Capítulo 1

Introducción a los anillos de división

Los anillo más completos desde el punto de vista de sus operaciones son sin duda los anillos de división ya que en ellos no sólo podemos sumar y multiplicar, sino dividir por elementos no nulos. Independientemente, el teorema de Wedderburn-Artin sobre los anillos artinianos semisimples nos obliga a concentrar la atención sobre este tipo de anillos. Un tanto de los mismo podría decirse de los anillos primitivos para los cuales, su propiedad de tener para cada natural $n > 1$ un subanillo epimórfico a un anillo $\mathcal{M}_n(\Delta)$ (con Δ un anillo de división), permite también reducir algunas cuestiones de anillos primitivos al caso de los anillos de división. Así por ejemplo la demostración de que un anillo tal que para cada conmutador $d = [a, b]$ existe un natural $n > 1$ con $d^n = d$, es necesariamente conmutativo, se reduce fácilmente al caso de los anillos primitivos (via cociente por el radical y usando los productos subdirectos de anillos primitivos). A partir de aqui la reducción al caso de anillos de división es también cosa de coser y cantar.

A grandes rasgos los anillos de división se dividen en dos grandes clases según que la dimensión del anillo sobre su centro sea de dimensión finita o no. La Teoría de Los anillos de división *centralmente finitos* (es decir los que tiene $(D, Z(D))$ finita) está muy bien desarrollada y merece un capítulo especial para su estudio. Sin embargo en esta introducción nos vamos a ocupar de ciertos resultados generales sobre anillos de división no necesariamente finito-dimensionales sobre su centro.

1.1. Teorema de Wedderburn

Entre los resultados sobre anillos de división que vamos a estudiar, destaca en primer lugar el Teorema de Wedderburn (también llamado el 'pequeño' teorema de Wedderburn). La demostración que vamos a dar esta basada en la ecuación de clases de teoría de grupos así como en las propiedades de los polinomios

ciclotómicos.

Para los cuerpos finitos es conocido el resultado según el cual los subgrupos del grupo de elementos inversibles de un tal cuerpo, son cíclicos. Vamos a extender este resultado en el siguiente

Corolario 1 *Sea D un anillo de divisón de característica prima y G un subgrupo finito de D^*. Entonces G es cíclico.*

Dem. Sea $F = \mathbb{Z}_p$ el cuerpo primo de D y consideremos el conjunto

$$K = \{\sum_i \alpha_i g_i : \alpha_i \in F, g_i \in G\}.$$

Evidentemente K es un subanillo finito de D por tanto un dominio finito lo que implica que es un subanillo de división y aplicando el Teorema de Wedderburn un cuerpo finito. Como G es un subgrupo de K^*, aplicando el resultado correspondiente para cuerpos finitos, resulta que G es cíclico.■

La hipótesis de característica prima del último corolario es irrenunciable. Por ejemplo si consideramos el anillo de los cuaterniones reales de división $\mathbb{H}$, podemos considerar el grupo cuaterniónico $G = \{\pm 1, \pm i, \pm j, \pm k\}$ que es subgrupo de $\mathbb{H}^*$ pero no es cíclico. Otro grupo finito más grande aún contenido en $\mathbb{H}$ es el llamado grupo *binario tetraedrico*:

$$\{\pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2\}$$

que es de orden 24. Uno podría plantearse de forma natural acerca de cuáles son los grupos finitos que aparecen como subgrupos de D^* para algún anillo de división D de característica cero. La respuesta completa a esta cuestión fué dada por Amitsur en 1955.

1.2. Teorema de Jacobson-Herstein

Para empezar demostraremos una serie de resultados que necesitaremos más tarde.

Proposición 1 *Sea D un anillo de división. Si un elemento $y \in D$ conmuta con todos los conmutadores aditivos (elementos $[a, b] := ab - ba$), entonces $y \in Z(D)$.*

Dem. Supongamos $y \notin Z(D)$, entonces existe $x \in D$ tal que $xy \neq yx$. Pero dada la igualdad $[x, xy] = x(xy) - (xy)x = x[x, y]$ se tiene $x = [x, xy][x, y]^{-1}$ lo que implica que y conmuta con x en contradicción con la suposición inicial.■

Corolario 2 *Si todos los conmutadores aditivos son centrales en un anillo de división D, entonces D es un cuerpo.*

Corolario 3 *Sea D un anillo de división no conmutativo. Entonces D está generado por todos los conmutadores aditivos junto con los elementos de $Z(D)$.*

Dem. Hablando en otros términos, lo que este corolario asegura es que el menor subanillo de división de D que contiene a $Z(D)$ y a todos los conmutadores aditivos, es el propio D. Para demostrarlo sea D' el subanillo de división de D generado por $Z(D)$ junto con los conmutadores aditivos. Tomemos $x \notin Z(D)$, entonces $xy \neq yx$ para algún $y \in D$. El anillo D' contiene a $[x, xy] = x[x, y]$, por tanto contiene a $[x, xy][x, y]^{-1} = x$. En consecuencia $D' = D$.■

Lema 1 (Lema de Herstein). *Sea D un anillo de división de característica prima p. Sea $a \in D^*$ un elemento no central y de torsión. Entonces existe $y \in D^*$ tal que $yay^{-1} = a^i \neq a$ para algún $i > 0$. Más aún, y puede elegirse siendo un conmutador aditivo.*

Dem. Denotemos por $\mathbb{F}_p$ el cuerpo primo de D. Adjuntado a al cuerpo primo obtenemos un cuerpo finito $K := \mathbb{F}_p(a) \subset D$. Si suponemos que $|K| = p^n$ entonces $a^{p^n} = a$. Consideremos la derivación $\delta_a : D \to D$ definida por $\delta_a(x) = [a, x] = ax - xa$ para cada x. Esta derivación es no nula al ser a un elemento no central. Además $\delta_a(K) = 0$ lo que implica que δ_a es una aplicación K-lineal de ${}_KD$ en ${}_KD$. La parte mas importante de esta demostración consiste en constatar que δ_a tiene un vector propio en ${}_KD$.

Sea $E = \mathrm{End}_K({}_KD)$ el anillo de endomorfismos del K-espacio vectorial ${}_KD$. Entonces para cada $f \in E$ se tiene $pf = 0$. Definamos los operadores de multiplicación a izquiera y derecha $L_a, R_a :_K D \to_K D$ por $L_a(x) = ax$, $R_a(x) = xa$ para cada x. Estos operadores conmutan evidentemente. Además $\delta_a = L_a - R_a$ y en consecuencia

$$\delta_a^{p^n} = (L_a - R_a)^{p^n} = L_a^{p^n} - R_a^{p^n} = L_a - R_a = \delta_a$$

al ser los números combinatorios $\binom{p^n}{j}$ multiplos de p para $j = 1, \ldots, p^n - 1$. Por tanto tenemos $\delta_a^{p^n} = \delta_a$. Por otra parte, sobre el cuerpo K de p^n elementos se tiene que el polinomio $t^{p^n} - t \in K[t]$ se factoriza de la forma

$$t^{p^n} - t = \prod_{b \in K} (t - b)$$

y por tanto en el anillo E tendremos

$$0 = \delta_a^{p^n} - \delta_a = (\prod_{b \in K^*} (\delta_a - b))\delta_a$$

y como $\delta_a \neq 0$, esto implica que algunos de los factores $\delta_a - b$ no es un monomorfismo (para $b \in K^*$). En consecuencia $(\delta_a - b)(x) = 0$ para algún $x \neq 0$ y hemos demostrado que x es un vector propio de δ_a con autovalor $b \in K^*$. Entonces $bx = \delta_a(x) = ax - xa$ y por tanto $xa = (a - b)x$ o bien $xax^{-1} = a - b \in K - \{a\}$. Ahora bien el grupo de elementos inversibles de un cuerpo finito es cíclico luego K^* lo es. Así los elementos a y xax^{-1} que tienen el mismo orden en el grupo K^* general el mismo subgrupo cíclico. (en un grupo cíclico existe un único subgrupo cíclico de un orden dado). Podemos concluir entonces que los subgrupos

generados por a y por xax^{-1} son el mismo y por tanto $xax^{-1} = a^i \neq a$ para algún i. No puede ocurrir $i = 0$ ya que en esta caso $xax^{-1} = 1$ lo que implicaría $a = 1$ en contra de que a no es central. Si ahora sustituimos x por el conmutador aditivo $y = \delta_a(x) = [a, x] \neq 0$, entonces

$$ya = (ax - xa)a = aa^i x - a^i xa = a^i y$$

y por tanto $yay^{-1} = a^i \neq a$. ■

Vamos ahora a atar un cabo suelto de habíamos dejado en el capítulo dedicado a los anillos primitivos. Tal es el Teorema de Jacobson-Herstein en su versión para anillos de división. Aunque tal teoerema es válido para anillos en general, la demostración que se hizo en su momento descansaba sobre el hecho de que dicho teorema se satisface para los anillos de división. Este es el momento de demostrarlo:

Teorema 1 *Sea D un anillo de división tal que para cualesquiera $a, b \in D$ existe un entero $n > 1$ tal que $[a, b]^n = [a, b]$. Entonces D es conmutativo.*

Dem. Por hipótesis cada conmutador aditivo no nulo tiene orden finito en D^*. Supongamos que D no es conmutativo, entonces algún conmutador aditivo $a = [b, b'] \notin F$ (véase el Corolario 2). Sea $c \in F^*$ cualquiera, entonces $ca = cbb' - cb'b = cbb' - b'cb = [cb, b']$ es también un conmutador aditivo no nulo. Como a y ca tienen ambos orden finito, existe un entero $k > 0$ tal que

$$1 = a^k = (ca)^k = c^k a^k,$$

por tanto $c^k = 1$. Esto implica que la característica de F (que conincide con la de D) es distinta de cero (si F fuera de característica cero su cuerpo primo sería $\mathbb{Q}$ donde $c^k = 1$ no ocurre para todo elemento no nulo). El elemento a que hemos considerado antes es no central y de torsión. Aplicando el Lema de Herstein sabemos la existencia de un conmutador aditivo $y \in D^*$ tal que $yay^{-1} = a^i \neq a$ para algún $i > 0$. Las hipotesis de este teorema implican entonces que y es de torsión. Además El producto $(a)(y)$ es un subgrupo finito de D^*. En virtud del Corolario 1, este subgrupo es conmutativo lo que implicaría $a = yay^{-1} = a^i \neq a$, una contradicción. ■

1.3. Álgebras de división

Para motivar la definición de álgebra sobre un cuerpo consideremos un anillo de división D y sea F su centro. Entonces D es un F-espacio vectorial y además para cualesquiera elementos $\lambda \in F$, $x, y \in D$ se tiene $(\lambda x)y = x(\lambda y) = \lambda xy$. Haciendo abstracción de este hecho podemos dar la siguiente definición:

Definición 1 Sea F un cuerpo y R un anillo que tiene estructura de F-espacio vectorial de modo que para cualesquiera $x, y \in R$, $\lambda \in F$ se tiene $(\lambda x)y = x(\lambda y) = \lambda xy$. Entonces diremos que R es una F-álgebra. Un ideal I (a derecha,

izquierda o bilátero) de la F-álgebra R es por definición un ideal del anillo subyacente a R, que es a su vez subespacio del espacio vectorial R. En forma análoga se definen las subalgebras de R.

Hay numerosos ejemplos de álgebras. Por ejemplo si F es un cuerpo el anillo de las matrices cuadradas con coeficientes en F es una F-álgebra con las operaciones obvias. En forma más general, si R es una F-álgebra, entonces $\mathcal{M}_n(R)$ es una F-álgebra con las operaciones usuales.
Una de las ventajas de trabajar con álgebras es la posibilidad de aplicar álgebra lineal a nuestros razonamientos. En lo sucesivo vamos a tratar de describir ciertos tipos de álgebras de división sobre diferentes cuerpos. Dejaremos sin embargo claro, que este problema es en general dificil, y sólo en unos pocos casos están descritas las álgebras de división sobre cuerpos determinados.

Definición 2 Una F-álgebra R diremos que es algebraica sobre F si cada elemento de R es algebraico sobre F, es decir, satisface un polinomio mónico con coeficientes en F. Diremos que una F-álgebra D es de división si el anillo subyacente es un anillo de división.

Evidentemente cada F-álgebra de dimensión finita es algebraica pero el resultado recíproco no es cierto en general. Vamos a empezar describiendo las álgebras de división algebraicas sobre cuerpos finitos.

Teorema 2 *Sea F un cuerpo finito y D una F-álgebra de división algebraica (sobre F). Entonces D es conmutativa (y por tanto es un cuerpo finito extensión de F).*

Dem. Sea p la característica de F y para cada $d \in D$ consideremos la subálgebra $F[d]$ de D generada por d. Ésta no es más que el conjunto de polinomios en d con coeficientes en F. Por tanto es un dominio finito y en consecuencia un cuerpo. Así si $|F[d]| = p^n$ se tiene $d^{p^n} = d$. Se satisfacen entonces la hipótesis del Teorema 1 lo que nos permite concluir que D es conmutativa.■

Teorema 3 (Teorema de Frobenius). *Sea D un álgebra de división algebraica sobre $\mathbb{R}$, entonces D es isomorfa a $\mathbb{R}$, $\mathbb{C}$ o $\mathbb{H}$.*

Dem. Si $\dim_{\mathbb{R}}(D) = 1$ se tiene un isomorfismo $D \cong \mathbb{R}$ y no hay nada más que demostrar. Supongamos entonces $\dim_{\mathbb{R}}(D) \geq 2$ y tomemos $\alpha \in D - \mathbb{R}$. Entonces la subálgebra de D generada por α (denotada $\mathbb{R}[\alpha]$) es una extensión algebraica propia de $\mathbb{R}$ luego es isomorfa a $\mathbb{C}$. Supondremos entonces en lo sucesivo a $\mathbb{C}$ sumergido en D y consideremos a D como $\mathbb{C}$-espacio vectorial por la izquierda. Definamos ahora los siguientes subespacios

$$D^+ := \{d \in D : di = id\}, \qquad D^- := \{d \in D : di = -id\}.$$

Se tiene entonces $D^+ \cap D^- = 0$ y para cada $d \in D$ el elemento $di + id \in D^+$ ya que $i(di + id) = idi - d = (id + di)i$. Además $di - id \in D^-$ ya que $(di - id)i = -d - idi = i(id - di) = -i(di - id)$. Como

$$d = \frac{1}{2i}(di + id) + \frac{1}{2i}(di - id)$$

queda demostrado que $D = D^+ \oplus D^-$.
Tomemos ahora un elemento $d^+ \in D^+$, entonces la subálgebra de D generada por d^+ (denotada $\mathbb{C}[d^+]$) es una extensión algebraica finita de $\mathbb{C}$. Por tanto coincide con $\mathbb{C}$. Esto demuestra que $D^+ = \mathbb{C}$. Si $D^- = 0$ entonces $D \cong \mathbb{C}$. En caso contrario podemos fijar un elemento no nulo $z \in D^-$. La aplicación $\mu : D^- \to D^+$ tal que $z \mapsto xz$ es inyectiva lo que demuestra que $\dim_{\mathbb{C}}(D^-) = 1$. En consecuencia $\dim_{\mathbb{R}}(D) = 2\dim_{\mathbb{C}}(D) = 4$.
Como el elemento z satisface un polinomio mónico de segundo grado con coeficientes reales, podemos escribir $z^2 \in \mathbb{R} \oplus \mathbb{R}z$. Además $z^2 = \mu(z) \in D^+ = \mathbb{C}$. Así $z^2 \in \mathbb{C} \cap (\mathbb{R} + \mathbb{R}z) = \mathbb{R}$ lo que implica que $z^2 \in \mathbb{R}$. Si $z^2 > 0$ podemos escribir $z^2 = r^2$ para un $r \in \mathbb{R}$ y entonces $z = \pm r \in \mathbb{R}$ una contradicción. Necesariamente entonces $z^2 < 0$ lo que nos lleva a escribir $z^2 = -r^2$ para $r \in \mathbb{R}^*$. Podemos ahora definir $j := z/r$ y tenemos $j^2 = z^2/r^2 = -1$. Como $z \in D^-$ se tiene $ij = -ji$ y definiendo $k := ij$ tenemos $D^- = \mathbb{R}j + \mathbb{R}k$ de donde

$$D = D^+ \oplus D^- = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$

así es que D es isomorfa al álgebra de cuaterniones reales de división $\mathbb{H}$. ■

1.4. El teorema de Cartan-Brauer-Hua.

Para establecer este teorema necesitaremos la siguiente indentidad:

$$a(a^{-1}ca - b^{-1}cb) = c - b^{-1}cb \neq 0$$

que es válida para dos elementos a, c que no conmutan en un anillo de división D, y para $b := 1 - a$. Para demostrarla hagamos

$$a(a^{-1}ca - b^{-1}cb) = ca - ab^{-1}cb = c(b+1) - (b+1)b^{-1}cb =$$

$$= cb + c - cb - b^{-1}cb = c - b^{-1}cb \neq 0.$$

Gracias a esta fórmula estamos en condiciones de demostrar el

Teorema 4 (Teorema de Cartan-Brauer-Hua). *Sean K y D anillos de división tales que K es subanillo de D. Supongamos que el grupo K^* es normal en D^*. Entonces $K \subset Z(D)$.*

Dem. Sea $a \in D - K$ y $c \in K$. Veamos que conmutan. Si no lo hicieran, la fórmula que acabamos de demostrar arriba implica que $a \in K^*$ al ser $c, a^{-1}ca, b^{-1}cb \in K^*$. Así pues c conmuta con todo elemento de $D - K$. Veamos ahora que también conmuta con los elementos de K. Tomemos $c' \in K^*$ cualquiera. Fijemos $a \in D - K$ como antes. Entonces $ac' \in D - K$ y por tanto c conmuta con ac'. Como c conmuta también con a, tendrá que conmutar con $a^{-1}ac' = c'$. Por tanto c conmuta con los elementos de K también y concluimos que $c \in Z(D)$. ■

Capítulo 2

Teoría de Goldie

En este capítulo haremos un estudio de los anillos que satisfacen ciertas condiciones de cadena ascendente. Nos centraremos en el caso no conmutativo donde los resultados clave se deben a Goldie. En este capítulo, los anillos se supondran unitarios a menos que se especifique.

Definición 3 Un elemento a de un anillo R se dice regular si no es divisor de cero por la derecha ni por la izquierda. El conjunto de elementos regulares de R se denotará $\mathrm{Reg}(R)$. Un anillo $Q(R) \supset R$ se dice que es un anillo de cocientes por la izquierda de R si:

1. Cada $a \in R$ regular es inversible en $Q(R)$.
2. Para todo $x \in Q(R)$ existen $a, b \in R$ (con a regular en R) tales que $x = a^{-1}b$,

Seguiremos a continuación con un teorema debido a Ore donde se da una condición necesaria y suficiente para la existencia de un anillo de cocientes por la izquierda:

Teorema 5 *Una condición necesaria y suficiente para que un anillo R tenga un anillo de cocientes por la izquierda es que para todos $a \in R$, $b \in Reg(R)$, se tenga $Reg(R)a \cap Rb \neq \emptyset$.*[1]

Dem. Si $Q(R)$ existe $ab^{-1} \in Q(R)$ luego $ab^{-1} = b_1^{-1}a_1$ con $b_1 \in \mathrm{Reg}(R)$. Entonces $a = b_1^{-1}a_1b$ luego $b_1a = a_1b \in \mathrm{Reg}(R)a \cap Rb$. Hemos demostrado una de las implicaciones. Antes de abordar el recíproco, pensemos en el hecho de que dos elementos del anillo de fracciones sean iguales. Es decir si $b^{-1}a = d^{-1}c$ con $a, b, c, d \in R$, $b, d \in \mathrm{Reg}(R)$, entonces $a = bd^{-1}c$ y como $bd^{-1} \in Q(R)$ se tendrá $bd^{-1} = d_1^{-1}b_1$ para ciertos elementos $b_1, d_1 \in R$ con $d_1 \in \mathrm{Reg}(R)$. En consecuencia $a = d_1^{-1}b_1c$ y por tanto $d_1a = b_1c$. Además $d_1b = b_1d$. En definitiva:

$$b^{-1}a = d^{-1}c \Leftrightarrow (\exists\ b_1, d_1 \in \mathrm{Reg}(R) : d_1a = b_1c, d_1b = b_1d).$$

[1] Ésta, es conocida como la condiciòn de Ore.

Demostremos ahora la otra implicación supongamos que R satisface la condición $\mathrm{Reg}(R)a \cap Rb \neq \emptyset$ (para b regular). Para construir un anillo de cocientes $Q(R)$ partiremos del conjunto

$$\mathcal{M} := \{(a,b) \in R \times R : b \in \mathrm{Reg}(R)\}$$

donde definiremos una relación de equivalencia

$$(a,b) \equiv (c,d) \Leftrightarrow (\exists\ b_1, d_1 \in R : d_1 a = b_1 c, d_1 b = b_1 d \in \mathrm{Reg}(R)).$$

Vamos a demostrar que se trata de una relación de equivalencia. Las propiedades reflexiva y simétrica de $\equiv$ son triviales. Para demostrar la transitividad sean $(a,s) \equiv (c,t) \equiv (e,u)$. Entonces existen elementos $\alpha, \beta, \delta, \gamma$ de R tales que $\alpha a = \beta c$, $\alpha s = \beta t \in \mathrm{Reg}(R)$, $\delta c = \gamma e$, $\delta t = \gamma u \in \mathrm{Reg}(R)$. Como $\mathrm{Reg}(R)\delta t \cap R\beta t \neq \emptyset$ podemos escribir $r\beta t = s\delta t$ para ciertos elementos $r \in R$, $s \in \mathrm{Reg}(R)$. Como $t \in \mathrm{Reg}(R)$ se deduce que $r\beta = s\delta$. Por lo tanto

$$\begin{gathered}(r\alpha)a = r\beta c = s\delta c = (s\gamma)e \\ (r\alpha)s = r\beta t = s\delta t = (s\gamma)u \in \mathrm{Reg}(R).\end{gathered}$$

En consecuencia $(a,s) \equiv (e,u)$. Denotaremos por $Q(R)$ al conjunto cociente $R \times \mathrm{Reg}(R)/\equiv$. la clase de equivalencia de un par $(x,s) \in R \times \mathrm{Reg}(R)$ vamos a denotarla mediante $s^{-1}x$ y la llamaremos *fracción* (con denominadores por la izquierda). Definamos una operación de suma en $Q(R)$. Para ello veremos que cada par de fracciones $s^{-1}x, t^{-1}y$ se pueden reducir a común denominador. La condición de Ore $\mathrm{Reg}(R)s \cap Rt \neq \emptyset$ implica la posibilidad de escribir $s_1 s = rt$ para ciertos elementos $r \in R$, $s_1 \in \mathrm{Reg}(R)$. Entonces se tiene $(x,s) \equiv (s_1 x, s_1 s)$, $(y,t) \equiv (ry, rt)$ de donde las fracciones dadas se pueden reducir al común denominador $rt = s_1 s$. Aprovechando esta circunstancia definimos la suma

$$s^{-1}x + s^{-1}y = s^{-1}(x+y)$$

en $Q(R)$. Esta definición plantea el problema de la independencia respecto a los representantes de clase elegidos. Vamos a resolverlo. Supongamos $(x,s) \equiv (x',s')$, $(y,s) \equiv (y',s')$. Debemos demostrar que $(x+y,s) \equiv (x'+y',s')$. Para ello tengamos en cuenta que $\exists \alpha, \alpha' : \alpha x = \alpha' x'$, $\alpha s = \alpha' s' \in \mathrm{Reg}(R)$. Además existen β, β' tales que $\beta y = \beta' y'$, $\beta s = \beta' s' \in \mathrm{Reg}(R)$. A partir de la condición de Ore $\mathrm{Reg}(R)\alpha s \cap R\beta s \neq \emptyset$ se tiene que $\exists s_1 \in \mathrm{Reg}(R)$, $\exists r \in R$ tales que

$$s_1 \alpha s = r\beta s \tag{2.1}$$

implicando $s_1\alpha = r\beta$. Además a partir de la ecuación 2.1 se deduce $s_1\alpha' s' = r\beta' s'$ lo que permite concluir también que $s_1\alpha' = r\beta'$. Entonces

$$s_1\alpha(x+y) = s_1\alpha x + s_1\alpha y = s_1\alpha' x' + r\beta y = s_1\alpha' x' + r\beta' y' = s_1\alpha'(x' + y')$$

siendo además $s_1\alpha s = r\beta s = r\beta' s' = s_1\alpha' s' \in \mathrm{Reg}(R)$ lo que demuestra que $(x+y,s) \equiv (x'+y',s')$. Así la definición de suma en $Q(R)$ es correcta. Evidentemente todos los elementos $(0,s)$ estan en la misma clase de equivalencia, siendo este por

tanto el elemento neutro para la suma de $Q(R)$. Se comprueban sin dificultad el resto de las propiedades de $(Q(R),+)$ que de hecho dotan a esta pareja de estructura de grupo abeliano.

Vamos ahora de definir una multiplicación en $Q(R)$ de manera que $Q(R)$ se convierta en un anillo que cumpla los requisitos de un anillo de cocientes. Definimos entonces la multiplicación de la clase de equivalencia de (x,s) por la de (y,t) como la clase de (x_1y, s_1s) donde $x_1, s_1 \in R$, $s_1 \in \mathrm{Reg}(R)$ y $s_1x = x_1t$. Veamos en primer lugar que la definición no depende de los elementos intermedios s_1 y x_1 elegidos. Supongamos pues que $x_2, s_2 \in R$ con s_2 regular y $s_2x = x_2t$. Entonces debemos probar que $(x_1y, s_1s) \equiv (x_2y, s_2s)$. La condición de Ore $\mathrm{Reg}(R)s_1s \cap Rs_2s \neq \emptyset$ implica que podamos escribir $s_0s_1s = rs_2s$ para $s_0 \in \mathrm{Reg}(R)$. Entonces $s_0s_1 = rs_2$. Por otra parte

$$s_0x_1t = s_0s_1x = rs_2x = rx_2t$$

de donde $s_0x_1 = rx_2$. Entonces $s_0x_1y = rx_2y$ que junto con $s_0s_1s = rs_2s$ (demostrada antes) implica $(x_1y, s_1s) \equiv (x_2y, s_2s)$. Independicemos ahora la definición del producto del representante elegido en el primer factor. Es decir, sea que $s^{-1}x.t^{-1}y = (s_1s)^{-1}x_1y$ donde $s_1x = x_1t$. Supongamos que $s^{-1}x = s'^{-1}x'$ y que $s'^{-1}x'.t^{-1}y = (s'_1s')^{-1}x'_1y$ donde $s'_1x' = x'_1t$. Debemos demostrar que $(x_1y, s_1s) \equiv (x'_1y, s'_1s')$. A partir de la relación $(x,s) \equiv (x',s')$ tenemos la existencia de α, α' tales que

$$\alpha x = \alpha' x', \qquad \alpha s = \alpha' s' \in \mathrm{Reg}(R).$$

En primer lugar la condición de Ore $\mathrm{Reg}(R)\alpha \cap Rs_1 \neq \emptyset$ nos hace escribir $\beta\alpha = rs_1$ (donde β es regular). Se tiene entonces

$$\beta\alpha' x' = \beta\alpha x = rs_1x = rx_1t.$$

La condición de Ore $\mathrm{Reg}(R)\beta\alpha' \cap Rs'_1 \neq \emptyset$ nos permite deducir que $s_2\beta\alpha' = r_1s'_1$ para algún s_2 regular. Por tanto

$$r_1x'_1t = r_1s'_1x' = s_2\beta\alpha' x' = s_2rx_1t$$

y dada la regularidad de t tenemos

$$r_1x'_1 = s_2rx_1.$$

En consecuencia $(s_2r)x_1y = r_1x'_1y$ lo que nos lleva por el buen camino para demostrar $(x_1y, s_1s) \equiv (x'_1y, s'_1s')$. Nos quedaría ver que $(s_2r)s_1s = r_1s'_1s'$ pero esto es así de fácil:

$$(s_2r)s_1s = s_2\beta\alpha s = s_2\beta\alpha' s' = r_1s'_1s'.$$

Con semejante tipos de razonamientos se demuestra que la definición del producto no depende del representante elegido en el segundo factor. Ahora podemos proponer al lector como ejercicio el comprobar:

1. Que todas las parejas (s, s) (con s regular) están relacionadas y que de hecho la clase de equivalencia de ellas es el elemento neutro para la multiplicación definida en $Q(R)$.

2. Que para cada elemento regular $s \in \mathrm{Reg}(R)$, los elementos $1^{-1}s$ (es decir, las clases de equivalencia de $(s, 1)$ son inversibles en $Q(R)$ con inverso $s^{-1}1$ (es decir la clase de $(1, s)$).

3. El resto de las propiedades del producto, así como del producto en relación con la suma, que hacen de $(Q(R), +, \cdot)$ un anillo.

Por último resaltemos el hecho de que la aplicación $j : R \to Q(R)$ tal que $j(x) = 1^{-1}x$ es un monomorfismo de anillos. Además el lector puede comprobar que para cualquier homomorfismo de anillos $f : R \to X$ tal que f transforme los elementos regulares de R en elementos inversibles del anillo X, existe un único homomorfismo de anillos $g : Q(R) \to X$ tal que $g \circ j = f$. Esta propiedad universal del anillo de cocientes permite asimismo demostrar la únicidad salvo isomorfismos de esta construcción.