THE CLASSIFICATION OF GROUPS BY COCLASS

Workshop in Istanbul, June 2011

Charles Leedham-Green, Queen Mary, University of London

Introduction

The theory of finite p-groups has changed its character over the last thirty or so years. Apart from the heroically difficult problems associated with the Burnside groups, most theorems concerning finite p-groups that were proved before 1980 could be proved in a few pages at most, and used relatively little machinery. But now many areas of research in the theory of finite p-groups involve a serious amount of theory, and require a whole book to describe them. The coclass project is such an area, and in describing this work I shall cut many corners, concentrating on the construction of groups rather than on the proving of theorems.

Proofs of the basic theorems are described in the book *The structure of groups of prime-power order* by Susan McKay and myself. As we shall see, the title of the group is probably rather bombastic. Within the theory of finite p-groups our structure theorems are universally applicable, but, as we shall see, they are not universally useful.

The coclass project has involved a large number of mathematicians; let me just acknowledge the fact that the latest research that I am reporting on is joint work with B. Eick, M.F. Newman, and E. O'Brien.

Having mentioned 'coclass' twice already, I should define this term.

Definition. *If P is a group of order p^n and nilpotency class c then the coclass of P is $n - c$.*

So the coclass project studies p-groups by regarding the coclass as the primary invariant. But I present these lectures in part as an essay on how one can study p-groups more generally.

The first suggestion, which is simple enough, is to find some condition that gives us structural information, and then find some way of successively weakening the condition in such a way that the corresponding weakening of the structural information does not deprive the resultant theorem of interest. Here is a very simple example to illustrate the idea. An abelian p-group has derived length 1. This is vacuous. Now we successively weaken the condition of being abelian, taking p-groups of class at most c for $c = 1, 2, 3, \ldots$, and prove that a p-group of class less than 2^d has derived length at most d.

Now let us start from a more subtle place. Consider the set of finite p-groups P that have an automorphism that fixes exactly p elements of P. We shall see that these groups satisfy strong structure theorems, and we continue to improve our understanding of them. Now one can weaken this condition; for example by considering groups with an automorphism of order p^n that fixes exactly p element, or with an automorphism of order p that fixes exactly p^m elements. Since every p-group (of order greater than p) has an automorphism of order p, as we increase m we see that we encompass 'all' finite p-groups; so if theorems can be proved about such groups we have a universal structure theorem for finite p-groups. Now Theorem 8.1 of E.I. Khukhro's brilliant book 'p-Automorphisms

of Finite p-groups' tells us that if P is a p-group with an automorphism group of order p that fixes exactly p^m elements of P then P has a subgroup of small index and very small nilpotency class. Here 'small' means 'bounded as a function of p and m', and 'very small' means 'bounded as a function of p alone. Explicit bounds appear. Now I have a group of order 3^{17} that has an automorphism of order 3 that fixes exactly 3^4 elements of my group. Computing the bound from the proof in the book (by doing Exercise 8.1) I learn that my group has a subgroup of index at most 3^{492} and class 2. So this theorem is universally applicable, but not universally useful. Now the book has been written to be interesting rather than technical, and perhaps a much better bound than 3^{492} could be proved; but even if we were to obtain the best possible bound it would still be far too big to be universally useful.

There is a subtle point about bounds of this type. Suppose, for sake of simplicity, that we are only interested in the case $p = 3$ and $m = 4$, and suppose that we prove that a 3-group with an automorphism corresponding to these parameters must have a subgroup of index k and class 2 for some explicit k, and suppose that this value of k is the best possible. This would not be the last word on the subject. There could be a much better bound that is satisfied with only finitely many counter-examples. In the coclass project we can prove absolute bounds and much better asymptotic bounds in many important cases.

It should be mentioned that a theorem of Khukhro (Theorem 12.15 in his book) proves a structure theorem for p-groups P with an automorphism of order p^n fixing exactly p^m points.

The coclass project starts with groups of coclass 1; but by an easy theorem, a p-group P has an automorphism of order p that fixes exactly p elements if and only if P is a maximal subgroup of a p-group of coclass 1. So we start from essentially the same place as Khukhro, but move in a similar but different direction, as we, naturally, weaken our condition by considering the class of p-groups of coclass at most r for $r = 1, 2, \ldots$ We then produce structure theorems that are, in a sense, much stronger, than Khukhro's We not only prove that our groups have a subgroup of low index and low class, but we also give rather explicit constructions for these groups, modulo a small normal subgroup. But while boasting that our theorems are better than Khukhro's theorems, let us suppose that our group of order 3^{17} has class 13, and hence has coclass 4. Now the generic bound for our small normal subgroup, in the case of a 3-group of coclass 4, turns out to be 3^{11934}. This is probably not best possible. In the case of 3-groups of second maximal class the generic bound given by general theory is 3^{234}; but the best possible generic bound is probably 3^4 in this case. To re-emphasise the point; our theorems, while applicable to all finite p-groups, only give non-vacuous information about p-groups that are of order p^n where n is very much bigger than the coclass, and this will remain the case, even if we manage to strengthen our theorems to give the best possible bounds.

A second methodological suggestion involves pro-finite groups. Let $(G_n : n \geq 0)$ be a sequence of groups, where we assume, for convenience, that $G_0 = \langle 1 \rangle$. Let $\pi_n : G_n \to G_{n-1}$ be a surjection for all n. Then the *inverse limit* of this system is the subgroup G of the Cartesian product $\prod_n G_n$ consisting of all sequences (g_n) such that $g_n \pi_n = g_{n-1}$ for all $n > 0$. We write

$$G = \varprojlim G_n.$$

The inverse limit of a family of finite groups is called a *pro-finite* group, and the inverse limit of a family of finite p-groups is called a *pro-p-group*. More generally, if $\mathcal{C}$ is any class of finite groups the inverse limit of a family of groups in $\mathcal{C}$ is called a pro-$\mathcal{C}$-group. Now G comes with a topology. $\prod_n G_n$, as a product of finite groups, is compact; and G, as a closed subgroup of a compact group, is compact. There is a more general definition of a pro-finite group. The pro-finite groups that can be defined as above are the countably based pro-finite groups. They are also the pro-finite groups whose topology can be defined by a metric. If (g_n) and (h_n) are distinct elements of G then there is an $i \geq 0$ such that $g_j \neq h_j$ for all $j > i$ and $g_j = h_j$ for all $j \leq i$. Then define $d((g_n),(h_n)) = 1/i$.

It turns out that all infinite countably based pro-finite groups are homeomorphic to the Cantor set.

It is usual to require a subgroup of a topological group to be closed in the containing group, as well as being closed under multiplication and inversion. So if G is a topological group, and X is a subset of G, the subgroup of G generated by X is the intersection of the (closed) subgroups of G containing X, and hence is the smallest (with respect to inclusion) (closed) subgroup of G containing X. The derived subgroup of G, the n-term $\gamma_n(G)$ of the lower central series of G, and so forth, are all defined as the group defined, in this topological sense, by the set of commutators that, by definition, defines the corresponding subgroup of a discrete group.

It is easy to see that a closed subgroup of $G = \lim_{\leftarrow} G_n$ is a subgroup of the form $\lim_{\leftarrow} H_n$, where, for all n, H_n is a subgroup of G_n, and π_n maps H_n onto H_{n-1} for all n. The homomorphisms of H_n onto H_{n-1} that define the inverse limit are, of course, the restrictions of the π_n. The open subgroups of G are the closed subgroups of finite index. H is of finite index in G if the index of H_n in G_n is ultimately constant.

My second methodological suggestion is as follows. Suppose that we wish to study a class $\mathcal{C}$ of finite p-groups. It will be convenient to assume that $\mathcal{C}$ is quotient closed. Now analyse the infinite pro-$\mathcal{C}$-groups. (Note that $\lim_{\leftarrow} G_n$ is infinite if and only if $|G_n|$ tends to infinity with n. In this case we may assume that $|G_n| > |G_{n-1}|$ for all n.) If G is a pro-$\mathcal{C}$-group then every finite homomorphic image of G will be in $\mathcal{C}$, since $\mathcal{C}$ is quotient closed; so one infinite pro-$\mathcal{C}$ group gives rise to infinitely many finite groups in $\mathcal{C}$. In general, not every group in $\mathcal{C}$ arises in this way; but, as we shall see, finding the infinite pro-$\mathcal{C}$ groups may be the first step in understanding all the groups in $\mathcal{C}$.

Let us try this idea in the simplest case. Take a prime p, and define $\mathcal{C}_p$ to be the class of cyclic p-groups. This class is quotient closed. I shall write the cyclic group of order p^n additively as $\mathbf{Z}/p^n\mathbf{Z}$. Now define the inverse system $(\mathbf{Z}/p^n\mathbf{Z})$, with π_n mapping $a + p^n\mathbf{Z}$ to $a + p^{n-1}\mathbf{Z}$. The inverse limit is the additive group $\mathbf{Z}_p$ of p-adic integers. We must familiarise ourselves with this group. Let $(a_n) \in \mathbf{Z}_p$, so $a_n \in \mathbf{Z}/p^n\mathbf{Z}$. By abuse of notation I shall write an element $a+p^n\mathbf{Z}$ as a when n is determined by context; so a_n is an integer. So define $b_0 = a_0 = 1$; and $b_1 = a_1$, where $0 \leq b_1 < p$; and then, since $a_2\pi_2 = a_1$, $a_2 = b_1 + pb_2$, where $0 \leq b_2 < p$, and, in general, $a_n = b_1 + pb_2 + p^2b_3 + \cdots$, and so we may write any element of $\mathbf{Z}_p$ uniquely as a formal sum $\sum_0^\infty b_{n-1}p^n$, where $0 \leq b_n < p$ for all n. Note that we can embed $\mathbf{Z}$ as a subgroup of $\mathbf{Z}_p$ by mapping any k in $\mathbf{Z}$ to (k), or, to remove our abuse of notation, to $(k + p^n\mathbf{Z})$. Note that $\mathbf{Z}$ is not a closed subgroup of $\mathbf{Z}_p$; any closed subgroup of a pro-finite group is finite or uncountable. In fact $\mathbf{Z}$ is dense in $\mathbf{Z}_p$,

since any element $a_n + p^n\mathbf{Z}$ is the limit in $\mathbf{Z}_p$ of the sequence (a_n) in $\mathbf{Z}$. In fact $\mathbf{Z}_p$ is a ring, with multiplication $(a_n)(b_n) = (a_n b_n)$. Moreover $\mathbf{Z}$ is a local ring, with maximal ideal (p), and every non-zero ideal of $\mathbf{Z}$ is of the form (p^i) for some $i > 0$. The field of fractions of $\mathbf{Z}_p$ is the field of p-adic numbers $\mathbf{Q}_p$. Any element of $\mathbf{Q}_p$ can be written uniquely in the form $\sum_n b_n p^n$ where $0 \leq b_n < p$ for all n, and the sum is over all integers, but subject to the condition that $b_n \neq 0$ for only finitely many negative values of n. For any integer i the fractional ideal (p^i) is the additive subgroup $p^i\mathbf{Z}_p$.

Exercise. Prove that, in $\mathbf{Z}_2$

$$1 + 2 + 2^2 + 2^3 + \cdots = -1.$$

Solution. The simple solution is to add 1 to the L.H.S. and show that this evaluates to 0. The experienced reader will use the fact that the sum of any convergent infinite geometric series of the form $a + ar + ar^2 + \cdots$ is $a/(1-r)$, which here is $1/(1-2) = -1$.

Section 1. p-groups of maximal class

It turns out that the basic theorems about p-groups of maximal class can be proved by elementary means; though there remain unanswered questions.

In the spirit of these lectures, I shall concentrate more on constructing examples than on proving the structure theorems.

We should start with the case $p = 2$. The classification of the 2-groups of maximal class is an old and easy result; but these groups are also, in some way, typical; so that the whole coclass project might be regarded as the fruit of people thinking about these groups for twenty or thirty years.

Theorem. *Let G be a 2-group of maximal class, and order 2^n, where $n \geq 4$. Then G is isomorphic to exactly one of the following:*

$D_{2^n} = \langle a, t | a^2 = t^{2^{n-1}} = 1, t^a = t^{-1} \rangle$

$Q_{2^n} = \langle a, t | a^2 = t^{2^{n-2}}, t^{2^{n-1}} = 1, t^a = t^{-1} \rangle$

$SD_{2^n} = \langle a, t | a^2 = t^{2^{n-1}} = 1, t^a = t^{2^{n-2}-1} \rangle$.

These three groups are called the dihedral, (generalised) quaternion and semi-dihedral groups of order 2^n. Note that, although these groups are as far from being abelian as possible, in that they have maximal class, they all have an abelian (in fact cyclic) group of index 2. Note also that they all have centre $\langle t^{2^{n-2}} \rangle$ of order 2; and if we divide out by this centre in all three cases the quotient is $D_{2^{n-1}}$. It is also worth noting that if we write these three groups as extensions of the cyclic group of order 2^{n-1} by the cyclic group of order 2 then the Q_{2^n} differs from D_{2^n} in that the extension is not split, and SD_{2^n} differs from D_{2^n} in that the action of a is different.

Since any quotient (of order greater than 4) of any one of these groups is a dihedral group, the only infinite pro-2 group of maximal class is $G = \lim_{\leftarrow} D_{2^n}$. Now D_{2^n} contains a cyclic subgroup $\langle t \rangle$ of order 2^{n-1}, and G contains the inverse limit of these subgroups, which is $\mathbf{Z}_2$, as an open subgroup of index 2. So $G = \mathbf{Z}_2 : C$, where C is cyclic of order 2, and acts on $\mathbf{Z}_2$ by multiplication by -1.

We now turn to the case of arbitrary primes.

As suggested by our philosophy, we start by constructing the infinite pro-p groups of maximal class. We need an analogue of the group $\mathbf{Z}_2 : C_2$. Looking at Blackburn's pioneering work, perhaps as presented in Huppert's *Endliche Gruppen*, it becomes clear that, as in the case $p = 2$, there is exactly one such group for each prime p. This example is constructed as follows. Let $K = K_p$ be the p-th local cyclotomic number field, and let $\mathcal{O} = \mathcal{O}_p$ be its ring of integers. Thus $K = \mathbf{Q}_p[\theta]/(1 + \theta + \cdots + \theta^{p-1})$, and $\mathcal{O}$ is the subring of K that, as an additive group, is a free $\mathbf{Z}_p$-module with basis $\{1, \theta, \ldots, \theta^{p-2}\}$. Now $\mathcal{O}$ is a local ring, with maximal ideal $\mathcal{P} = (\theta - 1)$, and every non-zero ideal of $\mathcal{O}$ is of the form $\mathcal{P}^i$. Then $\mathcal{O} = \mathcal{P}^0 > \mathcal{P} > \mathcal{P}^2 > \cdots$, and $\mathcal{P}^i : \mathcal{P}^{i+1} = p$ for all $i \geq 0$. Now let a be an element of order p, acting on $\mathcal{O}$ by multiplication by θ, and form the split extension $G = \mathcal{O} : C$ where $C = \langle a \rangle$. Now it is easy to see that $G/\mathcal{P}^{n-1}$ is a p-group of maximal class, so G is a pro-p group of maximal class, and in fact is the unique infinite pro-p group of maximal class.

We now turn to the study of arbitrary p-groups of maximal class.

It is convenient to assume that if G is a p-group of maximal class then G is required to have order p^n where n is at least 4. For $n \geq i \geq 2$ let G_i denote the i-th term of the lower central series of G, so $G > G_2 > \cdots > G_n = \langle 1 \rangle$. Now G/G_2 cannot have order p, since if G is any p-group with $G/\gamma_2(G)$ cyclic, then G is cyclic. So since here G is of maximal class it follows that G/G_2 is isomorphic to $C_p \times C_p$, and G_i/G_{i+1} is of order p for $2 \leq i \leq n-1$. Now G_i/G_{i+1} is a central section of G for all i; that is to say, $[G, G_i] \leq G_{i+1}$. In fact, of course, equality holds by definition, But G_i/G_{i+2} is not a central section for $i \leq n$, and it is easy to see that the centraliser in G of G_i/G_{i+2} is a maximal subgroup of G for all i. Call his group 'the i-th two-step centraliser of G'. Now, following Blackburn, define G_1 to be the second 2-step centraliser of G; so now $G > G_1 > G_2 > \cdots$ is a chief series for G. Now $[G_i, G_j] \leq G_{i+j}$ for all i and j (defining $G_k = \langle 1 \rangle$ if $k > n$), and we define the *degree of commutaivity* ℓ of G to be the greatest integer such that $[G_i, G_j] \leq G_{i+j+\ell}$ for all positive i and j, with a suitable convention if G_1 is abelian. By definition, if the degree of commutativity is positive then all the 2-step centralisers of G are equal.

We now come to a fundamental result.

Theorem. *Let G be a p-group of maximal class of order p^n and degree of commutativity ℓ. If $p = 2$ then G_1 is abelian. If $p = 3$ then $\ell \geq n - 4$, so $|G_1'| \leq 3$. If $p > 3$ then $2\ell \geq n - 2p + 4$.*

It follows at once from this theorem that the order of $\gamma_3(G_1)$ is small (bounded in terms of p alone), and that G has a normal subgroup of class 2 and of small index, and that if G is of sufficiently large order then G_1 is nilpotent of class at most 3.

The bound $2\ell \geq n - 2p + 4$ is due to Fernández-Alcober, replacing the earlier bound of $2\ell \geq n - 3p + 6$ which was due independently to Shepherd and to L-G and McKay.

Rather than prove this theorem, I shall produce examples to show that these results cannot be much improved.

The Nottingham group is the subgroup S of the group of automorphisms of the ring $F_p[[t]]$ consisting of automorphisms of the type $t \mapsto \sum_{i>0} a_i t^i$ where $a_1 = 1$. For odd primes p the lower central factors $\gamma_i(S)/\gamma_{i+1}(S)$ are of order p if $i \not\equiv 1 \bmod p - 1$, and are isomorphic to $C_p \times C_p$ otherwise. So $S/\gamma_{p-1}(S)$ is of maximal class, and has derived length approximately $\log_2(p)$, which is in effect as big at it can be for a group of order p^p.

So not only is the nilpotency class of G_1 not bounded but neither is its derived length (as p varies). This exemplifies the distinction between asymptotic and absolute bounds.

The following example will be of more importance to us.

Let p be an odd prime, and consider the group $G_{(n)} = G/\mathcal{P}^n$, where $G = \mathcal{O} : C$ is the infinite pro-p group of maximal class. We call these the 'main line' groups. They are the analogues, for odd primes, of the dihedral groups. With the notation introduced above, $G_{(n),i}$ is $\mathcal{P}^{i-1}/\mathcal{P}^n$, and $G_{(n),1}$ is abelian. We want to change this group so that $G_{(n),1}$ is replaced by a group of nilpotency class 2, and with as large a derived subgroup as possible.

We shall need to consider the exterior square of a P-module A. The tensor square $A \otimes A$ of A is the tensor product $A \otimes_{\mathbf{Z}} A$, where P acts diagonally; that is to say, $(a \otimes b)g = ag \otimes bg$, where $a, b \in A$, and $g \in P$. And then $A \wedge A$ is the quotient of $A \otimes A$ by $\langle a \otimes a : a \in A \rangle$, and the image in $A \wedge A$ of an element $a \otimes b$ of $A \otimes B$ is denoted by $a \wedge b$. So if A is a free abelian group, or a free $\mathbf{Z}/n\mathbf{Z}$-module for some n, freely generated by $\{a_1, \ldots, a_d\}$ then $A \wedge A$ is freely generated by $\{a_i \wedge a_j : i < j\}$, and $a_i \wedge a_j + a_j \wedge a_i = 0$ for all i, j. If A is a $\mathbf{Z}_p$-module then $A \otimes A$ and $A \wedge A$ are defined by replacing $\mathbf{Z}$ in the definitions by $\mathbf{Z}_p$.

Now suppose that A is a $\mathbf{Z}_p(P)$-module for some p-group P. If A is finite this simply means that A is a P-module of order a power of p. Suppose that p is odd, and let $\gamma \in \mathrm{Hom}_P(A \wedge A, A)$. Let B be the image of γ, and suppose that $\gamma(a \wedge b) = 0$ for all $a \in A$ and $b \in B$. Now define a new binary operation $\cdot$ on A by

$$a_1 \cdot a_2 = a_1 + a_2 + \tfrac{1}{2}\gamma(a_1 \wedge a_2).$$

Note that this makes sense as p is odd. Now it is a triviality to check that A, with this operation, is nilpotent of class 2, with $[a_1, a_2] = \gamma(a_1 \wedge a_2)$, and that P acts on this group by automorphisms, so that the split extension $A : P$ can be constructed where A has this new operation. This is a fundamental construction, and we shall extend it later to non-split extensions.

We have looked at the 2-groups of maximal class, and the 3-groups of maximal class are rather similar, and of no great interest, so let us now look at the 5-groups of maximal class. The examples that we already have that are of interest here are finite quotients of $G = \mathcal{O} : C$, where $\mathcal{O}$ is the ring of integers in the 5-th cyclotomic number field, and C is a cyclic group of order 5, so the finite groups that we have are of the form $(\mathcal{O}/\mathcal{P}^n) : C$. To apply our construction we need to consider $\mathrm{Hom}_C(\mathcal{O}/\mathcal{P}^n \wedge \mathcal{O}/\mathcal{P}^n, \mathcal{O}/\mathcal{P}^n)$; but it turns out that we gain considerably in simplicity, and loose only a little in power, if we consider instead $\mathrm{Hom}_C(\mathcal{O} \wedge \mathcal{O}, \mathcal{O})$. Now $\mathcal{O} \wedge \mathcal{O}$ has rank $\binom{4}{2} = 6$, and it turns out that $\mathcal{O} \wedge \mathcal{O}$ is isomorphic to $\mathcal{O} \oplus \mathbf{Z}_5 \oplus \mathbf{Z}_5$, and hence $\mathrm{Hom}_C(\mathcal{O} \wedge \mathcal{O}, \mathcal{O})$ is a free $\mathcal{O}$-module of rank 1. Define $S \in \mathrm{Hom}(\mathcal{O} \wedge \mathcal{O}, \mathcal{O})$ by $S(x \wedge y) = \sigma_2(x)\sigma_{-1}(y) - \sigma_{-1}(x)\sigma_2(y)$, where σ_i is the automorphism of $\mathcal{O}$ defined by $\sigma_i(\theta) = \theta^i$. Now one sees that S maps $\mathcal{O} \wedge \mathcal{O}$ onto $\mathcal{P}$, and more generally, if $x \in \mathcal{P}^i$ and $y \in \mathcal{P}^j$ then $S(x \wedge y) \in \mathcal{P}^{i+j+\epsilon}$, where $\epsilon = 1$ if $i \equiv j \bmod 4$, and $\epsilon = 0$ otherwise.

It remains to construct suitable homomorphisms $\gamma \in \mathrm{Hom}_C(\mathcal{O}/\mathcal{P}^n \wedge \mathcal{O}/\mathcal{P}^n, \mathcal{O}/\mathcal{P}^n)$. We take an element cS, where $c \in \mathcal{O}$, such that cS induces a homomorphism, also denoted by cS, in $\mathrm{Hom}_C(\mathcal{O}/\mathcal{P}^n \wedge \mathcal{O}/\mathcal{P}^n, \mathcal{O}/\mathcal{P}^n)$. If $c \in \mathcal{P}^{j-1} \setminus \mathcal{P}^j$ then the image of cS is $\mathcal{P}^j$, and the condition that $cS(x \wedge y) = 0$ if $x \in \mathcal{O}$ and $y \in \mathcal{P}^j$ is satisfied if $2j \geq n$.

The conclusion is as follows:

Theorem. *If $n \geq 6$ and $n-3 \geq l$ and $2l \geq n-4$ then there exist 5-groups of order 5^n and maximal class with degree of commutativity l.*

The bound $2l \geq n-4$ allows one to construct a 5-group of maximal class that have a maximal subgroup that is nilpotent of class 2 with a big derived subgroup; that is to say, with derived subgroup of order approximately $5^{n/2}$.

Groups constructed according to the above recipe are called *constructible* groups.

It is not too hard to prove that every 5-group G of maximal class has a small normal subgroup N such that G/N is constructible. In fact I think we can take $|N| = p$, so N is the centre of G (or trivial).

It is also not hard to construct the graph defined by all 5-groups of maximal class, where the vertices are the isomorphism classes of 5-groups of maximal class, and vertex joins a group G to $G/\zeta(G)$, where $\zeta(G)$ is the centre of G. It follows, from examining this graph, that the number of isomorphism classes of 5-groups of order n and maximal class is bounded by a function that is linear in n.

This analysis now extends to cover p-groups of maximal class for any prime $p \geq 5$. If $2 \leq a \leq (p-1)/2$ define $S_a \in \mathrm{Hom}_C(\mathcal{O} \wedge \mathcal{O}, \mathcal{O})$ by $S_a(x \wedge y) = \sigma_a(x)\sigma_{1-a}(y) - \sigma_{1-a}(x)\sigma_a(y)$, where now $\mathcal{O}$ is the ring of integers in the p-th local cyclotomic number field, and C is the cyclic group of order p. Now $\mathrm{Hom}_C(K \wedge K, K)$ is of dimension $(p-3)/2$ with these homomorphisms S_a as a basis, so in constructing $\mathrm{Hom}_C(\mathcal{O}/\mathcal{P}^n \wedge \mathcal{O}/\mathcal{P}^n, \mathcal{O}/\mathcal{P}^n)$ we will have $(p-3)/2$ parameters to choose, and every vertex of the graph that is not a leaf will have at least $p^{(p-5)/2}$ immediate descendants; so for $p > 5$ the number of p-groups of maximal class and order p^n increases exponentially with n. There remain serious unanswered questions about the groups of maximal class for $p > 5$, but the above exponential explosion inhibits computation.

Pro-p groups of finite coclass

A difficult theorem (with two very different but difficult proofs) asserts that every infinite pro-p group G of finite coclass r is an extension of a free $\mathbf{Z}_p$-module T of finite rank by a p-group P. It is easy to see that this is equivalent to the statement that every pro-p group of finite coclass is soluble. If G (as above) has a non-trivial centre A then A is finite, and if A is of order p^h then G/A is if coclass $r-h$ (so $h < r$), and we lose little by assuming that the centre of G is trivial. In this case P acts faithfully on T, and G is a *p-adic space group of coclass r*. It is not hard to prove that if every pro-p-group G of finite coclass, with trivial centre, is a p-adic space group then there are only finitely many p-adic space groups of given coclass r. However, it is by no means obvious that there are only finitely many p-adic space groups of given coclass r. As possible indications of the fact that we are dealing here with rather difficult theorems, I remark that there exist infinite pro-p groups G, some p-adic analytic and others not, with the property that the coclass of $G/\gamma_n(G)$ tends to infinity rather slowly. More striking is the following table, due to Bettina Eick.

r	$p=2$	$p=3$	$p=5$
1	1	1	1
2	2	10	95
3	21	1271	1,110,136,753,555,665
4	268	137,299,952,383	
5	15013		

This gives the number of p-adic space groups of coclass r, for some values of p and r. Let us check these entries.

The first row is easy; we have seen that there is a unique infinite pro-p group of coclass 1 for any prime p. Before checking the other entries, a little theory.

A p-adic space group G of finite coclass r has a unique maximal abelian normal subgroup T, and since the quotient $P = G/T$ acts irreducibly on T it follows, by elementary representation theory, that T is of rank $p^x(p-1)$ for some integer x, and a theorem of Susan McKay's tells us that $x \leq r-1$. Suppose first that p is odd. Then the maximal finite p-groups contained in $\mathrm{GL}((p-1)p^x, \mathbf{Q}_p)$ are all conjugate, and are isomorphic to the iterated wreath product of r copies of C_p, and may be constructed as follows. If $x = 0$ then we have seen how C_p acts on the p-h cyclotomic number field, which has dimension $p-1$ over $\mathbf{Q}_p$. If $x = 1$ then we can form the direct sum of p copies of this number field, and $C_p \wr C_p$ acts naturally on this direct sum, and so forth. Thus the case $x = 0$ is the only primitive example. Note that these examples can be equally well defined over $\mathbf{Z}$, rather than over $\mathbf{Z}_p$. If $p = 2$ another, rather unexpected example arises. The generalised quaternion group of order 16 acts irreducibly and primitively as a subgroup of $\mathrm{GL}(4, \mathbf{Q}_2)$, but not as a subgroup of $\mathrm{GL}(4, \mathbf{Q})$, which does not contain a copy of Q_{16}. Thus $\mathrm{GL}(4, \mathbf{Q}_2)$ has two conjugacy classes of maximal finite 2-groups, the iterated wreath product of 3 copes of C_2, which has order 128, and the quaternion group of order 16. Similarly $\mathrm{GL}(8, \mathbf{Q}_2)$ contains 2 conjugacy of maximal finite 2-subgroups, namely the iterated wreath product of 4 copies of C_2, and $Q_{16} \wr C_2$; and so forth.

Of course a finite p-group can be embedded in $\mathrm{GL}(d, \mathbf{Q}_p)$ if and only if it can be embedded in $\mathrm{GL}(d, \mathbf{Z}_p)$, and we are more concerned here with $\mathrm{GL}(d, \mathbf{Z}_p)$. The reason for considering $\mathrm{GL}(d, \mathbf{Q}_p)$ is that subgroups of $\mathrm{GL}(d, \mathbf{Z}_p)$ that are conjugate in $\mathrm{GL}(d, \mathbf{Q}_p)$ need not be conjugate in $\mathrm{GL}(d, \mathbf{Z}_p)$. This is to say, if P is the p-group in question, then P may act faithfully on a $\mathbf{Z}_p$-module T of rank d, and there may be a sub-P-module S of T that is not isomorphic to T. Thus S and T define embeddings of P into $\mathrm{GL}(d, \mathbf{Z}_p)$ that are not conjugate in $\mathrm{GL}(d, \mathbf{Z}_p)$, but are conjugate in $\mathrm{GL}(d, \mathbf{Q}_p)$.

We shall say that P acts *uniserially* on T if the following condition is satisfied. Define $T_0 = T$, and $T_i = [T_{i-1}, P]$ for $i > 0$. Then the condition is that $T : T_i = p^i$ for all i. If this condition is satisfied then the non-zero P-submodules of T are all equal to T_i for some i. It is a triviality to see that a p-adic space group $G = T.P$ is of finite coclass if and only if P acts uniserially on T. The big question is: what is this coclass? It is easy to see that if P is of order p^n then the coclass of G is at most n, and achieves this bound if and only if the extension splits, so $G = T : P$. It is also clear that the coclass of G is at least equal to the coclass of P; whether this bound can be achieved I don't know; probably not. Another unknown. Is it the case that, for odd primes p, the coclass of P tends to infinity

with the coclass of G? For $p = 2$ this fails. It is easy to show how the dihedral group of order 2^n acts uniserially in dimension 2^{n-1}; but D_{2^n} has coclass 1.

We now want a criterion for a p-group to act unserially. Let me restrict myself to the case when P is embedded in the wreath product W of $x+1$ copies of C_p (for example, if p is odd). Now W/W' is the direct product of $x+1$ copies of C_p, which we shall write as the direct sum V of $x+1$ copies of $\mathbf{Z}/p\mathbf{Z}$, and V comes provided with a frame. That is to say, if we choose a generator for each copy of C_p this will give rise to a basis for V, and each basis vector is unique up to a constant multiple, as we change the choice of generator for C_p. Now define a co-ordinate hyperplane to be the subspace of V spanned by all but one of these basis vectors, so V has $x+1$ co-ordinate hyperplanes. Then it is easy to see that P acts uniserially on V if and only if the image of P in W/W' does not lie in any co-ordinate hyperplane.

Armed with this information, we can check the second row of Eick's table. We start with $r = p = 2$. We have $G = T.P$, where P is a $\mathbf{Z}_2$-module of rank 1 or 2. If T has rank 1 then P has order 2 (as P acts faithfully by assumption), and we are led to $G = \mathbf{Z}_2 : C_2$; but then G has coclass 1; so T must have rank 2. Now P is a subgroup of $C_2 \wr C_2$, and if P is to act uniserially it is easy to see that P must be C_4 or $P = D_8$. If $P = C_4$ then we may assume that T is the ring of integers $\mathcal{O}$ in the 2-nd cyclotomic number field, so $T = \mathbf{Z}_2[\theta]/(\theta^2+1)$, and P is generated by an element a that acts by multiplication by θ. Then $G = T : P$ has coclass 2, as required. We see that the submodules of T are all isomorphic to T, and so this is the only example with point group C_4. Now we consider the case $P = D_8$. We need to construct an example $T.P$ that is not split; for otherwise G would have coclass 3. So we take $P = \langle a, b : a^4 = b^2 = 1, a^b = a^{-1}\rangle$, and first construct the extension $H = T : P$, where $H = \langle a, b, t \ : \ a^4 = b^2 = 1, a^b = a^{-1}, [t, t^a] = t^{a^2}t = 1, t^b = 1\rangle$, and then define $G = \langle a, bt\rangle$. It is easy enough to check that G has coclass 2, and that any pro-2-group of coclass 2 with point group D_8 is isomorphic to G. There is one subtle point. If T_i is the P-submodule of T of index p^i then $T_i \cong T_{i+2}$ for all i, indeed $T_{i+2} = 2T_i$, but $T_0 \ncong T_1$, since b centralises t, but centralises no element of $T_1 \setminus T_2$. So if $t_1 = [t, a]$ and $G_1 = \langle a, bt_1\rangle$ then $G = T_1.D_8$ and $G_1 = T_2.D_8$, so how are these groups isomorphic? The answer is that there is an outer automorphism of D_8 that takes b to ab, and it is easy to see that ab centralises t_1, so this automorphism extends to an isomorphism of G onto G_1.

The other entries in the table may be checked in the same way.

The definition of 'consructible group' needs to be extended to include p-groups of coclass r. In the case of a split space group $T : P$ there is no problem, and a constructible group is defined in terms of homomorphisms in $\mathrm{Hom}_P(T \wedge T, T)$. If the space group $G = T.P$ is not split then G is a subgroup of finite index in a split space group $H = T_{-i} : P$ for some (small) i, and a constructible group for G is a corresponding subgroup of a constructible group for H.

Classification up to isomorphism

We have seen how to construct all pro-p groups of finite coclass, and from these we have seen how to construct all constructible groups. Moreover, every sufficiently large p-group P of coclass r has a normal subgroup N of (p, r)-bounded order such that P/N is constructible.. It remains to classify the p-groups of coclass r up to isomorphism. This is ambitious, so our classification theorem (or rather conjecture) is not completely explicit.

Define a graph $\mathcal{G}(p,r)$ whose vertices are the p-groups of coclass at most r, and whose edges join a group G of class c to $G/\gamma_c(G)$. The infinite chains in $\mathcal{G}(p,r) \setminus \mathcal{G}(p,r-1)$ correspond to the pro-p groups of coclass r. There are only finitely many of these infinite chains, so if $|P|$ is big enough then P can lie in at most one infinite chain. In this case P is a *main line* group for the corresponding pro-p group. So D_{2^n} is a main line group for $\mathbf{Z}_2 : C_2$. Now let $\mathcal{G}(p,r,k)$ be the full subgraph of $\mathcal{G}(p,r)$ consisting of groups that are at a distance (in the graph) of at most k from a main line group. If $p = 2$ then for some $k = k(r)$ almost all groups in $\mathcal{G}(p,r) \setminus \mathcal{G}(p,r-1)$ lie in $\mathcal{G}(p,r,k)$. Note that $k(1) = 1$. Now let $\mathcal{G}(G,k,i)$, where G is a pro-p group of coclass r, be the subgraph of $\mathcal{G}(p,r,k)$ whose nearest (in the graph) mainline ancestor has order p^i (so i must not be too small) and that is a quotient of G. If i is big enough, and if $G = T.P$ where T has rank d, then $\mathcal{G}(G,k,i)$ is isomorphic to $\mathcal{G}(G,k,i+d)$. This theorem was first proved by Marcus duSautoy, using zeta functions, and later by Eick and L-G using cohomology, and finding explicit bounds.

It will be seen that this reduces the calculation of $\mathcal{G}(p,r,k)$ to a finite calculation for given p,r,k, and hence, for $p = 2$, reduces the calculation of $\mathcal{G}(p,r)$ to a finite calculation for any given r.

For odd primes the situation is more complicated, but a conjecture in a paper by Eick, L-G, Newman and O'Brien http://www.math.auckland.ac.nz/õbrien/research/coclass.pdf will, if proved, reduce the construction of $\mathcal{G}(p,r)$ to a finite calculation for all p and r. That is to say, a single calculation for each fixed value of p and r. The bulk of this paper is concerned with the 3-groups of coclass 2. In particular, we construct all the constructible groups, which is easy, and determine their isomorphism classes, which is a delicate matter. This raises our understanding of the 3-groups of coclass 2 to the same level as our understanding of the 5-groups of maximal class. A proof of the conjecture (with sensible bounds) will enable us to complete the classification in both cases, and we will then have a complete classification of the p-groups of coclass r (given a little more computation) for $(p,r) \in \{(2,1),(2,2),(2,3),(3,1),(3,2),(5,1)\}$. The case $(2,4)$ may be (or become) technically feasible.

My thanks to the organisers for their very many kindnesses, and for organising such a splendid and unforgettable conference.