

Groups and their presentations: Lecture 1

Gilbert Baumslag

© *Draft date September 1, 2008*

My objective here is to take a quick trip through some interesting areas of combinatorial and geometric group theory with an eye on applications to cryptography and internet security. There are no pre-requisites besides an elementary knowledge of group theory. These include the isomorphism theorems, the Sylow theorems and a cursory acquaintance of permutations, direct products, the definition of an abelian group and the fact that finitely generated abelian groups are direct products of cyclic groups, a few of the subgroups that people generally come across in basic group theory such as the center of a group and what it means for elements in a group to be conjugate.

Contents

I hope to cover a good part of the following list of topics.

1. Presentations and various algorithmic results
 - 1.1. Cayley's description of a group
 - 1.2. How a presentation defines a group
 - 1.3. Expacon
 - 1.4. Dehn's algorithmic problems
 - 1.5. Novikov, Adian, Rabin, Neumann, Boone, Baumslag
 - 1.6. Challenge response protocols
2. Free groups and their normal subgroups
 - 2.1. Schreier's subgroup theorem
 - 2.2. Working with presentations: Tietze transformations
 - 2.3. The Reidemeister-Schreier procedure
 - 2.4. The difference between algorithms and procedures
 - 2.5. Magnus
3. Finitely generated groups
 - 3.1. Counting finitely generated groups
 - 3.2. There exist 2-generator groups which are not finitely presented
 - 3.3. The Neumann groups

4. Higman's theorem
 - 3.1. Recursively enumerable sets
 - 3.2. Higman's subgroup theorem
 - 3.3. Finitely presented simple groups
 - 3.4. Boone-Higman theorem
5. Hyperbolic and automatic groups
 - 4.1. The Cayley graph
 - 4.2. Hyperbolic groups
 - 4.3. Automatic groups
6. Residual properties
 - 5.1. Residually finite groups
 - 5.2. Problems and properties
 - 5.3. Examples
7. Abelian and nilpotent groups
 - 6.1. The isomorphism problem
 - 6.2. Basic commutators
 - 6.3. The word problem
 - 6.4. The conjugacy problem
 - 6.5. The isomorphism problem for finitely generated nilpotent groups
8. Metabelian groups
 - 7.1. The Bieri-Strebel invariant
 - 7.2. The Baumslag-Remeslennikov subgroup theorem
9. Applications to cryptography
 - 8.1. RSA
 - 8.2. Challenge response protocols
 - 8.3. Social Security Groups
 - 8.4. Controlling access

The possible applications of finite presentations to cryptography and internet security are in their initial stages and can be thought of as exploratory.

References

- [1] Wilhelm Magnus, Abraham Karrass and Donald Solitar, *Combinatorial group theory*, Dover Publishing Company.
- [2] Roger C. Lyndon and Paul E. Schupp, *Combinatorial group theory*, Springer-Verlag.

- [3] Gilbert Baumslag, *Topics in combinatorial group theory*, Lectures in Mathematics ETH, Springer Verlag, Basel, 1993.
- [4] Derek J. Robinson and J.C. Lennox, *The Theory of Infinite Soluble Groups*, (with J.C. Lennox), Oxford, 2004.
- [5] Joseph J. Rotman, *An introduction to the theory of groups*, Fourth Edition, Springer-Verlag.
- [6] David B A. Epstein, with J.W. Cannon, D.F. Holt, S.V.F. Levy, M.S. Paterson and W.P. Thurston, *Word processing in group theory*, Jones and Bartlett.
- [7] H.S.M. and W.O.J.Moser, *Generators and relations for discrete groups*, Springer.
- [8] H. Davenport, *The higher arithmetic*, Seventh Edition, Cambridge University Press