ISRAEL JOURNAL OF MATHEMATICS 78 (1992), 65–73

ON PRO-p-GROUPS WITH A SINGLE DEFINING RELATOR

BY

NICOLAI S. ROMANOVSKII

Institute of Mathematics
Novosibirsk 630090
Russia

ABSTRACT

We find necessary and sufficient conditions for the factor groups of the derived series of a pro-p-group with a single defining relation to be torsion free. For such groups G we prove that the group algebra $\mathbb{Z}_pG$ is a domain and the cohomological dimension of G is at most 2.

1. Introduction

Let F be a free pro-p-group with a basis X, and let r be an element of F. Then a pro-p-group with a single defining relation $G = \langle X | r \rangle$ is the factor group F/r^F, where r^F is the closed normal subgroup of F generated by the element r. It is natural for pro-p-groups with a single defining relation to try to prove statements which are similar to the classical facts about abstract groups with a single defining relation. When r is not a p-th power of any element of F, Serre has asked whether the cohomological dimension $\operatorname{cd} G$ is less than or equal to 2 (see, for instance, Gildenhuys [1]). Gildenhuys has constructed a counter-example to this conjecture which shows also that the direct analog of the Magnus' Freiheitssatz does not hold for pro-p-groups. Nevertheless, it follows from Romanovskii [2] that there is some element $x \in X$ such that the elements from $X \setminus \{x\}$ freely generate, in G, a free pro-p-group. If we define an equivalence relation by $r \sim s$ if and only if $r^F = s^F$, it seems reasonable that one can improve Serre's conjecture to within this equivalence class.

Received December 2, 1990 and in revised form October 1, 1991

Everywhere in the sequel such terms as subgroups, factor groups and so forth will be regarded in the sense of topological groups. For a pro-p-group G, $G^{(n)}$ will denote the n-th commutator subgroup of G. A subset S of G is called a system of generators if S generates the pro-p-group G and every neighborhood of the unit of G contains almost all elements of S. A free system of generators of a free pro-p-group (or free abelian pro-p-group) is called a **basis** of this group. If a pro-p-group G is a projective limit of finite p-groups G_i, then a group algebra $\mathbb{Z}_pG$ over the ring of p-adic integers $\mathbb{Z}_p$, is defined as $\varprojlim \mathbb{Z}_p[G_i]$.

In this paper we shall prove the following.

THEOREM: *Let F be a free pro-p-group with a basis X, let r be an element of F and let $G = \langle X|r\rangle$ be a pro-p-group with a single defining relator. Let $r \in F^{(k)} \setminus F^{(k+1)}$ Then the factors of the derived series $G^{(n)}/G^{(n+1)}$ of the group G are torsion free if and only if the element r is not a p-th power of an element of $F^{(k)}$ modulo $F^{(k+1)}$, in which case the group algebra $\mathbb{Z}_pG$ is a domain and* $\operatorname{cd} G \leq 2$.

We note that the corresponding results about the lower central series of pro-p-groups with a single defining relator follow from Labute's article [3].

2. Profinite $\mathbb{Z}_p$-modules

If A is an abelian pro-p-group then one can define on A a structure of a topological $\mathbb{Z}_p$-module, which we will call a profinite $\mathbb{Z}_p$-module. So the class of profinite $\mathbb{Z}_p$-modules is closed under direct products and projective limits. The usual operation of tensor product does not apply in this class. Therefore it is natural to give the following:

Definition: Let A , B be two profinite $\mathbb{Z}_p$-modules. We represent them as projective limits of finite modules: $A = \varprojlim A_i$, $B = \varprojlim B_j$. Then the tensor product $A \otimes B$ is defined to be the module $\varprojlim A_i \otimes B_j$. ∎

The validity of this definition is verified by the usual arguments, as well as the following properties of the tensor product :

$$(1) \qquad A \otimes \mathbb{Z}_p \cong A, \quad \prod_k A_k \otimes \prod_l B_l \cong \prod_{k,l} (A_k \otimes B_l),$$
$$\varprojlim A_k \otimes \varprojlim B_l \cong \varprojlim A_k \otimes B_l.$$

Here $\prod$ means the direct product in the category of projective $\mathbb{Z}_p$-modules.

It is known that any profinite torsion free $\mathbb{Z}_p$-module is free, i.e. it has a basis – a free system of generators converging to zero. Let A, B be free modules with bases $\{a_i\}, \{b_j\}$ respectively. Then it follows from (1) that $A \otimes B$ is a free $\mathbb{Z}_p$-module with basis $\{a_i \otimes b_j\}$.

LEMMA 1: *Let A be a normal subgroup of a pro-p-group G and let $B = G/A$. Then the group algebra $\mathbb{Z}_pG$ is isomorphic, as $\mathbb{Z}_p$-module, to the tensor product $\mathbb{Z}_pB \otimes \mathbb{Z}_pA$.*

This statement follows easily from the fact that it is true for a finite p-group G.

3. Group algebras for some pro-p-groups

Let A be a free abelian pro-p-group with a countable basis $\{a_1, a_2, \ldots\}$. It follows from Lazard [4] that the group algebra $\mathbb{Z}_pA$ is the algebra of formal series of the form $u = \sum_M \gamma_M M$, where $\gamma_M \in \mathbb{Z}_p$ and M is a monomial of the form $(1-a_1)^{\alpha_1} \cdots (1-a_n)^{\alpha_n}$, $\alpha_i \in \{0, 1, 2, \ldots\}$. As a basis of neighborhoods of zero, we can choose the ideals $p^n\mathbb{Z}_pA + U_n$, where U_n consists of series whose terms are monomials of degree $\geq n$ or whose terms contain a nontrivial factor $1 - a_i$, where $i \geq n$.

Now let G be a pro-p-group of countable type with a normal series

$$G = G_1 > G_2 > \cdots > G_s > G_{s+1} = 1,$$

whose factor groups $A_i = G_i/G_{i+1}$ are free abelian pro-p-groups. Since the intersection of the members of the lower central series of G is equal to 1, in every group G_i one can choose a sequence of elements $a_{i1}, a_{i2}, \ldots$ converging to 1 whose canonical images in the abelian group A_i constitute a basis, and satisfying

$$[G, a_{ij}] \leq \langle a_{i,j+1}, a_{i,j+2}, \ldots \rangle G_i^p G_{i+1}. \tag{2}$$

Consider a formal series $u = \sum_M \gamma_M M$, where $\gamma_M \in \mathbb{Z}_p$, $M = M_1 \cdots M_s, M_i$ are monomials of the form $(1-a_{i1})^{\alpha_1} \cdots (1-a_{in})^{\alpha_n}$. Since any neighborhood of zero in the algebra $\mathbb{Z}_pG$ contains almost all monomials M, the series u represents some element of this algebra. By Lemma 1, as a $\mathbb{Z}_p$-module, $\mathbb{Z}_pG$ decomposes into the tensor product $\mathbb{Z}_pA_1 \otimes \mathbb{Z}_pA_2 \otimes \cdots \otimes \mathbb{Z}_pA_s$. Using the representation of elements of the algebras $\mathbb{Z}_pA_i$ as series we can state that the representation of elements of the algebra $\mathbb{Z}_pG$ as formal series is faithful. We define an order of monomials by $M_1\cdots M_s < M_1'\cdots M_s'$ if for some i:

$$\begin{aligned} M_s =& M_s', \dots, M_{i+1} = M_{i+1}',\\ M_i =& (1-a_{i1})^{\alpha_1}\cdots(1-a_{in})^{\alpha_n} \neq M_i' = (1-a_{i1})^{\beta_1}\cdots(1-a_{in})^{\beta_n}, \end{aligned}$$

and either $\alpha_1+\cdots+\alpha_n < \beta_1+\cdots+\beta_n$, or $\alpha_1+\cdots+\alpha_n = \beta_1+\cdots+\beta_n$ and for some j $\alpha_n=\beta_n,\dots,\alpha_{j+1}=\beta_{j+1},\alpha_j<\beta_j$.

Let $u\in p^k\mathbb{Z}_pG\setminus p^{k+1}\mathbb{Z}_pG$. For the series u we consider those monomials M for which $\gamma_M\notin p^{k+1}\mathbb{Z}_p$, and among these we choose M_0, the minimal one. The term $\gamma_{M_0}M_0$ is called the **lowest term** of the element u.

LEMMA 2: *Let u,v be non-zero elements of $\mathbb{Z}_pG$, and let $\gamma_M M_1\cdots M_s$ and $\gamma_M' M_1'\cdots M_s'$ be their lowest terms respectively. Then $\gamma_M\gamma_M' M_1''\cdots M_s''$ will be the lowest term of the element uv, where $M_i''=(1-a_{i1})^{\alpha_1+\beta_1}\cdots(1-a_{in})^{\alpha_n+\beta_n}$ if $M_i=(1-a_{i1})^{\alpha_1}\cdots(1-a_{in})^{\alpha_n}$ and $M_i'=(1-a_{i1})^{\beta_1}\cdots(1-a_{in})^{\beta_n}$.*

Proof: Let H be an arbitrary open normal subgroup of the group G. Let I be the kernel of the canonical homomorphism $\mathbb{Z}_pG\to(\mathbb{Z}/p^r\mathbb{Z})[G/H]$ where r is a fixed natural number. Modulo the ideal I the elements u,v are represented as finite linear sums of monomials. It is sufficient to prove that, modulo I, the product of these sums is equal to a linear sum of monomials with the lowest term $\gamma_M\gamma_M' M_1''\cdots M_s''$. Then passing to the projective limit we get a representation of the element uv as a series with the corresponding lowest term.

We first define a "collecting process" with the help of which one can represent an arbitrary unordered product of the elements $1-a_{ij}$ modulo I as a linear sum of ordered products which we call monomials. Let L be an arbitrary unordered product of the elements $1-a_{ij}$. We denote by $\bar{L}$ the ordered monomial obtained from L using permutations of factors. We distinguish unordered factors $(1-a_{ij})$ and $(1-a_{kl})$ in $L=L_1(1-a_{ij})(1-a_{kl})L_2$, where either $i>k$, or $i=k$, $j>l$. We use the following standard identities which hold in an arbitrary group ring R for all elements x,y of the group:

$$\begin{aligned} 1-xy =& (1-x)+(1-y)-(1-x)(1-y),\\ 1-x^p \equiv& (1-x)^p \mod pR,\\ (1-y)(1-x) =& (1-x)(1-y)-(1-[x,y])+(1-xy)(1-[x,y]). \end{aligned}$$

With the help of these identities, together with the inclusions (2), we can represent the element L modulo I as

$$L = L_1(1 - a_{kl})(1 - a_{ij})L_2 + \sum_t \sigma_t K_t,$$

where $\{K_t\}$ is some finite set of unordered products, $\sigma_t \in \mathbb{Z}_p$, and either σ_t is divisible by p, or the corresponding K_t is such that $\bar{K}_t > \bar{L}$. Thus, modulo higher terms we could interchange the factors $1 - a_{ij}$ and $1 - a_{kl}$. Therefore the collecting process is defined and the lemma is proved. ∎

COROLLARY: *Let G be a pro-p-group of countable type with a normal series $G = G_1 \geq G_2 \geq \cdots \geq G_n \geq G_{n+1} \geq \cdots$, such that $\bigcap G_n = 1$ and the factor groups G_n/G_{n+1} are torsion free abelian pro-p-groups. Then the group algebra $\mathbb{Z}_p G$ is a domain.*

Proof: It follows directly from Lemma 3 that the algebras $\mathbb{Z}_p[G/G_n]$ are domains. So the algebra $\mathbb{Z}_p G$ has this property since it has a representation as a projective limit $\varprojlim \mathbb{Z}_p[G/G_n]$. ∎

4. Magnus' embedding for pro-p-groups

Let F be a free pro-p-group with a finite basis $\{x_1, \ldots, x_m\}$, N a normal subgroup, and $\varphi : F \to A = F/N$ the canonical homomorphism. We consider the right free (topological) module T with a basis $\{t_1, \ldots, t_m\}$ over the ring $\mathbb{Z}_p A$. This gives rise to a natural extension of the additive group of the module T by the group A, which we shall identify with the multiplicative group of matrices:

$$\begin{bmatrix} A & 0 \\ T & 1 \end{bmatrix}.$$

Let ψ be the homomorphism from F to this group determined by the mapping

$$x_1 \to \begin{bmatrix} x_1\varphi & 0 \\ t_1 & 1 \end{bmatrix}, \ldots, x_m \to \begin{bmatrix} x_m\varphi & 0 \\ t_m & 1 \end{bmatrix}.$$

By analogy with abstract groups Remeslennikov [5] proved that $\ker \psi = [N, N]$. The following statement for pro-p-groups is transferred from the corresponding statement proved in [6] for abstract groups without change.

LEMMA 3: *Let H be a normal subgroup of F generated by the elements h_i. Let $h_i\psi = \begin{bmatrix} a_i & 0 \\ v_i & 1 \end{bmatrix}$ and let B be the normal subgroup of $\begin{bmatrix} A & 0 \\ T & 1 \end{bmatrix}$ generated by all elements $\begin{bmatrix} a_i & 0 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ v_i & 1 \end{bmatrix}$. Then $B \bigcap F\psi = H\psi$.*

This lemma gives a convenient method to study the factor groups of $F/[N, N]$. Indeed, the factor group of $\begin{bmatrix} A & 0 \\ T & 1 \end{bmatrix}$ by the normal subgroup generated by the elements $\begin{bmatrix} a_i & 0 \\ 0 & 1 \end{bmatrix}$ is isomorphic to $\begin{bmatrix} A' & 0 \\ T' & 1 \end{bmatrix}$, where $A' = F/NH$ and T' is the free $\mathbb{Z}_pA'$-module of rank m. By Lemma 3 the group $F/[N, N]H$ will be embedded into the group $\begin{bmatrix} A' & 0 \\ T'/L & 1 \end{bmatrix}$, where L is the submodule of the module T' generated by the canonical images of the elements v_i.

5. Proof of the theorem

We have $G = F/R$, where $R = r^F$ is the normal subgroup of F generated by an element r.

5.1. First assume that there is an element s of $F^{(k)}$ such that $r \equiv s^p \bmod F^{(k+1)}$. Note that then the factor group $G^{(k)}/G^{(k+1)}$ has torsion. To see this let us denote by φ the canonical homomorphism $F \to F/F^{(k+1)}$. The group $F\varphi$ acts by conjugation on $F^{(k)}\varphi$. This action extends to the action of the group algebra $\mathbb{Z}_p[F\varphi]$. From this point of view $R\varphi$ is the right $\mathbb{Z}_p[F\varphi]$-module generated by the element $r\varphi$. We have, in the module language, $(s\varphi)p = r\varphi$. Assume that $s\varphi \in R\varphi$. Then there is an element u of $\mathbb{Z}_p[F\varphi]$ such that $s\varphi = (r\varphi)u$. This means that $s\varphi(1 - pu) = 0$. The element $1 - pu$ is invertible in the algebra $\mathbb{Z}_p[F\varphi]$. Therefore $s\varphi = 0$, which contradicts the fact that $r \in F^{(k)} \setminus F^{(k+1)}$. Therefore $s\varphi \notin R$ and the group $G^{(k)}/G^{(k+1)}$ has torsion.

5.2. Now we come to the most difficult part of the proof of the theorem. Assume that the element r is not a p-th power of an element of $F^{(k)}$ modulo $F^{(k+1)}$. It is sufficient to prove that the factors of the derived series of G are torsion free, and the group algebra $\mathbb{Z}_pG$ is a domain. This together with Brumer [7] yields $\operatorname{cd} G \leq 2$.

We first reduce the problem to the case when X is a finite set. Indeed, let $\{X_\alpha\}$ be the finite subsets of X, F_α be the free pro-p-group with the basis X_α, φ_α be an endomorphism $F \to F_\alpha$, which is the identity on F_α and which maps the elements of $X \setminus X_\alpha$ to 1. It is obvious that $F = \varprojlim F_\alpha$, $G = \varprojlim G_\alpha$, where $G_\alpha = \langle X_\alpha | r\varphi_\alpha \rangle$. Therefore there is an index α_0 such that the element $r\varphi_{\alpha_0}$ is not a p-th power of an element of $F_{\alpha_0}^{(k)}$ modulo $F_{\alpha_0}^{(k+1)}$. Consider the union $\{X_\beta\}$ of all finite subsets of X containing X_{α_0}. We have for every β the condition that the element $r\varphi_\beta$ is not a p-th power of an element of $F_\beta^{(k)}$ modulo $F_\beta^{(k+1)}$. If we prove that the factors of the derived series of the groups G_β are torsion free, then the factors of the derived series of the group $G = \varprojlim G_\beta$ must be torsion free, and by the corollary of the Lemma 2 the algebras $\mathbb{Z}_p G_\beta$ are domains and therefore the algebra $\mathbb{Z}_p G = \varprojlim \mathbb{Z}_p G_\beta$ is also a domain.

So let $X = \{x_1, \dots, x_m\}$ be a finite set and let the element r satisfy the condition of the theorem. We must prove that the factors of the derived series of G are torsion free.

Let $F_n = F/F^{(n)}$, $G_n = G/G^{(n)}$ and let φ_n, ψ_n denote the canonical homomorphisms $F \to F_n$, $G \to G_n$ correspondingly. It is obvious that $F_k = G_k$. Let T be a free right module with a base $\{t_1, \dots, t_m\}$ over the ring $\mathbb{Z}_p F_k$. By the Magnus' embedding we identify the group F_{k+1} with the subgroup of the group $\begin{bmatrix} F_k & 0 \\ T & 1 \end{bmatrix}$ generated by the matrices $\begin{bmatrix} x_1\varphi_k & 0 \\ t_1 & 1 \end{bmatrix}, \dots, \begin{bmatrix} x_m\varphi_k & 0 \\ t_m & 1 \end{bmatrix}$. Then the element $r\varphi_{k+1}$ is represented as some matrix $\begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}$, where $u = t_1u_1 + \cdots + t_m u_m$. From [4] we have the equality, $(1 - x_1\varphi_k)u_1 + \cdots + (1 - x_m\varphi_k)u_m = 0$. We note that there is an element u_i which is not divisible by p. Otherwise if $u_i = pv_i$ then $(1 - x_1\varphi_k)v_1 + \cdots + (1 - x_m\varphi_k)v_m = 0$ and this means by [5] that the matrix $\begin{bmatrix} 1 & 0 \\ v & 1 \end{bmatrix} \in F_{k+1}^{(k)}$, where $v = t_1v_1 + \cdots + t_m v_m$. Since $\begin{bmatrix} 1 & 0 \\ v & 1 \end{bmatrix}^p = \begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}$ we have a contradiction to the fact that r is not a p-th power of an element of $F^{(k)}$ modulo $F^{(k+1)}$.

Now let $n \geq k$ and assume by the induction that the factors of the derived series of the group G_n are torsion free. Denote by T' the free right module with basis $\{t'_1, \dots, t'_m\}$ over the ring $\mathbb{Z}_p G_n$. Let σ denote the homomorphism $F \to \begin{bmatrix} G_n & 0 \\ T' & 1 \end{bmatrix}$ defined by the mapping $x_1 \to \begin{bmatrix} x_1\psi_n & 0 \\ t'_1 & 1 \end{bmatrix}, \dots, x_m \to \begin{bmatrix} x_m\psi_n & 0 \\ t'_m & 1 \end{bmatrix}$.

It is clear that the element $r\sigma$ is a unitriangular matrix $\begin{bmatrix} 1 & 0 \\ u' & 1 \end{bmatrix}$, where $u' = t'_1u'_1 + \cdots + t'_m u'_m$. The canonical homomorphism $G_n \to F_k$ and the mapping

$t'_1 \to t_1, \ldots, t'_m \to t_m$ define the homomorphism of matrix groups

$$\tau : \begin{bmatrix} G'_n & 0 \\ T' & 1 \end{bmatrix} \to \begin{bmatrix} F_k & 0 \\ T & 1 \end{bmatrix}.$$

We have $\varphi_{k+1} = \sigma\tau$. Therefore $\begin{bmatrix} 1 & 0 \\ u' & 1 \end{bmatrix} \tau = \begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}$. Since the element u of the module T is not divisible by p, the element u' is also not divisible by p in the module T'. By Lemma 3 the group G_{n+1} is embedded into the group of matrices $\begin{bmatrix} G_n & 0 \\ T'/L & 1 \end{bmatrix}$, where L is the submodule of the module T generated by the element u', and the last nontrivial commutator subgroup $G_{n+1}^{(n)}$ of the group G_{n+1} is embedded into the additive group of the factor module T'/L. For the next inductive step it is sufficient to prove that the module T'/L is torsion free. For, otherwise there is an element v of T' which does not belong to L and $vp \in L$. Let $vp = u'w$, where $w \in \mathbb{Z}_pG_n$. In Section 2 we found the representation of the elements of the algebra $\mathbb{Z}_pG$ by series. Since some element u'_i does not belong to $p\mathbb{Z}_pG_n$, its lowest term is not divisible by p. Since the lowest term of the product u'_iw is divisible by p, by Lemma 2 the lowest term of the element w is divisible by p. Thus all coefficients of the series w are divisible by p. Then $w = pw'$, where $w' \in \mathbb{Z}_pG_n$. We have $vp = u'w'p$ and $v = u'w'$, contrary to the fact $v \notin L$. This completes the proof of the theorem.

ACKNOWLEDGEMENT: This manuscript was prepared during the author's visit to the University of Manitoba, Canada. The author wishes to thank the Department of Mathematics for its hospitality.

References

[1] D. Gildenhuys, *On pro-p-groups with a single defining relator*, Invent. Math. **5** (1968), 357–366.

[2] N. Romanovskii, *A generalized Freiheitssatz for pro-p-groups*, Sib. Math. Zh. **27** (1986), 154–170.

[3] J. Labute, *Algèbres de Lie et pro-p-groupes définis par une seule relation*, Invent. Math. **4** (1967), 142–158.

[4] M. Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Annales Ecole Normale Supérieure **71** (1954), 101–190.

[5] V. Remeslennikov, *Embedding theorems for profinite groups*, Izv. Akad. Nauk SSSR, Ser. Mat. **43** (1979), 399–417.

[6] N. Romanovskii, *On some algorithmic problems for soluble groups*, Algebra i Logika **13** (1974), 26–34.

[7] A. Brumer, *Pseudocompact algebras, profinite groups and class formations*, J. Algebra **4** (1966), 442–470.