Lista 2.

1. Sea H un subgrupo de un grupo G. Pruebe que la relación sobre G de congruencia por la izquierda módulo H es una relación de equivalencia tal que para cada $a \in G$ su clase es la clase lateral izquierda aH.

Dem:

Definimos la relación de congruencia por la izquierda módulo H como sigue:

$$\forall a,b \in G, \quad a \equiv_I b \bmod H \Leftrightarrow a^{-1}b \in H$$

Probaremos que es relación de equivalencia:

i) $a \equiv_I a \bmod H \ \forall a \in G$.

Sea $a \in G$. Como $e = a^{-1}a$, y $e \in H$, entonces $a^{-1}a \in H \Rightarrow a \equiv_I a \bmod H$.

ii) $\forall a,b \in G \ \ni \ a \equiv_I b \bmod H \Rightarrow b \equiv_I a \bmod H$.

Sean $a,b \in G \ni a \equiv_I b \bmod H \Rightarrow a^{-1}b \in H$. Como H es subgrupo, entonces $(a^{-1}b)^{-1} \in H \Rightarrow b^{-1}a \in H \Rightarrow b \equiv_I a \bmod H$.

iii) $\forall a,b,c \in G \ni a \equiv_I b \bmod H$ y $b \equiv_I c \bmod H \Rightarrow a \equiv_I c \bmod H$.

Sean $a,b,c \in G \ni a \equiv_I b \bmod H$ y $b \equiv_I c \bmod H$, entonces $a^{-1}b \in H$ y $b^{-1}c \in H$, como H es subgrupo, entonces $(a^{-1}b)(b^{-1}c) = a^{-1}((bb^{-1})c) = a^{-1}c \in H \Rightarrow a \equiv_I c \bmod H$.

Por (i), (ii) y (iii), $\equiv_I \bmod H$ es relación de equivalencia.

Probaremos ahora que:

$$[a]_I = aH = \{ah \mid h \in H\}$$

En efecto:

$$x \in [a]_I \Leftrightarrow x \equiv_I a \bmod H \Leftrightarrow a \equiv_I x \bmod H \Leftrightarrow a^{-1}x \in H \Leftrightarrow \exists h \in H \ni a^{-1}x = h$$
$$\Leftrightarrow \exists h \in H \ni x = ah \Leftrightarrow x \in aH.$$

q.e.d.

2. Encuentre un grupo G el cual contenga un subgrupo H teniendo una infinidad (ó una cantidad finita) de clases laterales derechas módulo H.

Sol.

Tome $G=(\mathbb{Q}^*, \cdot)$ y como subgrupo a $H=\{-1,1\}$ con la operación de G.

H es subgrupo, en efecto:

a) $\forall\ a\in H,\ a^{-1}\in H$

Sea $a\in H$, entonces $a=1$ ó $a=-1$. Si $a=1 \Rightarrow a^{-1}=1 \Rightarrow a^{-1}\in H$.

Si $a=-1 \Rightarrow a^{-1}=-1 \Rightarrow a^{-1}\in H$

Luego $a^{-1}\in H$.

b) $\forall\ a,b\in H,\ ab^{-1}\in H$

$ab^{-1}=1$ ó $ab^{-1}=-1$, en cualquier caso, $ab^{-1}\in H$.

Por a) y b), $H<G$.

Veamos que: $\forall\ a\in G,\ Ha=\{ah \mid h\in H\}=\{a,-a\}$, luego G tiene una cantidad infinita de clases laterales derechas, pues $Ha=Hb \Leftrightarrow a=b^{-1}$ ó $a=b$. En efecto:

3. Encuentre un grupo G el cual contenga un subgrupo H y un elemento $a \in G$ tal que $Ha \neq bH$ para cada $b \in G$.

Sol.

4. Sea H un subconjunto no vacío de un grupo G. Definimos la relación sobre G: Para cada $a, b \in G$, $a \sim b$ si, y sólo si $ab^{-1} \in H$. Pruebe que $\sim$ es una relación de equivalencia sobre G si, y sólo si H es subgrupo de G.

Dem:

$\Rightarrow$) Suponga que $\sim$ es una rel. de equivalencia. Probaremos que H es subgrupo de G. Sean $a, b \in H$.

Como $a \sim a$, entonces $e = aa^{-1} \in H$. Además $ae^{-1} = ae = a \in H$, luego $a \sim e$. De manera similar, $b \sim e$. Por transitividad, $a \sim b$, luego $ab^{-1} \in H$.

Así, $H < G$.

$\Leftarrow$) Suponga que $H < G$.

i) Sea $a \in G$. Como $a^{-1} \in G$, entonces $e = a \cdot a^{-1} \in H$, por tanto, $a \sim a$.

ii) Sean $a, b \in G$, tales que $ab^{-1} \in H$, como $H < G$: $(ab^{-1})^{-1} = ba^{-1} \in H$, luego $b \sim a$.

iii) Sean $a, b, c \in G$ $\sqcap$ $a \sim b$ y $b \sim c$, entonces $ab^{-1} \in H$ y $bc^{-1} \in H$, luego $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$, así $a \sim c$.

Por (i), (ii) y (iii), $\sim$ es rel. de equivalencia.

q.e.d.

5. a) Sea $n \in \mathbb{N}$. Determine el índice $[\mathbb{Z} : n\mathbb{Z}]$.

   b) ¿Qué subgrupo de $\mathbb{Z}$ es $n\mathbb{Z} \cap m\mathbb{Z}$?

Sol.

De (i):

Como $\mathbb{Z}/n\mathbb{Z} = \{[m] \mid 0 \leq m < n\}$, entonces $[\mathbb{Z} : n\mathbb{Z}] = |\mathbb{Z}/n\mathbb{Z}| = n$.

De (ii):

$n\mathbb{Z} \cap m\mathbb{Z} = \{nq \mid q \in \mathbb{Z}\} \cap \{mq \mid q \in \mathbb{Z}\}$. Si $l = \text{mcm}\{m, n\}$, entonces $n\mathbb{Z} \cap m\mathbb{Z} = l\mathbb{Z}$.

6. Sea G un grupo y $a, b \in G$ tales que $a^5 = e$ y $aba^{-1} = b^2$. Calcule $|b|$.

7. Calcule todos los subgrupos del grupo 4-Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Sol.

Veamos que

$$
\begin{aligned}
b &= a^5 b (a^{-1})^5 \\
&= a^4 (a b a^{-1}) (a^{-1})^4 \\
&= a^4 b^2 (a^{-1})^4 \\
&= a^4 b a^{-1} a b (a^{-1})^4 \\
&= a^3 (b^2)(b^2)(a^{-1})^3 \\
&= a^3 b a^{-1} a b a^{-1} a b a^{-1} a b (a^{-1})^3 \\
&= a^2 b^2 b^2 b^2 b^2 (a^{-1})^2 \\
&= a^2 b^8 (a^{-1})^2 = a b^{16} a^{-1} = b^{32}
\end{aligned}
$$

$\Rightarrow e = b^{31}$, por tanto, $|b| = 31$. //

6. Sea G un grupo y $a, b \in G$ tales que $a^5 = e$ y $aba^{-1} = b^2$. Calcule $|b|$.

7. Calcule todos los subgrupos del grupo 4-Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

La tabla de multiplicación del grupo 4-Klein está dada por:

$\cdot$	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

Los subgrupos de este grupo son: $\{(0,0)\}, \{(0,0),(0,1)\}, \{(0,0),(1,0)\}, \{(0,0),(1,1)\}$ y el propio 4-Klein.

8. Sea G un grupo de orden $p^k m$ con p número primo y $(p,m) = 1$. Supóngase que existe un subgrupo H de G de orden p^k y un subgrupo K de G de orden p^d con $0 < d \leq k$ y $K \not\subseteq H$. Pruebe que HK no es subgrupo de G.

Dem:

Procederemos por reducción al absurdo. Suponga que $HK < G$. Por una proposición sabemos que:

$$|H| \cdot |K| = |H \cap K| \cdot |HK|$$

Como $|H| = p^k$ y $|K| = p^d$, entonces:

$$p^{K+d} = |H\cap K| \cdot |HK|$$

como $H\cap K < G$, pues $H\cap K < H$, entonces $|H\cap K| \mid |G|$, luego $\exists\ l \in \mathbb{N}$

$$|G| = l \cdot |H\cap K|$$

$$\Rightarrow p^K m = l \cdot |H\cap K|$$

veamos que, como $H\cap K < K$ (pues $H\cap K \leq K$), entonces $|H\cap K| \mid |K|$, así, como $|K| = p^d$, entonces $|H\cap K| = p^r$, donde $0 \leqslant r \leqslant d$. Como $K \not\subseteq H$, entonces $|H\cap K| < p^d$, pues $|H\cap K| < |K|$. Así, $0 \leqslant r < d$. Luego

$$p^K m = l \cdot p^r$$

$$\Rightarrow p^{K-d} m = l$$

Sustituyendo en lo anterior:

$$p^{K+d} = p^r \cdot |HK|$$

$$\Rightarrow p^{K+d-r} = |HK|$$

veamos que, $r < d \Rightarrow 0 < d-r \Rightarrow K+d-r > K$, luego $|HK| \nmid |G| = p^K m$, pues $(m,p)=1$. $\#_c$ Luego, $HK \not< G$.

Nota: se puede hacer la prueba directa.

q.e.d.

9. Sean H, K y N subgrupos de un grupo G tales que H es subgrupo de N. Pruebe que $HK\cap N = H(K\cap N)$.

Dem:

Probaremos la doble contención.

- $HK\cap N \subset H(K\cap N)$

  Sea $x \in HK\cap N$, entonces $\exists\ h\in H$ y $K \in K \ni x = hK \in N$. Como $H<N$, entonces $h\in N$, luego $K = h^{-1}(hK) \in N$, luego $K \in K\cap N$, así $x = hK \in H(K\cap N)$.

- $H(K\cap N) \subset HK\cap N$

  Sea $x \in H(K\cap N)$, entonces $\exists\ h\in H$ y $K\in K\cap N \ni x = hK$. Claramente $hK \in HK$, además, como $H \leq N$, entonces $h\in N$. Luego con $K\in N$, se sigue que $hK\in N$. Así

$x = hk \in HK \cap N.$

q.e.d.

10. Sean H, K y N subgrupos de un grupo G tales que H es subgrupo de K, $H \cap N = K \cap N$ y $HN = KN$. Pruebe que $H = K$.

Dem:

Probaremos la doble contención.

- $H \subseteq K$.

  Como $H < K$, entonces $H \subseteq K$.

- $K \subseteq H$

  Sea $x \in K$. Para $n \in N$ fijo arbitrario, tenemos que $xn \in KN = HN$, entonces $\exists$ $h_1 \in H$ y $n_1 \in N$ $\ni$ $xn = h_1 n_1 \Rightarrow h_1^{-1} x = n_1 n^{-1} \in N$. Como $H < K$, entonces $h_1 \in K \Rightarrow$ $h_1^{-1} x \in K$, luego $h_1^{-1} x \in N \cap K = N \cap H \Rightarrow h_1^{-1} x \in H \Rightarrow x = h_1 (h_1^{-1} x) \in H$.

por lo tanto, $H = K$.

q.e.d.

11. Pruebe que en todo campo finito F, todo elemento de F es suma de dos cuadrados. (Sugerencia: Use el Ejercicio 20 de la Lista de Grupos).

Dem:

12. Sean H y K subgrupos de un grupo G con índices en G de orden finito. Pruebe que el índice de $H \cap K$ en G es también de orden finito.

Dem:

Considere los conjuntos $G/_D H$, $G/_D K$, $G/_D H\cap K$, m

$$|G/_D H| = [G:H], |G/_D K| = [G:K] < \infty$$

probaremos que $|G/_D H\cap K| \leq |G/_D H| \cdot |G/_D K|$. Defina $f: G/_D H\cap K \to G/_D H \times G/_D K$, como sigue:

$$\forall \; g \in G, \; f((H\cap K)g) = (Hg, Kg)$$

probaremos que f está bien definida. Sean $g, b \in G$ m $b \in (H\cap K)g$. Entonces $\exists$ $h \in H\cap K$ m $b = hg$, entonces $b \in Hg$ y $b \in Kg$, luego $Hb = Hg$ y $Kb = Kg$. Así: $f((H\cap K)g) = f((H\cap K)b)$. Luego, f está bien definida.

Probaremos que f es inyectiva: en efecto, sean $(H\cap K)a, (H\cap K)b \in G/_D H\cap K$ m $f((H\cap K)a) = f((H\cap K)b)$. Entonces $Ha = Hb$ y $Ka = Kb$. Entonces $a = hb$ y $a = kb$, con $h \in H$ y $k \in K$. Así: $hb = kb \Rightarrow h = k$, luego $a = hb$, donde $h \in H\cap K$. Así $a \in (H\cap K)b \Rightarrow (H\cap K)a = (H\cap K)b$.

Por el teorema de Cantor-Bernstein: $[G:H\cap K] = |G/_D H\cap K| \leq |G/_D H| \cdot |G/_D K| = [G:H] \cdot [G:K]$, luego, como $[G:H], [G:K] < \infty$, se tiene que $[G:H\cap K]$ es finito.

q.e.d.

13. Sean H y K subgrupos de un grupo G tal que el índice de H en G es finito. Pruebe que $[K : H \cap K] \leq [G : H]$.

Dem:

Antes de probar el resultado, probaremos un resultado preliminar:

- $\forall \; k_1, k_2 \in K, \; k_1 H = k_2 H \Leftrightarrow k_1(H\cap K) = k_2(H\cap K)$

$\Rightarrow$) Sean $k_1, k_2 \in K$ m $k_1 H = k_2 H$. Probaremos la doble contención.

a) $k_1(H\cap K) \subseteq k_2(H\cap K)$.

Sea $x \in k_1(H\cap K)$, entonces $\exists$ $u \in H\cap K$ m $x = k_1 u \in k_1 H$, pues $u \in H$, así $x \in$

$K_2H \Rightarrow \exists\ l \in H \ m\ x = K_2 l = K_1 u$. Notemos que $l = K_2^{-1} \cdot K_1 \cdot u$, donde $K_1, K_2 \in K$ y $u \in K$, como $K < G \Rightarrow l \in K$, así $l \in H \cap K \Rightarrow x = K_2 l \in K_2(H \cap K)$.

b) $K_2(H \cap K) \subseteq K_1(H \cap K)$.

Es análoga a a).

$\Leftarrow$) Sean $K_1, K_2 \in K \ m\ K_1(H \cap K) = K_2(H \cap K)$. Probaremos la doble contención.

a) $K_1 H \subseteq K_2 H$.

Sea $x \in K_1 H$, entonces $\exists\ h \in H \ m\ x = K_1 h_1$. Como $K_1(H \cap K) = K_2(H \cap K)$ y $e \in H \cap K$, entonces $\exists\ h_0 \in H \cap K \ m\ K_1 = K_1 e = K_2 h_0 \Rightarrow h_0 = K_2^{-1} K_1 \in H$, así $h_0 h_1 = K_2^{-1} K_1 h_1 \in H \Rightarrow \exists\ h_2 \in H \ m\ h_2 = K_2^{-1} K_1 h_1 \Rightarrow x = K_1 h_1 = K_2 h_2 \in K_2 H$.

Por tanto, $K_1 H \subseteq K_2 H$.

b) $K_2 H \subseteq K_1 H$.

Es análogo a a).

q.e.d.

Sea $f: K/_I H \cap K \to G/_I H$, dada como sigue:

$$\forall\ a \in K,\ f(a(H \cap K)) = aH.$$

Probaremos que f está bien definida. Sean $a, b \in K \ m\ b \in a(H \cap K)$, entonces $b(H \cap K) = a(H \cap K)$, por lo demostrado anteriormente $bH = aH$. Así f está bien definida.

Probaremos que f es inyectiva. Sean $a, b \in K \ m\ f(a(H \cap K)) = f(b(H \cap K)) \Rightarrow aH = bH$, por lo probado anteriormente $a(H \cap K) = b(H \cap K)$. Así, f es inyectiva.

Luego, por el teorema de Cantor-Bernstein $[K : H \cap K] \leqslant [G : H]$.

q.e.d.

14. Sean H y K subgrupos de un grupo G tales que el índice de H en G y el índice de K en G son de orden finito. Pruebe que $[K : H \cap K] = [G : H]$ si, y sólo si $G = HK = KH$.

Dem:

$\Leftarrow$) Por 13, $[K : H \cap K] \leqslant [G : H]$. Retomando la f de ese ejercicio, probaremos que f es suprayectiva.

Sea $gH \in G/_{I}H$. Como $G = KH$, entonces $\exists\ k_1 \in K$ y $h_1 \in H \ni g = k_1 h_1$. Probaremos que $gH = k_1 H$.

Sea $x \in gH \Rightarrow \exists\ h_2 \in H \ni x = g h_2 = (k_1 h_1) h_2 = k_1 (h_1 h_2) \in k_1 H$.

Sea $x \in k_1 H \Rightarrow \exists\ h_2 \in H \ni x = k_1 h_2$, como $k_1 = g h_1^{-1}$, entonces $x = (g h_1^{-1}) h_2 = g(h_1^{-1} h_2) \in gH$.

Por lo anterior, $gH = k_1 H$. Entonces, $\exists\ k_1(H \cap K) \in K/_{I} H \cap K \ni$

$$f(k_1(H \cap K)) = k_1 H = gH$$

Luego, f es supráyectiva. Se sigue que f biyectiva, así

$$[K : H \cap K] = [G : H]$$

$\Rightarrow$) Probaremos que $G = KH$. Como $[K : H \cap K] = [G : H]$, entonces $\exists\ f : K/_{I} H \cap K \to G/_{I}H \ni f$ es biyectiva.

Probaremos la doble contención.

a) Sea $x \in G$. Como $xH \in G/_{I}H$ y f es supráyectiva, $\exists\ k_1 \in K \ni f(k_1(H \cap K)) = xH$.