7 Subgroups

7.1 Introduction

It often happens that our groups contain subsets that are themselves groups. For example the set **Z** of integers (with respect to the operation of addition) is a group contained within the larger group **Q** of rational numbers (also with respect to addition). When this happens we say that we have a *subgroup*.

Definition 7.1.1:

Suppose G (.) is a group and that H is a non-empty subset of G that also forms a group with respect to the same operation. Then H is said to be a *subgroup* of G.

Clearly G is a subgroup of itself and so is the set that just consists of the identity element of G. G and $\{1_G\}$ are called *improper subgroups*. All other subgroups are said to be *proper*.

Example 7.1.2:

Suppose we consider the group Z_{12} with respect to addition. Then we have the following subgroups:

{0}	-	improper
{0,6}	-	proper
{0,4,8}	-	proper
{0,3,6,9}	-	proper
{0,2,4,6,8,10}	-	proper
{0,1,2,3,4,5,6,7,8,9,10,11}	-	improper

Example 7.1.3:

Now consider the group $Z_{13} - \{0\}$ with respect to multiplication. This has subgroups:

{1}	-	improper
{1,12}	-	proper
{1,3,9}	-	proper
{1,5,8,12}	-	proper
{1,3,4,9,10,12}	-	proper
{1,2,3,4,5,6,7,8,9,10,11,12}	-	improper

Exercises 7.1:

1. Write down operation tables for each of the proper subgroups described above and convince yourself that the subsets really are closed with respect to the given operations.

2. Try to find all possible subsets of the following groups that are closed with respect to the given operation.

a) Z_8 with respect to addition
b) Z_{11}-{0} with respect to multiplication
c) Z_{13} with respect to addition
d) Z_{19}-{0} with respect to multiplication

3. Can you say anything about the number of elements that can possibly form closed subsets when compared to the number of elements in the original group? We will see later that a very important theorem links these numbers together.

4. Show that every subgroup of an abelian group is also abelian.

7.2 How to find subgroups of finite groups

So far we have seen that some subsets of elements are closed under our given operation but we have not shown that these are in fact subgroups. The following theorem shows that, for finite groups, every closed subset is a subgroup. It is an important theorem as it means we only have one axiom to check instead of four.

Theorem 7.2.1

Suppose G is a finite group and that H is a closed, non-empty subset of G. Then H is a subgroup.

Proof:

We need to convince ourselves that H satisfies each of the four group axioms:

1. H is certainly closed as this is given in the statement of the theorem;
2. Our operation is certainly associative in H as it is associative for all elements of G;
3. G is finite and so the order of every element is finite (Theorem 5.3.9). Hence if $a \in H$ it follows that $a^n = 1_G$ for some n. But since H is closed it follows that all powers of a must belong to H and so in particular $1_G \in H$. Hence H has an identity element.
4. If $a \in H$ then, as above, $a^n = 1$ for some n and all powers of $a \in H$. But then $a^{-1} = a^{n-1}$ and so $a^{-1} \in H$. Hence H contains inverses.

Thus all four group axioms are satisfied and so H is itself a group.
•

Note 7.2.2:

This result does not hold if G is an infinite group and we have to be more careful. For example let G = **Z** with respect to addition. The set H = {1,2,3,4, . . . } is certainly closed with respect to the given operation but does not contain an identity element.

We see, below Theorem 7.3.1, that a similar theorem does exist for infinite groups but that the conditions are not quite the same.

Suppose $G(\cdot)$ is a finite group and that we wish to find possible subgroups of G. The first approach we take is to use the idea of generating elements. We have seen that some sets of group elements allow us to construct the whole of our group (these are our *generating sets* from section 6.1) but that some sets only give us part of the group. However we do know that the set that can be generated must be closed and so these subsets that are generated when we don't get the whole group will form the proper subgroups of G.

Hence one way of finding subgroups is to investigate what subsets can be generated using particular sets of generating elements.

Example 7.2.3

Suppose G is the group $\{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$ where $a^4=1$, $b^2=1$, $a^3b=ba$ and we want to find all possible subgroups.

1. Improper subgroups:

G itself and $\{1\}$ will always be subgroups so we write these down to begin with.

2. Cyclic subgroups:

(The subgroups generated by a single element will be called *cyclic subgroups*). Clearly the sets

$\langle a\rangle = \{1, a, a^2, a^3\}$
$\langle b\rangle = \{1, b\}$

are cyclic subgroups and we can write these down immediately from the defining equations $a^4=1$ and $b^2=1$ respectively. The other cyclic subgroups are

$\langle a^3\rangle = \{1, a^3, a^2, a\}$	(which we have seen before)
$\langle a^2\rangle = \{1, a^2\}$	
$\langle ab\rangle = \{1, ab\}$	(as $(ab)^2 = abab = a(a^3b)b = a^4b^2 = 1.1 = 1$)
$\langle a^2b\rangle = \{1, a^2b\}$	(as $(a^2b)^2 = a^2ba^2b = a^2(ba)ab = a^2(a^3b)ab = a^5(ba)b = a^5(a^3b)b = a^8b^2 = 1$)
$\langle a^3b\rangle = \{1, a^3b\}$	(as $(a^3b)^2=1$ similarly)

3. Non-cyclic subgroups

These can be difficult to find and in general we will not expect you to consider subgroups generated by more than two elements. If we see what we can generate using pairs of elements of G we find that the only new subgroups are:

$\langle a^2,b\rangle = \{1, a^2, b, a^2b\}$
$\langle a^2,ab\rangle = \{1, ab, a^2, a^3b\}$

Since these non-cyclic subgroups must be groups themselves we know in advance what sort of structure they should have. For example:

- there is only one non-cyclic group of order 4 (the Klein 4-group) and so if we are looking for a non-cyclic subgroup with four elements we know it is of this type and so must be generated by two elements of order 2.

- there is only one possible non-cyclic groups of order 6. Hence any non-cyclic subgroup of order six must look like

  $\{1, x, x^2, y, xy, x^2y\}$ where $x^3 = y^2 = 1$, $x^2y = yx$

  and so is generated by one element of order three and one element of order two. If our original group is abelian then all its subgroups must also be abelian and so this possibility cannot arise. We can only have non-cyclic subgroups of order six if the original group is non-abelian.

This sort of process will reduce the amount of work we have to do when we search for non-cyclic subgroups.

Exercises 7.2:

1. Consider the following groups and write down all subgroups (proper and improper) by considering generating sets. The number of non-cyclic subgroups that you need to find is stated alongside the definition of the group.

   a) $G = \{1, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\}$ where $a^6=1$, $b^2=1$, $ab=ba$. (G contains one non-cyclic subgroup of order 4).

   b) $D_6 = \{1, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\}$ where $a^6=1$, $b^2=1$, $a^5b=ba$. (G contains 3 non-cyclic subgroups of order 4 and 2 non-cyclic subgroups of order 6).

   c) $Q = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$ where $a^4=1$, $a^2=b^2$, $a^3b=ba$. (G contains no non-cyclic subgroup).

   d) $A_4 = \{1, a, b, b^2, ab, ba, ab^2, aba, bab, abab, b^2ab, bab^2\}$ where $a^2=1$, $b^3=1$, $(ab)^3=1$. (G contains one non-cyclic subgroup of order 4).

2. Consider the group $S_3 = \left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}$

   with operation multiplication of permutations. Identify all the proper subgroups of S_3 (they are all cyclic).

3. Repeat question 2 for the permutation group

$$\left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\right\}$$

   (This group has 2 non-cyclic subgroups of order 4).

7.3 Subgroups of Infinite Groups

Our example above (see note 7.2.2) showed that finding subgroups of an infinite group is more difficult than finding the subgroups of finite groups. It turns out though, that we have a theorem similar to 7.2.1 above that we can use. The theorem below will be our main weapon when we want to show that we have subgroups of infinite groups.

Theorem 7.3.1

A non-empty subset H of a group G is a subgroup if an only if

$$a,b \in H \Rightarrow ab^{-1} \in H \qquad (*)$$

for all elements a and b.

Proof

This is an if and only if statement so we need to prove two things:

$\Rightarrow$ If H is a subgroup then condition (*) holds for any elements a and b in H.

$\Leftarrow$ If condition (*) holds for any elements a and b in a subset H then H is a subgroup.

1. Suppose H is a subgroup. Then H is a group and so each of the four axioms can be applied to H. But then

   $a,b \in H \Rightarrow b^{-1} \in H$ (inverses belong to H)
   $\Rightarrow ab^{-1} \in H$ (H is closed)

2. Suppose (*) holds for all $a,b \in H$. We need to show that H is a group by demonstrating that each of the group axioms holds. Clearly if our operation in G is associative then it will also be associative in H and so this axiom certainly holds. In addition

   i) Taking b = a in (*) tells us that $aa^{-1} \in H$. But $aa^{-1} = 1$ so H contains the identity element.

   ii) Taking a = 1 in (*) tells us that $b \in H \Rightarrow 1b^{-1} = b^{-1} \in H$. Hence H contains inverse elements.

   iii) Finally if a and $b \in H$ then i) tells us that $b^{-1} \in H$. But then applying (*) with a and b^{-1} tells us that $a(b^{-1})^{-1} = ab \in H$. Hence H is closed under the given operation.

•

Example 7.3.2

Suppose H is the set of all 2x2 matrices of the form

$$\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$$

Then H is a subgroup of the set of all 2x2 matrices with operation matrix multiplication.

Proof:

Suppose $A = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$ are two elements of H. Then $B^{-1} = \begin{pmatrix} 1 & 0 \\ -b & 1 \end{pmatrix}$ and so $AB^{-1} = \begin{pmatrix} 1 & 0 \\ a-b & 1 \end{pmatrix}$

But then $AB^{-1} \in H$ and so H is a subgroup.

Example 7.3.3

Suppose G is the set of all non-zero complex numbers with operation multiplication and let H be the set of all elements of G with modulus 1. Then H is a subgroup of G.

Proof:

If $z = x+iy$ then $|z| = \sqrt{(x^2+y^2)}$. Furthermore $|zw| = |z||w|$. But then if $z \in H$ we have

$$1 = zz^{-1} \Rightarrow 1 = |1| = |zz^{-1}| = |z||z^{-1}| = 1\ |z^{-1}| \Rightarrow |z^{-1}| = 1$$

Hence if $z \in H$, $w \in H$, then $|z| = 1$, $|w^{-1}| = 1$ and so $|zw^{-1}| = |z||w^{-1}| = 1 \times 1 = 1$.

Hence $zw^{-1} \in H$ and so H is a subgroup.

Example 7.3.4

Let G be the set of integers with operation addition and let H be the set of all integers that are a multiple of 5. Then H is a subgroup of G.

Proof

Suppose $x,y \in H$. Then $x = 5k$, $y = 5l$ for some k, l. But then $y^{-1} = -5l$ and so

$$xy^{-1}\ (= x-y) = 5k - 5l = 5(k-l) \in H.$$

Exercises 7.3

1. Does the set of odd integers form a subgroup of **Z(+)**? What about the set of even integers.

2. Does the set $H = \{z \in C : |z| = 2\}$ form a subgroup of the set of complex numbers under multiplication.

3. Use Theorem 7.3.1 to determine that each of the following are subgroups of a group G.

   a) $G = Z(+)$, $H = \{3k: k \in Z\}$;

   b) $G = [R - \{0\}]\ (.)$, $H = \{2^k : k \in Z\}$

   c) G is any group and g is a *fixed* element of G, $H = \{x : x \in G \text{ and } gxg^{-1} = x\}$

   d) G is any abelian group and n is a fixed integer, $H = \{x : x^n = 1\}$

   e) G is any group and K is a fixed subgroup,
   $H = \{x : x \in G \text{ and } kx = xk \text{ for all } k \text{ in } K\}$

4. Suppose H and K are any subgroups of a group G. Show that $H \cap K$ is a subgroup.

5. Is $H \cup K$ always a subgroup? Write down a proof if you think it is or a counter example if you think it isn't.

6. If G is a group we define the centre of G to be the set

   $H = \{x \in G : xg = gx \text{ for every } g \text{ in } G\}$.

   The centre is thus the set of elements which commute with all other elements. Write down the centre of the groups:

   a) D_4
   b) S_3
   c) A_4

   where these groups are defined in the table at the end of section 8.

   Show that in each case the centre of G is a subgroup. Prove (using Theorem 7.3.1) that the centre is always a subgroup.

   How can we use the group operation table to decide if an element x belongs to the centre of the group? What can we say about the row and the column beginning x?