Quaternion group

15 languages

Article Talk Read Edit View history Tools

From Wikipedia, the free encyclopedia

In group theory, the **quaternion group** Q_8 (sometimes just denoted by Q) is a non-abelian group of order eight, isomorphic to the eight-element subset $\{1, i, j, k, -1, -i, -j, -k\}$ of the quaternions under multiplication. It is given by the group presentation

$$Q_8 = \langle \bar{e}, i, j, k \mid \bar{e}^2 = e,\ i^2 = j^2 = k^2 = ijk = \bar{e} \rangle;$$

where e is the identity element and $\bar{e}$ commutes with the other elements of the group. These relations, discovered by W. R. Hamilton, also generate the quaternions as an algebra over the real numbers.

Another presentation of Q_8 is

$$Q_8 = \langle a, b \mid a^4 = e, a^2 = b^2, ba = a^{-1}b \rangle.$$

Like many other finite groups, it can be realized as the Galois group of a certain field of algebraic numbers.[1]

Quaternion group multiplication table (simplified form)

	1	i	j	k
1	1	i	j	k
i	i	−1	k	−j
j	j	−k	−1	i
k	k	j	−i	−1

Algebraic structure → Group theory

Group theory

$i \cdot j = k$

→ Is it commutative or non commutative

→ Because it's not symmetric.

Integral Powers of an element

(G, o) → Group.

$a, b, c \in G$.

$a \circ (b \circ c) = (a \circ b) \circ c$ ' $\circ$ ' is associative.

↳ $a \circ b \circ c$.

'a', $a \circ a \circ a$, $a \circ a \circ a \circ a \circ a \ldots a \in G$.

$a^n = a \circ a \circ a \ldots$ (n factors).

$a^0 = e$.

$a^{-n} = a^{-1} \circ a^{-1} \circ \dots\dots a^{-1}$ (n factors).

Laws of Indices in Groups

Let a be an element of a group $(G, \circ)$. Then for integers m and n:

i) $a^m \circ a^n = a^{m+n} = \underbrace{a \circ a \dots\dots \circ a}_{(m+n)}$.

ii) $(a^m)^n = a^{mn} = \underbrace{a \circ a \circ \dots\dots a}_{(mn)}$.

iii) $(a^n)^{-1} = a^{-n}$.

Order of an element

Let $(G, \circ)$ be a group and let $a \in G$, 'a' is said to be of finite order if there exists a $n \in \mathbb{Z}^+$ such that $a^n = e_G$ holds,

$e_G \rightarrow$ identity element. (least n).

e_G → identity element. (least ord)

$a^n = e_G$ $\quad$ $a \cdot a \cdot a \cdots = e_G$

$\bar{0}$ → identity element.

$(\mathbb{Z}_6, +)$

$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$O(\bar{1}) = \bar{1} + \bar{1} + \cdots + \bar{1} = \bar{6}$

$\bar{0}$

$(\bar{1})^6 = e_G$

So, $O(\bar{1}) = 6$.

$O(\bar{2}) = 3$. $\quad$ $O(\bar{3}) = 2$

$O(\bar{4}) = \bar{4} + \bar{4} + \bar{4} = \bar{12} = \bar{6} + \bar{6}$

$= \bar{0} + \bar{0}$

$= \bar{0}$

3

$O(\bar{5}) = \underbrace{\bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5}}_{6 \text{ times}}$

6 times

So, $o(\bar{3}) = 6$.

Let's consider group $U_8 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.

$$U_8 = \{x \in Z_8 : \gcd(x, 8) = 1\}.$$

$$Z_8 = \{\bar{0}, \bar{1}, \ldots \bar{7}\}$$

$$U_8 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}.$$

$$a^n \equiv 1 \pmod 8$$

$$3^2 \equiv 1 \pmod 8.$$

$o(\bar{3}) = 2.$

$$7^2 \equiv 1 \pmod 8$$

$o(\bar{7}) = 2.$

$$5^2 \equiv 1 \pmod 8$$

$o(\bar{5}) = 2.$

$$U_{10} = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}.$$

$o(\bar{3}) = 4$

$o(\bar{7}) = 4$

$$3^4 \equiv 1 \pmod{10}.$$

$O(\bar{7}) = 4$.

$O(\bar{5}) = 2$.

$7^4 \equiv 1 \pmod{10}$

$9^4 \equiv 1 \pmod{10}$

$9^2 \equiv 1 \pmod{10}$

Note :- The order of the identity element in a group is 1 and no other element in a group is of order 1.

Thm : Let a be an element of a group $(G, \cdot)$ then.

i) $O(a) = O(a^{-1})$.

ii) $O(a) = n$ and $a^m = e$

$n \mid m$, i.e n is a divisor of m.

iii) $O(a) = n$, then $a, a^2, \ldots a^n = e$ are distinct elements of G.

iv) $O(a) = n$, $m \in \mathbb{Z}^+$. $o(a^m) = \dfrac{n}{\text{g.c.d}(m,n)}$.

v) $O(a) = n$, then $o(a^p) = n$, if and only if p is prime to n.

vi) $o(a) \to$ infinite, $p \in \mathbb{Z}^+$, then.

$o(a^p) \to$ infinite.

Th^m: Each element of a finite group is of finite order.

Problems:

If $(G, \circ)$ be a finite group of even order, P.T G contains an odd number of elements of order = 2.

$|G|$ = even

Sol^n: $S = \{a \in G : a \neq a^{-1}\}$, $T = \{a \in G : a = a^{-1}\}$ } are complements of each other.

$a = a^{-1} \Rightarrow a \cdot a = a^{-1} \cdot a$

$\Rightarrow a^2 = e_G$ which implies either.

$a = e_G$ or

$o(a) = 2$.

Hence T contains the identity element e_G (of order 1) and all elements of order 2 of the group.

Let, $x \in S$, $x \neq x^{-1}$

$\Rightarrow x^{-1} \neq [x^{-1}]^{-1}$ in G.

This shows that $x^{-1} \in S$.

$(1 \;\; 1^{-1})$
$(2 \;\; 2^{-1})$
$(3 \;\; 3^{-1})$

So, $x \in S \Rightarrow x^{-1} \in S$.

x and x^{-1} form a pair of elements in S.

So, the number of elements in S is even.

$o(G)$ = even. $\quad |G|$ = even.

$(1 \;\; \cdot)$
$(2 \;\; \cdot)$
$(3 \;\; \cdot)$
$[4 \;\; \cdot]$

$a^2 = e_n$

$\Rightarrow a \cdot a^{-1} =$

$|S| \rightarrow$ even $\quad |G| \rightarrow$ even.

$|G| = |S| + |T|$.

$\Rightarrow |T| = |G| - |S|$.

even.

→ even.

2nd soln.

$e \rightarrow$ identity element.

$B = G \setminus \{e\}$.

$|G| \rightarrow$ even. $\quad |B| = |G| - e$

$\rightarrow$ odd.

Partition B into subsets of the form $\{x, x^{-1}\}$.

So, for any $x \in B$.

with, $x \neq x^{-1}$

$\{x, x^{-1}\}$ is a 2 element pair.

'K'

$x = x^{-1} \cdot x$

$\Rightarrow x^2 = e$.

x is an element of order 2 $\{x\}$ (singleton).

'm'

$|B| = 2K + m$.

$|B|$ — odd; $2K$ — even; m — odd.

* In a group $(G, \circ)$ the elements a and b

In a group $(G, \circ)$, the elements a and b commute and $o(a)$ and $o(b)$ are prime to each other. Show that $o(a \circ b) = o(a) \cdot o(b)$.

$\Rightarrow$ Let $o(a) = m$, $o(b) = n$

Let $o(a \circ b) = K$.

$\Big\rangle K = m \cdot n$

$a^m = e_G$ $\quad b^n = e_G$

$(a \circ b)^K = e$.

$(a \circ b)^{mn} = a^{mn} \circ b^{mn}$

$= (e)^n \circ (e)^m$

$= e \circ e = e$.

So, K is a divisor of mn.

Again. $(a \circ b)^K = e$.

$\Rightarrow a^K \circ b^K = e$.

$\Rightarrow a^K = b^{-K}$

$\Rightarrow a^{nK} = b^{-nK}$

$\Rightarrow a^{nK} = (b^n)^{-K}$

$a^K \circ b^K = e$.

$a^K \circ (b^K \circ b^{-K}) = e \circ b^{-K}$

$\Rightarrow a^K \circ e = b^{-K}$

$\Rightarrow e^K = b^{-K}$.

$\Rightarrow a^{nK} = (b^n)^{-K}$

$\Rightarrow a^{nK} = e$.

$\hookrightarrow$ m is a divisor of nK.

$\Rightarrow$ m is a divisor of K ---(1)

since g.c.d $(m, n) = 1$.

Also, $(a \circ b)^K = e$

$\Rightarrow a^K \circ b^K = e$.

$\Rightarrow b^K = a^{-K}$.

$\Rightarrow b^{mK} = e$.

$\Rightarrow n$ is a divisor mK.

$\Rightarrow n$ is a divisor of K ---(1).

g.c.d$(m, n) = 1$

'mn' is a divisor K. since g.c.d $(m, n) = 1$.

$K = mn$.

$\Rightarrow o(a \circ b) = o(a) \cdot o(b)$.

PROVED.

In a group $(G, \circ)$, 'a' is an element $\neq e$, then the order of 'a' is

In a group $(G, \circ)$, a is an element of order 30. Find the order of a^{18}.

$\Rightarrow a^{30} = e$.

Let, $O(a^{18}) = m$.

$$(a^{18})^m = e.$$

$$\Rightarrow a^{18m} = e.$$

So, 30 is a divisor of $18m$.

$30 = 5 \times 6$

$18m = 3m \times 6$

So, 5 is a divisor of $3m$.

Since 'm' is the least $\in Z^+$

So, $m = 5$.

$\therefore O(a^{18}) = 5$.

Find all elements of order 8 in the group $(Z_{24}, +)$.

Sol^n: $\mathbb{Z}_{24} = \{\bar{0}, \bar{1}, \bar{2}, \ldots \bar{23}\}$.

$O(\bar{0}) = 1$. $O(\bar{1}) = 24$

but $O(\bar{m}) = 8$, when $0 < m < 24$.

$O(\bar{1}) = 24$, $O(\bar{3}) = 8$

$\bar{3} + \bar{3} + \ldots + \bar{3}$

$= \overline{24} = \bar{0} = e$ |||.

order of $k \in \mathbb{Z}_{24} = \dfrac{24}{g.c.d(k, 24)} = 8$.

$\Rightarrow g.c.d(k, 24) = 24/8$

$\Rightarrow g.c.d(k, 24) = 3$

$k = 3r$. $\boxed{g.c.d(3r, 24) = 3 \times g.c.d(r, 8)}$.

3. $gcd(r, 8) = 3$

$\Rightarrow g.c.d(r, 8) = 1$.

Unit mod 8 $\rightarrow \{1, 3, 5, 7\}$.

Unit mod 8 → {1, 3, ·, ·}.

$\overline{3}$, $\overline{5}$, $\overline{15}$, $\overline{21}$.