Anillos - Definición y ejemplos básicos

Facultad de Ciencias UNAM

Introducción

En esta sección introducimos el concepto de anillo y presentamos algunos ejemplos básicos. Un anillo es una estructura algebraica que tiene dos[1] operaciones llamadas “suma” y “multiplicación”. Como veras, estas operaciones son *muy* parecidas a la suma y multiplicación que conocemos de toda la vida. Sin embargo, para alcanzar mayor generalidad, relajamos las condiciones sobre la “multiplicación”[2]. Específicamente, no pedimos que la “multiplicación” de un anillo satisfaga todas las propiedades que satisface la multiplicación usual.

[1] En contraste, recuerda que un grupo tiene una sola operación.

[2] Como veras, no hacemos esto con la “suma”.

Anillos

Definición

Una tripleta ordenada $(R, +, \times)$ es un **anillo** si (i) R es un conjunto no vacío, (ii) $+$ es una operación en R, la cual llamamos **suma**, (iii) $\times$ es una operación en R, la cual llamamos **multiplicación**, y (iv) la suma y la multiplicación satisfacen las siguientes propiedades:

1. $(R, +)$ es un grupo abeliano.
2. $\times$ es asociativa.
3. $\times$ se distribuye respecto a $+$ por ambos lados.

Específicamente, $+$ y $\times$ satisfacen las siguientes propiedades:

I. Asociatividad aditiva: $(a+b)+c = a+(b+c)$ para toda $a, b, c \in R$.

II. Neutro aditivo: Existe un elemento $0 \in R$ tal que $a+0 = a = 0+a$ para toda $a \in R$.

III. Inverso aditivo: Para toda $a \in R$ existe un elemento $-a \in R$ tal que $a+(-a) = 0 = -a+a$. Por brevedad, escribimos $x - y \coloneqq x + (-y)$ para toda $x, y \in R$.

IV. Conmutatividad aditiva: $a+b = b+a$ para toda $a, b \in R$.

V. Asociatividad multiplicativa: $(a \times b) \times c = a \times (b \times c)$ para toda $a, b, c \in R$.

VI. Ley distributiva izquierda: $a \times (b+c) = (a \times b) + (a \times c)$ para toda $a, b, c \in R$.

VII. Ley distributiva derecha: $(b+c) \times a = (b \times a) + (c \times a)$ para toda $a, b, c \in R$.

Las propiedades I-IV son otra forma de decir "$(R, +)$ es un grupo abeliano"; la propiedad V es otra forma de decir "$\times$ es asociativa"; y las propiedades VI-VII son otra forma de decir "$\times$ se distribuye respecto a $+$ por ambos lados".

Notación

Cuando no haya ambigüedad respecto a las operaciones, simplemente decimos que R es un anillo, es decir, no especificamos la notación para las operaciones. En este caso, "+" siempre denota la suma, "$\times$" siempre denota la multiplicación, y por brevedad también escribimos

$$a \cdot b \coloneqq a \times b \quad \text{o} \quad ab \coloneqq a \times b \quad \text{para toda } a, b \in R$$

En caso de que sí haya ambigüedad, le agregamos un subíndice a las operaciones. Específicamente, $+_R$ y $\times_R$ denotan las operaciones de un anillo R. Finalmente, para toda $n \in \mathbb{Z}_{\geq 1}$ definimos

$$n \cdot a \coloneqq \underbrace{a + \cdots + a}_{n-\text{veces}}, \quad (-n) \cdot a \coloneqq -(n \cdot a), \quad \text{y} \quad a^n \coloneqq \underbrace{a \cdots a}_{n-\text{veces}}.$$

Es facil verificar que para toda $n, m \in \mathbb{Z} \setminus \{0\}$ y toda $a, b \in R$ tenemos

$$\begin{aligned} n \cdot a + m \cdot a &= (n+m) \cdot a \\ (n \cdot a)(m \cdot b) &= (nm) \cdot ab \\ a^n \cdot a^m &= a^{n+m} \text{ si } n, m \geq 1 \end{aligned}$$

Cuidado

En contraste con la multiplicación usual de $\mathbb{Z}$, a la multiplicación de un anillo arbitrario *no* le pedimos conmutatividad y *no* le pedimos la existencia de un neutro multiplicativo. Sin embargo, esto no significa que estas propiedades no nos interesen. De hecho, pronto le pondremos nombre a los anillos que tengan estas propiedades, pero todo a su tiempo.

Otra cosa: algunos autores *sí* piden la existencia de un neutro multiplicativo en la definición de anillo, y al objeto que acabamos de definir le llaman "rng". Este desacuerdo no presenta problemas, pero de cualquier manera hay que tener cuidado.

Anillos triviales

- Supongamos que $(R,+)$ es un grupo abeliano. Sea $\times$ la operación en R dada por $a \times b = 0$ para toda $a, b \in R$. Es fácil verificar que $(R,+,\times)$ es un anillo conmutativo, pero también debería ser claro que $(R,+,\times)$ contiene la misma información que $(R,+)$.
- Recordemos que el grupo abeliano que consiste de un solo elemento es dentado por 0. Si lo consideramos con la multiplicación definida en el inciso anterior (que es la única que se puede definir), lo llamamos el **anillo cero**.

Los sistemas numéricos - parte 1

Claramente, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, y $\mathbb{C}$ son anillos con sus operaciones usuales. Las inclusiones

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

y el hecho de que todos tengan las "mismas operaciones" (pero adecuadamente restringidas) sugieren que introduzcamos la siguiente definición.

Subanillos

Definición

Supongamos que R es un anillo y S es un subconjunto de R. Decimos que S es un **subanillo** de R si S es un anillo con las mismas operaciones que R (pero restringidas a S). Es fácil verificar que esto es equivalente a que

$$\forall a, b \in S\, (ab \in S \text{ y } a - b \in S)\,.$$

En palabras, S es un subanillo de R si y sólo si, S es cerrado bajo resta y multiplicación[3].

[3] Recuerda que decir "S es cerrado bajo resta" es lo mismo que decir "S es un subgrupo aditivo".

Los subanillos triviales

Supongamos que R es un anillo. Es fácil ver que

- R es un subanillo de R.
- El subconjunto que consiste únicamente del 0 es un subanillo de R. Por brevedad, lo denotamos de la misma manera que al anillo cero. Es decir, denotamos $0 \coloneqq \{0\} \subset R$.

Decimos que 0 y R son los **subanillos triviales de** R. Por ejemplo, en vez de decir "$S \subset R$ es un subanillo de R tal que $0 \subsetneqq$[4]$S \subsetneqq R$" podemos decir "$S \subset R$ es un subanillo no trivial de R".

[4]Recordemos que (i) todo subanillo es un subgrupo aditivo y (ii) todo subgrupo aditivo contiene al neutro aditivo.

Ejemplo: Los sistemas numéricos - parte 2

Las inclusiones

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

nos dicen (i) que $\mathbb{Z}$ es subanillo de $\mathbb{Q}$, $\mathbb{R}$, y $\mathbb{C}$, (ii) que $\mathbb{Q}$ es subanillo de $\mathbb{R}$ y $\mathbb{C}$, y (iii) que $\mathbb{R}$ es subanillo de $\mathbb{C}$.

De hecho, en general, es fácil verificar que la relación "es subanillo de" es transitiva. En otras palabras, si T es subanillo de S y S es subanillo de R, entonces T es subanillo de R.

Los múltiplos de un entero

Sea $n \in \mathbb{Z}$ y

$$n\mathbb{Z} := \left\{ nk \mid k \in \mathbb{Z} \right\}.$$

Veamos que $n\mathbb{Z}$ es subanillo de $\mathbb{Z}$. Supongamos que $k, k' \in \mathbb{Z}$. Tenemos

$$\begin{aligned} nk - nk' &= n(k - k') \in n\mathbb{Z} \\ nk \cdot nk' &= n \cdot (knk') \in n\mathbb{Z} \end{aligned}$$

donde las pertenencias se cumplen porque $k - k' \in \mathbb{Z}$ y $knk' \in \mathbb{Z}$. Por lo tanto, $n\mathbb{Z}$ es cerrado bajo resta y multiplicación.

Los subanillos de $\mathbb{Z}$

Veamos que todo subanillo de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ para alguna $n \in \mathbb{Z}$.

Primero, notemos que basta demostrar que todo subgrupo aditivo de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ para alguna $n \in \mathbb{Z}$. En efecto, supongamos que esto es cierto y que S es un subanillo de R. En particular, S es un subgrupo aditivo de $\mathbb{Z}$ y por lo tanto es de la forma $n\mathbb{Z}$ para alguna $n \in \mathbb{Z}$.

Con esto en mente, supongamos que S es un subgrupo aditivo no trivial[5] de $\mathbb{Z}$. En particular, existe $m \in S$ distinta de 0. Como S es un subgrupo, también tenemos que $-m \in S$. Una consecuencia de las pertenencias $m, -m \in S$ es que $S \cap \mathbb{Z}_{\geq 1} \neq \varnothing$. Usando esto y el axioma del buen orden de $\mathbb{Z}$, podemos definir

$$n \coloneqq \text{mín}\left(S \cap \mathbb{Z}_{\geq 1}\right)$$

En palabras, n es el entero positivo mas chico que pertenece a S.

[5]Podemos suponer esto porque $0 = 0\mathbb{Z}$ y $\mathbb{Z} = 1\mathbb{Z}$.

Veamos que $n\mathbb{Z} = S$.

$\subset$) Supongamos que $k \in \mathbb{Z}_{\geq 1}$. Como $n \in S$ y S es subgrupo aditivo de $\mathbb{Z}$, entonces

$$kn = \underbrace{n + \cdots + n}_{k\text{-veces}} \in S$$

De nuevo usando que S es subgrupo aditivo de $\mathbb{Z}$, la pertenencia anterior implica que $(-k)n = -kn \in S$. En resumen, vimos que $kn, (-k)n \in S$ para toda $k \in \mathbb{Z}_{\geq 1}$. Equivalentemente, $kn \in S$ para toda $k \in \mathbb{Z} \setminus \{0\}$. Juntando esto con el hecho de que $0n = 0 \in$[6] S, obtenemos lo deseado.

$\supset$) Procedamos por contradicción. Es decir, supongamos que $m \in S \setminus n\mathbb{Z}$. Es fácil ver que esto implica que también $-m \in S \setminus n\mathbb{Z}$. Por eso, podemos suponer sin perdida de generalidad que $m > 0$ (en caso de que $m < 0$, simplemente trabajaríamos con $-m$).

[6] De nuevo, recuerda que todo subgrupo aditivo contiene al neutro aditivo.

Ahora bien, por el algoritmo de la división en $\mathbb{Z}_{\geq 0}$, existen $q, r \in \mathbb{Z}_{\geq 0}$ tales que

$$m = nq + r \text{ con } r = 0 \text{ ó } 0 < r < n$$

Como $m \notin n\mathbb{Z}$, entonces $r \neq 0$ y por lo tanto $0 < r < n$. Juntando esto con la pertenencia $r = m - nq \in S$ obtenemos una contradicción a nuestra elección de n.

Por lo tanto, $S = n\mathbb{Z}$ y los subgrupos aditivos / subanillos de $\mathbb{Z}$ son precisamente los $n\mathbb{Z}$.

En particular, los conceptos "subgrupo aditivo" y "subanillo" son iguales en $\mathbb{Z}$ (con las operaciones usuales). Sin embargo, en lo que sigue veremos que en general esto no es cierto.

Subgrupos aditivos que *no* son subanillos

- Sea $\pi\mathbb{Z} \coloneqq \{\pi k \mid k \in \mathbb{Z}\} \subset \mathbb{R}$. Como para toda $k, k' \in \mathbb{Z}$ tenemos $\pi k + \pi k' = \pi \cdot (k + k') \in \pi\mathbb{Z}$, entonces $\pi\mathbb{Z}$ es un subgrupo aditivo de $\mathbb{R}$.

  Sin embargo, $\pi 1 \cdot \pi 1 = \pi^2 \notin \pi\mathbb{Z}$. De lo contrario, existiría $n \in \mathbb{Z} \setminus \{0\}$ tal que $\pi^2 = \pi n$, lo cual implicaría $\pi = n \in \mathbb{Z}$. Una contradicción. Por lo tanto, $\pi\mathbb{Z}$ *no* es cerrado bajo multiplicación.
- Sea $A \coloneqq \{ix \mid x \in \mathbb{R}\} \subset \mathbb{C}$. Como para toda $x, y \in \mathbb{R}$ tenemos $ix - iy = i \cdot (x - y) \in A$, entonces A es un subgrupo aditivo de $\mathbb{C}$.

  Sin embargo, para $x \neq 0$ tenemos $ix \cdot ix = -x^2 \notin A$. Es decir, A *no* es cerrado bajo multiplicación.