Profesor: Martín Matamala
Auxiliares: Bastián Espinoza, José Palacios
MA3101: Elementos de Algebra

Ejercicio Uno

2016

1. Demuestre TC para grupos cíclicos
   Si $G =< \{g\} >, n = |G|$, definamos $x = g^{n/p}$. Se verifica que n/p es entero y que x tiene orden p

2. Demuestre que para todo grupo G, si $H \triangleleft G$ y G/H tiene un elemento de orden p, entonces G también tiene un elemento de orden p.
   Que gH sea un elemento de orden p en G/H significa que existe $h \in H$ tal que $g^p = h$. Sea $n = ord(h)$. $x = g^n$ cumple lo pedido.

3. Demuestre TC para grupos abelianos no cíclicos. Considere un subgrupo cíclico no trivial y aplique inducción.
   Si $|G| = p$, entonces ya acabamos. Si $|G| > p$, tomemos $h \in G$ no nulo. Como G es abeliano, $H :=< \{h\} > \triangleleft G$. Debemos estudiar dos casos:
   Si $p||G/H|$: en este caso, tenemos un elemento de orden p en G/H y así, dado lo hecho en **2**, hay un elemento de orden p en G.
   Si p no divide a G/H: como además $p||G|$, necesariamente $p||H|$. Usando la hipótesis de inducción en H acabamos.

4. Demuestre que para todo grupo finito G y para todo $x \in G$, el cardinal de su clase de conjugación es igual al índice del subgrupo $c(x) := \{g \in G : gx = xg\}$. Considere la asignación $g^{-1}xg \to c(x)g$.
   Sea $x \in G,\ C(x) = \{g^{-1}xg : g \in G\},\ f : C(x) \to G/c(x),\ f(g^{-1}xg) = c(x)g$.
   f esta bien definida: $g^{-1}xg = h^{-1}xh \Leftrightarrow hg^{-1}x = xhg^{-1} \Leftrightarrow hg^{-1} \in c(x) \Leftrightarrow h = c(x)g \Leftrightarrow c(x)h = c(x)c(x)g = c(x)g \Leftrightarrow f(g) = f(h)$.
   f es inyectiva: basta devolverse en los bicondicionales de arriba.
   f es epiyectiva: Dado $c(x)g$, se tiene $f(g^{-1}xg) = c(x)g$.
   Luego, $|C(x)| = |G/c(x)|$.

5. Demustre TC para grupos no abelianos. Considere la ecuación de clases y aplique inducción.
   La ecuación de clases para la acción por conjugación de G en G da $|G| = \bigcup_{g\in G} orb(g$. Si tomamos un representante por cada órbita, tendremos una unión disjunta. Luego $|G| = \sum_i |orb(g_i)|$. Usando la fórmula para cada órbita obtenida en la parte anterior y notando que $|orb(g)| = 1$ ssi $g \in Z(G) = centro\ de\ G$, tenemos $|G| = |Z(G)| + \sum_{g_i \notin Z(G)} |orb(g_i)|$. Como p divide tanto al orden de G como a cada término de la sumatoria, p debe dividir al orden del centro de G. Luego, por lo hecho en la parte **3**. $Z(G)$ tiene un elemento de orden p, por lo que G también.
   NOTA: no sé bien qué matería habían visto cuando dieron el ejercicio. Creo que esa fórmula la habían visto en clases y gran parte de lo escrito aqui es innecesario.

6. Sea G un grupo de orden n y sea $k \in \mathbb{Z}$. Demuestre que k es invertible en $(\mathbb{Z}_n^*, \cdot)$ si, y sólo si la ecuación $x^k = e$ tiene exactamente una solución en G.
   Si k es invertible en $\mathbb{Z}$, entonces existe m tal que $km = 1\ mod\ n$. Notemos que e soluciona la ecuación. Si $x^k = e$, entonces $x = x^{km} = (x^k)^m = e^m = e$. Recíprocamente, supongamos que $x^k = e$ tiene solución única y k no es invertible. Entonces hay un primo p que divide a k y a n. Debe existir un $x \in G$ de orden p. Como $x^k = e^k = e$, tenemos $x = e$, por lo que x no tiene orden $p \rightarrow\leftarrow$.