Q.2) Define the operation $*$ on $\mathbb{Z}$ by $a*b=a+b+2$ for all a, b in $\mathbb{Z}$.

a) Show that $*$ is a commutative operation on $\mathbb{Z}$.

b) Show that $\mathbb{Z}$ is a group with respect to $*$.

c) For $n\in\mathbb{Z}^+$, find an explicit formula to compute 0^n, verify it. (the formula should not have any * in it).

d) Determine whether $<0>$ is finite or infinite. Explain

a) Let $a,b\in\mathbb{Z}$. $a*b=a+b+2=b+a+2=b*a$.
Hence $*$ is commutative.

b) $\mathbb{Z}$ is closed w.r.to $*$ because $a*b=a+b+2\in\mathbb{Z}$ for $a,b\in\mathbb{Z}$.

$*$ is associative because for all $a,b,c\in\mathbb{Z}$ we have

$a*(b*c)=a+b*c+2=a+b+c+2+2=$

$=a+b+2+c+2=(a*b)*c$.

$*$ has an identity element; $a*x=a \Leftrightarrow a+x+2=a$

$\Leftrightarrow x=-2$.

By (a) $*$ is commutative, so -2 is the identity element.

Let $a\in\mathbb{Z}$. $a*x=-2 \Leftrightarrow a+x+2=-2 \Leftrightarrow x=-4-a$.

Hence $a^{-1}=-4-a\in\mathbb{Z}$. Thus inverses exist in $\mathbb{Z}$ w.r.to $*$.

Therefore $\mathbb{Z}$ is a group w.r.to $*$.

c) $0^1=0$, $0^2=0*0=0+0+2=2$, $0^3=0*0^2=0+2+2=4$,

$0^4=0^2*0^2=2*2=2+2+2=6$, ...

$0^1=0$
$0^2=2$
$0^3=4$
$0^4=6$
⋮

Claim: $0^n=2(n-1)$, for all $n\in\mathbb{Z}^+$.

$n=1$, $n=2$ are true.

Suppose $0^{n-1}=2((n-1)-1)=2(n-2)$ is true.

Then $0^n=0*0^{n-1}=0*2(n-2)=2(n-2)+2=$
$=2n-4+2=2(n-1)$.

Therefore by P.M.I. $0^n=2(n-1)$ for all $n\in\mathbb{Z}^+$.

d) Since $0^n=2(n-1)$ for all $n\in\mathbb{Z}^+$, $0^n\neq-2$ for all $n\in\mathbb{Z}^+$.

Because $2(n-1)=-2 \Leftrightarrow 2n-2=-2 \Leftrightarrow 2n=0 \Leftrightarrow n=0$.

Therefore $0^n\neq-2$ for all $n\in\mathbb{Z}^+$.

Then $<0>$ is an infinite group.

Q.3) Let $\mathbb{Z}_{12}=\{\bar{0},\bar{1},\ldots,\overline{11}\}$ be the additive group of integers modulo 12.

a) Find all distinct subgroups of $\mathbb{Z}_{12}$.

b) Find all generators of $\mathbb{Z}_{12}$.

Let G denote the set of all invertible elements of $\mathbb{Z}_{12}$ with respect to multiplication. It is known that G is a group with respect to multiplication.

c) Find all elements of G.

d) Find the order of each one of the elements of G.

e) Determine if G a cyclic group or not and write down all cyclic subgroups of G.

a) $\mathbb{Z}_{12}=<\bar{1}>$, all subgps of $\mathbb{Z}_{12}$ are of the form $<\bar{1}^d>$ where d is a positive divisor of 12.

Divisors of 12 are $1,2,3,4,6,12$.

Hence $<\bar{1}>, <\bar{2}>, <\bar{3}>, <\bar{4}>, <\bar{6}>, <\bar{0}>$ are all distinct subgroups of $\mathbb{Z}_{12}$.

b) a^m is a generator of $<a>$ if and only if $\gcd(m,n)=1$ where $|<a>|=n$.

Hence $\bar{1}, \bar{5}, \bar{7}, \overline{11}$ are generators of $\mathbb{Z}_{12}$, there is no other generator.

c) $G=\{\bar{1},\bar{5},\bar{7},\overline{11}\}$,

d) $o(\bar{1})=1$, $o(\bar{5})=2$ because $\bar{5}\bar{5}=\overline{25}=\bar{1}$.

$o(\bar{7})=2$ because $\bar{7}.\bar{7}=\overline{49}=\bar{1}$.

$o(\overline{11})=2$ " $\overline{11}.\overline{11}=\overline{121}=\bar{1}$.

e) G is not cyclic every element when squared is itself, so, there is no generator for G.

$<\bar{1}>=\{\bar{1}\}$,

$<\bar{5}>=\{\bar{1},\bar{5}\}$

$<\bar{7}>=\{\bar{1},\bar{7}\}$

$<\overline{11}>=\{\bar{1},\overline{11}\}$.