

Orders of Elements in a Group, Part II  
Math 100A UCSD Fall 2001

Let  $G$  be a group and  $g \in G$ . In the previous handout on orders, we defined the order of  $g$  as the size of the group  $\langle g \rangle$ . If the order of  $g$  is finite (as is the case for all elements in a finite group), then the order of  $g$  was shown to be the *minimal positive* exponent  $n$  such that  $g^n = e$  (and when there is such an exponent,  $g$  does have finite order).

The key result for an element of finite order  $n$  is that  $g^a = e$  if and only if  $n|a$ . Know the proof for this cold! Only by mastering proofs of important results will you develop any sense of technique in mathematics.

There are two basic questions we want to address in this handout: how is the order of a power  $g^j$  related to the order of  $g$ , and how is the order of a product  $g_1g_2$  related to the orders of the factors  $g_1$  and  $g_2$ ? Throughout, we assume the group elements we are dealing with in our hypotheses have finite order.

When  $g$  has order  $n$ , clearly  $g^{-1}$  has order  $n$ , since its powers are the same as the powers of  $g$ , but simply appear in reverse order. The next case to consider is  $g^d$  when  $d|n$ . If  $n$  powers of  $g$  are required to first reach the identity, it is plausible that  $g^d$  should take  $n/d$  powers to first reach the identity. (For example,  $i$  has order 4 and  $i^2 = -1$  has order  $2 = 4/2$ .)

**Theorem 1.** *If  $g$  has order  $n$  and  $d|n$ ,  $d > 0$ , then  $g^d$  has order  $n/d$ .*

*Proof.* First, note  $n/d \in \mathbf{Z}$ . Let  $t$  be the order of  $g^d$ . Since

$$(g^d)^{n/d} = g^n = e,$$

we see  $t \leq n/d$ . (In fact,  $t|(n/d)$ .)

By definition,  $(g^d)^t = e$ , so  $g^{dt} = e$ . A basic property of orders implies  $n|dt$ , say  $nk = dt$  for  $k \in \mathbf{Z}$ . Then  $(n/d)k = t$ , so  $(n/d)|t$ . Considering that  $t \leq n/d$ , we conclude  $t = n/d$ .  $\square$

What about the order of  $g^j$  for arbitrary  $j$ , which may not divide  $d$ ? For example, if  $g$  has order 12, what is the order of  $g^8$ ? It can't be  $12/8$ , as that is not an integer. The philosophy here is that the order wants to be  $12/8$ , but since 8 isn't a factor of 12 we compromise by only dividing by the greatest common factor of 8 and 12, which is 4. The order of  $g^8$  is  $12/4 = 3$ . Here is the precise result along these lines. Pay close attention to how the handout on greatest common divisors is used!

**Theorem 2.** *Let  $g$  have order  $n$  and  $j \in \mathbf{Z}$ . The order of  $g^j$  is  $n/\gcd(j, n)$ .*

In other words, when  $n/j$  isn't an integer, we compute instead  $n$  divided by the largest factor of  $j$  which is a factor of  $n$  (i.e., divide by  $\gcd(j, n)$ ).

*Proof.* Let  $t$  be the order of  $g^j$  and  $d = \gcd(j, n)$ . We want to show  $t = n/d$ .

Write  $n = dn'$  and  $j = dj'$  for integers  $n'$  and  $j'$ . We want to show  $t = n'$ .

Since  $d = nx + jy$  for some integers  $x$  and  $y$  (why?), division by  $d$  shows  $1 = n'x + j'y$ , so  $\gcd(n', j') = 1$ .

To show  $g^j$  has order  $n'$ , we first compute

$$(g^j)^{n'} = g^{jn'} = g^{dj'n'} = g^{nj'} = (g^n)^{j'} = e.$$

Therefore  $t \leq n'$ . (Remember,  $t$  is the order of  $g^j$  and we want  $t = n'$ .)

On the other hand, since  $(g^j)^t = e$  by definition of  $t$ ,

$$e = g^{jt} = g^{dj't},$$

so  $n|dj't$ . Writing  $dj't = nk$  for some integer  $k$ , dividing both sides by  $d$  gives  $j't = n'k$ , so  $n'|j't$ . Since  $\gcd(n', j') = 1$ , this implies  $n'|t$ . Considering that we already have  $t \leq n'$ , we conclude that  $t = n'$ .  $\square$

For example, if  $g$  has order 12, here is a list of orders of the initial powers of  $g$ .

$j$	1	2	3	4	5	6	7	8	9	10	11	12
order of $g^j$	12	6	4	3	12	6	12	3	4	6	12	1

**Corollary 1.** For  $j \in \mathbf{Z}$ , its additive order in  $\mathbf{Z}_n$  is  $n/\gcd(j, n)$ .

*Proof.* Use Theorem 2 with  $G = \mathbf{Z}_n$ , an additive group.  $\square$

**Corollary 2.** Let  $g \in G$  have order  $n$ . Then  $g^j$  has order  $n$  if and only if  $\gcd(j, n) = 1$ .

*Proof.* The order of  $g^j$  is  $n/\gcd(j, n)$ , which equals  $n$  if and only if  $\gcd(j, n) = 1$ .  $\square$

Now we ask how the order of a product  $g_1g_2$  is related to the orders of the factors  $g_1$  and  $g_2$ . Alas, in this generality nothing can be said. This makes sense, since a relation between the order of  $g_1g_2$  and the orders of  $g_1$  and  $g_2$  ought to flow from a relation between powers of  $g_1g_2$  and powers of  $g_1$  and  $g_2$ . When  $g_1$  and  $g_2$  commute, we have  $(g_1g_2)^j = g_1^jg_2^j$ , and then we can expect to prove something. For simplicity, we only consider the case of relatively prime orders.

**Theorem 3.** Let  $g_1$  and  $g_2$  commute, where  $g_1$  has order  $a$  and  $g_2$  has order  $b$ , with  $\gcd(a, b) = 1$ . Then  $g_1g_2$  has order  $ab$ .

In words, for commuting elements with relatively prime orders, the order of their product is the product of their orders.

For example, if  $g_1$  has order 5,  $g_2$  has order 8, and  $g_1$  and  $g_2$  commute, then  $g_1g_2$  has order 40.

As another, more concrete, example, in  $\mathbf{Z}_{21}^\times$ ,  $-1$  has order 2 and 4 has order 3. Therefore  $-4 = 17$  has order 6.

For noncommuting elements with relatively prime order, Theorem 3 can fail. In  $S_3$ ,  $(12)$  has order 2 and  $(123)$  has order 3 while  $(12)(123) = (23)$  has order 2, not  $2 \cdot 3 = 6$ .

*Proof.* Let  $n$  be the order of  $g_1g_2$ . We want to show  $n = ab$ . Since

$$(g_1g_2)^{ab} = g_1^{ab}g_2^{ab} = (g_1^a)^b(g_2^b)^a = e,$$

we have  $n|ab$ .

By definition,  $(g_1g_2)^n = e$ . From this we show  $a|n$  and  $b|n$ . By commutativity,

$$(1) \quad g_1^n g_2^n = e.$$

Raising both sides of (1) to the power  $b$  (to kill off the  $g_2$  factor) gives

$$g_1^{nb} = e.$$

Therefore  $a|nb$  by a basic property of orders. Since  $\gcd(a, b) = 1$ , we conclude  $a|n$ . Now raising both sides of (1) to the power  $a$  gives  $g_2^{na} = e$ , so  $b|na$ , so  $b|n$  by exactly the same reasons as before.

Since  $a|n$  and  $b|n$  and  $\gcd(a, b) = 1$ , we conclude that  $ab|n$ . Since we already showed  $n|ab$  (in the first paragraph of the proof), we conclude  $n = ab$ .  $\square$

While Theorem 3 shows that a product of commuting elements with relatively prime orders has a predictable order, what if we *start* with  $g \in G$  of order  $n$  and write  $n = ab$  where  $\gcd(a, b) = 1$ ? Can we express  $g$  as a product of commuting elements with orders  $a$  and  $b$ ? Yes! That is, Theorem 3 admits a (strong) converse, as follows.

**Theorem 4.** *Let  $g \in G$  have order  $n$ , where  $n = ab$  with  $\gcd(a, b) = 1$ . Then we can write  $g = g_1g_2$  where  $g_1$  has order  $a$ ,  $g_2$  has order  $b$ , and  $g_1g_2 = g_2g_1$ . Moreover, such  $g_1$  and  $g_2$  are unique in  $G$ .*

*Proof.* To concretely illustrate the construction we will give in the proof, we start with an example. Suppose  $g$  has order  $40 = 5 \cdot 8$ . Then  $g = g_1g_2$  where  $g_1 = g^{16}$  and  $g_2 = g^{-15}$  have respective orders 5 and 8 (using Theorem 2). Since  $g_1$  and  $g_2$  are powers of  $g$ , they commute!

There is no uniqueness in the exponents used in the definition of  $g_1$  and  $g_2$ , but only in  $g_1$  and  $g_2$  themselves. For instance, we could just as well write  $g_1 = g^{96}$  and  $g_2 = g^{25}$ . These are the same  $g_1$  and  $g_2$  as before, since  $g$  has order 40 and  $96 \equiv 16 \pmod{40}$ ,  $25 \equiv -15 \pmod{40}$ . For example,

$$g^{96}g^{25} = g^{121} = g(g^{40})^3 = g,$$

as it should be.

Now we turn to the construction of  $g_1$  and  $g_2$  in the general case.

Since  $\gcd(a, b) = 1$ ,  $ax + by = 1$  for some integers  $x$  and  $y$ . In particular,  $ax \equiv 1 \pmod{b}$  and  $by \equiv 1 \pmod{a}$ . Then

$$g = g^1 = g^{ax}g^{by}.$$

We know  $g^a$  has order  $n/a = b$ . Since  $\gcd(x, b) = 1$  (why?),  $(g^a)^x = g^{ax}$  has order  $b$  by Corollary 2. Similarly,  $g^{by}$  has order  $n/b = a$ .

Let  $g_1 = g^{by}$  and  $g_2 = g^{ax}$ . These elements commute, since they are powers of  $g$ . (Note: We don't set  $g_1 = g^{ax}$  and  $g_2 = g^{by}$  because we want  $g_1$  to have order  $a$ ; although  $g^{ax}$  has an  $a$  in the exponent, its order is actually  $ab/a = b$ .)

Now we treat uniqueness. To prove this, suppose

$$g = g_1 g_2 = g'_1 g'_2,$$

where  $g_1, g_2 \in G$  and  $g'_1, g'_2 \in G$  have the relevant properties:  $g_1$  has order  $a$ ,  $g_2$  has order  $b$ ,  $g_1 g_2 = g_2 g_1$ , and likewise for  $g'_1$  and  $g'_2$ . We want to show  $g_1 = g'_1$  and  $g_2 = g'_2$ .

Since  $g_1 g_2 = g'_1 g'_2$ , raising to the power  $a$  implies  $g_2^a = (g'_2)^a$  (here we need commutativity of  $g_1, g_2$  and  $g'_1, g'_2$ ). Raising further to the power  $x$  gives  $g_2^{ax} = (g'_2)^{ax}$ . Since  $g_2$  and  $g'_2$  both have order  $b$  and  $ax \equiv 1 \pmod{b}$ , we can replace the exponent  $ax$  with 1 and find that  $g_2 = g'_2$ . Then the equation  $g_1 g_2 = g'_1 g'_2$  implies  $g_1 = g'_1$ .  $\square$

**Corollary 3.** *The unique elements  $g_1$  and  $g_2$  from the previous theorem are powers of  $g$ .*

*Proof.* In the constructive part of the proof of Theorem 4, we defined  $g_1$  and  $g_2$  as suitable powers of  $g$ .  $\square$

That  $g_1$  and  $g_2$  commute in Theorem 4 is essential in the proof of their uniqueness, and without commutativity we can find additional pairs satisfying the other conditions. For example, in  $S_9$  let

$$g = (124)(35)(6789).$$

This has order  $12 = 3 \cdot 4$ . We can write  $g$  in two ways as a product  $g_1 g_2$  of an element  $g_1$  of order 3 and an element  $g_2$  of order 4:

$$g_1 = (124), \quad g_2 = (35)(6789)$$

and

$$g_1 = (123), \quad g_2 = (2435)(6789).$$

The first pair commutes while the second pair does not. It is the first pair that is constructed in Theorem 4.