Math 403 Chapter 4: Cyclic Groups

1. **Introduction:** The simplest type of group (where the word “type” doesn’t have a clear meaning just yet) is a cyclic group.

2. **Definition:** A group $G$ is cyclic if there is some $g \in G$ with $G = \langle g \rangle$. Here $g$ is a generator of the group $G$. Recall that $\langle g \rangle$ means all “powers” of $g$ which can mean addition if that’s the operation.

   (a) **Example:** $\mathbb{Z}_6$ is cyclic with generator 1. Are there other generators?
   (b) **Example:** $\mathbb{Z}_n$ is cyclic with generator 1.
   (c) **Example:** $\mathbb{Z}$ is cyclic with generator 1.
   (d) **Example:** $\mathbb{R}^*$ is not cyclic.
   (e) **Example:** $U(10)$ is cyclic with generator 3.

3. **Important Note:** Given any group $G$ at all and any $g \in G$ we know that $\langle g \rangle$ is a cyclic subgroup of $G$ and hence any statements about cyclic groups applies to any $\langle g \rangle$.

4. **Properties Related to Cyclic Groups Part 1:**

   (a) **Intuition:** If $|g| = 10$ then $\langle g \rangle = \{1, g, g^2, \ldots, g^9\}$ and the elements cycle back again. For example we have $g^2 = g^{12}$ and in general $g^i = g^j$ iff $10 \mid (i - j)$.

   (b) **Theorem:** Let $G$ be a group and $g \in G$.
   
   - If $|g| = \infty$ then $g^i = g^j$ iff $i = j$.
   - if $|g| = n$ then $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ and $g^i = g^j$ iff $n \mid (i - j)$.

   **Proof:** If $|g| = \infty$ then by definition we never have $g^i = e$ unless $i = 0$. Thus $g^i = g^j$ iff $g^{i-j} = e$ iff $i - j = 0$.

   If $|g| = n < \infty$ first note that $\langle g \rangle$ certainly includes $\{1, g, g^2, \ldots, g^{n-1}\}$. Suppose $g^k \in \langle g \rangle$. Write $k = qn + r$ with $0 \leq r < n$ and then $g^k = (g^n)^q g^r = e^q g^r = g^r$ so $g^k$ is one of those elements.

   Now for the iff. If $g^i = g^j$ then $g^{i-j} = e$. Write $i - j = qn + r$ with $0 \leq r < n$. Then $e = g^{qn} g^r = g^r$. Since $n$ (the order) is the least positive but $r < n$ we must have $r = 0$ and so $n \mid (i - j)$.

   If $n \mid (i - j)$ then $i - j = qn$ and then $g^i = g^j g^{qn} = g^j$. $\Box$

   (c) **Corollary:** For any $g \in G$ we have $|g| = |\langle g \rangle|$.

   **Proof:** Follows directly. $\Box$

   (d) **Corollary:** For any $g \in G$ with $|g| = n$, $g^i = e$ iff $n \mid i$.

   **Proof:** This is the theorem with $j = 0$. $\Box$

   **Example:** If $|g| = 10$ then if $g^i = e$ then $10 \mid i$, meaning we only get $e$ when the powers are multiples of 10.
5. Properties Related to Cyclic Groups Part 2:

(a) Intuition: If $|g| = 30$ then if we examine something like $\langle g^{24} \rangle$ we find:

\[
\begin{align*}
g^{24} &= g^{24} \\
(g^{24})^2 &= g^{48} = g^{18} \\
(g^{24})^3 &= g^{72} = g^{12} \\
(g^{24})^4 &= g^{96} = g^6 \\
(g^{24})^5 &= g^{120} = g^0 = e
\end{align*}
\]

We then see that $\langle g^{24} \rangle = \{e, g^6, g^{12}, g^{18}, g^{24}\} = \langle g^6 \rangle$. which is a bit nicer since the 6 is easier to work with. Note that $6 = \gcd(30, 24)$.

Likewise we can easily compute the order of $g^{24}$. We see it cycles every 5, just like $g^6$, and $5 = 30/\gcd(30, 24)$.

(b) Theorem: Let $g \in G$ with $|g| = n$ and let $k \in \mathbb{Z}^+$ then

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

(ii) $|g^k| = |g^{\gcd(n,k)}|$

(iii) $|g^k| = n/\gcd(n, k)$

Proof: For (i) since $\gcd(n, k) \mid k$ we know that $\alpha \gcd(n, k) = k$ and so

\[
g^k = \left(g^{\gcd(n,k)}\right)^\alpha \in \langle g^{\gcd(n,k)} \rangle
\]

and so:

$\langle g^k \rangle \subseteq \langle g^{\gcd(n,k)} \rangle$

Then write $\gcd(n, k) = \alpha n + \beta k$ and observe that

\[
g^{\gcd(n,k)} = (g^n)^\alpha + (g^k)^\beta = (g^k)^\beta \in \langle g^k \rangle
\]

so that

$\langle g^{\gcd(n,k)} \rangle \subseteq \langle g^k \rangle$

Thus the two are equal.

Then (ii) follows immediately from the previous theorem.

For (iii) first observe that

\[
(g^{\gcd(n,k)})^{n/\gcd(n,k)} = g^n = e
\]

so that:

\[
|g^{\gcd(n,k)}| \leq \frac{n}{\gcd(n, k)}
\]

On the other hand if we had $|g^{\gcd(n,k)}| = b < n/\gcd(n, k)$ then we have $e = (g^{\gcd(n,k)})^b = g^{b\gcd(n,k)}$ with $b\gcd(n, k) < n$, contradicting $|g| = n$. Thus we have:

\[
|g^{\gcd(n,k)}| = \frac{n}{\gcd(n, k)}
\]

Thus we have:

\[
|g^k| = |g^{\gcd(n,k)}| = \frac{n}{\gcd(n, k)}
\]

QED
(c) **Corollary:** In a finite cyclic group the order of an element divides the order of a group.

**Proof:** Follows since every element looks like \( g^k \) and we have \( |g^k| \mid \text{gcd} (n, k) = n \). \( \square \)

**Example:** In a cyclic group of order 200 the order of every element must divide 200. In such a group an element could not have order 17, for example.

(d) **Corollary:** Suppose \( g \in G \) and \( |g| = n < \infty \). Then:

\[ \langle a^i \rangle = \langle a^j \rangle \text{ iff } \text{gcd} (n, i) = \text{gcd} (n, j) \text{ iff } |a^i| = |a^j| \]

**Proof:** Follows immediately. \( \square \)

**Example:** If \( |g| = 18 \) then the fact that \( \text{gcd} (18, 12) = 6 = \text{gcd} (18, 6) \) guarantees that \( |g^{12}| = |g^6| \).

(e) **Corollary:** Suppose \( g \in G \) and \( |g| = n < \infty \). Then:

\[ \langle a \rangle = \langle a^i \rangle \text{ iff } \text{gcd} (n, j) = 1 \text{ iff } |a| = |a^j| \]

**Proof:** Follows immediately. \( \square \)

**Example:** If \( |g| = 32 \) then the fact that \( \text{gcd} (15, 32) = 1 \) guarantees that \( \langle g^{15} \rangle = \langle g \rangle \), meaning \( g^{15} \) is a generator of \( \langle g \rangle \).

(f) **Corollary:** An integer \( k \in \mathbb{Z}_n \) is a generator of \( \mathbb{Z}_n \) iff \( \text{gcd} (n, k) = 1 \).

**Proof:** Follows immediately. \( \square \)

**Example:** The generators of \( \mathbb{Z}_{10} \) are 1, 3, 7, 9.
6. Classification of Subgroups of Cyclic Groups:

(a) **Theorem (Fundamental Theorem of Cyclic Groups):**
Suppose \( G = \langle g \rangle \) is cyclic.

(i) Every subgroup of \( G \) is cyclic.

(ii) If \( |G| = n \) then the order of any subgroup of \( G \) divides \( n \).

(iii) If \( |G| = n \) then for any \( k \mid n \) there is exactly one subgroup of order \( k \) and if \( g \) generates \( G \) then \( g^{n/k} \) generates that subgroup.

**Proof:**

(i) Let \( H \leq G \). If \( H = \{e\} \) then we’re done so assume \( H \neq \{e\} \). Choose \( g^n \in H \) with minimal \( m \in \mathbb{Z}^+ \) by well-ordering. Clearly \( \langle g^m \rangle \subseteq H \). If some \( g^k \in H \) then put \( k =qm+r \) with \( 0 \leq r < m \) so \( r = k - qm \) and then \( g^r = g^k (g^m)^{-q} \in H \) and so \( r = 0 \) by minimality of \( m \) and so \( g^k = (g^m)^t \) and hence \( g^k \in \langle g^m \rangle \).

(ii) Take a subgroup \( H \leq G \). We know \( H \) is cyclic by (i) with \( H = \langle g^m \rangle \) with minimal \( m \in \mathbb{Z}^+ \) by well-ordering. Write \( n = qm + r \) with \( 0 \leq r < m \) so \( r = n - qm \) and then \( g^r = g^n (g^m)^{-q} \in H \) and so \( r = 0 \) by minimality of \( m \) and so \( n = qm \) and then

\[
|H| = |\langle g^m \rangle| = |g^m| = \frac{n}{\gcd(n,m)} = \frac{n}{m}
\]

and so \( m|H| = n \) and so \( |H| \mid n \).

(iii) Observe first that for any \( k \mid n \) we have

\[
\left| \langle g^{n/k} \rangle \right| = |g^{n/k}| = \frac{n}{\gcd(n,n/k)} = \frac{n}{n/k} = k
\]

Thus certainly \( \langle g^{n/k} \rangle \) is a subgroup of order \( k \). We must show that it is unique.

Let \( H \leq G \) with \( |H| = k \mid n \). Since \( H \leq G \) by (ii) we have \( H = \langle g^m \rangle \) with \( m \mid n \).

Then we have:

\[
k = |H| = |\langle g^m \rangle| = |g^m| = \frac{n}{\gcd(n,m)} = \frac{n}{m}
\]

Thus \( m = n/k \) and so \( H = \langle g^m \rangle = \langle g^{n/k} \rangle \).

**QED**

**Example:** This categorizes cyclic groups completely. For example suppose a cyclic group has order 20. Every subgroup is cyclic and there are unique subgroups of each order 1, 2, 4, 5, 10, 20. If \( G \) has generator \( g \) then generators of these subgroups can be chosen to be \( g^{20/1} = g^{20}, g^{20/2} = g^{10}, g^{20/4} = g^5, g^{20/5} = g^4, g^{20/10} = g^2, g^{20/20} = g \) respectively.

(b) **Corollary:** For each positive divisor \( k \) of \( n \in \mathbb{Z}^+ \), the set \( \langle n/k \rangle \) is the unique subgroup of \( \mathbb{Z}_n \) of order \( k \). Moreover these are the only subgroups of \( \mathbb{Z}_k \).

**Proof:** Follows immediately. **QED**

**Example:** In \( \mathbb{Z}_{10} = \langle 1 \rangle \) the subgroup \( \langle 1 \rangle \) is the unique subgroup of order 10/1 = 10, the subgroup \( \langle 2 \rangle \) is the unique subgroup of order 10/2 = 5, the subgroup \( \langle 5 \rangle \) is the unique subgroup of order 10/1 = 2, the subgroup \( \langle 10 \rangle = \langle 0 \rangle \) is the unique subgroup of order 10/10 = 1.

(c) **Definition:** Define \( \phi(1) = 1 \) and for any \( n \in \mathbb{Z} \) with \( n > 1 \) define \( \phi(n) \) to be the number of positive integers less than \( n \) and coprime to \( n \).

**Example:** We have \( \phi(20) = 8 \) since 1, 3, 7, 9, 11, 13, 17, 19 are coprime.
(d) **Theorem:** Suppose $G$ is cyclic of order $n$. If $d \mid n$ then there are $\phi(d)$ elements of order $d$ in $G$.

**Proof:** Every element of order $d$ generates a cyclic subgroup of order $d$ but there is only one such cyclic subgroup, thus every element of order $d$ is in that single cyclic subgroup of order $d$. If that cyclic subgroup is $\langle g \rangle$ with $|g| = d$ then note that the only elements of order $d$ in it are those $g^k$ with gcd $(d, k) = 1$ and there are $\phi(d)$ of those.

**Example:** In a cyclic group of order 100 noting that $20 \mid 100$ we then know there are $\phi(20) = 8$ elements of order 20.

(e) **Theorem:** If $G$ is a finite group then the number of elements of order $d$ is a multiple of $\phi(d)$.

**Outline of Proof:** Elements of order $d$ can be collected $\phi(d)$ at a time into subgroups of order $d$.

**Example:** If $G$ is an arbitrary finite group then the number of elements of order 20 is a multiple of 8. Keep in mind that this might be zero!