Some topics in the theory of finite groups

Primož Moravec

University of Ljubljana, Slovenia

Phd Summer School on Discrete Mathematics, Rogla 2014

Some important problems

"All groups are finite"

- Classify all groups of given order up to isomorphism.
- Classify all finite groups up to some common property.
- Describe the structure of given groups.
- Find a way of constructing new finite groups from known ones.
- Count the number of groups of order n.

Abelian groups

How a classification result should really look like

Theorem (Fundamental Theorem of Abelian Groups)

Every finitely generated abelian group is a direct product of cyclic groups

$$C_{m_1} \times C_{m_2} \times \cdots \times C_{m_r} \times C_\infty^k,$$

where $m_i | m_{i+1}$ for all $i = 1, \ldots, r-1$. Two groups of this form are isomorphic if and only if the numbers $m_1, \ldots, m_r$ and k are the same for the two groups.

Alternatively, all finite abelian groups are direct products of cyclic groups of prime power order.

Sylow theorems

Basic structure of finite groups

Theorem (Sylow's theorems)

Let G be a group of order $p^a \cdot m$, where m is not divisible by the prime p. Then the following holds:

1. *G contains at least one subgroup of order p^a. Any two subgroups of this order are conjugate in G. They are called the* **Sylow p-subgroups** *of G.*
2. *For each $n \leq a$, G contains at least one subgroup of order p^n. Every such subgroup is contained in a Sylow p-subgroup.*
3. *Let s_p be the number of Sylow p-subgroups of G. Then $s_p \equiv 1 \mod p$ and s_p divides m.*

Example: groups of order pq, $p > q$

Example

Let P be a Sylow p-subgroup, and Q a Sylow q-subgroup of G. Then Sylow's theorem implies that $s_p = 1$, i.e., P is a normal subgroup of G. Similarly, $s_q \in \{1, p\}$, and $s_p = 1$ if and only if $p \equiv 1 \mod q$. We separate the two cases:

1. $s_q = 1$. One can prove $G \cong C_p \times C_q \cong C_{pq}$.
2. $s_q = p$. Then q divides $p - 1$. We get a group with presentation

$$\langle a, b \mid a^p = b^q = 1, a^b = a^k \rangle$$

for some k satisfying $k^q \equiv 1 \mod p$, $k \not\equiv 1 \mod p$.

GAP

GAP

Just because nobody wants to get her/his hands dirty

`http://www.gap-system.org/`

GAP is a system for computational discrete algebra, with particular emphasis on Computational Group Theory. GAP provides a programming language, a library of thousands of functions implementing algebraic algorithms written in the GAP language as well as large data libraries of algebraic objects.

- Large library of mathematical functions
- Programming language
- Interactive environment
- Extensive documentation and support
- Open source

GAP libraries of groups

- Some basic groups, such as cyclic groups, abelian groups or symmetric groups,
- Classical matrix groups,
- The transitive permutation groups of degree at most 30,
- A library of groups of small order,
- The finite perfect groups of size at most 10^6,
- The primitive permutation groups of degree < 2499,
- The irreducible solvable subgroups of $\mathrm{GL}(n, p)$ for $n > 1$ and $p^n < 256$,
- The irreducible maximal finite integral matrix groups of dimension at most 31,
- The crystallographic groups of dimension at most 4.

Small group library

- Those of order at most 2000 except 1024 (423 164 062 groups);
- Those of cubefree order at most 50 000 (395 703 groups);
- Those of order p^7 for the primes $p = 3, 5, 7, 11$ (907 489 groups);
- Those of order p^n for $n \leq 6$ and all primes p;
- Those of order $q^n \cdot p$ for q^n dividing 2^8, 3^6, 5^5 or 7^4 and all primes p with $p \neq q$;
- Those of squarefree order;
- Those whose order factorises into at most 3 primes.

Example

```
gap> S4 := SymmetricGroup( 4 );
Sym( [ 1 .. 4 ] )
gap> Order( S4 );
24
gap> el := Elements( S4 );
[ (), (3,4), (2,3), (2,3,4), (2,4,3), (2,4), (1,2),
  (1,2)(3,4), (1,2,3), (1,2,3,4), (1,2,4,3), (1,2,4),
  (1,3,2), (1,3,4,2), (1,3), (1,3,4), (1,3)(2,4),
  (1,3,2,4), (1,4,3,2), (1,4,2), (1,4,3), (1,4),
  (1,4,2,3), (1,4)(2,3) ]
gap> a := el[ 4 ];
(2,3,4)
gap> b := el[ 7 ];
(1,2)
gap> a * b;
(1,2,3,4)
```

More examples

```
gap> G := SymmetricGroup( 5 );
Sym( [ 1 .. 5 ] )
gap> H := Subgroup( G, [(1, 2), (1, 3)]);
Group([ (1,2), (1,3) ])
gap> Order( H );
6
gap> (1,2,3,4) in H;
false
gap> N := NormalClosure(G, H);
Group([ (2,3), (1,3,2), (2,4), (3,5) ])
gap> Order( N );
120
gap> StructureDescription( H );
"S3"
gap> StructureDescription( N );
"S5"
```

Normal subgroups

```
gap> G := SymmetricGroup( 4 );
Sym( [ 1 .. 4 ] )
gap> norm := NormalSubgroups( G );
[ Sym( [ 1 .. 4 ] ), Group([ (2,4,3), (1,4)(2,3),
(1,3)(2,4) ]), Group([ (1,4)(2,3), (1,3)(2,4) ]),
Group(()) ]
gap> List( norm, StructureDescription );
[ "S4", "A4", "C2 x C2", "1" ]
gap> Q := G / norm[ 2 ];
Group([ f1 ])
gap> StructureDescription( Q );
"C2"
```

Homomorphisms

```
gap> G := SymmetricGroup( 4 );;
gap> norm:= NormalSubgroups( G );;
gap> N:=norm[ 2 ];
Group([ (2,4,3), (1,4)(2,3), (1,3)(2,4) ])
gap> hom := NaturalHomomorphismByNormalSubgroup( G, N );
[ (1,2,3,4), (1,2) ] -> [ f1, f1 ]
gap> Kernel( hom ) = N;
true
gap> StructureDescription( Image( hom ) );
"C2"
```

Linear groups

```
gap> G := GL( 2, 4);
GL(2,4)
gap> Order( G );
180
gap> el := Elements( G );;
gap> a := el[ 5 ];
[ [ 0*Z(2), Z(2)^0 ], [ Z(2^2), 0*Z(2) ] ]
gap> b := el[ 7 ];
[ [ 0*Z(2), Z(2)^0 ], [ Z(2^2), Z(2^2) ] ]
gap> Determinant( a );
Z(2^2)
gap> a * b^2;
[ [ Z(2^2)^2, Z(2)^0 ], [ Z(2^2)^2, Z(2^2)^2 ] ]
gap> H := SL( 2, 4 );
SL(2,4)
gap> Order( H );
60
```

Small groups and GAP

```
gap> AllSmallGroups( 16 );;
gap> NrSmallGroups( 512 );
10494213
gap> AllSmallGroups(Size, 16, IsAbelian, true);;
gap> List( last, StructureDescription );
[ "C16", "C4 x C4", "C8 x C2", "C4 x C2 x C2",
> "C2 x C2 x C2 x C2" ]
gap> G := DihedralGroup( 64 );
<pc group of size 64 with 6 generators>
gap> IdGroup( G );
[ 64, 52 ]
```

How GAP presents groups?

1. Permutation groups;
2. Matrix groups;
3. Finitely presented (fp) groups;
4. Polycyclic (pc) groups (finite solvable groups.

Warning

A group can be represented in several different ways; GAP does **not** consider them as identical objects.

```
gap> F := FreeGroup("x", "y");;
gap> AssignGeneratorVariables(F);;
#I  Assigned the global variables [ x, y ]
gap> G := F / [x^2, y^3, (x*y)^2];;
gap> StructureDescription(G);
"S3"
gap> G = SymmetricGroup(3);
false
```

How many groups are there?

Hint: Look for big jumps.

```
gap> List([1..64], i -> [i, NrSmallGroups(i)]);
[ [ 1, 1 ], [ 2, 1 ], [ 3, 1 ], [ 4, 2 ], [ 5, 1 ],
[ 6, 2 ], [ 7, 1 ], [ 8, 5 ], [ 9, 2 ], [ 10, 2 ],
[ 11, 1 ], [ 12, 5 ], [ 13, 1 ], [ 14, 2 ], [ 15, 1 ],
[ 16, 14 ], [ 17, 1 ], [ 18, 5 ], [ 19, 1 ], [ 20, 5 ],
[ 21, 2 ], [ 22, 2 ], [ 23, 1 ], [ 24, 15 ], [ 25, 2 ],
[ 26, 2 ], [ 27, 5 ], [ 28, 4 ], [ 29, 1 ], [ 30, 4 ],
[ 31, 1 ], [ 32, 51 ], [ 33, 1 ], [ 34, 2 ], [ 35, 1 ],
[ 36, 14 ], [ 37, 1 ], [ 38, 2 ], [ 39, 2 ], [ 40, 14 ],
[ 41, 1 ], [ 42, 6 ], [ 43, 1 ], [ 44, 4 ], [ 45, 2 ],
[ 46, 2 ], [ 47, 1 ], [ 48, 52 ], [ 49, 2 ], [ 50, 5 ],
[ 51, 1 ], [ 52, 5 ], [ 53, 1 ], [ 54, 15 ], [ 55, 2 ],
[ 56, 13 ], [ 57, 2 ], [ 58, 2 ], [ 59, 1 ], [ 60, 13 ],
[ 61, 1 ], [ 62, 2 ], [ 63, 4 ], [ 64, 267 ] ]
```

Decomposing groups

Composition series

Prime decomposition of groups

Definition

A group G is **simple** if $\{1\}$ and G are the only normal subgroups of G.

The abelian simple groups are precisely C_p where p is a prime.

Definition

A **composition series** of a group G is a sequence of subgroups

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_r = G$$

such that all the factors G_{i+1}/G_i are simple groups.

Jordan-Hölder theorem

Every finite group has a composition series.

Theorem (Jordan-Hölder Theorem)

Any two composition series of a finite group G give rise, up to the order and isomorphism type, to the same list of composition factors.

Example: C_{12}

Possible composition series of C_{12}:

$$1 \lhd C_2 \lhd C_6 \lhd C_{12}$$

$$1 \lhd C_2 \lhd C_4 \lhd C_{12}$$

$$1 \lhd C_3 \lhd C_6 \lhd C_{12}$$

List of composition factors: C_2, C_2, C_3.

How to construct all finite groups?

Grand plan

If N is a normal subgroup of G, we say that G is an **extension** of N by G/N.

Algorithm

1. Given groups N and Q, find a way of construction all groups G with $N \triangleleft G$ and $G/N \cong Q$ (**Extension Problem**).
2. Classify all finite simple groups.
3. Use these repeatedly to construct all groups with prescribed composition series.

Finite simple groups

Simple groups

Building blocks

Definition

A group G is **simple** if $\{1\}$ and G are the only normal subgroups of G.

Examples of finite simple groups:

- C_p where p is a prime;
- Alternating groups A_n, where $n \geq 5$;
- $\mathrm{PSL}(n, p)$, except in the two cases, $n = 2$, $p = 2$ or $n = 2$, $p = 3$.

In the notes we prove that $\mathrm{PSL}(2, 2) \cong S_3$ and $\mathrm{PSL}(2, 3) \cong A_4$.

```
gap> StructureDescription(PSL(2, 2));
"S3"
gap> StructureDescription(PSL(2, 3));
"A4"
```

Classification (CFSG)

1. **Cyclic groups of prime order**;
2. **Alternating groups** A_n for $n \geq 5$;
3. **Groups of Lie type**; these groups arise as automorphism groups of simple Lie algebras. An example is $\mathrm{PSL}(n, F)$.
4. **26 sporadic groups**; these do not fall into any infinite family of simple groups described above. They are usually defined as symmetry groups of various algebraic or combinatorial configurations. The largest of them has order

   $$808017424794512875886459904961710757005754368000000000$$

   and is called the **Monster Group**.

A common way of proving theorems about finite groups:

- Reduction to finite simple groups;
- List checking.

ATLAS of finite groups

`http://brauer.maths.qmul.ac.uk/Atlas/`

It lists basic information about 93 finite simple groups, the information being generally:

- order,
- Schur multiplier,
- outer automorphism group,
- various constructions (such as presentations),
- conjugacy classes of maximal subgroups (with characters group action they define),
- character tables.

Finite simple groups and GAP

Simple groups up to order 10^6 are available in GAP. The notations GAP uses are consistent with that of ATLAS.

```
gap> AllSmallNonabelianSimpleGroups( [1..1000000] );
[ A5, PSL(2,7), A6, PSL(2,8), PSL(2,11), PSL(2,13),
  PSL(2,17), A7, PSL(2,19), PSL(2,16), PSL(3,3), PSU(3,3),
  PSL(2,23), PSL(2,25), M11, PSL(2,27), PSL(2,29),
  PSL(2,31), A8, PSL(3,4), PSL(2,37), PSp(4,3), Sz(8),
  PSL(2,32), PSL(2,41), PSL(2,43), PSL(2,47), PSL(2,49),
  PSU(3,4), PSL(2,53), M12, PSL(2,59), PSL(2,61), PSU(3,5),
  PSL(2,67), J_1, PSL(2,71), A9, PSL(2,73), PSL(2,79),
  PSL(2,64), PSL(2,81), PSL(2,83), PSL(2,89), PSL(3,5),
  M22, PSL(2,97), PSL(2,101), PSL(2,103), J_2, PSL(2,107),
  PSL(2,109), PSL(2,113), PSL(2,121), PSL(2,125), PSp(4,4)]
```

Extension theory – building new groups from old

Formal definition

A **group extension** of a group N by a group G is a short exact sequence

$$1 \longrightarrow N \xrightarrow{\mu} E \xrightarrow{\epsilon} G \longrightarrow 1.$$

A **morphism** between extensions $N \rightarrowtail E \twoheadrightarrow G$ and $\bar{N} \rightarrowtail \bar{E} \twoheadrightarrow \bar{G}$ is a triple of group homomorphisms (α, β, γ) such that the following diagram commutes:

$$\begin{array}{ccccc} N & \xrightarrow{\mu} & E & \xrightarrow{\epsilon} & G \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\ \bar{N} & \xrightarrow{\bar{\mu}} & \bar{E} & \xrightarrow{\bar{\epsilon}} & \bar{G} \end{array} .$$

The collection of all group extensions and morphisms between them is a category.

Semidirect products – external version

Suppose that H and N are groups and that we have a homomorphism

$$\alpha : H \to \mathrm{Aut}(N).$$

The **(external) semidirect product** $H \ltimes_\alpha N$ of N and H is the set of all pairs (h, n), where $h \in H$, $n \in N$, with the operation

$$(h_1, n_1)(h_2, n_2) = (h_1 h_2, n_1^{h_2^\alpha} n_2).$$

This is a group with the identity element $(1_H, 1_N)$, and the inverse of (h, n) is $(h^{-1}, n^{-(h^\alpha)^{-1}})$.

Semidirect products – internal version

We have embeddings $H \to H \ltimes_\alpha N$ and $N \to H \ltimes_\alpha N$ given by $h \mapsto (h, 1_N)$ and $n \mapsto (1_H, n)$, respectively. If H^* and N^* are images of these maps, then $N^* \lhd H \ltimes_\alpha N$, $H^* \cap N^* = 1$ and $H^*N^* = H \ltimes_\alpha N$. We say that

$$H \ltimes_\alpha N$$

is the **internal semidirect product** of N^* and H^*. The group H^* is said to be a **complement** of N^* in G. The group G is an extension of N^* by H^*; we say that this extension is a **split extension**.

Examples of semidirect products

- The direct product $H \times N$ is a special case of semidirect product; H acts trivially on N.
- Groups of order pq, where $p > q$; we have either $C_p \times C_q$ or

$$\langle a, b \mid a^p = b^q = 1, a^b = a^k \rangle = \langle b \rangle \ltimes \langle a \rangle,$$

where the action is given by $a^b = a^k$.

Example: $C_4 \ltimes (C_2 \times C_2)$

Let us build all possible semidirect products of $C_2 \times C_2$ by C_4:

```
gap> H := CyclicGroup(4);;
gap> N := AbelianGroup([2,2]);;
<pc group of size 4 with 2 generators>
gap> hom := AllHomomorphisms(H, AutomorphismGroup(N));;
gap> for map in hom do
> Print(IdGroup(SemidirectProduct(H, map, N)),"\n");
> od;
[ 16, 10 ]
[ 16, 3 ]
[ 16, 3 ]
[ 16, 3 ]
gap> StructureDescription(SmallGroup(16,10));
"C4 x C2 x C2"
gap> StructureDescription(SmallGroup(16,3));
"(C4 x C2) : C2"
```

The Schur-Zassenhaus theorem

Theorem

Suppose that A and G are finite groups satisfying $\gcd(|A|, |G|) = 1$. *Then every extension of A by G splits.*

Wreath product

Let G and H be groups and let H act on the set $X = \{x_1, x_2, \ldots, x_n\}$. We take

$$G^X = \prod_{i=1}^{n} G_{x_i}$$

to be the direct product of n copies of G indexed by the set X. Then H also acts on G^X by the rule

$$(g_{x_1}, g_{x_2}, \ldots, g_{x_n})h = (g_{x_1 h}, g_{x_2 h}, \ldots, g_{x_n h}).$$

Therefore we have a homomorphism $\alpha : H \to \mathrm{Aut}(G^X)$ and we can form the semidirect product $H \ltimes_\alpha G^X$ which is denoted by $G \wr_X H$ and called the **wreath product** of G by H.

Standard wreath product

A special case is when $X = H$, and H acts on X by right multiplication. Then the corresponding wreath product is denoted by $G \wr H$ and called the **regular (standard) wreath product**.

```
gap> G := StandardWreathProduct(CyclicGroup(2), CyclicGroup(4));
<group of size 64 with 3 generators>
gap> IdGroup(G);
[ 64, 32 ]
```

Alternatively, we can think of C_4 as the group $\langle (1\,2\,3\,4) \rangle$ acting on C_2^4 by permuting the indices:

```
gap> G := SemidirectProduct(Group((1,2,3,4)), GF(2)^4);
<matrix group of size 64 with 2 generators>
gap> IdGroup(G);
[ 64, 32 ]
```

Importance of wreath products

Wreath products are important in the theory of extensions because of the following:

Theorem

Every extension of G by H is isomorphic to a subgroup of $G \wr H$.

Also:

Theorem

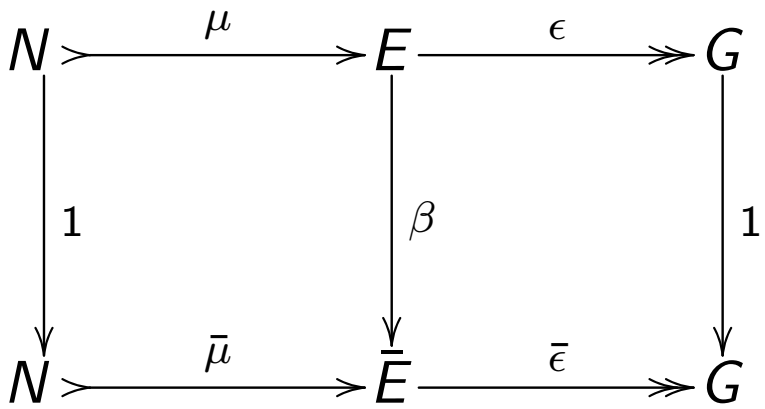
a Sylow p-subgroup of S_{p^n} is isomorphic to

$$(\cdots(C_p \wr Cp) \wr \cdots) \wr C_p,$$

the number of factors being n.

Equivalence of extensions

A morphism of the type



is said to be an **equivalence** of extensions.

Main problem

Classify all extensions of N by G up to equivalence.

Extensions with abelian kernel – transversals

Consider

$$A \overset{\mu}{\rightarrowtail} E \overset{\epsilon}{\twoheadrightarrow} G \ ,$$

where A is an abelian group (written additively).

When choosing a transversal $\mathcal{T}$ to $M = \operatorname{im}\mu = \ker\epsilon$ in E, we get a function $\tau : G \to E$ defined by $g^\tau = x$, where $x \in \mathcal{T}$ is such that $g = x^\epsilon$. The function τ is called a **transversal function**.

Note that τ is not necessarily a homomorphism. We also see that $\tau\epsilon = 1_G$, and that any function $\tau : G \to E$ with the property $\tau\epsilon = 1_G$ determines a transversal to M in E, namely $\{g^\tau \mid g \in G\}$.

Extensions with abelian kernel – action

$$A \rightarrowtail^{\mu} E \twoheadrightarrow^{\epsilon} G\ .$$

Suppose that we have fixed τ. Then the elements $\{g^\tau : g \in G\}$ act on M by conjugation. Since $\mu : A \to M$ is an isomorphism, we can define $g^\chi \in \mathrm{Aut}(A)$ by the rule

$$(a^{g^\chi})^\mu = (g^\tau)^{-1} a^\mu (g^\tau)$$

for $a \in A$ and $g \in G$. We obtain a function $\chi : G \to \mathrm{Aut}(A)$.

The map $\chi : G \to \mathrm{Aut}(A)$ is a homomorphism which arises by conjugation in $\mathrm{im}\,\mu$ by elements of E.

Why is equivalence so good?

$$A \overset{\mu}{\rightarrowtail} E \overset{\epsilon}{\twoheadrightarrow} G$$

Let $\chi : G \to \mathrm{Aut}(A)$ be a homomorphism. Then χ induces a G-action A given by $a \cdot g = a^{g\chi}$. We say that A is a G-**module**.

Theorem

Equivalent extensions of A by G, where A is abelian, induce the same G-module structure on A.

Factor sets a.k.a. cocycles

Choose a transversal function $\tau : G \to E$, Let $x, y \in G$. As $x^\tau y^\tau$ and $(xy)^\tau$ belong to the same coset of $\ker \epsilon = \operatorname{im} \mu$ in E, we may write

$$x^\tau y^\tau = (xy)^\tau ((x,y)\phi)^\mu$$

for some $(x,y)\phi \in A$. Thus we get a function $\phi : G \times G \to A$ defined by

$$((x,y)\phi)^\mu = (xy)^{-\tau} x^\tau y^\tau .$$

From the associative law $x^\tau (y^\tau z^\tau) = (x^\tau y^\tau) z^\tau$ we get that ϕ satisfies the identity

$$(x, yz)\phi + (y,z)\phi = (xy, z)\phi + (x,y)\phi \cdot z.$$

A function $\phi : G \times G \to A$ satisfiying this functional equation is called a **factor set** (or a **2-cocycle**).

The group of cocycles

The set $Z^2(G, A)$ of all 2-cocycles in G with coefficients in the G-module A has the structure of an abelian group with the operation

$$(x, y)(\phi_1 + \phi_2) = (x, y)\phi_1 + (x, y)\phi_2.$$

Example

In the situation above, what happens if $(x, y)\phi = 0$ for all $x, y \in G$? In this case, the transversal map $\tau : G \to E$ is a homomorphism. It is easy to see that the image of τ is then a complement of $\operatorname{im} \mu \cong A$ in E, therefore $E \cong G \ltimes_\chi A$.

How does the choice of τ affect ϕ?

Let τ' be another transversal function for given extension. Then we get another factor set ϕ', i.e., $x^{\tau'}y^{\tau'} = (xy)^{\tau'}((x,y)\phi')^{\mu}$.
As x^{τ} and $x^{\tau'}$ belong to the same coset of $\ker\epsilon = \operatorname{im}\mu$, we can write $x^{\tau'} = x^{\tau}((x)\psi)^{\mu}$ for some $(x)\psi \in A$.

$$(x,y)\phi = (x,y)\phi' + (xy)\psi - (x)\psi \cdot y - (y)\psi.$$

Define $\psi^* : G \times G \to A$ by

$$(x,y)\psi^* = (y)\psi - (xy)\psi + (x)\psi \cdot y,$$

so that $\phi' = \phi + \psi^*$. It follows that $\psi^* \in Z^2(G,A)$. The 2-cocycle ψ^* is called a **2-coboundary**. 2-coboundaries form a subgroup $B^2(G,A)$ of $Z^2(G,A)$. We have proved:

Proposition

The extension $A \overset{\mu}{\rightarrowtail} E \overset{\epsilon}{\twoheadrightarrow} G$ *, where* A *is abelian, determines a unique element* $\phi + B^2(G,A)$ *of the group* $Z^2(G,A)/B^2(G,A)$.

Does every factor set induce an extension?

Let A be a G-module and $\phi : G \times G \to A$ a factor set. Let $E(\phi)$ be (as a set) $G \times A$, with the operation

$$(x, a)(y, b) = (xy, ay + b + (x, y)\phi).$$

$E(\phi)$ becomes a group. Define $\mu : A \to E(\phi)$ by the rule

$$a^\mu = (1, a - (1, 1)\phi),$$

and $\epsilon : E(\phi) \to G$ by the rule

$$(x, a)^\epsilon = x.$$

Then we have

$$A \rightarrowtail^{\mu} E(\phi) \xrightarrow{\epsilon} \twoheadrightarrow G\ .$$

Classification of extensions with abelian kernel

Proposition

Let A be a G-module and $\phi : G \times G \to A$ a factor set. Then the extension

$$A \rightarrowtail^{\mu} E(\phi) \twoheadrightarrow^{\epsilon} G$$

induces the given G-module structure. There exists a transversal $\tau : G \to E(\phi)$ such that ϕ is the factor set for this extension with respect to τ.

Theorem

Let G be a group and A a G-module. Then there is a bijection between the set of equivalence classes of of extensions of A by G inducing the given module structure and the group $Z^2(G, A)/B^2(G, A)$. The split extension corresponds to $B^2(G, A)$.

Extensions and GAP

GAP can compute extensions of elementary abelian p-groups by solvable groups, which have to be presented as pc groups.

One has to define an elementary abelian group A together with an action of G on A as a MeatAxe module for G over a finite field.

In this case, $Z^2(G, A)$, $\mathrm{B}^2(G, A)$ and $H^2(G, A)$ are elementary abelian p-groups and can be considered as vector spaces over $\mathrm{GF}(p)$.

All extensions of $A = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ by $G = D_8$ (trivial action)

```
gap> G := DihedralGroup(8);;
gap> mats := List( Pcgs( G ), x -> IdentityMat( 2, GF(2) ) );;
gap> A := GModuleByMats( mats, GF(2) );;
gap> co := TwoCocycles( G, A );;
gap> Extension( G, A, co[2] );;
gap> StructureDescription(last);
"C2 x (C4 : C4)"
gap> SplitExtension( G, A );;
gap> StructureDescription(last);
"C2 x C2 x D8"
gap> ext := Extensions( G, A );;
gap> Length(ext);
64
gap> DuplicateFreeList(List(ext, IdGroup));
[ [ 32, 46 ], [ 32, 40 ], [ 32, 22 ], [ 32, 39 ],
  [ 32, 9 ], [ 32, 23 ], [ 32, 13 ], [ 32, 41 ],
  [ 32, 10 ], [ 32, 2 ], [ 32, 14 ] ]
```

Second cohomology $H^2(D_8, \mathbb{Z}_2 \oplus \mathbb{Z}_2)$

```
gap> z2 := AdditiveGroupByGenerators(co);;
gap> Length(Elements(z2));
256
gap> h2 := TwoCohomology(G, A);;
h2.cohom;
<linear mapping by matrix, <vector space of dimension
8 over GF(2)> -> ( GF(2)^6 )>
gap> dimensionZ2 := Dimension(Source(h2.cohom));
8
gap> dimensionB2 := Dimension(Kernel(h2.cohom));
2
gap> dimensionH2 := Dimension(Image(h2.cohom));
6
```

The last line tells us that $H^2(G, A) \cong C_2^6$.

Nilpotent groups

Nilpotent groups

We call

$$1 = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

a **normal series** of G if each of its members is a normal subgroup of G.

Definition

A group G is **nilpotent** if it has a **central series**, i.e. a normal series

$$1 = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

in which each factor G_{i+1}/G_i is contained in the center of G/G_i.

The length of the shortest central series of G is called the **nilpotency class** of G.

Basic properties

- All nilpotent groups are solvable.
- Nilpotent groups of class no more than 1 are abelian.
- The smallest solvable non-nilpotent group is S_3.

Proposition

Subgroups, homomorphic images and finite direct products of nilpotent groups are nilpotent.

Nilpotency is not closed under extensions, since S_3 is an extension of C_3 by C_2.

Examples

```
gap> l := AllSmallGroups(Size, 54, IsNilpotent, true);
[ <pc group of size 54 with 4 generators>,
  <pc group of size 54 with 4 generators>,
  <pc group of size 54 with 4 generators>,
  <pc group of size 54 with 4 generators>,
  <pc group of size 54 with 4 generators> ]
gap> NilpotencyClassOfGroup(l[3]);
2
gap> ForAll(AllSmallGroups(54), IsNilpotent);
false
gap> G:= First(AllSmallGroups(54), x->not IsNilpotent(x));;
gap> StructureDescription(G);
"D54"
gap> List(l, StructureDescription);
[ "C54", "C18 x C3", "C2 x ((C3 x C3) : C3)", "C2 x (C9 : C3)",
  "C6 x C3 x C3" ]
```

Very important examples

Theorem

All finite p-groups are nilpotent.

Proof.

First prove that $Z(G)$ is nontrivial. Now use induction on the order of G to show that $G/Z(G)$ is nilpotent. From here it easily follows that G is nilpotent as well. □

Unitriangular groups

Let S be the ring of all $n \times n$ matrices over a commutative ring with identity R. Further, let N be the subring of all strictly upper triangular matrices. It is not hard to see

$$U = 1 + N$$

is a group with respect to ring multiplication.

Let U_i consist of all upper unitriangular matrices whose first $i - 1$ super diagonals are zero. It is easy to prove that this is a central series of U, and that U is nilpotent of class exactly $n - 1$.

In the case that $R = \mathrm{GF}(p)$ we find U to be a finite p-group of order $p^{n(n-1)/2}$.

Characterizations of finite nilpotent groups

Theorem

The following conditions are equivalent for a finite group G:

1. *G is nilpotent;*
2. *every subgroup of G is subnormal;*
3. *Every proper subgroup H of G is properly contained in its normalizer;*
4. *Every maximal subgroup of G is normal;*
5. *G is the direct product of its Sylow subgroups.*

Commutators

A **simple commutator of length** n of elements $x_1, \ldots, x_n \in G$ is defined inductively by $[x_1] = x_1$ and

$$\begin{aligned}[x_1, x_2, \ldots, x_n] &= [[x_1, \ldots, x_{n-1}], x_n] \\ &= [x_1, \ldots, x_{n-1}]^{-1} \cdot [x_1, \ldots, x_{n-1}]^{x_n}.\end{aligned}$$

Lemma

Let x, y, z be elements of a group. Then

1. $[x, y] = [y, x]^{-1}$;
2. $[xy, z] = [x, z]^y [y, z]$ *and* $[x, yz] = [x, z][x, y]^z$;
3. $[x, y^{-1}] = ([x, y]^{y^{-1}})^{-1}$ *and* $[x^{-1}, y] = ([x, y]^{x^{-1}})^{-1}$;
4. *(the Hall-Witt identity)* $[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1$.

Proof by computer

```
gap> F := FreeGroup( "x", "y", "z" );;
gap> AssignGeneratorVariables( F );;
gap> Comm( x * y, z ) = Comm( x, z )^y * Comm( y, z );
true
```

Lower central series

There are two canonical central series of a given group.

Definition

Define $\gamma_1(G) = G$ and inductively

$$\gamma_{n+1}(G) = [\gamma_n G, G].$$

The result is the **lower central series**

$$G = \gamma_1 G \geqslant \gamma_2 G \geqslant \cdots$$

of fully invariant (and therefore normal) subgroups of G.

Upper central series

Definition

Define $Z_0(G) = 1$ and inductively

$$Z_{n+1}(G)/Z_n(G) = Z(G/Z_n(G)).$$

We obtain the **upper central series**

$$1 = Z_0(G) \leqslant Z_1(G) \leqslant Z_2(G) \leqslant \cdots$$

of characteristic (and therefore normal) subgroups of G.

Nilpotency

Proposition

If $1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_n = G$ *is a central series of a nilpotent group* G*, then*

1. $\gamma_i(G) \leqslant G_{n-i+1}$ *so that* $\gamma_{n+1}G = 1$*;*
2. $G_i \leqslant Z_i(G)$*so that* $Z_n(G) = G$*;*
3. *the nilpotency class of* G *equals the length of the upper central series which also equals the length of the lower central series.*

Example

```
gap> G := SmallGroup(128, 50);;
gap> NilpotencyClassOfGroup(G);
4
gap> LowerCentralSeriesOfGroup(G);
[ <pc group of size 128 with 7 generators>,
  Group([ f3, f5, f7 ]), Group([ f5, f7 ]),
  Group([ f7 ]), Group([ <identity> of ... ]) ]
gap> UpperCentralSeriesOfGroup(G);
[ Group([ f6, f7, f5, f3, f4, f1, f2 ]),
  Group([ f6, f7, f5, f3, f4 ]),
  Group([ f6, f7, f5 ]),
  Group([ f6, f7 ]), Group([  ]) ]
```

The Fitting subgroup

Theorem (Fitting)

Let M and N be normal nilpotent subgroups of a group G. If c and d are nilpotency classes of M and N, then $L = MN$ is nilpotent of class $\leq c + d$.

Definition

The subgroup $\mathrm{Fit}(G)$ generated by all the normal nilpotent subgroups of a group G is called the **Fitting subgroup** of G.

If the group G is finite, then $\mathrm{Fit}(G)$ is nilpotent. In these cases, $\mathrm{Fit}(G)$ is the unique largest normal nilpotent subgroup of G.

Theorem

Let G be a finite group. For a prime p let $O_p(G)$ be the largest normal p-subgroup of G. Then $\mathrm{Fit}(G)$ is equal to the direct product of all $O_p(G)$, where p divides $|G|$.

The Frattini subgroup

Definition

The **Frattini subgroup** $\mathrm{Frat}(G)$ of G is the intersection of all maximal subgroups of G. Clearly $\mathrm{Frat}(G)$ is a characteristic subgroup of G.

We say that $g \in G$ is a **nongenerator** of G if $G = \langle g, X \rangle$ implies $G = \langle X \rangle$ for every $X \subseteq G$.

Theorem

$\mathrm{Frat}(G)$ *equals the set of nongenerators of* G.

Proof

Proof.

Let $g \in \mathrm{Frat}(G)$, $G = \langle g, X \rangle$, but $G \neq \langle X \rangle$. There exists $M \leq G$ which is maximal subject to $\langle X \rangle \leq M$ and $g \notin M$. M is a maximal subgroup of G, hence $g \in M$, a contradiction.

Let g be a nongenerator and $g \notin \mathrm{Frat}(G)$. Thus $g \notin M$ for some maximal subgroup M. It follows $\langle g, M \rangle = G$, hence $G = M$, a contradiction. □

Theorem of Gaschütz

Theorem (Gaschütz)

Let G be a group.

(a) *If $\mathrm{Frat}(G) \leq H \leq G$, where H is finite and $H/\mathrm{Frat}(G)$ is nilpotent, then H is nilpotent.*

(b) *If G is finite, $\mathrm{Frat}(G)$ is nilpotent.*

(c) *Define $\mathrm{FFrat}(G)$ by*

$$\mathrm{FFrat}(G)/\mathrm{Frat}(G) = \mathrm{Fit}(G/\mathrm{Frat}(G)).$$

If G is finite, then $\mathrm{FFrat}(G) = \mathrm{Fit}(G)$.

(d) *If G is finite, $\mathrm{FFrat}(G)/\mathrm{Frat}(G)$ is the product of all the abelian minimal normal subgroups of $G/\mathrm{Frat}(G)$.*

Another characterization of finite nilpotent groups

Proposition

Let G be a finite group. Then G is nilpotent if and only if $G' \leq \mathrm{Frat}(G)$.

Proof.

If G is nilpotent and M a maximal subgroup of G, then $G' \leq M$. Conversely, if $G' \leq \mathrm{Frat}(G)$ then every maximal subgroup of G is normal. □

Finite p-groups

Burnside basis theorem

Theorem (The Burnside Basis Theorem)

Let G be a finite p-group. Then $\mathrm{Frat}(G) = \gamma_2(G)G^p$. *Also if* $|G : \mathrm{Frat}(G)| = p^r$, *then every set of generators of G has a subset of r elements which also generates G.*

Extraspecial p-groups

Definition

A finite p-group is said to be **extraspecial** if

$$G' = Z(G) \cong C_p.$$

Proposition

Let G be a nonabelian group of order p^3. If p is odd, then G is isomorphic with

$$\langle x, y \mid x^p = y^p = 1, [x, y]^x = [x, y]^y = [x, y] \rangle$$

or

$$\langle x, y \mid x^{p^2} = 1 = y^p, x^y = x^{1+p} \rangle.$$

These groups have exponent p and p^2 respectively. If $p = 2$, then G is isomorphic with D_8 or quaternion group Q_8. In particular, all non-abelian groups of order p^3 are extraspecial.

Characterization of extraspecial p-groups

Definition

A group G is said to be the **central product** of its normal subgroups $G_1, \ldots, G_n$ if $G = G_1 \cdots G_n$, $[G_i, G_j] = 1$ for $i \neq j$, and $G_i \cap \prod_{j \neq i} G_j = Z(G)$.

Theorem

An extraspecial p-group is a central product of n nonabelian subgroups of order p^3, and has order p^{2n+1}. Conversely, a finite central product of nonabelian groups of order p^3 is an extraspecial p-group.

Classification of p-groups of given order

1. C_p are the only groups of order p;
2. All groups of order p^2 are abelian, hence $C_p \times C_p$ or C_{p^2};
3. Groups of order p^3 are classified above;
4. Groups of order p^4 are also known; 15 isomorphism types;
5. Groups of order p^5 or p^6: James (1988);
6. Groups of order p^7: O'Brien, Vaughan-Lee (2005).

Coclass

Proposition

Let G be a group of order p^n, $n > 1$, and let c be its nilpotency class. Then $c < n$.

Definition

Under the above notations, the number

$$n - c$$

is called the **coclass** of G.

Finite p-groups of coclass 1 are also known as p-**groups of maximal class**.

Coclass graph $\mathcal{G}(p, r)$

- The vertices of $\mathcal{G}(p, r)$ correspond to the isomorphism types of p-groups of coclass r.
- Two vertices G and H are joined by a directed edge from G to H if and only if $G \cong H/\gamma_{\mathrm{cl}(H)}(H)$.

Coclass trees

Definition

If a group is an inverse limit of p-groups of coclass r, then it said to be a **pro-p group** of coclass r.

Every infinite pro-p group S of coclass r determines a **maximal coclass tree** $\mathcal{T}(S)$ in $\mathcal{G}(p, r)$, namely, the subtree of $\mathcal{G}(p, r)$ consisting of all descendants of $S/\gamma_i(S)$, where i is minimal such that $S/\gamma_i(S)$ has coclass r and $S/\gamma_i(S)$ is not a quotient of another infinite pro-p group R of coclass r not isomorphic to S.

Coclass conjectures; now theorems

E Given p and r, there are only finitely many isomorphism types of infinite solvable pro-p groups of coclass r.

D Given p and r, there are only finitely many isomorphism types of infinite pro-p groups of coclass r.

C Pro-p groups of finite coclass are solvable.

B For some function g, every finite p-group of coclass r has derived length bounded by $g(p, r)$.

A For some function f, every finite p-group of coclass r has a normal subgroup N of class 2 (1 if $p = 2$) whose index is bounded by $f(p, r)$.

Consequence for the coclass graph

The coclass theorems imply that $\mathcal{G}(p, r)$ consists of finitely many maximal coclass trees and finitely many groups lying outside these trees.

Shaved trees and periodicity theorem

Let S be an infinite pro-p group of coclass r.

The subtree $\mathcal{T}(S,k)$ of $\mathcal{T}(S)$ containing all groups of distance at most k from the main line is called a **shaved tree**. We denote its branches by $\mathcal{B}_j(S,k)$.

Theorem P (du Sautoy, 2001)

Let S be an infinite pro-p group of coclass r. Then there exist integers $d = d(\mathcal{T}(S,k))$ and $f = f(\mathcal{T}(S,k))$ such that $\mathcal{B}_j(S,k)$ and $B_{j+d}(S,k)$ are isomorphic as rooted trees for all $j \geq f$.

p-groups of maximal class

Proposition

Let G be a group of order p^n, wher $n \geq 3$, and of maximal class. Then

1. *G^{ab} is an elementary abelian p-group of order p^2 and $|\gamma_i(G) : \gamma_{i+1}(G)| = p$ for $2 \leq i \leq n-1$. The group G can be generated by two elements.*
2. *For every $i \geq 2$ we have that $\gamma_i(G)$ is the only normal subgroup of G of index p^i.*
3. *$Z_i(G) = \gamma_{n-i}(G)$ for all $i = 0, \ldots, n-1$.*

Examples of p-groups of maximal class

- Groups of order p^2;
- Nonabelian groups of order p^3;
- $C_p \wr C_p$;
- Generalized quaternion groups
  $Q_{2^n} = \langle x, y \mid y^{2^{n-1}} = 1, x^2 = y^{2^{n-2}}, y^x = y^{-1} \rangle$;
- Dihedral groups D_{2^n};
- Semidihedral groups
  $SD_{2^n} = \langle x, y \mid y^{2^{n-1}} = 1, x^2 = 1, y^x = y^{2^{n-2}-1} \rangle$, $n > 3$.

2-groups of maximal class

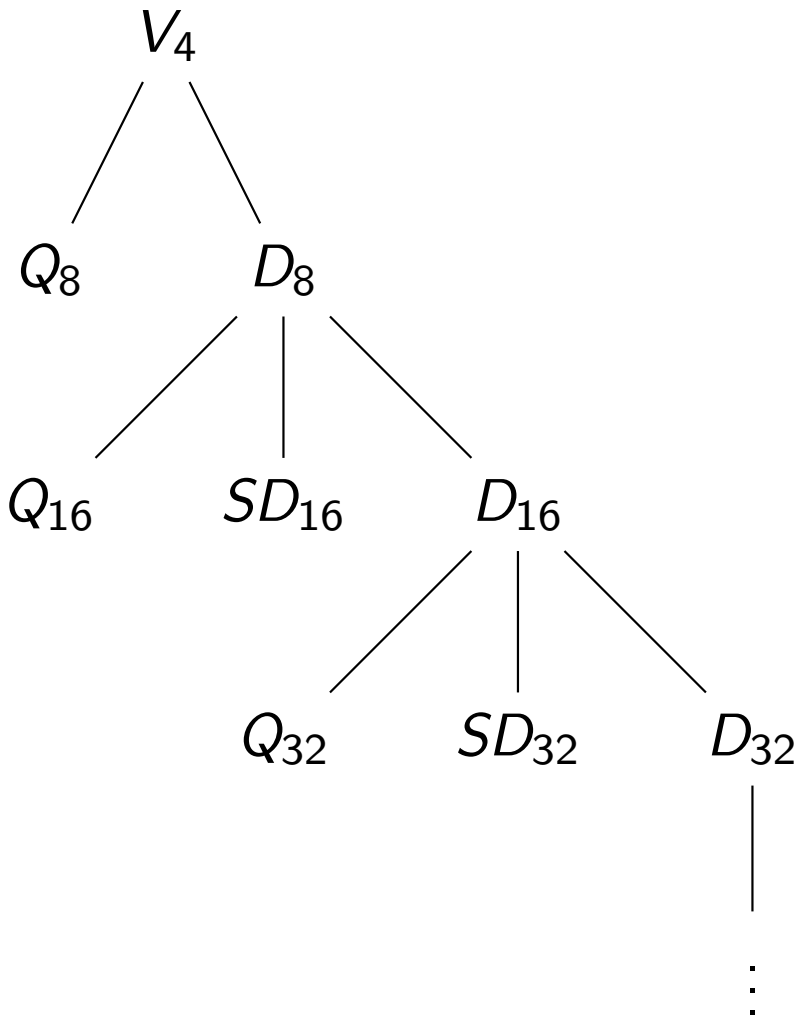
Theorem

2-groups of maximal class are precisely the following:

1. $C_2 \times C_2$ *and* C_4*;*
2. *Dihedral 2-groups;*
3. *Semidihedral 2-groups;*
4. *Generalized quaternion groups.*

The coclass graph for 2-groups of maximal class

There is an isolated vertex C_4 and one infinite tree



Enumeration of finite groups

Numerical evidence

there are

$$49,910,529,484$$

different isomorphism classes of groups of order at most 2000, and

$$49,487,365,422$$

which is just over 99%, are groups of order 1024.

```
gap> Sum(List([1..2000], i -> NrSmallGroups(i)));
49910529484
gap> Float(NrSmallGroups(1024) / last);
0.991522
```

Asymptotic result

Theorem (Phillip Hall)

The number of isomorphism classes of groups of order p^n is

$$p^{\frac{2}{27}n^3+O(n^{8/3})}.$$

We will sketch a proof of the fact that the number of groups of order p^n is roughly p^{n^3}.

Higman's PORC conjecture

Conjecture (Higman's PORC conjecture)

For each positve integer n there exists a positive integer m such that the number of isomorphism types of groups of order p^n is a **p***olynomial in p which depends* **o***n* **r***esidue* **c***lasses modulo m.*

Example (James, 1988)

If $p > 3$, then the number of groups of order p^6 is

$$\frac{13p^2 + 145p + 80(p-1,3) + 45(p-1,4) + 8(p-1,5) + 8(p-1,6)}{4}.$$

Elementary bound

A group of order n is determined by its multiplication table. Hence there are at most n^{n^2} groups of order n.

Lemma

A group G of order n can be generated by a set of at most $\log_2 n$ elements.

Proposition

The number of groups of order n is at most $n^{n \log_2 n}$.

Less (but still) elementary way of counting p-groups

Let r be a positive integer and F_r a free group on $\{x_1, \ldots, x_r\}$. Denote

$$G_r = F_r / F_r^{p^2} \gamma_2(F_r)^p \gamma_3(F).$$

We identify x_i with their images in G_r, so $x_1, \ldots, x_r$ generate G_r.

Definition

A finite p-group G is said to have Φ-**class 2** if there exists a central elementary abelian subgroup H of G such that G/H is elementary abelian. In other words, G is a central extension of an elementary abelian group by an elementary abelian group.

Every group of Φ-class 2 is a homomorphic image of some G_r.

The group G_r

Lemma

1. *The group G_r is a finite p-group.*
2. *The Frattini subgroup* $\mathrm{Frat}(G_r)$ *is central of order* $p^{r(r+1)/2}$ *and index* p^r.
3. *Any automorphism* $\alpha \in \mathrm{Aut}(G_r$ *that induces an identity mapping on* $G_r/\mathrm{Frat}(G_r)$ *fixes* $\mathrm{Frat}(G_r)$ *pointwise.*

Lemma

Let N_1 and N_2 be subgroups of $\mathrm{Frat}\, G_r$. *Then* $G_r/N_1 \cong G_r/N_2$ *if and only if there exists* $\alpha \in \mathrm{Aut}\, G_r$ *such that* $N_1^\alpha = N_2$.

Counting

Proposition

Let r be a positive integer, and s an integer such that $1 \leq s \leq r(r+1)/2$. Then there are at least $p^{rs(r+1)/2-r^2-s^2}$ isomorphism classes of groups of order p^{r+s}.

Idea of proof

Let G_r be as above. Let X be the set of subgroups $N \leq \operatorname{Frat} G_r$ of index p^s in $\operatorname{Frat} G_r$. Each $N \in X$ gives rise to a group G_r/N of order p^{r+s}.

The above discussion implies that the set of isomorphism classes of these groups is in 1-1 correspondence with the set of orbits of $\operatorname{Aut} G_r$ acting on X. Now count the orbits using the above auxiliary results.

Lower bound

The above result yields roughly $p^{x^2yn^3/2}$ groups with Frattini subgroup of index p^{xn} and order p^{yn}. Maximizing the function $z = x^2y/2$ under the constraint $x + y = 1$ yields the maximum value $z = 2/27$.

Theorem

The number of groups of order p^n is at least

$$p^{\frac{2}{27}n^2(n-6)}.$$

An elementary upper bound – preparations

Let G be a group of order p^n and let

$$G = G_0 \geq G_1 \geq \cdots \geq G_{n-1} \geq G_n = \{1\}$$

be its chief series. For each i choose $g_i \in G_{i-1} - G_i$. Then every $g \in G$ may be written uniquely in **normal form** $g = g_1^{\alpha_1} \cdots g_n^{\alpha_n}$, where $\alpha_i \in \{0, 1, \ldots, p-1\}$.

We have

$$g_i^p = g_{i+1}^{\beta_{i,i+1}} \cdots g_n^{\beta_{i,n}}$$

and

$$[g_j, g_i] = g_{j+1}^{\gamma_{i,j,j+1}} \cdots g_n^{\gamma_{i,j,n}}$$

for some $\beta_{i,j}, \gamma_{i,j,k} \in \{0, 1, \ldots, p-1\}$, $j > i$.

It is easy to see that the above generators and relations form a presentation for G (called a **power commutator presentation** or **polycyclic presentation**).

An example

GAP calls the groups given by power-commutator presentations pcp groups. Here is an example of how GAP prints out presentations of pcp groups:

```
gap> G := PcGroupToPcpGroup(DihedralGroup(16));;
gap> PrintPcpPresentation(G);
g1^2 = id
g2^2 = g3
g3^2 = g4
g4^2 = id
g2 ^ g1 = g2 * g3 * g4
g3 ^ g1 = g3 * g4
```

Note that the conjugation relations can be rewritten into commutator ones using the identity $x^y = x[x, y]$, and that the trivial commutator relations are left out.

An upper bound

Theorem

The number of groups of order p^n is at most

$$p^{\frac{1}{6}(n^3-n)}.$$

Proof.

Let G be as above. The isomorphism class of G is determined by the values of $\beta_{i,j}$ and $\gamma_{i,j,k}$. There are at most p choices for each of these $(n^3 - n)/6$ elements, so there are at most $p^{\frac{1}{6}(n^3-n)}$ isomorphism classes of groups of order p^n. □

Pyber's result

Theorem (Pyber, 1993)

The number of groups of order $n = \prod p_i^{a_i}$ *is at most*

$$n^{\frac{2}{27}\mu(n)^2 + O(\mu(n)^{5/3})},$$

where $\mu(n) = \max a_i$.

- Special case: solvable groups;
- General case: using CFSG.