

Wir haben oben bereits festgestellt, daß bei dem Polynom $f(x)=2x^2-1$ die singulären Punkte im Intervall $[-1, 1]$ dicht liegen. Für die Funktion $g(x, y)=4y-4(1-x^2)^2$ ist

$$g_y(x, y) = 4,$$

d. h. die Gleichung (15) erfüllt die Voraussetzungen unseres Eindeutigkeitssatzes. Wie man leicht bestätigt, ist $\varphi(x)=1-x^2$ eine stetige Lösung der Gleichung (15), und nach dem Eindeutigkeitssatz ist dies auch die einzige. Hieraus ergibt sich nun, daß $\varphi(\cos t)=\sin^2 t$ die einzige stetige Lösung der Gleichung (14) ist.

Literatur

- [1] B. BARNA, Über die Iteration reeller Funktionen I, II, III. *Publ. Math. (Debrecen)* **7**, (1960) 16—40; **13**, (1966), 169—172; **22** (1975), 269—278.
- [2] E. JACOBSTHAL, Über vertauschbare Polynome, *Math. Z.* **63**, (1955), 243—276.
- [3] M. KUCZMA, Functional equations in a single variable, *Warszawa*, 1968.
- [4] M. KRÜPPEL, Beiträge zur Theorie der vertauschbaren Funktionen, *Math. Nachr.* **56** (1973), 73—100.
- [5] — — Über nichtmonotone, vertauschbare Funktionen, (In Vorbereitung)
- [6] — — Über die Verteilung der singulären Punkte bei Polynomen, *Wiss. Zeitschr. der PH Güstrow, Jahrgang 1977, Heft 1*.

(Eingegangen am 30. Juli 1976.)

Covering groups and presentations of finite groups II.

By SIEGFRIED MORAN (Canterbury)

§ 3. Presentations of Finite Groups

3.1 Notation. By $\mathbf{Z}_p(y_\gamma; \gamma \in \Gamma)$ we denote the free associative algebra with unit element on set of free generators $y_\gamma, \gamma \in \Gamma$, over the field $\mathbf{Z}_p$. If we are working with a specific algebra, then $\mathcal{J}(\quad)$ will denote the ideal generated by the elements exhibited within the brackets in this algebra.

3.2 Lemma. Let p be a fixed prime number and, for every $\gamma \in \Gamma$, let $\langle x_\gamma \rangle$ be a cyclic group of order p^{x_γ} . Then there exists an algebra isomorphism $\bar{\varphi}$ between the algebra

$$\mathbf{Z}_p(y_\gamma; \gamma \in \Gamma) / \mathcal{J}(y_\gamma^{p^{x_\gamma}}; \gamma \in \Gamma)$$

and the group algebra $\mathbf{Z}_p(\prod_{\gamma}^* \langle x_\gamma \rangle)$ which is defined by

$$\bar{\varphi}(y_\gamma + \mathcal{J}(y_\gamma^{p^{x_\gamma}}; \gamma \in \Gamma)) = x_\gamma - 1$$

for all γ in Γ .

PROOF. It is well known that there exists a natural isomorphism

$$\mathbf{Z}_p(\prod_{\gamma}^* \langle x_\gamma \rangle) \cong \mathbf{Z}_p(F(X)) / \mathcal{J}(x_\gamma^{p^{x_\gamma}} - 1; \gamma \in \Gamma),$$

where $F(X)$ is the free group on the set of symbols $X = \{x_\gamma, \gamma \in \Gamma\}$. Further it is well known (see for instance M. LAZARD [11]) *) that the mapping

$$\varphi(y_\gamma) = x_\gamma - 1, \quad \text{for all } \gamma \text{ in } \Gamma,$$

induces an algebra isomorphism φ of $\mathbf{Z}_p(y_\gamma; \gamma \in \Gamma)$ into $\mathbf{Z}_p(F(X))$. Now

$$\varphi(y_\gamma^{p^{x_\gamma}}) = (x_\gamma - 1)^{p^{x_\gamma}} = x_\gamma^{p^{x_\gamma}} - 1.$$

So φ induces an algebra homomorphism

$$\bar{\varphi}: \mathbf{Z}_p(y_\gamma; \gamma \in \Gamma) / \mathcal{J}(y_\gamma^{p^{x_\gamma}}; \gamma \in \Gamma) \rightarrow \mathbf{Z}_p(F(X)) / \mathcal{J}(x_\gamma^{p^{x_\gamma}} - 1; \gamma \in \Gamma).$$

Suppose that

$$\bar{\varphi}(f(y_\gamma) + \mathcal{J}(y_\gamma^{p^{x_\gamma}}; \gamma \in \Gamma)) = \mathcal{J}(x_\gamma^{p^{x_\gamma}} - 1; \gamma \in \Gamma),$$

*) See References in I.

where $f(y_\gamma)$ belongs to $\mathbf{Z}_p(y_\gamma; \gamma \in \Gamma)$. We now show that

$$f(y_\gamma) \text{ belongs to } \mathcal{J}(y_\gamma^{p^{\alpha_\gamma}}; \gamma \in \Gamma).$$

Let $\mathfrak{M}$ denote the Magnus completion of $\mathbf{Z}_p(y_\gamma; \gamma \in \Gamma)$, that is, the algebra of all formal power series in the non-commuting variables $y_\gamma, \gamma \in \Gamma$, with coefficients in $\mathbf{Z}_p$ (see for instance M. Lazard [11]). Then it is well known (and follows easily from the isomorphic embedding of $F(X)$ in $\mathfrak{M}$ due to W. Magnus) that the mapping

$$\psi: \mathbf{Z}_p(F(X)) \rightarrow \mathfrak{M}$$

defined by

$$\psi(x_\gamma) = 1 + y_\gamma \quad \text{and} \quad \psi(x_\gamma^{-1}) = \sum_{k=0}^{\infty} (-1)^k y_\gamma^k,$$

for every γ in Γ , is an algebra isomorphism into. Hence we know that

$$\psi(f(x_\gamma - 1)) \text{ belongs to } \psi(\mathcal{J}(x_\gamma^{p^{\alpha_\gamma}} - 1; \gamma \in \Gamma)).$$

This gives that $f(y_\gamma)$ belongs to the topological closure of $\mathcal{J}(y_\gamma^{p^{\alpha_\gamma}}; \gamma \in \Gamma)$ in $\mathfrak{M}$, where we consider $\mathbf{Z}_p(y_\gamma; \gamma \in \Gamma)$ to be a subset of $\mathfrak{M}$. Hence

$$f(y_\gamma) \text{ belongs to } \mathcal{J}(y_\gamma^{p^{\alpha_\gamma}}; \gamma \in \Gamma)$$

in $\mathbf{Z}_p(y_\gamma; \gamma \in \Gamma)$, since $\mathcal{J}(y_\gamma^{p^{\alpha_\gamma}}; \gamma \in \Gamma)$ is closed in $\mathbf{Z}_p(y_\gamma; \gamma \in \Gamma)$. So the mapping $\bar{\varphi}$ is injective.

In order to show that $\bar{\varphi}$ is surjective we need to find an inverse image of $x_\gamma^{-1} + \mathcal{J}(x_\gamma^{p^{\alpha_\gamma}} - 1; \gamma \in \Gamma)$ under $\bar{\varphi}$. We have that

$$\begin{aligned} \bar{\varphi} \left(\sum_{j=0}^{p^{\alpha_\gamma}-1} (-1)^j y_\gamma^j + \mathcal{J}(y_\gamma^{p^{\alpha_\gamma}}; \gamma \in \Gamma) \right) &= \sum_{j=0}^{p^{\alpha_\gamma}-1} (-1)^j (x_\gamma - 1)^j + \mathcal{J}(x_\gamma^{p^{\alpha_\gamma}} - 1; \gamma \in \Gamma) = \\ &= x_\gamma^{-1} + (-1)^{p^{\alpha_\gamma}+1} x_\gamma^{-1} (x_\gamma - 1)^{p^{\alpha_\gamma}} + \mathcal{J}(x_\gamma^{p^{\alpha_\gamma}} - 1; \gamma \in \Gamma) = x_\gamma^{-1} + \mathcal{J}(x_\gamma^{p^{\alpha_\gamma}} - 1; \gamma \in \Gamma). \end{aligned}$$

3.3 Lemma. *If, in the notation of Lemma 3.2, we let Δ denote the augmentation ideal of $\mathbf{Z}_p(\prod_{\gamma}^* \langle x_\gamma \rangle)$, then $\bar{\varphi}^{-1}$ maps Δ^k onto*

$$\mathbf{Z}_p^k(y_\gamma; \gamma \in \Gamma) + \mathcal{J}(y_\gamma^{p^{\alpha_\gamma}}; \gamma \in \Gamma) / \mathcal{J}(y_\gamma^{p^{\alpha_\gamma}}; \gamma \in \Gamma),$$

where $\mathbf{Z}_p^k(y_\gamma; \gamma \in \Gamma)$ is the ideal of $\mathbf{Z}_p(y_\gamma; \gamma \in \Gamma)$ which consists of all associative polynomials whose homogeneous components of degree less than k are equal to zero. This is so for $k=1, 2, \dots$.

PROOF. It is easy to see that Δ^k is generated as an ideal in $\mathbf{Z}_p(\prod_{\gamma}^* \langle x_\gamma \rangle)$ by all elements of the form

$$\prod_{j=1}^k (g_j - 1),$$

where every g_j belongs to $\prod_{\gamma}^* \langle x_\gamma \rangle$. Now on using the fact that

$$ab - 1 = (a-1)(b-1) + (a-1) + (b-1)$$

and

$$x_\gamma^{-1} - 1 = \sum_{j=1}^{p^{x_\gamma}-1} (-1)^j (x_\gamma - 1)^j$$

in $\mathbf{Z}_p(\Pi^* \langle x_\gamma \rangle)$, one obtains that $\bar{\varphi}^{-1}|_{\Delta^k}$ is the required mapping into. The fact that it is onto follows from the assertion that if $f_k(y_\gamma)$ belongs to $\mathbf{Z}_p^k(y_\gamma; \gamma \in \Gamma)$, then

$$\bar{\varphi}^{-1}(f_k(x_\gamma - 1)) = f_k(y_\gamma) + \mathcal{J}(y_\gamma^{p^{x_\gamma}}; \gamma \in \Gamma)$$

and $f_k(x_\gamma - 1)$ belongs to Δ^k .

3.4 Remark. Let G be an arbitrary group and $\Delta(G)$ be the augmentation ideal of the group algebra $\mathbf{Z}_p(G)$. Then the normal subgroup

$$G \cap (1 + \Delta^k(G))$$

is denoted by $D_{k,p}(G)$ and is called k -th dimension subgroup of G modulo p . It is known (see S. A. JENNINGS [8] and M. LAZARD [11]) that

$$D_{k,p}(G) = G_{k,p},$$

where $G_{k,p} = \langle ({}^jG)^{p^h}; j p^h \equiv k \rangle$, for $k=1, 2, \dots$, and jG denotes j -th member of lower central series of G .

3.5 Theorem. Let the group G have a p^λ -smooth presentation on $X = \{x_1, \dots, x_d\}$ with a set of defining relations R and $d \geq 2$. Suppose that $x_i^{p^{z_i}}$ belongs to R , where α_i is an integer $\geq \lambda (\geq 1)$, for $i=1, 2, \dots, d$. Let

$$R = \bigcup_{i=1}^d \{x_i^{p^{z_i}}\} \cup R^*$$

be a partition of R . Let $F(X)$ be the free group on the set of symbols X and

$$\mathcal{J} = \prod_{i=1}^d \langle x_i; x_i^{p^{z_i}} \rangle$$

with θ being the natural homomorphism of $F(X)$ onto $\mathcal{J}$. Suppose that, for each integer k , we take r_k to be the number of elements of $\theta(R^*)$ which belong to $\mathcal{J}_{k,p}$ but not to $\mathcal{J}_{k+1,p}$ plus the number of x_i with the property that $p^{z_i} = k$. If G is a finite group, then the power series

$$\varphi(t) = 1 - dt + \sum_{k=2}^{\infty} r_k t^k > 0$$

for $0 < t < 1$.

PROOF. The natural homomorphism

$$\theta: F(X) \rightarrow \mathcal{J}$$

extends in a natural way to a surjective algebra homomorphism

$$\theta: \mathbf{Z}_p(F(X)) \rightarrow \mathbf{Z}_p(\mathcal{J})$$

with $\ker \theta = \mathcal{J}(x_i^{p^{\alpha_i}} - 1; i=1, 2, \dots, d)$. Now

$$\begin{aligned} \mathbf{Z}_p(G) &\cong \mathbf{Z}_p(F(X))/\mathcal{J}(R-1) \\ &\cong (\mathbf{Z}_p(F(X))/\mathcal{J}(x_i^{p^{\alpha_i}} - 1; 1 \leq i \leq d))/(\mathcal{J}(R-1)/\mathcal{J}(x_i^{p^{\alpha_i}} - 1)) \\ &\cong \mathbf{Z}_p(\mathcal{J})/\mathcal{J}(\theta(R^*)-1) \\ &\cong (\mathbf{Z}_p(y_i; 1 \leq i \leq d)/\mathcal{J}(y_i^{p^{\alpha_i}}; 1 \leq i \leq d))/\bar{\varphi}^{-1}(\mathcal{J}(\theta(R^*)-1)), \end{aligned}$$

where $\bar{\varphi}$ is the algebra isomorphism given by Lemma 3.2. Hence, by Lemma 3.3 and Remark 3.4, we have that

$$\mathbf{Z}_p(G) \cong \mathbf{Z}_p(y_i; 1 \leq i \leq d)/\mathcal{J}(S-1),$$

where $S-1$ is a subset of $\mathbf{Z}_p(y_1, \dots, y_d)$ with

$$|(S-1) \cap \mathbf{Z}_p^k(y_1, \dots, y_d)| = \sum_{i \equiv k} r_i$$

for $k=2, 3, \dots$. The required result now follows from the celebrated theorem of E. S. GOLOD and I. R. ŠAFAREVIČ [2] as refined by E. B. VINBERG [14] and H. KOCH [9], § 7.

3.6 Theorem. *Let a finite group G have a p^λ -smooth presentation ($\lambda \geq 1$) on set X of d generators and $r(k)+r(n)$ defining relations all of which belong to $F(X)_{k,p}$, while $r(n)$ of them belong to $F(X)_{n,p}$, where k and n are positive integers satisfying $1 < k \leq n$. We also assume that among the above defining relations are the relations $x_i^{p^{\alpha_i} \cdot \beta_i} = 1$ for all x_i in X , where every $p^{\alpha_i} \geq k$ and $\beta_i \geq 1$. Then*

$$r(n) > ((d/2)^k - r(k)) \cdot (d/2)^{n-k}.$$

PROOF. We consider the finite factor group of G which has the same generators and the same defining relations as G except that $x_i^{p^{\alpha_i} \cdot \beta_i} = 1$ is replaced by $x_i^{p^{\alpha_i}} = 1$ for every i . By Theorem 3.5,

$$0 < \varphi(t) \leq 1 - dt + r(k) \cdot t^k + r(n) \cdot t^n$$

for $0 < t < 1$. Suppose that contrary to the above assertion

$$r(n) \leq ((d/2)^k - r(k)) \cdot (d/2)^{n-k}.$$

Then $\varphi(t) \leq 1 - dt + (d/2)^n \cdot t^n + r(k) \cdot (t^k - (d/2)^{n-k} \cdot t^n)$. If $d \geq 3$, then $0 < \varphi(2/d) \leq 0$ and $0 < (2/d) < 1$. This contradiction establishes the theorem for $d \geq 3$. The case when $d=1$ is trivially true. The case when $d=2$ follows from the fact that the free product of two non-trivial groups is infinite.

3.6.1 Corollary. *If the above finite group G is such that $r(n)=d$, then*

$$r(k) > (d/2)^k - d \cdot (2/d)^{n-k}.$$

In particular

$$r(2) > (d^2/4) - d \cdot (2/d)^{n-2}.$$

3.6.2 Corollary. *If the above given finite group G is such that the defining relations*

$$(3.6.2.1) \quad x_1^{p^{\alpha_1} \cdot \beta_1} = 1, \dots, x_i^{p^{\alpha_i} \cdot \beta_i} = 1, \dots, x_d^{p^{\alpha_d} \cdot \beta_d} = 1$$

have the property that $p^{\alpha_i} \geq n \geq k$ for all i , then there are more than

$$(d/2)^k - d \cdot (2/d)^{n-k}$$

other defining relations taken from $F(X)_{k,p}$.

3.6.2.1 Corollary. *Suppose that one of the following conditions hold:*

- $p^\alpha = 4$ and d is even $\neq 4$,
- $p^\alpha \geq 5$ and d is even,
- $p^\alpha = 4$ and d is odd ≥ 17 ,
- $p^\alpha = 5$ and d is odd ≥ 7 ,
- $p^\alpha = 7$ and d is odd ≥ 5 ,
- $p^\alpha = 8$ and d is odd ≥ 5 ,
- $p^\alpha \geq 9$ and d is odd ≥ 3 , where $\alpha = \min \{\alpha_1, \alpha_2, \dots, \alpha_d\}$.

Then besides the relations (3.6.2.1) the above given finite group G has not less than $d^2/4$ other defining relations.

3.6.3 Corollary. *Suppose that the above given finite group G is such that all the $r(k) + r(n) - d$ defining relations, other than the relations (3.6.2.1), belong to $F(X)_{n,p}$. Then*

$$r(n) > (d/2)^n - d \cdot (d/2)^{n-k},$$

provided every $p^{\alpha_i} \geq k$ and taking $r(k) = d$.

3.7 Lemma. *Suppose that a finite group G has a p^λ -smooth presentation ($\lambda \geq 1$) on a set X of d generators with all the defining relations belonging to $F(X)_{k,p}$ and among them are the relations*

$$x_1^{p^{\alpha_1} \cdot \beta_1} = 1, \dots, x_i^{p^{\alpha_i} \cdot \beta_i} = 1, \dots, x_d^{p^{\alpha_d} \cdot \beta_d} = 1,$$

where $X = \{x_1, \dots, x_d\}$, every $p^{\alpha_i} \geq k \geq 2$ and every $\beta_i > 0$. Then there are more than

$$(d/k)^k \cdot (k-1)^{k-1} - d$$

other defining relations taken from $F(X)_{k,p}$.

PROOF. We consider the finite factor group of G , which has the same defining relations as G except that $x_i^{p^{\alpha_i} \cdot \beta_i} = 1$ is replaced by $x_i^{p^{\alpha_i}} = 1$ for every i . Now the required result follows at once from Theorem 3.5 and proof of Satz 7.21 of *H. Koch* [9].

3.8 Theorem. *Let λ be a positive integer. Then every finite group G has a presentation of the form*

$$\langle x_1, \dots, x_d; x_1^{p^\lambda \cdot \beta_1} = \dots = x_d^{p^\lambda \cdot \beta_d} = u_1 = \dots = u_s = y_1 = \dots = y_t = 1 \rangle,$$

where p is any fixed prime number, every $\beta_i > 0$, $X = \{x_1, x_2, \dots, x_d\}$, every u_i belongs to $F(X)^{p^\lambda} \cdot F(X)'$, no y_i belongs to $F(X)^{p^\lambda} \cdot F(X)'$ and $d \geq 2$. Furthermore in any such presentation

$$s > (d^2/4) - d \cdot (2/d)^{p^\lambda - 2}$$

and thus in particular *

$$s \geq d^2/4 \quad \text{for } p^\lambda \geq 9,$$

where p^λ is the largest power of p dividing every $p^\lambda \cdot \beta_i$. Here t denotes the minimal number of generators of the finite abelian group $\pi_{p^\lambda}(G, X)$. If every u_i is known to belong to $F(X)_{k,p}$, then

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

for $p^\lambda \geq k \geq 2$.

PROOF. We form the p^λ -smooth covering group $G_{p^\lambda}^*(X^*)$ of G with respect to X . Then, by Note 2.4 and Definition 2.14, we have that

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

where $\pi_{p^\lambda}(G, X)$ is a finite abelian group of exponent dividing p^λ . Now obviously $G_{p^\lambda}^*(X^*)$ has a presentation of the form

$$\langle x_1^*, \dots, x_d^*; x_1^{p^\lambda \cdot \beta_1} = \dots = x_d^{p^\lambda \cdot \beta_d} = u_1(x^*) = \dots = u_s(x^*) = 1 \rangle,$$

where $X = \{x_1, \dots, x_d\}$ is a set of generators of the group G . Also every $u_i(x^*)$ belongs to $F(X^*)^{p^\lambda} \cdot F(X^*)'$, where $X^* = \{x_1^*, \dots, x_d^*\}$. The required inequalities for s now follow from Corollary 3.6.2 and Lemma 3.7.

3.9 Lemma. *Suppose that a finitely generated group G has a presentation on a set X of d generators with a set R of defining relations. If for $k \geq 2$*

$$R \subseteq F(X)_{k,p}$$

and r_k denotes the number of elements of R which do not belong to $F(X)_{k+1,p}$, then

$$r_k \geq e_k(F(X)) - e_k(G),$$

where

$$e_k(G) = \dim_{\mathbb{Z}_p} (G_{k,p}/G_{k+1,p}),$$

for $k=2, 3, \dots$. It is always possible to go over to a presentation of the above type so that

$$r_k = e_k(F(X)) - e_k(G)$$

and the total number of defining relations remain unaltered.

*) For more detailed bounds on p so that $s \geq d^2/4$ holds, see Corollary 3.6.2.1.

PROOF. Let K be the normal subgroup generated by R in the free group $F(X) = F$. Then

$$G \cong F/K.$$

Hence

$$G_{k,p} \cong F(X)_{k,p}/K \quad \text{and} \quad G_{k+1,p} \cong F(X)_{k+1,p} \cdot K/K.$$

So

$$G_{k,p}/G_{k+1,p} \cong (F_{k,p}/F_{k+1,p})/(K.F_{k+1,p}/F_{k+1,p}).$$

Hence

$$r_k \cong e_k(F(X)) - e_k(G).$$

In order to go over to a presentation of the above type on X , in which the above inequality becomes equality, one can proceed as follows. First one takes a set R_k of elements of which form a basis for

$$K.F_{k+1,p} \text{ modulo } F_{k+1,p}.$$

Now it is straightforward to construct, by means of 'linear combinations', a set of elements $R_{k+1} \subseteq F_{k+1,p}$ so that

$$|R_k \cup R_{k+1}| = |R_k| + |R_{k+1}| = |R|$$

and $R_k \cup R_{k+1}$ is a set of defining relations for G .

3.10 Theorem. Suppose that a finite group G has a p^λ -smooth presentation (with $\lambda \geq 1$) on a set X of d generators with a set R of defining relations. If $x_i^{p^{\lambda_i} \beta_i}$ belongs to R for every x_i in X with every $\beta_i > 0$ and

$$R \subseteq F(X)_{k,p} \quad \text{with} \quad k \geq 2,$$

then

$$|R| > (d/2)^{k+1} - \left(\frac{1}{2}d - 1\right) \cdot (e_k(F(X)) - e_k(G)),$$

where

$$e_k(G) = \dim_{\mathbb{Z}_p}(G_{k,p}/G_{k+1,p}), \quad \text{for } k = 2, 3, \dots$$

PROOF. This follows at once from Lemma 3.9 and Theorem 3.6 with $n = k + 1$.

3.11 Note. It is easy to see that

$$e_2(F(X)) = (d^2/2) - (-1)^{p-1} \cdot (d/2).$$

§ 4. Presentations of finite p -groups

4.1 Note. Some of the results of § 3 are new even for finite p -groups. They can be improved, in a well known way, by considering presentations of a p -group as a factor group of a free pro- p -group $\overline{F(X)}$. Then it has presentations

$$\langle \overline{F(X)}; \overline{R} \rangle \text{ as a pro-} p\text{-group and } \langle F(X); R \rangle$$

with

$$\bar{r} = |\overline{R}| \leq |R| = r.$$

Adopting similar notation to that given in § 3, one can establish, in a similar way, the following results.

4.2 Theorem. *Let a finite p -group have a minimal set of d generators. Then*

$$\bar{r}(n) > ((d/2)^k - \bar{r}(k)) \cdot (d/2)^{n-k}$$

for $1 < k \leq n$.

4.2.1 Corollary. *If the finite p -group is such that $\bar{r}(n) = d$, then*

$$\bar{r}(k) > (d/2)^k - d \cdot (2/d)^{n-k}.$$

In particular

$$\bar{r}(2) > (d^2/4) - d \cdot (2/d)^{n-2}.$$

4.3 Theorem. *Suppose that a finite p -group has a minimal set of $d (\geq 2)$ generators and a presentation of the form*

$$\langle x_1, \dots, x_d; x_1^{p^{\alpha_1}} = \dots = x_d^{p^{\alpha_d}} = u_1 = \dots = u_{\bar{r}(k)} = 1 \rangle$$

as a pro- p -group, where every u_i belongs to $\overline{F(X)}_{k,p}$ with every $p^{\alpha_i} \geq k \geq 2$. Then

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

where $\alpha = \text{Min} \{ \alpha_1, \dots, \alpha_d \}$.

4.3.1 Corollary. $\bar{r}(2) \geq d^2/4$ for $p^{\alpha} \geq 9$ (see Corollary 3.6.2.1 for more details).

4.4 Theorem. *Suppose that the finite p -group G has a minimal set of d generators and a presentation as a pro- p -group of the form $\langle \overline{F(X)}; \bar{R} \rangle$, where $\bar{R}$ is a subset of $\overline{F(X)}_{k,p}$ and $k \geq 2$. Then*

$$|\bar{R}| \geq e_k(F(X)) - e_k(G)$$

and

$$|\bar{R}| > (d/2)^{k+1} - \left(\frac{1}{2}d - 1\right) \cdot (e_k(F(X)) - e_k(G)),$$

where

$$e_k(G) = \dim_{\mathbb{Z}_p} (G_{k,p}/G_{k+1,p}) \text{ for each } k \geq 2.$$

4.4.1 Note. The particular case when $k=2$ gives the inequalities of W. GASCHÜTZ and M. F. NEWMAN [1], since

$$e_2(F(X)) = (d^2/2) - (-1)^{p-1}(d/2).$$

§ 5. A numerical lemma and some examples

5.1 Lemma. *Let d and k be integers greater than 1. Then*

$$(d/k)^k \cdot (k-1)^{k-1} - d \geq (d/2)^k$$

when $k \geq 6$ or $k=4,5$ and $d \geq 3$ or $k=3$ and $d \geq 7$. For all other values of d and k the above inequality is false. Also

$$(2/k)^k \cdot (k-1)^{k-1} - 2 \geq \frac{1}{2}k - 3 + (2/k).$$

PROOF. The inequality holds if and only if

$$(5.1.1) \quad d \equiv \left[\frac{(k-1)^{k-1}}{k^k} - \frac{1}{2^k} \right]^{-1/(k-1)}.$$

Now

$$\left[\frac{(k-1)^{k-1}}{k^k} - \frac{1}{2^k} \right]^{-1/(k-1)} < \left[\frac{1}{ek} - \frac{1}{2^k} \right]^{-1/(k-1)} < 2 \cdot (2)^{1/(k-1)} < 3,$$

for $k \geq 5$, since $2^{k-1} > e \cdot k$ for $k \geq 5$. Hence the first inequality in Lemma holds when $k \geq 5$ and $d \geq 3$.

Now let $k=3$. Then from (5.1.1) it follows that

$$d \geq 6 \sqrt[6]{5} \quad \text{and so} \quad d \geq 7.$$

Now let $k=4$. Then from (5.1.1) it follows that

$$d \geq 4 \cdot (4/11)^{1/3} \quad \text{and so} \quad d \geq 3, \quad \text{since} \quad \frac{1}{2} < (4/11)^{1/3} < \frac{3}{4}.$$

Now

$$\begin{aligned} (2/k)^k \cdot (k-1)^k &= \left[1 + \left(1 - \frac{2}{k} \right) \right]^k \geq 1 + k - 2 + \frac{1}{2} k(k-1) \left(1 - \frac{4}{k} + \frac{4}{k^2} \right) = \\ &= 1 + k - 2 + \frac{1}{2} k^2 - \frac{1}{2} k - 2k + 2 + 2 - \frac{2}{k} = \frac{1}{2} k^2 - \frac{3}{2} k + 1 + \frac{2}{k} (k-1) = \\ &= \frac{1}{2} (k-1)(k-2) + \frac{2}{k} (k-1). \end{aligned}$$

One can check directly that $(2/k)^k \cdot (k-1)^{k-1} \geq 3$ for $6 \leq k \leq 7$ and it is false for $2 \leq k \leq 5$.

5.2 Example. The group

$$\langle x, y; x^{p^\lambda} = y^{p^\lambda} = (x, y) = 1 \rangle$$

is a finite p -group with its minimal set of generators consisting of two elements.

5.3 Example. The group

$$\langle x, y, z; x^{p^\lambda} = y^{p^\lambda} = z^{p^\lambda} = (x, y) = (x, z) = (y, z) = 1 \rangle$$

is a finite p -group with its minimal set of generators consisting of three elements.

5.4 Example. A. I. KOSTRIKIN [10] has constructed a finite p -group G of class two on generators

$$x_1, \dots, x_d, \quad \text{where} \quad d = 2^n$$

and n is any positive integer. It has defining relations

$$x_1^p = \dots = x_d^p = 1$$