Orders of elements

Definition: Let G be a group and $g \in G$. Then the order of g is the number of elements in $\langle g \rangle$, assuming $\langle g \rangle$ is finite. If $\langle g \rangle$ is infinite we say that the order of g is ∞. $|g|$ - order of g in G.

Examples

$G = \mathbb{Z}$, $2 \in \mathbb{Z}$ $\langle 2 \rangle = 2\mathbb{Z} = \{-2, -4, -6, \ldots, 0, 2, 4, \ldots\}$

$|\langle 2 \rangle| = \infty$ $|2| = \infty$ in $\mathbb{Z}$.

$G = \mathbb{Z}_{12}$

$2 \in G$ $\langle 2 \rangle = \{2, 4, 6, 8, 10, 0\}$ $|2| = 6$.

$3 \in G$ $\langle 3 \rangle = \{3, 6, 9, 0\}$ $|3| = 4$

$5 \in G$ $\langle 5 \rangle = \{5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0\}$

$|5| = 12$

5 generates $\mathbb{Z}_{12}$

$\langle 5 \rangle \subseteq \mathbb{Z}_{12}$

$|5| = 12 \iff 5$ generates $\mathbb{Z}_{12}$.

$Q = \{\pm 1, \pm i, \pm j, \pm k\}$.

$\langle i \rangle = \{i, i^2 = -1, i^3 = -i, i^4 = 1\}$ $|i| = 4$

$\langle -1 \rangle = \{-1, 1\}$ $|-1| = 2$.

Key theorems about orders

Proposition: If G $= \langle a \rangle$ is cyclic of order n generated by a – or, equivalently, if a has order n – then $a^k = e$ if and only if n divides k.

i) $|a|$ in G is the smallest ~~positive~~ n such that $a^n = e$
(or ∞ if no such n exists).

Suppose $a^n \neq e$ for all n. Then $a, a^2, a^3, \ldots$ are all different.
Because if $a^i = a^j$ for $i \neq j$, then $a^{i-j} = e$ so we would have $n \in \mathbb{Z}$ with $a^n = e$, and $a^{-n} = e$ so we can assume $n > 0$.

a has finite order means, for some $m > 0$, we have $a^m = e$. Choose smallest n so that $n > 0$ and $a^n = e$.
Look at $\{a^0, a^1, a^2, \ldots, a^{n-1}\} \subseteq \langle a \rangle$
Given a^k, write $k = sn + r$ with $0 \leq r < n$.

$$a^k = a^{sn+r} = (a^n)^s a^r = e \cdot a^r$$

so $a^k \in \{a^0, a^1, \ldots, a^{n-1}\}$.
So every power of a is in $\{a^0, \ldots, a^{n-1}\}$ so
$\{a^0, \ldots, a^{n-1}\} = \langle a \rangle$.

Suppose $a^i = a^j$ $\quad 0 \leq i < j \leq n-1$
$a^{j-i} = e$ $\quad j-i$ is smaller than n
and $a^{j-i} = e$. $j-i$ must $= 0$ so $j = i$.
$|a| = n$.

---

if $n | k$, then $a^k = a^{tn} = (a^n)^t = e$. $\quad 0 \leq r < n$

$a^k = e \quad k = sn + r \quad 0 \leq r < n$

$$a^k = a^{sn+r} = (a^n)^s a^r = e^s a^r = a^r = e$$

$\Rightarrow r = 0$ $\quad k$ is a multiple of n.

Proposition: Let G be a cyclic group of order n and let a be a generator of G. If $b = a^k$, then the order of b is n/d where $d = \gcd(k, n)$.

Given $b = a^k$, if $|a| = n$, what is order of $b = a^k$?

$G = \mathbb{Z}_{12}$, $a = 1$ $b = 3 \cdot 1$ so $k = 3$

$\langle 3 \rangle = 4$ $k = 3$ $n = 12$ $\gcd(k,n) = \gcd(3,12) = 3$ ✓

order $12/3 = 4$

$k = 5$

$\langle 5 \rangle = \langle 5 \cdot 1 \rangle$ $\gcd(5,12) = 1$

order $|5| = 12/1 = 12$

Lemma: Suppose $n, k, r \in \mathbb{Z}$ and $n | kr$. If $d|n$ and $d|k$, then $\frac{n}{d} \Big| \frac{k}{d} r$.

Pf $kr = yn$ $n = ad$ $k = bd$

$bdr = yad$ $\frac{n}{d} = a$ $\frac{k}{d} = b$

$br = ya$

$\frac{k}{d} r = y \frac{n}{d}$.

Lemma: If $n | kr$, and $d = \gcd(k, n)$, then $\frac{n}{d}$ divides r.

$6 | 4 \cdot 3$

$d = \gcd(6,4) = 2$

$3 | 2 \cdot 3 \Rightarrow 3|3$

Proof: By Euclid we have

$xk + yn = d$

$x \frac{k}{d} + y \frac{n}{d} = 1$

$x\frac{k}{d}r + y\frac{n}{d}r = r$ By lemma, $\frac{n}{d} \mid \frac{k}{d}r$

So $\frac{n}{d} \mid r$.

$b = a^k$ $|b|$ = smallest m so that $b^m = e$.

$a^{km} = e \iff n \mid km$. $n \mid km \Rightarrow \frac{n}{d} \mid m$.

smallest choice is $m = n/d$. order$(b) = n/d$.

Corollary: A congruence class $[r]$ generates $\mathbb{Z}_n$ if and only if $\gcd(r, n) = 1$. More generally, if G is a cyclic group of order n generated by g, then g^r is a generator of G if and only if $\gcd(r, n) = 1$.

$\mathbb{Z}_{12}$

$\langle 1 \rangle, \langle 5 \rangle, \langle 7 \rangle, \langle 11 \rangle = \mathbb{Z}_{12}$

k	1	2	3	4	5	6	7	8	9	10	11	0
order	12	6	4	3	12	2	12	3	4	6	12	1

$\frac{12}{\gcd(12,k)}$ $\{8, \underset{4}{16}, 0\} = \langle 8 \rangle$