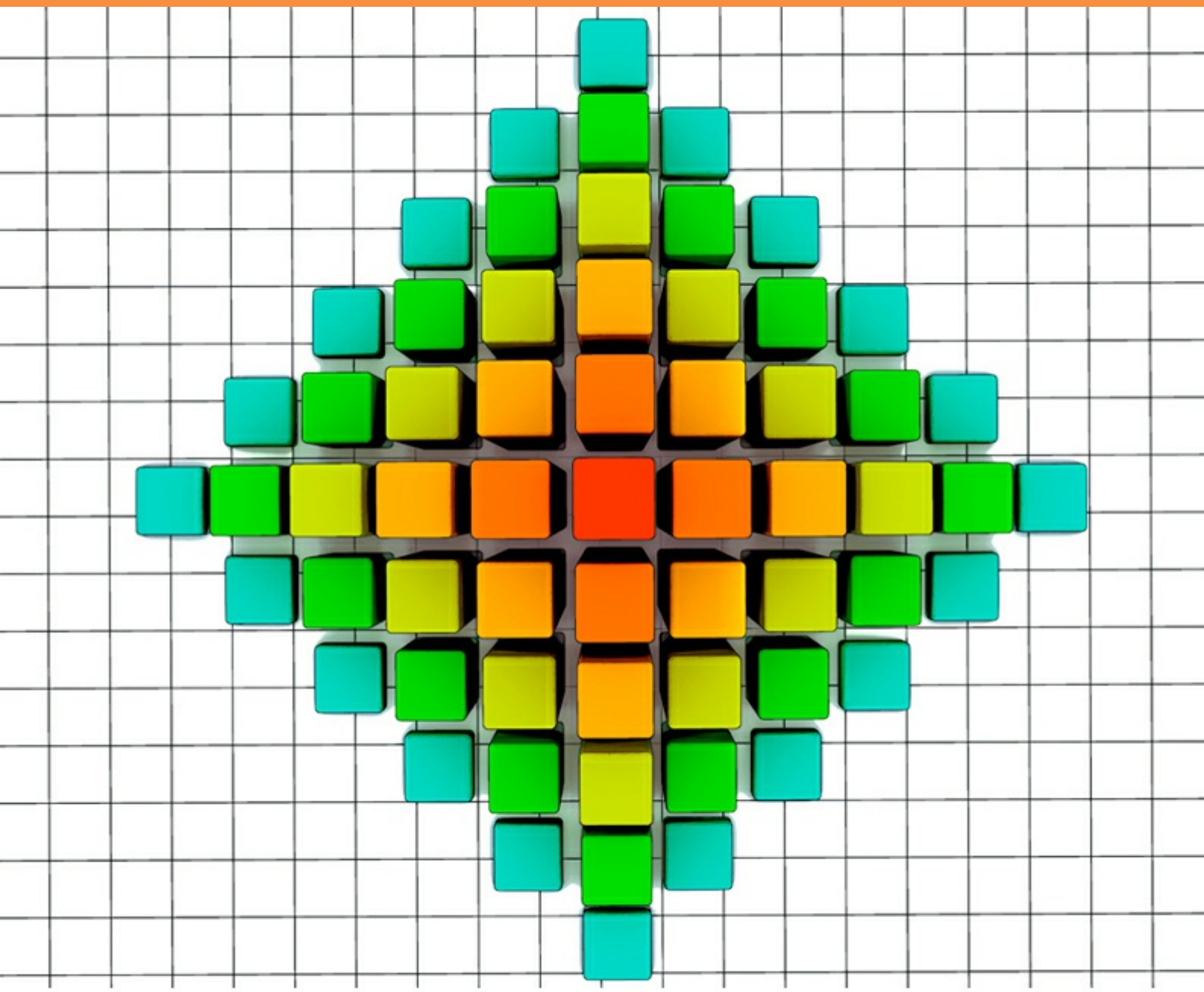


Essential Group Theory

Michael Batty

bookboon.com
The eBook company

Michael Batty

Essential Group Theory

Download free eBooks at bookboon.com

Essential Group Theory
© 2012 Michael Batty & bookboon.com
ISBN 978-87-403-0301-8

Download free eBooks at bookboon.com

Contents

	Introduction	**9**
1	**Sets and Maps**	**10**
1.1	Sets	10
1.2	Maps	11
1.3	Equivalence Relations and Partitions	12
1.4	Modular Arithmetic	13
2	**Groups**	**14**
2.1	Binary Operations	14
2.2	Groups: Basic Definitions	15
2.3	Examples of Groups	17
3	**Subgroups**	**21**
3.1	Definition of a Subgroup	21
3.2	Cosets	22
3.3	Lagrange's Theorem	23

Click on the ad to read more

Download free eBooks at bookboon.com

4	**Generators and Cyclic Groups**	**24**
4.1	Orders of Group Elements	24
4.2	Generating Sets	25
4.3	Cyclic Groups	26
4.4	Fermat's Little Theorem	27
5	**Mappings of Groups**	**28**
5.1	Homomorphisms	28
5.2	Isomorphisms	29
6	**Normal Subgroups**	**31**
6.1	Conjugates and Normal Subgroups	31
6.2	Cosets of Normal Subgroups	32
6.3	Kernels of Homomorphisms	32
7	**Quotient Groups**	**35**
7.1	Products of Cosets	35
7.2	Quotient Groups	35
8	**The First Isomorphism Theorem**	**37**
8.1	The First Isomorphism Theorem	37

Click on the ad to read more

Download free eBooks at bookboon.com

8.2	Centres and Inner Automorphisms	39
9	**Group Actions**	**40**
9.1	Actions of Groups	40
9.2	The Orbit-Stabilizer Theorem	41
10	**Direct Products**	**43**
10.1	Direct Products	43
10.2	Direct Products of Finite Cyclic Groups	43
10.3	Properties of Direct Products	44
11	**Sylow Theory**	**47**
11.1	Primes and p-Groups	47
11.2	Sylow's Theorem	48
12	**Presentations of Groups**	**51**
12.1	Introduction to Presentations	51
12.2	Alphabets and Words	53
12.3	Von Dyck's Theorem	56
12.4	Finitely Generated and Finitely Presented Groups	57
12.5	Dehn's Fundamental Algorithmic Problems	58

Discover the truth at www.deloitte.ca/careers

Deloitte.

© Deloitte & Touche LLP and affiliated entities.

Click on the ad to read more

Download free eBooks at bookboon.com

13	**Free Groups**	**60**
13.1	Reduced Words and Free Groups	60
13.2	Normal Closure	61
13.3	Torsion Free Groups	62
14	**Abelian Groups**	**64**
14.1	Commutator Subgroups and Abelianisations	64
14.2	Free Abelian Groups	65
14.3	Finitely Generated Abelian Groups	67
14.4	Generalisations of Abelian Groups	67
15	**Transforming Presentations**	**69**
15.1	Tietze Transformations	69
15.2	Properties of Tietze Transformations	71
16	**Free Products**	**74**
16.1	Free Products	74
16.2	A Normal Form for Free Products	76
16.3	The Universal Property of Free Products	77
16.4	Independence of Presentation	78
16.5	Decomposability	78

SIMPLY CLEVER

ŠKODA

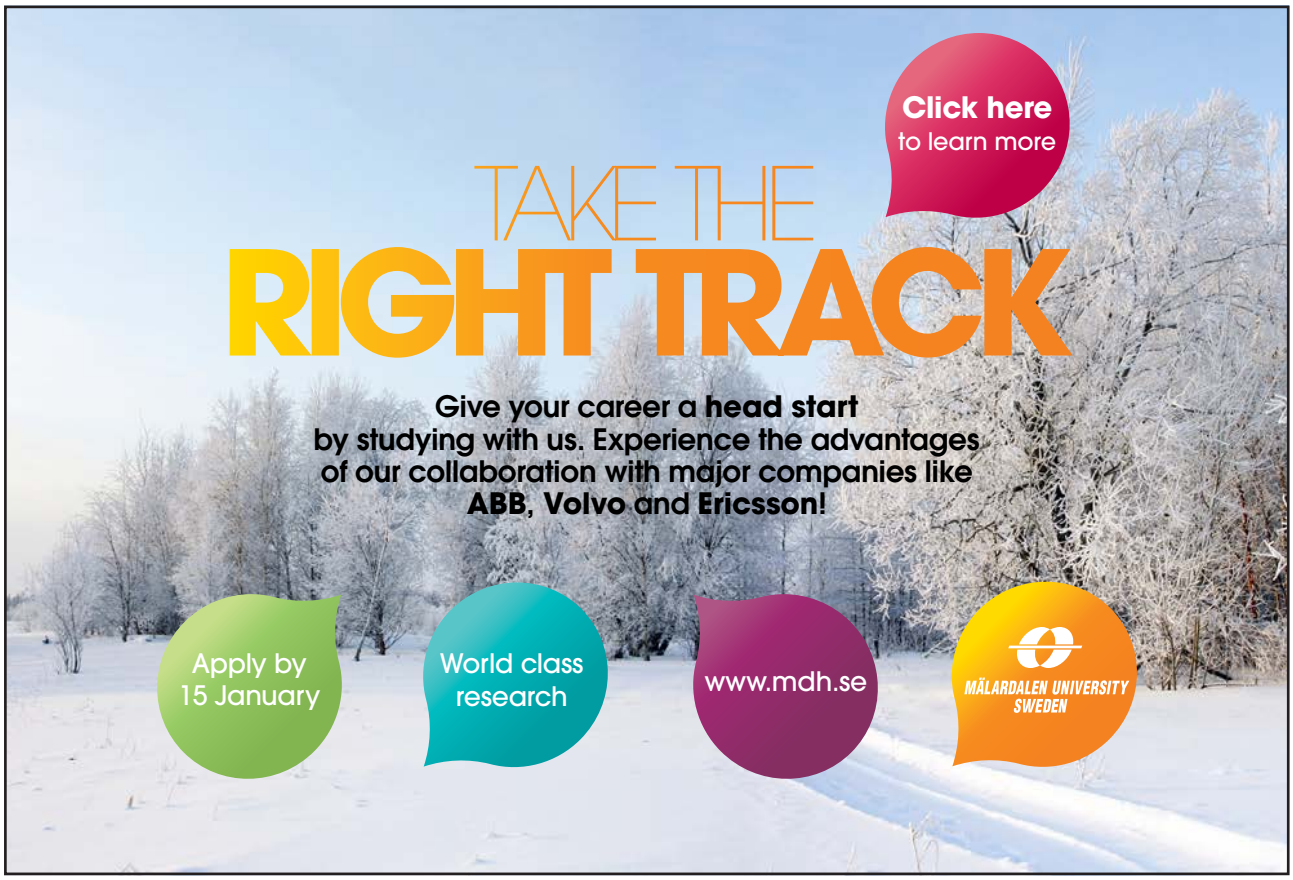
Do you like cars? Would you like to be a part of a successful brand?
We will appreciate and reward both your enthusiasm and talent.
Send us your CV. You will be surprised where it can take you.

Send us your CV on
www.employerforlife.com

Click on the ad to read more

Download free eBooks at bookboon.com

17	**Free Products With Amalgamation**	**80**
17.1	Free Products with Amalgamation	80
17.2	Pushouts	81
17.3	Independence of Presentation	85
18	**HNN Extensions**	**86**
18.1	HNN Extensions	86
18.2	Relation to Free Products with Amalgamation	87
18.3	The Higman-Neumann-Neumann Embedding Theorem	90
19	**Further Reading**	**92**
20	**Bibliography**	**94**
21	**Index**	**95**



Click on the ad to read more

Download free eBooks at bookboon.com

Introduction

This short book on group theory is partly based on notes from lectures I gave at Trinity College Dublin in 1999 and at Edinburgh University in 2001. The first part of the book is an introduction to elementary group theory. It doesn't aim to cover everything that might be in your introductory course in abstract algebra, but just to give a summary of the important points. Perhaps you could read it before you begin your course, if you want to read something gentle in advance, or it could be a starting point for revision. The second part of the book is about free groups and presentations of groups. This would typically appear in a second course on group theory.

Group theory can seem very abstract and strange when you first encounter it. It involves a different mindset and most likely you will not have done this type of mathematics before. But it has a set of techniques and beauty of its own and is worth perservering with, and you will find that the Gs and Hs will soon come to life.

As with a lot of university mathematics, it depends very much on the language and logic of sets and their elements, containment, equality and maps and unless you understand these fully, it is unlikely that you will be able to apply them in the context of group theory, where there is even more to think about. Most of the elementary proofs in group theory involve these simple but important techniques. I can't stress this enough and have included a preliminary section on sets and maps before the main theme of group theory starts.

I hope that there are as few mistakes as possible, but if you find any, have suggestions to improve the book or feel that I have not covered something which should be included please send an email to me at batty.mathmo@googlemail.com

Michael Batty, Durham, 2012.

Download free eBooks at bookboon.com

1 Sets and Maps

This section is primarily for reference, as you will probably have seen most of these definitions before. But please at least skim lightly through them as a reminder and refer to them later when necessary.

1.1 Sets

Sets are at the very foundation of mathematics. They are difficult to define formally, in order to avoid things going wrong. This can be done, with various systems of axioms. But it's a subject in its own right. Better for now if we just naively think of them as collections of elements, and take that as a starting point. We will liberally use set notation throughout the book, summarized as follows:

- $x \in X$ means x *is an element of the set* X.
- $x \notin X$ means x *is not an element of the set* X.
- $\{x, y\}$ means *the set consisting of* x *and* y.
- $X \subset Y$ or $Y \supset X$ means *all the elements of* X *are in* Y. We say X *is a* subset *of* Y or Y *contains* X.
- $X = Y$ means $X \subset Y$ *and* $Y \subset X$. This is how sets are proved to be equal, so such proofs have two parts.
- $X \subset Y$ will also include the possibility that $X = Y$. We will not use notation like $X \subseteq Y$.
- $X \cup Y$ means the *union* of X and Y, *the set of elements that are in* X *or* Y *(or both).*
- $X \cap Y$ means the *intersection of* X *and* Y, the set of elements that are in X and Y.
- $X - Y$ *means* the set of elements that are in X but not in Y.
- $\emptyset$ *denotes the set* $\{\}$ *containing no elements.*

A special type of set is a *pair* which has two elements. This can be either *unordered*, in which case it is of the form

$$\{x, y\}$$

Download free eBooks at bookboon.com

or *ordered*, in which case it is of the form

$$\{x, \{y\}\}$$

Let X and Y be sets. Then the *cartesian product* of X and Y, written $X \times Y$ is the set of all ordered pairs (x, y) with $x \in X$ and $y \in Y$.

Example 1.1 If $X = \{1, 2, 3\}$ and $Y = \{a, b\}$ then

$$X \times Y = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

1.2 Maps

A *map* f from a set X to a set Y is a subset of $X \times Y$ such that for all $x \in X$ there exists a unique $y \in Y$ with (x, y) in the map. X is called the *domain* of the map and Y is called the *range* of the map.

We usually write $f : X \to Y$. We also write $f(x) = y$ to denote the unique y with (x, y) in the map, or $x \mapsto y$.

Let $f : X \to Y$ be a map of sets.

1. We write $f(X)$ or $\mathrm{Im}(f)$ to denote the subset of Y given by

   $$\{f(x) | x \in X\}.$$

   This is called the *image* of f.

2. Let Z be a subset of Y. We write $f^{-1}(Z)$ for the subset of X given by

   $$\{x | f(x) \in Z\}.$$

   This is called the *inverse image* of Z under f.

3. f is called *injective* if for all w and x in X, $f(w) = f(x)$ implies that $w = x$.

4. f is called *surjective* if for all $y \in Y$ there exists $x \in X$ with $f(x) = y$.

5. f is called *bijective* if it is injective and surjective.

Download free eBooks at bookboon.com

1.3 Equivalence Relations and Partitions

A map from a set X to itself is, by definition, a special kind of subset of $X \times X$.

An arbitrary subset of $X \times X$ is called a *relation* on X.

For example, let X be the set of all people. Then we can define a function from X to itself given by

$$x \mapsto \text{ father of } x$$

This is a function because everyone has a unique father. If we attempt to define a function by

$$x \mapsto \text{ child of } x$$

then this doesn't define a function correctly because

- x may have no children
- x may have more than one child

However, it still defines a valid relation. Let X be a set and let R be a relation on X. If w and x are both elements of X then we will write $w \sim x$ to mean $(w, x) \in R$ and refer to the relation as .

A relation $\sim$ on X is *reflexive* if for all $x \in X$ we have $x \sim x$.

A relation $\sim$ on X is *symmetric* if for all w and x in X , $w \sim x$ implies $x \sim w$.

A relation $\sim$ on X is *transitive* if for all v , w and x in X , $v \sim w$ and $w \sim x$ implies that $v \sim x$.

Definition 1.2 *An* equivalence relation *on a set X is a relation on X that is reflexive, symmetric and transitive.*

If x is an element of x then we write

$$[x] = \{y \in X | y \sim x\}.$$

Download free eBooks at bookboon.com

This is called the *equivalence class* of x. Note that it is well defined, i.e. if $w \sim x$ then $[w] = [x]$.

Definition 1.3 *Let X be a set. A* partition *of X is a collection of subsets A_i of X such that*

$$x = \cup_i A_i$$

and

$$A_i \cap A_j = \emptyset$$

whenever $i \neq j$

So, given an element x of X, there is exactly one subset A_i with $x \in A_i$.

Proposition 1.4 *Let X be a set and let $\sim$ be an equivalence relation on X. Then*

$$\{[x] | x \in X\}$$

is a partition of X.

Proof. Exercise. □

The set of equivalence classes formed is called the *quotient set* of the original set under the equivalence relation.

1.4 Modular Arithmetic

Recall that if a and $n > 0$ are integers then $a \bmod n$ means the remainder when we divide a by n (mod is short for modulo). For example, $10 \bmod 3 = 1$.

We also $a = b \bmod n$ if $a \bmod n = b \bmod \mathrm{n}$, and say that a and b are equal, or congruent mod n.

The important thing here is that congruence mod n forms an equivalence relation on the integers. The set of equivalence classes are called congruence classes mod n. It is the quotient set under congruence. Ordinary addition, subtraction and multiplication of integers then become operations on congruence classes. If we write $[a]$ for the congruence class of $[a]$ then for example $[3] + [7] = [0] \bmod [10]$. Here $+$ might just look like ordinary addition but it is not. It is implicit in the notation that we are adding, then taking the remainder mod 10. We have defined a new operation on a different set.

Download free eBooks at bookboon.com

2 Groups

This section defines what is meant by a group and outlines its basic properties. As we will see, a group is a set with just enough extra structure to capture the idea of all symmetries of an object, and how the symmetries are related. But while this might be the original motivation for studying groups, we will see that they take on an algebraic character of their own, and become mathematical objects worthy of study in their own right.

2.1 Binary Operations

Let X be a set. A *binary operation* on X is a map from $X \times X$ to X.

Let's take a while to unravel this definition. Remember that formally

- A map from a set A to a set B is a subset of $A \times B$. So in this case, it is a subset of $(X \times X) \times X = X \times X \times X$.
- For each $a \in A$ there exists exactly one $b \in B$ such that (a, b) is in the map. So in this case, for each $(x, y) \in X \times X$ there is exactly one $z \in X$ with $((x, y), z)$ in the map.

Click on the ad to read more

Download free eBooks at bookboon.com

In a nutshell, the binary operation maps pairs to a single element and the result of the operation always exists and is uniquely defined. The elementary arithmetic operations $+$, $-$, $*$ and $/$ are examples of binary operations, although to be precise we have to also say what X is. For example we might think that $/$ is a binary operation on $\mathbb{Z}$ but it is not, for two reasons:

- The quotient of two integers might not be an integer. Really this is an issue about how we define division. If we define it as a fraction then the binary operation does not map to the correct set and you could argue that it simply doesn't make sense in the integers.

- Even if we define division by taking the result of an integer division and ignoring the remainder, we have to worry about division by zero.

So, if we define division by taking the result of integer division and ignore remainders, we finally obtain a binary operation on $\mathbb{Z} - \{0\}$. Note that what we have defined also then excludes legal division operations like $0/2$.

2.2 Groups: Basic Definitions

In this section we will be dealing with a special type of binary operation. First of all we will denote the binary operation by *juxtaposition*, which is a fancy way of saying writing things next to each other, as we do when we write down multiplication in elementary algebra. That is, suppose we have a binary operation m on a set X. Then we write

$$m(x, y) = xy$$

We will write down binary operations like this from now on but it is *very* important to realise that what we write is far more general than just multiplication in elementary algebra.

Suppose we then write xyz. What does this mean? Does it mean $m(m(x, y), z)$ or does it mean $m(x, m(y, z))$. In other words, does it matter which order we evaluate the binary operation? Is

$$(xy)z = x(yz)$$

always, for any binary operation? Well, no. Why should it be? We have simply defined binary operations in terms of subsets of cartesian products and they could be anything. The above is a special property called *associativity*.

A binary operation on a set X is called an *associative* operation if for all x, y and z in X we have

$$(xy)z = x(yz)$$

Download free eBooks at bookboon.com

An *identity* for a binary operation on a set X is an element e of X such that for all $x \in X$,

$$ex = xe = x.$$

That is, multiplication by e has no effect on any element, just leaves it as it is. Again, there is no reason whatsoever why such an element should exist. For example, suppose X is the set $\{1, \ldots, 100\}$ and define a binary operation on X that sends every single pair of elements of X to 1. Then for any integer x in $\{2, \ldots, 100\}$ there can be no element e with $ex = x$.

The final property of binary operations that will concern us is the following.

Suppose that a binary operation on a set X has an identity e. Then an *inverse* for $x \in X$ is an element $w \in X$ such that

$$xw = wx = e$$

So that the inverse x "undoes" the effect of multiplying by x. It is usually denoted by x^{-1}.

The definition of a group puts these three concepts together.

Definition 2.1 *A* group *is a pair $G = (X, m)$, where X is a set called the* underlying set *of G and m is a binary operation on X called the* group law *or* multiplication *of G, written $m(g, h) = gh$, such that the following axioms hold. (Typically we say $g \in G$ to mean $g \in X$).*

1. *For all g, h and k in G, $g(hk) = (gh)k$, i.e. the group law is associative.*
2. *The group law has an identity. That is, there exists $e \in G$ such that for all $g \in G$, $eg = ge = g$.*
3. *Every element of G has an inverse. That is, for all $g \in G$ there exists $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$.*

Exercise 2.2 Show that if G is a group and g and h are elements of G then $(gh)^{-1} = h^{-1}g^{-1}$.

In a group G the identity is unique. For suppose that e and f are identities in G. Then $e = ef = f$.

Given an element $g \in G$ the inverse of g is unique…

Let g be a group and let $g \in G$. As in everyday arithmetic, we write g^2 for gg and, inductively, g^n for $g^{n-1}g$ if n is an integer greater than 1. Similarly we write g^{-n} for $(g^n)^{-1} = (g^{-1})^n$.

Download free eBooks at bookboon.com

Did you find it a little strange there, where $(gh)^{-1} = h^{-1}g^{-1}$ and not $g^{-1}h^{-1}$? This is because in general in a group, gh is not equal to hg. The groups where this does occur are quite special.

Definition 2.3 *Let G be a group such that for all g and h in G we have $gh = hg$. Then G is called an* abelian *group.*

Exercise 2.4 Let G be a group. Show

1. G is abelian if and only if for all g and h in G, $(gh)^2 = g^2h^2$.
2. If for all $g \in G$, $g^2 = e$, then G is abelian.

In an abelian group we usually denote the group law by $+$ and the inverse of a group element g by $-g$. Similarly we write ng instead of g^n.

Definition 2.5 *If the underlying set X of a group G is finite then we say that G is a* finite *group. The number of elements of X is then called the* order *of G and is written $|G|$. A group that is not finite is called an* infinite *group.*

Download free eBooks at bookboon.com

2.3 Examples of Groups

We now give some examples of groups. The reader should verify the axioms for a group in each case.

Example 2.6

1. The empty set can't be given a group structure since the identity axiom for a group requires the existence of at least one element. Thus the simplest possible group is the *trivial group* which has order 1. This has one element e and the product structure must be $e^2 = e$. The next smallest group has order 2. If we denote its elements by e and a then the product structure is given by $e^2 = e$, $ea = a = ae$ and $a^2 = e$. This is called the *cyclic group of order* 2, denoted $\mathbb{Z}_2$.

   It is convenient for low order examples to record the product structure of a finite group in a table. For the trivial group this is

	e
e	e

   And for $\mathbb{Z}_2$ it is

	e	a
e	e	a
a	a	e

2. To generalize the last two examples, let n be a positive integer. The integers modulo n form a group of order n under addition modulo n. This is denoted by $\mathbb{Z}_n$ and is called the *cyclic group of order* n. Also if p is a prime then the nonzero integers modulo p form a group of order $p-1$ under multiplication modulo p.

3. The *Klein Four-Group* has elements e (the identity), a, b and c such that every element squared is the identity, and the product of any two nonidentity elements always gives the third. It has the following group table.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

4. The following are all examples of groups.

Download free eBooks at bookboon.com

- The set of integers $\mathbb{Z}$ with the operation of addition
- The set of rational numbers $\mathbb{Q}$ with the operation of addition
- The set of real numbers $\mathbb{R}$ with the operation of addition
- The set of complex numbers $\mathbb{C}$ with the operation of addition
- The set of rational numbers, excluding zero, $\mathbb{Z} - \{0\}$ with the operation of multiplication
- The set of real numbers, excluding zero, $\mathbb{R} - \{0\}$ with the operation of multiplication
- The set of complex numbers, excluding zero, $\mathbb{C} - \{0\}$ with the operation of multiplication

These are all examples of infinite groups.

5. The set of $n \times n$ invertible matrices over $\mathbb{R}$ forms a group under matrix multiplication, denoted $\mathrm{GL}(n, \mathbb{R})$. called the *general linear group* Similarly for invertible matrices over $\mathbb{Q}$ or $\mathbb{C}$.

6. A bijection (bijective map) from a set X to itself is called a *permutation* of X. Let $\mathrm{Sym}(X)$ denote the set of permutations of a set X. If f and g are in $\mathrm{Sym}(X)$ then we write fg for the composition $f \circ g$. Now composition of maps is associative, and there is the identity map $\mathrm{id} : X \to X$ given by $\mathrm{id}(x) = x$ which satisfies $f \circ \mathrm{id} = f = \mathrm{id} \circ f$ for all maps $f : X \to X$. Moreover, every bijection f from X to itself has an inverse f^{-1}, which is also a bijection. Hence $\mathrm{Sym}(X)$ is a group under composition. In particular, if X is a finite set of n elements then we obtain a finite group, called the nth *symmetric group*, which we denote by S_n. It is easy to see that for each n, S_n has order $n!$.

   Let $X = \{1, 2, 3\}$ be a set with three elements. Then $\mathrm{Sym}(X)$ has $3! = 6$ elements. These are as follows.

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad a^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$u = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad v = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad w = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Exercise 2.7 Verify that S_3 has the following multiplication table:

Download free eBooks at bookboon.com

	e	a	a^2	u	v	w
e	e	a	a^2	u	v	w
a	a	a^2	e	v	w	u
a^2	a^2	e	a	w	u	v
u	u	w	v	e	a^2	a
v	v	u	w	a	e	a^2
w	w	v	u	a^2	a	e

7. The *dihedral group* D_{2n} is the group of symmetries of an n -sided regular polygon. For example a square has 8 such symmetries, 4 rotational symmetries through angles of 0, 90 , 180 and 270 degrees, and 4 reflectional symmetries. If r denotes reflection through 90 degrees and s denotes one of the reflections then the 8 elements of D_8 are e ,r ,r^2,r^3,s ,rs ,r^2s and r^3s . The corresponding group table is as follows.

	e	r	r^2	r^3	s	rs	r^2s	r^3s
e	e	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
r^2	r^2	r^3	e	r	r^2s	r^3s	s	rs
r^3	r^3	e	r	r^2s	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	e	r^3	r^2	r
rs	rs	s	r^3s	r^2s	r	e	r^3	r^2
r^2s	r^2s	rs	s	r^3s	r^2	r	e	r^3
r^3s	r^3s	r^2s	rs	s	r^3	r^2	r	e

Click on the ad to read more

Download free eBooks at bookboon.com

3 Subgroups

This section concerns subgroups, groups within groups. The type of subgroups a group can contain is a primary concern of group theory.

3.1 Definition of a Subgroup

A subgroup is the group-theoretic analogy of a subset in set theory. To be a genuine analogy the definition has to say something about group structure too.

Definition 3.1 *Let $G = (X, m)$ be a group. A nonempty subset H of X is called a* subgroup *of G if (H, m) is also a group.*

So a subgroup of a group G is a nonempty subset of G which is a group with respect to the multiplication it inherits from G.

Example 3.2 Consider multiplication table of the symmetric group S_3 from the last section. We see that $\{e\}$ $\{e, u\}$, $\{e, v\}$, $\{e, w\}$ and $\{e, a, a^2\}$ are all subgroups of S_3. In fact these are the only ones.

Exercise 3.3 List the subgroups of D_8.

The following is important. It is usually how you would prove that something is a subgroup:

Theorem 3.4 *Let G be a group. Then a nonempty subset H of G is a subgroup of G if and only if the following two conditions hold*

1. *For all h and k in H, hk is in H.*
2. *For all h in H, h^{-1} is in H.*

Proof. It is clear that a subgroup satisfies the two conditions. Conversely, suppose that H is any subset of G which satisfies the two conditions. By the first condition the group law on G defines a group law on H. The axiom of associativity holds since it does in H. Since H is nonempty there exists an element $h \in H$. By the second condition the inverse h^{-1} of h in G belongs to H. Thus by the first condition, $hh^{-1} = e_G \in H$, which is also the identity of H. Now the axiom of inverses holds by the second condition. □

Exercise 3.5 Show that the two conditions in the previous theorem are equivalent to the following one: For all h and k in H, $hk^{-1} \in H$.

Download free eBooks at bookboon.com

If G is a group then G and $\{e\}$ are always subgroups of G. A subgroup of G not equal to G is called a *proper* subgroup. Sometimes you will see the notation $H \leqslant G$ meaning H *is a subgroup of* G and $H < G$ meaning H *is a proper subgroup of* G. This is analogous to the set-theoretic notation $X \subset Y$ and $X \subseteq Y$. But we will not stick to this convention strictly, so $H < G$ is usually just used to mean any subgroup.

Exercise 3.6 Let G be a group and let H and K be subgroups of G.

1. Show that $H \cap K$ is a subgroup of G.

2. Show that if $H \cup K$ is a subgroup of G then either $H \subset K$ or $K \subset H$.

3. Define HK to be the subset $\{hk \mid h \in H_1, k \in K\}$ and define KH analogously. Show that HK is a subgroup of G if and only if $HK = KH$. (This happens, for example, when G is abelian.)

3.2 Cosets

Definition 3.7 *Let H be a subgroup of G. Then given an element g of G, we define $gH = \{gh \mid h \in H\}$ and $Hg = \{hg \mid h \in H\}$. Any set of the form gH for some $g \in G$ is called a* left coset *of H. Similarly, any set of the form Hg for some $g \in G$ is called a* right coset.

Exercise 3.8 Let H be the subgroup $\{e, u\}$ of S_3. Calculate the left and right cosets of H.

In a non-abelian group the left cosets and right cosets of a subgroup are not necessarily the same. But cosets always have the following important property:

Theorem 3.9 *The left (or right) cosets of a subgroup H of G form a partition of G. Moreover there is a bijection between any two left (or right) cosets.*

Proof. We prove the case for left cosets. The case for right cosets is identical. Let g be in G. Then g is in the coset Hg. Hence G is equal to the union of all cosets of H. To show that the cosets of H partition G we must show that two non-equal cosets are disjoint. Let Hg_1 and Hg_2 be two cosets of H in G. Suppose that there exists $g \in Hg_1 \cap Hg_2$. We want to show that $Hg_1 = Hg_2$. Let $hg_1 \in Hg_1$ and choose h_1 and h_2 in H such that $g = h_1g_1$ and $g = h_2g_2$. Then equating, we have $h_1g_1 = h_2g_2$. So $hg_1 = hh_1^{-1}h_2g_2$. Since H is a subgroup of G, $hh_1^{-1}h_2 \in H$ and we have $hg_1 \in Hg_2$. Similarly every element of Hg_2 is in Hg_1 and these cosets are equal. Thus the cosets of H in G form a partition of G.

Download free eBooks at bookboon.com

We now show that given two cosets Hg_1 and Hg_2 of H in G there exists a bijection $\theta : Hg_1 \to Hg_2$. If $hg_1 \in Hg_1$ then define $\theta(hg_1) = hg_2$. Then θ is surjective since given $hg_2 \in Hg_2$ the element $hg_1 \in Hg_1$ satisfies $\theta(hg_1) = hg_2$. Suppose that $\theta(h_1g_1) = \theta(h_2g_1)$. Then $h_1g_2 = h_2g_2$ and hence $h_1 = h_2$. This shows that θ is also injective and hence a bijection. □

3.3 Lagrange's Theorem

Theorem 3.10 (Lagrange's Theorem) *If G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$.*

Proof. By the previous theorem in the last section, each left coset of H contains $|H|$ elements. Now since G is partitioned by the left cosets of H, we must have $|G| = n|H|$ for some integer n. □

Corollary 3.11 *Let G be a finite group of prime order. Then the only subgroups of G are $\{e\}$ and G.*

Proof. If H is a subgroup of G and $|G|$ is a prime number p then $|H|$ divides p so $|H|$ is 1 or p. Hence $H = \{e\}$ or $H = G$. □

If G is a group and H is a subgroup of G then the number, if finite, of cosets of H in G is called the *index* of H in G and is written $|G : H|$. (If H has infinitely many cosets in G then we say that it has *infinite index* in G.) If G is finite then clearly every subgroup H of G has finite index, and we see by Lagrange's theorem above that in this case $|G : H|$ must divide $|G|$.

Exercise 3.12 Find the left and right cosets of the subgroups of D_8.

Exercise 3.13 Let G be a group and let H be a subgroup of G. If g and k are elements of G, write $g \sim k$ if and only if $gk^{-1} \in H$. Show that $\sim$ is an equivalence relation on G. What are the equivalence classes of $\sim$?

Download free eBooks at bookboon.com

4 Generators and Cyclic Groups

In this section we will look at cyclic groups, which are directly related to modular arithmetic. Cyclic groups have strong number-theoretic properties.

4.1 Orders of Group Elements

Definition 4.1 *Let G be a group and let g be an element of G. If there exists an integer $n \geqslant 1$ such that $g^n = e$ then we call g a* finite order *element of G and the smallest integer $n \geqslant 1$ such that $g^n = e$ is called the* **order** *of G, written $o(g)$. Otherwise we say that g has* infinite order.

Exercise 4.2 If G is an abelian group, then show that its set of finite order elements forms a subgroup (called its *torsion subgroup*). Find an example to show that this is not true in general groups. (Hint: Consider 2 by 2 matrices.)

Theorem 4.3 (Properties of Orders) *Let G be a group and let $o(g) = n$. Then*

1. $g^k = e$ *if and only if* n *divides* k.
2. $g^i = g^j$ *if and only if* i *is congruent to* $j \mod n$.

Proof.

Click on the ad to read more

Download free eBooks at bookboon.com

1. If n divides k then $k = nq$ for some natural number q and hence
$$g^k = g^{nq} = g^q = e.$$
Conversely, suppose that $g^k = e$. Suppose that $k = nq + r$ for some natural numbers q and r with $0 \leqslant r < n$. Then
$$e = g^k = g^{nq+r} = (g^n)^q g^r = e^q g^r = g^r.$$
But n is the smallest integer with $g^n = e$ and $r < n$ so we must have $r = 0$. This means that $k = nq$ and that n divides k.

2. If $g^i = g^j$ then $g^{i-j} = e$, in which case n divides $(i - j)$ by the first part, i.e. i is congruent to $j \mod n$.

□

Exercise 4.4 Let G be a group and let g and h be finite order elements of G.

1. Show that $o(g) = o(g^{-1})$, $o(g) = o(h^{-1}gh)$ and $o(gh) = o(hg)$.
2. If G is abelian, $o(g) = m$ and $o(h) = n$, show that $o(gh)$ divides mn. Give an example to show that $o(gh)$ need not be equal to mn. What more can be said?

4.2 Generating Sets

Definition 4.5 *If X is a subset of a group G then the subgroup of X* generated by *X, written $\langle X \rangle$, is the unique subgroup of G containing X such that for all subgroups H of G containing X, H contains $\langle X \rangle$.*

Proposition 4.6 *Let X be a subset of a group G. Then $\langle X \rangle$ is the set of all elements of G of the form*
$$x_1^{n_1} x_2^{n_2} \cdots x_m^{n_m},$$
where $x_i \in X$ for each i, $n_i \in \mathbb{Z}$ for each i and $m \in \mathbb{N}$.

Proof. Exercise. □

If X is a subset of a group G and $\langle X \rangle = G$ then we say that G is *generated by* X or that X is a *generating set* for G, and call the elements of X *generators* of G. If there exists a finite generating set for G then we say that G is *finitely generated*.

Download free eBooks at bookboon.com

4.3 Cyclic Groups

Definition 4.7 *A group is called* cyclic *if it has a generating set consisting of a single element.*

Theorem 4.8 *Finite groups of prime order are cyclic.*

Proof. Suppose that the order of G is p where p is a prime. Either G is trivial, in which case it is cyclic of order 1, or there exists an element $g \in G$ with $g \neq e$. Now the order of $\langle a \rangle$ divides p by Lagrange's theorem, and since $a \neq e$, $\langle a \rangle$ has order p and $G = \langle g \rangle$. Hence G is cyclic. □

Exercise 4.9

1. Show that cyclic groups are abelian.

2. Show that subgroups of cyclic groups are cyclic.

3. Let G be a finite cyclic group of order n generated by g.

   a) Show that every subgroup of G is of the form $\langle g^t \rangle$, where t divides n.
   b) Show that for any natural number k, the subgroup of G generated by g^k is that generated by g^t where t is the highest common factor of k and n.
   c) Hence show that g^k is a generator of G if and only if k and n are coprime.

4. Consider the cyclic group $\mathbb{Z}$ under addition and denote by $n\mathbb{Z}$ the subgroup generated by n.

   a) Find a necessary and sufficient condition on the positive integers m and n for $m\mathbb{Z}$ to be a subgroup of $n\mathbb{Z}$.
   b) Show that $6\mathbb{Z} \cap 9\mathbb{Z} = 18\mathbb{Z}$. If $m\mathbb{Z} \cap n\mathbb{Z} = q\mathbb{Z}$ then what is the relation between q, m and n?

Proposition 4.10 *Let G be a finite group of order n. Then for all $g \in G$,*

1. $o(g)$ *divides* n.

2. $g^n = e$.

Proof. Let $g \in G$.

1. The order of $\langle g \rangle$ is equal to $o(g)$, so this follows from Lagrange's theorem.

2. Let $k = o(g)$. Then by the first part $n = kr$ for some integer r. Hence $a^n = (a^k)^r = e^r = e$
.

□

Download free eBooks at bookboon.com

4.4 Fermat's Little Theorem

The following exercise gives an application of group theory to number theory.

Exercise 4.11 Let n be a natural number and let $\mathbb{Z}_n$ be the set of congruence classes of integers mod n. Let $U(\mathbb{Z}_n)$ denote the set of such classes $[m]$ with $(m, n) = 1$. Then show that $U(\mathbb{Z}_n)$ is a group under multiplication and if p is a prime then $U(\mathbb{Z}_p)$ has order $p - 1$

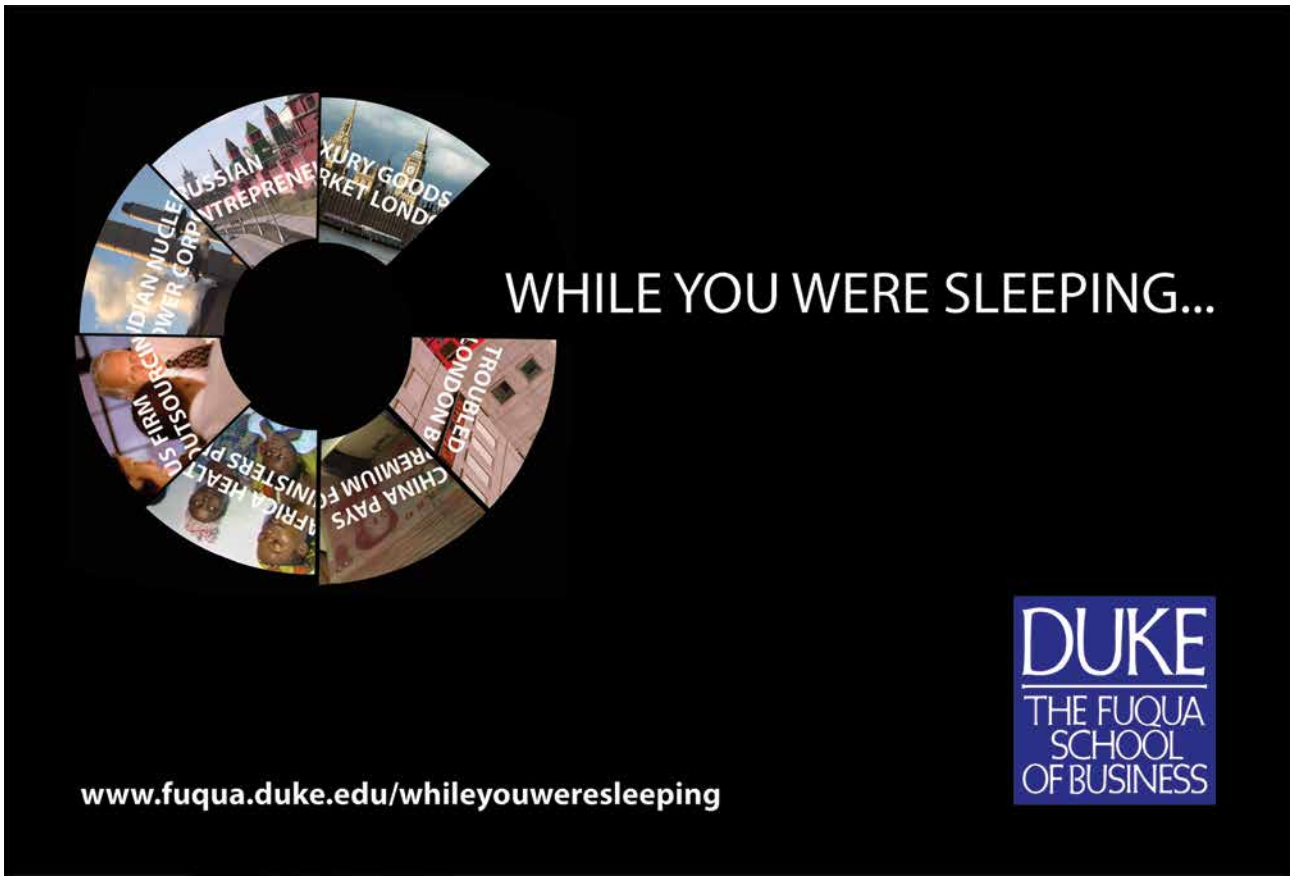
Hence prove

1. (Fermat's Little Theorem) Let p be a prime. Then for all $a \in \mathbb{Z}$ with $a \neq 0 \mod p$ we have $a^{p-1} = 1 \mod p$ and hence $a^p = a \mod p$.

2. What does Fermat's Little Theorem allow us to deduce about

   a) 2^6
   b) 2^7
   c) numbers of the form 2^n?

3. (Euler's Generalisation) Define the *Euler function* ϕ from $\mathbb{N}$ to $\mathbb{N}$ as follows. $\phi(n)$ is the number of integers k with $1 \leqslant k < n$ and $(k, n) = 1$. Then for any $n > 0$ and a such that $(a, n) = 1$ we have $a^{\phi(n)} = 1 \mod n$.



Click on the ad to read more
Download free eBooks at bookboon.com

5 Mappings of Groups

In most types of mathematics there are objects and maps which preserve the structure of these objects. In group theory, a map should preserve the multiplicative structure of the group in order to count as a real group-theoretic map.

5.1 Homomorphisms

Definition 5.1 *Let G and H be groups. Then a map $\phi : G \to H$ is called a* homomorphism *if for all g and k in G, $\phi(gk) = \phi(g)\phi(k)$.*

Exercise 5.2 If G is an abelian group then show that the map $\phi : G \to G$ given by $\phi(g) = g^n$ is a homomorphism.

Proposition 5.3 (Properties of Homomorphisms) *Let $\phi : G \to H$ be a homomorphism of groups. Then*

1. $\phi(e_G) = e_H$.
2. *For all $g \in G$, $(\phi(g))^{-1} = \phi(g^{-1})$.*

Proof.

1. For all $g \in G$, $ge_G = g$ so we have
$$\phi(ge_G) = \phi(g)\phi(e_G) = \phi(g).$$
Thus $\phi(e_G) = e_H$.

2. Since $gg^{-1} = e_G$ we have
$$\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e_G) = e_H.$$
Thus as claimed, $(\phi(g))^{-1} = \phi(g^{-1})$.

□

Example 5.4 To specify a homomorphism ϕ from G to H we only need to specify the images under ϕ of a generating set X of G. Since every element g of G can be written as a product $x_1^{n_1} \cdots x_m^{n_m}$ of terms $x_1, \ldots, x_m$ in X, we have

Download free eBooks at bookboon.com

$$\begin{aligned}\phi(g) &= \phi(x_1^{n_1}\cdots x_m^{n_m})\\ &= \phi(x_1^{n_1})\cdots\phi(x_m^{n_m})\\ &= \phi(x_1)^{n_1}\cdots\phi(x_m)^{n_m}.\end{aligned}$$

There are, however, restrictions on the possible images under ϕ of the generators. For example suppose that we wish to find all possible homomorphisms from $\mathbb{Z}_3$ to $\mathbb{Z}_{12}$. $\mathbb{Z}_3$ is cyclic, generated by 1, so a homomorphism $\phi : \mathbb{Z}_3 \to \mathbb{Z}_{12}$ is determined by $\phi(1)$. Now we also have to have

$$\phi(1+1+1) = \phi(0) = 0,$$

i.e. $3\phi(1)$ is congruent to 0 mod 12, which means that $\phi(1) = 4k$ for some integer k. This gives us the trivial homomorphism where $\phi(1) = 0$ and $\mathrm{Im}(\phi) = \{0\}$ and two nontrivial injective homomorphisms given by $\phi(1) = 4$ and $\phi(1) = 8$.

Exercise 5.5 Calculate all homomorphisms $\mathbb{Z}_6 \to \mathbb{Z}_4$ and $\mathbb{Z}_{12} \to \mathbb{Z}_5$. Generalise to $\mathbb{Z}_m \to \mathbb{Z}_n$ for arbitrary natural numbers m and n.

5.2 Isomorphisms

Definition 5.6 *An* isomorphism *is a homormorphism between groups that is also a bijection.*

We say that groups G and H are **isomorphic** if there exists an isomorphism between them, and write $G \cong H$. We usually consider two groups to be "the same" if they are isomorphic. More formally,

Theorem 5.7 *Isomorphism is an equivalence relation on any set of groups.*

Proof. Let G, H and K be groups. The identity map is an isomorphism from a group G to itself so isomorphism is reflexive. Suppose that $\phi : G \to H$ is an isomorphism. Then ϕ^{-1} is an isomorphism (check) from H to G so isomorphism is symmetric. Transitivity follows since if $\phi : G \to H$ and $\psi : H \to K$ are isomorphisms then $\phi \circ \psi : G \to K$ is an isomorphism (check). □

Example 5.8 We can write down a list of finite groups of order n up to isomorphism, where $n \leqslant 6$. There is clearly only one group of order 1, the trivial group. Also, since 2, 3 and 5 are primes, there is only one group of each of these orders, up to isomorphism, and this is the cyclic group of the given order. There are, however, two non-isomorphic groups of order 4. Suppose G is a group of order 4. If there exists an element of G of order 4 then $G \cong \mathbb{Z}_4$. Otherwise, by Lagrange's theorem, each non-identity element of G, say a, b and c, must have order 2. Now $ab \neq a$ since $b \neq e$. Also, $ab \neq e$ since $a^{-1} = a$. Thus $ab = c$ and similarly $ba = c$, $ac = ca = b$ and $bc = cb = a$. Thus G is isomorphic to the Klein four group.

Download free eBooks at bookboon.com

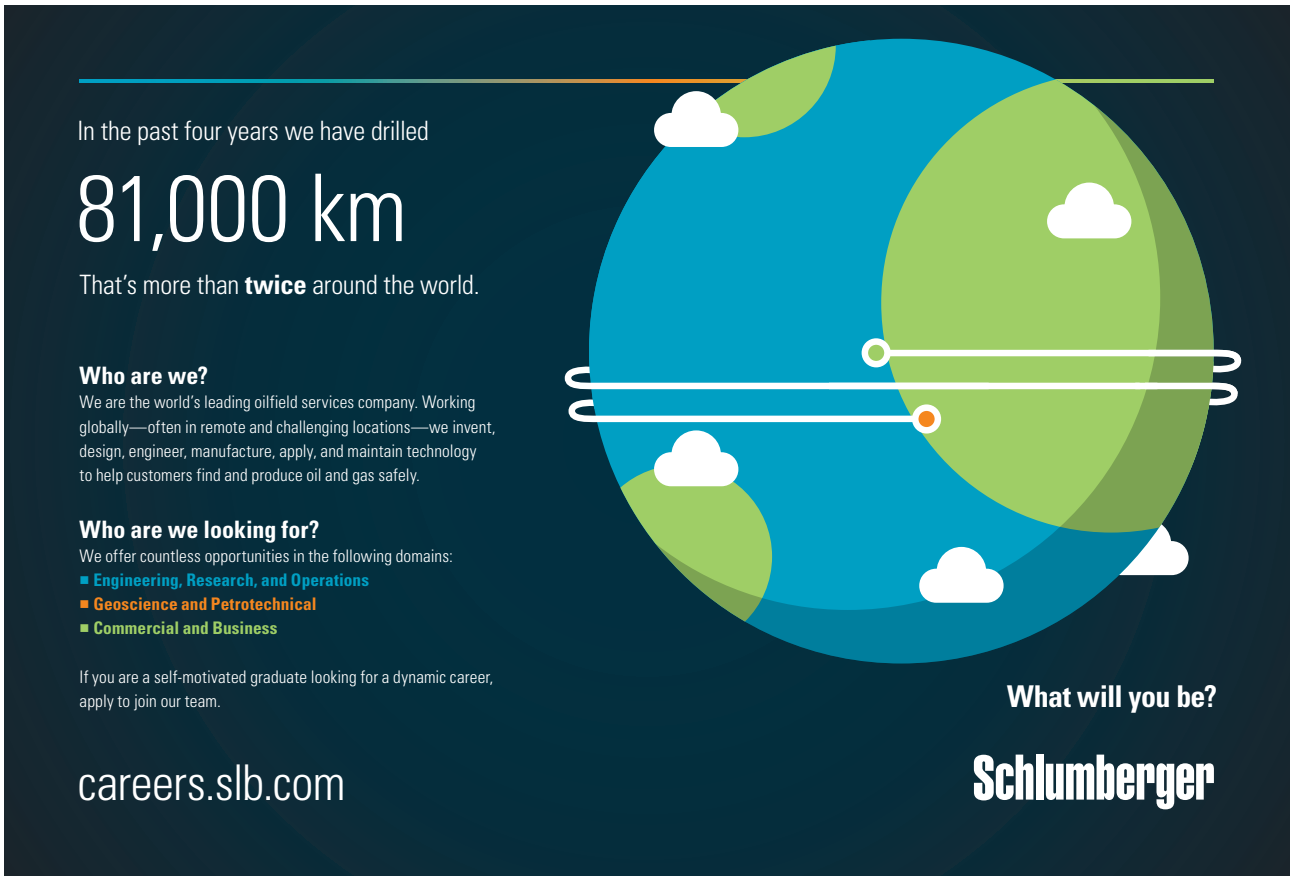
Exercise 5.9 Now suppose that G is a group of order 6. Show, by considering possible orders of elements, that G is isomorphic to either $\mathbb{Z}_6$ or S_3.

Exercise 5.10 Let G be a group. An isomorphism from G to itself is called an **automorphism** of G.

1. Prove that the set of automorphisms of G forms a group under composition (which we denote by $\mathrm{Aut}(G)$).

2. Show that $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

3. Show that $\mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$ and generalise to cyclic groups of all orders.



Click on the ad to read more

Download free eBooks at bookboon.com

6 Normal Subgroups

In this section we define a special type of subgroup called a normal subgroup. It will become apparent in the next section on quotient groups why this is such an important concept.

6.1 Conjugates and Normal Subgroups

Let H be a subgroup of a group G and let $g \in G$. Then consider the subset

$$g^{-1}Hg = \{g^{-1}hg | h \in H\}$$

of G. In fact, $g^{-1}Hg$ is a subgroup of G for suppose that $g^{-1}h_1g$ and $g^{-1}h_2g$ are elements of $g^{-1}Hg$, where h_1 and h_2 are in H. Then $g^{-1}h_1gg^{-1}h_2g = g^{-1}h_1h_2g$. Since h_1 and h_2 are in H and H is a subgroup of G, $h_1h_2 \in H$, so we have that the product of two elements of $g^{-1}Hg$ is in $g^{-1}Hg$. Similarly, if $g^{-1}hg \in g^{-1}Hg$, where $h \in H$, then $(g^{-1}hg)^{-1} = g^{-1}h^{-1}g$. Since $h \in H$ and H is a subgroup of G, $h^{-1} \in H$. Hence the inverses of elements of $g^{-1}Hg$ are also in $g^{-1}Hg$ and we have shown that $g^{-1}Hg$ is a subgroup of G. We can in fact say more.

Proposition 6.1 *Let H be a subgroup of a group G. Then for all $g \in G$, $g^{-1}Hg$ is isomorphic to H.*

Proof. Fix $g \in G$ and define the map $\phi : H \to g^{-1}Hg$ by $\phi(h) = g^{-1}hg$. Then for all h_1 and h_2 in H we have

$$\phi(h_1h_2) = g^{-1}h_1h_2g = g^{-1}h_1gg^{-1}h_2g = \phi(h_1)\phi(h_2).$$

Thus ϕ is a homomorphism. ϕ is clearly surjective, since given $g^{-1}hg \in g^{-1}Hg$, the element $h \in H$ satisfies $\phi(h) = g^{-1}hg$. Suppose that $g^{-1}h_1g = g^{-1}h_2g$. Premultiplying by g and postmultiplying by g^{-1} we see that $h_1 = h_2$. Thus ϕ is injective. We have shown that ϕ is an isomorphism and hence H is isomorphic to $g^{-1}Hg$. □

We call $g^{-1}Hg$ a *conjugate* of H. We say that two subgroups H_1 and H_2 of a group G are *conjugate* if there exists $g \in G$ such that $H_1 = g^{-1}H_2g$. Conjugacy is an equivalence relation on the set of subgroups of G, and the corresponding equivalence classes are called *conjugacy classes*.

Definition 6.2 *A subgroup H of a group G is called* normal *if for all $g \in G$ and for all $h \in H$, $g^{-1}hg \in H$.*

Equivalently a subgroup H of a group G is normal if and only if the only subgroup of G conjugate to H is H itself.

Download free eBooks at bookboon.com

Example 6.3 If G is an abelian group then every subgroup H of G is normal, since for all $g \in G$ and $h \in H$, $g^{-1}hg = g^{-1}gh = h$.

Exercise 6.4 List all the proper subgroups of the symmetric group S_3. For which subgroups are the left cosets equal to the right cosets? What are the conjugacy classes of subgroups of S_3?

6.2 Cosets of Normal Subgroups

Theorem 6.5 *Let G be a group and let H be a subgroup of G. Then H is a normal subgroup of G if and only if for all $g \in G$, $gH = Hg$.*

Proof. Suppose that H is a normal subgroup of G and let hg be an element of Hg, where $h \in H$. Then $g^{-1}hg \in H$. Suppose that it is equal to the element h' of H. Then $hg = gh'$ and $hg \in gH$. We have shown that $Hg \subset gH$. Similarly $gH \subset Hg$ and these two cosets are equal.

Conversely given $g \in G$ and $h \in H$ we have by hypothesis $hg \in gH$. Hence $hg = gh'$ for some $h' \in H$. Hence as required, $g^{-1}hg = h'$, which is in H, and H is a normal subgroup of G. □

Thus normal subgroups have the same left and right cosets.

Exercise 6.6 Show that if G is a group and H is a subgroup of G of index 2 then H is normal.

Exercise 6.7

1. Let N be a normal subgroup of a group G and let H be any subgroup of G. Show that NH is a subgroup of G.

2. If H and K are normal subgroups of a group G then show that $H \cap K$ is a normal subgroup of G.

3. If H is a subgroup of a group G and K is a normal subgroup of G then show that $H \cap K$ is a normal subgroup of H.

6.3 Kernels of Homomorphisms

Definition 6.8 *Let G and H be groups and let ϕ be a homomorphism from G to H. Then the* kernel *of ϕ, written $\ker(\phi)$ is the subset of G given by*

$$\{g \in G | \phi(g) = e_H\}.$$

Download free eBooks at bookboon.com

In other words, the kernel is the inverse image of e_H under ϕ. The kernel of a homomorphism measures its lack of injectivity: Clearly the kernel of a homomorphism $\phi : G \to H$ is equal to G if and only if ϕ is the zero map. At the opposite end of the scale, we have the following.

Proposition 6.9 *Let G and H be groups, and let $\phi : G \to H$ be a homomorphism. Then $\ker(\phi) = \{e_G\}$ if and only if ϕ is injective.*

Proof. Suppose that $\phi : G \to H$ is injective and $\phi(g) = e_H$. Then since $\phi(e_G) = e_H$ for any homomorphism ϕ, we have $g = e_G$ by injectivity. Thus $\ker(\phi) = \{e_G\}$. Conversely, suppose that $\ker(\phi) = \{e_G\}$ and that for g_1 and g_2 in G, $\phi(g_1) = \phi(g_2)$. Then by the homomorphism law, $\phi(g_1 g_2^{-1}) = e_H$. So $g_1 g_2^{-1} \in \ker(\phi)$, i.e. we have $g_1 g_2^{-1} = e_G$ by assumption. Hence $g_1 = g_2$ and ϕ is injective. □

Theorem 6.10 *If G and H are groups and ϕ is a homomorphism from G to H then $\ker(\phi)$ is a normal subgroup of G.*

Proof. Let k_1 and k_2 be in $\ker(\phi)$. Then

$$\phi(k_1 k_2) = \phi(k_1)\phi(k_2) = e_G e_G = e_G.$$

Click on the ad to read more

Download free eBooks at bookboon.com

Thus $k_1k_2 \in \ker(\phi)$. Also, if $k \in \ker(\phi)$ then

$$\phi(k^{-1}) = (\phi(k))^{-1} = e_G^{-1} = e_G,$$

so $k^{-1} \in ker(\phi)$. So far we have shown that $\ker(\phi)$ is a subgroup of G. Now let $k \in \ker(\phi)$ and $g \in G$. Then we have

$$\phi(g^{-1}kg) = \phi(g^{-1})\phi(k)\phi(g) = (\phi(g))^{-1}\phi(g) = e_G.$$

Hence $g^{-1}kg \in \ker(\phi)$, showing that $\ker(\phi)$ is a normal subgroup of G. $\square$

Exercise 6.11 Let ϕ be a homomorphism from a group G to a group H. Then $\ker(\phi)$ is the inverse image under ϕ of e_H. Show that if K is any subgroup of H then its inverse image under ϕ is a subgroup of G. Moreover show that if K is normal then so is its inverse image.

Exercise 6.12 Let H be a subgroup of a group G. Then the *normaliser* N_GH of H is the subset $\{g \in G \mid Hg = gH\}$ of G. Note that if H is a normal subgroup of G then $N_GH = G$.

1. Show that N_GH is a subgroup of G and that H is a normal subgroup of N_GH. Show that N_GH is the largest subgroup of G in which H is normal.

2. Show that $g_1^{-1}Hg_1 = g_2^{-1}Hg_2$ if and only if g_1 and g_2 belong to the same right coset of $N(H)$ in G. Hence show that if G is finite then the number of subgroups of G conjugate to H is equal to $\mid G \mid / \mid N(H) \mid$.

As a converse to theorem 6.10, given a normal subgroup H of G we can always find a group K and a homomorphism $\phi : G \to K$ such that $H = \ker(\phi)$. This idea is embodied in the next two sections.

Download free eBooks at bookboon.com

7 Quotient Groups

This section shows how a quotient of a group may be formed by grouping together cosets to form elements of the quotient group. It is a direct generalisation of division in arithmetic.

7.1 Products of Cosets

Let H be a normal subgroup of a group G and let g_1H and g_2H be two left cosets of H. Then we define their product $(g_1H)(g_2H)$ to be the left coset g_1g_2H of H. Now there is a potential problem here. Suppose that $g_1H = g_3H$ were equal to $g_4H = g_2H$ without g_1g_2H being equal to g_3Hg_4H. Then which of these cosets do we define the product to be? This situation occurs often in mathematics and is usually referred to as checking that something is well defined.

Proposition 7.1 *If H is a normal subgroup of a group G then the product of left cosets of H is well defined, i.e. if $g_1H = g_3H$ and $g_2H = g_4H$ then $g_1g_2H = g_3g_4H$.*

Proof. Suppose that $g_1H = g_3H$ and $g_2H = g_4H$. Then $g_3^{-1}g_1 \in H$. Suppose that $g_3^{-1}g_1 = h_1 \in H$. Similarly we can find $h_2 \in H$ such that $g_4^{-1}g_2 = h_2$. Thus $g_1g_2 = g_3h_1g_4h_2$. But since H is a normal subgroup, $Hg_4 = g_4H$ and we can find $h_3 \in H$ such that $h_1g_4 = g_4h_3$. Hence

$$g_1g_2H = g_3g_4h_3h_2H = g_3g_4H$$

as required. □

Thus the product of left cosets is a binary operation on the set of left cosets of H. Note how this depends on H being a *normal* subgroup.

7.2 Quotient Groups

Proposition 7.2 *If H is a normal subgroup of a group G then the product of left cosets equips the set of left cosets of H with the structure of a group.*

Proof. Let g_1H, g_2H and g_3H be three left cosets of H. Then

$$\begin{aligned}
[(g_1H)(g_2H)](g_3H) &= (g_1g_2H)(g_3H) \\
&= (g_1g_2)g_3H \\
&= g_1(g_2g_3)H \\
&= g_1H(g_2g_3H) \\
&= g_1H[(g_2H)(g_3H)].
\end{aligned}$$

Download free eBooks at bookboon.com

Thus the product of left cosets is associative. Now an identity is the left coset $eH = H$, since for all $g \in G$, $(eH)(gH) = egH = gH$ and $(gH)(eH) = geH = gH$. Also, if $g \in G$, then $(gH)(g^{-1}H) = eH = H$ and $(g^{-1}H)(gH) = eH = H$. Thus $g^{-1}H$ is the inverse of the left coset gH. $\square$

We call the group defined above the *quotient group* of G by the normal subgroup H, written G/H. Note that we could equally well have defined quotient groups in terms of right cosets.

Example 7.3 Let G be the cyclic group $\mathbb{Z}_{12}$. The subgroup H of G generated by 4 consists of the elements $4,8$ and 0 and is isomorphic to $\mathbb{Z}_3$. It is clearly normal. The cosets of H are H, $1+H$, $2+H$ and $3+H$ (since $\mathbb{Z}_{12}$ is abelian, we use additive instead of multiplicative notation). The product structure on the cosets is exemplified as follows. $(1+H)+(1+H) = (1+1)+H = 2+H$, $(2+H)+(1+H) = 3+H$ and $(3+H)+(1+H) = H$. From this information we readily deduce that the coset $1+H$ generates G/H and that $G/H \cong \mathbb{Z}_4$.

Exercise 7.4 Show that if G is an abelian group and N is a subgroup of G (which is automatically normal) then G/N is abelian. Thus quotients of abelian groups are abelian.

Exercise 7.5

1. Let G be a group and let H_1 and H_2 be subgroups of G. Let $\sim$ be the relation defined on pairs of elements g_1 and g_2 of G by $g_1 \sim g_2$ if and only if there exist $h_1 \in H_1$ and $h_2 \in H_2$ such that $x = h_1 y h_2$. Show that $\sim$ is an equivalence relation on G.

2. The corresponding equivalence classes are called *double cosets* of the pair (H_1, H_2), and we write $H_1 g H_2$ for the double coset containing g. Give an example to show that, unlike ordinary cosets, two double cosets $H_1 g_1 H_2$ and $H_1 g_2 H_2$ don't necessarily have the same cardinality.

One of the big achievements in twentieth century mathematics was the *Classification of the Finite Simple Groups* (For an account, see [7]). Quotient groups are one of the tools used to study finite groups. A group is called *simple* if it has no normal subgroups other than the identity subgroup and itself. Finite simple groups are analogous to prime numbers. Finite groups that are not simple can be broken down into a chain of finitely many simple groups called a *composition series*. These series are essentially unique, by a theorem called the Jordan-Hölder theorem.

Download free eBooks at bookboon.com

8 The First Isomorphism Theorem

The main theorem in this section, the first isomorphism theorem, is used in many places in group theory.

8.1 The First Isomorphism Theorem

Suppose that we are given a homomorphism of groups $\phi : G \to H$. Then $\mathrm{Im}(\phi)$ is a subgroup of H. For suppose we are given h_1 and h_2 in $\mathrm{Im}(\phi)$. Then there exist g_1 and g_2 in G such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. By the homomorphism law,

$$h_1 h_2^{-1} = \phi(g_1)\,(\phi(g_2))^{-1} = \phi(g_1 g_2^{-1}),$$

i.e. $h_1 h_2^{-1} \in \mathrm{Im}(\phi)$ and $\mathrm{Im}(\phi)$ is a subgroup of H.

Exercise 8.1 Let G and H be groups where G is cyclic and let $\phi : G \to H$ be a homomorphism. Show that the image of ϕ is also cyclic and that if G is finite then the order of the image divides the order of G. Hence show that if G and H are any finite groups of coprime orders then there is a unique homomorphism from G to H.

Click on the ad to read more

Download free eBooks at bookboon.com

Theorem 8.2 (First Isomorphism Theorem) *Let G and H be groups and let $\phi : G \to H$ be a homomorphism. Then*

$$\frac{G}{\ker(\phi)} \cong \mathrm{Im}(\phi).$$

Proof. Let $K = ker(\phi)$ and define a map θ from G/K to $\mathrm{Im}(\phi)$ via the rule $\theta(gK) = \phi(g)$. This is well defined because suppose that $hK = gK$. Then $h \in gK$ and there exists $k \in K$ such that $h = gk$. So we have

$$\phi(h) = \phi(g)\phi(k) = \phi(g)e_G = \phi(g)$$

and hence $\theta(hK) = \theta(gK)$. We now show that θ is a homomorphism. Let g_1K and g_2K be two elements of gK. Then

$$\begin{aligned} \theta((g_1K)(g_2K)) &= \theta(g_1g_2K) \\ &= \phi(g_1g_2) \\ &= \phi(g_1)\phi(g_2) \\ &= \theta(g_1K)\theta(g_2K) \end{aligned}$$

It remains to show that θ is a bijection. Suppose that $\theta(gK) = e_H$. Then $\phi(g) = e_H$ and $g \in K$. Hence $gK = K$ which is the identity of G/K. This means that θ is injective. But if $h \in \mathrm{Im}(\phi)$ then there exists $g \in G$ with $\phi(g) = h$. Thus $\theta(gK) = \phi(g) = h$ and θ is surjective and hence an isomorphism. □

In particular, if ϕ is an surjective then $G/\ker(\phi) \cong H$.

There are also second and third isomorphism theorems. We will not treat these here but a good reference is [3]. These are also used in many places, such as the proof of the Jordan-Hölder theorem, mentioned in the last section.

Exercise 8.3 Show, using exercise 8.1, that all quotient groups of cyclic groups are cyclic.

Exercise 8.4 Consider D_{12}, the dihedral group of order 12, generated by elements a of order 6 and b of order 2. Show that $H = \{e, a^3\}$ is a normal subgroup of D_{12} (Hint: The easiest way to do this is to find a group G and a homomorphism $\phi : D_{12} \to G$ such that $H = \ker(\phi)$). The quotient group D_{12}/H is of order 6 so it is either S_3 or C_6. Which is it?

Exercise 8.5 Let $\mathrm{SL}(n, \mathbb{R})$ be the subset of the group $\mathrm{GL}(n, \mathbb{R})$ of invertible $n \times n$ matrices defined by the rule $M \in \mathrm{SL}(n, \mathbb{R})$ if and only if M has determinant 1. ($\mathrm{SL}(n, \mathbb{R})$ is called the *special linear group* over $\mathbb{R}$.) Show that $\mathrm{SL}(n, \mathbb{R})$ is a normal subgroup of $\mathrm{GL}(n, \mathbb{R})$ and that the quotient is isomorphic to the group of nonzero real numbers under multiplication.

Download free eBooks at bookboon.com

8.2 Centres and Inner Automorphisms

Exercise 8.6

1. Let G be a group. Show that the subset

$$Z(G) = \{z \in G | \text{ for all } g \in G, zg = gz\}$$

that is, the set of all elements that commute with every other element, is a normal subgroup of G. $Z(G)$ is called the *centre* of G. A group G is abelian if and only if $Z(G) = G$.

2. Recall from exercise 5.10 that the set of all automorphisms (homomorphisms from a group to itself) forms a group called $\mathrm{Aut}(G)$. Show that if we take any element g of G then we may define an automorphism of G by

$$\phi_g : g \mapsto ghg^{-1}.$$

3. Show that the set of all automorphisms of the above form is a normal subgroup of $\mathrm{Aut}(G)$. It is called the *Inner Automorphism Group* of G and is denoted by $\mathrm{Inn}(G)$.

4. Define a map $G \to \mathrm{Aut}(G)$ by $g \mapsto \phi_g$. Show that it is a homomorphism and its kernel is $Z(G)$. Hence deduce that

$$G/Z(G) \cong \mathrm{Inn}(G).$$

Incidentally, the quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the *outer automorphism group* and is denoted by $\mathrm{Out}(G)$.

Download free eBooks at bookboon.com

9 Group Actions

We have seen that the set of bijections of a set forms a group. In this section we will look at how, given a group, we can sometimes consider it as the set of bijections of a set. This can often be used to deduce facts about the structure of the group.

9.1 Actions of Groups

Let X be a set.

An *action* of a group G on X is a homomorphism $\phi : G \to \mathrm{Sym}(X)$. If $x \in X$ and $g \in G$ then we always write gx instead of $(\phi(g))(x)$. Thus the homomorphism condition tells us that for all g and h in G and for all $x \in X$, $(gh)x = g(hx)$ and $ex = x$.

Definition 9.1 *Suppose that G is a group acting on a set X and let $x \in X$. Then the* stabilizer *of x, written G_x, is the subset $\{g \in G \mid gx = x\}$ of X.*

Proposition 9.2 *If a group G acts on a set X then for all $x \in X$, G_x is a subgroup of G.*

Click on the ad to read more

Download free eBooks at bookboon.com

Proof. Let g and h be elements of G_x. Then $ghx = gx = x$. Thus $gh \in G_x$. Also if $g \in G_x$ then $g^{-1}gx = ex = x$. But $g^{-1}gx = g^{-1}x$ since g stabilizes x. Hence $g^{-1}x = x$ and $g^{-1} \in G_x$. Thus G_x is a subgroup of G. □

Definition 9.3 *Let G be a group acting on a set X and let $x \in X$. Then the* orbit *of x is the subset $Gx = \{gx \mid g \in G\}$ of X.*

If we define two elements of X to be equivalent if one lies in the orbit of the other then this is an equivalence relation (exercise). Thus the orbits partition X.

9.2 The Orbit-Stabilizer Theorem

Let G be a group acting on a set X and let $x \in X$. Denote the set of left cosets of G_x in G by G/G_x, even though this is not necessarily a quotient group as G_x may not be normal.

Theorem 9.4 (Orbit-Stabilizer Theorem) *Let G be a group acting on a set X and let $x \in X$. Then there is a bijection from G/G_x to Gx. In particular, if G is finite then for all $x \in X$,*

$$\mid G \mid = \mid Gx \mid \mid G_x \mid .$$

Proof. Let $x \in X$ and define the map $\theta : G/G_x \to Gx$ via the rule $\theta(gG_x) = gx$. Then θ is well defined, for suppose that $h \in G_x$. Then $g^{-1}h \in G_x$ so $g^{-1}hx = x$, i.e. $hx = gx$.

Let gx be in the orbit Gx. Then $\theta(gG_x) = gx$. Thus θ is surjective. Now suppose that $\theta(gG_x) = \theta(hG_x)$. Then $gx = hx$, i.e. $g^{-1}hx = x$, which means that $g^{-1}h \in G_x$. Thus $gG_x = hG_x$. So θ is injective and hence a bijection.

The last statement follows from Lagrange's theorem. □

Proposition 9.5 *Suppose that G is a group acting on a set X. Let $x \in X$ and suppose that $y \in Gx$. Then G_y is conjugate in G to (and in particular isomorphic to) G_x.*

Proof. We have $y = gx$ for some $g \in G$. Let $h \in G_x$. Then

$$ghg^{-1}(y) = ghg^{-1}gx = ghx = gx = y,$$

which means that $g^{-1}G_yg \subset G_x$. Similarly, since $x = g^{-1}y$ we have $G_x \subset g^{-1}G_yg$. Thus $g^{-1}G_yg = G_x$. □

Download free eBooks at bookboon.com

Exercise 9.6

1. Show that a group acts on itself by left multiplication (or right multiplication).

2. Show that there is only one orbit in the above action. Such an action is called *transitive*.

3. Show that the stabilizer of every element in the above action is trivial. Such an action is called *free*.

4. Show that if H is a subgroup of G then G acts on the set of left cosets by left multiplication. (It is easy to write down the action, but you need to show that it is well defined and satisfies the axioms for an action).

Click on the ad to read more

Download free eBooks at bookboon.com

10 Direct Products

In this book we will look at various ways of building up a group from other groups. The simplest of these is the direct product, which is a group-theoretic analogue of the cartesian product in set theory.

10.1 Direct Products

Definition 10.1 *Let $(G, \cdot_G)$ and $(H, \cdot_H)$ be groups. Then their* **direct product** *$G \times H$ is the group whose underlying set is the cartesian product $G \times H$ and whose multiplication is given by defining the product of two pairs (g_1, h_1) and (g_2, h_2) in $G \times H$ as follows.*

$$(g_1, h_1)(g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2).$$

As with cartesian products of sets, we can extend the definition of a direct product in the obvious way to allow us to form the direct product of finitely many (or even arbitrarily many) groups.

Exercise 10.2

1. Check that this multiplication does indeed equip the cartesian product $G \times H$ of two groups G and H with the structure of a group, that the identity of $G \times H$ is (e_G, e_H) and that the inverse of a pair $(g, h) \in G \times H$ is (g^{-1}, h^{-1}).

2. Show that the direct product of two abelian groups is abelian.

3. Show that for any groups G and H we have $G \times H \cong H \times G$.

4. Let $G = H \times K$. Prove that $G/H \cong K$ and $G/K \cong H$.

10.2 Direct Products of Finite Cyclic Groups

Exercise 10.3 Show that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to the Klein four group (hence is not cyclic), whereas $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

Lemma 10.4 *If p is a prime number then $\mathbb{Z}_p \times \mathbb{Z}_p$ is not cyclic.*

Proof. Let g and h generate the first and second copies of $\mathbb{Z}_p$ respectively. Then let (g^m, h^n) be an element of $\mathbb{Z}_p \times \mathbb{Z}_p$. Suppose that $(g^m, h^n)^r = e_{\mathbb{Z}_p \times \mathbb{Z}_p}$. Then $g^{mr} = e$ and $h^{nr} = e$. Thus mr and nr both divide p. Since p is a prime, m and n both divide p. Thus the order of (g^m, h^n) must divide p. So no single element can generate $\mathbb{Z}_m \times \mathbb{Z}_n$, since a generating element would have to have order p^2. □

Theorem 10.5 *$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if and only if m and n are coprime.*

Download free eBooks at bookboon.com

Proof. Suppose that $G = \mathbb{Z}_m$ is generated by the element g and $H = \mathbb{Z}_n$ is generated by the element h. Suppose further that m and n are coprime. Since the order of $\mathbb{Z}_m \times \mathbb{Z}_n$ is mn, we only need to show that this group is cyclic. We claim that the element (g, h) generates $\mathbb{Z}_m \times \mathbb{Z}_n$. To see this, let $t = o((a, b))$. Then $a^t = e_G$ and $b^t = e_H$. Thus m and n divide t. Hence so does their least common multiple which is mn since m and n are coprime. Thus mn divides t. However, by Lagrange's theorem, t divides mn also. Hence $o((a, b)) = mn$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic.

Conversely suppose that m and n are not coprime and let p be a prime number which divides both m and n. Then $\langle g^{\frac{m}{p}} \rangle \times \langle h^{\frac{n}{p}} \rangle$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ so by lemma 10.4 it is a non-cyclic subgroup of $\mathbb{Z}_m \times \mathbb{Z}_n$. Since subgroups of cyclic groups are cyclic, $\mathbb{Z}_m \times \mathbb{Z}_n$ can't be cyclic. □

10.3 Properties of Direct Products

Proposition 10.6 *Let $G \times H$ be the direct product of two groups G and H. Let $G_0 = \{(g, e) \mid g \in G\}$ and let $H_0 = \{(e, h) \mid h \in H\}$. Then*

1. *G_0 and H_0 are normal subgroups of $G \times H$.*
2. *$G_0 \cong G$ and $H_0 \cong H$.*
3. *Each element of G_0 commutes with each element of H_0.*
4. *$G_0 \cap H_0 = \{(e_G, e_H)\}$, the identity of $G \times H$.*

Proof.

1. G_0 is a subgroup of G since if (g_1, e) and (g_2, e) are in G_0 then
$$(g_1, e)(g_2, e) = (g_1 \cdot_G g_2, e) \in G_0$$
and if $(g, e) \in G_0$ then $(g, e)^{-1} = (g^{-1}, e) \in G_0$. Now suppose that $(g_1, h) \in G$ and $(g_2, e) \in G_0$. Then
$$(g_1, h)^{-1}(g_2, e)(g_1, h) = (g_1^{-1} g_2 g_1, h^{-1} e h) = (g^{-1} g_2 g_1, e) \in G_0.$$
Thus G_0 is a normal subgroup of G. Similarly H_0 is a normal subgroup of G.

2. Define the map $\theta : G \to G_0$ by $\theta(g) = (g, e)$. It is easily checked that θ is an isomorphism. Thus $G \cong G_0$. Similarly $H \cong H_0$.

Download free eBooks at bookboon.com

3. Let $(g, e) \in G_0$ and let $(e, h) \in H_0$. Then

$$(g, e)(e, h) = (g, h) = (e, h)(g, e).$$

4. Suppose that $(g, h) \in G_0 \cap H_0$. Then $g = e$ and $h = e$. Hence $G_0 \cap H_0 = \{(e_G, e_H)\}$.

□

Theorem 10.7 *Let H and K be subgroups of a group G such that the following three conditions hold.*

1. $HK = G$.
2. $H \cap K = \{e\}$.
3. *For all* $g \in G$ *and* $h \in H$, $gh = hg$.

Then $G \cong H \times K$.

Need help with your dissertation?

Get in-depth feedback & advice from experts in your topic area. Find out what you can do to improve the quality of your dissertation!

Get Help Now

Go to www.helpmyassignment.co.uk for more info

Helpmyassignment

Click on the ad to read more

Download free eBooks at bookboon.com

Proof. Define the map $\theta : H \times K \to G$ by $\theta((h,k)) = hk$. Then θ is a homomorphism since for all (h_1, k_1) and (h_2, k_2) in $H \times K$,

$$\begin{aligned}\theta[(h_1,k_1)(h_2,k_2)] &= \theta((h_1 \cdot_H h_2, k_1 \cdot_K k_2)) \\ &= h_1 h_2 k_1 k_2 \\ &= h_1 k_1 h_2 k_2 \text{ (by condition 3)} \\ &= \theta((h_1,k_1))\theta((h_2,k_2)).\end{aligned}$$

To see that θ is surjective, let $g \in G$. Then by condition 1, $g = hk$ for some $h \in H$ and $k \in K$. Thus, under θ, (h,k) maps to g and θ is surjective Before we show that θ is injective, we claim that every $g \in G$ can be written uniquely as a product hk with $h \in H$ and $k \in K$. To see this, suppose that h_1 and h_2 are in H, k_1 and k_2 are in K and $g = h_1 k_1 = h_2 k_2$. Then $h_1 h_2^{-1} = k_2 k_1^{-1}$. But $h_1 h_2^{-1} \in H$ and $k_2 k^{-1} \in K$ since H and K are subgroups of G. Hence $h_1 h_2^{-1} \in H \cap K$ and is equal to e. Thus $h_1 = h_2$. Similarly $k_1 = k_2$. This completes the proof of the claim.

Now suppose that $\theta((h,k)) = e$. Then $hk = e$. But $ee = e$ also, where $e \in H$ and $e \in K$ (since H and K are subgroups of G). Thus $h = e$ and $k = e$ by the claim. Hence $(h,k) = (e_H, e_K) = e_{H \times K}$. Hence $\ker(\theta) = \{e_{H \times K}\}$, i.e. θ is injective. We have now shown that θ is an isomorphism, which completes the proof. □

Corollary 10.8 *Suppose that a group G can be written as a product HK, where H and K are normal subgroups of G such that $H \cap K = \{e\}$. Then $G \cong H \times K$.*

Proof. In the light of theorem 10.7, we only need to show that if H and K are normal subgroups of G with $G = HK$ and $H \cap K = \{e\}$ then every element of H commutes with every element of G. Let $h \in H$ and $k \in K$. Then since K is a normal subgroup of G, $h^{-1}k^{-1}h \in K$. Thus $(h^{-1}k^{-1}h)k \in K$ as K is a subgroup of G. Similarly, $k^{-1}hk \in H$ so $h^{-1}(k^{-1}hk) \in H$. Thus $h^{-1}k^{-1}hk \in H \cap K$. Thus $h^{-1}k^{-1}hk = e$, i.e. $hk = kh$. □

Exercise 10.9 Show that S_3 and D_4 are not isomorphic to direct products of cyclic groups.

Download free eBooks at bookboon.com

11 Sylow Theory

Sylow theory can be regarded as the starting point of the theory of finite groups. Recall that Lagrange's theorem states that the order of a subgroup of a finite group must divide the order of the larger group. Sylow theory is concerned with the *existence* of subgroups of a particular order, and is an excellent example of the use of actions of groups.

11.1 Primes and p-Groups

We will need the following number-theoretic lemma in the next section.

Lemma 11.1 *Let $p^m k$ be a natural number, where p does not divide k. Then p does not divide the binomial coefficient*

$$\binom{p^m k}{p^m}.$$

Proof. Because p is involved in most of the resulting binomial coefficients, we have

$$(a+b)^{p^m} = a^{p^m} + b^{p^m} \bmod p$$

Thus we obtain two binomial expansions for $(a+b)^{p^m k}$,

$$\sum_{i=1}^{p^m k} \binom{p^m k}{i} a^i b^{p^m k - i} = \sum_{j=1}^{k} \binom{k}{j} (a^{p^m})^j (b^{p^m})^{k-j} \bmod p$$

If we let $i = p^m$ and $j = 1$ we obtain

$$\binom{p^m k}{p^m} = k \bmod p.$$

□

Definition 11.2 *Let p be a prime. A group G is a* p-group *if every element of G has order p^n for some $n \geqslant 1$.*

Proposition 11.3 *Subgroups of finite p-groups are p-groups.*

Proof. Apply Lagrange's theorem. □

Download free eBooks at bookboon.com

11.2 Sylow's Theorem

Example 11.4 Consider the groups $G_1 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $G_2 = \mathbb{Z}_4 \times \mathbb{Z}_4$ and $G_3 = \mathbb{Z}_2 \times \mathbb{Z}_8$. All of these groups have order 16 but no two are isomorphic. G_1 has no element of order 4 as every nontrivial element has order 2 and G_2 has no element of order 8. So we can deduce nothing at all about the existence of subgroups of a group of order 16. It may or may not have a subgroup of order 8 and it may or may not have a subgroup of order 4.

The following is a partial converse to Lagrange's theorem, and is in contrast to Example 11.4. In some sense it is the k in the following theorem that "reacts with the p^m and forms the subgroup".

Theorem 11.5 (Sylow) *Let G be a group with order $p^m k$ where k is not divisible by p. Then G has a subgroup of order p^m.*

Proof. There are many ways of proving this theorem. We will follow Wielandt's proof which uses the left action of G on itself, and the number-theoretic fact about binomial coefficients from the last section.

Let X be the set of all subsets of G of order p^m. Then G acts on X by left multiplication, as in exercise 9.6.

Click on the ad to read more

Download free eBooks at bookboon.com

First note that if $Y \in X$ then for all $y \in Y$, $gy = hy$ implies that $g = h$. Suppose then that $g \in G_Y$, the stabilizer of G_Y and choose $y \in Y$. Then there can be at most p^m distinct elements of G which keep y in Y by the action. This means that the stabilizer G_Y has to satisfy $|G_Y| \leqslant p^m$.

Let O be a set consisting of exactly one element of X from each orbit of this action. Then clearly

$$|X| = \sum_{o \in O} |Go|$$

By Lemma 11.1, p does not divide $|X|$ so there must be an orbit Go such that p does not divide $|Go|$. (If p divided all of the orbit sizes then we would be able to pull it out as a common factor in the right hand side of the above sum, contradicting the fact that p does not divide $|X|$).

By the orbit-stabilizer theorem (theorem 9.4) we have

$$|G_o| = \frac{|G|}{|Go|} = \frac{p^m k}{|Go|} \geqslant p^m$$

Since we have shown above that $|G_o| \leqslant p^m$ too we must have $|G_o| = p^m$, so G_o is a subgroup of order p^m as required. □

Corollary 11.6 *The order of a finite p-group is a power of p.*

Proof. Suppose G is a finite p-group with $|G| = p^n k$ where $k \neq 1$ and k is not divisible by p. Let q be a prime dividing k. Then by Sylow's theorem, G has a subgroup of order q, which is cyclic. Thus G has an element of order q. But this contradicts the fact that G is a p-group. □

Exercise 11.7 Generalise theorem 11.5 to show that every finite group G with $|G|$ divisible by a prime power p^k has a subgroup of order p^k.

Sylow also proved theorems other than Theorem 11.5, which we will not prove here, but the techniques used are similar. Recall that every integer n can be written as a unique product of powers of prime numbers. By theorem 11.5, if p is a prime number and $|G|$ is any group then G has a subgroup H of order p^m where m is the highest power of p appearing in the prime decomposition of p (although m could be 0 and H the trivial subgroup). We will call H a *Sylow p-subgroup* of G.

- if p is a prime appearing only as a single power in the prime decomposition of $|G|$, then all the Sylow p-subgroups of G are conjugate, and hence isomorphic.

Download free eBooks at bookboon.com

- If r is the number of Sylow p-subgroups of a group G then

  1. If H is a Sylow p-subgroup of G then r divides the index $|G : H|$.
  2. $r = 1 \bmod p$.

Exercise 11.8 What are the Sylow 2-subgroups of the dihedral groups D_5 and D_4?

Exercise 11.9 Let G be a group such that the order of G only has two prime divisors, p and q, with $p \neq q$. Let P be a p-Sylow subgroup of G and let Q be a q-Sylow subgroup. Show that $P \cap Q = \{e_G\}$. Suppose that P is the only p-Sylow subgroup of G and Q is the only q-Sylow subgroup. Show that $G \cong P \times Q$.

Exercise 11.10 Find a 2-Sylow subgroup and a 3-Sylow subgroup of $S_3 \times S_3$.

Click on the ad to read more

Download free eBooks at bookboon.com

12 Presentations of Groups

Presentations of groups give a way of writing down a "minimal" amount of algebraic information which defines a group. Often it is relatively easy to write down a presentation of a group, but to deduce facts about a group from its presentation can sometimes involve deep mathematics. Notation: We will typically use 1, rather than e, when referring to the identity of a group, because e is sometimes used as a generator.

12.1 Introduction to Presentations

Recall that a subset X of a group G *generates* G, written $G = \langle X \rangle$, if for all $g \in G$ there exist finitely many elements $x_1 \dots x_n$ of X such that

$$g = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n},$$

where in each case ε_i is either 1 or -1. Note that the x_i are not necessarily distinct and that the identity of G is the special case where there are no x_i.

For example G is cyclic if $G = \langle \{x\} \rangle$ for a single element x, and we usually just write $G = \langle x \rangle$. In this case, G could be a finite cyclic group (if $s^n = 1_G$ for some n) or an infinite cyclic group.

Example 12.1

1. Suppose that we wish to equationally define the finite cyclic group $\mathbb{Z}_4$, and we declare it to be "the" group G generated by a single element s, and such that $s^4 = 1$. We abbreviate this to

   $$G \cong \langle s | s^4 = 1 \rangle$$

   or more usually just

   $$G \cong \langle s | s^4 \rangle.$$

   The problem is that other groups satisfy this property as well. For instance $\mathbb{Z}_2$ is generated by a single element s such that $s^4 = 1$, and so is the trivial group, for that matter. So we want the above notation to define "the group which satisfies this and no other constraints".

2. Let D_8 denote the dihedral group of order 8 (the group of symmetries of a square). This can easily be seen to be generated by a rotation r through 90 degrees and a reflection s in one of the diagonals of the square. In fact we have

   $$D_8 = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\},$$

Download free eBooks at bookboon.com

where rs, r^2s and r^3s are reflections as well as s. So the following equations hold in D_8.

$$r^4 = 1 \tag{12.1}$$

$$s^2 = 1 \tag{12.2}$$

$$(rs)^2 = 1 \tag{12.3}$$

$$(r^2s)^2 = 1 \tag{12.4}$$

$$(r^3s)^2 = 1 \tag{12.5}$$

It is easy to show that (4) and (5) are consequences of (3). Thus a candidate for a "presentation" (definition in terms of generators and relations) is

$$D_8 \cong \langle r, s | r^4, s^2, (rs)^2 \rangle.$$

3. Consider the symmetric group S_3, which is the group of permutations of the set $\{1, 2, 3\}$. We have

$$S_3 = \{1, (12), (23), (31), (123), (321)\}$$

and some quick calculations show that if we define $x = (12)$ and $y = (23)$ then $xy = (321)$, whence $(xy)^{-1} = yx = (123)$, and $xyx = (31)$. So $S_3 = \langle x, y \rangle$. Now x and y are transpositions, so $x^2 = y^2 = 1$ and xy is a 3-cycle, so $(xy)^3 = 1$. As in the last example we find that the facts that $(yx)^3 = 1$ and $(xyx)^2 = 1$ are redundant. So we have the following possibility for a presentation.

$$S_3 \cong \langle x, y | x^2, y^2, (xy)^3 \rangle$$

On the other hand it is readily seen that if we let $a = (12)$ and $b = (123)$, then a and b also generate G and the presentation we obtain this time is

$$S_3 \cong \langle a, b | a^2, b^3, (ab)^2 \rangle.$$

Which of these is the "right" presentation? In fact they both are. We shall see that a group can have many different presentations, although in the next section we shall see that, with the definition we give, a given presentation gives rise to a unique group, up to isomorphism.

Download free eBooks at bookboon.com

12.2 Alphabets and Words

We now define precisely what is meant by a presentation of a group

Definition 12.2 *A* paired alphabet *is a set* X *together with two disjoint subsets* X^+ *and* X^- *of* X*, such that* $X^+ \cup X^- = X$ *and a bijection* $\phi : X \to X$ *such that* $\phi(X^+) = X^-$, $\phi(X^-) = X^+$ *and* $\phi \circ \phi$ *is the identity map* $X \to X$.

We write x^{-1} for $\phi(x)$ and x^{+1} for x. Note that if X is finite then $|X|$ must be even.

Definition 12.3 *A* word w *in* X *is a finite sequence* $x_1^{\varepsilon_1}, \ldots, x_n^{\varepsilon_n}$*, where for each i,* $x_i \in X^+$ *and* ε_i *is* 1 *or* -1.

We usually write $w = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ and $L(w) = n$, where L stands for the *length* of w. A product $x \cdots x$ of m xs is denoted x^m, and x^{-m} is a corresponding product of x^{-1}s. The *inverse* of w is defined to be the word $w^{-1} = x_n^{-\varepsilon_1} \cdots x_1^{-\varepsilon_1}$. If $v = y_1^{\delta_1} \cdots y_m^{\delta_m}$ is another word in X then we define the *(word) product* wv to be the word $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} y_1^{\delta_1} \cdots y_m^{\delta_m}$. The *empty word*, i.e. the unique word of length 0, is denoted by ε. The set of all words in X is denoted by X^*.

Definition 12.4 *Let* X *be a paired alphabet. A* presentation *in* X *is a pair* (X, R) *where* R *is a set of words in* X.

Click on the ad to read more

Download free eBooks at bookboon.com

Henceforth, we always use the notation $\langle X|R\rangle$ to denote the data (X,R). The elements of R are called *relators*.

We define the group presented by $\langle X|R\rangle$ as a set of equivalence classes of words.

Let w be a word in X. A *simple operation* on w is an operation of one of the following types. By a *subword* of a word w we mean a *consecutive* subsequence of w. For example, xyx is a subword of $xyxyx$ but xxx is not.

1. Insert one of the words $r \in R$, xx^{-1} or $x^{-1}x$ for some $x \in X$ or ε between any two consecutive symbols of w or before w or after w.

2. Delete a subword $r \in R$, xx^{-1}, $x^{-1}x$ or ε from w.

Notice that these two operations are reverses of each other.

If we can obtain a word w_2 from a word w_1 by applying a simple operation then we write $w_1 \to w_2$.

Definition 12.5 *Let w_1 and w_2 be words in X. We write $w_1 \sim w_2$ if there exist finitely many words $v_1, \ldots, v_n$ in X such that*

$$w_1 \to v_1 \to \cdots \to v_n \to w_2.$$

Proposition 12.6 *$\sim$ is an equivalence relation on X^*.*

Proof. $w \to w$ by inserting the empty word anywhere in w. Thus $\sim$ is reflexive. It is symmetric because if $w_1 \sim w_2$ then for some v_i we have

$$w_1 \to v_1 \to \cdots \to v_n \to w_2$$

and by applying the reverse of the corresponding simple operations we have

$$w_2 \to v_n \to \cdots \to v_1 \to w_1.$$

Hence $w_2 \sim w_1$. It remains to prove transitivity of $\sim$. Suppose that $w_1 \sim w_2$ and $w_2 \sim w_3$. Say that we have

$$w_1 \to v_1 \to \cdots \to v_n \to w_2$$

and

Download free eBooks at bookboon.com

$$w_2 \to v_1' \to \cdots \to v_m' \to w_3.$$

Then by stringing these sets of operations together,

$$w_1 \to v_1 \to \cdots \to v_n \to w_2 \to v_1' \to \cdots \to v_m' \to w_3,$$

which gives us $w_1 \sim w_3$. $\square$

Lemma 12.7 *Let w_1, w_2, w_3 and w_4 be words in X. If $w_1 \sim w_2$ and $w_3 \sim w_4$ then $w_1 w_3 \sim w_2 w_4$.*

Proof. Suppose that

$$w_1 \to v_1 \to \cdots \to v_n \to w_2$$

and

$$w_3 \to v_1' \to \cdots \to v_m' \to w_4.$$

Then

$$\begin{aligned} w_1 w_3 \to v_1 w_3 \to \cdots \to v_n w_3 \to \quad & w_2 w_3 \quad \to w_2 v_1' \to \cdots \\ \to \quad & w_2 v_m' \quad \to w_2 w_4. \end{aligned}$$

$\square$

Denote an equivalence class of words in $\langle X|R\rangle$ by $[w]$ and define the product of two equivalence classes by the rule $[w_1][w_2] = [w_1 w_2]$. By the previous lemma the product is well defined.

Note that this construction is similar to that of a quotient group. This is no coincidence, as we shall see in the next section.

Proposition 12.8 *With the above product, the set of equivalence classes of words in X becomes a group.*

Proof. Let $[w_1]$, $[w_2]$ and $[w_3]$ be equivalence classes of words in X. Then

$$\begin{aligned} ([w_1][w_2])[w_3] &= [w_1 w_2][w_3] \\ &= [(w_1 w_2) w_3] \\ &= [w_1 (w_2 w_3)] \text{ (since the word product is associative)} \\ &= [w_1][w_2 w_3] \\ &= [w_1]([w_2][w_3]). \end{aligned}$$

Download free eBooks at bookboon.com

Hence the product of equivalence classes is associative. $[\varepsilon]$ is clearly an identity for the product. For any class $[w]$ we have $[w]^{-1} = [w^{-1}]$ because we can obtain $[\varepsilon]$ from ww^{-1} by repeatedly deleting terms of the form xx^{-1}. $\square$

12.3 Von Dyck's Theorem

From now on the notation $\langle X|R\rangle$ will refer to the above group.

Let $G = \langle X|R\rangle$ and let H be any group. If f is a map from X to H then there is a map $f^* : X^* \to H$ defined by

$$f^*(x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}) = f(x_1)^{\varepsilon_1} \cdots f(x_n)^{\varepsilon_n}.$$

Lemma 12.9 *If $f^*(R) = \{1_H\}$ then f^* induces a homomorphism $f' : G \to H$.*

This e-book
is made with
SetaPDF
SETASIGN
PDF components for PHP developers
www.setasign.com
Click on the ad to read more

Download free eBooks at bookboon.com

Proof. Define $f'([w]) = f^*(w)$. We need to show that this is well defined, i.e. that whenever $w_1 \sim w_2$ we have $f^*(w_1) = f^*(w_2)$. It suffices to show that if $w_1 \to w_2$ then $f^*(w_1) = f^*(w_2)$. There are several cases. We deal with the case where w_2 arises from w_1 via insertion of a relator and leave the other cases as an exercise for the reader. Suppose that $w_1 = vw$ and $w_2 = vrw$. Then

$$\begin{aligned} f^*(w_2) &= f^*(vrw) \\ &= f^*(v)f^*(r)f^*(w) \\ &= f^*(v)1_H f^*(w) \text{ (since } f^*(R) = \{1_H\}) \\ &= f^*(vw) \\ &= f^*(w_1). \end{aligned}$$

That f is a homomorphism follows easily from the definition of the word product. □

Corollary 12.10 (von Dyck's theorem) *If $G = \langle X|R\rangle$, $H = \langle Y|S\rangle$ and $f : X \to Y^*$ satisfies $f^*(R) \subset S$ then f extends to a homomorphism from G to H.*

Proof. If $f^*(R) \subset S$ then $f^*(R) = \{1_H\}$ since all relators in S are clearly equivalent to the identity of $\langle Y|S\rangle$ (we can delete them in a simple move). Now apply the previous lemma. □

Corollary 12.11 *Every group is isomorphic to $\langle X|R\rangle$ for some X and R.*

Proof. Let $X = G$ and let R be the set of all words in X which are equal to the identity in G. By lemma 12.9 there is a homomorphism $f' : \langle X|R\rangle \to G$ which is clearly surjective. A typical element of $\langle X|R\rangle$ is $[g]$, where $g \in G$. Suppose that $f'([g_1]) = f'([g_2])$. Then $f^*(g_1) = f^*(g_2)$ which means that $g_1 = g_2$ and hence $[g_1] = [g_2]$. This shows that f' is also injective and hence it is an isomorphism. □

12.4 Finitely Generated and Finitely Presented Groups

Recall that a group G is *finitely generated* (f.g.) if it has finite generating set, i.e. a presentation $\langle X|R\rangle$ with X finite. We say that G is *finitely presented* (f.p.) if it has a presentation $\langle X|R\rangle$ with X finite and R finite. It is possible for a group to be finitely generated but not finitely presented.

Example 12.12 We now show that the group

$$G = \langle r, s | r^4, s^2, (rs)^2\rangle$$

is isomorphic to D_8. Let $[w] \in G$ and delete all occurrences of rr^{-1}, $r^{-1}r$, ss^{-1} and $s^{-1}s$ to obtain an equivalent word of the form

$$w' = r^{n_1}s^{m_1}r^{n_2}s^{m_2}\cdots r^{n_k}s^{m_k}r^{n_{k+1}}$$

Download free eBooks at bookboon.com

with each $m_i \neq 0$ and $n_i \neq 0$ except possibly when $i = 1$ or $i = k + 1$. We can assume all m_i are equal to 1 since we can replace s^2 by ε, i.e.

$$w' \sim r^{n_1} s r^{n_2} s \cdots r^{n_k} s r^{n_{k+1}}.$$

Now $rsrs = 1$ which implies that $rs = s^{-1}r^{-1}$. Since $s^2 = 1$, $s^{-1} = s$ and we have $rs = sr^{-1}$. This allows us to gather all the s terms at the right hand side to show that $w' \sim r^n s^m$ where $m = 0$ or 1. Since $r^4 = 1$ we may also assume that $0 \leqslant n \leqslant 3$. This gives us eight words 1,r, r^2, r^3, s,rs,r^2s and r^3s which are the distinct elements of G since no further reductions are possible. By lemma 12.9 there is a homomorphism $f' : G \to D_8$. f' is injective as it maps each of the above words to a distinct element of D_8. Since $|G| = 8 = |D_8|$ it must also be surjective and is hence an isomorphism.

Exercise 12.13

1. Show that

   a) $\langle x, y | x^2, y^2, (xy)^3 \rangle \cong S_3$

   b) $\langle a, b | a^2, b^3, (ab)^2 \rangle \cong S_3$

3. Generalise the first of these presentations to obtain a presentation $\langle X_4 | R_4 \rangle$ of S_4, proving formally that $\langle X_4 | R_4 \rangle \cong S_4$.

4. Generalise further to obtain a presentation $\langle X_n | R_n \rangle$ of S_n, proving formally that $\langle X_n | R_n \rangle \cong S_n$.

12.5 Dehn's Fundamental Algorithmic Problems

In the previous section we constructed a "normal form" for G, which is a unique choice for all $g \in G$, of a word representing g. This is closely related to the first of three fundamental problems posed by Dehn in 1912:

1. *The word problem:* Given $G = \langle X | R \rangle$, does there exist an algorithm which takes a word $w \in X^*$ as its input and after finitely many steps gives the output either "yes" or "no", "yes" if the word is equal to the identity in G and "no" otherwise.

2. *The conjugacy problem:* Given $G = \langle X | R \rangle$, does there exist an algorithm which takes two words w_1 and w_2 in X as its input and after finitely many steps give the output either "yes" or "no", "yes" if the two elements are conjugate in G (i.e. there exists an element $g \in G$ such that $[w_1] = g^{-1}[w_2]g$) and "no" otherwise.

Download free eBooks at bookboon.com

3. *The isomorphism problem:* Given a class C of groups, does there exist an algorithm which takes as its input two presentations $\langle X_1|R_1\rangle$ and $\langle X_2|R_2\rangle$ of groups in C and after finitely many steps gives the output either "yes", the two groups are isomorphic, or "no", they are not.

If the algorithm in any of these problems exists then we say that the problem is *solvable* for the given group or class of groups. The precise mathematical definition of an *algorithm* depends on the notion of a *Turing machine* and is beyond the scope of this book.

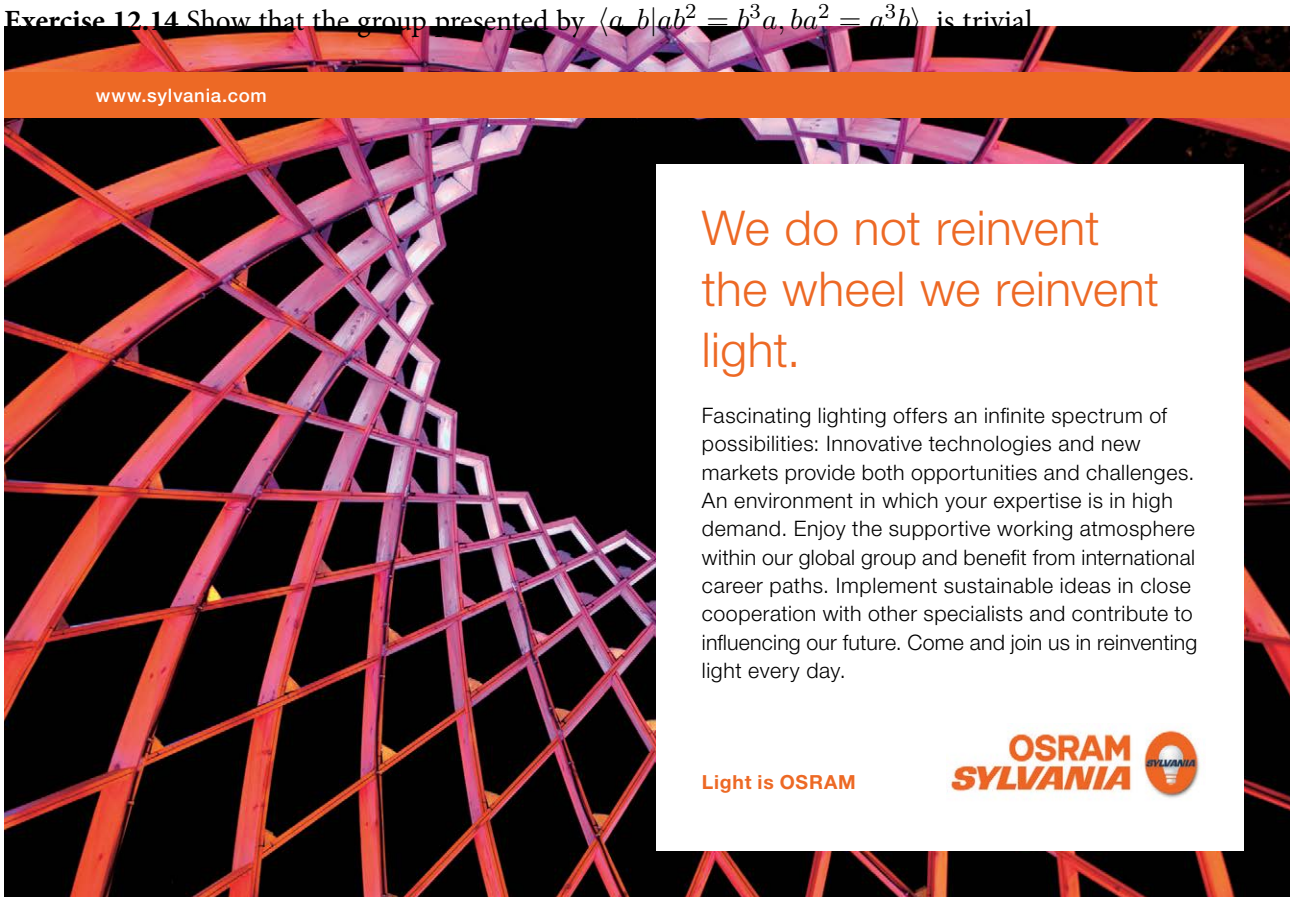
Note that the word problem for G is a special case of the conjugacy problem. There are deep theorems of Novikov and Boone which assert that

1. There exists a finitely presented group with unsolvable word problem (and hence unsolvable conjugacy problem).

2. The isomorphism problem is unsolvable for the class of finitely presented groups.

In fact there is no algorithm which takes as its input a finite presentation $\langle X|R\rangle$ and after finitely many steps tells us either "yes" if the group it presents is trivial or "no" if it is not. The following exercise may give you some appreciation of this fact.

Exercise 12.14 Show that the group presented by $\langle a, b|ab^2 = b^3a, ba^2 = a^3b\rangle$ is trivial.



Click on the ad to read more

Download free eBooks at bookboon.com

13 Free Groups

Free groups are groups with the simplest types of presentations, in that they have presentations without any relators. Every group is a quotient of a free group, because by adding relators to form a presentation, we are really forming quotient groups.

13.1 Reduced Words and Free Groups

Let $\emptyset$ denote the empty set.

Definition 13.1 *A group G is said to be* free *on a set X if $G \cong \langle X|\emptyset\rangle$. G is said to be* free *if it is free on some set.*

We also write $G = F(X)$, meaning that G is free on X. If X is finite then we say that G has *rank* n, where $n = |X^+|$, and write F_n for $F(X)$, usually for $n \geqslant 2$.

The equivalence relation we introduced in the last section now becomes $w_1 \to w_2$ if we can obtain w_2 from w_1 by inserting or deleting a word of the form xx^{-1}, $x^{-1}x$ ($x \in X$) or ε, and if we can obtain w_2 from w_1 by finitely many of these operations.

Let $w \in X^*$. By deleting all occurrences of xx^{-1} or $x^{-1}x$, we obtain a representative w_r of $[w]$ called a *reduced word*. We shall write X_r^* for all reduced words in the paired alphabet X.

Exercise 13.2 Show that every element of the free group $F(X)$ is represented by a unique reduced word in X.

Example 13.3

1. Let $X = \{x, x^{-1}\}$. A reduced word in X is a word of the form x^n for some $n \in \mathbb{Z}$. These words all represent distinct elements of $F(X)$ and it is easy to see that $F(X) \cong \mathbb{Z}$.

2. The free group F_2 of rank 2 is a more interesting group. Let $X = \{a^{\pm 1}, b^{\pm 1}\}$. Reduced words of length two in $F(X)$ are a^2, ab, ab^{-1}, b^2, ba, ba^{-1}, a^{-2}, $a^{-1}b$, $a^{-1}b^{-1}$, b^{-2}, $b^{-1}a$ and $b^{-1}a^{-1}$. These all represent distinct elements of F_2. Don't confuse F_2 with $\mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$, the direct product of two inifinte cyclic groups. This has presentation

$$\langle a, b | aba^{-1}b^{-1}\rangle$$

and is abelian. By looking at the above list of words we see that F_2 is definitely not abelian. For instance ab is not equal to ba.

Download free eBooks at bookboon.com

The following is sometimes taken as the definition of a free group.

Theorem 13.4 *Let X be a set and G be a group. Then every map $f : X \to G$ extends to a unique homomorphism $\theta : F(X) \to G$.*

Proof. There is a homomorphism $\theta : F(X) \to G$ by von Dyck's theorem, whose conditions are satisfied vacuously. Suppose that $\theta' : F(X) \to G$ is another homomorphism which extends f. Let $x_1^{n_1} \cdots x_m^{n_m}$ be a typical element of $F(X)$. Then

$$\begin{aligned} \theta'(x_1^{n_1} \cdots x_m^{n_m}) &= \theta'(x_1)^{n_1} \cdots \theta'(x_m)^{n_m} \\ &= \theta(x_1)^{n_1} \cdots \theta(x_m)^{n_m} \\ &= \theta(x_1^{n_1} \cdots x_m^{n_m}) \end{aligned}$$

And so $\theta' = \theta$. □

Corollary 13.5 *Every group is isomorphic to a quotient of a free group.*

Proof. Let G have the presentation $\langle X|R\rangle$ (recall that every group has a presentation). Now the inclusion map $f : X \to G$ given by $f(x) = x$ extends to a homomorphism $f' : F(X) \to G$. X generates G so f' is surjective. Thus, by the first isomorphism theorem, $F(X)/\ker(f) \cong G$. □

13.2 Normal Closure

The following exercise investigates the structure of $\ker(f)$ as in the last proof.

Exercise 13.6 Let H be any group and let Y be a subset of H . Then the *normal closure* of Y in H is defined to be the subgroup

$$\langle h^{-1}yh|y \in Y, h \in H\rangle$$

of H , written $\langle\langle Y\rangle\rangle_H$.

1. Show that if N is any normal subgroup of H containing Y then $\langle\langle Y\rangle\rangle_H \subseteq N$.

2. Show that $\langle\langle Y\rangle\rangle_H$ is equal to the intersection of all normal subgroups of H which contain Y.

3. Suppose that $G = \langle X|R\rangle$ and that $G \cong F(X)/K$. Denote by $[R]$ the subset

$$\{[r]|r \in R\}$$

of $F(X)$. Show that $K = \langle\langle [R]\rangle\rangle_F$.

Download free eBooks at bookboon.com

Exercise 13.7 Show that if G is a group and H and K are subgroups of finite index of G then $H \cap K$ has finite index in G.

13.3 Torsion Free Groups

A group G is said to be *torsion free* if the only element of finite order in G is e_G, the identity of G.

Theorem 13.8 *Free groups are torsion free.*

Proof. Let F be free on a set X and let $w = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ be a nonempty word in X_r^*, where each $\varepsilon_i \in \{-1, 1\}$ and each $x_i \in X$. If $((x_n)^{\varepsilon_n})^{-1} \neq x_1^{\varepsilon_1}$ then $w^n \in X_r^*$ and

$$w^n = (x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n})(x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}) \cdots (x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n})$$

which is not the empty word.

On the other hand, if $((x_n)^{\varepsilon_n})^{-1} = x_1^{\varepsilon_1}$ then there exists $j < n/2$ such that $w = u^{-1}vu$, where $u^{-1} = x_1^{\varepsilon_1} \cdots x_j^{\varepsilon_j}$, $u = (x_j^{\varepsilon_j})^{-1} \cdots (x_1^{\varepsilon_1})^{-1}$ and v is reduced. Then as w is nonempty, so is v and v has infinite order by the first case. Since $w^n = u^{-1}v^n u$ is a reduced word of length $2j + nL(v)$, w^n is never trivial in F and has infinite order. $\square$

Exercise 13.9 This shows that subgroups of finitely generated groups need not necessarily be finitely generated. Let

$$\theta : F_2 = \langle a, b \rangle \ \to \mathbb{Z} = \langle x \rangle$$

be the homomorphism induced by mapping $a \mapsto x$ and $b \mapsto x$. Show that $\ker(\theta)$ is not finitely generated. (Hint: Let $x_1, \ldots, x_k$ be arbitrary elements of F_2 and find an element of F_2 not in $\langle x_1, \ldots, x_k \rangle$.)

The direct product $F_2 \times F_2$ is an interesting group. It can be shown that $F_2 \times F_2$ has uncountably many non-isomorphic subgroups, including subgroups which are finitely generated but not finitely presented [2]. Such a group is called *incoherent* (a group G is *coherent* if, on the other hand, every finitely generated subgroup of G is finitely presented).

Download free eBooks at bookboon.com

The theory of free groups can be surprisingly deep and is still an active area of mathematical research. It is a well known theorem that every subgroup of a free group is free. Furthermore, if H and K are non-trivial finitely generated subgroups of a free group F, then their intersection is also finitely generated. It was an open problem since 1956 that

$$\text{rank } H \cap K - 1 \leq (\text{rank } H - 1)(\text{rank } K - 1)$$

This is an extremely difficult problem known as the *Hanna Neumann Conjecture*. A full proof of this result was announced in 2011 by Mineyev[10].

Click on the ad to read more

Download free eBooks at bookboon.com

14 Abelian Groups

In this section we look at abelian groups and some constructions related to abelian parts of groups. We will apply these to free groups to show that free groups of different rank are non-isomorphic. A well known structure theorem for finitely generated abelian groups is given, and we mention various generalisations of abelian groups.

14.1 Commutator Subgroups and Abelianisations

We now aim to show that F_n is not isomorphic to F_m unless $n = m$. This will involve introducing one or two new concepts.

Definition 14.1 *Let G be a group and let g and h be in G. The* commutator *of g and h is $g^{-1}h^{-1}gh$, written $[g, h]$. The* commutator subgroup *of G, written G', is*

$$\langle [g, h] \mid g, h \in G \rangle.$$

Proposition 14.2 *Let G be a group. Then*

1. *G' is a normal subgroup of G.*
2. *G/G' is abelian. Moreover, if H is any normal subgroup of G, then G/H is abelian if and only if $G' \subseteq H$.*

Proof.

1. Clearly G' is a subgroup of G. So we only have to show that it is normal. First observe that for any g, h and k in G we have

$$\begin{aligned} g^{-1}[h, k]g &= g^{-1}h^{-1}k^{-1}hkg \\ &= g^{-1}h^{-1}gg^{-1}k^{-1}gg^{-1}hgg^{-1}kg \\ &= [g^{-1}hg, g^{-1}kg]. \end{aligned}$$

Now let $g \in G$ and $g' \in G'$. Since $g' \in G'$ we can write it as a product of powers of commutators, say

$$g' = [g_1, h_1]^{n_1} \cdots [g_r, h_r]^{n_r}.$$

Then we have

$$\begin{aligned} g^{-1}g'g &= g^{-1}[g_1, h_1]^{n_1} \cdots [g_r, h_r]^{n_r} g \\ &= (g^{-1}[g_1, h_1]g)^{n_1} \cdots (g^{-1}[g_r, h_r]g)^{n_r} \\ &= [g^{-1}g_1g, g^{-1}h_1g]^{n_1} \cdots [g^{-1}g_rg, g^{-1}h_rg] \in G'. \end{aligned}$$

So G' is a normal subgroup of G as required.

Download free eBooks at bookboon.com

2. Suppose that H is a normal subgroup of G and let g_1 and g_2 be in G. Then $g_1 g_2 H = g_2 g_1 H$ if and only if $[g_1, g_2]H = H$, i.e. if and only if $[g_1, g_2] \in H$. Thus G/H is abelian if and only if $G' \subset H$.

□

Thus G/G' is the "largest abelian quotient" of G. It is called the *abelianisation* of G, and is written G_{ab}.

The commutator subgroup is an example of what is called a *verbal* subgroup. If $w_1, \ldots, w_n$ are words in a paired alphabet X then the *verbal* subgroup generated by $w_1, \ldots, w_n$ is the subgroup $\langle w_1(G), \ldots, w_n(G) \rangle$ (i.e. the subgroup generated by all elements of G obtained by replacing each $x^{\pm 1}$ in each w by $g^{\pm 1}$ for some element g of G). Another example is the subgroup of G generated by n^{th} powers $G^n = \langle g^n \mid g \in G \rangle$.

Exercise 14.3

1. Show that if V is a verbal subgroup of a group G then for all homomorphisms $\theta : G \to G$ (called *endomorphisms* of G) we have $\theta(V) \subseteq V$. A subgroup with the above property is called *fully characteristic*, and *characteristic* if it is invariant under at least all automorphisms of G. Show that both of these properties generalise the idea of a normal subgroup. Deduce that verbal subgroups are normal.

2. Show that if F is a free group and H is a subgroup of F such that $\theta(H) \subseteq H$ for all endomorphisms θ of F then H is verbal.

14.2 Free Abelian Groups

Definition 14.4 *A* free abelian *group is a group which is isomorphic to a direct product of (zero or more) infinite cyclic groups.*

For example, the free abelian group of *rank* n is the group $\mathbb{Z}^n = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ with n free factors. This has a presentation

$$\langle x_1, \ldots x_n \mid [x_i, x_j] \text{ for all } 1 \leqslant i < j \leqslant n \rangle.$$

Before giving a presentation of the abelianisation of a group, we have the following general theorem which shows us how to present quotient groups.

Theorem 14.5 *Let $G \cong \langle X \mid R \rangle$, let W be a set of words in X and let N be the normal closure $\langle\langle W \rangle\rangle_G$ (see exercise 13.6). Then $G/N \cong \langle X \mid R \cup W \rangle$.*

Download free eBooks at bookboon.com

Proof. Define $p : X \to G/N$ via $p(x) = xN$. Denote $\langle X \mid R \cup W \rangle$ by Q. If $r \in R$ then $[r] = 1_Q$ so $p^*([r]) = N = 1_{G/N}$ and if $w \in W$ then $p^*([w]) = N = 1_{G/N}$ since $[w] \in N$. So by Lemma 12.9 there is a homomorphism

$$p' : Q \to \frac{G}{N}.$$

Since $G = \langle X \rangle$, $p'(X)$ generates G/N and p' is surjective. To show that p' is injective we show that $\ker(p') = \{1_Q\}$. Suppose that $[k] \in \ker(p')$. Then $p'([k]) = 1_{G/N} = N = \langle\langle W \rangle\rangle_G$. By definition of p', $[k] \in N$. So there exist $g_i \in G$ and $w_i \in W^{\pm 1}$ such that

$$k \sim g_1^{-1}[w_1]g_1 g_2^{-1}[w_2]g_2 \cdots g_r^{-1}[w_r]g_r.$$

But in $\langle X \mid R \cup W \rangle$ we can delete all words w_i and cancel each $g_i^{-1}g_i$ term to obtain $k \sim \varepsilon$. Thus $[k] = 1_Q$ and p' is injective and an isomorphism. $\square$

Proposition 14.6 *Let* $G = \langle X \mid R \rangle$. *Then*

$$G_{\mathrm{ab}} \cong \langle X \mid R \cup \{[x_1, x_2] \mid x_1, x_2 \in X\} \rangle.$$

Deloitte.

Discover the truth at www.deloitte.ca/careers

© Deloitte & Touche LLP and affiliated entities.

Click on the ad to read more

Download free eBooks at bookboon.com

Proof. G' is a normal subgroup of G so $\langle\langle G'\rangle\rangle_G = G'$. Thus $G_{\mathrm{ab}} = G/G'$ has a presentation

$$G_{\mathrm{ab}} \cong \langle X \mid R \cup \{[g_1, g_2] \mid g_1, g_2 \in G\}\rangle.$$

by the previous theorem. However it is easy to see that the set of relators $\{[g_1, g_2] \mid g_1, g_2 \in G\}$ can be derived from the set of relators $\{[x_1, x_2] \mid x_1, x_2 \in X\}$. □

Thus for all n, $(F_n)_{\mathrm{ab}} \cong \mathbb{Z}^n$.

Theorem 14.7 *$F_n \cong F_m$ if and only if $m = n$.*

Proof. It is clear that if $m = n$ then $F_n \cong F_m$. Conversely if $F_n \cong F_m$ then $F_n' \cong F_m'$ and hence $(F_n)_{ab} \cong (F_m)_{ab}$, i.e. $\mathbb{Z}^n \cong \mathbb{Z}^m$. But then

$$\begin{aligned} \frac{\mathbb{Z}^n}{2\mathbb{Z}^n} &\cong \frac{\mathbb{Z}^n}{\langle 2g \mid g \in \mathbb{Z}^n\rangle} \\ &\cong \frac{\mathbb{Z}^m}{2\mathbb{Z}^m} \end{aligned}$$

which means that $\mathbb{Z}_2^n \cong \mathbb{Z}_2^m$. But $\mathbb{Z}_2^n$ is a vector space of dimension n over the finite field $\mathbb{Z}_2$ and if $\mathbb{Z}_2^n \cong \mathbb{Z}_2^m$ then their dimensions are equal. Thus $m = n$. □

14.3 Finitely Generated Abelian Groups

The structure of finitely generated abelian groups is very simple, as the following theorem shows:

Theorem 14.8 *If G is an abelian group that can be generated by n elements then G is isomorphic to a direct product of $m \leqslant n$ cyclic subgroups.*

Proof. Omitted as it is quite long – the idea is to mimic ideas from linear algebra, and to formulate the concept of a basis in finitely generated abelian groups. □

14.4 Generalisations of Abelian Groups

Two important generalisations of abelian groups are *soluble* (or *solvable*) groups and nilpotent groups. We will only give a rough idea of these here, but if you want to read more there is some recommended reading in chapter 19.

Download free eBooks at bookboon.com

When we form the commutator subgroup of a group, we can repeat the process. In general if A and B are subsets of a group G, write

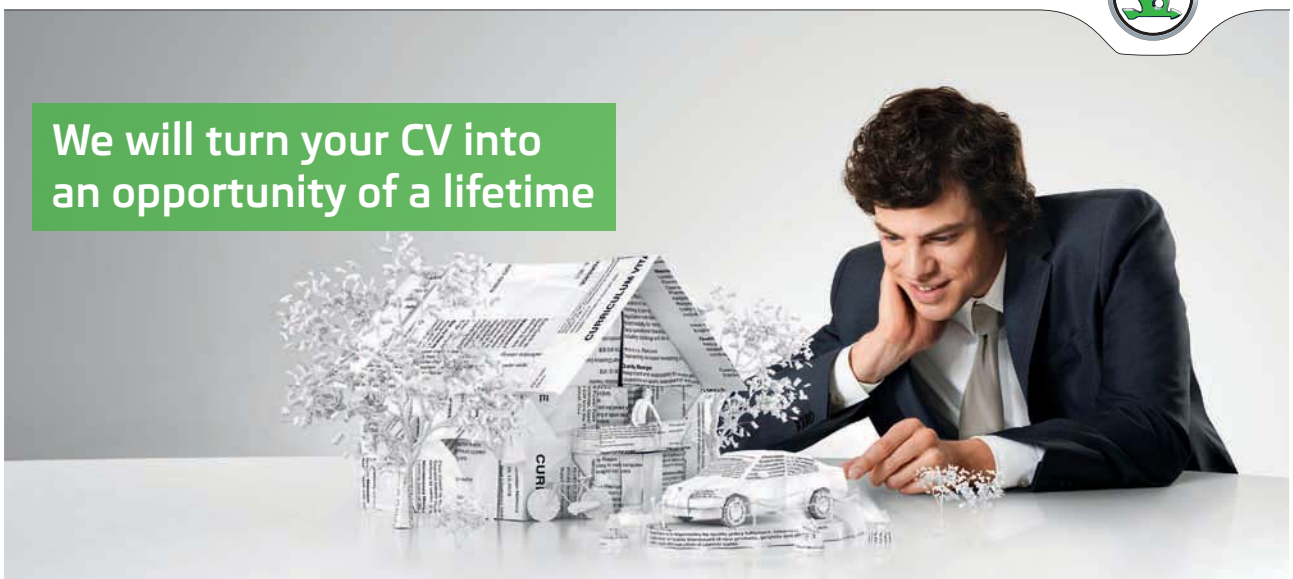
$$[A, B] = \langle\{[a, b] | a \in A, b \in B\}\rangle.$$

That is, the subgroup generated by all of the commutators shown. Let $G^{(0)} = G$, $G^1 = G' = [G, G]$ and define $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$ for all n. Clearly $G^{(0)} = 1$ iff G is trivial and $G^{(1)} = 1$ iff G is abelian. If $G^{(n)} = 1$ for some n then we say that G is *soluble*.

Solubility was one of the first important concepts defined in group theory, by Evariste Galois, who used the concept to show that it is not possible to solve a quintic equation by a general formula using radicals (roots). This had already been proved slightly earlier by Niels Abel (after whom abelian groups are named) but the ideas of Galois were further reaching: we can define a *symmetry group* of such an equation and it turns out we can solve by radicals if and only if this group is soluble.

In another generalisation of abelian groups we write $\gamma_1(G) = G$ and $\gamma_n(G) = [\gamma_{(n-1)}(G), G]$. The series of subgroups so obtained is called the *lower central series* of G. If for some n we have $\gamma_n = 1$ then we say that G is *nilpotent*. Nilpotent groups have also been extensively studied. They enjoy strong properties – for example every subgroup and quotient group of a nilpotent group is solvable. They also have some of the properties of abelian groups. For instance, the set of finite order elements forms a subgroup (see exercise 4.2 for the abelian case).

SIMPLY CLEVER
ŠKODA



Do you like cars? Would you like to be a part of a successful brand?
We will appreciate and reward both your enthusiasm and talent.
Send us your CV. You will be surprised where it can take you.

Send us your CV on
www.employerforlife.com

Click on the ad to read more

Download free eBooks at bookboon.com

15 Transforming Presentations

Tietze transformations give us a way of passing between different presentations of the same group. Given two such presentations, we can always find a finite sequence of these transformations which carries one presentation to the other.

15.1 Tietze Transformations

Example 15.1

1. We saw in section 1.2 that

$$S_3 \cong \langle x, y \mid x^2, y^2, (xy)^3 \rangle.$$

Let $a = x$ and let $b = xy$. We can then add the generators a and b to the presentation, provided that we also add as relators what they are equal to as words in the other generators. This gives

$$S_3 \cong \langle x, y, a, b \mid x^2, y^2, (xy)^3, xa^{-1}, xyb^{-1} \rangle.$$

Now, since x is given as an expression in terms of the other generators via the relator xa^{-1} we may replace x by a in the other relators and delete x and the relator xa^{-1}. This gives

$$S_3 \cong \langle y, a, b \mid a^2, y^2, (ay)^3, ayb^{-1} \rangle.$$

We may also solve for y; $y = a^{-1}b$ from the relator ayb^{-1}. So we can replace y by $a^{-1}b$ in the other relators and delete y and the final relator. Hence

$$S_3 \cong \langle a, b \mid a^2, (a^{-1}b)^2, b^3 \rangle.$$

Finally we may add the relator $(ab)^2$ as it is a consequence of the relators a^2 and $(a^{-1}b)^2$. We may then delete $(a^{-1}b)^2$ as it is a consequence of a^2 and $(ab)^2$. So we arrive at the second presentation of S_3 given in section 1.2:

$$S_3 \cong \langle a, b \mid a^2, b^3, (ab)^2 \rangle.$$

2. We now show that

$$\langle x, y \mid x^2 = y^3 \rangle \cong \langle a, b \mid aba = bab \rangle.$$

Download free eBooks at bookboon.com

Start with the second presentation and add the generators x and y and the relators $x = aba$ and $y = ab$ to obtain

$$\langle a, b, x, y \mid aba = bab, x = aba, y = ab \rangle.$$

Noting that $x^2 = y^3$ is a consequence of these relators we change the presentation to

$$\langle a, b, x, y \mid aba = bab, x = aba, y = ab, x^2 = y^3 \rangle.$$

Solving for a and b we have $a = xy^{-1}$ and $b = a^{-1}y = yx^{-1}y$. Deleting a and b and the relators we used to solve for them we have

$$\langle x, y \mid x^2 = y^3 \rangle.$$

Incidentally, by letting $y = bab^{-1}$ in the second presentation we can also show that this group is isomorphic to

$$\langle a, b, y \mid y = bab^{-1}, aya^{-1} = b \rangle$$

which is the presentation of the trefoil knot group from chapter 12.

The *Tietze transformations* of a finite presentation are as follows.

1. If w is a word in X such that $w \sim \varepsilon$ in $\langle X \mid R \rangle$ then change

$$\langle X \mid R \rangle \ \to \langle X \mid R \cup \{w\} \rangle.$$

2. If w is a word in X such that $w \sim \varepsilon$ in $\langle X \mid R \rangle$ then change

$$\langle X \mid R \cup \{w\} \rangle \ \to \langle X \mid R \rangle.$$

3. If w is a word in X and $y \notin X$ then change

$$\langle X \mid R \rangle \ \to \langle X \cup \{y\} \mid R \cup \{y = w\} \rangle.$$

4. If $y \notin X$ and $y = w$ is a relator, where w is a word in X, then change

$$\langle X \cup \{y\} \mid R \cup \{y = w\} \rangle \ \to \langle X \mid R' \rangle$$

where R' is the set of relators R with every occurrence of y replaced by w.

Download free eBooks at bookboon.com

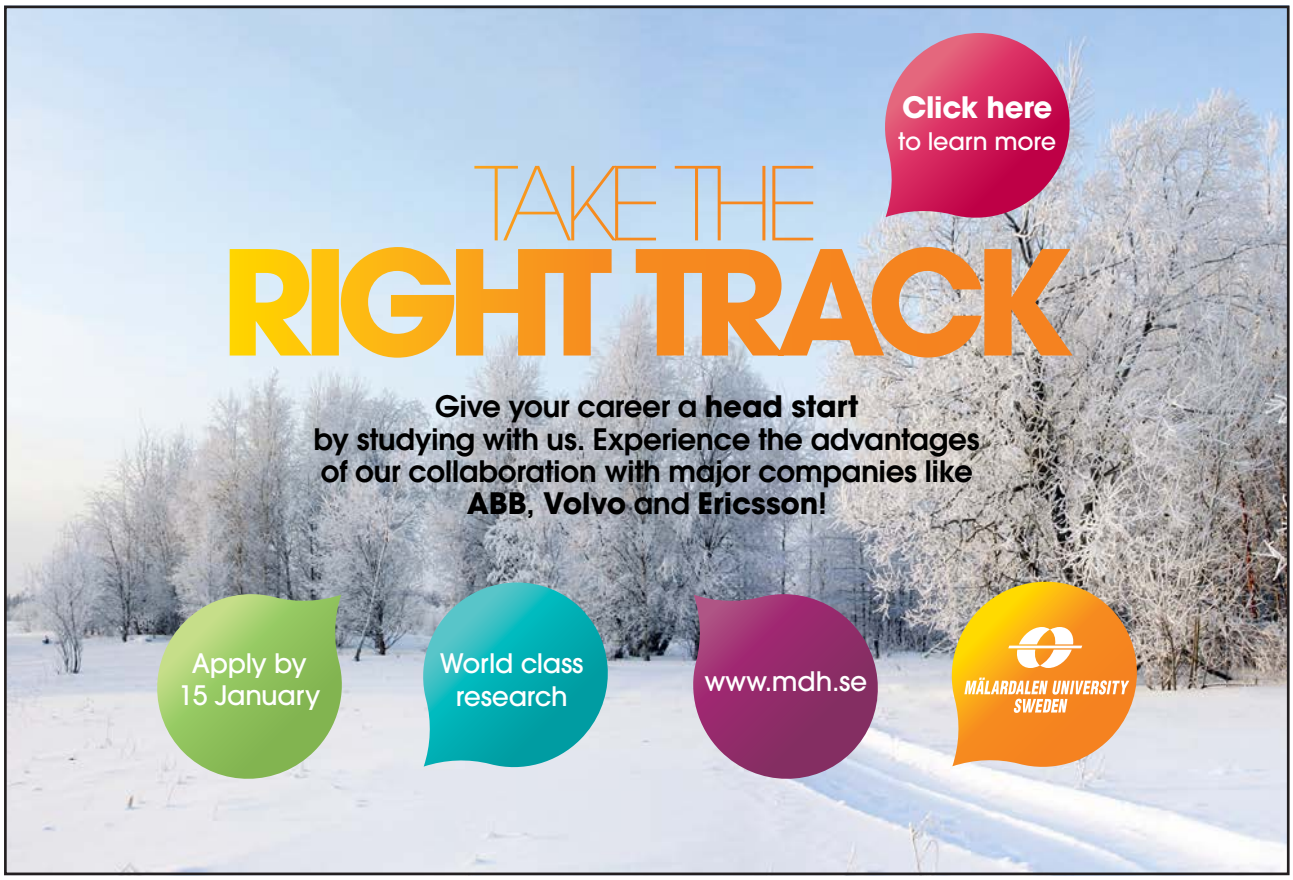
Note that the opposite of a transformation of type 2 is one of type 1 and the opposite of a transformation of type 4 is one of type 3 followed by finitely many of type 1 and finitely many of type 2.

We now analyse the Tietze transformations in the examples above. In the first example we performed two type 3 transformations, a type 4, another type 4, a type 1 then a type 2. In the second we performed two of type 3 followed by a type 1, a type 2 then two of type 4.

15.2 Properties of Tietze Transformations

Theorem 15.2 *The Tietze transformations do not affect the isomorphism type of the group presented.*

Proof. Let $G = \langle X \mid R \rangle$ and $H = \langle X \mid R \cup \{w\} \rangle$. By von Dyck's theorem we may construct a homomorphism $p' : H \to G$ extending the map $p : X \to X$ defined by $p(x) = x$ for all $x \in X$. It is surjective as X generates G and its kernel is $\{1_H\}$ because if $p^*(v) = v \sim \varepsilon$ in G then we can reduce v in H to ε by inserting or deleting a word in R or one of the form xx^{-1}, $x^{-1}x$. Adding another relator doesn't affect this so $v \sim \varepsilon$ in H. Since $\ker(p') = \{1_H\}$, p' is injective and hence an isomorphism. This shows invariance under transformations of types 1 and 2 of the isomorphism type of the group presented.



Click on the ad to read more

Download free eBooks at bookboon.com

It remains to show invariance under type 3 and invariance under type 4 will then follow because of the nature of its opposite transformation. Let $G = \langle X \mid R \rangle$ and $H = \langle X \cup \{y\} \mid R \cup \{y = w\} \rangle$ where $y \notin X$. Again there is a homomorphism $p' : G \to H$ induced by mapping $p(x)$ to x for all $x \in X$. It is surjective because $(X \cup \{y\})^* = (X \cup \{w\})^* = X^*$ so X generates H. It is also injective since if $p^*(x) \sim \varepsilon$ in H we can also reduce x to ε in G since y is equal to a word in X. Hence it is bijective and an isomorphism. □

Theorem 15.3 *Given two finite presentations of a group G there exists a finite sequence of Tietze transformations which changes one presentation into the other.*

Proof. Suppose that

$$\begin{aligned} G &\cong \langle x_1, \ldots, x_n \mid r_1, \ldots, r_p \rangle \\ &\cong \langle y_1, \ldots, y_m \mid s_1, \ldots, s_q \rangle \end{aligned}$$

Let $X = \{x_1, \ldots, x_n\}$ and $y = \{y_1, \ldots, y_m\}$. Since X generates G we may write

$$y_1 = w_1(x_1, \ldots, x_n), \ldots, y_m = w_m(x_1, \ldots, x_n)$$

where $w_i(x_1, \ldots, x_n)$ are all words in X. By m moves of type 3 we can change to the following presentation.

$$\langle x_1, \ldots, x_n, y_1, \ldots, y_m \mid r_1, \ldots, r_p, y_1 = w_1, \ldots, y_m = w_m \rangle.$$

We can now use q moves of type 1 to add $s_1, \ldots, s_q$ to the list of relators, since each of these is equivalent to ε in G. This results in

$$\langle x_1, \ldots, x_n, y_1, \ldots, y_m \mid r_1, \ldots, r_p, s_1, \ldots, s_q, y_1 = w_1, \ldots, y_m = w_m \rangle.$$

Now since Y generates G we can write

$$x_1 = v_1(y_1, \ldots, y_m), \ldots, x_n = v_n(y_1, \ldots, y_m)$$

where $v_i(y_1, \ldots, y_m)$ are words in Y. Using moves of type 1 we can add these to the presentation to obtain

$$\begin{aligned} \langle x_1, \ldots, x_n, y_1, \ldots, y_m \mid r_1, \ldots, \quad r_p \quad &, s_1, \ldots, s_q, x_1 = v_1, \ldots, \\ x_n \quad &= v_n, y_1 = w_1, \ldots, y_m = w_m \rangle. \end{aligned}$$

Download free eBooks at bookboon.com

Now we could equally have obtained this presentation from the second of the initial presentations. Thus the inverse of the moves we would have done in order to make this transformation will now complete the transformation of the first presentation to the second. (If these are written out explicitly it is seen that moves of type 2 and 4 are also used.) □

It can be shown that the solvability of the word problem is not affected by Tietze transformations. Thus a corollary of the previous theorem is that the solvability of the word problem only depends on a group G and not a particular finite presentation of G.

Click on the ad to read more

Download free eBooks at bookboon.com

16 Free Products

Free products are a generalisation of free groups and a very important construction in group theory. A free group of rank 2 is a free product of two infinite cyclic groups. We define free products of arbitrary groups and discuss some of their properties.

16.1 Free Products

Recall that the direct product $G = H \times K$ of two groups H and K satisfies the following (really we mean $H \times \{1_K\}$ when we write H and we mean $\{1_H\} \times K$ when we write K).

1. $G = \langle H, K \rangle$
2. $H \cap K = \{1_G\}$.
3. For all $h \in H$ and for all $k \in K$ we have $hk = kh$.

There are many other notions of "product" in group theory. Usually the third condition is weakened. The first type of product we study, the *free product*, satisfies the first two conditions but not the third. Later we shall study another type of product in which the second condition is usually also weakened.

Definition 16.1 *Let $A = \langle X_A \mid R_A \rangle$ and $B = \langle X_B \mid R_B \rangle$ be groups. Then the* free product *of A and B , written $A * B$, is the group with presentation*

$$\langle X_A \cup X_B \mid R_A \cup R_B \rangle$$

Note that we are assuming that X_A and X_B are disjoint sets, and the same for R_A and R_B.

Example 16.2

1. Let $A = \langle a \mid \rangle$ and $B = \langle b \mid \rangle$. Then $A \cong \mathbb{Z}$, $B \cong \mathbb{Z}$ and $A * B \cong F_2$. More generally, $F_{n-1} * \mathbb{Z} \cong F_n$ for all n.
2. Let $A = \mathbb{Z}_2 = \langle a \mid a^2 \rangle$ and let $B = \mathbb{Z}_2 = \langle b \mid b^2 \rangle$. Suppose that $G = A * B$, i.e G is the group with presentation

   $$\langle a, b \mid a^2, b^2 \rangle.$$

   A general element of G is of the form

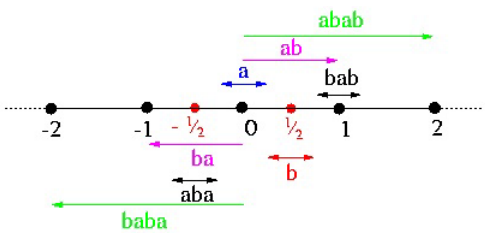
   $$a^{n_1} b^{n_2} \cdots a^{n_r} b^{m_r}$$

Download free eBooks at bookboon.com

but since $a^2 = b^2 = 1$ we can write it as

$$(a)baba \cdots aba(b)$$

and this is a normal form for G. G arises as a group of isometries of the real line $\mathbb{R}$. (Recall that an *isometry* $f : \mathbb{R} \to \mathbb{R}$ is a bijection from $\mathbb{R}$ to $\mathbb{R}$ such that distances between points are preserved, i.e. for all x and y in $\mathbb{R}$ we have $|f(x) - f(y)| = |x - y|$. It is easy to see that such a map is determined by the images of 2 points.) In fact G is the group of isometries of $\mathbb{R}$ which fix $\mathbb{Z}$. Let a be reflection of $\mathbb{R}$ in the point 0 and let b be reflection of $\mathbb{R}$ in the point $\frac{1}{2}$. Then $a^2 = b^2 = 1$. We can use von Dyck's theorem to set up an isomorphism between G and the group of isometries of $\mathbb{R}$ generated by a and b. This is a good exercise, but in this example we will only describe some of the products of a and b.



We have

$$ab(0) = b(a(0)) = b(0) = 1$$

and

$$ab(1) = b(a(1)) = b(-1) = 2$$

Hence ab is the (infinite order) translation of $\mathbb{R}$ one unit to the right. $ba = (ab)^{-1}$ since a and b both have order 2. So ba is the translation of $\mathbb{R}$ one unit to the left.

$$aba(0) = a(ab(0)) = a(1) = -1$$

and

$$aba(1) = a(ab(1)) = a(2) = -2$$

Thus aba is reflection in the point $-\frac{1}{2}$. Similarly,

$$bab(0) = b(ba(0)) = b(-1) = 2$$

and

$$bab(1) = b(ba(1)) = b(0) = 1$$

Download free eBooks at bookboon.com

So bab is reflection in the point 1. We can continue to obtain all isometries of $\mathbb{R}$ which fix $\mathbb{Z}$. Words of even length correspond to translations and words of odd length correspond to reflections.

This group can be considered as the symmetry group of an infinitely many sided polygon. For this reason it is known as the *infinite dihedral group* and is denoted D_∞.

Exercise 16.3 Show that $D_\infty \cong \langle s, t \mid tst^{-1} = s^{-1} \rangle$.

Note that we need to show that the definition of the direct product does not depend on the chosen presentations of A and B. This will be proven later.

16.2 A Normal Form for Free Products

Theorem 16.4 *Let $G = A * B$. Then for all $g \in G$, g can be written uniquely as a product $a_1 b_1 \cdots a_n b_n$ where $a_i \in A$ for all i, $b_i \in B$ for all i, $a_i \neq 1_G$ for all $i \neq 1$ and $b_n \neq 1_G$ for all $i \neq n$.*

Note that we can clearly write every element of G as above. The point is that the expression is unique.

Click on the ad to read more

Download free eBooks at bookboon.com

Proof. This is analogous to the case for free groups, where we used the van der Waerden trick. Let $G = A * B$ where $A = \langle X_A \mid R_B \rangle$ and $B = \langle X_B \mid R_B \rangle$. Assume that R_A contains all words of the form xx^{-1} and $x^{-1}x$ where $x \in X_A$, and that R_B is also defined to include such words. Let $R = R_A \cup R_B$ and $X = X_A \cup X_B$. Let W_G denote the set of all words of the form $a_1 b_1 \cdots a_n b_n$ where $a_i \in A$ and $b_i \in B$ for all i and a_1 and b_r are the only letters which may take the value 1_G. For all $x \in X^{\pm}$ we construct a bijection $f_x : W_G \to W_G$ as follows. f_x is rather complicated to write down. If $b_n = 1$ then f_x is defined analogously. By composition we extend f to a map from X^* to W_G via the following rule, where $w = x_1^{n_1} \cdots x_r^{n_r}$ is a word in $(X_A \cup X_B)^*$.

$$f_w(v) = (f_{x_r})^{n_r}(v) \circ \cdots \circ (f_{x_1})^{n_1}(v)$$

It is easily checked that f_r is the identity for all $r \in R$ and hence by von Dyck's theorem there is a homomorphism induced. Now suppose that

$$g = a_1 b_1 \cdots a_n b_n = a_1' b_1' \cdots a_m' b_m'$$

Then by construction,

$$f_g(1) = a_1 b_1 \cdots a_n b_n = a_1' b_1' \cdots a_m' b_m'$$

and both words must be equal since f_g is well defined. □

Exercise 16.5 Show that if the word problem is solvable in groups A and B then it is solvable in $A * B$.

16.3 The Universal Property of Free Products

The following theorem is called a "universal property". The terminology comes from a branch of mathematics called category theory, in which properties involving commutative diagrams are one of the fundamental objects of study.

Proposition 16.6 *Let H be any group, let $G = A * B$ and let $f : A \to H$ and $g : B \to H$ be homomorphisms. Then there is a unique homomorphism $\phi : G \to H$ such that for all $a \in A$, $\phi(a) = f(a)$ and for all $b \in B$, $\phi(b) = g(b)$.*

Note that technically we mean that ϕ satisfies $\phi \circ i_A = f$ and $\phi \circ i_B = g$, where $i_A : A \to G$ and $i_B : B \to G$ are the inclusion maps.

$$\begin{tikzcd}
A \arrow[r, "i_A"] \arrow[dr, "f"'] & G = A * B \arrow[d, "\phi"] & B \arrow[l, "i_B"'] \arrow[dl, "g"] \\
& H &
\end{tikzcd}$$

Download free eBooks at bookboon.com

Proof. Let $g \in G$, where $g = a_1 b_1 \cdots a_n b_n$. Define

$$\phi(g) = f(a_1)g(b_1) \cdots f(a_n)g(b_n).$$

Clearly, $\phi(a) = f(a)$ for all $a \in A$ and $\phi(b) = g(b)$. The map ϕ is well defined by uniqueness of the normal form. Suppose that $g = a_1 b_1 \cdots a_n b_n$, where $a_i \in A$ and $b_i \in B$ for each i and $g' = a'_1 b'_1 \cdots a'_m b'_m$, where $a'_i \in A$ and $b'_i \in B$ for each i.

Then

$$\begin{aligned}
\phi(gg') &= \phi((a_1 b_1 \cdots a_n b_n)(a'_1 b'_1 \cdots a'_m b'_m)) \\
&= \phi(a_1 b_1 \cdots a_n b_n a'_1 b'_1 \cdots a'_m b'_m) \\
&= f(a_1)g(b_1) \cdots f(a_n)g(b_n) f(a'_1)g(b'_1) \cdots f(a'_m)g(b'_m) \\
&= \phi(g)\phi(g')
\end{aligned}$$

(Note that above we allow $a_1 = 1_G$, $b_n = 1_G$, $a'_1 = 1_G$ and $b'_m = 1_G$). Thus ϕ is a homomorphism.

Uniqueness of ϕ follows because since A and B generate G, ϕ is determined by $\phi(A)$ and $\phi(B)$. □

16.4 Independence of Presentation

We now show that, up to isomorphism, $A * B$ does not depend on the presentations of A and B. Let $A \cong \langle X_A \mid R_A \rangle \cong \langle X'_A \mid R'_A \rangle$ and $B \cong \langle X_B \mid R_B \rangle \cong \langle X'_B \mid R'_B \rangle$. Also, let $G \cong \langle X_A \cup X_B \mid R_A \cup R_B \rangle$ and $G' \cong \langle X'_A \cup X'_B \mid R'_A \cup R'_B \rangle$. If $f'_A : A \to G'$ is given by $f'_A(a) = a$ for all $a \in A$ and $f'_B : B \to G'$ is given by $f'_B(b) = b$ for all $b \in B$ then let $\phi : G \to G'$ be the unique homomorphism such that for all $a \in A$, $\phi(a) = f'_A(a)$ and for all $b \in B$, $\phi(b) = f'_B(b)$. Similarly, if f_A and f_B are the analogous homomorphisms from A and B to G and $\psi : G \to G'$ is the analogous unique homomorphism, then $\psi \circ \phi : G \to G$ and $\mathrm{id} : G \to G$ are both homomorphisms $\chi : G \to G$ such that for all $a \in A$, $f_A(a) = \chi(a)$ and for all $b \in B$, $f_B(b) = \chi(b)$. By uniqueness of this homomorphism, $\psi \circ \phi = \mathrm{id} : G \to G$. Similarly, $\phi \circ \psi$ is the identity map. Thus ϕ is an isomorphism with inverse ψ.

Exercise 16.7 Let A and B be groups with $1_A \neq a \in A$ and $1_B \neq b \in B$. Let $G = A * B$. Show that G is infinite by showing that $aba^{-1}b^{-1}$ has infinite order in $A * B$. Use this fact to show also that the centre $Z(G)$ is trivial.

16.5 Decomposability

Exercise 16.8 Show that if A and B are both nontrivial groups and $G \cong A * B$ then there are no nontrivial groups H and K with $G \cong H \times K$. (Hint: Choose nontrivial elements $a \in A$ and $b \in B$ and consider the centraliser $C_G(ab)$).

Download free eBooks at bookboon.com

We say that a group G is *freely decomposable* if it can be written as a free product of nontrivial groups. Otherwise it is said to be *freely indecomposable*. We have similar notions of a *directly decomposable* and a *directly indecomposable* group. The above exercise shows that a freely decomposable group is directly indecomposable and that a directly decomposable group is freely indecomposable. Thus, for example, $\mathbb{Z} \oplus \mathbb{Z}$ is freely indecomposable and F_2 is directly indecomposable.

Click on the ad to read more

Download free eBooks at bookboon.com

17 Free Products With Amalgamation

Free products with amalgamation generalise free products. In a free product with amalgamation we have two groups A and B with an isomorphic copy of the same subgroup C and we form a group in which the two groups appear as subgroups such that the two copies of C are joined together. In the case of a free product the subgroup C is the identity subgroup of both A and B.

17.1 Free Products with Amalgamation

Recall that the free product $G = A * B$ of two groups A and B satisfied $G = \langle A, B \rangle$ and $A \cap B = \{1_G\}$. Suppose that the group C appears as a common subgroup of the groups A and B. In this section we construct a product $A *_C B$ which satisfies $G = \langle A, B \rangle$ and $A \cap B = C$. The free product is thus a special case where C is the trivial group.

Since C may appear as a subgroup of A and B in different ways, we must formally specify injective homomorphisms $f : C \to A$ and $g : C \to B$. This should really appear in the notation as $A *_C^{f,g} B$ but the maps are often omitted from the notation when they are clear from the context.

Definition 17.1 *Let $A = \langle X_A \mid R_A \rangle$ and $B = \langle X_B \mid R_B \rangle$ be groups. Suppose that X_C is a generating set of C and we are given injective homomorphisms $f : C \to A$ and $g : C \to B$. Then the* free product with amalgamation

$$A *_C^{f,g} B$$

is the group presented by

$$\langle X_A \cup X_B \mid R_A \cup R_B \cup \{f(x) = g(x) \mid x \in X_C\} \rangle$$

As in the definition of a free product, we understand that X_A and X_B are disjoint.

Example 17.2

1. $A * B = A *_{\{1\}} B$
2. Let $A = \langle a \rangle$, $B = \langle b \rangle$ and $C = \langle c \rangle$ be infinite cyclic groups. Take the homomorphisms $f : C \to A$ given by $f(c) = a^2$ and $g : C \to B$ given by $g(c) = b^3$. Then $A *_C^{f,g} B = \langle a, b \mid a^2 = b^3 \rangle$. This is an interesting infinite group. In the subject of knot theory, every knot has a group associated with it. This one is associated with a trefoil knot.

Download free eBooks at bookboon.com

3. Let $A = F(x, y)$ and let $B = \langle b \rangle$ and $C = \langle c \rangle$ be infinite cyclic groups. If $f : C \to A$ is given by $f(c) = x$ and $g : C \to B$ is given by $g(c) = b$ then

$$A *_C^{f,g} B = \langle x, y, b \mid x = b \rangle \cong \langle x, y \mid \rangle \cong F_2$$

This is a *trivial* free product with amalgamation.

4. Let $A = \langle a \mid a^6 \rangle \cong \mathbb{Z}_6$, $B = \langle b \mid b^6 \rangle \cong \mathbb{Z}_6$ and $C = \langle c \mid c^3 \rangle \cong \mathbb{Z}_3$. If $f : C \to A$ is given by $f(c) = a^2$ and $g : C \to B$ is given by $g(c) = b^2$ then

$$A *_C^{f,g} B = \langle a, b \mid a^6, b^6, a^2 = b^2 \rangle$$

17.2 Pushouts

Warning: what follows is a very long definition! Let $a, b, c, \ldots$ be groups and let $\alpha, \beta, \gamma, \ldots$ be homomorphisms. We say that the data

$$\begin{tikzcd} a \arrow[dr, "\gamma"'] & & b \arrow[dl, "\delta"] \\ & d & \end{tikzcd}$$

is a *pushout* of the data

$$\begin{tikzcd} & c \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & \\ a & & b \end{tikzcd}$$

if the diagram

$$\begin{tikzcd} & c \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & \\ a \arrow[dr, "\gamma"'] & & b \arrow[dl, "\delta"] \\ & d & \end{tikzcd}$$

commutes, and for all diagrams

$$\begin{tikzcd} a \arrow[dr, "\phi"'] & & b \arrow[dl, "\psi"] \\ & e & \end{tikzcd}$$

such that the diagram

$$\begin{tikzcd} & c \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & \\ a \arrow[dr, "\phi"'] & & b \arrow[dl, "\psi"] \\ & e & \end{tikzcd}$$

Download free eBooks at bookboon.com

commutes, there exists a *unique* map $\theta : d \to e$ such that the following diagram commutes.

$$\begin{tikzcd}
 & c \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & \\
a \arrow[r, "\gamma"] \arrow[dr, "\phi"'] & d \arrow[d, "\theta"] & b \arrow[l, "\delta"'] \arrow[dl, "\psi"] \\
 & e &
\end{tikzcd}$$

Proposition 17.3 *If pushouts exist then they are unique up to isomorphism.*

Proof. Suppose that we have two pushouts

$$\begin{tikzcd}
a \arrow[dr, "\gamma"'] & & b \arrow[dl, "\delta"] \\
 & d &
\end{tikzcd}$$

and

$$\begin{tikzcd}
a \arrow[dr, "\mu"'] & & b \arrow[dl, "\nu"] \\
 & r &
\end{tikzcd}$$

Click on the ad to read more

Download free eBooks at bookboon.com

of the data

$$\begin{tikzcd} & c \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & \\ a & & b \end{tikzcd}$$

Then there exist unique maps $\theta : d \to r$ and $\chi : r \to d$ such that the diagrams

$$\begin{tikzcd} & c \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & & \\ a \arrow[r, "\gamma"] \arrow[dr, "\mu"'] & d \arrow[d, "\theta"] & b \arrow[l, "\delta"'] \arrow[dl, "\nu"] \\ & r & \end{tikzcd}$$

and

$$\begin{tikzcd} & c \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & & \\ a \arrow[r, "\gamma"] \arrow[dr, "\mu"'] & d & b \arrow[l, "\delta"'] \arrow[dl, "\nu"] \\ & r \arrow[u, "\chi"'] & \end{tikzcd}$$

commute. We may then form the commutative diagrams

$$\begin{tikzcd} & c \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & & \\ a \arrow[r, "\gamma"] \arrow[dr, "\gamma"'] & d \arrow[d, "\chi\circ\theta"'] & b \arrow[l, "\delta"'] \arrow[dl, "\delta"] \\ & d & \end{tikzcd}$$

and

$$\begin{tikzcd} & c \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & & \\ a \arrow[r, "\gamma"] \arrow[dr, "\gamma"'] & d \arrow[d, "\mathrm{id}"'] & b \arrow[l, "\delta"'] \arrow[dl, "\delta"] \\ & d & \end{tikzcd}$$

By uniqueness, $\chi \circ \theta = id : d \to d$. Similarly, $\theta \circ \phi = id : e \to e$. Hence θ and χ are mutually inverse isomorphisms. $\square$

Download free eBooks at bookboon.com

Lemma 17.4 *If $\psi : K \to H$ is a homomorphism of groups and N is a normal subgroup of K with $N \leqslant \ker\ \psi$ then there is a homomorphism $\phi : K/N \to H$ defined by $\phi(kN) = \psi(k)$.*

Proof. We clearly have

$$\begin{aligned}\phi((k_1N)(k_2N)) &= \phi(k_1k_2N)\\ &= \psi(k_1k_2)\\ &= \psi(k_1)\psi(k_2)\\ &= \phi(k_1N)\phi(k_2N)\end{aligned}$$

but the point is that ϕ is well defined. If $k_1N = k_2N$ then $k_1k_2^{-1} \in N$ which means that $k_1k_2^{-1} \in \ker\ \psi$. Thus $\psi(k_1k_2^{-1}) = 1$, i.e. $\psi(k_1)\psi(k_2)^{-1} = 1$ which means that $\psi(k_1) = \psi(k_2)$. □

Proposition 17.5 *Let A, B and C be groups and let $f : C \to A$ and $g : C \to B$ be homomorphisms. Suppose that X_C is a generating set for C. If*

$$\begin{tikzcd} A \arrow[dr, "h"'] & & B \arrow[dl, "k"] \\ & D & \end{tikzcd}$$

is a pushout of this data then

$$D \cong \frac{A * B}{N}$$

where

$$N = \langle\langle\{f(c)g(c)^{-1} \mid x \in X_C\}\rangle\rangle_{A*B}$$

Proof. Let D be as in the statement of the theorem. Define the maps $h : A \to D$ by $h(a) = aN$ and $k : B \to D$ by $k(b) = bN$. (Technically, if we let i_A be the inclusion map of A in $A * B$ and let i_B be the inclusion map of B in $A * B$ then we mean $h(a) = i_A(a)N$ and $k(b) = i_B(b)N$.) Let H be an arbitrary group, and let $p : A \to H$ and $q : B \to H$ be arbitrary homomorphisms. Take $\psi : A * B \to H$ to be the homomorphism with $\psi|_A = p$ and $\psi|_B = q$. N is contained in $\ker\ \psi$ since if $c \in X_C$ then $\psi(f(c)g(c)^{-1}) = p(f(c))q(g(c))^{-1} = 1$ since $p(f(c)) = q(g(c))$. By the previous lemma, there is a homomorphism induced from D to N by $\phi(aN) = \psi(a)$ and $\phi(bN) = \psi(b)$. The homomorphism ψ is unique since D is generated by $\{aN \mid a \in A\}$ and $\{bN \mid b \in B\}$, and since C is generated by X_C. □

Download free eBooks at bookboon.com

17.3 Independence of Presentation

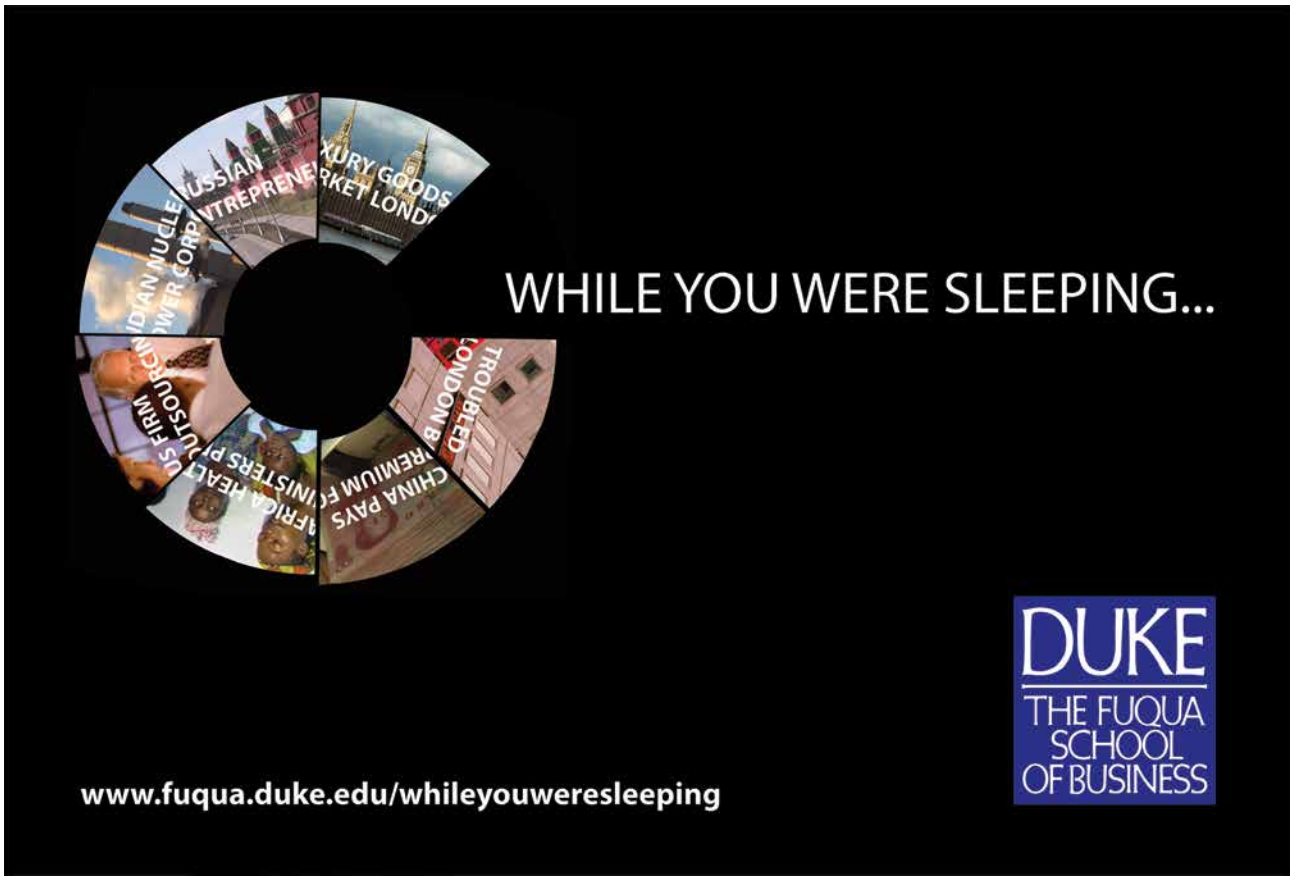
Let $A = \langle X_A \mid R_A \rangle$ and $B = \langle X_B \mid R_B \rangle$. Then from chapter 12 we see that a presentation of the pushout is

$$\langle X_A \cup X_B \mid R_A \cup R_B \cup \{f(c)g(c)^{-1} \mid c \in X_C\} \rangle$$

In particular, when f and g are injective, the pushout is a free product with amalgamation.

Corollary 17.6 *Free products with amalgamation are independent of presentations*

Free products with amalgamation have an important application in topology. In topology, a group can be associated with a topological space X satisfying a certain condition called path-connectedness. This is called the *fundamental group* of X. If X can be written as $A \cup B$ where $A \cap B = C$ and these pieces are path connected and their fundamental groups inject into that of X then the fundamental group is the free product of that of A and B, amalgamated on the subgroup C. This is called *van Kampen's Theorem*. It basically says that pushouts in topology are mapped to pushouts in group theory by the fundamental group. A good reference for this material is [9].



Click on the ad to read more

Download free eBooks at bookboon.com

18 HNN Extensions

In the final section of this book we look at a construction which is closely related to free products with amalgamation, but where a subgroup appears twice as different isomorphic copies of the same group, and we form a new group in which these copies become nontrivially conjugate.

18.1 HNN Extensions

Definition 181 *Let $A = \langle X_A \mid R_A \rangle$ be a group and let B and C be subgroups of A which are isomorphic via an isomorphism $\theta : B \to C$. Let X_B be a generating set of B and let t be a letter which is not in X_A. Then the* HNN Extension *of A along B and C with respect to θ is the group*

$$A*^{\theta}_{B,C} = \langle X_A \cup \{t\} \mid R_A \cup \{t^{-1}bt = \theta(b) \mid b \in X_B\} \rangle$$

A is called the base *of the HNN extension, t is its* stable letter of an HNN Extension *and B and C are the* associated subgroups.

The name stands for Higman-Neumann-Neumann Extension, after Graham Higman, Bernard H. Neumann and Hanna Neumann. It also has a topological interpretation – it is the fundamental group of a space with a *handle* added. Such constructions are useful in studying surfaces and three-manifolds.

Example 18.2

1. Let $A = \mathbb{Z}$, generated by a and take the subgroups $B = \langle a^p \rangle$ and $C = \langle a^q \rangle$, where p and q are integers. Let $\theta : B \to C$ be the isomorphism specified by $\theta(a^p) = a^q$. Then

$$A*^{\theta}_{B,C} = \langle a, t \mid t^{-1}a^p t = a^q \rangle$$

   This is called the *Baumslag-Solitar group* $B_{p,q}$. These provide interesting examples of groups. For example, it can be shown that $G = B_{2,3}$ has a proper quotient which is also isomorphic to G. If this property holds, G is called a *non-hopfian group*. Examples of non-hopfian finitely presented groups are rare.

2. Let $A = B = C = 1$, the trivial group. Then θ is also trivial and

$$1*^{\theta}_{1,1} = \langle t \mid \rangle \cong \mathbb{Z}$$

   Thus, unlike free products with amalgamation, the HNN extension of the trivial group is nontrivial.

Download free eBooks at bookboon.com

3. In general there is more than one extra relation introduced in an HNN extension. For example, suppose that $A = F_2 = \langle a, b \mid \rangle$. Let B be the subgroup of A generated by a^2 and b^3 and let C be the subgroup of A generated by a^5 and b^7. Both B and C are isomorphic to A. Let θ the obvious isomorphism from B to C specified by $\theta(a^2) = a^5$ and $\theta(b^3 = b^7)$. Then

$$A*^{\theta}_{B,C} = \langle a, b, t \mid t^{-1}a^2t = a^5, t^{-1}b^3t = b^7 \rangle$$

18.2 Relation to Free Products with Amalgamation

We now interpret HNN extensions as subgroups of free products with amalgamation.

Lemma 18.3 *Let A, B, G and H be groups. If $\theta : A \to G$ and $\phi : B \to H$ are homomorphisms (isomorphisms) then there exists a unique homomorphism (isomorphism) $\psi : A * B \to G * H$ such that $\psi|_A = \theta$ and $\psi|_B = \phi$.*

Proof. Let i_G and i_H be the inclusion maps of G and H in $G * H$. Define i_A and i_B similarly. Since $A * B$ is a free product then there exists, by Proposition 16.6, a unique map ψ making the following diagram commute.

$$\begin{tikzcd}
A \arrow[r, "i_A"] \arrow[dr, "i_G \circ \theta"'] & A * B \arrow[d, "\psi"] & B \arrow[l, "i_B"'] \arrow[dl, "i_H \circ \phi"] \\
& G * H &
\end{tikzcd}$$

Suppose further that θ and ϕ are isomorphisms. Then there exists a unique homomorphism $\chi : G * H \to A * B$ such that $\chi|_G = \theta^{-1}$ and $\chi|_H = \phi^{-1}$. Thus $(\chi \circ \phi)|_A = \mathrm{id} : A \to A$ and $(\chi \circ \phi)|_B = \mathrm{id} : B \to B$. Thus by uniqueness, $\chi \circ \psi = \mathrm{id} : A * B \to A * B$ and, similarly, $\psi \circ \chi = \mathrm{id} : G * H \to G * H$. Therefore ψ is an isomorphism with inverse χ. $\square$

Now suppose that $A \cong B$ via an isomorphism f, and A and B are subgroups of G. Let U be the free product $G * \langle u \rangle$ and let V be the free product $G * \langle v \rangle$. Consider the subgroups $J = \langle G, u^{-1}Au \rangle$ of U and $K = \langle G, v^{-1}Bv \rangle$ of V. Suppose also that

$$g_1(u^{-1}a_1u)g_2(u^{-1}a_2u) \cdots g_n(u^{-1}a_nu) = 1$$

Then since $g_1 \in G$, $u^{-1} \in \langle u \rangle$, $a_1 \in G$, $u \in \langle u \rangle$ and so on, by uniqueness of the normal form for free products, $g_1 = g_2 = \cdots = g_n = 1$ and $a_1 = a_2 = \cdots = a_n = 1$. There can therefore be no relators involving both elements of G and elements of $u^{-1}Au$ in a presentation of J. Thus $J \cong G * u^{-1}Au$ and similarly $K \cong G * v^{-1}Bv$. Let $\theta : G \to G$ be the identity map and let $\phi : u^{-1}Au \to v^{-1}Bv$ be defined by $\phi(u^{-1}au) = v^{-1}f(a)v$. Then both θ and ϕ are isomorphisms and by the lemma above there is an isomorphism $\psi : J \to K$. such that $\psi|_G = id$ and $\psi|_u^{-1}Au = \phi$. Let

Download free eBooks at bookboon.com

$$H = U *^{\chi}_{J \cong K} V$$

which we define to be the free product of amalgamation given by the pushout of

$$\begin{tikzcd} & J \arrow[dl, "i_U"'] \arrow[dr, "i_V \circ \chi"] & \\ U & & V \end{tikzcd}$$

where i_U is the inclusion $J \to U$ and i_V is the inclusion $J \to V$. For all $a \in A$ we have $u^{-1}au = v^{-1}f(a)v$, i.e. $vu^{-1}auv^{-1} = f(a)$. If we let $t = uv^{-1}$ then $t^{-1}at = f(a)$ and the subgroup of H generated by G and t is isomorphic to $G*^{f}_{A \cong B}$.

We now want to show that free products with amalgamation $A *_C B$ contain isomorphic copies of A and B (this is false for pushouts in general) and it will follow that HNN extensions $A*_C$ contains an isomorphic copy of A.

Lemma 18.4 *Let G be a group. If A is a subgroup of G and N is a normal subgroup of G. If $A \cap N = \{1_G\}$ then the map $p : A \to G/N$ given by $p(a) = aN$ is injective.*

Proof. Suppose that for a_1 and a_2 in A we have $p(a_1) = p(a_2)$. Then $a_1N = a_2N$ which means that $a_1a_2^{-1} \in N$. Since $a_1a_2^{-1} \in A$ also we have $a_1a_2^{-1} \in A \cap N$. Thus $a_1a_2^{-1} = 1_G$ and $a_1 = a_2$. $\square$

Consider the pushout

$$\begin{tikzcd} & C \arrow[dl, "f"'] \arrow[dr, "g"] & \\ A \arrow[dr, "h"'] & & B \arrow[dl, "k"] \\ & \dfrac{A * B}{N} & \end{tikzcd}$$

where

$$N = \langle\langle \{ f(c)g(c)^{-1} \mid c \in C \} \rangle\rangle_{A*B}$$

and the maps $h : A \to (A * B)/N$ and $k : B \to (A * B)/N$ are given by $h(a) = aN$ and $k(b) = bN$.

Proposition 18.5 *In the above situation, if f is injective then k is injective. If g is injective then h is injective.*

Download free eBooks at bookboon.com

Proof. We prove that if g is injective then so is h. The other case is identical.

Let $x \in A \cap N$. Since $x \in N$ we can write it as a product

$$x = x_1^{-1} f(c_1) g(c_1)^{-1} x_1 \cdots x_n^{-1} f(c_n) g(c_n)^{-1} x_n$$

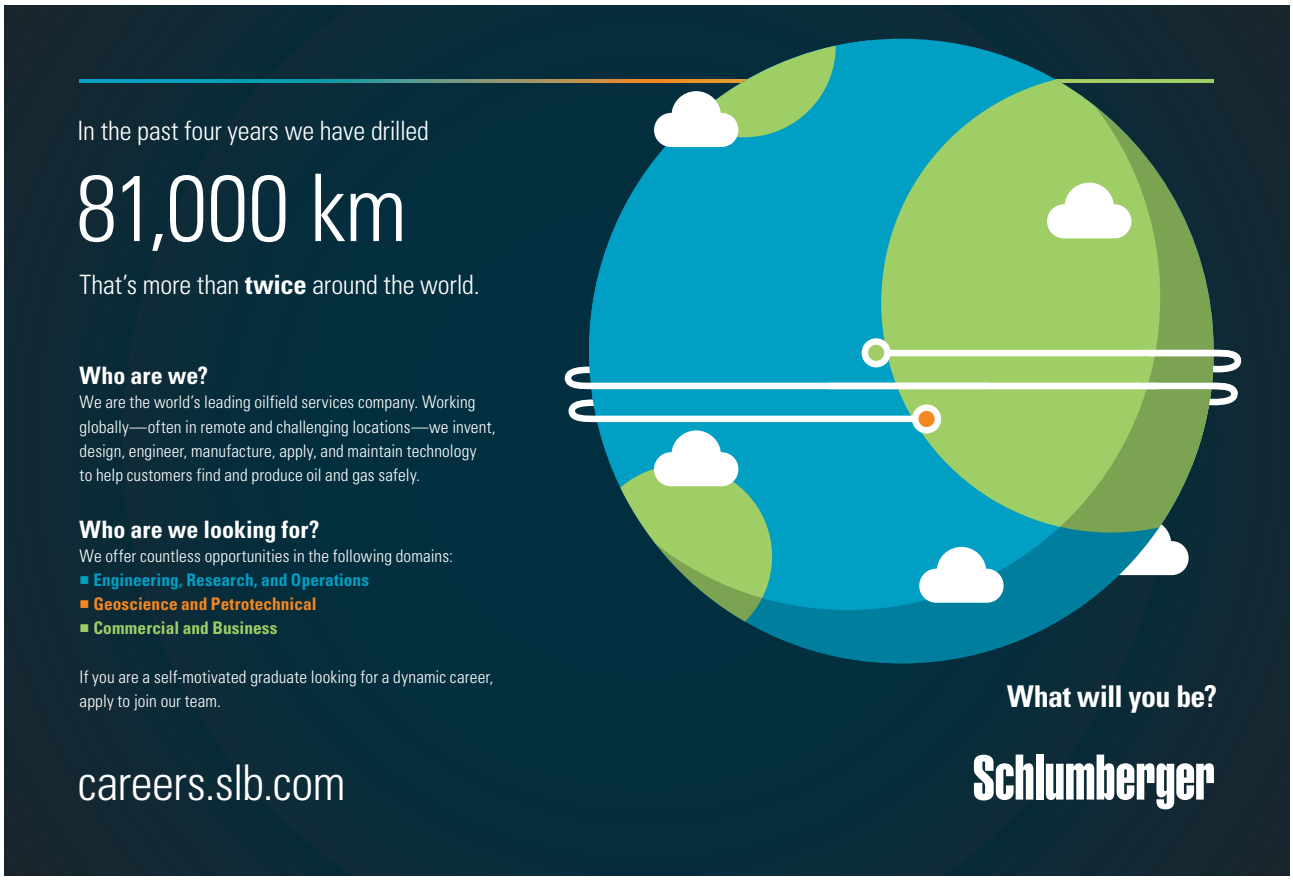
where, say

$$x_i = a_1^{(i)} b_1^{(i)} \cdots a_{m_i}^{(i)} b_{m_i}^{(i)} \in A * B$$

for each i and $c_i \in C$ for each i. Then we also have

$$\begin{aligned} x \quad = \quad & (b_{m_1}^{(1)})^{-1} (a_{m_1}^{(1)})^{-1} \cdots (b_1^{(1)})^{-1} (a_1^{(1)})^{-1} f(c_1) g(c_1)^{-1} a_1^{(1)} b_1^{(1)} \cdots \\ & \cdots a_{m_1}^{(1)} b_{m_1}^{(1)} \cdots \\ & \cdots (b_{m_n}^{(n)})^{-1} (a_{m_n}^{(n)})^{-1} \cdots (b_1^{(n)})^{-1} (a_1^{(n)})^{-1} f(c_n) g(c_n)^{-1} a_1^{(n)} b_1^{(n)} \cdots \\ & \cdots a_{m_n}^{(n)} b_{m_n}^{(n)} \end{aligned}$$

Which is in A. Then $b_i^{(j)} = 1_{A*B}$ for all i and j by the uniqueness of normal form in free products. Let $\alpha_i = \prod_j a_i^{(j)}$. Then we have



Click on the ad to read more

Download free eBooks at bookboon.com

$$x = \alpha_i^{-1} f(c_1) g(c_1)^{-1} \alpha_1 \cdots \alpha_n^{-1} f(c_n) g(c_n)^{-1} \alpha_n$$

Again, by uniqueness of the normal form, since the above is in A we have $g(c_1)^{-1} = 1_B \ldots, g(c_n)^{-1} = 1_B$ which gives $g(c_1) = 1_B \ldots, g(c_n) = 1_B$ and since g is injective we have $c_1 = 1_C, \ldots c_n = 1_C$, from which it follows that $f(c_1) = 1_A, \ldots f(c_n) = 1_A$. Thus $x = \prod_i \alpha_i^{-1} \alpha_i = 1_{A*B}$. Hence $A \cap N = 1_{A*B}$ and h is injective by the previous lemma. □

In particular, if both f and g are injective then the pushout $(A * B)/N$ is a free product with amalgamation $A *_C^{f,g} B$ and this contains $h(A)$ as an isomorphic copy of A and $k(B)$ as an isomorphic copy of B.

Thus the group $H = H = U *_{J \cong K}^{\chi} V$ constructed above contains an isomorphic copy of G and hence so does the subgroup $\langle G, t \rangle \cong G *_{A \cong B}^{f}$.

Lemma 18.6 *Let H be the subgroup of the free group $F(x, y)$ generated by*

$$y, x^{-1}yx, x^{-2}yx^2, \ldots$$

Then $H \cong F(y, x^{-1}yx, x^{-2}yx^2, \ldots)$.

Proof. Suppose that $x^{-2}yx^2 \in \langle y, x^{-1}yx \rangle$. Then for some $n_1 \ldots n_r$ and $m_1 \ldots m_r$ we have

$$x^{-2}yx^2 = y^{n_1}(x^{-1}yx)^{m_1} \cdots y^{n_r}(x^{-1}yx)^{m_r}.$$

Thus $y_{n_1} = 1$ and $n_0 = 0$. Then $x^{-2} = x^{-1}$ which gives $x = 1$, a contradiction, unless $m_1 = 0$. Similarly we see that all m_i and n_i are 0. But this tells us that $x^{-2}yx^2 = 1$ which is a contradiction. Hence

$$x^{-2}yx \notin \langle y, x^{-1}yx \rangle$$

It follows in exactly the same manner that for all n,

$$x^{-(n+1)}yx^{(n+1)} \notin \langle y, x^{-1}yx, \ldots x^{-n}yx^n \rangle$$

□

Download free eBooks at bookboon.com

18.3 The Higman-Neumann-Neumann Embedding Theorem

As a highlight we now prove the remarkable Higman-Neumann-Neumann Embedding Theorem, due to Higman, B. Neumann and H. Neumann in 1949, which states that every countable group appears as a subgroup of a two-generator group. Note that this is in stark contrast to the situation for one-generator groups (cyclic groups). Every subgroup of a cyclic group is itself cyclic. The following tells us that there is no such restriction on subgroups of two-generator groups.

Theorem 18.7 *Every countable group is isomorphic to a subgroup of some two-generator group.*

Proof. Let $g_0 = 1, g_1, g_2, \ldots$ be the elements of G. The idea is that we build a group in which these are all conjugate. We let $H = G * F(x, y)$ and form the subgroups

$$A = \langle y, x^{-1}yx, \ldots, x^{-n}yx^n, \ldots \rangle$$

and

$$B = \langle x, g_1y^{-1}xy, \ldots, g_ny^{-n}xy^n, \ldots \rangle$$

of H. Define the map $\phi : A \to B$ given by

$$\phi(x^{-n}yx^n) = g_ny^{-n}xy^n$$

Then ϕ is easily seen to be an isomorphism. Let $K = H*^{\phi}_{A\cong B}$. Then K contains an isomorphic copy of H as a subgroup, hence an isomorphic copy of G as a subgroup. For all $a \in A$ we have $t^{-1}at = \phi(t)$. Thus

$$t^{-1}x^{-n}yx^nt = \phi(x^{-n}yx^n) = g_ny^{-n}xy^n$$

which gives

$$g_n = t^{-1}x^{-n}yx^nty^{-n}x^{-1}y^n \in \langle x, y, t \rangle$$

But since $x = t^{-1}yt$, we have $\langle x, y, t \rangle = \langle y, t \rangle$ and for all $n \geqslant 0$ we have $g_n \in \langle y, t \rangle$. Thus G is a subgroup of a two-generator group. $\square$

Note that the previous theorem tells us that, since there are only countably many words on a finite alphabet, every finitely generated group is isomorphic to a subgroup of a two-generator group.

Download free eBooks at bookboon.com

19 Further Reading

Group theory is a vast subject, this is only a tiny book, and there are many further directions you could explore. Here are just a few of them. Most of this is reading aimed at final year maths students or postgraduates.

1. *Solvable and Nilpotent Groups:* These have been mentioned in chapter 14. A good concise reference is chapter 5 of [3]. For Galois theory I would recommend [11].

2. *Finite Group Theory and Simple Groups:* There are many books on finite group theory. The classification of the finite simple groups is a very difficult read (I certainly haven't read it, just flicked through books about it) and almost a mathematical subject in its own right. As a field of current research there is a strong overlap with computational group theory and algorithms in group theory.

3. *Topological groups, Lie Groups and Profinite Groups:* If you have studied topology at all you will know of the concept of a topological space. A topological group is an object which is both a group and a topological space, and its multiplication and inverse maps are continous. A Lie group is similar, but has added geometric structure and smoothness. Profinite groups are a type of topological group but are arrived at by taking limits of finite groups, and have

Click on the ad to read more

Download free eBooks at bookboon.com

4. *Group Representations:* Groups can be studied by how they act on vector spaces. By replacing a group with a group of matrices which is a homomorphic image of it, we can use all the tools of linear algebra to study groups. The resulting theory, called representation theory, is an interesting fusion of groups and matrices and there is a lot of interplay between the two. By taking the traces of the matrices obtained we obtain a notion of *characters* of groups, also very important. My favourite book on this topic, without a doubt, is [8].

5. *Bass-Serre Theory:* Bass-Serre theory is a central area of group theory. It builds well upon the topics in the later parts of this book. It is similar to representation theory in that we study groups by what they act upon, but in this case we look at how they act on graphs. In the case where the graph is a tree we can decompose the group entirely into free products with amalgamation and HNN extensions of smaller groups, given by stabilizers of vertices and edges under the action. Applications include Dunwoody's proof of Stallings' Ends Theorem. Stallings' Ends Theorem is one of the jewels in the crown of infinite group theory. It concerns when a group splits over a finite subgroup as a free product with amalgamation or HNN extension, and relates this to topological properties of the group "at infinity". I would recommend Baumslag's book [1] as a good exposition of Bass-Serre theory, and Dicks and Dunwoody's landmark book [5] for the more ambitious.

6. *Combinatorial Group Theory:* This is the study of groups given by presentations, i.e. generators and relations as in the second half of this book. Often it is easy to write down a presentation of a group in mathematics, but not so easy to deduce algebraic facts given a presentation, and a whole array of techniques have been developed to do this, both algebraic and geometric. There is no single book which covers the whole foundations of this subject but probably the most comprehensive is [12].

7. *Geometric Group Theory:* Geometric group theory is a way to understand infinite groups and provides a certain philosophy on what properties are important: "all finite groups are virtually trivial". Groups are studied up to a relation called quasi-isometry. That is, the properties of groups of interest are invariant under quasi-isometry, such as hyperbolicity of groups. Bowditch has written a nice introduction for students [4]. Hyperbolic groups were introduced by Gromov in the 1980s and form the most fundamental class of groups in geometric group theory. The techniques in geometric group theory tend to be large-scale geometric, which is actually more like analysis than algebra in flavour. Topology also plays a hugely important part, especially asymptotic topology. The subject is still very much under active research.

Download free eBooks at bookboon.com

20 Bibliography

[1] Baumslag, G. *Topics in Combinatorial Group Theory* Birkhäuser (1993).

[2] Baumslag, G. and Roseblade, *Subgroups of Direct Products of Free Groups* J. LMS (2), 30 (1984), 44–52.

[3] Blyth, T.S. and Robertson, E.F., *Groups* Essential Student Algebra series vol. 5, Chapman and Hall (1986).

[4] Bowditch, B.H., *A Course on Geometric Group Theory* MSJ Memoirs, (2006).

[5] Dicks, W. and Dunwoody, M.J., *Groups Acting on Graphs* C.U.P. (1989).

[6] Dixon, J.D., Du Sautoy, M.P.F., Mann, A. and Segal, D. *Analytic Pro-P Groups* Cambridge University Press (2003 edition).

[7] Gorenstein, D., Lyons, R. and Solomon, R., *The Classification of the Finite Simple Groups*, AMS Mathematical Surveys and Monographs (1994).

[8] James, G. and Liebeck, M. *Representations and Characters of Groups* C.U.P. 2nd Ed. (2001).

[9] Massey, W.S., *A Basic Course in Algebraic Topology*, Springer Graduate Texts in Mathematics no. 56 (1991).

[10] Mineyev, I. *Submultipicativity and the Hanna Neumann Conjecture*, Preprint (2011).

[11] Stewart, I. *Galois Theory*, 3rd Ed, Chapman and Hall (2004).

[12] Magnus, W., Karrass, A. and Solitar, D. (2004 reprint), Combinatorial Group Theory, New York: Dover Publications.

Download free eBooks at bookboon.com

21 Index

abelian group, 17
abelianisation of a group, 65
action of a group, 40
algorithm, 58
associated subgroups of an HNN Extension, 86
associative operation, 15
automorphism, 30

base group of an HNN Extension, 86
Bass-Serre theory, 93
Baumslag-Roseblade theorem, 62
Baumslag-Solitar group, 86
Bernard H. Neumann, 86
bijective map, 11
binary operation, 14

cartesian product, 11
centre of a group, 39
characteristic subgroup, 65
characters of groups, 93
classification of the finite simple groups, 36
coherent group, 62
commutator, 64
commutator subgroup, 64
composition series, 36
congruence classes, 13
congruence of integers, 13
conjugacy classes, 31
conjugacy problem, 58
conjugate of a subgroup, 31
cyclic group, 26

dihedral group, 20
directly decomposable/ indecomposable group, 79
direct product, 43
domain, 11
double coset, 36
empty word, 53
endormorphism, 65
Euler function, 27
Evariste Galois, 68

finite group, 17
finitely generated group, 25
finitely presented group, 57
finite order element of a group, 24
free abelian group, 65
free action, 42
free group, 60
freely decomposable /indecomposable group, 79
free product, 74
fully characteristic subgroup, 65
fundamental group of a topological space, 85

general linear group, 19
generating set for a group, 25
generator, 25
geometric group theory, 93
Graham Higman, 86
Gromov, 93
group, 16
group action, 40
group law, 16
group representation theory, 93

Hanna Neumann, 86
Hanna Neumann Conjecture, 63
HNN Extension, 86
homomorphism, 28
hyperbolic group, 93

identity, 16
image, 11

Download free eBooks at bookboon.com

incoherent group, 62
index of a subgroup, 23
infinite dihedral group, 76
infinite group, 17
infinite index, 23
infinite order element of a group, 24
injective map, 11
inner automorphism group, 39
intersection of sets, 10
inverse, 16
inverse image, 11
isometry group, 75
isomorphism, 29
isomorphism problem, 58

Jordan-Hölder theorem, 36
kernel of a homomorphism, 32
Klein four-group, 18
left coset, 22
lower central series, 68

map, 11
modulo, 13
multiplication, 16

nilpotent group, 68
non-hopfian group, 86
normaliser of a subgroup, 34
normal subgroup, 31
Novikov-Boone Theorems, 58

orbit, 41
ordered pair, 10
order of a group, 17
order of a group element, 24
outer automorphism group, 39

pair, 10
paired alphabet, 52
presentation, 53
proper subgroup, 22

quasi-isometry, 93
quotient set, 13

range, 11
rank of a free abelian group, 65
rank of a free group, 60
reduced word, 60
reflexive relation, 12
relation, 12
relator, 53
right coset, 22

set, 10
simple group, 36
soluble group, 67
solution of quintic by radicals, 68
solvable group, 67
special linear group, 38
stabilizer, 40
stable letter, 86
Stallings ends theorem, 93
subgroup, 21
subset, 10
subword, 54
surjective map, 11
Sylow [###.\l2r_1768.eps###]-subgroup, 49
symmetric group, 19
symmetric relation, 12

torsion free group, 62
torsion subgroup, 24
transitive action, 42
transitive relation, 12
trivial group, 18
Turing machine, 58

Download free eBooks at bookboon.com

underlying set, 16
union of sets, 10
unordered pair, 10

van der Waerden trick, 77
van Kampens Theorem, 85
verbal subgroup, 65

word, 53
word problem, 58
word product, 53

Click on the ad to read more

Download free eBooks at bookboon.com