p-groups and pro-p-groups, to infinity and back.

Bettina Eick and Charles Leedham-Green

This lecture is not a lecture, but is rather a shameless advertisement for the book 'The structure of groups of prime power order', London Mathematical Society Monographs, New Series 27, Oxford University Press, ISBN 0-19-853584-1, by Susan McKay and myself. Most of the lectures in this conference would require a book to give an adequate background to the material presented. For this lecture, the book has been written.

The lecture is based on the concept of 'coclass', as defined and elaborated by the previous speaker (Yiftach Barnea), but to remind you, if P is a p-group of order p^n and class c, the coclass of P is defined to be $n - c$.

I have tried counting the mathematicians involved in the coclass project as a means of getting to sleep, and have got up to 16; I mention a few. The initial work that lead to the conjectures was joint work with Susan McKay, who also played the central role in the first major breakthrough in proving the conjectures. The conjectures themselves were made by Mike Newman and myself. The proofs of the conjectures rely heavily on the work of Avinoam Mann and Alex Lubotsky on powerful p-groups, and a huge and brilliant contribution was made by Aner Shalev. The theorem that I wish to discuss proves (with explicit bounds) a conjecture made by Mike Newman and Eamonn O'Brien. An amazing proof of the conjecture, without bounds, was given by Marcus du Sautoy, using zeta functions. His techniques have rather general applicability, but as an unavoidable consequence, do not give such a precise result as the theorem in question.

This theorem is joint work with Bettina Eick, and is about to be published in the Bulletin of the London Mathematical Society.

The coclass project, with the proof of the five conjectures, as displayed in the previous lecture, has got to the point that, given a reasonable problem about p-groups, we can either find a counterexample (as with the class-breadth conjectures); or prove a positive result, which you may or may not like (Bettina Eick proved that the conjecture stating that every finite p-group, with a few obvious exceptions, has order dividing the order of its automorphism group, has only finitely many counterexample among p-groups of coclass r, for fixed p and r); or we can assert that the problem was not reasonable in the first case.

So, does anyone have any problems about finite p-groups that they want solved? (Shocked silence.) How about classifying finite p-groups up to isomorphism? (Dismissive laughter.) Well, I shall classify finite p-groups up to isomorphism in the case $p = 2$ (odd primes in this case are harder; we hope to deal with these groups as well).

I shall illustrate our techniques with the case of 2-groups of coclass 1. There are three such groups of order 2^n (for $n \geq 4$), denoted by D_{2^n}, the dihedral group; SD_{2^n}, the semi-dihedral group; and Q_{2^n}, the quaternion group. All these groups have a cyclic subgroup of order 2^{n-1}, so we can make a table as follows.

$$
\begin{array}{ll}
D_{2^n} & C_{2^{n-1}} : C_2 \\
SD_{2^n} & C_{2^{n-1}} : C_2 \, . \\
Q_{2^n} & C_{2^{n-1}} . C_2
\end{array}
$$

This exhibits the fact that the dihedral and semi-dihedral groups are split extensions of a cyclic group of order 2^{n-1} by a cyclic group of order 2, and the quaternion group is a

non-split extension. The distinction between the semi-dihedral and dihedral groups lies in a (slight) difference in the actions of the cyclic group of order 2 on the cyclic group of order 2^{n-1}. The quaternion and dihedral groups exhibit the same action: the cyclic group of order 2 acts in both cases by inversion; but in the quaternionic case the extension does not split. (Hence the full stop (or period), as opposed to a colon, in the notation.) While proving this trivial result on 2-groups of coclass 1 to your third year undergraduates you observe that the semi-dihedral and quaternion groups have departed from the straight and narrow path followed by the dihedral groups in two different ways. In one case the module has been corrupted, and in the other case the cohomology has caused the problem. There being two different types of obstruction, one observes 'this will never generalise'. Indeed, in the spirit of the coclass conjectures, we note that all three of the above groups have centres of order 2, and that, after dividing out by these centres, we are reduced to dihedral groups. So if we divide out by a contemptibly small normal subgroup we get a dihedral group, and the semi-dihedral and quaternion groups may be ignored. However, we have set our minds on the classification of 2-groups up to isomorphism; so we have to undivide out by the centre, and gaze at the three groups in our table, saying 'Om' until the following thought occurs. The three groups in question (for given n) contain unique cyclic normal subgroups C of order 2^{n-2}, namely the unique subgroup of that order in the maximal cyclic subgroup. Moreover, the quotient group is the Klein 4-group V (elementary abelian of order 4), and we can pick generators x and y of V in such a way that x centralises C and y inverts C. The module structure is identical for all three groups; and all are now of the form $C.V$. So now we have only one invariant to concern ourselves with, name the cohomology.

Homological algebra is, in a sense, at the heart of the theory of p-groups. If all the cohomology groups vanished, all p-groups would degenerate into elementary abelian groups. But because cohomology explains everything it explains nothing, and in general p-groups are too flaccid for us to be able to compute the cohomology groups. However, in this case we can compute the cohomology groups, as follows. I shall write the cyclic group C as T/S, where T is the ring of 2-adic integers, considered as an additive group, and S is the unique subgroup of index 2^{n-2}. Now T, and S, and T/S, are V-modules, where x centralises and y multiplies by -1; and it turns out, by a simple exercise in homological algebra, that $\mathrm{H}^2(V, T/S) \cong \mathrm{H}^2(V, T) \oplus \mathrm{H}^3(V, S)$. Now we do not wish to consider every element of $\mathrm{H}^2(V, T/S)$; only those elements that give rise to 2-groups of coclass 1. Unsurprisingly the classes that correspond to groups of coclass 1 are those that correspond to elements $(\alpha, \beta) \in \mathrm{H}^2(V, T) \oplus \mathrm{H}^3(V, S)$ where α defines the limit group $\mathbf{Z}_2 : C_2$. Here $\mathbf{Z}_2$ is the additive group of p-adic integers, with the generator of C_2 acting as multiplication by -1; so this limit group is the unique pro-2-group of coclass 1, and is the inverse limit of the dihedral groups of order 2^n: that is, $\mathbf{Z}_2 : C_2 = \lim_{\leftarrow} D_{2^n}$. It is easy to see that $\mathrm{H}^2(V, T)$ is cyclic of order 2, so α is constrained to be the unique non-trivial element of this group, and β can be chosen freely from $\mathrm{H}^3(V, S)$, a group isomorphic to $C_2 \times C_2$. Thus we have four cohomology classes to describe three isomorphism classes of groups. This corresponds to the fact that different cohomology classes, that is to say different extension classes, can give rise to isomorphic extension groups. So we need to consider, not elements of $\mathrm{H}^3(V, S)$, but rather equivalence classes of elements of $\mathrm{H}^3(V, S)$

under a certain automorphism group. This is a minor technical detail that will be clear to the experts, and of no interest to the rest.

We can now describe our three classes of groups by presentations that describe these groups as extensions of the form $(T/S).V$ as follows.

$$G_{a,b} = \langle t, x, y \mid t^{2^{n-2}} = 1, \ t^x = t, \ t^y = t^{-1}, \ x^2 = t, \ y^2 = t^{a2^{n-3}}, \ [y,x] = t^{1+b2^{n-3}} \rangle.$$

Here t generates T/S, which is cyclic of order 2^{n-2}; and x and y generate V. Note that $\mathbf{Z}_2 : C_2$ has the presentation

$$\mathbf{Z}_2 : C_2 = \langle t, x, y \mid t^x = t, \ t^y = t^{-1}, \ x^2 = t, \ y^2 = 1, \ [y,x] = t \rangle.$$

The above presentation for $G_{a,b}$ is obtained from this presentation by adding the extra relation $t^{2^{n-2}} = 1$, and introducing the (small) variations given by a and b. Clearly a and b can be regarded as lying in C_2; so we see that the above parametrisation of the presentation may be regarded as a parametrisation by $\mathrm{H}^3(V, S) \cong C_2 \times C_2$. One sees easily that G_{00} is the dihedral group, the isomorphic groups G_{01} and G_{11} are semi-dihedral, and that G_{10} is the quaternion group.

All of the above remarks have been relatively elementary. Our theorem states that these descriptions of the isomorphism classes of 2-groups of coclass 1 can be extended to give descriptions of the isomorphism classes of all sufficiently large 2-groups of any coclass. This requires the full force of the coclass theory (for $p = 2$). At the centre of this theory are conjectures C, D and E, as given in the previous lecture, that describe the pro-p-groups of finite coclass, and assert that there are only finitely many such for fixed p and fixed coclass. These pro-p-groups in the general case play the role of $\mathbf{Z}_2 : C_2$ in the case of coclass 1. To give an example of such a pro-p-group consider the split extension of $T = \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$ by $P = C_2 \wr C_2 \wr C_2$. The wreath product has a base group that is elementary abelian of rank 4, and acts on T by multiplying each of the direct summands powers of -1. Modulo this base group we have $C_2 \wr C_2 = D_8$ that permutes naturally the four summands by the usual permutational wreath product action of D_8. Now certain subgroups of $G = T : P$ will also be of finite coclass. The delicate issue is that these subgroups will generally be of smaller coclass than the parent group. Moreover, these subgroups may be non-split extensions of an open subgroup of T by a subgroup of P, and the fact that the extension is non-split will reduce the coclass. In other words, if the coclass is given, the existence of non-split extensions has the potential to increase the dimensions of the pro-p-groups in question, and this introduced serious problems with proving the coclass conjectures. As another example of a pro-2-group of finite coclass, there is a representation of the quaternion group of order 16, acting in dimension 4 over $\mathbf{Z}_2$: the corresponding (split) extension gives rise to a pro-2-group of coclass 4. Thus all examples of just-infinite pro-2-groups of finite coclass arise either from $\mathbf{Z}_2 : C_2$, or from $\mathbf{Z}_2^4 : Q_{16}$, by taking wreath products with C_2 and taking certain open subgroups. The case of $\mathbf{Z}_2^4 : Q_{16}$ has the property that it is not the 2-adic completion of a discrete representation, since Q_{16} has no faithful 4-dimensional representation over the integers (or over the rationals).

The methodology of this work may be described as follows. We first examine the pro-2-groups of finite coclass (going to infinity), and then use the structure of these infinite

groups to deduce the precise structure of the 2-groups of finite coclass (returning to the finite universe).

Apart from dealing with odd primes, there are also similar theorems to be proved to classify p-groups by rank and obliquity.

I thank Fabrizio Catanese for his very constructive questions during the lecture, and Dan Segal for shedding a bright light on the proceedings.