Can. J. Math., Vol. XXVII, No. 6, 1975, pp. 1355–1360

FAITHFUL REPRESENTATIONS OF FINITELY GENERATED METABELIAN GROUPS

B. A. F. WEHRFRITZ

1. In [**3**] Remeslennikov proves that a finitely generated metabelian group G has a faithful representation of finite degree over some field F of characteristic zero (respectively, $p > 0$) if its derived group G' is torsion-free (respectively, of exponent p). By the Lie-Kolchin-Mal'cev theorem any metabelian subgroup of $GL(n, F)$ has a subgroup of finite index whose derived group is torsion-free if char $F = 0$ and is a p-group of finite exponent if char $F = p > 0$. Moreover every finite extension of a group with a faithful representation (of finite degree) has a faithful representation over the same field. Thus Remeslennikov's results have a gap which we propose here to fill.

1.1 THEOREM. *If the group G is a finite extension of a finitely generated metabelian group G_0 whose derived group G_0' is a p-group for some prime p, then G has a faithful representation of finite degree over some field of characteristic p.*

A *quasi-linear group* is a group of matrices over a direct sum of a finite number of fields, its characteristic being the set of the characteristics of the ground fields. (This is a slight modification of the definition in [**4**]). If G is a metabelian group, by the characteristic of G we mean the set of prime divisors of the orders of the elements of G' of finite order, together with zero if G' is not a torsion group. An immediate corollary of 1.1 above and Remeslennikov's 'characteristic zero' case is the following.

1.2 COROLLARY. *If the group G is a finite extension, of a finitely generated metabelian group of characteristic π, then G is isomorphic to a quasi-linear group of characteristic π.*

There are no corresponding results without the finite generation. For example, for any non-trivial group P the complete wreath product $P \,\bar{\wr}\, \mathbf{Z}$ is not isomorphic to any group of automorphisms of any finitely generated module over any commutative Noetherian ring R. For R a field this is a special case of [**4**, 10.22] and essentially the same proof works in general.

Given a field F of characteristic $p > 0$ there exists one and, up to isomorphism, only one complete and unramified, discrete valuation ring with residue class field F [**1**, Lemma 13 and Theorem 11, Corollary 2]. This ring we

Received October 21, 1974 and in revised form, February 13, 1975.

The author is indebted to Carleton University, Ottawa for their hospitality while working on this paper.

denote by $J(0, F)$. For each positive integer m set

$$J(m, F) = J(0, F)/(p^m).$$

$J(m, F)$ is a commutative local ring of characteristic p^m, with maximal ideal generated by p and residue class field F. These properties uniquely determine $J(m, F)$ up to isomorphism in view of [**1**, Theorem 11, Corollary 3] and the ideal structure of $J(0, F)$.

To prove 1.1 we swiftly reduce to the split extension $X[M$ of a finitely generated X-module M over the finitely generated abelian group X, by X. (Whenever X is a group and M is an X-group $X[M$ denotes the external semi-direct product of M by X.) A series of module theoretic reductions leaves us with the case of the split extension of $J(m, F)$ by a finitely generated p-free subgroup of the group of units of $J(m, F)$.

Suppose that R is a commutative local ring of characteristic p^m and residue class field F. If $\mathfrak{m}$ is the maximal ideal of R then there is a multiplicative exact sequence

$$(1.3) \quad 1 \rightarrow 1 + \mathfrak{m} \rightarrow R\backslash\mathfrak{m} \rightarrow F^* \rightarrow 1.$$

Now F^* is p-free since char $F = p$. If $\mathfrak{m}$ is nilpotent, for example if $\mathfrak{m} = pR$, then $1 + \mathfrak{m}$ is a p-group of finite exponent and the sequence (1.3) splits. When (1.3) splits a complement U of $1 + \mathfrak{m}$ in $R\backslash\mathfrak{m}$ we call a *unit complement* of R. In general U will not be unique though it will be of course if F is a locally finite field. The final step of the proof of 1.1, which in fact we present first in § 2, is to construct representations of certain split extensions of the type $U[R$ with U and R as above. The proof of 1.1 is then completed in § 3.

In this note all rings have an identity, all modules are unital and ring homomorphisms are identity preserving.

2. Let F be a field of characteristic $p > 0$, let m be a positive integer and set $n = p^{m-1} + 1$. For each $\alpha \in F$ put

$$\begin{aligned} t_\alpha &= (\alpha_{ij}) \in \mathrm{Tr}(n, F) \text{ where} \\ \alpha_{ij} &= 1 \text{ if } i = j \\ &= \alpha \text{ if } i = j + 1 \end{aligned}$$

and is zero otherwise. Set $A = \langle t_\alpha : \alpha \in F \rangle \subseteq \mathrm{Tr}(n, F)$. It is easy to check that $|t_\alpha| = p^m$ if $\alpha \neq 0$ and that $t_\alpha t_\beta = t_\beta t_\alpha$ for all α, β in F, [**4**, pp. 19–20]. In particular A is an abelian group of exponent p^m.

We now define a new law of composition on A to make A into a ring. For $\beta \in F^*$ let

$$d_\beta = \mathrm{diag}(\beta^{n-1}, \beta^{n-2}, \ldots, \beta, 1) \in GL(n, F).$$

Then $D = \{d_\beta : \beta \in F^*\}$ is an abelian group, and since $d_\beta^{-1} t_\alpha d_\beta = t_{\alpha\beta}$ for all $\alpha, \beta \in F^*$ conjugation makes A into a cyclic D-module generated by t_1. Thus A is an image of the commutative ring $\mathbf{Z}D$ and hence A can be made into a commutative ring with identity t_1. Note that the multiplication on A, which we denote by circle, is determined by

$$t_\alpha \circ t_\beta = t_{\alpha\beta} = d_\beta^{-1} t_\alpha d_\beta.$$

Any field automorphism of F induces a ring automorphism of A by acting on the matrix entries. In particular if F is perfect the Frobenius automorphism $\alpha \mapsto \alpha^p$ of F induces an automorphism θ of A. Since A/A^p is a commutative ring of characteristic p the binomial theorem yields that modulo A^p the circle product of a with itself p^k times is

$$\circ^{p^k} a \equiv \prod_i (t_{\alpha_i{}^{p^k}})^{e_i} = a\theta^k, \quad \text{where } a = \prod_i t_{\alpha_i}{}^{e_i},$$

for any positive integer k. If a is a nilpotent element of A then for sufficiently large k we have $\circ^{p^k} a = 1$. In this situation $a\theta^k \in A^p$, whence $a \in A^p$. We have now proved that A^p is the nilradical of A.

For $l \geqq 0$ put

$$M_l = \{a = (a_{ij}) \in A : a_{ij} = 0 \text{ whenever } 0 < \mathrm{i} - \mathrm{j} \leqq l\}.$$

Clearly M_l is a subgroup of A and $d_\beta^{-1} M_l d_\beta \subseteq M_l$ for all $\beta \in F^*$. Thus M_l is an ideal of A for $l \geqq 1$ and $M_0 = A$. Suppose $a = (a_{ij}) \in M_{l-1} - M_l$. Then $a_{i,i-l} \neq 0$ and the $(i, i - l)$ component of $a \circ b$ is

$$(a \circ b)_{i,i-l} = a_{i,i-l}\left(\sum_{j=1}^{s} f_j \beta_j{}^l\right).$$

In particular for $l \geqq 1$ with $M_{l-1} \neq M_l$ the map $\varphi_l : A \to F$ given by $b\varphi_l = \sum_j f_j \beta_j{}^l$ is well defined. Also φ_l is a ring homomorphism—this can easily be checked directly but it is also an immediate consequence of

$$(\mathrm{a} \circ (bc))_{i,i-l} = ((a \circ b)(a \circ c))_{i,i-l} = (a \circ b)_{i,i-l} + (a \circ c)_{i,i-l}$$

and

$$(a \circ (b \circ c))_{i,i-l} = ((a \circ b) oc)_{i,i-l}$$

Now assume that every polynomial $X^l - \alpha$ has a root in F for every α in F and every integer l satisfying $0 < l < n$ and $M_{l-1} \neq M_l$. This will certainly be the situation if F is algebraically closed, which is the only case that we shall actually use. Then in particular $A\varphi_l = F$ for each such l and for all $l \geqq 1$ either $M_{l-1} = M_l$ or M_{l-1}/M_l is an irreducible A-module such that modulo its annihilator, A is isomorphic to F. Hence A satisfies the minimal condition and so is a direct sum of a finite number of local rings A_i whose maximal ideals are nilpotent (e.g. [**5**, p. 205]). Moreover the above implies that for each i the residue class field of A_i is isomorphic to F and that the maximal ideal of A_i is generated by p. Thus A_i is isomorphic to $J(m_i, F)$ for some integer $m_i \leqq m$ and since A has characteristic p^m we have $m_i = m$ for at least one i.

For $M_{l-1} \neq M_l$ our assumption on F ensures that the ring homomorphism φ_l maps the subgroup $W = \{t_\alpha : \alpha \in F^*\}$ of the group of units of A isomorphically onto F^*. Thus if π_i denotes the projection of A onto A_i then $W\pi_i$ is a unit complement of A_i. For any $a \in A$ and $\beta \in F^*$ we have

$$(a\pi_i)^{d_\beta} = a\pi_i \circ t_\beta = a\pi_i \circ t_\beta\pi_i$$

since $A_i \circ A_j = \{1\}$ if $i \neq j$. Set $D = \langle d_\beta : \beta \in F^* \rangle$. Then $\langle A_i, D \rangle \subseteq \mathrm{Tr}(n, F)$ is isomorphic to the natural split extension of A_i by $W\pi_i$. In particular we have now proved the following.

2.1 THEOREM. *If F is any algebraically closed field of characteristic $p > 0$ and if m is any positive integer there exists a unit complement V of $J = J(m, F)$ such that the natural split extension $V[J$ is isomorphic to a subgroup of* $\mathrm{Tr}(p^{m-1} + 1, F)$.

An easy fact that we shall not need is that $J(m, F)$ has a unique unit complement whenever F is perfect. I am indebted to Warren Dicks for pointing out to me that for F a perfect field $J(m, F)$ is isomorphic to the ring of Witt vectors over F of length m and that the representations above of $U(m, F)[J(m, F)$ can be given explicitly by means of the Artin-Hasse exponential.

3.

3.1 LEMMA. *If E is a finitely generated subfield of the field F of positive characteristic and if m is a positive integer then $J(m, E)$ is isomorphic to a subring of $J(m, F)$.*

A slight variant of the argument below yields the corresponding result for $m = 0$. The finite generation of E is irrelevant.

Proof. $R = J(m, F)$ contains a finitely generated (and hence Noetherian) subring S whose image in R/pR generates a copy of E. The localization T in R of S at $S \cap pR$ is a commutative Noetherian ring with residue class field E and nilpotent maximal $T \cap pR$. Thus T is also complete and Theorem 11, Corollary 1 of [**1**] yields a homomorphism φ of $J = J(0, E)$ into T. Since φ preserves the identity $\ker \varphi = p^m J$ and hence φ induces an embedding of $J(m, E) = J/p^m J$ into R.

3.2 *Proof of Theorem* 1.1. By hypothesis our group G contains a finitely generated metabelian group G_0 of finite index such that G_0' is a p-group. Putting $H = G_0/G_0'$ consider the Kalužnin-Krasner embedding φ of G_0 into $W = G_0' \wr H$ and denote the base group of W by B. Then $G_1 = \langle G_0\varphi, H \rangle$ is a finitely generated metabelian group, $M = G_1 \cap B$ is an abelian normal p-subgroup of G_1 and G_1 is the split extension of M by H. M is a finitely generated H-module and in particular has finite exponent (e.g. [**4**], p. 189). By [**4**, 2.3] it suffices to construct a faithful representation of $G_1 = HM$.

If $\sigma : G_1 \to GL(r, F)$ and $\tau : G_1 \to GL(s, F)$ are homomorphisms with $\ker \sigma \cap \ker \tau = \langle 1 \rangle$ then

(3.3) $\quad x \mapsto \mathrm{diag}(x\sigma, x\tau)$

https://doi.org/10.4153/CJM-1975-138-0 Published online by Cambridge University Press

is a faithful representation of G_1 into $GL(r + s, F)$. By choosing a primary decomposition of $\{1\}$ in the finitely generated $\mathbf{Z}H$-module M and applying (3.3) it follows that we may assume that M is a primary $\mathbf{Z}H$-module. Clearly there exist fields of characteristic p over which H has a faithful representation of finite degree, e.g. 2.2 of [**4**]. Hence it suffices to construct a faithful representation of $HM/C_H(M) \cong (H/C_H(M))[M$. That is, we may also assume that H acts faithfully on M.

Let R denote the subring of $\mathrm{End}_{\mathbf{Z}}\, M$ generated by H and set $\mathfrak{r} = \mathrm{rad}\, M$. Then $\mathfrak{r}$ is a nilpotent prime ideal. We localize at $\mathfrak{r}$; whence $S = R_{\mathfrak{r}}$ is a commutative Noetherian local ring with nilpotent maximal ideal $\mathfrak{m} = \mathfrak{r}_{\mathfrak{r}}$ and, since M is primary, M embeds into $N = M \otimes_R S$. Regarding R as a subring of S we have that $G_1 = HM$ is isomorphic to a subgroup of $H[N$. Also M has finite exponent p^m say, whence S has characteristic p^m.

By [**1**, Theorem 11] there exists a subring J of S satisfying $S = J + \mathfrak{m}$ and $J \cap \mathfrak{m} = pJ$. If we put $F = S/\mathfrak{m}$ then clearly J is isomorphic to $J(m, F)$. Since S is Noetherian each $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ has finite F-dimension. Thus the nilpotency of $\mathfrak{m}$ yields that S is a finitely generated J-module and therefore N is also a finitely generated J-module.

If U is a unit complement of J then U is also a unit complement of S and $H \subseteq U \times (1 + \mathfrak{m})$. Now $1 + \mathfrak{m}$ is a p-group and H is finitely generated, hence $H \subseteq H_1 \times P$ for some finitely generated subgroup H_1 of U and some finite subgroup P of $1 + \mathfrak{m}$. If $H_1[N$ is isomorphic to a subgroup of $GL(n, E)$ for some n and some field E then G_1 is isomorphic to a subgroup of $GL(n|P|, E)$ by [**4**, 2.3] again. J is an image of the principal ideal domain $J(0, F)$ so N is a direct sum of cyclic J-modules. The only cyclic J-modules up to isomorphism are the J/p^iJ for $i = 1, 2, \ldots, m$ and as rings $J/p^iJ \cong J(i, F)$. Applying the reduction 3.3 again this shows that it suffices to construct a faithful representation of the split extension $H_1[J$ of characteristic p.

Let $\bar{F}$ denote the algebraic closure of F. Now F is the quotient field of the finitely generated ring $R/\mathfrak{r}$ and hence by 3.1 there exists a copy $\bar{J}$ of $J(m, \bar{F})$ containing J as a subring. Now there exists by 2.3 a unit complement V of $\bar{J}$ such that $GL(p^{m-1} + 1, \bar{F})$ contains an isomorphic copy of $V[\bar{J}$. Since $H_1 \subseteq V \times (1 + p\bar{J})$ the finite generation of H_1 yields that $H_1 \subseteq V \times Q$ for some finite p-subgroup Q. Then

$$H_1[J \subseteq H_1[\bar{J} \subseteq QV[\bar{J}$$

and by [**4**, 2.3] the latter group is isomorphic to a subgroup of $GL(|Q|(p^{m-1} + 1), \bar{F})$. This completes the proof of 1.1.

References

1. I. S. Cohen, *On the structure and ideal theory of complete local rings*, Trans. Amer. Math. Soc. *59* (1946), 54–106.

2. V. N. Remeslennikov, *Finite approximability of metabelian groups* (Russian), Alg. i Logika *7* (1968), 106–113; Alg. and Logic *7* (1968), 268–272.

3. ——— *Representations of finitely generated metabelian groups by matrices* (Russian), Alg. i Logika *8* (1969), 72–75; Alg. and Logic *8* (1969), 39–40

4. B. A. F. Wehrfritz, *Infinite linear groups*, Ergeb. d. Math. Bd. 76 (Springer-Berlin Heidelberg New York, 1973).

5. O. Zariski and P. Samuel, *Commutative algebra Vol. 1* (Van Nostrand-Princeton, 1958).

Queen Mary College,
London, England