PROC. 18th SRI
CANBERRA 1978, 205-229.

20E10
(20C30)

VARIETIES OF NILPOTENT GROUPS OF SMALL CLASS

L.G. Kovács

1. Introduction

In the dreamtime of the theory of varieties of groups, one might have hoped for the individual knowledge of each variety: for a classification in the strongest sense. The extent to which such hopes have been realized is a remarkable achievement of the subject. R.A. Bryce [7], [8] knows each variety of metabelian groups 'modulo the nilpotent case'. The classification of varieties of nilpotent groups 'of small class' is the subject of this report. Our knowledge in this area comes essentially from Graham Higman's 1965 lecture [12], given to an international conference held here, which dealt with varieties of nilpotent groups of prime exponent p and class less than p. In 1968, M.F. Newman and I presented (in a course of lectures at this University) an extended version of this theory, for varieties of p-power exponent and class less than p, and also for 'torsionfree' nilpotent varieties of arbitrary class. (Our treatment was clumsy, and remained unwritten, but considerable further work is on record in Paul Pentony's thesis [23].) A 1971 paper [14] by A.A. Kljačko (in an extremely inaccessible publication) described yet another version for the case of p-power exponent (and class less than p), apparently independently of Higman's work.

One remarkable aspect of Kljačko's paper was the application of this method to derive information also about certain varieties of p-groups of class *not* less than p. Namely, he established the following

DISTRIBUTIVITY THEOREM. *The lattice of varieties of p-power exponent and class at most c is distributive if and only if $c \leq 3$, or $c = 4$ and $p > 2$, or $c = 5$ and $p > 5$.*

In fact, it was precisely the cases of $c = 4$, $p = 3$ and $c = 5$, $p = 5$ which were still outstanding then. (I must confess that I still can not handle the case $c = 4$, $p = 3$ by this method: Kljačko's paper suppressed the details. I have used *ad hoc* arguments to classify all 3-power exponent varieties of class 4 [unpublished], and found their lattice distributive, in agreement with Kljačko's claim.)

I refer to 'method' with good reason. The situation is so complex that only some qualitative aspect of it can be expressed in any single statement (for example, in the Distributivity Theorem above). On the other hand, while the problem of classifying all nilpotent varieties is theoretically solvable (in an algorithmic sense)*, the approach elucidated by Higman yields a significantly more efficient solution in the small class case, and indeed enables one to prove general statements (instead of having to be content with the knowledge that the proposition at hand is 'decidable'). By general statement I mean not only the Distributivity Theorem, which could be regarded as a case where the decision algorithm fortuitously terminated before we ran out of time: I mean also results like A.G.R. Stewart's theorem [25] that for each c (at least 4) there exist precisely two join-irreducible center-by-metabelian varieties of exponent p and class c (provided $p > c$), or the fact that the variety $\underline{\underline{N}}_c$ of all nilpotent groups of class at most c is generated by $(c-1)$-generator groups but not by $(c-2)$-generator groups (Kovács, Newman, Pentony [16]; see also Levin [18]).

The aim of these lectures is to make 'the method' more accessible. Higman's original [12] is terse to the point of being quite a challenge to read; as a record of a single lecture, it is really just an outline, virtually without proofs, attributions, or references: also, restriction to prime exponent seems worth avoiding today. Nevertheless, it is so rich that I can not cover half his material: I hope the reader will be encouraged, and better prepared, to sample his feast further. Kljačko's [14] is also on the terse side, and as far as I know can not be found in our libraries.

Inevitably, this report will also fail to be self-contained, and there will be many a point where I will wish I had a (better) reference: still, I hope to account for all omissions of non-routine arguments. Instead of attempting to formalize 'the method', I aim to prove two results. One is the Distributivity Theorem (except for

---

* Set one machine to enumerate laws and their consequences: if u is a consequence of v, this will be shown in a finite time. Set another to enumerate finite nilpotent groups and test them for laws: if u is not a consequence of v, a group will turn up to demonstrate this. This does it, for each nilpotent variety is generated by finite groups and definable by a single law.

the case $c = 4$, $p = 3$). The other is also in Kljačko's [14]. For each prime p and positive integer m, let A_p^m denote the dual of the lattice of all subgroups of p-power index in a free abelian group of rank m.

CLASSIFICATION THEOREM. *For $c < p$, the lattice of all varieties of nilpotent groups of p-power exponent and class at most c, is a subdirect product of c lattices, each of which is the direct product of the lattices $A_p^{l(\pi)}$ where π runs through a suitable index set. The index sets and the integers $l(\pi)$ are independent of p* (and will be made explicit in Section 6).

The name 'Classification Theorem' sounds too pretentious for such a result; I use it to suggest that its proof is constructive and would enable us, if we wished, to attach convenient labels to the varieties in question, labels from which one can instantly read off at least some of the most important relationships between these varieties. Unfortunately, I must also acknowledge the incomplete nature of the theorem. For, the phrase 'a subdirect product' hides *the first important open problem* of small class theory: just which subdirect product is it? Thus we do not know precisely which of the available labels would be used. (In the equivalent language of subgroups of free groups: the trouble is that 'the method' only deals conclusively with fully invariant subgroups which lie between successive terms of the lower central series.)

I shall also prove the torsionfree analogues of the two theorems. A variety is called *torsionfree* if it is generated by its torsionfree groups; equivalently, if its free groups are torsionfree. With respect to partial order by set-theoretic inclusion, these varieties form a lattice (which is *not* a sublattice of the lattice of all varieties, for the meet is now the variety generated by the torsionfree groups in the intersection and so can be smaller than the intersection). *The lattice of all torsionfree varieties of nilpotent groups of class at most c is distributive if and only if $c \leq 5$. The Classification Theorem* has the same form as before, with the same index sets and parameters $l(\pi)$, and without any restriction on c; the only change is that A_p^m is replaced by the subspace lattice A_0^m of an m-dimensional rational vector space.

The general case may now be approached as follows. If $\underline{\underline{V}}$ is any variety, it has a well-defined torsionfree core: the variety $\underline{\underline{V}}_0$ generated by the torsionfree groups of $\underline{\underline{V}}$. If $\underline{\underline{V}}$ is nilpotent, it is the join of $\underline{\underline{V}}_0$ and certain varieties $\underline{\underline{V}}_p$, one for each prime p from a finite set, each $\underline{\underline{V}}_p$ of p-power exponent. In a sense, this reduces the study of nilpotent varieties to the torsionfree and prime-power-exponent cases. Of course, when $\underline{\underline{V}}_0$ is trivial, the $\underline{\underline{V}}_p$ are uniquely determined by $\underline{\underline{V}}$ and the reduction is as good as one might wish. However, when $\underline{\underline{V}}_0$ is nonabelian, it does happen that the $\underline{\underline{V}}_p$ are not determined by $\underline{\underline{V}}$, not even if we insist that they be chosen as small as possible and only primes greater than the class of $\underline{\underline{V}}$ occur. The resolution of this difficulty is *the second important open problem* of small class theory.

To conclude this introduction on a more cheerful note, let me draw attention to the unrecorded fact that the torsionfree Classification Theorem leads, via the work of Stewart (*loc. cit*), to such specific results as the following. There are precisely 39 torsionfree varieties of class at most 5 (only one, namely the variety $\underline{\underline{N}}_5 \wedge \underline{\underline{A}}^2$ of all metabelian varieties of class at most 5, failing to lie in, or between successive terms of, the sequence $\underline{\underline{E}}, \underline{\underline{A}}, \underline{\underline{N}}_2, \underline{\underline{N}}_3, \underline{\underline{N}}_4, \underline{\underline{N}}_5$: it is to establish this that Stewart's work is needed here); but there exist infinitely many torsionfree varieties of class 6.

The next six sections contain the technicalities; classification first, distributivity last. Finally, in a postscript I comment on the earlier history of the key ideas. Some of those comments are based on references (included in the list at the end) which only came to my attention after the end of the Institute.

2. Subdirect decompositions

Let F be a noncyclic free group; for convenience, take it to have finite rank (the whole argument would remain valid *mutatis mutandis* without this restriction), and let Y be a free generating set of F. Write the lower central series of F as

$$F = \underline{\underline{N}}_0(F) > F' = \underline{\underline{N}}_1(F) > \dots > \underline{\underline{N}}_c(F) > \dots :$$

thus $\underline{\underline{N}}_c(F)$ is the verbal subgroup of F corresponding to the variety $\underline{\underline{N}}_c$ of all nilpotent groups of class (at most) c. As is well known (*cf.* 34.13 in Hanna Neumann's book [22]), if the rank of F is at least c then the lattice of subvarieties of $\underline{\underline{N}}_c$ is dual to the (modular) lattice N_c of fully invariant subgroups of F containing $\underline{\underline{N}}_c(F)$. In this duality, torsionfree subvarieties of $\underline{\underline{N}}_c$ correspond to isolated fully invariant subgroups of F (that is, subgroups U with F/U torsionfree). These subgroups form a lattice N_c^0, in which meet is set intersection and the join $U \vee V$ is obtained by taking $(U \vee V)/UV$ to be the subgroup of F/UV consisting of the elements of finite order (thus N_c^0 is not a sublattice of N_c). It is easy to prove that N_c^0 is modular. For a fixed prime p, the p-power exponent subvarieties of $\underline{\underline{N}}_c$ correspond to fully invariant subgroups of p-power index in F : these form a sublattice N_c^p of N_c. Our subject is therefore the study of the N_c^p and N_c^0. (These lattices do vary with the rank of F when that rank is small, but this dependence will not effect our arguments until the last moment, so for the time being we may ignore it.)

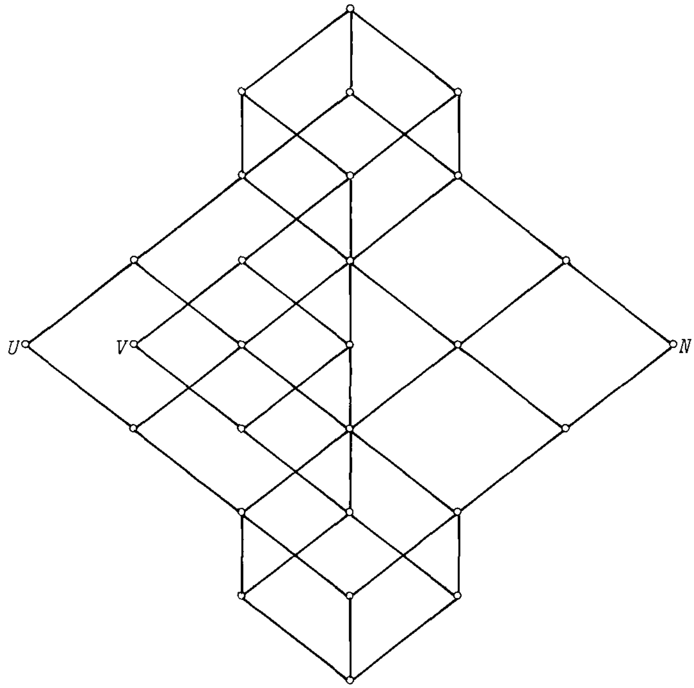
The aim of this section is the following reduction of the problem. Let L_c^0 denote the sublattice $\left\{U \in N_c^0 \;\middle|\; U \le \underline{\underline{N}}_{c-1}(F)\right\}$ of N_c^0, and L_c^p the sublattice

$$\{U \in N_c \mid U \le \underline{\underline{N}}_{c-1}(F) \text{ and } |\underline{\underline{N}}_{c-1}(F)/U| \text{ is a power of } p\}$$

of N_c (so L_c^p avoids N_c^p except when $c = 1$). We shall prove that, for $c > 1$, *N_c^0 is always a subdirect product of N_{c-1}^0 and L_c^0, and N_c^p is a subdirect product of N_{c-1}^p and L_c^p provided $c \le p+1$.* Beyond this section, our time will be devoted to the analysis of the L_c^p and L_c^0, for this reduction (and induction on c) will have established that *N_c^p and N_c^0 are subdirect products of the L_i^p and the L_i (with $1 \le i \le c$), respectively.*

Some more comments before we embark on the proof. This reduction is in effect contained in Kljačko's paper [14] for N_c^p and $c < p$ provided F has sufficiently large rank. Our proof needs no restriction on the rank of F. For the Classification Theorem only the case $c < p$ is relevant, and for that the proof we are about to see is really easy. The negative parts of the Distributivity Theorem could be reached via a much simpler version of the reduction, but I can not imagine how the positive part for N_4^3 could be reached by 'the method' without the relevant reduction. The present version of the reduction goes just about as far as possible: when the rank of F is 2, N_4^2 is not a subdirect product of N_3^2 and L_4^2, for the latter are distributive but N_4^2 is not. (In fact, Bryce had shown, in the footnote of page 335 in [7], that N_{p+2}^p is never distributive.)

For the proof, let us write N for $\underline{\underline{N}}_{c-1}(F)$. The key fact is that if $U, V \in N_c^p$ (or N_c^0) then the sublattice of N_c^p (or of N_c^0) generated by U, V, and N, is distributive: assume this for the moment. Then $U \mapsto U \vee N$ and $U \mapsto U \wedge N$ are lattice homomorphisms of N_c^p (or N_c^0) onto N_{c-1}^p (or N_{c-1}^0) and L_c^p (or L_c^0), respectively. The only nontrivial part of this claim is that $N_c^p \to L_c^p$ is onto. To see this, take any W in L_c^p and consider F/W; this is a finitely generated nilpotent group in which the elements of finite order form a finite p-group, namely N/W. Thus F/W is residually a finite p-group (Gruenberg [11], Theorem 2.1 (ii)) and so has a normal subgroup H/W of p-power index which avoids N/W. Take U to be the verbal subgroup of F corresponding to the variety generated by F/H : then $U \in N_c^p$ and $U \wedge N = W$. The subdirect decompositions now follow from the fact that $U \vee N = V \vee N$ and $U \wedge N = V \wedge N$ imply that $U = V$, this implication being valid in every distributive lattice. Instead of memorizing lots of simple results and scattered references, I prefer to keep handy the diagram of the free modular lattice on three generators from which all such claims are easily read off (or disproved):



This picture will also start us on our way to deriving a contradiction in case the lattice generated by U, V, and N, is not distributive. Recall that two intervals (pairs of comparable elements), say, $U_1 < U_2$ and $V_1 < V_2$, of a lattice are called perspective if $U_1 = U_2 \wedge V_1$ and $U_2 \vee V_1 = V_2$. Projectivity is then the smallest equivalence relation on the set of all intervals of the lattice such that perspective intervals are projective. If $U_1 < U_2$ and $V_1 < V_2$ are perspective in N_c then by an isomorphism theorem U_2/U_1 and V_2/V_1 are (End F)-isomorphic; if they are perspective in N_c^0 then a finite-index subgroup of U_2/U_1 is (End F)-isomorphic to some finite-index subgroup of V_2/V_1. In these two observations the conclusions are in terms of equivalence relations, hence in the hypotheses perspectivity may be replaced by projectivity. What we need from these comments and the diagram above is that if U, V, N generate a nondistributive sublattice in N_c (or in N_c^0) then $N/\underline{\underline{N}}_c(F)$ and F/N must have (abelian) nontrivial (End F)-isomorphic sections: namely,

$$\frac{(U\vee V)\wedge N}{(U\wedge N)\vee(V\wedge N)} \text{ and } \frac{(U\vee N)\wedge(V\vee N)}{(U\wedge V)\vee N}$$

(which are p-groups) if we are in N_c, or finite-index (torsionfree) subgroups of these if we are in N_c^0.

The next step is to 'refine' this section of F/N according to the lower central series of F/N. This is routine group theory and I omit the details. The conclusion is that, for some i (with $1 \le i < c$), $N/\underline{\underline{N}}_c(F)$ and $\underline{\underline{N}}_{i-1}(F)/\underline{\underline{N}}_i(F)$ have nontrivial (End F)-isomorphic sections which are p-groups if we started in N_c^p and torsionfree if in N_c^0.

At this point, elementary commutator calculus enters the argument. For each positive integer n, consider the endomorphism of F which is defined by $y \mapsto y^n$ for all y in the free generating set Y of F. Induction on j readily yields that this acts as $w \mapsto w^{n^j}$ on every element of (every section of) $\underline{\underline{N}}_{j-1}(F)/\underline{\underline{N}}_j(F)$. The result of the previous paragraph then implies that $n^i \equiv n^c \pmod p$ if we started in N_c^p, or $n^i = n^c$ if in N_c^0, for all n. In the latter case we have the desired contradiction; in the former, only two possibilities remain: either $i = 1$ and $c = p$, or $i = 2$ and $c = p+1$.

To eliminate the first, consider an endomorphism of F which leaves one element of Y fixed and takes all others to 1. This endomorphism annihilates F' and hence every section of $N/\underline{\underline{N}}_c(F)$; on the other hand we know all fully invariant subgroups of F containing F' and can see that this endomorphism does not annihilate any nontrivial (End F)-admissible section of F/F'.

It is much harder to deal with the second case. Let U_1, U_2, V_1, V_2 be fully invariant subgroups of F such that $\underline{\underline{N}}_2(F) < U_1 < U_2 \le F'$ and $\underline{\underline{N}}_{p+1}(F) < V_1 < V_2 \le \underline{\underline{N}}_p(F)$ while U_2/U_1 and V_2/V_1 are (End F)-isomorphic p-groups: we may as well take these sections to have exponent p. Let G be the subgroup of F generated by any two elements of Y; embed End G in End F by letting every endomorphism of G map all elements of Y outside G to 1, and denote by ε the identity of End G. Then $(U_2/U_1)\varepsilon$ is $(U_2 \cap G)U_1/U_1$ which is (End G)-isomorphic to $(U_2 \cap G)/(U_1 \cap G)$; also $(U_2/U_1)\varepsilon$ is (End G)-isomorphic to $(V_2/V_1)\varepsilon$; so $(U_2 \cap G)/(U_1 \cap G)$ and $(V_2 \cap G)/(V_1 \cap G)$ are (End G)-isomorphic groups of exponent (dividing) p. All fully invariant subgroups of F between F' and $\underline{\underline{N}}_2(F)$ are known: $U_2 = \underline{\underline{B}}_k(F')\underline{\underline{N}}_2(F)$ and $U_1 = \underline{\underline{B}}_{kp}(F')\underline{\underline{N}}_2(F)$ for some k, and so $U_2 \cap G > U_1 \cap G$. (Reminder: $\underline{\underline{B}}_n$ is the variety of all groups of exponent dividing n.) Thus G inherits all the information we need about F and we could work on in G. To simplify notation, we forget G and assume instead that $|Y| = 2$; say, $Y = \{y_1, y_2\}$.

It is time for more commutator calculus. For each positive integer n, we consider the endomorphism of F defined by $y_1 \mapsto y_1^n$, $y_2 \mapsto y_2$. On the cyclic quotient $F'/\underline{\underline{N}}_2(F)$, and hence also on the quotient U_2/U_1 of order p, this endomorphism acts as $u \mapsto u^n$, thus it must act the same way on V_2/V_1. The quotient $\underline{\underline{N}}_p(F)/\underline{\underline{N}}_{p+1}(F)$ has a basis (as free abelian group) consisting of the cosets of the basic commutators of total weight $p+1$ in y_1 and y_2. On the coset b of a basic commutator of weight k in y_1 and $p+1-k$ in y_2, the endomorphism acts as $b \mapsto b^{n^k}$. If V_2/V_1 were (End F)-isomorphic to some section of $[F'' \cap \underline{\underline{N}}_p(F)]\underline{\underline{N}}_{p+1}(F)/\underline{\underline{N}}_{p+1}(F)$, one could exploit the fact that the latter is generated by the cosets of the non-left-normed basic commutators of weight $p+1$, whose weight k in y_1 satisfies $2 \le k \le p-1$, and derive that $n \equiv n^k \pmod p$ for some such k and all n, which is clearly impossible. The alternative is that V_2/V_1 is (End F)-isomorphic to a section of $\underline{\underline{N}}_p(F)/[F'' \cap \underline{\underline{N}}_p(F)]\underline{\underline{N}}_{p+1}(F)$ and therefore also to some section, say W_2/W_1, of $F''\underline{\underline{N}}_p(F)/F''\underline{\underline{N}}_{p+1}(F)$. Let p^e denote the exponent of the Sylow p-subgroup of the finitely generated abelian group $F''\underline{\underline{N}}_p(F)/W_1$: then W_2/W_1 is (End F)-isomorphic to a section of

$$\frac{\underline{\underline{B}}_{p^{f-1}}[F''\underline{\underline{N}}_p(F)]F''\underline{\underline{N}}_{p+1}(F)}{\underline{\underline{B}}_{p^f}[F''\underline{\underline{N}}_p(F)]F''\underline{\underline{N}}_{p+1}(F)}$$

for some f with $1 \le f \le e$. The desired contradiction now follows from the fact that these quotients, for all f, are irreducible (End F)-modules of order p^p (while W_2/W_1 has order p). Indeed, a basis $\{b_i \mid 1 \le i \le p\}$ is made up of the cosets of the $[y_2, \underbrace{y_1, \ldots, y_1}_{i}, \underbrace{y_2, \ldots, y_2}_{p-i}]^{p^{f-1}}$, and we shall find it sufficient to contemplate only the action of those endomorphisms φ of F which satisfy

$$y_1\varphi \in y_1^{f_{11}} y_2^{f_{12}} F', \quad y_2\varphi \in y_1^{f_{21}} y_2^{f_{22}} F' ,$$

$$\det \begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} \equiv 1 \pmod p .$$

These endomorphisms of F act on this basis exactly the way the corresponding elements of $SL(2, p)$ act by homogeneous linear substitutions on the monomials $x^{i-1}y^{p-i}$ in the 2-variable (commutative) polynomial algebra over the field of p elements. The space of homogeneous polynomials of degree $p - 1$ is well known to be an irreducible $SL(2, p)$-module (Brauer and Nesbitt [5]), and our argument is complete.

In the last step, representation theory may be replaced by commutator calculations of Brisley [6]. However, that is a case where 'bare-handed' commutator calculus is pushed near its limits, and we get a clear indication that systematic exploitation of connections with representation theory offers the only hope of further progress. That is precisely what 'the method' does, as we are about to see.

3. Lie representations

The upshot of the previous section is that we are to study certain fully invariant subgroups of a noncyclic free group F which lie between successive terms of the lower central series of F . This is greatly facilitated by a number of shifts in context.

Consider the lower central factors of F as modules for the monoid End F of all endomorphisms of F : our task is to study their submodules. It is convenient to write these modules additively. As is well known (see G.E. Wall's lectures [28] in this volume as general reference), the restricted direct sum of these modules may be turned into a graded Lie ring gr F by defining Lie multiplication from group commutator formation, so the action of End F on gr F is compatible with this graded Lie ring structure. Thus we have a (monoid) homomorphism from End F to the monoid End(gr F) of all graded Lie ring endomorphisms of gr F , expressing the action of End F on gr F . Two restriction maps complete a commutative diagram

$$\begin{tikzcd} \mathrm{End}\, F \arrow[r] \arrow[dr] & \mathrm{End}(\mathrm{gr}\, F) \arrow[d] \\ & \mathrm{End}(F/F') \end{tikzcd}$$

where F/F' is both the commutator factor group of F and the homogeneous component of degree 1 in $\operatorname{gr} F$. Since F is free, each endomorphism of F/F' is the restriction of some endomorphism of F, so this restriction map is onto, and therefore by the diagram so is the other. Because F/F' generates $\operatorname{gr} F$ (see 1.12 in Wall [28]), the vertical restriction map is also one-to-one, hence an isomorphism. It now follows that the horizontal arrow is also onto. The conclusion we want to retain is that the monoid $\operatorname{End}(F/F')$ acts on $\operatorname{gr} F$ as $\operatorname{End}(\operatorname{gr} F)$ and our problem is the study of the $\operatorname{End}(F/F')$-submodules of (the homogeneous components of) $\operatorname{gr} F$. Just before we move on, a warning. As F/F' is abelian, $\operatorname{End}(F/F')$ is usually regarded as a ring; however, its action on $\operatorname{gr} F$ was derived from homomorphisms of mere multiplicative monoids, and it is in fact not compatible with the additive structure of $\operatorname{End}(F/F')$, so $\operatorname{gr} F$ is *not* a module for the *ring* $\operatorname{End}(F/F')$. As a reminder of the need to ignore addition in $\operatorname{End}(F/F')$, one might write $\operatorname{End}^{\times}(F/F')$ instead, but we cannot afford to carry even the notation we have used so far, let alone complicate it: so we shall write simply E.

To prepare for the next shift, let A stand for the ring of all polynomials with integer coefficients in a set of noncommuting indeterminates (the number of indeterminates being the rank of F), and A_c for the additive group of homogeneous polynomials of degree c. Now A_1 is identified with F/F', and then E acts on A_1, and hence on all of A, as the monoid of all linear homogeneous substitutions. Note that each such substitution is a ring endomorphism of A, mapping each A_c into itself. Next, consider the usual Lie multiplication $[a, b] = ab - ba$ which turns A into a graded Lie ring with homogeneous components A_c, and denote by L the Lie subring generated by the indeterminates in A; put $\mathsf{L}_c = \mathsf{L} \cap \mathsf{A}_c$, and note $\mathsf{L}_1 = \mathsf{A}_1 = F/F'$. Thus L is a graded Lie ring with homogeneous components L_c, and it is clear that L and each L_c admit the given action of E. So far this section has amounted to immediate observations concerning a long string of definitions; by contrast the next point is a deep theorem due to Magnus and Witt (see 3.14 in Wall [28]): the identification of L_1 with F/F' may be extended to an identification of L with $\operatorname{gr} F$. Thus our task becomes the study of E-submodules of the L_c (where by now $E = \operatorname{End}^{\times}(F/F') = \operatorname{End}^{\times}\mathsf{A}_1 = \operatorname{End}^{\times}\mathsf{L}_1$).

In this task A_c will remain an important aid. Contemplate for a moment: A_c is a free abelian group (with the finite set of all monomials of degree c as basis), so its endomorphism ring $\operatorname{End} \mathsf{A}_c$ is just the full matrix ring (of appropriate size) over the ring $\mathbb{Z}$ of integers. Each element e of E acts on A_c as an element, say $e^{\otimes c}$, of $\operatorname{End} \mathsf{A}_c$, and $e \mapsto e^{\otimes c}$ is a (multiplicative) homomorphism. The set

$E^{\otimes c}$ of all $e^{\otimes c}$ is a multiplicative submonoid of End A_c, and so the additive subgroup, say E_c, of End A_c generated by $E^{\otimes c}$ is a subring. As additive group, End A_c is free abelian of finite rank, and therefore so is E_c, but beware: $E^{\otimes c}$ is just an additive generating set, not a free basis, for E_c. (I emphasize that the original addition in E remains forgotten, and whatever additive relations there are on $E^{\otimes c}$ are relations in End A_c.) We are after the E_c-submodules of L_c, but the representation theory of the ring E_c is too complicated to approach head on and classification in this generality eludes us.

The final shift will focus on the submodules we really hope to reach: those which are either isolated or of p-power index. Allowing the coefficients of our polynomials to range over the ring $\mathbb{Z}_{(p)}$ of all rational numbers with denominators prime to p (the localization of $\mathbb{Z}$ at p), we obtain a corresponding polynomial algebra $\mathbb{Z}_{(p)}\mathsf{A}$ with homogeneous components $\mathbb{Z}_{(p)}\mathsf{A}_c$. As the notation suggests, each element of $\mathbb{Z}_{(p)}\mathsf{A}_c$ is a product of an element of $\mathbb{Z}_{(p)}$ and an element of A_c. Clearly $\mathbb{Z}_{(p)}\mathsf{A}_c$ is a free $\mathbb{Z}_{(p)}$-module with the set of monomials of degree c as basis, and $\mathrm{End}_{\mathbb{Z}_{(p)}}\mathbb{Z}_{(p)}\mathsf{A}_c$ is also finitely generated and free as $\mathbb{Z}_{(p)}$-module, embedding End A_c so that $\mathrm{End}_{\mathbb{Z}_{(p)}}\mathbb{Z}_{(p)}\mathsf{A}_c = \mathbb{Z}_{(p)}\,\mathrm{End}\,\mathsf{A}_c$. The $\mathbb{Z}_{(p)}$-submodule $\mathbb{Z}_{(p)}E_c$ is a $\mathbb{Z}_{(p)}$-subalgebra of $\mathrm{End}_{\mathbb{Z}_{(p)}}\mathbb{Z}_{(p)}\mathsf{A}_c$. If B is a subgroup of p-power index in L_c, then $\mathbb{Z}_{(p)}B$ is a $\mathbb{Z}_{(p)}$-submodule of finite index in $\mathbb{Z}_{(p)}\mathsf{L}_c$ and $\mathsf{L}_c \cap \mathbb{Z}_{(p)}B = B$. Conversely, if C is any $\mathbb{Z}_{(p)}$-submodule of finite index in $\mathbb{Z}_{(p)}\mathsf{L}_c$ then $\mathsf{L}_c \cap C$ is a subgroup of p-power index in L_c and $\mathbb{Z}_{(p)}(\mathsf{L}_c \cap C) = C$. If B admits E_c then $\mathbb{Z}_{(p)}B$ admits $\mathbb{Z}_{(p)}E_c$, and if C admits $\mathbb{Z}_{(p)}E_c$ then $\mathsf{L}_c \cap C$ admits E_c. Thus $B \mapsto \mathbb{Z}_{(p)}B$ defines a bijection from the set of all E_c-submodules of p-power index in L_c to the set of all $\mathbb{Z}_{(p)}E_c$-submodules of finite index in $\mathbb{Z}_{(p)}\mathsf{L}_c$ (it is a bijection because the map defined by $C \mapsto \mathsf{L}_c \cap C$ is a twosided inverse for it), and this bijection obviously respects partial order by inclusion. It is an elementary fact that all order-preserving bijections of lattices are lattice isomorphisms. So we may sum up this section: *L_c^p is isomorphic to, and will from now on be thought of as, the lattice of all $\mathbb{Z}_pE_c$-submodules of finite index in $\mathbb{Z}_{(p)}\mathsf{L}_c$.* Similarly, *$L_c^0$ is isomorphic to, and will from now on be thought of as, the lattice of all $\mathbb{Q}E_c$-submodules of $\mathbb{Q}\mathsf{L}_c$*, where as usual $\mathbb{Q}$ stands for the field of rational numbers. The point of this last shift is that we shall be able to show that, for $c < p$, $\mathbb{Z}_{(p)}E_c$ is a direct sum of full matrix algebras over $\mathbb{Z}_{(p)}$, and for every case $\mathbb{Q}E_c$ is a direct sum of full matrix algebras over $\mathbb{Q}$, so their representation theory is trivial compared to that of E_c .

4. Symmetric groups

We have reached the point where some detailed calculation can no longer be avoided; please bear with me if I defer motivation for a while. Let X stand for the set of indeterminates in A , and C for the ordered set $\{1, 2, \ldots, c\}$. A monomial $\overline{\mu}$ of degree c is given by choosing c factors from X , in order, with repetitions allowed: that is, by an arbitrary map $\mu : \mathrm{C} \to X$. For the corresponding monomial $\overline{\mu}$ we have $\overline{\mu} = (1\mu)(2\mu) \ldots (c\mu) = \prod_{i \in \mathrm{C}} i\mu$. Let M_c stand for the set of all monomials of degree c . (It is customary to index the elements of X by the first so many natural numbers: this loads the context with an irrelevant order on X and increases typographical complexity so I avoid it, but the reader might prefer to domesticate this section by translation into that traditional form.) Realize the symmetric group S_c as the group of invertible maps σ from C to C , written on the right and composed accordingly. Then S_c also acts on M_c via the composition of maps: $\sigma\overline{\mu} = \overline{\sigma\mu}$ (where $\sigma\mu$ is σ followed by μ from C to C to X). Extend this action linearly to A_c (and also to $\mathbb{Z}_{(p)}\mathrm{A}_c$ and $\mathbb{Q}\mathrm{A}_c$), so A_c becomes a left module for the group ring $\mathbb{Z}S_c$. Let us agree to write endomorphisms of A_c (*qua* abelian group) on the right, and to compose them accordingly: thus A_c is a right $(\mathrm{End}\ \mathrm{A}_c)$-module. However, we are not dealing with a bimodule, because left action of $\mathbb{Z}S_c$ and right action of $\mathrm{End}\ \mathrm{A}_c$ do not commute: in other words, $\mathrm{End}_{\mathbb{Z}S_c}\mathrm{A}_c < \mathrm{End}\ \mathrm{A}_c$. The aim of this section is to show that $\mathrm{End}_{\mathbb{Z}S_c}\mathrm{A}_c \geq E_c$ and, better still, $\mathrm{End}_{\mathbb{Z}_{(p)}S_c}\mathbb{Z}_{(p)}\mathrm{A}_c = \mathbb{Z}_{(p)}E_c$ whenever $p \geq c$, whence of course $\mathrm{End}_{\mathbb{Q}S_c}\mathbb{Q}\mathrm{A}_c = \mathbb{Q}E_c$.

To this end, we shall need to manipulate elements of $\mathrm{End}\ \mathrm{A}_c$. A convenient basis for $\mathrm{End}\ \mathrm{A}_c$ as free abelian group consists of the 'elementary matrices': $e_{\mu\nu}$ takes $\overline{\mu}$ to $\overline{\nu}$, and all monomials other than $\overline{\mu}$ to 0 . An element $\sum k_{\mu\nu}e_{\mu\nu}$ of $\mathrm{End}\ \mathrm{A}_c$ commutes on A_c with an element σ of S_c if and only if

$$(\sigma\overline{\kappa}) \sum_{\mu,\nu} k_{\mu\nu}e_{\mu\nu} = \sigma\left\{\overline{\kappa} \sum_{\mu,\nu} k_{\mu\nu}e_{\mu\nu}\right\} ,$$

that is,

$$\sum_{\nu} k_{\sigma\kappa,\nu}\bar{\nu} = \sum_{\nu} k_{\kappa\nu}\overline{\sigma\nu} \quad \text{for all } \bar{\kappa} \text{ in } M_c .$$

Comparing coefficients of $\overline{\sigma\nu}$, the last condition amounts to

$$k_{\sigma\kappa,\sigma\nu} = k_{\kappa,\nu} \quad \text{for all } \bar{\kappa}, \bar{\nu} \text{ in } M_c .$$

Consider therefore the action of S_c on the cartesian square $X^{\mathbf{c}} \times X^{\mathbf{c}}$, namely $\sigma : (\mu, \nu) \mapsto (\sigma\mu, \sigma\nu)$: we have that $\sum k_{\mu\nu}e_{\mu\nu} \in \mathrm{End}_{\mathbb{Z}S_c}\mathsf{A}_c$ if and only if $k_{\mu\nu}$ is constant on each S_c-orbit in $X^{\mathbf{c}} \times X^{\mathbf{c}}$. Yet another form of this fact is that one basis of $\mathrm{End}_{\mathbb{Z}S_c}\mathsf{A}_c$ as free abelian group consists of the "orbit sums" $\sum e_{\mu\nu}$ of elementary matrices where each sum is taken over one complete S_c-orbit of elementary matrices with respect to the action $\sigma : e_{\mu\nu} \mapsto e_{\sigma\mu,\sigma\nu}$.

Consider now an element e of E : it may be described by the matrix of integers $\varepsilon_{x,y}$ $(x, y \in X)$ such that

$$x\varepsilon = \sum_{y \in X} \varepsilon_{x,y}y ,$$

and then $e^{\otimes c}$ acts on M_c as the c-fold Kronecker power:

$$\bar{\mu}e^{\otimes c} = \sum_{\nu}\left(\prod_{i \in \mathbf{c}} \varepsilon_{i\mu,i\nu}\right)\bar{\nu} \quad \text{for all } \bar{\mu} \text{ in } M_c ,$$

in other words,

$$\varepsilon^{\otimes c} = \sum_{\mu,\nu}\left(\prod_{i \in \mathbf{c}} \varepsilon_{i\mu,i\nu}\right)e_{\mu\nu} .$$

The product $\prod \varepsilon_{i\mu,i\nu}$ does not change when (μ, ν) is replaced by $(\sigma\mu, \sigma\nu)$, for this amounts only to a permutation of its factors which are ordinary integers, so $E^{\otimes c}$ is contained in $\mathrm{End}_{\mathbb{Z}S_c}\mathsf{A}_c$ and the easy half of the aim of this section has already been reached.

Towards the hard half, note that the orbit sums $\sum e_{\mu\nu}$ form a basis also for $\mathrm{End}_{\mathbb{Z}_{(p)}S_c}\mathbb{Z}_{(p)}\mathsf{A}_c$ as free $\mathbb{Z}_{(p)}$-module. By the easy half, $\mathbb{Z}_{(p)}E_c$ is contained in this module; if it were properly contained, it would lie in some maximal submodule which in turn would be the kernel of a $\mathbb{Z}_{(p)}$-homomorphism onto the unique simple

$\mathbb{Z}_{(p)}$-module $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$. Thus it suffices to show that if

$$\varphi : \mathrm{End}_{\mathbb{Z}_{(p)}S_c}\mathbb{Z}_{(p)}A_c \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$$

is a $\mathbb{Z}_{(p)}$-homomorphism such that $\varphi\left(e^{\otimes c}\right) = 0$ for all $e^{\otimes c}$, then $\varphi = 0$. This is how we shall proceed (adapting the proof of 67.3 in Curtis and Reiner [10]).

The first step is to extend φ to $\mathrm{End}_{\mathbb{Z}_{(p)}}\mathbb{Z}_{(p)}A_c$ by defining it to map to 0 all but one elementary matrix $e_{\mu\nu}$ from each S_c-orbit: these, together with the orbit sums on which φ is already defined, form another $\mathbb{Z}_{(p)}$-free basis, so this definition is legitimate. Part of the assumption is that

$$\varphi\left(e^{\otimes c}\right) = \sum_{\mu,\nu} \varphi\left(e_{\mu\nu}\right) \prod_{i\in C} \varepsilon_{i\mu,i\nu} = 0$$

for all $e^{\otimes c}$, that is, for all choices of the $\varepsilon_{x,y}$ in $\mathbb{Z}$. This means that the polynomial

$$\sum_{\mu,\nu} \varphi\left(e_{\mu\nu}\right) \prod_{i\in C} z_{i\mu,i\nu}$$

in the set $\{z_{x,y} \mid x, y \in X\}$ of commuting indeterminates vanishes at all substitutions from $\mathbb{Z} + p\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$, that is, from $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$. Now of course a nonzero polynomial may well vanish at all substitutions from a finite field: but this polynomial is homogeneous of degree c , so as long as $c \le p$ we can conclude* that it must be the zero polynomial. On the other hand, even the commutative monomials $\prod z_{i\mu,i\nu}$ are different for different S_c-orbits of the pairs (μ, ν) , and for each orbit at most one $\varphi\left(e_{\mu\nu}\right)$ could be nonzero, so it follows that in fact all $\varphi\left(e_{\mu\nu}\right)$ are 0 as required.

Thus we have proved that $\mathrm{End}_{\mathbb{Z}S_c}A_c \ge E_c$ *and* $\mathrm{End}_{\mathbb{Q}S_c}\mathbb{Q}A_c = \mathbb{Q}E_c$ *for all* c , *while* $\mathrm{End}_{\mathbb{Z}_{(p)}S_c}\mathbb{Z}_{(p)}A_c = \mathbb{Z}_{(p)}E_c$ *whenever* $c \le p$. We whall not really need the case $c = p$. (It is easy to see from this argument that the result is sharp, in that the

---

* A nonzero polynomial of degree less than p in each indeterminate cannot vanish at all substitutions from the field of order p : see the proof of Theorem 12.21 in Lausch and Nöbauer [17]. This deals with $c < p$. If $c = p$, use the fact that $z^p - z$ vanishes at all substitutions, so a nonzero homogeneous polynomial of degree p represents the same function as a nonzero polynomial of degree less than p in each indeterminate. (There the argument stops, for $z_1^p z_2 - z_1 z_2^p$ vanishes identically.)

claim fails for $c > p$.)

What makes this result useful is the fact that, *for* $c < p$ *, the group algebra* $\mathbb{Z}_{(p)}S_c$ *is a direct sum of full matrix algebras over* $\mathbb{Z}_{(p)}$. The corresponding claim for $\mathbb{Q}S_c$ is better known: but observe that in expressing the relevant elementary matrices as rational linear combinations of elements of S_c , one can get away with denominators which divide $c!$ and are therefore prime to p when $c < p$ (see §5 of Chapter IV in Boerner's text [3]). It will be convenient to exploit this in a separate section.

5. Morita equivalence

This is a pretentious heading, for we need only a very special case of Morita equivalence which is much older: Brauer equivalence might be a more appropriate appellation. For a convenient modern reference, see Chapter 6 in Anderson and Fuller [1]; in particular, Propositions 21.2, 21.7, and Exercises 21.6, 21.5. Let K be a commutative ring with 1 $\big($take $K = \mathbb{Z}_{(p)}$ if that is reassuring, but not if it clouds the issue$\big)$, m a positive integer, K_m the algebra of $m \times m$ matrices over K . Regard the direct sum $K^{\oplus m}$ of m copies of K first as left K , right K_m module U_m ("row vectors"), then as left K_m , right K module $\overline{U}_m$ ("column vectors"). For the tensor products of these bimodules we have that $U_m \otimes_{K_m} \overline{U}_m \cong K$ and $\overline{U}_m \otimes_K U_m \cong K_m$. It follows that the additive functors $U_m \otimes_{K_m}$ - and $\overline{U}_m \otimes_K$ - provide an equivalence between the categories of left K_m-modules and (left) K-modules (that is, the composites of the two functors are naturally equivalent to the identity functors on these categories). Thus two modules corresponding to each other in this equivalence have isomorphic endomorphism rings and isomorphic submodule lattices.

Suppose now that K is a principal ideal domain and V is any finitely generated left K_m-module such that the product of a nonzero scalar matrix and a nonzero element of V is never zero. Then the corresponding K-module is also finitely generated and "torsionfree", hence a direct sum of, say, n copies of K . It follows that V is the direct sum of n copies of $\overline{U}_m$ as left K_m-module, and the endomorphism ring of V is just K_n (thought of as acting on the right of V). By the same argument with left and right interchanged, a finitely generated "torsionfree" right K_n-module W is a direct sum of, say, l copies of U_n as right K_n-module, and the submodule lattice of W is isomorphic to the submodule lattice of the free K-module of rank l . It is easy to see that in this lattice isomorphism submodules of finite index correspond to submodules of finite index.

It is now a tedious but perfectly elementary exercise to extend these conclusions to the case of direct sums of full matrix rings. Let K remain a principal ideal domain; for π ranging through some finite index set, choose positive integers $m(\pi)$ and let $\oplus K_{m(\pi)}$ be the direct sum of the corresponding matrix rings. Denote by U_π the left K, right $\oplus K_{m(\pi)}$ bimodule obtained from $U_{m(\pi)}$ by letting all the $K_{m(\pi')}$ with $\pi' \neq \pi$ annihilate it, and define $\overline{U}_{m(\pi)}$ similarly. (Note U_π and $\overline{U}_\pi$ depend on π, not just on the integer $m(\pi)$ which may be the same for several distinct elements of the index set.) Let e_π be the identity element of $K_{m(\pi)}$, so $\sum e_\pi$ is the identity element of $\oplus K_{m(\pi)}$. Take any finitely generated left $\oplus K_{m(\pi)}$-module V which is torsionfree in the sense that $\left(k \sum e_\pi\right)v = 0$ with $k \in K$, $v \in V$ implies $k = 0$ or $v = 0$: then V is the direct sum of the $e_\pi V$ and the earlier case can be applied to describe the structure of each $e_\pi V$. The conclusion is that $V = \oplus \overline{U}_\pi^{\oplus n(\pi)}$ for suitable nonnegative integers $n(\pi)$, and the endomorphism ring of V (acting on the right) is $\oplus K_{n(\pi)}$ with π ranging through those indices for which $n(\pi) \neq 0$.

At this stage we are ready to establish the structure of $\mathbb{Z}_{(p)}E_c$ and $\mathbb{Q}E_c$. For we know that $\mathbb{Z}_{(p)}S_c$ has the form $\oplus K_{m(\pi)}$ and $\mathbb{Z}_{(p)}\mathrm{A}_c$ is finitely generated and torsionfree: thus $\mathbb{Z}_{(p)}E_c$, which is just the endomorphism ring $\mathrm{End}_{\mathbb{Z}_{(p)}S_c}\mathbb{Z}_{(p)}\mathrm{A}_c$, is of the form $\oplus K_{n(\pi)}$; all this with $K = \mathbb{Z}_{(p)}$. The same goes of course for $\mathbb{Q}E_c$, with $K = \mathbb{Q}$. However, there is more to be had from this approach.

To this end, we carry on with extending the comments of the second paragraph of this section. Interchanging right and left, we know that a finitely generated torsionfree right $\oplus K_{n(\pi)}$ module W has the structure $\oplus U_\pi^{\oplus l(\pi)}$ where now the range of π may be smaller than before and the U_π are defined with reference to the $n(\pi)$ rather than the $m(\pi)$. Adapting notation still further, let e_π denote now the identity element of $K_{n(\pi)}$. Every submodule W' of W is of the form $\oplus W'e_\pi$, and W' has finite index in W if and only if each $W'e_\pi$ has finite index in the corresponding We_π. Thus the lattice of finite index submodules of W is the direct product of the lattices of finite index submodules of the We_π. Again, each involves essentially just one matrix ring $K_{n(\pi)}$, so by the previous observation the lattice of finite index submodules of We_π is isomorphic to the lattice of finite index K-submodules of $K^{\oplus l(\pi)}$. In case $K = \mathbb{Z}_{(p)}$, the latter is in turn isomorphic to the lattice $A^p_{l(\pi)}$ of subgroups of p-power index in a free abelian group of rank $l(\pi)$.

We have almost finished the proof of the qualitative part of the Classification Theorem stated in the Introduction. The subdirect decompositions were established in Section 2; we have just proved (read $W = \mathbb{Z}_{(p)}L_c$) that L^p_c is the direct product of the $A^p_{l(\pi)}$ whenever $c < p$; and the same argument with $\mathbb{Q}$ in place of $\mathbb{Z}_{(p)}$, counting all submodules of $\mathbb{Q}L_c$, gives that L^0_c is the direct product of the subspace lattices $A^0_{l(\pi)}$. What remains is the explicit determination of the appropriate range of π and the integers $l(\pi)$. However, the qualitative claims made about these in the Introduction are already at hand. For, from the second paragraph of this section on, all modules and algebras considered have been free as K-modules, so the whole discussion remains invariant as we change K from $\mathbb{Z}_{(p)}$ to $\mathbb{Q}$ or even all the way to the complex field $\mathbb{C}$ - neither the range of π nor the multiplicities $l(\pi)$ change in the process. Thus indeed they are independent of the prime p : all they depend on is the class c and that long forgotten parameter, the rank of F . The quantitative details will be given in the next section.

6. The multiplicity formula

Let r denote the common rank of F and A . The quantitative details needed to complete the Classification Theorem have been worked out long ago, in the context of the representation theory of the general linear groups $\mathrm{GL}(r, \mathbb{C})$. Put $G = \mathrm{GL}(r, \mathbb{C})$: this also acts on $\mathbb{C}A_c$, by invertible linear homogeneous substitutions with complex coefficients, and the Kronecker powers $g^{\otimes c}$ (for $g \in G$) also span $\mathrm{End}_{\mathbb{C}S_c}\mathbb{C}A_c$, that is, $\mathbb{C}E_c$: for a qualitative description, see §67 in Curtis and Reiner [10]; for a wealth of detail, I find Boerner [3] the most readable source. What we need here is that the complex irreducible representations of S_c are traditionally indexed by the partitions π of c , so initially the set of all these is our range for π . There are formulas for the $m(\pi)$, but we don't need those here. The irreducibles which occur with positive multiplicity $n(\pi)$ in $\mathbb{C}A_c$ are precisely those labelled with partitions into at most r parts, so the set of these becomes our final range for π , relevant in describing $\mathbb{Z}_{(p)}E_c$ and $\mathbb{Q}E_c$. Again, there are formulas for the dimensions $n(\pi)$, but we don't need them either. The character of G afforded by $\mathbb{C}L_c$ was, I believe, first given by Angeline Brandt [4], and the corresponding formula for the multiplicities $l(\pi)$ follows so directly that it must have been known to her, though the earliest that I can find it in print is in Wever's paper [29]. It is

$$l(\pi) = \frac{1}{c} \sum_{d \mid c} \mu(d)\chi_\pi\left(\sigma^{c/d}\right)$$

where μ is the Möbius function, χ_π is the irreducible character of S_c indexed by π, and σ is the cyclic permutation $(12 \ldots c)$. There are various ways of evaluating $\chi_\pi\left(\sigma^{c/d}\right)$; let me give one, just for flavour. If the parts of π are $k_1, \ldots, k_s$ so that $k_1 \geq k_2 \geq \ldots \geq k_s$ (and $k_1 + k_2 + \ldots + k_s = c$), then $\chi_\pi\left(\sigma^{c/d}\right)$ is the alternating sum of the multinomial coefficients

$$\left(\begin{array}{c} c/d \\ \frac{k_1+1\tau-1}{d}, \frac{k_2+2\tau-2}{d}, \ldots, \frac{k_s+s\tau-s}{d} \end{array}\right)$$

over all permutations τ of $\{1, 2, \ldots, s\}$, with sign according to the parity of τ, and subject to the convention that the multinomial coefficient is 0 unless all its entries are nonnegative integers. At least, this is how I read pp. 134-135 in Murnaghan's book [21].

As I said, the multiplicity formula is obtained from the character formula. That, in turn, may be easily derived (as in Wever [30]) from the second of 'Witt's formulas' (reporduced as Theorem 5.11 in Magnus, Karrass, Solitar [20], for instance), although Brandt preferred a different argument. The proof in Kljačko's [14] left as exercise for the reader a step which seems every bit as hard as the multiplicity formula itself, but in a more recent paper [15] he indicates a nice proof and gives a fascinating interpretation - paraphrased via Frobenius reciprocity, this reads as follows. Take any faithful linear (complex) character of the cyclic group generated by σ, and induce it to S_c: then $l(\pi)$ is also the multiplicity of χ_π in this induced character. He deduces that, when $c > 6$, the only partitions π with $l(\pi) = 0$ are those corresponding to the two linear characters of S_c. (This was conjectured in Pentony's unpublished thesis [23].) The multiplicities for $c \leq 6$ are as follows (from Thrall [27] who used a recursive method and tabulated l for $c \leq 10$; but see Brandt's [4] for a correction in the case $c = 10$ itself):

the value of l is	0	1	2	3
at the partitions		1		
	2	1^2		
	$3,\ 1^3$	21		
	$4,\ 2^2,\ 1^4$	$31,\ 21^2$		
	$5,\ 1^5$	$41,\ 32,\ 31^2,\ 2^21,\ 21^3$		
	$6,\ 2^3,\ 1^6$	$51,\ 42,\ 3^2,\ 31^3,\ 21^4$	$41^2,\ 2^21^2$	321

where the usual notation for partitions has been used: for example, 41^2 stands for the partition $4 + 1 + 1$ of 6.

7. Large class

Having completed the Classification Theorems, there is relatively little left to establish the Distributivity Theorems. The fact that $l(\pi) \leq 1$ whenever $c \leq 5$ but $l(\pi) > 1$ for some π when $c = 6$ means that the torsionfree Classification Theorem implies the torsionfree Distributivity Theorem, and the same happens for the p-power exponent case whenever $p \geq 7$. The case of $c \leq 3$ has been covered by Jónsson [13] and Remeslennikov [24]. As I have already mentioned, Bryce [7] has demonstrated the nondistributivity of N^p_{p+2} for all primes p, exploiting the breakdown of the subdirect reduction discussed in our Section 2. This leaves the cases N^3_4, N^5_4, N^5_5. For N^3_4 I need *ad hoc* methods which are not suitable for presentation here. The distributivity of N^5_4 follows from the Classification Theorem. What is left then is N^5_5 ; by Section 2, it will suffice to prove that L^5_5 is not distributive. (Kljačko [14] proves the nondistributivity of L^2_4, a different route to N^2_4 from Bryce's. The argument is exactly analogous to that which I will present for L^5_5. The case of N^2_4 was also dealt with by Belov [2].)

Before embarking on the discussion of this "large class" case, some general comments. As observed before the final shift in Section 3, the elusive general problem is the analysis of the E_c-submodules of L_c. We have proved that $\mathbb{Q}E_c$ is a direct sum of full matrix rings over $\mathbb{Q}$, and observed that additively E_c is free abelian of finite rank: so E_c is a $\mathbb{Z}$-order in the excellent algebra $\mathbb{Q}E_c$. What we have done for primes with $p > c$ may be viewed as describing the localizations of

E_c (and L_c) at these primes, standard steps in the investigation of any $\mathbb{Z}$-order. The main step of Section 4 can be reinterpreted to say that E_c is contained in another, more tractable, $\mathbb{Z}$-order in the same algebra, namely in $\mathrm{End}_{\mathbb{Z}S_c} A_c$, and that the finite index of E_c in $\mathrm{End}_{\mathbb{Z}S_c} A_c$ is divisible only by primes strictly less than c. It is useful to know that L_c admits the action of this larger $\mathbb{Z}$-order (for $L_c = \Omega_c A_c$ where Ω_c is a suitable element of $\mathbb{Z}S_c$, whose introduction was attributed to Otto Grün by Magnus in [19]: see Theorems 5.16, 5.17 in Magnus, Karrass, Solitar [20]. For example, the lattice of $(\mathrm{End}_{\mathbb{Z}S_c} A_c)$-submodules of L_c is a sublattice of the lattice of E_c-submodules, and in aiming for a nondistributivity result it is sufficient if one can succeed in that sublattice. (This help is not needed in dealing with L_5^5, for then $p \geq c$, but it does matter in the case of L_4^2.) The point is that we have more information on $\mathbb{Z}S_c'$ (and hence also on $\mathrm{End}_{\mathbb{Z}S_c} A_c$) even in the context of small primes, and this can be exploited to good effect.

As the situation is now tighter, for comfort let us assume that the rank r is large. Then there exist one-to-one maps $\mu : \mathbf{c} \to X$, and the corresponding monomials $\overline{\mu}$ have trivial stabilizers in S_c, so S_c acts regularly on the orbit of such a $\overline{\mu}$. What we need is that A_c has a direct summand, namely $\mathbb{Z}S_c\overline{\mu}$, which is a regular $\mathbb{Z}S_c$-module. (This makes it particularly easy to see that $\mathrm{End}_{E_c} A_c$ is just the image of $\mathbb{Z}S_c$ in $\mathrm{End}_{\mathbb{Z}} A_c$: a potentially useful fact, but irrelevant to our immediate purpose.)

To come to the point, let us take $p = c = 5 \leq r$ and $\mu : \mathbf{c} \to X$ one-to-one so $\mathbb{Z}_{(5)}S_5\overline{\mu}$ is a regular direct summand of $\mathbb{Z}_{(5)}A_5$, and recall from Section 4 that in this case $\mathrm{End}_{\mathbb{Z}_{(5)}S_5} A_5 = \mathbb{Z}_{(5)}E_5$. If W is an indecomposable direct summand of $\mathbb{Z}_{(5)}S_5\overline{\mu}$ (*qua* $\mathbb{Z}_{(5)}S_5$-module), then it is also a direct summand of $\mathbb{Z}_{(5)}A_5$; equivalently, $\mathbb{Z}_{(5)}A_5$ has an idempotent $\mathbb{Z}_{(5)}S_5$-endomorphism, say f, with $\mathbb{Z}_{(5)}A_5 f = W$. The indecomposability of W means that f is primitive in $\mathbb{Z}_{(5)}E_5$. When $\mathbb{Q}W$ decomposes as a direct sum, $\oplus\, \overline{U}_\pi^{\oplus t(\pi)}$ say, of irreducible $\mathbb{Q}S_c$-modules, this corresponds to f being no longer primitive in $\mathbb{Q}E_5$: instead, $f = \sum_\pi \sum_{i=1}^{t(\pi)} f_{\pi,i}$ with the $f_{\pi,i}$ pairwise orthogonal idempotents primitive in $\mathbb{Q}E_5$ and $\mathbb{Q}Wf_{\pi,i} \cong \overline{U}_\pi$. The way we labelled the simple components of $\mathbb{Q}E_5$ by partitions means, in this context, that $f_{\pi,1}, \ldots, f_{\pi,t(\pi)}$ are in the simple component labelled by π. In exact parallel, of course, $f\mathbb{Z}_{(5)}E_5$ is an indecomposable right ideal in $\mathbb{Z}_{(5)}E_5$ but $f\mathbb{Q}E_5 = \oplus\oplus f_{\pi,i}\mathbb{Q}E_5$, with $f_{\pi,i}\mathbb{Q}E_5$ belonging to the isomorphism type of irreducible $\mathbb{Q}E_5$-modules labelled by π. As W was an indecomposable direct summand of the regular $\mathbb{Z}_{(5)}S_5$-module $\mathbb{Z}_{(5)}S_5\bar{\mu}$, we know that the $t(\pi)$ form a column in the decomposition matrix (see the beginning of the proof of 83.9 in Curtis and Reiner [10], including the comment in the footnote which enables one to avoid completion given that $\mathbb{Q}$ is a splitting field for S_5); and we are still free to choose W to obtain whichever column we like. (I shall not reproduce the decomposition matrix here; it is not hard to calculate.) Let us choose W so we get the column corresponding to the 3-dimensional composition factor of the permutation representation of degree 5 over the field of 5 elements: then $t(41) = t(31^2) = 1$ (and t vanishes at all other partitions). Since we also have $l(41) = l(31^2) = 1$, in this case $f\mathbb{Q}E_5$ is isomorphic to a submodule of $\mathbb{Q}L_5$, namely to a submodule which is a direct sum of two irreducibles, say, of U and V. What we need is that $f\mathbb{Q}E_5$ has homomorphisms onto each of U and V, say, $\alpha : f\mathbb{Q}E_5 \twoheadrightarrow U$ and $\beta : f\mathbb{Q}E_5 \twoheadrightarrow V$. Now $U = \mathbb{Q}\alpha(f\mathbb{Z}_{(5)}E_5) = \mathbb{Q}(U \cap \mathbb{Z}_{(5)}L_5)$ and so for some power of 5, say 5^a, we have $0 \neq 5^a\alpha(f\mathbb{Z}_{(5)}E_5) \leq U \cap \mathbb{Z}_{(5)}L_5$; similarly, $0 \neq 5^b\beta(f\mathbb{Z}_{(5)}E_5) \leq V \cap \mathbb{Z}_{(5)}L_5$ for some b. All we need of this is that $f\mathbb{Z}_{(5)}E_5$ has two disjoint nonzero homomorphic images in $\mathbb{Z}_{(5)}L_5$: for brevity, let us call these U' and V'. The last point is that, because f is primitive in $\mathbb{Z}_{(5)}E_5$, all proper submodules of $f\mathbb{Z}_{(5)}E_5$ are contained in a unique maximal submodule. (I find this rather awkward to dig out of Curtis and Reiner [10]. For a start, as $\mathbb{Q}E_5$ is a direct sum of full matrix rings over $\mathbb{Q}$, the proof of 76.29 gives that $f\mathbb{Z}_{(5)}E_5$ remains indecomposable after 5-adic completion, so f remains primitive; then a standard result on lifting idempotents, 77.10, yields that f is primitive modulo 5. Thus modulo 5 we get that $f\mathbb{Z}_{(5)}E_5$ becomes a principal indecomposable module for the finite image of $\mathbb{Z}_{(5)}E_5$, and hence by 54.11 has a unique maximal submodule. The preimage of this modulo 5 will do, by Nakayama's Lemma.) This maximal submodule then contains the kernels of the homomorphisms onto U' and V'; let U'' and V'' be the images of the maximal submodule in U' and V', respectively. Now U'/U'' and V'/V'' are both isomorphic to the unique simple homomorphic image of

$f\mathbb{Z}_{(5)}E_5$. Recall that $U \oplus V$ was a direct summand of ΦL_5 ; let C be any direct complement, so $U \oplus V \oplus C = \Phi L_5$, and put $C' = C \cap \mathbb{Z}_{(5)}L_5$. Then $U'' \oplus V'' \oplus C'$ has finite index in $\mathbb{Z}_{(5)}L_c$, and the quotient $(U' \oplus V' \oplus C')/(U'' \oplus V'' \oplus C')$ is a direct sum of two isomorphic summands, namely, of $(U' \oplus V'' \oplus C')/(U'' \oplus V'' \oplus C')$ and $(U'' \oplus V' \oplus C')/(U'' \oplus V'' \oplus C')$. Thus these two summands and their 'diagonal' violate the distributive law, proving that L_5^5 is not distributive. This completes the proof.

8. Postscript

All the background for this was available by the late 1930's: the Magnus-Witt Theorem, and enough of Brauer's theory of modular representations (including his observation that results from Schur's dissertation concerning representations of general linear groups on tensor spaces remain valid in finite characteristic for the small degree case). The first mention of Grün's Ω_c was in a lecture [19] given by Magnus to a week-long group theory meeting at Göttingen in June 1939 (*Crelle* devoted a whole issue to the proceedings): Magnus drew attention to the problem of investigating the action of homogeneous linear substitutions on homogeneous components of free Lie rings, and to the relevance of this in the study of fully invariant subgroups. There are indications that not only Grün and Magnus but also Witt and Zassenhaus were using such ideas at the time, though I have found no evidence for Higman's guess [12] that Witt might have been in possession of the character formula. On the other side of the Atlantic, Thrall got very much closer to the developments reported on here. In his paper [26] (which was submitted before *Crelle*'s Göttingen issue appeared), he used Lie representations systematically for determining all characteristic subgroups in the last term of the lower central series of free groups of $\underline{\underline{B}}_p \wedge \underline{\underline{N}}_c$ for $c < p$, and referred also to the p-power exponent case. Presumably with this motivation, he proceeded with a systematic study of Lie representations in [27], and this was carried on by Brandt in [4]. In the late 1940's Wever took the matter further in several papers, but his applications concerned specific fully invariant subgroups rather than general classification, and interest in Lie representations favoured one-dimensional submodules ("invariants"), perhaps on account of a similar emphasis in Magnus [19]. When variety theory came to life again in the 1950's, it seemed to have no contact with these efforts. Even after Magnus had drawn Hanna Neumann's attention to the relevance of Burrow's then still recent work [9] on 'Lie invariants' (see page 104 in [22]), we did not catch on. From our point of view it did not help to focus on invariants - this seems to have led to the incorrect conjecture expressed in Problem 14 of [22] and, by making the result plausible, encouraged the oversight in 35.35 of [22]. Still, we had little excuse for being as stunned as we were by Graham Higman's lecture [12] which finally opened our eyes.

Higman's account [12] is in terms of prime characteristic. Kljačko [14] worked with p-adic completions (even to the point of starting with a free pro-p-group). Newman and I used localization at p (Mal'cev completions of free nilpotent groups). The present approach is closest to that envisaged in the closing paragraph of Pentony's thesis [23]; it developed in the course of writing up this paper, and (as well as including more detail) deviates substantially from what I actually said in the lectures. In allowing one to view much of the work as a study of the $\mathbb{Z}$-order E_c, it may point in the direction one could proceed beyond the present boundaries.

I am indebted to several participants of the Institute for long and helpful discussions; particularly to P. Fitzpatrick, M.F. Newman, M.G. Schooneveldt, and G. E. Wall.

References

[1] Frank W. Anderson, Kent R. Fuller, *Rings and Categories of Modules* (Graduate Texts in Mathematics, **13**. Springer-Verlag, New York, Heidelberg, Berlin, 1974).

[2] Ю.А. Белов [Ju.A. Belov], "К вопросу а решетке нильпотентных многообразий групп класса 4" [On the question of the lattice of nilpotent varieties of groups of class 4], *Algebra i Logika* **9** (1970), 623-628; *Algebra and Logic* **9** (1970), 371-374.

[3] Hermann Boerner, *Representations of Groups* (North-Holland, Amsterdam, 1963).

[4] Angeline J. Brandt, "The free Lie ring and Lie representations of the full linear group", *Trans. Amer. Math. Soc.* **56** (1944), 528-536.

[5] R. Brauer and C. Nesbitt, "On the modular characters of groups", *Ann. of Math.* (2) **42** (1941), 556-590.

[6] Warren Brisley, "Varieties of metabelian p-groups of class p, $p+1$ ", *J. Austral. Math. Soc.* **12** (1971), 53-62.

[7] R.A. Bryce, "Metabelian groups and varieties", *Philos. Trans. Roy. Soc. London Ser. A* **266** (1970), 281-355.

[8] R.A. Bryce, "Varieties of metabelian p-groups", *J. London Math. Soc.* (2) **13** (1976), 363-380.

[9] Martin D. Burrow, "Invariants of free Lie rings", *Comm. Pure Appl. Math.* **11** (1958), 419-431.

[10] Charles W. Curtis, Irving Reiner, *Representation Theory of Finite Groups and Associative Algebras* (Pure and Applied Mathematics, 11. Interscience [John Wiley & Sons], New York, London, 1962).

[11] K.W. Gruenberg, "Residual properties of infinite soluble groups", *Proc. London Math. Soc.* (3) 7 (1957), 29-62.

[12] Graham Higman, "Representations of general linear groups and varieties of p-groups", *Proc. Internat. Conf. Theory of Groups*, Canberra, 1965, 167-173 (Gordon and Breach, New York, London, Paris, 1967).

[13] Bjarni Jónsson, "Varieties of groups of nilpotency three", *Notices Amer. Math. Soc.* 13 (1966), 488.

[14] А.А. Клячко [A.A. Kljačko], "Многообразия p-групп малого класса" [Varieties of p-groups of a small class], *Ordered Sets and Lattices* No.1, 31-42 (Izdat. Saratov Univ., Saratov, 1971).

[15] А.А. Клячко [A.A. Kljačko], "Элементы Ли в тензорной алгебре" [Lie elements in a tensor algebra], *Sibirsk. Mat. Ž.* 15 (1974), 1296-1304, 1430; *Siberian Math. J.* 15 (1974), 914-921.

[16] L.G. Kovács, M.F. Newman and P.F. Pentony, "Generating groups of nilpotent varieties", *Bull. Amer. Math. Soc.* 74 (1968), 968-971.

[17] Hans Lausch and Wilfred Nöbauer, *Algebra of Polynomials* (North-Holland Mathematical Library, 5. North-Holland, Amsterdam, London; American Elsevier, New York, 1973).

[18] Frank Levin, "Generating groups for nilpotent varieties", *J. Austral. Math. Soc.* 11 (1970), 28-32; Corrigendum, *ibid.* 12 (1971), 256.

[19] Wilhelm Magnus, "Über Gruppen und zugeordnete Liesche Ringe", *J. reine angew. Math.* 182 (1940), 142-149.

[20] Wilhelm Magnus, Abraham Karrass, Donald Solitar, *Combinatorial Group Theory: Presentations of groups in terms of generators and relations* (Pure and Appl. Math. 13. Interscience [John Wiley & Sons], New York, London, Sydney, 1966).

[21] Francis D. Murnaghan, *The Theory of Group Representations* (The Johns Hopkins Press, Baltimore, 1938).

[22] Hanna Neumann, *Varieties of Groups* (Ergebnisse der Mathematik und ihrer Grenzgebiete, 37. Springer-Verlag, Berlin, Heidelberg, New York, 1967).

[23] Paul Pentony, "Laws in torsion-free nilpotent varieties with particular reference to the laws of free nilpotent groups" (PhD thesis, Australian National University, Canberra, 1970. See also: Abstract: *Bull. Austral. Math. Soc.* 5 (1971), 283-284).

[24] В.Н. Ремесленников [V. N. Remeslennikov], "Два замечания о 3-ступенно нильпотентных группах" [Two remarks on 3-step nilpotent groups], *Algebra i Logika Sem.* **4** (1965), no. 2, 59-65.

[25] A.G.R. Stewart, "On centre-extended-by-metabelian groups", *Math. Ann.* **185** (1970), 285-302.

[26] Robert M. Thrall, "A note on a theorem by Witt", *Bull. Amer. Math. Soc.* **47** (1941), 303-308.

[27] R.M. Thrall, "On symmetrized Kronecker powers and the structure of the free Lie ring", *Amer. J. Math.* **64** (1942), 371-388.

[28] G.E. Wall, "Lie methods in group theory", these proceedings, 137-173.

[29] Franz Wever, "Operatoren in Lieschen Ringen", *J. reine angew. Math.* **187** (1949), 44-55.

[30] Franz Wever, "Über Invarianten in Lie'schen Ringen", *Math. Ann.* **120** (1949), 563-580.

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