Orders of group elements

Let G be an arbitrary group, and let $a \in G$ be an element. The *order* of a, written $\text{ord}(a)$, is the smallest positive integer k such that a^k is the identity:

$$\text{ord}(a) = \min\left\{k \in \mathbb{Z} : \ k > 0, \ a^k = e\right\}$$

Our convention is that if the set appearing in this definition is empty, in other words if a^k is never the identity, then $\text{ord}(a) = \infty$.

▶ **If $a \in G$ and G is a finite group, then $\text{ord}(a) \leqslant |G|$.**

To prove this, consider the sequence $a, a^2, a^3, \ldots$. Because this is a sequence of elements in G and G has $|G|$ elements, after $|G| + 1$ terms in this sequence we must have a repeated entry. In other words, there are positive integers i, j such that $i < j$, and $j \leqslant |G| + 1$, and $a^i = a^j$. Then $e = a^j a^{-i} = a^{j-i}$ and therefore $\text{ord}(a) \leqslant j - i \leqslant |G|$.

Let's consider some examples. First, note if $\text{ord}(a) = 1$, then $a = a^1 = e$, so a is the identity.

Consider the group $(\mathbb{Z}_n, +)$. If $a \in \mathbb{Z}_n$ is equal to $m \pmod n$, then "$a^k = a \cdots a$" is given by

$$m + \cdots + m \equiv km \pmod n$$

In this case $|G| = n$ and $n \cdot m \equiv 0 \pmod n$, which exhibits $\text{ord}(a) \leqslant |G|$. Let us consider the case $n = 8$. The element $6 \pmod 8$ has $4 \cdot 6 \equiv 24 \equiv 0 \pmod 8$, while $3 \cdot 6 \equiv 18 \equiv 2 \pmod 8$, $2 \cdot 6 \equiv 12 \equiv 4 \pmod 8$. Thus the order of $6 \pmod 8$ in the group $\mathbb{Z}_8$ is equal to 4.

▶ **The order of $m \pmod n$ in the group $(\mathbb{Z}_n, +)$ is equal to $n/\mathbf{gcd}(n, m)$.**

Let us prove this. Note $n/\gcd(n, m)$ and $m/\gcd(n, m)$ are integers. Then we have

$$\frac{n}{\gcd(n, m)} \cdot m \equiv n \cdot \frac{m}{\gcd(n, m)} \equiv 0 \pmod n$$

Therefore $\text{ord}(m) \leqslant n/\gcd(n, m)$. On the other hand, letting $\text{ord}(m) = k$, we have $km \equiv 0 \pmod n$, i.e. $km = nl$ for some $l \in \mathbb{Z}$. Then we have the following relation:

$$k \cdot \frac{m}{\gcd(n, m)} = \frac{n}{\gcd(n, m)} \cdot l$$

Each factor is an integer. From the definition of the greatest common divisor it follows that $n/\gcd(n, m)$ and $m/\gcd(n, m)$ are relatively prime. From this it follows that k is divisible by $n/\gcd(n, m)$, and in particular $\text{ord}(m) = k \geqslant n/\gcd(n, m)$. Thus $\text{ord}(m) = n/\gcd(n, m)$.

For example, $8/\gcd(8, 6) = 8/2 = 4$ and this agrees with our previous determination of the order of $6 \pmod{10}$ inside $(\mathbb{Z}_{10}, +)$ from above.

▶ **If gcd$(n, m) = 1$, then $m \pmod n$ generates the group $(\mathbb{Z}_n, +)$.**

This follows from the fact that $\gcd(n, m) = 1$ implies m has order $n = |\mathbb{Z}_n|$. (See also the next proposition below.) Recall that in general $a \in G$ *generates* G if all elements in G can be written as a^k for some $k \in \mathbb{Z}$. To illustrate this for $3 \in (\mathbb{Z}_{10}, +)$, we compute in $\mathbb{Z}_{10}$:

$$1 \cdot 3 = 3, \qquad 2 \cdot 3 = 6, \qquad 3 \cdot 3 = 9, \qquad 4 \cdot 3 = 2, \qquad 5 \cdot 3 = 5,$$

$$6 \cdot 3 = 8, \qquad 7 \cdot 3 = 1, \qquad 8 \cdot 3 = 4, \qquad 9 \cdot 3 = 7, \qquad 10 \cdot 3 = 0.$$

Thus we get all of the group $(\mathbb{Z}_{10}, +)$ by successively adding 3 to itself.

We next turn to the group $(\mathbb{Z}_n^\times, \times)$. Unlike the previous examples, the notation in this group agrees nicely with the general notation $a^k = a \cdots a$ for the k^{th} power of an element.

Suppose $n = 10$. Then $\mathbb{Z}_{10}^\times = \{1, 3, 7, 9\}$. We have $3^2 \equiv 9 \pmod{10}$ and $3^3 \equiv 27 \equiv 7 \pmod{10}$ while $3^4 \equiv 3 \cdot 7 \equiv 21 \equiv 1 \pmod{10}$. Thus the order of $3 \in \mathbb{Z}_{10}^\times$ is equal to 4. On the other hand, $9^2 \equiv 81 \equiv 1 \pmod{10}$ so the order of 9 is equal to 2.

It is important, as always, to know what group we are working in and what the group operation is. For example, $3 \pmod{10}$ can also be viewed as an element of the group $(\mathbb{Z}_{10}, +)$, but in this case it has order $10/\gcd(10, 3) = 10$ as we saw above.

▶ **Given $a \in G$, let $\langle a \rangle = \{a^k : k \in \mathbb{Z}\} \subset G$. Then $\langle a \rangle$ is a subgroup, and ord$(a) = |\langle a \rangle|$. If ord$(a)$ is finite, then $\langle a \rangle$ consists of the distinct elements**

$$e = a^0,\ a^1,\ a^2,\ a^3,\ \ldots,\ a^{\mathbf{ord}(a)-1}$$

If ord$(a) = \infty$ then $a^k = a^l$ for $k, l \in \mathbb{Z}$ if and only if $k = l$.

The verification that $\langle a \rangle$ is a subgroup is straightforward and left as an exercise. So let us suppose $\mathrm{ord}(a)$ is finite. Let $m \in \mathbb{Z}$. We aim to show that $a^m \in \langle a \rangle$ is among the list of elements shown above. For this we use division with remainder: write

$$m = \mathrm{ord}(a) \cdot q + r$$

where $q, r \in \mathbb{Z}$ and $0 \leqslant r < \mathrm{ord}(a)$, the remainder. Then we compute

$$a^m = a^{\mathrm{ord}(a) \cdot q + r} = a^{\mathrm{ord}(a) \cdot q} a^r = (a^{\mathrm{ord}(a)})^q a^r = e^q a^r = a^r$$

Furthermore, a^r is on the list, because $0 \leqslant r < \mathrm{ord}(a)$. This shows $\langle a \rangle$ consists of the elements in the list given, and in particular $|\langle a \rangle| \leqslant \mathrm{ord}(a)$. Finally, we know $\mathrm{ord}(a) \leqslant |\langle a \rangle|$, and so $|\langle a \rangle| = \mathrm{ord}(a)$, and consequently the elements in the list must all be distinct. The case in which $\mathrm{ord}(a) = \infty$ is left as an exercise.

Recall that a group G is *cyclic* if there is an $a \in G$ such that $\langle a \rangle = G$. Thus G is cyclic if and only if there is an element of order $|G|$. Recall $(\mathbb{Z}, +)$ and $(\mathbb{Z}_n, +)$ are cyclic.

Let us illustrate these concepts with a few more examples. Consider $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$. This is a group of order 4 and we display its Cayley table below. Note $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 3$, where of course all operations are modulo 5. Thus $2 \in \mathbb{Z}_5^\times$ generates the group. The same is true for 3 (but not for 1 or 4). Thus $\mathbb{Z}_5^\times$ is cyclic.

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Next, consider the group $(\mathbb{Z}_8^\times, \times)$. We have $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$ and so like the previous example, this is a group of order 4. Its Cayley table is displayed below.

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

However we see that every element squares to the identity. In particular, no element is of order 4. Therefore $\mathbb{Z}_8^\times$ is *not cyclic*.

Finally, consider the following element of the general linear group $\mathrm{GL}_2(\mathbb{R})$:

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

A short computation shows $A^2 = -I$, $A^3 = -A$, $A^4 = I$ where I is the 2×2 identity matrix. Thus $\mathrm{ord}(A) = 4$. This is an example of an element of finite order in an infinite group.