Subgroups of $\mathbb{Z}_n$

Corollary For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k; Moreover these are the only subgroups of $\mathbb{Z}_n$

Proof. $\mathbb{Z}_n = \langle 1 \rangle$

$\langle a \rangle$ has exactly one subgroup of order k - namely $\langle a^{n/k} \rangle$ | $a = 1$ in the previous th^m

subgroups are $\langle (1)^{n/k} \rangle = \langle n/k \rangle$

Euler's Phi Function

It is defined as, $\phi(1) = 1$

and for any integer $n > 1$, $\phi(n)$ denotes the number of positive integers less than n and relatively prime to n.

$\phi(n) =$ no. of elements of $\{ a \in \mathbb{N} \mid \gcd(a,n) = 1 \}$ for $n > 1$

$U(n)$

$$U(n) = \{ a \in \mathbb{N} \mid \gcd(a,n) = 1 \}$$

$$\phi(n) = |U(n)| \quad \forall n \in \mathbb{N}$$

$\phi(12) = 4.$ $\quad\left[\because U(12) = \{1, 5, 7, 11\}\right]$

$\phi(30) = 8$ $\quad\left[\because U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}\right]$

If $n = p_1^{r_1} p_2^{r_2} p_3^{r_3} \cdots p_k^{r_k}$

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$30 = 2 \times 3 \times 5$

$$\phi(30) = 30\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 8$$

$12 = 2^2 \times 3$

$$\phi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$$

$$\phi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) \qquad \left[\because 100 = 2^2 \times 5^2\right]$$

$= 40.$

Thm If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$

Proof: $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} = \langle 1 \rangle$

$|\mathbb{Z}_6| = 6$, 2 is a positive divisor of 6.

no. of elements of order 2 $\quad \phi(2)$

of 6.

no. of elements of order 2 $= \phi(2)$
$= 1$

the only element of order $2 = 3$,

$|0| = 1$, $|1| = 6$, $|2| = 3$, $|3| = 2$, $|4| = 3$, $|5| = 6$.

Proof: Let $G = \langle a \rangle$ be a cyclic group of order n.

d is a positive divisor of n,

from fundamental theorem of cyclic group, there is exactly one subgroup of order d. say it $\langle b \rangle$.

Every element of order d also generates the subgroup $\langle b \rangle$.

$G = \langle a \rangle$
$|G| = |a|$.

Now, an element b^k generates $\langle b \rangle$, if and only if $\gcd(k, d) = 1$.

$\langle b \rangle = \{e, b, b^2, \dots b^{d-1}\}$
$\langle c \rangle = \{e, c, c^2, \dots c^{d-1}\}$

The number of such elements is exactly $\phi(d)$.

$G = \langle a \rangle$, $|G| = n$.
$G = \langle a^k \rangle$ iff $\gcd(a, n) = 1$

Subgroup Lattice

Example.

$\mathbb{Z}_{30} = \{0, 1, 2, \ldots, 28, 29\}$

divisors of 30 are 1, 2, 3, 5, 6, 10, 15, 30

Subgroups are $\langle 30/30 \rangle, \langle 30/15 \rangle, \langle 30/10 \rangle, \langle 30/6 \rangle, \langle 30/5 \rangle, \langle 30/3 \rangle, \langle 30/2 \rangle, \langle 30/1 \rangle$

$= \langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 5 \rangle, \langle 6 \rangle, \langle 10 \rangle, \langle 15 \rangle, \langle 0 \rangle.$

subgroups of $\mathbb{Z}_n$ are $\langle n/k \rangle$ for each positive divisor k of n

we can easily see that

$\langle 6 \rangle \subseteq \langle 2 \rangle$

$\langle 6 \rangle \subseteq \langle 3 \rangle$

$\langle 10 \rangle \subseteq \langle 5 \rangle$

$\langle 15 \rangle \subseteq \langle 5 \rangle$

$\langle 2 \rangle = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 0\}$

$\langle 6 \rangle = \{6, 12, 18, 24, 0\}$

$\langle 6 \rangle \subseteq \langle 2 \rangle.$

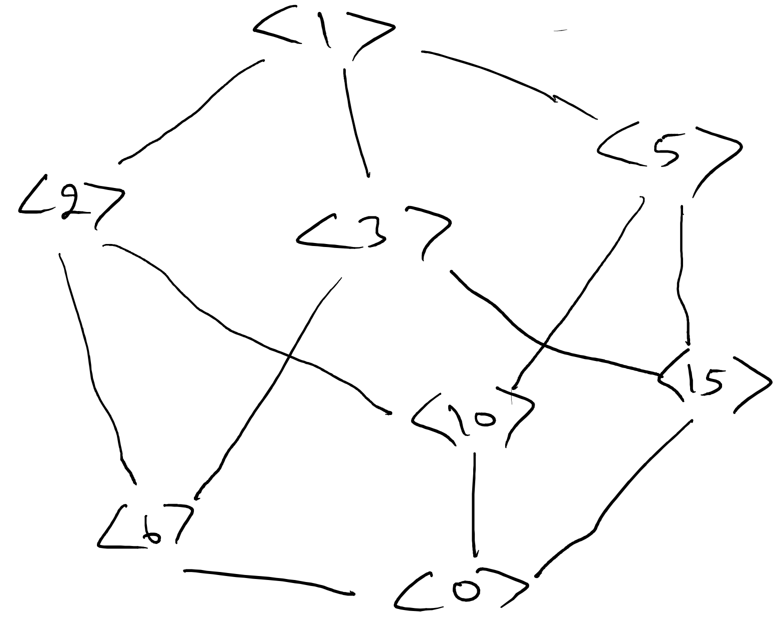
$\langle 6 \rangle$ is a subgroup of $\langle 2 \rangle$.

Subgroup Lattice:

Subgroup lattice is a diagram that includes all the subgroups of the group and connects a subgroup H at one level to a subgroup K at a higher level with a sequence of line segments iff H is a proper subgroup of K.

Note: Subgroup Lattice is not unique. There are many ways to draw subgroup Lattice, but the connections between the subgroups must be the same.

Subgroup Lattice for $\mathbb{Z}_{30}$ is as follows:



$\mathbb{Z}_{30} = \langle 1 \rangle$

$\langle 2 \rangle$

$\langle 3 \rangle$

$\langle 5 \rangle$

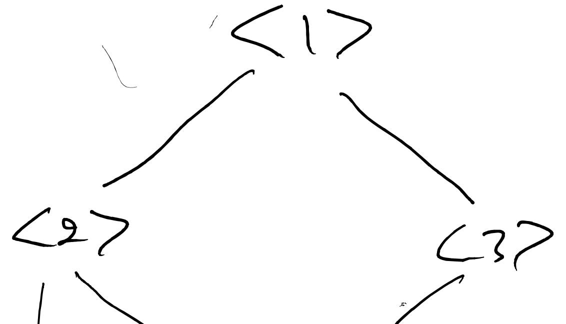
$\langle 6 \rangle$

$\langle 10 \rangle$

$\langle 0 \rangle$, $\langle 15 \rangle$

$\langle 3 \rangle \subseteq \langle 2 \rangle$ / No

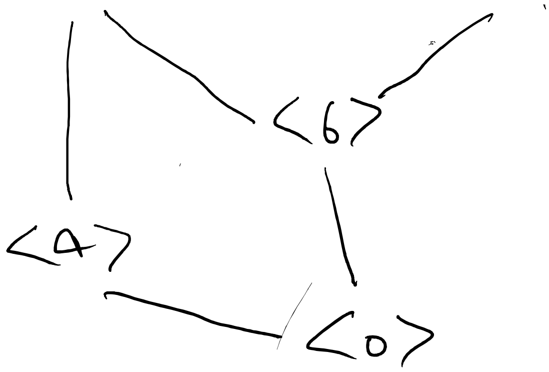
Subgroup Lattice for $\mathbb{Z}_{12}$



Subgroups are

$\langle 1 \rangle$, $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 4 \rangle$, $\langle 6 \rangle$, $\langle 0 \rangle$

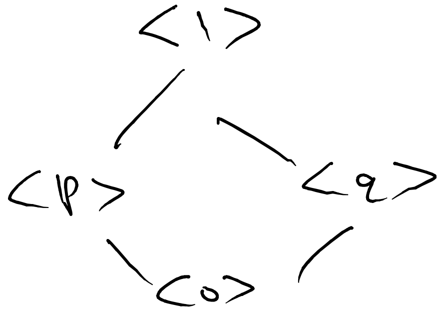
Note:



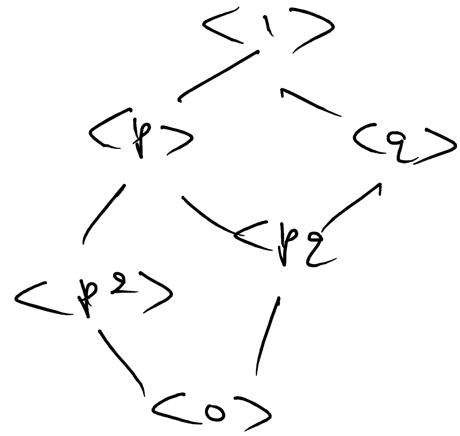
Note:
H is connected with K if K is just higher subgroup from H.

Q. Find subgroup lattice for $\mathbb{Z}_{pq}$ & $\mathbb{Z}_{p^2q}$, where p & q are distinct primes.

Soln



subgroup lattice for $\mathbb{Z}_{pq}$



Subgroups lattice for $\mathbb{Z}_{p^2q}$

$(12 = 2^2 \times 3)$

Q. Draw subgroup lattice for $\mathbb{Z}_{p^n}$, where p is prime & $n \geq 1$.

also draw subgroup lattice for $\mathbb{Z}_8$

Soln// Subgroups of $\mathbb{Z}_8$ are, $\langle 1\rangle, \langle 2\rangle, \langle 4\rangle, \langle 0\rangle$.

$$\begin{array}{c} \langle 1\rangle \\ | \\ \langle 2\rangle \\ | \\ \langle 4\rangle \\ | \\ \langle 0\rangle \end{array}$$

Subgroup lattice for $\mathbb{Z}_8$

Subgroup of $\mathbb{Z}_{p^n}$ are

$\langle 1\rangle, \langle p\rangle, \langle p^2\rangle, \langle p^3\rangle, \langle p^4\rangle, \ldots, \langle p^{n-1}\rangle, \langle 0\rangle$.

$$\begin{array}{c} \langle 1\rangle \\ | \\ \langle p\rangle \\ | \\ \langle p^2\rangle \\ \vdots \\ \langle p^{n-1}\rangle \\ | \\ \langle 0\rangle \end{array}$$

Subgroup lattice for $\mathbb{Z}_{p^n}$.

Q. List all the elements of $\mathbb{Z}_{40}$ that have order 10.

Soln// $\mathbb{Z}_{40}$ is a cyclic group.

if d is divisor of n, then no. of element of order d in a cyclic group of order n is $\phi(d)$.

$\therefore$ no. of elements of order 10 $= \phi(10) = 4$

Clearly, $|4| = 10$.

then $|4^k| = |4|$ iff $\gcd(k,10) = 1$.

$\therefore$ the elements of order 10 are $4^1, 4^3, 4^7, 4^9$

i.e. $4, 12, 28, 36$.

Q. List all the elements of order 8 in $\mathbb{Z}_{8000000}$.

How do you know your list is

Complete?

Sol// no. of elements of order $8 = \phi(8) = 4$,

clearly 1000000 is the element of order 8.

$|1000000| = |\langle(1000000)^k\rangle|$ iff $\gcd(k,8) = 1$

elements of order 8 are $(1000000)^1, (1000000)^3,$

$(1000000)^5, (1000000)^7$.

$\because$ 8 divides 8000000

$\therefore$ the elements of order 8 in $\mathbb{Z}_{8000000}$

are exactly $\phi(8) = 4$.

we have already found 4 elements of order 8.

$\therefore$ the list is complete.

Cayley table for groups:

$G = \{1, -1, i, -i\}$, operation — multiplication

	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

In general, if $G = \{e, a, b\}$

	e	a	b
e	e	a	b
a	a	a^2	ab
b	b	ba	b^2

Q. Let G be a group and $|G| = n$.

if k is a positive divisor of n,

then how many subgroups of order k.

Sol^n Exactly one. (It's not true)

we can't say anything about the number.

Q. Prove that if $(ab)^2 = a^2b^2$ in a group G, $\forall a,b \in G$, then show that G is abelian.

Sol^n $ab = ba \ \forall a,b \in G$.

$$(ab)^2 = a^2b^2$$

$$\Rightarrow abab = aabb$$

$$\Rightarrow a^{-1}(abab)b^{-1} = a^{-1}(aabb)b^{-1}$$

$$= (a^{-1}a)(ba)(bb^{-1}) = (a^{-1}a)(ab)(bb^{-1})$$

$$= (e)(ba)(e) = (e)(ab)(e)$$

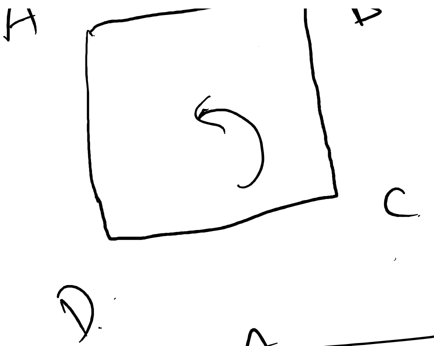
$$\Rightarrow ba = ab \Rightarrow ab = ba \ \forall a,b \in G$$

$\Rightarrow G$ is abelian.

Symmetries of a Square:

Rotate 0°

Rotate 90°



Rotate 90°

Rotate by 180°

Rotate by 270°