Capítulo 10 - Orden de Elementos de un Grupo

A. Leyes de Exponentes

1. Probar $a^m a^n = a^{m+n}$

$$(a) \quad m = 0 : a^m a^n = a^0 a^n = a^n = a^{0+n}$$

$$(b) \quad m < 0, n > 0 : a^m a^n = (a^{-m})^{-1}(a^n) = \underbrace{(a \cdots a)^{-1}}_{-m \text{ veces}} \underbrace{(a \cdots a)}_{n \text{ veces}} = \underbrace{(a^{-1} \cdots a^{-1})}_{-m \text{ veces}} = \underbrace{(a \cdots a)}_{n-(-m) \text{ veces}}$$

$$(c) \quad m < 0, n < 0 : (a^{-m})^{-1}(a_{-n})^{-1} = \underbrace{(a \cdots a)^{-1}}_{-m \text{ veces}} \underbrace{(a \cdots a)^{-1}}_{-n \text{ veces}} = \underbrace{a^{-1} \cdots a^{-1}}_{-n-m \text{ veces}} = (a^{-1})^{-n-m} = a^{m+n}$$

2. Probar que $(a^m)^n = a^{mn}$ en los siguientes casos:

$$(a) \quad m = 0 : (a^m)^n = (a^0)^n = e^n = e^0 = a^{0n} \quad \text{(no)}$$

$$(b) \quad n = 0 : (a^m)^0 = \underbrace{(a \cdots a)^0}_{m \text{ veces}} = \underbrace{a^0 \cdots a^0}_{m \text{ veces}} = a^{m \cdot 0}$$

$$(c) \quad m < 0, n > 0 : (a^m)^n = \left((a^{-m})^{-1}\right)^n = \underbrace{(a^{-m})^{-1} \cdots (a^{-m})^{-1}}_{n \text{ veces}} = \underbrace{\underbrace{(a^{-1} \cdots a^{-1})}_{-m \text{ veces}} \cdots \underbrace{(a^{-1} \cdots a^{-1})}_{-m \text{ veces}}}_{n \text{ veces}} = (a^{-1})^{-mn} = a^{mn}$$

$$(d) \quad m > 0, n < 0 : (a^m)^n = \left((a^m)^{-n}\right)^{-1} = \underbrace{(a^m \cdots a^m)^{-1}}_{-n \text{ veces}} = \underbrace{(a \cdots a)^{-1}}_{-nm \text{ veces}} = a^{-1} \cdots a^{-1} = (a^{-1})^{-nm} = a^{nm}$$

$$(e) \quad m < 0, n < 0 : (a^m)^n = \left((((a^{-m}))^{-1})^{-n}\right)^{-1} = (\underbrace{(a^{-m})^{-1} \cdots (a^{-m})^{-1}}_{-n \text{ veces}})^{-1}$$

$$= (\underbrace{\underbrace{(a \cdots a)^{-1}}_{-m \text{ veces}} \cdots (a \cdots a)^{-1}}_{-n \text{ veces}})^{-1} = \underbrace{(a^{-1} \cdots a^{-1})^{-1}}_{mn \text{ veces}} = ((a^{-1})^{nm})^{-1} = (a^{-nm})^{-1} = a^{nm}$$

3. Probar que $(a^n)^{-1} = a^{-n}$

$$(a) \quad n = 0 : (a^n)^{-1} = (a^0)^{-1} = a^{-0} = a^0$$

$$(b) \quad n < 0 : (a^n)^{-1} = ((a^{-n})^{-1})^{-1} = (a^{-1} \cdots a^{-1})^{-1} = a^{-1} \cdots a^{-1} = a^{-n}$$

B. Ejemplo de Ordenes de Elementos

1. Orden de 10 en $\mathbb{Z}_{25}$

$$5 \cdot 10 = 0 \pmod{\mathbb{Z}_{25}}$$

2. Orden de 6 en $\mathbb{Z}_{16}$

$$8 \cdot 6 = 0 \pmod{\mathbb{Z}_{16}}$$

3. Orden de $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 2 & 5 & 4 \end{pmatrix}$

$$f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 1 & 5 & 2 \end{pmatrix} \qquad f^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 5 & 1 \end{pmatrix} \qquad f^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

4. Orden de 1 en $\mathbb{R}^*$ y en $\nvdash$.

Uhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh

5. Orden de $f(x) = \frac{2}{2-x}$

$$f^2 = \frac{2-x}{1-x} \qquad f^3 = \frac{2x-2}{x} \qquad f^4 = \frac{2}{2-x}$$

6. Encontrar un grupo infinito tal que tenga un elemento de orden finito:

Sea el cociente $\mathbb{Q}/\mathbb{Z}$, entonces para $p/q + \mathbb{Z}$, el elemento posee orden q: $q \cdot (p/q) + \mathbb{Z} = p + \mathbb{Z} = 0 + \mathbb{Z}$

7. En $\mathbb{Z}_{24}$ listar todos los elementos de orden 2, 3, 4, 6.

$$\begin{aligned} \text{Orden } 2: &\quad 12 \\ \text{Orden } 3: &\quad 8, 16 \\ \text{Orden } 4: &\quad 6, 18 \\ \text{Orden } 6: &\quad 4, 8, 16, 20 \end{aligned}$$

C. Propiedades Elementales del Orden
Sean a, b y c elementos de un grupo G.

1. $\text{ord}(a) = 1$ ssi $a = e$
$\Longrightarrow$) $a^1 = e \Longleftrightarrow a = e$.
$\Longleftarrow$) $a = e \Longleftrightarrow a^1 = e$

2. Si $\text{ord}(a) = n$, entonces $a^{n-r} = (a^r)^{-1}$
$\longrightarrow$) $a^{n-r} = a^n \cdot a^{-r} = e \cdot a^{-r} = (a^r)^{-1}$

3. Si $a^k = e$ donde k es impar, entonces el orden de a es impar.

Si $a^k = e$, entonces k es múltiplo de $\text{ord}(a) = n$, es decir $k = n \cdot q$, tanto n como q no pueden ser pares, pues tendríamos una contradición por la imparidad de n.

4. $\text{ord}(a) = \text{ord}(bab^{-1})$

Sea $a^n = e$, luego $(bab^{-1})^n = (ban^{-1})(bab^{-1}) \cdots (bab^{-1}) = ba^nb^{-1} = beb^{-1} = bb^{-1} = e$

5. El orden de a^{-1} es el mismo que el orden de a

Sea n el orden de a, luego $(a^{-1})^n = a^{-n} = (a^n)^{-1} = e^{-1} = e$

6. El orden de ab es el mismo que el de ba.

$(ba)^n = baba \cdots ab = e \Longleftrightarrow \underbrace{(baba \cdots bab)}_{x} a = e$, es decir a es el inverso de x, entonces, $a(baba \cdots bab) = e = (ab)^n$

7. $\text{ord}(abc) = \text{ord}(cab) = \text{ord}(bca)$

$$\begin{aligned} (abc)^n = (ab)c \cdot (ab)c \cdots (ab)c = e &\Longleftrightarrow c(ab)c(ab) \cdots (ab)c(ab) = e \\ &\Longleftrightarrow (cab)^n = e \\ &\Longleftrightarrow (ca)b \cdot (ca)b \cdots (ca)b = e \\ &\Longleftrightarrow b(ca)b(ca)b \cdots (ca) = e \\ &\Longleftrightarrow (bca)^n = e \end{aligned}$$

8. Sea $x = a_1 a_2 \cdots a_n$ y sea y el producto de los mismos factores permutados de forma cíclica.

Argumentamos por inducción

D. Más propiedades del orden
Sea a un elemento de orden finito en un grupo G.

1. Si $a^p = e$, con p primo, entonces a posee orden p $(a \neq e)$

Si a tuviese orden no p, se tendría que p posee como factor el orden, $p = \text{ord}(a) \cdot q$, pero los únicos divisores de p son p y 1. No puede ser 1 ya que por hipótesis $a \neq e$, entonces $\text{ord}(a) = p$

2. El orden de a^k es un divisor (factor) del orden de a.

Sea n el orden de a^k, es decir $(a^k)^n = e$ si y solo si $a^{kn} = e$, luego, $kn = \text{ord}(a) \cdot q + r$: $a^{\text{ord}(a) \cdot q + r} = e \cdot a^r = e$, entonces $r = 0$, por lo que $kn = \text{ord}(a) \cdot q \Longleftrightarrow k\,\text{ord}(a^k) = \text{ord}(a) \cdot q$, entonces $\text{ord}(a) = \frac{k}{q} \cdot \text{ord}(a^k)$

3. Si $\text{ord}(a) = km$, entonces $\mathrm{a^k} = m$

$a^{km} = e \Longleftrightarrow (a^k)^m = e \Longrightarrow \text{ord}(a^k) = m$

4.

5. Si a posee orden n y $a^r = a^s$, entonces n es factor de $r - s$:

$a^r = a^s$ si y solo si $a^{r-s} = e$, entonces por teorema $r - s = n \cdot q$

6. Si a es el único elemento de orden j en G, entonces a está en el centro de G.

Por ejercicio anterior, $\text{ord}(a) = \text{ord}(bab^{-1})$, pero a es el único elemento con este orden, por lo que $a = bab^{-1} \Longleftrightarrow ab = ba$, por lo que a está en el centro.

7. Si el orden de a no es un múltiplo de m, el orden de a^k no es múltiplo de m

Sea $\text{ord}(a) \neq m \cdot q$, se tiene que $\text{ord}(a^k) \mid \text{ord}(a)$, entonces $k \cdot \mathrm{a^k} = \text{ord}(a) \neq m \cdot q$.

8. Si $\mathrm{a} = mk$ y $a^{rk} = e$, entonces r es múltiplo de m.

$rk = mr \cdot q + r$, Luego, $a^{mk \cdot q + r} = a^{mk \cdot q} \cdot a^r = e \cdot a^r = e$, entonces $r = 0$, por lo que $rk = mkq$ si y solo si $r = mq$.

F. Orden de Potencias de Elementos
Sea a un elemento de orden 12 en un grupo G.

1. ¿Cuál es el entero positivo k más pequeño tal que $a^{8k} = e$?

$8k = 12q \Longleftrightarrow 8k \equiv 0 \pmod{12} \Longleftrightarrow k = 3$

2. ¿Cuál es el orden de a^8?

Por punto anterior $k = 3$

3. ¿Cuáles son los órdenes de a^9, a^{10}, a^5?

- $9k = 12q \Longleftrightarrow 9k \equiv 0 \pmod{12} \Longleftrightarrow k = 4$
- $10k \equiv 0 \pmod{12} \Longleftrightarrow k = 6$
- $5k \equiv 0 \pmod{12} \Longleftrightarrow k = 12$

4. ¿Cuál de las potencias de a poseen el mismo orden que a?

$(\text{ord}(a^k))k = 12q = \text{ord}(a)q \iff \text{ord}(a^k)k \equiv 0 \pmod{12} \iff \text{ord}(a^k) \equiv 0 \pmod{m}$ donde $m = \frac{12}{\gcd(12,k)}$, como queremos que el orden sea 12 buscamos los k tal que sean coprimos con 12, es decir $k = 1, 5, 7, 11$.

5. Sea a un elemento de orden m en cualquier grupo G. ¿Cuál es el orden de a^k? (viendo los ejemplos anteriores y generalizando, no hay que probar nada)

$$\text{ord}(a^k) = \frac{\text{ord}(a)}{\gcd(\text{ord}(a), k)}$$

6. Sea a un elemento de orden m en cualquier grupo G. ¿Para qué valores de k es $\text{ord}(a^k) = m$

Para aquellos k coprimos al orden de a.

G. Relación entre $\text{ord}(a)$ y $\text{ord}(a^k)$
Sea a un elemento de orden n en un grupo G.

1. Probar que si m y n sn coprimos, entonces a^m posee orden n.

Por parte anterior, podemos ver que $\text{ord}(a^k) = \frac{\text{ord}(a)}{\gcd(\text{ord}(a),k)} = \frac{n}{\gcd(m,n)} = n$

Por otro lado, usando el teorema anterior, $mk = nq$, entonces n es factor de mk, pero como m es coprimo con n, no comparten factores primos, entonces n es factor de k, es decir $a^{mnk_0} = e$

2. Probar que si a^m posee orden n, entonces m y n son coprimos.

$$n = \frac{n}{\gcd(n,m)}, \text{ entonces } \gcd(m,n) = 1$$

3. Sea l el mínimo común múltiplo de m y n. Sea $l/m = k$. Explicar por qué $(a^m)^k = e$

$(a^m)^k = a^l, l = nq$, si y solo si $a^l = a^{nq} = (a^n)^q = e^q = e$

4. Probar que si $(a^m)^t = e$, entonces n es un factor de mt. Entonces mt es un múltiplo común de m y n. Concluir que:

$$l \leq mt$$

donde $l = mcm(m,n)$

Se tiene por teorema que $mt = nq$, entonces mt es factor común de m y n, luego, por definición, l es el mínimo entero positivo factor común entre m y n. Entonces $l \leq mt$.

4. Concluir que el orden de a^m es $\text{mcm}(\text{m}, \text{n})/m$

Se tiene que $(a^m)^k = e$, con k minimal, si y solo si $mk = nq$, entonces $\text{mcm}(m,n)/m = k$, entonces, $\text{ord}(a^k) = \text{mcm}(m,n)/m$

H. Relación entre el orden de a y el orden de cualquier raíz k-ésima de a

1. Sea a de orden 12. Probar que si a posee una raíz cuadrática, sease $a = b^3$ para algún $b \in G$, entonces b posee orden 36.

$a^{12} = b^{36} = e$

2. Sea a de orden 6, si a posee una raíz cuarta en G, $a = b^4$. ¿Cuál es el orden de b?

$a^6 = b^{24} = e$

3. Sea a de orden 10, $a = b^6$, ¿cuál es el orden de b?

$a^{10} = b^{60} = e$

4. Sea a de orden n. Si $a = b^k$, explicar por que el orden de b es factor de nk.

$a^n = (b^k)^n = b^{kn} = e$, por teorema, $kn = \text{ord}(b)q$