Algebra II (Doble grado Informática-Matemáticas)

18 de marzo de 2020

1. Tema 4: Grupos cocientes. Teoremas de isomorfía.

CONSTRUCCIÓN DEL GRUPO COCIENTE

Sea N un subgrupo NORMAL de un grupo G y consideremos el conjunto

$$G/N = \{aN/a \in G\}$$

de las clases laterales a izquierda módulo N. Dados dos elementos $aN, bN \in G/N$ definimos su producto por:

$$(aN)(bN) := (ab)N \tag{1.1}$$

Veamos que esta operación **está bien definida**, esto es, no depende del representate elegido en cada clase. En efecto supongamos que $aN = a_1N$ y que $bN = b_1N$ entonces

$$\begin{cases} aN = a_1N \Rightarrow (a_1)^{-1}a \in N \Rightarrow \exists n \in N \text{ tal que } a = a_1n \\ bN = b_1N \Rightarrow (b_1)^{-1}b \in N \Rightarrow \exists m \in N \text{ tal que } b = b_1m \end{cases}$$

Consideramos el elemento $nb_1 \in Nb_1$, como N es normal tenemos

$$nb_1 \in Nb_1 = b_1N \;\Rightarrow\; \exists n' \in N \text{ tal que } nb_1 = b_1n',$$

y entonces

$$ab = (a_1n)(b_1m) = a_1(nb_1)m = a_1(b_1n')m = (a_1b_1)n'm \text{ con } n'm \in N$$

consecuentemente

$$(ab)N = (a_1b_1)N$$

y la operación está bien definida.

El producto (1.1) define entonces una operación interna en el conjunto G/N que claramente es asociativa, tiene un elemento neutro o unidad que es la clase del 1, $1N = N$ (pues $(aN)(1N) = aN = (1N)(aN)$) y toda clase aN tiene una inversa para este producto que es $(aN)^{-1} = a^{-1}N$ (pues $(aN)(a^{-1}N) = (aa^{-1})N = 1N = N$). Hemos construido un nuevo grupo que nos lleva a la siguiente definición:

Definición 1.1. *Si N es un subgrupo normal de un grupo G, el conjunto de clases laterales a izquierda módulo N, G/N dotado de la estructura de grupo dada por (1.1), se llama el GRUPO COCIENTE de G por N. La aplicación*

$$p : G \to G/N, \; a \mapsto aN,$$

que aplica cada elemento del grupo en su clase, es un epimorfismo de grupos llamado LA PROYECCIÓN CANÓNICA de G sobre el grupo cociente G/N.

Observación 1.2. Notemos que si el subgrupo no es normal no tenemos asegurado que la operación (1.1) esté bien definida. Por ejemplo, consideremos el grupo diédrico $D_3 = \{1, r, r^2, s, rs, r^2s\}$ y el subgrupo $H = \{1, s\}$ que no es normal en D_3 (pues $rH = \{r, rs\} \neq Hr = \{r, r^2s\}$). El conjunto G/H tiene 3 clases (pues $[G : H] = 3$) que son $1H = H = \{1, s\}$, $rH = \{r, rs\}$ y $r^2H = \{r^2, r^2s\}$ tenemos que

$$(rH)(r^2H) = (\{r, rs\})(\{r^2, r^2s\}) = \{1, s, r^2s, r^2\}$$

que no es ninguna clase módulo H

Nos disponemos a continuación a demostrar los teoremas de isomorfía. Para ello es fundamental el resultado siguiente:

Teorema 1.3. *Sea $N \trianglelefteq G$ un subgrupo normal de un grupo G. Supongamos $f : G \to G'$ un homomorfismo de grupos tal que $N \leq Ker(f)$. Entonces*

(1) Existe un único homomorfismo de grupos

$$\bar{f} : G/N \to G'$$

tal que el diagrama

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "p"'] & G' \\ G/N \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

es conmutativo. Esto es $\bar{f} \circ p = f$.

Este homomorfismo $\bar{f}$ se llama EL HOMOMORFISMO INDUCIDO POR f EN EL COCIENTE.

(2) $\bar{f}$ es epimorfismo si y sólo si f es epimorfismo.

(2) $\bar{f}$ es monomorfismo si y sólo si $N = Ker(f)$.

Demostración. Veamos (1): Definimos

$$\bar{f} : G/N \to G' \text{ por } \bar{f}(aN) := f(a).$$

Supongamos que $aN = bN$ entonces $b^{-1}a \in N$. Por hipótesis $N \leq Ker(f)$ con lo que $1 = f(b^{-1}a) = f(b)^{-1}f(a) \;\Rightarrow f(a) = f(b)$. Por tanto $\bar{f}$ está bien definido pues no depende del representante elegido. Puesto que

$$\bar{f}(aN\,bN) = \bar{f}(abN) = f(ab) = f(a)f(b) = \bar{f}(aN)\bar{f}(bN),$$

tenermos que $\bar{f}$ es un homomorfismo de grupos. Claramente se tiene que $\bar{f}p = f$.

Veamos la unicidad. Sea $h : G/N \to G'$ otro homomorfismo tal que $h \circ p = f$, entonces para todo $aN \in G/N$ tenemos

$$h(aN) = (h \circ p)(a) = f(a) = \bar{f}(aN).$$

Esto es $h = \bar{f}$.
Veamos (2): Puesto que

$$Img(\bar{f}) = \{\bar{f}(aN)/aN \in G/N\} = \{\bar{f}(aN)/a \in G\} = \{f(a)/a \in G\} = Img(f),$$

entonces

$\bar{f}$ es un epimorfismo $\Leftrightarrow$ $Img(\bar{f}) = G'$ $\Leftrightarrow$ $Img(f) = G'$ $\Leftrightarrow$ f es un epimorfismo.

Finalmente, veamos (3): $\Rightarrow$) Supongamos que $\bar{f}$ es un momonorfismo, entonces su núcleo está únicamente formado por el uno de G/N, esto es $Ker(\bar{f}) = \{N\}$.
Sea $a \in Ker(f)$ entonces $1 = f(a) = f(aN)$ con lo que $aN \in Ker(\bar{f}) \Rightarrow aN = N \Rightarrow a \in N$. Consecuentemente $Ker(f) \leq N$, y como por hipótesis $N \leq Ker(f)$ se tiene que $N = Ker(f)$.
$\Leftarrow$) Recíprocamente, supongamos que $N = ker(f)$ y sea $aN \in Ker(\bar{f})$, entonces $\bar{f}(aN) = f(a) = 1$, con lo que $a \in Ker(f) \Rightarrow a \in N \Rightarrow aN = N$. Luego $Ker(\bar{f}) = \{N\}$ y $\bar{f}$ es un monomorfismo. □

Como corolario al teorema anterior deducimos el primer teorema de isomorfía:

Teorema 1.4. *(PRIMER TEOREMA DE ISOMORFÍA). Cada homomorfismo de grupos $f : G \to G'$ induce un isomorfismo de grupos*

$$G/Ker(f) \overset{\bar{f}}{\cong} Img(f), \quad aKer(f) \mapsto f(a).$$

Demostración. Consideramos $f : G \to Img(f)$ que es un epimorfismo y tomamos $N = Ker(f)$. Entonces por el teorema anterior, el homomorfismo inducido por f en el cociente

$$\bar{f} : G/Ker(f) \to Img(f)$$

es un isomorfismo. □

Este primer teorema de isomorfía es fundamental para la demostración de los demás teoremas de isomorfía que vamos a ver.
En el caso de grupos finitos, na primera consecuencia del primer teorema de isomorfía es

Corolario 1.5. *Sean G y G' grupos finitos y $f : G \to G'$ un homomorfismo entre ellos. Entonces*

$$|G| = |Ker|\,|Img(f)|.$$

Demostración. En efecto, por el teorema de Langrange sabemos que

$$|G| = |ker(f)|\,[G : Ker(f)] = |Ker(f)|\,|G/Ker(f)|$$

Como $G/Ker(f) \cong Img(f)$ entonces tienen el mismo orden, con lo que

$$|G| = |ker(f)|\,|Img(f)|.$$

□

Ejercicio. Ejercicio 12. Relación 3. Sean G y H dos grupos cuyos órdenes sean primos relativos. Probar que si $f : G \to H$ es un homomorfismo, entonces necesariamente $f(x) = 1$ para todo $x \in G$, es decir, que el único homomorfismo entre ellos es el trivial.

Resolución. En efecto, como

$$\begin{cases} |G| = |Ker|\,|Img(f) \Rightarrow |Img(f)| \text{ es un divisor de } |G|, \\ Img(f) \leq H \Rightarrow |Img(f)| \text{ es un divisor de } |H|, \end{cases}$$

entonces, como $|G|$ y $|H|$ son primos relativos, necesariamente $|Img(f)| = 1$ con lo que $\{1\} = Img(f)$, esto es $f(x) = 1$ para todo $x \in G$.