El anillo de convolución sobre un semigrupo finito

Objetivos. Estudiar la definición y las propiedades básicas del anillo de convolución sobre un semigrupo finito.

Prerrequisitos. Semigrupos, monoides y grupos, el producto de Minkowski de dos conjuntos en un semigrupo (o la suma de Minkowski, en la notación aditiva), el soporte de una función, anillos.

Definición 1. Sean X un conjunto y R un anillo. El *soporte* de una función $f\colon X \to R$ es el conjunto de los puntos del dominio X, en los cuales f toma valores no nulos:

$$\operatorname{supp}(f) \coloneqq f^{-1}[R \setminus \{0_R\}], \qquad \text{esto es,} \qquad \operatorname{supp}(f) = \big\{x \in X\colon\ f(x) \neq 0_R\big\}.$$

Observación 2. La Definición 1 se utiliza en álgebra, cuando el dominio X no tiene ninguna topología o está dotado de la topología discreta. En el contexto de análisis y topología, cuando X es un espacio topológico, el soporte de una función se puede definir como la cerradura del conjunto $\big\{x \in X\colon\ f(x) \neq 0_R\big\}$. Para las funciones medibles definidas en un espacio de Borel, el soporte esencial se define de manera aún más complicada.

Definición 3. Sean G un semigrupo finito y R un anillo asociativo. Denotemos por A al conjunto de todas las funciones $G \to R$:

$$A \coloneqq R^G.$$

Dadas f, g en A, definimos su suma de manera usual:

$$(f * g)(x) \coloneqq f(x) + g(x).$$

Dado z en G, pongamos

$$M_z \coloneqq \big\{(x, y) \in G^2\colon\ xy = z\big\}.$$

Dadas f, g en A, definimos su *convolución* de la siguiente manera:

$$(f * g)(z) \coloneqq \sum_{(x,y)\in M_z} f(x)g(y).$$

Si el conjunto T_z es vacío, entonces la suma correspondiente se define como 0_R.

Observación 4. Estos apuntes se generalizan de manera trivial a la situación cuando G no es finito, pero tiene la siguiente propiedad: para cada z en G, el conjunto M_z es finito.

Proposición 5. *Si $f, g \in A$, entonces*

$$\operatorname{supp}(f + g) \subseteq \operatorname{supp}(f) \cup \operatorname{supp}(g).$$

Idea de demostración. Notamos que para cada x en X,

$$\big(f(x)=0 \quad \wedge \quad g(x)=0\big) \quad \Rightarrow \quad f(x)+g(x)=0.$$

Pasando a la forma contrapositiva, obtenemos el resultado. □

Definición 6 (el producto de Minkowski de dos conjuntos en un semigrupo)**.** Dados $X, Y \subseteq G$, denotamos por XY su producto de Minkowski:

$$XY \coloneqq \big\{z \in G\colon \ \exists x \in X \quad \exists y \in Y \quad xy = z\big\}.$$

Proposición 7. *Si R es un dominio entero y $f, g \in A$, entonces*

$$\operatorname{supp}(f * g) \subseteq \operatorname{supp}(f)\operatorname{supp}(g).$$

Demostración. Sean $f, g \in A$. Sea $z \in \operatorname{supp}(f * g)$. Entonces, $M_z \neq \emptyset$ y

$$\sum_{(x,y)\in M_z} f(x)g(y) \neq 0_R.$$

Elegimos $(a, b) \in M_z$ tal que $f(a)g(b) \neq 0_R$. Como R es un dominio entero, concluimos que

$$f(a) \neq 0_R, \qquad g(b) \neq 0_R.$$

Los puntos a y b tienen las siguientes propiedades:

$$a \in \operatorname{supp}(f), \qquad b \in \operatorname{supp}(g), \qquad z = ab.$$

Esto implica que $z \in \operatorname{supp}(f)\operatorname{supp}(g)$. □

Proposición 8 (la operación $*$ es distributiva respecto a la operación $+$)**.** *Si $f, g, h \in A$, entonces*

$$(f+g)*h = (f*h)+(g*h), \qquad f*(g+h) = (f*g)+(f*h).$$

Demostración. Demostremos solamente la primera igualdad (la segunda se demuestra de manera similar). Supongamos que $z \in G$.

$$\begin{aligned}((f+g)*h)(z) &= \sum_{(x,y)\in M_z} (f(x)+g(x))h(y) = \sum_{(x,y)\in M_z} (f(x)h(y)+g(x)h(y)) \\ &= \sum_{(x,y)\in M_z} f(x)h(y) + \sum_{(x,y)\in M_z} g(x)h(y) = (f*h)(z)+(g*h)(z). \quad \square\end{aligned}$$

Proposición 9 (la convolución de tres funciones)**.** *Sean $f, g, h \in A$. Para cada $t \in G$, pongamos*

$$V_t \coloneqq \big\{(x, y, z) \in G^3\colon \ (xy)z = t\big\}.$$

Entonces, para cada t en G,

$$((f*g)*h)(t) = \sum_{(x,y,z)\in V_t} f(x)g(y)h(z).$$

Demostración. Tenemos que aplicar la definición de la convolución dos veces:

$$((f*g)*h)(t) = \sum_{(s,z)\in M_t} (f*g)(s)h(z) = \sum_{(s,z)\in M_t} \left(\sum_{(x,y)\in M_s} f(x)g(y) \right) h(z)$$

Pongamos

$$J_t \coloneqq \big\{(x,y,z,s)\colon\ (s,z)\in M_t,\ (x,y)\in M_s\big\}.$$

En otras palabras,

$$J_t = \big\{(x,y,z,s)\colon\ sz=t,\ xy=s\big\} = \big\{(x,y,z,s)\colon\ (xy)z=t,\ xy=s\big\}.$$

Definimos $\varphi\colon J_t \to V_t$,

$$\varphi(x,y,z,s) \coloneqq (x,y,z).$$

Debido a la condición $xy=s$ en la descripción de J_t, es fácil de ver que φ es una biyección. Su inversa actúa mediante la regla

$$\varphi^{-1}(x,y,z) \coloneqq (x,y,z,xy).$$

Por lo tanto, la suma se puede transformar de la siguiente manera:

$$((f*g)*h)(t) = \sum_{(x,y,z,s)\in J_t} f(x)g(y)h(z) = \sum_{(x,y,z)\in V_t} f(x)g(y)h(z). \qquad \square$$

Ejercicio 10. Demuestre que si $f,g,h\in A$, entonces para cada t en G,

$$(f*(g*h))(t) = \sum_{(x,y,z)\in V_t} f(x)g(y)h(z).$$

Utilice la suposición que la operación en G es asociativa y represente el conjunto V_t en la forma

$$V_t = \big\{(x,y,z)\in G^3\colon\ x(yz)=t\big\}.$$

Proposición 11 (la operación de convolución es asociativa)**.** *Si $f,g,h\in A$, entonces*

$$(f*g)*h = f*(g*h).$$

Demostración. Se sigue de la Proposición 9 y del Ejercicio 10. $\square$

Teorema 12. *A es un anillo asociativo.*

Demostración. Se sigue de las proposiciones anteriores. $\square$

Proposición 13. *Si R es conmutativo, entonces A es conmutativo.*

Demostración. Ejercicio. $\square$

Proposición 14. *Si G es un monoide con cancelación y R tiene identidad, entonces A tiene identidad.*

Demostración. Usamos la suposición que G tiene un elemento neutro 1_G. Definimos $u\colon G \to R$,

$$u(x) \coloneqq \begin{cases} 1_R, & x = 1_G; \\ 0_R, & x \neq 1_G. \end{cases}$$

Sea $f \in A$. Demostremos que $f * u = f$.

Sea $z \in G$. Notemos que $(z, 1_G)$ es un elemento de M_z.

Si $(x, y) \in M_z$ tal que $y = 1_G$, entonces usamos la igualdad

$$x1_G = z = z1_G,$$

aplicamos la ley de cancelación y obtenemos que $x = z$.

Se sigue que si $(x, y) \in M_z$ y $x \neq z$, entonces $y \neq 1_G$. Luego

$$(f * u)(z) = f(z)u(1_G) + \sum_{(x,y)\in M_z\colon\, x\neq z} f(x)g(y) = f(z)1_R + 0_R = f(z). \qquad \square$$

Definición 15. Por simplifidad, supongamos que R es conmutativo. Dados ξ en R y f en A, definimos $\xi f\colon G \to R$,

$$(\xi f)(x) \coloneqq \xi f(x).$$

Es fácil de ver que A es un módulo conmutativo sobre R.

Proposición 16. *Si G es un monoide con cancelación y R es un campo, entonces A es un álgebra sobre R, asociativa, conmutativa y con identidad.*

Observación 17. En vez de escribir los elementos de A como funciones, en varios libros de álgebra y de la teoría de representaciones los elementos de A se escriben como "combinaciones lineales formales" de los elementos de G, con coeficientes en R:

$$r_1g_1 + r_2g_2 + \ldots + r_mg_m.$$

Se puede ver que si multiplicamos las combinaciones lineales formales aplicando ciertas leyes usuales, entonces obtenemos nuevos coeficientes por la misma ley que está escrita en la Definición 3.