Pauta Ayudantía 2 Estructuras Algebraicas

21 de marzo de 2023

Problema 1. Clasifique, módulo isomorfismo, todos los grupos de orden primo.

Indicación: Considere un elemento $x \in G$ grupo de orden primo y use el teorema de Lagrange en $\langle x \rangle$. Muestre que todo par de grupos cíclicos del mismo orden son isomorfos.

Demostración. Sea G un grupo de orden primo $|G| = p$ y $x \in G \setminus \{e\}$. Podemos considerar su subgrupo generado $\langle x \rangle \leq G$ y luego el teorema de Lagrange implica que $|\langle x \rangle| \overset{\text{def}}{=} \operatorname{ord}|x||p$ es un divisor de p, y como p es primo se sigue que $\operatorname{ord}(x) = 1$ o bien $\operatorname{ord}(x) = p$. Dado que $x \neq e$ entonces $\operatorname{ord}(x) = p$, es decir, x es un generador de G y por lo tanto es cíclico. De esta forma hemos deducido que todo grupo de orden primo es cíclico.
Veamos ahora que todo par de grupos cíclicos finitos del mismo orden son finitos. Sean G, H cíclicos de orden n y $g \in G, h \in H$ tales que $\langle g \rangle = G, \langle h \rangle = H$. Podemos definir entonces la función

$$\varphi : G \to H, \qquad g^n \mapsto h^n \qquad \forall n \in \mathbb{Z}$$

la cual es claramente una biyección pues los conjuntos subyacentes a los grupos G, H corresponden a:

$$G = \{e, g, g^2, \ldots, g^{n-1}\}, \qquad H = \{e, h, h^2, \ldots, h^{n-1}\}$$

Demostramos a continuación que esta función es un morfismo de grupos. Sean $g_1, g_2 \in G$. Como g es un generador de G existen $n_1, n_2 \in \mathbb{Z}$ tales que $g_1 = g^{n_1}, g_2 = g^{n_2}$ y entonces

$$\varphi(g_1 g_2) = \varphi(g^{n_1+n_2}) = h^{n_1+n_2} = h^{n_1} h^{n_2} = \varphi(g^{n_1})\varphi(g^{n_1}) = \varphi(g_1)\varphi(g_2)$$

Probamos así que todo par de grupos cíclicos del mismo orden son finitos y de esta forma existe un único grupo de orden primo para cada primo p, y corresponde a $\mathbb{Z}/p\mathbb{Z}$. □

Teorema (Pequeño teorema de Fermat)**.** *Si $p \in \mathbb{Z}$ es un número primo entonces $a^p \equiv a \pmod{p}$ para todo $a \in \mathbb{Z}$.*

Problema 2. Demuestre el pequeño teorema de Fermat utilizando el teorema de Lagrange en el grupo multiplicativo $(\mathbb{Z}/p\mathbb{Z})^\times$ con p primo.

Demostración. En la Ayudantía 1 Problema 5 se demostró que $m \in (\mathbb{Z}/p\mathbb{Z})^\times$ si y sólo si $\operatorname{mcd}(m, p) = 1$, y dado que en este caso estamos considerando p primo es claro que entero $1 \leq m < p$ será invertible módulo p, es decir, $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, \ldots, p\}$ y por lo tanto $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$. Si $a \in \mathbb{Z}/p\mathbb{Z}$ entonces por el teorema de Lagrange tenemos que $\operatorname{ord}(a)|(p-1)$ y entonces $a^{p-1} = 1$ en $\mathbb{Z}/p\mathbb{Z}$, y multiplicando por a tenemos $a^p = a$ en $\mathbb{Z}/p\mathbb{Z}$. □

Problema 3. Sea G un grupo y $H \trianglelefteq G$ un subgrupo normal. Demuestre que:

1. Si G es de tipo finito (o finitamente generado) entonces G/H es de tipo finito.
2. Si H y G/H son de tipo finito, entonces G es de tipo finito.

Demostración.

1. Sea G un grupo de tipo finito, es decir, existe un conjunto finito $A \subseteq G$ tal que $\langle A \rangle = G$ y consideremos $[g] \in G/H$ un elemento en el cociente. Dado que A es generador de G tenemos que existen $g_1, \ldots, g_m \in A$, $n_1, \ldots, n_m \in \mathbb{Z}$ tales que

$$g = g_1^{n_1} g_2^{n_2} \cdots g_n^{n_m} \quad \Rightarrow \quad [g] = [g_1^{n_1}][g_2^{n_2}] \cdots [g_n^{n_m}]$$

y de la última igualdad tenemos entonces que $p(A)$ es un conjunto generador de G/H, donde $p : G \to G/H$ denota la proyección al cociente.

2. Sea H subgrupo normal de G tal que H y G/H son de tipo finito. existe entonces $A \subseteq G$ finito tal que $\langle p(A) \rangle = G/H$ y un conjunto finito $B \subseteq H$ tal que $\langle B \rangle = H$. Sea $g \in G$. Por hipótesis existen $[g_1], \ldots, [g_m] \in p(A), n_1, \ldots, n_m \in \mathbb{Z}$ tales que

$$[g] = [g_1^{n_1}][g_2^{n_2}] \cdots [g_n^{n_m}]$$

y multiplicando por los inversos de los elementos de A tenemos

$$[g_n^{-n_m}] \cdots [g_1^{-n_1}][g] = [e]$$

es decir, $g_n^{-n_m} \cdots g_1^{-n_1} g \in H$. Ahora, como B es generador de H existen a su vez $h_1, \ldots, h_k \in H, s_1, \ldots, s_k \in \mathbb{Z}$ tales que

$$g_n^{-n_m} \cdots g_1^{-n_1} g = h_1^{s_1} \cdots h_k^{s_k}$$

y multplicando de vuelta por los elementos de A tenemos que

$$g = g_1^{n_1} \cdots g_n^{n_m} h_1^{s_1} \cdots h_k^{s_k}$$

Deducimos así que el conjunto finito $A \cup B$ genera G y en consecuencia es de tipo finito.

□

Problema 4. Sea G un grupo, $H \trianglelefteq G$ subgrupo normal y $K \leq G$ subgrupo.

1. Muestre que si K es también normal en G y $K \leq H$, entonces se tiene un isomorfismo $(G/K)/(H/K) \cong G/H$.
2. Muestre que HK es un subgrupo de G y que $HK = KH$.
3. Demuestre que H es normal en HK y que $K/(K \cap H) \cong (HK)/H$.

Demostración.

1. Definimos la aplicación

$$\varphi : G/K \to G/H, \qquad gK \mapsto gH$$

y veamos en primer lugar que está aplicación está bien definida, es decir, que la clase lateral en G/H está únicamente determinada por su clase en G/K. Sean entonces $g_1, g_2 \in G$ tales que $g_1 K = g_2 K$. Entonces

$$g_1 K = g_2 K \quad \Rightarrow \quad g_2^{-1} g_2 \in K \quad \underbrace{\Rightarrow}_{K \leq H} \quad g_2^{-1} g_1 H = H \Rightarrow \varphi(g_1 K) = \varphi(g_2 K)$$

Veamos ahora que es un morfismo de grupos:

$$\varphi(g_1 K)\varphi(g_2 K) = (g_1 H)(g_2 H) = (g_1 g_2) H = \varphi(g_1 g_2 K)$$

en donde hemos utilizado únicamente la estructura de grupo del cociente. Es evidente que φ es sobreyectivo pues si $gH \in G/H$ entonces $g \in G$ es tal que $\varphi(gK) = gH$. Ahora, notemos que

$$\begin{aligned}\ker(\varphi) &= \{gK \in G/K | \varphi(gK) = e_{G/H}\} \\ &= \{gK \in G/H | gH = H\} \\ &= \{\{gK \in G | g \in H\} \\ &= H/K\end{aligned}$$

Así, la propiedad universal del cociente nos asegura la existencia del isomorfismo deseado, el cual viene dado explícitamente por $\overline{\varphi} : (G/K)/(H/K) \to G/H, (gK)(H/K) \mapsto gH$.

2. Sean $g_1, g_2 \in HK$, es decir, existen $h_1, h_2 \in H, k_1, k_2 \in K$ tales que $g_1 = h_1k_1, g_2 = h_2k_2$, y usando la normalidad de H vemos que

$$g_1g_2 = h_1k_1h_2k_2 = h_1k_1h_2(k_1^{-1}k_1)k_2 = h_1 \underbrace{(k_1h_2k_1^{-1})}_{=:h' \in H} k_1k_2 = (h_1h')(k_1k_2) \in HK$$

De manera similar, si $g = hk \in HK$ entonces por normalidad de H

$$g^{-1} = (hk)^{-1} = k^{-1}h^{-1} = k^{-1}h^{-1}(kk^{-1}) = \underbrace{(k^{-1}h^{-1}k)}_{=:h' \in H} k^{-1} = h'k^{-1} \in HK$$

Usando argumentos similares a los anteriores tenemos que $\exists h' \in H$ tal que $hk = kh'$, así que $HK \subseteq KH$ y análogamente se prueba que $KH \subseteq HK$.

3. El hecho que $H \trianglelefteq HK$ es evidente pues H es normal en G así que en particular lo será cualquier subgrupo que lo contenga. Podemos definir el morfismo de inclusión $i : K \to HK, k \mapsto k$ y la proyección al cociente $p : HK \to (HK)/H$ puesto que como H es normal en HK el conjunto $(HK)/H$ posee una única estructura de grupo tal que p es un morfismo. Componiendo tenemos un morfismo $\varphi = p \circ i : K \to (HK)/H$, el cual es sobreyectivo. En efecto, si $(hk)H \in (HK)/H$ entonces por normalidad de H

$$(hk)H = \{hkh' | h' \in H\} = \{kh'' | h'' \in H\} = kH$$

así que $\varphi(k) = (hk)H$.
Finalmente, vemos que el kernel de φ está dado por

$$\ker(\varphi) = \{k \in K | kH = H\} = \{k \in K | k \in H\} = H \cap K$$

La conclusión se sigue de la propiedad universal del cociente. Note que no es necesario verificar que $K \cap H$ es normal en K puesto que es el kernel de la aplicación.

□

Problema 5. Sea G grupo finito y H, K subgrupos de G con H normal y tales que $|K|$ y $[G : H]$ son primos relativos. Demuestre que K está contenido en H.

Demostración. Considerar el subgrupo $HK/H \leq G/H$. El teorema de Lagrange implica que $|HK/H|$ divide a $[G : H] := |G/H|$. Ahora, por el Problema 4. tenemos que $HK/H \cong K/(K \cap H)$ y luego por Lagrange:

$$|K| = |K \cap H|[K : K \cap H] \Rightarrow |HK/H| \text{ divide a } |K|$$

y de esta manera vemos que $|HK/H|$ es divisor común de $|K|$ y $[G : H]$, y dado que estos son relativamente primos tenemos que $HK = H \Rightarrow K \leq H$. □