COUNTING CLASSES AND CHARACTERS OF GROUPS OF PRIME EXPONENT

BY

NOBORU ITO

Amble Road, Shoreview, MN 55126-2216, USA

AND

AVINOAM MANN

Einstein Institute of Mathematics, The Hebrew University of Jerusalem
Givat Ram, Jerusalem 91904, Israel
e-mail: mann@math.huji.ac.il

ABSTRACT

We determine the conjugacy class sizes, the character degrees, and the multiplicities of these sizes and degrees, for some relatively free p-groups.

Introduction

In this paper we obtain information about the conjugacy classes and irreducible characters of some finite groups of an odd prime exponent p. The groups that we consider are the relatively free groups in the varieties of groups of exponent p and a given nilpotency class. We determine the sizes of the conjugacy classes, and the number of classes of each size, for nilpotency classes up to 4. We also determine the degrees of the irreducible characters for classes 2 and 3, and for the groups of small rank of class 4. For class 2 we determine the multiplicity of each degree, and we also determine the number of characters of degree p of the relatively free groups of exponent p and arbitrary nilpotency class. Finally, we consider one variety of groups of class 2 and exponent p^2.

Since the number of p-groups is vast, results obtained for some of them can hardly be considered as typical. Still, for what it is worth, we note that in all the cases that we consider there occur very few class sizes, not more than four. In

Received January 23, 2005

contrast, the number of character degrees tends to infinity with the rank of the group. Moreover, with a single exception (see Lemma 9) the character degrees are consecutive powers of p. A curious situation occurs for one group of order 3^{14}. The class sizes are exactly the squares of the character degrees, and the multiplicities of the classes and of the characters are the same (see Lemma 11).

Our notation is mostly standard. We use $\gamma_i(G)$, $Z(G)$, G', and $\Phi(G)$ for the lower central series, center, commutator (derived) subgroup, and Frattini subgroup of G, $cs(G)$ and $cd(G)$ denote the sets of conjugacy class sizes and of irreducible character degrees of G, respectively, and $k(G)$ is the **class number**, i.e. the number of conjugacy classes. We denote by $d(G)$ the minimal number of generators of G, which for a p-group is given by $|G:\Phi(G)| = p^{d(G)}$. If F is a p-group which is relatively free in some variety, we refer to $d(F)$ as the **rank** of F. Finally, $[x]$ is the integral part of the number x, and $\mu(n)$ is the möbius function.

We recall the structure of the relevant groups. Let p be an odd prime, let $r \geq 2$, let $F_{r,c}$ be the free group of rank r in the variety of groups of exponent p and class c, and let $\{x_1, \ldots, x_r\}$ be free generators of $F_{r,c}$. We sometimes just write F, suppressing the subscripts r, c, when they are understood from the context. First, $F_{r,2}$ has order $p^{\binom{r+1}{2}}$, $F'_{r,2}$ can be considered as a vector space over $GF(p)$ with the commutators $[x_i, x_j]$, $i < j$, as a basis, and $Z(F) = F'$.

For higher classes we have to separate the prime $p = 3$ from the bigger ones. A group of exponent 3 has class three at most, so for $p = 3$ it remains to consider only $F_{r,3}$. This has order $3^{\binom{r}{3}+\binom{r}{2}+r}$, with the (images of the) commutators above being a basis for $F'/\gamma_3(F)$, we have $Z(F) = \gamma_3(F)$, and the triple commutators $[x_i, x_j, x_k]$, $i < j < k$ are a basis for $Z(F)$ ([Hm], Ch. 18).

For $p > 3$, there is no general bound for the class, even if p is fixed, but there is one if p and r are given. However, the exact class, and order, of $F_{r,c}$ are unknown in most cases [VL]. For class three the structure is described in [Me]. For completeness, we include the following result, dealing with groups of a small class, for which we have not found a convenient reference. We refer to ([Hm], Ch. 11) for the Witt function and basic commutators, and to [K] for the correspondences between groups and Lie rings. The Witt function is given by

$$W_r(c) = \frac{1}{c}\sum_{d|c} \mu(d) r^{c/d}.$$

PROPOSITION 1: *Let $c \leq d$ and $c \leq p-1$. Then $|\gamma_c(F_{r,d}) : \gamma_{c+1}(F_{r,d})| = p^{W_r(c)}$.*

Proof: Let F be the (absolutely) free group of rank r. Then $\gamma_c(F)/\gamma_{c+1}(F)$ is a free abelian group of rank $W_r(c)$, therefore for any group G with r generators, the factor group $\gamma_c(G)/\gamma_{c+1}(G)$ can be generated by $W_r(c)$ elements. Thus, if $exp(G) = p$ and $d(G) \leq r$, then that factor group has order at most $p^{W_r(c)}$. To complete the proof it suffices to find a group of exponent p and r generators for which the order of that factor group is exactly $p^{W_r(c)}$. We start with the group $F/\gamma_p(F)$, and let L be its associated Lie ring. Then L/pL is a Lie algebra over $GF(p)$ with factors in the lower central series of orders $p^{W_r(c)}$, and the group associated to L/pL by means of the Lazard correspondence is the one that we are looking for.

It follows that $F_{r,c}$ is the group associated to L/pL, and that the basic commutators of weight c form a basis for $\gamma_c(F)/\gamma_{c+1}(F)$. For later reference, we record that for $c = 3$ (and $p > 3$), these can be taken as the commutators $[x_i, x_j, x_k]$; $i > j \leq k$. For $c = 4$ there are two types of basic commutators: one type consists of the commutators $[[x_i, x_j], [x_k, x_l]]$, with $i > j$, $k > l$, and the pair (k, l) precedes (i, j) lexicographically. The other type consists of the commutators $[x_i, x_j, x_k, x_l]$, with $i > j \leq k \leq l$.

1. Class two

We start the discussion of classes and characters with the group $F := F_{r,2}$. Any element x outside $F' = Z(F)$ is one of a set of r free generators, say $x_1 = x, x_2, \ldots, x_r$. Since the commutators $[x_1, x_i]$ are independent, $C_F(x) = \langle x, Z(F)\rangle$, and thus x has p^{r-1} conjugates, and there are $p^{\binom{r}{2}-r+1}(p^r - 1)$ non-central classes, yielding a class number

$$k(F) = p^{\binom{r}{2}+1} + p^{\binom{r}{2}} - p^{\binom{r}{2}-r+1} = p^{\binom{r}{2}-r+1}(p^r + p^{r-1} - 1).$$

The determination of the degrees and multiplicities of the irreducible characters require some preparations.

Lemma 2: *Two epimorphisms ϕ and ψ of a group G onto a group H have the same kernel iff $\psi = \phi\alpha$, for some $\alpha \in Aut(H)$.*

Proof: It is clear that if $\psi = \phi\alpha$, then ϕ and ψ have the same kernel. Conversely, suppose that the two homomorphisms have the same kernel, N say, then α is the composite of the two isomorphisms $x^\phi \to xN$ and $xN \to x^\psi$ between H and G/N.

Lemma 3: *Let F be a relatively free finite p-group of rank r, and let G be a group of order p^n with $d(G) = d \leq r$. Then the number of homomorphisms of F onto G is $p^{r(n-d)}(p^r - 1)\cdots(p^r - p^{d-1})$.*

Proof: Given a homomorphism ϕ of F into G, it is onto iff the induced homomorphism of F into $G/\Phi(G)$ is onto. Since the inverse image of $\Phi(G)$ contains $\Phi(F)$, the above-induced homomorphism is onto iff the induced homomorphism from $F/\Phi(F)$ into $G/\Phi(G)$ is onto. Write A_k for the elementary abelian subgroup of rank k. Then $F/\Phi(F)$ and $G/\Phi(G)$ are isomorphic to A_r and A_d, respectively. The number of epimorphisms of A_r onto A_d is equal, by duality, to the number of monomorphisms of A_d into A_r, i.e. the number of independent d-tuples in A_r, which is $(p^r-1)\cdots(p^r-p^{d-1})$. Given an epimorphism ψ of F onto $G/\Phi(G)$, let $x^\psi = y\Phi(G)$, and let ϕ be any homomorphism of F onto G inducing ψ. Then x^ϕ can be any of the p^{n-d} elements of $y\Phi(G)$. To determine ϕ we have to specify its value on any one of r free generators of F, and thus the number of homomorphisms ϕ inducing ψ is $p^{r(n-d)}$.

LEMMA 4: *Let p be odd, and let E be an extraspecial group of order p^{2k+1}. The order of $Aut(E)$ is $(p-1)p^{2k+k^2}(p^{2k}-1)(p^{2k-2}-1)\cdots(p^2-1)$, if $exp(E)=p$, and $(p-1)p^{2k+k^2}(p^{2k-2}-1)\cdots(p^2-1)$, if $exp(E)=p^2$.*

Proof: Commutation in E induces a non-degenerate alternate bilinear form from the vector space $V := E/E'$ to E'. First assume that $exp(E)=p$. Then the structure of E is determined by the above form. Let z generate E', and let $x_1, y_1, x_2, \ldots, y_k$ be a set of generators which are a symplectic basis (*modulo* E'), i.e. $[x_i, y_i] = z$, and all other commutators are 1. If $(n,p)=1$, the map $x_i \to x_i^n$, $y_i \to y_i$, $z \to z^n$ determines an automorphism of E, and therefore the map from $Aut(E)$ to $Aut(E')$ is onto, and

$$|Aut(E)| = (p-1)\cdot(\text{the order of the kernel of that map}).$$

Each automorphism in that kernel induces a symplectic linear transformation on E/E' and, given such a transformation, we see, as in the proof of Lemma 2, that this transformation is induced by p^{2k} automorphisms, so

$$|Aut(E)| = (p-1)p^{2k}|Sp(2k,p)| = (p-1)p^{2k+k^2}(p^{2k}-1)(p^{2k-2}-1)\cdots(p^2-1).$$

We recall that $|Sp(2k,p)|$ is equal to the number of symplectic bases of V, and to determine that number we note first that x_1E' can be any one of the $p^{2k}-1$ non-zero vectors in V; then y_1E' can be any one of p^{2k-1} vectors, and then we repeat the process in the $(2k-2)$-dimensional orthogonal complement to $\langle x_1E', y_1E'\rangle$.

Now suppose that $exp(E)=p^2$, let H be the maximal subgroup of E consisting of the elements of order p, and let W be the subspace H/E' of V. The orthogonal complement U of W in V has dimension 1, and since W is odd dimensional, it has a non-trivial radical, which must then be U. Writing $U = Z/E'$, that means that $Z = Z(H)$, and each automorphism of E keeps invariant both H and Z. We choose a symplectic basis as above, choosing $x_1 \in Z$. Then $x_2, \dots, y_k$ lie (*modulo* E') in the orthogonal complement of U, which is W, and y_1 lies outside it. An automorphism α which is the identity on E' fixes y_1^p, which implies that it fixes the coset y_1H. The commutator $[x_1, y_1]$ is also fixed, which implies that the coset x_1E' is fixed, among the cosets of E' in Z. Thus when choosing now the symplectic basis which is the α-image of the given one, its first element is given, and for the others we have the same number of possibilities as before, therefore $|Aut(E)|$ differs from the order in the previous case by the factor $1/(p^{2k} - 1)$.

Note: Naturally, this lemma is not new (see, e.g., [W]), but we gave the proof because a similar argument is needed below in the proof of Theorem 18.

THEOREM 5: *The character degrees of $F_{r,2}$ are $1, p, \dots, p^{[r/2]}$. If $0 < 2k \leq r$, then the number of characters of degree p^k of $F_{r,2}$ is*

$$\frac{p^{r+k^2-3k}(p^r - 1)(p^{r-1} - 1) \cdots (p^{r-2k+1} - 1)}{(p^{2k} - 1)(p^{2k-2} - 1) \cdots (p^2 - 1)}.$$

Proof: Write F for $F_{r,2}$. Since $|F : Z(F)| = p^r$, the character degrees of F are bounded by $p^{[r/2]}$. On the other hand, if $0 < 2k \leq r$, then F maps onto the extraspecial group of exponent p and order p^{2k+1}, and the latter has irreducible characters of degree p^k, hence so does F. Let χ be an irreducible character of degree p^k of F, and let N be its kernel. Then $E := F/N$ is a p-group having a faithful irreducible character, hence it has a cyclic centre. Since $exp(E) = p$ and $cl(E) = 2$, we obtain that $Z(E) = E'$ has order p. Thus E is extraspecial, and since it has an irreducible character of degree p^k, it has order p^{2k+1}, and it is the unique extraspecial group of that order and exponent p. Moreover, E has $p - 1$ irreducible characters of degree p^k, and therefore the number of such characters of F is

$$(p-1) \cdot (\text{the number of normal subgroups } N \text{ such that } F/N \cong E).$$

To count the number of these normal subgroups, we note that the number of epimorphisms of F onto E is given by Lemma 3, and by Lemma 2 the number of N's is the number of those epimorphisms divided by $|Aut(E)|$. Putting all this together yields the formula of the theorem.

2. Degree p

Given any finite group F which is relatively free of rank r in some variety $\mathbf{V}$, the number of its irreducible characters of any degree k can be evaluated in a manner similar to the proof of Theorem 5. We need to have, first of all, a list of the groups in $\mathbf{V}$ which can be generated by r elements and have a faithful irreducible character of degree k. Moreover, for each such group we need to know the number of its faithful irreducible characters of degree k, the number of its generating r-tuples, and the order of its automorphism group. This method is easier to implement when F is a p-group, because of Lemma 3, and because a p-group G has a faithful irreducible character iff it has a cyclic centre. It remains to determine the number of automorphisms of G, and the number of its relevant characters. We formalize the method in

PROPOSITION 6: *Let F be a relatively free finite group in some variety. Let $E_1, \ldots, E_n$ be the set of groups with a faithful irreducible character of degree k which are epimorphic images of F, let t_i be the number of epimorphisms of F onto E_i, and let s_i be the number of faithful irreducible characters of degree k of E_i. Then the number of irreducible characters of degree k of F is*

$$\sum_1^n \frac{t_i s_i}{|Aut(E_i)|}.$$

The next result is another illustration of the same method.

THEOREM 7: *Let $p > 3$ be a prime, and let $F = F_{r,c}$ be a free group of rank r in the variety of groups of exponent p and nilpotency class $c > 2$. Then the number of irreducible characters of degree p of F is*

$$\frac{p^{r-2}(p^r-1)(p^{(r-1)(c-1)+1} + p^{(r-1)(c-1)} - p^r - 1)}{p^2-1},$$

provided $c < p$. For $c \geq p$, the number is the same as for $c = p-1$. In particular, the latter number is the number of irreducible characters of degree p of the biggest finite group of exponent p with r generators.

We require here that $c > 2$, because the case of class two is covered by Theorem 5, and the result there is different. Also, it will be seen in the proof that a group of exponent 3 with a faithful character of degree 3 has class two $(= p-1)$, so again the number of characters is given by Theorem 5.

Proof: Let G be a finite group in the above variety which has a faithful irreducible character of degree p. Then G contains an abelian subgroup H of index p ([BZ], Theorem 18.1). If $x \notin H$, then commutation with x is an endomorphism of H, with kernel $C_H(x) = Z(G)$ and image $[H, x] = [H, G] = G'$, and so $|H : G'| = |Z(G)| = p$. If $y \in H - G'$, then the elementary abelian group H has a basis consisting of the elements $y, [y, x], [y, x, x], \dots, [y, x, \dots x]$, where if the last commutator has weight s, so has $s - 1$ occurrences of x, then $|G| = p^{s+1}$, $cl(G) = s$, and G is a group of maximal class. Note that s determines G uniquely. If $s \geq p$, then G contains the similar group with $s = p$, and the latter is isomorphic to the wreath product of two groups of order p, which has exponent p^2. Thus the assumption $exp(G) = p$ forces $s < p$. If $s = 2$, then G is extraspecial of order p^3, so its characters can be considered as characters of $F/\gamma_3(F)$, and the number of such characters is given in Theorem 5. Assume now that $s \geq 3$. Since G has p^2 linear characters, it has $p^{s-1} - 1$ irreducible characters of degree p. By the same token, $G/Z(G)$ has $p^{s-2} - 1$ irreducible characters of that degree, so G has $p^{s-2}(p - 1)$ faithful irreducible characters.

The number of automorphisms of G is the number of pairs (x, y) as above, i.e. $p^{2s-1}(p - 1)^2$. Since G has two generators, the number of epimorphisms of F onto G is $p^{r(s-1)}(p^r - 1)(p^r - p)$. As above, the number of normal subgroups N with factor groups isomorphic to G is obtained by dividing this number by $|Aut(G)|$, so in all we obtain $(p^{(r-1)(s-1)-1}(p^r - 1)(p^{r-1} - 1))/(p - 1)$ characters corresponding to a given value of s. Here s varies from 3 to c. Summing, and adding the number $(p^{r-2}(p^r - 1)(p^{r-1} - 1))/(p^2 - 1)$ corresponding to $s = 2$, yields our result.

3. Class three

Here we have to separate the prime 3 from the bigger ones, and we start with the latter. To avoid confusion, we denote by $L = L_r$ the free group of rank r in the variety of groups of exponent p and class three. For $r = 2$ we have $|L| = p^5$, with $|L'| = p^3$ and $|Z(L)| = |\gamma_3(L)| = p^2$. It follows that $cs(L) = (1, p^2)$, with multiplicities $(p^2, p^3 - 1)$, and $cd(L) = (1, p)$, with the same multiplicities.

THEOREM 8: *Let L_r be as just defined. Assume that $p > 3$ and $r \geq 3$. Then $cs(L_r) = (1, p^r, p^{\binom{r+1}{2}-1})$, and $cd(L_r) = (1, p, \dots, p^r)$. The classes occur with multiplicities $(p^{\frac{r^3-r}{3}}, p^{\frac{r^3-4r}{3}}(p^{\frac{r(r-1)}{2}} - 1), p^{\frac{r^3-4r}{3}+1}(p^r - 1))$, and the class number is $p^{\frac{r(r^2-4)}{3}}(p^{\binom{r}{2}} + p^{r+1} + p^r - p - 1)$.*

Proof: Write L for L_r. We know that $|L : L'| = p^r$, $|L' : \gamma_3(L)| = p^{\frac{r(r-1)}{2}}$, and $|\gamma_3(L)| = p^{\frac{r^3-r}{3}}$. Let $(x_1, \dots, x_r)$ be a set of free generators of L. Then the elements $[x_i, x_j, x_r]$, $i > j$, are distinct basic commutators, so they are independent elements of $\gamma_3(L)$. It follows that x_r induces, by commutation, a 1-1 map of $L'/\gamma_3(L)$ into $\gamma_3(L)$, and in particular x_r commutes with no element of $L' - \gamma_3(L)$. But x_r does not commute with elements outside $\langle L', x_r\rangle$ either (this holds already in $L/\gamma_3(L) \cong F_{r,2}$). Thus $Z(L) = \gamma_3(L)$, and $C_L(x_r) = \langle Z(L), x_r\rangle$. Now if x is any element outside L', that element lies in some set of r generators of L, and, because L is free, there is an automorphism of L mapping that set of generators onto $(x_1, \ldots, x_r)$, and in particular mapping x to x_r. It follows that $C_L(x) = \langle Z(L), x\rangle$. Moreover, taking an element $y \in L' - Z(L)$, this shows that y does not commute with any element outside L', and thus $C_L(y) = L'$. It is now trivial to determine $cs(L)$ and $k(L)$.

For the character degrees we note first that since L' is abelian, a well known result implies that they are bounded by $|L : L'| = p^r$. Let first $r = 3$. Then $|L| = p^{14}$, $k(L) = p^5(p^4 + 2p^3 - p - 1)$, and L has p^3 linear characters and $p(p^3-1)(p^3+p^2+1)$ characters of degree p. The expressions for $k(L)$ and $|L|$ yield two equations for the numbers n_2 and n_3 of characters of degrees p^2 and p^3, and solving them we obtain $n_2 = p(p^3-1)(p^5+p^4-1)$ and $n_3 = p^4(p-1)(p^3-p-1)$. In particular, both degrees occur, and our claim about $cd(L_r)$ holds for $r = 3$. We will next show that if $r \geq 3$, then L_r has an irreducible character of degree p^r. Since L_{r-1} is a homomorphic image of L_r, this will prove our claim by induction.

Let $x \notin L'$. Then $C_{L'}(x) = Z(L)$, so x fixes $|L'|/p^{\binom{r}{2}}$ elements of L', and the same number of linear characters of L'. Since L/L' has $(p^r - 1)/(p - 1)$ subgroups of order p, the total number of linear characters of L' that are fixed by some subgroup outside L' is less than $|L'|$. Thus there are linear characters of L' whose inertial subgroup in L is L', and these characters induce an irreducible character of degree p^r of L.

Note that that argument fails for $r = 2$.

For $p = 3$ the centralizer $C_L(x)$ is determined in the proof of Theorem 10 below, and it follows that $|C_{L'}(x)| = |L'|/p^{\binom{r-1}{2}}$. The argument still applies, provided $r \geq 5$. We have to consider separately the groups of small rank. From now on let L_r denote the free group of rank r in the variety of groups exponent 3 (we recall that if $r \geq 3$, then L_r has class three).

Lemma 9: *Write $L := L_3$. Then $cs(L) = (1, 3, 27)$, with multiplicities $(3, 26, 78)$, and $cd(L) = (1, 3, 27)$, with multiplicities $(27, 78, 2)$.*

Proof: The structure of L_r was described above, and in particular $|L| = 3^7$, $|L'| = 3^4$, $|Z(L)| = 3$, and $L/Z(L) \cong F_{3,2}$. It follows that each element of $L' - Z(L)$ has three conjugates, and elements of $L - L'$ have 27 conjugates. This yields the class sizes and shows that $k(L) = 107$. Similarly, $k(F_{3,2}) = 105$. Therefore L has two faithful irreducible characters, and the sum of squares of their degrees is $2 \cdot 3^6$, so these degrees are equal to 27. The characters of smaller degrees must occur already as characters of $L/Z(L)$, which has a centre of index 27, so the degrees can be only 1 and 3, and since there are 27 linear characters, the result follows.

THEOREM 10: *Still assuming that $p = 3$, write $L := L_r$, and let $r \geq 4$. Then $cs(L) = (1, 3^{r-2}, 3^r, 3^{\binom{r}{2}})$, these sizes occurring with multiplicities*

$$\Big(3^{\binom{r}{3}}, \frac{3^{\binom{r}{3}-r+2}(3^r-1)(3^{r-1}-1)}{8}, 3^{\binom{r}{3}-r}(3^{\binom{r}{2}} - \frac{(3^r-1)(3^{r-1}-1)}{8} - 1),$$
$$3^{\binom{r}{3}}(3^r-1)\Big).$$

The class number is $3^{\binom{r}{3}-1}(3^{\binom{r-1}{2}} + 3^{r+1} + 3^r - 4)$. If $r \geq 5$, then $cd(L) = (1, 3, \ldots, 3^r)$.

Proof: Let $x_1, \ldots, x_r$ be free generators of L. Then $L'/\gamma_3(L)$ is generated by the (images of the) commutators $[x_i, x_j]$, $i < j$, and $\gamma_3(L) = Z(L)$ is generated by the triple commutators $[x_i, x_j, x_k]$, $i < j < k$. Moreover, the $\binom{r}{2}$ simple commutators and the $\binom{r}{3}$ triple commutators are bases for the corresponding groups. Any element outside L' belongs to a set of free generators, so we may as well assume that it is x_r. It then commutes with $Z(L)$ and with elements of the form $[x_r, y]$, and does not commute with the commutators not involving it. Moreover, its commutators with these latter commutators yield independent generators of $Z(L)$. Therefore

$$C_L(x_r) = \langle Z(L), x_r, [L, x_r]\rangle = \langle Z(L), x_r, [x_1, x_r], \ldots, [x_{r-1}, x_r]\rangle,$$

and x has $3^{\binom{r}{2}}$ conjugates.

Now consider a commutator $u = [x, y]$. If it is not central, then x and y are independent (*mod* L'), so we may as well assume that $u = [x_1, x_2]$. Then $[u, L]$ is the subspace of $Z(L)$ spanned by the commutators $[x_1, x_2, x_k]$, with $2 < k$, so u has 3^{r-2} conjugates. An element of the form uz, with $z \in Z(L)$, has the same centralizer as u, so the same class size. If an element v of L' is not a commutator (*mod* $Z(L)$), then the previous paragraph implies that v does not commute with any element outside L', and thus $C_L(v) = L'$ and v has 3^r conjugates. It remains to count the number of elements like u or v. Each pair of independent elements in L/L' yields one commutator, and another pair which spans the same subspace of L/L' yields, *modulo* $Z(L)$, the same commutator or its inverse, while pairs spanning different subspaces yield commutators that are independent *modulo* $Z(L)$. The number of 2-dimensional subspaces of L/L' is $(3^r - 1)(3^{r-1} - 1)/16$, yielding twice that number of commutators, and we still have to multiply by $|Z(L)|$ to get the number of elements lying in classes of size 3^{r-2}. A routine calculation ends the determination of $cs(L)$ and $k(L)$.

For $cd(L)$, note first that since L_5 maps onto $L_2 \times L_3$, it has irreducible characters of all degrees up to 3^4. Together with the observation, made following the proof of Theorem 8, that L_r has irreducible characters of degree p^r, if $r \geq 5$, this ends the proof.

In the one remaining case, $r = 4$, an intriguing situation occurs.

LEMMA 11: *Let $L := L_4$. Then $cs(L) = (1, 3^2, 3^4, 3^6)$, and these sizes occur with multiplicities $(81, 2340, 468, 6480)$, and $cd(L) = (1, 3, 3^2, 3^3)$, these degrees occurring with the same multiplicities as the class sizes.*

Proof: The claims about the conjugacy classes are just special cases of Theorem 10, so consider the characters. The number of characters of degree 3 is given by Theorem 5, and it is 2340. Theorem 5 also shows that L has at least 468 irreducible characters of degree 9. L has irreducible characters of degree 27, because it maps onto L_3, which has such characters. We count the number of characters obtained like that. First, L_3 has two irreducible characters of that degree. The number of epimorphisms of L onto L_3 is given by Lemma 3, and dividing by $|Aut(L_3)|$ yields the number of subgroups $N \lhd L$ such that $L/N \cong L_3$. Lemma 3 also yields $|Aut(L_3)|$, if we take $r = d = 3$. This yields 6480 characters of degree 27. Since we have already found as many characters as conjugacy classes, we have found them all.

COROLLARY 12: *Among the groups of exponent 3 which have at most four generators, the extraspecial one of order 3^3 is the only one with a faithful irreducible character of degree 3, the extraspecial one of order 3^5 is the only one with a faithful irreducible character of degree 9, and L_3, of order 3^7, is the only one with a faithful irreducible character of degree 27. None has an irreducible character of degree 81.*

4. Class four

THEOREM 13: *Write $K = K_r$ for $F_{r,4}$. Then*

$$cs(K) = (1, p^r, p^{(r+2)(r-1)/2}, p^{(r-1)(2r^2+5r+6)/6}),$$

with corresponding multiplicities

$$(p^{r^2(r^2-1)/4}, p^{(r^4-r^2-4r)/4}(p^{(r^3-r)/3}-1), p^{(r-1)(3r^3+7r^2-2r-12)/12}(p^{r(r-1)/2}-1),$$
$$p^{(r-1)(r^3+r^2-4)/4}(p^r-1)).$$

Proof: By Proposition 1, the orders of the lower central factors of K are $p^r, p^{(r^2-r)/2}, p^{(r^3-r)/3}, p^{(r^4-r^2)/4}$, and $|K| = p^{r(3r^3+4r^2+3r+2)/12}$. Let $x \notin K'$. As in previous cases, we may assume that $x = x_r$ is one of r free generators of K. Then the description of basic commutators shows that if $u \neq x$ is a basic commutator of weight at most 3, then $[u, x]$ is also a basic commutator. Therefore commutation by x induces a 1-1 transformation from $\gamma_i(K)/\gamma_{i+1}(K)$ into $\gamma_{i+1}(K)/\gamma_{i+2}(K)$, provided $i \leq 3$. This shows that $Z(K) = \gamma_4(K)$, and that $C_K(x) = \langle Z(K), x\rangle$, and therefore the elements outside K' lie in classes of size $p^{(r-1)(2r^2+5r+6)/6}$, and there are $p^{(r-1)(r^3+r^2-4)/4}(p^r-1)$ of them. Next, $[\gamma_3(K), K'] = 1$, and we have just seen that the non-central elements of K' do not commute with any element outside K', therefore the non-central elements of $\gamma_3(K)$ have K' for their centralizer, and thus these elements lie in classes of size p^r, and there are $p^{r(r^3-r-4)/4}(p^{(r^3-r)/3}-1)$ of them. Now note that $K'/\gamma_3(K)$ is generated by the commutators $[x_i, x_j]$, $i > j$, and that the commutators of these elements are themselves basic commutators, so independent elements of $\gamma_4(K) = Z(K)$, and therefore the $\binom{r}{2}$ simple commutators generate a subgroup H isomorphic to $F_{\binom{r}{2},2}$. Let Z be a complement to H' in $\gamma_3(K)$. Then $K' = H \times Z$, which shows that if $y \in K' - \gamma_3(K)$, then $C_K(y) = \langle y, \gamma_3(K)\rangle$, and this completes the determination of the class sizes and multiplicities.

We can determine the character degrees, and in one case also the multiplicities, for the groups of small rank of class four.

LEMMA 14: *Let $G := F_{2,4}$ be the free group of rank 2 in the variety of groups of exponent p and class four, $p \geq 5$. Then $|G| = p^8$, $cs(G) = (1, p^2, p^4)$ and $cd(G) = (1, p, p^2)$. The classes and characters occur with multiplicities $(p^3, p^4 - p, p^4 - p^2)$ and $(p^2, p^4 + p^3 - p^2 - 1, p^4 - p^2 - p + 1)$, respectively, and $k(G) = p(2p^3 + p^2 - p - 1)$.*

Proof: The order, class sizes, and multiplicities were already determined in Theorem 13. By Proposition 1, the orders of the lower central factors are

p^2, p, p^2, p^3. Since G has two generators, it is metabelian ([Hu], III.2.12.b), so G' is an abelian subgroup of index p^2, and therefore the character degrees are $1, p$, or p^2. There are p^2 linear characters, and Theorem 7 gives the number of the ones of degree p, so since we know the class number, the number of the characters of degree p^2 is also determined. Alternatively, we can forego the use of Theorem 7, by noting that the order and class number of G yield two equations for the numbers of characters of degrees p and p^2, and solving them we obtain the above numbers.

LEMMA 15: *Let $H := F_{3,4}$ be the free group of rank 3 in the variety of groups of exponent p and class four, $p \geq 5$. Then $|H| = p^{32}$, $cs(H) = (1, p^3, p^5, p^{13})$, and $cd(H) = (1, p, p^2, p^3, p^4)$. The classes occur with multiplicities $(p^{18}, p^{15}(p^8 - 1), p^{21}(p^3 - 1), p^{16}(p^3 - 1))$, so $k(H) = p^{15}(p(p^5 + 1)(p^3 + p^2 - 1) - 1)$.*

Proof: Only the claim about $cd(H)$ needs to be verified. First note that the proof of Theorem 13 shows that $Z(H') = \gamma_3(H)$. Thus $|H' : Z(H')| = p^3$, implying that $cd(H') = (1, p)$. Since each irreducible character of H is a component of some character that is induced from an irreducible character of H', the character degrees of H are at most p^4. Write $H = \langle x, y, z \rangle$. Then $H'/Z(H')$ is generated by the three commutators $[y, x]$, $[z, x]$, and $[z, y]$, and the double commutators of these elements are distinct basic commutators. That means that $|H''| = p^3$, and the non-central conjugacy classes of H' are of size p^2, and are contained in cosets uH''. The proof of Theorem 13 shows that if $u \notin \gamma_4(H)$, then $[u, x] \notin H''$; actually, the subgroup Z there can be chosen to contain $[H', x]$. Therefore x does not keep invariant any class of H' outside $\gamma_4(H)$, and the number of x-invariant classes of H' is $|\gamma_4(H)| = p^{18}$.

Characters of degrees at most p^2 occur already as characters of the group G of the previous lemma, which is a factor group of H. We will show that H has irreducible characters of degrees p^3 and p^4, by showing that H' has characters of both degrees 1 and p whose inertial subgroup in H is H'. The induced characters will then be the desired irreducible characters of H.

Write $K = \langle H', x \rangle$, and let M be any subgroup of H such that $|M : H'| = p$. There are $p^2 + p + 1$ such subgroups, and each of them has the form $M = \langle H', w \rangle$. Here the element w belongs to some set of three free generators of H, so there is an automorphism sending K to M. Therefore the numbers of characters of each degree of H' invariant under M is the same as for K, so in all there are at most $p^{18}(p^2 + p + 1)$ irreducible characters of H' which are invariant under some subgroup containing H' properly. We saw in the proof of Theorem 13 that $H' \cong F_{3,2} \times Z$, where Z is elementary abelian, and checking the orders yields $|Z| = p^{23}$. Therefore H' has more than p^{23} irreducible characters of each degree, and some of these characters cannot be invariant under any subgroup like M, and so induce an irreducible character of H, as required.

Almost identical considerations apply for the next two ranks, and we are content to just state the results, without detailed proofs.

LEMMA 16: *The group $F_{4,4}$ has class sizes $(1, p^4, p^9, p^{29})$, with corresponding multiplicities $(p^{60}, p^{56}(p^{20}-1), p^{71}(p^6-1), p^{57}(p^4-1))$, and the character degrees are $(1, p, \ldots, p^7)$.*

LEMMA 17: *The group $F_{5,4}$ has class sizes $(1, p^5, p^{14}, p^{54})$, with corresponding multiplicities $(p^{150}, p^{145}(p^{40}-1), p^{176}(p^{10}-1), p^{146}(p^5-1))$. The character degrees are $(1, p, \ldots, p^{10})$.*

5. Class two and exponent p^2

We now discuss the variety of groups of exponent p^2, class two, and derived subgroup of exponent p. The last requirement is equivalent to the pth powers being central. The free group P of rank r in this variety, with generators $x_1, \ldots, x_r$, say, has order $p^{r(r+3)/2}$, with $Z(P)$ elementary abelian with a basis consisting of the elements x_i^p, and $[x_i, x_j]$ $(i < j)$. It is easy to see that if $x \notin Z(P)$, then $C_P(x) = \langle x, Z(P)\rangle$, and thus $cs(P) = (1, p^{r-1})$, the class multiplicities are $(p^{\binom{r+1}{2}}, p^{\binom{r}{2}+1}(p^r-1))$, and $k(P) = p^{\binom{r}{2}+1}(p^r + p^{r-1} - 1)$.

THEOREM 18: *Let $P := P_r$ be the free group of rank r in the variety of groups of class two, exponent p^2, and derived group of exponent p. Then $cd(P) = (1, p, \ldots, p^{[r/2]})$. If $2k \leq r$, then the number of irreducible characters of degree p^k of P is p^r times the number given in Theorem 5 for $F_{r,2}$.*

Note that that result applies also for $p = 2$, even though Theorem 5 is stated only for odd p, and even though there is some difference in the proof between $p = 2$ and the odd primes.

Proof: The calculation of $cd(P)$ is identical to the one in Theorem 5, so we have only to determine the multiplicities. For odd p this is a simple corollary of Theorem 5, because the groups P_r and $F_{r,2}$ are isoclinic, so the ratio between the numbers of characters of each degree of the two groups is equal to the ratio between their orders (see [Hp] for isoclinism, and [Ma], section 6, for proofs). That argument does not apply for $p = 2$, so we give a proof that applies for all primes. Let E be a group in the named variety with r generators and a faithful irreducible character of degree p^k. Then $Z(E)$ is cyclic so of order p or p^2, and $E' \leq Z(E)$. If $|Z(E)| = p$, then E is extraspecial of order p^{2k+1}, and this time both extraspecial groups of that order are factor groups of F. Suppose $|Z(E)| = p^2$, and let $Z(E) = \langle z \rangle$. The laws of P imply that $exp(\Phi(E)) = exp(\Phi(P)) = p$, hence $z \notin \Phi(E)$, and if M is a maximal subgroup not containing z, then $E = MZ(E)$, implying $E' = M' = Z(E) \cap M = Z(M)$, a subgroup of order p, so that M is extraspecial and E is a central product of M and $Z(E)$. The character degrees of E are the same as of M, therefore $|M| = p^{2k+1}$ and $|E| = p^{2k+2}$. It is easy to see that both extraspecial groups of order p^{2k+1} yield isomorphic central products with $Z(E)$ (multiply generators of M by z, if necessary), so the structure of E is uniquely determined. Moreover, we must have $2k + 1 \leq r$ for E to be a factor group of P. Thus we have three possibilities for E if $2k + 1 \leq r$, and two possibilities if $2k = r$.

First, let p be odd, and let E be the extraspecial group of exponent p. Then the number of irreducible characters of P with kernel N such that $P/N \cong E$ is calculated in the same way as in the proof of Theorem 5, and is equal to the number given in that theorem (indeed, these characters can be considered as characters of $P/P^p \cong F_{r,2}$). Next, if E is extraspecial of exponent p^2, the only difference is in the order of the automorphism group, which is given in Lemma 4. Therefore the number of relevant characters now is obtained by multiplying the number in the earlier case by $p^{2k} - 1$. There remains the case when E is not extraspecial. In this case E has $p(p-1)$ faithful irreducible characters of degree p^k. We choose the subgroup M above to consist of all elements of order p of E. Then M is characteristic, and an automorphism of E is determined by combining automorphisms of M and of $Z(E)$ which agree on E', implying $|Aut(E)| = p|Aut(M)|$. Since E has now $2k + 1$ generators, the number of epimorphisms of P onto E is $(p^r - p^{2k}) \cdot$ (the previous number), and the number of relevant characters is obtained by multiplying the previous number by $p(p^r - p^{2k})/p$. Collecting everything together, we see that the number of characters is the corresponding number for $F_{r,2}$, multiplied by $1 + (p^{2k} - 1) + (p^r - p^{2k}) = p^r$.

Now let $p = 2$. The only difference from the case of odd primes is in the calculation of $|Aut(E)|$. If E is extraspecial, the map $x \rightarrow x^2$ induces a quadratic form on $E/Z(E)$, with values in $Z(E)$, and this quadratic form determines the structure of E, with the two non-degenerate quadratic forms corresponding to the two extraspecial groups of the right order. Thus $Aut(E)$ maps onto the corresponding orthogonal group. An automorphism in the kernel of this homomorphism is determined by its effect on the $2k$ generators, and each such generator, x say, can be mapped either to itself or to xz, where z is the unique central involution. Thus $|Aut(E)| = 2^{2k}|O^{\pm}(2k,2)|$. When E is not extraspecial, we can consider it as the central product of a cyclic group $Z = \langle z\rangle$ of order four by an extraspecial group M corresponding to O^+, i.e. a central product of dihedral groups. $Aut(E)$ is transitive on the subgroups isomorphic to M which supplement Z, and the stabilizer of M in this action is of order $2|Aut(M)|$, as before. Fix a symplectic basis x_i, y_i for M, where we may assume that all these elements have order 2. A supplement N of Z is generated by elements of the form x_iu_i, y_iv_i, where u_i and v_i are either 1 or z. Different choices of u_i, v_i yield distinct supplements. The subgroup $\langle x_iu_i, y_iv_i\rangle$ is quaternion if $u_i = v_i = z$, and dihedral otherwise, and $N \cong M$ iff the number of quaternion subgroups is even. For each subset of even size $2s$ of the set of indices $\{1,\dots,k\}$, the number of N's with this subset as the set of changes from dihedral to quaternion factors is 3^{k-2s}. Therefore the number of supplements N isomorphic to M is

$$\sum_s \binom{k}{2s} 3^{k-2s} = ((3+1)^k + (3-1)^k)/2 = 2^{k-1}(2^k+1),$$

and

$$|Aut(E)| = 2^{k-1}(2^k+1)2|Aut(M)| = 2^k(2^k+1)2^{2k}|O^+(2k,2)|.$$

Write $n = |O^+(2k,2)|$. Then $|O^-(2k,2)| = n(2^k+1)/(2^k-1)$, and therefore $|Aut(E)|$ is one of the three numbers $2^{2k}n$, $2^{2k}(2^k+1)n/(2^k-1)$, and $2^{3k}(2^k+1)n$. The number of epimorphisms of P onto E is given by Lemma 3, and E has one or two irreducible character of degree 2^k, according to whether E is extraspecial or not. Note also that if $r = 2k$, only the two extraspecial groups can occur as E. Now substitute the value

$$n = 2^{k^2-k+1}(2^k-1)(2^{2k-2}-1)\cdots(2^2-1),$$

and use Proposition 6 to obtain the claimed result.

References

[BZ] Ya. G. Berkovich and E. Zhmud', *Characters of Finite Groups*, Part 2, American Mathematical Society, Providence, RI, 1999.

[Hm] M. Hall, *The Theory of Groups*, Macmillan, New York, 1959.

[Hp] P. Hall, *The classification of prime-power groups,* Journal für die reine und angewandte Mathematik (Crelle's) **182** (1940), 206–214.

[Hu] B. Huppert, *Endliche Gruppen I,* Springer, Berlin, 1967.

[K] E. I. Khukhro, *p-Automorphisms of Finite p-Groups,* Cambridge University Press, Cambridge, 1997.

[Ma] A. Mann, *Minimal characters of p-groups,* Journal of Group Theory **2** (1999), 225–250.

[Me] H. Meier-Wunderli, *Metabelsche Gruppen,* Commentarii Mathematici Helvetici **25** (1951), 1–10.

[VL] M. R. Vaughan-Lee, *The Restricted Burnside Problem,* 2nd ed., Oxford University Press, Oxford, 1993.

[W] D. L. Winter, *The automorphism group of an extraspecial group,* Rocky Mountain Journal of Mathematics **2** (1972), 159–168.