Mas ejemplos de anillos

Facultad de Ciencias UNAM

Introducción

En esta sección presentamos más ejemplos de anillos. Como veras, probablemente ya estés familiarizado con casi todos ellos. Cabe recalcar que en las siguientes secciones estos mismos ejemplos volverán a aparecer muchas veces.

Unos recordatorios

- Supongamos que $a \in \mathbb{Z} \setminus \{0\}$ y $b \in \mathbb{Z}$. Decimos que b **es divisible por** a o que a **divide a** b y escribimos $a|b$ si existe $c \in \mathbb{Z}$ tal que $ac = b$.
- Supongamos que $m, n \in \mathbb{Z} \setminus \{0\}$. Decimos que m y n son **primos relativos** si no existe p primo tal que $p|m$ y $p|n$. Es un hecho que m y n son primos relativos si existen enteros x y y tales que $mx + ny = 1$.
- Sea $n \in \mathbb{Z}_{\geq 2}$, denotamos por $[\,\cdot\,]_n$ a la clase de equivalencia inducida por la relación $a \sim b \iff n|(a-b)$; $a, b \in \mathbb{Z}$. Notemos que $[a]_n = [0]_n$ si y sólo si $n|a$.
- **Los enteros modulo** n son los elementos del siguiente conjunto

$$\mathbb{Z}_n \coloneqq \big\{[a]_n \mid a \in \mathbb{Z}\big\} = \big\{[a]_n \mid a = 0, 1, \ldots, n-1\big\}$$

Los enteros modulo n

Es fácil verificar que el conjunto $\mathbb{Z}_n$ con las operaciones $+$ y $\times$ dadas por

$$[a]_n + [b]_n = [a +_{\mathbb{Z}} b]_n \text{ y } [a]_n \times [b]_n = [a \times_{\mathbb{Z}} b]_n \text{ para toda } a, b \in \mathbb{Z}$$

forma un anillo. Demostramos que $\times$ se distribuye respecto a $+$. Para simplificar la notación, omitimos el subíndice de las operaciones de $\mathbb{Z}$.

$$\begin{aligned}
[a]_n \times \big([b]_n + [c]_n\big) &= [a]_n \times \big([b+c]_n\big) \\
&= \big[a \times (b+c)\big]_n \\
&= [a \times b + a \times c]_n \\
&= [a \times b]_n + [a \times c]_n \\
&= \big([a]_n \times [b]_n\big) + \big([a]_n \times [c]_n\big)
\end{aligned}$$

Mas recordatorios

- El teorema fundamental de la aritmética nos dice que todo entero mayor que 1 tiene una factorización en primos que es única salvo el orden de los factores.
- Supongamos que $q \in \mathbb{Q}$. Es un hecho que existen dos únicos enteros $a, b \in \mathbb{Z}$ tales que a, b son primos relativos y $q = \frac{a}{b}$; a esta descomposición de q le llamamos la **forma reducida de** q.
- También, necesitaremos el siguiente lema:

Una propiedad del denominador de la forma reducida

Lema 1

Sea $p \in \mathbb{Z}$ un primo fijo. Si $m, n \in \mathbb{Z}$ y n no es divisible por p, entonces la forma reducida de $\frac{m}{n}$ tiene un denominador que no es divisible por p.

Demostración. La idea es la siguiente: (1) consideras las factorizaciones en primos de m y n observando que como p no divide a n, te das cuenta de que p no aparece en la factorización de n, (2) simplificas para obtener la forma reducida, (3) te das cuenta que el denominador de la forma reducida es 1 o es un producto de primos distintos de p (al fin y al cabo, solo eliminaste factores de un producto que desde un principio no contenía a p). $\square$

Un subanillo de $\mathbb{Q}$ cortesía del teorema fundamental de la aritmética

Sea $p \in \mathbb{Z}$ un primo fijo y

$$R \coloneqq \left\{ \frac{m}{n} \in \mathbb{Q} \mid m, n \in \mathbb{Z} \text{ son primos relativos y } n \text{ no es divisible por } p \right\}.$$

Veamos que R es un subanillo de $\mathbb{Q}$. Supongamos que $\frac{a}{b}, \frac{c}{d} \in R$. Por definición, b, d no son divisibles por p y por lo tanto, bd tampoco[1]. Por el lema 1, la forma reducida de $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ tiene un denominador que no es divisible por p y por lo tanto, pertenece a R. Por la misma razón, $\frac{a}{b} - \frac{c}{d} = \frac{ad-cb}{bd} \in R$. Por lo tanto, R es un subanillo de $\mathbb{Q}$.

[1] De lo contrario, como p es primo, $p|bd$ implica $p|b$ o $p|d$. En cualquier caso, una contradicción.

Anillos de funciones

Supongamos que X es un conjunto no vacío y A es un anillo. Sea

$$A^X := \left\{ f \mid f : X \to A \text{ es función} \right\}.$$

Es fácil ver que A^X forma un anillo con las operaciones

$$(f+g)(x) := f(x) +_A g(x) \quad \text{y} \quad (f \cdot g)(x) := f(x) \cdot_A g(x).$$

En efecto, cada una de las propiedades que hay que verificar se siguen de las respectivas propiedades de A.

Aprovechamos esta oportunidad para definir un concepto que resulta útil cuando estudiamos anillos de funciones. Para toda $f \in A^X$, definimos el **soporte de** f como el conjunto

$$\operatorname{supp}(f) := \left\{ x \in A \mid f(x) \neq 0 \right\} \subset A.$$

Anillos de funciones reales

- Sea $\mathcal{C}\left([0,1]\right)$ el conjunto de todas las funciones continuas de $[0,1] \subset \mathbb{R}$ en $\mathbb{R}$. Como $f - g$ y $f \cdot g$ son continuas cuando f y g son continuas, entonces $\mathcal{C}\left([0,1]\right)$ es un subanillo de $\mathbb{R}^{[0,1]}$.
- Sea $\mathbb{R}^{\mathbb{R}}_{\mathrm{supp}}$ el conjunto de todas las $f : \mathbb{R} \to \mathbb{R}$ tales que $\mathrm{supp}(f) \subset [a,b]$ para algunas $a, b \in \mathbb{R}$. Veamos que $\mathbb{R}^{\mathbb{R}}_{\mathrm{supp}}$ es un subanillo de $\mathbb{R}^{\mathbb{R}}$. Supongamos que $f, g \in \mathbb{R}^{\mathbb{R}}_{\mathrm{supp}}$. Por definición, existen $a, b, a', b' \in \mathbb{R}$ tales que $\mathrm{supp}(f) \subset [a,b]$ y $\mathrm{supp}(g) \subset [a',b']$. Es fácil verificar que

$$\mathrm{supp}(f-g), \mathrm{supp}(f \cdot g) \subset [\text{mín}\{a,a'\}, \text{máx}\{b,b'\}].$$

  Por lo tanto, $f - g, f \cdot g \in \mathbb{R}^{\mathbb{R}}_{\mathrm{supp}}$.

Anillos de polinomios

Supongamos que R es un anillo y que x es una variable indeterminada. Una suma formal

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \tag{1}$$

con $n \in \mathbb{Z}_{\geq 0}$ y $a_i \in R$ es un **polinomio en x con coeficientes en R**. A el conjunto de todos los polinomios en x con coeficientes en R lo denotamos por $R[x]$ y lo llamamos **el anillo de polinomios en x sobre R**. Específicamente,

$$R[x] := \left\{ a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mid n \in \mathbb{Z}_{\geq 0} \text{ y } a_i \in R \right\}$$

Por brevedad, normalmente denotamos a los elementos de $R[x]$ por símbolos como "$p(x)$" o "$a(x)$". Hay que tener cuidado de no confundir esta notación con la notación usual de evaluar una función en un valor. De hecho, pronto veremos que si R no es conmutativo, no es formalmente correcto pensar en los polinomios sobre R como funciones de R en R.

Supongamos que $p(x) \coloneqq a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$.

- Si $a_i = 0$ para toda $i > 0$, decimos que $p(x)$ es un **polinomio constante**. En este caso tendremos $p(x) = a_0$ con $a_0 \in R$. Por eso hay una inclusión natural $R \hookrightarrow R[x]$ y de hecho identificamos a R con el conjunto de polinomios constantes. De esta manera, hacemos la natural convención de que $R \subset R[x]$.
- Si $a_n \neq 0$, decimos que $p(x)$ tiene **grado** n y escribimos $\deg p(x) = n$. Mas aun, decimos que $a_n x^n$ es su **termino delantero** y que a_n es su **coeficiente delantero**. Si $a_n = 1$, decimos que $p(x)$ es **mónico**.
- Si $a_i = 0$ para toda i, decimos que $p(x)$ es el **polinomio cero**, y escribimos $p(x) = 0$. También, definimos $\deg 0 = -1$.

Cabe recalcar que el grado de todo polinomio constante no cero es 1, pero el grado del polinomio cero es -1.

Las operaciones que hacen que $R[x]$ sea un anillo son precisamente las que estas pensando. Específicamente,

La suma se hace componente a componente:

$$\Big(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0\Big) + \Big(b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0\Big) =$$
$$(a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0).$$

Cabe recalcar que aquí, a_n o b_n puede ser cero y por lo tanto, la igualdad anterior define la suma entre polinomios de cualesquiera grados.

La multiplicación se define por pasos: Primero, definimos la multiplicación para polinomios con exactamente un solo coeficiente distinto de 0 de la siguiente manera: $(ax^i)(bx^j) = abx^{i+j}$. Luego, extendemos esta definición a todos los polinomios usando las leyes distributivas (a este procedimiento, usualmente se le conoce como "expandir y agrupar términos similares"):

$$(a_0 + a_1 x + a_2 x^2 + \cdots)(b_0 + b_1 x + b_2 x^2 + \cdots) =$$
$$a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots$$

Para ser precisos,

$$\left(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0\right)\left(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0\right) = c_{n+m}x^{n+m} + c_{n+m-1}x^{n+m-1} + \cdots + c_1 x + c_0.$$

donde

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} \text{ para toda } k \in \{1, \ldots, n+m\}.$$

En otras palabras, el k-esimo coeficiente del producto, es la suma de todos los productos $a_i b_j$ cuyos coeficientes suman k, es decir, $i + j = k$.

Por otro lado, notemos que si R es tal que $a \neq 0 \neq b \implies ab \neq 0$ para toda $a, b \in R$, entonces para cualesquiera $p(x), q(x) \in R[x]$,

$$\deg(p(x) + q(x)) = \deg p(x) + \deg q(x).$$

En efecto, si $p(x)$ y $q(x)$ tienen términos delanteros $a_n x^n$ y $b_m x^n$ respectivamente, entonces (como $a_n b_m \neq 0$) el termino delantero de $p(x)q(x)$ es $a_n b_m x^{n+m}$.

Ahora, veamos una cuenta especifica: Sea $R = \mathbb{Z}_3$ y denotemos (haciendo abuso de la notación) $k = [k]_3$. Si

$$p(x) = x^2 + 2x + 1, \quad \text{y} \quad q(x) = x^3 + x + 2,$$

entonces

$$\begin{aligned} p(x) + q(x) &= (0+1)x^3 + (1+0)x^2 + (2+1)x + (1+2) \\ &= x^3 + x^2 + 3x + 3 = x^3 + x^2 \end{aligned}$$

y (el lector podrá fácilmente verificar que)

$$p(x)q(x) = x^5 + 2x^4 + 2x^3 + x^2 + 2x + 2.$$

Finalmente, notemos que una de las razones por la que la elección de R es importante es el siguiente tipo de situaciones: el polinomio $x^2 + 1$ no es un cuadrado perfecto en $\mathbb{Z}[x]$, pero *si* es un cuadrado perfecto en $\mathbb{Z}_2[x]$. En efecto, en $\mathbb{Z}_2[x]$,

$$(x+1)^2 = x^2 + 2x + 1 = x^2 + 1.$$

Anillos de matrices

Supongamos que $n \in \mathbb{Z}_{\geq 1}$ y que R es un anillo. Sea $M_n(R)$ el conjunto de matrices $n \times n$ con entradas en R. Con la suma y el producto usual de matrices, $M_n(R)$ es un anillo.

Los cuaterniones (el conjunto)

El siguiente ejemplo tal vez el mas complicado hasta el momento. Históricamente fue muy importante y como después veremos, también será importante para nosotros.

Supongamos que i, j, k son cualesquiera 3 elementos (distintos) fijos. Sea $\mathbb{H}$ el conjunto de todas las sumas formales[2]

$$\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$$

donde $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$. A los elementos de $\mathbb{H}$ les llamamos **cuaterniones**. Si $\alpha_n = 0$ para alguna $n = 0, 1, 2, 3$, simplemente omitimos el sumando que contiene a α_n. Por ejemplo, escribiríamos $\alpha_1 i + \alpha_3 k$ en vez de $0 + \alpha_1 i + 0j + \alpha_3 k$.

[2] Una forma de pensar en $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ es como el elemento $(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \in \mathbb{R}^4$, pero es mucho mas conveniente escribirlo como suma. Por ejemplo, en vez de escribir "$(0, 1, 0, 0)$" simplemente escribimos "i". Otra forma de pensar en la estructura aditiva de $\mathbb{H}$ es como el $\mathbb{R}$-modulo libre generado por el conjunto $\{1, i, j, k\}$.

Los cuaterniones (las operaciones)

La suma en $\mathbb{H}$ se hace coordenada a coordenada, es decir

$$\begin{aligned}(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) &+ (\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k) \\ &= (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)\, i + (\alpha_2 + \beta_2)\, j + (\alpha_3 + \beta_3)\, k.\end{aligned}$$

Para definir el producto en $\mathbb{H}$, basta definir las siguientes reglas

$$\begin{aligned} i^2 = j^2 = k^2 &= -1 \\ ij = k,\ \ jk = i,\ \ ki &= j \\ ji = -k,\ \ kj = -i,\ \ ik &= -j \end{aligned}$$

La razón por la que es suficiente dar estas reglas para definir el producto, es que para calcular

$$(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) \cdot (\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k)\,,$$

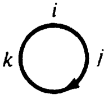
distribuimos como lo haríamos usualmente (teniendo cuidado con el orden de los factores) y ocupamos las reglas para obtener una suma formal

$$\gamma_0 + \gamma_1 i + \gamma_2 j + \gamma_3 k.$$

De hecho, si haces las cuentas, podrás encontrar que

$$\begin{aligned}
\gamma_0 &= \alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3\\
\gamma_1 &= \alpha_0\beta_1 + \alpha_1\beta_0 - \alpha_2\beta_3 - \alpha_3\beta_2\\
\gamma_2 &= \alpha_0\beta_2 - \alpha_1\beta_3 + \alpha_2\beta_0 + \alpha_3\beta_1\\
\gamma_3 &= \alpha_0\beta_3 + \alpha_1\beta_2 - \alpha_2\beta_1 + \alpha_3\beta_0
\end{aligned}$$

Claramente, con estas operaciones, $\mathbb{H}$ es un anillo. Una manera de fácilmente recordar la multiplicación en $\mathbb{H}$ es considerar el siguiente dibujo



Si recorremos el circulo en el sentido de las manecillas del reloj, el producto de dos elementos consecutivos es el siguiente; y si recorremos el circulo en sentido opuesto al de las manecillas del reloj, el producto de dos elementos consecutivos es el siguiente pero en negativo.