

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

Let G be a group and $g \in G$. By definition,

$$\langle g \rangle = \{g^k : k \in \mathbf{Z}\}.$$

This is called the group generated by g . It is a subgroup of G . The size of $\langle g \rangle$, i.e., the number of different powers g^k , is called the *order* of g .

Theorem 1. *To say g has finite order is equivalent to saying $g^m = e$ for some integer $m \geq 1$.*

Proof. If g has finite order, i.e., $\langle g \rangle$ is finite, then the set

$$\{g, g^2, g^3, \dots\}$$

is finite. So we must have $g^i = g^j$ for some positive integers $i < j$. Then $g^{j-i} = e$ (why?), and $j - i$ is a positive integer. Take $m = j - i$.

Conversely, suppose $g^m = e$ for some $m \geq 1$. We want to show $\langle g \rangle$ is finite. That is, we want to show g has only finitely many distinct powers. An arbitrary power of g has the form g^k for some $k \in \mathbf{Z}$. We *expect* that since $g^m = e$, the powers of g should repeat in cycles of length m . To prove this, use the division algorithm to write

$$k = mq + r, \quad 0 \leq r < m.$$

Then

$$g^k = g^{mq+r} = g^{mq}g^r = (g^m)^qg^r = eg^r = g^r,$$

so the only powers of g are $\{e, g, g^2, \dots, g^{m-1}\}$. \square

Note that we have not insisted that the exponent m be minimal, so the repetition in the powers of g may really have length less than m . For example, $(-1)^4 = 1$, so the only powers of -1 are $(-1)^j$ for $j = 0, 1, 2, 3$, but we know that in fact a more economical list is $(-1)^j$ for $j = 0, 1$.

If we choose m to be minimal, then we can make some stronger statements, as follows.

Theorem 2. *Let $g^n = e$ for some $n \geq 1$, where n is as small as possible.*

Then

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

2) $\#\langle g \rangle = n$. *That is, the powers listed in (1) are different from each other.*

3) *For integers a and b , $g^a = g^b$ if and only if $a \equiv b \pmod{n}$.*

In particular, when g has finite order, its order is equal to the smallest integer n such that $g^n = e$.

Proof. First we show (1). Given an arbitrary power g^k , write $k = nq + r$ where $0 \leq r < n$. Then $g^k = g^r$, just as in the previous proof, so every power of g is some g^r where $0 \leq r < n$. This means

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

which establishes (1). So far we have *not* used minimality of the exponent n .

Now we prove (2). We already have a list of n powers that exhaust $\langle g \rangle$, namely g^r for $0 \leq r \leq n-1$. To prove $\#\langle g \rangle = n$, we must prove these powers are all distinct. Here is where the minimality of n is going to be used.

If our list of powers contains any repetitions, then

$$g^i = g^j$$

where $1 \leq i < j \leq n-1$. (Be attentive to the inequalities here.) Then

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

and $0 < j-i < n$. This contradicts the definition of n , since we found a power of g equal to e where the exponent $j-i$ is a positive integer less than n , and n is the minimal positive integer whose power of g is e . Hence we have a contradiction, so none of the powers among $\{e, g, g^2, \dots, g^{n-1}\}$ are equal. Thus $\#\langle g \rangle = n$.

Finally, to prove (3), first assume $a \equiv b \pmod{n}$. Then $a = b + nt$ for some integer t , so

$$g^a = g^{b+nt} = g^b g^{nt} = g^b$$

since $g^n = e$. Conversely, assume $g^a = g^b$. We want to prove $a \equiv b \pmod{n}$, i.e., $n|(a-b)$. Well, by the division algorithm

$$a - b = nq + r, \quad 0 \leq r \leq n-1.$$

Thus $a = b + nq + r$. Using both sides as exponents for g ,

$$g^a = g^{b+nq+r} = g^b g^r$$

since $g^n = e$. Because $g^a = g^b$ by hypothesis, we're left with $g^r = e$. Since $0 \leq r < n$, the only way that $g^r = e$ is possible is when $r = 0$ (because n is the smallest positive integer for which we can say $g^n = e$, and thus r is not positive). Once we have $r = 0$, we see $a - b = nq$, so $a \equiv b \pmod{n}$. \square

Corollary 1. *Let $g \in G$ and g have order n . Then $g^a = e$ if and only if $n|a$.*

Proof. This is a special case of (3) in Theorem 2, with $b = 0$. The ideas involved here (especially the use of the division algorithm) are essentially contained in exercise 5b on homework 2. Review that exercise and its solution. \square