

ANILLOS DE FRACCIONES CASO NO COMUTATIVO

Oswaldo Lezama¹ y Hector Linares²

§1. INTRODUCCION.

La construcción del campo de cocientes de un dominio de integridad se generaliza no sólamente a anillos comutativos (Ver [1]), sino a anillos en general no comutativos. En este trabajo mostramos dicha generalización siguiendo las ideas de [2], pero incluyendo las pruebas allí omitidas. Ilustramos además la teoría expuesta con suficiente cantidad de ejemplos, no tratados por lo general en la literatura clásica de esta temática.

§2. EXISTENCIA Y UNICIDAD.

A lo largo de todo el trabajo A denotará un

(1) Profesor Asistente, Universidad Nacional de Colombia.

(2) Est. de Magister, Depto. de Mat. Univ. Nal. de Colombia.

anillo no necesariamente conmutativo, con unidad 1. Decimos que $S \subseteq A$, $S \neq \emptyset$ es un sistema multiplicativo de A si $0 \notin S$, $1 \in S$ y el producto de dos elementos cualesquiera de S está en S .

DEFINICION 2.1. Sean A un anillo y S un sistema multiplicativo de A . Se dice que el anillo B es un anillo derecho de fracciones de A respecto de S , si existe un homomorfismo de anillos,

$$\phi: A \longrightarrow B$$

tal que,

(i) $\phi(S) \subseteq B^*$, donde B^* denota el grupo multiplicativo del anillo B .

(ii) Siendo $a \in A$ se cumple

$$\phi(a) = 0 \iff au = 0 \text{ para algún } u \in S.$$

(iii) Cada elemento $x \in B$ puede escribirse en la forma

$$x = \phi(a)\phi(s)^{-1},$$

para ciertos $a \in A$, $s \in S$.

Antes de enfrentar la existencia y unicidad resulta conveniente preguntarse bajo qué condición un anillo puede sumergirse en un anillo de fracciones.

LEMA. Sean A un anillo y B un anillo derecho de fracciones de A respecto del sistema S con homo-

morfismo ϕ . Entonces,

- (i) ϕ es inyectivo si y sólo si S no posee divisores de cero.
- (ii) ϕ es biyectivo si y sólo si $S \subseteq A^*$.

La demostración es muy sencilla y será omitida.

A diferencia del caso conmutativo ([1]), la existencia de un anillo derecho de fracciones está supeditada al cumplimiento de dos condiciones.

TEOREMA 1. (de existencia, [2]). Sea A un anillo y S un subconjunto multiplicativo de A . A posee anillo derecho de fracciones respecto de S si y sólo si S satisface las siguientes condiciones:

- (1) Para cualesquiera elementos $a \in A$, $s \in S$ tales que $sa = 0$ existe $u \in S$ tal que $au = 0$.
- (2) Para cualesquiera elementos $s \in S$, $a \in A$ existen elementos $t \in S$, $b \in A$ tales que

$$at = sb \quad (1)$$

Demostración: \Rightarrow Supongamos que B es un anillo derecho de fracciones de A respecto de S con homomorfismo ϕ que cumple las condiciones (i)-(iii) de la

(1) Si a y s están en S entonces el elemento $at = sb \in S$.

definición. Si $sa = 0$ entonces $\phi(s)\phi(a) = 0$ con lo cual $\phi(a) = 0$. Existe entonces $u \in S$ tal que $au = 0$ y hemos probado (1).

Dados $s \in S$ y $a \in A$ entonces $\phi(s)^{-1}\phi(a) \in B$.

Según (iii) existen $b_0 \in A$, $t_0 \in S$ tales que $\phi(s)^{-1}\phi(a) = \phi(b_0)\phi(t_0)^{-1}$. Según (i) existe $u \in S$ tal que $(at_0 - sb_0)u = 0$. Tomando $t = t_0u$, $b = b_0u$ obtenemos (2).

Veamos el recíproco. La idea de esta demostración fue tomada de [2], nosotros la dividimos en varios pasos.

Paso 1: En el conjunto $A \times S$ definimos la relación \equiv como sigue: $(a,s) \equiv (b,t)$ si y sólo si existen $c, d \in A$ tales que $ac = bd$ y $sc = td \in S$ ⁽¹⁾.

La relación \equiv es de equivalencia: $(a,s) \equiv (a,s)$ ya que $as = as$, $ss = ss \in S$; la simetría de \equiv es consecuencia de la simetría de la relación de igualdad; finalmente supóngase que $(a,s) \equiv (b,t)$ y $(b,t) \equiv (c,r)$. Existen elementos $c, d, c_1, d_1 \in A$ tales que

$$ac = bd, \quad sc = td \in S$$

(1) Aplicando la condición (2) a los elementos s, t encontramos elementos c, d tales que $sc = td$, donde alguno c ó d es de S , por eso $sc = tde$.

$$bc_1 = ed_1, \quad tc_1 = rd_1 \in S$$

Aplicamos (2) a los elementos sc , rd_1 : existen entonces $x, y \in A$ tales que $scx = rd_1y \in S$. Resulta pues $acx = bdx$, $bc_1y = ed_1y$, $tdx = scx = rd_1y = tc_1y$; y, de esto último, obtenemos $t(dx - c_1y) = 0$ con $t \in S$. Segundo (1) existe $u \in S$ tal que $(dx - c_1y)u = 0$, e.d., $dxu = c_1yu$. Por lo tanto, $bdu = bc_1yu$, e.d.

$$acxu = ed_1yu$$

$$scxu = rd_1yu \in S$$

y hemos probado que $(a, s) \equiv (e, r)$

Paso 2: Denotemos por $\frac{a}{s}$ la clase de equivalencia que contiene el par (a, s) y mediante AS^{-1} el conjunto de clases determinadas. Sean $\frac{a}{s}, \frac{b}{t} \in AS^{-1}$; definimos

$$(3) \quad \frac{a}{s} + \frac{b}{t} =: \frac{ac + bd}{m},$$

donde c, d están determinados por la condición (2) aplicada a los elementos s, t , e.d., $sc = td =: m \in S$.

Inicialmente demostremos que (3) no depende de los elementos c y d . En efecto, sean $c_1, d_1 \in A$ tales que $sc_1 = td_1 =: m_1 \in S$. Aplicamos (2) a m_1 , m_1 : existen $u, v \in A$ tales que $mu = m_1v \in S$; $scu = sc_1v$, $tdu = td_1v$, e.d., $s(cu - c_1v) = 0$, $t(du - d_1v) = 0$. Segundo (1) existen $x, y \in S$ tales que $cux = c_1vx$, $duy = d_1vy$. Aplicamos (2) a los elementos x, y : existen w, z tales que $xw = yz \in S$.

Se tiene entonces $muw = m_1vxw \in S$ y además $acuxw = ac_1vxw$, $bduyz = bd_1vyz$; de aquí resulta $acuxw + bduyz = ac_1vxw + bd_1vyz$, o también

$$(ac + bd)uxw = (ac_1 + bd_1)vxw, \text{ e.d.}$$

$$\frac{ac + bd}{m} = \frac{ac_1 + bd_1}{m_1}$$

Ahora demostremos que (3) es independiente de las fracciones elegidas:

Supóngase que

$$\frac{a}{s} = \frac{a_1}{s_1}, \quad \frac{b}{t} = \frac{b_1}{t_1}$$

Sean $c, d \in A$ tales que $sc = s_1d =: m \in S$, $ac = a_1d$, sean también c', d' tales que $m' =: tc' = t_1d' \in S$, $bc' = b_1d'$. Aplicando (2) a m y m' tenemos $mu = m'v \in S$ con $u, v \in A$ (alguno de estos en S). Resulta entonces $scu = tc'v =: n \in S$, $s_1du = t_1d'v =: p \in S$.

Por la independencia ya probada

$$\frac{a}{s} + \frac{b}{t} = \frac{acu + bc'v}{n}, \quad \frac{a_1}{s_1} + \frac{b_1}{t_1} = \frac{a_1du + b_1d'v}{p},$$

pero $acu = a_1du$, $bc'v = b_1d'v$ y siendo además $n = scu = mu = m'v = t_1d'v = p$ entonces

$$\frac{a}{s} + \frac{b}{t} = \frac{a_1}{s_1} + \frac{b_1}{t_1}$$

Todo lo anterior muestra que la adición en (3) está correctamente definida.

El producto se define por

$$(4) \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ac}{tu} \quad ,$$

donde $c \in A$, $u \in S$ están determinados por la condición (2) aplicada a los elementos s, b :

$$sc = bu$$

(4) no depende de los elementos c, u : sean $c_1 \in A$, $u_1 \in S$ tales que $sc_1 = bu_1$. Aplicamos (2) a u, u_1 ; existen entonces elementos x, y tales que $ux = u_1y \in S$ y de aquí $bux = bu_1y = sc_1y = scx$, e.d., $s(cx - c_1y) = 0$. De acuerdo a (1) existe $m \in S$ tal que $cxm = c_1ym$. Hemos encontrado pues elementos xm, ym tales que $tuxm = tu_1ym \in S$, $acxm = ac_1ym$, e.d., $\frac{ac}{tu} = \frac{ac_1}{tu_1}$.

Concluimos el Paso 2 mostrando que (4) no depende de las fracciones elegidas: Supóngase que

$$\frac{a}{s} = \frac{a_1}{s_1}, \quad \frac{b}{t} = \frac{b_1}{t_1} .$$

Es suficiente mostrar que

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{a_1}{s_1} \cdot \frac{b}{t} \quad y \quad \frac{a_1}{s_1} \cdot \frac{b}{t} = \frac{a_1}{s_1} \cdot \frac{b_1}{t_1} .$$

Consideremos la demostración de la primera igualdad: sea $\frac{a}{s} \cdot \frac{b}{t} = \frac{ac}{tu}$ con $c \in A$, $u \in S$, $sc = bu$; $\frac{a_1}{s_1} \cdot \frac{b}{t} = \frac{a_1c_1}{tu_1}$, con $c_1 \in A$, $u_1 \in S$, $s_1c_1 = bu_1$; $am = a_1n$, $sm = s_1n \in S$ (ya que $\frac{a}{s} = \frac{a_1}{s_1}$).

Aplicamos (2) a tu y tu_1 : existen $w \in S$, $l \in A$ tales que

$$tuw = tu_1l \quad (w \in S)$$

Resulta de aquí que $t(uw - u_1l) = 0$ con lo cual existe $v \in S$ tal que $uwv = u_1lv$, y resulta $buwv = bu_1lv$, e.d.,

$$scwv = s_1c_1lv .$$

Aplicamos nuevamente (2) a $scwv \in A$, $sm \in S$: existen entonces $p \in S$, $q \in A$ tales que

$$scwvp = smq ;$$

$s(cwvp - mq) = 0$ y existe $r \in S$ tal que

$$cwvpr = mqr ;$$

$$acwvpr = amqr = a_1nqr .$$

De otra parte, $s_1c_1lvp = s_1nq$ y existe $r' \in S$ tal que $c_1lvp r' = nqr'$, de aquí $a_1c_1lvp r' = a_1nqr'$. Aplicamos (2) a r, r' : existen $x \in A$, $y \in S$ tales que

$$ry = r'x \in S.$$

Obtenemos $acwvpry = a_1nqr'y = a_1nqr'x = a_1c_1lvp r'x$; además $tuwvpry = tu_1lvp r'x \in S$ estableciéndose la primera igualdad.

$$\begin{aligned} \text{Sea } \frac{a_1}{s_1} \cdot \frac{b}{t} &= \frac{a_1c}{tu} \text{ con } c \in A, u \in S, s_1c = bu; \\ \frac{a_1}{s_1} \cdot \frac{b_1}{t_1} &= \frac{a_1c_1}{t_1u_1} \text{ con } c_1 \in A, u_1 \in S, s_1c_1 = b_1u_1; \\ bm &= b_1n, tm = t_1n \in S \quad \left(\frac{b}{t} = \frac{b_1}{t_1} \right) . \end{aligned}$$

Aplicamos (2) a $t_1 u_1$: existen $w \in S$, $\ell \in A$ tales que $t_1 u_1 w = t_1 u_1 \ell$. Aplicamos ahora (2) a $u_1 w \in S$, $m \in A$: existen $x \in A$, $y \in S$ tales que $u_1 w x = m y$, e.d., $t_1 u_1 w x = t_1 m y$. Resulta entonces $v \in S$ tal que $u_1 w x v = m y v$ y de aquí $b_1 u_1 w x v = b_1 m y v$, e.d.,

$$s_1 c w x v = b_1 n y v$$

De $t_1 u_1 w x = t_1 m y$ resulta $t_1 u_1 \ell x = t_1 n y$ y existe $v' \in S$ tal que $u_1 \ell x v' = n y v'$ con lo cual $b_1 u_1 \ell x v' = b_1 n y v'$, e.d.,

$$s_1 c_1 \ell x v' = b_1 n y v'$$

Aplicamos (2) a v , v' y encontramos $p \in S$, $q \in A$ con $vq = v'p$. Obtenemos entonces

$$s_1 c w x v q = s_1 c_1 \ell x v' p$$

Aplicando (1), existe $z \in S$ tal que $c w x v q z = c_1 \ell x v' p z$, de donde $a_1 c w x v q z = a_1 c_1 \ell x v' p z$, $t_1 u_1 w x v q z = t_1 u_1 \ell x v' p z \in S$.

Esto completa la demostración de la segunda igualdad.

Paso 3: El conjunto AS^{-1} con las operaciones definidas en el paso 2 es un anillo. El cero es la fracción $\frac{0}{1}$, la identidad 1 es la fracción $\frac{1}{1}$, la verificación de las propiedades de anillo, tales como asociatividad de la adición y de la multiplicación y propiedades distributivas, así como conmutatividad

de la adición es rutinaria.

Paso 4: AS^{-1} es un anillo derecho de fracciones de A respecto de S . En efecto, la función

$$(5) \quad \begin{aligned} \phi: A &\rightarrow AS^{-1} \\ a &\mapsto \frac{a}{1} \end{aligned}$$

es un homomorfismo de anillos, pues fácilmente se demuestra que

$$\phi(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \phi(a) + \phi(b)$$

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

$$\phi(1) = \frac{1}{1}$$

Sea $s \in S$, entonces $\phi(s) = \frac{s}{1}$ y $\frac{s}{1} \cdot \frac{1}{s} = \frac{1}{1}$, e.d., $\phi(s) \in (AS^{-1})^*$ y $\phi(S) \subseteq (AS^{-1})^*$.

Además, si $a \in A$ es tal que $\phi(a) = \frac{a}{1} = \frac{0}{1}$ entonces existen $c, d \in A$ tales que $1.c = 1.d \in S$, $ac = 0.d = 0$, e.d., existe $c \in S$ tal que $ac = 0$.

De otra parte, si $au = 0$ con $a \in A$ y $u \in S$, entonces $\phi(au) = 0 = \phi(a)\phi(u)$, con lo cual $\phi(a) = 0$ ya que $\phi(u)$ es invertible.

Por último, es claro que dado $\frac{a}{s} \in AS^{-1}$

$$\frac{a}{s} = \frac{a}{1} \cdot \frac{1}{s} = \phi(a)\phi(s)^{-1}$$

Hemos completado la demostración del teorema
1. ▲

Pasamos ahora a considerar la unicidad del anillo derecho de fracciones, en caso de que éste exista....

PROPOSICION. Sean A un anillo y S un subconjunto multiplicativo de A que cumple las condiciones (1) - (2) del teorema anterior. Sea $g: A \rightarrow A_0$ un homomorfismo de anillos tal que $g(S) \subseteq A_0^*$. Entonces existe un único homomorfismo h tal que el diagrama

$$\begin{array}{ccc} A & \xrightarrow{g} & A_0 \\ \phi \downarrow & \nearrow h & \\ AS^{-1} & & \end{array} \quad \phi(a) = \frac{a}{1}$$

es commutativo, e.d., $h \circ \phi = g$. Si además g es inyectivo, h también lo es.

Demostración: Existencia. Definimos,

$$(6) \quad h\left(\frac{a}{s}\right) := g(a)g(s)^{-1}, \quad a \in A, \quad s \in S.$$

h está bien definida: si $\frac{a}{s} = \frac{b}{t}$ entonces existen elementos $c, d \in A$ tales que $sc = td \in S$, $ac = bd$.

De aquí resulta $g(a)g(c) = g(b)g(d)$, $g(s)g(c) = g(t)g(d)$. Además $g(c) \in A_0^*$ ya que $g(s), g(sc) \in A_0^*$.

Se sigue que $g(a)g(c)[g(s)g(c)]^{-1} = g(b)g(d)[g(t)g(d)]^{-1}$, e.d., $g(a)g(s)^{-1} = g(b)g(t)^{-1}$ y $h\left(\frac{a}{s}\right) = h\left(\frac{b}{t}\right)$. h es un homomorfismo de anillos: Si $\frac{a}{s} + \frac{b}{t} = \frac{ac+bd}{sc+td}$ con $sc = td =: m \in S$ entonces

$$h\left(\frac{a}{s} + \frac{b}{t}\right) = g(ac+bd)g(m)^{-1}$$

$$= [g(a)g(c) + g(b)g(d)]g(c)^{-1}g(s)^{-1}.$$

$$\begin{aligned}
 &= g(a)g(s)^{-1} + g(b)g(d)g(c)^{-1}g(c)^{-1}g(s)^{-1} \\
 &= g(a)g(s)^{-1} + g(b)g(d)g(d)^{-1}g(t)^{-1}(g(d) = A^*!) \\
 &= h\left(\frac{a}{s}\right) + h\left(\frac{b}{t}\right).
 \end{aligned}$$

Además si $\frac{a}{s} \cdot \frac{b}{t} = \frac{ac}{tu}$, con $sc = bu$, $u \in S$, entonces $h\left(\frac{a}{s} \cdot \frac{b}{t}\right) = g(ac)g(tu)^{-1} = g(a)g(c)g(u)^{-1}g(t)^{-1} = g(a)g(s)^{-1}g(b)g(t)^{-1} = h\left(\frac{a}{s}\right)h\left(\frac{b}{t}\right)$. $h\left(\frac{1}{1}\right) = g(1)g(1)^{-1} = 1$.

Sean ϕ el homomorfismo definido en (5), $a \in A$. Entonces, $h \circ \phi(a) = h\left(\frac{a}{1}\right) = g(a)g(1)^{-1} = g(a)$, es decir, $h \circ \phi = g$.

Unicidad. Sea $f: AS^{-1} \rightarrow A_0$ un homomorfismo tal que $f \circ \phi = g$. Entonces $f\left(\frac{a}{s}\right) = f\left(\frac{a}{1} \cdot \frac{1}{s}\right) = f(\phi(a)\phi(s)^{-1}) = g(a)g(s)^{-1} = h\left(\frac{a}{s}\right)$, e.d., $f = h$.

Finalmente nótese que si $h\left(\frac{a}{s}\right) = 0$ entonces $g(a) = 0$; suponiendo g inyectivo $a = 0$ y $\frac{a}{s} = \frac{0}{1}$ resulta h inyectiva. ▲

LEMA 2. Sean A y S como en la hipótesis de la proposición anterior. Si A se puede sumergir en AS^{-1} (esto es, si ϕ en (5) es inyectivo) entonces AS^{-1} es el menor anillo que contiene A en el cual todos los elementos de S son invertibles. ▲

De la última proposición se desprende el siguiente teorema de unicidad para los anillos derechos de fracciones.

TEOREMA 2. (de unicidad, [1]). Sean A un anillo y S un sistema multiplicativo que satisfacen las con-

diciones (1) - (2) del teorema 1. Sea A_0 un anillo y $g: A \rightarrow A_0$ un homomorfismo que satisface las condiciones i) - iii) de la definición. Entonces existe un único isomorfismo $h: AS^{-1} \rightarrow A_0$ tal que $h \circ \phi = g$, donde ϕ es el homomorfismo definido en (5). La demostración es inmediata.

§3. CASOS PARTICULARES.

1º Anillo clásico de fracciones. Sean A un anillo y $S = \{a \in A \mid a \text{ no es divisor de cero}\}$. S es un sistema multiplicativo de A . La condición (1) del teorema 1 es supérflua. La condición (2) se denomina en este caso condición derecha de Ore, y en caso de cumplirse $AS^{-1} =: A_{cl}$ se denomina anillo de recho clásico de fracciones del anillo A . El teorema 1 toma en este caso la forma siguiente: A posee anillo derecho clásico de fracciones si y sólo si A cumple la condición derecha de Ore. De acuerdo al Lema 1, A puede sumergirse en A_{cl} y A_{cl} es el menor anillo que contiene A en el cual todos los elementos de A no divisores de cero son invertibles.

2º Cuerpo de fracciones. Si A es un anillo sin divisores de cero, el anillo derecho clásico de fracciones de A es un cuerpo (anillo de división) que denotamos T_A y denominamos cuerpo derecho de fracciones de A : Si $\frac{a}{b} \neq 0$ entonces $a \neq 0$ y $a \in S$. Resulta

pues $\frac{a}{s} \cdot \frac{s}{a} = \frac{as}{as} = 1$ ya que $ss = ss$; e.d., $\frac{as}{as} = 1$ y $\frac{a}{s}$ es invertible.

Nótese nuevamente que T_A existe si y sólo si A cumple la condición derecha de Ore; en tal caso T_A es el menor cuerpo que contiene A . En otras palabras, un anillo sin divisores de cero puede sumergirse en un cuerpo si y sólo si satisface la condición derecha de Ore.

3º Anillo izquierdo de fracciones. Es claro a partir de la definición y teoremas 1 - 2 del segundo parágrafo, cómo definir y caracterizar un anillo izquierdo de fracciones.

PROPOSICION. Sea A un anillo y S un sistema multiplicativo de A . Si AS^{-1} y $S^{-1}A$ existen, entonces son isomorfos.

Demostración: Sean $\phi_d: A \rightarrow AS^{-1}$ y $\phi_i: A \rightarrow S^{-1}A$ los homomorfismos definidos como en (5). Según la proposición del parágrafo anterior existen homomorfismos $h_d: AS^{-1} \rightarrow S^{-1}A$ y $h_i: S^{-1}A \rightarrow AS^{-1}$ tales que $h_d \circ \phi_d = \phi_i$ y $h_i \circ \phi_i = \phi_d$, e.d., $(h_d \circ h_i) \circ \phi_i = \phi_i$, $(h_i \circ h_d) \circ \phi_d = \phi_d$. Por la unicidad en la proposición mencionada obtenemos que $h_d \circ h_i = 1$ y $h_i \circ h_d = 1$, e.d., $AS^{-1} \cong S^{-1}A$. \blacksquare

En [2] pag. 53, se da un ejemplo de anillo que tiene anillo clásico derecho de fracciones pero no izquierdo.

4º Caso conmutativo. Queremos ahora mostrar como las construcciones efectuadas en el segundo parágrafo son generalización del caso conmutativo.

Sea R un anillo conmutativo y S un sistema multiplicativo de R . Nótese en primer lugar que $RS^{-1} = S^{-1}R$.

En [1] la construcción del anillo de fracciones RS^{-1} se da por la relación de equivalencia $(a,s) \sim (b,t)$ equivale a que:

$$(7) \quad \begin{aligned} &\text{existe } u \in S \text{ tal que} \\ &atu = bsu, \quad a,b \in R, \quad s,t \in S \end{aligned}$$

De las relaciones $\sim = \equiv$: Si $(a,s) \sim (b,t)$ deducimos que existe $u \in S$ tal que $atu = bsu$. Toman do $c =: tu$, $d =: su$ entonces $sc = td$ con lo cual $(a,s) \equiv (b,t)$. Recíprocamente, si $(a,s) \equiv (b,t)$ entonces existen $c,d \in R$ tales que $ac = bd$ y $sc = td \in S$. De aquí resulta $at(td) = at(sc) = acts = bdts = bs(td)$, con $dt \in S$, e.d., $(a,s) \sim (b,t)$.

Las operaciones en [1] se definen por

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$$

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

(3) y (4) coinciden con estas definiciones. Como $st = ts \in S$ entonces (3) coincide con la suma de arriba. Para el producto basta tener en cuenta que $sb = bs$.

Si R es un dominio de integridad entonces su cuerpo de fracciones es un campo K_R , y se denomina campo de cocientes (fracciones) del dominio R .

Nótese que si $R = \mathbb{Z}$ entonces $K_{\mathbb{Z}} = \mathbb{Q}$.

§4. EJEMPLOS.

EJEMPLO 1. Siendo A un anillo, el grupo A^* de elementos invertibles de A es un sistema multiplicativo para el cual el anillo de fracciones $A(A^*)^{-1}$ siempre existe, y coincide con A (Ver **LEMA 1**): $A(A^*)^{-1} = A = (A^*)^{-1}A$.

De lo anterior se concluye que para $n \geq 2$

$$(\mathbb{Z}_n)^*_{cl} = \mathbb{Z}_n$$

En efecto, basta mostrar que el sistema S de elementos no divisores de cero en \mathbb{Z}_n , coincide con \mathbb{Z}_n^* : Evidentemente $\mathbb{Z}_n^* \subseteq S$. Recíprocamente, si $x \notin \mathbb{Z}_n^*$ entonces existe $2 \leq d \leq n$ tal que $d|x$, $d|n$. Sean entonces $1 \leq r, s \leq n-1$ tales que $x = dr$, $n = ds$. Entonces $xs \equiv 0 \pmod{n}$ y $x \notin S$.

EJEMPLO 2. Consideraremos en \mathbb{C} el dominio de integridad

$$\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$

Este anillo no es un dominio de integridad porque $2 \in \mathbb{Z}[\sqrt{-3}]$ y 2 no es un divisor de cero. Sin embargo, $\mathbb{Z}[\sqrt{-3}]$ es un dominio de fracciones porque se tiene que todo anillo de fracciones para un dominio de integridad es un dominio de integridad.

Su campo de cocientes es

$$\mathbb{Q}[\sqrt{-3}] = \{x + y\sqrt{-3} \mid x, y \in \mathbb{Q}\}$$

En efecto, la función

$$g: \mathbb{Z}[\sqrt{-3}] \rightarrow \mathbb{Q}[\sqrt{-3}]$$

$$a + b\sqrt{-3} \mapsto \frac{a}{1} + \frac{b}{1}\sqrt{-3}$$

es un homomorfismo inyectivo de anillos. Siendo a, b enteros no simultáneamente nulos entonces $g(a + b\sqrt{-3})$ es no nulo, y por lo tanto invertible. Nótese además que cada elemento $\frac{a}{r} + \frac{b}{s}\sqrt{-3} \in \mathbb{Q}[\sqrt{-3}]$ se escribe en la forma

$$\frac{a}{r} + \frac{b}{s}\sqrt{-3} = g[(as - 3br) + (as + br)\sqrt{-3}] g(r\delta + r\delta\sqrt{-3})^{-1}$$

Según el teorema 2, $\mathbb{Q}[\sqrt{-3}]$ es (salvo isomorfismo) el campo de cocientes de $\mathbb{Z}[\sqrt{-3}]$.

EJEMPLO 3. Sea $\{A_i\}_{i \in I}$ una familia cualquiera no vacía de anillos, y sea para cada $i \in I$ S_i un sistema multiplicativo de A_i . Supóngase que $A_i S_i^{-1}$ existe para cada $i \in I$. Sean

$$A := \prod A_i, S := \prod S_i$$

donde \prod denota producto cartesiano.

Nótese que S es un sistema multiplicativo de A . ¿Existe AS^{-1} ? Sean $a = (a_i) \in A$, $s = (s_i) \in S$ tales que $sa = 0$. Existen entonces $u_i \in S_i$, $i \in I$, para los cuales $a_i u_i = 0$; de aquí resulta $au = 0$ con $u = (u_i) \in S$. Sean otra vez $s \in S$ y $a \in A$.

Existen $x_i \in S_i$, $b_i \in A_i$, $i \in I$ tales que

$$a_i x_i = s_i b_i, \quad i \in I.$$

Se tiene entonces que $ax = sb$, con $a = (a_i)$ $\in S$, $b = (b_i) \in A$. Queda de esta manera probada la existencia de AS^{-1} .

Resulta natural preguntarse si los anillos AS^{-1} y $\prod A_i S_i^{-1}$ son isomorfos.

Vemos que la función

$$g: A \rightarrow \prod A_i S_i^{-1}$$

$$(a_i) \mapsto \left(\frac{a_i}{s_i} \right)$$

cumple las condiciones del teorema 2: De (3) del parágrafo 12 se concluye que g es un homomorfismo de anillos. Evidentemente si $s = (s_i) \in S$ entonces $g(s) = \left(\frac{s_i}{s_i} \right) \in (\prod A_i S_i)^0$. Si $a = (a_i) \in A$ y $g(a) = 0$ entonces $\frac{a_i}{s_i} = 0$ para cada $i \in I$. De aquí existe $u_i \in S_i$ tal que $a_i u_i = 0$, c.d., $au = 0$ con $u = (u_i) \in S$. Resta observar que cada elemento de $\prod A_i S_i^{-1}$ se escribe en la forma

$$\left(\frac{a_i}{s_i} \right) = \left(\frac{a_i}{s_i} \cdot \frac{1}{s_i} \right) = \left(\frac{a_i}{s_i} \right) \left(\frac{1}{s_i} \right) = g(a)g(s)^{-1} \text{ con } a = (a_i), s = (s_i).$$

Consideremos como caso particular una familia finita de dominios de integridad R_1, \dots, R_n . Siendo $S_i = R_i - \{0\}$, $1 \leq i \leq n$, entonces $S = S_1 \times \dots \times S_n$ es el conjunto de elementos de $R = R_1 \times \dots \times R_n$ que no son divisores de cero, y por tanto

$(R_1 \times \dots \times R_n)_{cl} \cong K_{R_1} \times \dots \times K_{R_n}$,
donde K_{R_i} es el campo de cocientes de R_i , $1 \leq i \leq n$.

Por ejemplo

$$(Z \times \dots \times Z)_{cl} \cong Q \times \dots \times Q.$$

EJEMPLO 4. Sean A un anillo y S un sistema multiplicativo de A tal que AS^{-1} existe. Sea X un conjunto no vacío cualquiera. Puesto que el anillo de funciones A^X es un producto cartesiano, entonces de acuerdo a lo obtenido en el ejemplo 3 se tiene el isomorfismo

$$A^X (S^X)^{-1} \cong (AS^{-1})^X$$

donde $S^X = \{f \in A^X \mid f(X) \subseteq S\}$

Si $A = R$ es un dominio de integridad y $S = R - \{0\}$ entonces S^X es el conjunto de elementos de R^X que no son divisores de cero, con lo cual

$$(R^X)_{cl} \cong (K_R)^X,$$

siendo K_R el campo de cocientes de R . Por ejemplo

$$(Z^{\mathbb{N}})_{cl} \cong Q^{\mathbb{N}}$$

$$(Q^{\mathbb{N}})_{cl} = Q^{\mathbb{N}}$$

$$(R^{\mathbb{N}})_{cl} = R^{\mathbb{N}}$$

$$(C^{\mathbb{N}})_{cl} = C^{\mathbb{N}}$$

EJEMPLO 5. Este ejemplo figura como ejercicio propuesto en [2]. Sea A un anillo y S un sistema mul-

tiplicativo de A tal que AS^{-1} existe. Sea $M(n, A)$ el anillo de matrices de orden $n \geq 1$ sobre A y sea $D(n, S)$ el conjunto de matrices diagonales de $M(n, A)$ cuyos elementos diagonales son tomados de S . Note se que entonces $D(n, S)$ es un sistema multiplicativo de $M(n, A)$. Se desea probar que $M(n, A)D(n, S)^{-1} \cong M(n, AS^{-1})$. En primer lugar estudiamos la existencia de $M(n, A)D(n, S)^{-1}$: Sean $M = (m_{ij}) \in M(n, A)$, $D = (d_{ij}) \in D(n, S)$ tales que $DM = 0$. Entonces

$$d_{ii} m_{ij} = 0, \quad 1 \leq i, j \leq n$$

Según la condición (1) del teorema 1 existen $u_{ij} \in S$ tales que

$$(8) \quad m_{ij} u_{ij} = 0, \quad 1 \leq i, j \leq n$$

Si logramos anular todos los elementos de M mediante multiplicaciones sucesivas a la derecha de ella por matrices de $D(n, S)$, entonces habríamos probado la condición (1) del teorema 1, ya que $D(n, S)$ es un sistema multiplicativo.

Comenzamos anulando los elementos de la primera fila: Sea $U^{(0)} = D(u_{11} t_{11}^{(0)}, \dots, u_{nn} t_{nn}^{(0)}) \in D(n, S)$, donde $t_{11}^{(0)} = 1$ y $t_{jj}^{(0)} \in S$ están determinados aplicando la condición (2) a u_{jj} , u_{1j} , $j \geq 2$:

$$u_{jj} t_{jj}^{(0)} = u_{1j} b_{1j}, \quad b_{1j} \in A, \quad j \geq 2.$$

Según (8)

$$m_{1j} u_{jj} t_{jj}^{(0)} = m_{1j} u_{1j} b_{1j} = 0, \quad j \geq 2.$$

Nótese que entonces $M^{(1)} =: MU^{(0)}$ toma la forma

$$\begin{bmatrix} 0 & 0 & \dots & 0 \\ m_{21}u_{11}t_{11}^{(0)} & m_{22}u_{22}t_{22}^{(0)} \dots m_{2n}u_{nn}t_{nn}^{(0)} \\ \dots & \dots & \dots & \dots \\ m_{n1}u_{11}t_{11}^{(0)} & m_{n2}u_{22}t_{22}^{(0)} \dots m_{nn}u_{nn}t_{nn}^{(0)} \end{bmatrix}$$

Procedemos ahora a anular los elementos de la segunda fila de $M^{(1)}$: Aplicando la condición (2) a los elementos $u_{jj}t_{jj}^{(0)}$, u_{2j} , $j \geq 1$, encontramos $t_{jj}^{(1)} \in S$, $b_{2j} \in A$, $j \geq 1$, tales que

$$u_{jj}t_{jj}^{(0)}t_{jj}^{(1)} = u_{2j}b_{2j}, \quad j \geq 1.$$

Aplicando (8)

$$m_{2j}u_{jj}t_{jj}^{(0)}t_{jj}^{(1)} = m_{2j}u_{2j}b_{2j} = 0, \quad j \geq 1.$$

Nótese que entonces $M^{(2)} =: M^{(1)}U^{(1)}$, donde $U^{(1)} =: D(t_{11}^{(1)}, \dots, t_{nn}^{(1)}) \subset D(n, \delta)$, toma la forma

$$\begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ m_{31}u_{11}t_{11}^{(0)}t_{11}^{(1)} & m_{32}u_{22}t_{22}^{(0)}t_{22}^{(1)} \dots m_{3n}u_{nn}t_{nn}^{(0)}t_{nn}^{(1)} \\ \dots & \dots & \dots & \dots \\ m_{n1}u_{11}t_{11}^{(0)}t_{11}^{(1)} & m_{n2}u_{22}t_{22}^{(0)}t_{22}^{(1)} \dots m_{nn}u_{nn}t_{nn}^{(0)}t_{nn}^{(1)} \end{bmatrix}$$

De manera análoga encontramos matrices diagonales $U^{(2)}, \dots, U^{(n)} \in D(n, s)$ tales que

$$MU^{(0)}, \dots, U^{(n)} = 0,$$

lo cual prueba la condición (1).

Pasamos ahora a probar (2): Sean $M = (m_{ij}) \in M(n, A)$, $D = (d_{ij}) \in D(n, s)$.

Aplicamos (2) a los elementos $m_{1j}, d_{11}, 1 \leq j \leq n$, encontramos $x_{jj}^{(0)} \in S$, $b_{1j} \in A$, $1 \leq j \leq n$, tales que

$$(1) \quad m_{1j} x_{jj}^{(0)} = d_{11} b_{1j}, \quad 1 \leq j \leq n$$

Aplicamos (2) a los elementos $m_{2j}, d_{22}, 1 \leq j \leq n$, encontramos $x_{jj}^{(1)} \in S$, $b_{2j} \in A$, $1 \leq j \leq n$, tales que

$$(2) \quad m_{2j} x_{jj}^{(0)} x_{jj}^{(1)} = d_{22} b_{2j}, \quad 1 \leq j \leq n$$

Continuando de esta manera, aplicamos (2) a los elementos $m_{nj}, x_{jj}^{(0)} \dots x_{jj}^{(n-2)}, d_{nn}$ y encontramos $x_{jj}^{(n-1)} \in S$, $b_{nj} \in A$, $1 \leq j \leq n$ tales que

$$(n) \quad m_{nj} x_{jj}^{(0)} \dots x_{jj}^{(n-1)} = d_{nn} b_{nj}, \quad 1 \leq j \leq n$$

Aplicando combinadamente (1), ..., (n) resulta
 $MT = DB$, donde

$$T = \begin{bmatrix} x_{11}^{(0)} \dots x_{11}^{(n-1)} & & & & & \\ & \ddots & & & & \\ & & & & & \\ & & & & & \\ & 0 & & x_{nn}^{(0)} \dots x_{nn}^{(n-1)} & & \end{bmatrix} \in D(n, s)$$

$$B = \begin{bmatrix} b_{11}x_{11}^{(1)} \dots x_{11}^{(n-1)} & b_{12}x_{22}^{(1)} \dots x_{22}^{(n-1)} \dots b_{1n}x_{nn}^{(1)} \dots x_{nn}^{(n-1)} \\ b_{21}x_{11}^{(2)} \dots x_{11}^{(n-1)} & b_{22}x_{22}^{(2)} \dots x_{22}^{(n-1)} \dots b_{2n}x_{nn}^{(2)} \dots x_{nn}^{(n-1)} \\ \dots & \dots \\ b_{n-1,1}x_{12}^{(n-1)} & b_{n-1,2}x_{22}^{(n-1)} \dots b_{n-1,n}x_{nn}^{(n-1)} \\ b_{n1} & b_{n2} \dots b_{nn} \end{bmatrix}$$

lo cual completa la demostración de la existencia de $M(n, A)D(n, S)^{-1}$.

Veamos ahora que la función

$$g : M(n, A) \longrightarrow M(n, AS^{-1})$$

$$(m_{ij}) \longmapsto \left(\frac{m_{ij}}{1}\right)$$

satisface las condiciones del teorema 2.

Según (5) del parágrafo §2 g es un homomorfismo de anillos. Si $D = (d_{ij}) \in D(n, S)$ entonces $g(D) = \left(\frac{d_{ij}}{1}\right) = D\left(\frac{d_{11}}{1}, \dots, \frac{d_{nn}}{1}\right) \in M(n, AS^{-1})^*$ con inversa $D\left(\frac{d_{11}}{1}, \dots, \frac{d_{nn}}{1}\right)^{-1} = D\left(\frac{1}{d_{11}}, \dots, \frac{1}{d_{nn}}\right)$.

Sea $M = (m_{ij}) \in M(n, A)$ tal que $g(M) = 0$. Existen entonces $u_{ij} \in S$ tales que

$$m_{ij}u_{ij} = 0, \quad 1 \leq i, j \leq n.$$

Repetiendo el procedimiento que sigue a (8) encontramos $V \in D(n, S)$ tal que $MV = 0$.

Resta probar que cada matriz $X = \left(\frac{a_{ij}}{s_{ij}} \right) \in M(n, A\delta^{-1})$ se puede expresar en la forma

$$X = g(A)g(D)^{-1}, \text{ con } A \in M(n, A), D \in D(n, s) .$$

Comencemos con una observación muy sencilla. Dados $\frac{a}{s}, \frac{b}{t} \in AS^{-1}$ existen fracciones con denominador común $\frac{a^t}{r}, \frac{b^t}{r}$ tales que $\frac{a}{s} = \frac{a^t}{r}, \frac{b}{t} = \frac{b^t}{r}$. En efecto, aplicando (2) a s, t encontramos $v \in S, \ell \in A$ tales que $r =: sv = t\ell \in S$; entonces claramente $\frac{av}{sv} = \frac{a}{s}, \frac{b\ell}{t\ell} = \frac{b}{t}$.

Aplicamos esta observación a los elementos de cada columna de X y encontraremos $X^* = X$ donde los denominadores por columnas son iguales, digamos

$$X = X^* = \begin{pmatrix} \frac{a_{11}^*}{r_1} & \cdots & \frac{a_{1n}^*}{r_n} \\ \vdots & & \vdots \\ \frac{a_{n1}^*}{r_1} & & \frac{a_{nn}^*}{r_n} \end{pmatrix} .$$

Nótese que $X = X^* = g(A)g(D)^{-1}$ donde $A = (a_{ij}^*)$, $D = D(r_1, \dots, r_n) \in D(n, S)$.

BIBLIOGRAFIA

- [1] Atiyah, M.F. and MacDonald, I.G., *Introduction*

to commutative algebra, Addison-Wesley, 1969.

[2] Stenström, Bo., *Rings of quotients: An introduction to methods of ring theory*, Springer, 1975.

D. M. Luna: Descomposición de un polinomio en la \mathbb{Z}_p , en sus factores irreducibles mediante un algoritmo de Euclides. ****** Algunas soluciones al problema de la factorización de polinomios en \mathbb{Z}_p .

Departamento de Matemáticas y Estadística
Universidad Nacional de Colombia
BOGOTÁ. D.E.