

Álgebra I

Curso 2020/21

Índice

1	El lenguaje de los conjuntos	5
1.1	Sobre la teoría axiomática de conjuntos	6
1.1.1	Proposiciones y Demostraciones.	11
1.2	El conjunto producto cartesiano. Aplicaciones	15
1.2.1	Imágenes directas e inversas	19
1.3	Relaciones de equivalencia. Conjuntos cocientes.	21
2	Anillos conmutativos	25
2.1	Los anillos \mathbb{Z}_n	26
2.2	Generalidades	28
2.3	Los anillos de enteros cuadráticos $\mathbb{Z}[\sqrt{n}]$	30
2.4	Múltiplos y potencias naturales	32
2.5	Unidades. Cuerpos	33
2.6	Múltiplos negativos y potencias de exponente negativo	35
2.7	Los anillos de polinomios $A[x]$	37
2.8	Homomorfismos	40
3	Divisibilidad en Dominios Euclideos	43
3.1	Dominios de Integridad	43
3.2	El cuerpo de fracciones de un DI	44
3.3	Divisibilidad	46
3.4	Dominios Euclideos	48
3.5	Máximo común divisor	52
3.6	Ecuaciones diofánticas	56
3.7	Mínimo común múltiplo	58
3.8	Congruencias	59
3.9	La ecuación básica $ax \equiv b \pmod{m}$	61
3.10	Sistemas de congruencias	62
3.10.1	Sistemas de 2 congruencias	62
3.10.2	Sistemas de r congruencias	63
4	Anillos cocientes	65
4.1	Complementos sobre \mathbb{Z}_n	66
4.1.1	La ecuación $ax = b$ en \mathbb{Z}_n	66
4.1.2	La función φ de Euler	67

5	Dominios de Factorización Única	73
5.1	Caracterización de DFU	74
5.2	Todo DE es un DFU	75
5.3	Irreducibles y primos en $\mathbb{Z}[\sqrt{n}]$	76
5.4	Factorización única en anillos de polinomios	78
5.4.1	Criterios básicos de irreducibilidad de polinomios	81

1.3 Relaciones de equivalencia. Conjuntos cocientes.

Definimos una *relación* (binaria) entre los elementos de un conjunto S (o, simplemente, en S) como un subconjunto $R \subseteq S \times S$.

Si $(a, b) \in R$, se dice que a *está relacionado con* b por la relación R , y se escribe aRb . Muchas relaciones tienen una o más de las siguientes propiedades:

- **Reflexiva.** $\forall a \in S, aRa$.
- **Simétrica.** $\forall a, b \in S$, si aRb , entonces bRa .
- **Transitiva.** $\forall a, b, c \in S$, si aRb y bRc , entonces aRc .

Por ejemplo:

1. La relación “ a es padre de b ” referida al conjunto de los humanos, no tiene ninguna de estas propiedades.
2. La relación “ a tiene los mismos parientes que b ” tiene las tres.
3. La relación “ a es antecesor de b ” es transitiva.
4. La relación “ a es hermano de b ” es simétrica.

Una relación R en un conjunto S que es reflexiva, simétrica y transitiva es llamada una *relación de equivalencia* sobre S .

Una relación de equivalencia separa los elementos del conjunto S en *bloques* o *clases de equivalencia* donde se agrupan todos los elementos que se relacionan entre sí por la relación dada. Si $a \in S$ es cualquier elemento, definimos “*su clase de equivalencia*” o “*la clase de equivalencia que representa a*”, denotada por \bar{a} (o $[a]$), como el subconjunto de S

$$\bar{a} = \{x \in S \mid xRa\},$$

donde se reúnen todos los elementos equivalentes a a . Cada uno de estos subconjuntos es no vacío, pues por la reflexividad $a \in \bar{a}$, y se verifica que cualesquiera dos bloques \bar{a} , \bar{b} bien son disjuntos o coinciden:

Proposición 1.3.1. *para cualesquiera $a, b \in S$, son equivalentes*

1. $\bar{a} \cap \bar{b} \neq \emptyset$.
2. aRb .
3. $\bar{a} = \bar{b}$.

DEMOSTRACIÓN. (1) \Rightarrow (2): Supongamos que $\exists c \in \bar{a} \cap \bar{b}$. Como cRa y cRb , por la simetría, tenemos aRc y cRb , y entonces, por la transitividad, aRb .

(2) \Rightarrow (3): Si $x \in \bar{a}$, entonces $xRa \wedge aRb \Rightarrow xRb \Rightarrow x \in \bar{b}$, así que $\bar{a} \subseteq \bar{b}$. Un argumento similar prueba que $\bar{b} \subseteq \bar{a}$ y por tanto $\bar{a} = \bar{b}$.

(3) \Rightarrow (1) Es obvio. □

Resulta así que las diferentes clases de equivalencia proporcionan una descomposición S en subconjuntos no vacíos dos cualesquiera de ellos son disjuntos. Esto es lo que se llama una *partición* de S .

Por ejemplo, si R es la relación “ a tiene los mismos parientes que b ” entre los españoles, que es claramente de equivalencia, agrupa a los españoles en bloques conformados por las familias.

Si R es la relación entre los puntos del plano \mathbb{R}^2 estableciendo que pRq si p y q están a la misma distancia del origen, los bloques son las circunferencias $C_r = \bar{r}$ centradas en el origen y radio r , con $r \geq 0$.

Similarmente, si R es la relación “ a da el mismo resto que b al dividirlo por 2” sobre el conjunto $\mathbb{N} = \{0, 1, \dots\}$ de los números naturales, esta relación parte el conjunto de naturales en dos subconjuntos disjuntos, de una parte el conjunto de los números pares, $\bar{0}$, y de otra el conjunto de los impares, $\bar{1}$.

Dada una relación de equivalencia R sobre un conjunto S , se define el *conjunto cociente de S por la relación R* , denotado S/R , como el conjunto cuyos elementos son los diferentes bloques o clases de equivalencia para tal relación:

$$S/R = \{\bar{a} \in \mathcal{P}(S) \mid a \in S\}.$$

En tal descripción, es muy importante tener claro que, aunque los elementos de S/R están parametrizados por los elementos a de S , tal parametrización no es unívoca pues tenemos que tener muy presente que

$$\bar{a} = \bar{b} \Leftrightarrow aRb.$$

Desde esa observación, puede pensarse en el conjunto cociente S/R como el *que se obtiene a considerar iguales (el mismo, identificados) todos los elementos de S que son equivalentes entre sí por la relación dada*.

Así, por ejemplo, para la relación R sobre \mathbb{N} donde dos números son equivalentes si dan el mismo resto al dividirlos por 2, el conjunto cociente tiene exactamente dos elementos

$$S/R = \{\bar{0}, \bar{1}\},$$

puesto que para cualquier natural n , $\bar{n} = \bar{0}$ si n es par, y $\bar{n} = \bar{1}$ si n es impar.

Análogamente, Si R es la relación entre los puntos del plano \mathbb{R}^2 estableciendo que dos puntos p y q son equivalentes si están a la misma distancia del origen, el conjunto cociente

$$\mathbb{R}^2/R = \{C_r \mid r \in \mathbb{R}, r \geq 0\}$$

es el conjunto de las diferentes circunferencias centradas en el origen del plano \mathbb{R}^2 (¡sus elementos son circunferencias, no puntos!).

La proyección canónica. Dada una relación de equivalencia R en un conjunto S se tiene una aplicación que llamaremos la proyección canónica $p : S \rightarrow S/R$ y que lleva un elemento $x \in S$ en su clase de equivalencia, $p(x) = \bar{x}$. Esta aplicación es claramente sobreyectiva.

La relación núcleo de una aplicación. Toda aplicación $f : S \rightarrow T$ da lugar a una relación de equivalencia R_f en su dominio S , definida por $xR_f y \Leftrightarrow f(x) = f(y), \forall x, y \in S$. Esta relación es llamada la relación núcleo de f .

Notación. A la relación núcleo de una aplicación f también la denotaremos como \sim_f .

Notemos que la relación de equivalencia asociada a la proyección canónica $p : S \rightarrow S/R$ es precisamente R , i.e. $R_p = R$.

La siguiente observación es muy útil para definir aplicaciones desde un conjunto cociente.

Proposición 1.3.2. Sea R una relación de equivalencia sobre un conjunto S . Sea $f : S \rightarrow T$ una aplicación con la propiedad

$$\forall a, b \in S, \text{ si } aRb \text{ entonces se verifica que } f(a) = f(b).$$

Entonces hay una aplicación $\bar{f} : S/R \rightarrow T$ definida por la fórmula

$$\bar{f}(\bar{a}) = f(a), \forall \bar{a} \in S/R.$$

Se verifica que $Im(\bar{f}) = Im(f)$, por tanto que \bar{f} es sobreyectiva si y solo si f lo es. Además \bar{f} es inyectiva si y solo si se verifica que

$$\forall a, b \in S, \text{ si } f(a) = f(b), \text{ entonces } aRb.$$

DEMOSTRACIÓN. Hemos de comprobar que la correspondencia $\bar{a} \mapsto f(a)$ define una aplicación de S/R en T . La primera condición de aplicación es clara, pues $\forall \bar{a} \in S/R$ tenemos que $(\bar{a}, f(a)) \in f$, esto es, todo elemento tiene asignada una imagen. Para ver la segunda, esto es que cada elemento tiene asignada una única imagen, supongamos que $(\bar{a}, f(a)), (\bar{b}, f(b)) \in S/R$, y que $\bar{a} = \bar{b}$. Entonces aRb y, por hipótesis, $f(a) = f(b)$. Luego, efectivamente, tenemos una aplicación bien definida.

La afirmación $Im(\bar{f}) = Im(f)$, y su consecuencia sobre la sobreyectividad, es inmediata. Para estudiar la inyectividad de \bar{f} , notemos que $\bar{f}(\bar{a}) = \bar{f}(\bar{b}) \Leftrightarrow f(a) = f(b)$. Por tanto, \bar{f} será inyectiva si y solo si $f(a) = f(b) \Rightarrow \bar{a} = \bar{b}$ o, equivalentemente, $f(a) = f(b) \Rightarrow aRb$. \square

La aplicación $\bar{f} : S/R \rightarrow T$ es llamada la *inducida por f en el cociente*. Esta asigna a cada clase de equivalencia el valor que f asigna a cualquiera de sus representantes lo que, lógicamente, explica la condición de que f sea constante sobre elementos relacionados.

EJEMPLO. Consideremos $[0, 1] \subseteq \mathbb{R}$, el intervalo cerrado de la recta real formado por los números t tales que $0 \leq t \leq 1$. Definamos en él la relación de equivalencia R por la que identificamos los puntos 0 y 1, y solo estos. Más precisamente, decimos que

$$tRu \Leftrightarrow \begin{cases} \text{si } t, u \in \{0, 1\} \\ t = u \text{ en otro caso} \end{cases}$$

De manera que el conjunto cociente $[0, 1]/R$ consiste del bloque $\bar{0} = \bar{1} = \{0, 1\}$ y de los bloques unitarios $\bar{t} = \{t\}$ con $0 < t < 1$.

Consideremos ahora la aplicación $f : [0, 1] \rightarrow C_1$, donde $C_1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ es la circunferencia del plano real con radio 1 y centrada en el origen, definida por

$$f(t) = (\cos(2\pi t), \sin(2\pi t)), \quad 0 \leq t \leq 1.$$

Puesto que f es sobreyectiva y $f(t) = f(u) \Leftrightarrow tRu$, tenemos una biyección inducida

$$[0, 1]/R \cong C_1$$

que permite pensar a la circunferencia como el resultado de identificar los extremos del intervalo $[0, 1]$.

Como consecuencia inmediata de la Proposición 1.3.2 tenemos el siguiente

Teorema 1.3.3 (Descomposición canónica de una aplicación.). *Dada una aplicación $f : S \rightarrow T$ existe un isomorfismo $b : S/R_f \xrightarrow{\cong} Im(f)$ que hace conmutar el siguiente diagrama:*

$$\begin{array}{ccc} S & \xrightarrow{f} & T \\ p \downarrow & & \uparrow i \\ S/R_f & \xrightarrow[b]{\cong} & Im(f) \end{array}$$

donde p es la proyección canónica e i es la inclusión.

Demostración. Ya que, por definición $xR_f y \Leftrightarrow f(x) = f(y)$, la Proposición 1.3.2 nos permite definir $\bar{f} : S/R_f \rightarrow T$ como $\bar{f}(\bar{x}) = f(x)$ que además será inyectiva y cumple $f p(x) = f(x)$. Definimos entonces $b : S/R_f \rightarrow \text{Im}(f)$ como $b(\bar{x}) = \bar{f}(\bar{x}) = f(x)$ y tenemos el teorema. ■

EJERCICIOS

1. Sea $\mathbb{N} = \{0, 1, 2, \dots\}$ el conjunto de los números naturales, Sobre $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ definimos $(a, b) \sim (c, d)$ si $a + d = b + c$.
 - (a) Verificar que \sim es una relación de equivalencia.
 - (b) Sea $f : \mathbb{N}^2 \rightarrow \mathbb{Z}$ la aplicación definida por $f(a, b) = a - b$. Verificar que f induce una biyección $\mathbb{N}^2 / \sim \cong \mathbb{Z}$.
2. ¿Qué está mal en la siguiente demostración de que toda relación R sobre S que es simétrica y transitiva es reflexiva? Para $a, b \in S$, aRb , implica bRa (por simetría) y entonces (por transitividad) aRa .
3. Sea $f : S \rightarrow T$ una aplicación. Probar que, si f es sobreyectiva, induce una biyección $S/R_f \cong T$.
4. Sea $Y \subseteq X$ un subconjunto. Sea $f : \mathcal{P}(X) \rightarrow \mathcal{P}(Y)$ la aplicación tal que $f(A) = A \cap Y$, para cada $A \in \mathcal{P}(X)$.
 - (a) Probar que f es una sobreyección.
 - (b) Describir la relación R_f , núcleo de f .
 - (c) Probar que f induce una biyección $\mathcal{P}(X)/R_f \cong \mathcal{P}(Y)$.
5. Sea R una relación de equivalencia sobre el conjunto S . La aplicación $p : S \rightarrow S/R$ definida por $p(a) = \bar{a}$ es llamada la *proyección canónica* de S sobre el cociente ¿Qué relación hay entre R y R_p ?
6. Un subconjunto $P \subseteq \mathcal{P}(S)$, recordar, es llamado una *partición del conjunto* S si
 - (a) $\forall A \in P, A \neq \emptyset$.
 - (b) $\bigcup_{A \in P} A = S$.
 - (c) Para cualesquiera $A, B \in P, A \neq B$, se verifica que $A \cap B = \emptyset$.

Así, por ejemplo, el conjunto cociente S/R , para R una relación de equivalencia sobre S , es una partición.

Sea P una partición de S . Definimos la aplicación $p : S \rightarrow P$ por $p(a) = A$ si $a \in A$. ¿Qué relación hay entre P y S/R_p ?