Cyclic Subgroups If a subgroup of a group can be generated using the power of an element, th subgroup is called the **cyclic subgroup.** The term *power* here means repeatedly applying the grou operation to the element:

$$a^n \rightarrow a \bullet a \bullet \ldots \bullet a \qquad (n \text{ times})$$

he set made from this process is referred to as <*a*>. Note that the duplicate elements must be discarde ote also that $a^0 = e$.

Example 4.7 Four cyclic subgroups can be made from the group $G = \langle Z_6, + \rangle$. They are $H_1 = \langle \{0\}, + \rangle$, $H_2 = \langle \{0, 2, 4\}, + \rangle$, $H_3 = \langle \{0, 3\}, + \rangle$, and $H_4 = G$. Note that when the operation is addition, a^n mean multiplying *n* by *a*. Note also that in all of these groups, the operation is addition modulo 6. The followin how how we find the elements of these cyclic subgroups.

a. The cyclic subgroup generated from 0 is H_1, which has only one element, the identity element.

$0^0 \bmod 6 = 0$ (stop: the process will be repeated)

b. The cyclic subgroup generated from 1 is H_4, which is G itself.

$1^0 \bmod 6 = 0$
$1^1 \bmod 6 = 1$
$1^2 \bmod 6 = (1 + 1) \bmod 6 = 2$
$1^3 \bmod 6 = (1 + 1 + 1) \bmod 6 = 3$
$1^4 \bmod 6 = (1 + 1 + 1 + 1) \bmod 6 = 4$
$1^5 \bmod 6 = (1 + 1 + 1 + 1 + 1) \bmod 6 = 5$ (stop: the process will be repeated)

The cyclic subgroup generated from 2 is H_2, which has three elements: 0, 2, and 4.

$2^0 \bmod 6 = 0$
$2^1 \bmod 6 = 2$
$2^2 \bmod 6 = (2 + 2) \bmod 6 = 4$ (stop: the process will be repeated)

Scanned with CamScanner

d. The cyclic subgroup generated from 3 is H_3, which has two elements: 0 and 3.

$3^0 \bmod 6 = 0$
$3^1 \bmod 6 = 3$ (stop: the process will be repeated)

e. The cyclic subgroup generated from 4 is H_2; this is not a new subgroup.

$4^0 \bmod 6 = 0$
$4^1 \bmod 6 = 4$
$4^2 \bmod 6 = (4 + 4) \bmod 6 = 2$ (stop: the process will be repeated)

f. The cyclic subgroup generated from 5 is H_4, which is **G** itself.

$5^0 \bmod 6 = 0$
$5^1 \bmod 6 = 5$
$5^2 \bmod 6 = 4$
$5^3 \bmod 6 = 3$
$5^4 \bmod 6 = 2$
$5^5 \bmod 6 = 1$ (stop: the process will be repeated)

Example 4.8 Three cyclic subgroups can be made from the group $G = <Z_{10}^*, \times>$. **G** has only four elements: 1, 3, 7, and 9. The cyclic subgroups are $H_1 = <\{1\}, \times>$, $H_2 = <\{1, 9\}, \times>$, and $H_3 = G$. The following show how we find the elements of these subgroups.

a. The cyclic subgroup generated from 1 is H_1. The subgroup has only one element, the identity element.

$1^0 \bmod 10 = 1$ (stop: the process will be repeated)

b. The cyclic subgroup generated from 3 is H_3, which is **G** itself.

$3^0 \bmod 10 = 1$
$3^1 \bmod 10 = 3$
$3^2 \bmod 10 = 9$
$3^3 \bmod 10 = 7$ (stop: the process will be repeated)

c. The cyclic subgroup generated from 7 is H_3, which is **G** itself.

$7^0 \bmod 10 = 1$
$7^1 \bmod 10 = 7$
$7^2 \bmod 10 = 9$
$7^3 \bmod 10 = 3$ (stop: the process will be repeated)

d. The cyclic subgroup generated from 9 is H_2. The subgroup has only two elements.

$9^0 \bmod 10 = 1$
$9^1 \bmod 10 = 9$ (stop: the process will be repeated)

Scanned with CamScanner