

## 6. CYCLIC GROUPS

**Definition 6.1.** A cyclic group is a group  $G$  which is equal to  $\langle g \rangle$  for some  $g \in G$ . Thus

$$G = \langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$$

We say that  $g$  generates  $G$

Examples:

- (1)  $(\mathbb{Z}, +)$  is a cyclic group generated by  $g = 1$ .
- (2)  $(U_n, \cdot)$  is a cyclic group generated by  $\zeta = e^{2\pi i/n}$ .
- (3) For any element  $g$  of any group  $G$ ,  $\langle g \rangle$  is a cyclic group generated by  $g$ .

Problem: Show that any cyclic group is abelian (commutative).

**6.1. division and order.** We use the word *order* for the cardinality of a group. For example  $\mathbb{Z}_5$  is a group of order 5.  $\mathbb{Z}$  is an additive group of infinite order.

**Definition 6.2.** The **order** of an element  $g$  of any group is defined to be the order of the cyclic group that it generates:

$$o(g) := |\langle g \rangle|$$

For example, in  $\mathbb{Z}_6$  the order of the 6 elements and the cyclic subgroup that they generate are:

$g$	$o(g)$	$\langle g \rangle$
0	1	$\{0\}$
1	6	$\{0, 1, 2, 3, 4, 5\}$
2	3	$\{0, 2, 4\}$
3	2	$\{0, 3\}$
4	3	$\{0, 4, 2\}$
5	6	$\{0, 5, 4, 3, 2, 1\}$

The properties of the order of an element are related to the *division algorithm* also called the *Euclidean algorithm* since it was first written down by Euclid.

**Theorem 6.3** (division algorithm). *If  $n$  is a positive integer and  $k$  is any integer, there exist unique integers  $q$  and  $r$  so that*

$$k = qn + r$$

*and  $0 \leq r < n$ .  $q$  is called the quotient and  $r$  is called the remainder of  $k$  when divided by  $n$ .*

Euclid did not know about negative numbers. He assumed that  $k$  was positive and his algorithm was just to keep subtracting  $n$  from  $k$  until you can't. Then you are left with  $r$  and the number of times you subtracted was  $q$ .

You can read the proof in the book. Here I will explain what this has to do with  $o(g)$ , the order of  $g \in G$ .

**Theorem 6.4.** *Suppose that  $G$  is a group and  $g \in G$  is an element of finite order  $o(g) = |\langle g \rangle| < \infty$ . Then*

(1) *the subgroup  $\langle g \rangle \leq G$  is equal to the set*

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

*for some positive  $n$  and there is no repetition in this list of elements.*

(2)  $o(g) = n$ .

(3)  $g^n = e$

*Proof.* By definition,  $\langle g \rangle$  consists of all powers  $g^k$  of  $g$ . Since this is assumed to be a finite set, the elements

$$g, g^2, g^3, g^4, \dots$$

cannot all be different. So, two of them are equal, say  $g^i = g^j$  where  $j > i$ . This equation can be written as:

$$g^i g^{j-i} = g^j = g^i = g^i e$$

By cancellation this gives:

$$(6.1) \quad g^{j-i} = e$$

Let  $n = j - i$ . Then  $g^n = e$  and  $n > 0$ . This shows that condition (3) holds for some positive integer  $n$ . Let  $n$  be the smallest positive integer satisfying equation (3).

If  $g^k$  is any element of  $\langle g \rangle$  then the division algorithm gives

$$k = nq + r$$

where  $q, r$  are integers and  $0 \leq r \leq n - 1$ . So,

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

So,  $e, g, g^2, \dots, g^{n-1}$  are all the elements of  $\langle g \rangle$ .

To see that there are no repetitions suppose that  $0 \leq i < j \leq n - 1$  and  $g^i = g^j$ . Then, we have equation (6.1)

$$g^{j-i} = e$$

But  $j - i < n$  which is a contradiction to the minimality of  $n$ . Therefore, there are no repetitions in the list.  $\square$

**Corollary 6.5.** *If  $g \in G$  has finite order  $n$  then  $\langle g \rangle$  is isomorphic to  $\mathbb{Z}_n$ .*

*Proof.* The isomorphism  $\phi : \mathbb{Z}_n \rightarrow \langle g \rangle$  is given by  $\phi(k) = g^k$ . The first part (1) in the theorem above tells us that this mapping is a bijection. The third equation tells us that this satisfies the isomorphism property since, if  $x + y \geq n$  then  $x +_n y = x + y - n$  and

$$\phi(x+_n y) = \phi(x+y-n) = g^{x+y-n} = g^x g^y g^{-n} = \phi(x)\phi(y)e^{-1} = \phi(x)\phi(y)$$

And if  $x + y < n$  then  $x +_n y = x + y$  and it is clear that  $\phi(x +_n y) = \phi(x)\phi(y)$ .  $\square$

Problem: Show that  $g^k = e$  if and only if  $k$  is a multiple of the order of  $g$ .

Example: Let  $G = GL(2, \mathbb{Z})$  and

$$g = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

Then

$$g^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad g^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 = e$$

Then  $o(g) = 3$  and  $g^{3k} = I_2, g^{3k+1} = g, g^{3k+2} = g^2$  are the three elements of  $\langle g \rangle$ .

**6.2. subgroups of cyclic groups.** The main theorem about cyclic groups is the following.

**Theorem 6.6.** *Every subgroup of a cyclic group is cyclic.*

*Proof.* We are given that  $G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ . If  $H \leq G$ , let  $k$  be the smallest positive integer so that  $g^k \in H$ . Then  $H = \langle g^k \rangle$ . If there is no such  $k$  then  $H = \{e\}$  which is also cyclic.  $\square$

This theorem has a very nice application.

**Corollary 6.7.** *The greatest common divisor  $d$  of two positive integers  $r$  and  $s$  can be written as*

$$d = nr + ms$$

where  $n, m \in \mathbb{Z}$ .

*Proof.* Let  $G = \mathbb{Z}$  and

$$H = \{nr + mx \mid n, m \in \mathbb{Z}\}$$

Then  $H$  is a subgroup of  $\mathbb{Z}$ . The theorem implies  $H = \langle d \rangle$  for some integer  $d$ . So,  $H = d\mathbb{Z}$ . Since  $d \in H$  it has the form  $d = nr + ms$ . So, we just need to show the following.

Claim:  $d$  is the greatest common divisor (gcd) of  $r$  and  $s$ .

Pf: Since  $r = 1r + 0s \in H$ ,  $r$  is a multiple of  $d$ . Similarly,  $s$  is a multiple of  $d$ . So,  $d$  is a common divisor of  $r$  and  $s$ . Suppose that  $d$  is not the gcd. Then there is another common divisor  $D$ . Then  $D$  divides both  $r$  and  $s$  so it divides  $nr + ms = d$ . So,  $D \leq d$ . Therefore  $d$  is the greatest common divisor.  $\square$

Euclid's algorithm for finding  $d = \gcd(r, s)$  was to take the two positive integers  $r, s$  and subtract the smaller from the larger, and repeat this until the two numbers are equal. Then the result is  $d, d$ .

#### Homework 4

page 56 numbers 21, 22, 23, 26, 31, 32, 41, 54. (Do all these problems for next Thursday, Sept 24. I will give you a practice quiz on that day.)

Problems from section 6 will be in the HW5/review problems. HW5 will consist of a number of review problems which I will give you answers to most of them. A small number of these will be left for you to do. Remember: Quiz one will be on Wednesday, Oct 7, in class.