Algebra II (Doble grado Informática-Matemáticas)

23 de marzo de 2020

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

Continuamos en esta clase con el Tema 4 del programa. Nos ocupamos ahora de estudiar los subgrupos del grupo cociente y, particularmente a obtener el "segundo teorema de isomorfía", que nos ayuda a describir los cocientes de los grupos cocientes.

Proposición 1.1. *Sea $N \trianglelefteq G$ un subgrupo normal de un grupo G. Entonces:*

(1) *Si $H \in Sub(G)$ es cualquier subgrupo tal que $N \leq H$, entonces $N \trianglelefteq H$ y H/N es un subgrupo de G/N.*

(2) *Sean $H_1, H_2 \in Sub(G)$, con $N \leq H_i$, $i = 1, 2$, entonces*

$$H_1/N = H_2/N \Longleftrightarrow H_1 = H_2.$$

(3) *Sea $L \leq G/N$ un subgrupo del grupo cociente. Entonces existe un único subgrupo $H \leq G$ tal que $N \leq H$ y $L = H/N$.*

Como consecuencia de las afirmaciones anteriores tenemos que

$$Sub(G/N) = \{H/N \text{ con } N \leq H \leq G\},$$

esto es, los subgrupos del grupo cociente G/N son de la forma H/N con $N \leq H \leq G$.

Demostración. Puesto que para todo $a \in G$ se tiene $aNa^{-1} = N$, entonces también se tendrá la igualdad para todo $a \in H$ y por tanto $N \trianglelefteq H$. Podemos considerar entonces el cociente H/N que es claro que es un subgrupo de G/N. Tenemos así (1).
Veamos (2): Supongamos que $H_1/N = H_2/N$ y sea $a \in H_1$, entonces

$$aN \in H_1/N = H_2/N \Rightarrow \exists b \in H_2 \text{ tal que } aN = bN$$
$$\Rightarrow b^{-1}a \in N \leq H_2 \Rightarrow a = b(b^{-1}a) \in H_2, \Rightarrow a \in H_2$$

Consecuentemente $H_1 \leq H_2$. De forma análoga se demuestra que $H_2 \leq H_1$ y se tiene la implicación hacia la derecha. Es obvio que se verifica la implicación hacia la izquierda y por tanto se tiene (2).

Veamos (3): Consideremos el homomorfismo de proyección canónica $p : G \to G/N$ (que recordemos está definido por $p(a) = aN$) y sea $L \leq G/N$. Sabemos entonces que $H := p^*(L) = \{a \in G/p(a) \in L\} = \{a \in G/aN \in L\}$ es un subgrupo de G.

Veamos que este este es el subgrupo de G buscado. En efecto, si $a \in N$ entonces $p(a) = aN = N \in L$ (pues si $L \leq G/N$ entonces ha de contener al uno del grupo) y entonces $a \in H$. Consecuentemente, $N \leq H$ y es claro que $L = H/N$.

La unicidad de H es consecuencia directa de (2). □

Podemos ya demostrar el segundo teorema de isomorfía que nos dice quiénes son los subgrupos normales de G/N:

Teorema 1.2. *(SEGUNDO TEOREMA DE ISOMORFÍA O DEL DOBLE COCIENTE)*
Sea $N \trianglelefteq G$ un subgrupo normal de un grupo G y $H/N \leq G/N$, donde $N \leq H \leq G$. Entonces

$$H/N \trianglelefteq G/N \iff H \trianglelefteq G,$$

y en tal caso hay un isomorfismo

$$(G/N)/(H/N) \cong G/H, \quad \textit{dado por } \; aN(H/N) \mapsto aH.$$

Demostración. Supongamos que $H \trianglelefteq G$, entonces para cualesquiera $a \in G$ y $b \in H$ se tiene que $ab^{-1}a \in aHa^{-1} = H$, y entonces

$$(aN)(bN)(aN)^{-1} = (aba^{-1})N \in H/N,$$

lo que nos dice que $H/N \trianglelefteq G/N$.

Recíprocamente, supongamos que $H/N \trianglelefteq G/N$. Podemos entonces considerar el correspondiente grupo cociente $(G/N)/(H/N)$. Sea $f : G \to (G/N)/(H/N)$ el homomorfismo obtenido al componer las proyecciones canónicas:

$$f : G \to G/N \to (G/N)/(H/N), \; a \mapsto aN(H/N).$$

Como las proyecciones canónicas son epimorfismo, entonces f es también epimorfismo (por ser composición de epimorfismos), es decir

$$Img(f) = (G/N)/(H/N).$$

Por otro lado, su núcleo $Ker(f) = \{a \in G/f(a) = H/N\} = \{a \in G/N/aN \in H/N\}$ y entonces es claro que $H \leq Ker(f)$. Por otro lado, si $a \in Ker(f)$ entonces $aN \in H/N$ y existirá $h \in H$ tal que $aN = hN \Rightarrow h^{-1}a \in N \leq H \Rightarrow a = h(h^{-1}a) \in H$. Esto es $Ker(f) \leq H$ y la doble inclusión deducimos entonces

$$H = Ker(f).$$

Como el núcleo de un homomorfismo es siempre un subgrupo normal del dominio (véase Ejemplo 1.4 de la clase del 17-marzo-2020), tenemos que

$$H \trianglelefteq G,$$

y aplicando el primer teorema de isomorfía al homomorfismo f, concluimos que

$$G/H \cong (G/N)/(H/N),$$

como queríamos demostrar.

□

Teorema 1.3. *(TERCER TEOREMA DE ISOMORFÍA).*
Sea G un grupo y H, K subgrupos de G con $H \trianglelefteq G$. Entonces:

(1) *El conjunto KH es un subgrupo de G y $H \trianglelefteq KH$.*

(2) *$H \cap K \trianglelefteq K$.*

(3) *Existe un isomorfismo*

$$K/H \cap K \cong KH/H.$$

Demostración. Veamos (1): Recordemos que $KH := \{kh/k \in K, h \in H\}$ y que si $KH = HK$ entonces este conjunto es un subgrupo de G. Como H es un subgrupo normal de G entonces $kH = Hk$, para todo $k \in K$, con lo que $KH = HK$ y KH es un subgrupo de G.

Como $H \trianglelefteq G$ y $H \leq KH$, entonces también es $H \trianglelefteq KH$ y se tiene (1)

Denotemos por $g : K \to G$ el homomorfismo inclusión, esto es dado por $g(k) = k$, $k \in K$. Sea $p : G \to G/H$ la proyección canónca y consideremos la composición

$$K \xrightarrow{g} G \xrightarrow{p} G/H,\ k \mapsto kH.$$

Entonces

$$Ker(pg) = \{k \in K/(pg)(k) = H\} = \{k \in K/kH = H\} = \{k \in K/k \in H\} = K \cap H,$$

con lo que $K \cap H \trianglelefteq K$ (recuérdese que el núcleo de un homomorfismo es un subgrupo normal del dominio) y se tiene (2).

Finalmente, para ver (3) aplicamos el primer teorema de isomorfía al homomorfismo pg, entonces como $Ker(pg) = K \cap H$, tendremos que

$$K/K \cap H \cong Img(pg).$$

Veamos que $Img(pg)) = KH/H$: En efecto, $Img(pg) = \{(pg)(k)/k \in K\} = \{kH/k \in K\}$, y entonces, puesto que $K \leq KH$, es claro que $Img(pg) \leq KH/H$. Recíprocramente, un elemento de KH/K será la clase xH de un elemento $x \in KH$. Sea $k \in K$ y $h \in H$ tal que $x = kh$, entonces

$$xH = (kh)H = (kH)(hH) = (kH)H = kH \in Img(pg),$$

consecuentemente, $KH/H \leq Img(pg)$ y de la doble inclusión tenemos que $Img(pg) = KH/H$ y también el isomorfismo en (3).

□

Dedicaremos el resto de la clase a hacer algunos ejercicios de la relación 4.

Comenzaremos con un par de ejercicios de aplicación de los teoremas de isomorfía.

Ejercicio. (Ejercicio 14. Relación 3). Sea N un subgrupo normal de G tal que N y G/N son abelianos. Sea H un subgrupo cualquiera de G. Demostrar que existe un subgrupo normal $K \trianglelefteq H$ tal que K y H/K son abelianos.

Resolución. En efecto, tomamos como $K = H \cap N$, entonces, por el tercer teorema de isomorfía aplicado a H y $N \trianglelefteq G$, sabemos que $K \trianglelefteq H$: Además como $K \leq N$ y N es abeliano, entonces también lo es K.

Por otro lado, aplicando de nuevo el tercer teorema de isomorfía, $H/K = H/H \cap N \cong HN/N$ y entonces H/K es isomorfo a un subgrupo de G/N con lo que por ser éste último abeliano, también lo es cualquier subgrupo suyo. Consecuentemente H/K es también abeliano.

Ejercicio. (Ejercicio 15. Relación 3) Sea G un grupo finito, y sean H, K subgrupos de G, con H normal y tales que $|K|$ y $[G : H]$ son primos relativos. Demostrar que K está contenido en H.

Resolución. Puesto que estamos en las hipótesis del tercer teorema de isomorfía, entonces será $K/H \cap K \cong KH/H$, con lo que $|KH/H| = |K/H \cap K| = [K : H \cap K]$ y, como por el teorema de Langrange, $[K : H \cap K]$ es un divisor del orden de K, tendremos que $|KH/H|$ es un divisor de $|K|$.

Por otro lado, considerando $H \leq KH \leq G$, haciendo uso del Ejercicio 13 de la Relación 2, tendremos que $[G :: H] = [G : KH][KH : H]$, con lo que $|KH/H| = [KH : H]$ es un divisor de $[G : H]$.

Por hipótesis, $|K|$ y $[G : H]$ son primos relativos, con lo que $|KH/H| = 1$, esto es (de nuevo haciendo uso del Ejercicio 13 de la Relación 2) $KH = H$ y entonces $K \leq H$, como queríamos demostrar.

Nos ocupamos ahora de hacer algunos ejercicios de la relación 3 relativos al centro de un grupo.

Ejercicio. (Ejercicio 6. Relación 3)

Resolución. En este ejercicio se introduce el **centro** de un grupo G como

$$Z(G) = \{a \in G / ax = xa, \forall x \in G\}.$$

Esto es $Z(G)$ consiste de aquellos elementos de G que conmutan con todos los elementos de G.

Es claro que $Z(G) \neq \emptyset$ pues $1 \in Z(G)$. Es fácil ver que $Z(G)$ es un subgrupo normal de G (apartados 1 y 2) así como que $Z(G) = G \Leftrightarrow G$ es abeliano (apartado 3).

Veamos el apartado 4 que dice: Demostrar que si $G/Z(G)$ es cíclico entonces G es abeliano:

En efecto, supongamos que $G/Z(G)$ es cíclico, entonces existirá $aZ(G) \in G/Z(G)$, tal que $G/Z(G) = \langle aZ(G) \rangle$.

Sean $x, y \in G$ dos elementos arbitrarios de G. Considerando $xZ(G), yZ(G) \in G/Z(G)$, tendremos que

$$\begin{cases} \exists n \in \mathbb{Z} \text{ tal que } xZ(G) = (aZ(G))^n = a^n Z(G) \Rightarrow x = a^n z \text{ para algún } z \in Z(G) \\ \exists m \in \mathbb{Z} \text{ tal que } yZ(G) = (aZ(G))^m = a^m Z(G) \Rightarrow y = a^m z' \text{ para algún } z' \in Z(G), \end{cases}$$

entonces

$$xy = a^n z a^m z' \overset{(*)}{=} a^n a^m zz' = a^{n+m} zz' = a^m a^n zz' \overset{(*)}{=} a^m z' a^n z = yx,$$

donde en las identidades $(*)$, hemos utilizado que z y z' son elementos de $Z(G)$ y por tanto conmutan con cualquier elemento de G. Tenemos pues que $xy = yx$ para cualesquiera $x, y \in G$, es decir G es abeliano.

Calculamos ahora el centro de los grupos simétricos, los grupos alternados y los grupos diédricos.

Ejercicio. (Ejercicio 8. Relación 3.)

1. Demostrar que $Z(S_2) = S_2$ y que $Z(S_n)$ es trivial si $n \geq 3$.
2. Demostrar que $Z(A_3) = A_3$ y que $Z(A_n)$ es trivial si $n \geq 4$.

Resolución. !.- Puesto que S_2 es un grupo abeliano, la primera afirmación es clara. Sea $n \geq 3$ y $\sigma \in S_n$ con $\sigma \neq id$, entonces existirá $i \in \{1, 2, \ldots, n\}$ tal que $\sigma(i) = j \neq i$. Elegimos $k \in \{1, 2, \ldots, n\}$ con $k \neq i, j$ (notemos que puesto que $n \geq 3$ siempre podemos elegir tal k) y sea $\tau = (j\ k)$, entonces

$$\begin{cases} (\sigma\tau)(i) = \sigma(i) = j \\ (\tau\sigma)(i) = \tau(j) = k \end{cases} \Longrightarrow (\sigma\tau)(i) \neq (\tau\sigma)(i),$$

consecuentemente $\sigma \notin Z(S_n)$ y por tanto $Z(S_n) = \{id\}$.

!.- Puesto que A_3 es un grupo abeliano, la primera afirmación es clara. Sea $n \geq 4$ y $\sigma \in A_n$ con $\sigma \neq id$, entonces existirá $i \in \{1, 2, \ldots, n\}$ tal que $\sigma(i) = j \neq i$. Elegimos $k, l \in \{1, 2, \ldots, n\}$ con $k \neq l$ y $k, l \neq i, j$ (notemos que puesto que $n \geq 4$ siempre podemos elegir tales k, l) y sea $\alpha = (j\ k\ l) \in A_n$, entonces

$$\begin{cases} (\sigma\alpha)(i) = \sigma(i) = j \\ (\alpha\sigma)(i) = \alpha(j) = k \end{cases} \Longrightarrow (\sigma\alpha)(i) \neq (\alpha\sigma)(i),$$

consecuentemente $\sigma \notin Z(A_n)$ y por tanto $Z(A_n) = \{id\}$.

Ejercicio. (Eercicio 9. Relación 3) Demostrar que $Z(D_n) = \{1, r^m\}$ si $n = 2m$ y que $Z(D_n)$ es trivial si $n = 2m + 1$.

Resolución. Sabemos que

$$D_n = \langle r, s / r^n = 1 = s^2, sr = r^{-1}s \rangle = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}.$$

En primer lugar veamos que

(a) $r^k s \notin Z(D_n)$ para todo $0 \leq k \leq n-1$

En efecto, supongamos que para algún k, $r^k s \in Z(D_n)$, entonces dicho elemento conmuta con todos los elementos de D_n, en particular con el generador r, pero entonces tendríamos:

$$r(r^k s) = (r^k s)r \Rightarrow r^{k+1}s = r^{k-1}s \Rightarrow r^{k+1} = r^{k-1} \Rightarrow r = r^{-1} \Rightarrow r^2 = 1,$$

llegaríamos entonces a que $ord(r) = 2$ lo cual es una contradicción pues $ord(r) = n \geq 3$.

Nos ocupamos ahora de los elementos de la forma r^k, $0 \leq k \leq n-1$.

Para $k = 0$, $r^0 = 1 \in Z(G)$.

Sea $1 \leq k \leq n-1$. Es obvio que r^k conmuta con los elementos de la forma r^j, $0 \leq j \leq n-1$. Entonces

$$r^k \in Z(D_n) \Longleftrightarrow r^k(r^j s) = (r^j s)r^k,\ \forall 0 \leq j \leq n-1, \Longleftrightarrow r^k s = sr^k,$$

y como $sr^k = r^{-k}s$,

$$r^k \in Z(D_n) \Longleftrightarrow r^k = r^{-k} \Longleftrightarrow (r^k)^2 = 1 \Longleftrightarrow ord(r^k) = 2.$$

Sabemos que $ord(r^k) = \frac{n}{\text{m.c.d.}(k,n)}$ y entonces

$$r^k \in Z(D_n) \Longleftrightarrow n = 2\,\text{m. c. d.}(k,n),$$

con lo que,

(b) si $n = 2m+1$ entonces $r^k \notin Z(D_n)$ para todo $1 \leq k \leq n-1$.

Entonces , utilizando (a) y (b), concluimos que

$$Z(D_{2m+1}) = \{1\}.$$

Supongamos $n = 2m$ entonces

$$2m = 2\,\text{m. c. d.}(k,2m) \Longleftrightarrow m = \text{m. c. d.}(k,2m) \Longleftrightarrow k = m,$$

con lo que utilizando (a), concluimos que

$$Z(D_{2m}) = \{1, r^m\}.$$

Los ejercicios desde el 16 al 20 de la Relación 3 tienen que ver con el grupo de automorfismos de un grupo que definimos a continuación.

Definición 1.4. *Sea G un grupo. Un* **automorfismo** *de G es un homomorfismo $f : G \to G$ que es isomorfismo. Denotaremos por*

$$Aut(G) = \{f : G \to G / f \text{ es automorfismo}\}.$$

Es claro que $Aut(G)$ es un grupo con operación dada por la composición

El ejercicio siguiente nos da una descripción completa del grupo de automorfismos de un grupo cíclico finito:

Ejercicio. (Ejercicio 18. Relación 3) Sea G un grupo y sea $C_n = \langle x | x^n = 1\rangle$ el grupo cíclico de orden n. Demostrar que:

1. Si $\theta : C_n \to G$ es un homomorfismo de grupos, con $\theta(x) = g$, entonces $ord(g)|n$, y $\theta(x^k) = g^k \ \forall k \in \{0, \ldots, n-1\}$.
2. Para cada $g \in G$ tal que $ord(g)|n$, existe un único homomorfismo de grupos $\theta_g : C_n \to G$ tal que $\theta_g(x) = g$.
3. Si $g \in G$ es tal que $ord(g)|n$, entonces el morfismo θ_g es monomorfismo si, y sólo si, $ord(g) = n$.
4. Existe un isomorfismo de grupos

   $$(\mathbb{Z}_n)^\times \cong Aut(C_n),$$

   dado por $r \mapsto f_r$ para cada $r = 1, \ldots, n$ con $mcd(r,n) = 1$, donde el automorfismo f_r se define mediante $f_r(x) = x^r$.

   En particular, $Aut(C_n)$ es un grupo abeliano de orden $\varphi(n)$.

Resolución. 1.- Sea $\theta : C_n \to G$ un homomorfismo de grupos, con $\theta(x) = g$. Entonces $g^n = (\theta(x))^n = \theta(x^n) = \theta(1) = 1$, con lo que $ord(g)|n$.

La segunda afirmación es inmediata por ser θ un homomorfismo de grupos.

2.- Sea $g \in G$ con $ord(g) = t$ y supongamos que $t|n$, entonces $\exists n' \in \mathbb{Z}$ tal que $n = tn'$.

Veamos que la aplicación $\theta_g : C_n \to G$ dada por $\theta_g(x^k) = g^k$, $0 \leq k \leq n-1$, define un homomorfismo de grupos.

Sean $x^k, x^r \in C_n$, $0 \leq k, r \leq n-1$. Sabemos que si $k + r = qn + s$, $0 \leq s \leq n-1$, entonces $x^k x^r = x^s$ con lo que

$$\theta_g(x^k x^r) = \theta_g(x^s) = g^s = g^h,$$

donde $h = Res(s;t)$, ya que $ord(g) = t$. Por otro lado

$$\theta_g(x^k)\theta_g(x^r) = g^k g^r = g^{Res(k+r;t)}.$$

Supongamos que $s = ts' + h$, con $0 \leq h \leq t-1$, entonces $k + r = qn + s = qtn' + ts' + h = (qn' + s')t + h$ y por tanto $Res(k + r; t) = h$ con lo que

$$\theta_g(x^k x^r) = \theta_g(x^k)\theta_g(x^r),$$

y θ_g es en efecto un homomorfismo. La unicidad es consecuencia directa del apartado anterior.

3.- Sea $g \in G$ con $ord(g) = t$ y supongamos que $t|n$. Supongamos que $\theta_g : C_n \to G$ es un monomorfismo. Como $\theta_g(x^t) = g^t = 1$ entonces $x^t = 1$ (pues el núcleo de θ_g es trivial) y entonces $n|t$. Consecuentemente $t = ord(g) = n$.

Recíprocamente, Supongamos que $ord(g) = n$ y sea $x^k \in Ker(\theta_g)$, entonces $1 = \theta_g(x^k) = g^k$ con lo que, como $ord(g) = n$, $n|k \Rightarrow x^k = 1$, esto es $Ker(\theta_g)$ es trivial y θ_g es un monomorfismo.

4.- Recordemos que $(\mathbb{Z}_n)^\times = \{r/1 \leq r \leq n-1, \text{m. c. d.}(r,n) = 1\}$. Para cada $r \in (\mathbb{Z}_n)^\times$, puesto que $ord(x^r) = \frac{n}{\text{m.c.d.}(r,n)} = n$, entonces, por el apartado 2, la aplicación $f_r : C_n \to C_n$ dada por $f_r(x) = x^r$ es un homomorfismo de grupos que, por el apartado 3, también es monomorfismo. Por otro lado $Img(f_r) = \langle x^r \rangle = \langle x \rangle = C_n$ y entonces f_r es también un epimorfismo. Tenemos pues una aplicación

$$\lambda : (\mathbb{Z}_n)^\times \longrightarrow Aut(C_n), \text{ dada por } \lambda(r) = f_r.$$

Veamos que es un homomorfismo de grupos (recuerdese que la operación en el grupo de automorfismos es la composició): Sean $r, k \in (\mathbb{Z}_n)^\times$, entonces

$$\lambda(rk) = \lambda(Res(rk;n)) = f_{Res(rk;n)}; \text{ mientras que } \lambda(r)\lambda(k) = f_r \circ f_k,$$

como

$$(f_r \circ f_k)(x) = f_r(x^k) = (f_r(x))^k = (x^r)^k = x^{rk} = x^{Res(rk;m)} = f_{Res(rk;n)}(x),$$

de nuevo usando el apartado 2, es

$$\lambda(rk) = \lambda(r)\lambda(k).$$

Finalmente, que λ es un isomorfismo es también consecuencia directa del apartado 2 (concretadlo vosotros).