Capítulo 4

Cuerpo de fracciones de un dominio de integridad

Objetivos del capítulo

- En este tema vamos a estudiar mas en profundidad los dominios de integridad. Demostraremos que un anillo conmutativo y unitario es de integridad si y sólo si verifica las leyes de cancelación, lo que nos llevara a demostrar que todo dominio de integridad finito es cuerpo.
- Se recuerda la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$ y se generaliza para construir el cuerpo de fracciones de cualquier dominio de integridad. Como resultado particular se demuestra que un anillo es un dominio de integridad si y sólo si es subanillo de un cuerpo.
- Por último generalizaremos la construcción anterior para ciertos conjuntos de denominadores.

---

1. Caracterizaciones de un dominio de integridad

Definición 1 (Recordatorio) Sea R un anillo. Se dice que $0 \neq a \in R$ es:

- Un **divisor de cero por la izquierda** si existe $0 \neq b \in R$ tal que $a \cdot b = 0$.
- Un **divisor de cero por la derecha** si existe $0 \neq b \in R$ tal que $b \cdot a = 0$.

Nota: (Ejercicio) Si un anillo no tiene divisores de cero por la izquierda, entonces no tiene divisores de cero por la derecha.

Definición 2 (Recordatorio) Un anillo conmutativo y unitario sin divisores de cero se denomina un **dominio de integridad** (normalmente denotaremos los dominios de integridad por D.I.)

Definición 3 (Recordatorio) Recordamos que un anillo R verifica la **ley de cancelación por la izquierda** si dados $a, b, c \in R$ con $c \neq 0$, $ca = cb$ entonces $a = b$. Diremos que un anillo R verifica la **ley de cancelación por la derecha** si dados $a, b, c \in R$ con $c \neq 0$, $ac = bc$ entonces $a = b$.

Proposición 4 (Ejercicio) Sea R un anillo. Las siguientes condiciones son equivalentes:

(i) R verifica la ley de cancelación por la izquierda.
(ii) R no tiene divisores de cero por la izquierda.
(iii) R no tiene divisores de cero por la derecha.
(iv) R verifica la ley de cancelación por la derecha.

Demo: $(i) \implies (ii)$. Supongamos que R verifica la ley de cancelación por la izquierda y sea $0 \neq a \in R$ tal que existe $b \in R$ con $ab = 0$. Tenemos entonces que $ab = 0 = a0$ y como R verifica la ley de cancelación por la izquierda $b = 0$ (luego en R no hay divisores de cero por la izquierda). $(iv) \implies (iii)$ es similar a esta demostración.

$(ii) \implies (iii)$. Supongamos que $0 \neq b$ es un divisor de cero por la derecha, entonces existe $0 \neq a \in R$ tal que $ab = 0$. pero entonces a es un divisor de cero por la izquierda (contradicción). $(iii) \implies (ii)$ es similar a esta demostración.

$(iii) \implies (iv)$. Supongamos que R no tiene divisores de cero por la derecha y sean $a, b, c \in R$, con $a \neq 0$ tales que $ba = ca$. Entonces $0 = ba - ca = (b - c)a$ y como en R no hay divisores de cero por la derecha, $b - c = 0$, es decir $b = c$. $(i) \implies (ii)$ es similar a esta demostración. ■

Nota: A partir de ahora hablaremos de anillos que verifican la ley de cancelación y anillos sin divisores de cero (ya no nos hace falta hablar de derecha o izquierda).

Nota: Todo dominio de integridad y todo anillo de división (en particular todo cuerpo) verifica la ley de cancelación.

Proposición 5 Sea R un anillo. Las siguientes condiciones son equivalentes:

(i) R no posee divisores de cero.
(ii) Para todo par de elementos $a, b \in R$ con $a \neq 0$, la ecuación $aX + b = 0$ si poseen solución, ésta es única.
(iii) Para todo par de elementos $a, b \in R$ con $a \neq 0$, la ecuación $Xa + b = 0$ si poseen solución, ésta es única.

Demo: $(i) \implies (ii)$. Supongamos que en R no hay divisores de cero y sean s, s' dos soluciones de la ecuación. Entonces $as + b = 0$ y $as' + b = 0$. Por tanto $as = -b = as'$ y como en R se verifica la ley de cancelación $s = s'$. $(i) \implies (iii)$ es similar.

$(ii) \implies (i)$. Supongamos que la ecuación $aX + b = 0$ de tener solución ésta es única. Por reducción al absurdo supongamos que R posee un divisor de cero. Entonces existen $a, b \in R$ no nulos tales que $ab = 0$ y por tanto la ecuación $aX = 0$ tiene dos soluciones $s = b$ y $s = 0$, contradicción. $(iii) \implies (i)$ es similar. ■

Proposición 6 Sea R un anillo. Las siguientes condiciones son equivalentes:

(i) R es un anillo de división.
(ii) Para todo par de elementos $a, b \in R$ con $a \neq 0$, la ecuación $aX + b = 0$ poseen solución única.
(iii) Para todo par de elementos $a, b \in R$ con $a \neq 0$, la ecuación $Xa + b = 0$ poseen solución única.

Demo: $(i) \implies (ii)$. Supongamos que R es un anillo de división y sea la ecuación $aX + b = 0$ con $a \neq 0$. Entonces, sea el elemento $s = -a^{-1}b$ que existe ya que R es un anillo de división y $a \neq 0$. Entonces $as + b = a(-a^{-1}b) + b = -b + b = 0$. Luego s es solución de la ecuación. Es más como en un anillo de división no hay divisores de cero, la solución es única. $(i) \implies (iii)$ es similar: es claro que la solución de la ecuación $Xa + b = 0$ es $s' = -ba^{-1}$ (que no tiene que coincidir con s, ya que R no tiene que ser conmutativo).

$(ii) \implies (i)$. En primer lugar demostremos que R es un anillo unitario (ya sabemos que no hay divisores de cero en R por la proposición 5 (Pag. 82)). Dado $0 \neq a \in R$ la ecuación $aX - a = 0$ posee una única solución. Sea $e \in R$ tal que $ae = a$.

Nota: sólo sabemos que $ae = a$ para cualquier otro elemento de $0 \neq b \in R$, el elemento be no sabemos que coincida con b. Planteando la ecuación $bX - b = 0$ sólo conseguiríamos un elemento e' tal que $be' = b$.

Como $ae = a$, si multiplicamos por e por la derecha tendríamos $ae^2 = ae$ y como no hay divisores de cero (por la izquierda) en R, $e^2 = e$ (es decir, e es un idempotente), no nulo de R, ya que si $e = 0$, $ae = 0$, una contradicción. Ahora, dado cualquier $x \in R$, $xe^2 = xe$ y aplicando la ley de simplificación $xe = x$. De forma similar $e^2x = ex$ y por tanto $ex = x$, es decir, e es elemento neutro del producto de R, por lo que R es unitario con unidad e (desde este momento al elemento e se denota por 1). Por último, solo tenemos que demostrar que todo elemento no nulo de R tiene inverso. Dado $0 \neq a \in R$, la ecuación $aX = 1$ posee solución, luego existe $s \in R$ tal que $as = 1$ (con lo que $s \neq 0$). Por tanto, la ecuación $sX = 1$ tiene solución (única) por lo que existe $b \in R$ con $sb = 1$. Ahora,

$$a = a1 = a(sb) = (as)b = 1b = b$$

lo que implica que s es el inverso de a en R. $(iii) \implies (i)$ es similar. ■

Nota: La siguiente noción es muy importante y se usara repetidamente a lo largo de la carrera.

Definición 7 • Sea R un anillo y sea $a \in R$ se define:

- la aplicación de **multiplicación por la izquierda de** a en R y se denota por $\lambda_a : R \to R$ como la aplicación $\lambda_a(x) = a \cdot x$ para todo $x \in R$.
- la aplicación de **multiplicación por la derecha de** a en R y se denota por $\rho_a : R \to R$ como la aplicación $\rho_a(x) = x \cdot a$ para todo $x \in R$.

Proposición 8 (Ejercicio) *Sea R un anillo y sea $a \in R$. Entonces:*

- *a no es divisor de cero por la izquierda si y sólo si $\lambda_a : R \to R$ es una aplicación inyectiva.*
- *a no es divisor de cero por la derecha si y sólo si $\rho_a : R \to R$ es una aplicación inyectiva.*
- *Si a es inversible, $\lambda_a : R \to R$ es biyectiva.*
- *Si a es inversible, $\rho_a : R \to R$ es biyectiva.*
- *Si R es conmutativo y unitario, a es inversible si y sólo si $\lambda_a : R \to R$ es biyectiva.*
- *Si R es conmutativo y unitario, a es inversible si y sólo si $\rho_a : R \to R$ es biyectiva.*

- *Si en R no hay divisores de cero, a es inversible si y sólo si $\lambda_a : R \to R$ es biyectiva.*
- *Si en R no hay divisores de cero, a es inversible si y sólo si $\rho_a : R \to R$ es biyectiva.*

Teorema 9 Todo dominio de integridad finito es cuerpo.

Demo: Sea D un dominio de integridad finito y $0 \neq a \in D$. Veamos que a es un elemento inversible de D. Consideremos la aplicación de multiplicación por la izquierda de a en R,

$$\lambda_a : D \to D \quad \text{definida por} \quad \lambda_a(x) = a \cdot x.$$

Como D verifica la ley de cancelación por la izquierda, λ_a es una aplicación inyectiva: si $\lambda_a(x) = \lambda_a(y)$, entonces $ax = ay$, y por tanto, aplicando la ley de simplificación, $x = y$. Ahora, como D es finito, λ_a es sobreyectiva, luego existe $b \in D$ con $ab = \lambda_a(b) = 1$. Por último, como D es conmutativo $ab = ba = 1$ y a es inversible con inverso b. ■

Nota: Esta demostración te puede ayudar a resolver varios ejercicios del tema.

2. Cuerpo de fracciones de un dominio de integridad

En temas anteriores se ha estudiado $\mathbb{Z}$, el anillo de los enteros. Veamos como se puede construir $\mathbb{Q}$ a partir de $\mathbb{Z}$:

Construcción de los racionales.

⋆ Definimos una relación de equivalencia en el conjunto de los pares $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, en donde $\mathbb{Z}^*$ denota los enteros menos el cero.

Diremos que

$$(a, b) \sim (a', b') \text{ si y sólo si } ab' = a'b.$$

La clase de equivalencia del elemento (a, b) se denota por $\frac{a}{b}$. Sea $\mathbb{Q}$ el conjunto cociente:

$$\mathbb{Q} := \{\frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0\}$$

⋆ Definimos la suma y el producto en el conjunto cociente:

◇ La suma: $\frac{a}{b} + \frac{a'}{b'} := \frac{ab'+ba'}{bb'}$.

◇ El producto: $\frac{a}{b} \cdot \frac{a'}{b'} := \frac{aa'}{bb'}$.

Nos encontramos con que $(\mathbb{Q}, +, .)$ es el cuerpo de los racionales.

En este tema vamos a demostrar que esta construcción no es exclusiva de $\mathbb{Z}$, sino que dado cualquier dominio de integridad D podemos construir un cuerpo Q, tal que D se "sumerge" en Q de forma similar a como $\mathbb{Z}$ se "sumerge" en $\mathbb{Q}$.

Construcción del cuerpo de fracciones de un dominio de integridad.

Aunque la construcción que aquí damos comienza con un dominio de integridad D, realmente no nos van a hacen falta tantas hipótesis, por lo que tras cada una de las demostraciones de las proposiciones de este tema nombraremos las propiedades que se han usado.

Sea D un dominio de integridad. Consideremos

$$D \times D^* := \{(a, b) \in D \times D \mid b \neq 0\}$$

Proposición 1 Sea D un dominio de integridad. Entonces, en $D \times D^*$ la relación,

$$(a, s) \approx (b, r) \text{ si y sólo si } ar = bs,$$

es de equivalencia.

Demo: Veamos que $\approx$ verifica las propiedades reflexiva, simétrica y transitiva:

$\star$ Reflexiva: sea $(a, s) \in D \times D^*$. Entonces $as = as$, con lo que $(a, s) \approx (a, s)$.

$\star$ Simétrica: Supongamos que $(a, s) \approx (b, r)$. Entonces, $ar = bs$ que directamente da $(b, r) \approx (a, s)$.

$\star$ Transitiva: Supongamos que $(a, s) \approx (b, r)$ y $(b, r) \approx (c, t)$. Entonces:

$$ar = bs \quad \text{y} \quad bt = cr.$$

$\star$ Multiplicamos en la primera igualdad por t y $art = bst$.
$\star$ Sustituimos bt por cr (segunda igualdad) obtenemos $art = bts = crs$.
$\star$ Simplificando r, ya que es no nulo y D verificar las leyes de simplificación, $at = cs$. Es decir, $(a, s) \approx (c, t)$. ■

Observación 2 *Las propiedades reflexivas y simétricas solo necesitan que D sea un anillo. Mientras que la propiedad transitiva necesita que los denominadores no sean divisores de cero y conmuten entre sí.*

Definición 3 *El conjunto cociente anterior, $D \times D^*/\approx$, se denotará por $\mathcal{Q}(D)$. La clase de equivalencia de un elemento $(a, s) \in D \times D^*$ será denotada por $\frac{a}{s}$. Dado un elemento $\frac{a}{s} \in \mathcal{Q}(D)$, diremos que a es el numerador y s el denominador.*

Observación: En toda las demostraciones intentaremos usar letras tipo a, b, c, d para los numeradores y s, r, t para los denominadores (en algunos casos con primas, a', s').

Teorema 4 Sea D un dominio de integridad. Entonces, en $\mathcal{Q}(D)$, las operaciones

$\diamondsuit$ Suma: $\frac{a}{s} + \frac{b}{r} := \frac{ar+bs}{rs}$

$\diamondsuit$ Producto: $\frac{a}{s} \cdot \frac{b}{r} := \frac{ab}{rs}$

dotan a $\mathcal{Q}(D)$ de estructura de cuerpo (llamado el **cuerpo de fracciones** del dominio de integridad D). Es más, la aplicación $i : D \to \mathcal{Q}(D)$ definida por $i(d) = \frac{d}{1}$ es un monomorfismo de anillos unitarios.

Demo: Veamos que la suma anterior define una estructura de grupo abeliano en $\mathcal{Q}(D)$, para ello tendremos que demostrar:

(i). Que está bien definida (hace falta ver que el elemento $(ar+bs, rs) \in D \times D^*$ y que esta suma no depende de los representantes.

(i.1) Es claro que $rs \neq 0$ ya que D es un dominio de integridad y $s \neq 0 \neq r$.

(i.2) Veamos que esta suma no depende de los representantes. Supongamos que $(a,s) \approx (a',s')$ y que $(b,r) \approx (b',r')$. Tenemos entonces que:

$$as' = a's \quad \text{y} \quad br' = b'r \tag{H}$$

y queremos demostrar que $(ar+bs, rs) \approx (a'r'+b's', r's')$:

$$\begin{aligned}(ar+bs)r's' &=^{*^1} arr's' + bsr's' =^{*^2} (as')rr' + (br')ss' = \\ &=^{*^3} (a's)rr' + (b'r)ss' =^{*^2} a'r'sr + b's'sr =^{*^1} (a'r'+b's')rs\end{aligned}$$

$*^1$ aplicando la propiedad asociativa y la distributiva.
$*^2$ aplicando la propiedad asociativa y la conmutativa.
$*^3$ aplicando las identidades de (H).
$*^4$ aplicando la propiedad asociativa, la conmutativa y la distributiva.
Luego la suma está bien definida en $\mathcal{Q}(D)$.

(ii). Veamos ahora que $(\mathcal{Q}(D), +)$ tiene estructura de grupo abeliano. Antes veamos algunas propiedades útiles:

(P_1). Dado un elemento no nulo $r \in D$, para todo $\frac{a}{s} \in \mathcal{Q}(D)$, $\frac{a}{s} = \frac{ra}{rs}$.

(P_2). Dos elementos $\frac{a}{s}$, $\frac{b}{r}$ de $\mathcal{Q}(D)$ tienen representantes con el mismo denominador:

$$\frac{a}{s} = \frac{ar}{rs} \text{ y } \frac{b}{r} = \frac{bs}{rs}.$$

Naturalmente, con este proceso se consigue encontrar denominador común a un conjunto finito de elementos de $\mathcal{Q}(D)$.

(P_3). La suma de dos elementos $\frac{a}{s}$ y $\frac{b}{s}$ con el mismo denominador consiste en sumar numeradores:

$$\frac{a}{s} + \frac{b}{s} = \frac{as+bs}{s^2} = \frac{a+b}{s}$$

con estas tres propiedades, ya podemos demostrar fácilmente que $(\mathcal{Q}(D), +)$ tiene estructura de grupo abeliano. Por P_2 voy a tomar, cuando me sea de interés, "fracciones" con el mismo denominador.

(ii.1) Asociativa: sean $\frac{a}{s}, \frac{b}{s}, \frac{c}{s} \in \mathcal{Q}(D)$. Entonces:

$$\left(\frac{a}{s} + \frac{b}{s}\right) + \frac{c}{s} = \frac{a+b}{s} + \frac{c}{s} = \frac{a+b+c}{s} = \frac{a}{s} + \frac{b+c}{s} = \frac{a}{s} + \left(\frac{b}{s} + \frac{c}{s}\right)$$

(ii.2) Conmutativa: sean $\frac{a}{s}, \frac{b}{s} \in \mathcal{Q}(D)$. Entonces:

$$\frac{a}{s} + \frac{b}{s} = \frac{a+b}{s} = \frac{b+a}{s} = \frac{b}{s} + \frac{a}{s}$$

(ii.3) El neutro de la suma es cualquier elemento de la forma $\frac{0}{s}$ con $s \in D^*$.
(ii.4) Opuesto: dado $\frac{a}{s} \in \mathcal{Q}(D)$, $\frac{-a}{s}$ es su opuesto, ya que $\frac{a}{s} + \frac{-a}{s} = \frac{0}{s} = 0$.

(iii). Veamos ahora que el producto está bien definido: (hace falta ver que el elemento $(ab, rs) \in D \times D^*$ y que este producto no depende de los representantes.
(iii.1) Es claro que $rs' \neq 0$ ya que D es un dominio de integridad y $s \neq 0 \neq r$.
(iii.2) Veamos que el producto no depende de los representantes. Supongamos que $(a, s) \approx (a', s')$ y que $(b, r) \approx (b', r')$. Tenemos entonces que:

$$as' = a's \quad \text{y} \quad br' = b'r \tag{H'}$$

Tenemos que demostrar que $(ab, rs) \approx (a'b', r's')$:

$$abr's' = (as')(br') = (a's)(b'r) = a'b'rs.$$

(iii.3) Asociativa: sean $\frac{a}{s}, \frac{b}{r}, \frac{c}{t} \in \mathcal{Q}(D)$. Entonces:

$$\left(\frac{a}{s} \cdot \frac{b}{r}\right) \cdot \frac{c}{t} = \frac{ab}{rs} \cdot \frac{c}{t} = \frac{abc}{rst} = \frac{a}{s} \cdot \frac{bc}{rt} = \frac{a}{s} \cdot \left(\frac{b}{r} \cdot \frac{c}{t}\right)$$

(iv). Distributiva: demostramos sólo la distributiva por un lado, ya que vamos a demostrar que el producto es conmutativo. Sean $\frac{a}{s}, \frac{b}{s}, \frac{c}{t} \in \mathcal{Q}(D)$. Entonces:

$$\left(\frac{a}{s} + \frac{b}{s}\right) \cdot \frac{c}{t} = \frac{a+b}{s} \cdot \frac{c}{t} = \frac{(a+b)c}{st} = \frac{ac+bc}{st} = \frac{ac}{ct} + \frac{bc}{st} = \frac{a}{s} \cdot \frac{c}{t} + \frac{b}{s} \cdot \frac{c}{t}$$

(v). $\mathcal{Q}(D)$ es un cuerpo (anillo conmutativo, unitario en donde todo elemento no nulo tiene inverso):
(v.1) Conmutativa: sean $\frac{a}{s}, \frac{b}{r} \in \mathcal{Q}(D)$. Entonces:

$$\frac{a}{s} \cdot \frac{b}{r} = \frac{ab}{rs} = \frac{ba}{rs} = \frac{b}{r} \cdot \frac{a}{s}$$

(v.2) La unidad de $\mathcal{Q}(D)$: el elemento $\frac{1}{1} = \frac{s}{s}$ para todo $s \in D^*$, es el elemento neutro de la suma.
(v.3) Sea $\frac{a}{s}$ un elemento no nulo de $\mathcal{Q}(D)$. Como es no nulo, ver (ii.3), $a \neq 0$ y por tanto, $\frac{s}{a}$ tiene sentido, y es el inverso de $\frac{a}{s}$:

$$\frac{s}{a}\frac{a}{s} = \frac{sa}{as} = \frac{1}{1}$$

(vi). Veamos que la aplicación $i : D \to \mathcal{Q}(D)$, definida por $i(d) := \frac{d}{1}$, es un monomorfismo de anillos.

$$i(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = i(a) + i(b)$$
$$i(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = i(a)i(b)$$

Por último si $i(b) = 0$, entonces $\frac{b}{1} = \frac{0}{1}$ por lo que $b \cdot 1 = 0 \cdot 1 = 0$ y $b = 0$, es decir, i es una aplicación inyectiva. ■

Corolario 5 Un anillo D es un dominio de integridad si y sólo si es subanillo (unitario) de un cuerpo.

Teorema 6 (Ejercicio) Sea D un dominio de integridad, $\mathbb{F}$ un cuerpo y $h : D \to \mathbb{F}$ un monomorfismo de anillos. Entonces existe un único monomorfismo de anillos $f : \mathcal{Q}(D) \to \mathbb{F}$ que hace conmutativo el diagrama.

$$\begin{tikzcd} D \arrow[r, "i"] \arrow[dr, "h"'] & \mathcal{Q}(D) \arrow[d, dotted, "f"] \\ & \mathbb{F} \end{tikzcd}$$

Demo: En principio nos dicen que existe un único homomorfismo f de $\mathcal{Q}(D)$ en $\mathbb{F}$ que hace conmutativo el diagrama. Veamos en primer lugar que podemos saber de f (supongamos que existe un homomorfismo f y veamos como tiene que definirse):

Dado $d \in D$, como el diagrama es conmutativo,

$$h(d) = f \circ i(d) = f(d/1).$$

Por otro lado, como i y h son aplicaciones inyectivas, si d' es un elemento no nulo de D, $i(d') = d'/1$ es un elemento no nulo de $\mathcal{Q}(D)$, $h(d')$ es un elemento no nulo de $\mathbb{F}$ y $f(d'/1)$ es un elemento no nulo de $\mathbb{F}$. Por tanto estos elementos son inversibles por lo que

$$f(1/d') = f(d'/1)^{-1} = h(d')^{-1}$$

Por tanto, tenemos una única forma de definir f: Dado $a/r \in \mathcal{Q}(D)$,

$$f(a/r) = f(a/1 \cdot 1/r) = f(a/1) \cdot f(1/r) = h(a)h(r)^{-1}$$

Veamos que esta única forma de definir f es un monomorfismo de anillos que hace conmutativo el diagrama:

i). Veamos que f está bien definida: Si $a/r = a'/r'$, entonces $ar' = a'r$, por lo que $h(a)h(r') = h(ar') = h(a'r) = h(a')h(r)$. Como $h(r)$ y $h(r')$ son no nulos, podemos multiplicar por sus inversos, con lo que $h(a) = h(a)h(r')h(r')^{-1} = h(a')h(r)h(r')^{-1} = h(a')h(r')^{-1}h(r)$ y multiplicando pro el inverso de $h(r)$, $h(a)h(r)^{-1} = h(a')h(r')^{-1}$, es decir, $f(a/r) = f(a'/r')$.

ii). Veamos que es un homomorfismo de anillos:

$$\begin{aligned} \star\ f(a/r + b/r) &= f((a+b)/r) = h(a+b)h(r)^{-1} = (h(a)+h(b))h(r)^{-1} \\ &= h(a)h(r)^{-1} + h(b)h(r)^{-1} = f(a/r) + f(b/r) \\ \star\ f(a/r \cdot b/s) &= f(ab/rs) = h(ab)h(rs)^{-1} = h(a)h(b)(h(r)h(s))^{-1} = h(a)h(b)h(s)^{-1}h(r)^{-1} \\ &= h(a)h(r)^{-1}h(b)h(s)^{-1} = f(a/r)f(b/s) \end{aligned}$$

iii). Veamos que f es un monomorfismo de anillos: sea $a/r \in \mathrm{Ker}(f)$. Entonces $0 = f(a/r) = h(a)h(r)^{-1}$, multiplicando, en ambos miembros, por $h(r)$, $h(a) = 0$ y como h es un monomorfismo de anillos, $a = 0$, por lo que $a/r = 0/r$, es decir, $\mathrm{Ker}(f) = \{0\}$ y por tanto f es inyectiva. ∎

3. Complemento de la Teoría

La segunda parte importante del cuerpo de fracciones $\mathcal{Q}(D)$ de un dominio de integridad D es que es el cuerpo "más pequeño" que contiene a D. Naturalmente la noción de "ser más pequeño que" significa (este teorema es complemento del anterior):

Teorema 1 Sea D un dominio de integridad, $\mathbb{F}$ un cuerpo y $h : D \to \mathbb{F}$ un monomorfismo de anillos. Entonces existe un único monomorfismo de anillos $f : \mathcal{Q}(D) \to \mathbb{F}$ que hace conmutativo el diagrama.

$$\begin{tikzcd} D \arrow[r, "i"] \arrow[dr, "h"'] & \mathcal{Q}(D) \arrow[d, dotted, "f"] \\ & \mathbb{F} \end{tikzcd}$$

Es más, si Q es un cuerpo tal que existe un monomorfismo de anillos $i : D \to Q$ y tal que para cada cuerpo $\mathbb{F}$ y cada monomorfismo de anillos $h : D \to \mathbb{F}$, existe un único monomorfismo de anillos $f : Q \to \mathbb{F}$ que hace conmutativo el diagrama. Se tiene que Q es isomorfo al cuerpo de fracciones de D.

$$\begin{tikzcd} D \arrow[r, "i"] \arrow[dr, "h"'] & Q \arrow[d, dotted, "f"] \\ & \mathbb{F} \end{tikzcd} \implies \quad Q \approx \mathcal{Q}(D).$$

En todo este tema hemos partido de D, un dominio de integridad, pero ¿nos hacia falta tanto?

Corolario 2 Un anillo R es conmutativo y sin divisores de cero si y sólo si es subanillo de un cuerpo.

Si nos fijamos bien en la demostraciones que hemos hecho, ¿donde se usa que D sea unitario?

En la proposición 1 (Pag. 85) no se usa el carácter unitario: la relación $(a, b) \approx (a', b')$ si y sólo si $ab' = a'b$ es de equivalencia, sea D unitario o no.

El Teorema 4 (Pag. 85) demuestra que el conjunto cociente, $\mathcal{Q}(D)$ con las operaciones definidas tiene estructura de anillo (aquí no hace falta la unidad. Para demostrar que $\mathcal{Q}(D)$ es un cuerpo (luego unitario), parece ser que sí. No obstante, dado $0 \neq a \in D$, $\frac{a}{a}$ es la unidad de $\mathcal{Q}(D)$ y el inverso de un elemento no nulo $\frac{b}{a}$ sigue siendo $\frac{a}{b}$. Por lo que la unidad de D, en realidad, no ha hecho falta.

Si nos damos cuenta, los últimos teoremas tampoco hacen uso de que D tiene un elemento unitario.

Definición 3 Sea R un anillo. Se define $Z(R)$, el centro de R, como:

$$Z(R) = \{z \in R \mid za = az \quad \forall\, a \in R\}$$

Definición 4 Sea R un anillo. Se dice que un subconjunto $S \subset R$ es un conjunto de denominadores para R si.

- $S \subset Z(R)$,
- S no contiene divisores de cero y
- $S \cdot S \subset S$ (S es un subconjunto multiplicativamente cerrado de R).

Corolario 5 Sea R un anillo y sea $S \subset R$ es un conjunto de denominadores para R. Entonces existe un anillo Q que contiene a R como subanillo y tal que todo elemento de S es inversible en Q.

Se puede dar una construcción idéntica a la construcción del cuerpo de fracciones:

⋆ Se considera el conjunto $R \times S$ y la relación $(a, s) \approx (b, r)$ si y sólo si $ar = bs$. Se comprueba que es un relación de equivalencia. La clase de equivalencia de un elemento (a, s) se denota por $\frac{a}{s}$ y el conjunto cociente por $S^{-1}R$.

⋆ Se define una suma y un producto en $S^{-1}R$ como:

  - La suma: $\frac{a}{s} + \frac{b}{r} := \frac{ar+bs}{rs}$.
  - El producto: $\frac{a}{s} \cdot \frac{b}{r} := \frac{ab}{rs}$.

Siguiendo la demostración del Teorema 4 (Pag. 85) se demuestra que $(S^{-1}R, +, \cdot)$ tiene estructura de anillo que tiene la propiedad que todo elemento de S es inversible en $S^{-1}R$.

Nota: Observar que el Teorema 4 (Pag. 85) es consecuencia de este último resultado: si D es un dominio de integridad puedo considerar como conjunto de denominadores D^* (comprobar que verifica las tres propiedades) y el anillo $S^{-1}D$ es precisamente $\mathcal{Q}(D)$, el cuerpo de fracciones del dominio de integridad D.

4. Ejercicios del Tema

1 Sea $D = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.

(i) Demuestra que D es un dominio de integridad.

(ii) Calcula el cuerpo de fracciones de D, denotado por $\mathcal{Q}(D)$, y da el único monomorfismo $f : \mathcal{Q}(D) \to \mathbb{R}$ que es la inclusión cuando restringimos a D.

(iii) Por si no te has dado cuenta, demuestra que $\mathcal{Q}(D) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Calcula el inverso de $2 + 3\sqrt{2}$ y dalo en la forma $a + b\sqrt{2}$ con $a, b \in \mathbb{Q}$.

2 Sea D un dominio de integridad y D' un subanillo unitario de D. Demuestra que D' es también un dominio de integridad. ¿El cuerpo de fracciones de D y D' coinciden?

3 Calcula el menor subanillo unitario de $\mathbb{R}$ que contiene a $\sqrt[3]{5}$. [∗]

4 Sea R un anillo sin divisores de cero y sea $e \in R$ un elemento no nulo tal que $e^2 = e$. Demuestra que R es un anillo unitario. [∗]

5 Sea D y D' dos dominios de integridad y $f : D \to D'$ un monomorfismo de anillos. ¿Puedes encontrar un homomorfismo de anillos $\bar{f} : \mathcal{Q}(D) \to \mathcal{Q}(D')$ tal que $\bar{f}(\frac{b}{1}) = \frac{f(b)}{1}$? ¿Y si f no es un monomorfismo?

6 *Sea R un anillo y sea $a \in R$. Entonces:*

- *a no es divisor de cero por la izquierda si y sólo si $\lambda_a : R \to R$ es una aplicación inyectiva.*
- *a no es divisor de cero por la derecha si y sólo si $\rho_a : R \to R$ es una aplicación inyectiva.*
- *Si a es inversible, $\lambda_a : R \to R$ es biyectiva.*
- *Si a es inversible, $\rho_a : R \to R$ es biyectiva.*
- *Si R es conmutativo y unitario, a es inversible si y sólo si $\lambda_a : R \to R$ es biyectiva.*
- *Si R es conmutativo y unitario, a es inversible si y sólo si $\rho_a : R \to R$ es biyectiva.*
- *Si en R no hay divisores de cero, a es inversible si y sólo si $\lambda_a : R \to R$ es biyectiva.*
- *Si en R no hay divisores de cero, a es inversible si y sólo si $\rho_a : R \to R$ es biyectiva.*

7 Sea R un anillo unitario y finito y sea $a \in R$ que no es divisor de cero por la izquierda. Entonces a es inversible. [∗]

8 Sea R un anillo unitario y finito y sea $a \in R$ que no es divisor de cero por la izquierda. Entonces a no es divisor de cero por la derecha. [∗]

9 Sea R un anillo finito y sea $a \in R$ que no es divisor de cero (ni por la izquierda ni por la derecha). Entonces R es unitario. [∗∗]

10 Si D es dominio de integridad, $D[X]$ es dominio de integridad. ¿Será el cuerpo de fracciones de $D[X]$ el anillo de polinomios sobre el cuerpo de fracciones de D?

11 Encuentra dos dominios de integridad, $D \subset D'$ tales que $\mathcal{Q}(D) = \mathcal{Q}(D')$ (aquí el igual puede significar isomorfos).

12 Encuentra dos dominios de integridad, $D \subset D'$ tales que $\mathcal{Q}(D) \neq \mathcal{Q}(D')$ (aquí el igual puede significar no isomorfos).

13 Demuestra que $\{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ es un subcuerpo de $\mathbb{R}$. [$*$]

14 Demuestra que $\mathbb{Z}+\mathbb{Z}i$ es un subanillo de $\mathbb{C}$ que es dominio de integridad. Demuestra que el cuerpo de fracciones de $\mathbb{Z}+\mathbb{Z}i$ es $\mathbb{Q}+\mathbb{Q}i$. [$*$]

15 Sea D un dominio de integridad de característica p (p un número primo). Demuestra que la característica de $\mathcal{Q}(D)$ es también p.

16 Sea D un dominio de integridad y sean n elementos $\frac{a_i}{s_i} \in \mathcal{Q}(D)$, $i = 1, \dots, n$. Demuestra que puedes encontrar representantes de estos elementos con el mismo denominador. ¿Podrías conseguir que este denominador común fuera el mínimo común múltiplo de $\{s_1, s_2, \dots, s_n\}$?

17 Sea D un dominio de integridad, $\mathbb{F}$ un cuerpo y $h : D \to \mathbb{F}$ un monomorfismo de anillos. Demuestra que existe un único monomorfismo de anillos $f : \mathcal{Q}(D) \to \mathbb{F}$ que hace conmutativo el diagrama. [$*$]

$$\begin{tikzcd} D \arrow[r, "i"] \arrow[dr, "h"'] & \mathcal{Q}(D) \arrow[d, dotted, "f"] \\ & \mathbb{F} \end{tikzcd}$$

18 Sea D un dominio de integridad y sea Q un cuerpo tal que existe un monomorfismo de anillos $i : D \to Q$ tal que para cada cuerpo $\mathbb{F}$ y cada monomorfismo de anillos $h : D \to \mathbb{F}$, existe un único monomorfismo de anillos $f : Q \to \mathbb{F}$ que hace conmutativo el diagrama. Se tiene que Q es isomorfo a $\mathcal{Q}(D)$, cuerpo de fracciones de D. [$*$]

$$\begin{tikzcd} D \arrow[r, "i"] \arrow[dr, "h"'] & Q \arrow[d, dotted, "f"] \\ & \mathbb{F} \end{tikzcd} \quad \Longrightarrow \quad Q \approx \mathcal{Q}(D).$$

Algunos ejercicios de temas anteriores

19 Sea R un anillo y sea $S \leq R$. ¿Que puedes decir de la característica de R y S? [$**$]

20 Sea $n \in \mathbb{N}$. Entonces un elemento $\overline{a} \in \mathbb{Z}_n$ o es inversible o es divisor de cero. [$*$]

21 Encuentra un anillo R y un elemento $x \in R$ tal que x no sea ni inversible ni divisor de cero.

22 Sea R un anillo. Demuestra que un elemento inversible no puede ser divisor de cero. En particular, demuestra en un anillo de división (y por tanto en un cuerpo) no hay divisores de cero.

23 Demuestra que un anillo unitario y finito sin divisores de cero por la derecha (o por la izquierda) es un anillo de división. [$*$]