

## §1 Tutorial 5: Cyclic Groups - 10-04

### Theorem 1.1

Every cyclic group is abelian.

### Theorem 1.2

Every subgroup of a cyclic group is cyclic.

Let  $G$  be a cyclic group and let  $a \in G$  be of order  $n$ .

### Theorem 1.3

$$a^m = e \Leftrightarrow n \mid m$$

### Theorem 1.4

$b = a^k \in G$ , then  $|b| = \frac{n}{\gcd(n,k)}$

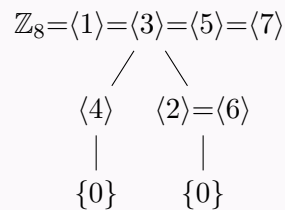
**Corollary: In additive notation**

- $\mathbb{Z}_n = \langle 1 \rangle$  with  $|1| = n$ .
- $k = k \cdot 1$ , then  $|k| = \frac{n}{\gcd(n,k)}$
- Generators of  $\mathbb{Z}_n$  are the integers  $k$  such that  $1 \leq k < n$  and  $\gcd(k, n) = 1$ .

**Example 1.5**

Subgroups of  $(\mathbb{Z}_8, +)$ . Observe that 1, 2, 4, 8 divide 8. We have to find  $k \in \mathbb{Z}_8$  such that:

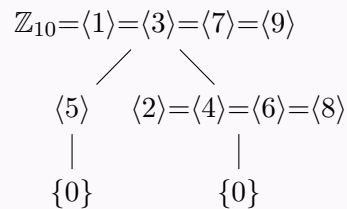
- $\gcd(8, k) = 1$   
 $\{1, 3, 5, 7\}$ . These generate subgroups of order  $\frac{8}{\gcd} = 8$ . There is only one such subgroup of  $\mathbb{Z}_8$  so they must all be the same.
- $\gcd(8, k) = 2$   
 $\{2, 6\}$ . These generate subgroups of order 4:  $\{0, 2, 4, 6\}$   
 A question arises: Do 2 and 6 generate the same subgroup?  $\langle 2 \rangle = \{0, 2, 4, 6\}$ .  
 $6 \in \langle 2 \rangle$  so  $\langle 2 \rangle = \langle 6 \rangle$ .
- $\gcd(8, k) = 4$   
 $\{4\}$ . Generates a group of order 2:  $\{0, 4\}$
- $\gcd(8, k) = 8$   
 $\{0\}$ . Generates a subgroup of order 1:  $\{0\}$



**Example 1.6**

List all the subgroups of  $\mathbb{Z}_{10}$ . Observe that 1, 2, 5, and 10 divide 10. Find  $k \in \mathbb{Z}_{10}$  such that:

- $\gcd(k, 10) = 1$ .  
 $k = 1, 3, 7, 9$ .  $\mathbb{Z}_{10} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$
- $\gcd(k, 10) = 2$ .  
 $k = 2, 4, 6, 8$ . These generate subgroups of order 5.  
 $\langle 2 \rangle = \langle 4 \rangle = \langle 6 \rangle = \langle 8 \rangle = \{0, 2, 4, 6, 8\}$
- $\gcd(k, 10) = 5$ .  
 $k = 5$ .  $\langle 5 \rangle = \{0, 5\}$ .
- $\gcd(k, 10) = 10$ .  
 $k = 0$ .  $\langle 0 \rangle = \{0\}$

**Example 1.7**

Let  $G$  be a group. Assume  $a \in G$  such that  $a^{24} = e$ . What are the possible orders of  $a$ ?

Recall that when  $a^n = e$ , the possible orders of  $a$  are those which divide  $n$ . Possible orders are therefore 1, 2, 3, 4, 6, 8, 12, 24.

$|a| = n \Rightarrow a^n = e$ . NOT  $\Leftarrow$

**Example 1.8**

Let  $a, b \in G$ . Prove the following statements:

(a)  $|a| = |a^{-1}|$

*Proof.*  $|a| = n$ .  $|a^{-1}| = m$

$$\begin{aligned} a^n &= e \\ \Rightarrow (a^n)^{-1} \cdot a^n &= (a^n)^{-1} \cdot e \\ \Rightarrow e &= (a^n)^{-1} \\ \Rightarrow e &= (a^{-1})^n \Rightarrow m|n \end{aligned}$$

You can show similarly that  $n|m$ . By proving that  $m|n$  and that  $n|m$ , we have proven that  $n = m$ .  $\square$

(b)  $\forall g \in G, |a| = |g^{-1}ag|$

*Proof.* Let  $g \in G$ ,  $|a| = n$ ,  $|g^{-1}ag| = m$ . Observe that:

$$\begin{aligned} (g^{-1}ag)^m &= e \\ \Rightarrow (g^{-1}ag)(g^{-1}ag) \dots (g^{-1}ag) &= e \\ \Rightarrow g^{-1}a^m g &= e \\ \Rightarrow g \cdot g^{-1}a^m g \cdot g^{-1} &= g \cdot e \cdot g^{-1} \\ \Rightarrow a^m &= e \end{aligned}$$

Therefore  $n|m$  because  $|a| = n$ . Similarly  $m|n$ . Therefore  $m = n$ .  $\square$

(c)  $|ab| = |ba|$

*Proof.* By (b),  $|ab| = |a^{-1}(ab)a| = |a^{-1}aba| = |ba|$   $\square$

**Exercise 1.9.** Show that if  $G$  has no proper non-trivial subgroups, then  $G$  is a cyclic group of prime orders.

*Proof.*

(a) Showing that  $G$  is cyclic. Let  $g \in G : g \neq e$ .  $\langle g \rangle$  is a non-trivial subgroup of  $G$  because  $g \in \langle g \rangle$  and  $g \neq e$ . By assumption that  $G$  has no proper non-trivial subgroups,  $\langle g \rangle = G$ .

(b) Showing that  $G$  must be of prime order.

a) Case where  $|G| = \infty$ . Let  $G$

Observe that  $\langle g^2 \rangle$  is a non-trivial subgroup of  $G$ . Observe that  $\langle g^2 \rangle \neq G$  because  $g \notin \langle g^2 \rangle$ . "If the order of a group is infinity, we will always be able to generate non-trivial proper subgroups."

b) Case where  $|G| = n < \infty$

Assume that  $n = d \cdot m$  for some  $d, m$ . Since  $d|n$ , then  $G$  must have a subgroup  $H$  of order  $d$ . This would mean that  $H$  is non-trivial and  $H \neq G$ . This is a contradiction  $\Rightarrow |G| = p$  for some prime number.  $\square$

**Exercise 1.10.** An infinite cyclic group  $G$  has exactly 2 generators.

$G = \langle a \rangle = \langle b \rangle$ . This would mean that  $a = b^k$  for some  $k$ , and that  $b = a^l$  for some  $l$ .

$$\begin{aligned} a &= b^k = (a^l)^k = a^{lk} \\ \Rightarrow a^{-1} \cdot a &= a^{-1} a^{lk} \\ \Rightarrow e &= a^{lk-1} \end{aligned}$$

We know that  $|a| = \infty$ , therefore  $lk - 1 = 0 \Rightarrow lk = 1$ . This gives two possible cases:  $l = k = 1$  or  $l = k = -1$  because  $l$  and  $k$  must be integers. Therefore either  $b = a$  or  $b = a^{-1}$ . This means that the only generators of  $G$  are  $a$  and  $a^{-1}$ .