Grupos
Hungerford

Pablo Brianese

30 de agosto de 2021

Teorema 1. *Si G es un monoide, entonces el elemento identidad e es único. Si G es un grupo, entonces*

1. *$cc = c$ implica $c = e$, para todo $c \in G$;*
2. *para todo $a, b, c \in G$, $ab = ac$ implica $b = c$ y $ba = ca$ implica $b = c$ (cancelación a izquierda y a derecha);*
3. *para cada $a \in G$, el elemento inverso a^{-1} es único;*
4. *para cada $a \in G$, $(a^{-1})^{-1} = a$;*
5. *para $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$;*
6. *para $a, b \in G$, las ecuaciones $ax = b$ e $ya = b$ tienen soluciones únicas en G: $x = a^{-1}b$ e $y = ba^{-1}$.*

Demostración. Si G es un monoide y e, e' son identidades bilaterales, entonces $e = ee' = e'$. $\square$

Demostración. 1. Porque e es la identidad $c = cc \Rightarrow ce = (cc)e = cc$. Por la existencia de inversos en el grupo, podemos decir que $ce = cc \Rightarrow c^{-1}(ce) = c^{-1}(cc)$. La asociatividad de la operación del grupo implica $c^{-1}(ce) = c^{-1}(cc) \Rightarrow (c^{-1}c)e = (c^{-1}c)c$. Por definición del inverso c^{-1}, se sigue $(c^{-1}c)e = (c^{-1}c)c \Rightarrow ee = ec$. Nuevamente, porque e es la identidad del grupo, $ee = ec \Rightarrow e = c$. $\square$

Demostración. 2. Suponemos $ab = ac$. La existencia de inversos en el grupo implica $a^{-1}(ab) = a^{-1}(ac)$. La asociatividad de la operación del grupo implica $(a^{-1}a)b = (a^{-1}a)c$. Por definición del inverso a^{-1}, se sigue $eb = ec$. Porque e es la identidad, concluímos $b = c$.

Suponemos $ba = ca$. La existencia de inversos en el grupo implica $(ba)a^{-1} = (ca)a^{-1}$. La asociatividad de la operación del grupo implica $b(aa^{-1}) = c(aa^{-1})$. Por definición del inverso a^{-1}, se sigue $be = ce$. Porque e es la identidad, concluímos $b = c$. $\square$

Demostración. 3. Sea b tal que $ab = ba = e$. Por la existencia de inversos en el grupo, podemos decir que $(ba)a^{-1} = ea^{-1}$. La asociatividad de la operación del grupo implica $b(aa^{-1}) = ea^{-1}$. Por definición del inverso a^{-1}, se sigue $be = ea^{-1}$. Porque e es la identidad, concluímos $b = a^{-1}$. $\square$

Demostración. 4 Sea $b = a^{-1}$. Por definición del inverso a^{-1}, tenemos $ab = ba = e$. Por definición del inverso b^{-1} tenemos $b^{-1}b = bb^{-1} = e$. Por unicidad del inverso (ver 3) $a = b^{-1}$. $\square$

Demostración. 5 Por la unicidad del elemento inverso (ver 3) basta con calcular los productos $(ab)(b^{-1}a^{-1})$ y $(b^{-1}a^{-1})(ab)$.

Usando la asociatividad del producto deducimos $(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1}))$ y $a(b(b^{-1}a^{-1})) = a((bb^{-1})a^{-1})$. Por la definición del inverso $a((bb^{-1})a^{-1}) = a(ea^{-1})$. Porque e es la identidad del grupo $a(ea^{-1}) = aa^{-1}$. Por la definición del inverso $aa^{-1} = e$. Concluímos $(ab)(b^{-1}a^{-1}) = e$.

Usando la asociatividad del producto deducimos $(b^{-1}a^{-1})(ab) = b(a(a^{-1}b^{-1}))$ y $b(a(a^{-1}b^{-1})) = b((aa^{-1})b^{-1})$. Por la definición del inverso $b((aa^{-1})b^{-1}) = b(eb^{-1})$. Porque e es la identidad del grupo $b(eb^{-1}) = bb^{-1}$. Por la definición del inverso $bb^{-1} = e$. Concluímos $(b^{-1}a^{-1})(ab) = e$. □

Proposición 1. *Sea G un semigrupo. Entonces G es un grupo si y solo si se verifican las siguientes condiciones*

1. *existe un elemento $e \in G$ tal que $ea = a$ para todo $a \in G$ (elemento identidad izquierdo).*
2. *para cada $a \in G$, existe un elemento $a^{-1} \in G$ tal que $a^{-1}a = e$ (inversos izquierdos).*

Observación 1. Cambiando la condición del elemento identidad izquierdo por una condición del "elemento identidad derecho", o cambiando la condición de los inversos izquierdos por una condición de los "inversos derechos", se obtienen resultados análogos que siguen siendo verdaderos.

Demostración. Las condiciones 1 y 2 se deducen fácilmente cuando G es un grupo. La implicación recíproca sí tiene interés.

Supongamos 1 y 2. Entonces $aa = a$ implica $a = e$ para todo $a \in G$. En efecto, suponiendo $aa = a$ se deduce

$$\begin{aligned}
aa = a &\Rightarrow a^{-1}(aa) = a^{-1}a && \text{por 2} && (1)\\
&\Rightarrow (a^{-1}a)a = a^{-1}a && \text{por asociatividad} && (2)\\
&\Rightarrow ea = e && \text{por 2} && (3)\\
&\Rightarrow a = e && \text{por 1} && (4)
\end{aligned}$$

Este hecho es muy importante. ¿Por qué? Porque para todo elemento $a \in G$

$$\begin{aligned}
(aa^{-1})(aa^{-1}) &= a(a^{-1}(aa^{-1})) && \text{por asociatividad} && (5)\\
&= a((a^{-1}a)a^{-1}) && \text{por asociatividad} && (6)\\
&= a(ea^{-1}) && \text{por 2} && (7)\\
&= aa^{-1} && \text{por 1} && (8)
\end{aligned}$$

Lo cual nos permite deducir $aa^{-1} = e$, cuando en un principio sólo sabíamos $a^{-1}a = e$ por la condición 2. Es decir que los inversos izquierdos son inversos bilaterales. Habiendo completado la propiedad de los inversos bilaterales podemos deducir la bilateralidad del elemento identidad e como sigue

$$\begin{aligned}
ae &= a(a^{-1}a) && \text{por 1} && (9)\\
&= (aa^{-1})a && \text{por asociatividad} && (10)\\
&= ea && \text{porque los inversos son bilaterales} && (11)\\
&= a && \text{por 1} && (12)
\end{aligned}$$

□

Teorema 2. *Sea R ($\sim$) una relación de congruencia sobre un monoide G, es decir, una relación de equivalencia tal que $a_1 \sim a_n$ y $b_1 \sim b_2$ implican $a_1b_1 \sim a_2b_2$ para todo $a_i, b_i \in G$. Entonces el conjunto G/R formado por todas las clases de equivalencia de G bajo R es un monoide bajo la operacion binaria definida por $\overline{a}\overline{b} = \overline{ab}$, donde $\overline{x}$ denota la clase de equivalencia de $x \in G$. Si G es un grupo [abeliano], entonces también lo es G/R.*

Demostración. Lo primero que debemos probar es que la operación binaria propuesta está bien definida, es decir que el producto $\overline{a}\overline{b} = \overline{ab}$ es independiente de la elección de elementos representativos a, b. Por eso tomamos un par de elementos $a_1, a_2 \in G$ tales que $\overline{a_1} = \overline{a_2}$, y otro par $b_1, b_2 \in G$ con $\overline{b_1} = \overline{b_2}$. Se sigue que $a_1 \sim a_2$ y $b_1 \sim b_2$, por propiedades elementales de las relaciones de equivalencia. Por ser R una relación de congruencia deducimos $a_1b_1 \sim a_2b_2$. Usando, nuevamente, propiedades elementales de las relaciones de equivalencia deducimos $\overline{a_1b_1} = \overline{a_2b_2}$.

Esta operación en G/R hereda su asociatividad de G. Si $a, b, c \in G$ entonces $\overline{a}(\overline{b}\overline{c}) = \overline{a}\overline{bc} = \overline{a(bc)} = \overline{(ab)c} = \overline{ab}\overline{c} = (\overline{a}\overline{b})\overline{c}$. También hereda su elemento neutro. Si $a \in G$ entonces $\overline{e} \cdot \overline{a} = \overline{ea} = \overline{a}$ y $\overline{a} \cdot \overline{e} = \overline{ae} = \overline{a}$, lo cual hace de $\overline{e}$ el elemento neutro de G/R. Por lo tanto G/R es un monoide, dado que G lo es.

Si G es un grupo, entonces G/R hereda los elementos inversos del primero. Si $a \in G$, entonces $\overline{a}\overline{a^{-1}} = \overline{aa^{-1}} = \overline{e}$ y $\overline{a^{-1}}\overline{a} = \overline{a^{-1}a} = \overline{e}$ de modo tal que $\overline{a^{-1}} = \overline{a}^{-1}$. Esto hace de G/R un grupo.

Si G es conmutativo, entonces también G/R es conmutativo. Si $a, b \in G$ entonces $\overline{a}\overline{b} = \overline{ab} = \overline{ba} = \overline{b}\overline{a}$. □