Anillos conmutativos y anillos con 1

Facultad de Ciencias UNAM

Introducción

En la sección anterior mencionamos que la suma y multiplicación de un anillo son muy similares a la suma y multiplicación en los sistemas numéricos. Sin embargo, ya hemos visto que un anillo arbitrario puede ser *muy* diferente a un sistema numérico. Tal vez, las dos diferencias mas obvias entre un anillo arbitrario y un sistema numérico son:

- La multiplicación en R no es necesariamente conmutativa.
- R no necesariamente tiene un neutro multiplicativo.

En esta sección introducimos clases especiales de anillos que cumplen estas propiedades y analizamos cuales de los ejemplos que ya conocemos las cumplen.

Anillos conmutativos

Definición

Decimos que R es **conmutativo** si la multiplicación es conmutativa. Es decir, $ab = ba$ para toda $a, b \in R$.

¿Cuales de los ejemplos que ya conocemos son conmutativos?

- Los sistemas numéricos.
- $n\mathbb{Z}$.
- $\mathbb{Z}_n$.
- $\left\{\frac{m}{n} \in \mathbb{Q} \mid m, n \in \mathbb{Z} \text{ son primos relativos y } n \text{ no es divisible por } p\right\}$.
- Si A es conmutativo, entonces A^X también.
- $\mathcal{C}\left([0,1]\right)$.
- $\mathbb{R}^{\mathbb{R}}_{\text{supp}}$.
- Si R es conmutativo, entonces $R[x]$ también.

¿Cuales de los ejemplos que ya conocemos *no* son conmutativos?

- Si A no es conmutativo, entonces A^X tampoco.
- Si R no es conmutativo, entonces $R[x]$ tampoco.
- $M_n(R)$ (si existe $a \in R$ tal que $a^2 \neq 0$). En efecto,

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ a^2 & 0 \end{pmatrix}$$

- Los cuaterniones. Recordemos que por definición,

$$ij = k \;\; y \;\; ji = -k$$

Subanillos y anillos conmutativos

Supongamos que R es un anillo y S es un subanillo de R

- R es conmutativo $\implies$ S es conmutativo. Es inmediato de la definición.
- S es conmutativo $\not\implies$ R es conmutativo. En otras palabras, un anillo no conmutativo puede tener subanillos conmutativos. Considera el siguiente subconjunto de los cuaterniones:

$$\mathbb{R} + \mathbb{R}i := \{\alpha + \beta i \mid \alpha, \beta \in \mathbb{R}\} \subset \mathbb{H}$$

Es facil verificar que $\mathbb{R} + \mathbb{R}i$ es un subanillo de $\mathbb{H}$ que es conmutativo[1] pero ya sabemos que los cuaterniones no lo son.

Por supuesto, la $i \in \mathbb{H}$ no tiene nada de especial. Es decir, $\mathbb{R} + \mathbb{R}j$ y $\mathbb{R} + \mathbb{R}k$ satisfacen la misma propiedad.

[1] De hecho, debería ser claro que (desde nuestro punto de vista) este anillo es esencialmente igual a $\mathbb{C}$. Por supuesto, cuando introduzcamos homomorfismos de anillos podremos precisar esta idea de "esencialmente iguales".

Anillo con 1

Definición

Supongamos que R es un anillo. Decimos que R es un **anillo con 1** o que es un **anillo con unidad** si R tiene un neutro multiplicativo (al cual llamamos **unidad**) distinto[2] del neutro aditivo 0.

Específicamente, R es un anillo con 1 si existe un elemento $1 \in R \setminus \{0\}$ tal que $a \times 1 = a = 1 \times a$ para toda $a \in R$.

Cuando haya ambigüedad respecto a la unidad, escribimos 1_R para denotar la unidad de un anillo R.

[2] La razón por la que pedimos $1 \neq 0$ es porque de lo contrario, $R = \{0\}$. En efecto, después veremos que en cualquier anillo, $a0 = 0 = 0a$ para toda $a \in R$. Por lo tanto, si $1 = 0$, entonces para toda $a \in R$, $a = a1 = a0 = 0$.

¿Cuales de los ejemplos que ya conocemos tienen 1?

- Los sistemas numéricos.
- $\mathbb{Z}_n$.
- $\left\{\frac{m}{n} \in \mathbb{Q} \mid m, n \in \mathbb{Z} \text{ son primos relativos y } n \text{ no es divisible por } p\right\}$.
- Si A es un anillo con 1, entonces A^X también: la función constante 1.
- $\mathcal{C}\left([0,1]\right)$.
- Si R es un anillo con 1, entonces $R[x]$ también: el polinomio constante $p(x) = 1$ es el neutro multiplicativo.
- Si R es un anillo con 1, entonces $M_n(R)$ también: la matriz identidad

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

  es el neutro multiplicativo.
- Los cuaterniones $\mathbb{H}$.

¿Cuales de los ejemplos que ya conocemos *no* tienen 1?

- Si A no tiene 1, entonces A^X tampoco.
- Si R no tiene 1, entonces $R[x]$ tampoco.
- $n\mathbb{Z}$, donde $n \in \mathbb{Z} \setminus \{0, 1\}$.
- $\mathbb{R}^{\mathbb{R}}_{\text{supp}}$: si tuviera, debería de ser la función constante 1, pero esta no tiene soporte contenido en un intervalo cerrado.

Subanillos y anillos con 1

Supongamos que R es un anillo y S es un subanillo de R. Entonces,

1. R tiene 1 $\not\Longrightarrow$ S tiene 1. Sea $R = \mathbb{Z}_4$ y $S = \{[0]_4, [2]_4\}$. Es fácil verificar que S es un subanillo de $\mathbb{Z}_4$. Sin embargo, no tiene unidad porque $[2]_4 \times [2]_4 = [4]_4 = [0]_4 \neq [2]_4$.
2. R tiene unidad 1_R y S tiene unidad 1_S $\not\Longrightarrow$ $1_R = 1_S$. Sea $R = \mathbb{Z}_6$ y $S = \{[0]_6, [3]_6\}$. Es fácil verificar que S es subanillo de $\mathbb{Z}_6$ y como $[3]_6 \times [3]_6 = [9]_6 = [3]_6$, entonces $[3]_6$ es la unidad de S. Sin embargo, $[1]_6$ es la unidad de $\mathbb{Z}_6$ y $[1]_6 \neq [3]_6$.

Elementos invertibles

Definición

Supongamos que R es un anillo con 1. Decimos que $a \in R$ es **invertible** (en R) si existe un elemento $a^{-1} \in R$ tal que

$$a \times a^{-1} = 1 = a^{-1} \times a$$

También, denotamos

$$R^{\times} := \{a \in R \mid a \text{ es invertible en } R\}$$

Es fácil ver que si $\cdot$ es la multiplicación en R, entones con la multiplicación en R, entonces, $(R^{\times}, \cdot\ )$ forma un grupo (no necesariamente abeliano).

¿Cuáles son los elementos invertibles de los anillos con 1 que ya conocemos?

Como veremos, esta pregunta es un poquito mas complicada que la anterior.

- Los únicos elementos invertibles de $\mathbb{Z}$ son ± 1. Pero todo elemento no nulo en $\mathbb{Q}$, $\mathbb{R}$, o $\mathbb{C}$ es invertible. Por lo tanto, la propiedad "ser invertible" no solo depende del elemento en cuestión, también depende del anillo donde consideremos al elemento.
- Los elementos invertibles de $\mathbb{Z}_n$ son los $[a]_n$ tales que a y n son primos relativos: Supongamos que $a \in \mathbb{Z} \setminus \{0\}$ es tal que a y n son primos relativos. Es decir, existen x y y enteros no nulos tales que $ax + ny = 1$. En particular,

$$[1]_n = [ax + ny]_n = [ax]_n + [ny]_n = [ax]_n + [0]_n = [a]_n \times [x]_n$$

Además, $[x]_n \neq 0$ porque de lo contrario, $n|x$ y tendríamos

$$1 = ax + ny = a(nk) + ny = n(ak + y) \text{ para alguna } k \in \mathbb{Z}.$$

Como $n, ak + y \in \mathbb{Z}$, esto implica $n = 1$. Contradiciendo $n \in \mathbb{Z}_{\geq 2}$. Por lo tanto, si a y n son primos relativos, entonces $[a]_n$ es invertible en $\mathbb{Z}_n$.

En particular, si p es primo, todo elemento no nulo de $\mathbb{Z}_p$ es invertible. En efecto, como p es primo, entonces para toda $a \in \{1, \ldots, p-1\}$, a y p son primos relativos.

- Los elementos invertibles de $R[x]$ son los polinomios constantes cuyo valor es un elemento invertible en R. En efecto, si $p(x) \in R[x]$ es invertible, digamos $p(x)q(x) = 1$ y $q(x)p(x) = 1$, entonces $\deg p(x) + \deg q(x) = 0$. En particular, $\deg p(x) = \deg q(x) = 0$. Por lo tanto, $p(x)$ y $q(x)$ son constantes y (como $p(x)q(x) = 1$) sus valores son invertibles en R.

- Los elementos invertibles de

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

  son los $\frac{m}{n}$ tales que m tampoco es divisible por p.
- Si A tiene 1, los elementos invertibles de A^X son las $f \in A^X$ que satisfacen la siguiente propiedad: para toda $x \in X$, $f(x)$ es invertible en A.
- Los elementos invertibles de $\mathcal{C}\left([0,1]\right)$ son las $f \in \mathcal{C}\left([0,1]\right)$ que satisfacen la siguiente propiedad: $f(x) > 0$ para toda $x \in [0,1]$ o $f(x) < 0$ para toda $x \in [0,1]$. En efecto, en el inciso anterior vimos que necesitamos $f(x)$ invertible para toda $x \in [0,1]$. Como todo elemento no nulo de $\mathbb{R}$ es invertible, esto es equivalente a que $f(x) \neq 0$ para toda $x \in [0,1]$. Finalmente, la continuidad de f implica la afirmación.

- En álgebra lineal se demuestra que los elementos invertibles de $M_n(\mathbb{R})$ son las matrices con determinante no nulo.
- Supongamos que R es un anillo conmutativo con 1 y

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R).$$

Definimos $det(A) := ad - bc \in R$. Veamos que A es invertible en $M_2(R)$ si y sólo si $det(A)$ es invertible en R.

Si $det(A)$ es invertible en R, entonces por una cuenta directa

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} d \cdot \det(A)^{-1} & -b \cdot \det(A)^{-1} \\ -c \cdot \det(A)^{-1} & a \cdot \det(A)^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Conversamente, es fácil ver que para toda $A, B \in M_2(R)$, $det(A \cdot B) = det(A) \cdot det(B)$. Por lo tanto, si A es invertible,

$$det(A) \cdot det(A^{-1}) = det(A \cdot A^{-1}) = det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$$

- Veamos que todo cuaternion no nulo es invertible. Supongamos que $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$. Una cuenta directa demuestra que

$$\begin{aligned}(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) \cdot (\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) \\ = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2.\end{aligned}$$

Si ponemos $\beta = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2$, la igualdad anterior implica

$$(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) \cdot \left(\frac{\alpha_0}{\beta} - \frac{\alpha_1}{\beta} i - \frac{\alpha_2}{\beta} j - \frac{\alpha_3}{\beta} k \right) = 1$$

cuando $\beta \neq 0$ o equivalentemente, cuando $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \neq 0$. Por lo tanto, todo cuaternion no nulo es invertible.

Una propiedad básica de los anillos con 1

Proposición 1

Si R tiene 1, entonces $(-1)a = -a$.

Demostración. Para todo $a \in R$ tenemos

$$(-1)a + a = (-1)a + 1a = (-1+1)\,a = 0a = 0.$$

a^0 y a^{-n}

Definición

Supongamos que R es un anillo con 1.

- Para toda $a \in R$ definimos $a^0 := 1$.
- Si $a \in R$ es invertible, entonces para toda $n \in \mathbb{Z}_{\geq 1}$ definimos $a^{-n} := (a^n)^{-1}$.