

MATH 4/51001  
SUBGROUPS OF CYCLIC GROUPS

**EXAMPLE 1:**

Let  $G = \langle g \rangle$  be a (multiplicative) cyclic group of order 12, so  $g^{12} = e$  and

$$G = \{e, g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, g^{11}\}.$$

GENERATORS

The **generators** of  $G$  are the elements  $g^m$  with  $1 \leq m \leq 12$  and  $(m, 12) = 1$ . Hence we have

$$\text{Generators of } G : g, g^5, g^7, g^{11}$$

so that

$$G = \langle g \rangle = \langle g^5 \rangle = \langle g^7 \rangle = \langle g^{11} \rangle.$$

For example,

$$\begin{aligned} \langle g^5 \rangle &= \{e, g^5, (g^5)^2, (g^5)^3, (g^5)^4, (g^5)^5, (g^5)^6, (g^5)^7, (g^5)^8, (g^5)^9, (g^5)^{10}, (g^5)^{11}\} \\ &= \{e, g^5, g^{10}, g^{15}, g^{20}, g^{25}, g^{30}, g^{35}, g^{40}, g^{45}, g^{50}, g^{55}\} \\ &= \{e, g^5, g^{10}, g^3, g^8, g^1, g^6, g^{11}, g^4, g^9, g^2, g^7\} \quad (\text{using } g^{12} = e) \\ &= \{e, g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, g^{11}\} = G. \end{aligned}$$

ORDERS

The **order** of  $g^m$  is  $o(g^m) = \frac{12}{(12, m)}$ , so we have:

Element	$e$	$g$	$g^2$	$g^3$	$g^4$	$g^5$	$g^6$	$g^7$	$g^8$	$g^9$	$g^{10}$	$g^{11}$
Order Formula	$\frac{12}{(12,0)}$	$\frac{12}{(12,1)}$	$\frac{12}{(12,2)}$	$\frac{12}{(12,3)}$	$\frac{12}{(12,4)}$	$\frac{12}{(12,5)}$	$\frac{12}{(12,6)}$	$\frac{12}{(12,7)}$	$\frac{12}{(12,8)}$	$\frac{12}{(12,9)}$	$\frac{12}{(12,10)}$	$\frac{12}{(12,11)}$
Order	1	12	6	4	3	12	2	12	3	4	6	12

## SUBGROUPS

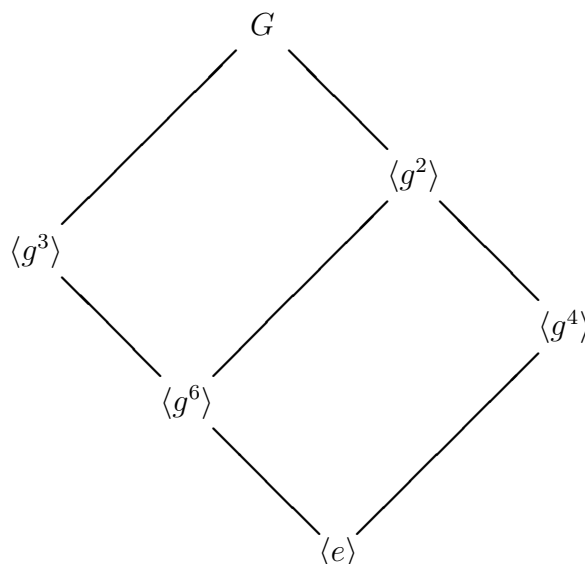
There is exactly one **subgroup** of  $G = \langle g \rangle$  of order  $m$  for each positive divisor  $m$  of  $12 = |G|$ , and this subgroup is  $\langle g^{12/m} \rangle$ . Therefore, the subgroups of  $G$  are as follows.

Order	Generators	Elements
1	$\langle e \rangle$	$\{e\}$
2	$\langle g^6 \rangle$	$\{e, g^6\}$
3	$\langle g^4 \rangle = \langle g^8 \rangle$	$\{e, g^4, g^8\}$
4	$\langle g^3 \rangle = \langle g^9 \rangle$	$\{e, g^3, g^6, g^9\}$
6	$\langle g^2 \rangle = \langle g^{10} \rangle$	$\{e, g^2, g^4, g^6, g^8, g^{10}\}$
12	$\langle g \rangle = \langle g^5 \rangle = \langle g^7 \rangle = \langle g^{11} \rangle$	$\{e, g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, g^{11}, g^{12}\}$

Notice that if  $a$  is a generator for the subgroup of order  $m$ , then so is  $a^k$  for all  $1 \leq k \leq m$  with  $(k, m) = 1$ . For example, the subgroup of order 6 is  $\langle g^{12/6} \rangle = \langle g^2 \rangle$ . The other generators are  $(g^2)^k$ , where  $1 \leq k \leq 6$  and  $(k, 6) = 1$ ; that is,  $k = 1$  and  $k = 5$ . Hence the generators of  $\langle g^2 \rangle$  are  $g^2$  and  $(g^2)^5 = g^{10}$ .

## SUBGROUP DIAGRAM

For subgroups  $H_1$  and  $H_2$ , we have the **containment**  $H_1 \leq H_2$  if and only if  $|H_1|$  divides  $|H_2|$ . Using the table of subgroups above, we have the following diagram (where downward edges and paths denote containment):



**EXAMPLE 2:**

Let  $G = \mathbb{Z}_{18} = \langle [1] \rangle$ , a cyclic group of order 18 under addition, so  $18[1] = [18] = [0]$  and

$$G = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17]\}$$

$$= \{0[1], 1[1], 2[1], 3[1], 4[1], 5[1], 6[1], 7[1], 8[1], 9[1], 10[1], 11[1], 12[1], 13[1], 14[1], 15[1], 16[1], 17[1]\}$$

GENERATORS

The **generators** of  $G$  are the elements  $m[1] = [m]$  with  $1 \leq m \leq 18$  and  $(m, 18) = 1$ . Hence we have

$$\text{Generators of } G : [1], [5], [7], [11], [13], [17]$$

so that

$$G = \langle [1] \rangle = \langle [5] \rangle = \langle [7] \rangle = \langle [11] \rangle = \langle [13] \rangle = \langle [17] \rangle.$$

For example,

$$\begin{aligned} \langle [7] \rangle &= \{0[7], 1[7], 2[7], 3[7], 4[7], 5[7], 6[7], 7[7], 8[7], 9[7], 10[7], 11[7], 12[7], 13[7], 14[7], 15[7], 16[7], 17[7]\} \\ &= \{[0], [7], [14], [21], [28], [35], [42], [49], [56], [63], [70], [77], [84], [91], [98], [105], [112], [119]\} \\ &= \{[0], [7], [14], [3], [10], [17], [6], [13], [2], [9], [16], [5], [12], [1], [8], [15], [4], [11]\} \quad (\text{using } [18] = [0]) \\ &= \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17]\} = G. \end{aligned}$$

ORDERS

The **order** of  $m[1] = [m]$  is  $o([m]) = \frac{18}{(18, m)}$ , so we have:

Element	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
Order Formula	$\frac{18}{(18,0)}$	$\frac{18}{(18,1)}$	$\frac{18}{(18,2)}$	$\frac{18}{(18,3)}$	$\frac{18}{(18,4)}$	$\frac{18}{(18,5)}$	$\frac{18}{(18,6)}$	$\frac{18}{(18,7)}$	$\frac{18}{(18,8)}$
Order	1	18	9	6	9	18	3	18	9

Element	[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[17]
Order Formula	$\frac{18}{(18,9)}$	$\frac{18}{(18,10)}$	$\frac{18}{(18,11)}$	$\frac{18}{(18,12)}$	$\frac{18}{(18,13)}$	$\frac{18}{(18,14)}$	$\frac{18}{(18,15)}$	$\frac{18}{(18,16)}$	$\frac{18}{(18,17)}$
Order	2	9	18	3	18	9	6	9	18

## SUBGROUPS

There is exactly one **subgroup** of  $G = \langle [1] \rangle$  of order  $m$  for each positive divisor  $m$  of  $18 = |G|$ , and this subgroup is  $\langle [18/m] \rangle$ . Therefore, the subgroups of  $G$  are as follows.

Order	Generators	Elements
1	$\langle [0] \rangle$	$\{[0]\}$
2	$\langle [9] \rangle$	$\{[0], [9]\}$
3	$\langle [6] \rangle = \langle [12] \rangle$	$\{[0], [6], [12]\}$
6	$\langle [3] \rangle = \langle [15] \rangle$	$\{[0], [3], [6], [9], [12], [15]\}$
9	$\langle [2] \rangle = \langle [4] \rangle = \langle [8] \rangle = \langle [10] \rangle = \langle [14] \rangle = \langle [16] \rangle$	$\{[0], [2], [4], [6], [8], [10], [12], [14], [16]\}$
18	$\langle [1] \rangle = \langle [5] \rangle = \langle [7] \rangle = \langle [11] \rangle = \langle [13] \rangle = \langle [17] \rangle$	$\{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17]\}$

Notice that if  $[a]$  is a generator for the subgroup of order  $m$ , then so is  $k[a]$  for all  $1 \leq k \leq m$  with  $(k, m) = 1$ . For example, the subgroup of order 9 is  $\langle [18/9] \rangle = \langle [2] \rangle$ . The other generators are  $k[2] = [2k]$ , where  $1 \leq k \leq 9$  and  $(k, 9) = 1$ ; that is,  $k = 1, 2, 4, 5, 7, 8$ . Hence the generators of  $\langle [2] \rangle$  are  $[2], [4], [8], [10], [14]$ , and  $[16]$ .

## SUBGROUP DIAGRAM

For subgroups  $H_1$  and  $H_2$ , we have the **containment**  $H_1 \leq H_2$  if and only if  $|H_1|$  divides  $|H_2|$ . Using the table of subgroups above, we have the following diagram (where downward edges and paths denote containment):

