Anillos con división y dominios

Facultad de Ciencias UNAM

Introducción

Empecemos esta sección con una observacion: en el anillo $\mathbb{Z}$, los únicos enteros que tienen inverso multiplicativo son[1] ± 1. Por otro lado, en el anillo $\mathbb{Q}$, todos los elementos tiene un inverso multiplicativo. Esta diferencia nos lleva a definir una clase especial de anillo que por obvias razones, llamamos *anillos con división*.

En esta sección definimos a los anillos con división y analizamos cuales de nuestros ejemplos satisfacen (o no) esta definición. Después, introducimos otra clase especial de anillos que tiene una relación interesante con los anillos con división. La razón por la que es un poco larga esta sección es justo porque analizamos esta relación.

[1] Por supuesto, si $n \in \mathbb{Z} \setminus \{0, \pm 1\}$, entonces $\frac{1}{n} \in \mathbb{Q} \setminus \mathbb{Z}$ es su inverso multiplicativo en $\mathbb{Q}$. Lo importante es que $\frac{1}{n} \notin \mathbb{Z}$.

Unos recordatorios de la sección anterior

1. Los elementos invertibles de $\mathbb{Z}_n$ son los $[a]_n$ tales que a y n son primos relativos. En particular, si p es primo, todo elemento no nulo de $\mathbb{Z}_p$ es invertible.
2. Todo cuaternion no nulo es invertible.

Anillos con división

Definición

Decimos que R es un **anillo con división** si R es un anillo con 1 y todo elemento no nulo en R es invertible.

¿Cuales de los anillos con 1 que ya conocemos son anillos con división?

Como un anillo con división es aquel que tiene todos sus elementos invertibles, nuestro trabajo anterior va a resultar útil.

- $\mathbb{Q}$, $\mathbb{R}$, y $\mathbb{C}$.
- Si p es primo, $\mathbb{Z}_p$ es anillo con división (c.f. recordatorio 1).
- Los cuaterniones (c.f. recordatorio 2). De hecho, esta es una de las propiedades que hace tan importantes a los cuaterniones: son un anillo no conmutativo con división.

¿Cuales de los anillos con 1 que ya conocemos son anillos *sin* división?

- $\mathbb{Z}$: Sus únicos elementos invertibles son ± 1.
- $\mathbb{Z}_n$ si n no es primo (c.f. recordatorio 1).
- $\left\{ \frac{m}{n} \in \mathbb{Q} \mid m, n \in \mathbb{Z} \text{ son primos relativos y } n \text{ no es divisible por } p \right\}$.
- $R[x]$, para cualquier anillo R.

- A^X cuando A tiene 1 y X no consiste de un solo elemento: Recordemos que un elemento $f \in A^X$ es invertible si y solo si satisface la siguiente propiedad: para toda $x \in X$, $f(x)$ es invertible. Por lo tanto, si $A \neq 0$ y X no consiste de solo un elemento, entonces A^X es un anillo sin división. En efecto, si $a \in A \setminus \{0\}$ y $x_0 \in X$ es fijo, considera

$$f : X \to A$$

$$x \mapsto \begin{cases} a & \text{si } x = x_0 \\ 0 & \text{si } x \neq x_0 \end{cases}$$

- $M_n(R)$ donde R es un anillo con 1: Recordemos que en el caso $n = 2$ dimos condiciones y necesarias para que una matriz fuese invertible.

Subanillos y anillos con división

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

- R anillo con división $\not\Longrightarrow$ S anillo con división:
  Considera $R = \mathbb{Q}$ y $S = \mathbb{Z}$.
- S anillo con división $\not\Longrightarrow$ R anillo con división:
  En otras palabras, un anillo sin división puede tener un subanillo con división. Considera $R = \mathbb{R}^{\mathbb{R}}$ y

$$S := \left\{ f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ es constante} \right\}$$

  Es fácil verificar que S es un subanillo de R con división.

Divisores de 0, dominios, y dominios enteros

Definición

- Decimos que $a \in R \setminus \{0\}$ es un **divisor de 0** si existe $b \in R \setminus \{0\}$ tal que $ab = 0$.
- Decimos que R es un **dominio** si

$$\forall a, b \in R \, (ab = 0 \implies a = 0 \text{ o } b = 0) \, .$$

  Es fácil verificar que R no es un dominio si y sólo si R tiene un divisor de 0.
- Decimos que R es un **dominio entero** si R es un dominio conmutativo.

Comentario

En lo que sigue, veremos que el concepto “dominio” complementa muy bien al concepto “anillo con división”. Por eso, en vez de presentar ejemplos inmediatamente después de la definición (como usualmente hacemos), primero establecemos la relación que tiene esta clase especial de anillo con los anillos con división.

Los primero que veremos es que hay una propiedad que se satisface en dominios y en anillos con división.

En un dominio podemos cancelar factores no nulos

Proposición 1

Supongamos que R es un dominio y que $a \neq 0, b, c \in R$. Si $ab = ac$, entonces $b = c$.

Demostración. La igualdad $ab = ac$ implica

$$a(b - c) = ab - ac = 0.$$

Como R es dominio, $a = 0$ o $b - c = 0$. Pero por hipótesis, $a \neq 0$. De donde, $b - c = 0$ y $b = c$. □

Observación. En un anillo con división también podemos cancelar factores no nulos[2].

[2] $a \neq 0$ implica a invertible. Por lo tanto, podemos multiplicar a^{-1} por la izquierda en la ecuación.

Comentario

Una diferencia inmediata entre los anillos con división y los dominios es que los anillos con división siempre tienen unidad, pero hay dominios sin unidad (por ejemplo $2\mathbb{Z}$). Por eso, excluimos este caso de nuestro análisis.

Por otro lado, como (1) ningún elemento de un dominio es un divisor de 0 y (2) todo elemento de un anillo con división es invertible, es buena idea primero comparar divisores de 0 contra elementos invertibles.

Elementos invertibles vs. Divisores de 0

Proposición 2

Supongamos que R es un anillo con 1. Si $a \in R$ es invertible, entonces $a \in R$ no es divisor de cero.

En particular,

$$\text{Anillo con división} \implies \text{dominio con 1.} \tag{1}$$

Demostración. Sea R un anillo, procedemos por contradicción. Es decir, supongamos que existe $a \in R \setminus \{0\}$ invertible y divisor de 0. Entonces, existe $b \in R \setminus \{0\}$ tal que $ab = 0$. Multiplicando a^{-1} por la izquierda obtenemos $0 = a^{-1}0 = a^{-1}ab = 1b = b$. Contradiciendo $b \in R \setminus \{0\}$.

La implicación (1) es consecuencia inmediata del resultado anterior y de las definiciones

- Anillo con división $\iff$ todo elemento es invertible.
- Dominio $\iff$ ningún elemento es divisor de 0.

□

Comentario

Es natural preguntarse si el converso de la implicación (1) es cierto. Es decir,

$$\text{Dominio con 1} \implies \text{anillo con división?}$$

En lo que sigue, veremos que esta implicación *no* es cierta, pero también daremos condiciones suficientes para que se satisfaga.

Anillos con división vs. Dominios con 1

Proposición 3

1. Dominio con 1 $\not\Longrightarrow$ anillo con división.
2. Dominio finito con 1 $\Longrightarrow$ anillo con división.

Demostración.

1. Considera

$$R := \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \mid \alpha_i \in \mathbb{Z} \text{ para toda } i\} \subset \mathbb{H}$$

Es fácil verificar que R es subanillo (para ver que es cerrado bajo multiplicación, usa las expresiones de las γ_i's). Como $\mathbb{H}$ es un anillo con división, el ejercicio 1 implica que es dominio; y como ser dominio se preserva bajo subanillos, R también es dominio. Sin embargo, $1 + i \in R$ pero su inverso multiplicativo $\frac{1}{2} - \frac{1}{2}i \notin R$. De donde, R no es un anillo con división.

2. Damos dos demostraciones:

   Demostración 1. Supongamos que R es un dominio finto. Para cada $a \in R \setminus \{0\}$, sea $f_a : R \to R$ tal que $f_a(x) = ax$.

   Como en un dominio podemos cancelar factores no nulos, f_a es inyectiva. Mas aun, como R es finito y f_a va de R en R, entonces f_a es suprayectiva[3]. En particular, existe $b \in R$ tal que $ab = f_a(b) = 1$.

   Resta probar[4] que $ba = 1$. Como $ab = 1$, multiplicando a por la derecha obtenemos

$$a(ba) = (ab)a = 1a = a1$$

   Finalmente, cancelando a por la izquierda, obtenemos $ba = 1$.

[3] Recuerda que A, B son conjuntos finitos con la misma cardinalidad, $f : A \to B$ es inyectiva $\iff$ $f : A \to B$ es suprayectiva.

[4] Si asumiéramos R conmutativo, ya habríamos acabado.

Demostración 2. Procedamos por contradicción. Es decir, supongamos que existe un anillo R que es un dominio finito con 1 sin división. Como no tiene división, existe un $a \in R \setminus \{0\}$ que no tiene inverso multiplicativo. Veamos que $a^n \neq a^m$ si $n, m \in \mathbb{Z}_{\geq 1}$ son distintos. Supongamos lo contrario, es decir, existen $n, m \in \mathbb{Z}_{\geq 1}$ distintos tales que $a^n = a^m$; así contradiciendo la finitud de R. Sin perdida de generalidad, supongamos que $n > m$. Entonces,

$$a^m a^{n-m} = a^n = a^m = a^m 1$$

Cancelando a^m por la izquierda[5] obtenemos $a^{n-m} = 1$. Pero entonces, $a^{n-m-1} \cdot a = a \cdot a^{n-m-1} = 1$. Contradiciendo que a no tiene inverso multiplicativo. Por lo tanto, $a^n \neq a^m$ si $n, m \in \mathbb{Z}_{\geq 1}$.

□

[5] Podemos cancelar porque como R es dominio, entonces $a^m \neq 0$.

Comentario

Otra diferencia entre los dominios con 1 y los anillos con división es que todo subanillo de un dominio es un dominio (verifícalo), pero (como ya vimos anteriormente) no todo subanillo de un anillo con división es un anillo con división.

Ahora bien, antes de proceder a ver ejemplos de dominios encontramos los divisores de 0 de nuestros ejemplos. La razón para hacer esto es que la propiedad "ser dominio" esta determinado por la existencia o falta de divisores de 0 en el anillo.

¿Cuales son los divisores de 0 de los anillos que ya conocemos?

- Los sistemas numéricos: No tienen ningún divisor de 0.
- $\mathbb{Z}_n$: Los $[a]_n$ tales que a y n no son primos relativos: Supongamos que $a \in \mathbb{Z} \setminus \{0\}$ es tal que a y n no son primos relativos. Es decir, existe p primo tal que $p|a$ y $p|n$. En particular, $\frac{a}{p}, \frac{n}{p} \in \mathbb{Z} \setminus \{0\}$, $\left[\frac{n}{p}\right]_n$ es no nulo[6], y podemos hacer la siguiente cuenta

$$[a]_n \times \left[\frac{n}{p}\right]_n = \left[a \cdot \frac{n}{p}\right]_n = \left[\frac{a}{p} \cdot n\right]_n \left[\frac{a}{p}\right]_n \times [n]_n = \left[\frac{a}{p}\right]_n \times [0]_n = [0]_n.$$

  Por lo tanto, juntando esto con el Recordatorio 1, tenemos que para toda $n \in \mathbb{Z}_{\geq 2}$, $[a]_n$ es invertible ó divisor de 0.

[6] Claramente, $\frac{n}{p} \in \{1, \ldots, n-1\}$.

- A^X: Es fácil ver que si $f, g \in A^X$ son tales que $\operatorname{supp}(f) \cap \operatorname{supp}(g) = \emptyset$, entonces $f \cdot g = 0$. Para garantizar la existencia de funciones con soportes ajenos, basta suponer que X no consiste de solo un elemento y que $A \neq 0$. En efecto, sean $x_0 \in X$ y $a \in A \setminus \{0\}$ fijos, definimos

$$f : X \to A \qquad\qquad g : X \to A$$

$$x \mapsto \begin{cases} a & \text{si } x = x_0 \\ 0 & \text{si } x \neq x_0 \end{cases} \qquad x \mapsto \begin{cases} a & \text{si } x \neq x_0 \\ 0 & \text{si } x = x_0 \end{cases}$$

  Claramente, $f \neq 0 \neq g$ y $f \cdot g = 0$. De hecho, es fácil verificar que si A es dominio, el converso se vale. Es decir, si $f \cdot g = 0$, entonces $\operatorname{supp}(f) \cap \operatorname{supp}(g) = \emptyset$.
- $\mathcal{C}\left([0,1]\right)$: Sus divisores de 0 son aquellas funciones f tales que $\operatorname{supp}(f)$ contiene un intervalo[7]. Mas aun, $\mathcal{C}\left([0,1]\right)$ tiene elementos no invertibles que tampoco son divisores de 0[8].

[7] Si I es este intervalo y g es la función característica de I, entonces $f \cdot g = 0$.

[8] Considera $f(x) = x - \frac{1}{2}$.

- $R[x]$: En la siguiente sección veremos que

$$R \text{ no tiene divisores de } 0 \iff R[x] \text{ no tiene divisores de } 0$$

o equivalentemente,

$$R \text{ es un dominio} \iff R[x] \text{ es un dominio.}$$

- Lamentablemente, no vamos a encontrar todos los divisores de 0 en $M_n(R)$ porque requiere bastante mas teoría. Lo que si vamos a ver es que $M_n(R)$ tiene divisores de 0 si $R \neq 0$: Supongamos que $a \in R \setminus \{0\}$. Una cuenta directa demuestra que

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

¿Cuales de los anillos que ya conocemos son dominios?

Como anillo con división implica dominio, omitimos a los anillos con división en la siguiente lista.

- $\mathbb{Z}$ es el ejemplo mas sencillo de un dominio sin división. En particular $n\mathbb{Z}$ también es domino.
- $\left\{\frac{m}{n} \in \mathbb{Q} \mid m, n \in \mathbb{Z} \text{ son primos relativos y } n \text{ no es divisible por } p\right\}$ porque es subanillo de $\mathbb{Q}$.
- Si R es dominio, entonces $R[x]$ también.

¿Cuales de los anillos que ya conocemos *no* son dominios?

- $\mathbb{Z}_n$ si n no es primo.
- A^X si $A \neq 0$ y X no consiste de un solo elemento.
- $\mathcal{C}\left([0,1]\right)$.
- $\mathbb{R}^{\mathbb{R}}_{\text{supp}}$.
- $R[x]$ si R no es dominio.
- $M_n(R)$.