Problema 8. Sigui G un grup cíclic d'ordre n.

(a) Demostreu que tot subgrup de G és cíclic.

(b) Demostreu que, per a cada divisor d de n, existeix un únic subgrup de G d'ordre d.

Solució. Sigui G generat per a.

(a) Agafem $H \subseteq G$ subgrup.

Tenim dos casos:

Si $H = \{e\}$ és el conjunt format sols pel neutre, H és cíclic.

Si $H = \{e, g, ...\}$ és el conjunt, no trivial, format per almenys un element més a part del neutre. Com H es un subgrup de G, els seus elements seran poténcies de a i, per tant, $g = a^l$ per algun l enter positiu.

Sigui m el menor enter positiu tal que $a^m \in H$, provarem que $h = a^m$ genera H, és a dir, que $H =< h >$.

Volem veure que per a qualsevol $h' \in H$ podem esciure h' com a potència de h. Com $h' \in H$ i $H \subseteq G$ subgrup: $h' = a^k$ per una k enter.

Per la minimalitat de m, podem aplicar l'algorisme de la divisió i escriure $k = mq + r$ on $q \geqslant 0$ i $0 \leq r < m$, i obtenim $a^k = a^{mq+r} = (a^m)^q a^r = h^q a^r$.

Llavors $a^r = h^{-q} a^k$. Com H és subgup $a^r \in H$ ja que $a^k \in H$ per defició i $h^{-q} \in H$ ja que hem definit h com a generador de H. Però r ha de ser més petit que m i m está definit com el mínim, per tant r ha de ser 0.

Si $r = 0$ tindrem $k = mq$: $h' = a^k = a^m q = (a^m)^q = h^q$. Com volíem demostrar.

(b) Existència:

Considerem $a^{(\frac{n}{d})}$, clarament veiem que te d potències, per tant, $< a^{(\frac{n}{d})} >$ és un grup d'ordre d.

Unicitat:

Suposem que existeix $H \subseteq G$ subgrup tal que $H \neq < a^{(\frac{n}{d})} >$ d'ordre d generat per $x = a^r$ per algun r enter. Llavors $x^{rd} = e$, per tant $n|rd$ i podem escriure $r = k(\frac{n}{d})$ per algun k enter. Llavors tenim que x és una potència de $a^{(\frac{n}{d})}$ i, per tant, H és un subgrup de $< a^{(\frac{n}{d})} >$. Com que H i $< a^{(\frac{n}{d})} >$ tenen el mateix cardinal, coincideixen