Lista De Grupos Cíclicos.

1. Sean a, b elementos de un grupo G. Pruebe que $|a| = |a^{-1}|$, $|ab| = |ba|$ y que $|a| = |gag^{-1}|$ para cada $g \in G$.

Dem:

a) Sea $a \in G$. Suponga que $|a| = n$. Veamos que:

$$(a^{-1})^n = (a^{-n}) = (a^n)^{-1} = e^{-1} = e$$

Si $0 < r < n$ es tal que

$$(a^{-1})^r = e$$

entonces

$$a^r = (a^{-1})^{-r} = ((a^{-1})^r)^{-1} = e^{-1} = e \;\#_c$$

pues $n = |a|$. Por tanto, $|a^{-1}| = n$.

Suponga que $|a| = \infty$. Entonces $|a^{-1}| = \infty$. En efecto, si $|a^{-1}| = n$ con $n \in \mathbb{N} \Rightarrow |(a^{-1})^{-1}| = |a| = n \;\#_c$. Así $|a^{-1}| = n$.

b) Sea $n = |ab|$. Veamos que:

$$(ba)^n = (ba)\cdot(ba)\cdot\ldots\cdot(ba) = b(ab)\cdot(ab)\cdot\ldots\cdot(ab)\cdot a$$
$$= b(ab)^{n-1}a$$

Como $(ab)^{n-1} = (ab)^{-1} = b^{-1}a^{-1}$, entonces:

$$(ba)^n = b(b^{-1}a^{-1})a = e\cdot e = e$$

Si $\exists\, r \in \mathbb{N}$, $0 < r < n \ni (ba)^r = e$, entonces $(ab)^r = e \;\#_c$. Así, $|ba| = n$.

c) Suponga que $|a| = n$. Sea $g \in G$, entonces

$$(gag^{-1})^n = (gag^{-1})\cdot(gag^{-1})\cdot\ldots\cdot(gag^{-1}) = ga(g^{-1}g)a(g^{-1}g)\cdot\ldots\cdot ag^{-1}$$
$$= ga^ng^{-1} = gg^{-1} = e$$

Si $\exists\, r \in \mathbb{N}$, $0 < r < n \ni (gag^{-1})^r = e$, entonces, por lo probado anteriormente, como $g^{-1} \in G$:

$$a^r = (g^{-1}gag^{-1}g)^r = e \;\#_c, \text{ pues } |a| = n.$$

Así, $|gag^{-1}| = n$, $\forall g \in G$.

q.e.d.

2. Sea G un grupo abeliano el cual tiene elementos a y b de órdenes m y n respectivamente. Pruebe que G contiene un elemento cuyo orden es el mínimo común múltiplo de m y n. (Sugerencia: Primero trate el caso $(m, n) = 1$).

Dem:

Probaremos un resultado preeliminar:

- Sea $a \in G$ m $|a| = n$. Entonces $a^r = e \Leftrightarrow n \mid r$.

$\Rightarrow$) Suponga que $n \nmid r$. Por el algoritmo de la división $\exists\, q, r \in \mathbb{Z}$ m

$$r = nq + r, \; 0 < r < n$$

donde $r \neq 0$, pues si $r = 0$, entonces $n \mid r$ #c. Así

$$a^r = a^{nq+r} = a^{nq} \cdot a^r = e \cdot a^r = a^r \neq e$$

pues $|a| = n$ y $0 < r < n$.

$\Leftarrow$) Es inmediata.

$\square$