LIE REPRESENTATIONS AND GROUPS OF PRIME POWER ORDER

R. M. BRYANT AND L. G. KOVÁCS

1. *Automorphism Groups of p-Groups*

Let p be a prime, P a finite non-cyclic p-group and $\Phi(P)$ the Frattini subgroup of P. Then every automorphism $\theta: x \mapsto x\theta$ of P restricts to an automorphism $\bar{\theta}: x\Phi(P) \mapsto (x\theta)\Phi(P)$ of the factor group $P/\Phi(P)$, and the map $\theta \mapsto \bar{\theta}$ is a homomorphism from the automorphism group Aut P of P to the automorphism group of $P/\Phi(P)$. When $P/\Phi(P)$ is regarded as a vector space over the field of order p, the restriction of Aut P to $P/\Phi(P)$ is a group of linear transformations of this vector space. Our main result is to establish that every linear group arises in this way.

THEOREM 1. *For each linear group H of finite dimension d, with $d \geqslant 2$, over the field of order p there exists a finite p-group P such that the restriction of* Aut P *to $P/\Phi(P)$ is isomorphic, as linear group, to H.*

The authors are indebted to Dr. John Cossey and Dr. Hans Lausch for provoking this work by the comment that such a result, in conjunction with a recent paper **[8]** of Laue, Lausch and Pain, yields that if p and q are distinct primes then there is an extension of a finite p-group by a finite q-group which does not lie in the smallest normal Fitting class of finite soluble groups: this refutes Conjecture 2 of Cossey's survey **[3]**.

It should be acknowledged that an analogue of the above theorem, where the restriction of Aut P to the central factor group of P is prescribed as an abstract (rather than linear) group, was obtained by Heineken and Liebeck **[6]**.

Theorem 1 will be derived in this section from two other results, Theorem 2 and Theorem 3. Theorem 2 will be proved in §2 and Theorem 3 in §3.

Let K be a field and let A be the free associative K-algebra (with unity) on d generators $x_1, x_2, \ldots, x_d$ $(d \geqslant 2)$. Then A is the direct sum

$$A = \bigoplus_{i=0}^{\infty} A_i$$

where A_i is the homogeneous component of degree i. Now A carries the structure of a Lie algebra over K under the usual bracket multiplication: $[u, v] = uv - vu$. Let Λ be the Lie subalgebra generated by $x_1, \ldots, x_d$. As is well-known, Λ is actually a free Lie algebra on $x_1, \ldots, x_d$: see Theorem 5.9 of Magnus, Karrass and Solitar **[10]**. We have

$$\Lambda = \bigoplus_{i=1}^{\infty} \Lambda_i$$

where $\Lambda_i = \Lambda \cap A_i$. Note also that $\Lambda_1 = A_1$.

Received 12 September, 1977.

Let Σ be the general linear group of degree d over K. Thus Σ can be regarded as the group of K-automorphisms of A_1. Since A is freely generated by $x_1, \ldots, x_d$, the action of each element of Σ can be extended uniquely to an algebra automorphism of A. Thus Σ may be regarded as a group of automorphisms of A. Clearly the A_i and the Λ_i admit the action of Σ, so may be regarded as $K\Sigma$-modules. In fact, as $K\Sigma$-module, A_i is isomorphic to the tensor product of i copies of A_1.

Let G be a finite subgroup of Σ, let M be the subgroup of G consisting of the elements of G with scalar action on A_1, and write $m = |M|$. Then, in the present notation, Theorem 2 of [**1**] states that for all sufficiently large i the KG-module $A_i \oplus A_{i+1} \oplus \ldots \oplus A_{i+m-1}$ contains a regular KG-module. The first result needed for Theorem 1 above is a refinement of this.

THEOREM 2. *For all sufficiently large i the KG-module $\Lambda_i \oplus \Lambda_{i+1} \oplus \ldots \oplus \Lambda_{i+m-1}$ contains a regular KG-module.*

We shall apply Theorem 2 in the case where K is the field of order p and $G = \Sigma$. Here it may be used in conjunction with the fact that the modules Λ_i occur as sections of certain p-groups. An application of this sort has already been useful elsewhere: see Harris [**5**]. The second result needed for Theorem 1 above allows us to exploit the full force of Theorem 2 by establishing that the modules $\Lambda_i \oplus \ldots \oplus \Lambda_{i+m-1}$ occur as sections of certain p-groups.

Let F be a free group on d generators $y_1, \ldots, y_d$. Define $F_1 = F$ and, for $i \geqslant 1$, $F_{i+1} = F_i^p[F_i, F]$. Thus F_{i+1} is the smallest normal subgroup of F contained in F_i such that F_i/F_{i+1} has exponent p and is central in F/F_{i+1}. It is not difficult to verify that $[F_i, F_j] \leqslant F_{i+j}$ for all i, j. Note also that F/F_{i+1} is a finite p-group with $\Phi(F/F_{i+1}) = F_2/F_{i+1}$. In the above notation, taking K to be the field of order p, Σ may be regarded as the automorphism group of F/F_2. Of course, we choose the actions of Σ on A_1 and F/F_2 so that there is a $K\Sigma$-module isomorphism $\phi\colon F/F_2 \to A_1$ with $(y_j F_2)\phi = x_j$ $(1 \leqslant j \leqslant d)$.

Suppose $F_{i+1} \leqslant N \leqslant F_2$ where N is normal in F. Let θ be an automorphism of F/N. Then θ can be "lifted" to an automorphism θ^* of F/F_{i+1} such that N/F_{i+1} admits θ^* and θ^* acts as θ does on F/N. To prove this note that, since F is free, there is an endomorphism θ' of F such that $y_j\theta' \in (y_j N)\theta$ for all j. Hence $f\theta' \in (fN)\theta$ for all $f \in F$. It follows that N admits θ' and θ' acts as θ does on F/N. Now F_{i+1} is a fully-invariant subgroup of F. Hence θ' yields an endomorphism θ^* of F/F_{i+1}. Clearly N/F_{i+1} admits θ^* and θ^* acts as θ does on F/N. Since $N \leqslant F_2$, θ^* acts as an automorphism on the Frattini factor group of F/F_{i+1}. Thus θ^* is an automorphism.

Let $\alpha \in \Sigma$. Then α may be lifted to an automorphism α^* of F/F_{i+1}. It is straightforward to verify by induction on i that the action of α^* on F_i/F_{i+1} depends only on α and is independent of the choice involved in defining α^*. Hence F_i/F_{i+1} may be regarded as a $K\Sigma$-module. The second result needed for Theorem 1 is the following.

THEOREM 3. *F_i/F_{i+1} has a submodule isomorphic to $\Lambda_2 \oplus \ldots \oplus \Lambda_i$.*

We can now derive Theorem 1. By Theorems 2 and 3 we can choose i so that $i \geqslant 2$ and F_i/F_{i+1} contains a regular $K\Sigma$-module. Write $P^* = F/F_{i+1}$ and $W = F_i/F_{i+1}$. Thus W contains a regular $K\Sigma$-module. Let w be a generator for this regular $K\Sigma$-module.

Let H be a subgroup of Σ and let W_H denote the KH-submodule of W generated by w. Then, for all $\alpha \in \Sigma \setminus H$, W_H does not admit α. Let $P = P^*/W_H$. We shall identify $P^*/\Phi(P^*)$, $P/\Phi(P)$ and F/F_2 in the obvious way.

To show that P has the property described in Theorem 1, let θ be any automorphism of P. Then θ may be lifted to an automorphism θ^* of P^* such that W_H admits θ^* and θ^* acts as θ does on P. Let α be the element of Σ obtained by restriction of θ^* to $P/\Phi(P)$. Then W_H admits α, since it admits θ^*. Thus $\alpha \in H$.

Conversely, let $\beta \in H$ and let β^* be an automorphism of P^* which acts on $P^*/\Phi(P^*)$ as β does. Then β^* acts on W as β does. Thus W_H admits β^*. Thus β^* yields an automorphism of P whose restriction to $P/\Phi(P)$ is equal to β.

Thus the restriction of Aut P to $P/\Phi(P)$ is equal to H, as required.

2. *Lie Representations*

In this section we prove Theorem 2. But first we make some preliminary observations about field extensions. Let K be a field, L an extension field of K, and G a finite group. Let U and V be finite-dimensional KG-modules and let U^L and V^L be the LG-modules $U \otimes_K L$ and $V \otimes_K L$, respectively.

LEMMA 1. *If U^L and V^L have a common non-zero direct summand then U and V have a common non-zero direct summand.*

This is result (2.18) of [**2**].

COROLLARY 1. *If U^L is a direct summand of V^L then U is a direct summand of V.*

Proof. We can write $U = W \oplus U_1$ and $V = W \oplus V_1$ where U_1 and V_1 have no common non-zero direct summand. If U^L is a direct summand of V^L it follows by the Krull–Schmidt Theorem that ${U_1}^L$ is isomorphic to a direct summand of ${V_1}^L$. Hence ${U_1}^L$ is zero, by Lemma 1. Hence U_1 is zero and U is a direct summand of V.

COROLLARY 2. *If V^L contains a regular LG-module then V contains a regular KG-module.*

Proof. Since the regular LG-module is injective the hypothesis is equivalent to the regular LG-module being a direct summand of V^L. But the regular LG-module has the form U^L where U is a regular KG-module. Thus the result follows from Corollary 1.

We now prove Theorem 2 using the notation introduced in §1. In particular, K is a field and G is a finite group of K-automorphisms of A_1. To put this last statement another way, A_1 is a KG-module on which G acts faithfully. The associative algebra A acquires a KG-module structure, as described in §1. M is the subgroup of G consisting of the elements with scalar action on A_1, and $m = |M|$.

Suppose L is an extension field of K. Then $A \otimes_K L$ is the free associative L-algebra generated by $x_1 \otimes 1, \ldots, x_d \otimes 1$. The homogeneous component of degree i is $A_i \otimes L$ and the Lie subalgebra generated by $x_1 \otimes 1, \ldots, x_d \otimes 1$ is $\Lambda \otimes L$, with $\Lambda_i \otimes L$ as homogeneous component of degree i. Also, $A_1 \otimes L$ is an LG-module on which G acts faithfully, with M as the subgroup of G consisting of the elements with scalar action. The LG-module structure of $A \otimes L$ defined via algebra automorphisms from

$A_1 \otimes L$ is identical with the LG-module structure of $A \otimes L$ derived from the KG-module structure of A. If $(\Lambda_i \otimes L) \oplus \ldots \oplus (\Lambda_{i+m-1} \otimes L)$ contains a regular LG-module then Corollary 2 shows that $\Lambda_i \oplus \ldots \oplus \Lambda_{i+m-1}$ contains a regular KG-module. Thus it is enough to prove Theorem 2 for the field L. Consequently it is enough to prove Theorem 2 with the additional assumption that K is infinite. We make this assumption henceforth. It allows us to prove the following lemma.

LEMMA 2. *There is an element v of A_1 such that v and $v\alpha$ are linearly independent for all $\alpha \in G \setminus M$.*

Proof. Let $\alpha \in G \setminus M$. Then the eigenspaces of α in A_1, of which there are at most d, are all proper subspaces of A_1. Since G is finite, the eigenspaces of elements of $G \setminus M$ form a finite collection of proper subspaces of A_1. But, since K is infinite, A_1 is not the set-theoretic union of any finite collection of proper subspaces: this is easily proved by induction on d. A non-zero element v of A_1 which is not in any of the above eigenspaces has the required properties.

Now M is a cyclic central subgroup of G. Let σ be a generator of M. Then σ acts like a scalar ξ on A_1, where ξ is a primitive mth root of unity in K. Let T be a set of coset representatives for M in G, where $1 \in T$.

Let U be a regular KM-module. Then $U = U_0 \oplus \ldots \oplus U_{m-1}$ where U_i is a 1-dimensional KM-module on which σ acts as the scalar ξ^i $(0 \leqslant i < m)$. Let U^G denote the KG-module induced from U. Then U^G is a regular KG-module and we have $U^G = U_0{}^G \oplus \ldots \oplus U_{m-1}^G$. Now σ acts as the scalar ξ^i on $U_i{}^G$. Also $U_i{}^G$ contains an element u_i such that $\{u_i\tau : \tau \in T\}$ is a basis for $U_i{}^G$. These two facts serve to characterise $U_i{}^G$ as a KG-module.

If $k \equiv i \pmod{m}$ where $0 \leqslant i < m$ then σ acts like the scalar ξ^i on A_k. The proof will be completed by showing that, for large enough k, with $k \equiv i \pmod{m}$, Λ_k contains a submodule isomorphic to $U_i{}^G$. This will be done by showing that Λ_k contains an element u such that $\{u\tau : \tau \in T\}$ is linearly independent. It is enough to find an element u which does not belong to the subspace $\langle u\tau : \tau \in T \setminus \{1\}\rangle$, because this implies $u\tau' \notin \langle u\tau : \tau \in T \setminus \{\tau'\}\rangle$ for all $\tau' \in T$.

The result is clear if $|T| = 1$, so we assume that $|T| \geqslant 2$.

Let v be chosen as in Lemma 2, and let w be any element of A_1 such that v and w are linearly independent. Let $\tau_1, \ldots, \tau_n$ be the non-identity elements of T. Then for each j $(1 \leqslant j \leqslant n)$ there is a vector space decomposition $A_1 = X_j \oplus Y_j$ where $v \in X_j$ and $v\tau_j \in Y_j$.

Let $k \geqslant 3n$. Then regarding A_k as the tensor product of k copies of A_1 we can write A_k in the form

$$(X_1 \oplus Y_1) \otimes (X_1 \oplus Y_1) \otimes (X_1 \oplus Y_1) \otimes (X_2 \oplus Y_2) \otimes (X_2 \oplus Y_2) \otimes (X_2 \oplus Y_2) \otimes \\ \ldots \otimes (X_n \oplus Y_n) \otimes (X_n \oplus Y_n) \otimes (X_n \oplus Y_n) \otimes A_1 \otimes \ldots \otimes A_1.$$

Thus A_k is the direct sum of a certain collection of subspaces of the form

$$Z_1 \otimes \ldots \otimes Z_{3n} \otimes A_1 \otimes \ldots \otimes A_1$$

where each factor Z_i is equal to some X_j or some Y_j. Let B be the sum of those subspaces in the collection with at most one factor Z_i belonging to $\{Y_1, \ldots, Y_n\}$ and let C be the sum of those subspaces with at least two factors Z_i belonging to $\{Y_1, \ldots, Y_n\}$. Thus $A_k = B \oplus C$.

Consider the element u of A_k given by the left-normed product $[w, v, v, \ldots, v]$ with $k-1$ copies of v. It is easy to verify that

$$u = \sum_{s=0}^{k-1} \binom{k-1}{s} (-1)^s v^s w v^{k-1-s}.$$

Since v and w are linearly independent they are part of a free generating set for A. Hence u is a non-zero element of Λ_k. Clearly u belongs to B. Thus u does not belong to C. But, for all j,

$$u\tau_j = \sum_{s=0}^{k-1} \binom{k-1}{s} (-1)^s (v\tau_j)^s (w\tau_j)(v\tau_j)^{k-1-s}.$$

In each summand at least two of the factors $v\tau_j$ occur in positions where we have used $X_j \oplus Y_j$ in place of A_1. Thus, for all j, $u\tau_j \in C$. Hence $u \notin \langle u\tau_1, \ldots, u\tau_n \rangle$. This completes the proof of Theorem 2.

By additional argument it is possible to deduce the following more general result. *Let t be a positive integer. Then for all sufficiently large i the KG-module $\Lambda_i \oplus \ldots \oplus \Lambda_{i+m-1}$ contains a free KG-module of rank t.* We now sketch an alternative proof of this generalisation.

Of the two proofs, the one we have already described is more attractive in the special case of Theorem 2 and gives a better lower bound for i. But the proof which follows has the advantage of establishing the generalisation directly.

Let $n = [G:M]-1$ and write $B = A_n \oplus \ldots \oplus A_{n+m-1}$. Then Theorem 2 of **[1]** shows that B contains a regular KG-module. Hence, for any finite-dimensional KG-module U, $B \otimes U$ contains a free KG-module of rank equal to the dimension of U: this follows from Lemma 60.2(i) of Dornhoff **[4]** because free KG-modules are induced from the identity subgroup.

For each positive integer i there is a KG-homomorphism from $\Lambda_i \otimes A_1$ to Λ_{i+1} in which $u \otimes v \mapsto [u, v]$ for all $u \in \Lambda_i$, $v \in A_1$. This homomorphism is easily seen to be onto: for example, by use of Exercise 5.4.18 of **[10]**. Hence for any positive integer j there exists a KG-homomorphism from $\Lambda_i \otimes A_j$ onto Λ_{i+j}. Hence there exists a KG-homomorphism ψ_i from $B \otimes \Lambda_i$ onto $\Lambda_{n+i} \oplus \ldots \oplus \Lambda_{n+m-1+i}$. Using Witt's formula (Theorem 5.11 of **[10]**) for the dimension λ_r of Λ_r, the dimension d_i of the kernel of ψ_i may be calculated. (In fact all that is needed is an estimate for d_i based on the estimate

$$\frac{1}{r} d^r - d^{r/2} < \lambda_r < \frac{1}{r} d^r + d^{r/2}$$

for λ_r.) Now, by the remarks above, $B \otimes \Lambda_i$ contains a free KG-module of rank λ_i. It may be verified that, for all large enough i, $\lambda_i \geqslant (d_i+1)t$. Hence $B \otimes \Lambda_i$ contains a free KG-module of rank t which has zero intersection with the kernel of ψ_i. It follows that $\Lambda_{n+i} \oplus \ldots \oplus \Lambda_{n+m-1+i}$ contains a free KG-module of rank t.

3. *The Modules F_i/F_{i+1}*

In this section we shall prove Theorem 3 by determining the structure of the $K\Sigma$-modules F_i/F_{i+1}: here K is the field of order p. What we need is essentially contained in the literature, but unfortunately not in a very convenient form. Skopin's papers [11] and [12] cover the case where p is odd. Lazard [9] treats the general case but omits some of the details, especially in the case $p = 2$. Koch [7] also treats the general case but seems to be partly in error: see below. We have considered it most satisfactory to run through the arguments again in broad terms, adding some details which are not readily accessible in the above papers.

Let Γ be the power series ring in non-commuting variables $z_1, z_2, \ldots, z_d$. Then, by means of the Magnus embedding, F may be regarded as a subgroup of the group of units of Γ, where $y_j = 1+z_j$ $(1 \leqslant j \leqslant d)$: see §5.5 of [10].

Let D be the ideal of Γ consisting of those elements with constant term divisible by p. Then, as proved in [7] (and also, implicitly, in [9]),

$$F_i = F \cap (1+D^i)$$

for all i. (The proof of this shows incidentally that

$$F_i = (\gamma_1 F)^{p^{i-1}} (\gamma_2 F)^{p^{i-2}} \ldots (\gamma_i F)$$

where $\gamma_r F$ is the rth term of the lower central series of F.) It follows easily that there is a group embedding of F_i/F_{i+1} into D^i/D^{i+1} given by

$$f_i F_{i+1} \mapsto (f_i - 1) + D^{i+1}$$

for all $f_i \in F_i$.

Using the notation introduced before in which A refers to the free d-generator associative K-algebra, there is an obvious isomorphism

$$D^i/D^{i+1} \cong A_0 \oplus A_1 \oplus \ldots \oplus A_i.$$

Hence for each i we obtain a group embedding

$$\tilde{\phi}_i\colon\ F_i/F_{i+1} \to A_0 \oplus A_1 \oplus \ldots \oplus A_i.$$

Detailed information concerning the embeddings $\tilde{\phi}_i$ is more easily stated in terms of the associated group homomorphisms

$$\phi_i\colon F_i \to A_0 \oplus A_1 \oplus \ldots \oplus A_i.$$

For the case of p odd calculations show

$$y_j \phi_1 = x_j \ (1 \leqslant j \leqslant d),$$

$$f_i^p \phi_{i+1} = f_i \phi_i \quad \text{for all} \quad f_i \in F_i,$$

and $$[f_i, f_1]\phi_{i+1} = [f_i \phi_i, f_1 \phi_1] \quad \text{for all} \quad f_i \in F_i, f_1 \in F_1.$$

These are given on p. 139 of [9]. For $p = 2$ the only difference is that the condition $f_1{}^2 \phi_2 = f_1 \phi_1$ for all $f_1 \in F_1$ must be replaced by

$$f_1{}^2 \phi_2 = f_1 \phi_1 + (f_1 \phi_1)^2 \quad \text{for all} \quad f_1 \in F_1.$$

These conditions give an inductive description of the homomorphisms ϕ_i. For all $\alpha \in \Sigma$ an easy induction on i shows that the homomorphisms

$$\alpha^{-1} \tilde{\phi}_i \alpha\colon F_i/F_{i+1} \to A_0 \oplus A_1 \oplus \ldots \oplus A_i$$

satisfy $\alpha^{-1} \tilde{\phi}_i \alpha = \tilde{\phi}_i$. Thus the $\tilde{\phi}_i$ are $K\Sigma$-module embeddings.

For the case of p odd the image of $\tilde{\phi}_i$ is easily calculated to be $\Lambda_1 \oplus \ldots \oplus \Lambda_i$, as remarked by Skopin and Lazard. Thus

$$F_i/F_{i+1} \cong \Lambda_1 \oplus \ldots \oplus \Lambda_i$$

as $K\Sigma$-module.

For the case of $p = 2$ the calculation is slightly more complicated. The image of $\tilde{\phi}_1$ is Λ_1. The image E of $\tilde{\phi}_2$ satisfies

$$E + A_2 = A_1 \oplus A_2 \quad \text{and} \quad E \cap A_2 = \Lambda_2,$$

so E is an extension of Λ_2 by Λ_1. For $i \geqslant 3$ the image of $\tilde{\phi}_i$ is $E \oplus \Lambda_3 \oplus \ldots \oplus \Lambda_i$. Thus F_i/F_{i+1} is, in all cases, an extension of $\Lambda_2 \oplus \ldots \oplus \Lambda_i$ by Λ_1. This completes the proof of Theorem 3.

Koch's statement in [7] that, for all p, F_i/F_{i+1} is canonically isomorphic to $\Lambda_1 \oplus \Lambda_2 \oplus \ldots \oplus \Lambda_i$ seems to be false because direct calculation shows that when $p = 2$ and $d = 3$ the extension E referred to above does not split.

References

1. R. M. Bryant and L. G. Kovács, " Tensor products of representations of finite groups ", *Bull. London Math. Soc.*, 4 (1972), 133–135.
2. R. M. Bryant and L. G. Kovács, " The skeleton of a variety of groups ", *Bull. Austral. Math. Soc.*, 6 (1972), 357–378.
3. J. Cossey, " Classes of finite soluble groups ", Proceedings of the Second International Conference on the Theory of Groups (Canberra, 1973), *Lecture Notes in Mathematics* (Springer–Verlag) No. 372 (1974), 226–237.
4. L. Dornhoff, *Group Representation Theory* (Marcel Dekker, New York, 1971).
5. L. F. Harris, *Varieties and Section Closed Classes of Groups* Ph.D. thesis (Australian National University, 1973).
6. H. Heineken and H. Liebeck, " The occurrence of finite groups in the automorphism group of nilpotent groups of class 2 ", *Arch. der Math.*, 25 (1974), 8–16.
7. H. Koch, " Über die Faktorgruppen einer absteigenden Zentralreihe ", *Math. Nachr.*, 22 (1960) 159–161.
8. H. Laue, H. Lausch and G. R. Pain, " Verlagerung und normale Fittingklassen endlicher Gruppen ", *Math. Z.*, 154 (1977), 257–260.
9. M. Lazard, " Sur les groupes nilpotents et les anneaux de Lie ", *Ann. Sci. École Norm. Sup.* (3), 71 (1954), 101–190.
10. W. Magnus, A. Karrass and D. Solitar, *Combinatorial Group Theory* (Interscience, New York, 1966).
11. A. I. Skopin, " The factor groups of an upper central series of free groups " (Russian), *Dokl. Akad. Nauk SSSR*, 74 (1950), 425–428.
12. A. I. Skopin, " Ideal of relations ", *Trudy Mat. Inst. Steklov.*, 80 (1965), 117–128.

Department of Mathematics,
University of Manchester,
Institute of Science and Technology,
Manchester, M60 1QD,
England.

Department of Mathematics,
Institute of Advanced Studies,
Australian National University,
Canberra, ACT 2600,
Australia.