Lecture 7

Now that we have seen that all subgroups of cyclic groups are cyclic, we want to understand cyclic groups in more depth and would try to classify the subgroups of cyclic groups.
First an important theorem.

Theorem [Criterion for $a^i = a^j$]
Let G be a group and $a \in G$. If $\operatorname{ord}(a) = \infty$ then $a^i = a^j$ if and only if $i = j$. If $\operatorname{ord}(a) < \infty$, say n, then

$$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$$

and $a^i = a^j$ if and only if n divides $i-j$.

Proof If $\operatorname{ord}(a) = \infty \Rightarrow \nexists$ any non-zero n such that $a^n = e$. Now $a^i = a^j \Rightarrow a^{i-j} = e$ and so $i-j=0$.

Now assume $\operatorname{ord}(a) = n$. We want to prove that $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$.
Clearly all the elements are in $\langle a \rangle$, so we want to prove that there are no more elements.
Let $a^k \in \langle a \rangle$. By the division algorithm

$$k = \alpha n + r \quad , \quad 0 \leq r < n$$

Then $a^k = a^{\alpha n + r} = (a^n)^\alpha . a^r = e a^r$ and $r < n$
so a^k is one of the elements in $\{e, a, \dots, a^{n-1}\}$.

Now, suppose $a^i = a^j \Rightarrow a^{i-j} = e$. Again by division algorithm

$$i-j = qn + r \quad , \quad 0 \le r < n$$

$$\Rightarrow \quad a^{i-j} = a^{qn+r} = (a^n)^q \cdot a^r = a^r$$

$$\Rightarrow \quad a^r = e$$

but by the definition of ord(a), n is the least positive integer such that $a^n = e$

$$\Rightarrow \quad r = 0$$

$$\Rightarrow \quad n \mid i-j.$$

Conversely, if $n \mid i-j \Rightarrow i-j = \alpha n \Rightarrow$

$$a^{i-j} = a^{\alpha n} = (a^n)^\alpha = e \Rightarrow a^i = a^j.$$

$\blacksquare$

We have the following corollary of the above theorem

Corollary Let G be a group and $a \in G$ with $\text{ord}(a) = n$. If $a^k = e \Rightarrow n$ divides k.

Remark Many student make the mistake by saying that if $a^k = e \Rightarrow \text{ord}(a) = k$. This is wrong! All we can say is that $\text{ord}(a) \mid k$.

Now suppose we have a cyclic group $G = \langle a \rangle$. Then we know that all it's subgroups are cyclic.

We also know that since $a^k \in G$ $\Rightarrow$ $\langle a^k \rangle$ is a subgroup of G.

What is the order of the group $\langle a^k \rangle$?

The next theorem gives a simple method to compute $|\langle a^k \rangle|$. Moreover, it has many important corollaries.

Theorem Let G be a group, $a \in G$ and $\text{ord}(a) = n$. Let k be any positive integer. Then

$$\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$$

and

$$\text{ord}(a^k) = |\langle a^k \rangle| = \frac{n}{\gcd(n,k)}$$

Proof Suppose $d = \gcd(n,k)$ and $k = dr$.

We first prove that $\langle a^k \rangle = \langle a^d \rangle$.

Since $a^k = a^{dr} = (a^d)^r \Rightarrow \langle a^k \rangle \subseteq \langle a^d \rangle$.

So we want to prove that $\langle a^d \rangle \subseteq \langle a^k \rangle$

Enough to prove that $a^d \in \langle a^k \rangle$.

Recall from MATH 135 that if $d = \gcd(n,k) \Rightarrow \exists\ s, t \in \mathbb{Z}$ such that

$$d = ns + kt$$

So $a^d = a^{ns+kt} = (a^n)^s \cdot (a^k)^t = (a^k)^t \in \langle a^k \rangle$

Hence proved.

We now want to prove that $ord(a^k) = \frac{n}{d}$.

i.e., $\frac{n}{d}$ is the smallest positive integer with $(a^k)^{\frac{n}{d}} = e$. It's same as proving that $ord(a^d) = \frac{n}{d}$. If $\exists\ \alpha < \frac{n}{d}$ such that $(a^d)^\alpha = e \Rightarrow (a^{d\alpha}) = e$. But $d\alpha < \frac{n}{d} \cdot d = n$ which contradicts that $ord(a) = n$.

$$\Rightarrow$$

$$ord(a^k) = |\langle a^k \rangle| = ord(a^{gcd(n,k)}) = \frac{n}{gcd(n,k)}$$

$\boxed{\text{///}}$

Before stating and proving the corollaries, let's see why this theorem is important.

Suppose $G = \langle a \rangle$ with $\operatorname{ord}(a) = 30$. Then we know immediately that $\langle a^{26} \rangle = \langle a^2 \rangle$ (as $\gcd(30, 26) = 2$) or that $\langle a^{23} \rangle = \langle a \rangle$.
It's much easier to write the elements of $\langle a^2 \rangle$ than $\langle a^{26} \rangle$ and these are the same subgroups.

Corollary 1 In a finite cyclic group, the order of an element divides the order of the group.
Since every subgroup is cyclic $\Rightarrow$ generated by an element of the group, so

In a finite cyclic group, the order of a subgroup divides the order of the group. $\boxed{\text{I}}$

Remark As we will see that the last statement is true for every finite groups. That is called the Lagrange's Theorem.

Corollary 2 Generators of a finite cyclic group.

Let G be a cyclic group with $G = \langle a \rangle$ and $\operatorname{ord}(a) = |G| = n$.
Then $\langle a \rangle = \langle a^j \rangle \iff \gcd(n, j) = 1$ and so all such a^j are generators of G.

Proof We want $\langle a^j \rangle = \langle a \rangle$. But $\langle a^j \rangle = \langle a^{\gcd(n,j)} \rangle$.

$\boxed{\text{II}}$

Corollary 2 is telling us all the generators of a cyclic group.

e.g. One can check that $U(50)$ is a cyclic group with $|U(50)| = 20$. Suppose we know that 3 is a generator.

now $\{k \mid \gcd(k,20)=1\} = \{1,3,7,9,11,13,17,19\} = A$

So all the generators of $U(50)$ are $3^i \bmod 50$ where $i \in A$.

Corollary 3 Generators of $\mathbb{Z}_n$

An integer k in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ $\iff$ $\gcd(n,k)=1$.

Proof:- Since $\mathbb{Z}_n$ is a cyclic group of order n, the corollary follows. $\square$

In the next lecture, using these theorems and corollaries, we will classify all the subgroups of a cyclic group !!! which is a pretty powerful and amazing result.

o———x———x———o