AMPLIACIÓN DE MATEMÁTICAS

GRUPOS PRODUCTO Y COCIENTE.

El **producto cartesiano** de dos grupos y el **conjunto cociente** de un grupo respecto de ciertas relaciones, son dos formas de construir nuevos grupos. Estas dos nuevas construciones: **grupos productos** y **grupos cocientes** las vamos a desarrollar en lo que sigue. La idea del cociente nos va a ser útil en el desarrollo del Teorema de Lagrange (esencial en las propiedades de la función de Euler). El producto cartesiano de grupos es necesario para dar el Teorema de Clasificación de Grupos Abelianos Finitos (éste lo necesitaremos para describir el grupo multiplicativo de los cuerpos finitos). Empecemos.

PRODUCTO CARTESIANO DE GRUPOS.

Definición 1. *Sean* $(\mathbb{G}_1, *_1)$ *y* $(\mathbb{G}_2, *_2)$ *dos grupos. Consideramos su producto cartesiano*

$$\mathbb{G} = \mathbb{G}_1 \times \mathbb{G}_2.$$

Sobre $\mathbb{G}$ *definimos la operación* $*$

$$\begin{array}{cccccc} * & : & \mathbb{G} \times \mathbb{G} & \to & \mathbb{G} & \\ & & ((g_1, g_2), (h_1, h_2)) & \to & (g_1, g_2) * (h_1, h_2) & = & (g_1 *_1 h_1, g_2 *_2 h_2). \end{array}$$

A $(\mathbb{G}, *) = \mathbb{G}_1 \times \mathbb{G}_2 = \mathbb{G}_1 \oplus \mathbb{G}_2$ *se le llama* ***producto directo*** *de los grupos* $\mathbb{G}_1$ *y* $\mathbb{G}_2$.

Teorema 1. *Dados* $(\mathbb{G}_1, *_1)$ *y* $(\mathbb{G}_2, *_2)$ *dos grupos, su producto directo* $(\mathbb{G}, *) = \mathbb{G}_1 \oplus \mathbb{G}_2$ *es un grupo.*

Demostración:

- Probar la propiedad asociativa es un simple ejercicio.
- Si e_1 y e_2 son los elementos neutros de $\mathbb{G}_1$ y $\mathbb{G}_2$ respectivamente, entonces

$$e = (e_1, e_2) \qquad \text{es el elemento neutro de} \qquad (\mathbb{G}; *).$$

- Si $(g,h) \in \mathbb{G}$, entonces claramente $(g,h)^{-1} = (g^{-1}, h^{-1})\square$

Observación 1. **A:** *Si* $(\mathbb{G}_1, *_1)$ *y* $(\mathbb{G}_2, *_2)$ *son grupos abelianos, claramente su producto directo* $(\mathbb{G}, *) = \mathbb{G}_1 \oplus \mathbb{G}_2$ *también es un grupo abeliano.*

B: *Si* $(\mathbb{G}_i, *_i)_{i \in I}$ *es una familia de grupos, el conjunto*

$$\mathbb{G} = \bigoplus_{i \in I} \mathbb{G}_i \qquad \textit{con} \qquad (g_i) * (h_i) = (g_i *_i h_i)$$

es también un grupo.

Ejemplo 1. *Sea* $(\mathbb{Z}_{30}, +)$*. Como* $30 = 2 \times 3 \times 5$*, vimos que el grupo* $(\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5, +)$ *era equivalente a* $(\mathbb{Z}_{30}, +)$ *en el sentido de que existe una biyección entre ellos que conserva la operación (usabamos para ello el Teorema Chino del Resto).* $(\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5, +)$ *es un ejemplo de* ***grupo producto*** *o de producto directo de los grupos* $\mathbb{Z}_2, \mathbb{Z}_3$ *y* $\mathbb{Z}_5$*.*

Un poco más adelante diremos que los grupos $(\mathbb{Z}_{30}, +)$ y $(\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5, +)$ son **isomorfos**.

EL GRUPO COCIENTE.

El modelo de construcción del **grupo cociente** lo podemos encontrar en los grupos $(\mathbb{Z}_n, +)$ que estudiamos anteriormente. En $\mathbb{Z}$, fijado un $n \in \mathbb{N}\backslash\{0\}$, tenemos la relación de congruencia $k_1 \, R \, k_2$ si y solo si $n | k_1 - k_2$ o equivalentemente decimos que $k_1 \equiv k_2 \mod \text{n}$. O también podemos decir que $k_1 \, R \, k_2$ si y solo si $k_1 - k_2 \in n\mathbb{Z}$. El grupo cociente asociado a esta relación de equivalencia es

$$\mathbb{Z}_n = \mathbb{Z}/R = \mathbb{Z}/n\mathbb{Z}.$$

De todas estas formas lo podemos denotar. Además es claro que con la suma en congruencias tenemos un grupo, $(\mathbb{Z}_n, +)$.

De forma análoga, pero abstracta, podemos preguntarnos si dados un grupo $(\mathbb{G}, *)$, una relación de equivalencia sobre él, $\sim$, y el correspondiente conjunto cociente

$$\mathbb{G}/\sim = \{[g] \ : \ [g] = \{h \in \mathbb{G} \ : \ g \sim h\} \ \}$$

¿va a tener el conjunto cociente $\mathbb{G}/\sim$ una estructura de grupo?

Ejemplos 1.

- *Para todo* $n \in \mathbb{N}\backslash\{0\}$, $(\mathbb{Z}_n, +)$ *es un grupo. Como señalamos arriba.*
- *Sea el grupo aditivo de los enteros* $(\mathbb{Z}, +)$ *y sea la relación* $n \sim m$ *si y solo si* $|n| = |m|$. *Ésta es claramente una relación de equivalencia. Para esta relación podemos observar que*

$$3 \sim 3 \qquad y \qquad 4 \sim -4$$

y ahora

$$7 = 3 + 4 \nsim 3 + (-4) = -1$$

Así, si consideramos la suma de clases de equivalencia como $[n]+[k] = [n+k]$, *tendríamos que*

$$[3] + [4] = [7] \neq [-1] = [3] + [-4].$$

Esta suma no estaría bien definida.

El ejemplo último muestra que no es evidente que un conjunto cociente de un grupo $\mathbb{G}/\sim$ pueda ser de nuevo un grupo. De hecho, para que ésto sea así hay que pedir condiciones adicionales a la relación de equivalencia.

Definición 2. *Sean* $(\mathbb{G}, *)$ *un grupo y una relación de equivalencia* $\sim$ *sobre* $\mathbb{G}$. *Se dice que la relación* $\sim$ *es compatible o que es una* ***relación de congruencia*** *(o simplemente que es una* ***congruencia****) si para todo* $g, g', h, h' \in \mathbb{G}$ *con*

$$g \sim g' \qquad y \qquad h \sim h' \qquad \Rightarrow \qquad g * h \sim g' * h'.$$

Con esta condición adicional ya podemsos asegurar que el conjunto cociente tiene estructura de grupo.

Teorema 2. *Sea* $\sim$ *una* ***congruencia*** *sobre un grupo* $(\mathbb{G}, *)$. *Sobre el conjunto cociente* $\mathbb{G}/\sim$ *se define la operación* $\odot$ *por*

$$\begin{array}{rcccl} \odot & : & \mathbb{G}/\sim \times \mathbb{G}/\sim & \to & \mathbb{G}/\sim \\ & & ([g],[h]) & \to & [g]\odot[h] \;=\; [g*h]. \end{array}$$

Entonces $(\mathbb{G}/\sim, \odot)$ *es un grupo que llamamos* ***grupo cociente*** *de* $(\mathbb{G}, *)$ *con respecto a la congruencia* $\sim$.

Observación 2.
- *Lo anterior es la* ***abstracción*** *del proceso que seguimos para construir los grupos* $(\mathbb{Z}_n, +)$.
- *Y como veremos en el tema de* ***Anillos****, es el procedimiento que nos permitirá construir el* ***cuerpo de descomposición de un polinomio****.*

Demostración: Por ser $\sim$ una congruencia la operación $\odot$ está **bien definida**. Ádemás

- Como $[(g * h) * t] = [g * (h * t)]$ la operación $\odot$ es **asociativa**.
- Si $e \in \mathbb{G}$ es el elemento neutro, es claro que $[e] \in \mathbb{G}/\sim$ es el **elemento neutro** de $(\mathbb{G}/\sim, \odot)$.
- Si $[g] \in \mathbb{G}/\sim$, entonces $[g^{-1}] \in \mathbb{G}/\sim$ es su **inverso**$\square$

Observación 3. *Si* $(\mathbb{G}, *)$ *es un grupo abeliano y* $\sim$ *es una congruencia, entonces* $(\mathbb{G}/\sim, \odot)$ *también es un grupo abeliano.*

Ejemplos 2.
- *En* $\mathbb{Z}$*, la congruencia "habitual",* $m \equiv_n k \text{ mód } n$ *es una congruencia en el sentido de la definición anterior. Y como ya sabiamos* $(\mathbb{G}/\equiv_n, \odot) = (\mathbb{Z}_n, +)$ *es un grupo abeliano.*
- *También si* p *es primo*

$$(\mathbb{Z}/\equiv_p \backslash\{0\}, \times) = (\mathbb{Z}_p\backslash\{0\}, \times)$$

es un grupo; aquí lo novedoso es que $(\mathbb{Z}, \times)$ *no lo es. Por tanto, aunque* $(\mathbb{Z}_p, \times)$ *lo hemos construido como un cociente,* ***no es*** *propiamente un grupo cociente.*
- *Si* $(\mathbb{G}, *)$ *es un grupo* ***abeliano*** *y* $N \trianglelefteq \mathbb{G}$ *es un subgrupo, entonces la relación sobre* $\mathbb{G}$ *dada por*

$$g \sim_N g' \qquad \Leftrightarrow \qquad g * g'^{-1} \in N, \qquad \text{para todo} \qquad g, g' \in \mathbb{G}$$

es una ***congruencia*** *y por tanto el subconjunto cociente* $(\mathbb{G}/\sim_N, \odot)$ *es un grupo abeliano.*

Veamos que $\sim_N$ es efectivamente una congruencia. Para todo $g, g', h, h' \in \mathbb{G}$ con

$$g \sim_N g' \qquad \text{y} \qquad h \sim_n h' \qquad \text{tenemos que ver que} \qquad g * h \sim g' * h'.$$

Claro,

$$g * h * (g' * h')^{-1} = g * h * (h'^{-1} * g'^{-1})$$

por ser $\mathbb{G}$ abeliano

$$= (g * g'^{-1}) * (h * h'^{-1}) \in N \quad \square$$

Observación 4. *La construcción del grupo cociente $\mathbb{G}/N$ de un grupo $\mathbb{G}$ respecto a un subgrupo N es sencilla en el caso de que el grupo $\mathbb{G}$ sea abeliano, como acabamos de ver. En el caso general hay que imponer que el subgrupo N sea* ***normal****.*

Esta noción de subgrupo normal se escapa de nuestros objetivos y queda relegada al siguiente **apéndice** de carácter informativo.

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain
E-mail address: Cesar_Ruiz@mat.ucm.es