

Covering groups and presentations of finite groups I

By SIEGFRIED MORAN (Canterbury)

Suppose one is given a finitely generated group G and a prime power p^λ . Then associated with this data one has a uniquely determined group $G_{p^\lambda}^*$ with the following properties. In a presentation F/N of $G_{p^\lambda}^*$ on a minimal number of generators

$$N \subseteq F^{p^\lambda} \cdot F'$$

and $G_{p^\lambda}^*$ is the minimal group with this property lying above G . Also

$$G_{p^\lambda}^*/\pi_{p^\lambda}(G) \cong G.$$

The p^λ -th fundamental group $\pi_{p^\lambda}(G)$ lies in the centre of $G_{p^\lambda}^*$ and has exponent dividing p^λ . The group G is finite if and only if $G_{p^\lambda}^*$ is finite.

If $G_{p^\lambda}^*$ is finite, then it has a presentation of the form

$$\langle x_1, \dots, x_d; x_1^{p^\lambda \cdot \beta_1} = \dots = x_d^{p^\lambda \cdot \beta_d} = u_1 = \dots = u_{r(k)} = 1 \rangle,$$

where every $\beta_i > 0$, $X = \{x_1, x_2, \dots, x_d\}$, every u_i belongs to $F(X)_{k,p}$ — the k -th dimension subgroup of the free group $F(X)$ modulo p — and k is a natural number greater than 1. It can be shown, using results of E. S. GOLOD and I. R. ŠAFAREVIČ [2], E. B. VINBERG [14] and H. KOCH [9], that

$$r(k) > \text{Max} \{(d/2)^k - d(2/d)^{p^\lambda - k}, (d/k)^k (k-1)^{k-1} - d\}$$

for $p^\lambda \geq k$. Thus in particular

$$r(2) \geq d^2/4 \quad \text{for} \quad p^\lambda \geq 9.$$

This result is new even for finite p -groups. The basic inequality (Theorem 3.6) enables us also to give a generalisation of two inequalities of W. GASCHÜTZ and M. F. NEWMAN [1] (see Lemma 3.9, Theorem 3.10 and Theorem 4.4).

§ 1. Smooth Groups

1.1 Definition. Let m be a positive integer greater than 1. Suppose that the group G has a set of generators X . Then G is said to be m -smooth with respect to X if and only if $G/(G' \cdot G^m)$ is naturally isomorphic to $|X|(Z_m)$ (via its set of generators X). Here and subsequently $|X|(Z_m)$ stands for the (restricted) direct product of $|X|$ copies of Z_m .

The proofs of the following two lemmas are quite easy.

1.2 Lemma. Let $m = \prod_{i=1}^t p_i^{a_i}$ be the decomposition of m into a product of distinct prime powers. Then G is m -smooth with respect to X if and only if G is $p_i^{a_i}$ -smooth with respect to X for every $i=1, \dots, t$.

1.3 Lemma. Suppose that G is m -smooth with respect to X . Then X is a minimal set of generators for G .

1.4 Definition. Let $F = F(X)$ denote the free group on the set X of free generators. An element of F is said to be m -smooth with respect to X if and only if it belongs to $F^m F'$.

1.5 Note. An element of $F = F(X)$ is m -smooth with respect to X if and only if it has a representation of the form

$$x_{\alpha_1}^{mn_1} x_{\alpha_2}^{mn_2} \dots x_{\alpha_k}^{mn_k} u,$$

where $x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_k}$ are distinct elements of X , every n_i is an integer and u belongs to F' .

1.6 Notation. Let $\langle X; R \rangle$ be a presentation of a group G . Then the presentation is said to be m -smooth if and only if every element of R is m -smooth with respect to X . If $f=1$ is some relation holding in a presentation for a group G in terms of a set Y of generators and f is m -smooth with respect to Y , then $f=1$ is said to be an m -smooth relation in G with respect to Y .

1.7 Lemma. If G has an m -smooth presentation on a finite set X of generators, then any presentation of G on a set Y of generators with $|Y|=|X|$ is m -smooth with respect to Y .

PROOF. *)

$$G \cong F(X)/R(X) \cong F(Y)/R(Y),$$

where $R(X)$ is contained in $F(X)^m \cdot F(X)'$. Now

$$G/G^m G' \cong F(X)/F(X)^m \cdot F(X)' \cong F(Y)/R(Y) \cdot F(Y)^m \cdot F(Y)'.$$

Thus $G/G^m G'$ is the direct product of $|X|$ copies of Z_m , which gives that $R(Y) \subseteq F(Y)^m \cdot F(Y)'$.

We state without proof the following easy result.

1.8 Lemma. G is m -smooth with respect to X if and only if G has an m -smooth presentation on X .

1.9 Examples

(i) Every perfect group is not m -smooth with respect to any set of generators and any m .

*) We do not assume here and elsewhere, although the notation might be considered to suggest it, that $R(Y)$ is obtained from $R(X)$ on replacing x_i by y_i for $i=1, 2, \dots, n$, where

$$X = \{x_1, x_2, \dots, x_n\} \quad \text{and} \quad Y = \{y_1, y_2, \dots, y_n\}.$$

(ii) Every finitely generated nilpotent group G is p -smooth with respect to a minimal set of generators. If G is such that G/G' is torsion-free, then p can be chosen to be any prime number. If the torsion subgroup $T(G/G')$ of G/G' is non-trivial, then p can be chosen to be any prime number p such that the p -Sylow subgroup of $T(G/G')$ has the largest minimal generating set amongst all the Sylow subgroups of $T(G/G')$.

(iii) Let G be a finite group, P be a p -Sylow subgroup of G and $d(G)$ denote the number of elements in a minimal generating set X for G . Then G is p -smooth with respect to X if and only if

$$d(G) = d(P/P^p \cdot (P \cap G')).$$

This follows at once from a well known theorem in transfer theory (see for instance B. HUPPERT [6] Satz 3.3, p. 422).

(iv) A finite non-cyclic group all of whose Sylow subgroups are cyclic is not m -smooth with respect to any set of generators for any m . This is so since the factor commutator group is cyclic (see for instance H. ZASSENHAUS [15] p. 145).

§ 2. Smooth Covering Groups

2.1 *Definition.* Let G be a group having a presentation $F(X)/K(X)$, where $K(X)$ is a normal subgroup of the free group $F(X)$ on the set X of free generators. Then

$$F(X)/(K(X) \cap (F(X)^m \cdot F(X)'))$$

is denoted by $G_m^\circ(X)$ and is called the m -smooth covering group of G with respect to X .

2.2 *Note.* The relations of $G_m^\circ(X)$ are those relations of G which are m -smooth with respect to X .

2.3 *Note.* If a group H has an m -smooth presentation on X and there exists a natural homomorphism of H onto G , then there exists a natural homomorphism of H onto $G_m^\circ(X)$, which makes the obvious diagram commutative. Here natural homomorphisms are defined via the identity mapping on X .

2.4 *Note.* $G_m^\circ(X)$ is a central extension of an abelian m -group A by the group G . If X is a finite set, then A has a finite number of generators. In fact

$$A \cong K(X) \cdot F(X)^m \cdot F(X)' / F(X)^m \cdot F(X)',$$

where $G \cong F(X)/K(X)$.

2.5 **Lemma.** Let m_1 and m_2 be coprime integers greater than 1. Then

$$G_{m_1 m_2}^\circ(X) \cong (G_{m_2}^\circ(X))_{m_1}^\circ(X).$$

2.6 *Construction.* Let X be a set of generators for a group G . For every x in X let $\langle z_x \rangle$ denote a cyclic group of order m . By $\bar{G}_m(X)$ we denote the group

$$G \times \left(\prod_{x \in X}^\times \langle z_x \rangle \right),$$

where Π^* denotes the restricted direct product. Let $X^* = \{(x, z_x); x \in X\}$. Then $G_m^*(X^*)$ will denote the subgroup of $\bar{G}_m(X)$ generated by the set of elements X^* . By calculating in $\bar{G}_m(X)$ one can easily establish the following result.

2.7 Lemma. *A relation (in terms of the set X^* of generators) holds in $G_m^*(X^*)$ if and only if*

- (i) *it is m -smooth with respect to X^* and*
- (ii) *under the natural mapping $X^* \rightarrow X$ it goes over to a relation which holds between the elements of X in G .*

2.7.1 Corollary

$$G_m^\circ(X) \cong G_m^*(X^*)$$

under the natural mapping induced by $x \rightarrow x^*$.

2.8 Theorem. *Let the group G have a presentation of the form $F(X)/K(X)$, where $K(X)$ is a normal subgroup of the free group $F(X)$. Then, for every prime number p ,*

$$G_p^\circ(X) \cong G \times d' \cdot (Z_p),$$

where $d' = \dim_{Z_p}(K(X) \cdot F(X)^p \cdot F(X)' / F(X)^p \cdot F(X)')$ and $d' + \dim_{Z_p}(G/G^p G') = |X|$.

PROOF. Let X_1 be a subset of X such that $\{x \cdot G^p G'; x \in X_1\}$ forms a basis for $G/G^p G'$. Let X_2 be the complement of X_1 in X . By X_1^* and X_2^* we denote the corresponding subsets of X^* . We have the following mapping

$$\Theta : G_p^*(X^*) \rightarrow \bar{G}_p(X)$$

defined by

$$\Theta(x^*) = \begin{cases} x & \text{if } x^* \in X_1^* \\ x \cdot z_x & \text{if } x^* \in X_2^* \end{cases}$$

and $\Theta(x_{\alpha_1}^{*n_1} \dots x_{\alpha_k}^{*n_k} \cdot u(x^*)) = \Theta(x_{\alpha_1}^*)^{n_1} \dots \Theta(x_{\alpha_k}^*)^{n_k} \cdot u(x^*)$, where every $x_{\alpha_i}^* \in X^*$, every n_i is an integer and $u(x^*)$ belongs to $(G_p^*(X^*), G_p^*(X^*))$.

Θ is single-valued. For suppose

$$x_{\alpha_1}^{*n_1} \dots x_{\alpha_k}^{*n_k} \cdot u(x^*) = 1 \quad \text{in } G_p^*(X^*).$$

Then, by Lemma 2.7, we have that

$$\Theta(x_{\alpha_1}^{*n_1} \dots x_{\alpha_k}^{*n_k} \cdot u(x^*)) = 1 \quad \text{in } \bar{G}_p(X).$$

Θ is a group homomorphism. For suppose that

$$x_{\alpha_1}^{*n_1} \dots x_{\alpha_k}^{*n_k} \cdot u_1(x^*) \cdot x_{\alpha_1}^{*m_1} \dots x_{\alpha_k}^{*m_k} \cdot u_2(x^*) = x_{\alpha_1}^{*n_1+m_1} \dots x_{\alpha_k}^{*n_k+m_k} \cdot u_3(x^*)$$

in $F(X^*)$. Then

$$\begin{aligned} & \Theta(x_{\alpha_1}^{*n_1} \dots x_{\alpha_k}^{*n_k} \cdot u_1(x^*) \cdot x_{\alpha_1}^{*m_1} \dots x_{\alpha_k}^{*m_k} \cdot u_2(x^*)) = \\ &= \Theta(x_{\alpha_1}^*)^{n_1+m_1} \dots \Theta(x_{\alpha_k}^*)^{n_k+m_k} \cdot u_3(x^*) = \\ &= \Theta(x_{\alpha_1}^*)^{n_1} \dots \Theta(x_{\alpha_k}^*)^{n_k} \cdot u_1(x^*) \cdot \Theta(x_{\alpha_1}^*)^{m_1} \dots \Theta(x_{\alpha_k}^*)^{m_k} \cdot u_2(x^*) = \\ &= \Theta(x_{\alpha_1}^{*n_1} \dots x_{\alpha_k}^{*n_k} \cdot u_1(x^*)) \cdot \Theta(x_{\alpha_1}^{*m_1} \dots x_{\alpha_k}^{*m_k} \cdot u_2(x^*)). \end{aligned}$$

The kernel of Θ is trivial. For suppose that

$$\Theta(x_{\alpha_1}^{*n_1} \dots x_{\alpha_k}^{*n_k} \cdot u(x^*)) = 1 \quad \text{in} \quad \bar{G}_p(X).$$

Then

$$x_{\alpha_1}^{n_1} \dots x_{\alpha_k}^{n_k} \cdot u(x) = 1 \quad \text{in} \quad G.$$

Also if $x_{\alpha_i}^* \in X_2^*$, then p divides n_i for every i . On considering the latter relation in G modulo $G^p G'$, one has, by the construction of the set X_1 , that p divides n_i if $x_{\alpha_i}^* \in X_1^*$. So, by Lemma 2.7,

$$x_{\alpha_1}^{*n_1} \dots x_{\alpha_k}^{*n_k} \cdot u(x^*) = 1 \quad \text{in} \quad G_p^*(X^*).$$

Finally we show that if $x \in X_2$, then z_x belongs to $\Theta(G_p^*(X^*))$. This will show that Θ is the required isomorphism. By the construction of the set X_1 , we have that if $x \in X_2$, then

$$x = x_{\alpha_1}^{m_1} \dots x_{\alpha_k}^{m_k} \cdot w(x),$$

where $0 \leq m_i < p$, the element $x_{\alpha_i} \in X_1$ for every i and $w(x)$ belongs to $G^p G'$. Now

$$\Theta(x^*) = x \cdot z_x$$

while

$$\Theta(x_{\alpha_1}^{*m_1} \dots x_{\alpha_k}^{*m_k} \cdot w(x^*)) = x_{\alpha_1}^{m_1} \dots x_{\alpha_k}^{m_k} \cdot w(x).$$

So

$$\Theta(x^* \cdot (x_{\alpha_1}^{*m_1} \dots x_{\alpha_k}^{*m_k} \cdot w(x^*))^{-1}) = z_x$$

and

$$\Theta(G_p^*(X^*)) = G \times \prod_{x \in X_2}^{\times} \langle z_x \rangle.$$

The results concerning the number d' now follow from the established fact that, by corollary 2.7.1,

$$G_p^{\circ}(X) \cong G \times \prod_{x \in X_2}^{\times} \langle z_x \rangle.$$

2.9 Example. If m is not a prime number, then it is no longer true in general that $G_m^*(X^*)$ is isomorphic to a group of the form $G \times A$. Thus for instance the p^2 -smooth covering group of Z_p with respect to a single generator is Z_{p^2} .

2.10 Lemma. Let $\varphi: G \rightarrow H$ be a homomorphism of groups which have a set of generators X and Y respectively. Suppose that

$$(2.10.1) \quad \varphi(x_{\alpha}) = f_{\alpha}(y_{\beta}),$$

where $X = \{x_{\alpha}, \alpha \in M\}$ and $f_{\alpha}(y_{\beta})$ is a word in the elements of the set $Y = \{y_{\beta}, \beta \in N\}$ for every $\alpha \in M$. Then

$$(2.10.2) \quad \varphi_f^*(x_{\alpha}^*) = f_{\alpha}(y_{\beta}^*)$$

for every $\alpha \in M$ defines a homomorphism

$$\varphi_f^*: G_m^*(X^*) \rightarrow H_m^*(Y^*)$$

by means of

$$\varphi_f^*(x_{\alpha_1}^{*n_1} \dots x_{\alpha_k}^{*n_k} \cdot u(x^*)) = \varphi_f^*(x_{\alpha_1}^*)^{n_1} \dots \varphi_f^*(x_{\alpha_k}^*)^{n_k} \cdot u(\varphi_f^*(x^*)),$$

where $u(x^*)$ belongs to $G_m^*(X^*)'$. The following diagram is commutative

$$\begin{array}{ccc} G_m^*(X) & \xrightarrow{\varphi_f^*} & H_m^*(Y) \\ \downarrow & & \downarrow \\ G & \xrightarrow{\varphi} & H \end{array}$$

Further suppose that $\psi: H \rightarrow K$ is a homomorphism and K has a set T of generators such that

$$\psi(y_\beta) = g_\beta(t_\gamma)$$

for every $\beta \in N$, where $T = \{t_\gamma\}$ and $g_\beta(t_\gamma)$ is a word in the elements of T for every $\beta \in N$. Then

$$\psi_g^* \circ \varphi_f^* = (\psi \circ \varphi)_{f \circ g}^*.$$

PROOF. (i) φ_f^* is single-valued. For suppose that

$$x_{\alpha_1}^{*n_1} \dots x_{\alpha_k}^{*n_k} \cdot u(x^*) = 1 \quad \text{in} \quad G_m^*(X^*).$$

Then n_i is divisible by m for every i and

$$x_{\alpha_1}^{n_1} \dots x_{\alpha_k}^{n_k} \cdot u(x) = 1 \quad \text{in} \quad G,$$

by Lemma 2.7. So

$$f_{\alpha_1}(y_\beta)^{n_1} \dots f_{\alpha_k}(y_\beta)^{n_k} \cdot u(f(y_\beta)) = 1 \quad \text{in} \quad H.$$

Since m divides n_i for every i , the latter relation implies that

$$f_{\alpha_1}(y_\beta^*)^{n_1} \dots f_{\alpha_k}(y_\beta^*)^{n_k} \cdot u(f(y_\beta^*)) = 1 \quad \text{in} \quad H_m^*(Y^*).$$

This says that

$$\varphi_f^*(x_{\alpha_1}^*)^{n_1} \dots \varphi_f^*(x_{\alpha_k}^*)^{n_k} \cdot u(\varphi_f^*(x^*)) = 1 \quad \text{in} \quad H_m^*(Y^*).$$

Hence φ_f^* is single-valued.

(ii) φ_f^* preserves the group operation. For suppose that

$$\begin{aligned} & x_{\alpha_1}^{*n_1} \dots x_{\alpha_k}^{*n_k} \cdot u_1(x^*) \cdot x_{\alpha_1}^{*m_1} \dots x_{\alpha_k}^{*m_k} \cdot u_2(x^*) = \\ & = x_{\alpha_1}^{*n_1+m_1} \dots x_{\alpha_k}^{*n_k+m_k} \cdot u_3(x^*) \quad \text{in} \quad F(X^*). \end{aligned}$$

Then, as in the proof of Theorem 2.8, we have that

$$\begin{aligned} & \varphi_f^*(x_{\alpha_1}^{*n_1} \dots x_{\alpha_k}^{*n_k} \cdot u_1(x^*) \cdot x_{\alpha_1}^{*m_1} \dots x_{\alpha_k}^{*m_k} \cdot u_2(x^*)) = \\ & = \varphi_f^*(x_{\alpha_1}^{*n_1} \dots x_{\alpha_k}^{*n_k} \cdot u_1(x^*)) \cdot \varphi_f^*(x_{\alpha_1}^{*m_1} \dots x_{\alpha_k}^{*m_k} \cdot u_2(x^*)). \end{aligned}$$

(iii) By definition,

$$(\psi \circ \varphi)_{f \circ g}^* : G_m^*(X^*) \rightarrow K_m^*(T^*)$$

and the group homomorphism is defined by

$$\begin{aligned}
 (\psi \circ \varphi)_{f \circ g}^*(x_\alpha^*) &= f_\alpha(g_\beta(t_i^*)) \\
 &= f_\alpha(\psi_g^*(y_\beta^*)) \\
 &= \psi_g^*(f_\alpha(y_\beta^*)) \\
 &= \psi_g^*(\varphi_f^*(x_\alpha^*)) \\
 &= (\psi_g^* \circ \varphi_f^*)(x_\alpha^*)
 \end{aligned}$$

for all $\alpha \in M$.

2.11 Lemma. Let $\varphi: G \rightarrow H$ be an isomorphism of groups which have a set of generators X and Y respectively. Using the notation of Lemma 2.10, we further suppose that the homomorphism $\varphi: F(X) \rightarrow F(Y)$ defined by $\varphi(x_\alpha) = f_\alpha(y_\beta)$, for all α in M , induces an isomorphism of $F(X)/F(X)^m \cdot F(X)'$ onto $F(Y)/F(Y)^m \cdot F(Y)'$. Then the homomorphism φ_f^* is an isomorphism of $G_m^*(X^*)$ onto $H_m^*(Y^*)$.

PROOF.* Denote $G_m^*(X^*)$ and $H_m^*(Y^*)$ by G_m^* and H_m^* respectively. Now

$$(G_m^*)^m \cdot (G_m^*)' = G^m \cdot G' \quad \text{and} \quad (H_m^*)^m \cdot (H_m^*)' = H^m \cdot H'.$$

Also $G_m^*/(G_m^*)^m \cdot (G_m^*)' \cong F(X)/F(X)^m \cdot F(X)'$ and

$$H_m^*/(H_m^*)^m \cdot (H_m^*)' \cong F(Y)/F(Y)^m \cdot F(Y)'$$

under natural isomorphisms. Now

$$\varphi_f^*|_{(G_m^*)^m \cdot (G_m^*)'} = \varphi|_{G^m \cdot G'}$$

which gives an isomorphism onto $H^m \cdot H'$. Also φ_f^* induces an isomorphism of

$$G_m^*/(G_m^*)^m \cdot (G_m^*)' \quad \text{onto} \quad H_m^*/(H_m^*)^m \cdot (H_m^*)'.$$

Hence φ_f^* is an isomorphism onto.

2.12 Lemma. Let $X = X_1 \cup Y$ be a set of generators of a group G such that

$$X_1 \cap Y = \emptyset \quad \text{and} \quad Y \subseteq G^m \cdot G'.$$

Further let H be the subgroup $\langle w, y^*; w \in X_1, y \in Y \rangle$ in $\bar{G}_m(X)$. Then

$$H = G \times (|Y|(Z_m)) \quad \text{and} \quad H_m^*((X_1 \cup Y^*)^*) \cong G_m^*(X^*).$$

Further if X is a finite set and X_1 is a minimal set of generators for G modulo $G^m \cdot G'$, then $X_1 \cup Y^*$ is a minimal set of generators for the group H .

PROOF. (i) We have that for every $y \in Y$

$$y = x_{\alpha_1}^{n_1} \dots x_{\alpha_k}^{n_k} \cdot u(x),$$

*) I am grateful to Dr. V. AGHOOBZADEH for drawing my attention to the fact that my original proof was not convincing.

where every x_{α_i} belongs to X , every n_i is divisible by m and $u(x)$ belongs to G' . Let

$$\bar{x} = \begin{cases} x & \text{if } x \text{ belongs to } X_1 \\ x^* & \text{if } x \text{ belongs to } Y \end{cases}$$

for all x in X . Then the product of the elements

$$y^* \quad \text{and} \quad (\bar{x}_{\alpha_1}^{n_1} \dots \bar{x}_{\alpha_k}^{n_k} \cdot u(\bar{x}))^{-1}$$

of H is z_y , which thus also belongs to H , for all y in Y . Hence

$$H \supseteq G \times (|Y|(Z_m))$$

which gives the required equality, since the reverse inclusion obviously holds.

(ii) The mapping $\varphi: H \rightarrow G$ defined by

$$\varphi(\bar{x}) = x \quad \text{for all } x \text{ in } X$$

is a homomorphism onto G with kernel $|Y|(Z_m)$. By Lemma 2.10, we have the corresponding homomorphism

$$\varphi^*: H_m^*(\bar{X}^*) \rightarrow G_m^*(X^*),$$

where $\bar{X} = \{\bar{x}; x \in X\}$ and $\varphi^*(\bar{x}^*) = x^*$ for all $\bar{x}^*$ in $\bar{X}^*$. φ^* is clearly surjective. Suppose that

$$\varphi^*(\bar{x}_{\alpha_1}^{*n_1} \dots \bar{x}_{\alpha_k}^{*n_k} \cdot u(\bar{x}^*)) = 1,$$

where every $\bar{x}_{\alpha_i}^*$ belongs to $\bar{X}^*$, every n_i is an integer and $u(\bar{x}^*)$ belongs to $H_m^*(\bar{X}^*)'$. Then

$$x_{\alpha_1}^{*n_1} \dots x_{\alpha_k}^{*n_k} \cdot u(x^*) = 1 \quad \text{in } G_m^*(X^*).$$

Hence, by Lemma 2.7,

$$x_{\alpha_1}^{n_1} \dots x_{\alpha_k}^{n_k} \cdot u(x) = 1 \quad \text{in } G$$

and every n_i is divisible by m . Hence

$$\bar{x}_{\alpha_1}^{n_1} \dots \bar{x}_{\alpha_k}^{n_k} \cdot u(x) = 1 \quad \text{in } H$$

and, by Lemma 2.7,

$$\bar{x}_{\alpha_1}^{*n_1} \dots \bar{x}_{\alpha_k}^{*n_k} \cdot u(\bar{x}^*) = 1 \quad \text{in } H_m^*(\bar{X}^*).$$

So φ^* is also injective.

(iii) No proper subset of $X_1 \cup Y$ is a set of generators for H . For otherwise either a proper subset of X_1 is a set of generators for G modulo $G^m \cdot G'$ or $|Y|(Z_m)$ has a set of generators with less than $|Y|$ elements. Both of these assertions contradict our assumptions. If T is a set of generators for H , then T is a set of generators for H modulo $H^m \cdot H'$. Now

$$H/H^m \cdot H' \cong (G/G^m \cdot G') \times (|Y|(Z_m)).$$

Hence $|T| \geq |X|$.

2.12.1 *Note.* A proof similar to Proof (ii) above shows that if $X = X_1 \cup Y$ is a set of generators for G and $X_1 \cap Y = \emptyset$, then

$$G_m^*(X^*) \cong H_m^*((X_1 \cup Y^*)^*).$$

2.13 Theorem. *Let G be a finitely generated group and X and Y be finite sets of generators of G . Then*

$$G_m^*(X^*) \cong G_m^*(Y^*)$$

if and only if $|X| = |Y|$.

PROOF. Suppose that $G_m^*(X^*) \cong G_m^*(Y^*)$. Then, by Lemma 1.3, the set X^* and the image of the set Y^* under the above isomorphism are minimal sets of generators of $G_m^*(X^*)$. Hence $|X^*| = |Y^*|$, which gives that $|X| = |Y|$.

Conversely suppose now that $|X| = |Y|$. By Lemma 2.5, and Corollary 2.7.1 we may assume that m is of the form p^λ . We are given that

$$G \cong F(X)/R(X) \cong F(Y)/R(Y),$$

where $F(X)$ and $F(Y)$ are free groups on sets of free generators X and Y respectively. Let

$$F(X)^{p^\lambda} \cdot F(X)' \cdot R(X) = K(X) \quad \text{and} \quad F(Y)^{p^\lambda} \cdot F(Y)' \cdot R(Y) = K(Y).$$

By W. MAGNUS, A. KARRASS, D. SOLITAR [12] Theorem 3.5 (p. 140), Theorem 3.2 (p. 131) and Lemma 3.2 (p. 133), one can pass from a set X to another set A of free generators for $F(X) = F(A)$ by applying a finite number of elementary Nielsen transformations so that the following situation holds.

$$G/G^{p^\lambda} \cdot G' \cong F(A)/K(A)$$

and $\{a_i^{d_i} \cdot q_i(a); \text{ with } i=1, 2, \dots, k\}$ forms a set of generators for $K(A)$, where $q_i(a)$ belongs to $F(A)'$ for every i . Also $k \equiv |X|$ and there exists an integer k' with $1 \leq k' \leq k$ such that $d_i = 0$ for every $i > k'$ while $d_i \equiv 1$ for every $i \leq k'$. Here every d_i is a non-negative integer and d_i divides d_{i+1} with each of them being a power of p , for $i=1, 2, \dots, k'-1$. There is an exactly similar situation holding for Y, B , and $F(Y) = F(B)$ with the same k, k' and d_i .

Since every elementary Nielsen transformation is invertible, one has, by Lemma 2.11, that

$$G_{p^\lambda}^*(X^*) \cong G_{p^\lambda}^*(A^*) \quad \text{and} \quad G_{p^\lambda}^*(Y^*) \cong G_{p^\lambda}^*(B^*).$$

So we now proceed to show that

$$G_{p^\lambda}^*(A^*) \cong G_{p^\lambda}^*(B^*).$$

By Lemma 2.12, we may assume that A and B are minimal sets of generators of G and

$$k' = |A| = |B| \quad \text{and every } d_i \neq 1.$$

So we may assume that

$$(2.13.1) \quad K(A) \subseteq F(A)^p \cdot F(A)' \quad \text{and} \quad K(B) \subseteq F(B)^p \cdot F(B)'.$$

We know, since B is a set of generators for G , that

$$(2.13.2) \quad a_i = b_1^{\beta_{11}} \dots b_j^{\beta_{1j}} \dots b_k^{\beta_{1k}} \cdot v_i(b) \quad \text{in } G,$$

where $v_i(b)$ belongs to $G^{p^\lambda} \cdot G'$ for $i=1, 2, \dots, k'$. Here every β_{ij} is an integer such that

$$0 \leq \beta_{ij} < d_j \leq p^\lambda.$$

The equations (2.13.2) can be considered to define a homomorphism

$$\Theta : F(A) \rightarrow F(B)$$

by taking $\Theta(a_i)$ to be equal to the right hand side of (2.13.2) for every i . This induces a homomorphism

$$\bar{\Theta} : F(A)/F(A)^{p^\lambda} \cdot F(A)' \rightarrow F(B)/F(B)^{p^\lambda} \cdot F(B)'.$$

By Lemma 2.11, it remains to show that $\bar{\Theta}$ is surjective. Suppose that contrary to assertion we have that $\bar{\Theta}$ is not surjective. Then $\bar{\Theta}$ induces a homomorphism

$$F(A)/F(A)^p \cdot F(A)' \rightarrow F(B)/F(B)^p \cdot F(B)'$$

which is not surjective. Hence, by (2.13.1), we have that the equations (2.13.2) induce both a surjective and a non-surjective endomorphism of $G/G^p \cdot G'$. This contradiction establishes the fact that $\bar{\Theta}$ is surjective.

2.14 Definition. The kernel of the natural projection of $G_m^*(X^*)$ onto G (it is denoted by A in Note 2.4) will from now on be denoted by $\pi_m(G, X)$ and will also be called *m-th fundamental group of G with respect to X* . The group $G_m^*(X^*)$ is called *m-smooth covering group** of G with respect to X . If X is a finite minimal set of generators for G , then $G_m^*(X^*)$ is denoted by G_m^* and called *m-smooth covering group of G* . If $m=p$, then we do not require X to be finite.

2.15 Theorem. Let $\varphi : G \rightarrow H$ be a homomorphism of groups and X and Y be sets of generators of G and H respectively. Suppose that

$$\varphi(x_\alpha) = f_\alpha(y_\beta) \quad \text{for all } \alpha \in M.$$

Then φ_f^* induces a homomorphism of $\pi_m(G, X)$ into $\pi_m(H, Y)$.

PROOF. We have the following diagram:

$$\begin{array}{ccccccc} 1 & \rightarrow & \pi_m(G, X) & \xrightarrow{\delta} & G_m^*(X^*) & \xrightarrow{\gamma} & G \rightarrow 1 \\ & & & & \downarrow \varphi_f^* & & \downarrow \varphi \\ 1 & \rightarrow & \pi_m(H, Y) & \xrightarrow{\theta} & H_m^*(Y^*) & \xrightarrow{\psi} & H \rightarrow 1. \end{array}$$

Its rows are exact, by definition, and the square is commutative. For

$$\psi \varphi_f^*(x_\alpha^*) = \varphi \gamma(x_\alpha^*) = f_\alpha(y_\beta).$$

*) See Definition 2.1 and Corollary 2.7.1.

Let x^* belong to $\pi_m(G, X)$. Then

$$\psi\varphi_f^*\delta(x^*) = \varphi_f\delta(x^*) = 1.$$

So there exists y^* in $\pi_m(H, Y)$ so that

$$\Theta(y^*) = \varphi_f^*(\delta(x^*)).$$

We define

$$\varphi_f^*|_\pi : \pi_m(G, X) \rightarrow \pi_m(H, Y)$$

by $x^* \rightarrow y^*$.

(i) The mapping $\varphi_f^*|_\pi$ is single-valued. For suppose that

$$\Theta(y_1^*) = \Theta(y_2^*) = \varphi_f^*(\delta(x^*)) \quad \text{for } y_1^*, y_2^* \in \pi_m(H, Y).$$

Then $y_1^* = y_2^*$, since Θ is an isomorphism into.

(ii) The mapping $\varphi_f^*|_\pi$ preserves the group operation. For if for $i=1, 2$,

$$\Theta(y_i^*) = \varphi_f^*(\delta(x_i^*)),$$

then

$$\varphi_f^*(\delta(x_1^* \cdot x_2^*)) = \varphi_f^*(\delta(x_1^*)) \cdot \varphi_f^*(\delta(x_2^*)) = \Theta(y_1^*) \cdot \Theta(y_2^*) = \Theta(y_1^* \cdot y_2^*),$$

since Θ , φ_f^* and δ are homomorphisms.

2.15.1 Corollary*). Let $|X|=|Y|<\infty$ and φ be an isomorphism onto. Then φ_f^* induces an isomorphism of $\pi_m(G, X)$ onto $\pi_m(H, Y)$.

2.16 Notation. If G has a minimal set X of generators and $|X|$ is finite or $m=p$, then we denote $\pi_m(G, X)$ by $\pi_m(G)$.

2.16.1 Note. Theorem 2.8 asserts that

$$G_p^* \cong G \times \pi_p(G).$$

2.17 Theorem. Let G_α , $\alpha \in M$, be a collection of groups with X_α being a set of generators for G_α for every $\alpha \in M$. Then

$$\pi_m\left(\prod_{\alpha}^{VV} G_{\alpha}, \bigcup_{\alpha} X_{\alpha}\right) \cong \prod_{\alpha}^{\times} \pi_m(G_{\alpha}, X_{\alpha}),$$

where $\prod_{\alpha}^{VV} G_{\alpha}$ denotes a neutral VV -product as defined in O. N. GOLOVIN [3].

PROOF. Let $J = \prod_{\alpha}^* G_{\alpha}$, while $F_{\alpha} = F(X_{\alpha})$, for every $\alpha \in M$, and $F = F(\bigcup_{\alpha} X_{\alpha})$ be the corresponding free groups. Then

$$\prod_{\alpha}^{VV} G_{\alpha} = J/VV(J) \quad \text{and} \quad G_{\alpha} \cong F_{\alpha}/R_{\alpha}$$

for every $\alpha \in M$. By [3] Theorem 2,

$$\prod_{\alpha}^{VV} G_{\alpha} \cong F / \left(\prod_{\alpha} R_{\alpha}^F \cdot VV(F) \right) = F / \left(\prod_{\alpha} R_{\alpha} \cdot \prod_{\alpha \neq \beta} (R_{\alpha}, F_{\beta})^F \cdot VV(F) \right).$$

*) One also has to use Theorem 2.13.

Now

$$\left(\prod_{\alpha} R_{\alpha} \cdot \prod_{\alpha \neq \beta} (R_{\alpha}, F_{\beta})^F \cdot VV(F) \right) \cap (F^m \cdot F') = \prod_{\alpha} (R_{\alpha} \cap F_{\alpha}^m \cdot F'_{\alpha}) \cdot \prod_{\alpha \neq \beta} (R_{\alpha}, F_{\beta})^F \cdot VV(F),$$

since

$$F^m \cdot F' = \prod_{\alpha} F_{\alpha}^m \cdot F'_{\alpha} \cdot (F_{\alpha})^F.$$

So

$$\pi_m \left(\prod_{\alpha}^{VV} G_{\alpha}, \bigcup_{\alpha} X_{\alpha} \right) \cong \prod_{\alpha}^{\times} (R_{\alpha} / (R_{\alpha} \cap F_{\alpha}^m \cdot F'_{\alpha})) \cong \prod_{\alpha}^{\times} \pi_m(G_{\alpha}, X_{\alpha}).$$

2.17.1 Corollary. *If $\prod_{\alpha}^V G_{\alpha}$ denotes the V -product as defined in S. MORAN [13], then*

$$\pi_m \left(\prod_{\alpha}^V G_{\alpha}, \bigcup_{\alpha} X_{\alpha} \right) \cong \prod_{\alpha}^{\times} \pi_m(G_{\alpha}, X_{\alpha}).$$

$$\text{2.17.1.1 Corollary. } \pi_m \left(\prod_{\alpha}^{\times} G_{\alpha}, \bigcup_{\alpha} X_{\alpha} \right) \cong \prod_{\alpha}^{\times} \pi_m(G_{\alpha}, X_{\alpha}).$$

$$\text{2.17.1.2 Corollary. } \pi_m \left(\prod_{\alpha}^* G_{\alpha}, \bigcup_{\alpha} X_{\alpha} \right) \cong \prod_{\alpha}^{\times} \pi_m(G_{\alpha}, X_{\alpha}).$$

2.17.1.3 Corollary. *Let $G_1, G_2, \dots, G_n$ be finitely generated groups. Then*

$$\pi_m \left(\prod_{i=1}^n G_i \right) \cong \prod_i^{\times} \pi_m(G_i).$$

This is a consequence of Gruško's Theorem (see for instance W. MAGNUS, A. KARRASS, D. SOLITAR [12], p. 192).

2.18 Example. The homomorphism φ_f^* in Lemma 2.10 and Theorem 2.15 depends in general not only on the homomorphism φ but also on the words f_{α} . For let G and H be cyclic groups of order p^4 and p^2 which are generated by the elements x and y respectively. Define

$$\varphi_1: G \rightarrow H \quad \text{and} \quad \varphi_2: G \rightarrow H$$

by $\varphi_1(x) = y^p$ and $\varphi_2(x) = y^{p^2+p}$ respectively. Then

$$\varphi_1 = \varphi_2.$$

We now have that

$$\varphi_i^*: G_{p^8}^*(\{x^*\}) \rightarrow H_{p^8}^*(\{y^*\}) \quad \text{for } i = 1, 2,$$

is defined by

$$\varphi_1^*(x^*) = y^{*p} \quad \text{and} \quad \varphi_2^*(x^*) = y^{*p^2+p}.$$

So

$$\varphi_1^* \neq \varphi_2^*.$$

Also they give different homomorphisms of $\pi_{p^8}(G, \{x\})$ into $\pi_{p^8}(H, \{y\})$. For

$$\varphi_1^*(x^{*p^4}) = y^{*p^5} \quad \text{and} \quad \varphi_2^*(x^{*p^4}) = y^{*p^6+p^5}.$$

These elements are not equal in $\pi_{p^8}(H, \{y\})$, since

$$\pi_{p^8}(G, \{x\}) = \langle x^{*p^4} \rangle \cong Z_{p^4}$$

while

$$\pi_{p^8}(H, \{y\}) = \langle y^{*p^2} \rangle \cong Z_{p^0}.$$

2.19 *Example.* Theorem 2.13 does not hold in general for infinite sets of generators X and Y . For let

$$X = \{x_1, x_2, \dots, x_i, \dots\} \quad \text{and} \quad Y = \{x_2, \dots, x_i, \dots\}.$$

Then the free group $G = \langle x_1, x_2, \dots, x_i, \dots; x_1 = 1 \rangle$ also has Y as a set of generators. However the covering groups $G_m^*(X^*)$ and $G_m^*(Y^*)$ are not isomorphic, by Lemma 2.12.

References

- [1] W. GASCHÜTZ and M. F. NEWMAN, On presentations of finite p -groups. *J. Reine Angew. Math.* **245** (1970), 172—176.
- [2] E. S. GOLOD and I. R. ŠAFAREVIČ, On towers of class fields, *Izv. Akad. Nauk SSSR Ser. Mat.* **28** (1964), 261—272.
- [3] O. N. GOLOVIN, Polyidentical relations in groups and operations defined by them on the class of all groups, *Trudy Moscow Math. Soc.* **12** (1963), 413—435.
- [4] M. HALL, The theory of groups, *New York* 1959.
- [5] P. HALL, A contribution to the theory of groups of prime power order, *Proc. London Math. Soc.* **36** (1933), 29—95.
- [6] B. HUPPERT, Endliche Gruppen I, *Berlin* 1967.
- [7] N. JACOBSON, Lie algebras, *New York* 1962.
- [8] S. A. JENNINGS, The structure of the group ring of a p -group over a modular field, *Trans. Amer. Math. Soc.* **50** (1951), 175—185.
- [9] H. KOCH, Galois'sche Theorie der p -Erweiterungen, *Berlin* 1970.
- [10] A. I. KOSTRIKIN, On presenting groups by generators and defining relations, *Izv. Akad. Nauk. SSSR Ser. Mat.* **29** (1965), 1119—1122.
- [11] M. LAZARD, Sur les groupes nilpotents et les anneaux de Lie, *Ann. Sci. École Norm. Sup. (3)* **71** (1954), 101—190.
- [12] W. MAGNUS, A. KARRASS, D. SOLITAR, Combinatorial group theory, *New York* 1966.
- [13] S. MORAN, Associative operations on groups I, *Proc. London Math. Soc. (3)* **6** (1956), 581—596.
- [14] E. B. VINBERG, On the theorem concerning the infiniteness of an associative algebra, *Izv. Akad. Nauk SSSR* **29** (1965), 209—214.
- [15] H. ZASSENHAUS, The theory of groups, *New York* 1959.

THE UNIVERSITY,
CANTERBURY,
KENT.

(Received January 18, 1977.)