Universidad de la República
Facultad de Ingeniería
IMERL: Matemática Discreta 2, semipresencial

Tercer prueba - 3 de noviembre de 2018.
Solución

Ejercicio 1. (15 puntos)

a. Demostrar el Teorema de Lagrange:
Si G es un grupo finito y $H < G$, entonces $|H|$ divide a $|G|$.

Solución:
Copiamos aquí la demostración que aparecen en las notas de teórico.

La idea de la demostración es la siguiente: definiremos en G una relación de equivalencia de forma tal que si C es una clase de equivalencia, entonces $\#C = |H|$. Entonces, como G es finito, la cantidad de clases de equivalencia también lo es; sean $C_1, C_2, \cdots, C_k$ las clases de equivalencia distintas. Sabemos que el conjunto de clases de equivalencia (de cualquier relación de equivalencia) es una **partición** de G; es decir que $G = C_1 \cup C_2 \cup \cdots \cup C_k$ y esta unión es disjunta ($C_i \cap C_j = \emptyset$ si $i \neq j$). Por lo tanto tendremos que $|G| = \#C_1 + \#C_2 + \cdots + \#C_k = \underbrace{|H| + |H| + \cdots + |H|}_{k \text{ veces}} = k|H|$ y por lo tanto obtendremos que $|H|$ divide a $|G|$.

Resta entonces definir la relación de equivalencia en G que cumpla con lo deseado: para $g, g' \in G$ definimos $g \sim g'$ si existe $h \in H$ tal que $g = hg'$; o equivalentemente, $g \sim g'$ si $g(g')^{-1} \in H$. Veamos primero que esto define una relación de equivalencia:

- (reflexiva) Para todo $g \in G$, tenemos que $g \sim g$ pues $g = eg$ y $e \in H$ (pues H es subgrupo de G.)
- (simétrica) Sean $g, g' \in G$ tales que $g \sim g'$. Entonces $g(g')^{-1} \in H$. Al ser H un subgrupo, es cerrado por inversos y por lo tanto $\left(g(g')^{-1}\right)^{-1} \in H$. Por lo tanto $g'g^{-1} \in H$ y entonces $g' \sim g$.
- (transitiva) Si $g \sim g'$ y $g' \sim g''$ entonces existen $h, h' \in H$ tales que $g = hg'$ y $g' = h'g''$. Por lo tanto tenemos que $g = hg' = h(h'g'') = (hh')g''$. Al ser H un subgrupo (en particular cerrado con la operación) tenemos que $hh' \in H$ y entonces $g \sim g''$.

Resta ver entonces que una clase de equivalencia tiene tantos elementos como H. Observar que si $g' \in G$ entonces la clase de equivalencia de g' es $C = \{g \in G : g \sim g'\} = \{g \in G : \exists h \in H : g = hg'\}$. Por lo tanto $C = \{hg' : h \in H\}$. Además, al multiplicar a todos los elementos de H por g', no hay repeticiones; es decir que si $h_1 \neq h_2$ entonces $h_1 g' \neq h_2 g'$ (por la propiedad cancelativa). Por lo tanto $\#C = |H|$.

b. Demostrar los siguientes puntos:
Si $(G, *, e)$ es un grupo de orden finito y $g \in G$ entonces:

i) $\mathrm{o}(g) \mid |G|$.
ii) $g^{|G|} = e$.
iii) Si $|G|$ es primo, entonces G es cíclico.

Solución:
Copiamos aquí las demostraciones que aparecen en las notas de teórico.

Consideramos $H = \langle g \rangle$; sabemos que H es un subgrupo de G y que $|H| = \mathrm{o}(g)$. Entonces, por el Teorema de Lagrange tenemos que $\mathrm{o}(g) = |H|$ divide a $|G|$ y hemos probado la primer parte.

Además, como $|G|$ es un múltiplo de $\mathrm{o}(g)$, se deduce que $g^{|G|} = e$.

Para la tercer parte, como $|G| \geq 2$ entonces existe un $g \in G$ tal que $g \neq e$. Por el Teorema de Lagrange debemos tener que $|\langle g \rangle|$ divide a $|G|$. Como $|\langle g \rangle| > 1$ y $|G|$ es primo tenemos que $|\langle g \rangle| = |G|$ y entonces $\langle g \rangle = G$.

c. Escriba la tabla de multiplicación de $U(18)$. Hallar los órdenes de los elementos de $U(18)$. ¿Es $U(18)$ cíclico?

Solución:
$U(18) = \{1, 5, 7, 11, 13, 17\}$.

La tabla del producto en $U(18)$ es:

$\cdot$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

Luego los órdenes de los elementos son:
$o(1) = 1$; $o(5) = 6$; $o(7) = 3$; $o(11) = 6$; $o(13) = 3$; $o(17) = 2$.

Como existen dos elementos: 5 y 11, con orden igual a la cantidad de elementos del grupo $U(18)$, entonces $U(18)$ es cíclico (tanto 5 como 11 son generadores).