Groups of prime-power order

Bettina Eick

TU Braunschweig – Germany

L'Aquila, July 2023, Talk 1

History

Very selected ...

Groups and Symmetries

Groups and Symmetries

- Groups are a mathematical model for studing symmetries.

Groups and Symmetries

Groups and Symmetries

- Groups are a mathematical model for studing symmetries.
- Example: Permutation groups (Rubik's cube)

Groups and Symmetries

Groups and Symmetries

- Groups are a mathematical model for studing symmetries.
- Example: Permutation groups (Rubik's cube)
- Example: Crystallographic groups (Wall papers and crystals)

Groups and Symmetries

Groups and Symmetries

- Groups are a mathematical model for studing symmetries.
- Example: Permutation groups (Rubik's cube)
- Example: Crystallographic groups (Wall papers and crystals)
- Example: Galois groups (Solving polynomial equations)

Cayley

Cayley 1854

- Introduced the abstract definition for groups:

Cayley

Cayley 1854

- Introduced the abstract definition for groups:
- Groups are sets with an associative multiplication.

Cayley

Cayley 1854

- Introduced the abstract definition for groups:
- Groups are sets with an associative multiplication.
- Defined isomorphism between groups.

Cayley

Cayley 1854

- Introduced the abstract definition for groups:
- Groups are sets with an associative multiplication.
- Defined isomorphism between groups.
- Project: classify groups of a given order up to isomorphism.

Sylow

Sylow 1872

Let G be a group of order $p^n m$ with $p \nmid m$. Then

Sylow

Sylow 1872

Let G be a group of order $p^n m$ with $p \nmid m$. Then

- G has a subgroup of order p^n.

Sylow

Sylow 1872

Let G be a group of order $p^n m$ with $p \nmid m$. Then

- G has a subgroup of order p^n.
- All subgroups in G of order p^n are conjugate.

Sylow

Sylow 1872

Let G be a group of order $p^n m$ with $p \nmid m$. Then

- G has a subgroup of order p^n.
- All subgroups in G of order p^n are conjugate.
- The number of subgroups of order p^n has the form $1 + kp$.

Power-conjugate presentations

The proof of Sylow's theorem

contains many interesting observations on p-groups. For example:

Power-conjugate presentations

The proof of Sylow's theorem

contains many interesting observations on p-groups. For example:

- Each finite p-group has a non-trivial center.

Power-conjugate presentations

The proof of Sylow's theorem

contains many interesting observations on p-groups. For example:

- Each finite p-group has a non-trivial center.
- Each finite p-group is solvable.

Power-conjugate presentations

The proof of Sylow's theorem

contains many interesting observations on p-groups. For example:

- Each finite p-group has a non-trivial center.
- Each finite p-group is solvable.
- If $|G| = p^n$, then G has generators $g_1, \ldots, g_n$ with

$$\begin{array}{rcll} g_i^p & = & g_{i+1}^{e_{i,i+1}} \cdots g_n^{e_{i,n}} & 1 \le i \le n \\ g_j^{-1} g_i g_j & = & g_i g_{i+1}^{f_{j,i,i+1}} \cdots g_n^{f_{j,i,n}} & 1 \le j < i \le n \end{array}$$

with exponents e_{ik} and f_{jik} in $\{0, \ldots, p-1\}$.

Power-conjugate presentations

The proof of Sylow's theorem

contains many interesting observations on p-groups. For example:

- Each finite p-group has a non-trivial center.
- Each finite p-group is solvable.
- If $|G| = p^n$, then G has generators $g_1, \ldots, g_n$ with

$$\begin{aligned} g_i^p &= g_{i+1}^{e_{i,i+1}} \cdots g_n^{e_{i,n}} \quad 1 \leq i \leq n \\ g_j^{-1} g_i g_j &= g_i g_{i+1}^{f_{j,i,i+1}} \cdots g_n^{f_{j,i,n}} \quad 1 \leq j < i \leq n \end{aligned}$$

  with exponents e_{ik} and f_{jik} in $\{0, \ldots, p-1\}$.
- First steps twowards power-conjugate presentations.

P. Hall

Philip Hall (1932/1940/1960)

P. Hall

Philip Hall (1932/1940/1960)

- Used power-conjugate presentations.

P. Hall

Philip Hall (1932/1940/1960)

- Used power-conjugate presentations.
- Invented the 'Collection' algorithm (multiplication).

P. Hall

Philip Hall (1932/1940/1960)

- Used power-conjugate presentations.
- Invented the 'Collection' algorithm (multiplication).
- Introduced 'isoclinism'.

P. Hall

Philip Hall (1932/1940/1960)

- Used power-conjugate presentations.
- Invented the 'Collection' algorithm (multiplication).
- Introduced 'isoclinism'.
- Classified the groups of order 2^5.

P. Hall

Philip Hall (1932/1940/1960)

- Used power-conjugate presentations.
- Invented the 'Collection' algorithm (multiplication).
- Introduced 'isoclinism'.
- Classified the groups of order 2^5.
- Determined the groups of order 2^7 (unpublished).

GAP Examples 1

GAP Examples 1

SmallGroups Library I

SmallGroups Library in GAP

```
gap> ll := AllSmallGroups(8);
[ <pc group of size 8 with 3 generators>,
  <pc group of size 8 with 3 generators>,
  <pc group of size 8 with 3 generators>,
  <pc group of size 8 with 3 generators>,
  <pc group of size 8 with 3 generators> ]

gap> List(ll, StructureDescription);
[ "C8", "C4 x C2", "D8", "Q8", "C2 x C2 x C2" ]

gap> PrintPcpPresentation(PcGroupToPcpGroup(ll[4]));
g1^2 = g3
g2^2 = g3
g3^2 = id
g2 ^ g1 = g2 * g3
```

Permutation groups

Permutation Groups

```
gap> G := SymmetricGroup(100);
Sym( [ 1 .. 100 ] )
gap> Collected(Factors(Size(G)));
[ [2, 97], [3, 48], [5, 24], [7, 16], [11, 9], [13, 7],
  [17, 5], [19, 5], [23, 4], [29, 3], [31, 3], [37, 2],
  [41, 2], [43, 2], [47, 2], [53, 1], [59, 1], [61, 1],
  [67, 1], [71, 1], [73, 1], [79, 1], [83, 1], [89, 1],
  [97, 1] ]
gap> H := SylowSubgroup(G, 7);
<permutation group of size 33232930569601 ...>
gap> iso := IsomorphismPcGroup(H);;
gap> U := Image(iso);
<pc group of size 33232930569601 with 16 generators>
```

Matrix groups

Matrix Groups

```
gap> G := GL(4, 9);
GL(4,9)
gap> U := SylowSubgroup(G, 3);
<matrix group of size 531441 with 6 generators>
```

Numbers of groups

Numbers of groups

```
gap> NumberSmallGroups(128);
2328
gap> Sum(List([1..200], NumberSmallGroups));
6065

gap> NumberSmallGroups(2^(10));
49487367289
gap> Sum(List([1..2000], NumberSmallGroups));
49910531351
```

Groups of order 2^n

	Number	Comment
2^1	1	
2^2	2	
2^3	5	
2^4	14	Hölder 1893
2^5	51	Miller 1898
2^6	267	Hall & Senior 1964
2^7	2328	James, Newman & O'Brien 1990
2^8	56 092	O'Brien 1991
2^9	10 494 213	Eick & O'Brien 2000
2^{10}	49 487 367 289	Eick & O'Brien 2000, Burrell 2021

Classifying p-groups

Classifying p-groups

Classifying of p-groups by order

Aims

- **(Strong)** Determine up to isomorphism a complete and irredundant list of groups of order p^n.

Classifying of p-groups by order

Aims

- **(Strong)** Determine up to isomorphism a complete and irredundant list of groups of order p^n.
- **(Weaker)** Determine the number $f(n,p)$ of isomorphism types of groups of order p^n.

Classifying of p-groups by order

Aims

- **(Strong)** Determine up to isomorphism a complete and irredundant list of groups of order p^n.
- **(Weaker)** Determine the number $f(n,p)$ of isomorphism types of groups of order p^n.
- **(Variation)** Investigate $f(n,p)$ as a function in n or as a function in p.

As a function in n

Theorem (Higman 1960 -Sims 1964)

Consider $f(n, p)$ as a function in n and write

$$f(n, p) = p^{An^3} \text{ with } A = A(n, p).$$

Then there exists $\epsilon_n > 0$ with $\epsilon_n \to \infty$ if $n \to \infty$ and

$$\frac{2}{27} - \epsilon_n \leq A \leq \frac{2}{27} + \epsilon_n.$$

GAP Examples 2

GAP Examples 2

Descendants

Computing Descendants

```
gap> PqDescendants(SmallGroup(4,2) : AllDescendants:=true);
[ <pc group of size 8 with 3 generators>,
  <pc group of size 8 with 3 generators>,
  <pc group of size 8 with 3 generators>,
  <pc group of size 16 with 4 generators>,
  <pc group of size 16 with 4 generators>,
  <pc group of size 16 with 4 generators>,
  <pc group of size 32 with 5 generators> ]
gap> List(last, IdGroup);
[[8,2], [8,3], [8,4], [16,2], [16,3], [16,4], [32,2]]
```