FAITHFUL LINEAR REPRESENTATIONS OF CERTAIN FREE NILPOTENT GROUPS

by B. A. F. WEHRFRITZ

(Received 2 April 1993)

Brian Hartley asked me whether a free (nilpotent of class 2 and exponent p^2)-group of countable rank has a faithful linear representation of finite degree, p here being a prime of course. The answer is yes. The point is that this then yields via work of F. Leinen and M. J. Tomkinson, see [**3**, 3.6] an image of a linear p-group, which is not even finitary linear. The question of which relatively free groups have faithful linear representations dates back at least to work of W. Magnus in the 1930's, see [**4**, pp. 33, 34 and the final comment on p. 40] for a discussion of this. Our construction, which works more generally, is a further contribution. We write $\mathfrak{N}_c$ for the variety of nilpotent groups of class at most c and $\mathfrak{E}_q$ for the variety of groups of exponent dividing q.

THEOREM. *Let c and e be positive integers, p a prime and $q = p^e$. Any free $\mathfrak{N}_c \cap \mathfrak{E}_q$ group has a faithful representation of finite degree over any perfect field of characteristic p and sufficiently large transcendence degree, provided at least one of the following conditions hold.*

(a) $c \leq 2$.

(b) $c = 3 \neq p$.

(c) $c < p$.

Here (a) settles positively Hartley's question. We give an existence proof. I have not troubled to compute the actual representation constructed or even to find the precise degree, but in principle it would not be difficult to follow through the proofs and determine these. The case $c = p = q = 3$ remains open. By the Levi—van der Waerden theorem [**2**, III.6, 5&6] the groups in question are just the Burnside groups of exponent 3.

Our notation is accumulative. Trivially a free $\mathfrak{N}_c \cap \mathfrak{E}_q$-group of rank 1 has a faithful representation of degree q (of degree $p^{e-1}+1$ in fact) over GF(p). From now on we consider only such groups of rank at least 2. Clearly free $\mathfrak{N}_c \cap \mathfrak{E}_q$-groups of finite rank are finite and hence have a faithful linear representation of finite degree over GF(p), but we need an economical representation in order to construct faithful representations of the groups of infinite rank.

Let I be a set with at least two members and let $\Xi = \{\xi_{ij} : i \in I;\ j = 1, 2, \ldots, c\}$ be a family of independent indeterminates. Set $R = (\mathbb{Z}/q)[\Xi]$, the polynomial ring in Ξ over the integers modulo q. Initially we consider matrix representations over R. Throughout $\{e_{jk}\}$ denotes a set of standard matrix units, the degree of the matrices and the ground ring being determined by context. For each i in I set

$$g_i = 1 + \sum_{1 \leq j \leq c} \xi_{ij} e_{j+1,j} \in \mathrm{Tr}_1(c+1, R) \leq \mathrm{GL}(c+1, R)$$

and put $G = \langle g_i : i \in I \rangle$.

(a) *G is nilpotent of class c and exponent at least q. It has exponent q if and only if $p > c$.*

For certainly G is nilpotent of class of most c and for $1, 2 \in I$, direct calculation

yields that $[g_{1,c-1}\, g_2] \neq 1$. (This is most easily seen by specializing ξ_{1j} to 0 for $1 \leq j < c$ and ξ_{1c} and ξ_{2j} for $1 \leq j \leq c$ to 1.) Thus G has class exactly c.

The exponent of G is certainly a power of p. Let $g \in G$. Then $u = g - 1$ satisfies $u^{c+1} = 0$ and so

$$g^q = (1+u)^q = \sum_{0 \leq h \leq c} {}^qC_h u^h,$$

where ${}^qC_h$ denotes the appropriate binomial coefficient. Suppose $p > c$. Since q divides ${}^qC_h$ for $0 < h < p$ we obtain $g^q = 1$. Also the $(2,1)$ entry of g_i^r is $r\xi_{i1}$ for any i in I and $r \geq 1$. Hence G has exponent exactly q. Now assume that $p \leq c$. The $(p+1,1)$ entry of g_i^q is ${}^qC_p \prod_{1 \leq h \leq p} \xi_{ih}$, which is non-zero since q does not divide ${}^qC_p$. Thus in this case the exponent of G exceeds q.

Set $R_0 = \mathbb{Z}[\Xi]$, $g_{0i} = 1 + \sum_{1 \leq j \leq c} \xi_{ij} e_{j+1,j} \in \mathrm{Tr}_1(c+1, R_0)$ and $G_0 = \langle g_{0i} : i \in I \rangle$. Then G_0 is a free $\mathfrak{N}_c$-group on the exhibited generators, see [**4**, 2.12] and its proof. Reduction modulo q maps R_0 to R, g_{0i} to g_i and G_0 to G. Let $1 \leq h \leq c$ and set $h' = c + 1 - h$. Let π_h be the map of G_0 into $R_0^{(h')}$ that maps a matrix onto its h-th lower off-diagonal; specifically

$$\pi_h : (x_{jk}) \mapsto (x_{h+1,1}, x_{h+2,2}, \ldots, x_{c+1,h'}).$$

Let

$$G_{0h} = \{(g_{jk}) \in G_0 : g_{jk} = 0 \text{ for } 0 < j - k < h\}.$$

(b) *$\gamma^h G_0 = G_{0h}$ and $G_{0h}\pi_h$ is a $\mathbb{Z}$-direct summand of $R_0^{(h')}$.*

The h-th member $\gamma^h G_0$ of the lower central series of G_0 is generated by the basic commutators in the g_{0i} of weight at least h, see [**1**, 5.6 Corollary], and clearly $\gamma^h G_0 \leq G_{0h}$. Also by [**1**, 5.4] the $\mathbb{Z}$-submodule $(\gamma^h G_0)\pi_h$ is spanned by the images under π_h of the basic Lie commutators of weight h in the $u_{0i} = g_{0i} - 1$. Let M_h denote the $\mathbb{Z}$-module spanned by the products of the u_{0i} of weight h. If $(x_{jk}) \in M_h$ then $x_{jk} = 0$ if $j - k \neq h$, the map π_h is an embedding on M_h and $M_h\pi_h$ is spanned by all $(\omega_1, \omega_2, \ldots, \omega_{h'})$, where $\omega_j = \prod_{1 \leq k \leq h} \xi_{i_k, h+j-k}$ and the $i_k \in I$; see [**4**, 2.12] and proof. Now the ω_j are part of a $\mathbb{Z}$-basis of R_0. Hence $M_h\pi_h$ is a $\mathbb{Z}$-direct summand of $R_0^{(h')}$. Further the basic Lie commutators of weight h in the u_{0i} form part of a $\mathbb{Z}$-basis of M_h, see [**1**, 5.3], and hence generate a $\mathbb{Z}$-direct summand of M_h. Therefore $(\gamma^h G_0)\pi_h$ is a $\mathbb{Z}$-direct summand of $R_0^{(h')}$ with the images of the basic commutators in the g_{0i} as a basis. Finally $\gamma^1 G_0 = G_{01}$ by definition and for $h \geq 1$ we have

$$\gamma^h G_0 \cap G_{0,h+1} = \gamma^h G_0 \cap \ker \pi_h = \gamma^{h+1} G_0$$

by [**1**, 5.6 Corollary]. Consequently $\gamma^h G_0 = G_{0h}$.

(c) *If $p > c$ then G is a free $\mathfrak{N}_c \cap \mathfrak{E}_q$-group of rank $|I|$ on the exhibited generators.*

Suppose first that I is finite and let $r(h)$ denote the rank of $G_{0h}/G_{0,h+1}$; that is $r(h)$ is the number of basic commutators of weight h in the g_{0i} and is given by Witt's formula [**1**, 5.7]. By (b) the order of $G_{0h}\pi_h$ modulo q is $q^{r(h)}$. Thus $|G| = \prod_{1 \leq h \leq c} q^{r(h)}$. But clearly

https://doi.org/10.1017/S0017089500030354 Published online by Cambridge University Press

$(\gamma^h G_0)^q \leq G_0^q$ for any q, so $(G_0 : G_0^q) \leq \prod_{1 \leq h \leq c} q^{r(h)}$. Finally, since $p > c$, the group G is a homomorphic image of G_0/G_0^q via $g_{0i}G_0^q \mapsto g_i$ by (a). Thus $|G| = |G_0/G_0^q|$ and this map is an isomorphism; that is G is a free $\mathfrak{N}_c \cap \mathfrak{E}_q$-group on the g_i.

Now suppose I is infinite. The above yields that $\langle g_k : k \in K \rangle$ is a free $\mathfrak{N}_c \cap \mathfrak{E}_q$ group on the exhibited generators for every finite subset K of I (technically with $|K| \geq 2$, though actually for all such K). The claim (c) follows.

For any ring S let ϕ be the map of the ring $\sum_{j \geq k} Se_{jk}$ into itself given by $\phi : (a_{jk}) \to (\pi_{jk} a_{jk})$, where $\pi_{jk} = \prod_{k \leq t < j} t$, the empty product being interpreted as 1. Then ϕ is a ring homomorphism, for clearly ϕ preserves addition, maps the identity matrix to itself and

$$\sum_{m \leq k \leq j} \pi_{jk} a_{jk} \cdot \pi_{km} b_{km} = \pi_{jm} \sum_{m \leq k \leq j} a_{jk} b_{km}.$$

If S is $\mathbb{Z}$-torsion-free clearly ϕ is one-to-one. We now combine this with our earlier notation. For any positive integer h let q_h denote the largest power of p to divide $h!$.

(d) *$G\phi$ has exponent q and is nilpotent of class at most c. It has class exactly c if and only if $q_c \leq q$.*

For let $g \in G$ and set $u = g - 1$; then $(g\phi)^q = \sum_{0 \leq h \leq c} {}^qC_h u^h \phi$. Now $u^h \phi = (u_{jk}^h)$, where $u_{jk}^h = 0$ if $j - k < h$ and $u_{jk}^h \in \pi_{jk} R$ if $j - k \geq 1$. Also $\pi_{jk}/(j-k)! = {}^{j-1}C_{j-k} \in \mathbb{Z}$ and so q divides $\pi_{jk}\, {}^qC_h$ for $1 \leq h \leq j - k$ and $k \geq 1$. Therefore $(g\phi)^q = 1$ and $G\phi$ has exponent dividing q. Finally the $(2,1)$ entry of $g_i^r \phi$ is $r\xi_{i1}$ for any i in I and so $|g_i| \geq q$. Consequently $G\phi$ has exponent q.

Since ϕ is a homomorphism, (a) yields that $G\phi$ is nilpotent of class at most c. Let $1, 2 \in I$. Specialize ξ_{1j} to 0 for $1 \leq j < c$ and ξ_{1c} and ξ_{2j} for $1 \leq j \leq c$ to 1. Then the $(c+1, 1)$ entry of $[g_1\phi, {}_{c-1}\, g_2\varphi]$ specializes to $c!$. Hence if $q_c < q$ then $[g_1\phi, {}_{c-1}\, g_2\phi] \neq 1$ and $G\phi$ has class exactly c. Suppose $q_c \geq q$. Then q divides $\pi_{c+1,1} = c!$ and the $(c+1, 1)$ entry of $g\phi$ is zero for every g in G. It follows that $G\phi$ is nilpotent of class at most $c - 1$.

(e) *Let $|I| = n < \infty$ and let f_{nh} be the exponent of the h-th lower central factor of the free $\mathfrak{N}_c \cap \mathfrak{E}_q$-group of rank n. Then $G\phi$ is a free $\mathfrak{N}_c \cap \mathfrak{E}_q$-group if and only if $f_{nh} q_h \leq q$ for $2 \leq h \leq c$, and then it is free on $\{g_i\phi : i \in I\}$.*

Let $1 \leq h \leq c$. The natural map of G_0 onto $G\phi$, namely that given by $g_{0i} \mapsto g_i\phi$, induces a homomorphism of $\gamma^h(G_0/G_0^q)/\gamma^{h+1}(G_0/G_0^q)$ onto $\gamma^h(G\phi)/\gamma^{h+1}(G\phi)$. The latter, by (b), is homocyclic of exponent q/q_h (and rank $r(h)$). Thus $f_{nh} \geq q/q_h$ and the map is an isomorphism if and only if $f_{nh} = q/q_h$. Thus the given map of G_0 to $G\phi$ induces an isomorphism of G_0/G_0^q onto $G\phi$ if and only if $(G_0 : G_0^q) = |G\phi|$, which happens if and only if $f_{nh} q_h \leq q$ for $1 \leq h \leq c$. Finally $f_{n1} = q$ and $q_1 = 1$, so always $f_{n1} q_1 = q$. The claim follows.

(f) *If either $p > c$ or $c \leq 2$ or $c = 3 \neq p$ then $G\phi$ is a free $\mathfrak{N}_c \cap \mathfrak{E}_q$-group on $\{g_i\phi : i \in I\}$.*

If $p > c$ then $q_h = 1$ for $1 \leq h \leq c$ and always $f_{nh} \leq q$, so $f_{nh} q_h \leq q$. Suppose $c = 2$. If $p > 2$ then $p > c$ and we are in the previous case. Let $p = 2$. If x and y are elements of some $\mathfrak{N}_2 \cap \mathfrak{E}_q$-group H and if $z = [x, y]$, then $1 = (xy)^q = x^q y^q z^{q/2} = z^{q/2}$. Hence H' has

https://doi.org/10.1017/S0017089500030354 Published online by Cambridge University Press

exponent dividing 2^{e-1} and $f_{n2} \leq 2^{e-1}$. Clearly $q_2 = 2$ and hence $f_{n2}q_2 \leq q$. Now let $c = 3$. If $p > 3$ the first case applies, so again let $p = 2$. A simple induction yields that the exponents of the lower central factors of any group form a monotonic decreasing sequence. Consequently $f_{n3} \leq f_{n2} \leq 2^{e-1}$. Also $q_3 = 2$, so $f_{n3}q_3 \leq q$.

In view of (e) above this proves that $\langle g_k\phi : k \in K\rangle$ is a free $\mathfrak{N}_c \cap \mathfrak{E}_q$-group on the exhibited generators for every finite subset K of I and hence the claim (f) follows.

We have yet to construct any linear representations. The following completes the proof of the theorem.

(g) *Let F be a perfect field of characteristic p and transcendence degree at least $c\,|I|$. Then the groups G and $G\phi$ above have faithful linear representations of finite degree over F.*

There is a commutative ring J of characteristic q such that J/pJ is isomorphic to F, see [**5**, 2.9] for example. Pick in J a family $\Xi = \{\xi_{ij} \in J : i \in I;\ j = 1, 2, \ldots, c\}$ that, modulo pJ, is algebraically independent over the prime subfield. Then Ξ generates a subring of J isomorphic to the ring R above. Hence G and $G\phi$ are identified with subgroups of $\mathrm{GL}(c+1, J)$.

Now J is isomorphic to a ring of Witt vectors over F by [**5**, 4.7] and the latter has its operation $(+, -, .)$ given by polynomials over $\mathrm{GF}(p)$. Thus the matrix ring over J of degree $c+1$ can be identified with a $c(c+1)^2$-dimensional vector space over F such that the multiplication is given by polynomials over F (and such that the zero matrix is identified with the zero vector if we wish). Then $\mathrm{GL}(c+1, J)$, and hence also G and $G\phi$, embed into $\mathrm{GL}(n, F)$ for some integer n by [**5**, 5.2] (or by [**5**, 5.1] if you prefer).

REFERENCES

1. P. Hall, *The Edmonton Notes on Nilpotent Groups* (Queen Mary Coll. Maths. Notes, London 1969).

2. B. Huppert, *Endliche Gruppen I* (Springer-Verlag, Berlin etc. 1967).

3. F. Leinen, Hypercentral unipotent finitary skew linear groups, *Comm. Algebra* **22** (1994), 929–950.

4. B. A. F. Wehrfritz, *Infinite Linear Groups* (Springer-Verlag, Berlin etc. 1973).

5. B. A. F. Wehrfritz, *Lectures around Complete Local Rings* (Queen Mary Coll. Maths. Notes, London 1979).

SCHOOL OF MATHEMATICAL SCIENCES
QUEEN MARY AND WESTFIELD COLLEGE
MILE END ROAD
LONDON E1 4NS
ENGLAND