

## 9. CYCLIC GROUPS

Recall that a group  $G$  is cyclic if it is generated by one element  $a$ . In other words,  $G = \langle a \rangle$ .

One reason that cyclic groups are so important, is that any group  $G$  contains lots of cyclic groups, the subgroups generated by the elements of  $G$ . On the other hand, cyclic groups are reasonably easy to understand. First an easy lemma about the order of an element.

**Lemma 9.1.** *Let  $G$  be a group and let  $g \in G$  be an element of  $G$ .*

*Then the order of  $g$  is the smallest positive number  $k$  such that  $a^k = e$ .*

*Proof.* Replacing  $G$  by the subgroup  $\langle g \rangle$  generated by  $g$ , we might as well assume that  $G$  is cyclic, generated by  $g$ .

Suppose that  $a^l = e$ . I claim that in this case

$$G = \{ e, g, g^2, g^3, g^4, \dots, g^{l-1} \}.$$

Indeed it suffices to show that the set is closed under multiplication and taking inverses.

Suppose that  $g^i$  and  $g^j$  are in the set. Then  $g^i g^j = g^{i+j}$ . If  $i + j < l$  there is nothing to prove. If  $i + j \geq l$ , then use the fact that  $g^l = e$  to rewrite  $g^{i+j}$  as  $g^{i+j-l}$ . In this case  $i + j - l > 0$  and less than  $l$ . So the set is closed under products.

Given  $g^i$ , what is its inverse? Well  $g^{l-i} g^i = g^l = e$ . So  $g^{l-i}$  is the inverse of  $g^i$ . Alternatively we could simply use the fact that  $H$  is finite, to conclude that it must be closed under taking inverses.

Thus  $|G| \leq l$  and in particular  $|G| \leq k$ . In particular if  $G$  is infinite, there is no integer  $k$  such that  $g^k = e$  and the order of  $g$  is infinite and the smallest  $k$  such that  $g^k = e$  is infinity. Thus we may assume that the order of  $g$  is finite.

Suppose that  $|G| < k$ . Then there must be some repetitions in the set

$$\{ e, g, g^2, g^3, g^4, \dots, g^{k-1} \}.$$

Thus  $g^a = g^b$  for some  $a \neq b$  between 0 and  $k - 1$ . Suppose that  $a < b$ . Then  $g^{b-a} = e$ . But this contradicts the fact that  $k$  is the smallest integer such that  $g^k = e$ .  $\square$

**Lemma 9.2.** *Let  $G$  be a finite group of order  $n$  and let  $g$  be an element of  $G$ .*

*Then  $g^n = e$ .*

*Proof.* We know that  $g^k = e$  where  $k$  is the order of  $g$ . But  $k$  divides  $n$ . So  $n = km$ . But then

$$g^n = g^{km} = (g^k)^m = e^m = e. \quad \square$$

**Lemma 9.3.** *Let  $G$  be a cyclic group, generated by  $a$ .*

*Then*

(1)  *$G$  is abelian.*

(2) *If  $G$  is infinite, the elements of  $G$  are precisely*

$$\dots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, \dots$$

(3) *If  $G$  is finite, of order  $n$ , then the elements of  $G$  are precisely*

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

*and  $a^n = e$ .*

*Proof.* We first prove (1). Suppose that  $g$  and  $h$  are two elements of  $G$ .

As  $G$  is generated by  $a$ , there are integers  $m$  and  $n$  such that  $g = a^m$  and  $h = a^n$ . Then

$$\begin{aligned} gh &= a^m a^n \\ &= a^{m+n} \\ &= a^{n+m} \\ &= hg. \end{aligned}$$

Thus  $G$  is abelian. Hence (1).

(2) and (3) follow from (9.1). □

Note that we can easily write down a cyclic group of order  $n$ . The group of rotations of an  $n$ -gon forms a cyclic group of order  $n$ . Indeed any rotation may be expressed as a power of a rotation  $R$  through  $2\pi/n$ . On the other hand,  $R^n = 1$ .

However there is another way to write down a cyclic group of order  $n$ . Suppose that one takes the integers  $\mathbb{Z}$ . Look at the subgroup  $n\mathbb{Z}$ . Then we get equivalence classes modulo  $n$ , the left cosets.

$$[0], [1], [2], [3], \dots, [n-1].$$

I claim that this is a group, with a natural method of addition. In fact I define

$$[a] + [b] = [a + b].$$

in the obvious way. However we need to check that this is well-defined. The problem is that the notation

$$[a]$$

is somewhat ambiguous, in the sense that there are infinitely many numbers  $a'$  such that

$$[a'] = [a].$$

In other words, if the difference  $a' - a$  is a multiple of  $n$  then  $a$  and  $a'$  represent the same equivalence class. For example, suppose that  $n = 3$ . Then  $[1] = [4]$  and  $[5] = [-1]$ . So there are two ways to calculate

$$[1] + [5].$$

One way is to add 1 and 5 and take the equivalence class.  $[1] + [5] = [6]$ . On the other hand we could add 4 and  $-1$  to get 3,  $[1] + [5] = [4] + [-1] = [3]$ . Of course  $[6] = [3] = [0]$ , so we are okay.

So now suppose that  $a'$  is equal to  $a$  modulo  $n$  and  $b'$  is equal to  $b$  modulo  $n$ . This means

$$a' = a + pn$$

and

$$b' = b + qn,$$

where  $p$  and  $q$  are integers.

Then

$$a' + b' = (a + pn) + (b + qn) = (a + b) + (p + q)n.$$

So we are okay

$$[a + b] = [a' + b'],$$

and addition is well-defined. The set of left cosets with this law of addition is denoted  $\mathbb{Z}/n\mathbb{Z}$ , the integers modulo  $n$ . Is this a group? Well associativity comes for free. As ordinary addition is associative, so is addition in the integers modulo  $n$ .

$[0]$  obviously plays the role of the identity. That is

$$[a] + [0] = [a + 0] = [a].$$

Finally inverses obviously exist. Given  $[a]$ , consider  $[-a]$ . Then

$$[a] + [-a] = [a - a] = [0].$$

Note that this group is abelian.

How about the integers modulo  $n$  under multiplication? There is an obvious choice of multiplication.

$$[a] \cdot [b] = [a \cdot b].$$

Once again we need to check that this is well-defined. Exercise left for the reader.

Do we get a group? Again associativity is easy, and  $[1]$  plays the role of the identity. Unfortunately, inverses don't exist. For example  $[0]$  does not have an inverse. The obvious thing to do is throw away zero. But even then there is a problem. For example, take the integers modulo 4. Then

$$[2] \cdot [2] = [4] = [0].$$

So if you throw away  $[0]$  then you have to throw away  $[2]$ . In fact given  $n$ , you should throw away all those integers that are not coprime to  $n$ , at the very least. In fact this is enough.

**Definition-Lemma 9.4.** *Let  $n$  be a positive integer.*

*The **group of units**,  $U_n$ , for the integers modulo  $n$  is the subset of  $\mathbb{Z}/n\mathbb{Z}$  of integers coprime to  $n$ , under multiplication.*

*Proof.* We check that  $U_n$  is a group.

First we need to check that  $U_n$  is closed under multiplication. Suppose that  $[a] \in U_n$  and  $[b] \in U_n$ . Then  $a$  and  $b$  are coprime to  $n$ . This means that if a prime  $p$  divides  $n$ , then it does not divide  $a$  or  $b$ . But then  $p$  does not divide  $ab$ . As this is true for all primes that divide  $n$ , it follows that  $ab$  is coprime to  $n$ . But then  $[ab] \in U_n$ . Hence multiplication is well-defined.

This rule of multiplication is clearly associative. Indeed suppose that  $[a]$ ,  $[b]$  and  $[c] \in U_n$ . Then

$$\begin{aligned} ([a] \cdot [b]) \cdot [c] &= [ab] \cdot c \\ &= [(ab)c] \\ &= [a(bc)] \\ &= [a] \cdot [bc] \\ &= [a] \cdot ([b] \cdot [c]). \end{aligned}$$

So multiplication is associative.

Now 1 is coprime to  $n$ . But then  $[1] \in U_n$  and this clearly plays the role of the identity.

Now suppose that  $[a] \in U_n$ . We need to find an inverse of  $[a]$ . We want an integer  $b$  such that

$$[ab] = 1.$$

This means that

$$ab + mn = 1,$$

for some integers  $b$  and  $m$ . But  $a$  and  $n$  are coprime. So by Euclid's algorithm, such integers exist.  $\square$

**Definition 9.5.** *The **Euler  $\varphi$  function** is defined to be the order of  $U_n$ .*

**Lemma 9.6.** *Let  $a$  be any integer, which is coprime to the positive integer  $n$ .*

*Then  $a^{\varphi(n)} = 1 \pmod{n}$ .*

*Proof.* Let  $g = [a] \in U_n$ . By (9.2)  $g^{\varphi(n)} = e$ . But then

$$[a^{\varphi(n)}] = [1].$$

Thus

$$a^{\varphi(n)} = 1 \pmod n$$

as required.  $\square$

Given this, it would be really nice to have a quick way to compute  $\varphi(n)$ .

**Lemma 9.7.** *The Euler  $\varphi$  function is multiplicative.*

*That is, if  $m$  and  $n$  are coprime positive integers,*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

*Proof.* We will prove this later in the series.  $\square$

Given (9.7), and the fact that any number can be factored, it suffices to compute  $\varphi(p^k)$ , where  $p$  is prime and  $k$  is a positive integer.

Consider first  $\varphi(p)$ . Well every number between 1 and  $p - 1$  is automatically coprime to  $p$ . So  $\varphi(p) = p - 1$ .

**Theorem 9.8.** *(Fermat's Little Theorem) Let  $a$  be any integer. Then  $a^p = a \pmod p$ . In particular  $a^{p-1} = 1 \pmod p$  if  $a$  is coprime to  $p$ .*

*Proof.* Follows from (9.6).  $\square$

How about  $\varphi(p^k)$ ? Let us do an easy example.

Suppose we take  $p = 3$ ,  $k = 2$ . Then of the nine numbers between 1 and 9 and three are multiples of 3, 3, 6 = 2 · 3 and 9 = 3 · 3. More generally, if a number between 1 and  $p^k$  is not coprime to  $p$ , then it is a multiple of  $p$ . But there are  $p^{k-1}$  such multiples,

$$p = 1 \cdot p, 2p, 3p, \dots, (p^{k-1} - 1)p, p^k.$$

Thus  $p^k - p^{k-1}$  numbers between 1 and  $p^k$  are coprime to  $p$ . We have proved

**Lemma 9.9.** *Let  $p$  be a prime number. Then*

$$\varphi(p^k) = p^k - p^{k-1}.$$

**Example 9.10.** *What is the order of  $U_{5000}$ ?*

$$5000 = 5 \cdot 1000 = 5 \cdot (10)^3 = 5^4 \cdot 2^3.$$

Now

$$\varphi(2^3) = 2^3 - 2^2 = 4,$$

and

$$\varphi(5^4) = 5^4 - 5^3 = 5^3(4) = 125 \cdot 4.$$

As the Euler-varphi function is multiplicative, we get

$$\varphi(5000) = 4 \cdot 4 \cdot 125 = 2,000.$$

It is also interesting to see what sort of groups one gets. For example, what is  $U_6$ ?

$\varphi(6) = \varphi(2)\varphi(3) = 1 \cdot 2 = 2$ . Thus we get a cyclic group of order 2. In fact 1 and 5 are the only numbers coprime to 6.

$$5^2 = 25 = 1 \pmod{6}.$$

How about  $U_8$ ? Well

$$\varphi(8) = 4.$$

So either  $U_8$  is either cyclic of order 4, or every element has order 2. 1, 3, 5 and 7 are the numbers coprime to 8. Now

$$3^2 = 9 = 1 \pmod{8},$$

$$5^2 = 25 = 1 \pmod{8},$$

and

$$7^2 = 49 = 1 \pmod{8}.$$

So

$$[3]^2 = [5]^2 = [7]^2 = [1]$$

and every element of  $U_8$ , other than the identity, has order two. But then  $U_8$  cannot be cyclic.