Monoides abelianos en álgebra y geometría*

Cristhian E. Garay
email: cristhian.garay@cimat.mx

November 21, 2019

Abstract

Los monoides abelianos son grupos abelianos *en los que no necesariamente todo elemento tiene inverso*. Un ejemplo importante es el booleano $\mathbb{B} = (\{0,1\}, +, 0)$, en el cual $1+1=1$.

Los semi-anillos conmutativos se definen de manera similar (anillos conmutativos con 1 *en el que no necesariamente todo elemento tiene inverso aditivo*). Ejemplos interesantes de semi-anillos son los números naturales $\mathbb{N}$ con las operaciones usuales, o el semi-anillo tropical $\mathbb{T}$.

A pesar de ser objetos clásicos, sus propiedades algebraicas y geométricas apenas se han comenzado a explorar recientemente, estudio motivado por su aparición en ramas (también de reciente aparición) de la geometría algebraica, como la logarítmica y la tropical. Asimismo, los monoides forman parte esencial del intento de *algebrizar la geometría* que surge de estructuras más generales que los anillos -como los semi-anillos-.

En esta plática hablaremos un poco de la geometría de los monoides, y de aplicaciones concretas a la geometría algebraica y la teoría de módulos sobre semi-anillos.

Contents

1 Introducción

Como (casi) todo será conmutativo, omitiré esta palabra. También trataremos de ir esbozando en el camino conexiones explícitas con la combinatoria.

Los monoides son estructuras algebraicas que aparecen de manera temprana y natural en matemáticas.

1.1 Example:

1. Los números naturales $\mathbb{N} = (\{0,1,\ldots\}, 0, +)$,
2. Si S es un conjunto, $\mathcal{P}(S) = (\{A \subset S\}, \emptyset, \cup)$,
3. Los números tropicales $\mathbb{T} = (\mathbb{R} \cup \{-\infty\}, -\infty, \max)$,

*Este texto es el guión de mi intervención en la Escuela de Otoño de Álgebra Conmutativa, llevada a cabo en el CIMAT (Noviembre 2019).

4. Si R es un anillo con 1 (no necesariamente conmutativo), las clases de isomorfismo de R-módulos $\mathrm{Iso}(\mathrm{Mod}(R)) = (\{[M] \in \mathrm{Mod}(R)/\mathrm{iso}\}, [0], \oplus)$,
5. los reales no negativos $\mathbb{R}_{\geq 0} = (\mathbb{R}_{\geq 0}, +, 0)$,
6. cualquier grupo abeliano $G = (G, 0, +)$

Observación 1.2: *Como todo grupo es en particular un monoide, cuando introduzcamos un concepto para monoides, nos preguntaremos: y qué pasa si el monoide es un grupo?*

Definición: Un monoide es un triple $M = (M, +, 0)$ que consta de un conjunto con una operación binaria asociativa (y conmutativa) con elemento neutro 0. Un mapeo de monoides es una función $f : M_1 \to M_2$ que satisface $f(0) = 0$ y $f(a + b) = f(a) + f(b)$.

Escribimos **Mon** para la categoría de monoides. A partir de ahora, M denotará un monoide.

Definición: Un elemento $x \in M$ es **invertible** si existe $y \in M$ tal que $x + y = 0$.

Podemos mostrar que el conjunto $M^\times$ de invertibles de M es el subgrupo más grande contenido en M. Veremos que los monoides se pueden alejar bastante del concepto de grupo, tanto como sea posible, de hecho.

Definición: Un monoide M es **agudo** (sharp) si $M^\times = \{0\}$.

1.3 Ejercicio: Encontrar $M^\times$ para los casos del Ejemplo 1.1.
Idea. Intentar resolver la ecuación $x + y = 0$.

1.4 Ejercicio (Idempotentes): Decimos que M es **idempotente** si $m + m = m$ para todo m. Mostrar que todo idempotente es agudo.
Idea. $m + n = 0$ implica $m + m + n = m$, por lo tanto $m = n = 0$.

Denotamos por **Ab** la categoría de grupos abelianos. A todo monoide M se le puede asociar (y de manera óptima y funtorial) un grupo $K(M)$, esto es, hay un morfismo $f : M \to K(M)$ de monoides tal que cualquier otro morfismo a un grupo $M \to G$ se factoriza por f.

Un problema del funtor $K : \mathbf{Mon} \to \mathbf{Ab}$ (que parece no perturbar bastante a la gente) es que a veces destruye información de M.

1.5 Ejercicio (!): Decimos que M es **entero** si cada vez que $a + x = b + x$ sucede, entonces $a = b$. Encontrar cuales de los casos del Ejemplo 1.1 son enteros[1].

1.6 Ejercicio: Sabiendo que[2] $K(M) = M \times M/\sim$, donde $(a, b) \sim (c, d)$ sii existe $x \in M$ tal que $a + d + x = b + c + x$, mostrar que

1. el mapeo $m \mapsto [(m, 0)]$ es una inyección $M \to K(M)$ sii M es entero,
2. si M es idempotente, entonces $K(M) = 0$.
   Idea. Mostrar que $(a, b) \sim (c, d)$ siempre, al tomar $x = a + b + c + d$.

Los monoides tienen conexión con la teoría de estructuras ordenadas, pues todo monoide M carga carga canónicamente un preorden (una relación binaria que es reflexiva y transitiva).

1.7 Ejercicio:
1. Mostrar que la relación en M dada por $a \leq b$ sii $a + c = b$ para algún c define un preorden en M, el cual es compatible con la suma.

[1] El caso 4 es un caso bastante antiguo e importante en teoría de módulos. Rara vez son enteros.
[2] Las dos coordenadas representan una parte positiva y otra negativa, respectivamente.

2. Mostrar que si M es un grupo, entonces este preorden es trivial.

1.8 Ejercicio (Monoides y semiretículos acotados): Un **semiretículo** es un conjunto parcialmente ordenado $(S, \leq)$ tal que el supremo de cualesquiera dos elementos $x, y \in S$ siempre existe (lo denotamos $x \vee y$). Decimos que el semiretículo $(S, \leq)$ es **acotado** si tiene un elemento mínimo.
Mostrar que los semiretículos acotados y los monoides idempotentes representan el mismo concepto.

Para terminar esta parte introductoria, diremos como el caso 4 del Ejemplo 1.1 sirve para definir un objeto clásico muy importante.

Definición (El grupo K_0 de un anillo): Sea R un anillo con 1 e $\mathrm{Iso}(\mathrm{PMod}(R))$ el monoide que consiste de las clases de isomorfismo de módulos proyectivos finitamente generados sobre R. El 0-ésimo grupo K de R es $K_0(R) := K(\mathrm{Iso}(\mathrm{PMod}(R)))$.

Observación 1.9: *Como ya hemos visto, el grupo $K_0(R)$ en general va a perder información, del monoide $\mathrm{Iso}(\mathrm{PMod}(R))$ (a menos que este sea entero). Por otro lado, se espera que calcular el monoide en vez del grupo sea una tarea difícil.*

2 Álgebra semi-conmutativa

La referencia más completa para esta parte es [3]. Los semianillos también aparecen temprana y naturalmente en matemáticas.

2.1 Example:

1. Los números naturales $\mathbb{N} = (\{0, 1, \ldots\}, 0, 1, +, \times)$,
2. Si S es un conjunto, $\mathcal{P}(S) = (\{A \subset S\}, \emptyset, S, \cup, \cap)$,
3. Los números tropicales $\mathbb{T} = (\mathbb{R} \cup \{-\infty\}, -\infty, 0, \max, +)$,
4. Las clases de isomorfismo de R-módulos $\mathrm{Iso}(R\text{−Mod}) = (\{[M] \in (R\text{−Mod})/\mathrm{iso}\}, [0], [R], \oplus, \otimes_R)$,
5. los reales no negativos $\mathbb{R}_{\geq 0} = (\mathbb{R}_{\geq 0}, +, \times, 0, 1)$
6. cualquier anillo conmutativo con 1: $R = (R, 0, 1, +, \times)$.

Definición: Un **semianillo**[3] es un 5-tuple $(R, +, \times, 0, 1)$ que consta de

1. $(R, +, 0)$ y $(R, \times, 1)$ son monoides,
2. $a(b + c) = ab + ac$,
3. $0a = 0$ para todo a.

Decimos que R es un **semicampo** si todo elemento de $R \setminus \{0\}$ es invertible con respecto a la multiplicación.

2.2 Ejercicio (!): Calcular los invertibles multiplicativos $R \setminus \{0\}$ de cada uno de los semianillos[4] del Ejemplo 2.1.

Un morfismo de semi-anillos es un mapeo $f : R_1 \to R_2$ tal que f induce morfismos en los correspondientes monoides. Decimos que R_2 es una R_1-algebra.

2.3 Ejercicio:

1. Mostrar que la cateogría de semianillos es equivalente categoría de $\mathbb{N}$-álgebras.

[3]Supondremos que $1 \neq 0$.
[4]El caso 4 es el grupo de Picard.

2. Mostrar que un semianillo es idempotente sii 1+1=1. Mostrar que la cateogría de semianillos idempotentes es equivalente cateogría de $\mathbb{B}$-álgebras[5].

2.4 Ejercicio: Sea S una R-álgebra.

1. Mostrar que si R es un anillo, entonces S es un anillo[6].

2. Mostrar que si R es idempotente, entonces S es idempotente.

Definición: Sea R un semianillo. Un R-**módulo** es un monoide $(M, +, 0_M)$ equipado con una operación $\cdot : R \times M \longrightarrow M$ que satisface las propiedades usuales de módulo sobre un anillo, más $0_R \cdot m = 0_M = a \cdot 0_M$ para todo $a \in R$, $m \in M$. Un **ideal** de R es un submódulo de R, cuando vemos a R como un R-módulo.

Es claro que estas definiciones extienden naturalmente las que ya teníamos para anillos. De hecho la prueba del Ejercicio 2.4 se puede adaptar para probar que si M es un módulo sobre un semianillo R, entonces será un grupo (respectivamente idempotente) si R es un anillo[7] (respectivamente si R es idempotente).

2.5 Ejercicio:

1. Mostrar que si K es un semicampo, entonces sus únicos ideales son K y (0).

2. Mostrar que el conjunto de ideales de $\mathbb{N}$ coincide con el conjunto de los submonoides de $(\mathbb{N}, 0, +)$.

El álgebra semi-conmutativa es el estudio de los semi-anillos, sus ideales y los módulos sobre éstos. También hemos mostrado que álgebra conmutativa es un caso particular de la semi-conmutativa.

Para terminar con esta sección, veremos como con semianillos podemos *algebrizar* ciertos objetos combinatorios.

2.6 Ejercicio (!): Sea $C \subset \mathbb{R}^n$ un cono poliedral.

1. Muestre que C es un $\mathbb{R}_{\geq 0}$-módulo finitamente generado.

2. Supongamos que C es de dimension n, y sea C° su interior topológico (con la topología Euclideana). Muestre que $C^\circ \cup \{0\}$ es un $\mathbb{R}_{\geq 0}$-módulo que no es finitamente generado.

3 La geometría de los semianillos

Sea R un semianillo.

Definición: Un ideal propio de R es **primo** si su complemento es cerrado bajo el producto.

3.1 Ejercicio: Calculemos los ideales primos finitamente generados de $\mathbb{N}$. Sea $S \subset \mathbb{N}$ un submonoide aditivo finitamente generado, esto es, existen $n_1, \ldots, n_r \in \mathbb{N} \setminus \{0\}$ tales que $S = \left\{ \sum_{i=1}^r x_i n_i \, : \, x_i \geq 0 \right\}$. Sea $d =$gcd$(n_1, \ldots, n_r)$.

1. Mostrar que existe un conjunto finito $F \subset (d)$ tal que $S = (d) \setminus F$.

2. Deducir que si $I \subset \mathbb{N}$ es un ideal finitamente generado, entonces I es primo si y solo si $I = (p)$ para un número primo p.

[5] Aquí $\mathbb{B}$ es el semianillo Booleano $\mathbb{B} = (\{0, 1\}, +, 0)$, donde $1 + 1 = 1$.

[6] Por lo tanto, el uso del nombre *R-álgebra* (y no el más complicado de R-semiálgebra) está justificado.

[7] Por lo tanto, el uso del nombre *R-ḿódulo* (y no el más complicado de R-semimódulo) está justificado.

Si $I \subset R$ es un ideal de un semianillo, no siempre se puede definir la relación de equivalencia $a \sim_I b$ sii $a - b \in I$, y por lo tanto no siempre podemos hacer el cociente R/I. Esto se soluciona introduciendo el siguiente concepto.

Definición: Una congruencia en S es una relación binaria $\mathcal{R}$ en S que satisface

1. $\mathcal{R}$ es una relación de equivalencia,
2. $\mathcal{R}$ es estable bajos las operaciones de S, i.e. si $\alpha_1 \mathcal{R} \beta_1$ y $\alpha_2 \mathcal{R} \beta_2$, entonces $(\alpha_1 + \alpha_2)\mathcal{R}(\beta_1 + \beta_2)$ y $(\alpha_1\alpha_2)\mathcal{R}(\beta_1\beta_2)$.

3.2 Ejercicio: Si $f : S \longrightarrow R$ es un morfismo de semianillos, entonces $\mathrm{Ker}(f) = \{(\alpha, \beta) \in S \times S : f(\alpha) = f(\beta)\}$ es una congruencia.

Una relación de equivalencia $\mathcal{R}$ en un semianillo S define un semianilo $S/\mathcal{R}$ sii $\mathcal{R}$ es una congruencia. Si $\mathcal{R}$ es una congruencia, entonces la proyección $\pi : S \longrightarrow S/\mathcal{R}$ es un homomorfismo sobreyectivo y $\mathrm{Ker}(\pi) = \mathcal{R}$. Reciprocamente, si $f : S \longrightarrow R$ es un morfismo de semianillos, entonces $f(S)$ es un seusemianillo que satisface $S/\mathrm{Ker}(f) \cong f(S)$. Deducimos que toda congruencia en un semianillo S aparece de esta manera.

La intersección de cualquier familia de congruencias en un semianillo S es una congruencia. Por lo tanto, si $J \subset S \times S$, entonces podemos definir la congruencia más pequeña $\langle J \rangle$ en S que contiene a J.

Sea S un semianillo, $\mathcal{R}$ una congruencia en S e $I \subset S$ un ideal. El conjunto $\mathrm{Ideal}(\mathcal{R}) = \{x \in S : (x, 0_S) \in \mathcal{R}\}$ es un ideal en S, y el conjunto $\mathrm{Cong}(I) = \langle I \times \{0_S\} \rangle$ es una congruencia en S.

3.3 Ejercicio: Sea S un semianillo. Mostrar que

1. en general se tiene $\mathrm{Ideal} \circ \mathrm{Cong}(I) = I$, y $\mathrm{Cong} \circ \mathrm{Ideal}(\mathcal{R}) \subset \mathcal{R}$,
2. si S es un anillo, entonces $\mathrm{Cong} \circ \mathrm{Ideal}(\mathcal{R}) = \mathcal{R}$

4 Aplicaciones a la Geometría Algebraica

Observación 4.1: *Decimos que un submonoide $S \subset \mathbb{N}$ es un **semigrupo numérico** si $\mathbb{N} \setminus S$. Deducimos del ejercicio anterior que S es numerico ssi es de la forma $< n_1, \ldots, n_r >$ con $gcd(n_i) = 1$. Los semigrupos numéricos aparecen en geometría algebraica.*

En particular tenemos que el concepto de ideal primo existe a nivel de semianillos. Luego podríamos avizorar la creación de una teoría de esquemas más general, salvo por la correspondencia entre subesquemas cerrados e ideales.

Citamos de [2]: *The construction of schemes modeled on semirings proceeds exactly as in the classical setting of rings. At a formal level, the classical theory of schemes and this extended theory of semiring schemes are nearly identical when considering open subschemes and gluing. However, novel features appear when considering closed subschemes; this is essentially because the bijection between ideals and congruences breaks down when passing from rings to semirings.*

En particular, queremos usar estas ideas para definir algebraicamente la Geometría Algebraica Tropical, es decir, la Geometría algebraica sobre el semianillo tropical $\mathbb{T}$.

Finalmente, tenemos el siguiente concepto, del cual se puede leer más en [1]. Sea X un esquema. Una estructura pre-logaritmica en X es una pareja $(\mathcal{M}_X, \alpha)$ que consta de una gavilla de monoides[8] $\mathcal{M}_X$ junto con un morfismo de monoides $\alpha : \mathcal{M}_X \to (\mathcal{O}_X, \times)$. Decimos que $(\mathcal{M}_X, \alpha)$ es una log estructura si α induce un isomorfismo de gavillas de monoides entre $\alpha^{-1}(\mathcal{O}_X^*)$ y $\mathcal{O}_X^*$. Un log esquema es un par $(X, \mathcal{M}_X)$.

[8] Para ser honestos, la gavilla $\mathcal{M}_X$ se debe de definir en el sitio étale $X_{\text{ét}}$ de X.

References

[1] Ogus, A. *Lectures on Logarithmic Algebraic Geometry*, (Cambridge University Press, 2018).

[2] Giansiracusa, J. and Giansiracusa, N. *Equations of tropical varieties.*

[3] J. Golan, *Semirings and their Applications.* Springer-Science. 1999.