Some topics in the theory of finite groups[1]

Primož Moravec

[1] Version: June 19, 2014

Contents

Introduction

c:intro

These notes form a background material for a short course on group theory that will be given at *2014 PhD Summer School in Discrete Mathematics and SYGN, Rogla, Slovenia.* The main purpose of the course will be to give an overview of some topics of the theory of finite groups that often appear as applications in discrete mathematics. Since the summer school is aimed primarily at PhD students who are working in the latter area and may not necessarily be experts in group theory, I will give a fairly general introduction to three main topics: Finite Simple Groups, Extension Theory of Groups, and Nilpotent groups and Finite p-groups. The choice of the first two topics is clear from the point of view of classifying all finite groups. It turns out that the knowledge of all finite simple groups, together with knowing how to "glue" two groups together to produce new ones, in principle provides a way of constructing *all* finite groups. The first problem, classification of finite simple groups (CFSG), has been resolved satisfactory, and one can operate with a full list of these groups. In these notes we will only touch this vast area by showing simplicity of alternating groups and projective special linear groups. We will sketch the classification, but ommit almost all further details. We will move on to extension theory which tells us how to construct new groups from old. The extension problem of classifying all possible extensions of one group by another appears to be hard (impossible?) to solve in general. We will only study a very special case of it.

There are two main reasons why to deal with finite p-groups, i.e., groups whose orders are powers of a prime p. The first is clear to an undergraduate student: finite p-groups appear as Sylow p-subgroups of finite groups. The second is more delicate and motivated by a vague statement "*Almost all finite groups are p-groups.*" We will not make any attempt of making this statement more precise, but rather develop some basic theory of these groups and indicate their complexity within the universe of all finite groups.

In addition to the above, we include preliminaries that will be needed in subsequent chapters. We collect some basic properties of groups with focus on finite groups. We also exhibit as many examples as possible in order to illustrate and motivate the theory. A general experience is that most of the students only know some standard types of groups, such as abelian groups, dihedral groups, symmetric and alternating groups,... Other groups which do not have clean descriptions are usually put aside. In order to avoid this, I will use `GAP` (`G`roups, `A`lgorithms, and `P`rogramming), a computational system designed for constructing and manipulating with groups. `GAP` will be applied in exploring properties of groups, and even providing proofs of statements. Examples with full `GAP` code will be given, but I have decided to leave out all explanations of the syntax and programming rules. There are two reasons for this. One is that the reader will mostly find it easy to figure out what a given line of `GAP` code does, since the syntax is very much self-explanatory. The second one is that there is an extensive manual of `GAP`, together with tons of tutorials and self-study material available at `GAP`'s web page [5]. We encourage the reader to download `GAP` (it's open source) and try out all of the examples in these notes.

I have closely followed Robinson's book *A course in the theory of groups* [8] and Cameron's lecture notes on finite groups [4], thus I claim very little originality as far as for the exposition goes.

CHAPTER 1

Basic notions and examples

c:prelim

In this chapter we collect some basic properties of groups and important examples the reader should be familiar with in order to read these notes. Most of the proofs in this chapter will be omitted. We will also show how to use GAP in performing explicit calculations with groups. Concrete examples of computations will be presented.

A convention about the notations. All (or most) of the functions we consider will be acting from the right. This means that if $f : X \to Y$ is a function and $x \in X$, then the image of x under f will (usually) be denoted by x^f or xf.

The main sources of the material covered here are [6] and [8].

1. Groups

s:groups

A non-empty set G equipped with a binary operation $\circ$ is a *group* if the following hold:

- Associativity: $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$;
- Identity element: there exists $e \in G$ such that $e \circ a = a \circ e = a$ for all $a \in G$;
- Inverse: For every $a \in G$ there exists $a' \in G$ such that $a \circ a' = a' \circ a = e$.

It is easy to show that the identity element e is uniquely determined, and that every $a \in G$ has a unique inverse, denoted by a^{-1}. For most of the time we write $\cdot$ instead of $\circ$; in this case, when there is no confusion, we write 1 instead of e (multiplicative notation). If $g, h \in G$, we will often use the notation $g^h = h^{-1}gh$ for *conjugation* of g by h. If the set G is finite, then we say that G is a *finite group*, and $|G|$ is called the *order* of G.

A group G is *abelian* if $a \circ b = b \circ a$ for all $a, b \in G$. In this case we often write $+$ instead of $\circ$, and the identity element is denoted by 0 (additive notation).

A subset H of G is called a *subgroup* of G if it is a group under the same operation. We write $H \leq G$. One can verify directly that H is a subgroup of G if and only if $ab^{-1} \in H$ for all $a, b \in H$.

If H is a subgroup of G and $a \in G$, then we define *left (right) cosets* of H by

$$aH = \{ah \mid h \in H\},$$
$$Ha = \{ha \mid h \in H\}.$$

The set of all left cosets of H in G is denoted by G/H, and the set of all right cosets by $H\backslash G$. Different left (right) cosets form a partition of G. The number of left (= the number of right) cosets of H in G is the *index* of H in G and is denoted by $|G : H|$. If G is a finite group then *Lagrange's theorem* says that $|G| = |H| \cdot |G : H|$. In particular, if $H \leq G$, then $|H|$ divides the order of G.

The intersection of a family of subgroups of a given group G is again a subgroup of G. Thus, if X is a non-empty subset of G, then there exists the smallest subgroup of G containing X. It is denoted by $\langle X \rangle$ and called the *subgroup generated by* X. We say that a group G is *finitely generated* if there exists a finite set X of its elements such that $G = \langle X \rangle$.

Let G_1 and G_2 be groups. A map $\phi : G_1 \to G_2$ is said to be a homomorphism of groups if it preserves group operation, that is,

$$(ab)^\phi = a^\phi b^\phi \text{ for all } a, b \in G_1,$$

where the products are calculated in the corresponding groups. The set

$$\ker \phi = \{x \in G_1 \mid x^\phi = 1\}$$

is said to be *the kernel* of ϕ and is a subgroup of G_1. The set

$$\operatorname{im} \phi = \{x^\phi \mid x \in G_1\}$$

is a subgroup of G_2 and is called the *image* of ϕ. A group homomorphism $\phi : G_1 \to G_2$ is said to be an *epimorphism* if $\operatorname{im}\phi = G_2$; *monomorphism* if $\ker\phi = \{1\}$; isomorphism if it is epimorhism and monomorphism; *endomorphism* if $G_1 = G_2$. A bijective endomorphism is also called an *automorphism*.

A subgroup H of G is said to be a *normal subgroup* of G if $xH = Hx$ for every $x \in G$. Equivalently, $x^{-1}Hx \subseteq H$ for all $x \in G$, i.e., H is *closed under conjugation* by the elements of G. If H is a normal subgroup of G then the sets of left and right cosets of H in G coincide, and we use common notation G/H for these. The operation on G/H given by $Ha \cdot Hb = H(ab)$ is well defined and turns G/H into a group called the *factor group* of G over H. The map $\rho : G \to G/H$ given by $g^\rho = Hg$ is a surjective homomorphism of groups with $\ker\rho = H$.

The intersection of a family of normal subgroups of G is again a normal subgroup of G. Thus, given a set $X \subseteq G$, there exists the smallest normal subgroup of G containing X. It is denoted by $\langle\langle X\rangle\rangle$ and called the *normal closure* of X in G.

t:firstiso

Theorem 1.0.1 (First Isomorphism Theorem). *Let $\phi : G_1 \to G_2$ be a homomorphism of groups. Then $G_1/\ker\phi \cong \operatorname{im}\phi$.*

t:secondiso

Theorem 1.0.2 (Second Isomorphism Theorem). *Let H be a subgroup and N a normal subgroup of G. Then $H \cap N \lhd H$, and $HN/N \cong H/(H \cap N)$.*

t:thirdiso

Theorem 1.0.3 (Third Isomorphism Theorem). *Let M and N be normal subgroups of G and let $N \leq M$. Then $M/N \lhd G/N$ and $(G/N)/(M/N) \cong G/M$.*

One can generalize the notion of normal subgroups as follows. A subgroup H of G is said to be *subnormal* in G if there exists a finite series $H = H_0 \lhd H_1 \lhd H_1 \lhd \cdots \lhd H_d = G$. The shortest length of such a series is called the *defect* of H in G. Subnormal subgroups of defect one are precisely normal subgroups.

Two other notions related to normal subgroups are the following. A subgroup H of G is said to be *fully invariant* if $H^\alpha \leq H$ for every endomorphism α of G. Similarly, H is *characteristic* in G if $H^\alpha \leq H$ for every automorphism α of G. The following is straightforward:

l:finvchar

Lemma 1.0.1. *The properties of being a 'characteristic subgroup' and 'fully invariant subgroup' are transitive relations. If H is characteristic in K and K normal in G then $H \lhd G$.*

Let G be a group and $x, y \in G$. The *commutator* of x and y is defined by $[x, y] = x^{-1}y^{-1}xy = x^{-1}x^y$. The subgroup G' generated by all the commutators $[x, y]$, where $x, y \in G$, is called the *derived subgroup* or the *commutator subgroup* of G. Since $[x, y]^\alpha = [x^\alpha, y^\alpha]$ for all endomorphisms α of G, it follows that G' is a fully invariant subgroup of G. It is easy to verify that G/G' is abelian. Furthermore, if N is normal subgroup of G with G/N abelian, then $G' \leq N$. Thus G/G' can be seen as the largest abelian quotient of G. It is called the *abelianization* of G. If $G = G'$, then G is said to be a *perfect group*.

For a group G we define its *center* to be $Z(G) = \{g \in G \mid [g, x] = 1 \text{ for all } x \in G\}$. It is easy to verify that $Z(G)$ is a characteristic subgroup of G.

Let G_1 and G_2 be groups. The *direct product* $G_1 \times G_2$ is the group whose elements are all pairs $(g_1, g_2) \in G_1 \times G_2$, and the operation is given by

$$(a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2).$$

p:direct

Proposition 1.0.1. *Let G, G_1 and G_2 be groups. Then $G \cong G_1 \times G_2$ if and only if there exist normal subgroups H_1 and H_2 of G such that $H_i \cong G_i$ for $i = 1, 2$, $H_1 \cap H_2 = 1$ and $H_1H_2 = G$.*

More generally, $G \cong G_1 \times G_2 \times \cdots \times G_n$ if and only if there exist normal subgroups $H_1, \ldots, H_n$ of G such that $H_i \cong G_i$, $G = H_1H_2 \cdots H_n$, and

$$H_i \cap H_1 \cdots H_{i-1}H_{i+1} \cdots H_n = \{1\}$$

for all i. This follows from Proposition 1.0.1 by induction.

Let X be a non-empty set, F a group, and $\iota : X \to F$ a function. Then F, together with ι, is said to be a *free group* on X if for each function α from X to a group G there exists a homomorphism $\beta : F \to G$ such that $\alpha = \iota\beta$. It is easy to show that ι has to be injective. Up to isomorphism, there is precisely one free group on a given set X. It can be constructed as a group whose elements are reduced words in $X \cup X^{-1}$, and the operation is concatenation, followed by reduction of terms of the form $x^{\pm 1}x^{\mp 1}$ if necessary. For further details we refer to [8].

Let X be a set and let F be a free group on X. Choose a subset Y of F, and let $R = \langle\langle Y \rangle\rangle$ be its normal closure in F. The we say that the group $G = F/R$ is given by *generators* X and *relations* Y. We write $G = \langle X \mid Y \rangle$.

The following result is simple but useful in recognizing groups from their presentations:

l:dyck **Lemma** 1.0.2 (von Dyck's Lemma). *Let G be a group generated by $x_1, \ldots, x_m$ satisfying relators $r_1 = 1, \ldots, r_n = 1$. Let H be a group generated by $y_1, \ldots, y_m$, and suppose that $r_i(y_1, \ldots, y_m) = 1$ for all $i = 1, \ldots, n$. Then there exists a uniquely determined epimorphism $\phi : G \to H$ with $x_j^\phi = y_j$ for all $j = 1, \ldots, m$.*

A sample application von Dyck's lemma will be given in the next section.

s:examples

2. Examples of groups and GAP

In this section we present some important examples of groups. Along the way we show how to use GAP to construct groups and study their properties. More information on how to obtain GAP and apply its commands can be found at [5].

2.1. Cyclic groups. A group generated by one element is called a *cyclic group*. If G is a cyclic group, two possibilites can occur. Either G is infinite, in which case it is isomorphic to $(\mathbb{Z}, +)$, or it is finite of order n, in which case it is isomorphic to $(\mathbb{Z}_n, +)$. In multiplicative notation, cyclic groups will be denoted by C_∞ and C_n, respectively.

In general, if G is an arbitrary group and $g \in G$, then the order of the cyclic subgroup $\langle g \rangle$ of G is called the *order* of g, and denoted by $|g|$.

In GAP, one can construct cyclic groups in several different ways. The standard one is as follows:

```
gap> G := CyclicGroup( 6 );
<pc group of size 6 with 2 generators>
gap> Elements( G );
[ <identity> of ..., f1, f2, f1*f2, f2^2, f1*f2^2 ]
```

The list of the elements above may be a bit unexpected, as it does not indicate that the group in question is cyclic. Rather, it reflects the fact that C_6 is isomorphic to $C_2 \times C_3$, and f1 and f2 are the corresponding generators of these factors.

It is possible to examine basic properties of the group we constructed above:

```
gap> Order( G );
6
gap> IsCyclic( G );
true
gap> IsAbelian( G );
true
```

Another way is to represent a cyclic group of order n with a generator x and relation $x^n = 1$. We first construct a free group on $\{x\}$ and then factor out the relation $x^n = 1$. For $n = 6$, this goes as follows:

```
gap> F := FreeGroup( "x" );
<free group on the generators [ x ]>
gap> AssignGeneratorVariables( F );
#I  Assigned the global variables [ x ]
gap> G := F / [ x^6 ];
<fp group on the generators [ x ]>
gap> Order( G );
6
gap> StructureDescription( G );
"C6"
gap> Elements( G );
[ <identity ...>, x^3, x^2, x^-1, x^-2, x ]
```

Note that the groups in the first and second example both represent C_6, yet, in GAP's eyes they are not identical objects, because GAP represents them in different ways. The first example represents C_6 as a `pc group`, and the second one as an `fp group`.

2.2. Abelian groups. Finitely generated *abelian groups* are classified by the following result:

t:fund **Theorem** 2.2.1 (Fundamental Theorem of Abelian Groups). *Every finitely generated 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. This follows from the fact that if m and n are relatively prime then $C_m \times C_n \cong C_{mn}$. A group that is isomorphic to the direct product of a number of copies of C_p is called an *elementary abelian p-group*. Every elementary abelian p-group (written additively) is also a vector space over GF(p). The scalar multiplication is given by

$$\lambda x = \underbrace{x + \cdots + x}_{\lambda-\text{times}}.$$

For example, one can construct $C_2 \times C_4 \times C_{12}$ in GAP as follows:

```
gap> G := AbelianGroup( [2, 4, 12 ] );
<pc group of size 96 with 3 generators>
gap> AbelianInvariants( G );
[ 2, 3, 4, 4 ]
```

The last command tells us that our group is isomorphic to $C_2 \times C_3 \times C_4 \times C_4$. In general, `AbelianInvariants( G );` returns a cyclic decomposition of G^{ab}.

2.3. Symmetric groups. If X is a non-empty set, then the set of all bijections $X \to X$ becomes a group under the operation of composition. It is denoted by Sym X. If X is a finite set, then we can write $X = \{1, 2, \ldots, n\}$, and we use the abbreviation S_n for Sym X in this case. The group S_n is called the *symmetric group* on n letters. Its elements are *permutations* that can be written as products of *cycles* of the form $(x_1\, x_2\, \ldots x_k)$ that represents the map $x_1 \mapsto x_2 \mapsto \cdots \mapsto x_k \mapsto x_1$, and all other elements are fixed. The order of S_n is $n!$. If $n > 2$, then S_n is clearly a non-abelian group.

Let us use GAP to play around with S_4 and its elements:

```
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)
gap> a^(-1);
(2,4,3)
gap> a^b;
(1,3,4)
gap> Order( a );
3
```

We can also present symmetric groups in terms of generators and relations. Here is an example:

e:S3 *Example* 2.3.1. Let $G = \langle x, y \mid x^2 = y^3 = (xy)^2 = 1\rangle$. We claim that $G \cong S_3$. Denote $a = (1\,2)$ and $b = (1\,2\,3)$. Then $a^2 = b^3 = (ab)^2 = 1$. By von Dyck's Lemma, there exists a surjective homomorphism $\phi : G \to \langle a, b\rangle = S_3$. Now consider G. We have that $yx = xy^2$, hence every element of G can be written as $x^m y^n$, where $0 \leq m \leq 1$, $0 \leq n \leq 2$. It follows that $|G| \leq 6$. Comparing the orders, we conclude that ϕ must be an isomorphism between G and S_3. Another proof can be done with GAP:

```
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"
```

In general, the group S_n has a following presentation:

$$\langle x_1, \ldots, x_{n-1} \mid x_i^2 = 1, [x_i, x_j] = 1, x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1} \text{ for all } i \text{ and } j \neq i \pm 1\rangle.$$

Using GAP, one can also construct subgroups generated by certain sets of elements, and normal closures of subgroups. It is also possible to test memberships to subgroups.

```
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"
```

The *parity* of s permutation $g \in S_n$ is defined to be the parity of the number $n - c(g)$, where $c(g)$ is the number of cycles of g (including the cycles of length 1). We regard the parity as an element of $\mathbb{Z}_2$. One can show that the parity is a homomorphism from S_n onto the group $\mathbb{Z}_2$. Its kernel consists of all permutations of even parity. It is denoted by A_n and called the *alternating group* on n letters.

Alternating groups can be constructed with GAP:

```
gap> G := AlternatingGroup( 4 );
Alt( [ 1 .. 4 ] )
gap> Order( G );
12
```

One can also locate A_4 within the list of all normal subgroups of S_4:

```
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"
```

We can also construct the natural homomorphism $S_4 \to S_4/A_4$ as follows:

```
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"
```

2.4. Linear groups. Let F be a field. The set of all invertible $n \times n$ matrices over F is a group under multiplication. It is called the *general linear group* of dimension n over F, and denoted by $\mathrm{GL}(n, F)$. By Galois' theorem, the order of a finite field is alwasy a prime power, and if q is a prime power, then there is, up to isomorphism, a unique field of order q. It is denoted by $\mathrm{GF}(q)$. The group $\mathrm{GL}(n, \mathrm{GF}(q))$ is also denoted as $\mathrm{GL}(n, q)$.

The determinant map $\det : \mathrm{GL}(n, F) \to F^\times$ is clearly a surjective homomorphism of groups. Its kernel is denoted by $\mathrm{SL}(n, F)$ and called the *special linear group* of dimension n over F. Its elements are precisely all the matrices $A \in \mathrm{GL}(n, F)$ with $\det A = 1$.

Let us consider some examples using GAP:

```
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
gap> StructureDescription( H );
"A5"
```

p:glorder **Proposition** 2.4.1. $|\mathrm{GL}(n, q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$.

Proof. A matrix is invertible if and only if its rows are linearly independent. This holds if and only if the first row is non-zero and, for $k = 2, \dots, n$, the k-th row is not in the subspace spanned by the first $k - 1$ rows. The number of possible rows is q^n, and the number lying in any k-dimensional subspace is q^k. So the number of choices for the first row is $q^n - 1$, and for $k = 2, \dots, n$, the number of choices for the k-th row is $q^n - q^{k-1}$. Multiplying these, we get the formula. □

c:slorder **Corollary** 2.4.1. $|\mathrm{SL}(n, q)| = |\mathrm{GL}(n, q)|/(q - 1)$.

Proof. Let $F = \mathrm{GF}(q)$. We already saw above that $\mathrm{GL}(n, q)/\mathrm{SL}(n, q) \cong F^\times$, and this gives the result. □

2.5. Dihedral groups. A *symmetry* of a figure in Euclidian space is a rigid motion (or a combination of a rigid motion with reflection) of the space that carries the figure to itself. If we think of a rigid motion as a linear map of the real vector space, then it can be rpresented by a matrix. Alternatively, if we label the vertices of the figure, then a symmetry can be represented as a permutation of these labels.

The group of symmetries of a regular n-gon is called a *dihedral group* D_{2n}. If a denotes the rotation around the center by the angle $2\pi/n$, and b the reflection over a chosen diagonal, then the elements of D_{2n} can be written uniquely in the form $a^k b^\ell$ where $0 \le k < n$ and $\ell \in \{0,1\}$. Thus $|D_{2n}| = 2n$. The group D_{2n} has a presentation

$$D_{2n} = \langle a, b \mid a^n = 1,\, b^2 = 1,\, a^b = a^{-1} \rangle.$$

In GAP, one can construct dihedral groups directly by

```
gap> G := DihedralGroup( 6 );
<pc group of size 6 with 2 generators>
gap> Order( G );
6
```

Another way is to present it by generators and relations. This is done by first constructing a free group on two generators and then factor out the relations.

```
gap> F := FreeGroup( "a", "b" );
<free group on the generators [ a, b ]>
gap> AssignGeneratorVariables(F);
#I  Assigned the global variables [ a, b ]
gap> H := F / [ a^3, b^2, a^b / a^(-1) ];
<fp group on the generators [ a, b ]>
gap> StructureDescription( H );
"S3"
```

The last command tells us that $D_6 \cong S_3$. We can compare both constructions of D_6 above and see that they are not identical objects in GAP, yet they are isomorphic:

```
gap> H = G;
false
gap> IsomorphismGroups(G, H);
[ f1, f2 ] -> [ b, a ]
```

The reason is that GAP represents D_6 in two different ways, first as a pc group and then as an fp group. The reader should consult GAP's manual for further details.

s:aut

3. Automorphisms

An *automorphism* of a group G is an isomorphism G to itself. There are special types of automorphisms called *conjugations* or *inner automorphisms*; they are of the form $c_g : x \to g^{-1}xg$.

p:aut

Proposition 3.0.1. *Let G be a group.*

(a) *The set* $\operatorname{Aut}(G)$ *of all automorphisms of G is a group under composition. This is the automorphism group of G.*
(b) *The set* $\operatorname{Inn}(G)$ *of all inner automorphisms of G is a normal subgroup of* $\operatorname{Aut} G$*. This is called the inner automorphism group of G.*
(c) $\operatorname{Inn}(G) \cong G/Z(G)$.

The proof is straightforward and we leave it as an exercise. The group $\operatorname{Out}(G) = \operatorname{Aut}(G)/\operatorname{Inn}(G)$ is the *outer automorphism group* of G. Note that its elements are not automorphisms, but rather right cosets $\operatorname{Inn}(G)\alpha$, where $\alpha \in \operatorname{Aut}(G)$.

GAP can deal with automorphisms very naturally:

```
gap> G := DihedralGroup( 12 );
<pc group of size 12 with 3 generators>
gap> A := AutomorphismGroup( G );
<group of size 12 with 3 generators>
gap> Elements( A );
[ [ f1*f3, f1*f2*f3^2, f1*f2*f3 ] -> [ f1*f2, f1*f3^2, f1 ],
  [ f1*f3, f1*f2*f3^2, f1*f2*f3 ] -> [ f1*f2*f3^2, f1*f3, f1 ],
  [ f1*f3, f1*f2*f3^2, f1*f2*f3 ] -> [ f1, f1*f2*f3, f1*f2 ],
  [ f1*f3, f1*f2*f3^2, f1*f2*f3 ] -> [ f1*f3, f1*f2*f3^2, f1*f2 ],
  [ f1*f3, f1*f2*f3^2, f1*f2*f3 ] -> [ f1*f2, f1*f3^2, f1*f3 ],
  [ f1*f3, f1*f2*f3^2, f1*f2*f3 ] -> [ f1*f2*f3, f1, f1*f3 ],
  [ f1*f3, f1*f2*f3^2, f1*f2*f3 ] -> [ f1*f3, f1*f2*f3^2, f1*f2*f3 ],
  [ f1*f3, f1*f2*f3^2, f1*f2*f3 ] -> [ f1*f3^2, f1*f2, f1*f2*f3 ],
  [ f1*f3, f1*f2*f3^2, f1*f2*f3 ] -> [ f1*f2*f3, f1, f1*f3^2 ],
  [ f1*f3, f1*f2*f3^2, f1*f2*f3 ] -> [ f1*f2*f3^2, f1*f3, f1*f3^2 ],
  [ f1*f3, f1*f2*f3^2, f1*f2*f3 ] -> [ f1, f1*f2*f3, f1*f2*f3^2 ],
  [ f1*f3, f1*f2*f3^2, f1*f2*f3 ] -> [ f1*f3^2, f1*f2, f1*f2*f3^2 ] ]
gap> StructureDescription( A );
"D12"
gap> inn := InnerAutomorphismsAutomorphismGroup( A );
<group with 3 generators>
gap> Order( inn );
6
gap> IsomorphismGroups( inn, G / Center( G ) );
CompositionMapping( [ (2,6)(3,5), (1,3,5)(2,4,6), (1,5,3)(2,6,4) ] ->
[ f1, f2^2, f2 ], <action isomorphism> )
```

Next we compute some automorphism groups:

p:autcyclic

Proposition 3.0.2. *$\operatorname{Aut} C_n \cong C_{\phi(n)}$, where ϕ is Euler's totient function.*

Proof. Let $C_n = \langle g \rangle$ and take $\alpha \in \operatorname{Aut} G$. Then $g^\alpha = g^i$ for some $0 \le i \le n-1$, and since $\langle g^i \rangle = C_n$, this can only happen if $\gcd(i,n) = 1$. Conversely take an endomorphism α of C_n with $g^\alpha = g^i$, where $\gcd(i,n) = 1$. Then it is elementary to see that α is an automorphism. Thus the map $\operatorname{Aut} C_n \to \mathbb{Z}_n^\times$ given by $\alpha \mapsto i$ is an isomorphism of groups. This proves the result. □

p:autCpn

Proposition 3.0.3. $\operatorname{Aut}(C_p^n) \cong \operatorname{GL}(n,p)$.

Proof. This follows from the fact that C_p^n is an n-dimensional vector space over $\operatorname{GF}(p)$. □

s:actsylow

4. Group actions and Sylow's theorems

Sylow theorems are central in the theory of finite groups, as they describe the structure of such groups in terms of their subgroups of prime power order. These theorems are closely related to another fundamental notion of group theory, actions.

4.1. Actions. An *action* of a group G on a non-empty set X is a map $\mu : X \times G \to X$ satisfying the following rules:

$$\mu(\mu(x,g),h) = \mu(x,gh),$$
$$\mu(x,1) = x$$

for all $x \in X$ and $g,h \in G$. We usually suppres μ and write $\mu(x,g)$ as xg. It is clear that the above definition is equivalent to the fact that the map $G \to \operatorname{Sym} X$ given by $g \mapsto (x \mapsto xg)$ is a homomorphism of groups. An action μ is *faithful* if the condition that $\mu(x,g) = \mu(x,h)$ for all $x \in X$ implies $g = h$.

Let G act on X. The relation $\equiv$ defined on X by $x \equiv y \iff \exists g \in G : xg = y$ is an equivalence relation on X. The equivalence class of $x \in X$ is called the *orbit* of x, and is denoted by $\operatorname{orb}_G(x)$. The set of orbits of G on X will be denoted by X/G. The action is said to be *transitive* if it has only one orbit, i.e., $|X/G| = 1$. For $x \in X$, the *stabilizer* of x is

$$\operatorname{stab}_G(x) = \{g \in G \mid xg = x\}.$$

It is easy to see that $\operatorname{stab}_G(x)$ is a subgroup of G.

e:actreg

Example 4.1.1. A group G acts on itself by *right multiplication*, i.e., we have an action $G \times G \to G$ given by $(g,h) \mapsto g \cdot h = gh$. It is not hard to see that this action is transitive and faithful.

```
gap> G := Group((1,2,3),(2,3,4));;
gap> el := Elements( G);;
gap> OnRight(el[2], el[3]) = el[2] * el[3];
true
gap> orbit := Orbit(G, el[7], OnRight);
[ (1,3,2), (), (1,4,2), (1,2,3), (2,3,4), (1,4,3), (1,2)(3,4), (1,3)(2,4),
  (2,4,3), (1,4)(2,3), (1,3,4), (1,2,4) ]
gap> Size( orbit ) = Order( G );
true
```

e:actconj

Example 4.1.2. A group G acts on itself by *conjugation*, i.e., $(g, h) \mapsto g^h$. The orbits of this actions are called *the conjugacy classes* of G. The stabilizer of $g \in G$ is denoted by $C_G(g)$ and called the *centralizer* of g in G.

```
gap> G := DihedralGroup( 8 );;
gap> ConjugacyClasses( G );
[ <identity> of ...^G, f1^G, f2^G, f3^G, f1*f2^G ]
gap> el := Elements( G );;
gap> Centralizer( G, Subgroup( G, [ el[ 5 ] ] ) );
Group([ f1*f2, f3 ])
```

More generally, any subgroup $H \leq G$ acts on G by conjugation. At the other end of scale, if N is a normal subgroup of G, then G, by definition, acts on N by conjugation.

e:actsubg

Example 4.1.3. A subgroup H of a group G acts on the set of all subgroups of G by conjugation; $(K, h) \mapsto K^h$. If $K \leq G$, then the stabilizer of K is under this action is the *normalizer* of K:

$$N_H(K) = \{h \in H \mid K^h = K\}.$$

e:actcosets

Example 4.1.4. Let H be a subgroup of G and $H\backslash G$ the set of all right cosets of H in G. Then G acts on $H\backslash G$ by right multiplication: $(Hx) \cdot g = Hxg$.

```
gap> G := Group((1, 2, 3, 4, 5), (1, 2) );;
gap> H := Subgroup( G, [ (1, 2) ] );;
gap> Index( G, H );
60
gap> act := FactorCosetAction( G, H );
<action epimorphism>
gap> Range( act );
<permutation group of size 120 with 2 generators>
gap> Kernel( act );
Group(())
```

e:actonpoints

Example 4.1.5. Let X be a non-empty set and $G \leq \operatorname{Sym} X$. Then G acts *on points* of X by the rule $(x, g) \mapsto x^g$.

```
gap> G := Group( (1, 2, 3), (2, 3, 4) );;
gap> Orbit(G, 1, OnPoints);
[ 1, 2, 3, 4 ]
```

Let G be a finite group acting on a set X. One can observe that there is a 1-1 correspondence between the elements of $\operatorname{orb}_G(x)$ and the right cosets of $\operatorname{stab}_G(x)$ in G. This implies the following fundamental result:

t:orbitstab

Theorem 4.1.1 (Orbit-stabilizer theorem). *Let G be a finite group acting on a set X. Choose $x \in X$. Then $|\operatorname{orb}_G(x)| \cdot |\operatorname{stab}_G(x)| = |G|$.*

In the special case when G acts on itself by conjugation, we obtain:

c:class

Corollary 4.1.1 (Class equation). *Let G be a finite group and let $x_1, \ldots, x_r$ be the representatives of conjugacy classes of non-central elements of G. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(x_i)|.$$

For $g \in G$ denote by $\operatorname{fix}(g)$ the number of fixed points of g (considered as an element of $\operatorname{Sym} X$). We have:

t:orbitcount

Theorem 4.1.2 (Orbit-counting Lemma). *Let a finite group G act on a set X. Then*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} \operatorname{fix}(g).$$

Proof. We will count the pairs $(x, g) \in X \times G$ with the property that $xg = x$; let us call these pairs good pairs. On one hand, a given $g \in G$ is a member of $\mathrm{fix}(g)$ good pairs, hence the total number of good pairs is $\sum_{g \in G} \mathrm{fix}(g)$. On the other hand, $x \in X$ is a member of $|\operatorname{stab}_G(x)|$ good pairs. The orbit of x thus produces $|\operatorname{orb}_G(x)| \cdot |\operatorname{stab}_G(x)| = |G|$ good pairs, hence there are $|X/G| \cdot |G|$ good pairs in total. We get the result. □

4.2. Sylow theorems. Since the action of G on itself by right multiplication is faithful, we have that the corresponding homomorphism $G \to \operatorname{Sym} G$ is injective. In particular, we have:

t:cayley

Theorem 4.2.1 (Cayley's theorem). *Every finite group is isomorphic to a subgroup of S_n for some positive integer n.*

Another classical result that can be proved using actions is Cauchy's theorem which provides a basis for Sylow theorems. It goes as follows:

t:cauchy

Theorem 4.2.2 (Cauchy's theorem). *Let G be a finite group. If a prime p divides $|G|$, then G contains an element of order p.*

t:sylow

Theorem 4.2.3 (Sylow's theorem). *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.*

This result has numerous consequences for the structure of finite groups, see the problems at the end of this chapter. We mention here that GAP can compute a Sylow p-subgroup of a given group as follows:

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

How many Sylow 2-subgroups of S_4 are there? A consequence of Sylow's theorem is also that if P is a Sylow p-subgroup of G, then $s_p = |G : N_G(P)|$. Thus:

```
gap> Index( G, Normalizer( G, P ) );
3
```

Thus there are three Sylow 2-subgroups of S_4. All of them are conjugate to P:

```
gap> ConjugacyClassSubgroups( G, P );
Group( [ (1,2), (3,4), (1,3)(2,4) ] )^G
gap> Elements( last );
[ Group([ (1,2), (3,4), (1,3)(2,4) ]), Group([ (2,3), (1,4), (1,3)(2,4) ]),
  Group([ (1,3), (2,4), (1,4)(2,3) ]) ]
```

A finite group is said to be a *p-group* if every element has order a power of p. Equivalently, the order of the group is p^n for some n (exercise).

p:pgrpbasic

Proposition 4.2.1. *Let G be a p-group. Then $Z(G)$ is non-trivial, and G contains a normal subgroup of order p.*

Proof. We may assume that G is non-abelian of order p^n. Let $x_1, \dots, x_r$ be the representatives of non-central conjugacy classes of G. By the Class Equation,

$$p^n = |Z(G)| + \sum_{i=1}^{r} |G : C_G(x_i)|.$$

Since $C_G(x_i) \neq G$, the prime p divides $|G : C_G(x_i)|$ for all $i = 1, \dots, r$. It follows that p divides $|Z(G)|$. The rest is now straightforward. □

e:p2 *Example* 4.2.1. There is only one group of order p, namely C_p. Let us show that all groups of order p^2 are abelian (hence there are only two possibilities, $C_p \times C_p$ and C_{p^2}). Suppose there exists a non-abelian group G of order p^2. Then $Z(G) \cong C_p$ and $G/Z(G) \cong C_p$. Let $Z(G)x$ be a generator of $G/Z(G)$. Then $G = Z(G)\langle x\rangle$, but the latter group is abelian, which is a contradiction.

e:pq *Example* 4.2.2. Let us classify all groups of order pq, where p and q are distinct primes (for $p = q$ see Example 4.2.1). Assume that $p > q$. 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:

Suppose $s_q = 1$. Denote $P = \langle a\rangle$ and $Q = \langle b\rangle$. Then $a^b = a^k$ and $b^a = b^\ell$ for some integers k and ℓ. Therefore $a^{k-1} = [a,b] = b^{-\ell+1}$. Since the orders and b are coprime, it follows that $[a,b] = 1$, hence $G \cong C_p \times C_q \cong C_{pq}$.

Now let $s_q = p$, that is, let q divide $p-1$. We still have $a^b = a^k$. By induction, $a^{b^s} = a^{k^s}$. Since $|b| = q$, we conclude that $k^q \equiv 1 \mod p$. There are exactly q solutions to this equation; if k is one of them, the others are powers of k. By replacing b by a power of itself we see that all these solutions give rise to the same group, namely, a group with presentation

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

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

More on finite p-groups will be discussed later on. We conclude with two useful lemmas which are of similar nature:

Lemma 4.2.1 (The Frattini argument). *Let G be a group and H a finite normal subgroup. If P is a Sylow p-subgroup of H, then $G = N_G(P)H$.*

Proof. For $g \in G$ we have $P^g \le H$ and $P^g = P^h$ for some $h \in H$. Thus $gh^{-1} \in N_G(P)$. □

l:norm **Lemma** 4.2.2. *If P is a Sylow p-subgroup of a finite group G and $N_G(P) \leqslant H \leqslant G$, then $H = N_G(H)$.*

Proof. Clearly $P \leqslant H \lhd N_G(H)$. By Frattini's argument we have that $N_G(H) = N_{N_G(H)}(P)H$. But $N_{N_G(H)}(P) \le N_G(P) \le H$, hence the result. □

5. An estimate of the number of finite groups

s:enum

In this short section we derive a rough bound for the number of of groups of order n.

l:nrgen **Lemma** 5.0.3. *A group G of order n can be generated by a set of at most $\log_2 n$ elements.*

Proof. Choose a non-trivial element $g_1 \in G$, and let $G_1 = \langle g_1\rangle$. If $G_1 = G$, then stop. Otherwise choose $g_2 \in G - G_1$ and let $G_2 = \langle g_1, g_2\rangle$. Repeat the procedure until we find $g_1, \dots, g_k \in G$ such that $G = \langle g_1, \dots, g_k\rangle$.

We prove the $|G_i| \ge 2^i$ for all $i = 1, \dots, k$; this suffices to prove our lemma. The proof is by induction on i, the case $i = 1$ being obvious, Suppose that $|G_i| \ge 2^i$. Since $|G_i|$ divides $|G_{i+1}|$ and $G_i \ne G_{i+1}$, we have $|G_{i+1}| \ge 2|G_i| \ge 2^{i+1}$, as required. □

p:basiccount **Proposition** 5.0.2. *The number of groups of order n is at most $n^{n\log_2 n}$.*

Proof. By Cayley's theorem, every group of order n can be embedded as a subgroup of S_n, and can be generated by $k = \lfloor \log_2 n\rfloor$ elements. There are at most $n!$ choices for each g_i, so the number of subgroups of S_n is at most

$$(n!)^k \le (n^n)\log_2 n = n^{n\log_2 n},$$

as required. □

GAP offers a Small Groups library which gives access to all groups of certain "small" orders. The groups are sorted by their orders and they are listed up to isomorphism; that is, for each of the available orders a complete and irredundant list of isomorphism type representatives of groups is given. The library also has an identification function: it returns the library number of a given group. More on this can be found in GAP's manual. Here are some examples.

```
gap> AllSmallGroups( 16 );;
gap> NrSmallGroups( 512 );
10494213
gap> AllSmallGroups(Size, 16, IsAbelian, true);
[ <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 16 with 4 generators>,
  <pc group of size 16 with 4 generators> ]
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 ]
gap> H := SmallGroup( 64, 52 );
<pc group of size 64 with 6 generators>
gap> G = H;
false
gap> StructureDescription( H );
"D64"
```

s:jordhold

6. Jordan-Hölder theorem

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 (exercise). More examples of finite simple groups will be exhibited in Chapter 2.

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

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

such that all the factors G_{i+1}/G_i are simple groups. A related concept is that of *chief series*, where G_i are all normal in G and each G_{i+1}/G_i is a minimal normal subgroup of G/G_i.

The *Correspondence Theorem* says that if N is a normal subgroup of G then there is a bijection between subgroups of G/N and subgroups of G containing N. The bijection is canonical in the sense that all subgroups of G/N are of the form H/N, where H is a subgroup of G containing N. This result enables construction of a composition series of a finite group G as follows. Start with the series $\{1\} \triangleleft G$. If G is simple, we are done. Otherwise there is a proper non-trivial normal subgroup N of G. Now we repeat the procedure with $\{1\} \triangleleft N$ and $N \triangleleft G$. More precisely, if we have $G_i \triangleleft G_{i+1}$ and the corresponding quotient is not simple, then we choose (by the Correspondence Theorem) $N/G_i \triangleleft G_{i+1}/G_i$ with $N \neq G_i$ and $N \neq G_{i+1}$. In this way we refine the series, and since the group is finite, the procedure eventually results in a composition series of G. Given a composition series of G as above, we have r simple groups G_{i+1}/G_i.

t:jordhold

Theorem 6.0.4 (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.*

Proof. The proof is by induction on $|G|$. Let

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

and

$$G = H_0 \triangleright H_1 \triangleright G_2 \triangleright \cdots \triangleright H_s = \{1\}$$

be two composition series of G. If $G_1 = H_1$, then the parts of the series below this term are two composition series of G_1 and by induction they have the same length and composition factors. So assume from here on that $G_1 \neq H_1$. Let $K_2 = G_1 \cap H_1$. Let

$$K_2 \triangleright K_3 \triangleright \cdots \triangleright K_t = \{1\}$$

be a composition series of K_2. The group G_1H_1 is a normal subgroup of G and $G_1 < G$. It follows that $G = G_1H_1$. Therefore $G/G_1 = G_1H_1/G_1 \cong H_1/K_2$, and similarly also $G/H_1 \cong G_1/K_2$. Thus

$$G_1 \triangleright G_2 \triangleright \cdots \triangleright G_r = \{1\}$$

and

$$G_1 \triangleright K_2 \triangleright K_3 \triangleright \cdots \triangleright K_t = \{1\}$$

are two composition series of G_1 and hence they have the same length and same composition factors. A similar statement holds true for H_1, so each of the given series for G has the composition factors of K_2 together with G/G_1 and G/H_1. Therefore the result holds. □

Let us calculate a composition series of D_{32}:

```
gap> G := DihedralGroup( 32 );
<pc group of size 32 with 5 generators>
gap> cs := CompositionSeries( G );
[ Group([ f1, f2, f3, f4, f5 ]), Group([ f2, f3, f4, f5 ]),
  Group([ f3, f4, f5 ]), Group([ f4, f5 ]), Group([ f5 ]), Group([  ]) ]
gap> List( [1..5], i -> StructureDescription( cs[ i ] / cs[ i + 1 ] ) );
[ "C2", "C2", "C2", "C2", "C2" ]
```

The result is not surprising as D_{32} is a 2-group.

6.1. Solvable groups. A finite group is said to be *solvable* if all of its composition factors are cyclic of prime order. One can prove the following:

t:solv **Theorem** 6.1.1. *A finite group G is solvable if it has a series*

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

with all G_i/G_{i+1} abelian.

The statement of Theorem 6.1.1 is usually taken as the definition of solvable groups in the infinite case. Every abelian group is solvable. The smallest non-abelian solvable group is $1 \triangleleft A_3 \triangleleft S_3$. The smallest non-solvable group is A_5. The *derived length* of a solvable group G is the length of the shortest abelian series of G. A group is called *metabelian* if its derived length is no more than two.

l:solv **Lemma** 6.1.1. *The following hold:*

1. *A subgroup of a solvable group is solvable.*
2. *A homomorphic image of a solvable group is solvable.*
3. *If a normal subgroup and its factor are solvable, then the group is solvable.*

l:prodsolv **Lemma** 6.1.2. *A product of two normal solvable subgroups of a group is again solvable.*

Proof. Let $H \triangleleft G$ and $K \triangleleft G$ be solvable. Then $(KH)/K \simeq H/(H \cap K)$ is solvable by (2) above and consequently KH is solvable by (3). □

It follows that every finite group has a unique maximal normal solvable subgroup, i.e. the product S of all solvable normal subgroups, called the *solvable radical* of G.

The following shows that A_5 is the only non-solvable group of order 60:

```
gap> l60 := AllSmallGroups( 60 );;
gap> List( l60, IsSolvable );
[ true, true, true, true, false, true, true, true, true, true, true, true,
  true ]
gap> notsolv := Filtered( l60, G -> not IsSolvable( G ) );
[ Group([ (1,2,3,4,5), (1,2,3) ]) ]
gap> StructureDescription( notsolv[ 1 ] );
"A5"
```

Examples of solvable groups include the following:

t:pqr **Theorem** 6.1.2. *Let p, q, r be primes, Then all groups of orders p^mq^n or pqr are solvable.*

Solvability of groups of order $p^m q^n$ is also refered to as the *Burnside's $p^m q^n$-theorem*. It is proved using character theory.

A celebrated theorem by Feit and Thompson says that *every group of odd order is solvable*. The proof is very long (about 255 pages) and represents a milestone in the classification of finite simple groups as it was a first significant indication that such a classification might be possible. We mention here that the Feit-Thompson theorem was recently reproved using interactive theorem prover `Coq`.

s:cayley

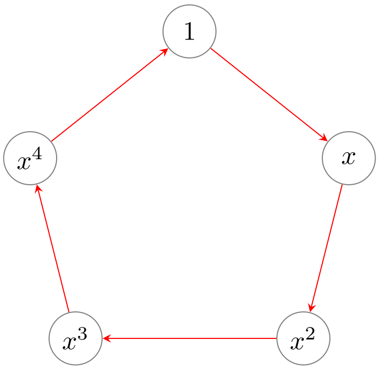
7. How to draw a group?

In this section we assume the reader is familiar with basic terminology of graph theory. Let G be a group generated by a set S. The *Cayley graph* $\Gamma = \mathrm{Cay}(G, S)$ is a colored directed graph given as follows: the vertex set of Γ is identified with G. To each $s \in S$ we assign a color c_s. The vertices g and sg are joined by a directed edge of color c_s for all $g \in G$ and $s \in S$. The set S is usually assumed to be finite, symmetric (i.e., $S = S^{-1}$) and not containing the identity element of the group. In this case, the uncolored Cayley graph is an ordinary graph: its edges are not oriented and it does not contain loops (single-element cycles).

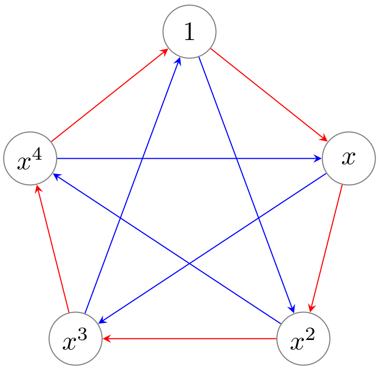
One can modify the above definiton to the case when S is a set of elements of G that does not generate G. We still get a graph, but it may not be connected. From the definition of Cayley graphs it also follows that the Cayley graph of a given group clearly depends on the choice of a generating set S. Here are some examples that illustrate this.

e:cycliccayley

Example 7.0.1. If we take the cyclic group $C_n = \langle x \rangle$ of order n and $S = \{x, x^{-1}\}$, then $\mathrm{Cay}(C_n, S)$ is an undirected cycle $\mathcal{C}_n$ of length n. If we take $S = \{x\}$, then, unless $n = 2$, the corresponding Cayley graph is a directed cycle of length n. In the case $n = 5$ the diagram is as follows:



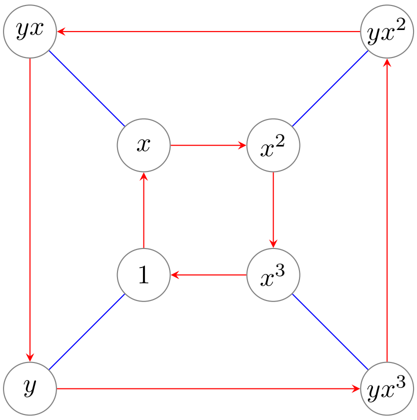
Every red directed edge between x^k and x^{k+1} resembles the fact that $x^{k+1} = x \cdot x^k$. If we take $S = \{x, x^2\}$, the corresponding graph is a directed circulant graph with jumps 1 and 2. Here is the diagram for $n = 5$:



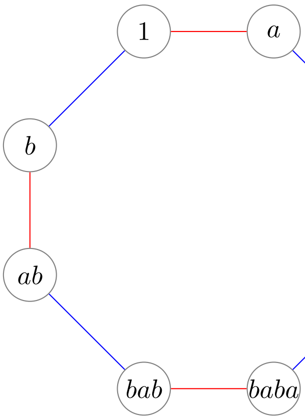
If we take $S = \{x^{\pm 1}, x^{\pm 2}\}$ then we get an undirected circulant graph with jumps 1 and 2. It turns out that undirected circulant graphs are precisely Cayley graphs of cyclcic groups with respect to symmetric generating sets.

e:d8cayley

Example 7.0.2. The dihedral group of order 8 has a presentation $D_8 = \langle x, y \mid x^4 = y^2 = 1, x^y = x^{-1}\rangle$. The Cayley graph $\mathrm{Cay}(D_8, \{x, y\})$ looks as follows:



The red arrows represent multiplication by x from the left, and the blue edges represent multiplication by y; since $y = y^{-1}$, the blue edges are undirected. The dihedral group of order 8 can be also given by the following presentation: $D_8 = \langle a, b \mid a^2 = b^2 = 1, (ab)^2 = (ba)^2\rangle$. In this case, $\mathrm{Cay}(D_8, \{a, b\})$ is as follows:



Cayley graphs can be constructed within GAP using a package called GRAPE. This package has to be loaded into GAP using LoadPackage. After that all the commands of the package are available. One can then construct Cayley graphs $\mathrm{Cay}(G, S)$; the result is a *record* that contain several attributes of the graph; we refer to GAP's manual for further details on records, and GRAPE's manual for further commands. Here we show how to construct a Cayley Graph of A_4 with respect to the generating set $\{(1\,2\,3), (1\,2\,4)\}$, and compute its adjacency matrix.

```
gap> LoadPackage("grape");;
----------------------------------------------------------------------------
Loading  GRAPE 4.6.1 (GRaph Algorithms using PErmutation groups)
by Leonard H. Soicher (http://www.maths.qmul.ac.uk/~leonard/).
Homepage: http://www.maths.qmul.ac.uk/~leonard/grape/
-----------------------------------------------------------------------------
gap> cay := CayleyGraph(AlternatingGroup(4), [(1,2,3),(1,2,4)]);
rec( adjacencies := [ [ 5, 6, 7, 10 ] ], group := Group([ (1,5,7)(2,4,8)
  (3,6,9)(10,11,12), (1,2,3)(4,7,10)(5,9,11)(6,8,12) ]), isGraph := true,
  isSimple := true,
  names := [ (), (2,3,4), (2,4,3), (1,2)(3,4), (1,2,3), (1,2,4), (1,3,2),
      (1,3,4), (1,3)(2,4), (1,4,2), (1,4,3), (1,4)(2,3) ], order := 12,
  representatives := [ 1 ],
  schreierVector := [ -1, 2, 2, 1, 1, 1, 1, 1, 2, 2, 2, 1 ] )
gap> CollapsedAdjacencyMat(cay);
[ [ 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0 ],
[ 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0 ],
[ 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1 ],
[ 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0 ],
[ 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0 ],
[ 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1 ],
[ 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1 ],
[ 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1 ],
[ 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0 ],
[ 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0 ],
[ 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0 ],
[ 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0 ] ]
```

s:problems_basic

Problems

(1) Supply the missing proofs in this chapter.

(2) Let H be a subgroup of a group G with $|G:H|=2$. Prove that H is a normal subgroup of G.

(3) Is it always true that if H is a subgroup of G with prime index, then $H \triangleleft G$?

(4) Let p be the smallest prime that divides the order of a finite group G. If H is a subgroup of G of index p, then H is normal in G.

(5) Find a group G and subgroups H and K with the property that $H \triangleleft K \triangleleft G$, but H is not normal in G.

(6) Let H and K be subgroups of finite index in G. Prove that $|G:H\cap K| \leq |G:H|\cdot|G:K|$, with equality if and only if $G=HK$.

(7) If H is a subgroup of G of finite index, then H contains a subgroup of finite index which is normal in G.

(8) A group in which every non-trivial element has order 2 is abelian.

(9) Let a and b be elements of order 2 of a finite group G. Prove that $\langle a,b\rangle$ is a dihedral group.

(10) Find all subgroups of D_{12}. Which of these are normal subgroups?

(11) Show that $\mathrm{GL}(2,2)\cong S_3$.

(12) What is the largest order of an element of S_{12}?

(13) Give an example of two non-isomorphic groups whose automorphism groups are isomorphic.

(14) If G is a non-cyclic abelian group, then $\operatorname{Aut} G$ is non-abelian.

(15) Let H be a subgroup of G. Show that $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\operatorname{Aut} H$.

(16) Find the center and all conjugacy classes of D_{2n}.

(17) Let P be a Sylow p-subgroup of a finite group G. Prove that if N is a normal subgroup of G, then $P\cap N$ is a Sylow p-subgroup of N, and PN/N is a Sylow p-subgroup of G/N.

(18) Let P be a Sylow p-subgroup of a finite group G and $H\leq G$. Is it true that $P\cap H$ is always a Sylow p-subgroup of H?

(19) Show that a group of order 40 cannot be simple. Do the same for groups of order 84.

(20) Show that A_4 has a presentation $\langle x,y \mid x^2=y^3=(xy)^3=1\rangle$.

(21) Identify the group $\langle x,y,z \mid z^y=z^2, x^z=x^2, y^x=y^2\rangle$.

(22) Find all the composition series of S_4.

CHAPTER 2

Simple groups

ch:simple

Quote from Wikipedia:

> In mathematics, the classification of finite simple groups states that every finite simple group is cyclic, or alternating, or in one of 16 families of groups of Lie type, or one of 26 sporadic groups... These groups can be seen as the basic building blocks of all finite groups, in a way reminiscent of the way the prime numbers are the basic building blocks of the natural numbers. The Jordan–Hölder theorem is a more precise way of stating this fact about finite groups. However, a significant difference with respect to the case of integer factorization is that such "building blocks" do not necessarily determine uniquely a group, since there might be many non-isomorphic groups with the same composition series or, put in another way, the extension problem does not have a unique solution.
>
> The proof of the theorem consists of tens of thousands of pages in several hundred journal articles written by about 100 authors, published mostly between 1955 and 2004. Gorenstein (d.1992), Lyons, and Solomon are gradually publishing a simplified and revised version of the proof.

1. Faithful primitive actions and Iwasawa's Lemma

s:iwasawa

In this section we prove Iwasawa's Lemma which provides a useful criterion for simplicity of a given finite group.

1.1. Transitive actions. Let H be a subgroup of G. Denote by $H\backslash G$ the set of right cosets of H in G (note that, unless H is a normal subgroup, $H\backslash G$ is only a set, not a group in general). The group G acts on $H\backslash G$ by right multiplication. This action is obviously transitive. Our first result shows that this example is, in a sense, generic. Before stating this in a precise form, we need a definition. Let G act on sets X_1 and X_2. An *isomorphism* between these two actions is a bijection $f : X_1 \to X_2$ such that $(xg)^f = (x^f)g$ for all $x \in X_1$ and $g \in G$.

p:trans

Proposition 1.1.1. *Any transitive action of a group G on a set X is isomorphic to the action of G on $H\backslash G$, where $H = \mathrm{stab}_G(x)$ for some $x \in X$. Furthermore, the actions of G on $H\backslash G$ and $K\backslash G$ are isomorphic if and only if H and K are conjugate.*

Proof. Fix $x \in X$ and denote $H = \mathrm{stab}_G(x)$. Since the action is transitive, is straightforward to show there is an obvious bijection between X and the set of subsets $O(x, y) = \{g \in G \mid xg = y\}$ of G. Note that $O(x, y) = Hg$ for any $g \in O(x, y)$. It is now easy that the map $y \mapsto O(x, y)$ is an isomorphism between the action of G on X, and the action of G on $H\backslash G$. The second part is left as an exercise. □

Suppose G acts transitively on a set X with $|X| > 1$. A *G-congruence* on X is an equivalence relation $\equiv$ on X that is compatible with the action, i.e., if $x \equiv y$, then $xg \equiv yg$ for all $g \in G$. An equivalence class of a G-congruence is called a *block*. There are two trivial G-congruences on X, namely, the *equality* $x \equiv y \iff x = y$, and the *universal relation* $x \equiv y$ for all $x, y \in X$. The action is called *imprimitive* if there is a non-trivial G-congruence on X, and *primitive* otherwise.

Examples of primitive actions can be obtained as follows. We say that an action of G on X is *doubly transitive* if for any two ordered pairs (x_1, x_2) and (y_1, y_2) of distinct elements of X there exists $g \in G$ such that $x_1g = y_1$ and $x_2g = y_2$.

p:doubly

Proposition 1.1.2. *A doubly transitive action is primitive.*

We leave the proof as an exercise. The following result provides a useful characterization of blocks:

p:block

Proposition 1.1.3. *Let G act transitively on X and let B be a non-empty subset of X. Then B is a block if and only if, for all $g \in G$, either $Bg = B$ or $Bg \cap B = \emptyset$.*

Proof. If B is a block then Bg is also a block and the claim follows by the fact that different equivalence classes are disjoint.

Conversely, let B be a non-empty subset of X such that, for all $g \in G$, either $Bg = B$ or $Bg \cap B = \emptyset$. Since the action is transitive, all different Bg form a partition of X, which is the set of equivalence classes of a congruence. □

p:cosetprimitive

Proposition 1.1.4. *Let H be a proper subgroup of G. Then the action of G on $H\backslash G$ is primitive if and only if H is a maximal subgroup of G.*

Proof. Suppose that G acts primitively on $H\backslash G$ and assume that $H < K < G$. Let B be the set of all cosets of H which are contained in K. By Proposition 1.1.3, B is a block which neither a singleton nor the whole $H\backslash G$, a contradiction.

Conversely, suppose that G acts imprimitively on $H\backslash G$. Let B be a block containing the coset H, and denote $K = \{g \in G \mid Bg = B\}$. Then $H < K < G$. □

p:prim

Proposition 1.1.5. *Let G act primitively on X, and let N be a normal subgroup of G. Then either N acts trivially on X, or N acts transitively on X.*

Proof. For $x, y \in X$ put $x \equiv y$ iff $xh = y$ for some $h \in N$. For any $g \in G$ we have $(xg)(g^{-1}hg) = yg$. By normality, $g^{-1}hg \in N$. Therefore $xg \equiv yg$, so $\equiv$ is a G-congruence. By primitivity, either all orbits have size 1 (i.e., N is in the kernel of the action), or there is a single orbit (i.e., N acts transitively on X). □

1.2. Minimal and maximal subgroups. The above discussion on actions provides some useful descriptions of minimal and maximal subgroups of finite groups.

l:minimal

Lemma 1.2.1. *A minimal normal subgroup of a finite group is isomorphic to the direct product of a number of copies of a simple group.*

Proof. Let H be a minimal normal subgroup of G. By Lemma 1.0.1, H has no proper non-tivial characteristic subgroups. Choose a minimal normal subgroup N of H of smallest possible order. Consider all subgroups of H of the form $N_1 \times \cdots \times N_n$, where $N_i \lhd H$, $N_i \cong N$. Let M be such group of largest possible order. If we show that $M = H$, then it follows from here that N is simple. For, if K is a normal subgroup of N, then it is a normal subgroup of $M = N_1 \times \cdots \times N_n = G$, and this contradicts the choice of N.

Thus it suffices to show that M is characteristic in H. Take $\phi \in \operatorname{Aut} H$. Then $N_i^\phi \cong N$. A straightforward argument shows that $N_i^\phi \lhd H$. If $N_i^\phi \not\le M$, then $N_i^\phi \cap M \not\le N_i^\phi$ and $|N_i^\phi \cap M| < |N|$. But $N_i^\phi \cap M \lhd H$, so the minimality of $|N|$ shows $N_i^\phi \cap M = \{1\}$. The subgroup $\langle M, N_i^\phi \rangle = M \times N_i^\phi$ is of the same type like M but of larger order, a contradiction. Thus M is characteristic in H. □

c:maxsol

Corollary 1.2.1. *Let G be a finite solvable group. Then any maximal subgroup of G has prime power index.*

Proof. Let H be a maximal subgroup of G and consider the action of G on $H\backslash G$. By Proposition 1.1.4, this action is primitive. The image of this action is a quotient of G, hence it is a solvable group. Therefore we may assume wlog that the action is faithful. Let N be a minimal normal subgroup of G. Then N is an elementary abelian p-group by Lemma 1.2.1. Snce G acts primitively, N acts transitively by Proposition 1.1.5. Using the Orbit-Stabilizer Theorem, $|H\backslash G|$ is a power of p. □

1.3. Faithful actions and Iwasawa's Lemma. From here on we consider only faithful actions. We say that such an action of G on X is *regular* if it is transitive and the point stabilizer is trivial. From the above we see that a regular action of G is isomorphic to the action of G on itself by right multiplication.

Let G act faithfully on X and let N be a normal subgroup of G whose action on X is regular. Then we can identify X with N, so that N acts by right multiplication. To be more precise, choose $x \in X$ and observe there is a bijection between N and X under which $n \in N$ corresponds to $xn \in X$. Under the above bijection, the action of $\operatorname{stab}_G(x)$ on N by conjugation corresponds to the given action on X. To see this, take $g \in \operatorname{stab}_G(x)$ and suppose that $yg = z$. Let $h, k \in N$ correspond to $y, z \in X$ under the above bijection, that is, $xh = y$, $xk = z$. Then $x(g^{-1}hg) = xhg = yg = z$. Since the action is faithful, we conclude that $g^{-1}hg = k$, as required.

t:iwasawa

Theorem 1.3.1 (Iwasawa's Lemma). *Let G be a group with a faithful primitive action on X. Suppose there exists an abelian normal subgroup A of* $\operatorname{stab}_G(x)$ *with the property that the conjugates of A generate G. Then any non-trivial normal subgroup of G contains G'. In particular, if G is perfect, then it is simple.*

Proof. Let N be a non-trivial normal subgroup of G. By Proposition 1.1.5, N acts transitively on X, therefore $N \not\leq \operatorname{stab}_G(x)$. By Proposition 1.1.4, $\operatorname{stab}_G(x)$ is a maximal subgroup of G. Hence $N \operatorname{stab}_G(x) = G$. Take $g \in G$ and write it as $g = nh$, where $n \in N$ and $h \in \operatorname{stab}_G(x)$. Then $gAg^{-1} = nhAh^{-1}n^{-1} = nAn^{-1}$. We conclude that $gAg^{-1} \leq NA$. By our assumption it follows that $G = NA$. Now, $G/N \cong A/(A \cap N)$ is abelian, hence $G' \leq N$. □

s:snan

2. Symmetric groups and alternating groups

Here we examine the normal subgroups of S_n and prove that if $n \geq 5$, then the alternating group A_n is simple.

p:conjclassSn

Proposition 2.0.1. *Two elements of S_n are conjugate if and only if they have the same cycle structure.*

Proof. If $\pi \in S_n$ and $\gamma = (a_1\, a_2\, \dots\, a_k)$ is a cycle, then $\gamma^\pi = (a_1^\pi\, a_2^\pi\, \dots\, a_k^\pi)$.

p:an3cyc

Proposition 2.0.2. *The alternating group A_n is generated by the 3-cycles.*

Proof. Note that 3-cycles are even permutations. If π is any even permutation, then it can be written as a product of an even number of transpositions. Thus we only need to consider products of two transpositions. If $a, b, c, d \in \{1, 2, \dots, n\}$ are pairwise different, then the following clearly hold:

$$\begin{aligned}(a\,b)(a\,b) &= 1,\\ (a\,b)(a\,c) &= (a\,b\,c),\\ (a\,b)(c\,d) &= (a\,b\,c)(a\,d\,c),\end{aligned}$$

and we are done. □

p:conjclassAn

Proposition 2.0.3. *The following are equivalent for $\pi \in A_n$:*

(1) *The S_n conjugacy class of π splits into two A_n-conjugacy classes;*
(2) *There is no odd permutation which commutes with π;*
(3) *π has no cycles of even length, and all of its cycless have distinct lengths.*

Proof. Let us proove that (1) is equivalent to (2). The group S_n acts transitively on A_n by conjugation. We have that $C_{A_n}(\pi) = C_{S_n}(\pi) \cap A_n$. If (2) holds, then $C_{A_n}(\pi) = C_{S_n}(\pi)$, therefore π has $|A_n : C_{A_n}(\pi)| = |S_n : C_{S_n}|/2$ conjugates in A_n. Thus (1) follows. If (2) does not hold then $|C_{A_n}(\pi)| = |C_{S_n}(\pi)|/2$, and π has $|A_n : C_{A_n}(\pi)| = |S_n : C_{S_n}|$ conjugates in A_n. Therefore (1) does not hold.

Now we prove that (2) and (3) are equivalent. If π has a cycle of even length, then this cycle is an odd permutation commuting with π. If π has only cycles of odd length, and two cycles of the same length ℓ, then a permutation interchanging them is a product of ℓ transpositions commuting with π. This proves that (2) implies (3). Assume now that (3) holds. Then any permutation commuting with π fixes each of its cycles and acts on it as a power of the corresponding cycle of π, hence it is an even permutation. □

p:A5 **Proposition** 2.0.4. *The group A_5 is simple.*

Proof. A lazy proof is

```
gap> IsSimple( AlternatingGroup( 5 ) );
true
```

A formal proof goes as follows. The conjugacy classes of A_5 can be determined using Proposition 2.0.3:

- Representative $(*)(*)(*)(*)(*)$: this class has size 1 and does not split into two conjugacy classes of A_5;
- Representative $(*)(**)(**)$: this class has size 15 and does not split into two conjugacy classes of A_5;
- Representative $(*)(*)(***)$: this class has size 20 and does not split into two conjugacy classes of A_5;
- Representative $(*****)$: this class has size 24 and splits into two conjugacy classes of A_5, each of size 12.

A normal subgroup N of A_5 would have to be a union of conjugacy classes and contain the identity, plus its order would have to divide 60. Checking all the possibilities, we see that either N is trivial or $N = A_5$. □

It turns out that A_5 is the only simple group of order 60. A formal proof can be found in [4]. Here is a proof using GAP:

```
gap> Filtered(AllSmallGroups(60), IsSimple);
[ Alt( [ 1 .. 5 ] ) ]
```

t:An **Theorem** 2.0.2. *If $n \geq 5$, then A_n is simple.*

Proof. The proof goes by induction on n. The case $n = 5$ is covered by Proposition 2.0.4. Suppose N is a non-trivial normal subgroup of A_n. Since A_n clearly acts doubly transitively on $X = \{1, 2, \ldots, n\}$, this action is primitive by 1.1.2. Therefore N acts transitively on X by 1.1.5. So N contains a set of coset representatives of A_n/A_{n-1}; therefore $NA_{n-1} = A_n$. The intersection $N \cap A_{n-1}$ is a normal subgroup of A_{n-1}. By assumption, either $N \cap A_{n-1} = \{1\}$ or $A_{n-1} \leq N$. In the latter case, $A_n/N = NA_{n-1}/N \cong A_{n-1}/(A_{n-1} \cap N) = \{1\}$, hence $N = A_n$. So assume that $N \cap A_{n-1} = \{1\}$. In this case N acts regularly and so $|N| = n$ by a discussion above. By Lemma 5.0.3, N can be generated by at most $\lfloor \log_2 n \rfloor$ elements. An automorphism of N is determined by the images of generators, hence $|\operatorname{Aut}(N)| \leq n^{\log_2 n}$. On the other hand, A_{n-1} acts faithfully on N by conjugation, so $(n-1)! \leq n^{\log_2 n}$ which is impossible for $n \geq 6$. □

c:Sn **Corollary** 2.0.1. *Let $n \geq 5$. Then the only normal subgroups of S_n are $\{1\}$, A_n and S_n.*

Proof. Let N be a normal subgroup of S_n. Then $N \cap A_n$ is a normal subgroup of A_n, hence either $A_n \cap N = \{1\}$ or $A_n \leq N$. Suppose the first possibility holds. Then $N = N/(N \cap A_n) \cong NA_n/A_n$. If N is non-trivial then $NA_n = S_n$ and hence $N \cong C_2$. This is impossible as there would have to be a non-identity element of A_n in a conjugacy class of size 1. The remaining possibility is $A_n \leq N$, but in this case we either have $N = A_n$ or $N = S_n$, as A_n is a maximal subgroup of S_n. □

The remaining cases of S_n and A_n for $1 \leq n \leq 4$ are somewhat exceptional, but easy to deal with. We show here how to use GAP to examine these groups:

```
gap> for n in [ 1..4 ] do
>      sn := SymmetricGroup( n );
>      an := AlternatingGroup( n );
>      Print("n = ", n, "\n");
>      Print("A_n: ", StructureDescription( an ), " ", IsSimple( an ), "\n" );
>      Print("S_n: ", StructureDescription( sn ), " ", NormalSubgroups( sn ), "\n" );
>    od;
```

```
n = 1
A_n: 1 false
S_n: 1 [ Group( () ) ]
n = 2
A_n: 1 false
S_n: C2 [ SymmetricGroup( [ 1 .. 2 ] ), Group( () ) ]
n = 3
A_n: C3 true
S_n: S3 [ SymmetricGroup( [ 1 .. 3 ] ), Group( [ (1,2,3) ] ), Group( () ) ]
n = 4
A_n: A4 false
S_n: S4 [ SymmetricGroup( [ 1 .. 4 ] ),
  Group( [ (2,4,3), (1,4)(2,3), (1,3)(2,4) ] ),
  Group( [ (1,4)(2,3), (1,3)(2,4) ] ), Group( () ) ]
```

s:linear

3. Simplicity of projective special linear groups

Unless stated otherwise, F will denote the Galois field $\mathrm{GF}(q)$, where q is a prime power. The *projective space* $\mathbb{P}^{n-1}(F)$ is the set of all one-dimensional subspaces of F^n. There are $q^n - 1$ non-zero vectors in F^n, each of which spans a one-dimensional subspace. Each such space is spanned by any of its $q-1$ non-zero vectors, hence $|\mathbb{P}^{n-1}(F)| = (q^n-1)/(q-1)$. The group $\mathrm{GL}(n,F)$ acts on $\mathbb{P}^{n-1}(F)$ from the left as follows: $(A, \mathrm{span}(v)) \mapsto \mathrm{span}(Av)$.

p:centgl

Proposition 3.0.5. *The following conditions for $A \in \mathrm{GL}(n,F)$ are equivalent:*

(1) *$A \in Z(\mathrm{GL}(n,F))$;*
(2) *A is in the kernel of the action of $\mathrm{GL}(n,F)$ on $\mathbb{P}^{n-1}(F)$;*
(3) *A is a scalar matrix, i.e., $A = \lambda I$ for some $\lambda \in F^\times$.*

Proof. Clearly (3) implies (1). To see that the converse holds, take $A \in Z(\mathrm{GL}_n(F))$. Then, in particular, A has to commute with all matrices with 1 on the diagonal and the position (i,j), $i \neq j$, and zero elsewhere. Easy calculation then shows that A is a scalar matrix.

Let us prove that (2) and (3) are equivalent. Clearly every scalar matrix fixes all 1-dimensional subspaces of F^n. Conversely suppose that A fixes all 1-dimensional subspaces. Let $e_1, \ldots, e_n$ be a standard basis of F^n. Then $Ae_i = \lambda_i e_i$ for some non-zero $\lambda_i \in F$. Fix different i and j. There also exists $\lambda \in F^\times$ such that $A(e_i + e_j) = \lambda(e_i + e_j)$, and this implies $\lambda = \lambda_j = \lambda_i$. Consequently, A is a scalar matrix. □

We define the *projective general and projective special linear groups* by

$$\mathrm{PGL}(n,F) = \mathrm{GL}(n,F)/Z(\mathrm{GL}(n,F))$$

and

$$\mathrm{PSL}(n,F) = \mathrm{SL}(n,F)/(Z(\mathrm{GL}(n,F)) \cap \mathrm{SL}(n,F)).$$

Therefore the projective groups are the images of ther linear group counterparts in the action on the projective space, so we can think of them as subgroups of $\mathrm{Sym}\,\mathbb{P}^{n-1}(F)$. We see that $|\mathrm{PGL}(n,q)| = |\mathrm{GL}(n,q)|/(q-1) = |\mathrm{SL}(n,q)|$.

p:pslorder

Proposition 3.0.6. $|\mathrm{PSL}(n,q)| = |\mathrm{SL}(n,q)|/\gcd(n,q-1)$.

Proof. The kernel of the action of $\mathrm{SL}(n,q)$ on the corresponding projective space consists of scalar matrices with determinant one, i.e., matrices of the form λI with $\lambda^n = 1$. The multiplicative group of $\mathrm{GF}(q)$ is cyclic of order $q-1$, so the number of solution of $\lambda^n = 1$ is $\gcd(n, q-1)$. □

If we restrict to the case $n = 2$, we see that $\mathbb{P}^1(F)$ has $q+1$ points, so $\mathrm{PGL}(2,q)$ and $\mathrm{PSL}(2,q)$ are subgroups of S_{q+1}. Let us consider some small cases:

$q = 2$: $\mathrm{PSL}(2,2) = \mathrm{PGL}(2,2)$ is a subgroup of S_3 of order 6, hence $PSL(2,2) \cong S_3$.

$q = 3$: $\mathrm{PGL}(2,3)$ is a subgroup of S_4 of order 24, hence $\mathrm{PGL}(2,3) = S_4$. The group $\mathrm{PSL}(2,3)$ is a subgroup of index 2 in $\mathrm{PGL}(2,3)$, hence $\mathrm{PSL}(2,3) \cong A_4$.

$q = 4$: $\mathrm{PGL}(2,4) = \mathrm{PSL}(2,4)$ is a subgroup of S_5 of order 60, so it is isomorphic to A_5; one can double-check this with GAP:

```
gap> StructureDescription(PSL(2,4));
"A5"
```

$q = 5$: $\mathrm{PSL}(2,5) \cong A_5$:

```
gap> StructureDescription(PSL(2,5));
"A5"
```

We also remark here that there is another way of interpreting the actions of $\mathrm{PGL}(2,F)$ and $\mathrm{PSL}(2,F)$ on the projective line. The one-dimensional subspaces of F^2 can be spanned by either a unique vector of the form $(1,x)$, where $x \in F$, or the vector $(0,1)$. We identify points of the first type with F, and the point of the second type with ∞. Then the elements of $\mathrm{PGL}(2,F)$ can be identified with *linear fractional maps*

$$z \mapsto \frac{az+b}{cz+d},$$

where $a,b,c,d \in F$, $ad-bc \neq 0$. The group $\mathrm{PSL}(2,F)$ then consists of those linear fractional maps with $ad-bc=1$.

We will prove the following result:

t:psl

Theorem 3.0.3. *For $n \geq 2$ and any field F, the group $\mathrm{PSL}(n,F)$ is simple, except in the two cases, $n=2$, $F=\mathrm{GF}(2)$ or $n=2$, $F=\mathrm{GF}(3)$.*

We will only prove this theorem for $n=2$, the proof for $n>2$ is similar, but somewhat technical. Our proof will rely on Iwasawa's lemma applied to the action of $G=\mathrm{SL}(2,F)$ on $\mathbb{P}^1(F)$. We will show in a series of steps that all the conditions of the lemma are satisfied.

p:psldoubl

Proposition 3.0.7. *If $n \geq 2$, then $\mathrm{SL}(2,F)$ acts doubly transitively on $\mathbb{P}^1(F)$.*

Proof. Let $\mathrm{span}(v_1)$ and $\mathrm{span}(v_2)$ be two distinct 1-dimensional subspaces of F^2. For any other pair $\mathrm{span}(w_1)$ and $\mathrm{span}(w_2)$ there exists a linear map that maps $v_i \mapsto w_i$, $i=1,2$. One can modify this map to obtain one with determinant 1. We let the reader fill in the details. □

Let e_1, e_2 be a standard basis of F^2. Denote $x = \mathrm{span}(e_1)$. The stabilizer of x is

$$\begin{aligned} \mathrm{stab}_G(x) &= \{A \in \mathrm{SL}(2,F) \mid \mathrm{span}(e_1) = \mathrm{span}(Ae_1)\} \\ &= \left\{ \begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix} \mid a \in F^\times, b \in F \right\}. \end{aligned}$$

There is an abelian normal subgroup of $\mathrm{stab}_G(x)$ given as follows:

$$U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in F \right\}.$$

Its elements are called *transvections.*

p:transv

Proposition 3.0.8. *The subgroup U and its conjugates generate $\mathrm{SL}_2(F)$.*

Proof. First we note that

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} U \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 0 \\ b & 0 \end{pmatrix} \mid b \in F \right\} = U'.$$

Now pick $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(F)$. Suppose first that $b \neq 0$. Then

$$A = \begin{pmatrix} 1 & 0 \\ (d-1)/b & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ (a-1)/b & 1 \end{pmatrix} \in \langle U, U' \rangle.$$

If $c \neq 0$, then

$$A = \begin{pmatrix} 1 & (a-1)/c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & (d-1)/c \\ 0 & 1 \end{pmatrix} \in \langle U, U' \rangle.$$

Finally assume that $b = c = 0$. Then

$$A = \begin{pmatrix} 1 & 0 \\ (1-a)/a & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ (a-1) & 1 \end{pmatrix} \begin{pmatrix} 1 & -1/a \\ 0 & 1 \end{pmatrix} \in \langle U, U' \rangle.$$

This proves the result. □

p:sl2perfect

Proposition 3.0.9. *If $|F| > 3$, then $\mathrm{SL}(2,F)$ is a perfect group.*

Proof. If $|F| > 3$ there exists $a \in F$ such that $a^2 \notin \{0,1\}$. Now we observe

$$\begin{pmatrix} 1 & b(a^2-1) \\ 0 & 1 \end{pmatrix} = \left[\begin{pmatrix} 1/a & 0 \\ 0 & a \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -b & 1 \end{pmatrix} \right].$$

Letting b run through F, we see that $U \leq \mathrm{SL}_2(F)'$. By Proposition 3.0.8 we conclude the result. □

Proof of Theorem 3.0.3 for $n = 2$. This follows by previous propositions and Iwasawa's lemma. □

s:cfsg

4. On the classification of finite simple groups (CFSG)

One of the greatest achievements of mathematics is a full classificiation of finite simple groups (CFSG) which was announced in the 1980's. Roughly speaking, the result says that all finite simple groups fall into one of the following four types:

(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

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000$$

and is called the *Monster Group*.

Since a thorough account on these groups is beyond the purpose of these notes, we only exhibit some properties and how to use GAP. The following are all non-abelian finite simple groups of order ≤ 1000000:

```
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) ]
```

Here is a construction of Mathieu groups M_{11} and M_{12} which are sporadic groups:

```
gap> p1 := (4,5,6)*(7,8,9)*(10,11,12);;
gap> p2 := (4,7,10)*(5,8,11)*(6,9,12);;
gap> p3 := (5,7,6,10)*(8,9,12,11);;
gap> p4 := (5,8,6,12)*(7,11,10,9);;
gap> p5 := (1,4)*(7,8)*(9,11)*(10,12);;
gap> p6 := (1,2)*(7,10)*(8,11)*(9,12);;
gap> p7 := (2,3)*(7,12)*(8,10)*(9,11);;
gap> m11 := Group(p1, p2, p3, p4, p5, p6);;
gap> IsSimple(m11);
true
gap> StructureDescription(m11);
"M11"
gap> m12 := Group(p1, p2, p3, p4, p5, p6,p7);;
gap> IsSimple(m12);
true
gap> StructureDescription(m12);
"M12"
```

There is a vast amount of properties of finite simple groups that follow from CFSG, too many to state here. Some of them are:

t:cfsg

Theorem 4.0.4. *Let S be a finite non-abelian simple group.*

(1) *S can be generated by two elements.*
(2) $\mathrm{Out}(S)$ *is a solvable group (used to be Schreier's conjecture).*
(3) *Every element of S is a commutator (used to be Ore's conjecture).*

CFSG also implies, that, given a positive integer n, there are at most two non-isomorphic finite simple groups of order n. It may happen that there are two non-isomorphic finite simple groups of the same order. For example, consider $\mathrm{PSL}(3,4)$ and $\mathrm{PSL}(4,2)$; they are both of order 20160, and

```
gap> G:=PSL(4,2);;
gap> H:=PSL(3,4);;
gap> IsomorphismGroups(G,H);
fail
```

Apart from using GAP, several useful information on finite simple groups can be obtained from *Atlas of Finite Group Representations* [1].

s:problems_simple

Problems

(1) Complete the proof of Proposition 1.1.1.
(2) Prove Proposition 1.1.2.
(3) Let G act transitively on X. Suppose that the stabilizer of $x \in X$ acts transitively on $X - \{x\}$. Then G acts doubly transitively on X.
(4) Let Ω be the set of 2-element subsets of $\{1, 2, \dots, n\}$. Then S_n acts on Ω by $\{i, j\}g = \{ig, jg\}$.
  (a) If $n = 2$, then the action is not faithful.
  (b) If $n = 3$, then the action is doubly transitive.
  (c) If $n = 4$, then the action is imprimitive.
  (d) If $n \geq 5$, then the action is primitive, but not doubly transitive.
(5) Let G be a group. The group $\mathrm{Aut}\, G$ acts naturally on the set G.
  (a) If $G - \{1\}$ is an orbit, prove that G is an elementary abelian p-group.
  (b) If $\mathrm{Aut}\, G$ acts doubly transitively on $G - \{1\}$, show that either G is a 2-group or $|G| = 3$.
(6) Let G be a group of order $2m$, where m is odd and $m > 1$. Prove that G is not simple.
(7) Let $n \geq 2$. Show that the transpositions $(1\,2)$, $(1\,3)$, ..., $(1\,n)$ generate S_n.
(8) Let $n \geq 3$. Show that the 3-cycles $(1\,2\,3)$, $(1\,2\,4)$, ..., $(1\,2\,n)$ generate A_n.
(9) Prove that there are no simple groups of order 312, 616, or 1960.
(10) Show that the only simple group of order 60 is A_5.
(11) Prove that $\mathrm{PSL}(4,2) \cong A_8$.
(12) Prove by hand that $\mathrm{PSL}(3,4)$ has no elements of order 15, so it is not isomorphic to A_8.
(13) Show that transvections in $\mathrm{SL}(2,F)$ need not be conjugate.

CHAPTER 3

Some extension theory

ch:extensions

Let N be a normal subgroup of G. Then we say that G is an extension of N by G/N. A precise definition of group extensions will be given in Section 1. The importance of extension theory can be outlined as follows. Let G be a finite group and $1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_r = G$ its composition series. By Jordan-Hölder theorem, the composition factors G_{i+1}/G_i are in a sense uniquely determined by G. On the other hand, these are simple groups, so they are known by CFSG. In order to build all finite groups with a given sequennce of composition factors, one can proceed as follows. Suppose we already know what G_i is, and we have a prescribed isomorphism type of the simple group G_{i+1}/G_i. If we knew how to build all the extensions (up to certain equivalence) of a given group by a (simple) group, then we would be able to construct all possible G_{i+1}. Proceeding this way, we would eventually be able to construct all finite groups. The trouble is that the problem of constructing all possible extensions is very difficult and still open.

We will briefly tackle the problem of classifying extensions of abelian groups. It will be shown that these are, up to equivalence, in 1-1 correspondence with the elements of a certain second cohomology group. Cohomological group theory is an area on its own, and we will not go deeply into it. We refer to [3] and [8] for further details.

s:basicext

1. Basic notions

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

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\mu"] & E \arrow[r, "\epsilon"] & G \arrow[r] & 1. \end{tikzcd}$$

From the above it clearly follows that μ is injective, ϵ is surjective, $M = \operatorname{im}\mu = \ker\epsilon$ is a normal subgroup of E, $M \cong N$, and $E/M \cong G$.

A *morphism* between extensions $N \overset{\mu}{\rightarrowtail} E \overset{\epsilon}{\twoheadrightarrow} G \longrightarrow 1$ and $\bar{N} \overset{\bar{\mu}}{\rightarrowtail} \bar{E} \overset{\bar{\epsilon}}{\twoheadrightarrow} \bar{G}$ is a triple of group homomorphisms (α, β, γ) such that the following diagram commutes:

$$\begin{tikzcd} N \arrow[r, tail, "\mu"] \arrow[d, "\alpha"] & E \arrow[r, two heads, "\epsilon"] \arrow[d, "\beta"] & G \arrow[d, "\gamma"] \\ \bar{N} \arrow[r, tail, "\bar{\mu}"] & \bar{E} \arrow[r, two heads, "\bar{\epsilon}"] & \bar{G} \end{tikzcd} .$$

The collection of all group extensions and morphisms between them is a category. A morphism of the type

$$\begin{tikzcd} N \arrow[r, tail, "\mu"] \arrow[d, "1"] & E \arrow[r, two heads, "\epsilon"] \arrow[d, "\beta"] & G \arrow[d, "1"] \\ N \arrow[r, tail, "\bar{\mu}"] & \bar{E} \arrow[r, two heads, "\bar{\epsilon}"] & G \end{tikzcd}$$

is said to be an *equivalence* of extensions.

s:semidirect

2. Semidirect products

Suppose that H and N are groups and that we have a homomorphism $\alpha : H \to \operatorname{Aut}(N)$. 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 $(h^{-1}, n^{-(h^\alpha)^{-1}})$.

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.*

GAP offers two ways of constructing semidirect products. The first one is directly via command SemidirectProduct(H, alpha, N). In the special case when $N = \mathrm{GF}(q)^n$, alpha must be a homomorphism from H into a matrix group of $n \times n$ matrices over a subfield of $\mathrm{GF}(q)$, or into a permutation group. The second option is to use SemidirectProduct(H, N), where $H \leq \mathrm{Aut}(N)$.

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"
```

Here are two more examples:

```
gap> SemidirectProduct(Group((1,2,3),(2,3,4)),GF(5)^4);
<matrix group of size 7500 with 3 generators>
gap> g:=Group((3,4,5),(1,2,3));;
gap> mats:=[[[Z(2^2),0*Z(2)],[0*Z(2),Z(2^2)^2]],
>          [[Z(2)^0,Z(2)^0], [Z(2)^0,0*Z(2)]]];;
gap> hom:=GroupHomomorphismByImages(g,Group(mats),[g.1,g.2],mats);;
gap> SemidirectProduct(g,hom,GF(4)^2);
<matrix group of size 960 with 3 generators>
```

An important example of a semidirect product is the following. Let N be any group and $H = \mathrm{Aut}(N)$. Let $\alpha : H \to \mathrm{Aut}(N)$ be the identity mapping. Then the semidirect product $\mathrm{Aut}(N) \ltimes_\alpha N$ is called the *holomorph* of N.

e:agl *Example* 2.0.1. Let $N = C_p^n$ be an elementary abelian p-group of order p^n. Its automorphism group is $\mathrm{GL}(n, p)$. The holomorph $\mathrm{AGL}(n, p) = \mathrm{GL}(n, p) \ltimes C_p^n$ is called the *affine group* of dimension n over $\mathbb{Z}_p$. Show that $\mathrm{AGL}(2, 2) \cong S_4$. Here is a proof using GAP:

```
gap> G := AbelianGroup([2,2]);;
gap> agl := SemidirectProduct(AutomorphismGroup(G), G);;
gap> StructureDescription(agl);
"S4"
```

Another construction related to semidirect products is that of a *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

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

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.

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.* Here is an example of how to build $C_2 \wr C_4$ with GAP:

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

Alternatively, we can build $C_2 \wr C_4$ as a semidirect product $C_4 \ltimes C_2^4$, where we 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 ]
```

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

t:kaluznin **Theorem** 2.0.5. *Every extension of G by H is isomorphic to a subgroup of $G \wr H$.*

We leave the proof as an exercise.

s:extab 3. Extensions with abelian kernels

Consider

$$\begin{tikzcd} A \arrow[r, tail, "\mu"] & E \arrow[r, two heads, "\epsilon"] & G \end{tikzcd},$$

where A is an abelian group (written additively). When choosing a transversal $\mathcal{T}$ to $M = \mathrm{im}\,\mu = \ker\epsilon$ in E, we get a function $\tau : G \to E$ defined by $g^\tau = x$, where $x \in \mathcal{T}$ is such that $g = x^\epsilon$ (note that this is well defined). 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 $\{g^\tau \mid g \in G\}$.

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 $\chi : G \to \mathrm{Aut}(A)$. We prove that χ does not depend on the choice of τ. Here we will use the fact that A is abelian. Suppose that τ' is another transversal function. Then $(g^\tau (g^{\tau'})^{-1})^\epsilon = g^{\tau\epsilon}(g^{\tau'\epsilon})^{-1} = 1$, hence $g^{\tau'} = g^\tau m_g$ for some $m_g \in M$. If τ' induces $\chi' : G \to \mathrm{Aut}(A)$ as above, then

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

hence $g^\chi = g^{\chi'}$. Thus χ is uniquely defined. We claim that χ is a homomorphism. Let $g_1, g_2 \in G$. Then $(g_1 g_2)^\tau \equiv g_1^\tau g_2^\tau \mod M$. Thus $(g_1 g_2)^\chi = g_1^\chi g_2^\chi$, hence χ is a homomorphism. We have proved:

BB0 **Proposition** 3.0.10. *Each extension $\begin{tikzcd} A \arrow[r, tail, "\mu"] & E \arrow[r, two heads, "\epsilon"] & G \end{tikzcd}$, where A is abelian, determines a unique homomorphism $\chi : G \to \mathrm{Aut}(A)$ which arises by conjugation in $\mathrm{im}\,\mu$ by elements of E.*

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.* More precisely, let $g \in G$ and $x \in E$ such that $x^\epsilon = g$. Then

$$(ag)^\mu = x^{-1} a^\mu x$$

for $a \in A$ (well defined, since A is abelian). Note that this action is trivial precisely when $\operatorname{im}\mu$ is central in E, i.e., when the corresponding extension is a *central extension.*

BB1 **Theorem** 3.0.6. *Equivalent extensions of A by G, where A is abelian, induce the same G-module structure on A.*

Proof. Suppose we have equivalent extensions

$$\begin{tikzcd}
A \arrow[r, tail, "\mu"] \arrow[d, "1"] & E \arrow[r, two heads, "\epsilon"] \arrow[d, "\beta"] & G \arrow[d, "1"] \\
A \arrow[r, tail, "\bar{\mu}"] & \bar{E} \arrow[r, two heads, "\bar{\epsilon}"] & G
\end{tikzcd}$$

Let χ and $\bar{\chi}$ be the respective homomorphisms $G \to \operatorname{Aut}(A)$. Choose a transversal function $\tau : G \to E$. Let $\bar{\tau} = \tau\beta$. Then $\bar{\tau}\bar{\epsilon} = \tau\beta\bar{\epsilon} = \tau\epsilon = 1_G$, hence $\bar{\tau}$ is a transversal function for the second extension. Then $(a^{g^\chi})^\mu = (g^\tau)^{-1}a^\mu(g^\tau)$ and $(a^{g^{\bar{\chi}}})^{\bar{\mu}} = (g^{\bar{\tau}})^{-1}a^{\bar{\mu}}(g^{\bar{\tau}})$ for $a \in A$ and $g \in G$. Applying β to the first equation and using the fact that $\mu\beta = \bar{\mu}$, we get $(a^{g^\chi})^{\bar{\mu}} = (g^{\tau\beta})^{-1}a^{\mu\beta}(g^{\tau\beta}) = (a^{g^{\bar{\chi}}})^{\bar{\mu}}$ and thus $g^\chi = g^{\bar{\chi}}$. □

Choose a transversal function $\tau : G \to E$, i.e., $\tau\epsilon = 1_G$. Then the above action can be rewritten as

$$(ag)^\mu = g^{-\tau}a^\mu g^\tau.$$

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*). Note that we can assume without loss of generality that $1^\tau = 1$, therefore we can always assume that $(1,x)\phi = (x,1)\phi = 0$ for all $x \in G$. 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

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

e:zerococycle *Example* 3.0.2. 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 $(x)\psi \in A$. We get

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

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:

DD1 **Proposition** 3.0.11. *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 with identity element $(1, -(1, 1)\phi)$ and inversion rule $(x, a)^{-1} = (x^{-1}, -ax^{-1} - (1, 1)\phi - (x, x^{-1})\phi)$. 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

$$\begin{tikzcd} A \arrow[r, tail, "\mu"] & E(\phi) \arrow[r, two heads, "\epsilon"] & G . \end{tikzcd}$$

DD2 **Proposition** 3.0.12. *Let A be a G-module and $\phi : G \times G \to A$ a factor set. Then the extension*

$$\begin{tikzcd} A \arrow[r, tail, "\mu"] & E(\phi) \arrow[r, two heads, "\epsilon"] & G \end{tikzcd}$$

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.

Proof. Let $g \in G$, $a \in A$. Note that $(g, 0)^{\epsilon} = g$. By definition, the G-module structure induced by the extension is given by $(a \circ g)^{\mu} = (g, 0)^{-1}a^{\mu}(g, 0) = (1, ag - (1, 1)\phi) = (ag)^{\mu}$, which gives the first part. For the second part, define $\tau : G \to E(\phi)$ by $g^{\tau} = (g, 0)$. This is a transversal function and $x^{\tau}y^{\tau} = (xy)^{\tau}((x, y)\phi)^{\mu}$. □

By looking at factor sets, how can we determine which extensions are equivalent? Let A be a fixed G-module and let

$$\begin{tikzcd} A \arrow[r, tail, "\mu_i"] & E_i \arrow[r, two heads, "\epsilon_i"] & G , \end{tikzcd} \qquad i = 1, 2$$

be two extensions realizing this module structure. Choose transversal functions τ_i and let ϕ_i be the resulting factor sets.

First suppose these extensions are equivalent:

$$\begin{tikzcd} A \arrow[r, tail, "\mu_1"] \arrow[d, "1"] & E_1 \arrow[r, two heads, "\epsilon_1"] \arrow[d, "\theta"] & G \arrow[d, "1"] \\ A \arrow[r, tail, "\mu_2"] & E_2 \arrow[r, two heads, "\epsilon_2"] & G \end{tikzcd}$$

Then $\bar{\tau}_2 = \tau_1\theta$ is a transversal for the second extension. Applying θ to $x^{\tau_1}y^{\tau_1} = (xy)^{\tau_1}((x, y)\phi_1)^{\mu_1}$, we get $x^{\bar{\tau}_2}y^{\bar{\tau}_2} = (xy)^{\bar{\tau}_2}((x, y)\phi_1)^{\mu_2}$, hence $\bar{\tau}_2$ determines the factor set ϕ_1 for the second extension. As the factor sets of τ_2 and $\bar{\tau}_2$ belong to the same coset of $B^2(G, A)$, we get

$$\phi_1 + B^2(G, A) = \phi_2 + B^2(G, A).$$

Conversely, assume that $\phi_1 + B^2(G, A) = \phi_2 + B^2(G, A)$. Write $\phi_1 = \phi_2 + \psi^*$ for some $\psi : G \to A$ as above. Define $\theta : E_1 \to E_2$ by the rule $(x^{\tau_1}a^{\mu_1})^{\theta} = x^{\tau_2}(a + (x)\psi)^{\mu_2}$ for $x \in G$ and $a \in A$. θ is a well defined homomorphism, $\mu_1\theta = \mu_2$ and $\epsilon_1 = \theta\epsilon_2$. Hence we have a commutative diagram

$$\begin{tikzcd} A \arrow[r, tail, "\mu_1"] \arrow[d, "1"] & E_1 \arrow[r, two heads, "\epsilon_1"] \arrow[d, "\theta"] & G \arrow[d, "1"] \\ A \arrow[r, tail, "\mu_2"] & E_2 \arrow[r, two heads, "\epsilon_2"] & G \end{tikzcd}$$

and θ must be an isomorphism.

DD3 **Theorem** 3.0.7. *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 $B^2(G, A)$.*

Let A be a G-module. We define $H^2(G,A) = Z^2(G,A)/B^2(G,A)$ to be the *second cohomology group* of G with coefficients in A. The elements of $H^2(G,A)$ thus correspond to equivalence classes of extensions of A by G. Unfortunately, different elements of $H^2(G,A)$ can still produce extensions of A by G that are isomorphic as groups.

ex:cpcp

Example 3.0.3. Consider $\mathbb{Z}_p$ as a trivial C_p-module. From Example 4.2.1 it follows that there are only two non-isomorphic extensions of $A = \mathbb{Z}_p$ by $G = C_p$, namely $C_p \times C_p$ and C_{p^2}. On the other hand, one can show that $H^2(C_p, \mathbb{Z}_p) \cong C_p$.

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; we refer to GAP's manual for further information. The action of G on A can be represented by matrices over GF(p). It is a requirement that the matrices that define the module must correspond to the pcgs of the group G. 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 GF(p).

As another example we build all the extensions of $A = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ by $G = D_8$, where we consider $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ as a trivial D_8-module. Along the way we show commands for computing 2-cocycles, extensions corresponding to given 2-cocycles, and split extensions. The way we build the action is as follows. To each element of Pcgs(G) we assign 2×2 identity matrix over GF(2). Then we build the module using the command GModuleByMats. The other commands we use are self-evident:

```
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 ] ]
```

Here note that the notation C4 : C4 means that the group in question is a semidirect product of C_4 by C_4. The command TwoCocycles(G, A) returns a list of vectors over the field underlying A, and the additive group *generated* by these vectors is the $Z^2(G,A)$. There is also a command TwoCohomology(G, A) that returns a record defining the second cohomology group as factor space of the vector space of cocycles by the subspace of coboundaries. We refer to GAP's manual for further details.

```
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 $H^2(G,A) \cong C_2^6$.

s:schur

4. The Schur-Zassenhaus theorem

Let A and G be groups. We say that an extension of A by G *splits* if it is a semidirect product.

t:schur

Theorem 4.0.8. *Suppose that A and G are finite groups satisfying $\gcd(|A|,|G|) = 1$. Then every extension of A by G splits.*

We will only prove this result in the case when A is abelian. In this form, the result was originally due to Schur. Zassenhaus improved it by showing that it suffices to assume that one of A or G is solvable. On the other hand, Feit-Thompson's Odd Order Theorem shows that this assumption is redundant.

Proof of Theorem 4.0.8 when A is abelian. Let $m = |A|$ and $n = |G|$. Let $\phi : G \times G \to A$ be a 2-cocycle representing an extension of A by G, and let $\chi : G \to \mathrm{Aut}(A)$ be the homomorphism that induces the corresponding G-module structure on A. We claim that $n\phi \in B^2(G,A)$. Define a function $d : G \to A$ by

$$(g)d = \sum_{g_1 \in G} (g_1, g)\phi.$$

Consider the cocycle identity:

$$(g_1, g_2g_3)\phi + (g_2, g_3)\phi = (g_1g_2, g_3)\phi + (g_1, g_2)\phi \cdot g_3.$$

Sum this equation over $g_1 \in G$:

$$\begin{aligned}(g_2g_3)d + n(g_2,g_3)\phi &= (g_2)d \cdot g_3 + \sum_{g_1 \in G} (g_1g_2, g_3)\phi \\ &= (g_2)d \cdot g_3 + \sum_{g_1g_2 \in G} (g_1g_2, g_3)\phi \\ &= (g_2)d \cdot g_3 + (g_3)d.\end{aligned}$$

Therefore $n(g_2, g_3)\phi = (g_2)d \cdot g_3 + (g_3)d - (g_2g_3)d$, which proves our claim. Now, there exist integers a and b with $am + bn = 1$. Since $|A| = m$, it follows that $m\phi = 0$. Therefore $\phi = (am + bn)\phi = bn\phi \in B^2(G,A)$. Thus every extension of A by G splits. □

problems_extension

Problems

(1) Let G_1, G_2 and G_3 be groups. Show that $(G_1 \wr G_2) \wr G_3$ may not be isomorphic to $G_1 \wr (G_2 \wr G_3)$.

(2) Find a proof of Theorem 2.0.5.

(3) Prove that a Sylow p-subgroup of S_{p^n} is isomorphic to $W(p,n) = (\cdots(C_p \wr Cp) \wr \cdots) \wr C_p$, the number of factors being n.

(4) Prove that every group of order p^n is isomorphic to a subgroup of $W(p,n)$.

(5) Let $1 \longrightarrow A \xrightarrow{\mu} E \xrightarrow{\epsilon} G \longrightarrow 1$ be a group extension, where A is abelian and $G = \langle g \rangle$ cyclic of order n. Choose $x \in E$ with $x^\epsilon = q$, and let $a = x^n$. Define a transversal function $\tau : G \to E$ by $(g^i)^\tau = x^i$ for $0 \le i < n$. Prove that the corresponding factor set $\phi : G \times G \to A$ is given by

$$(g^i, g^j)\phi = \left\{ \begin{array}{lcl} 0 & : & i + j < n \\ a & : & i + j \ge n \end{array} \right. .$$

(6) Find all equivalence classes of extensions of C_4 by C_2 by hand. Which groups arise this way?

(7) Find all equivalence classes of extensions of D_8 by C_2 by hand. Which groups arise this way?

(8) Fill in the details in Example 3.0.3.

(9) Let N be a normal subgroup of a finite group G, and assume that $|N| = n$ and $|G : N| = m$ are relatively prime. Let m_1 be a divisor of m. Then a subgroup of G of order m_1 is contained in a subgroup of order m.

CHAPTER 4

Nilpotent groups and p-groups

ch:nilpotent

Nilpotent groups are groups which can be constructed from abelian groups by repeatedly forming central extensions. We exhibit some of the classical theory of these groups, and show that they are closely related to finite p-groups. These form a very rich class of groups. We prove that there are lots of finite p-groups, hence there is little hope to classify them up to isomorphism.

s:nil

1. Nilpotent groups

1.1. Definition and basic properties. 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. 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.

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

Here is an example of how to manipulate nilpotent groups in GAP:

```
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[2]);
1
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" ]
```

From the above example we observe that all nilpotent groups of order 54 can be written as direct products of their Sylow p-subgroups. We will show later on that this property characterizes finite nilpotent groups. We now exhibit a large class of nilpotent groups:

l:pgroupsnil

Lemma 1.1.1. *All finite p-groups are nilpotent.*

Proof. We know that $Z(G)$ is nontrivial by Proposition 4.2.1. 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. □

The following is straightforward to prove:

l:nilclos

Lemma 1.1.2. *Subgroups, homomorphic images and finite direct products of nilpotent groups are nilpotent.*

We note that nilpotency is not closed under extensions, since S_3 is an extension of C_3 by C_2.

1.2. Commutators. The theory of nilpotent groups relies significantly on commutator calculus that we briefly develop here. A *simple commutator of length n* of elements $x_1, \dots, x_n \in$G is defined inductively by $[x_1] = x_1$ and

$$[x_1, x_2, \dots, x_n] = [[x_1, \dots, x_{n-1}], x_n].$$

l:comm

Lemma 1.2.1. *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. Let us only sketch the proof of the Hall-Witt identity. Observe that

$$[x, y^{-1}, z]^y = x^{-1}y^{-1}xz^{-1}x^{-1}yxy^{-1}zy = u^{-1}v,$$

where $u = z^{x^{-1}}yx$ and we obtain v by cyclically permuting x, y, z in the definition of u. The rest is now immediate. □

These identities could also be proved using GAP. For example, in order to prove the identity $[xy, z] = [x, z]^y [y, z]$, it suffices that this holds in the free group generated by x, y, z:

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

Let $X, Y \subset G$ be non-empty sets. Define the *commutator subgroup* of X and Y by $[X, Y] = \langle [x, y] \mid x \in X, y \in Y \rangle$ and note that $[X, Y] = [Y, X]$. For any $n \geqslant 2$ nonempty subsets $X_1, X_2, \dots, X_n$ of G denote

$$[X_1, X_2, \dots, X_n] = [[X_1, \dots, X_{n-1}], X_n].$$

Note that $[G, G] = G'$ is just the derived subgroup of G. Define also $X^Y = \langle x^y \mid x \in X, y \in Y \rangle$. If X is a subset and $H \leqslant G$, then $X \subset X^H \lhd \langle X, H \rangle$. Thus, $X^H = X^{\langle X, H \rangle}$ is the normal closure of X in $\langle X, H \rangle$.

Here is an example:

```
gap> G := SmallGroup( 64, 52);;
gap> gen := GeneratorsOfGroup(G);;
gap> H := Subgroup(G, [gen[1]]);;
gap> K := Subgroup(G, [gen[2], gen[3]]);;
gap> C := CommutatorSubgroup(H,K);;
gap> Order(H);
2
gap> Order(K);
32
gap> Order(C);
16
```

prva

Lemma 1.2.2. *Let $X \subset G$ and $H \leqslant G$. Then*

(1) $X^K = \langle X, [X, K] \rangle$;
(2) $[X, K]^K = [X, K]$;
(3) *if* $K = \langle Y \rangle$, *then* $[X, K] = [X, Y]^K$.

Proof. (1) Follows from $x^k = x[x, k]$.

(2) For $k, h \in K$ and $x \in X$ we have $[x, hk] = [x, k][x, h]^k$, so that $[x, h]^k \in [X, K]$.

(3) It suffices to show that $[x, k] \in [X, Y]^K$ what we prove for $k = y_1^{\pm 1} y_2^{\pm 1} \dots y_r^{\pm 1}$ by induction on r. For $r = 1$ we get $[x, y_1^{-1}] = ([x, y_1]^{y_1^{-1}})^{-1} \in [X, Y]^K$. For the inductive step we write $k = k' y_r^{\pm 1}$. Then $[x, k] = [x, k' y_r^{\pm 1}] = [x, y_r^{\pm 1}][x, k']^{y_r^{\pm 1}} \in [X, Y]^K$ by induction. □

druga

Corollary 1.2.1. *If $H = \langle X \rangle$ and $K = \langle Y \rangle$, then $[H, K] = [X, Y]^{HK}$.*

Proof. This follows from Lemma 1.2.2, (3). □

1.3. Derived series, upper and lower central series. Define $G' = [G, G]$ and inductively $G^{(0)} = G$ and $G^{(n+1)} = (G^{(n)})'$. The *derived series* of G is the series

$$G^{(0)} \geqslant G^{(1)} \geqslant G^{(2)} \geqslant \cdots$$

of fully invariant (and therefore normal) subgroups of G. The derived series of a group is in close connection with its solvability:

Proposition 1.3.1. *If $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ is an abelian series of a solvable group G, then $G^{(i)} \leqslant G_{n-i}$ and, in particular, $G^{(n)} = 1$. The derived length of G is equal to the length of the derived series.*

Proof. We prove this by induction, the case $i = 0$ being trivial. If the assertion is true for i, then $G^{(i+1)} = (G^{(i)})' \leqslant (G_{n-i})' \leqslant G_{n-i-1}$, as required. □

GAP can compute the derived series as follows:

```
gap> G := OneSmallGroup(Size, 120, IsAbelian, false, IsSolvable, true);;
gap> StructureDescription(G);
"C5 x (C3 : C8)"
gap> DerivedSeries(G);
[ C5 x (C3 : C8), Group([ f5 ]), Group([  ]) ]
gap> DerivedLength(G);
2
```

There are two canonical central series of a given group. 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. The factor group $\gamma_n G/\gamma_{n+1} G$ lies in the center of $G/\gamma_{n+1} G$.

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. If G is finite, it terminates in a subgroup called the *hypercenter* of G.

Proposition 1.3.2. *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.*

Proof. (1). This is true for $i = 1$. Since $G_{n-i+1}/G_{n-i} \subset Z(G/G_{n-i})$, we have $[G_{n-i+1}, G] \subset G_{n-i}$. By induction,$\gamma_{i+1} G = [\gamma_i G, G] \leqslant [G_{n-i+1}, G] \leqslant G_{n-i}$. The item (2) is another easy induction and (3) follows. □

l:threesub **Lemma** 1.3.1 (The three subgroup lemma). *Let $H, K, L \leqslant G$. If two of the commutator subgroups $[H, K, L], [K, L, H]$, $[L, H, K]$ are contained in a normal subgroup of G, then so is the third one.*

Proof. By Corollary 1.2.1, $[H, K, L]$ is generated by conjugates of commutators of the form $[h, k^{-1}, l]$. Apply the Hall-Witt identity. □

Proposition 1.3.3. *Let G be a group and $i, j \in \mathbb{N}$:*

(1) *$[\gamma_i G, \gamma_j G] \leqslant \gamma_{i+j} G$.*
(2) *$\gamma_i(\gamma_j G) \leqslant \gamma_{ij} G$.*
(3) *$[\gamma_i G, Z_j(G)] \leqslant Z_{j-i}(G)$ if $j \geqslant i$.*
(4) *$Z_i(G/Z_j(G)) = Z_{i+j}(G)/Z_j(G)$*

Proof. (1) Both $[\gamma_i G, \gamma_j G, G]$ and $[G, \gamma_i G, \gamma_j G]$ are inductively (on j) contained in $\gamma_{i+j+1}G$. And by the three subgroup lemma the same holds true for $[\gamma_j G, G, \gamma_i G] = [\gamma_i G, \gamma_{j+1} G]$.

(2) This goes by induction on i: $\gamma_{i+1}(\gamma_j G) = [\gamma_i(\gamma_j G), \gamma_j G] \leqslant [\gamma_{ij} G, \gamma_j G] \leqslant \gamma_{(i+1)j} G$.

(3) $[\gamma_{i+1}G, Z_j G] = [\gamma_i G, G, Z_j G] \leqslant [G, Z_j G, \gamma_i G][Z_j G, \gamma_i G, G] \leqslant Z_{j-i-1}G$ by induction on i.

(4) Induction on i. □

Corollary 1.3.1. *For any group G we have that $G^{(i)} \leqslant \gamma_{2^i} G$. If G is nilpotent of positive class c, then its derived length is at most $\lfloor \log_2 c \rfloor + 1$.*

Proof. Apply part (2) of the above proposition to

$$G^{(i)} = \underbrace{\gamma_2(\cdots(\gamma_2 G)\cdots)}_{i \text{ times}}$$

Now, let G be nilpotent of class c, let d be the derived length and let $2^i \geqslant c+1$. Then, $G^{(i)} \leqslant \gamma_{2^i} G \leqslant \gamma_{c+1} G = 1$. Since the smallest such i is $\lfloor \log_2 c \rfloor + 1$, it follows that $d \leqslant \lfloor \log_2 c \rfloor + 1$. □

Here is a sample computation of lower and upper series of a group:

```
gap> G := SmallGroup(128, 50);;
gap> NilpotencyClassOfGroup(G);
4
gap> DerivedLength(G);
2
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([  ]) ]
```

1.4. (Uni)triangular groups. Here is a ring-theoretic source of examples of nilpotent groups. Let S be a ring with identity and N a subring. Write $N^{(i)}$ for the set of all sums of products of i elements of N for $i > 0$, which is necessarily a subring. If $N^{(i)} = 0$ for some $i > 0$, then N is called *nilpotent*. Assume $N^{(n)} = 0$ and let U be the set of all elements of the form $1 + x$ for $x \in N$. Then U is a group with respect to the ring multiplication, i.e.

$$(1+x)(1+y) = 1 + (x + y + xy)$$

and

$$(1+x)^{-1} = 1 + (-x + x^2 - \cdots + (-x)^{n-1}).$$

Define $U_i = \{1 + x \mid x \in N^{(i)}\}$ and observe that U_i is an increasing series of subgroups. We want to show that this is actually a central series of U. Let $x \in N^{(r)}$ and $y \in N^{(s)}$, then

$$[1+x, 1+y] = (1 + x + y + yx)^{-1}(1 + x + y + xy).$$

We let $u = x + y + xy$ and $v = x + y + yx$:

$$[1+x, 1+y] = (1 - v + v^2 - \cdots + (-v)^{n-1})(1+u) =$$
$$1 + (1 - v + v^2 - \cdots + (-v)^{n-2})(u - v) + (-v)^{n-1}u.$$

Now, $u - v = xy - yx \in N^{(r+s)}$ and $(-v)^{n-1}u = 0$. We have thus shown that $[U_r, U_s] \leqslant U_{r+s}$ implying that U is nilpotent of class no more than $n-1$.

For an even more concrete example, let us take S to 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 that the class of U in this case is exactly $n-1$ showing that there are nilpotent groups of arbitrary class. We note here that in the case $n = 3$ we call the group U a *discrete Heisenberg group* over R.

Observe that U_i consists of all upper unitriangular matrices whose first $i-1$ super diagonals are zero. It easily follows that

$$U_i/U_{i+1} \simeq \underbrace{R \oplus R \oplus \cdots \oplus R}_{n-i \text{ times}}.$$

In the case that $R = \mathrm{GF}(p)$ we find U to be a finite p-group of order $p^{n(n-1)/2}$. On the other hand, if $R = \mathbb{Z}$, then U is a finitely generated torsion-free nilpotent group.

Now, let T denote the group of all upper triangular invertible matrices over R. Let $\theta : T \to (R^*)^n$ be the projection of a matrix to its diagonal. So, this is an epimorphism whose kernel is precisely equal to U and whose image is an abelian group. It follows that T is solvable, with the derived length being no more than $[\log_2(n-1)+2]$.

1.5. Properties of nilpotent groups.

l:intersZ **Lemma** 1.5.1. *If G is a nilpotent group and $1 \neq N \lhd G$, then $N \cap Z(G) \neq 1$.*

Proof. Let i be the smallest natural number s.t. $N \cap Z_i(G) \neq 1$. Then, $[N \cap Z_i(G), G] \leqslant N \cap Z_{i-1}(G) = 1$, so that $N \cap Z_i(G) \leqslant N \cap Z_1(G) \neq 1$ implying equality. □

Corollary 1.5.1. *A minimal normal subgroup of a nilpotent group is contained in the center.*

Proposition 1.5.1. *If A is a maximal normal abelian subgroup of the nilpotent group G, then $A = C_G(A)$.*

Proof. Clearly $A \leqslant C = C_G(A)$. Suppose that $A \neq C$. Then C/A is a nontrivial normal subgroup of the nilpotent G/A. By Lemma 1.5.1 there is an $A \neq Ax \in (C/A) \cap Z(G/A)$. Now $\langle x, A \rangle$ is abelian and normal leading to a contradiction. □

Theorem 1.5.1. *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.*

Proof. (1) $\Rightarrow$ (2). Let G be nilpotent with class c. If $H \leqslant G$, then $HZ_iG \lhd HZ_{i+1}G$ since $Z_{i+1}G/Z_iG = Z(G/Z_iG)$. So, HZ_iG is the series proving subnormality of H.

(2) $\Rightarrow$ (3). Let $H = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$ be the series proving subnormality of the proper subgroup H. Let i be the smallest integer s.t. $H \neq H_i$. Then, $H = H_{i-1} \lhd H_i \leqslant N_G(H)$.

(3) $\Rightarrow$ (4). If $M < G$ is maximal, then $M < N_G(M)$ implying $N_G(M) = G$.

(4) $\Rightarrow$ (5). Assume P is a non-normal Sylow subgroup. Then $N_G(P)$ is proper and therefore contained in a maximal subgroup M. Then $M \lhd G$ contradicting Lemma 4.2.2. Thus, Sylow p-subgroup is normal and consequently unique for each p. Their product is clearly direct and equal to G.

(5) $\Rightarrow$ (1). This follows since every p-group is nilpotent and direct sum of nilpotent groups is nilpotent. □

In the case of infinite groups, properties (2) to (5) are weaker than (1). Using the above result, one can refine Corollary 1.2.1 as follows:

c:maxnil **Corollary** 1.5.2. *A maximal subgroup M of a finite nilpotent group G has prime index.*

Proof. We known that $M \lhd G$, and $|G : M| = p^k$ by Corollary 1.2.1. If $k > 1$, then there exists $H < G$ containing M such that $|H : M| = p$ which is a contradiction. □

1.6. The Fitting Subgroup.

Theorem 1.6.1 (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 $\leq c + d$.*

Proof. By induction on i we show that

$$\gamma_i(L) = \prod_{X_j \in \{M,N\}} [X_1, \ldots, X_i].$$

Taking $i = c + d + 1$ and noting that $[A, G] \leq A$ for all $A \lhd G$, we conclude that each $[X_1, \ldots, X_i]$ is contained in either $\gamma_{c+1}(M)$ or $\gamma_{d+1}(N)$, both of which equal to 1. $\square$

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. Note also that $\mathrm{Fit}(G) = 1$ if and only if G is semisimple.

Let $N \leq H \leq G$ and $N \lhd G$. Define

$$C_G(H/N) = \{g \in G : [H, g] \leq N\}.$$

Clearly $C_G(H/N) \leq G$.

Theorem 1.6.2. *Let G be a finite group. For a prime p let $O_p(G)$ be the largest normal p-subgroup of G. The following groups are then equal to* $\mathrm{Fit}(G)$*:*

(a) *The direct product of all $O_p(G)$, where p divides $|G|$.*
(b) *The intersection of the centralizers of the chief factors of G.*

Proof. (a) If $N \lhd G$ is nilpotent, then $N = \times O_p(N)$. As the group $O_p(N)$ is a characteristic subgroup of N, it follows that $O_p(N) \lhd G$. Therefore $O_p(N) \leq O_p(G)$, and thus $N \leq \times O_p(G)$.

(b) Let $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ be a chief series of G and denote

$$I = \bigcap_i C_G(G_{i+1}/G_i).$$

Since $[G_{i+1}, I] \leq G_i$ for all i, we get $\gamma_{n+1}(I) = 1$, hence $I \leq \mathrm{Fit}(G)$. Conversely, let $F = \mathrm{Fit}(G)$. Since G_1 is a minimal normal subgroup of G, we get either $[G_1, F] = 1$ or $[G_1, F] = G_1$. In the latter case, $G_1 \leq \gamma_{c+1}(F) = 1$ for some c, a contradiction. Thus $[G_1, F] = 1$. Induction on n shows that $F \leq C_G(G_{i+1}/G_i)$ for all i. $\square$

```
gap> G := SmallGroup(96, 10);;
gap> IsNilpotent(G);
false
gap> F := FittingSubgroup(G);;
gap> Order(F);
48
gap> StructureDescription(F);
"C12 x C4"
```

1.7. The Frattini subgroup. The *Frattini subgroup* $\mathrm{Frat}(G)$ of G is the intersection of all maximal subgroups of G (if G does not have maximal subgroups, then we define $\mathrm{Frat}(G) = G$). 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 1.7.1. $\mathrm{Frat}(G)$ *equals the set of nongenerators of G.*

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. $\square$

Proposition 1.7.1. *Let G be a finite group.*

(a) *If $N \lhd G$, $H \leq G$ and $N \leq$* $\mathrm{Frat}(H)$*, then $N \leq$* $\mathrm{Frat}(G)$*.*
(b) *If $K \lhd G$, then* $\mathrm{Frat}(K) \leq \mathrm{Frat}(G)$*.*
(c) *If $N \lhd G$, then* $\mathrm{Frat}(G/N) \geq \mathrm{Frat}(G)N/N$*, with equality if $N \leq$* $\mathrm{Frat}(G)$*.*
(d) *If A is an abelian normal subgroup of G such that* $\mathrm{Frat}(G) \cap A = 1$*, there exists $H \leq G$ such that $G = HA$ and $H \cap A = 1$.*

Proof.

(a) If not, then there exists a maximal subgroup M such that $N \not\leq M$. Then $G = MN$, $H = (H \cap M)N$, thus $H \leq M$, therefore $N \leq M$, a contradiction.

(b) Apply (a) with $N = \operatorname{Frat}(K)$ and $H = K$.
(c) By definition.
(d) Let H be minimal subject to $G = HA$. Then $H \cap A \lhd G$. If $H \cap A \leq \operatorname{Frat}(H)$, then we claim that $H \cap A = 1$ by (a). Namely, if this were false, there would exist a maximal subgroup M of H such that $H \cap A \not\leq M$. Then $H = M(H \cap A)$ and $G = MA$, contrary to the minimality of H.

□

Theorem 1.7.2 (Gaschütz). *Let G be a group.*

(a) *If $\operatorname{Frat}(G) \leq H \leq G$, where H is finite and $H/\operatorname{Frat}(G)$ is nilpotent, then H is nilpotent.*
(b) *If G is finite, $\operatorname{Frat}(G)$ is nilpotent.*
(c) *Define $\operatorname{FFrat}(G)$ by*

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

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

Proof.

(a) Let P be a Sylow subgroup of H, $F = \operatorname{Frat}(G)$, and $K = PF \leq H$. K/F is a Sylow subgroup of H/F, hence K/F is characteristic in H/F. Hence K is normal in G. By the Frattini argument,

$$G = N_G(P)K = N_G(P)F = N_G(P).$$

(b) Follows from (a).
(c) Denote $H = \operatorname{FFrat}(G)$. H is nilpotent by (a), thus $H \leq \operatorname{Fit}(G)$.
(d) Taking quotients, we may assume that

$$\operatorname{Frat}(G) = 1.$$

Write $L = \operatorname{Fit}(G)$. $L/\operatorname{Frat}(L)$ is abelian, hence $L' \leq \operatorname{Frat}(L) \leq \operatorname{Frat}(G) = 1$. Thus L is abelian. Let N be the product of all the abelian minimal normal subgroups of G. Then $N \leq L$. There exists $H \leq G$ such that $G = HN$ and $N \cap H = 1$. $H \cap L$ is normal in $HL = G$. Since $H \cap L \cap N = 1$, it follows that $H \cap L = 1$ by the minimality. Then $L = L \cap (HN) = N$.

□

Proposition 1.7.2. *Let G be a finite group. Then G is nilpotent if and only if $G' \leq \operatorname{Frat}(G)$.*

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

```
gap> G := SmallGroup(96, 10);;
gap> F := FrattiniSubgroup(G);;
gap> StructureDescription(F);
"C4 x C2"
```

2. Finite p-groups

s:pgroups

2.1. Basic properties.

Proposition 2.1.1. *Let G be a group of order p^{m+1}.*

(a) *If G is nilpotent of class $c > 1$, then $G/Z_{c-1}(G)$ is not cyclic.*
(b) *$c \leq m$.*
(c) *If $0 \leq i \leq j \leq m+1$, every subgroup of order p^i is contained in some subgroup of order p^j.*
(d) *G has subgroups of every order dividing p^{m+1}.*

Proof. (a) If $G/Z_{c-1}(G)$ were cyclic, $G/Z_{c-2}(G)$ would be abelian, hence $Z_{c-1}(G) = G$, a contradiction.

(b) $|G : Z_{c-1}(G)| \geq p^2$ by (a), all upper central factors have order $\geq p$.

(c) Let H be a subgrup of order p^i. As H is subnormal in G, it is a part of a composition series $1 = H_0 \leq \cdots \leq H_i = H \leq \cdots \leq H_{m+1} = G$ by Jordan-Hölder's theorem. All composition factors have order p, hence the assertion.

(d) Follows from (c). □

Let G be a group of order p^n. Then its nilpotency class c is strictly smaller of n. The difference $n - c$ is called the *coclass* of G. p-groups of coclass 1 are also known as *p-groups of maximal class*. An example of a p-group of maximal class is $C_p \wr C_p$; its order is p^{p+1} and the nilpotency class is precisely p (exercise).

e:2maxclass *Example* 2.1.1. Define

$$Q_{2^n} = \langle x, y \mid y^{2^{n-1}} = 1, x^2 = y^{2^{n-2}}, y^x = y^{-1} \rangle$$

to be the *generalized quaternion group* of order 2^n (check that this is indeed its order). The group Q_8 is known as the *quaternion group*. Similarly, the group

$$SD_{2^n} = \langle x, y \mid y^{2^{n-1}} = 1, x^2 = 1, y^x = y^{2^{n-2}-1} \rangle$$

is said to be the *semi-dihedral group* of order 2^n. A classical result of the coclass theory is that 2-groups of maximal class are precisely dihedral, semi-dihedral, and generalized quaternion 2-groups.

As we will see, there are many p-groups of given order, too many to classify them all up to isomorphism. In recent years there has been an idea to clasify p-groups according to coclass. This has lead to coclass theory which has produced some fascinating results. We refer to [7] for further results.

Lemma 2.1.1. *Let G be an elementary abelian p-group. Then* $\mathrm{Frat}(G) = 1$.

Proof. Let $G = C_p^n$ and let $M_i = \{(x_1, \dots x_{i-1}, 1, x_{i+1}, \dots, x_n) : x_j \in C_p\}$ for $i = 1, \dots, n$. Then M_i are maximal subgroups of G and $\bigcap_{i=1}^n M_i = 1$, hence $\mathrm{Frat}(G) = 1$. □

Theorem 2.1.1 (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.*

Proof. Let M be a maximal subgroup of G. Then $M \triangleleft G$ and $|G : M| = p$. It follows that $\gamma_2(G)G^p \leq M$, hence $\gamma_2(G)G^p \leq \mathrm{Frat}(G)$. On the other hand, $G/\gamma_2(G)G^p$ is an elementary abelian p-group, hence $\mathrm{Frat}(G/\gamma_2(G)G^p) = 1$. It follows that $\mathrm{Frat}(G) \leq \gamma_2(G)G^p$.

Let $G = \langle x_1, \dots, x_s \rangle$ and $F = \mathrm{Frat}(G)$. Then $\bar{G} = G/F = \langle Fx_1, \dots, Fx_s \rangle$. $\bar{G}$ is a vector space over $\mathrm{GF}(p)$, hence it has a basis $\{Fx_{i_1}, \dots, Fx_{i_r}\}$. Write $Y = \langle x_{i_1}, \dots, x_{i_r} \rangle$. Then $G = \langle Y, F \rangle$, hence $G = \langle Y \rangle$. □

Let G be a finite p-group. By the Burnside Basis Theorem, we can think of $G/\mathrm{Frat}(G)$ as a vector space over $\mathrm{GF}(p)$.

Corollary 2.1.1. *Let G be a finite p-group and d the minimal number of generators of G. Then $d = \dim_{GF(p)} G/\mathrm{Frat}(G)$.*

2.2. Extraspecial p-groups.

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

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

Proposition 2.2.1. *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.

Proof. All the groups given above have order p^3. For $p = 2$, the assertion follows from the description of all groups of order 8 (exercise).

Assume that p is odd. We consider two cases:

Case 1. All elements of G have order p. Let $z \in Z(G)\backslash\{1\}$ and let $x \notin Z(G)$. Then $\langle z, x\rangle = \langle z\rangle \times \langle x\rangle$ is a subgroup of order p^2, hence it is a maximal subgroup and thus normal in G. Choose $w \notin \langle z, x\rangle$. Then $G = \langle z, x, w\rangle$. We have that $x^w = x^a z^b$ for some $0 \leq a, b < p$. If $a = 0$, then $x^y \in Z(G)$, hence $x \in Z(G)$, a contradiction. Thus there exists c such that $ac \equiv 1 \mod p$. Let $t = w^c$. We have that $G = \langle z, x, t\rangle$, and $x^t = xz^{b'}$ for some $0 \leq b' < p$. As G is nonabelian, $b' \neq 0$, hence there exists d such that $b'd \equiv 1 \mod p$. Put $y = t^d$. Then we get $[x, y] = z$ and $G = \langle x, y\rangle$. We have

$$x^p = y^p = 1, [x, y]^x = [x, y]^y = [x, y],$$

as required.

Case 2. G contains an element x of order p^2. Let $N = \langle x\rangle$. As N is a maximal subgroup of G, N is normal in G. Choose $z \in G\backslash N$ of order p. There exists $a \in \mathbb{Z}$ such that $x^z = x^a$. Since $x = x^{z^p}$, it follows that $a^p \equiv 1 \mod p^2$, hence $a \equiv 1 \mod p$. Write $a = 1 + kp$. Let l be such that $kl \equiv 1 \mod p$. Let $y = z^l$. Then $x^y = x^{1+p}$. Since $N \cap \langle y\rangle = 1$, we have $N\langle y\rangle = G$.

All the groups above are clearly extraspecial. □

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 2.2.1. *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.*

Proof. Let $C = Z(G) = G'$, and let c be a generator of C. The group $V = G/C$ is elementary abelian, hence a vector space over $\mathrm{GF}(p)$. We have a well defined skew-symmetric bilinear form $f : V \times V \to \mathrm{GF}(p)$ induced by

$$[x, y] = c^{(Cx, Cy)f}.$$

If $(Cx, Cy)f = 0$ for all $y \in G$, then $x \in C$, thus f is nondegenerate. Thus there exists a decomposition $V = V_1 \oplus \cdots \oplus V_n$ where V_i is a 2-dimensional space with basis $\{u_i, v_i\}$, such that

$$\begin{array}{rcl} (u_i, v_i)f & = & 1, \\ (u_i, v_j)f & = & 0 \text{ for } i \neq j, \\ (u_i, u_j)f & = & 0, \\ (v_i, v_j)f & = & 0. \end{array}$$

Write $u_i = Cx_i$, $v_i = Cy_i$. Then $G_i = \langle x_i, y_i\rangle$ is a nonabelian group of order p^3. We have that G is the central product of $G_1, \ldots G_n$. Clearly

$$G/C = G_1/C \times \cdots G_n/C,$$

hence $|G| = p^{2n+1}$.

Conversely, let G be the central product of $G_1, \ldots, G_n$, where each G_i is a nonabelian group of order p^3. Since $Z(G_i) \leq Z(G)$, it follows that $Z(G) = Z(G_i) \cong C_p$. Beside that, $[G_i, G_j] = 1$ for $i \neq j$, and $[G_i, G_i] = Z(G_i) = Z(G)$ for all i. Hence

$$[G, G] = [G_1 \cdots, G_n, G_1 \cdots G_n] = Z(G),$$

therefore G is extraspecial. □

3. Enumeration of finite p-groups

s:enumer

It turns out that most of the finite groups are p-groups. The proof is beyond the scope of these notes. To illustrate this result, there are 49, 910, 529, 484 different isomorphism classes of groups of order at most 2000, and 49, 487, 365, 422, or just over 99%, are groups of order 1024. We mention here that Phillip Hall proved that the number of isomorphism classes of groups of order p^n is

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

We will not prove this result. Instead we will derive some good upper and lower bounds on the number of finite p-groups of given order. We refer to [2] for a wealth of further estimates.

3.1. Preliminary results. Let r be a positive integer and F_r a free group on $\{x_1, \dots, x_r\}$. 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 $x_1, \dots, x_r$ generate G_r.

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. Our first result shows that every group of Φ-class 2 is a homomorphic image of some G_r:

l:Gr **Lemma** 3.1.1. *Let H be a group of Φ-class 2, and let $y_1, \dots, y_r \in H$. There is a homomorphism $\phi : G_r \to H$ such that $x_i^\phi = y_i$ for all $i = 1, \dots, r$.*

Proof. As F_r is free there exists a unique homomorphism $F_r \to H$ with $x_i \mapsto y_i$. As $F_r^{p^2} \gamma_2(F_r)^p \gamma_3(F)$ is contained in the kernel of this map, we get the result. □

l:Grprop **Lemma** 3.1.2. *The group G_r is a finite p-group. The Frattini subgroup $\operatorname{Frat}(G_r)$ is central of order $p^{r(r+1)/2}$ and index p^r. Moreover, any automorphism $\alpha \in \operatorname{Aut}(G_r$ that induces an identity mapping on $G_r/\operatorname{Frat}(G_r)$ fixes $\operatorname{Frat}(G_r)$ pointwise.*

Sketch of proof. The group $G_r^p \gamma_2(G_r)$ is a central elementary abelian p-subgroup of G_r, and the quotient by it is also elementary abelian. Thus G_r is a p-group. Observe that $\operatorname{Frat}(G_r)$ is generated by x_i^p and $[x_j, x_i]$, where $1 \le i < j \le r$. It is straightforward but technical to prove that this generating set is a minimal one, we skip the details. It follows that $\operatorname{Frat}(G_r)$ is central of order $p^{r(r+1)/2}$ and index p^r.

Now take $\alpha \in \operatorname{Aut}(G_r)$ that induces an identity mapping on $G_r/\operatorname{Frat}(G_r)$. So there exist $h_1, \dots, h_r \in \operatorname{Frat}(G_r)$ such that $x_i^\alpha = h_i x_i$. Since $\operatorname{Frat}(G_r)$ is central and $\operatorname{Frat}(G_r)^p = \{1\}$, we have

$$(x_i^p)^\alpha = (x_i^\alpha)^p = (h_i x_i)^p = h_i^p x_i^p = x_i^p$$

and

$$[x_j, x_i]^\alpha = [x_j^\alpha, x_i^\alpha] = [h_j x_j, h_i x_i] = [x_j, x_i].$$

Thus α fixes every generator of $\operatorname{Frat} G_r$ and we are done. □

l:isoGr **Lemma** 3.1.3. *Let N_1 and N_2 be subgroups of $\operatorname{Frat} G_r$. Then $G_r/N_1 \cong G_r/N_2$ if and only if there exists $\alpha \in \operatorname{Aut} G_r$ such that $N_1^\alpha = N_2$.*

Proof. It is obvious that if there exists $\alpha \in \operatorname{Aut} G_r$ such that $N_1^\alpha = N_2$, then it induces an isomorphism $G_r/N_1 \to G_r/N_2$. Conversely, suppose there is an isomorphism $\alpha' : G_r/N_1 \to G_r/N_2$. Let $y_1, \dots, y_r \in G$ be such that $(N_1 x_i)^{\alpha'} = N_2 y_i$. By Lemma 3.1.1 there exists a homomorphism $\alpha : G_r \to G_r$ with $x_i^\alpha = y_i$. Since α' is an isomorphism, $G_r = \langle y_1, \dots, y_r \rangle N_2$. But $N_2 \le \operatorname{Frat} G_r$, therefore $G_r = \langle y_1, \dots, y_r \rangle$. Thus α is surjective. Since G_r is finite, this implies that α is an isomorphism. It remains to show that $N_1^\alpha = N_2$. By definition, $N_2 x^\alpha = (N_1 x)^{\alpha'}$ for all $x \in G_r$, and the result follows easily from here. □

3.2. A lower bound. A similar argument as in the proof of 2.4.1 shows the following:

l:subsp **Lemma** 3.2.1. *Let V be a vector space over $\mathrm{GF}(q)$ of dimension d. For $0 \le k \le d$, let $n_{k,d}$ be the number of subspaces of V of dimension k. Then*

$$n_{k,d} = \frac{(q^d - 1)(q^d - q) \cdots (q^d - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})}.$$

In particular, $q^{k(d-k)} \le n_{k,d} \le q^{k(d-k+1)}$.

p:aux **Proposition** 3.2.1. *Let r be a positive integer, and s an integer such that $1 \le s \le r(r+1)/2$. Then there are at least $p^{rs(r+1)/2 - r^2 - s^2}$ isomorphism classes of groups of order p^{r+s}.*

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}. Furthermore, Lemma 3.1.3 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.

Let $\theta : \operatorname{Aut} G_r \to \operatorname{Aut}(G_r/\operatorname{Frat} G_r)$ be the natural homomorphism. By Lemma 3.1.2 every $\alpha \in \ker\theta$ fixes $\operatorname{Frat} G_r$ pointwise and so acts trivially on X. Therefore $\ker\theta$ is contained in the stabilizer of every element of X, and so the length of any orbit of $\operatorname{Aut} G_r$ acting on X is at most

$$|\operatorname{Aut} G_r|/|\ker\theta| \leq |\operatorname{Aut}(G_r/\operatorname{Frat} G_r)| = |\operatorname{Aut} C_p^r| = |\operatorname{GL}(r,p)| \leq p^{r^2}.$$

From Lemma 3.2.1 we conclude that $|X| \geq p^{s(r(r+1)/2-s}$, therefore there are at least

$$p^{s(r(r+1)/2-s}/p^{r^2}$$

orbits of $\operatorname{Aut} G_r$ on X. This gives the desired bound. □

Proposition 3.2.1 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 $z = 2/27$.

t:hig **Theorem** 3.2.1. *The number $f(p^n)$ of groups of order p^n is at least*

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

Proof. We may assume $n > 6$. Define $s = (n + 2(n \mod 3))/3$ and $r = n - s$. Then Proposition 3.2.1 gives $f(p^n) \geq p^{rs(r+1)/2-r^2-s^2} \geq p^{2n^2(n-6)/27}$. □

3.3. An elementary upper bound. 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 $\alpha_i \in \{0, 1, \ldots, p-1\}$. Furthermore, $g \in G_i$ iff $\alpha_1 = \cdots = \alpha_i = 0$.

Observe that, given $1 \leq i < j \leq n$, we have that $g_i^p \in G_i$ and $[g_j, g_i] \in G_j$. Hence we may write these elements in normal form, that is,

eq:power
$$g_i^p = g_{i+1}^{\beta_{i,i+1}} \cdots g_n^{\beta_{i,n}} \tag{3.3.1}$$

and

eq:comm
$$[g_j, g_i] = g_{j+1}^{\gamma_{i,j,j+1}} \cdots g_n^{\gamma_{i,j,n}} \tag{3.3.2}$$

for some $\beta_{i,j}, \gamma_{i,j,k} \in \{0, 1, \ldots, p-1\}$. It is easy to see that the generators $g_1, \ldots, g_n$ and all the relations of the form (3.3.1) and (3.3.2) form a presentation for G (called a *power commutator presentation* or *polycyclic presentation*). One has to prove that a product of two elements in normal form can again be written in normal form. This can be done using *collection process* described in [9].

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

```
gap> PrintPcpPresentation(PcGroupToPcpGroup(DihedralGroup(16)));
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.

The above discussion leads to the following:

t:upp **Theorem** 3.3.1. *We have that*

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

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. □

:problems_nilpotent

Problems

(1) Prove that the Pauli spin matrices

$$i=\begin{pmatrix}\sqrt{-1} & 0\\ 0 & -\sqrt{-1}\end{pmatrix},\ j=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\ k=\begin{pmatrix}0 & \sqrt{-1}\\ \sqrt{-1} & 0\end{pmatrix}$$

generate a subgroup of $\mathrm{GL}(2,\mathbb{C})$ that is isomorphic to Q_8.

(2) Let a group G be generated by $a_1,\ldots,a_d$. Show that $\gamma_i(G)$ is the normal closure in G of the set $\{[x_{j_1},\ldots,x_{j_i}] \mid 1\leq j_k\leq i\}$.

(3) Let $G=\langle a_1,\ldots,a_d\rangle$ be a nilpotent group. Then every element of G' can be written as $[x_1,a_1]\cdots[x_d,a_d]$ for some $x_1,\ldots,x_d\in G$.

(4) Suppose that $G=HN'$, where $H\leq G$ and $N\lhd G$. Prove that $G=H\gamma_i(N)$ for all i.

(5) Prove that the group $C_p\wr C_{p^n}$ is nilpotent of class precisely p^n.

(6) Let G be a group of order p^n. If G has a unique subgroup of order p^m for all $1<m<n$, prove that G is cyclic.

(7) Let G be a group of order p^n, wher $n\geq 3$, and of maximal class. Prove the following:
   (a) 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.
   (b) For every $i\geq 2$ we have that $\gamma_i(G)$ is the only normal subgroup of G of index p^i.
   (c) $Z_i(G)=\gamma_{n-i}(G)$ for all $i=0,\ldots,n-1$.

(8) Let G be a group in which $x^2\in Z(G)$ for every $x\in G$. Prove the following:
   (a) G is nilpotent of class ≤ 2.
   (b) Every element of G' has order at most 2.
   (c) For all $x,y\in G$, the element $(xy)^2y^{-2}x^{-2}$ belongs to G'.
   (d) For every $x,y\in G$ we have that $(xy)^4=x^4y^4$.

(9) Let G be a metabelian group and $x,y,z,z_1,\ldots,z_n\in G$. Prove:
   (a) $[x,y,z_1,\ldots,z_n]=[x,y,z_{\pi(1)},\ldots,z_{\pi(n)}]$ for every $\pi\in S_n$.
   (b) $[x,y,z][y,z,x][z,x,y]=1$.

(10) Let G be a group in which $x^3=1$ for all $x\in G$. Prove that $[x,y,y]=1$ for all $x,y\in G$.

(11) Let G be a finite group and F its Fitting subgroup.
   (a) Let N/F be an abelian normal subgroup of G/F such that $N\leq C_G(F)F$. Prove that $N=F(N\cap C_G(F))$.
   (b) Let N be as in (a). Prove that $N/(N\cap C_G(F))$ is nilpotent.
   (c) Let c be the nilpotency class of $N/(N\cap C_G(F))$, where N is as above. Show that N is nilpotent of class $\leq c+1$.
   (d) Conclude that $C_G(F)F/F$ contains no non-trivial abelian normal subgroup.
   (e) If G is solvable, show that $C_G(F)\leq F$.

(12) Let G be a finite nilpotent group and N a non-trivial normal subgroup of G. Show the following:
   (a) $[N,G]$ is a proper subgroup of N.
   (b) Some maximal proper subgroup of N is normal in G.
   (c) Suppose that G is a p-group and M and N normal subgroups of G with $N<M$. Prove that there exists $K\lhd G$ such that $N\leq K<M$ and $|M:K|=p$.

(13) Supply a proof of Lemma 3.2.1.

(14) Use GAP to explore the number $f(m)$ of groups of order m for small m, and in the case when $m=p^n$ for small primes p and integers n.

Bibliography

Atlas [1] *Atlas of Finite Group Representations*, http://brauer.maths.qmul.ac.uk/Atlas/v3/. 28

Blackburn2007 [2] S. R. Blackburn, P. M. Neumann, and G. Venkataraman, *Enumeration of finite groups*, Cambridge University Press, Cambridge, 2007. 45

Brown1982 [3] K. S. Brown, *Cohomology of groups*, Springer-Verlag, New York, 1982. 29

Cameron2013 [4] P. J. Cameron, *Notes on finite group theory*, October 2013. 4, 24

GAP4 [5] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.7.4*; 2014, (http://www.gap-system.org). 4, 7

Isaacs2008 [6] I. M. Isaacs, *Finite group theory*. Graduate Studies in Mathematics, 92. American Mathematical Society, Providence, RI, 2008. 5

Leedham2002 [7] C. R. Leedham-Green, and S. McKay, *The structure of groups of prime power order*, Oxford University Press, New York, 2002. 43

Robinson1996 [8] D. J. S. Robinson, *A course in the theory of groups*, 2nd. ed., Springer-Verlag, New York, 1996. 4, 5, 7, 29

Sims1994 [9] C. C. Sims, *Computation with finitely presented groups*, Cambridge University Press, Cambridge, 1994. 46