<u>Groups</u>: A nonempty set of elements G is said to form a <u>group</u> if in G there is defined a binary operation, called the product and denoted by $\cdot$, such that:

1. $a, b \in G$ implies that $a \cdot b \in G$ (closed).
2. $a, b, c \in G$ implies that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associative law)
3. There exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$ (the existence of an identity element in G).
4. For every $a \in G$ there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$ (the existence of inverses in G).

A group G is said to be <u>abelian</u> (or commutative) if for every $a, b \in G$, $a \cdot b = b \cdot a$. A group which is not abelian is called <u>non-abelian</u>. A <u>finite group</u> has finite number of elements. The number of elements in a finite group is called its order and is denoted $o(G)$, where G is a finite group.

<u>Examples of groups</u>:

1. $G_1 = (Z, +)$ where $Z = \{0, \pm 1, \pm 2, \dots\}$ is the set of all integers. G_1 is an abelian group of infinite order.
2. $G_2 = (\{1, -1\}, *)$. G_2 is an abelian group of order 2.
3. Let n be any integer. We construct an abelian group of order n as follows: G_3 will consist of all symbols a^i, $i = 0, 1, 2, \dots, n-1$ where we insist that $a^0 = a^n = e$, $a^i \cdot a^j = a^{i+j}$ if $i + j \le n$ and $a^i \cdot a^j = a^{i+j-n}$ if $i + j > n$. G_3 is called a cyclic group of order n.

④ $G_4 = (Z_n, +_n)$ where Z_n is the complete residue system modulo n, and $+_n$ is addition modulo n. G_4 is an abelian group of order n.

⑤ $G_5 = (Z_n^*, *_n)$ where Z_n^* is the reduced residue system modulo n, and $*_n$ is multiplication modulo n. G_5 is an abelian group of order $\phi(n)$.

<u>Subgroups</u>: A nonempty subset H of a group G is said to be a <u>subgroup</u> of G if, under the product in G, H itself forms a group.

<u>Examples of Subgroups</u>:

⑥ Let $G_1 = (Z, +)$, and let $H_n = (nZ, +)$, where nZ is the set of all integers which are multiples of n. H_n is a subgroup of G_1.

⑦ Let G be any group, $a \in G$. Let $(a) = \{a^i / i = 0, \pm 1, \pm 2, \dots\}$. (a) is a subgroup of G. It is called the cyclic subgroup generated by a. If for some choice of a, $G = (a)$, then G is said to be a <u>cyclic group</u>, a is a generator of G.

If G is a group and $a \in G$, the <u>order</u> of a is the least positive integer m such that $a^m = e$. If no such integer exists we say that a is of infinite order.

If G is a finite group and $a \in G$, then $o(a) \mid o(G)$.

If G is a finite group and $a \in G$, then $a^{o(G)} = e$.

<u>Primitive Roots</u>: If for some $g \in Z_n^*$, $(g) = G_S = (Z_n^*, *_n)$ then g is called a primitive root modulo n. This will happen when the order of g is $\phi(n)$: $g^{\phi(n)} \equiv 1 \pmod n$ but $g^i \not\equiv 1 \pmod n$ for $i < \phi(n)$. Here g will be a generator for Z_n^*.

There exists a primitive root modulo m if and only if $m = 1, 2, 4, p^\alpha$, or $2p^\alpha$, where p is an odd prime.

<u>Examples</u>: Consider $(Z_6^*, *_6) = \{1, 5\}$.

$$(5) = \{5, 5^2 (\mathrm{mod}\ 6)\} = \{1, 5\} = Z_6^*.$$

$\Rightarrow$ 5 is a primitive root mod 6.

$(1) = \{1\} \neq Z_6^* \Rightarrow 1$ is not a primitive root mod 6. $\Rightarrow Z_6^*$ is a cyclic group.

Consider $(Z_8^*, *_8) = \{1, 3, 5, 7\}$

$(1) = \{1\} \neq Z_8^*$

~~(2) = {2, 4}~~

$(3) = \{3, 3^2 \bmod 8\} = \{1, 3\} \neq Z_8^*$

$(5) = \{5, 5^2 \bmod 8\} = \{1, 5\} \neq Z_8^*$

$(7) = \{7, 7^2 \bmod 8\} = \{1, 7\} \neq Z_8^*$

$\Rightarrow Z_8^*$ does not have any primitive roots mod 8 $\Rightarrow$ it is not a cyclic group.