Chapter 2: Cyclic Groups

Definition: Cyclic group

A group G is called cyclic if there is an element $a \in G$ such that $G = \{a^n | n \in Z\}$

Notation:A G is a cyclic group generated by a is denoted by $G =< a >$.

Example: $Z =< 1 >=< -1 >$, $Z_n =< 1 >=< n-1 >$, $Z_8 =< 1, 3, 5, 7 >$

Theorem: Let G be a group and $a \in G$. If a has infinite order, then $a^i = a^j$ if and only if $i = j$. If a has finite order say n, then $< a >= \{e, a, a^2, ..., a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i - j$.

Proof: If a has infinite order, then there does not exists a positive integer n such that $a^n = e$. As $a^i = a^j \Rightarrow a^{i-j} = e$ so $i - j = 0 \Rightarrow i = j$.

Now suppose $|a| = n$ to prove $< a >= \{e, a, a^2, ..., a^{n-1}\}$

since $a, a^2, ..., a^{n-1}, a^n = e \in< a >$

now suppose a^k is an element of G.

Apply division algorithm to k and n, there exists an integer q and r such that $k = qn + r$ with $0 \leq r < n$

$a^k = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = e^q a^r = a^r$

so $a^k \in< a >$ therefore $< a >= \{e, a, a^2, ..., a^{n-1}\}$

now suppose $a^i = a^j$ to prove that n divides $i - j$.

As $a^i = a^j$ so $a^{i-j} = e$.

Apply division algorithm to $i - j$ and k there exists q and r such that $i - j = qn + r$ with $0 \leq r < n$

then $a^{i-j} = a^{qn+r} = (a^n)^q a^r = e^q a^r = ea^r = a^r$

Since $a^{i-j} = e \Rightarrow a^r = e$ but n is the least positive integer such that $a^n = e$

so $r = 0 \Rightarrow n$ divides $i - j$

Conversely suppose n divides $i - j$ so $i - j = nq$,

then $a^{i-j} = a^{nq} = (a^n)^q = e^q = e$ so thet $a^i = a^j$.

Corollary: For any element $a \in G$, $|a| =< a >$

Proof: Since if $|a| = n$ then $< a >= \{e, a, a^2, ..., a^{n-1}\}$

So $| < a > | = n = |a|$

Corollary: Let G be a group and let $a \in G$ such that $|a| = n$. If $a^k = e$, then n divides k.

Proof: Since $a^k = e = a^0$ so $a^k = a^0$ so n divides $k - 0$ that is k.

Theorem: Let a be an element of order n in a group and let k be a positive integer.

Then $< a^k >=< a^{gcd(n,k)} >$ and $|a^k| = n/gcd(n, k)$

Proof: Let G be a group and $a \in G$ such that $|a| = n$ let $d = gcd(n, k)$ and let $k = dr$

Since $a^k = (a^d)^r$ so $< a^k >\subset< a^d >$

as $d = gcd(n, k)$ so there exists s and t such that $d = ns + kt$

So $a^d = a^{ns+kt} = a^{ns}a^{kt} = (a^n)^s(a^k)^t = e(a^k)^t \in< a^k >$

$< a^d >\subset< a^k >$

Therefore $< a^k >=< a^{gcd(n,k)} >$

Since $|a| = n$, first to prove that $|a^d| = n/d$ for any divisor d of n

Consider $(a^d)^{n/d} = a^n = e$

So $|a^d| \leq n/d$ Suppose i be a positive integer less than n/d such that $(a^d)^i = e$

but as $i \leq n/d \Rightarrow di < n \Rightarrow a^{di} = e$ which is not posssible as n is the order of a so n should be smallest.

Therefore $|a^d| = n/d$ for any divisor d of n.

Since $< a^k >=< a^{gcd(n,k)} >\Rightarrow | < a^k > | = | < a^{gcd(n,k)} > | = |a^{gcd(n,k)}| = n/gcd(n, k)$

Corollary: In a finite cyclic group, the order of an element divides the order of the group.

Proof: Let G be a finite cyclic group such that $G =< a >$ and $|G| = n$

Since any element in G is of the form a^k so $|a^k| = n/gcd(n, k)$

Since $gcd(n, k)$ divides n so $n/gcd(n, k)$ is a divisor of n

S o order of any element in G divides the order of G.

Corollary: Let $|a| = n$. Then $< a^i >=< a^j >$ if and only if $gcd(n, i) = gcd(n, j)$ and $|a^i| = |a^j|$ if and only if $gcd(n, i) = gcd(n, j)$
Proof: Suppose $|a| = n$ and $< a^i >=< a^j >$
since $< a^i >=< a^{gcd(n,i)} >$ and $< a^j >=< a^{gcd(n,j)} >$
So we have $< a^{gcd(n,i)} >=< a^{gcd(n,j)} >\Rightarrow |a^{gcd(n,i)}| = |a^{gcd(n,j)}|$
Since $|a^{gcd(n,i)}| = n/gcd(n, i)$ and $|a^{gcd(n,j)}| = n/gcd(n, j)$
$n/gcd(n, i) = n/gcd(n, j) \Rightarrow gcd(n, j) = gcd(n, i)$
Conversely Suppose $gcd(n, j) = gcd(n, i) \Rightarrow< a^{gcd(n,i)} >=< a^{gcd(n,j)} >\Rightarrow< a^i >=< a^j >$
Similarly $|a^i| = |a^j|$ if and only if $gcd(n, i) = gcd(n, j)$

Corollary: Let $|a| = n$. Then $< a >=< a^j >$ if and only if $gcd(n, j) = 1$ and $|a| = | < a^j > |$ if and only if $gcd(n, j) = 1$.
Proof: Let $|a| = n$ and $< a >=< a^j >\Leftrightarrow< a^1 >=< a^j >\Leftrightarrow gcd(n, 1) = gcd(n, j) \Leftrightarrow 1 = gcd(n, j)$
Similarly $|a| = | < a^j > |$ if and only if $gcd(n, j) = 1$.

Fundamental theorem of cyclic groups:
Every subgroup of a cyclic group is cyclic. Moreover if $| < a > | = n$, then the order of any subgroup of $< a >$ is a divisor of n; and for each positive divisor k of n, the group $< a >$ has exactly one subgroup of order k namely $< a^{n/k} >$
Proof: Let G be a cyclic group such that $G =< a >$
Suppose H be a subgroup of G.
To prove H is cyclic. If $H = \{e\}$ then H is cyclic.
Suppose $H \neq \{e\}$. First we have to show that $a^t \in H$ for a positive integer t.
Since $G =< a >$ and H is a subset of G so elements of H is of the form a^t
If $t < 0$ then and H is a subgroup so $a^{-t} \in H$ so $-t > 0$ therefore $a^t \in H$ for a positive integer t.
Now let m be the least positive integer such that $a^m \in H$ so $< a^m >\subset H$
To prove $H =< a^m >$. Let $b \in H$ and $H \subset G$ so $b \in G$, we can write $b = a^k$ for some k.
Now apply division algorithm to k and m we get get an inetgers q and r such that
$k = mq + r$ where $0 \leq r < m$.
Then $a^k = a^{mq+r} = a^{mq}a^r \Rightarrow a^r = a^{-mq}a^k$
Since $a^k = b \in H$ and $a^{-mq} = (a^m)^{-q}$ is in H so $a^r \in H$.
But m is the least positive integer such that $a^m \in H$ and $r < m$
So $r = 0$ therefore $b = a^k = a^{mq} = (a^m)^q \in< a^m >$ so $H \subset< a^m >$
Therefore $H =< a^m >$ so H is cyclic.
Now suppose $| < a > | = n$ and H is any subgroup of $< a >$. Since $H =< a^m >$, where m is least positive integer such that $a^m \in H$. As $|H| = | < a^m > | = |a^m| = m/gcd(n, m)$ so $m/gcd(n, m)$ divides n so order of H divides order of group.
Since $a^n = e$ and $e \in H$ so $a^n \in H$ as a^k is in H so $k = mq$ so here $n = mq$.
Let k be a positive divisor of n. To show that $< a^{n/k} >$ is the one and only one subgroup of order k.
$| < a^{n/k} > | = |a^{n/k}| = n/gcd(n, n/k) = n/n/k = k$ So order of $< a^{n/k} >$ is k.
Now to prove uniqueness. Suppose H is another subgroup of $< a >$ of order k.
Since $H =< a^m >$, where m is a divisor of n.
So $gcd(n, m) = m$ and $|H| = | < a^m > | = |a^m| = k$ and $k = |a^m| = |a^{gcd(n,m)}| = n/gcd(n, m) = n/m$.
So $k = n/m \Rightarrow m = n/k$ so $H =< a^{n/k} >$.

Corollary: For each positive divisor k of n, the set $< n/k >$ is the unique subgroup of Z_n of order k. Moreover these are the only subgroups of Z_n.
Proof: Since the group Z_n is cyclic with $Z_n =< 1 >$.
And Z_n is additive group so for every divisor k of n we have a unique subgroup of order k namely $< n/k.1 >=< n/k >$

Theorem: If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(n)$.
Proof: Let G be a cyclic group such that $G =< a >$.
As d is a divisor so G has exaclty one subgroup of order d say H.
.Then every element of order d also generates the subgroup H.
An element a^k generates H if and only if $gcd(k, d) = 1$.
Number of such elements are $\phi(d)$.

Theorem: In a finite group, the number of elements of order d is dividsible by $\phi(d)$.
Proof: Let G be a finite group.
If G has no elements of order d then statement is true, since $\phi(d)$ divides 0.
Suppose $a \in G$ such that $|a| = d$. Since $< a >$ has $\phi(d)$ elements of order d.
If all elements of order d in G are in $< a >$ then done.
Suppose there is an element $b \in G$ of order d which is not in $< a >$
then $< b >$ also has $\phi(d)$ elements of order d so we have $2\phi(d)$ elements of order d in G provided that $< a >$ and $< b >$ have no elements of order d in common. If there is an element c of order d that is both $< a >$ and $< b >$, then we have $< a >=< c >=< b >$ so $b \in< a >$, which is contadiction.
Continuing in this way we see that number of elements of order d in a finite group is a multiple of $\phi(d)$.