6 Generating Sets and Cyclic Groups

6.1 Generating Sets

Examples 5.3.3, 5.3.4 and 5.3.5 concerned themselves with finding the order of a specific element of $\mathbf{Z}_6(\oplus)$. These examples can also be put to another purpose. We notice in 5.3.5 that every element of $\mathbf{Z}_6(\oplus)$ can be calculated by repeatedly combining the element [5] with itself.

We say that [5] generates the group $\mathbf{Z}_6(\oplus)$ and can write this by saying $\mathbf{Z}_6(\oplus) = <[5]>$.

Notice that neither [2] nor [3] generate the whole of $\mathbf{Z}_6(\oplus)$.

What would happen if we considered the remaining elements of $\mathbf{Z}_6(\oplus)$, ie [0], [1], [4]?

We should observe that [0] which is the identity element for $\mathbf{Z}_6(\oplus)$ will only generate itself, [1] will generate all the elements of $\mathbf{Z}_6(\oplus)$ and [4] will generate [2], [0] and itself.

So we also have $\mathbf{Z}_6(\oplus) = <[1]>$

Example 6.1.1

In $\{1, -1, i, -i\}(.)$ where $i^2 = -1$

$$\begin{aligned} i &= i \\ i \times i &= -1 \\ i \times i \times i &= -i \\ i \times i \times i \times i &= 1 \end{aligned}$$

i has order 4 and also generates the group

$$\begin{aligned} -i &= -i \\ -i \times -i &= -1 \\ -i \times -i \times -i &= i \\ -i \times -i \times -i \times -i &= 1 \end{aligned}$$

$-i$ has order 4 and also generates the group

$$\begin{aligned} -1 &= -1 \\ -1 \times -1 &= 1 \end{aligned}$$

-1 has order 2 and **does not** generate the group

1 has order 1 and can only generate itself

So $\{1, -1, i, -i\}(.) = <i> = <-i>$

In the above example and the discussion examples relating to $\mathbf{Z}_6(\oplus)$, we notice that each of these groups could be generated by a single element.

We notice also that the order of the generating element is the same as the order of the group. However the Klein 4 group, $K_4 = \{1, a, b, ab\}$ where $a^2 = b^2 = 1$ and $ab = ba$, clearly cannot be generated from a single element. It can however be generated from two elements.

$K_4 = <a, b>$ since $a^2 = 1$ and $a.b = ab$, and a and b are generators

Also
$K_4 = <a, ab>$ since $a^2 = 1$ and $a.ab = a^2 b = 1\, b = b$, and a and ab are generators

and
$K_4 = <ab, b>$ since $b^2 = 1$ and $ab.b = ab^2 = a.1 = a$, and ab and b are generators

So $K_4 = <a, b> = <a, ab> = <ab, b>$

All of this can be formalised with the following definition

6.1.2 Definition

A set of elements is said to generate a group if every element of the group can be expressed as a product of powers of these elements.

If G is generated by $\{g_1, g_2, \ldots\ldots\ldots, g_n\}$ then we write $G = <g_1, g_2, \ldots\ldots\ldots, g_n>$

Note

- A generating set can never contain the identity element. This is because the identity can only generate itself. ie $1 = 1^2 = 1^3 = \ldots\ldots\ldots$
- In this course we will usually only concern ourselves with groups that have generating sets containing either one or two elements.

Exerccise 6.1

1. Find all the generating sets containing one element which generate each of the following groups.
   a) $\mathbf{Z}_7(\oplus)$ b) $\mathbf{Z}_8(\oplus)$
   c) $\{\mathbf{Z}_5 - [0]\}\ (\odot)$ d) $\{\mathbf{Z}_7 - [0]\}\ (\odot)$

2. Find all the generating sets of each of the following groups
   a) $\{1, -1, i, j, k, -i, -j, -k\}$
   where $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$
   b) $\mathbf{Z}_2 \times \mathbf{Z}_3\ (*)$ where * is defined by $(a, b) * (c, d) = (a \oplus_2 c, b \oplus_3 d)$
   where $\oplus_2$ is addition mod 2 and $\oplus_3$ is addition mod 3.
   b) $\{1, a, a^2, b, ab, ba\}$ where $a^3 = b^2 = 1$ and $a^2 b = ba$

3. Find a generating set for S_3.

6.2 Cyclic Groups

Groups which can be generated by a single element are called cyclic groups.

6.2.1 Definition
A group is called cyclic if every element can be written in the form a^k for some group element a and some positive integer k. The cyclic group of order n is written $\mathbf{C}_n$ The element a is said to generate the group. We write $\mathbf{C}_n = \langle a \rangle$ where $a^n = 1$

It is clear that there is a cyclic group of every possible order.

$$\mathbf{C}_n = \langle a \rangle = \{ 1, a, a^2, a^3, a^4, \ldots\ldots\ldots\ldots, a^{n-1} \} \text{ where } a^n = 1$$

We also observe that the same cyclic group may be generated by a number of different elements.

$\mathbf{Z}_6$ (⊕) was generated by [1] and [5]

Example 6.2.2

Find all the generating sets of $\mathbf{C}_8 = \{1, a, a^2, a^3, a^4, a^5, a^6, a^7\}$ $a^8 = 1$
Clearly $\mathbf{C}_8 = \langle a \rangle$, however we must also consider what each of the other elements generates.

$\boldsymbol{a^2}$:	a^2	$(a^2)^2 = a^4$	$(a^2)^3 = a^6$	$(a^2)^4 = a^8 = 1$

$\boldsymbol{a^3}$:	a^3	$(a^3)^2 = a^6$	$(a^3)^3 = a^9 = a$	$(a^3)^4 = a^{12} = a^4$
	$(a^3)^5 = a^{15} = a^7$	$(a^3)^6 = a^{18} = a^2$	$(a^3)^7 = a^{21} = a^5$	$(a^3)^8 = a^{24} = 1$

$\boldsymbol{a^3}$ generates the whole of $\mathbf{C}_8$

$\boldsymbol{a^4}$:	a^4	$(a^4)^2 = a^8 = 1$

$\boldsymbol{a^5}$:	a^5	$(a^5)^2 = a^{10} = a^2$	$(a^5)^3 = a^{15} = a^7$	$(a^5)^4 = a^{20} = a^4$
	$(a^5)^5 = a^{25} = a$	$(a^5)^6 = a^{30} = a^6$	$(a^5)^7 = a^{35} = a^3$	$(a^5)^8 = a^{40} = 1$

$\boldsymbol{a^5}$ generates the whole of $\mathbf{C}_8$

$\boldsymbol{a^6}$:	a^6	$(a^6)^2 = a^{12} = a^4$	$(a^6)^3 = a^{18} = a^2$	$(a^6)^4 = a^{24} = 1$

$\boldsymbol{a^7}$:	a^7	$(a^7)^2 = a^{14} = a^6$	$(a^7)^3 = a^{21} = a^5$	$(a^7)^4 = a^{28} = a^4$
	$(a^7)^5 = a^{35} = a^3$	$(a^7)^6 = a^{42} = a^2$	$(a^7)^7 = a^{49} = a$	$(a^7)^8 = a^{56} = 1$

$\boldsymbol{a^7}$ generates the whole of $\mathbf{C}_8$

Thus $\mathbf{C}_8 = \langle a \rangle = \langle a^3 \rangle = \langle a^5 \rangle = \langle a^7 \rangle$, hence $\mathbf{C}_8$ has 4 possible generating sets.

We can also make some interesting observations about the other elements

$\langle a^2 \rangle = \langle a^6 \rangle = \{1, a^2, a^4, a^6\}$ and $\langle a^4 \rangle = \{1, a^4\}$

Note both $\{1, a^2, a^4, a^6\}$ and $\{1, a^4\}$ are also groups. the first one has the form $\mathbf{C}_4$ generated by either a^2 or a^6 and the second one has the form $\mathbf{C}_2$ generated by a^4.

Exercise 6.2

1. Find all the generating elements of the following cyclic groups
   a) $\mathbf{Z}_5\,(\oplus)$ b) $\mathbf{Z}_4\,(\oplus)$ c) $\{\mathbf{Z}_{11} - [0]\}\,(\odot)$ d) $\{\mathbf{Z}_7 - [0]\}\,(\odot)$

2. Can you make any observations between the number of generators for a cyclic group and the order of that group?

3. Show that Exercise 6.1 No 2b) is cyclic

4. Show that $\mathbf{Z}_2 \times \mathbf{Z}_2\,(*)$ where * is defined in a similar fashion to Exercise 6.1 No 2b) is not cyclic

5. $G(.) = \{1, x, y, y^2, y^4, xy, xy^2, xy^4\}$ where $x^2 = y^5 = 1$ and $xy = yx$. Prove that G is cyclic.