55th BMC: 7th–10th April 2003, Birmingham

Gareth Evans

April 13, 2003

Contents

1 Introduction 3

2 Monday 7th April 4

2.1 Michael Harris: The Local Langlands Conjecture 4

2.2 John Conway: Groups and Lattices 4

3 Tuesday 8th April 5

3.1 Martin Bridson: Curvature and Decidability in Geometry and Group Theory 5

3.2 Caroline Series: Recent Developments in Hyperbolic Geometry 6

3.3 Joseph Chuang: Symmetric Groups and Derived Categories 7

3.4 Paul Garcia: Major Percy Alexander MacMahon (1854-1929) 9

3.5 J. Tattersall: Mathematical Questions and their Solutions from the Educational Times 10

3.6 Peter L. Griffiths: John Machin and the Computation of π 11

3.7 Sergio Plata: The Work and Words of P.M.S. Blackett. The Early Years of OR (1939-1945) 11

3.8 Dan Segal: Subgroups of Profinite Groups and Uniform Bounds for Finite Groups . . 12

3.9 Jonathan Alperin: The Stable Equivalence Problem 14

4 Wednesday 9th April 16

4.1 Tom Körner: Besicovitch via Baire 16
4.2 Tom Bridgeland: Derived Categories in Algebraic Geometry 16
4.3 George Willis: A Canonical Form for Automorphisms of Totally Disconnected Groups 17
4.4 C. Roever: Co-Word Problems in Groups 19
4.5 Martyn Quick: Probabilistic Generation of Wreath Products of Non-Abelian Finite Simple Groups 20
4.6 John Bray: Double Coset Enumeration and Symmetric Presentations 20
4.7 Corinna Wiedorn: A 7-local Identification of the Monster 21
4.8 Simon Goodwin: Prehomogeneous Spaces for Parabolic Group Actions in Classical Groups 21
4.9 Attila Maróti: Bounding the Number of Conjugacy Classes of a Permutation Group . 22
4.10 George Andrews: Ramanujan's Lost Notebook, Reflections After 27 Years of Study . . 23
4.11 Simon Singh: Cracking the Cipher Challenge 23

5 Thursday 10th April **24**

5.1 Roderick Gow: New Light on William Rowan Hamilton 24
5.2 Edmund Robertson: Tait, Maxwell and Knot Theory 25
5.3 Tim Gowers: Interactions Between Harmonic Analysis and Combinatorial Number Theory 25

1 Introduction

This is a collection of notes I took whilst attending the 2003 BMC in Birmingham between the 7th and the 10th of April. The notes are sorted chronologically and the abstracts were taken from the conference website, namely http://www.mat.bham.ac.uk/bmc.

2 Monday 7th April

2.1 Michael Harris: The Local Langlands Conjecture

Time: 16:15 – 17:15. *Type:* Plenary Lecture.

Abstract

As a first step to understanding solutions to systems of polynomial equations $P_i(X_1, X_2, \ldots, X_n)$ with coefficients in the rational number field $\mathbb{Q}$, one views them as equations with coefficients in its various p-adic completions $\mathbb{Q}_p$, whose Galois theory is considerably simpler. Local class field theory classifies abelian extensions of a finite extension F of $\mathbb{Q}_p$ in terms of characters of the multiplicative group $F^\times$ of F. As a complement to his conjectures linking Galois theory of number fields to automorphic forms, Langlands proposed a non-abelian version of local class field theory, classifying non-abelian extensions of the p-adic field F, or rather n-dimensional representations of its absolute Galois group, in terms of representations of the totally disconnected topological group $GL(n, F)$.

The lecture is a report on the proof of this conjecture, obtained in joint work with Richard Taylor. As in the Lubin-Tate version of abelian local class field theory, the first step is to exploit the completeness of the local field F by working with formal power series rather than polynomial equations.

2.2 John Conway: Groups and Lattices

Time: 17:15 – 18:15. *Type:* Plenary Lecture.

(No Abstract Available)

3 Tuesday 8th April

3.1 Martin Bridson: Curvature and Decidability in Geometry and Group Theory

Time: 09:00 – 10:00. *Type:* Morning Lecture.

Abstract

How can one tell if two “given” manifolds, knots, or groups are “the same” (i.e. isomorphic in the appropriate category)? To what extent can such decision processes be simplified if one restricts attention to objects that satisfy a curvature restriction? In the case of groups, what does curvature mean?

As one explores issues of complexity, what horrors can lurk amongst the subgroups of seemingly benign groups?

I’ll explain how the serious study of such questions began with Dehn’s work on low-dimensional manifolds. I’ll then discuss recent results concerning the interplay of curvature and decision processes. I’ll explain why the isomorphism problem is unsolvable among arbitrary manifolds in high dimensions but solvable among negatively curved manifolds. I’ll then present recent results concerning the non-positively curved case.

This lecture will be accessible to an audience with no background in decision problems or curvature.

The word problem asks which words in the alphabet of a group correspond to the identity word. There is also the conjugacy problem and the isomorphism problem. Max Dehn (in 1906-1910) worked on the presentation of a fundamental group of a knot. A compact, orientable, 3-manifold M with $\delta M \neq \phi$ supports a metric of curvature $\leqslant 0$ iff every 2-sphere in M bounds a ball. Knot/link complements satisfy these hypotheses. An unsolvable problem: there exists recursively enumerable subsets (of $\mathbb{N}$) that are not recursive.

Transition to Group Theory. If $S \subset \mathbb{N}$ is a recursively enumerable set that is not recursive, then $G = \langle a, b, t \mid [t, b^n a b^{-n}] = 1 \ \forall\, n \in S \rangle$ has an unsolvable word problem.

The Higman Embedding Theorem says that every recursively presentable (i.e. ‘thinkable’) group G can be (algorithmically) embedded in a finitely presented group.

Corollary 3.1 *(Novikov, Boone) There exists finitely presented groups whose word problems are unsolvable. (Proof: Take G from the proposition).*

The isomorphism problem for finitely presented groups is unsolvable (by construction).

Theorem 3.2 *(Markov) In dimension $n \geqslant 4$, there is no algorithm to decide isomorphism amongst arbitrary sequences of closed (smooth, topological or PL) manifolds.*

We impose hypotheses to improve the situation, e.g. the homeomorphism problem is solvable amongst compact 3-manifolds and the isomorphism problem is solvable amongst 3-manifold groups (these are non-trivial consequences of the geometrisation conjecture).

In higher dimensions, we bring in curvatures. Let $n \geqslant 5$ and let M and N be closed non-positively curved n-manifolds. If $\pi_1 M \cong \pi_1 N$, then $M \cong N$ (homeomorphic).

Theorem 3.3 *(Sela) The isomorphism problem is solvable in the class of torsion-free hyperbolic groups that do not split over* $\{1\}$ *or* $\mathbb{Z}$*.*

Theorem 3.4 *(Gromov)* $\delta_r(n) \simeq n$ *iff* Γ *is hyperbolic.*

We use Cayley graphs to visualise hyperbolic groups.

Theorem 3.5 *The isomorphism problem is unsolvable in the class of combable groups.*

3.2 Caroline Series: Recent Developments in Hyperbolic Geometry

Time: 10:10-11:00. *Type:* Morning Lecture.

Abstract

It is now over twenty years since Thurston first announced his remarkable ideas about the existence of geometric structures on 3-manifolds. In the last few years, there have been a number of spectacular advances which have brought us to a state where we can now answer many questions posed but unresolved at that time.

In this talk I shall try to explain some of these developments, many of which involve deformations of hyperbolic structures, and outline how some of my recent work fits into this big picture.

Thurston's Geometrisation Conjecture (1976) says that any 3-manifold can be cut up canonically into pieces each of which carry one of eight possible types of geometrical structure. The cuts are along spheres and tori and the most surprising and most common type of geometry is hyperbolic.

We model $\mathbb{H}^3$ by the upper half-space. Any Mobius map $z \mapsto \frac{az+b}{cz+d}$ on $\mathbb{C} \cup \infty$ extends (by inversions in hemispheres) to an orientation preserving isometry of $\mathbb{H}^3$. So identify $\mathrm{Isom}_+\mathbb{H}^3$ with $\mathrm{PSL}(2,\mathbb{C})$. Further, if M^3 has a hyperbolic structure then $G = p(\pi_1(M)) \subset \mathrm{PSL}(2,\mathbb{C})$ is discrete and $M \cong \mathbb{H}^3/G$.

The Orbifold Geometrisation Conjecture (Thurston, 1987) says that any compact 3-manifold which is orbifold irreducible and orbifold-atoroidal admits a geometric structure. A sketch proof of this theorem was given, the details of which were completed in 1998-2000, with extra theory being uncovered by this process.

The hyperbolic cone manifold structure still gives the holonomy representation $p : \pi_1(M - \Sigma) \to \mathrm{Isom}_+\mathbb{H}^3 = \mathrm{PSL}(2, \mathbb{C})$. Hyperbolic cone manifolds are isometric iff their holonomy representations are conjugate in $\mathrm{Isom}\,\mathbb{H}^3$.

3.3 Joseph Chuang: Symmetric Groups and Derived Categories

Time: 11:40 - 12:30. *Type:* Morning Lecture.

Abstract

Michel Broué has used derived categories to elucidate certain remarkable numerical coincidences observed in finite groups. His precise conjectures along these lines are among of the most intriguing open problems in modular representation theory. I will try to explain some of the ideas involved in a proof of his conjectures in the case of symmetric groups.

Consider the Monster Group M. It has a Sylow-11 subgroup H where $|H| = 72600$ ($|M| \sim 8 \times 10^{53}$). If G is a finite group, consider $\mathbb{C}G = \{\sum_{g \in G} \alpha_g g \mid x_g \in \mathbb{C}\}$, a group ring; and let us look at the irreducible degrees.

M has 194 irreducible degrees while H has 50, none of which is divisible by 11. Moreover, exactly 50 of the 194 irreducible degrees of M are not divisible by 11.

Let G be a finite group and P a Sylow p-subgroup. Set $H = \mathrm{Norm}_G(p)$.

Conjecture 3.6 *(McKay, 1971) G and H have the same number of irreducible degrees not divisible by p.*

In modular group rings, we have $\mathbb{C}S_3 \simeq \mathrm{Mat}_2(\mathbb{C}) \times \mathbb{C} \times \mathbb{C}$, $\mathbb{F}S_3 \simeq \mathrm{Mat}_2(\mathbb{F}_2) \times (\mathbb{F}_2[x]/(x^2))$, and $\mathbb{F}_3 S_3$ is indecomposable.

If G is a finite group and if k is a field, then $kG \simeq B_0 \times B_1 \times \ldots \times B_n$ is a product of indecomposable rings known as *blocks*. Let $I = \{\sum \alpha_g g \mid \sum \alpha_g = 0\} \subseteq kG$. There is a unique block not contained in I called the principal block, denoted $B_0(kG)$.

Let k be a field, $\bar{k} = k$, and $\mathrm{char}(\bar{k}) = p$.

Conjecture 3.7 *(Alperin, 1986) If P is abelian then $B_0(kG)$ and $B_0(kH)$ have the same number of classes of irreducible modules.*

The following tables demonstrate the above conjecture. The first table shows the number of irreducible degrees mod 11 while the second table shows the number of irreducible degrees mod 13:

	±1	±2	±3	±4	±5
M	10	10	10	10	10
H	10	10	10	10	10

	±1	±2	±3	±4	±5	±6
M	12	18	12	6	3	4
$\mathrm{Norm}_H(p)$	12	18	12	6	3	4

Conjecture 3.8 *(Broué, 1990) If P is abelian then $D(B_0(kG)) \approx D(B_0(kH))$. Note that this conjecture implies the previous two conjectures.*

Let R be a ring. The objects of the derived category $D(R)$ are complexes of R-modules of the form

$$\ldots \xrightarrow{d_2} X_1 \xrightarrow{d_1} X_0 \xrightarrow{d_0} X_{-1} \xrightarrow{d_{-1}} \ldots$$

with $d_i d_{i-1} = 0$. Let $\mathrm{Irr}(R)$ be the set of isomorphism classes of irreducible R-modules. If B and B' are blocks then $D(B) \approx D(B') \Rightarrow \mathbb{Z}_{\mathrm{Irr}}(B) \cong \mathbb{Z}_{\mathrm{Irr}}(B') \Rightarrow \#\mathrm{Irr}(B) = \#\mathrm{Irr}(B')$.

Broué's conjecture is true for symmetric groups. One part of the proof features joint work with Raphael Rouquier:

Theorem 3.9 *Let k be an algebaically closed field. Let B and B' be blocks of kS_n and $kS_{n'}$ respectively. Then $D(B) \approx D(B') \Leftrightarrow \#\mathrm{Irr}(B) = \#\mathrm{Irr}(B')$.*

Example 3.10 If $\mathrm{char}(k) = 3$ and $\#\mathrm{Irr}(B) = 5$, then $B_0(kS_6) = B_6$, $B_0(kS_7) = B_7$, $B_0(kS_8) = B_8, B_8'$ and so on, and all the derived categories are equivalent.

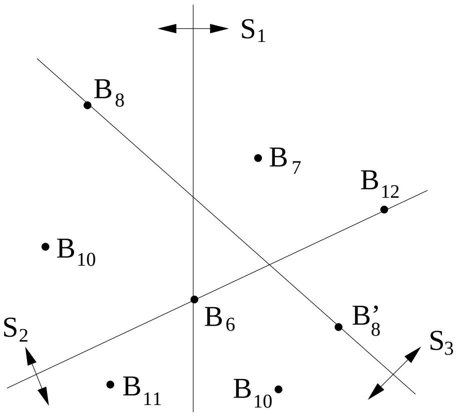
Let us now consider the Fock space approach to symmetric groups (Lascoux-Leclerc-Thibon (1998), Ariki, Gryrowski, ...). We have $\widehat{S\ell_p}(\mathbb{C}) \in$ the sequences $e_0, \ldots, e_{p-1}$, $f_0, \ldots f_{p-1}$ and $h_0, \ldots, h_{p-1}$, and we have $f = \oplus\mathbb{C}\lambda =_{n\geqslant 0}^{\oplus} \mathbb{C}(\mathrm{Irr}(\mathbb{C}S_n))$, a λ partition. Consider the case $p = 3, \lambda = (4, 3, 1)$ with the following diagram:

$$\begin{array}{cccccc}
\mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{0} & 1 & 2 \\
\mathbf{2} & \mathbf{0} & \mathbf{1} & 2 & 0 & \\
\mathbf{1} & 2 & 0 & 1 & & \\
0 & 1 & 2 & & &
\end{array}$$

For subtraction, we have $e_0\lambda = (3, 3, 1)$, $e_1\lambda = (4, 2, 1) + (4, 3)$, and $e_2\lambda = 0$. For addition, we have $f_0\lambda = (4, 3, 1, 1)$, $f_1\lambda = (5, 3, 1)$, and $f_2\lambda = (4, 4, 1) + (4, 3, 2)$. For addition $-$ subtraction, we have $h_0\lambda = (1 - 1)\lambda = 0$, $h_1\lambda = (1 - 2)\lambda = -\lambda$, and $h_2\lambda = (2 - 0)\lambda = 2\lambda$. With all of this, we get $[e_i, f_i] = h_i$ and $[e_i, [e_i, e_{i+1}]] = 0$ for $p > 2$.

Now let $\mathcal{F}_p =_{n\geqslant 0}^{\oplus} \mathbb{C}(\mathrm{Irr}(kS_n))$ with $\mathrm{char}(k) = p$. $\widehat{S\ell_p}(\mathbb{C})$ acts on this, and further it is equal to $\underset{\Psi}{\oplus}\ \mathbb{C}(\mathrm{Irr}(B))$ with weight space decomposition ($\Psi =$ Blocks B of kS_n for $n \geqslant 0$). In particular, $W = \langle s_0, \ldots, s_{p-1} \rangle$ (the Weyl group) acts transitively on {weight spaces of a fixed dimension} = {blocks with a fixed number of irreducibles}.

To prove this theorem, we need to show that $D(B) \approx D(S_i(B))$ for all B and i. As an example, consider the case $p = 3$ so that $W = \langle s_0, s_1, s_2 \rangle$ and $\#\mathrm{Irr}(B) = 5$.



To each simple reflection s_i associate $\theta_i = \exp(-f_i)\exp(e_i)\exp(f_i)$. Rickard (1990) constructed Θ_i acting on $\bigoplus_{n\geqslant 0} D(\mathcal{L}S_n)$ lifting θ_i. Now lift e_i and f_i acting on $\mathcal{F}_p$ to E_i and F_i acting on $\bigoplus_{n\geqslant 0} kS_n$-mod and then use the divided powers (Scopes, Puig, Ariki, Gryrowski).

Proposition 3.11 *Suppose M is an irreducible module with $D_iM = 0$ and $K_iM = \alpha M$. Then $\Theta_i(F_i^{(j)}(M)) \cong F_i^{(\alpha-j)}(M)[j]$.*

3.4 Paul Garcia: Major Percy Alexander MacMahon (1854-1929)

Time: 14:00 - 14:20. *Type:* Splinter Group: History of Mathematics.

Abstract

Percy Alexander MacMahon's work in ballistics led him to make important contributions to the fields of invariant theory and partition theory, and he believed combinatory analysis should be at the core of mathematics. His book, Combinatory Analysis, is still in print, more than 85 years after it was first published.

MacMahon was described in 1909 by a Member of Parliament as 'one of the leading mathematicians of our day'. He received four honorary doctorates during his lifetime, was a Fellow of the Royal Society, President of the London Mathematical Society (and an active member of the Council for many years), President of the Royal Astronomical Society, President and General Secretary of the British Association, and Vice President of the 5th International Congress of Mathematics in Cambridge (1912). He also was awarded the Royal Society Medal, the Sylvester Medal of the Royal Society and the De Morgan Medal of the London Mathematical Society.

MacMahon held posts as a Major in the Royal Artillery, a Professor of Physics at the Royal Artillery College, Deputy Warden of the Standards at the Board of Trade, and was an accomplished billiards player and congenial host.

A popular and respected figure in his lifetime, MacMahon is now known only to a few combinatorialists and puzzle enthusiasts. In this talk, I will describe how he rose in just a few years from the obscurity of the Royal Artillery's No 1 Mountain Battery on the North West Frontier of the British Indian Empire to become a friend and colleague of such well known figures as J. J. Sylvester, G. H. Hardy and S Ramanujan (whom he is reputed to have trounced soundly in calculating contests).

- Started in Ballistics.
- Extended Allegret's Problem in 1883.
- Partitions is where he made his mark.
- He published a book on combinatory analysis.
- A pamphlet with a short summary on MacMahon was given out during this talk.

3.5 J. Tattersall: Mathematical Questions and their Solutions from the Educational Times

Time: 14:20 - 14:40. *Type:* Splinter Group: History of Mathematics.

Abstract

The Educational Times was first published in England in the fall of 1847. In 1861 it was adopted by the College of Preceptors as their official publication. The journal contained notices of available scholarships, lists of successful candidates on examinations given by the College, notices of vacancies for teachers and governesses, reviews, and textbook advertisements. But undoubtedly, the most important feature of this monthly journal was a section devoted to mathematical problems and their solutions. From 1864 to 1918 problems and solutions which had appeared in the journal were republished semiannually in Mathematical Problems and Their Solutions from the 'Educational Times'. Many prominent European and American mathematicians contributed to the problems section of the journal. We will exhibit some interesting mathematical contributions and a few statistics gleaned from a recent classification scheme of the over 18,000 problems posed in The Educational Times.

- There were only ever three editors.
- 54% of the problems were geometry problems.
- There were complaints about the problems being too tough!

3.6 Peter L. Griffiths: John Machin and the Computation of π

Time: 14:40 - 15:00. *Type:* Splinter Group: History of Mathematics.

Abstract

The main historical techniques for an accurate computation of π include, 1) Archimedes's Half Angle Formula and its reversion the Double Angle Formula. 2) James Gregory's Arctan Series discovered in 1671. 3) John Machin's recognition in 1706 of the similarity between the Double Angle formula and the product of two complex numbers. There will be a reference to Abraham de Moivre's extension in 1708 of John Machin's double angle formula and also to Francis Maseres's comments in 1796 on Machin's discovery. Machin's formula was used by W. Shanks in 1874 and by D.F. Ferguson in a supporting role in 1947.

- A booklet of lecture notes was given out during this talk.

3.7 Sergio Plata: The Work and Words of P.M.S. Blackett. The Early Years of OR (1939-1945)

Time: 15:10 - 15:30. *Type:* Splinter Group: History of Mathematics.

Abstract

Operational research has its origins in WWII in England, with P.M.S. Blackett (Lord, Nobel Prize laureate, President of Royal Society and scientific advisor to the government) being one of the main characters involved in these early years. He directed the operational research sections. These sections were basically scientific teams working on the analysis of war operations. The early years of Operational Research gave a philosophical and organisational background to the further development of the discipline. But most of all it gave a crucial impact to the non-mathematical audience, including the general public. More than a technical basis or explicit methodology to develop the discipline, these war years extended, with the aid of literature and language, the applicability of science to other areas of human activity, like industry, transportation or agriculture. Concerning the methodology of operational research, one can see that some of the ideas permeated from Blackett's previous studies in cosmic radiation. An important anchor to extrapolate and compare this point of view can be found in his annotations on cosmic rays [Blackett P.M.S., 1935]. It is often by starting from the scientific background that the epistemological process develops, rather than from the moment of the report issue or the problem-posing itself, i.e., not from the moment of observation or picturing the very first images, but far before at the moment when the scientific background was born to affect the perception, methods and vision of Blackett that biased the way of communicating complex ideas such as a whole model of an operation of war. In this paper I will try to show some factors within the system of symbolic thought that triggered these scientific advisors' (Blackett's case) way of working. I will also analyse how elements of language achieved cognition, via the study of the appearance of writing forms, their denotation to syntax,

connation and, in general, to revise the structure of literary texts within the scientific influence, as well as the mathematical tools developed and used by these teams.

- Operational Research began during World War II.
- The work was similar to previous work done on cosmic rays by Blackett.
- There was no ‘real data’ to work with in the beginning.

3.8 Dan Segal: Subgroups of Profinite Groups and Uniform Bounds for Finite Groups

Time: 15:30 - 16:10. *Type:* Special Session on Group Theory.

Abstract

In a profinite group, every open subgroup has finite index. Is the converse true? Certainly not in general, but it may be if one sticks to finitely generated profinite groups. Recently Nikolay Nikolov and I have proved that if G is a finitely generated profinite group then all normal subgroups of odd finite index in G are open, and all subgroups of finite index in G are open if G is “non-universal” – that is, unless G involves every finite group as a closed section.

This is of some ‘philosophical’ interest: if all finite-index subgroups of G are open then the topology of G is uniquely determined by the group structure, and all group homomorphisms from G into profinite groups are continuous. However, it seems to me that the real interest of this problem is that it focuses our attention on certain uniformity questions about finite groups with a given number of generators. Lying behind the results stated above are the following (rather deep) theorems, in which g and f denote (effectively known) numerical functions:

(1) In a finite d-generator group every element of the derived group is the product of $g(d)$ commutators.

(2) In a finite d-generator group every product of qth powers is equal to a product of $f(c, d, q)$ qth powers, where c is maximal such that $Alt(c)$ is involved in G.

We believe that $f(c, d, q)$ should be independent of c; if it is, then it would follow that all subgroups of finite index in any finitely generated profinite group are open.

These results join a growing body of finite group theory in which detailed knowledge of the simple groups, coming from the Classification, is applied in a delicate manner to obtain information about composite groups in general.

Profinite groups are the inverse limits of families of finite groups. Natural questions about profinite groups lead to interesting questions about finite groups.

Theorem 3.12 *(Serre’s Remark, 1975) In a finitely generated pro p-group, every subgroup of finite index is open.*

Can the above theorem be extended to all finitely generated profinite groups?

Theorem 3.13 *In a finitely generated pro p-group, the derived group is closed.*

Theorem 3.14 *In a d-generator nilpotent group, every element of the derived group is a product of d-commutators.*

Let us now consider some new theorems (with Nikolw).

Theorem 3.15 *In a finitely generated profinite group, the derived group is closed. This implies that if (i) G is a finitely generated profinite group, (ii) $N \lhd G$ and (iii) G/N is finite and soluble, then N is open.*

Corollary 3.16 *In any finitely generated profinite group, every normal subgroup of finite odd index is open.*

Theorem 3.17 *In a finitely generated non-universal profinite group G, the subgroup $G^q = \langle g^q \,|\, g \in G \rangle$ is open for each $q \in \mathbb{N}$.*

Definition 3.18 G is universal if every finite group is a closed section of G, and non-universal otherwise.

Theorem 3.19 *In a finitely generated non-universal profinite group, every subgroup of finite index is open.*

Let us now consider an aside on words: For which words w is the verbal subgroup $w(G)$ closed whenever G is a finitely generated profinite group? For $w = [x, y]$, G' is the derived group. For $w = g^q$, G^q is the derived group. For $w = [[x, y], [z, t]]$, we don't have a derived group! *Equivalent question:* uniformity of finite groups.

Theorem 3.20 *There is a function $f : \mathbb{N} \to \mathbb{N}$ such that in any d-generator finite group G, every element of G' is the product of $f(d)$ commutators (f is sensible, e.g. $24d^2 + 16d$ if G is soluble).*

Theorem 3.21 *In a d-generator finite group G, every element of G^q is equal to a product of $g(c, d, q)$ q-th powers, where $c = \alpha(G)$, a measure of how complex G is ($\alpha(G) = \max\{n \,|\, \mathrm{Alt}(n)\}$ is a section of G).*

3.9 Jonathan Alperin: The Stable Equivalence Problem

Time: 17:00 - 18:00. *Type:* Plenary Lecture.

Abstract

In algebra there are many concepts which state that two objects or categories are "the same." Isomorphism, Morita equivalence and derived equivalence are well understood examples. However, stable equivalence of module categories is hardly understood at all and many basic questions in representation theory are tied in with this idea. A survey, open questions and examples are discussed.

Let us take a quick look at equivalences.

At the undergraduate level, we encounter isomorphisms, column vectors, matrices and linear transformations. At the graduate level, we may look at equivalence of categories or Morita (module) equivalence. At the advanced graduate level, we may consider G to be acting on the vector space V/k and look at kG-modules. We may also look at Wedderburn theory, characters, degrees, Clifford (a quotient algebra of kG is a matrix algebra over a quotient of kH), etc. A summand of kG is a matrix algebra over kP, where char $k = p$ and P is a Sylow p-subgroup. Next, we go to seminars!

Complexes of R-modules are sequences of the type

$$\ldots \to M_{n+1} \to M_n \to M_{n-1} \to \ldots$$

with $\delta\delta = 0$. This is an algebra of a space. For derived categories $D(R)$, we consider Rickard (derived) equivalence. We have G, char $k = p$ and $k = \bar{k}$. For $p = 2$, $k\Sigma_3 = k[x]/(x) + M_3(k)$ and $kG = B \oplus C$. Broué's Conjecture: B and $kN(P)$ are derived equivalent.

For stable equivalence, we consider a finite dimensional algebra over k with $k = \bar{k}$ and mod $A = f.d.$ modules. Stable category: $\mathrm{Hom}_A(U, V) = \mathrm{Hom}_A(U, V)/\sim$, $U \to A \oplus \ldots \oplus A \to V$, A and B are stably equivalent. *Problem 1:* Find the theory!

Example 3.22 Take $A = kG$, $B = k[N(P)]$, and $P =$ a Sylow p-subgroup. Then $p \cap gPg^{-1} = 1$ if $g \notin N(P)$ — for example, if $G = \mathrm{GL}(2, p^n)$, then

$$P = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \text{ and } N(P) = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

For restriction and induction, we have 'stable equivalence of Morita type' if it arises from an exact functor on module categories. *Problem 2:* Show that almost always a stable equivalence is of Morita type.

Problem 3: If the algebras A and B are stably equivalent (and neither has any matrix summand) then do they have the same number of isomorphism classes of simple modules? Linckelmann: Uniqueness holds (at least for self-injective algebras and stable equivalence of Morita type). Okuyama's trick: Weakly symmetric algebras, arbitrary stable equivalence, 'numerical' Morita equivalence.

Theorem 3.23 *The category of all A-modules filtered by the U_i is equivalent to the category of all finite dimensional modules for another algebra B, itself non necessarily finite dimensional.*

Conjecture 3.24 *(McKay) The number of irreducible complex representations of G of dimension coprime to p equals the number of complex irreducible representations of $N(P)$ of dimension coprime to p.*

4 Wednesday 9th April

4.1 Tom Körner: Besicovitch via Baire

Time: 09:10 - 10:00. *Type:* Morning Lecture.

Abstract

Baire's category theorem is a profound triviality. By applying it to a very natural metric space we obtain the theorem that there exists a closed bounded set of zero area containing unit line segments in every direction.

4.2 Tom Bridgeland: Derived Categories in Algebraic Geometry

Time: 10:10 - 11:00. *Type:* Morning Lecture.

Abstract

Derived categories of sheaves were first introduced into algebraic geometry by Grothendieck and Verdier in the late sixties, but have only recently become fashionable. Their recent popularity is due, at least in part, to the mysterious connections they have with string theory. In this introductory talk, I shall try to explain what derived categories are, what we know about them, and how they can be used to prove new results in algebraic geometry.

The general idea is to study varieties via categories of sheaves of them. If X is a smooth projective variety, then $\mathrm{Coh}(X)$ is an Abelian category of coherent sheaves and $D(X)$ is the derived category of $\mathrm{Coh}(X)$ (it is triangulated). How is the geometry of X reflected in $D(X)$? When do we have $D(X) \cong D(Y)$ (equivalent)?

Consider $\mathcal{A}$, an abelian category, and $C(\mathcal{A})$, the category of complexes:

$$\begin{tikzcd}
\cdots \arrow[r] & M^{i-1} \arrow[r, "d^{i-1}"] \arrow[d, "f^{i-1}"] & M^{i} \arrow[r, "d^{i}"] \arrow[d, "f^{i}"] & M^{i+1} \arrow[r] \arrow[d, "f^{i+1}"] & \cdots \\
\cdots \arrow[r] & N^{i-1} \arrow[r] & N^{i} \arrow[r] & N^{i+1} \arrow[r] & \cdots
\end{tikzcd}$$

A quasi-isomorphism in $C(\mathcal{A})$ is a morphism $f^\bullet : M^\bullet \to N^\bullet$ which gives the following isomorphisms: $H^i(f^\bullet).H^i(M^\bullet) \xrightarrow{n} H^i(N^\bullet)$. The derived category $D(\mathcal{A})$ is obtained by formally inverting quasi-isomorphisms in $C(\mathcal{A})$.

Definition 4.1 $\mathrm{Ext}\,^{i}_{\mathcal{A}}\,(M,N) = \mathrm{Hom}_{D(\mathcal{A})}(M, N[i])$ ($N[i]$ = shift to the left i times).

In derived equivalences, how does one construct the derived equivalence $D(X) \to D(Y)$? To see this, let X and Y be smooth projective n-folds.

Theorem 4.2 *Any equivalence* $\Phi : D(Y) \to D(X)$ *is of the form* $\Phi(-) = R\pi_{X_*}(P \otimes \pi_Y(-))$ *for some* $P \in D(Y \times X)$*. Such a functor is an equivalence iff (a)* $\mathrm{Ext}^i_{D(X)}(\phi\vartheta_{y_1}, \phi\vartheta_{y_2}) = 0$ *if* $y_1 \neq y_2 \in Y$*; (b)* $\mathrm{Hom}_{D(X)}(\phi\vartheta_y, \phi\vartheta_y) = \mathbb{C}$*; and (c)* $\phi\vartheta_y \otimes \omega_X \cong \phi\vartheta_y$*.*

The above theorem implies that Y must be a fine moduli space for the objects $\{\phi\vartheta_y : y \in Y\} \subset D(X)$.

The McKay correspondence was then discussed.

4.3 George Willis: A Canonical Form for Automorphisms of Totally Disconnected Groups

Time: 11:40 - 12:30. *Type:* Morning Lecture.

Abstract

Every locally compact group is the extension of a connected group by a totally disconnected one.

Connected groups may be approximated by Lie groups in a precise sense that constitutes the solution of Hilbert's fifth problem. The theory of Lie groups then makes tools from linear algebra available for the investigation of connected groups and a thorough understanding of these groups has been achieved.

Totally disconnected groups are less well understood. Important classes have been studied, including the profinite groups, the p-adic Lie groups and automorphism groups of locally finite graphs. The tools used are specific to these classes however and there are few general techniques for studying totally disconnected groups.

The talk will describe a canonical form for automorphisms of totally disconnected groups that promises to partly fill the role played in the connected case by Lie theory. Let G be a totally disconnected locally compact group and let α be an automorphism of G. The **scale** of α is the positive integer

$$s(\alpha) = \min\left\{[\alpha(U) : U \cap \alpha(U)] \mid U \text{ is a compact open subgroup of } G\right\}$$

and a compact open subgroup at which the minimum is attained is said to be **tidy** for α.

It will be explained why identifying a subgroup tidy for α is analogous to finding a basis that triangularises a linear transformation and how the scale of α relates to the eigenvalues of the linear transformation under this analogy. The explanation will be illustrated by examples where G is a p-adic vector group or the automorphism group of a tree.

Theorem 4.3 *(Approximation by Lie Groups) Let G be a connected locally compact group. Then each neighbourhood of the identity contains a compact normal subgroup k such that G/k is a Lie Group.*

The automorphisms of totally disconnected locally compact groups have a canonical form that is analogous to the Jordan canonical form of a linear group. *Background:* Totally Disconnected Groups. *Example:* Automorphism Groups of locally finite graphs.

Theorem 4.4 *(van Dantzig) Let G be a totally disconnected locally compact group. Then each neighbourhood of the identity contains a compact open subgroup U.*

Corollary 4.5 *Let G be a compact totally disconnected group. Then each neighbourhood of the identity contains a compact open normal subgroup U.*

Corollary 4.6 *(1) Every compact totally disconnected group is profinite. (2) Every compact totally disconnected group is isomorphic to a closed subgroup of a product of finite groups.*

Automorphisms of Totally Disconnected Groups. If α is an automorphism of a group G and if U is a compact open subgroup of G, then $\alpha(U) \cap U$ is open and $\alpha(U)$ is compact. Hence $[\alpha(U) : \alpha(U) \cap U] < \infty$.

Definition 4.7 Let α be an automorphism of G. The scale of α is the positive integer $S(\alpha) := \min([\alpha(U) : \alpha(U) \cap U] : U < G$ is compact and open$)$. The compact open subgroup U of G is tidy for α if $[\alpha(U) : \alpha(U) \cap U] = S(\alpha)$; that is, if the minimum is attained at U.

Theorem 4.8 *Let $\alpha \in \mathrm{Aut}(G)$ and let $U < G$ be compact and open. Define $U_+ := \cap_{k \geqslant 0} \alpha^k(U)$, $U_- := \cap_{k \geqslant 0} \alpha^{-k}(U)$. Then U is tidy for α iff (T1) $U = U_+ U_-$ and (T2) $U_{++} := \cup_{k \geqslant 0} \alpha^k(U_+)$ is closed (it is a subgroup).*

Since $\alpha(U_+) \geqslant U_+$ and $\alpha(U) \leqslant U_-$, T1 expresses U as the product of a subgroup on which α expands and one on which it contracts. For tidy subgroups, $S(\alpha) = [\alpha(U_+) : U_+]$, and hence the scale of α is the factor by which it expands U_+.

Example 4.9 Let G be the automorphism group of the homogeneous tree T_2, let $\alpha_x : y \mapsto xyx^{-1}$ be an inner automorphism, where x is translation along the path ℓ, and let $U = \mathrm{stab}(U)$, where U is a vertex of ℓ. Then $\alpha_x(U) = \mathrm{stab}(x.u)$ and $[\alpha_x(U) : \alpha_x(U) \cap U] = 3$. We see that $U \neq U_+ U_-$ and so U does not satisfy T1.

It may be shown that every tidy subgroup is the intersection of the stabilisers of a finite string of vertices on ℓ. The tidy steps for α_x are the associated w/ℓ, which yields the canonical form for x. Tidy steps are a canonical form for automorphisms, while the scale is related to eigenvalues.

Theorem 4.10 *(Commuting Automorphisms) Let H be a finitely generated abelian group of automorphisms of the totally disconnected group G. Then there is a compact open subgroup U of G that is tidy for every α in H.*

Theorem 4.11 *Let α and β be automorphisms of G and suppose that there is a compact open subgroup U-tidy for every automorphism in (α, β). Then $\alpha\beta\alpha^{-1}\beta^{-1}(U) = U$.*

4.4 C. Roever: Co-Word Problems in Groups

Time: 13:30 - 13:50. *Type:* Splinter Group: Group Theory.

Abstract

The co-word problem of a finitely generated group G with respect to the finite generating set X is the set of all word over elements of X and their inverses which represent nontrivial elements of G. I shall discuss recent results and open problems about groups with indexed co-word problems. For example, this class of groups contains various Grigorchuk groups and also all Higman-Thompson group.

Let G be a group with finite generating set A. The word problem is stated as follows: $W_A(G) = \{w \in (A^{\pm})^* \mid w =_G \text{Id}\}$. The co-word problem is the complement of the word problem. *Goal:* To find the interaction between the algebra and the complexity. *Fact:* $W_A(G)$ is a regular language.

Class	*Automaton*
Regular	Finite State
Deterministic Context Free	Deterministic Push Down
Context Free	Push Down
Indexed	Nested Stack

- The word problem is deterministic context free.
- What if $W_A(G)$ is indexed?
- Co-CF groups give interesting examples.
- Co-CF groups $\supset$ CF groups.

Theorem 4.12 *The classes of co-CF and co-indexed groups are closed under taking standard repeated wreath products with virtually free top-groups.*

Question: If A wreath B is co-indexed, is B virtually free (work with S. Rees & D. Holt)?

Theorem 4.13 *Polycyclic co-CF groups are virtually abelian (use Paric's classification).*

Problem: What about polycyclic co-indexed groups?

Theorem 4.14 *Every Higman-Thompson group* $G_{n,r}$ *is a co-indexed finitely presented virtually simple group (acting on a boundary of a rooted tree via homeomorphisms).*

Theorem 4.15 *All finitely generated directed automata groups are co-indexed.*

Problem: Is $\langle G_{n,r}, D\rangle$ co-indexed?

4.5 Martyn Quick: Probabilistic Generation of Wreath Products of Non-Abelian Finite Simple Groups

Time: 13:50 - 14:10. *Type:* Splinter Group: Group Theory.

Abstract

Work of Dixon, Kantor–Lubotzky and Liebeck–Shalev shows that the probability of generating a non-abelian finite simple group by two randomly chosen elements converges to 1 as the order of the group grows. Bhattacharjee has proved a similar result for generating an iterated permutational wreath product of alternating groups. I present results which first generalise this to wreath products of arbitrary non-abelian finite simple groups and then to arbitrary actions when constructing the wreath products.

General Problem: Let G be a d-generator finite group. What can one say about the probability that d randomly chosen elements generate G?

Theorem 4.16 *(Martyn Quick, 2001) Let* $X_1, X_2, \ldots$ *be a sequence of non-abelian finite simple groups. Define* $W_1 = X_1$*, and, for* $r \geqslant 2$*, recursively define* $W_r = X_r \operatorname{wr} W_{r-1}$*, the standard wreath product of* X_r *by* W_{r-1}*. Then* $p(W_r) \to 1$ *as* $|X_1| \to \infty$*.*

Theorem 4.17 *(Martyn Quick, 2003) Let* $X_1, X_2, \ldots$ *be a sequence of non-abelian finite simple groups. Let* $W_1 = X$ *act faithfully and transitively on some set* Ω_1*. For* $r \geqslant 2$ *recursively define* $W_r = X_r \operatorname{wr}_{\Omega_{r-1}} W_{r-1}$ *acting faithfully and transitively on some set* Ω_r*. Then* $p(W_r) \to 1$ *as* $|X_1| \to \infty$*.*

4.6 John Bray: Double Coset Enumeration and Symmetric Presentations

Time: 14:10 - 14:30. *Type:* Splinter Group: Group Theory.

Abstract

Symmetric presentations provide an algebraic framework in which double coset enumeration can be implemented in an effective manner. We describe how this has been done (inside MAGMA) and provide some examples of what has been achieved using my program. Among the program's successes are enumerations relating to the well-known Y-diagrams, including $Y_{433} \cong 2 \times 2^{\cdot}B$ over $Y_{333} \cong 2 \times 2^{2 \cdot 2}E_6(2)$ where the index is 27143910000. Some of these examples cannot be done using existing single coset enumeration programs.

- The new idea of pre-progenitors was introduced.
- Only Steve Linton has written a double coset enumerator.
- MAGMA was used to implement the algorithms.
- There are three types of coincidences in double coset enumeration.

4.7 Corinna Wiedorn: A 7-local Identification of the Monster

Time: 14:40 - 15:00. *Type:* Splinter Group: Group Theory.

Abstract

The two maximal 7-local subgroups of the monster containing a given Sylow 7-subgroup are of shape $7_{+}^{1+4}.2^{\cdot}Alt(7) : 6$ and $7^{2+1+2}.GL_2(7)$. I will talk about joint work with C. W. Parker in which we identify the monster from these two subgroups.

4.8 Simon Goodwin: Prehomogeneous Spaces for Parabolic Group Actions in Classical Groups

Time: 15:10 - 15:30. *Type:* Princeton Prize Contender.

Abstract

Reductive group actions are of great importance in pure mathematics. They appear in many areas of mathematics and have therefore been studied extensively. For example characteristic zero prehomogeneous spaces for reductive groups were classified by Sato and Kimura in 1977. (If H is an algebraic group, then a rational H-module V is said to be a prehomogeneous space for H, provided H acts on V with a dense orbit.) This result was extended to positive characteristic by Guralnick, Liebeck, MacPherson and Seitz in 1997.

Also of importance in mathematics are parabolic group actions. The first such actions to consider are those of a parabolic subgroup P on its unipotent radical P_u by conjugation and the adjoint action of P on $p_u = \mathrm{Lie}(P_u)$. One fundamental result is the so called Richardson's Dense

Orbit Theorem from 1973. This states that a parabolic group P acts on it unipotent radical P_u with a dense orbit; likewise for the adjoint action of P on p_u. Also of interest are the induced actions of P on higher terms $P_u^{(r)}$ and $p_u^{(r)}$ of the descending central series of P_u and p_u respectively. Not much is known about these actions.

One question to ask is when P acts on $p_u^{(r)}$ with a finite number of orbits. This question was answered for classical groups by Brüstle, Hille and Röhrle in 2001. For the exceptional groups it was answered for $r = 0$ by Jürgens and Röhrle using a computer program in 2002. For an exceptional group of type G_2 it follows from work of Popov and Röhrle in 1997 that P acts on $p_u^{(r)}$ with a finite number of orbits except when $r = 0$ and P is a Borel subgroup. Röhrle and the author have recently classified the instances when P acts on $p_u^{(r)}$ with finitely many orbits for the exceptional groups of type F_4 and E_6 for all $r \geqslant 1$.

Another question to consider is whether P acts on $p_u^{(r)}$ with a dense orbit. The answer for $r = 0$ is given by Richardson's Dense Orbit Theorem. For $r \geqslant 1$ the question is unsolved.

In this talk we give some results which partially answer this question for the classical groups. These results extend work of Hille and Röhrle. We present a technique which reduces questions about the orthogonal and the symplectic groups to questions about the general linear groups. If G is a classical group we view it as a fixed point subgroup of GL_n under a semisimple automorphism Θ. We show (under mild restrictions) that if a parabolic subgroup P of GL_n acts on a P-submodule n of p_u with a dense orbit, then P^{Θ} acts on n^{θ} with a dense orbit. This technique was used to show that a Borel subgroup B of a classical group acts on $b_u^{(r)}$ with a dense orbit for all $r \geqslant 0$. Further we present some results about other parabolic groups.

4.9 Attila Maróti: Bounding the Number of Conjugacy Classes of a Permutation Group

Time: 15:30 - 15:50. *Type:* Princeton Prize Contender.

Abstract

Let $k(G)$ be the number of conjugacy classes of the finite group G. Kovács and Robinson proved that if G is a subgroup of S_n, then $k(G) \leqslant 5^{n-1}$, and the proof of a proposed improvement of this to $k(G) \leqslant 2^{n-1}$ is reduced to the case where G is almost simple. For solvable permutation groups of degree $n > 2$, they obtained $k(G) \leqslant 3^{(n-1)/2}$. These results are independent of the classification of finite simple groups (CFSG). To do better, one needs to use CFSG. Liebeck and Pyber proved the general $k(G) \leqslant 2^{n-1}$ estimate for arbitrary permutation groups. Later, Riese and Schmid extended the Kovács-Robinson estimate of *solvable* permutation groups to certain p-solvable groups. In general, the following may be shown.

Theorem 1. If G is a subgroup of S_n with $n > 2$, then $k(G) \leqslant 3^{(n-1)/2}$.

In my talk I will describe the main ideas in the proofs of the above results. In particular, I will explain why a good lower bound for the partition function, p(n) was useful in proving Theorem 1.

4.10 George Andrews: Ramanujan's Lost Notebook, Reflections After 27 Years of Study

Time: 16:15 - 17:15. *Type:* Plenary Lecture.

Abstract

Ramanujan's Lost Notebook (rediscovered in 1976) has been a recurring focus of my research for 27 years. In it there are more than 600 formulas stated without proof and each is often unrelated to the one that follows it. In the past, I have spoken about specific collections of formulas that have been quite challenging. In this talk I hope to step back a little from the specifics and discuss the impact of the study of the Lost Notebook within number theory and other research areas. I shall conclude with some insights concerning an entirely bizarre formula in the notebook that frightened me for most of these 27 years.

4.11 Simon Singh: Cracking the Cipher Challenge

Time: 18:45 - 19:45. *Type:* Special Lecture.

Abstract

In "The Code Book", a history of codes and code breaking, the author Simon Singh included ten encrypted messages with a prize of 10,000 pounds for the first person to decipher all of them. Thousands of amateur and professional code breakers took up the Cipher Challenge, but it took over a year before the messages were cracked. Simon Singh will be talking about how he constructed the Cipher Challenge and how the winners eventually cracked it. He will also be using the Cipher Challenge to give an introduction to the history of cryptography, including the Enigma cipher. He will be demonstrating a genuine Enigma cipher machine during the talk. Finally, Simon will explain why encryption is more important today than ever before, and he will discuss what the Cipher Challenge can teach us about Internet security.

5 Thursday 10th April

5.1 Roderick Gow: New Light on William Rowan Hamilton

Time: 09:10 - 10:00. *Type:* Morning Lecture.

Abstract

In two years time, we will celebrate the bicentenary of the birth of William Rowan Hamilton. When he died, Hamilton left an enormous quantity of notebooks and letters detailing the minutiae of his life over 40 years. Two substantial and authoritative biographies have appeared, which used these sources extensively. One by Robert P. Graves, a close friend of Hamilton, was published in three volumes in the 1880's and amounts to over 2000 pages. The other, a one volume work by Thomas Hankins, published in 1980, addresses many aspects of Hamilton's life that Graves had to leave untouched. Despite the wealth of information provided by these two works, new and fascinating facts continue to emerge about Hamilton and his family, and we intend to discuss some of these, as well as giving a brief biographical sketch of Hamilton.

- Born Dublin, 4th August 1805.
- A child prodigy, linguistic ability.
- Brought up and educated by his Uncle James at Trim, Co. Heath.
- Presented his first paper to the Royal Irish Academy on the 23rd of April, 1827, while still an undergraduate.
- Appointed Professor of Astronomy at Trinity College, Dublin on the 10th of June, 1827 before taking his degree.
- Married Helen Bayley (1804-1868) in 1833.
- 3 Children: William, Archibald Henry and Helen.
- Knighted in 1835.
- Discovered Quaternions on the 16th of October, 1843.
- Died in Dublin on the 2nd of September, 1865.
- Four volumes of his work have been published, namely Geometrical Optics in 1931, Dynamics in 1940, Algebra in 1967 and Geometry, Analysis, etc. in 2000.

5.2 Edmund Robertson: Tait, Maxwell and Knot Theory

Time: 10:10 - 11:00. *Type:* Morning Lecture.

Abstract

We briefly look at the schooldays of Tait and Maxwell. We then examine their contributions to topology, particularly knot theory.

Helmholtz wrote a paper on fluid flow in 1858. This was read by Tait who first saw it as a fruitful area for applying Hamilton's quaternions. It later led to the Scottish theoretical physicists developing ideas in knot theory.

Tait discussed knots with Thomson and Maxwell. Thomson had the idea that atoms might be knots in the ether. Maxwell began to develop knot theory and wrote two manuscripts on the topic which were not published until 1995. They show that although the mathematics to deal with such ideas was not available, he still showed a remarkable intuition for the important ideas. Tait then began a major project to classify knots as a contribution to Thomson's theory of vortex atoms.

5.3 Tim Gowers: Interactions Between Harmonic Analysis and Combinatorial Number Theory

Time: 11:30 - 12:30. *Type:* Plenary Lecture.

Abstract

In this talk I shall attempt to show how combinatorics and harmonic analysis benefit from each other. In one direction, I shall describe a few results in combinatorics, mostly with a number-theoretic flavour, that can be solved using harmonic analysis. In the other, I shall point out where our current knowledge of harmonic analysis seems to be inadequate. I hope to show that combinatorics can be of service here: the difficulties are essentially combinatorial, and there seems to be a good chance that they will eventually be overcome.

Problem 1: What is the largest possible size of a subset $A \subset \{1, 2, \ldots, N\}$ that contains no arithmetic progression of length 3? Bounds for this problem have been found.

Problem 2: Let $\mathbb{Z}_N = \mathbb{Z}/n\mathbb{Z}$ and let $\delta > 0$. What is the correct $f(\delta, N)$ such that $A \subset \mathbb{Z}_N$ $(|A| \geqslant \delta N)$ implies that $2A - 2A$ contains an arithmetic progression (in $\mathbb{Z}_N$-sense, N prime) of length $\geqslant f(\delta, N)$? The bounds for this problem are as follows: $N^{c\delta^2} \leqslant f(\delta, N) \leqslant N^{(c \log \frac{1}{\sigma})^{-1}}$. The lower bound has been recently improved by Chang to $N^{c\delta}$.

Problem 3: Let $P_1, P_2, \ldots, P_m \subset \mathbb{Z}$ be arithmetic progressions of length n such that P_α has common difference d. How small can $|\cup_{d=1}^{n} P_d|$ be? In particular, if $m = n^k$, must we have $|\cup_{d=1}^{m} P_d| \geqslant n^{k+1-e}$? Notice that this problem is equivalent to the *Kakeya Problem:* Let $E \subset \mathbb{R}^n$ be a set that contains, for each line, some translate of that line. Must $\dim E = n$?

The following items were then discussed:

- Discrete Fourier Analysis: $\omega = e^{2\pi i/N}$, $f : \mathbb{Z}_N \to \mathbb{C}$. The Fourier transform has several properties.
- A Heuristic Principal: Random distortions don't make much difference.
- Define 'Randomness'.
- The Main Idea: Additive Number Theory Proofs.
- Roth's Twist.
- **Theorem 5.1** *Let* $\delta > 0$*. Then there exists an* N *such that every* $A \subset \{1, \ldots, N\}$ *of size* $\geqslant \delta N$ *contains an arithmetic progression of length 3 (an idea of the proof was given).*
- Bogolyokov's Method.