CYCLIC GROUPS

1. Definition

Recall that if G is a group and S is a subset of G then the notation

$$\langle S \rangle$$

signifies the subgroup of G *generated* by S, the smallest subgroup of G that contains S.

A group is *cyclic* if it is generated by one element, i.e., if it takes the form

$$G = \langle a \rangle \quad \text{for some } a.$$

For example, $(\mathbb{Z}, +) = \langle 1 \rangle$. However, $\langle 2 \rangle = 2\mathbb{Z}$ is a proper subgroup of $\mathbb{Z}$, showing that not every element of a cyclic group need be a generator.

2. Characterization

Since Gallian discusses cyclic groups entirely in terms of themselves, I will discuss them using an idea that will be ubiquitous in this course, the idea of a *characterizing mapping property*.

Proposition 2.1 (Characterizing Mapping Property of Cyclic Groups)**.** *A group G is cyclic if and only if it is a homomorphic image of $\mathbb{Z}$.*

Proof. If $G = \langle a \rangle$ then the map

$$\mathbb{Z} \longrightarrow G, \quad n \longmapsto a^n$$

is a homomorphism (since $a^{n+m} = a^n a^m$ for all $n, m \in \mathbb{Z}$) whose image is G. Conversely, if $f : \mathbb{Z} \longrightarrow G$ is an epimorphism then let $a = f(1)$. Every $g \in G$ takes the form $g = f(n)$ for some $n \in \mathbb{Z}$. If $n \geq 0$ then

$$g = f(1 + \cdots + 1) = f(1) \circ_G \cdots \circ_G f(1) = (f(1))^n = a^n.$$

And the same formula holds if $n < 0$ (exercise). Thus $G = \langle a \rangle$. □

3. Consequences of the Characterization

Immediately from the proposition, any cyclic group is abelian and any homomorphic image of a cyclic group is again cyclic.

Also, we argue that any subgroup of a cyclic group is again cyclic. Indeed, let G be cyclic, so that there is an epimorphism

$$f : \mathbb{Z} \longrightarrow G,$$

and let $H \subset G$ be a nontrivial subgroup (the trivial subgroup is trivially cyclic: $\{e\} = \langle e \rangle$). Then $f^{-1}(H)$ is a nontrivial subgroup of $\mathbb{Z}$, and as such, it takes the form

$$f^{-1}(H) = n\mathbb{Z} \quad \text{for some positive integer } n.$$

(Specifically, let n be the the least positive element of $f^{-1}(H)$; then $f^{-1}(H)$ contains $n\mathbb{Z}$, and the division algorithm shows that it contains nothing more.) The multiply-by-n map on $\mathbb{Z}$,

$$[n] : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad k \longmapsto nk,$$

is a homomorphism whose image is $n\mathbb{Z}$, and so the composite

$$f \circ [n] : \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow G$$

is a homomorphism whose image is H. Thus H is cyclic.

4. Possible Cyclic Groups

If G is cyclic and $f : \mathbb{Z} \longrightarrow G$ is an epimorphism then $\ker(f)$ is a subgroup of $\mathbb{Z}$.

If $\ker(f) = \{0\}$ then f is an isomorphism, making G essentially a copy of $\mathbb{Z}$ via f,

$$n \longmapsto a^n \quad \text{where } a = f(1).$$

Also, $a^{-1} = f(-1)$ generates G, and $\{a, a^{-1}\}$ are the only two generators.

If $\ker(f) = n\mathbb{Z}$ where $n > 0$ then we have the set-relation

$$G = \{e, a, a^2, \cdots, a^{n-1}\} \quad \text{where } a = f(1).$$

That is, $a^n = e$ is the first positive power of a that is trivial, and in general the group law in G is

$$a^k = a^{k \bmod n}, \quad k \in \mathbb{Z}.$$

That is, the map

$$k \longmapsto a^k \quad \text{where } a = f(1)$$

now makes G a copy of $(\mathbb{Z}/n\mathbb{Z}, +)$.

5. Subgroups

Since any infinite cyclic group is a copy of $\mathbb{Z}$, its subgroups are copies of the subgroups of $\mathbb{Z}$,

$$H = \langle a^n \rangle \quad \text{for some positive integer } n.$$

And distinct positive integers n give distinct such subgroups.

Now consider a finite cyclic group G of order n, so that there exists an epimorphism

$$f : \mathbb{Z} \longrightarrow G, \quad \ker(f) = n\mathbb{Z}.$$

Let $a = f(1)$ as usual. Let H be a subgroup of G. Then $f^{-1}(H)$ is a supergroup of $\ker(f)$ in $\mathbb{Z}$, so that

$$f^{-1}(H) = d\mathbb{Z} \quad \text{where } 0 < d \mid n.$$

Thus the subgroup is

$$H = \langle a^d \rangle, \quad 0 < d \mid n,$$

and we see that the order of the subgroup divides the order of the group,

$$|H| = n/d.$$

On the other hand, for any $m \in \{0, 1, \cdots, n-1\}$, the mth power of a generates a subgroup $H = \langle a^m \rangle$ of G regardless of whether $m \mid n$. From the previous paragraph we know that also H takes the form $H = \langle a^d \rangle$ where $d \mid n$. Thus

$$a^m = a^{kd} \quad \text{for some } k,$$

so that (since $a^n = e$)

$$m = kd \bmod n \quad \text{for some } k,$$

showing that $d \mid m$ since $d \mid kd$ and $d \mid n$. Thus $d \mid \gcd(m, n)$. But also,

$$a^d = a^{km} \quad \text{for some } k,$$

so that

$$d = km \bmod n \quad \text{for some } k,$$

showing that $\gcd(m, n) \mid d$ since $\gcd(m, n) \mid km$ and $\gcd(m, n) \mid n$. Thus $d = \gcd(m, n)$. In sum for the finite case, changing the notation slightly:

> *For each positive divisor d of n there is one order-d subgroup of G, generated by any element a^m such that* $\gcd(m, n) = n/d$.

The question of how many generators a cyclic group has is independent of the question of whether the cyclic group is a subgroup of some other cyclic group. (Gallian pushes these two issues together in a way that I find confusing.) For any positive integer n, if $\langle a \rangle$ is cyclic of order n then its generators are its elements a^k where $k \in \mathbb{Z}/n\mathbb{Z}$ and $\gcd(k, n) = 1$. Thus the number of generators is $\varphi(n)$ where φ is Euler's totient function.