- For any element a from a group, let (a) denote the set $\{a^n \mid n \in Z\}$.
- In particular, observe that the exponents of a include all negative integers as well as 0 and the positive integers (a^0 is defined to be the identity).
- **(a) is a Subgroup .** Let G be a group, and let a be any element of G. Then, (a) is a sub- group of G.
- Since $a \in (a)$, (a) is not empty.
- Let $a^n, a^m \in (a)$.
- Then, $a^n(a^m)^{-1} = a^{n-m} \in (a)$;
- so,(a) is a subgroup of G.
- Let H be a nonempty subset of a group G. If ab^{-1} is in H whenever a and b are in H, then H is a subgroup of G.

- The subgroup (a) is called the **cyclic subgroup** of G generated by a.
- In the case that G ∈(a), we say that G is cyclic and a is a generator of G.
- We indicate that *G* is a cyclic group generated by *a* by writing *G* = (a)
- **Cyclic Group.** A group G is called **cyclic** if there is an element a in G such that $G = \{a^n \mid n \in Z\}$.
- If operation is addition(+), then $G = \{ng \mid n \in Z\}$.
- Such an element *a* is called a **generator** of *G*.
- A cyclic group may have many generators.
- Notice that although the list . . . , $a^{-2}, a^{-1}, a^0, a^1, a^2$, . . . has infinitely many entries, the set $\{a^n \mid n \in Z\}$ might have only finitely many elements.
- Also note that, $a^i a^j = a^{i+j}$
- $= a^{j+i}$
- $= a^j a^i$,
- **Every cyclic group is Abelian.**

- **EXAMPLES.**

- **1.** In U(10), (3)= {1,3, 7, 9} = $\{3^0, 3^1, 3^3, 3^2\}$
- Here, $3^0 = 1$
- $3^1 = 3$,
- $3^2 = 9$,
- $3^3 = 7$,
- $3^4 = 1$,
- $3^5 = 3^4 .3 = 1.3$,
- $3^6 = 3^4.3^2 = 9, \dots;$
- $3^{-1} = 7$ (since 3.7=1),
- $3^{-2} = 3^{-1}.3^{-1} = 7.7 = 9$,
- $3^{-3} = 3^{-2}.3^{-1} = 9.7 = 3$,
- $3^{-4} = 3^{-2}.3^{-2} = 9.9 = 1$,
- $3^{-5} = 3^{-4}.3^{-1} = 1.7$,
- $3^{-6} = 3^{-4}.3^{-2} = 1.9 = 9, \dots.$
- Also, $\{1, 3, 7, 9\} = \{7^0, 7^3, 7^1, 7^2\} = (7)$. $(7^0 = 1, 7^1 = 7, 7^2 = 9, 7^3 = 3)$
- So both 3 and 7 are generators for *U*(10).

- **2.** In Z_{10}, $\langle 2 \rangle = \{2, 4, 6, 8, 0\}$. Remember, a^n means na when the operation is addition.
- 2=2
- 2+2=4
- 2+2+2=6
- 2+2+2+2=8
- 2+2+2+2+2=0
- 2+2+2+2+2+2=2
- 2+2+2+2+2+2+2=4
- 2+2+2+2+2+2+2+2=6,……and so on.

- **3.** The set of integers Z under ordinary addition is an infinite cyclic group because every element is a multiple of 1 (or of −1) .
- Both 1 and -1 are its generators.
- (-1) = Z. (Here each entry in the list ..., -2(-1), -1(-1), 0(-1), 1(-1), 2(-1), . . . represents a distinct group element).
- (1)=Z.
- Recall that, when the operation is addition,
- 1^n is interpreted as 1+1+...+1, n terms ,when n is positive
- and as (-1) + (-1) + ...+ (-1) , $|n|$ terms when n is negative.)
- **4.**The set Z_n ={0,1,...,n-1}, for $n \geq 1$ is a finite cyclic group under addition modulo n.
  Z_n =(1)=(-1)=(n-1) (Note n-1=-1modn).
- Other generators are possible depending on n.
- Unlike Z, which has only two generators, Z_n may have many generators (depending on n, we are given).
- **5.**Z_8=(1) =(3)=(5)=(7) .
- To verify, for instance, that Z_8 =(3), we note that (3)={3, 3+3,3+3+3,...}
  ={3, 6, 1, 4, 7, 2, 5, 0}
- = Z_8.
- Thus, 3 is a generator of Z_8.
- On the other hand, 2 is not a generator since (2) = {0, 2, 4, 6} ≠ Z_8

- 6. In Z_7, 1 generates Z_7, since
- 1+1=2,
- 1+1+1=3,
- 1+1+1+1=4,
- 1+1+1+1+1=5,
- 1+1+1+1+1+1=6,
- 1+1+1+1+1+1+1=0
- In other words, if you add 1 to itself repeatedly, you eventually cycle back to 0.
- Notice that 3 also generates Z_7:
- 3+3=6
- 3+3+3=2
- 3+3+3+3=5
- 3+3+3+3+3=1
- 3+3+3+3+3+3=4
- 3+3+3+3+3+3+3=0
- This "same" group can be written as: Z_7 ={1,a,2a,3a,4a,5a, 6a}. In this form, a is a generator of Z_7. It turns out that in Z_7 = {0, 1, 2, 3, 4, 5, 6}, every nonzero element generates the group.
- 7. In Z_6 = {0, 1, 2, 3, 4, 5}, only 1 and 5 are generaters.

- Quite often in mathematics, a “nonexample” is as helpful in understanding a concept as an example.
- With regard to cyclic groups, we shall study $U(8)$, which is not a cyclic group.
- How can we verify this?
- Notice that $U(8) = \{1, 3, 5, 7\}$.
- But $(1)= \{1\}$,
- $(3)= \{3, 1\}$,
- $(5)=\{5, 1\}$,
- $(7)= \{7, 1\}$
- so $U(8) \neq (a)$ for any a in $U(8)$.

  With these examples we are now ready to tackle cyclic groups in an abstract way and state their key properties.