+1} is normal in G_i, for $i = 0,..,n-1$, and no subgroup of G_n is normal in G, except the trivial subgroup (1).

Theorem 1.24: (Marc Krasner and Léo Kaloujnine)

Suppose $K_n \subset K_{n-1} \subset \ldots \subset K_1 \subset K_o = K$ is a generalized Schreier extension. Then K can be embedded in the repeated wreath product

$$(K_{n-1}/K_n) \wr ((K_{n-2}/K_{n-1}) \wr (\ldots((K_1/K_2) \wr (K_o/K_1))\ldots)).$$

Lemma 1.25 (the case $n = 2$):

If $K_2 \subset K_1 \subset K_o = K$ is a generalized Schreier extension, then there exists a monomorphism $\lambda : K \longrightarrow (K_1/K_2) \wr (K_o/K_1)$, such that the following diagram commutes:

$$\begin{tikzcd} K_o \arrow[r, "\lambda"] \arrow[d] & (K_1/K_2) \wr (K_o/K_1) \arrow[d] \\ K_o/K_1 \arrow[r, equal] & K_o/K_1 \end{tikzcd}$$

Proof of the lemma:

Put $F_0 = K_0/K_1$ and $F_1 = K_1/K_2$. Let ℓ: $K_0 \longrightarrow K_1 \wr F_0$ be the embedding of theorem 1.22, obtained from the canonical exact sequence:

$$1 \to K_1 \longrightarrow K_0 \longrightarrow F_0 \longrightarrow 1$$

and let p_*: $K_1 \wr F_0 \longrightarrow F_1 \wr F_0$ be the homomorphism induced by the canonical projection p: $K_1 \longrightarrow F_1$, as explained in Proposition 1.21. We shall prove that the composition $\lambda = p_* \circ \ell$ gives the desired monomorphism.

Since the kernel of $p_* \circ \ell : K_0 \longrightarrow F_1 \wr F_0$ is normal in K_0, it suffices to prove that it is contained in K_2. We identify K_0 with the set $F_0 \times K_1$, the multiplication being given by a normalized 2-cocycle f: $F_0^2 \longrightarrow K_1$ and a mapping v: $F_0 \longrightarrow \mathrm{Aut}(K_1)$, satisfying the usual conditions ((i) and (ii) in the proof of th. 1.22). K_1 is identified with the subgroup $\{(1,g): g \in K_1\}$ of K_0. Suppose $g_0 \in K_0$ and $1 = p_*(\ell(g_0)) = p_*(b,\psi) = (b, p \circ \psi)$, where $b \in F_0$, $g_0 = (b,a)$, $\psi(x) = f(b,x).v(x)(a)$ for all $x \in F_0$. Then $b = 1$, $f(b,x) = 1$ and $p(v(x)(a)) = 1$ for all $x \in F_0$. The equality $b = 1$ implies $g_0 \in K_1$, so that, according to the above identification, g_0 and a are the same. Choosing $x = 1$, one obtains $p(a) = 1$, whence it follows that $g_0 \in K_2$; and the proof is completed by verifying that the following diagram of groups and homomorphisms, the rows of which are exact, is commutative: (see proposition 1.21 and theorem 1.22)

$$\begin{tikzcd}
1 \arrow[r] & K_1 \arrow[r] \arrow[d] & K_0 \arrow[r] \arrow[d] & F_0 \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & K_1^{F_0} \arrow[r] \arrow[d] & K_1 \wr F_0 \arrow[r] \arrow[d, "p_*"] & F_0 \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & F_1^{F_0} \arrow[r] & F_1 \wr F_0 \arrow[r] & F_0 \arrow[r] & 1
\end{tikzcd}$$

Proof of theorem 1.24:

If $n = 1$, theorem 1.22 gives the result, and if $n = 2$, then the result follows from lemma 1.25. We may, therefore, suppose that $n > 2$. Put $K_o^* = K_o$, and, for $j > 0$, define inductively K'_j and K_j^* by the formulas $K'_j = K^*_{j-1} \cap K_j$ and $K^*_j = \bigcap_{x \in K} x^{-1}.K'_j.x$. Then

$$K_2/K_2^* \subset K_1/K_2^* \subset K/K_2^*$$

is a generalized Schreier extension. Indeed, if $p\colon K \longrightarrow K/K_2^*$ denotes the canonical projection, and $H \subset K_2/K_2^*$ is a normal subgroup in K/K_2^*, then $p(x).h.p(x^{-1}) \in H$ for all $x \in K$ and $h \in H$. If $y \in K_2$ is a representative of h ,i.e $p(y) = h$, then $xyx^{-1} \in p^{-1}(H) \subset K_2$, so that $y \in x^{-1}K_2x$ for all $x \in K$. Thus, $y \in \bigcap_{x \in K} x^{-1}K_2x = K_2^*$, (note that $K'_2 = K_2$), for all y with $p(y) \in H$, and, hence, $H = (1)$.

Applying lemma 1.25, we obtain an embedding

$$k_1\colon K/K_2^* \longrightarrow \left(\frac{K_1/K_2^*}{K_2/K_2^*}\right) \wr \left(\frac{K/K_2^*}{K_1/K_2^*}\right) = F_1 \wr F_o$$

By induction, we will define embeddings

$$k_i\colon K/K^*_{i+1} \longrightarrow F_i \wr (F_{i-1} \wr (\dots(F_1 \wr F_o))\dots) \qquad (i = 1,..,n).$$

So, suppose that $k_1,..,k_{i-1}$ have been defined $(2 \leqslant i \leqslant n)$. One has $K'_{i+1} \subset K_i^*$ and $K^*_{i+1} \subset K^*_i$. We shall show that

$$K'_{i+1}/K^*_{i+1} \subset K^*_i/K^*_{i+1} \subset K/K^*_{i+1}$$

is a generalized Schreier extension. Let $\bar{p}\colon K \longrightarrow K/K^*_{i+1}$ denote the canonical projection. Suppose $\bar{H} \subset K'_{i+1}/K^*_{i+1}$ is a normal subgroup of K/K^*_{i+1}. Then, $p(x).h.p(x^{-1}) \in \bar{H}$, for all $x \in K$ and $h \in \bar{H}$. There exists

$y \in K$, such that $h = \overline{p}(y)$; $xyx^{-1} \in \overline{p}^{-1}(\overline{H}) \subset K^{*}_{i+1}K'_{i+1} = K'_{i+1}$.
Therefore, $y \in \bigcap_{x \in K} x^{-1}K'_{i+1}x = K^{*}_{i+1}$, $h = \overline{p}(y) = 1$, and $\overline{H} = (1)$.

Applying lemma 1.25, we obtain an embedding

$$\ell_i: K/K^{*}_{i+1} \longrightarrow \left(\frac{K^{*}_i/K^{*}_{i+1}}{K'_{i+1}/K^{*}_{i+1}}\right) \wr \left(\frac{K/K^{*}_{i+1}}{K^{*}_i/K^{*}_{i+1}}\right) = (K^{*}_i/K'_{i+1}) \wr (K/K^{*}_i).$$

From the monomorphisms: $K^{*}_i/K'_{i+1} \longrightarrow K_i/K_{i+1}$, (induced by the inclusion $K^{*}_i \subset K_i$), and

$$k_{i-1}: K/K^{*}_i \longrightarrow F_{i-1} \wr (F_{i-2} \wr (\dots((F_1 \wr F_o))\dots)),$$

(induction hypothesis), we obtain a monomorphism

$$\ell'_i: (K^{*}_i/K'_{i+1}) \wr (K/K^{*}_i) \longrightarrow F_i \wr (F_{i-1} \wr (\dots(F_1 \wr F_o))..)),$$

(see proposition 1.21). Finally, define $k_i = \ell'_i \circ \ell_i$. If $i = n$, then the gen. Schreier extension above, becomes $(1) \subset K^{*}_n \subset K$;

$$k_n: K \xrightarrow{\ell_n} K_n \wr (K/K_n) \xrightarrow{\ell'_n} K_n \wr (F_{n-1} \wr (\dots(F_1 \wr F_o))\dots))$$
$$= F_n \wr (F_{n-1} \wr (\dots(F_1 \wr F_o))\dots));$$

and k_n can be taken as the embedding mentioned in the statement of the theorem.

Theorem 1.26:

Suppose $\{G_i\}_{i \in \underline{\underline{N}}}$ is a (countable) family of finite p-groups, G_i is of order p^{m_i}, $m_i \in \underline{\underline{N}}$, $m_{i+1} \geqslant m_i$, and, for $j \geqslant i$, $\rho_{i,j}: G_j \longrightarrow G_i$ is an epimorphism, such that $\rho_{i,j} \circ \rho_{j,k} = \rho_{i,k}$, whenever $k \geqslant j \geqslant i$. Then, for every $i \in \underline{\underline{N}}$, there exists a monomorphism

$$\lambda_i: G_i \longrightarrow C_p^{(m_i)} = \underbrace{C_p \wr (C_p \wr (\dots(C_p \wr C_p))\dots))}_{m_i \text{ times}},$$

where $C_p = \underline{\underline{Z}}/p\underline{\underline{Z}}$, the cyclic group of order p.

Denote by $\pi_r^{r+1}: C_p^{(r+1)} \longrightarrow C_p^{(r)}$ the canonical projection: $(b,\psi) \longmapsto b$, and, for $m > r$, define $\pi_r^m = \pi_{m-1}^m \circ \pi_{m-2}^{m-1} \circ \ldots \circ \pi_r^{r+1}$. If $m = r$, π_r^m will denote the identity map. The monomorphisms λ_i can be defined in such a way that for every pair (i,j) of positive integers, with $j \geqslant i$, the following diagram commutes:

$$\begin{tikzcd} G_j \arrow[r, "\lambda_j"] \arrow[d, "\rho_{i,j}"'] & C_p^{(m_j)} \arrow[d, "\pi_{m_i}^{m_j}"] \\ G_i \arrow[r, "\lambda_i"'] & C_p^{(m_i)} \end{tikzcd}$$

<u>Proof</u>:

Every finite p-group G admits a decomposition series

$$(1) = G'_n \subset G'_{n-1} \quad \ldots \subset G'_o = G,$$

G'_i normal in G, and $G'_i/G'_{i+1} \cong C_p$, for $i = 0,\ldots,n-1$ (see, for instance, [21], Chap. IX, Cor. to th. 1);

$$G'_{n-1} \subset \ldots \subset G'_1 \subset G'_o = G$$

is a generalized Schreier extension, and it follows, by theorem 1.24, that G can be embedded into $C_p^{(n)}$.

The monomorphisms λ_i will now be defined inductively. For $i = 1$, we define λ_1 to be any embedding of G_1 into $C_p^{(m_1)}$. We make the induction hypothesis that $\lambda_j: G_j \longrightarrow C_p^{(m_j)}$ has been defined for $j = 1,..,i$, in such a way that the inequalities $1 \leqslant h \leqslant j \leqslant i$ imply commutativity of the diagram:

$$\begin{tikzcd}
G_j \arrow[r, "\lambda_j"] \arrow[d, "\rho_{j,h}"'] & C_p^{(m_j)} \arrow[d, "\pi^{m_j}_{m_h}"] \\
G_h \arrow[r, "\lambda_h"'] & C_p^{(m_h)}
\end{tikzcd}$$

If $m_{i+1} = m_i$, then $\rho_{i,i+1}: G_{i+1} \longrightarrow G_i$ is an isomorphism. Putting $\lambda_{i+1} = \rho\circ\lambda_i\circ\rho_{i,i+1}$, one obtains a commutative diagram: $(\rho(b) = (b,1))$

$$\begin{tikzcd}
G_{i+1} \arrow[r, "\lambda_{i+1}"] \arrow[d, "\rho_{i,i+1}"'] & C_p^{(m_{i+1})} \arrow[d, "\pi^{m_{i+1}}_{m_i}"] \\
G_i \arrow[r, "\lambda_i"'] & C_p^{(m_i)}
\end{tikzcd}$$

and the induction process can continue. It now suffices to suppose $m_{i+1} > m_i$, and to define λ_{i+1} in such a way that the above diagram commutes. Let

$$1 = H_{m_i} \subset H_{m_i-1} \subset \ldots \subset H_o = H = G_i$$

be a decomposition series for G_i, H_j normal <u>in H</u>, $H_j/H_{j+1} \cong C_p$, for all $j = 0,..,m_i-1$, ([21],Cor. to th. 1 of Chap. IX). Put $K_j = \rho^{-1}_{i,i+1}(H_j)$, $(j = 0,..,m_i)$, then $K_j/K_{j+1} \cong C_p$, $(j = 0,...,m_i-1)$ and K_j is normal in $K_o = K = G_{i+1}$. By[1], §6, th. 7, the sequence

$$K_{m_i} \subset K_{m_i-1} \subset \ldots \subset K_1 \subset K_o = K = G_{i+1}$$

can be extended to a decomposition series

$$(1) = K_{m_{i+1}} \subset K_{m_{i+1}-1} \subset \ldots \subset \underset{\substack{\| \\ \ker\rho_{i,i+1}}}{K_{m_i}} \subset \ldots \subset K_1 \subset K_o = K$$

(K_{j+1} normal <u>in K_j</u>, for $j = 0,\dots,m_{i+1}-1$).

From now on, we shall use the same notation as in theorem 1.24, ($m_{i+1} = n$).

<u>Claim</u>: for $j = 0,\dots,m_i$, $K_j^* = K_j' = K_j$.

<u>Proof</u>: By definition, $K_o^* = K_o$. Suppose $K_j^* = K_j$ for some j $(0 \leq j < m_i)$; then $K_{j+1}' = K_j^* \cap K_{j+1} = K_{j+1}$ and $K_{j+1}^* = \bigcap_{x \in K} x^{-1}K_{j+1}'x = \bigcap_{x \in K} x^{-1}K_{j+1}x = K_{j+1}$, because K_{j+1} is normal in K. This induction argument proves the claim.

Thus, $K_{m_i}^* = K_{m_i}$, and $\rho_{i,i+1}:G_{i+1} \longrightarrow G_i$ induces an isomorphism σ: $K/K_{m_i}^* \longrightarrow H = G_i$. For $j = 1,\dots,m_{i+1}-m_i$, let p_j: $K/K_{m_i+j}^* \longrightarrow K/K_{m_i+j-1}^*$ denote the canonical projection. There exist epimorphisms u_h ($h = 1,\dots,m_{i+1}-m_i$), and isomorphisms θ_j ($j = 0,\dots,m_{i+1}-m_i-1$), such that, for every j the following diagram commutes:

$$\begin{tikzcd}
K/K^{*}_{m_{i+1}} \arrow[r, "\Theta_{m_{i+1}-m_i} = 1"] \arrow[d, "p_{m_{i+1}-m_i}"] & K \arrow[d, "u_{m_{i+1}-m_i}"] \arrow[ddddddd, bend left=60, "\rho_{i,i+1}"] \\
K/K^{*}_{m_{i+1}-1} \arrow[r, "\Theta_{m_{i+1}-m_i-1}"] \arrow[d, "p_{m_{i+1}-m_i-1}"] & K/K^{*}_{m_{i+1}-1} \arrow[d, "u_{m_{i+1}-m_i-1}"] \\
\vdots \arrow[d, "p_{j+2}"] & \vdots \arrow[d, "u_{j+2}"] \\
K/K^{*}_{m_i+j+1} \arrow[r, equal] \arrow[d, "p_{j+1}"] & K/K^{*}_{m_i+j+1} \arrow[d, "u_{j+1}"] \\
K/K^{*}_{m_i+j} \arrow[r, "\Theta_j"] \arrow[d, "p_j"] & K/K^{*}_{m_i+j} \arrow[d, "u_j"] \\
\vdots \arrow[d, "p_2"] & \vdots \arrow[d, "u_2"] \\
K/K^{*}_{m_i+1} \arrow[r, equal] \arrow[d, "p_1"] & K/K^{*}_{m_i+1} \arrow[d, "u_1"] \\
K/K^{*}_{m_i} \arrow[r, "\Theta_o"] & H
\end{tikzcd}$$

(One may, for instance, define $u_1 = \sigma \circ p_1, \Theta_o = \sigma$; $u_j = p_j$ and $\Theta_{j-1} = 1$ for $j = 2,\dots,m_{i+1}-m_i$).

Let $v_{m_i} = \lambda_i : G_i \longrightarrow C_p^{(m_i)}$. By induction on $h = 0,\dots,m_{i+1}-m_i$, we shall define monomorphisms v_{m_i+h} such that each diagram:

$$\begin{tikzcd}
K/K^*_{m_i+h+1} \arrow[r, "v_{m_i+h+1}"] \arrow[d, "u_{h+1}"'] & C_p^{(m_i+h+1)} \arrow[d, "\pi^{m_i+h+1}_{m_i+h}"] \\
K/K^*_{m_i+h} \arrow[r, "v_{m_i+h}"] & C_p^{(m_i+h)}
\end{tikzcd}$$

commutes $(0 \leq h \leq m_{i+1}-m_i-1)$. For $h = 0$, v_{m_i+h} has already been defined. Suppose that $v_{m_i},\dots,v_{m_i+j}$ have been defined $(0 \leq j < m_{i+1}-m_i)$, and satisfy the above condition of commutativity of the diagram.

We have shown, in the proof of theorem 1.24, that

$$K'_{m_i+j+1}/K^*_{m_i+j+1} \subset K^*_{m_i+j}/K^*_{m_i+j+1} \subset K/K^*_{m_i+j+1}$$

is a generalized Schreier extension, and that one obtains from it a monomorphism

$$\ell_{m_i+j} : K/K^*_{m_i+j+1} \longrightarrow (K^*_{m_i+j}/K'_{m_i+j+1}) \wr (K/K^*_{m_i+j}),$$

(see also lemma 1.25). From the monomorphisms: $K^*_{m_i+j}/K'_{m_i+j+1} \to K_{m_i+j}/K_{m_i+j+1} = C_p$, (induced by the inclusion $K^*_{m_i+j} \subset K_{m_i+j}$) and $v_{m_i+j} \circ \Theta_j : K/K^*_{m_i+j} \longrightarrow C_p^{(m_i+j)}$, we obtain a monomorphism

$$\ell'_{m_i+j} : (K^*_{m_i+j}/K'_{m_i+j+1}) \wr (K/K^*_{m_i+j}) \longrightarrow C_p^{(m_i+j+1)}$$

such that $\pi^{m_i+j+1}_{m_i+j} \circ \ell'_{m_i+j} = v_{m_i+j} \circ \Theta_j \circ \pi_j$ (See Proposition 1.21 - the last equality corresponds to the equality $\pi' \circ \gamma = \beta \circ \pi$ in the statement of Proposition 1.21; the canonical projection π_j is indicated in the diagram below.) Finally, put $v_{m_i+j+1} = \ell'_{m_i+j} \circ \ell_{m_i+j}$ to obtain a commutative diagram:

$$\begin{tikzcd}
 & & \left(\frac{K^*_{m_i+j}/K^*_{m_i+j+1}}{K'_{m_i+j+1}/K^*_{m_i+j+1}}\right)\wr\left(\frac{K/K^*_{m_i+j+1}}{K^*_{m_i+j}/K^*_{m_i+j+1}}\right) \arrow[d, equal] & \\
K/K^*_{m_i+j+1} \arrow[r, equal] \arrow[d, "u_j"'] \arrow[rrr, bend left=40, "v_{m_i+j+1}"] & K/K^*_{m_i+j+1} \arrow[r, "\ell_{m_i+j}"] \arrow[d, "p_j"] & (K^*_{m_i+j}/K'_{m_i+j+1})\wr(K/K^*_{m_i+j}) \arrow[r, "\ell'_{m_i+j}"] \arrow[d, "\pi_j"] & C_p^{(m_i+j+1)} \arrow[d, "\pi^{m_i+j+1}_{m_i+j}"] \\
K/K^*_{m_i+j} \arrow[r, shift left, "\theta_j^{-1}"] \arrow[rrr, bend right=30, "v_{m_i+j}"'] & K/K^*_{m_i+j} \arrow[l, shift left, "\theta_j"] \arrow[r, equal] & K/K^*_{m_i+j} \arrow[r, "v_{m_i+j} \circ \theta_j"'] & C_p^{(m_i+j)}
\end{tikzcd}$$

(The centre square is commutative, by virtue of lemma 1.25). The induction process on j, can continue. We now define $\lambda_{i+1} = v_{m_{i+1}}$. The proof is complete, since the following diagram is commutative:

$$\begin{tikzcd}
G_{i+1} \arrow[r, phantom, "="] \arrow[dddd, "\varrho_{i,i+1}"'] & K \arrow[r, "\lambda_{i+1} = v_{m_{i+1}}"] \arrow[d, "u_{m_{i+1}-m_i}"] & C_p^{(m_{i+1})} \arrow[d, "\pi^{m_{i+1}}_{m_{i+1}-1}"] \arrow[dddd, bend left=60, "\pi^{m_{i+1}}_{m_i}"] \\
 & K/K^*_{m_{i+1}-1} \arrow[r, "v_{m_{i+1}-1}"] \arrow[d, "u_{m_{i+1}-m_i-1}"] & C_p^{(m_{i+1}-1)} \arrow[d, "\pi^{m_{i+1}-1}_{m_{i+1}-2}"] \\
 & \vdots \arrow[d, "u_2"] & \vdots \arrow[d, "\pi^{m_i+2}_{m_i+1}"] \\
 & K/K^*_{m_i+1} \arrow[r, "v_{m_i+1}"] \arrow[d, "u_1"] & C_p^{(m_i+1)} \arrow[d, "\pi^{m_i+1}_{m_i}"] \\
G_i \arrow[r, phantom, "="] & H \arrow[r, "\lambda_i = v_{m_i}"'] & C_p^{(m_i)}
\end{tikzcd}$$

Definition 1.27:

Relative to the maps π^m_r $(m > r)$, defined in the statement of theorem 1.26, the groups $C_p^{(n)}$ $(n = 1,2,\ldots)$ form a projective system. Its inverse limit will, henceforth, be denoted by $W = \varprojlim C_p^{(n)}$.

Theorem 1.28:

Every pro-p-group P, satisfying the second axiom of countability,[#] cam be continuously embedded in the pro-p-group $W = \varprojlim C_p^{(n)}$.

Proof:

P admits a countable neighborhood base $\{V_i\}_{i\in\underline{\underline{N}}}$ of the identity 1, consisting of open, compact and normal subgroups V_i of P ([18] Chap. I §1). We may, furthermore, assume that $V_i \subset V_j$, whenever $i > j$. (If not, replace each V_i by $V_i' = \bigcap_{1\leq j\leq i} V_j$). Denote by $\pi_{j,i}: P/V_i \longrightarrow P/V_j$ the canonical homomorphism. We shall now prove the well-known fact that P is isomorphic to $\varprojlim P/V_i$; (here, the inverse limit is taken relative to the maps $\pi_{j,i}$). For each $i\in\underline{\underline{N}}$, let $\pi_i: P \longrightarrow P/V_i$ denote the canonical projection, and let $\rho: P \longrightarrow \varprojlim P/V_i$ be the canonical continuous homomorphism obtained from the maps π_i, by invoking the universal property of the functor $\varprojlim$; (note that $\pi_{j,i}\circ\pi_i = \pi_j$, whenever $i > j$). Suppose that $p = (p_1, p_2, \ldots)$ represents an element of $\varprojlim P/V_i$ ($p_i \in P/V_i$, $\pi_{j,i}(p_i) = p_j$). For each $i\in\underline{\underline{N}}$, let q_i denote a representative in P of p_i. Since P is compact ([18], Chap. I§1) and the sets $q_iV_i \subset P$ satisfy the finite intersection property, one has $\phi \neq \bigcap_{i\in\underline{\underline{N}}} q_iV_i$. It is clear that $\rho(x) = p$, whenever $x \in \bigcap_{i\in\underline{\underline{N}}} q_iV_i$. Thus ρ is surjective, and, to prove that it is an isomorphism, it suffices to show that $\bigcap_{i\in\underline{\underline{N}}} q_iV_i$ consists of exactly one element; but this is immediate, because $\bigcap_{i\in\underline{\underline{N}}} V_i = (1)$, (loc cit). We may, therefore, identify P with $\varprojlim P/V_i$.

[#] Note that the first and second axioms of countability are equivalent, for profinite groups.

Suppose P/V_i is of order p^{m_i}, for all $i \in \underline{\underline{N}}$. According to theorem 1.26, there exists, for each $i \in \underline{\underline{N}}$, a monomorphism λ_i such that the following diagram commutes whenever $i \geqslant j$:

$$\begin{tikzcd} P/V_i \arrow[r, "\lambda_i"] \arrow[d, "\pi_{j,i}"] & C_p^{(m_i)} \arrow[d, "\pi^{m_i}_{m_j}"] \\ P/V_j \arrow[r, "\lambda_j"] & C_p^{(m_j)} \end{tikzcd}$$

Since theinverse system $\left\{C_p^{(m_i)}, \pi^{m_i}_{m_j}\right\}_{i,j\in\underline{\underline{N}},\ i\geqslant j}$ is cofinal to the inverse system $\left\{C_p^{(r)}, \pi^r_s\right\}_{r,s\in\underline{\underline{N}},\ r\geqslant s}$, we may identify W with $\underleftarrow{\lim}\ C_p^{(m_i)}$. The result now follows from the fact that $\underleftarrow{\lim}$ is a left exact functor from the category of inverse systems of finite pro-p-groups to the category of pro-p-groups. To be more explicit, we write $\lambda(p_1,p_2,\dots,) = (\lambda_1(p_1),\lambda_2(p_2),\dots)$ for all $p_i \in P/V_i$. Then $\lambda: P \longrightarrow \underleftarrow{\lim}\ C_p^{(m_i)}$ is a well-defined continuous homomorphism, and is injective, because each λ_i is injective.

<u>Proposition 1.29</u>:

$H^1(C_p^{(n)},\underline{\underline{Z}}/p\underline{\underline{Z}})$ and $H^1(W,\underline{\underline{Z}}/p\underline{\underline{Z}})$ are vector spaces of dimension n and $\aleph_0$ respectively, over the field $\underline{\underline{Z}}/p\underline{\underline{Z}}$ $(n\in\underline{\underline{N}})$. The groups $C_p^{(n)}$ and $W = \underleftarrow{\lim}\ C_p^{(n)}$ both have infinite cohomological dimension.

<u>Proof</u>:

The first statement is trivially true for n = 1. Suppose it holds for a given positive integer n. We shall prove it to be true for n+1. The dimension of $H^1(C_p^{(n)},\underline{\underline{Z}}/p\underline{\underline{Z}})$ over $\underline{\underline{Z}}/p\underline{\underline{Z}}$ can be charaterized as the cardinality of any (and every) minimal system of generators $\{\gamma_1,\dots,\gamma_n\}$ for the group $C_p^{(n)}$ ([18] ,Chap. I, cor. to prop. 25). Suppose that α generates C_p. One has, as before, a canonical split exact sequence:

$$\begin{tikzcd} 1 \arrow[r] & (\underline{\underline{Z}}/p\underline{\underline{Z}})^{C_p^{(n)}} \arrow[r, "k"] & C_p^{(n+1)} \arrow[r, shift left, "\pi_n^{n+1}"] & C_p^{(n)} \arrow[l, shift left, "\rho_n"] \arrow[r] & 1 \end{tikzcd}$$

We make a formal distinction between C_p and $\underline{\underline{Z}}/p\underline{\underline{Z}}$, in the sense that the former is written multiplicatively, and the latter additively; $(\underline{\underline{Z}}/p\underline{\underline{Z}})^{C_p^{(n)}}$ is the additive group of mappings from $C_p^{(n)}$ into $\underline{\underline{Z}}/p\underline{\underline{Z}}$, and the group operation in $C_p^{(n+1)}$, (defined on the set $C_p^{(n)}\times(\underline{\underline{Z}}/p\underline{\underline{Z}})^{C_p^{(n)}}$), is given by the formula:

$$(b_1,\psi_1)(b_2,\psi_2) = (b_1b_2,\psi_1^{b_2}+\psi_2) \quad (b_1,b_2\in C_p^{(n)}, \psi_1, \psi_2\in(\underline{\underline{Z}}/p\underline{\underline{Z}})^{C_p^{(n)}})$$

It follows from [18], Chap. I, prop. 25, that one can find a $\underline{\underline{Z}}/p\underline{\underline{Z}}$ - base $\delta_1,\dots,\delta_n$ for $H^1(C_p^{(n)},\underline{\underline{Z}}/p\underline{\underline{Z}}) = \mathrm{Hom}(C_p^{(n)},\underline{\underline{Z}}/p\underline{\underline{Z}})$, such that

$$\delta_i(\gamma_j) = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}$$

Define a mapping $\bar{\psi}$: $C_p^{(n)} \longrightarrow \underline{\underline{Z}}/p\underline{\underline{Z}}$, by putting

$$\bar{\psi}(t) = \begin{cases} 0 & \text{if } t \neq 1 \\ 1 & \text{if } t = 1. \end{cases}$$

Define a homomorphism $\bar{\varepsilon}$: $C_p^{(n+1)} \longrightarrow \underline{\underline{Z}}/p\underline{\underline{Z}}$ by the formula

$$\bar{\varepsilon}(b,\psi) = \sum_{t\in C_p^{(n)}} \psi(t) \ , \quad \text{for all } b\in C_p^{(n)}, \psi\in(\underline{\underline{Z}}/p\underline{\underline{Z}})^{C_p^{(n)}} .$$

We proceed to show that $\{\delta_1\circ\pi_n^{n+1},\dots,\delta_n\circ\pi_n^{n+1}, \bar{\varepsilon}\}$ is a linearly independent set of elements of $H^1(C_p^{(n+1)},\underline{\underline{Z}}/p\underline{\underline{Z}})$. Suppose $a_i\in\underline{\underline{Z}}/p\underline{\underline{Z}}$ $(i = 1,\dots,n+1)$ and $\sum_{i=1}^{n} a_i\, \delta_i\circ\pi_n^{n+1} + a_{n+1}\,\bar{\varepsilon} = 0$ ---------(X)

Then $0 = \sum_{i=1}^{n} a_i\delta_i(\pi_n^{n+1}(k(\bar{\psi}))) + a_{n+1}\bar{\varepsilon}(k(\bar{\psi})) = a_{n+1}$.

From (X), one now obtains

$$0 = \sum_{i=1}^{n} a_i(\delta_i(\pi_n^{n+1}(\rho_n(\gamma_j)))) = \sum_{i=1}^{n} a_i\delta_i(\gamma_j) = a_j \text{ , for } j = 1,..,n.$$

It follows that the elements $\delta_1\circ\pi_n^{n+1},\ldots,\delta_n\circ\pi_n^{n+1}$, $\bar{\varepsilon}$ are linearly independent over $\mathbb{Z}/p\mathbb{Z}$. In order to prove that dim.$(H^1(C_p^{(n+1)},\mathbb{Z}/p\mathbb{Z}) = n+1$, it now suffices to show that the subgroup H of $C_p^{(n+1)}$, generated by $\{\rho_n(\gamma_1),\ldots,\rho_n(\gamma_n),k(\bar{\psi})\}$, coincides with $C_p^{(n+1)}$ ([18], Chap I, cor. to prop. 25). Clearly $\rho_n(C_p^{(n)})\subset H$. For each $b\in C_p^{(n)}$, one has

$$k(\bar{\psi})\rho_n(b) = (1,\bar{\psi}).(b,1) = (1,\bar{\psi}^b), \text{ whence } (1,\bar{\psi}^b)\in H.$$

One immediately verifies that each $\psi\in(\mathbb{Z}/p\mathbb{Z})^{C_p^{(n)}}$ can be written in the form

$$\psi = \sum_{b\in C_p^{(n)}} \psi(b)\bar{\psi}^{b^{-1}}$$

Thus, $k((\mathbb{Z}/p\mathbb{Z})^{C_p^{(n)}})\subset H$. Since the groups $k((\mathbb{Z}/p\mathbb{Z})^{C_p^{(n)}})$ and $\rho_n(C_p^{(n)})$ generate $C_p^{(n+1)}$, we may now conclude that $H = C_p^{(n+1)}$, and the induction argument is complete.

Denoting by $(\pi_n^{n+1})^*: H^1(C_p^{(n)},\mathbb{Z}/p\mathbb{Z}) \longrightarrow H^1(C_p^{(n+1)},\mathbb{Z}/p\mathbb{Z})$ and $\rho_n^*: H^1(C_p^{(n+1)},\mathbb{Z}/p\mathbb{Z}) \longrightarrow H^1(C_p^{(n)},\mathbb{Z}/p\mathbb{Z})$ the homomorphisms induced by $\pi_n^{n+1}$and ρ_n , respectively, one has $\rho_n^*\circ(\pi_n^{n+1})^* = 1$. Thus, $(\pi_n^{n+1})^*$ is a monomorphism, mapping the base, described above, of $H^1(C_p^{(n)},\mathbb{Z}/p\mathbb{Z})$, onto the first n base vectors of $H^1(C_p^{(n+1)},\mathbb{Z}/p\mathbb{Z})$. It follows that the direct limit $H^1(W,\mathbb{Z}/p\mathbb{Z})$ of the direct system $\{H^1(C_p^{(n)},\mathbb{Z}/p\mathbb{Z}),(\pi_n^m)^*\}_{m>n}$, where $(\pi_n^m)^* = (\pi_{m-1}^m)^* \ldots (\pi_n^{n+1})^*$, is a vector space of dimension $\aleph_0$ over $\mathbb{Z}/p\mathbb{Z}$.

The last two statements: $cd_p(C_p^{(n)}) = \infty$ and $cd_p(W) = \infty$, present no difficulties. The group $\underline{\underline{Z}}/p\underline{\underline{Z}}$ can be embedded in $C_p^{(n)}$, because the maps ρ_m are monomorphisms, and can also be embedded in W, by theorem 1.28. One, therefore, has

$$\infty = cd_p(\underline{\underline{Z}}/p\underline{\underline{Z}}) \leqslant cd_p(C_p^{(n)})$$

and

$$\infty = cd_p(\underline{\underline{Z}}/p\underline{\underline{Z}}) \leqslant cd_p(W)$$

([18], Chap. I, prop. 14).

Chapter II: Applications to Field Theory.

Definition 2.1:

Suppose (G,S) is a permutation group, (definition 1.2), and K a field. Consider S as a set of indeterminates over the field K. If the field L of invariants, with respect to the K-automorphisms defined on K(S) by the elements of G, is purely transcendantal over K, then K is said to have the *property P(G,S)*.

Example:

Let T be any finite set of n elements, and S_n the symmetric group of all permutations of T. Then every field K has the property $P(S_n,T)$, because the field L of invariants is generated over K by the n symmetric functions in the elements of T.

The property P(G,S), defined above, derives its importance from its relation to the so-called *inverse problem of Galois theory*. This latter problem consists of asking for which pairs (K,G), K a field and G a finite (or profinite) group, there exists a Galois extension of K, with Galois group G. To make the relationship between the inverse problem of Galois theory and the property P(G,S) more explicit, let us assume that G and S are both finite and that $u_1,..,u_n$ are algebraically independent elements of K(S), such that

$K(u_1,..,u_n)$ is the field of all those elements of $K(S)$, (defined above), that are left fixed by all the K-automorphisms of $K(S)$, induced by the elements of G. Suppose now that

$$f(x) = \prod_{s\in S}(x-s) = x^n + a_1(u_1,..,u_n) + \ldots + a_n(u_1,..,u_n) \in K(u_1,..,u_n)[x]$$

(x is an indeterminate, $a_i(u_1,..,u_n)\in K(u_1,..,u_n)$ for all $i = 1,..,n$). It is possible, for a large class of pairs (K,G), to obtain a Galois extension M of K, with Galois group G, by a process of "specialization of the parameters $u_1,..,u_n$", outlined below. In particular, if K is an hilbertian field and G any finite group, then it is possible to "specialize" the $u_1,..,u_n$, by finding a family $u_1',..,u_n'$ of elements in K, having the following properties:

(i) $a_i(u_1',..,u_n')$ is well-defined for each $i = 1,..,n$;

(ii) the polynomial $f_1(x)\in K[x]$, obtained by replacing u_i by u_i' $(i = 1,,.,n)$ in the above expression for $f(x)$, is irreducible;

(iii) the splitting field M of $f_1(x)$ is a Galois extension of K, with Galois group G.

Conversely, W. Kuyk has proved that for K infinite, every finite Galois extension of K, can be obtained by such a specialization process, (see his paper: On a theorem of E. Noether, Proc. of Kon.Nederl.Ak. van Wetenschappen - series A,67,no.1). For more details on this subject and for a proof of the following th., see [13].

Theorem 2.2 (Hilbert and E. Noether):

If K is an hilbertian field, with the property $P(G,S)$, and G and S are finite, then there exists a Galois ext. $M|K$, with group G.

Theorem 2.3: (W. Kuyk)

Let L be a finite Galois extension of an hilbertian field K, with group A. Suppose that K has the property P(G,G), (G,G) being the regular representation of some finite group G (definition 1.3). Then K admits a Galois extension M, with Galois group $G\wr A$, and M is the splitting field of a polynomial g, having the property that the restriction of the K-automorphisms in $G\wr A$ to the roots of g, defines a permutation group isomorphic to $(G,G)\wr(A,A)$.

Proof:

Let $\{x_1,..,x_n\}$ be a family of indeterminates over K, n the cardinality of G, and let $(G,\{x_1,..,x_n\})$ be a (transitive and faithful) permutation group isomorphic to (G,G), (see 1.3, 1.4, 1.5 and 1.6). By hypothesis, $K(x_1,..,x_n)$ admits a subfield $K(u_1,..,u_n)$, with $u_1,..,u_n$ algebraically independent over K, such that G may be identified with the Galois group of the Galois extension $K(x_1,..,x_n)|K(u_1,..,u_n)$; i.e. the Galois group of the polynomial

$$f(X) = \prod_{i=1}^{n} (X - x_i) \in K(u_1,..,u_n)[X]$$

(X is an indeterminate). Note that the number of u_i's equals n, by the invariance of the transcendental degree of an extension, ([2] Chap. V, § 5, th.3). Let $\{w_1,..,w_a\}$ be a normal base of L|K (a = the cardinality of A - [2] Chap. V, § 10, def.3). Adjoin a family $t = \{t_{j,i}\}_{j=1,..,a;\ i=1,..,n}$ of indeterminates to L. Each one of the elements $\alpha_1,..,\alpha_a$ of A admits a canonical extension to L(t), determined by the formulas: $\beta_k(\ell) = \alpha_k(\ell)$ and $\beta_k(t_{j,i}) = t_{j,i}$ $(\ell \in L)$ $(i = 1,..,n;\ j=1,..,a;\ k = 1,..,a)$. The correspondance $\alpha_k \leftrightarrow \beta_k$ defines an isomorphism of the Galois groups of $L|K$ and $L(t)|K(t)$ ([2]Chap.V, §10, th.1). Define

$$v_{k,i} = \sum_{j=1}^{a} t_{j,i}\alpha_k(w_j) = \beta_k(v_{1,i}) \text{ --------}(Y),$$

where α_1 is taken to be the identity element of A, $(i = 1,..,n;\ j = 1,..,a;\ k= 1,..,a)$. Define $v_k = \{v_{k,1},\dots,v_{k,n}\}$ and $v = \bigcup_{k=1}^{a} v_k$.

<u>Claim</u>: The elements $v_{k,i}$ are algebraically independent over L and $L(v) = L(t)$.

<u>Proof</u>: The determinant $|\alpha_k(w_j)|$ is nonzero, because $w_1,\dots,w_a$ constitute a normal base for $L|K$ ([2] Chap. V §10 Prop.13). Therefore, the equations (Y) can be solved for $t_{k,i}$, whence $t_{k,i} \in L(v)$, for $k = 1,..,a$ and $i= 1,..,n$; i.e. $L(t) \subset L(v)$. By the definition of the set v, the opposite inclusion is valid too, and $L(t) = L(v)$. The algebraic independence over L of the set v, now follows immediately from the invariance of the transcendental degree ([2] Chap.V, §5 th.3), and this completes the proof of the claim.

Since the elements of v are algebraically independent over L, and, therefore, over K, one can define a K-isomorphism $\tau: K(u_1,..,u_n) \longrightarrow K(v_{1,1},\dots,v_{1,n})$, by putting $\tau(u_i) = v_{1,i}$, for all $i = 1,..,n$. Extend the domain and range of τ to the rings $K(u_1,..,u_n)[X]$ and $K(v_{1,1},\dots,v_{1,n})[X]$ respectively, by putting $\tau(X) = X$. Also extend the domain and range of the automorphisms β_k

to the ring $L(t)[X]$, by putting $\beta_k(X) = X$. Define

$$h = \prod_{k=1}^{a} \beta_k(\tau(f(X))) \in K(t)[X]$$

and denote by $z_k = \{z_{k,1},\dots,z_{k,n}\}$ $(k = 1,..,a)$ the roots of $\beta_k(\tau(f(X)))$ in some algebraic closure of $L(t)$. Put $z = \bigcup_{k=1}^{a} z_k$. We shall prove that the splitting field $L(z)$ of h is a Galois extension of $K(t)$, with Galois group $G \wr A$. First, the Galois groups of the extensions $K(x_1,..,x_n)|K(u_1,..,u_n)$ and $K(z_k)|K(v_k)$ are isomorphic $(k = 1,..,a)$, because $K(x_1,..,x_n)$ is the splitting field of $f(X) \in K(u_1,..,u_n)[X]$, whereas $K(z_k)$ is the splitting field of its isomorphic image $\beta_k(\tau(f(X))) \in \beta_k(\tau(K(u_1,..,u_n) = K(v_k)$. The next step is to prove that $L(z_k)|L(v_k)$ is a Galois extension, whose Galois group is also isomorphic to G. According to [2] ,Chap.V, §10, th.1, it suffices to prove that $K(v_k) = K(z_k) \cap L(v_k)$. So, let $M = K(z_k) \cap L(v_k)$. $L(z_k)|K(z_k)$ and $L(v_k)|K(v_k)$ both have Galois groups isomorphic to A (loc cit), since z_k and v_k are families of algebraically independent elements over K; (the elements of z_k are algebraically independent over K, because $K(z_k)|K(v_k)$ is an algebraic extension and because of the invariance of the transcendental degree of the extension $K(z_k)|K$ - see [2],Chap.V, §5, th.3); consequently $K(z_k) \cap L = K$ and $K(v_k) \cap L = K$).

$$\begin{tikzcd}
 & L(z_k) \arrow[dl, dash] \arrow[dr, dash, "A"] & \\
L(v_k) \arrow[dr, dash, "A"'] & & K(z_k) \arrow[dl, dash, "G"] \\
 & K(v_k) &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & L(z_k) \arrow[dl, dash] \arrow[dr, dash, "A"] & \\
L(v_k) \arrow[dr, dash, "A"'] & & K(z_k) \arrow[dl, dash] \\
 & M \arrow[d, dash] & \\
 & K(v_k) &
\end{tikzcd}$$

By [2] Chap.V§10, th.1, $L(v_k)|M$ has Galois group A. Thus $[L(v_k):M] = a$. But, $[L(v_k):K(v_k)] = a$ and $K(v_k) \subset M$. It follows that $K(v_k) = M$. So, we conclude that the Galois group of $L(z_k)|L(v_k)$ is isomorphic to G, $(k = 1,..,a)$.

Repeated application of lemma 2.4, stated at the end of this proof, allows us to conclude that $L(z)|L(v)$ is a Galois extension, with Galois group isomorphic to G^a. For the convenience of the reader, we include the following diagram of field extensions, with Galois groups as indicated:

$$\begin{tikzcd}
 & L(z) \arrow[dl, dash, "A"'] \arrow[dd, dash] \arrow[drr, dash, "G^{a-1}"] \arrow[dddrr, dash, "G^a"] & & & \\
K(z) \arrow[dd, dash] & & & L(v_1,..,v_{k-1},z_k,v_{k+1},..,v_a) \arrow[dd, dash, "G"] & \\
 & L(z_k) \arrow[dl, dash, "A"'] \arrow[dd, dash, "G"] & & & \\
K(z_k) \arrow[dddr, dash, "G"'] & & & L(v) \arrow[r, phantom, "="] \arrow[dll, dash] \arrow[dd, dash, "A"] & L(t) \arrow[dd, dash, "A"] \\
 & L(v_k) \arrow[dd, dash, "A"] & & & \\
 & & & K(v) \arrow[dll, dash] \arrow[dd, dash] & K(t) \arrow[ddl, dash] \\
 & K(v_k) \arrow[drr, dash] & & & \\
 & & & K &
\end{tikzcd}$$

In the calculation of the indicated Galois groups, one makes repeated use of the fact that if $W|V$ is a finite Galois extension, and Y a family of indeterminates, then $W(Y)|V(Y)$ is a Galois extension with Galois group isomorphic to the Galois group of $W|V$ ([2] Chap.V,§10, th.1).

(Note that $V(Y) \cap U = V$, whenever U is an algebraic extension of V.) In particular, this argument, in conjunction with lemma 2.4 below, allows us to conclude that $L(z) \mid L(v_1,\ldots,v_{k-1},z_k,v_{k+1},\ldots,v_a)$ has Galois group G^{a-1} (a product of a-1 copies of G).

We now proceed to show that the elements of z are conjugate to one another over K(t). Since L(z) is the splitting field of h, $L(z) \mid K(t)$ is normal ([2] Chap.V §6,cor. of Prop. 9). By §6, Prop. 7 (loc cit), every K(t)-automorphism β_k on L(t), can be extended to a K(t)-automorphism of L(z). Note that the set $\beta_k(v_j)$ is of the form v_h. Suppose that β_k' is a K(t)-automorphism of L(z), that extends β_k; then each element of the set $\beta_k'(z_j)$ is algebraic over $L(v_h)$. On the other hand, none of the elements of $\beta_k'(z_j)$ are algebraic over $L(v_\ell)$, for $\ell \neq h$, because the fields $L(v_1),\ldots,L(v_a)$ are algebraically disjoint over L ([2] Chap. V §5, Prop. 4, Prop. 9 and its corollaries). It follows that $\beta_k'(z_j) = z_h$. We see from this that the sets $z_1,\ldots,z_a$ are imprimitivity domains ([6]) for a collection C of K(t)-automorphisms of L(z), that permute the family of sets $\{z_1,\ldots,z_a\}$ <u>transitively</u>. The K-isomorphism $\tau: K(u_1,\ldots,u_n) \longrightarrow K(v_1)$ admits an extension $\tau': K(x_1,\ldots,x_n) \rightarrow K(z_1)$ ([2] Chap.V,§4, cor. to th. 1). Each set $z_j = \{z_{j,1},\ldots,z_{j,n}\}$ is permuted <u>transitively</u> by a collection $C_j = \{\beta_j' \circ \tau' \circ \sigma \circ \tau'^{-1} \circ (\beta_j')^{-1} ; \sigma \in G =$ the Galois group of $K(x_1,\ldots,x_n) \mid K(u_1,\ldots,u_n)\}$ (β_j' extends β_j) of K(t)-automorphisms <u>on $L(z_j)$</u>. Given two arbitrary elements of z, it is possible to compose an element of C, with a K(t)-automorphism of L(z), that extends some element of $\bigcup_{j=1}^{a} C'_j$ ([2] Chap. V, §6 Prop. 7), to obtain a K(t)-automorphism, mapping the one element of z onto the other. Thus, the elements of z are conjugate to one another (and h is irreducible over K(t)). All the elements of z are distinct; in fact they are algebraically independent over L, because L(z) is an algebraic extension of L(v), which is of transcendental degree n.a over L ([2] Chap.V §5, th.3). Thus, h is a separable polynomial and $L(z)|K(t)$ is a Galois extension, with Galois group H, say.

We now show that $(1)\subset G^{a-1}\subset G^a\subset H$ is a generalized Schreier extension (definition 1.23), corresponding (in the sense of the fundamental theorem of Galois theory ([2] Chap.V §10, th.3)), to the field extensions: $L(z)\supset L(v_1,..,v_{k-1}z_k,v_{k+1},..,v_a)\supset L(t)\supset K(t)$. By the fundamental theorem of Galois theory (loc cit), it suffices to prove that the only extension N of $L(v_1,..,v_{k+1},z_k,v_{k+1},..,v_a)$, such that $N\subset L(z)$ and $N|K(t)$ is normal, is L(z) itself; (in terms of the groups, this would then mean that (1) is the only subgroup of G^{a-1}, that is normal in H). Since all the elements of z are conjugate to one another over K(t), any normal extension of K(t), containing one of them, must contain them all, whence $N = L(z)$.

By the embedding theorem 1.24, H can be embedded in $(G^a/G^{a-1})\wr(H/G^a) = G\wr A$. But, $[L(z):K(t)] = an^a$ = the cardinality of $G\wr A$. Thus, the cardinality of H equals that of $G\wr A$, and $H\cong G\wr A$.

It follows from the irreducibility theorem of Hilbert (see [13]), that there exist elements $\{t'_{j,i}: j = 1,..,a;\ i = 1,..,n\}$ in K, having the property that substitution of $t'_{j,i}$ for $t_{j,i}$, $(j = 1,..,a;\ i = 1,...,n)$, in the coefficients of the polynomial h, yields a polynomial $g \in K[X]$, with Galois group isomorphic to $G \wr A$; i.e. by adjoining to K the set z' of all the roots of g, one obtains a Galois extension M of K, with Galois group $H' \cong H$. Since the permutation groups (H',z') and (H,z) are isomorphic, it now only remains to prove that (H,z) is isomorphic to $(G,G)\wr(A,A) = (G\wr A, G\times A)$. In doing so, we shall also give an *explicit* isomorphism $H \cong G\int A$. From the *existence* of such an isomorphism, proved above, and the fact that the canonical exact sequence $1 \to G^a \to G\wr A \to A \to 1$ *splits*, we deduce that each K(t)-auto. β_k of L(t), can be extended to a K(t)-auto. $\bar{\alpha}_k$ of L(z), *in such a manner that:*

$$\bar{\alpha}_i . \bar{\alpha}_j = \bar{\alpha}_k \Longleftrightarrow \beta_i . \beta_j = \beta_k \Longleftrightarrow \alpha_i . \alpha_j = \alpha_k$$

One can define an action of A on $\{1,..,a\}$, in such a way that the permutation groups $(A,\{1,..,a\})$, $(A,\{v_1,..,v_a\})$, $(A,\{z_1,..,z_a\})$ and (A,A) are all isomorphic, and one may index the elements of $z \cup v$ in such a way that:

$$\bar{\alpha}_i(v_j) = \beta_i(v_j) = v_{\alpha_i(j)} \ ; \quad \bar{\alpha}_k(z_{j,h}) = z_{\alpha_k(j),h}$$

$(i = 1,..,a;\ j = 1,..,a;\ k = 1,..,a;\ h = 1,..,n)$.

(In the second and third of the above permutation groups, the action is derived from the fact that the sets $v_1,..,v_a$ and $z_1,..,z_a$ are imprimitivity domains, w.r.t. $\{\bar{\alpha}_1,..,\bar{\alpha}_a\}$). Define a mapping $\varepsilon : G\wr A \to H$, by putting $\varepsilon(\alpha_k,\psi) = \bar{\alpha}_k . \psi$ for all $\psi \in G^a$. (We shall write the elements ψ of G^a as mappings from the set $\{1,..,a\}$ into G, and we identify G^A with G^a). G^a may be considered to act on z according to the formula $\psi(z_{j,i}) = z_{j,\psi(j)(i)}$, (see the proof of lemma 2.4), G acting on $\{1,..,n\}$ in such a way that $(G,\{1,..,n\}) \cong (G,G)$. One then has $(\bar{\alpha}_1 \circ \psi_1 \circ \bar{\alpha}_2 \circ \psi_2)(z_{j,i}) =$

$$= (\bar{\alpha}_1 \circ \psi_1 \circ \bar{\alpha}_2)(z_{j,\psi_2(j)(i)}) = \bar{\alpha}_1(\psi_1(z_{\alpha_2(j),\psi_2(j)(i)}) = \bar{\alpha}_1(z_{\alpha_2(j),\psi_1(\alpha_2(j))(\psi_2(j)(i))}$$
$$= z_{(\alpha_1 \cdot \alpha_2)(j),(\psi_1^{\alpha_2} \cdot \psi_2)(j)(i)} \,.$$

These calculations show that

$$\varepsilon : H \longrightarrow G \wr A$$

is a homomorphism of groups, therefore an isomorphism, (by comparison of cardinalities). These calculations also show that the elements of H act on the roots $z_{j,i}$ of h, in the "same manner" as $G \wr A$ acts on $G \times A$, (see definition 1.7). To be more precise, it is possible to define bijective mappings

$$\varepsilon' : G \times A \longrightarrow z$$
$$\rho' : \{1,..,n\} \times \{1,..,a\} \longrightarrow G \times A,$$

as well as a group isomorphism ρ , in such a way that one obtains isomorphisms of permutation groups

$$(H,z) \xrightarrow[\cong]{(\varepsilon,\varepsilon')} (G,G) \wr (A,A) = (G \wr A, G \times A) \xleftarrow[\cong]{(\rho,\rho')} (G,\{1,..,n\}) \wr (A,\{1,..,a\}).$$

This completes the proof of the theorem (modulo the following lemma).

<u>Lemma 2.4</u>:

Suppose $y_1,...,y_n$; $z_1,...,z_m$ are indeterminates over a field K, Let G and H be groups of orders n and m respectively, operating regularly on the sets $y = \{y_1,...,y_n\}$ and $z = \{z_1,...,z_m\}$ respectively, (i.e. (G,y) and (H,z) are transitive permutation groups, isomorphic to (G,G) and (H,H) respectively). Suppose that the fields of invariants, relative to the K-automorphisms induced on K(y) and K(z) by G and H, are

$K(v_1,\dots,v_n)$ and $K(w_1,\dots,w_m)$ respectively. Suppose, furthermore, that the set $\{v_1,\dots,v_n\}\cup\{w_1,\dots,w_m\}$ is algebraically independent over K. Then $K(y,z)\,|\,K(v,w)$, (where $v=\{v_1,\dots,v_n\}$ and $w=\{w_1,\dots,w_m\}$), is a Galois extension, with Galois group isomorphic to $G\times H$.

$$\begin{tikzcd}
 & K(y,z) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "G\times H"] & \\
K(y) \arrow[dd, dash, "G"'] & & K(z) \arrow[dd, dash, "H"] \\
 & K(v,w) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash] & \\
K(v) \arrow[dr, dash] & & K(w) \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

Proof:

Let $f(x)$ and $g(x)$ denote minimal polynomials of the respective extensions $K(y)\,|\,K(v)$ and $K(z)\,|\,K(w)$, with respective sets of roots y and z, (x is an indeterminate). $K(y,z)\,|\,K(v,w)$ is a Galois extension, because it is the splitting field of the separable polynomial $f(x).g(x)$. Let X denote its Galois group. Every automorphism in X transforms the set y into itself, because the elements of y are roots of the polynomial $f(x)$, with coefficients in $K(v)\subset K(v,w)$. The same applies to the set z. Since the set $y\cup z$ is algebraically independent over K, the homomorphism $\lambda: X\longrightarrow G\times H$, which is well-defined by the formula $\lambda(\xi)=(\xi\,|\,K(y),\xi\,|\,K(z))$, is surjective. It is obviously injective, whence the result.

Theorem 2.5:

Let K be an hilbertian field, with property $P(\mathbb{Z}/p\mathbb{Z},\mathbb{Z}/p\mathbb{Z})$. Then there exists a Galois extension E of K, with Galois group W, (see definition 1.27). To every pro-p-group G, satisfying the second axiom of countability, there corresponds a Galois extension $M|L$, where L is some algebraic p-extension of K, such that G is the Galois group of $M|L$. In particular, G is the Galois group of a Galois extension $M_1|L_1$, where L_1 is some subfield of the field of all algebraic numbers.

Proof:

By theorem 2.2, K admits a Galois extension L', with Galois group $C_p \cong \underline{\underline{Z}}/p\underline{\underline{Z}}$. By repeated application of theorem 2.3, K admits Galois extensions K_n, with Galois groups $C_p^{(n)}$, $(n = 1,2,\ldots)$, and, therefore, it also admits a Galois extension $E = \underset{\longrightarrow}{\lim}\, K_n$, with Galois group $W = \underset{\longleftarrow}{\lim}\, C_p^{(n)}$; ($C_p^{(n)}$ and W are defined in the statement of theorem 1.26 and definition 1.27).

The second statement of the theorem follows from the fundamental theorem of Galois theory ([2] Chap.V, appendice II, th.1), and from the embedding theorem 1.28.

Finally, Masuda has proved that every field F, containing the p-th roots of unity, $p \neq$ the characteristic of K, has the property $P(\underline{\underline{Z}}/p\underline{\underline{Z}},\underline{\underline{Z}}/p\underline{\underline{Z}})$, ([10], [16]). The last statement of the theorem follows from this, and from the fact that the algebraic number fields are hilbertian ([13]).

PART II

Chapter III

Derivations of pro-p-groups and Applications to Cohomology Theory

1. Preliminaries; the mappings d and $\frac{\partial}{\partial x_i}$

Let $F(n)$ be the free pro-p-group on n generators $x_1,\dots, x_n$ The completed group algebra $\mathbb{Z}_p[[F(n)]]$ of $F(n)$ is isomorphic to the magnus algebra $A(n)$ of formal power series (not necessarily commutative) in n indeterminates $T_1,\dots, T_n$, with coefficients in $\mathbb{Z}_p$ (see [14]). This algebra is endowed with the topology of convergence of the coefficients. By means of the identifications $x_i = 1 + T_i$ $(i = 1,\dots, n)$, $F(n)$ can be considered as a compact, totally disconnected multiplicative subgroup of $A(n)$ ([14] and [18]).

We shall define continuous maps $d\colon A(n) \to A(n)^n$ and $\frac{\partial}{\partial x_i} : A(n) \to A(n)$ for $i = 1,\dots, n$. They are not derivations in the sense of [2] Chapter IV, but can be considered as extensions of the maps in [15], denoted by the same symbols, and defined on the dense subgroup $L(n)$ of $F(n)$, generated algebraically by $x_1,\dots, x_n$. Let M be the free monoid consisting of 1 and all products of the form $T_{i_1} \dots T_{i_k}$, and write the elements a of $A(n)$ as follows $a = \sum_{m\in M} a_m m$ $(a_m \in \mathbb{Z}_p)$, where the p-adic integer a_1 will be referred to as the constant term of a. The product $A(n)^n$ is a compact Z_p-algebra and a free $A(n)$-module, generated by the canonical base $\varepsilon_1 = (1, 0,\dots, 0),\dots, \varepsilon_n = (0,\dots, 0, 1)$. We write $da = \sum_{m \in M} a_m \, dm$ and $\frac{\partial a}{\partial x_i} = \sum_{m \in M} a_m \frac{\partial m}{\partial x_i}$ $(i = 1, \ldots, n)$, where, for every $m \in M$ of the form $T_{i_1} \ldots T_{i_k}$, dm and $\frac{\partial m}{\partial x_i}$ are defined by the following formulas:

$$dm = m \, \varepsilon_{i_k}$$

$$\frac{\partial m}{\partial x_i} = \begin{cases} T_{i_1} \ldots T_{i_{k-1}} & \text{if } i = i_k \quad \text{(we shall agree that } T_{i_o} = 1\text{)} \\ 0 & \text{if } i \neq i_k \end{cases}$$

and $dm = 0$, $\frac{\partial m}{\partial x_i} = 0$ if $m = 1$.

Proposition 3.1:

The mappings $d\colon A(n) \to A(n)^n$ and $\frac{\partial}{\partial x_i}\colon A(n) \to A(n)$, defined above, are continuous and satisfy the following identities:

(1) $d(a + b) = da + db$

(2) $d(ab) = (da)b_1 + adb$ (b_1 denotes the constant term of b)

(3) If $a \in A(n)$ is invertible, then its constant term a_1 is invertible in $\underline{\underline{Z}}_p$ (and vice versa); we have $d(a^{-1}) = -a^{-1} a_1^{-1} da$.

(4) $db = \sum_{i=1}^{n} \frac{\partial b}{\partial x_i} dx_i$ and the elements dx_i are linearly independent over $A(n)$.

(5) $d(x_{i_1}^{e_1} \ldots x_{i_m}^{e_m}) = \sum_{k=1}^{m} x_{i_1}^{e_1} \ldots x_{i_{k-1}}^{e_{k-1}} d(x_{i_k}^{e_k})$, where $e_i = \pm 1$, $d(x_i^{-1}) = -x_i^{-1}$ d

$x_{i_o} = 1$ and $\{i_1, \ldots, i_m\}$ $\{i, \ldots, n\}$ (compare with eq. (2) §3 of [15])

(6) $\sum_{i=1}^{n} \frac{\partial b}{\partial x_i} T_i = b - b_1$

(7) In (1), (2), (3) and (5) the letter d may be replaced by $\frac{\partial}{\partial x_i}$.

Proof:

Continuity of the maps d and $\frac{\partial}{\partial x_i}$ is obvious. The first formula is an immediate consequence of the definition of d.

In order to prove (2), we write $a = \sum_{m \in M} a_m m$, $b = \sum_{m \in M} b_m m$ and

$$ab = \sum_{m \in M} a_m b_1 m + \sum_{v \in M} \sum_{mu=v, u \neq 1} a_m b_u v \quad .$$

Denote by $p_i : A(n)^n \to A(n)$ i-th canonical projection $(i = 1, \ldots, n)$ and, for every $m \in M$, put

$$\delta_{m,i} = \begin{cases} 0 & \text{if } m = 1 \text{ or } m = T_{i_1} \ldots T_{i_k} \text{ and } i_k \neq i \\ 1 & \text{if } m = T_{i_1} \ldots T_{i_k} \text{ and } i = i_k \ . \end{cases}$$

Then $p_i(da) = \sum a_m \delta_{m,i} m$. For $1 \neq u \in M$, $m \in M$, $\delta_{mu,i} = \delta_{u,i}$ and $p_i(m \cdot du) = \delta_{u,i} mu = p_i(d(mu))$, so that

$$p_i(d(ab)) = \sum_{m \in M} a_m b_1 \delta_{m,i} m + \sum_{v \in M} \sum_{mu=v, u \neq 1} a_m b_u \delta_{u,i} v$$

$$= p_i(d(a)b_1 + ad(b)) \text{ for all } i = 1, \ldots, n.$$

The formula (2) follows.

One may verify (3) by making use of (2), or by writing a^{-1} as a formal power series.

One has $dx_i = T_i \varepsilon_i$ and $\sum_{i=1}^{n} \frac{\partial m}{\partial x_i} T_i \varepsilon_i = dm$. Formulas (4) and (5) are now immediately verified. Let us point out, once and for all, that every element of F(n) has constant term 1. This fact, together with (2), immediately gives (5). To prove (7) one may use (4).

2. Derivations and their composites.

Definition 3.2:

Let H be a closed subgroup of F(n) and B a (left) topological F(n)-module. A derivation of H into B is a continuous mapping $\delta: H \to B$, with the property that $\delta(fg) = \delta(f) + f\delta(g)$, for all $f,g \in H$.

Definition 3.3:

Every continuous mapping $d: A(n) \to A(n)$, satisfying identities (1) and (2) of Proposition 3.1, will be called a derivation.

Remarks:

(i) The restriction of a derivation to a closed subgroup H of F(n) is a derivation of H into A(n) (A(n) will always be considered to be endowed with its canonical structure of F(n)-module, defined by left multiplication).

(ii) The set S of derivations from a closed subgroup H of F(n), into A(n), form a right module with respect to the operations defined below:

$$(\delta_1 + \delta_2)(h) = \delta_1(h) + \delta_2(h)$$
$$(\delta_1 \cdot f)(h) = \delta_1(h) \cdot f \quad \text{for all } f \in F(n),$$

δ_1, $\delta_2 \in S$, $h \in H$. Similarly, the set of all derivations: $A(n) \to A(n)$ form a right $F(n)$-module.

(iii) The mappings $\frac{\partial}{\partial x_i}$ defined in §1, are derivations, and so is the mapping $\delta\colon A(n) \to A(n)$, defined by the formula $\delta(a) = a - a_1 = \sum_{1 \neq m \in M} a_m m$ for all $a \in A(n)$ (see Proposition 3.1). Direct calculation, (or formula (6) of Proposition 3.1) shows that δ is a derivation. It will be called the inner derivation.

(iv) The mapping $d\colon A(n) \to A(n)^n$ defined in §1, induces, by restriction to $F(n)$, a derivation of $F(n)$ into $A(n)^n$ (the product $A(n)^n$ is a (left) $F(n)$-module, with respect to left multiplication by elements of $F(n)$).

Definition 3.4:

Every derivation of a closed subgroup H of $F(n)$ into $A(n)$, will be called a special derivation of H into $A(n)$, if the constant term of each one of its images, is zero.

Lemma 3.5:

Suppose $\delta_1\colon A(n) \to A(n)$ is a derivation and δ_2 a special derivation of a closed subgroup H into $A(n)$. Then $\delta_1 \circ \delta_2$ is a derivation of H into $A(n)$.

Proof:

$$\begin{aligned}\delta_1(\delta_2(uv)) &= \delta_1(\delta_2(u) + u\delta_2(v)) \\ &= (\delta_1 \circ \delta_2)(u) + \delta_1(u)\ (\delta_2(v))_1 + u\cdot(\delta_1 \circ \delta_2)(v) \\ &= (\delta_1 \circ \delta_2)(u) + u\cdot(\delta_1 \circ \delta_2)(v).\end{aligned}$$

Definition 3.6:

The *natural augmentation* $\varepsilon\colon A(n) \to \mathbb{Z}_p$ maps every formal power series a onto its constant term a_1.

Remarks 3.7:

(i) ε is a continuous $\mathbb{Z}_p$-module homomorphism, extending the natural augmentation of the group algebra $\mathbb{Z}_p[F(n)]$, of the group $F(n)$ over the ring $\mathbb{Z}_p$, the algebra $\mathbb{Z}_p[F(n)]$ being dense in $A(n)$ ([14]).

(ii) Put $\tau_i = \varepsilon \circ \frac{\partial}{\partial x_i}$ $(i = 1,\dots, n)$. For every $a,b \in F(n)$ and $\lambda \in \mathbb{Z}_p$, one has $\tau_i(a.b) = \tau_i(a + b) = \tau_i(a) + \tau_i(b)$; $\tau_i(\lambda a) = \lambda\tau_i(a)$ and $\tau_i(a) = a_{T_i}$. To prove this, one writes a and b as formal power series.

(iii) If $a \in L(n) =$ the free discrete and dense subgroup of $F(n)$ generated *algebraically* by $x_1,\dots, x_n$, then $\tau_i(a)$ is the *exponent* ([15] §10, p.66) of x_i in the word a. More generally, if $c_1,\dots, c_m$ are *p-adic integers*, then $\tau_i(x_{i_1}^{c_1} \dots x_{i_m}^{c_m}) = \sum\limits_{i=i_r} c_r$ (for definition of p-adic exponents in a pro-p-group, see [14]).

Definition 3.8:

The *algebra D* is defined to be the free associative algebra over $\mathbb{Z}_p$, on the generators $\frac{\partial}{\partial x_i},\dots, \frac{\partial}{\partial x_n}$. The algebra D is graded by declaring the homogeneous component of degree one to consist of all linear combinations of the generators. The homogeneous component of degree k, of the algebra D is denoted by D_k. Each element of D can be considered as an endomorphism of the additive structure of $A(n)$, by interpreting multiplication in D, as composition of endomorphisms.

Remark 3.9:

For every sequence of integers $(i_1,\ldots, i_k)$, contained in $\{1,\ldots, n\}$, and every $a \in A(n)$, one has

$$\left(\varepsilon \circ \frac{\partial}{\partial x_{i_1}} \circ \cdots \circ \frac{\partial}{\partial x_{i_k}}\right)(a) = a_m ,$$

where $m = T_{i_1} \ldots T_{i_k}$ (and a_m is the coefficient of m in the formal series expansion of a).

Notations 3.10:

Let M_X denote the free magma on $X = \{x_1,\ldots, x_n\}$. (see [19]). M_X consists of non-associative words in $x_1,\ldots, x_n$. The length of a word $u \in M_X$ will be denoted by $\ell(u)$. The length of an associative word $m \in M$ = the free monoid on $\{T_1,\ldots, T_n\}$, will also be denoted by $\ell(m)$. A mapping $\phi: M_X \to F(n)$ is uniquely defined by the equalities

$$\phi(x_i) = x_i \qquad (i = 1,\ldots, n)$$

$$\phi(u\cdot v) = (\phi(u), \phi(v)) = \phi(u)\cdot\phi(v)\cdot\phi(u)^{-1}\ \phi(v)^{-1} .$$

Define inductively $F = F_1 = F(n)$, $F_{i+1} = (F_i, F)$, for every positive integer i. $((F_i, F)$ denotes the smallest closed normal subgroup, of F containing all the commutators (s,t), $s \in F_i$, $t \in F)$. Put $F_i' = \{t \in F(n): t_m = 0$, whenever $1 < \ell(m) < i\}$ and define $\mathrm{gr}_i\, F = F_i/F_{i+1}$, $\mathrm{gr}\, F = \sum_{i=1}^{\infty} \mathrm{gr}_i\, F$. The abelian group $\mathrm{gr}\, F$ is endowed with the structure of a Lie algebra over $\underline{\underline{Z}}_p$, in the usual manner (see below). Finally, let $I = \ker \varepsilon =$ the ideal in $A(n)$ generated by $T_1, \ldots, T_n$.

<u>Theorem 3.11</u>:

With the above notations, one has

(a) $F_i = F_i' = F \cap (1 + I^i)$ for every positive integer i.

(b) $\mathrm{gr}\, F$ is a free Lie algebra over $\underline{\underline{Z}}_p$, on the canonical images of $x_1, \ldots, x_n$.

(c) The restriction to F_k, of every element of D_k, is a derivation δ_k of F_k into $A(n)$, and $\varepsilon \circ \delta_k: F_k \to \underline{\underline{Z}}_p$ is a homomorphism of groups.

(d) Let $(i_1, \ldots, i_k)$ be a sequence of integers from the set $\{1, \ldots, n\}$. Put

$$\partial_{1,\ldots,k} = \varepsilon \circ \frac{\partial}{\partial x_{i_1}} \circ \cdots \circ \frac{\partial}{\partial x_{i_k}} \circ \phi: M_X \to \underline{\underline{Z}}_p \ .$$

Suppose $t = q \cdot s \in M_X$; q,s and t being words of lengths $j(\geqslant 1)$, $h(\geqslant 1)$ and $k = j + h$, respectively. Then

$$\partial_{1,\ldots,k}(t) = \partial_{1,\ldots,j}(q)\ \partial_{j+1,\ldots,k}(s) - \partial_{h+1,\ldots,k}(q)\ \partial_{1,\ldots,h}(s) \ .$$

Proof:

Let L_X denote the free Lie algebra on $X = \{x_1,..., x_n\}$, over $\underline{\underline{Z}}_p$ (see [19]). gr F is a Lie algebra over $\underline{\underline{Z}}_p$, with respect to the bracket operation, which is well-defined on the homogeneous components of gr F, by taking for $[x,y]$ $(x \in gr_h F, y \in gr_k F)$ the class of the commutator (x', y'), of two representatives $x', y' \in F$ of x and y respectively. The bracket operation is then extended to the whole of gr F, by linearity (see [14] or [19]). By the universal property of L_X, (loc cit), the mapping $\rho \circ \phi: X \to$ gr F, where ρ is the canonical mapping $F \to$ gr F, induces a morphism $\nu: L_X \to$ gr F of Lie algebras. We proceed to prove that ν is surjective. Later, we shall see that ν is an isomorphism. Denote by M_X^k the subset of M_X, consisting of all words of length k. We shall show, by induction on k, that the conjugates of the elements of $\phi(\bigcup_{j\geq k} M_X^j)$, generate algebraically a dense subgroup of F_k. For $k = 1$, the statement is true, because M_X^1 generates algebraically a dense subgroup $L(n)$ of F. Suppose that the statement is true for a given positive integer k. Denote by H_{k+1} the subgroup of F, generated algebraically by the conjugates of all elements from $\phi(\bigcup_{j\geq k+1} M_X^j)$. By repeated application of the identities

$$(y,z) = (z,y)^{-1}$$

and
$$(x^y, (y,z)).(y^z, (z,x)).(z^x, (x,y)) = 1,$$

every element of $\phi(M_X^j)$, for $j \geq 2$, belongs to the subgroup of F, generated algebraically by all elements of the form (s,t), $s \in \phi(M_X^1)$, $t \in \phi\ (M_X^{j-1})$. It follows that $H_{k+1} \subset F_{k+1}$. By the induction hypothesis, the subgroup H_k of F_k, generated algebraically by the conjugates of all elements from $\phi(\bigcup_{j\geq k} M_X^j)$, is dense in F_k; and the group $\overline{S}_{k+1}$, generated algebraically by the conjugates of all elements of the set

$$S_{k+1} = \{(u,v): u \in L(n),\ v \in H_k\}$$

is dense in F_{k+1}, by virtue of the continuity of the map: $F \times F \to F$, $(t,s) \to ts\,t^{-1}\,s^{-1}$, and the equality $F_{k+1} = (F,\ F_k)$. Let us denote by y^x the conjugate $x^{-1}\,yx$ of an element y. In every group, one has the identities:

$$(xy,\ z) = (y,z)^{x^{-1}} . (x,z)$$

$$(x,y) = (y,x)^{-1}$$

$$(x^{-1},\ y) = (y,x)^x$$

$$(y^{x^{-1}},\ z) = (x^{-1},\ z)^{y^{-1}x^{-1}} . (y,z)^{x^{-1}} . (x,z) .$$

Clearly $(x_i,\ s) \in H_{k+1}$, for all $s \in \phi(\bigcup_{j\geq k} M_X^j)$. By repeated use of the first and third identities, one obtains: $(u,s) \in H_{k+1}$ for all $u \in L(n)$, $s \in \phi(\bigcup_{j\geq k} M_X^j)$. Since the conjugates of $\phi(\bigcup_{j\geq k} M_X^j)$ generate H_k algebraically, the four above identities then give: $S_{k+1} \subset H_{k+1}$; so that $\overline{S}_{k+1} \subset H_{k+1}$, and H_{k+1} is dense in F_{k+1}. The induction argument is now complete.

If one endows F_k/F_{k+1} with its quotient topology, then the canonical image $\rho(\phi(M_X^k))$ of the set $\phi(M_X^k)$, generates a dense subgroup of the abelian group F_k/F_{k+1}. We proceed to show that $\rho(\phi(M_X^k))$ generates the $\underline{\underline{Z}}_p$-module F_k/F_{k+1} ; (multiplication of elements of F_k/F_{k+1} by p-adic integers, is induced by taking p-adic powers in F_k - [14]). If $M_X^k = \{z_1, \ldots, z_q\}$ (M_X^k is finite), then one can define a continuous mapping $\psi\colon Z_p^q \to F_k/F_{k+1}$, by putting $\psi(a_1, \ldots, a_q) = \sum_{j=1}^{q} a_j \, \rho(\phi(z_j))$. Since the subgroup $\psi(\underline{\underline{Z}}^q)$ of $\psi(\underline{\underline{Z}}_p^q)$ is already dense in F_k/F_{k+1}, the compact continuous image $\psi(\underline{\underline{Z}}_p^q)$, of the compact set $\underline{\underline{Z}}_p^q$, must coincide with F_k/F_{k+1}. Denote by L_X^k the homogeneous component of degree k, of the graded free Lie algebra L_X. Clearly, $\nu(L_X^k) = \psi(\underline{\underline{Z}}_p^q)$ so that $\nu(L_X^k) = F_k/F_{k+1} = gr_k\ F$. It follows that $\nu(L_X) = gr\ F$.

Having proved that $\nu\colon L_X \to gr\ F$ is surjective, the proof of parts (a) and (b) of the theorem proceeds in exactly the same way as the proof of theorems 6.1 and 6.2 of [19] Chapter IV, for the case of a <u>discrete</u> free group.

To show that $\{F_i'\}$ is a filtration, one has to prove that $(F_i', F_j') \subset F_{i+j}'$ for all positive integers i and j. Let $g \in F_i'$, $h \in F_j'$. One has

$$gh = 1 + (g-1) + (h-1) + (g-1)\ (h-1)$$
$$hg = 1 + (g-1) + (h-1) + (h-1)\ (g-1)$$

$(g,h) = gh(hg)^{-1}$

$$= [1 + (g-1) + (h-1) + (g-1)(h-1)]\cdot[\sum_{k=o}^{\infty} (-1)^k\{(g-1) + (h-1) + (h-1)(g-1$$

$(g,h) = 1 + (g-1)(h-1) - (h-1)(g-1) + \text{terms of degree} \geqslant i + j + 1 \ldots (X)$.

(The degree of a term $a_m\, m$ of the formal power series expansion $\sum\limits_{m\in M} a_m\, m$ of an element a of $A(n)$, is defined to be the length of m).
The formula (X) shows that $\{F_i'\}$ is a filtration. Let $gr'\, F = \sum\limits_{i=1}^{\infty} F_i'/F_{i+1}'$ be the corresponding Lie algebra ([19]). Denote by Ass_X the free associative $\underline{\underline{Z}}_p$-algebra on $X = \{x_1,\ldots, x_n\}$. Ass_X is a graded Lie algebra (the elements of X are of degree one), with $[x,y] = xy - yx$ for all $x,y \in Ass_X$. For every $a \in A$, put $\bar{a}_o(T) = a_1$, $\bar{a}_j(T) = \sum\limits_{\ell(m)=j} a_m\, m$.
The element a can be written as a formal power series

$$a = \sum_{j=o}^{\infty} \bar{a}_j(T) .$$

We now define a morphism $\eta\colon gr'\, F \to Ass_X$ of Lie algebras, as follows.
For every $\xi \in gr_k'\, F$, one chooses a representative $g = 1 + \bar{g}_k(T) + \bar{g}_{k+1}(T) + .$ in F_k' , and one puts $\eta(\xi) = \bar{g}_k(x) \in Ass_X^k$; (i.e. one replaces T_i by x_i in the expression for $\bar{g}_k(T)$). Clearly η is a well defined morphism on the homogeneous components $gr_k'\, F$ (see (X)), and, by linearity, one obtains a morphism η of graded Lie algebras. Obviously, η is injective.

Formula (X) can be used to prove (by induction on k) that $F_k \subset F_k'$ for all positive integers k, whence one obtains a morphism

γ: gr F $\to$ gr' F of graded Lie algebras. One now puts

$$\mu = \eta \circ \gamma \circ \nu \colon L_X \to \mathrm{gr}\, F \to \mathrm{gr}'\, F \to \mathrm{Ass}_X \ .$$

For every $x_i \in X$, one has $\mu(x_i) = x_i$, and for $u,v \in M_X$, one has $\mu(uv) = uv - vu$ (see (X)). It follows that μ is the canonical morphism of graded Lie algebras (universal property of L_X), obtained from the canonical injection $X \to \mathrm{Ass}_X$. By theorem 4.2 of [19], Chapter V, μ is injective. Thus, $\nu \colon L_X \to \mathrm{gr}\, F$ is both injective and surjective, which proves part (b). It also follows that $\gamma \colon \mathrm{gr}\, F \to \mathrm{gr}'\, F$ is injective. We proceed to prove, by induction on k, that $F'_k = F_k$ for all positive integers k. For $k = 1$, there is nothing to prove. For $k > 1$, one has $F_k \subset F'_k \subset F'_{k-1}$, and the induction hypothesis $F'_{k-1} = F_{k-1}$, implies $F'_k \subset F_{k-1}$. Since the kernel of $\gamma_{k-1} = \gamma|(F_{k-1}/F_k) \colon F_{k-1}/F_k \to F'_{k-1}/F'_k$ is zero, one has $F'_k \subset F_k$ and $F'_k = F_k$. This completes the proof of the first equality of part (a). Clearly, $F \cap (1 + I^i) \subset F'_i$. Let

$$F''_i = \{y = \sum_{m \in M} y_m\, m \in F'_i \colon \exists\, k \in \underline{\underline{N}} \text{ such that } y_m = 0 \text{ whenever } \ell(m) > k\} \ .$$

Then $F''_i \subset F \cap (1 + I^i)$ and F''_i is dense in F'_i. Now, I is compact, so that $F \cap (1 + I^i)$ is compact and closed. Consequently, $F'_i \subset F \cap (1 + I^i)$ and the proof of part (a) is complete.

It is clear that $(\varepsilon \circ \frac{\partial}{\partial x_{i_1}} \circ \dots \circ \frac{\partial}{\partial x_{i_k}})(a) = a_{m_o}$, where

$m_o = T_{i_1} \cdot T_{i_2} \ldots T_{i_k} \in M$ and $a = \sum_{m \in M} a_m m$ (for all $a \in A(n)$).

Thus, $$\varepsilon \circ \frac{\partial}{\partial x_i} | F_2 = 0, \ \varepsilon \circ \frac{\partial}{\partial x_{i_1}} \circ \frac{\partial}{\partial x_{i_2}} | F_3 = 0, \text{ etc.}$$

From lemma 3.5 , one concludes that $\delta_k | F_k$ is a derivation from F_k into $A(n)$, for all $\delta_k \in D_k$ and all $k = 1, 2, \ldots$. It follows trivially from this that $\varepsilon \circ \delta_k : F_k \to \underline{\underline{Z}}_p$ is a homomorphism of abelian groups.

Let a_1 and a_2 be two words of M, uniquely determined by the conditions $a_1 \cdot a_2 = T_{i_1} \ldots T_{i_k}$, $\ell(a_1) = j$ and $\ell(a_2) = h$. Similarly, let b_1 and b_2 be two words of M, uniquely determined by the conditions $b_2 \cdot b_1 = T_{i_1} \ldots T_{i_k}$, $\ell(b_1) = j$ and $\ell(b_2) = h$. To prove (d), we note that $\phi(q) \in F'_j$, $\phi(s) \in F'_h$, so that the formula (X) becomes:

$$\phi(t) = (\phi(q), \phi(s))$$
$$= 1 + (\phi(q)-1)(\phi(s)-1) - (\phi(s)-1)(\phi(q)-1) + \text{terms of degree} \geqslant j + h + 1.$$

It follows that for $m = T_{i_1} \ldots T_{i_k}$,

$$\phi(t)_m = (\phi(q)-1)_{a_1} (\phi(s)-1)_{a_2} - (\phi(s)-1)_{b_2} (\phi(q)-1)_{b_1}$$
$$= \phi(q)_{a_1} \phi(s)_{a_2} - \phi(s)_{b_2} \phi(q)_{b_1} .$$

Making use of the fact that

$$\phi(t)_m = \partial_{1,\ldots,k} (t),$$

$$\phi(q)_{a_1} = \partial_{1,\ldots,j} (q), \text{ etc.},$$

one obtains

$$\partial_{1,\dots,k}(t) = \partial_{1,\dots,j}(q)\ \partial_{j+1,\dots,k}(s) - \partial_{h+1,\dots,k}(q)\ \partial_{1,\dots,h}(s)\ .$$

This completes the proof of the theorem.

Examples 3.12:

In the definition of the symbols $\partial_{1,\dots,k}$ (3.11 (d)), we take $i_j = j$ for every j and we put $x = x_1$, $y = x_2$, $z = x_3$. One then has:

(i) $\partial_{1,2}(xy) = \partial_1(x)\ \partial_2(y) - \partial_2(x)\ \partial_1(y) = 1 - 0 = 1$;

(ii) $\partial_{1,2,3}(x(yz)) = \partial_1(x)\ \partial_{2,3}(yz) - 0 = 1$;

(iii) $\partial_{1,1,2}(y(yx)) = 0$, $\partial_{2,2,1}(x(xy)) = 0$, $\partial_{1,1,2}(x(xy)) = 1$;

(iv) $\partial_{1112}(x(x(xy))) = 1$, $\partial_{1112}(y(x(yx))) = 0$, $\partial_{1112}(y(y(xy))) = 0$;

(v) $\partial_{2112}(x(x(xy))) = 0, \partial_{2112}(y(x(yx))) = 1$, $\partial_{2112}(y(y(xy))) = 0$;

(vi) $\partial_{2212}(y(y(xy))) = \partial_{212}(y(xy)) - \partial_{221}(y(xy)) = 1 - \partial_{21}(xy) - \partial_{21}(xy) = 3$.

3. Applications to the cohomology of pro-p-groups.

Let G be a pro-p-group, defined by a finite number of generators and relations, in the sense that $H^1(G, \underline{\underline{Z}}/p\,\underline{\underline{Z}})$ and $H^2(G, \underline{\underline{Z}}/p\,\underline{\underline{Z}})$ are both finite dimensional vector spaces over $\underline{\underline{Z}}/p\,\underline{\underline{Z}}$ (see [18]). If the dimension of $H^1(G, \underline{\underline{Z}}/p\,\underline{\underline{Z}})$ over $\underline{\underline{Z}}/p\,\underline{\underline{Z}}$, is n, then G may be identified with some quotient $F(n)/R$ of $F(n)$; ($F(n)$ = the free pro-p-group on n generators $x_1, \dots, x_n$). Furthermore, if the dimension of $H^2(G, \underline{\underline{Z}}/p\,\underline{\underline{Z}})$ over $\underline{\underline{Z}}/p\,\underline{\underline{Z}}$ is $m \geqslant 1$, then one can find elements $r_1, \dots, r_m \in F(n)$, such that R is the smallest closed normal subgroup of $F(n)$, containing $r_1, \dots, r_m$. The elements $r_1, \dots, r_m$ are called <u>defining relations</u>, or simply <u>relations</u>, of G.

The completed group algebra $\underline{\underline{Z}}_p[[G]] = \varprojlim_U \underline{\underline{Z}}_p[G/U]$ (U runs through the filter of open normal subgroups of G), will always be denoted by Λ (see [14]). By virtue of the identification $A(n) = \underline{\underline{Z}}_p[[F(n)]]$, (loc cit) the natural projection: $F(n) \to G$ can be extended to a continuous epimorphism $\pi: A(n) \to \Lambda$ of compact $\underline{\underline{Z}}_p$-algebras. The group G acts continuously on $R/(R,R)$ by inner automorphisms, and the ring $\underline{\underline{Z}}_p$ acts continuously on $R/(R,R)$ by taking p-adic powers (loc cit). It follows (theorem 2.2.6 of [14]), that these actions can be extended in such a way that $R/(R,R)$ becomes a Λ-module. (One may also use a direct argument: the action of G can obviously be extended to $\underline{\underline{Z}}[G]$, which is dense in $\underline{\underline{Z}}_p[[G]]$). The epimorphism $\pi: A(n) \to \Lambda$ induces a continuous epimorphism $\pi^n: A(n)^n \to \Lambda^n$ of the product algebras. The formula $\lambda(\lambda_1, \dots, \lambda_n) = (\lambda\lambda_1, \dots, \lambda\lambda_n)$ $(\lambda, \lambda_i \in \Lambda)$ endows Λ^n with the structure of a (left) Λ-module. Define $\Delta: A(n) \to A(n)^n$ by the formula $\Delta(a) = \left(\frac{\partial a}{\partial x_1}, \dots, \frac{\partial a}{\partial x_n} \right)$.

<u>Theorem 3.13:</u>

Suppose that the elements $\pi^n(\Delta r_1), \dots, \pi^n(\Delta r_m)$ of Λ^n are linearly independent over Λ ; then

(i) the map $\pi^n \circ \Delta \colon A(n) \to \Lambda^n$ induces a continuous monomorphism $\mu \colon R/(R,R) \to \Lambda^n$ of Λ-modules (Δ is defined immediately above);

(ii) $R/(R,R)$ is a free Λ-module on the canonical images of $r_1, \dots, r_m$;

(iii) G has cohomological dimension 2.

Proof:

We first show that $\mu \colon R/(R,R) \to \Lambda^n$ is well defined. Let $t_1, t_2 \in R$. Then $\Delta((t_1, t_2)) = \Delta(t_1 \, t_2 \, t_1^{-1} \, t_2^{-1}) = (1 - t_1 \, t_2 \, t_1^{-1})\Delta t_1 + t_1(1 - t_2 \, t_1^{-1} \, t_2^{-1})\Delta t_2$, so that $\pi^n(\Delta((t_1, t_2))) = 0$. For every $f \in F(n)$, one has $\pi^n(\Delta(f(t_1, t_2)f^{-1})) = \pi^n[(1 - f(t_1, t_2)f^{-1})\Delta f + f\Delta((t_1, t_2))]$ $= 0$. One has $\pi^n(\Delta(t_1 \cdot t_2)) = \pi^n(\Delta t_1) + \pi^n(t_1 \, \Delta \, t_2) = \pi^n(\Delta t_1) + \pi^n(\Delta t_2)$, whence it can be seen that $\pi^n \circ \Delta \colon R \to \Lambda^n$ is a homomorphism of groups. It is continuous and is zero on the dense subgroup of (R,R), generated algebraically by the conjugates of the commutators (t_1, t_2) $(t_1, t_2 \in R)$. It follows that $\pi^n(\Delta((R,R))) = 0$, and μ is indeed a well defined continuous homomorphism of abelian groups. We now proceed to prove that μ is compatible with the Λ-module structures of $R/(R,R)$ and Λ^n. Suppose $g \in G$ and $s \colon G \longrightarrow F(n)$ is a continuous system of representatives ([18] Chapter I, Proposition 1). For every $t \in R$, we shall denote by $[t]$ its canonical image in $R/(R,R)$. We denote by

$$*\colon \Lambda X(R/(R,R)) \to R/(R,R)$$

the action of Λ on $R/(R,R)$. One has

$$g * [t] = [s(g)\ t\ s(g)^{-1}]$$

and
$$\begin{aligned}\mu(g * [t]) &= \pi^n(\Delta(s(g)t\ s(g)^{-1})) \\ &= \pi^n[(1 - s(g)t\ s(g)^{-1})\Delta(s(g)) + s(g)\Delta t] \\ &= g\ \pi^n(\Delta t) = g\ \mu([t]) \quad \text{for all} \quad t \in R,\ g \in G.\end{aligned}$$

Thus, μ is compatible with the action of G on $R/(R,R)$ (defined by inner automorphisms); it is compatible with the induced action of the group algebra $\mathbb{Z}[G]$ on $R/(R,R)$; and, finally, by virtue of $\mathbb{Z}[G]$ being dense in Λ , μ is a continuous Λ-module homomorphism.

The group R_o, consisting of all elements of the form $t = f_1 r_{i_1}^{e_1} f_1^{-1} \cdot f_2 r_{i_2}^{e_2} f_2^{-1} \dots f_k r_{i_k}^{e_k} f_k^{-1}$, $(\{i_1,\dots, i_k\} \subset \{1,\dots, m\})$ is dense in R. One has

$$\pi^n(\Delta t) = \sum_{j=1}^{k} \pi(f_j)\ e_j\ \pi^n(\Delta r_{i_j}) \quad \dots \quad (Y) .$$

One sees from this that $\pi^n(\Delta(R_o))$ is contained in the Λ-module, generated in Λ^n by the elements $\pi^n(\Delta r_1),\dots, \pi^n(\Delta r_m)$. Since Λ is compact, the Λ-module L, generated by $\pi^n(\Delta r_1),\dots, \pi^n(\Delta r_m)$, is compact in Λ^n, and must, therefore, contain the closure $\pi^n(\Delta R)$ of $\pi^n(\Delta R_o)$ ($\pi^n \circ \Delta$ is continuous). The equation (Y) shows that $\pi^n(\Delta R_o)$ = the $\mathbb{Z}[G]$-module L_o, generated by $\pi^n(\Delta r_1),\dots, \pi^n(\Delta r_m)$. Now, $\mathbb{Z}[G]$ is dense in $\mathbb{Z}_p[G]$, which, in turn, is dense in $Z_p[[G]] = \Lambda$ [see 14], so that L_o is dense in L. It follows that $\pi^n(\Delta R) = L$. So, the range of μ is the Δ-module L, generated by $\pi^n(\Delta r_1),\dots, \pi^n(\Delta r_m)$.

If these elements are linearly independent over Λ, then one can define a mapping $\psi\colon L \to R/(R,R)$, such that $\psi \circ \mu = 1$. Indeed, let

$$\phi_i\colon \underline{\underline{Z}}_p[G]\;\pi^n(\Delta r_i) \to R/(R,R)$$

be defined by the formula

$$\phi_i\Big(\sum_j n_j\, g_j\, \pi^n(\Delta r_i)\Big) = \Big[\prod_j s(g_j)\, r_i^{n_j}\, s(g_j)^{-1}\Big] \ldots \quad (Z)$$

$(i = 1,\ldots, m;\ n_j \in \underline{\underline{Z}}_p,\ g_j \in G)$. Since s is continuous, each ϕ_i is uniformly continuous, and can be extended to $\bar{\phi}_i\colon \Lambda\cdot\pi^n(\Delta r_i) \to R/(R,R)$. We may take ψ to be the mapping induced by $\phi_1,\ldots, \phi_n$; $(\pi^n(\Delta r_1),\ldots, \pi^n(\Delta r_m)$ being linearly independent over Λ). Note that $\phi_1,\ldots, \phi_m$ and ψ are independent of the choice of s. Indeed, if $u = f_j^{-1} f_j' \in R$, $(f_j, f_j' \in F(n))$, then

$$\begin{aligned} f_j\, r_i^{n_j}\, f_j^{-1}(f_j'\, r_i^{n_j}(f_j')^{-1})^{-1} &= f_j'(f_j')^{-1}\, f_j\, r_i^{n_j}\, f_j^{-1}\, f_j'\, r_i^{-n_j}(f_j')^{-1} \\ &= f_j'\, u^{-1}\, r_i^{n_j}\, u\, r_i^{-n_j}(f_j')^{-1} \in (R,R)\ ; \end{aligned}$$

so that one may replace $s(g_j)$, in the formula (Z), above, by any element lying in the same coset (mod R). Formulas (Y) and (Z) show that

$$\begin{aligned} \psi(\mu([t])) &= \psi\Big[\sum_{j=1}^{k} \pi(f_j)\, e_j\, \pi^n(\Delta r_{i_j})\Big] \\ &= \Big[\prod_{j=1}^{k} s(\pi(f_j))\, r_{i_j}^{e_j}\, s(\pi(f_j))^{-1}\Big] \\ &= \Big[\prod_{j=1}^{k} f_j\, r_{i_j}^{e_j}\, f_j^{-1}\Big] = [t] \qquad (t \in R_o) \end{aligned}$$

(we made use, here, of the preceding remark, concerning independence with respect to the choice of representatives). Thus $\psi \circ \mu$ is the identity map on the canonical image of R_o in $R/(R,R)$; and this canonical image is dense in $R/(R,R)$. Thus, $\psi \circ \mu = 1$ and μ is indeed injective. It also follows that $R/(R,R)$ is a free Λ-module on the canonical images $[r_1], \ldots, [r_m]$ of $r_1, \ldots, r_m$ respectively.

It now only remains to prove part (iii) of the theorem. We may use directly a result of Brumer ([3] corollary 5.3), which states that $\operatorname{cd} G \leqslant 2$ if $R/(R,R)$ is free on $[r_1], \ldots, [r_m]$; (In our case, we assumed $H^2(G, \mathbb{Z}/p\,\mathbb{Z}) \neq 0$). Or else, one may use the following free resolution of $\mathbb{Z}_p$:

$$\ldots \to 0 \to 0 \to R/(R,R) \overset{\mu}{\to} \Lambda^n \overset{\alpha}{\to} \Lambda \overset{\varepsilon}{\to} \mathbb{Z}_p .$$

Here, $\alpha(\lambda_1, \ldots, \lambda_n) = \sum_{i=1}^{n} \lambda_i \, \pi(T_i)$ and ε is the natural augmentation (that extends the natural augmentation of the group algebra $\mathbb{Z}_p[G]$ - see [14]).

$$\alpha(\mu[w]) = \sum_{i=1}^{n} \pi[(\frac{\partial w}{\partial x_i}) \, T_i] \quad \text{for all} \quad w \in R.$$

By formula (6) of Proposition 3.1, one has $\alpha \circ \mu = 0$. We proceed to prove that $\ker \alpha \subset L$. Let us denote by I the kernel of ε and let $\beta\colon A(n)^n \to I$ be the $A(n)$-homomorphism, given by $\beta(a_1, \ldots, a_n) = \sum_{i=1}^{n} a_i \, T_i$. By formula (6) of Proposition 3.1, β is invertible, and

$$\beta^{-1}(a) = (\frac{\partial a}{\partial x_1}, \ldots, \frac{\partial a}{\partial x_n}).$$

Claim: $\pi\left(\frac{\partial(\ker\,\pi)}{\partial x_i}\right) \subset \pi\left(\frac{\partial R}{\partial x_i}\right)$ for all $i = 1,\dots, n$.

Proof:

The elements of the form

$$c = \sum_{j=1}^{m} \sum_{k} a_k(r_k'-1)b_k \qquad (a_k,\ b_k \in F(n),\ r_k' \in R)$$

(To prove this, let V be an open normal subgroup of $F(n)$, $x_V\colon F(n) \to F(n)/V$ the canonical projection and $q_V\colon A(n) \to \mathbb{Z}_p[F(n)/V]$ its canonical extension to $A(n)$. There exists a commutative diagram of continuous epimorphisms:

$$\begin{tikzcd}
A(n) \arrow[r, "\pi"] \arrow[d, "q_V"] & \Lambda \arrow[d, "p_V"] \\
\mathbb{Z}_p[F(n)/V] \arrow[r, "\pi_V"'] & \mathbb{Z}_p[G/\pi(V)]
\end{tikzcd}$$

Suppose now that $c \in \ker\,\pi$. Then $\pi_V(q_V(c)) = 0$. By a well-known fact about group rings, (see, for instance [4], §2) $q_V(c)$ is of the form $q_V[\sum_i f_i(t_i-1)]$, where $f_i \in F(n)$ and $t_i \in R\cdot V$. If one writes $t_i = r_i'\cdot v_i$, where $r_i' \in R$ and $v_i \in V$, then $t_i - 1 = (r_i'-1)v_i + v_i - 1$. It follows that $c - \sum_i f_i(r_i'-1)v_i \in \ker\,q_V$. Now, the ideals $\{\ker\,q_V\}$ constitute a fundamental system of neighborhoods of $0 \in A(n)$ [14], and this proves that the elements of the form c, are dense in $\ker\,\pi$).

One has

$$\frac{\partial c}{\partial x_i} \equiv \sum_{j=1}^{m} \sum_{k} a_k \frac{\partial r_k'}{\partial x_i} \varepsilon(b_k) \qquad (\text{mod ker } \pi)$$

$$\equiv \frac{\partial}{\partial x_i} \Big(\prod_{j=1 \;\; k}^{m} a_k (r_k')^{\varepsilon(b_k)} a_k^{-1} \Big) \qquad (\text{mod ker } \pi) \ .$$

Thus $\pi(\frac{\partial D}{\partial x_i}) \subset \pi \frac{\partial R}{\partial x_i}$. Since the maps $\frac{\partial}{\partial x_i}$ are continuous and R is compact, the set $\pi(\frac{\partial R}{\partial x_i})$ is closed and $\pi(\frac{\partial (\ker \pi)}{\partial x_i}) \subset \pi(\frac{\partial R}{\partial x_i})$.

One has a commutative diagram

$$\begin{tikzcd}
A(n)^n \arrow[r, "\beta"] \arrow[d, "\pi^n"] & I \arrow[d, "\pi|I"] \\
\Lambda^n \arrow[r, "\alpha"'] & \Lambda
\end{tikzcd}$$

Suppose that $\lambda = (\lambda_1, \ldots, \lambda_n)$, $\lambda_i = \pi(a_i)$ $(i = 1, \ldots, n)$ and $\alpha(\lambda) = 0$. Then $\beta(a_1, \ldots, a_n) \in \ker \pi$ and $a_i \in \frac{\partial}{\partial x_i} (\ker \pi)$ $(i = 1, \ldots, n)$. By the above claim, one obtains $\pi(a_i) \in \pi(\frac{\partial R}{\partial x_i})$, so that

$$\lambda = \pi^n(a_1, \ldots, a_n) \in \pi^n(\Delta(R)) = L = \mu(R/(R,R)).$$

It follows from this discussion that the given complex is exact. The maps are continuous (left) Λ-module homomorphisms. It now only remains to state that the cohomology groups $\{H^n(G, \underline{\underline{Z}}/p\, \underline{\underline{Z}})\}$ are the cohomology groups of the complex obtained by applying the functor $\mathrm{Hom}_{\mathrm{cont}}(-, \underline{\underline{Z}}/p\, \underline{\underline{Z}})$ to this resolution. (This remains true if $\underline{\underline{Z}}/p\, \underline{\underline{Z}}$ is replaced by any p-primary discrete G-module - see [3] or [14] Chapter V. In [3], one finds the following definition of a pseudo-compact ring: a ring Λ is pseudo-compact if it is a complete Hansdorff topological ring, which admits a system of open neighborhoods of 0, consisting of two-sided ideals I, for which Λ/I is an Artin ring. In particular, the completed group algebra $\Lambda = \underline{\underline{Z}}_p[[G]]$ is pseudo-compact. A complete Hansdorff topological Λ-module M is said to be pseudo-compact, if it has a system of open neighborhoods of 0, consisting of submodules N, for which M/N has finite length.

Let $\mathcal{D}_\Lambda$ be the category of discrete p-primary G-modules, $\mathcal{C}_\Lambda$ = the category of pseudo-compact Λ-modules $(\Lambda = \underline{\underline{Z}}_p[[G]])$ and $\{\mathrm{Ext}_G^q\}$ the right derived functors of $\mathrm{Hom}_\Lambda^{\mathrm{cont}}: \mathcal{C}_\Lambda \times \mathcal{D}_\Lambda \to \mathcal{D}_{\underline{\underline{Z}}_p}$. In [3], lemma 4.1, Brumer points out that

$$H^q(G,A) = \mathrm{Ext}_G^q(\underline{\underline{Z}}_p, A)$$

for all pro-p-groups G and all $A \in (\mathcal{D}_\Lambda)_{0b}$; because both $H^q(G, -)$ and $\mathrm{Ext}_G^q(\underline{\underline{Z}}_p, -)$ are right derived functors of $A \leadsto A^G = \mathrm{Hom}_G(\underline{\underline{Z}}_p, A)$. Finally, it has to be said that the Λ-module Λ^k is a free object of $\mathcal{C}_\Lambda$ (for all positive integers k), so that our computation of the cohomology groups $H^q(G, \underline{\underline{Z}}/p\,\underline{\underline{Z}})$, from the above resolution, is justified).

Corollary 3.14:

Suppose that G is a pro-p-group, defined by a single relation r_1 (i.e. m = 1). If $\pi(\frac{\partial r_1}{\partial x_i}) \nequiv 0$ and $\pi(\frac{\partial r_1}{\partial x_i})$ is not a divisor of zero on the right in Λ , for some $i = 1,\dots, n$, then cd G = 2.

Proof:

The set consisting of the single element $\pi^n(\Delta r_1) = (\pi(\frac{\partial r_1}{\partial x_1}),\ldots, \pi(\frac{\partial r_1}{\partial x_n}$ is linearly dependent iff the equations $\lambda\pi(\frac{\partial r_1}{\partial x_i}) = 0$ $(i = 1,\ldots, n;\ \lambda \in \Lambda)$ imply $\lambda = 0$.

Proposition 3.15:

Let G be a pro-p-group of finite type (i.e. $H^1(G, \mathbb{Z}/p\,\mathbb{Z})$ is finite). If an element x of G is of infinite order, then $1 - x$ is not a zero divisor in $\Lambda = \mathbb{Z}_p[[G]]$.

Proof:

Let $\mathcal{F}$ be the filter of open normal subgroups of G. For each $U \in \mathcal{F}$, denote by q_U the order of the group G/U, and by

$$p_U\colon \mathbb{Z}_p[[G]] \to \mathbb{Z}_p[[G/U]] = \mathbb{Z}_p[G/U]$$

the canonical projection. Suppose that $a(1-x) = 0$, $a \in \Lambda = Z_p[[G]]$. For every $U \in \mathcal{F}$, put $y_U = 1 + x + \ldots + x^{q_U-1}$. One has $p_U(a)(1-p_U(x)) = 0$ in the group algebra $\mathbb{Z}_p[G/U]$. Applying [4], Proposition 6, to this group algebra, we conclude that $p_U(a)$ is divisible on the right by $p_U(y_U)$; i.e. there exist $v_U \in \ker p_U$ and $s_U \in \Lambda$ such that $v_U = a - s_U\, y_U$. Since $(0) = \bigcap_{U \in \mathcal{F}} \ker p_U$, it only remains to prove that y_U tends to 0, according to the filter $\mathcal{F}$. Since x is not of finite order in G, the set of positive integers $\{q_U\}_{U \in \mathcal{F}}$ is unbounded from above, which means that q_U tends to zero according to the filter $\mathcal{F}$; i.e. $\lim\limits_{U \to 1} q_U = 0$

in the p-adic topology. Since G is the continuous image of some free pro-p-group $F(n)$, and Λ is the continuous image of $A(n)$, we need only to prove that for $x' \in F(n)$ and $q_U \to 0$ in $\underline{\underline{Z}}_p$, one has

$$\lim_{U \to 1} (1 + x' + \dots + (x')^{q_U - 1}) = 0.$$

(Applying the canonical projection $\pi: A(n) \to \Lambda$ to this equality and choosing x' so that $\pi(x') = x$, one obtains the desired result). If $x' \neq 0$, then there exists some $i = 1, \dots, n$, such that $\frac{\partial x'}{\partial x_i} \neq 0$

$$\frac{\partial}{\partial x_i} ((x')^{q_U}) = [1 + x' + \dots + (x')^{q_U - 1}] \cdot \frac{\partial x'}{\partial x_i} .$$

Now, $(x')^{q_U}$ tends to 1, according to the filter $\mathcal{F}$, so that $[1 + x' + \dots + (x')^{q_U - 1}] \frac{\partial x'}{\partial x_i}$ tends to zero, $\frac{\partial}{\partial x_i} : A(n) \to A(n)$ being continuous. Since $A(n)$ contains no zero divisors, we may conclude that

$$\lim_{U \to 1} [1 + x' + \dots + (x')^{q_U - 1}] = 0.$$

This completes the proof of the proposition.

Definition 3.16:

Let G be a pro-p-group defined by a finite number of generators $x_1, \dots, x_n$ and a single relation r. We shall call r a simple relation if, for some $i = 1, \dots, n$, $\pi(\frac{\partial r}{\partial x_i})$ is a product of elements of the form $1 - g$ $(g \neq 1 \in G)$ and invertible elements of Λ.

Theorem 3.17:

Let G be a pro-p-group defined by a finite number of generators $x_1, \ldots, x_n$ and a single nontrivial simple relation r, (definition 3.16) Then $\mathrm{cd}\, G = 2$ or ∞.

Proof:

By corollary 3.14 and Proposition 3.15, $\mathrm{cd}\, G = 2$ if G contains no elements of finite order. If G contains an element of finite order, then it contains a finite cyclic-subgroup H. Since $\mathrm{cd}\, H = \infty$ and $\mathrm{cd}\, G \geqslant \mathrm{cd}\, H$ ([18] Proposition 14, [21] Chapter VIII, §4), one has $\mathrm{cd}\, G = \infty$ for the case where G contains an element of finite order.

Theorem 3.18:

Let G be a pro-p-group defined by a finite number of generators $x_1, \ldots, x_n$ and a single relation r of the form $r = ux_i\, vx_i^{-1}\, w$ with the following properties:

(i) u, v and w are independent of x_i, i.e. belong to the closed subgroup of $F(n)$ generated by the remaining generators $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$;

(ii) no power of uw belongs to the closed normal subgroup R of $F(n)$, generated by r and its conjugates.

Under these conditions, $\mathrm{cd}(G) = 2$.

Proof:

$$\pi\left(\frac{\partial r}{\partial x_i} \right) = \pi[u(1-x_i\, v\, x_i^{-1})] = \pi(u - w^{-1}) = \pi(uw - 1)\cdot\pi(w^{-1})$$

so that r is a simple relation. Since $\pi(uw)$ is of infinite order in G, $\pi(\frac{\partial r}{\partial x_i})$ is not a divisor of zero on the right, in $\Lambda = \underline{\underline{Z}}_p[[G]]$. The result follows by corollary 3.14.

Remarks 3.19:

It may happen that a given relation r is not simple (definition 3.16), but that it "becomes simple" when one changes the minimal system of generators of G. To be more precise: suppose that $H^1(G, \underline{\underline{Z}}/p\ \underline{\underline{Z}})$ is of dimension n over $\underline{\underline{Z}}/p\ \underline{\underline{Z}}$, $\pi: F(n) \to G$ is an epimorphism with kernel R, R being the smallest normal subgroup of $F(n)$, containing r; suppose, furthermore, that $y_1, \dots, y_n$ generate a dense subgroup of G; then one can define an epimorphism $\pi': F(n) \to G$, by putting $\pi'(x_i) = y_i$ $(i = 1, \dots, n)$ ([18]: Chapter I, Proposition 5). The kernel of π' is again the closed normal subgroup of $F(n)$ generated by a single relation r' ([18]: Corollary of Proposition 27, Chapter I), which may be simple, even when r is not simple. In particular, if G is a Demuskin group, of finite type, and $p \nmid 2$, then G may be considered as being defined by a relation of the form $x_1^q\ (x_1, x_2)\ (x_3, x_4) \dots (x_{n-1}, x_n)$ ([20], Theorem 3.1).

Such a relation is obviously simple (apply $\frac{\partial}{\partial x_2}$). For the case $p = 2$, and further classification of Demuskin groups, see [11] and [12]. It is already known that the Demuškin groups are of cohomological dimension 2. The following lemma plays an important role in connection with suitable choices of minimal systems of generators.

Lemma 3.20:

Given a pro-p-group G, defined by a finite number of generators $x_1, \dots, x_n$, and a single relation r; one may assume, without loss in generality, that the generators $x_1, \dots, x_n$ have been chosen in such a way that r is of the form

$$r = x_n^q \cdot t \ , \quad t \in (F(n), F(n)) \quad \text{and} \quad q \in p \, \underline{\underline{Z}}_p \ .$$

Proof:

Redefining π (see remarks 3.19), or replacing $x_1, \dots, x_n$ by $x_1', \dots, x_n'$, amounts to the same thing, provided that $x_1', \dots, x_n'$ generate algebraically a dense subgroup of $F = F(n)$. It is stated, in [20], that $r \in F^p.(F,F)$ (observe that π induces an isomorphism: $\pi_*: F/F^p(F,F) \to G/G^p(G,G))$. Denoting by v the usual p-adic valuation on $\underline{\underline{Z}}_p$, and permuting the x_i, if necessary, one may assume that $v(\tau_1(r)) \geq \dots \geq v(\tau_n(r))$, where $\tau_i = \varepsilon \circ \frac{\partial}{\partial x_i}$, as before

$(i = 1,\ldots, n)$. The canonical image of an element $y \in F$ in the $\underline{\underline{Z}}_p$-module $F/(F,F)$, will be denoted by $\bar{y}$.

Claim:

$$\bar{y} = \sum_{i=1}^{n} d_i\, \bar{x}_i \quad (d_i \in Z_p) \quad \text{iff} \quad \tau_i(y) = d_i \quad \text{for all} \quad i = 1,\ldots, n.$$

Proof:

Seeing that the functions τ_i are continuous, we may restrict ourselves, without loss in generality, to the case where $y \in L(n) =$ the dense subgroup of $F(n)$, generated algebraically by $x_1,\ldots, x_n$. If $y = x_{i_1}^{e_1} \ldots x_{i_k}^{e_k}$, then $\tau_i(y) = \sum_{i_j=1} e_j$ $(e_i = \pm 1)$ (preceding remark), and $\bar{y} = \sum_{i=1}^{n} \left(\sum_{i_j=1} e_j \right) \bar{x}_i$, whence the result.

Put $c_i = \tau_i(r)$ $(i = 1,\ldots, n)$. One can find elements $b_{2,1}, b_{3,2},\ldots, b_{n,n-1} \in \underline{\underline{Z}}_p$, such that

$$c_1 = -b_{2,1}\, c_2,\ c_2 = -b_{3,2}\, c_3,\ldots,\ c_{n-1} = -b_{n,n-1}\, c_n \,.$$

Put $b_{i,i} = 1$, for $i = 1,\ldots, n$ and $b_{i,j} = 0$, whenever $i \neq j \neq i - 1$. Denote the canonical projection: $\underline{\underline{Z}}_p \to \underline{\underline{Z}}/p\,\underline{\underline{Z}}$ by θ. Let $d_{ij} = \theta(b_{ij})$ $(1 \leq i, j \leq n)$. Then the matrices

$$(b_{ij}) = \begin{pmatrix} 1 & 0 & 0 & & \\ b_{2,1} & 1 & 0 & \bigcirc & \\ 0 & b_{3,2} & 1 & & \\ & & & 1 & \\ & \bigcirc & & \ddots & \\ & & & 1 & 0 \\ & & & b_{n,n-1} & 1 \end{pmatrix} \qquad (d_{ij}) = \left(\begin{matrix} 1 & 0 & 0 & & \\ d_{2,1} & 1 & 0 & & \bigcirc \\ 0 & d_{3,2} & 1 & & \\ & & & 1 & \\ & \bigcirc & & & 1 \\ & & & & d_{n,n-1} \end{matrix} \right.$$

are invertible, and one can find $x'_1, \dots, x'_n$ in F such that $\overline{x}_i = \sum_{j=1}^{n} b_{i,j}\, \overline{x}'_j$ in $F/(F,F)$, and such that the canonical images of $x'_1, \dots, x'_n$ in the $(\mathbb{Z}/p\,\mathbb{Z})$-vector space $F/F^p.(F,F)$, generate that vector space. By [18], Proposition 25, $\{x'_1, \dots, x'_n\}$ is a canonical system of generators for F. According to the above claim,

$$\begin{aligned}
\overline{r} &= \sum_{i=1}^{n} c_i\, \overline{x}_i \\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} c_i \cdot b_{i,j}\, \overline{x}'_j \\
&= \sum_{i=1}^{n} c_i\, \overline{x}'_i + \sum_{i=2}^{n} c_i\, b_{i,i-1} \cdot \overline{x}'_{i-1} \\
&= \sum_{i=1}^{n} c_i\, \overline{x}'_i - \sum_{i=2}^{n} c_{i-1}\, \overline{x}'_{i-1} \\
&= c_n\, \overline{x}'_n \ .
\end{aligned}$$

It follows that $r(x'_n)^{-c_n} \in (F,F)$. Since $r \in F^p.(F,F)$, one has $c_n \in p\,\mathbb{Z}_p$, and this completes the proof of the lemma.

<u>Examples 3.21</u>:

Let G be a pro-p-group, defined by the generators $x_1, \dots, x_n$, and a single relation r. Then r is simple (definition 3.16), if it is a product of the form

$$r = x_n^q \cdot (x_i, x_j)^c \cdot v$$

$n \neq j \neq i, c, q \in \mathbb{Z}_p$, $c \notin p\,\mathbb{Z}_p$, $v \in (F,F)$, $v \in F(x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_n) =$

the closed subgroup of $F(n)$, generated by $x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_n$.

(<u>Proof</u>: $\frac{\partial r}{\partial x_j} = x_n^q \, [1 + (x_i, x_j) + \dots + (x_i, x_j)^{c-1}] \, x_i(1 - x_j \, x_i^{-1} \, x_j^{-1})$.

Note that the element $1 + (x_i, x_j) + \dots + (x_i, x_j)^{c-1}$ is invertible in $A(n)$, because its constant term c is not an element of $p\mathbb{Z}_p$).

r is also simple, if it is of the form $x_1 \, x_2 \, x_3 \, x_1^{-1} \, x_2^{-1} \, x_3^{-1}$ or $x_1 \, x_2 \, x_4 \, x_3^{-1} \, x_4^{-1} \, x_2^{-1} \, x_3 \, x_1^{-1}$, etc.; and $cd(G) \leq 2$, (see theorem 3.18).

These results are superceded by an unpublished result of Labute; arrived at by different methods, according to which $cd \, G \leq 2$ if r is of the form $r = x_n^q \cdot t$, $t \in (F,F)$, and the canonical image of t in the free $\mathbb{Z}_p$-module $gr_2 \, F = (F,F)/(F,(F,F))$ is not divisible by p.

Concerning pro-p-groups G, defined by relations r, lying closer to the ~~group~~ set of p-th powers F^p than these relations, (in the sense that $r \in F^p . F_k$ for $k > 2$ - see theorem 3.11), almost nothing seems to be known. It, therefore, seems to be desirable to investigate pro-p-groups G, defined by relations of the form $x_n^q \cdot u$, where u is a "multiple commutator" in the generators $x_1, \dots, x_n$.

The relations $r_1 = x_1^q \, (x_1, (x_1, x_2))$ and $r_2 = x_1^q \, (x_1, (x_1, (x_1, x_2)))$ are both simple. Indeed,

$$\frac{\partial r_1}{\partial x_2} = x_1^{q+1}(1 - (x_1, x_2) \, x_1^{-1}(x_1, x_2)^{-1}) \; x_1(1 - x_2 \, x_1^{-1} \, x_2^{-1})$$

and

$$\frac{\partial r_2}{\partial x_2} = x_1^{q+1}[1 - (x_1, (x_1, x_2)) \, x_1^{-1}(x_1, (x_1, x_2))^{-1}] \; x_1[1 - (x_1, x_2) \, x_1^{-1}(x_1, x_2)^{-1}] .$$
$$x_1(1 - x_2 \, x_1^{-1} \, x_2^{-1}) .$$

In both cases, it seems to be difficult to determine the order of the canonical image of x_1 in the group G_i defined by the relation r_i $(i = 1, 2)$. If it is of infinite order in G_i, then $cd(G_i) \leqslant 2$, by Corollary 3.14 and Proposition 3.15. At least, we can say that $cd(G_1) \leqslant 2$ or ∞ and $cd(G_2) \leqslant 2$ or ∞ (Theorem 3.17). In both cases, if $q = 0$, then $cd(G_1) \leqslant 2$ and $cd(G_2) \leqslant 2$. ($r_1 \in F_3$, $r_2 \in F_4$, whereas x_1^k ($k \overset{\neq 0}{\in} \mathbb{Z}$), and its conjugates, all lie outside F_3, therefore outside the closed normal subgroups generated by r_1 and r_2 respectively).

Definitions and notations 3.22:

A multiple commutator of type (n,k,m), $(n,k,m \in \mathbb{N})$, is a mapping $c\colon F(n)^k \to F(n)$, defined inductively, as follows: for $m = 1$, c is a projection, i.e. of the form $c(a_1,\dots, a_k) = a_i$ for all $a_j \in F(n)$; for $m > 1$, there exist $h,q \in \mathbb{N}$, such that $h + q = m$, and there exist multiple commutators c_1 and c_2 of type (n,k,h) and (n,k,q), respectively, such that $c(a_1,\dots, a_k) = (y,z)$ $(= yzy^{-1} z^{-1})$, where $y = c_1(a_1,\dots, a_k)$, $z = c_2(a_1,\dots, a_k)$, for all $a_i \in F(n)$, $i = 1,\dots, k$.

A multiple commutator of type (n,k,m), is also said to be a multiple commutator in k variables, of length m.

Suppose c is a multiple commutator of type (n,k,m), $(n \geqslant k \geqslant 2)$, $X = \{x_1,\dots, x_k\}$, M_X the free magma on X, $\phi\colon M_X \to F(n)$ the mapping defined by the equalities: $\phi(x_i) = x_i$ $(i = 1,\dots, k)$, $\phi(ts) = (\phi(t), \phi(s))$, for all $t,s \in M_X$. Suppose that there exists $t \in M_X$, such that x_i

occurs exactly one in the word t and $1 \neq c(x_1, \ldots, x_k) = \phi(t)$; then c is said to be simple in the i-th variable.

Theorem 3.23:

Suppose that c is a multiple commutator of type (n,m,q) $(n \geqslant m \geqslant 2,\ q \geqslant 2)$, simple in the first variable, and $r = c(x_1, \ldots, x_n)$. Then r is a simple relation, and it defines a pro-p-group of cohomological dimension $\leqslant 2$.

Proof:

We may assume that $r \neq 1$. There exist $t,s \in M_X$, $(X = \{x_1, \ldots, x_n\})$, such that

$$r = (\phi(t),\ \phi(s)) = \phi(t \cdot s)$$

and x_1 occurs in either t or s, but not in both. If the length q' of c is equal to two, r reduces to a commutator of the form (x_1, x_i) or (x_i, x_1), and $\frac{\partial r}{\partial x_1} = 1 - x_1\, x_i\, x_1^{-1}$ or $x_i(1 - x_1\, x_i^{-1}\, x_1^{-1})$. The proof now goes by induction on the length of c. Suppose that for every multiple commutator c_1 of type (n,m,k), $2 \leqslant k < q$, $\frac{\partial c_1(x_1, \ldots, x_m)}{\partial x_1}$ is a product of invertible elements and elements of the form $1 - g$, where g^h lies outside the group F_k of the filter $\{F_i\}$ (notations 3.10) for each g and all $h \overset{\neq 0}{\in} \underline{\underline{Z}}_p$. If x_1 occurs in t, then

$$\frac{\partial r}{\partial x_1} = (1 - \phi(t) \cdot \phi(s) \cdot \phi(t)^{-1})\, \frac{\partial \phi(t)}{\partial x_1} \qquad (1)$$

and $\phi(t)$ equals x_1, or is of the form $c_1(x_1, \ldots, x_m)$, where c_1 is scme shorter multiple commutator in m variables, simple in the first variable. By the induction hypothesis, r is a simple relation. If, on the other hand x_1 occurs in s, then

$$\frac{\partial r}{\partial x_1} = \phi(t)\ (1 - \phi(s)\phi(t)^{-1}\ \phi(s)^{-1})\ \frac{\partial\phi(s)}{\phi x_1} \tag{2}$$

and simplicity of r follows, as before from the induction hypothesis. By Theorem 3.11, $\phi(t)^h$, $\phi(s)^h$ and their conjugates lie outside $F_{\ell(t\cdot s)}$ for all $0 \neq h \in \underline{\underline{Z}}_p$ $(\ell(t) < \ell(t\cdot s) > \ell(s))$. Since $r \in F_{\ell(t\cdot s)}$, the closed normal subgroup R of $F(n)$, generated by r, is contained in $F_{\ell(t\cdot s)}$. Thus, $\frac{\partial r}{\partial x_1}$ is a product of invertible elements, and elements of the form $1 - f$, with $f^h \notin R$ for each f and all $h \overset{\neq 0}{\in} \underline{\underline{Z}}_p$. The result now follows from Proposition 3.15 and Corollary 3.14.

<u>Lemma 3.24</u>:

Suppose that c is a multiple commutator in 2 variables (i.e. of type $(n,2,q)$, $n \geqslant 2$, $q \geqslant 2$) simple in the first variable and $r = c(x_1, x_2) \neq 1$. Then $\frac{\partial c(x_1, x_2)}{\partial x_1}$ is a product of invertible elements of $A(n)$, and elements of the form $1 - f$, each f being a <u>conjugate of</u> x_2 <u>or</u> x_2^{-1}.

<u>Proof</u>:

There exist $t,s \in M_X$ $(X = \{x_1, x_2\})$, such that

$$r = (\phi(t), \phi(s)) = \phi(t\cdot s)$$

and x_1 occurs in either t or s but not in both. If x_1 occurs in t, then $\phi(s) = x_2$ and equation (1) of the proof of the preceding theorem applies. If x_1 occurs in s, then $\phi(t) = x_2$, and equation (2) of the proof of the preceding theorem applies. The proof can be completed by an induction argument, as in the previous proof.

Theorem 3.25:

Let $(c_1,\dots, c_m)$ be a sequence of multiple commutators in two variables (i.e. c_i is of the type $(n,2,q_i)$), simple in the first variable. Let $r \in F(n)$, $n \geqslant 2$, and suppose that there exist sequences $(u_1,\dots, u_m)$ and $(y_1,\dots, y_{m-1})$ of elements of $F(n)$, with the following properties:

$$u_1 = c_1(x_1, x_2)$$

$$u_2 = c_2(x_2, y_1) \quad \text{if} \quad m \geqslant 2$$

$$u_j = c_j(y_{j-2}, y_{j-1}) \quad \text{if} \quad 3 \leqslant j \leqslant m$$

$$u_m = r \; ;$$

for each $j = 1,\dots, m$, $y_j = u_j$ or $y_j = x_{i_j} \in \{x_3,\dots, x_n\}$, subject to the condition that $y_k \neq x_{i_j}$, whenever $k \neq j$.

Then $cd(F(n)/R) \leqslant 2$, R being the closed normal subgroup generated by r.

Proof:

By virtue of theorem 3.23, we may restrict ourselves to the case $m \geqslant 2$. We shall assume that $F(n+m-1)$, the free group on $x_1,\dots, x_{n+m-1}$, contains $F(n)$ as closed subgroup, in the obvious way. Define for $j = 1,\dots, m-1$:

$$z_j = \begin{cases} x_{i_j} & \text{if } y_j = x_{i_j} \\ x_{n+j} & \text{if } y_j = u_j . \end{cases}$$

Define:

$$r_1 = x_{n+1}^{-1} c_1(x_1, x_2)$$

$$r_2 = \begin{cases} c_2(x_2, z_1) & \text{if } m = 2 \\ x_{n+2}^{-1} c_2(x_2, z_1) & \text{if } m > 2. \end{cases}$$

If $3 \leqslant j < m$, then put:

$$r_j = x_{n+j}^{-1} c_j(z_{j-2}, z_{j-1})$$

Put $$r_m = c_m(z_{m-2}, z_{m-1}) \quad \text{if } m \geqslant 3.$$

Define a morphism $\alpha\colon F(n+m-1) \to F(n)$, by putting

$$\alpha(x_i) = \begin{cases} x_i & \text{for } i = 1,\dots, n \\ u_{i-n} & \text{for } i = n+1,\dots, n+m-1. \end{cases}$$

Note that $\alpha(z_j) = y_j$ for all $j = 1,\dots, m-1$.

Let $G = F(n)/R$ and denote by N the closed normal subgroup of $F(n+m-1)$, generated by $r_1,\dots, r_m$, $G' = F(n+m-1)/N$, $\pi'\colon A(n+m-1) \to \Lambda' = \underline{\underline{Z}}_p[[G']]$ the canonical extension of the projection $F(n+m-1) \to G'$.

Claim (1):

$$\pi'(z_j) = \pi'(y_j) \quad \text{for all} \quad j = 1, \ldots, m-1.$$

Proof:

Either $y_1 = x_{i_1}$ or $y_1 = u_1$. In the first case $\pi'(z_1) = \pi'(y_1)$ and in the second case, $\pi'(z_1) = \pi'(x_{n+1}) = \pi'(c_1(x_1, x_2))$ (since $\pi'(r_1) = 1) = \pi'(u_1) = \pi'(y_1)$. If $m > 2$, then either $y_2 = x_{i_2}$ or $y_2 = u_2$. In the first case, $\pi'(z_2) = \pi'(y_2)$ and, in the second case, $\pi'(z_2) = \pi'(x_{n+2}) = \pi'(c_2(x_2, z_1))$ (since $\pi'(r_2) = 1) = c_2(\pi'(x_2), \pi'(z_1))$ $= c_2(\pi'(x_2), \pi'(y_1)) = \pi'(u_2) = \pi'(y_2)$. Now, let us assume the induction hypothesis that $\pi'(z_j) = \pi'(y_j)$ for $j = 1, \ldots, k$ $(2 \leqslant k < m-1)$. Again, if $y_{k+1} = x_{i_{k+1}}$, then $\pi'(z_{k+1}) = \pi'(y_{k+1})$, so we may suppose that $y_{k+1} = u_{k+1}$ and $z_k = x_{n+k+1}$, $\pi'(z_{k+1}) = \pi'(x_{n+k+1}) = \pi'(c_{k+1}(z_{k-1}, z_k)$ $= c_{k+1}(\pi'(z_{k-1}), \pi'(z_k)) = c_{k+1}(\pi'(y_{k-1}), \pi'(y_k))$, by the induction hypothesis. Thus, $\pi'(z_{k+1}) = \pi'(c_{k+1}(y_{k-1}, y_k)) = \pi'(u_{k+1}) = \pi'(y_{k+1})$, and the proof of claim (1) is completed.

Claim (2): $R \subset N$.

Proof:

If $m = 2$, then $\pi'(r) = \pi'(u_2) = \pi'(c_2(x_2, y_1)) = \pi'(c_2(x_2, z_1))$, by claim (1). Since $\pi'(r_2) = 1$, we obtain $\pi'(r) = 1$.

If $m > 2$, then $\pi'(r) = \pi'(u_m) = \pi'(c_m(y_{m-2}, y_{m-1})) = \pi'(c_m(z_{m-2}, z_{m-1}))$, by claim (1); therefore $\pi'(r) = \pi'(r_m) = 1$. It follows that $\pi'(R) = (1)$ and $R \subset N$, so that the proof of claim (2) is completed.

Claim (3): $\gamma(N) = 1$.

Proof:

It suffices to show that $\gamma(r_i) = 1$ for all $i = 1, \dots, m$. $\gamma(r_1) = \pi(\alpha(r_1)) = \pi(\alpha(x_{n+1})^{-1})\ \pi(c_1(x_1, x_2)) = \pi(u_1)^{-1}\ \pi(u_1) = 1$. If $m = 2$, $\gamma(r_2) = \pi(\alpha(c_2(x_2, z_1)) = \pi(c_2(x_2, \alpha(z_1))) = \pi(c_2(x_2, y_1)) = \pi(u_2) = \pi(r) = 1$. If $3 \leqslant j \leqslant m-1$, then $\gamma(r_j) = \pi(\alpha(x_{n+j}))^{-1}\ \pi(\alpha(c_j(z_{j-2}, z_{j-1}))) = \pi(u_j)^{-1}\ \pi(u_j) = 1$; because $\alpha(z_{j-1}) = y_{j-1}$ and $\alpha(z_{j-2}) = y_{j-2}$. If $m \geqslant 3$, $\gamma(r_m) = \pi(\alpha(c_m(z_{m-2}, z_{m-1}))) = \pi(u_m) = 1$. This completes the proof of claim (3).

The morphism γ: $F(n+m-1) \to G$ now induces a morphism ψ: $G' \to G$.

Claim (4): $\psi \circ \phi = 1$.

Proof:

Since $\pi(x_1), \dots, \pi(x_n)$ generate a dense subgroup of G, it suffices to show that $\psi(\phi(\pi(x_i))) = \pi(x_i)$ for $i = 1, \dots, n$. One has $\psi(\phi(\pi(x_i))) = \psi(\pi'(x_i)) = \gamma(x_i) = \pi(x_i)$ for all $i = 1, \dots, n$ and this completes the proof of claim (4).

$N/(N,N)$ is endowed with the structure of a Λ'-module, obtained from the action of G' on $N/(N,N)$, by inner automorphisms. We know that $cd(G') \leqslant 2$, iff $N/(N,N)$ is a free Λ'-module (see, for instance, Brumer's article [3] Corollary 5.3 or the resolution constructed in the proof of Theorem 3.13). Since, by claim (4), G is isomorphic to a closed subgroup of G', the proof of the theorem will be complete if we can show that $N/(N,N)$ is a free Λ'-module. Denoting the action of Λ' on $N/(N,N)$ by *, and the canonical images of $r_1,,,., r_m$ in $N/(N,N)$ by $[r_1],\ldots, [r_m]$ respectively, we shall suppose that $\prod_{j=1}^{m} \lambda_j*[r_j] = 1$, whence the m equations:

$$\lambda_1\ \pi'\frac{(\partial r_1)}{\partial x_1} = 0$$

$$\lambda_1\ \pi'\frac{(\partial r_1)}{\partial x_2} + \lambda_2\ \pi'\frac{(\partial r_2)}{\partial x_2} = 0$$

$$\lambda_1\ \pi'\frac{(\partial r_1)}{\partial z_1} + \lambda_2\ \pi'\frac{(\partial r_2)}{\partial z_1} + \lambda_3\ \pi'\frac{(\partial r_3)}{\partial z_1} = 0$$

$$\lambda_2\ \pi'\frac{(\partial r_2)}{\partial z_2} + \lambda_3\ \pi'\frac{(\partial r_3)}{\partial z_2} + \lambda_4\ \pi'\frac{(\partial r_4)}{\partial z_2} = 0$$

$$- \quad - \quad - \quad - \quad - \quad - \quad -$$

$$- \quad - \quad - \quad - \quad - \quad - \quad -$$

$$\lambda_{m-2}\ \pi'\frac{(\partial r_{m-2})}{\partial z_{m-2}} + \lambda_{m-1}\ \pi'\frac{(\partial r_{m-1})}{\partial z_{m-2}} + \lambda_m\ \pi'\frac{(\partial r_m)}{\partial z_{m-2}} = 0\ .$$

It, therefore, suffices to prove that the elements $\pi'\frac{(\partial r_1)}{\partial x_1}$. $\pi'\frac{(\partial r_2)}{\partial x_2}$, $\pi'\frac{(\partial r_3)}{\partial z_1}$,..., $\pi'\frac{(\partial r_m)}{\partial z_{m-2}}$ of Λ', are not zero-divisors on the right, or, equivalently, that the elements $\pi'(x_2)$, $\pi'(z_1),\ldots, \pi'(z_{m-1})$ of G' are not of finite order, (see Proposition 3.15, Theorem 3.13 and Lemma 3.2

It suffices to show that their images $\psi(\pi'(x_2)), \psi(\pi'(z_1)), \ldots, \psi(\pi'(z_{m-1}))$ in G are of infinite order. One has $\psi(\pi'(x_i)) = \pi(x_i)$ and $\varepsilon \circ \frac{\partial}{\partial x_i} \mid R = 0$ for all $i = 1, \ldots, n$, whereas $\varepsilon(\frac{\partial x_i^k}{\partial x_i}) = k$ for all $k \in \mathbb{Z}_p$. It follows that $\pi(x_i)$ is of infinite order in G for all $i = 1, \ldots, n$. One has $\psi(\pi'(z_j)) = \gamma(z_j) = \pi(y_j)$, and, in view of the remark contained in the preceding sentence, we suppose, without loss in generality, that $y_j = u_j$. We now distinguish between the following two cases (and we assume, without loss in generality, that $r \neq 1$):

<u>Case (i)</u>: <u>there exists a</u> k <u>such that</u> $j < k \leqslant m-1$ <u>and</u> $y_k = x_{i_k}$.

Define a morphism $\beta\colon F(n) \to F(n)$ by putting

$$\beta(x_i) = \begin{cases} x_i & \text{when } x_i \notin \{y_{j+1}, \ldots, y_m\}, \\ 1 & \text{when } x_i \in \{y_{j+1}, \ldots, y_m\}. \end{cases}$$

Then $\beta(u_j) = u_j$, $\beta(u_{k+1}) = \ldots = \beta(u_m) = \beta(r) = 1$ (because $c_{k+1}(y_{k-1}, 1) = 1$), $\beta(R) = (1)$, whence $u_j^k \notin R$, for all $k \overset{\neq 0}{\in} \mathbb{Z}_p$, $\pi(u_j)$ is of infinite order in G and $\pi'(z_j)$ is of infinite order in G'.

<u>Case (ii)</u>: <u>the inequality</u> $j < k \leqslant m-1$ <u>implies</u> $y_k = u_k$.

Then $u_{k+1} = c_{k+1}(u_{k-1}, u_k)$ and $U_{k+1} \subset U_k$ for $j \leqslant k \leqslant m-1$, where U_k designates the closed, normal subgroup of $F(n)$, generated by u_k. Now let m be a word of minimal length in the free monoid M on $T_1, \ldots, T_n$, such that, in the formal power series $u_j - 1 = \sum_{1 \neq m\ M} (u_j)_m$

the coefficient $(u_j)_m \neq 0$. Then $(u_j^k)_m \neq 0$ for all $k \overset{\neq 0}{\in} \mathbb{Z}_p$. On the other hand, for every $f \in F(n)$, $(fu_j\, f^{-1}\, u_j^{-1})_m = 0$, (by direct calculation, or theorem 3.11) so that the equality $u_{j+1} = c_{j+1}(u_{j-1}, u_j))$ implies $(u_{j+1})_m = 0$, and consequently, $a_m = 0$, for every $a \in U_{j+1} \supset U_m = R$. It follows that no power of u_j lies in R, $\pi(u_j)$ is of infinite order in G and $\pi'(z_j)$ is of infinite order in G'.

This completes the proof of the theorem.

<u>Example 3.26</u>:

(i) Let $n > 2$. One may define multiple commutators $c_1, \dots, c_5$ by the following identities:

$$c_1(a,b) = (a,b),\ c_2(a,b) = (b,(b,a)),\ c_3(a,b) = (a,b),\ c_4(a,b) = (a,b) = c_5(a,b)$$

Define $(y_1, \dots, y_5) = (u_1, u_2, x_3, u_4, u_5)$. Then

$$u_1 = c_1(x_1, x_2) = (x_1, x_2)$$

$$u_2 = c_2(x_2, u_1) = (u_1, (u_1, x_2)) = ((x_1, x_2), ((x_1, x_2), x_2))$$

$$u_3 = c_3(u_1, u_2) = ((x_1, x_2), ((x_1, x_2), ((x_1, x_2), x_2)))$$

$$u_4 = c_4(u_2, x_3) = (((x_1, x_2), ((x_1, x_2), x_2)), x_3)$$

$$u_5 = c_5(x_3, u_4) = (x_3, (((x_1, x_2), ((x_1, x_2), x_2)), x_3)) \ .$$

Each of the elements u_i $(i = 1, \dots, 5)$ defines a pro-p-group of coh. dim. $\leqslant 2$.

By theorem 3.25, one has $cd(G) \leqslant 2$ if G is defined by the "relation" $((x_1, x_2), ((x_1, x_2), (x_1, (x_1, x_2))))$, or by the "relation" $(((x_1, (x_1, x_2)), ((x_1, (x_1, x_2)), x_2)))$.

Every one of the "relations" $r_1 = x_3^q (x_1, x_2)$, $r_2 = x_3^q (x_1, (x_1, x_2))$, $r_3 = x_3^q (x_1, (x_1, (x_1, x_2)))$, etc., defines a pro-p-group of cohomological dimension $\leqslant 2$. Indeed, by lemma 3.24, $\frac{\partial r_i}{\partial x_2}$ is a product of invertible elements of $A(3)$, and elements of the form $1 - f$, each f being a conjugate of x_1 or x_1^{-1}. If R_i is the closed normal subgroup of $F(3)$, generated by r_i, $(i = 1, 2, \ldots)$, then $\varepsilon \circ \frac{\partial}{\partial x_1} \mid R_i = 0$. On the other hand, $\varepsilon(\frac{\partial x_1^k}{\partial x_1}) = k$, for all $k \in \underline{\underline{Z}}_p$. By corollary 3.14 and Proposition 3.15, $cd(F(3)/R_i) \leqslant 2$, for all $i = 1, 2, \ldots$.

Remarks 3.27:

In a recent letter to the author, Dr. J. Labute states that the morphism μ of theorem 3.13, is always injective, even when the elements $\pi^n(\Delta r_1), \ldots, \pi^n(\Delta r_m)$ of Λ^n, are not linearly independent over Λ . This would imply that $cd(G) = 2$ if, and only if, $\pi^n(\Delta r_1), \ldots, \pi^n(\Delta r_m)$ are linearly independent over Λ .

I wish to take this opportunity to thank Dr. Labute for his interest in my work, for his valuable comments on my letters, and for his encouragement, during the preparation of Part II of this thesis.

BIBLIOGRAPHY

[1] BOURBAKI, Livre II, Algèbre, Chap.I, Structures Algébriques, 2e édition, Hermann, Paris.

[2] BOURBAKI, Livre II, Algèbre, Chap.IV et V, 2e édition, Hermann Paris.

[3] A. BRUMER, Pseudo-compact algebras, profinite groups and class formation, to appear in the Journal of Algebra; research announcement in the Bulletin of the AMS, 72, #2.

[4] I. CONNELL, On the Group Ring, Can. J. of Maths, 15, #4 (1963).

[5] D. GILDENHUYS and W. KUYK, Extension de corps dont le pro-p-groupe de Galois est prescrit, C.R. Acad. Sc. Paris, t.262, pp.560-562 (1966).

[6] M. HALL, The Theory of Groups, The Macmillan Company, New York (1959).

[7] M. KRASNER and L. KALOUJNINE, Produit complet de groupes de permutations et problème d'extension de groupes III, Acta Szeged, 15 (1951).

[8] W. KUYK, Over het Omkeer-probleem van de Galois-theorie, thesis, Vrije Universiteit te Amsterdam (1960).

[9] W. KUYK, Report, Math. Centre, Amsterdam, ZW 1961-010.

[10] W. KUYK and P. MULLENDER, On the invariants of finite abelian groups, Proc. of Koninkl. Nederl. Akademie van Wetenschappen, Series A, 66, #2.

[11] J. LABUTE, Classification des Groupes de Demuskin, C.R. Acad. Sc. Paris, t.260.

[12] J. LABUTE, Les groupes de Demuskin de rang dénombrable, C.R. Acad. Sc. Paris, t.262 (janv. 1966).

[13] S. LANG, Diophantine Geometry, Interscience p.141 ff (1962).

[14] M. LAZARD, Groupes analytiques p-adiques, IHES Publ. no.26.

[15] R. LYNDON, Cohomology Theory of Groups with a single defining relation, Annals of Maths, Vol.52, No.3 (1950).

[16] K. MASUDA, On a problem of Chevalley, Nagoya Math. J., Vol.8, 1955.

[17] NEUMANN, Wreath products and varieties of groups, Math. Zeitschift, 80, pp.44-62 (1962).

[18] J.-P. SERRE, Cohomologie Galoisienne, Lecture Notes in Mathematics, Springer Verlag, Berlin (1964).

[19] J.-P. SERRE, Lie Algebras and Lie Groups, Harvard University Lecture Notes.

[20] J.-P. SERRE, Structures de certains pro-p-groupes, Séminaire Bourbaki, exp.252.

[21] J.-P. SERRE, Corps Locaux, Actualités Scientifiques et Industrielles 1296, Hermann, Paris.