Group Theory

Richard Earl (revised by E. Breuillard in 2025)

April 23, 2025

Contents

I Introduction **3**

1 Synopsis **3**

2 A Brief Summary of the Course **6**

3 Recap: Basic notions **7**

4 Recap: Basic Examples of Groups **10**

II Generators and Relations. Free Groups. **13**

5 Free Groups **14**

6 The Universal Mapping Property **17**

7 Presentations **18**

III Isomorphism Theorems. Simple Groups **23**

8 The First Isomorphism Theorem **23**

9 The Second and Third Isomorphism Theorems **24**

10 Simple Groups 26

IV Composition series. Jordan–Hölder Theorem 29

V Solvable Groups 33

VI Semi-direct Products 37

11 Extensions 42

VII Sylow's Theorems 44

12 Applications 47

Part I
Introduction

1 Synopsis

- Free groups. Uniqueness of reduced words and universal mapping property. Normal subgroups of free groups and generators and relations for groups. Examples. [2]
- Review of the First Isomorphism Theorem and proof of Second and Third Isomorphism Theorems. Simple groups, statement that A_n is simple (proof for $n = 5$). Definition and proof of existence of composition series for finite groups. Statement of the Jordan-Hölder Theorem. Examples. The derived subgroup and solvable groups. [3]
- Discussion of semi-direct products and extensions of groups. Examples. [1]
- Sylow's three theorems. Applications including classification of groups of small order. [2]

Reading List

- Armstrong, M. A. *Groups and Symmetry*, Springer, 1988
- Alperin, J. L.; Bell, Rowen B. *Groups and Representations* 162. Springer, 1995
- Humphreys, *A course in group theory*, Oxford, 1996.
- Neumann, Peter M.; Stoy, Gabrielle A.; Thompson, Edward C., *Groups and Geometry*, OUP, 1994

STANDARD GROUP NOTATION

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ – the integers/rationals/reals/complex numbers under $+$.
- C_n – the cyclic group of order n.
- $\mathbb{Z}_n$ – the integers, mod ulo n, under $+$, which is isomorphic to C_n.
- $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ – non-zero rationals/reals/complex numbers under $\times$.
- $\mathbb{Z}_p^*$ – the non-zero elements of $\mathbb{Z}_p$, where p is a prime, under $\times$.
- $\mathbb{Z}_n^*$ – more generally for composite n, the units of $\mathbb{Z}_n$ under $\times$, i.e. those integers coprime with n.
- $(0, \infty)$ – the positive real numbers under $\times$.
- $\mathrm{Sym}(S)$ – the permutations (i.e. bijections $S \to S$) of a set S under composition.
- S_n – permutations of $\{1, 2, \ldots n\}$ under composition.
- A_n – even permutations of $\{1, 2, \ldots, n\}$ under composition.
- D_{2n} – the symmetries of a regular n-sided polygon under composition.
- V or V_4 – the Klein four-group $C_2 \times C_2 \cong \{e, (12)(34), (13)(24), (14)(23)\}$.
- Q_8 – the quaternion group $\{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$.
- S^1 – the complex numbers with unit mod ulus under multiplication.
- $GL(n, F)$ – invertible $n \times n$ matrices with entries in the field F under matrix multiplication.
- $SL(n, F)$ – the subgroup of $GL(n, F)$ whose elements have determinant 1.
- $AGL(n, F)$ – the affine maps of F^n.
- $O(n)$ – orthogonal $n \times n$ real matrices ($A^{-1} = A^T$) under matrix multiplication. Also $SO(n)$.
- $U(n)$ – unitary $n \times n$ complex matrices ($A^{-1} = \bar{A}^T$) under matrix multiplication. Also $SU(n)$.

- $\mathrm{Aut}(G)$ – the automorphisms (i.e. isomorphisms $G \to G$) of a group G under composition.
- $G_1 \times G_2$ – the direct product group of two groups G_1 and G_2.
- $G_1 \rtimes_\varphi G_2$ – the semi-direct product of two groups G_1 and G_2 associated with the homomorphism $\varphi\colon G_2 \to \mathrm{Aut}(G_1)$.
- G/H – the quotient (or factor) group of a group G by a normal subgroup H of G.
- $\langle g \rangle$ – the cyclic subgroup of G generated by $g \in G$.
- $\langle S \rangle$ – the subgroup of a group G generated by a subset S of G.

2 A Brief Summary of the Course

This course includes various themes, which might at first glance seem unrelated. The summary below aims to give a narrative showing how these themes do indeed interconnect and provide us with some of the theory and tools to better understand the internal structure of groups. *This summary will not be covered in lectures and so may well be worth reading ahead of the course.*

A starting point for better understanding the nature of groups is the *Jordan-Hölder Theorem* (JHT). This says that for any finite group G there is a *composition series* of subgroups

$$\{e\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G$$

such that each composition factor G_i/G_{i-1} $(i = 1, \ldots, n)$ is *simple*. (A non-trivial group is simple if it has no non-trivial proper normal subgroups.) So for example the following are composition series of

$$\{e\} \lhd A_3 \lhd S_3; \qquad \{e\} \lhd \left\{e, g^2, g^4\right\} \lhd C_6; \qquad \{e\} \lhd \left\{e, g^3\right\} \lhd C_6.$$

The corresponding composition factors are C_3, C_2 for S_3, C_3, C_2 for C_6, and C_2, C_3 for C_6. JHT guarantees more than the existence of a composition series: it states that different composition series *for the same group* will list the same composition factors (as in the latter two cases for C_6). As the composition factors are simple they are, in some sense, the atomic components of the group. However the simple examples above demonstrate that knowing the atoms, we don't then necessarily know the molecule – the non-isomorphic group S_3 has the same composition factors as C_6.

Nonetheless JHT breaks the classification problem for finite groups into two (still difficult) problems: (i) identify the simple groups; (ii) identify the ways these simple groups may be put together to form bigger groups. The second of these problems is called the *extension problem*. Given two groups, a larger group may always be created by taking their direct product. With the example of C_3 and C_2 above we would obtain $C_3 \times C_2 \cong C_6$. However we could also create a *semi-direct product*. If $C_3 = \langle r \rangle$ and $C_2 = \langle s \rangle$ then there is a semi-direct product

$$C_3 \rtimes C_2 = \langle r, s : r^3 = e = s^2, rs = sr^{-1} \rangle = D_6 \cong S_3.$$

This is a twisted version of the direct product, where the two groups actually interact (unlike with the direct product). We will further need the language of generators and relations to properly describe such semi-direct products.

So, we have refined the problem of classifying groups into two smaller problems of determining the simple groups and understanding how we might combine them. Given a problem such as "how many groups are there of order n?" the three *Sylow Theorems* are key tools in answering this. They go a long way to providing a partial converse to Lagrange's Theorem and state the following for a group G of order $p^a m$, where p is a prime and p does not divide m.

- G has a subgroup of order p^a, a so-called Sylow p-group.
- All such Sylow p-groups are conjugate in G.
- The number n_p of such subgroups satisfies $n_p = 1 \pmod p$ and n_p divides m.

So, in the simple example of a group G of order 6, with $p = 3$ we know that $n_3 = 1 \pmod 3$ and that n_3 divides 2. This means that $n_3 = 1$ and in particular it means our Sylow 3-group is normal in G (as it is closed under conjugacy). This then means that G is an *extension* of C_3 by C_2 and both these extensions manifest as semi-direct products. For small values of n, at least, the Sylow theorems can prove similarly useful.

3 Recap: Basic notions

Below is a recap of some of the important definitions and theory from the first year. *This will not be covered in lectures.*

A group $(G, *)$ is a set G with an associative binary operation (product) $*$, with an identity element $e \in G$ and an inverse element g^{-1} for each $g \in G$ such that

$$g * g^{-1} = g^{-1} * g = e$$

for all $g \in G$. We will often omit $*$ from the notation and write the group operation as juxtaposition $g * h = gh$. A group G is *abelian* if $gh = hg$ for each pair g, h of elements; most interesting examples of groups are non-abelian. If G has finitely many elements (we will call such G *finite*), its *order* (size) is denoted by $|G|$. For an element $g \in G$, its *order* is defined to be the smallest positive integer n such that $g^n = e$; equivalently, it is the size of the subgroup $\langle g \rangle$ of G generated by g. For G finite, this is always a finite number of course but in general it may be infinite.

A subset $H \subseteq G$ is a *subgroup*, denoted $H \leqslant G$, if it is closed for the group operations: it contains the identity element, the inverse g^{-1} of every element $g \in H$, and the product gh of any two elements $g, h \in H$.

The left *cosets* of a subgroup H are the sets $gH = \{gh : h \in H\}$ for some $g \in G$. The different left cosets are disjoint subsets of G, and their union is G itself. The right cosets are $Hg = \{hg : h \in H\}$, which have the same properties. The number of left, equivalently right cosets is called the *index* $[G : H]$ of H in G (which may of course be infinite in general). Different group elements can represent the same left coset and $gH = kH$ if and only if $g^{-1}k \in H$.

Theorem 1 ***(Lagrange's Theorem)*** *If G is finite, then*

$$|G| = [G : H] \times |H| .$$

Conjugation by an element $g \in G$ is the operation on G defined by

$$h \mapsto g^{-1}hg.$$

Two group elements h_1, h_2 are *conjugate* if there exists $g \in G$ such that $h_1 = g^{-1}h_2g$. Conjugation by any group element is an isomorphism of G – so that conjugate elements have the same order and conjugate subgroups are isomorphic. Being conjugate is an equivalence relation, so splits up G as a union of *conjugacy classes*. Note that the notion here is being conjugate *in a group* and elements may be conjugate in a group but not conjugate in some smaller subgroup.

A subgroup $N \leqslant G$ is called a *normal subgroup*, if one of the following three equivalent conditions is satisfied.

(i) The left and right cosets coincide: $gN = Ng$ (as sets!) for all $g \in G$.

(ii) Conjugation by elements of G leaves N invariant: $g^{-1}Ng = N$ (as sets!) for all $g \in G$.

(iii) N is a union of conjugacy classes of G.

We will denote this by $N \lhd G$. All the subgroups of an Abelian group are normal but non-Abelian groups can also have normal subgroups. For a given group G it is always the case that G and $\{e\}$ are normal subgroups of G. Note that normality refers to one subgroup sitting inside another group; there isn't a notion of a normal group.

If N is normal in G, the (left and right) cosets form a group themselves under the group operation

$$g_1N * g_2N = g_1g_2N,$$

well defined precisely because N is normal in G. Being well-defined here means that the product of the cosets is independent of the choice of representatives for the cosets being multiplied; the above product is well-defined if and only if N is normal. This new group, whose elements are the cosets, is called the *quotient group* and denoted G/N. It is often easiest to think of G/N as "G mod N".

A map of groups $\phi\colon (G_1, *) \to (G_2, \circ)$ is called a *homomorphism* if it preserves the group operation:

$$\phi(g * h) = \phi(g) \circ \phi(h) \qquad \text{for all } g, h \in G_1.$$

In particular, this implies that ϕ takes the identity of G_1 to that of G_2, and inverses to inverses. The *kernel*

$$\ker \phi = \{g \in G \,|\, \phi(g) = e\}$$

is a subgroup and in fact a normal subgroup of G_1. The *image*

$$Im\phi = \{\phi(g) \in G_2 \,|\, g \in G_1\}$$

is a subgroup of G_2.

Note that ϕ is injective if and only if $\ker \phi = \{e\}$, and surjective if and only if $Im\phi = G_2$. If ϕ is both bijective then ϕ is an *isomorphism*, we say that the groups G_1, G_2 are *isomorphic* and we write $G_1 \cong G_2$. Being isomorphic is an equivalence relation as the inverse of an isomorphism and the composition of two isomorphisms are also isomorphisms.

Given a normal subgroup N of a group G there is a natural *quotient homomorphism*

$$q\colon G \to G/N \qquad \text{defined by} \qquad q(g) = gN.$$

Note that $\ker q = N$, and q is surjective. Conversely, we have:

Theorem 2 ***(The First Isomorphism Theorem)*** *Given a homomorphism $\phi\colon G_1 \to G_2$, there is a well-defined isomorphism*

$$G_1/\ker \phi \xrightarrow{\cong} \mathrm{Im}\phi, \qquad \textit{given by} \qquad g \ker \phi \mapsto \phi(g)$$

and the map ϕ factors into the canonical quotient map $G_1 \to G_1/\ker \phi$, the above isomorphism, and the inclusion $\mathrm{Im}\phi \to G_2$.

If G is a finite group and N is a non-trivial normal subgroup of G, then G is in some sense "made up" of the smaller groups N and G/N. Quite how the abstract groups N and G/N fit together can be rather subtle though. A non-trivial group G is *simple* if it cannot be decomposed in this way, i.e. if whenever $N \lhd G$ is a normal subgroup, either $N = G$ or $N = \{e\}$ (i.e. G does not admit a non-trivial proper normal subgroup).

4 Recap: Basic Examples of Groups

- Cyclic Groups

The *cyclic group* C_n is the group generated by a non-trivial generator g of order n. Concretely,

$$C_n \cong \mathbb{Z}_n,$$

the additive group of integer numbers mod ulo n. Choosing a primitive nth root of unity $\xi \in \mathbb{C}$ gives another realization of C_n as a multiplicative group of the powers of ξ.

Proposition 3 *If G is a group of prime order p, then $G \cong C_p$.*

This follows from Lagrange's Theorem as a non-trivial element g of G generates a subgroup whose order divides p and hence such a g is a generator.

- Symmetric and Alternating Groups

The *symmetric group* S_n is the group of all permutations (bijections) of the set $\{1, \ldots, n\}$, the group operation being composition. In this course, we agree once and for all that for permutations $\sigma, \tau \in S_n$, the composite $\sigma\tau$ means σ followed by τ. The order of S_n is $n!$.

The *sign homomorphism*

$$\operatorname{sgn}\colon S_n \to C_2 \cong \{\pm 1\}$$

was defined in Prelims Linear Algebra; one definition is that $\operatorname{sgn}(\sigma)$ is the parity of the number of transpositions in a decomposition of σ as a product of transpositions (remembering that this is always possible and that the resulting sign is well defined). The kernel

$$A_n = \ker \operatorname{sgn}$$

is the group of even permutations, the *alternating group.*

Two permutations σ_1, σ_2 are conjugate in S_n if and only if they have the same cycle decomposition type.

- Normal subgroups of S_3

We list the conjugacy classes in S_3 and their sizes.

Cycle type	Size of conjugacy class
(1)(1)(1)	1
(2)(1)	3
(3)	2

By Lagrange's theorem, the only proper non-trivial normal subgroup of S_3 is A_3.

- Normal subgroups of S_4

  Similarly, we list the conjugacy classes in S_4 and their sizes.

Cycle type	Size of conjugacy class
(1)(1)(1)(1)	1
(2)(1)(1)	6
(3)(1)	8
(2)(2)	3
(4)	6

By Lagrange's theorem, there are two proper non-trivial normal subgroups in S_4: as well as A_4, there is also the group usually denoted V_4, consisting of all (2)(2) types and the identity; note

$$V_4 \cong C_2 \times C_2.$$

- Normal subgroups of S_5

  Finally, here are the conjugacy classes in S_5.

Cycle type	Size of conjugacy class
(1)(1)(1)(1)(1)	1
(2)(1)(1)(1)	10
(3)(1)(1)	20
(2)(2)(1)	15
(3)(2)	20
(4)(1)	30
(5)	24

A normal subgroup of S_5 must be a union of conjugacy classes, must contain the class of the identity, and by Lagrange's theorem, it must have order dividing 120. A short check shows that the only non-trivial normal subgroup is A_5.

- Linear Groups

Let V be a vector space over a field K. The *general linear group* $\mathrm{GL}(V)$ is the group of invertible linear maps of V. Concretely, if V is finite dimensional, choosing a basis we can identify $V \cong K^n$ for $n = \dim V$, and then $\mathrm{GL}(V)$ becomes identified with the group $\mathrm{GL}(n, K)$ of $n \times n$ invertible matrices with entries in K. Usually these are infinite groups, but when K itself is finite, they become finite and very interesting groups. The subgroup $\mathrm{SL}(n, K) \lhd \mathrm{GL}(n, K)$ consists of matrices of determinant one, in other words the kernel of the determinant homomorphism to K^*, the group of nonzero elements in K under multiplication.

Part II
Generators and Relations. Free Groups.

The concept of generators for a group is fundamental for advanced group theory. We start with a slightly informal definition, which hopefully captures the essence of the idea, then formalize it.

- Let G be a group and let S be a subset of G. The subgroup of G generated by S is the smallest subgroup of G containing S.

The informality is in the use of the word "smallest": what if two different subgroups of the same order (i.e. size as sets) both contain S? In fact this cannot happen and by improving our definition, we can see this immediately. First, remember that the intersection of two subgroups is a subgroup – in fact, for any non-empty set I (possibly uncountable), if $\{G_i : i \in I\}$ is a set of subgroups of G then $\bigcap_{i\in I} G_i$ is again a subgroup. Now we can give a formal definition.

Definition 4 *Let G be a group and let S be a subset of G. The* ***subgroup of*** *G* ***generated by*** *S, written $\langle S\rangle$, is defined to be*

$$\langle S\rangle = \bigcap_{S\subseteq H\leqslant G} H.$$

(Note that $S \subseteq G \leqslant G$ and so the above intersection is non-empty and well-defined.)

This definition takes care of both the existence and uniqueness of $\langle S\rangle$. Notice that $\langle H\rangle = H$ for any subgroup H of G, and of course $\langle G\rangle = G$. Indeed $\langle H\rangle = H$ for a subset $H \subseteq G$ implies H is a subgroup. Note also $\langle\emptyset\rangle = \{e\}$.

Example 5 *In S_3 (the symmetric group on three symbols, $\{1, 2, 3\}$) we have*

$$\begin{aligned}
\langle(12)\rangle &= \{e, (12)\};\\
\langle(123)\rangle &= \{e, (123), (132)\};\\
\langle(12), (123)\rangle &= S_3;\\
\langle(12), (23)\rangle &= S_3;\\
\langle(12), (13), (23)\rangle &= S_3;
\end{aligned}$$

Note, as the last of our examples here shows, generating sets need not be minimal, though often we would prefer minimal ones.

Example 6 *In the Abelian group $\mathbb{Z}$ under addition, $\langle k \rangle = k\mathbb{Z}$. We know that $\mathbb{Z}$ is cyclic (needing only a single generator, say 1 or -1), and hence all subgroups of $\mathbb{Z}$ are also cyclic. We note that $\langle 6, 9 \rangle = 3\mathbb{Z}$ and for general integers a, b we have $\langle a, b \rangle = h\mathbb{Z}$ where h is the highest common factor of a and b.*

We placed no restrictions on the cardinality of G or of X – the above definition works fine in all cases. However, we are often interested in whether S can be chosen to be finite.

Definition 7 *Let G be a group. We say that G is **finitely generated** if there exists a finite subset $S \subseteq G$ such that $\langle S \rangle = G$.*

Example 8

- *S_n is generated by (12) and $(123 \dots n)$.*
- *All finite groups are finitely-generated (for example by taking the group itself as a set of generators).*
- *Finitely-generated groups are countable as there are countably many words in a finite alphabet.*
- *$\mathbb{Q}$ is countable but not finitely generated.*
- *There are finitely-generated groups with subgroups that are not finitely generated.*

5 Free Groups

For any set S, we will define a group $F(S)$, known as the *free group on S*. Informally, one should view S as an 'alphabet', and elements of $F(S)$ as 'words' in this alphabet. So, for example, if $S = \{a, b\}$, then ab and ba are elements of $F(S)$. The group operation is 'concatenation'; in other words, to compose two words in $F(S)$, we simply write one down and then follow it by the other. For example, the product of ab and ba is $abba$.

The above discussion is somewhat oversimplified, because it does not take account of the fact that groups have inverses. So, whenever a is an element of S, we must allow not only a but a^{-1} to appear in the words. But then, $aa^{-1}b$ and b should

represent the same element of the group. So, in fact, elements of $F(S)$ are not words in the alphabet S, but are equivalence classes of words.

We are now ready to give the formal definitions. Throughout, S is some set, known as the *alphabet*. From this set, create a new set S^{-1}. This is a copy of the set S, but for each element x of S, we denote the corresponding element of S^{-1} by x^{-1}. We insist that $S \cap S^{-1} = \emptyset$. When $x^{-1} \in S^{-1}$, we say that $(x^{-1})^{-1} = x$.

Definition 9 *A **word** w is a finite sequence $x_1, \ldots, x_m$, where $m \geqslant 0$ and each $x_i \in S \cup S^{-1}$. We write w as $x_1 x_2 \ldots x_m$. Note that the empty sequence, where $m = 0$ is a word, denoted $\emptyset$.*

Definition 10 *A word w' is an **elementary contraction** of a word w if $w = y_1 x x^{-1} y_2$ and $w' = y_1 y_2$,for words y_1 and y_2, and some $x \in S \cup S^{-1}$.*

Definition 11 *A word is **reduced** if it does not admit an elementary contraction.*

Example 12 *Let F_2 denote the group freely generated by two elements a and b. Then the word $a^{-1}bb^{-1}aba^{-1}a$ reduces to b as*

$$a^{-1}bb^{-1}aba^{-1}a \quad \searrow \quad a^{-1}aba^{-1}a \quad \searrow \quad a^{-1}ab \quad \searrow \quad b.$$

Proposition 13 *(a) Any word w can be transformed into a reduced word by a sequence of elementary contractions.*

(b) If a word w can be transformed into reduced words w_1 and w_2 by elementary contractions then $w_1 = w_2$.

Proof (a) As an elementary contraction reduce's a word's length by two, then w is either reduced or it can be transformed to a shorter length word by an elementary contraction. As the length of the original word is finite, and all words have non-negative length, then this process must eventually terminate.

(b) Suppose that the word w can be transformed to the reduced words w_1 and w_2. This means there is a sequence of words

$$w_1 = \alpha_k \swarrow \alpha_{k-1} \swarrow \cdots \swarrow \alpha_2 \swarrow \alpha_1 \swarrow w \searrow \beta_1 \searrow \beta_2 \searrow \cdots \searrow \beta_{l-1} \searrow \beta_l = w_2$$

where $\searrow$ means "transforms into by means of an elementary contraction" and $\swarrow$ means "transforms from by means of an elementary contraction". We now prove the following technical lemma: ■

Lemma 14 *If α, β, γ are words such that $\alpha \swarrow \beta \searrow \gamma$ then either $\alpha = \gamma$ or there is a word δ such that $\alpha \searrow \delta \swarrow \gamma$.*

Proof Since $\alpha \swarrow \beta$, we can write $\alpha = ab$, and $\beta = axx^{-1}b$, for some $x \in S \cup S^{-1}$ and some words a and b. As $\beta \searrow \gamma$, then γ is obtained from β by removing yy^{-1}, for some $y \in S \cup S^{-1}$. The words xx^{-1} and yy^{-1} intersect in either zero, one or two letters. We will consider these three possibilities in turn. If they do not intersect, then it is possible to remove yy^{-1} from α before inserting xx^{-1}. Hence, if we denote by δ the word obtained by removing yy^{-1} from α, then $\alpha \searrow \delta \nearrow \gamma$, as required. Suppose now that xx^{-1} and yy^{-1} intersect in a single letter. Then $x = y^{-1}$, and so in β, there is chain of letters $xx^{-1}x$ or $x^{-1}xx^{-1}$, and α and γ are obtained from β by the two possible ways of performing an elementary contraction on these three letters. In particular, $\alpha = \gamma$, as required. Finally, if xx^{-1} and yy^{-1} intersect in two letters, then clearly, all we have done in the sequence $\alpha \swarrow \beta \searrow \gamma$ is to insert a pair of letters and then remove it again, and so $\alpha = \gamma$. ■

Proof (Continuation of the proof of Proposition 13) If $k = l$ and $\alpha_i = \beta_i$ for each i then $w_1 = w_2$. So if $w_1 \neq w_2$ then there is a first instance where $\alpha_i \neq \beta_i$ and without loss of generality we can assume that $i = 1$. By the above lemma we can replace our sequence with

$$w_1 = \alpha_k \swarrow \alpha_{k-1} \swarrow \cdots \swarrow \alpha_2 \swarrow \alpha_1 \searrow \delta \swarrow \beta_1 \searrow \beta_2 \searrow \cdots \searrow \beta_{l-1} \searrow \beta_l = w_2.$$

If $\delta = \alpha_2$ then we can omit α_1 and α_2 and if not by the lemma again there is ε such that

$$w_1 = \alpha_k \swarrow \alpha_{k-1} \swarrow \cdots \swarrow \alpha_2 \searrow \varepsilon \swarrow \delta \swarrow \beta_1 \searrow \beta_2 \searrow \cdots \searrow \beta_{l-1} \searrow \beta_l = w_2.$$

Proceeding in this way, applying the above lemma to both the left and the right of δ we are eventually left with a sequence where all the $\searrow$ arrows appear to the left of the $\swarrow$arrows so that

$$w_1 = \alpha_k \searrow \cdots \searrow \omega \swarrow \cdots \swarrow \beta_l = w_2.$$

But this would imply that either w_1 or w_2 is not reduced which is a contradiction. ■

Notation 15 *Given a word w we shall write $[w]$ for the unique reduced word into which w can be transformed by elementary contractions.*

Definition 16 *The **concatenation** of two words $x_1x_2\dots x_m$ and $y_1y_2\dots y_n$ is the word*

$$x_1x_2\dots x_my_1y_2\dots y_n.$$

Definition 17 *The **free group on the set** S, denoted $F(S)$, consists of the reduced words in the alphabet S. The composition of two reduced words w and w' is the reduced word $[ww']$ where ww' denotes the concatenation of w and w. The identity element is $\emptyset$, and is denoted e.*

Proof $F(S)$, as defined above, does indeed have a group structure. We clearly have a binary operation. If w, w', w'' are reduced words then

$$[[ww']\,w''] = [w\,[w'w'']]$$

as both are reduced words that are achievable by elementary contractions of $ww'w''$ and so equal by uniqueness. Thus we have associativity. $\emptyset$ clearly plays the role of the identity. Finally if $w = x_1\cdots x_n$ is a reduced word then so is $w^{-1} = x_n^{-1}\cdots x_1^{-1}$ and we have

$$\left[w^{-1}w\right] = \left[x_n^{-1}\cdots x_1^{-1}x_1\cdots x_n\right] = [\emptyset] = \emptyset; \qquad \left[ww^{-1}\right] = \left[x_1\cdots x_nx_n^{-1}\cdots x_1^{-1}\right] = [\emptyset] = \emptyset,$$

after n elementary contractions in each case. ■

Proposition 18 *Every non-trivial element of a free group has infinite order.*

Proof Let w be a reduced non-empty word. We may write w as $w_1w_2w_1^{-1}$ for words w_1 and w_2 with the property that the initial and final letters of w_2 are not mutual inverses. Then for any $n \geqslant 0$ we note $[w^n] = w_1w_2^nw_1^{-1}$ and so is non-trivial. ■

6 The Universal Mapping Property

Given a set S, there is a function $i\colon S \to F(S)$, known as the *canonical inclusion*, sending each element of S to the corresponding generator of $F(S)$. The following is known as the *universal mapping property* of free groups.

Theorem 19 *(**Universal Mapping Property**) Given any set S, any group G and any function $f\colon S \to G$, there is a unique homomorphism $\phi\colon F(S) \to G$ such that the following diagram commutes*

$$\begin{array}{ccc} S & \xrightarrow{f} & G \\ \downarrow i & \nearrow \phi & \\ F(S) & & \end{array}$$

where $i\colon S \to F(S)$ is the canonical inclusion.

Remark 20 *The map f assigns elements of the group G to elements of the alphabet S, so that a word in this alphabet S corresponds to some long calculation in G; the map ϕ is simply evaluation of this calculation in G.*

Proof Given any reduced word $w = x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$, where each $x_i \in S$ and each $\epsilon_i \in \{-1, 1\}$ we define $\phi(w)$ to be $f(x_1)^{\epsilon_1} \dots f(x_n)^{\epsilon_n}$. It is also clear that ϕ is a homomorphism and any elementary contractions involved in transforming a product $w_1 w_2$ to $[w_1 w_2]$ correspond to similar contractions in transforming $\phi(w_1)\phi(w_2)$ to $[\phi(w_1)\phi(w_2)]$. Finally, ϕ is the unique such homomorphism for which the diagram commutes. This is because for each $x \in S$, $\phi(x) = f(x)$, and a homomorphism between groups is determined by what it does to a set of generators. ■

- We say that $f\colon S \to G$ *induces* the homomorphism $\phi\colon F(S) \to G$.

The significance of the class of free groups among all groups is indicated by the following theorem.

Theorem 21 *Any group is isomorphic to a quotient of a free group.*

Proof Let G be a group and S a generating set for G. Let F be the free group on S and let $\theta\colon S \to G$ be the identity set map. By the definition of a free group, θ extends to a homomorphism $\theta\colon F \to G$. Then $F/\ker\theta \cong Im\theta = G$. ■

7 Presentations

Most undergraduates have come across groups described using *generators* and *relations*. A common example is the dihedral group D_{2n}, which is 'defined' as

$$\langle \sigma, \tau \mid \sigma^n = e, \tau^2 = e, \tau\sigma\tau = \sigma^{-1} \rangle.$$

The idea is that σ and τ generate the group, and the 'relations' of the group are given by the equalities on the right-hand side. These relations should be, in some sense, the 'only' ones that hold. However, very rarely is it explained precisely what this means! Of course, one is allowed to 'deduce' relations from the given ones. For example, if $\sigma^n = e$ and $\tau^2 = e$, then $\sigma^n\tau^2 = e$. However, there are slightly more subtle relations that also follow. For example, $\tau\sigma^n\tau$ is also the identity, since $\tau\sigma^n\tau = \tau e\tau = e$. So, it is clear that some more work must be done before one can specify a group using generations and relation, *with complete rigour*. It turns out that free groups play a central rôle in this process.

Definition 22 *Let B be a subset of a group G. The* ***normal subgroup generated by*** *B or* ***normal closure*** *is the smallest normal subgroup of G that contains B. We will denote it $\langle\langle B\rangle\rangle$.*

Remark 23 *The intersection of a collection of normal subgroups is again a normal subgroup. Hence, $\langle\langle B\rangle\rangle$ is normal in G. It is therefore the smallest normal subgroup of G that contains B, in the sense that any other normal subgroup that contains B also contains $\langle\langle B\rangle\rangle$.*

It can be specified quite precisely, as follows.

Proposition 24 *For $B \subseteq G$ we have*

$$\langle\langle B\rangle\rangle = \langle g^{-1}bg : g \in G,\, b \in B\rangle$$

or more explicitly precisely $\langle\langle B\rangle\rangle$ consists of all expressions of the form

$$\prod_{i=1}^{n} g_i b_i^{\epsilon_i} g_i^{-1},$$

where $n \geqslant 0$, $g_i \in G$, $b_i \in B$ and $\epsilon_i = \pm 1$, for all i.

Proof Any normal subgroup containing B must contain all elements of the form gbg^{-1} and $gb^{-1}g^{-1}$ ($b \in B$, $g \in G$). Hence, it must contain all finite products of these:

$$\prod_{i=1}^{n} g_i b_i^{\epsilon_i} g_i^{-1}.$$

Let N be the set of all these finite products. We have therefore shown that $N \subseteq \langle\langle B\rangle\rangle$. We will show that N is in fact a normal subgroup; it clearly contains B, and so we would then have $\langle\langle B\rangle\rangle \subseteq N$ proving the proposition. To show that N is a normal subgroup, we check the various conditions:

- *Identity:* N clearly contains e.
- *Inverses:* The inverse of $\prod_{i=1}^{n} g_i b_i^{\epsilon_i} g_i^{-1}$ is $\prod_{i=n}^{1} g_i b_i^{-\epsilon_i} g_i^{-1}$, which also lies in N.
- *Closure:* The product of two elements in N clearly lies in N.

- *Normality:* For $\prod_{i=1}^{n} g_i b_i^{\epsilon_i} g_i^{-1}$ in N and $g \in G$,

$$g\left(\prod_{i=1}^{n} g_i b_i^{\epsilon_i} g_i^{-1}\right) g^{-1} = \prod_{i=1}^{n} (gg_i) b_i^{\epsilon_i} (g_i^{-1} g^{-1}) = \prod_{i=1}^{n} (gg_i) b_i^{\epsilon_i} (gg_i)^{-1},$$

  which lies in N.

■

We can now specify what it means to define a group via generators and relations. The generators will come from a set X. The relations will be words in X, which we can view as instructions that force these words to be the identity in the group. The precise definition is as follows.

Definition 25 *Let X be a set, and let R be a collection of elements of $F(X)$. The group with presentation $\langle X \mid R \rangle$ is defined to be $F(X)/\langle\langle R \rangle\rangle$.*

Definition 26 *Let G be a group. If $S \subseteq G$ and R is a set of reduced words in $S \cup S^{-1}$ such that $G = \langle S \mid R \rangle$, then we say $\langle S \mid R \rangle$ is a **presentation** of G.*

We sometimes slightly abuse notation by allowing relations of the form '$w_1 = w_2$', where this is shorthand for the relation $w_1 w_2^{-1}$.

Example 27 *We can now genuinely define the dihedral group D_{2n} to be*

$$\langle \sigma, \tau \mid \sigma^n, \tau^2, \tau\sigma\tau\sigma \rangle.$$

It is less than apparent from this definition that D_{2n} contains $2n$ elements. However the relation $\tau\sigma\tau\sigma$ can be rearrange to $\tau\sigma = \sigma\tau^{-1}$. We can see that this relation can be used to reduce any word in σ and τ to one of the form $\sigma^s\tau^t$. Because of the relations σ^2 and τ^n we can assume that $0 \leqslant s \leqslant 1$ and $0 \leqslant t < n$. A simple check shows that these $2n$ words represent distinct elements of the group.

Example 28

- $\langle x \mid \varnothing \rangle \cong \mathbb{Z}$.
- $\langle x \mid x^a = x^b = e \rangle \cong \{e\}$ *if a and b are coprime.*
- $\langle x, y \mid x^2 = y^2 = e,\ xy = yx \rangle \cong C_2 \times C_2$.

Example 29 *Determine the order of the group*

$$G = \langle a, b \,|\, a^4 = e,\ a^2 = b^2,\ b^{-1}ab = a^{-1} \rangle.$$

From these relations we can see that $ab = ba^{-1} = ba^3$ *and so every word in* a *and* b *can be put in the form* $b^j a^i$*. Further as* $a^2 = b^2$ *and* $a^4 = e$ *we can assume that* $0 \leqslant j \leqslant 1$ *and* $0 \leqslant i \leqslant 3$*. We then have*

$$G = \{e, a, a^2, a^3, b, ba, ba^2, ba^3\}$$

and we can see that the relations cannot be further used to equate any of these elements. So $|G| = 8$*. In fact this is the quaternion group* Q_8*. By way of showing how products can be calculated note*

$$\begin{aligned} (ba)(ba^3) &= b(ab)a^3 = b(ba^3)a^3 = b^2a^6 = a^8 = e. \\ (a^2)(ba) &= a(ab)a = a(ba^3)a = (ab)a^4 = (ba^3). \end{aligned}$$

Do not get however the wrong idea that one can always determine the order of a group given a presentation of the group. The Adian-Rabin theorem, proved in the 1950s, implies that there is no algorithm that, given any presentation, will be able to determine whether the associated group is trivial or not: it is an *undecidable problem!*

We now show that any group G has a presentation. Let $F(G)$ be the free group on the generating set G. Thus, $F(G)$ consists of all reduced words in the alphabet G. There is a canonical homomorphism $F(G) \to G$ sending each generator of $F(G)$ to the corresponding element of G, which is clearly surjective. Let $R(G)$ be the kernel of this homomorphism. Then, by the First Isomorphism Theorem for groups, G is isomorphic to $F(G)/R(G)$. Hence, G has presentation $\langle G \,|\, R(G) \rangle$.

Definition 30 *The* ***canonical presentation*** *for* G *is* $\langle G \,|\, R(G) \rangle$*.*

The canonical presentation of a group is extremely inefficient. Its main rôle comes from the fact that it depends only on the group G and involves no arbitrary choices.

The following result allows us to check whether a function from a group $\langle X \,|\, R \rangle$ to another group is a homomorphism.

Lemma 31 *Let* $\langle X \,|\, R \rangle$ *and* H *be groups. Let a map* $f \colon X \to H$ *induce a homomorphism* $\phi \colon F(X) \to H$*. This descends to a homomorphism* $\langle X \,|\, R \rangle \to H$ *if and only if* $\phi(r) = e$ *for all* $r \in R$*.*

Proof Clearly, the condition that $\phi(r) = e$ is necessary for ϕ to give a homomorphism, since any $r \in R$ represents the identity element of $\langle X|R\rangle$. Conversely, suppose that $\phi(r) = e$ for all $r \in R$. Any element w of $\langle\langle R\rangle\rangle$ can be written as

$$\prod_{i=1}^{n} w_i r_i^{\epsilon_i} w_i^{-1},$$

where $n \geqslant 0$, $w_i \in F(X)$, $r_i \in R$ and $\epsilon_i = \pm 1$, for all i. Since $\phi(r) = e$ for all $r \in R$, $\phi(w)$ is also e. Hence, ϕ descends to a homomorphism $F(X)/\langle\langle R\rangle\rangle \to H$, as required. ■

Part III
Isomorphism Theorems. Simple Groups

8 The First Isomorphism Theorem

Recall that a map of groups $\phi\colon (G_1, *) \to (G_2, \circ)$ is called a *homomorphism* if it preserves the group operation:

$$\phi(g * h) = \phi(g) \circ \phi(h) \qquad \text{for all } g, h \in G_1,$$

and ϕ is called an *isomorphism* if it is bijective. The *kernel*

$$\ker \phi = \{g \in G \,|\, \phi(g) = e\}$$

is a subgroup and in fact a normal subgroup of G_1. The *image*

$$Im\phi = \{\phi(g) \in G_2 \,|\, g \in G_1\}$$

is a subgroup of G_2.

Given a normal subgroup N of a group G there is a natural *quotient homomorphism*

$$q\colon G \to G/N \qquad \text{defined by} \qquad q(g) = gN.$$

Note that $\ker q = N$, and q is surjective. Conversely, we have:

Theorem 32 ***(The First Isomorphism Theorem)*** *Given a homomorphism $\phi\colon G_1 \to G_2$, there is a well-defined isomorphism*

$$G_1/\ker\phi \xrightarrow{\cong} \mathrm{Im}\phi, \qquad \textit{given by} \qquad g\ker\phi \mapsto \phi(g)$$

and the map ϕ factors into the canonical quotient map $G_1 \to G_1/\ker\phi$, the above isomorphism, and the inclusion $\mathrm{Im}\phi \to G_2$.

Example 33 *Let $G_1 = D_8 = \langle \sigma, \tau \,|\, \sigma^4 = \tau^2 = e,\ \sigma^{-1}\tau = \tau\sigma \rangle$ and $G_2 = C_2 \times C_2 = \langle g \rangle \times \langle h \rangle$. As a set*

$$G_1 = \left\{e, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\right\}.$$

The map $\phi\colon D_8 \to C_2 \times C_2$ *determined by*

$$\phi(\sigma) = g, \qquad \phi(\tau) = h,$$

is a well-defined homomorphism by Lemma 31 as

$$\phi(\sigma^4) = g^4 = e, \qquad \phi(\tau^2) = h^2 = e, \qquad \phi(\tau\sigma\tau\sigma) = ghgh = g^2h^2 = e.$$

The kernel of ϕ *equals* $\langle\sigma^2\rangle$ *and the First Isomorphism Theorem shows that*

$$D_8/\langle\sigma^2\rangle \cong C_2 \times C_2.$$

Example 34 *Let* $G_1 = S_4$ *and* $G_2 = S_3$*. Then* $a = (12)$ *and* $b = (234)$ *generate* S_4 *and a presentation for* S_4 *is*

$$S_4 = \langle a, b \,|\, a^2 = b^3 = e, (ab)^4 = e\rangle.$$

There is a well-defined homomorphism $\phi\colon S_4 \to S_3$ *induced by* $\phi(a) = (12)$ *and* $\phi(b) = (321)$ *by Lemma 31 as*

$$\phi\left(a^2\right) = (12)^2 = e, \qquad \phi\left(b^3\right) = (321)^3 = e, \qquad \phi\left((ab)^4\right) = ((12)(321))^4 = (13)^4 = e.$$

As (12) *and* (321) *generate* S_3 *then* ϕ *is onto and so* $|\ker\phi| = 24/6 = 4$*. Hence* $\ker\phi = V_4$ *and we have* $S_4/V_4 \cong S_3$*.*

9 The Second and Third Isomorphism Theorems

Lemma 35 *Let* G *be a group,* $H \leqslant G$ *and* $N \lhd G$*. The set* $HN = \{hn \,|\, h \in H, n \in N\}$ *is a subgroup of* G*.*

Proof Clearly $e = ee \in HN$. For $h \in H, n \in N$,

$$nh = h(h^{-1}nh) \in HN.$$

Hence $h_1n_1h_2n_2 \in HN$ and $(hn)^{-1} = n^{-1}h^{-1} \in HN$. ■

Theorem 36 ***(The Second Isomorphism Theorem)*** *Let* G *be a group, and* H, N *subgroups of* G *with* $N \lhd G$*. Then* $H \cap N \lhd H$ *and there is an isomorphism*

$$\frac{HN}{N} \cong \frac{H}{H \cap N}.$$

Proof The first statement follows from the fact that both N and H are closed under conjugation by elements of H. For the second, consider the composition

$$H \longrightarrow HN \to HN/N$$

where the first arrow is the inclusion and the second one is the quotient map. This composition is surjective with kernel $H \cap N$. Now apply the First Isomorphism Theorem. ■

Example 37 *Let $G = S_4$, $H = S_3 = \mathrm{Sym}(\{1,2,3\}) \leqslant S_4$ and $N = V_4 \lhd S_4$. Then $HN = S_4$ and $H \cap N = \{e\}$ so that the Second Isomorphism Theorem gives*

$$S_4/V_4 \cong S_3.$$

Theorem 38 ***(The Third Isomorphism Theorem)*** *Let N, K be normal subgroups of a group G, with $K \subseteq N$. Then $N/K \lhd G/K$ and there is an isomorphism*

$$(G/K)/(N/K) \cong G/N.$$

Proof To show the first statement, we note, for $g \in G$ and $n \in N$,

$$(gK)^{-1}(nK)(gK) = g^{-1}KnKgK = g^{-1}ngK \in N/K$$

since K is normal in G. To see the isomorphism, consider the composition of the quotient maps

$$G \longrightarrow G/K \longrightarrow (G/K)/(N/K).$$

As a composition of surjective maps, this is surjective, with kernel N. Now apply the First Isomorphism Theorem again. ■

Example 39 *Let $G = S_4$, $N = A_4 \lhd S_4$ and $K = V_4 \lhd S_4$. Then $G/K \cong S_3$ and $N/K \cong A_3$ so that the Third Isomorphism Theorem gives*

$$(S_4/V_4)/(A_4/V_4) \cong S_3/A_3 \cong C_2.$$

The first statement of the Third Isomorphism Theorem has a converse.

Proposition 40 *Let $K \lhd G$. Denote $\bar{G} = G/K$ and let $\bar{H} \leqslant \bar{G}$. Then*

$$H = \{h \in G \,|\, hK \in \bar{H}\}$$

is a subgroup of G, containing K as a normal subgroup, with $H/K = \bar{H}$. If $\bar{H}$ is normal in $\bar{G}$, then H is normal in G.

Proof This is left to Sheet 1, Exercise 1. ■

Corollary 41 *Given $K \lhd G$, there is a one-to-one correspondence*

$$H \mapsto \bar{H} = H/K$$

between subgroups of G containing K, and subgroups of G/K, which preserves normal subgroups.

Example 42 *Note that $V_4 \lhd S_4$ and that $S_4/V_4 \cong S_3$. In this case the above corollary is demonstrated by noting*

$$V_4/V_4 \cong \{e\}, \qquad A_4/V_4 \cong A_3 \qquad S_4/V_4 \cong S_3.$$

10 Simple Groups

Recall that a non-trivial group G is called *simple* if it has no non-trivial proper normal subgroups. In a sense – to be made more rigorous in the next chapter – the simple groups are the building blocks for general finite groups.

The symmetric group S_n of degree n is one of the first examples of a group that one meets, as the group of permutations of n objects. One learns quickly that S_n is interesting partly because it is not Abelian. Note for $n \geqslant 3$ that S_n is not simple: it has a subgroup of index 2, which is of course non-trivial, proper and normal. This subgroup is also well-known to us as the alternating group A_n i.e. the subgroup of even permutations.

For small n, these groups A_n are easily identified: both A_1 and A_2 are trivial and A_3 is cyclic of order 3; of these, only A_3 is simple (but it is Abelian). The group A_4 is a little more interesting: it has order $4!/2 = 12$ and is not Abelian. It is not simple as $V_4 = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ is a normal subgroup. However the alternating groups A_n *are* simple for $n \geqslant 5$. We shall prove this only for the case $n = 5$.

Theorem 43 *The alternating group of degree 5, A_5, is a simple group, of order 60.*

We begin by studying the conjugacy classes of A_5. Two permutations that are conjugate in A_5 are conjugate in S_5 and so of the same cycle type, but the converse does not follow.

Lemma 44 *The conjugacy classes of A_5 are:*

(a) the identity;

(b) all twenty 3-cycles;

(c) all fifteen double-transpositions;

(d) twelve (half) of the 5-cycles;

(e) twelve (half) of the 5-cycles, these being the squares of those in (d).

Proof (a) The identity commutes with every other element and so is conjugate only to itself.

(b) Let $\sigma = (123)$ and τ be two 3-cycles. There is an element $\rho \in S_5$ such that $\rho^{-1}\tau\rho = \sigma$. If ρ is odd then we can use $\rho\,(45)$ instead which is even. Hence all the 3-cycles are conjugate in A_5.

(c) Let $\sigma = (12)\,(34)$ and τ be two double-transpositions. There is an element $\rho \in S_5$ such that $\rho^{-1}\tau\rho = \sigma$. If ρ is odd then we can use $\rho\,(34)$ instead which is even. Hence all the double transpositions are conjugate in A_5.

(d) All 24 5-cycles are in A_5. These cannot form a single conjugacy class in A_5 as 24 does not divide 60. Given a 5-cycle, say $\sigma = (12345)$, then clearly $e, \sigma, \sigma^2, \sigma^3, \sigma^4$ all commute with σ. On the other hand if $\rho \in A_5$ commutes with σ then

$$(1\rho\, 2\rho\, 3\rho\, 4\rho\, 5\rho) = \rho^{-1}\,(12345)\,\rho = (12345)$$

and we see ρ is entirely determined by the choice of 1ρ. Hence only these 5 powers of σ commute with σ. It follows that σ has $60/5 = 12$ conjugates in A_5.

(e) Let $\sigma = (12345)$. Say that ρ is such that

$$(1\rho\, 2\rho\, 3\rho\, 4\rho\, 5\rho) = \rho^{-1}\,(12345)\,\rho = (13524) = \sigma^2.$$

If $1\rho = 1$ then $2\rho = 3$,... and we see $\rho = (2354)$, which is odd.
If $1\rho = 3$ then $2\rho = 5$,... and we see $\rho = (1325)$, which is odd.
If $1\rho = 5$ then $2\rho = 2$,... and we see $\rho = (1534)$, which is odd.
If $1\rho = 2$ then $2\rho = 4$,... and we see $\rho = (1243)$, which is odd.
If $1\rho = 4$ then $2\rho = 1$,... and we see $\rho = (1452)$, which is odd.

Hence σ is not conjugate to σ^2 *in* A_5. ■

Proof (Proof of Theorem) The possible orders of a proper non-trivial normal subgroup are proper factors of 60. If a normal subgroup contains a 5-cycle σ it must contain its 12 conjugates, but also its square σ^2 and its 12 conjugates, so all 24 in fact. Thus any normal subgroup must have an order which is a sum of numbers from

$$1, \quad 20, \quad 15, \quad 24,$$

and must include the 1. We can quickly see combinatorially that this is not possible – a choice of two of the larger numbers takes us past 30 and a choice of just one does not give us a factor of 60. Hence A_5 is simple. ■

In fact A_5 is, up to isomorphism, the only simple group of order 60, and is the smallest non-abelian simple group. In the next section we shall see that all finite groups are in some (nontrivial!) sense composed of simple groups. Thus the Classification of Finite Simple Groups, now complete, was a major and crucial success, a result coming from numerous mathematicians working over decades. The classification shows that:

Theorem 45 *(**The Classification of Finite Simple Groups**) Let G be a finite simple group. Then G is isomorphic to one of the following.*

(i) A cyclic group of prime order C_p.

(ii) A group A_n for $n > 4$.

(iii) A finite group of Lie type *such as* $\mathrm{PSL}(n, q)$ *for $n > 2$ or $q > 3$.*

(iv) An explicit list of 26 sporadic groups*, including as largest the* Monster *and* Baby Monster *of orders $\sim 8 \cdot 10^{53}$ and $\sim 4 \cdot 10^{33}$ respectively.*

Part IV
Composition series. Jordan–Hölder Theorem

Informally, a series for a group G is a sequence of nested subgroups of G. Here we study *composition series*; a group may have many such series but the Jordan–Hölder theorem tells us something of the invariants of such series and might be thought of as a "unique factorization" theorem. One should be wary of trusting this viewpoint too much as we shall see that different (i.e. non-isomorphic) groups can have the same "factorization" in some sense.

Definition 46 *A **composition series** for a group G is a sequence of subgroups*

$$\{e\} \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$$

*such that each **composition factor** G_{i+1}/G_i simple (or equivalently each G_i is a maximal proper normal subgroup of G_{i+1}).*

Proposition 47 *Let G be a finite non-trivial group. Then G possesses a composition series.*

Proof We shall prove this by induction on $|G|$, the case of groups of small order being clear. Let $H \lhd G$ be a maximal normal subgroup, a normal subgroup of G not equal to G which is not contained in any larger normal subgroup. Then G/H is simple by Corollary 41 above. If H is not trivial, apply the inductive hypothesis to H. ■

Example 48 • *C_{12} has several composition series, for example*

$$\{e\} \lhd C_2 \lhd C_4 \lhd C_{12}; \qquad \{e\} \lhd C_3 \lhd C_6 \lhd C_{12}; \qquad \{e\} \lhd C_2 \lhd C_6 \lhd C_{12},$$

thinking of $C_2 = \langle g^6 \rangle$, $C_3 = \langle g^4 \rangle$, $C_4 = \langle g^3 \rangle$, $C_6 = \langle g^2 \rangle$ where g is a generator of C_{12}. Note that the composition factors are respectively

$$C_2,\, C_2,\, C_{3,} \qquad C_3,\, C_2,\, C_{2,} \qquad C_2,\, C_3,\, C_{2,}.$$

- *A_4 has three composition series, all of the form*

$$\{e\} \lhd C_2 \lhd V_4 \lhd A_4$$

with composition factors C_2, C_2, C_3 also. (There are three choices of subgroups of V_4 that are isomorphic to C_2.)

- *$\mathbb{Z}$ does not have a composition series.*

Example 48 is suggestive of a special property of composition series: the set of composition factors of C_{12} is the same for all three series. In fact this turns out to be true for any finite group. This is the celebrated *Jordan–Hölder theorem.*

Theorem 49 ***(Jordan–Hölder theorem)*** *Let G be a finite group. Then all composition series of G have the same length and, moreover, have the same composition factors, including multiplicities, in some order.*

Proof (**Off-Syllabus**, but included here for completeness.) Let us introduce some terminology, to help simplify the proof of the theorem. We will say two composition series of a group G are *equivalent* if they have the same composition factors, including multiplicities. So we want to prove that any two composition series for a finite group G are equivalent.

Let

$$\{e\} \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_{r-1} \lhd G_r = G \tag{1}$$

and

$$\{e\} \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_{s-1} \lhd H_s = G \tag{2}$$

be two composition series of G. We will proceed by induction on r. If $r = 1$ then $G/\{e\} = G$ is simple and $\{e\} \lhd G$ is its only composition series. So, let $r > 1$ and assume that the theorem holds for any group having some composition series of length less than r.

If $G_{r-1} = H_{s-1}$ then G_{r-1} has two composition series

$$\{e\} \lhd G_1 \lhd \cdots \lhd G_{r-1}, \qquad \{e\} \lhd H_1 \lhd \cdots \lhd H_{s-1} = G_{r-1},$$

of length $r-1$ and $s-1$ respectively. By the inductive hypothesis, $r-1 = s-1$ and these two composition series of G_{r-1} are equivalent. Hence $r = s$ and $G/G_{r-1} \cong G/H_{s-1}$ so (1) and (2) are equivalent.

If $G_{r-1} \neq H_{s-1}$, since $G_{r-1} \lhd G$ and $H_{s-1} \lhd G$, we have $G_{r-1}H_{s-1} \lhd G$. But G/G_{r-1} is simple so we cannot have $G_{r-1} \lhd H_{s-1}$, else H_{s-1}/G_{r-1} is a non-trivial

proper normal subgroup of G/G_{r-1}. Therefore we must have $H_{s-1} < G_{r-1}H_{s-1}$, but since G/H_{s-1} is simple, we must have that $G_{r-1}H_{s-1}$ is equal to G. Let $K = G_{r-1} \cap H_{s-1} \lhd G$. By the Second Isomorphism Theorem, we have $G/G_{r-1} \cong H_{s-1}/K$ and $G/H_{s-1} \cong G_{r-1}/K$ and so G_{r-1}/K and H_{s-1}/K are simple.

Now K is finite so certainly has a composition series

$$\{e\} \lhd K_1 \lhd K_2 \lhd \cdots \lhd K_{t-1} \lhd K_t = K.$$

Then

$$\{e\} \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_{r-2} \lhd G_{r-1} \tag{3}$$

and

$$\{e\} \lhd K_1 \lhd K_2 \lhd \cdots \lhd K_{t-1} \lhd K \lhd G_{r-1} \tag{4}$$

are composition series of G_{r-1} of length $r-1$ and $t+1$ respectively. By the inductive hypothesis, $t = r-2$ and (3) is equivalent to (4). Similarly we have composition series

$$\{e\} \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_{s-2} \lhd H_{s-1} \tag{5}$$

and

$$\{e\} \lhd K_1 \lhd K_2 \lhd \cdots \lhd K_{t-1} \lhd K \lhd H_{s-1} \tag{6}$$

of H_{s-1} of length $s-1$ and $t+1 = r-1$ respectively, so again by the inductive hypothesis $r = s$ and (5) and (6) are equivalent.

Finally, since $G_{r-1}/K \cong G/H_{s-1} = G/H_{r-1}$ and $H_{r-1}/K \cong G/G_{r-1}$, we see that the composition series

$$\{e\} \lhd K_1 \lhd K_2 \lhd \cdots \lhd K_{t-1} \lhd K \lhd G_{r-1} \lhd G \tag{7}$$

and

$$\{e\} \lhd K_1 \lhd K_2 \lhd \cdots \lhd K_{t-1} \lhd K \lhd H_{s-1} \lhd G \tag{8}$$

are equivalent. So since (3) and (4) are equivalent, and (5) and (6) are equivalent, then (1) and (7) are equivalent and (2) and (8) are equivalent. Now since (7) and (8) are equivalent, (1) and (2) are equivalent. ■

Remark 50

- *Note that the composition factors of C_6 and S_3 are both C_2, C_3. Thus there exist non-isomorphic groups having the same composition factors including multiplicities.*
- *If G is finite and abelian then its composition factors must also be and so must be cyclic of prime order.*

- *Let G be a finite group and let $H \lhd G$. If $X_1, \ldots, X_r$ are the composition factors of H and $Y_1, \ldots, Y_s$ are the composition factors of G/H, then the composition factors of G are $X_1, \ldots, X_r, Y_1, \ldots, Y_s$.*
- *Let X and Y be non-Abelian finite simple groups, and let $G = X \times Y$. Then the only two composition series of G are*

$$\{e\} \lhd X \times \{e\} \lhd X \times Y \qquad \text{and} \qquad \{e\} \lhd \{e\} \times Y \lhd X \times Y.$$

Example 51 *The composition factors of A_4 are C_2, C_2, C_3 and of A_5 are just A_5.*

Example 52 *All five groups of order 8 has composition factors C_2, C_2, C_2.*

Example 53 *Note that applying the result to the finite group C_m for a positive integer m gives the Fundamental Theorem of Arithmetic.*

Part V
Solvable Groups

Definition 54 *A finite group G is said to be **solvable** (or in older terminology, **soluble**), if every composition factor of G is a cyclic group of prime order.*

Remark 55 *Note that the above definition – for finite groups – is equivalent to requiring that the group have a composition series whose composition factors are abelian. We might more generally say that a group (finite or infinite) is solvable if it has a subnormal series with abelian (and not necessarily simple) composition factors.*

The terminology comes from Galois theory, and in particular the following theorem: given a polynomial $f \in \mathbb{Q}[x]$, there is a group associated to f, its *Galois group* G, which permutes the roots of f. The roots of f can be expressed by radical expressions in rational numbers if and only if G is solvable.

Example 56

- *All finite abelian groups are solvable.*
- *S_4 is solvable as $\{e\} \lhd C_2 \lhd V_4 \lhd A_4 \lhd S_4$ with composition factors C_2, C_2, C_3, C_2*
- *Groups of order p^a where p is prime are solvable – see Sheet 2, Exercise 5.*

Two (very off-syllabus) significant theorems relating to solvable groups are:

Theorem 57 *(**Burnside's $p^\alpha q^\beta$ theorem**) If p and q are primes then any group of order $p^\alpha q^\beta$, $\alpha, \beta \in \mathbb{N}$, is solvable.*

However, there exist groups whose orders are divisible by only three distinct primes that are not solvable (for example, A_5).

Theorem 58 *(**Feit–Thompson**) All finite groups of odd order are solvable.*

One significant consequence of this result is that the only finite simple groups of odd order are cyclic of prime order.

Theorem 59 *Let G be finite.*

(i) If $N \lhd G$, and both N and G/N are solvable, then so is G.

(ii) If G is solvable, then any subgroup of G is solvable.

(iii) If G is solvable, then any quotient group of G is solvable.

Proof To prove (i), we'll show that the composition factors of G are those of N and G/N put together. To see this, let

$$\{e\} = \bar{K}_0 \lhd \bar{K}_1 \lhd \cdots \lhd \bar{K}_n = G/N$$

be a composition series for G/N with abelian factors, and let

$$\{e\} = N_0 \lhd N_1 \lhd \cdots \lhd N_k = N$$

be one for N. The subgroups $\bar{K}_i \leqslant G/N$ correspond, by Corollary 41, to subgroups $K_i \leqslant G$ containing N, and there are isomorphisms

$$K_i/K_{i+1} \cong (K_i/N)/(K_{i+1}/N) = \bar{K}_i/\bar{K}_{i+1}$$

by the Third Isomorphism Theorem. Hence we get a composition series

$$\{e\} = N_0 \lhd N_1 \lhd \cdots \lhd N_k = N = K_0 \lhd K_1 \lhd \cdots \lhd K_n = G.$$

with abelian factors. To show (ii), let $\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ be a composition series for G, and for a subgroup $H \leqslant G$, let $H_i = G_i \cap H$. Then clearly $H_i \lhd H_{i+1}$. Now apply the Second Isomorphism Theorem to get

$$H_{i+1}/H_i = H_{i+1}/(H_{i+1} \cap G_i) \cong H_{i+1}G_i/G_i$$

which is a subgroup of G_{i+1}/G_i, an abelian group of prime order. Hence H_{i+1}/H_i is either trivial (so that $H_i = H_{i+1}$ and one of these may be omitted) or abelian of prime order itself. Thus H is solvable.

(iii) Assume G is solvable with composition series $\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$, and $N \lhd G$. Let $N_i = NG_i/N$. It is easy to check that $N_i \lhd N_{i+1}$ and that there is a natural surjective map

$$G_{i+1}/G_i \to (NG_{i+1}/N)/(NG_i/N) = N_{i+1}/N_i.$$

Hence N_{i+1}/N_i is a quotient of the cyclic abelian group G_{i+1}/G_i, and hence it is cyclic abelian or trivial. Thus N is solvable. ■

Corollary 60 *For $n > 4$, the symmetric group S_n is not solvable.*

Continuing with our preview of Galois theory, this implies that the roots of a general polynomial of degree $n > 4$ are not expressible using radical expressions.

An alternative definition of solvable groups is via the **derived subgroup** and the **derived series**.

Definition 61 *Let G be a group. The **derived subgroup** or **commutator subgroup** of G is the subgroup*

$$G' = [\,G, G\,] = \langle a^{-1}b^{-1}ab \,|\, a,\, b \in G\rangle.$$

We commonly write $[a, b]$ for the commutator $a^{-1}b^{-1}ab$.

Example 62 *G is abelian if and only if $G' = \{e\}$.*

Example 63 $(S_n)' = A_n$.

Proof Certainly it is the case that $[a, b]$ is even for any $a, b \in S_n$ and so $[a, b] \leqslant A_n$. On the other hand when $a = (12)$ and $b = (13)$ we see

$$[a, b] = (12)(13)(12)(13) = (123)(123) = (132).$$

From similar calculations we can see that all 3-cycles are in $(S_n)'$ and the 3-cycles generate A_n. ■

Some elementary properties of commutator subgroups are useful:

Lemma 64 *Let G be a group.*

(i) $G' \lhd G$

(ii) If $H \lhd G$ and G/H is Abelian then $G' \leqslant H$.

(iii) Conversely, if $G' \leqslant H \leqslant G$ then $H \lhd G$ and G/H is Abelian.

(iv) If $H \lhd G$ then $H' \lhd G$.

Proof (i) We have $G' \leqslant G$ as it is by definition the subgroup generated by the commutators. Further it is a normal subgroup as

$$g^{-1}[a, b]g = g^{-1}a^{-1}b^{-1}abg = (g^{-1}a^{-1}g)(g^{-1}b^{-1}g)(g^{-1}ag)(g^{-1}bg) = [g^{-1}ag, g^{-1}bg], \tag{9}$$

with a similar calculation being true for the conjugates of words in the commutators. (ii) and (iii) are left to Sheet 2, Exercise 2. (iv) is a reapplication of (9). ■

The *derived series* arises out of repeated taking of commutator subgroups.

Definition 65 *Let G be a finite group. Set $G^{(0)} = G$ and for $k \geqslant 1$, define $G^{(k)} = (G^{(k-1)})'$. The series $G = G^{(0)} \geqslant G^{(1)}$ $(= G'^{(2)} \geqslant \cdots$ is called the* ***derived series*** *of G. By the preceding lemma, each $G^{(k)}$ is normal in G and $G^{(k-1)}/G^{(k)}$ is Abelian so the composition factors are abelian.*

Definition 66 *If the derived series is of finite length and $k \geqslant 0$ is the first instance that $G^{(k)} = \{e\}$, then k is known as the* ***derived length*** *of G.*

We can now prove the following theorem.

Theorem 67 *Let G be a finite group. Then the following are equivalent:*

1. *the derived length of G is finite, i.e. there exists $k \in \mathbb{N}$ such that $G^{(k)} = \{e\}$;*
2. *G has a subnormal series with Abelian factors, i.e. G is solvable.*

Proof $1 \Rightarrow 2$ follows from the classification of finite abelian groups. It remains to prove $2 \Leftarrow 1$. Suppose $\{e\} = G_r \lhd G_{r-1} \lhd \cdots \lhd G_0 = G$ is a subnormal series for G with Abelian factors (note the numbering is the reverse of our usual one). To show the existence of k with $G^{(k)} = \{e\}$, it suffices to show that $G^{(i)} \leqslant G^i$ for each i, as then $G^{(r)} \leqslant G_r = \{e\}$. We work by induction on i.

For $i = 0$, $G^{(0)} = G = G_0$, so this our base case. Now let $i \geqslant 1$ and assume by the inductive hypothesis that $G^{(i-1)} \leqslant G^{i-1}$. Then $G^{(i)} = (G^{(i-1)})' \leqslant (G_{i-1})'$ and $(G_{i-1})' \leqslant G_i$ (by Lemma 64), since G_{i-1}/G_i is Abelian. ■

Example 68

- *The derived series for S_4 is*

$$S_4 \rhd A_4 \rhd V_4 \rhd \{e\}\,.$$

- *The derived series for S_n where $n > 4$ is*

$$S_n \rhd A_n \rhd A_n \rhd \cdots$$

Part VI
Semi-direct Products

Given two groups G_1 and G_2 it is always possible to make their *direct product* $G_1 \times G_2$. However, algebraically, this is rather uninteresting as essentially no interaction goes on between the two groups. We also know that most groups are not the direct product of any pair of their subgroups. So we might try to better understand cases where a group is of the form $G = G_1G_2$ and each g can be written uniquely as g_1g_2 where $g_1 \in G_1$, $g_2 \in G_2$.

Say then that a group G has two subgroups G_1 and G_2 such that $G = G_1G_2$. Since $g_1g_2 = g_1'g_2'$ if and only if $g_1^{-1}g_1' = g_2g_2'^{-1}$ and the latter belongs to $G_1 \cap G_2$, we see that the expression $g = g_1g_2$ will always be unique if and only if $G_1 \cap G_2 = \{e\}$. However when we try to understand a product

$$g_1g_2 * \tilde{g}_1\tilde{g}_2,$$

it is rather unclear how we might express this as the product of an element in G_1 with an element in G_2. We can get around this problem if one of the factors G_1 or G_2 is a normal subgroup. Hence we define:

Definition 69 *Let G be a group, $H \leqslant G$ and $N \lhd G$. We say G is an **internal semi-direct product** of H and N, denoted*

$$G = N \rtimes H,$$

if $G = NH$ and $H \cap N = \{e\}$.

Example 70 *Here are some examples.*

- *Any direct product $G = N \times H$; in this case, both $\{e\} \times H$ and $N \times \{e\}$ are normal in G.*
- *$G = D_{2n}$, the dihedral group, $N = \langle\sigma\rangle$ is the group of rotations, $H = \langle\tau\rangle$ is any subgroup generated by a reflection.*
- *$G = S_n$, $N = A_n$ and H is any subgroup generated by a transposition.*
- *$G = S_4$, $H = S_3$ and $N = V_4$.*

Example 71 *Consider $G = S_3$, $A = \langle(1\ 2\ 3)\rangle$ and $B = \langle(1\ 2)\rangle$. As $A \cap B = \{e\}$ it follows that $AB = G$. Therefore $S_3 = \langle(1\ 2\ 3)\rangle \rtimes \langle(1\ 2)\rangle$. Notice that $(1\ 2)$ and $(1\ 2\ 3)$ do not commute and $S_3 \neq \langle(1\ 2\ 3)\rangle \times \langle(1\ 2)\rangle$ (the latter is Abelian, the former is not).*

We wish to understand how to recover the multiplication rule of the semidirect product G from information about H and N. First of all, note that if $n_1h_1 = n_2h_2$, then

$$n_2^{-1}n_1 = h_2h_1^{-1} \in H \cap N = \{e\},$$

so that $n_1 = n_2$ and $h_1 = h_2$ and the representation $g = nh$ is indeed unique as we claimed earlier. Set-theoretically we can identify G with $N \times H$, the set of ordered pairs (n, h). Also, if $g_1 = n_1h_1$ and $g_2 = n_2h_2$, then

$$g_1g_2 = n_1h_1n_2h_2 = \underbrace{n_1(h_1n_2h_1^{-1})}_{\in N}\underbrace{h_1h_2}_{\in H},$$

as N is normal. So this is almost like straightforward multiplication of pairs, except that the multiplication in N is "twisted" by conjugation with h_1.

Recall that in any group G, with $h \in G$, *conjugation by h* is an automorphism of G. That is the map $\phi_h \colon G \to G$ given by

$$\phi_h(g) = hgh^{-1}$$

is an isomorphism from G to itself. So we might rewrite the product in $G = N \rtimes H$ as

$$(n_1, h_1) \circ (n_2, h_2) = (n_1\phi_{h_1}(n_2), h_1h_2)\,.$$

This twist ϕ_h comes internally from the group G containing N and H as subgroups of. If instead we hoped to take two unrelated groups and make an *external* semidirect product $N \rtimes H$ we would need to somehow know how to twist our product. So we now note:

Lemma 72 *(a) If $N \lhd G$, then for each $h \in G$, ϕ_h restricts to an automorphism of N.*

(b) If $H \leqslant G$ the map $h \mapsto \phi_h$ gives a group homomorphism $H \to \mathrm{Aut}(N)$.

Remark 73 *Recall that the set of automorphisms of a group G form a group $\mathrm{Aut}(G)$ under composition.*

Proof (a) We know that ϕ_h is an automorphism of G; it restricts to a map $N \to N$ as normal subgroups are preserved by conjugation.

(b) For $h_1, h_2 \in H$ we have

$$\phi_{h_1 h_2}(n) = (h_1 h_2) n (h_1 h_2)^{-1} = h_1 (h_2 n h_2^{-1}) h_2 = \phi_{h_1} \phi_{h_2}(n).$$

■

This now shows precisely what information we need to build an *external* semidirect product.

Theorem 74 *Given two groups H and N, and a homomorphism*

$$\phi \colon H \to \mathrm{Aut}(N),$$

define $(N \rtimes H, \circ)$ to consist of the set of pairs (n, h) with $h \in H$, $n \in N$, with operation

$$(n_1, h_1) \circ (n_2, h_2) = (n_1 \phi(h_1)(n_2), h_1 h_2).$$

Then $(N \rtimes H, \circ)$ is a group. It contains subgroups $\tilde{H} = \{(e, h))\}$ and $\tilde{N} = \{(n, e)\}$, the latter normal, isomorphic respectively to H and N.

Proof This is left to Sheet 2, Exercise 3. ■

Example 75 *If $\phi \colon H \to \mathrm{Aut}(N)$ is the map $\phi(h) = \mathrm{id}_N$ then*

$$(n_1, h_1) \circ (n_2, h_2) = (n_1 \mathrm{id}_N(n_2), h_1 h_2) = (n_1 n_2, h_1 h_2),$$

and we have recreated the (external) direct product.

Example 76 *Let $C_n = \langle a \rangle$ for some $n \geqslant 2$ and let $C_2 = \langle b \rangle$. Let $\phi \colon C_2 \to \mathrm{Aut}(C_n)$ be the map determined by $\phi(b)(a^r) = a^{-r}$, for $r \in \mathbb{Z}$, i.e. the non-trivial element of C_2 acts by inverting elements of C_n. For $n \geqslant 3$ the group $C_n \rtimes_\phi C_2$ is isomorphic to D_{2n}, the dihedral group of order $2n$. To appreciate this we can see that $a^r = b^2 = e$ as we expect and*

$$ba = (e, b) \circ (a, e) = (\phi(b)\,(a), b) = \left(a^{-1} b\right) = a^{-1} b,$$

so that we can identify a with σ and b with τ. Note that $C_2 \rtimes_\phi C_2 = C_2 \times C_2 \cong D_4$ as $C_2 = \langle a \rangle$ has $a^{-1} = a$ so ϕ is trivial.

Example 77 *Recall that an automorphism $\sigma\colon \mathbb{Z}_n \to \mathbb{Z}_n$ must map a fixed generator to another generator, and is uniquely determined by this choice, so*

$$\mathrm{Aut}(\mathbb{Z}_n) \cong U(\mathbb{Z}_n),$$

the group of units of the ring $\mathbb{Z}_n$.

Example 78 *(a) What semi-direct products $\mathbb{Z}_3 \rtimes \mathbb{Z}_3$ are there? As*

$$\mathrm{Aut}(\mathbb{Z}_3) \cong U(\mathbb{Z}_3) = \{1, 2\} \cong \mathbb{Z}_2$$

then the only homomorphism $H = \mathbb{Z}_3 \to \mathbb{Z}_2 \cong \mathrm{Aut}(N)$ is the trivial map and so the only semidirect product is in fact the direct product $\mathbb{Z}_3 \times \mathbb{Z}_3$.

(b) What semi-direct products $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ are there? Again $\mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$ but now there are two homomorphisms $H = \mathbb{Z}_4 \to \mathbb{Z}_2 \cong \mathrm{Aut}(N)$. One is the trivial map and this again leads to the direct product $\mathbb{Z}_3 \times \mathbb{Z}_4$. The other is comes from the homomorphism

$$\mathbb{Z}_4 \to \mathbb{Z}_2 \qquad \textit{given by} \qquad n \mod 4 \mapsto n \mod 2.$$

In terms of the automorphisms of $\mathbb{Z}_3$ we are discussing here $0 \bmod 2$ represents the identity and $1 \bmod 2$ represents the negative map. So multiplication in $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ is given by

$$(n_1 \mod 3, h_1 \mod 4) \circ (n_2 \mod 3, h_2 \mod 4) = \left(n_1 + (-1)^{h_1} n_2 \mod 3, h_1 + h_2 \mod 4\right).$$

This may well be easier to understand in terms of generators and relations. If we take

$$x = (1 \mod 3, 0 \mod 4) \qquad y = (0 \mod 3, 1 \mod 4),$$

which are generators for our group, then we have

$$x^3 = y^4 = (0 \mod 3, 0 \mod 4) = e.$$

We also have

$$\begin{aligned} yx &= (0 \mod 3, 1 \mod 4) \circ (1 \mod 3, 0 \mod 4) \\ &= (-1 \mod 3, 1 \mod 4) \\ &= (-1 \mod 3, 0 \mod 4) \circ (0 \mod 3, 1 \mod 4) \\ &= x^{-1}y. \end{aligned}$$

Thus we have a presentation for this group

$$C_3 \rtimes C_4 = \langle x, y \,|\, x^3 = y^4 = e, yx = x^{-1}y \rangle.$$

This group manifests as a subgroup of the quaternions: we can set $x = e^{i\pi/3}$ *and* $y = j$*, noting that* $x^3 = 1 = y^4$ *and that*

$$yx = je^{i\pi/3} = j\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = \left(-\frac{1}{2}j - \frac{\sqrt{3}}{2}k\right) = \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)j = e^{2\pi i/3}j = x^{-1}y.$$

Note that this group is not isomorphic to any of C_{12}*,* $C_2 \times C_6$*,* A_4, D_{12} *(the first two are abelian and the last two have no order* 4 *elements). In fact we now have a complete list of the order* 12 *groups*

$$C_{12}, \qquad C_2 \times C_6, \qquad A_4, \qquad D_{12}, \qquad C_3 \rtimes C_4,$$

though we will need some further results before we can be sure of that.

Example 79 *Recall that* S_4 *is the internal semi-direct product of* V_4 *and* $S_3 = \mathrm{Sym}\{1,2,3\}$*. How might we have arrived at* S_4 *as an external semi-direct product* $V_4 \rtimes S_3$*? Note that*

$$\mathrm{Aut}(V_4) \cong S_3$$

as V_4 *can be thought of as* e *together with three commuting order two elements* a, b, c*. Thus any permutation of* a, b, c *is an automorphism of* V_4*. We will write*

$$a = (14)(23), \qquad b = (13)(24), \qquad c = (12)(34).$$

We need to work out which homomorphism $\phi\colon S_3 = \mathrm{Sym}\{1,2,3\} \to \mathrm{Aut}(V_4) \cong S_3 = \mathrm{Sym}\{a,b,c\}$ *comes internally from the group structure of* S_4*. Recall that* ϕ_σ *denotes conjugation by* σ *and so*

$$\phi_{(12)} = (ab); \qquad \phi_{(13)} = (ac)$$

and so $\phi\colon \mathrm{Sym}\{1,2,3\} \to \mathrm{Sym}\{a,b,c\}$ *is (essentially) the identity map* $1 \leftrightarrow a$*,* $2 \leftrightarrow b$*,* $3 \leftrightarrow c$*.*

11 Extensions

We now discuss the general extension problem.

Definition 80 *Let A and B be groups. Then an **extension** of A by B is a group G together with a normal subgroup K such that $K \cong A$ and $G/K \cong B$. Note necessarily that $|G| = |A|\,|B|\,|$.*

The *extension problem* is: given groups A and B, can one classify all extensions of A by B? This problem is hard but sophisticated methods to tackle it have been developed. Notice that some extensions certainly exist: $A \times B$ is an extension of A by B (and of B by A). Semi-direct products are also extensions, since $A \lhd A \rtimes B$ and $(A \rtimes B)/A \cong B$.

Another way to view an extension is as a short exact sequence of groups.

Definition 81 *Let M, N, P be groups. A **short exact sequence** involving M, N and P is a sequence*

$$\{e\} \to M \xrightarrow{i} N \xrightarrow{\pi} P \to \{e\}$$

with i injective, π surjective and $\mathrm{Im} i = \ker \pi$. (The last of these is "exactness at N"; exactness at M is equivalent to i being injective and exactness at P is equivalent to π being surjective, since i and π are maps from and to the trivial group, respectively.)

Observe that $i(M) = \ker \pi \lhd N$ and $P \cong N/M$. So an extension of A by B is a short exact sequence

$$\{e\} \to A \xrightarrow{i} G \xrightarrow{\pi} B \to \{e\}$$

Example 82 *Here are some examples.*

- *extensions of $C_2 = \langle a \rangle$ by $C_2 = \langle b \rangle$:*

$$\{e\} \to C_2 \xrightarrow{i_1} C_2 \times C_2 \xrightarrow{\pi_1} C_2 \to \{e\}\,. \qquad i_1(a) = (a, e)\,, \quad \pi_1\,(e, b) = b. \tag{10}$$

$$\{e\} \to C_2 \xrightarrow{i_2} C_4 = \langle c \rangle \xrightarrow{\pi_2} C_2 \to \{e\}\,. \qquad i_2(a) = c^2, \quad \pi_2\,(c) = b. \tag{11}$$

- *extensions of $C_3 = \langle a \rangle$ by $C_2 = \langle b \rangle$:*

$$\{e\} \to C_3 \xrightarrow{i_1} C_6 = \langle c \rangle \xrightarrow{\pi_1} C_2 \to \{e\}\,. \qquad i_1(a) = c^2, \quad \pi_2\,(c) = b. \tag{12}$$

$$\{e\} \to C_3 \xrightarrow{i_2} S_3 \xrightarrow{\pi_2} C_2 \to \{e\}\,. \qquad i_2(a) = (1\,2\,3)\,, \quad \pi_2\,(\rho) = \mathrm{sgn}(\rho). \tag{13}$$

- *extensions of* $C_n = \langle a \rangle$ *by* $C_2 = \langle b \rangle$*:*

$$\{e\} \rightarrow C_n \overset{i_1}{\rightarrow} C_{2n} = \langle c \rangle \overset{\pi_1}{\rightarrow} C_2 \rightarrow \{e\}. \qquad i_1(a) = c^2, \quad \pi_2(c) = b. \tag{14}$$

$$\{e\} \rightarrow C_n \overset{i_2}{\rightarrow} D_{2n} \overset{\pi_2}{\rightarrow} C_2 \rightarrow \{e\}. \qquad i_2(a) = \sigma, \quad \pi_2\left(\sigma^k \tau^l\right) = b^l. \tag{15}$$

- *extensions of* A_n *by* $C_2 = \{\pm 1\}$*:*

$$\{e\} \rightarrow A_n \overset{i_1}{\rightarrow} A_n \times C_2 \overset{\pi_1}{\rightarrow} C_2 \rightarrow \{e\}. \qquad i_1(\rho) = (\rho, e), \quad \pi_2\left(\rho, b^i\right) = b^i \tag{16}$$

$$\{e\} \rightarrow A_n \overset{i_2}{\rightarrow} S_n \overset{\pi_2}{\rightarrow} C_2 \rightarrow \{e\}. \qquad i_2(\rho) = \rho, \quad \pi_2(\rho) = \operatorname{sgn}(\rho). \tag{17}$$

We know direct and semi-direct products are extensions. But how do we know when an extension results from a semi-direct product?

Definition 83 *An extension of a group* A *by a group* B *described by the short exact sequence*

$$\{e\} \rightarrow A \overset{i}{\rightarrow} G \overset{\pi}{\rightarrow} B \rightarrow \{e\}$$

is said to ***split*** *if there exists a group homomorphism* $j \colon B \rightarrow G$ *such that* $\pi \circ j = \mathrm{id}_B$*. (Note that* j *is consequently injective.)*

The importance of the splitting of an extension (that is, a split extension) is given by the following.

Lemma 84 *There exists homomorphisms* i *and* π *making the sequence*

$$\{e\} \rightarrow A \overset{i}{\rightarrow} G \overset{\pi}{\rightarrow} B \rightarrow \{e\}$$

split if and only if $G \cong A \rtimes_\phi B$ *for some* $\phi \colon B \rightarrow \mathrm{Aut}(A)$*.*

Proof This is left as an exercise. Hint for ($\Rightarrow$): consider

$$\phi(b)(a) = i^{-1}(j(b)i(a)j(b^{-1})).$$

■

Example 85 *Here are some examples.*

- S_3 *as an extension of* C_3 *by* C_2 *splits.*
- S_n *as an extension of* A_n *by* C_2 *splits.*
- C_4 *as an extension of* C_2 *by* C_2 *does not split.*

Part VII
Sylow's Theorems

In the first year we saw that Lagrange's Theorem doesn't have a converse, the easiest instance of this being that the group A_4 doesn't have a subgroup of order 6. We did though see that there are partial converses to the result: for example if a prime p divides the order of a group G then there is an element of order p and hence a subgroup of order p. This is *Cauchy's Theorem*. We will substantially improve on that result in the next two lectures.

Definition 86 *Let G be a finite group. We say that G is a p-**group**, where p is a prime, if the order of G is a power of p.*

Definition 87 *Let G a group of order $p^a m$ where p is a prime and $p \nmid m$. Then we call a subgroup H of G a **Sylow p-subgroup** if H has order p^a. We denote by n_p the number of Sylow p-subgroups of G and we shall write $\mathrm{Syl}_p(G)$ for the set of those subgroups.*

We will state Sylow's theorems below; in what follows we assume that G is a finite group and p is a prime. We may then uniquely write $|G| = p^a m$ with $a \geqslant 0$, $m \geqslant 1$ and $p \nmid m$.

Theorem 88 *(**Sylow's First Theorem**) There is a Sylow p-subgroup of G.*

Theorem 89 *(**Sylow's Second Theorem**) Two Sylow p-subgroups of G are conjugate – i.e. if P_1, $P_2 \in \mathrm{Syl}_p(G)$ then there exists $g \in G$ such that $P_2 = g^{-1} P_1 g$.*

Theorem 90 *(**Sylow's Third Theorem**) $n_p \equiv 1 \bmod p$ and n_p divides m.*

Remark 91 *In the proof we will show that any p-subgroup of G is contained in a Sylow p-subgroup. Also, as two Sylow p-subgroups are conjugate they are isomorphic.*

Remark 92 *It is often possible to use Sylow's Third Theorem to demonstrate that there is a unique subgroup Sylow p-subgroup (for some p). As any conjugate of that subgroup is also a Sylow p-subgroup then we see that this subgroup is normal.*

Before proving the theorems we consider the following groups by way of examples.

Example 93 • *The Sylow subgroups of* D_{10}*:*

As $|D_{10}| = 10 = 2 \times 5$ *there are Sylow* p*-subgroups for* $p = 2$ *and* $p = 5$*.*

$$\begin{array}{rcl} \textit{Sylow 2-subgroups} & : & \langle s\rangle, \quad \langle sr\rangle, \quad \langle sr^2\rangle, \quad \langle sr^3\rangle, \quad \langle sr^4\rangle. \\ \textit{Sylow 5-subgroups} & : & \langle r\rangle. \end{array}$$

Being unique $\langle r\rangle$ *must be normal.*

We also note $n_5 = 1 \equiv 1 \bmod 5$ *and* $n_2 = 5 \equiv 1 \bmod 2$ *as expected. Also* n_5 *divides* $2 = 10/5$ *and* n_2 *divides* $5 = 10/2$*,*

- *The Sylow subgroups of* A_5*:*

  As $|A_5| = 60 = 2^2 \times 3 \times 5$ *there are Sylow* p*-subgroups for* $p = 2, 3$ *and* 5*.*

$$\begin{array}{rcl} \textit{Sylow 2-subgroups} & : & V_4\left(\{a, b, c, d\}\right). \\ \textit{Sylow 3-subgroups} & : & \langle (abc)\rangle \\ \textit{Sylow 5-subgroups} & : & \langle (abcde)\rangle. \end{array}$$

  $p = 2$*: these are of order* 4 *and are isomorphic to* $C_2 \times C_2$ *(as* A_5 *has no elements of order* 4*).* A_5 *has* 15 *elements of order* 2 *which make* 5 *such subgroups when combined with the identity (each subgroup fixes one of* $1, 2, 3, 4, 5$*.) Note* $n_2 = 5 \equiv 1 \bmod 2$ *and* n_2 *divides* $15 = 60/2^2$*.*

  $p = 3$*: these are cyclic of order* 3*.* A_5 *has* 20 3*-cycles which pair up and together with the identity make* 10 *such subgroups. So* $n_3 = 10$*. Note that* $n_3 \equiv 1 \bmod 3$ *and that* n_3 *divides* $60/3 = 20$*.*

  $p = 5$*: these are cyclic of order* 5*. There are* 24 5*-cycles; four of these and the identity make* 6 *such subgroups so* $n_5 = 6$*. Note that* $n_5 \equiv 1 \bmod 5$ *and that* n_5 *divides* $60/5 = 12$*.*

We return to the proof of Sylow's theorems.

Proof (First Theorem) Let P be a maximal p-subgroup of order p^b for some b, so that there does not exist a subgroup Q of G with $P \leqslant Q$ and $|Q| = p^c$ for $c > b$.

Let $H = N_G(P) = \{g \in G \mid g^{-1}Pg = P\}$, the *normalizer* of P, so that $P \lhd H$, and let $m_0 = |H/P|$. Let m_1 be the number of cosets of H in G. We then have

$$p^a m = |G| = |G : H||H| = m_1 p^b m_0.$$

Our strategy will be to prove the following three steps:

- STEP 1: p does not divide m_0.
- STEP 2: P is precisely the set of elements of H whose order is a power of p.
- STEP 3: p does not divide m_1.

It then follows that p does not divide $m_0 m_1$ and hence $a = b$. (In due course – for the Third Theorem – we shall see that $n_p = m_1$.)

STEP 1: If p divides m_0 then by Cauchy's theorem there exists a subgroup $\bar{A} \leqslant H/P$ of order p. As a consequence of the Third Isomorphism Theorem, there then exists $A \leqslant H$ such that $\bar{A} = A/P$ and $P \leqslant A \leqslant H$. Now $|A| = |A : P|\,|P| = \left|\bar{A}\right|\,|P| = p^{b+1}$ but this contradicts the maximality of P. So p cannot divide m_0 and $|H| = p^b m_0$ with $p \nmid m_0$.

STEP 2: Now P is a p-subgroup of G and hence of H, so that every element of P has order a power of p. In fact, P must be exactly the elements of H having order a power of p, as any such element in H but not in P would give rise to a subgroup of H/P with order divisible by p, but $p \nmid |H/P| = m_0$. In particular, if Q is a p-subgroup of H we must have $Q \leqslant P$.

STEP 3: Now let Σ denote the set of right cosets of H in G, with G acting naturally on the right. We defined $m_1 = |\Sigma|$. Denote by α the coset $He = H \in \Sigma$ so that $\mathrm{Stab}\,(\alpha) = H$. Consider now the action of P on Σ. Since $P \leqslant H$, P fixes α, so that there is at least one P-orbit of size 1, namely $\{\alpha\}$. Let $\{\beta\}$ be any other P-orbit of size 1. Then since the action of any group on one of its coset spaces is transitive, there exists $x \in G$ such that $\beta = \alpha \cdot x$. Thus $P \leqslant \mathrm{Stab}\,(\beta) = x^{-1}\mathrm{Stab}\,(\alpha)\,x = x^{-1}Hx$. So, $xPx^{-1} \leqslant H$. The elements of P have order a power of p and so this is also true of elements of xPx^{-1}. Thus by STEP 2 $xPx^{-1} \leqslant P$ and, comparing orders, $xPx^{-1} = P$ and so $x \in N_G(P) = H$. But then $\alpha \cdot x = H \cdot x = H$ so $\beta = \alpha \cdot x = \alpha$, and we have shown that there is a unique P-orbit of size 1, namely $\{\alpha\}$, for the action of P on Σ. ■

We now make use of the following lemma:

Lemma 94 *Let G be a finite group having order $|G| = p^r$ for some prime p and suppose G acts on a set Σ. Define* $\mathrm{Fix}_G\,(\Sigma) = \{\omega \in \Sigma : \omega \cdot g = \omega \ \text{ for all } g \in G\}$ *(i.e. the set of singleton orbits). Then*

$$|\mathrm{Fix}_G\,(\Sigma)| \equiv |\Sigma| \mod p.$$

Proof All orbits have a size divides p^r. Hence the sizes of the non-singleton orbits are multiples of p. As the orbits partition Σ the result follows. ■

Proof (of STEP 3 continued) Using this lemma for the p-group P acting on Σ, we see that

$$|\Sigma| = m_1 \equiv |\mathrm{Fix}_P(\Sigma)| \equiv 1 \ mod\ p.$$

But then $p \nmid m_1$ completing the proof of Step 3. ■

Proof (Second Theorem) We will show the stronger claim that for any Sylow p-subgroup P and any (not necessarily maximal) p-subgroup Q of G, there exists an element $x \in G$ such that $Q \leqslant x^{-1}Px$. For if Q is in fact maximal (i.e. Sylow) then $Q = x^{-1}Px$, hence the Second Theorem.

We consider the action of Q by right multiplication on Σ. By the above lemma again, $|\Sigma| \equiv |\mathrm{Fix}_Q(\Sigma)| \ \ mod\ p$ where $|\mathrm{Fix}_Q(\Sigma)|$ is the number of Q-orbits of size 1. But $p \nmid |\Sigma|$ so $|\mathrm{Fix}_Q(\Sigma)| \not\equiv 0 \ mod\ p$ and there exists at least one Q-orbit of size 1, $\{\beta\}$ say. The action of G on Σ is transitive so as before there exists $x \in G$ such that $\beta \cdot x = \alpha$. Thus $\mathrm{Stab}(\beta) = x^{-1}Hx$, also as before. Since $\{\beta\}$ is a Q-orbit of size 1, we see that $Q \leqslant \mathrm{Stab}(\beta) = x^{-1}Hx$ so xQx^{-1} is a p-subgroup of H, and therefore of P, so $Q \leqslant x^{-1}Px$ as required. This proves our claim, from which we deduce the Second Theorem. ■

Proof (Third Theorem) The conjugates of a subgroup are in 1-1 correspondence with the cosets of its normalizer: here $x^{-1}Px \longleftrightarrow N_G(P)x = Hx$. As the Sylow p-subgroups are conjugate to one another $n_p = |G : H| = |\Sigma| = m_1$ divides m and $n_p \equiv 1 \ mod\ p$ from STEP 3 above. This proves the Third Theorem. ■

12 Applications

The classification up to isomorphism of finite groups is one of the hardest problems in mathematics. In Prelims we were able to handle the following special cases.

- If p is prime and $|G| = p$ then G is cyclic.
- If $p \geqslant 3$ is prime and $|G| = 2p$ then $G \cong C_{2p}$ or $G \cong D_{2p}$.
- If p is a prime and $|G| = p^2$ then $G \cong C_{p^2}$ or $G \cong C_p \times C_p$.

On Exercise Sheet 2 it was left as an exercise to show that the groups of order 8 are, up to isomorphism,

$$C_8, \qquad C_4 \times C_2, \qquad C_2 \times C_2 \times C_2, \qquad D_8, \qquad Q_8.$$

For groups of order less than 16 this leaves only the orders 12 and 15 unresolved. The following general result shows, in particular, that groups of order 15 are cyclic.

Proposition 95 *Let G be a group of order pq with p, q prime, $p > q$ and $q \nmid p-1$. Then G is cyclic.*

Proof By Cauchy's theorem, G has subgroups of orders p and q. Consider the subgroup of order p, i.e. for the larger prime. If P_1 and P_2 were distinct subgroups of order p then their intersection would be trivial, so P_1P_2 would contain p^2 elements. This cannot happen, since $|G| = pq < p^2$. Hence there is a unique subgroup of order p, which must therefore be normal. Denoting the p-subgroup by P and letting Q be any q-subgroup, $P \cap Q = \{e\}$ and $PQ = G$ so G is a semi-direct product of P by Q. (Note that what we have so far proven applies to any group whose order is a product of two distinct primes.)

Observe that $P \cong C_p$ and $Q \cong C_q$. If there is only one q-subgroup Q, then Q is also normal and G is a direct product of P and Q and is therefore cyclic of order pq. Given $G = P \rtimes Q$ (possibly a direct product), it remains to determine the action of Q on P by conjugation.

As $q \nmid p-1$ then since any q-subgroup is a Sylow q-subgroup (q is the highest power of q dividing pq), $n_q = 1 + mq \neq p$ so we have only one q-subgroup and $G = C_p \times C_q \cong C_{pq}$. Alternatively we might have noted that the only homomorphism $C_q \to \mathrm{Aut}(C_p) \cong C_{p-1}$ is the one with kernel C_q. ∎

Remark 96 *A semi-direct product $N \rtimes H$ is in fact direct when N and H are normal. To see this recall that each element can be uniquely written nh where $n \in N$ and $h \in H$. Then note*

$$(n_1h_1)(n_2h_2) = (n_1h_1n_2h_1^{-1})(h_1h_2) = (n_1n_2)(n_2^{-1}h_1n_2h_2).$$

By uniqueness $n_1h_1n_2h_1^{-1} = n_1n_2$ so that $h_1n_2 = n_2h_1$ and hence the product is in fact direct.

Remark 97 *Similar arguments can be used to show that:*

- *Let G be a group of order pq where $p > q$ and $q \mid p-1$. Then $G \cong C_{pq}$ or $G \cong C_p \cdot C_q$ where $C_p \cdot C_q$ is the semi-direct product of C_p by C_q with $\phi(b)(a) = a^r$, where $\langle b \rangle = C_q$, $\langle a \rangle = C_p$ and $r \in \mathbb{N}$, $1 < r < p$ such that $r^q \equiv 1 \bmod p$. (Compare this with the first year result of groups of order $2p$.)*

- *Let G be a group of order pqr with p, q and r primes and $p > q > r$. Then G is not simple.*

We now look to classify the groups of order 12. The abelian groups are C_{12}, $C_2 \times C_6$, so suppose that G is a non-abelian group of order 12.

From Sylow's theorems, we have that n_2 is odd and divides 3, so is 1 or 3 and similarly $n_3 \equiv 1$ *mod* 3 and divides 4, so is 1 or 4. It is not possible to have $n_2 = 3$ and $n_3 = 4$, as this would require at least 4 elements of order 2 and 8 elements of order 3, as well as the identity, totalling more than 12. Hence there is exactly one Sylow 2-subgroup or exactly one Sylow 3-subgroup.

Now let p denote the prime for which there is exactly one Sylow p-subgroup, and q the other prime dividing 12. Then the unique Sylow p-subgroup must be normal, its intersection with any Sylow q-subgroup must be trivial and its product with any Sylow q-subgroup must be the whole of G. Hence G is a semi-direct product.

A Sylow 2-subgroup, being of order 4, is isomorphic to either C_4 or $C_2 \times C_2$. A Sylow 3-subgroup must be isomorphic to C_3. Therefore, to classify the groups of order 12, we must find all possible semi-direct products involving these groups. For this, we need to know their automorphism groups: these are as follows.

$$\mathrm{Aut}(C_3) \cong C_2 \qquad \mathrm{Aut}(C_2 \times C_2) \cong S_3 \qquad \mathrm{Aut}(C_4) \cong C_2$$

So we have the following possibilities:

$C_4 \rtimes C_3$: there can be no non-trivial homomorphisms from C_3 to $\mathrm{Aut}(C_4) \cong C_2$, as any non-trivial homomorphism would have non-trivial kernel and thus be injective, which is impossible since $|C_3| > |C_2|$. So the only semi-direct product of this form is in fact direct, so we obtain $C_4 \times C_3$ (which we already had in our Abelian classification, since this is isomorphic to C_{12}).

$(C_2 \times C_2) \rtimes C_3$: since $\mathrm{Aut}(C_2 \times C_2) \cong S_3$ has a unique subgroup of order 3, any two non-trivial (hence injective) homomorphisms from C_3 to S_3 have the same image and so define isomorphic semi-direct products. Now A_4 has a unique Sylow 2-subgroup isomorphic to $C_2 \times C_2$ and hence is of the right form, so we must have $(C_2 \times C_2) \rtimes C_3 \cong A_4$.

$C_3 \rtimes (C_2 \times C_2)$: since $\mathrm{Aut}(C_3) \cong C_2$ there are three non-trivial injective homomorphisms from $C_2 \times C_2$ to $\mathrm{Aut}(C_3) \cong C_2$, each with the same image, so again they define isomorphic semi-direct products. This time, the candidate D_{12} can be seen to have a unique Sylow 3-subgroup isomorphic to C_3 and thus $C_3 \rtimes (C_2 \times C_2) \cong D_{12}$.

$C_3 \rtimes C_4$: there is exactly one non-trivial homomorphism from C_4 to $\mathrm{Aut}(C_3) \cong C_2$ (it is the natural projection onto the quotient of C_4 by the subgroup $\langle x^2 \rangle$). This semi-direct product is not isomorphic to A_4 or D_{12} and completes our list of groups of order 12. It may be realized as the subgroup $\langle (5\ 6\ 7), (1\ 2\ 3\ 4)(6\ 7) \rangle$ of S_7.

Hence the non-Abelian groups of order 12 are A_4, D_{12} and $C_3 \rtimes C_4$.

Remark 98 *Note that all the above groups of order less than 16 are solvable. In fact, the smallest non-solvable group is A_5.*

One might legitimately ask why we single out the finite simple groups for classification. This is because *if* we knew all finite simple groups and *if* we could solve the extension problem for finite groups, then we would know *all* finite groups. As hard as this approach may appear, it is considerably easier than the order-by-order approach.

Example 99 *Determine up to isomorphism the groups of order 99*

Proof Let G be a group of order 99, and let H be a Sylow 3-subgroup of G and K a Sylow 11-subgroup. Since the number of 11-subgroups is 1 *mod* 11 and divides 9 then K is unique and so normal. The number of Sylow 3-subgroups is 1 *mod* 3 and divides 11. Hence H is also normal. Hence G is the direct product of H and K. Up to isomorphism the groups of order 9 are C_9 and $C_3 \times C_3$. Hence G is isomorphic to $C_9 \times C_{11}$ or $C_3 \times C_3 \times C_{11}$. ■

Example 100 *Determine up to isomorphism the groups of order 66*

Proof Let G be a group of order 66, let H be a Sylow 3-subgroup and K be a Sylow 11-subgroup. As the number of 11-subgroups is 1 *mod* 11 and divides 6 then it is unique and hence K is normal. Hence HK is a subgroup of order $33 = 3 \times 11$ and so cyclic as $3 \nmid 10$. Let x be a generator for HK and y be an element in G of order 2 (which exists by Cauchy's Theorem). As HK is normal, being of index 2, we have $yxy^{-1} = x^i$ for some $1 \leqslant i \leqslant 32$ and (beyond $x^{33} = e = y^2$) this relation entirely determines the group structure.

We claim that there are four possibilities for i. As x and x^i are conjugate they have the same order – thus i and 33 are coprime. Also since y has order 2 then

$$x = y^{-1}x^i y = (y^{-1}xy)^i = (yxy^{-1})^i = (x^i)^i = x^{i^2}.$$

Thus 33 divides $i^2 - 1$. With a little working this shows i is one of 1, 10, 23, 32.

This shows that there can be at most 4 groups of order 66 and we note

$$C_{66}, \qquad D_{66}, \qquad D_{22} \times C_3, \qquad D_6 \times C_{11}$$

are four non-isomorphic groups of order 66 and hence form a complete list. ■