Construction of finite groups

Bettina Eick

TU Braunschweig – Germany

Gap days, Brüssel, April 2025

Groups and Symmetries

Groups and Symmetries

- Groups are a mathematical model for studying symmetries.

Groups and Symmetries

Groups and Symmetries

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

Groups and Symmetries

Groups and Symmetries

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

Abstract Groups

Cayley 1854

- Introduced the abstract definition for groups:

Abstract Groups

Cayley 1854

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

Abstract Groups

Cayley 1854

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

Abstract Groups

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.

Simple groups

Simple groups

simple: has no non-trivial normal subgroup.

Simple groups

Simple groups

simple: has no non-trivial normal subgroup.

- The finite simple groups have been classified completely.

Simple groups

Simple groups

simple: has no non-trivial normal subgroup.

- The finite simple groups have been classified completely.
- Finite groups are not classified.

Aims I: fixed order

Aims

For a fixed given order n:

Aims I: fixed order

Aims

For a fixed given order n:

- Strong aim: Compute a complete and irredundant list of groups of order n up to isomorphism.

Aims I: fixed order

Aims

For a fixed given order n:

- Strong aim: Compute a complete and irredundant list of groups of order n up to isomorphism.
- Weaker aim: Enumerate the number of isomorphism types of groups of order n.

Aims II: generic orders

Aims

For a given factorisation of orders: (e.g. p^3q)

Aims II: generic orders

Aims

For a given factorisation of orders: (e.g. p^3q)

- Strong aim: Determine the groups of this given order up to isomorphism.

Aims II: generic orders

Aims

For a given factorisation of orders: (e.g. p^3q)

- Strong aim: Determine the groups of this given order up to isomorphism.
- Weaker aim: Enumerate the number of isomorphism types of groups of the given order.

Early history

Early history: hand calculations

- Cayley (1854): orders at most 12

Early history

Early history: hand calculations

- Cayley (1854): orders at most 12
- Netto (1882): orders p^2 and pq

Early history

Early history: hand calculations

- Cayley (1854): orders at most 12
- Netto (1882): orders p^2 and pq
- Hölder (1893): orders p^3, p^2q, pqr and p^4

Early history

Early history: hand calculations

- Cayley (1854): orders at most 12
- Netto (1882): orders p^2 and pq
- Hölder (1893): orders p^3, p^2q, pqr and p^4
- Le Vavasseur (1896) / Miller (1896): orders $8p$

Early history

Early history: hand calculations

- Cayley (1854): orders at most 12
- Netto (1882): orders p^2 and pq
- Hölder (1893): orders p^3, p^2q, pqr and p^4
- Le Vavasseur (1896) / Miller (1896): orders $8p$
- Miller (1896): order 32

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}	49 487 365 422	Eick & O'Brien 2000

Groups of order p^n, $p > 5$

	Number	Comment
p^1	1	
p^2	2	
p^3	5	
p^4	15	
p^5	$2p + 61 + (p-1,4) + 2(p-1,3)$	Bagnera 1898
p^6	$3p^2 + 39p + 344 + 24(p-1,3) + 11(p-1,4) + 2(p-1,5)$	Newman, O'Brien, Vaughan-Lee 2004
p^7	$3p^5 + \dots$	O'Brien, Vaughan-Lee 2005

As a function in p

PORC

A function is PORC if it is a Polynomial On Residue Classes.

PORC Conjecture (Higman 1960)

The number of groups of order p^n for fixed n as a function in p is PORC.

State

Proved for $n \leq 7$ and open for $n \geq 8$.

Examples of classifications

Examples of classifications

- Orders at most 200 (except 128 and 192):
  Lunn & Senior (1934) – by hand

Examples of classifications

Examples of classifications

- Orders at most 200 (except 128 and 192):
  Lunn & Senior (1934) – by hand
- Orders at most 2000 (1024 enumerated only):
  Besche, Eick & O'Brien (2000) – by computer

Examples of classifications

Examples of classifications

- Orders at most 200 (except 128 and 192):
  Lunn & Senior (1934) – by hand
- Orders at most 2000 (1024 enumerated only):
  Besche, Eick & O'Brien (2000) – by computer
- Orders at most 20.000 (39 exceptions):
  Eick, Horn & Hulpke (2018) – by computer

Algorithms

Algorithms for nilpotent groups

- Nilpotent groups are direct products of p-groups

Algorithms

Algorithms for nilpotent groups

- Nilpotent groups are direct products of p-groups
- p-group generation – O'Brien (1990)

Algorithms II

Algorithms for solvable groups

- Frattini extension method – Besche & Eick (2000)

Algorithms II

Algorithms for solvable groups

- Frattini extension method – Besche & Eick (2000)
- Solvable group construction – Eick & Horn (2018)

Algorithms II

Algorithms for solvable groups

- Frattini extension method – Besche & Eick (2000)
- Solvable group construction – Eick & Horn (2018)
- Split extension method – Besche & Eick (2000)

Algorithms III

Algorithms for non-solvable groups

- Cyclic extension method – Besche & Eick (2000)

Algorithms III

Algorithms for non-solvable groups

- Cyclic extension method – Besche & Eick (2000)
- Supplement method – Archer (2005), Eick, Horn & Hulpke (2018)

Examples of classifications

Examples of classification

- Squarefree orders – Slattery (2000), Besche (2000)

Examples of classifications

Examples of classification

- Squarefree orders – Slattery (2000), Besche (2000)
- Cubefree orders – Dietrich & Eick (2005)

Examples of classifications

Examples of classification

- Squarefree orders – Slattery (2000), Besche (2000)
- Cubefree orders – Dietrich & Eick (2005)
- Groups of order p^n with $n \leq 7$ – Vaughan-Lee & O'Brien (2005)

Examples of classifications

Examples of classification

- Squarefree orders – Slattery (2000), Besche (2000)
- Cubefree orders – Dietrich & Eick (2005)
- Groups of order p^n with $n \leq 7$ – Vaughan-Lee & O'Brien (2005)
- Groups of order $p^n q$ with $n \leq 5$ – Eick & Moede (2017)

Groups of order $p^n q$

Groups of order $p^n q$

Split the groups up into

- Nilpotent groups $G \times C_q$ with $|G| = p^n$.

Groups of order $p^n q$

Groups of order $p^n q$

Split the groups up into

- Nilpotent groups $G \times C_q$ with $|G| = p^n$.
- Groups with normal Sylow p-subgroup $G \rtimes C_q$.

Groups of order $p^n q$

Groups of order $p^n q$

Split the groups up into

- Nilpotent groups $G \times C_q$ with $|G| = p^n$.
- Groups with normal Sylow p-subgroup $G \rtimes C_q$.
- Groups with normal Sylow q-subgroup $C_q \rtimes G$.

Groups of order $p^n q$

Groups of order $p^n q$

Split the groups up into

- Nilpotent groups $G \times C_q$ with $|G| = p^n$.
- Groups with normal Sylow p-subgroup $G \rtimes C_q$.
- Groups with normal Sylow q-subgroup $C_q \rtimes G$.
- Groups without normal Sylow subgroup.

Groups of order $p^n q$ II

Groups $G \rtimes C_q$

- Take G a group of order p^n with $n \leq 5$.

Groups of order $p^n q$ II

Groups $G \rtimes C_q$

- Take G a group of order p^n with $n \leq 5$.
- Get the conjugacy classes of subgroups of order q in $Aut(G)$.

Groups of order $p^n q$ II

Groups $G \rtimes C_q$

- Take G a group of order p^n with $n \leq 5$.
- Get the conjugacy classes of subgroups of order q in $Aut(G)$.
- Yields groups $G \rtimes C_q$ up to isomorphism.

Groups of order $p^n q$ III

Groups $G \rtimes C_q$

- Take G a group of order p^n with $n \leq 5$.

Groups of order $p^n q$ III

Groups $G \rtimes C_q$

- Take G a group of order p^n with $n \leq 5$.
- Get $Aut(G)$-classes of $N \trianglelefteq G$ with $[G : N] \mid (q-1)$.

Groups of order $p^n q$ III

Groups $G \rtimes C_q$

- Take G a group of order p^n with $n \leq 5$.
- Get $Aut(G)$-classes of $N \trianglelefteq G$ with $[G : N] \mid (q-1)$.
- Yields groups $C_q \rtimes G$ up to isomorphism.

Results

Resulting group libraries

- Small Group Library (GAP and MAGMA)

Results

Resulting group libraries

- Small Group Library (GAP and MAGMA)
- Lie p-ring package (GAP)

Challenges

Challenges

Among the orders at most 20.000:

- Orders divided by 2^{10} or 3^9.

Challenges

Challenges

Among the orders at most 20.000:

- Orders divided by 2^{10} or 3^9.
- Orders $2^9 \cdot m$ with m not prime.

Challenges

Challenges

Among the orders at most 20.000:

- Orders divided by 2^{10} or 3^9.
- Orders $2^9 \cdot m$ with m not prime.
- Orders divided by $2^8 p^2$.

Challenges

Challenges

Among the orders at most 20.000:

- Orders divided by 2^{10} or 3^9.
- Orders $2^9 \cdot m$ with m not prime.
- Orders divided by $2^8 p^2$.
- Exceptional cases: $2^2\ 3^7$, $2^7\ 3^4$, $2^7\ 5^3$, $2^3\ 3^7$, $2^7\ 3\ 7^2$.

GAP Session

GAP Session

SmallGroups Library

SmallGroupsLibrary

```
gap> NumberSmallGroups(1999);
1
gap> NumberSmallGroups(2000);
963
gap> List([1..10], x -> NumberSmallGroups(2^x));
[ 1, 2, 5, 14, 51, 267, 2328, 56092, 10494213, 49487367289 ]
gap> Sum(List([1..2000], NumberSmallGroups));
49910531351
```

SmallGroups Library II

SmallGroupsLibrary II

```
gap> SmallGroupsAvailable(2000);
true
gap> SmallGroupsAvailable(2016);
false
gap> 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(last, StructureDescription);
[ "C8", "C4 x C2", "D8", "Q8", "C2 x C2 x C2" ]
gap> SmallGroup(8,1);
<pc group of size 8 with 3 generators>
```

SmallGroups Library III

SmallGroupsLibrary III

```
gap> G := SylowSubgroup(SymmetricGroup(4),2);
Group([ (1,2), (3,4), (1,3)(2,4) ])
gap> IdGroup(G);
[ 8, 3 ]
gap> SmallGroupsInformation(8);

  There are 5 groups of order 8.

  The groups whose order factorises in at most 3 primes
  have been classified by O. Hoelder. This classification is
  used in the SmallGroups library.

  This size belongs to layer 1 of the SmallGroups library.
  IdSmallGroup is available for this size.
```

GrpConst Package

GrpConst Package

```
gap> SmallGroup(2016, 1);
Error, the library of groups of size 2016 is not available
....
```

GrpConst Package II

GrpConst Package II

```
gap> LoadPackage("grpconst");
...
gap> SetInfoLevel(InfoGrpCon, 1);
gap> ConstructAllGroups(2016);
...
... 102 nilpotent groups
... 313 Frattini factor candidates
... 6417 solvable non-nilpotent groups
... 20 non-solvable groups
```