

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

1.2 El conjunto producto cartesiano. Aplicaciones

Si S y T son conjuntos, su *producto cartesiano*, denotado $S \times T$, es el conjunto de todos los pares ordenados (x, y) con $x \in S$ e $y \in T$:

$$S \times T = \{(x, y) \mid x \in S, y \in T\}.$$

En este conjunto, los elementos (x, y) y (x', y') son considerados iguales si y solo si $x = x'$ e $y = y'$. Así, si $|S| = m$ y $|T| = n$, entonces $|S \times T| = mn = |S| |T|$. Los conjuntos S y T no tienen que ser distintos. Cuando $S = T$, escribimos también S^2 en lugar de $S \times S$.

Más generalmente, desde n conjuntos dados listados en un cierto orden, S_1, \dots, S_n , podemos formar el producto

$$S_1 \times S_2 \times \cdots \times S_n = \prod_{i=1}^n S_i = \{(x_1, x_2, \dots, x_n) \mid x_i \in S_i \forall i = 1, \dots, n\};$$

cuando $S_1 = S_2 = \cdots = S_n = S$ uno también escribe S^n en lugar de $S_1 \times S_2 \times \cdots \times S_n$.

Definición 1.2.1. Una “aplicación” es una terna de datos (S, T, f) , donde S es un conjunto, llamado el “dominio” de la aplicación, T es otro conjunto, llamado el “rango” de la aplicación, y $f \subseteq S \times T$ es un subconjunto del producto cartesiano, llamado su “grafo”, tal que las siguientes dos propiedades se verifican.

1. Para cualquier $x \in S$ existe un $y \in T$ tal que $(x, y) \in f$.
2. Si $(x, y), (x', y') \in f$, entonces $x = x' \Rightarrow y = y'$.

Dos aplicaciones son consideradas iguales si y solo si tienen el mismo dominio, el mismo rango y los mismos grafos.

La notación usual para una tal aplicación es escribir $f : S \rightarrow T$ o $S \xrightarrow{f} T$, y uno se refiere a ella como la *aplicación f del conjunto S en el conjunto T* . Las condiciones anteriores establecen que para cualquier elemento x del dominio hay un único elemento y del rango tal que (x, y) pertenece al grafo. La notación usual para ese elemento es $f(x)$, al que uno se refiere como la *imagen de x por f* , o *el elemento de T que corresponde a x por f* .

Para conocer una aplicación $f : S \rightarrow T$ es suficiente especificar la imagen $f(x)$ en T de cada elemento x de S . Usualmente, esto se hace proponiendo una fórmula que determina, para cada $x \in S$, su imagen $f(x) \in T$. Pero hay que ser cuidadoso en esto: Es necesario garantizarse que cada elemento de S tiene “bien definida su imagen” $f(x)$, esto es, que cada elemento S tiene una imagen y solo una.

EJEMPLOS.

1. Sea $\mathbb{N} = \{0, 1, 2, \dots\}$ el conjunto de los números naturales. No existe una aplicación $f : \mathbb{N} \rightarrow \mathbb{N}$ tal que la imagen de cada natural x venga dada por la fórmula $f(x) = x - 1$, pues el 0 no tiene asignado imagen. Esa fórmula, sin embargo si define una aplicación $f : \mathbb{Z} \rightarrow \mathbb{Z}$.
2. No existe una aplicación $f : \mathbb{N} \rightarrow \mathbb{N}$ tal que la imagen $f(x)$ de cada natural x venga dada por la fórmula

$$f(x) = \begin{cases} x & \text{si } x \text{ no es múltiplo de 2 ni de 3} \\ x/2 & \text{si } x \text{ es un múltiplo de 2,} \\ x/3 & \text{si } x \text{ es un múltiplo de 3,} \end{cases}$$

pues hay naturales que corresponden a más de uno (es decir, con más de una imagen): $f(6) = 6/2 = 3$ y $f(6) = 6/3 = 2$. Esto es, los elementos $(6, 2)$ y $(6, 3)$ pertenecerían al grafo!.

3. Hay una aplicación $+: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ tal que $(m, n) \mapsto m + n$.
4. La correspondencia $x \mapsto f(x) = \frac{x^2+1}{x-1}$ define una aplicación $f: (0, 1) \rightarrow \mathbb{R}$, pero no una aplicación $f: [0, 1] \rightarrow \mathbb{R}$.

Usualmente, el subconjunto de todas las imágenes de una aplicación $f: S \rightarrow T$

$$Im(f) = \{y \in T \mid y = f(x) \text{ para algún } x \in S\} = \{f(x) \mid x \in S\}$$

es llamado la *imagen* de la aplicación.

La aplicación es llamada *sobreyectiva* si $Im(f) = T$, esto es, cuando todo elemento del rango es imagen de algún elemento del dominio.

La aplicación es llamada *inyectiva* si distintos elementos del dominio tienen distintas imágenes, esto es, si $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.

Si la aplicación f es simultáneamente inyectiva y sobreyectiva, entonces es llamada una *biyección*. Así, una aplicación $f: S \rightarrow T$ es una biyección cuando y solo cuando $\forall y \in T, \exists! x \in S \mid f(x) = y$. Si es posible establecer una biyección $f: S \rightarrow T$, se dice que S es biyectivo con T , y se expresa escribiendo $S \cong T$.

EJEMPLOS. Sea $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ el conjunto de los números enteros.

1. La aplicación $f: \mathbb{Z} \rightarrow \mathbb{Z}$ tal que $f(x) = x^2$, no es inyectiva ni sobreyectiva.
2. La aplicación $f: \mathbb{Z} \rightarrow \mathbb{Z}$ tal que $f(x) = 2x$, es inyectiva pero no sobreyectiva.
3. La aplicación $f: \mathbb{Z} \rightarrow \mathbb{Z}$ tal que $f(x) = x + 2$ es biyectiva.
4. Denotemos por $\mathbf{2} = \{0, 1\}$ al conjunto con dos elementos, y sea $\mathbf{2}^S$ al conjunto de todas las aplicaciones $f: S \rightarrow \mathbf{2}$. Si $A \in \mathcal{P}(S)$, se define su *aplicación característica* $\chi_A: S \rightarrow \mathbf{2}$ por

$$\chi_A(x) = \begin{cases} 1 & \text{si } x \in A, \\ 0 & \text{si } x \notin A. \end{cases}$$

La correspondencia $A \mapsto \chi_A$, nos define una aplicación biyectiva $\chi: \mathcal{P}(S) \cong \mathbf{2}^S$: Si $\chi_A = \chi_B$, entonces $A = \{x \in S \mid \chi_A(x) = 1\} = \{x \in S \mid \chi_B(x) = 1\} = B$, por tanto χ es inyectiva. Para ver que es sobreyectiva, supongamos $f: S \rightarrow \mathbf{2}$ cualquier aplicación. Sea $A = \{x \in S \mid f(x) = 1\}$. Entonces $\chi_A = f$, pues dado cualquier $x \in S$, si $f(x) = 1$ entonces $x \in A$ y $\chi_A(x) = 1$, y si $f(x) = 0$, entonces $x \notin A$ y también $\chi_A(x) = 0$.

Sean $S \xrightarrow{f} T$ y $T \xrightarrow{g} U$ dos aplicaciones, donde el rango de f coincide con el dominio de g , de manera que se pueden escribir consecutivamente como $S \xrightarrow{f} T \xrightarrow{g} U$. Se define su *composición* como la aplicación $S \xrightarrow{gf} U$, cuyo dominio es S , el rango es U y, para cualquier $x \in S$,

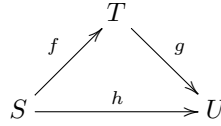
$$(gf)(x) = g(f(x)).$$

La composición de aplicaciones satisface la *ley asociativa*: Si $S \xrightarrow{f} T \xrightarrow{g} U \xrightarrow{h} V$ son aplicaciones, entonces $h(gf) = (hg)f$. En efecto, ambas tienen el mismo dominio S , el mismo rango T y, para cualquier $x \in S$,

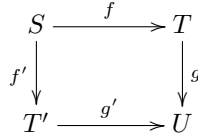
$$\begin{aligned}(h(gf))(x) &= h((gf)(x)) = h(g(h(x))), \\ ((hg)f)(x) &= (hg)(f(x)) = h(g(f(x))),\end{aligned}$$

por tanto que son la misma aplicación. Es usual escribir simplemente hgf para designarla.

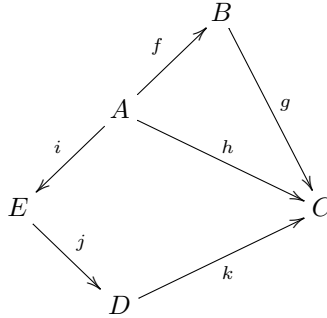
Si $S \xrightarrow{f} T \xrightarrow{g} U$ son aplicaciones componibles y $h : S \rightarrow U$ es una aplicación, es usual indicar la igualdad $h = gf$ diciendo que el triángulo



es conmutativo, o que $h \neq gf$, diciendo que el triángulo no es conmutativo. Análogamente, un rectángulo de aplicaciones



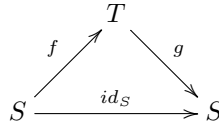
es conmutativo, si $gf = g'f'$. En general, la conmutatividad de un diagrama de aplicaciones, cuando tiene sentido, significa que las aplicaciones obtenidas por composición desde un vértice inicial hasta uno terminal según las diferentes rutas son la mismas. Por ejemplo, la conmutatividad del diagrama



significa que $gf = h = kji$.

Para cualquier conjunto S , se define la aplicación *identidad* en S , $id_S : S \rightarrow S$ (o 1_S , o 1 si S es claro por el contexto) como la aplicación tal que $id_S(x) = x$, para todo $x \in S$. Es la aplicación de S en sí mismo cuyo grafo es la *diagonal* $\Delta = \{(x, x) \mid x \in S\}$. Si $f : S \rightarrow T$ es cualquier aplicación, uno verifica inmediatamente que $id_T f = f = f id_S$.

Lema 1.2.2. Si $S \xrightarrow{f} T$ y $T \xrightarrow{g} S$ son dos aplicaciones tal que $gf = id_S$, es decir, tal que el triángulo



conmuta, entonces f es inyectiva y g es sobreyectiva.

DEMOSTRACIÓN. Supongamos que $f(x) = f(y)$, para ciertos $x, y \in S$. Entonces $x = id_S(x) = gf(x) = gf(y) = id_S(y) = y$. Así que f es inyectiva. Dado cualquier $x \in S$, como $x = id_S(x) = gf(x) = g(f(x))$, es $x \in Im(g)$, luego g es sobreyectiva. \square

Supongamos ahora que $S \xrightarrow{f} T$ tal que existe una otra $T \xrightarrow{g} S$ tal que $gf = id_S$ y $fg = id_T$. Entonces f es inyectiva y sobreyectiva, por el lema, y por tanto una biyección. Recíprocamente, si f es biyectiva, entonces podemos encontrar una aplicación $g : T \rightarrow S$ tal que $gf = id_S$ y $fg = id_T$: Para cada $y \in T$, sea $g(y) \in S$ el único elemento de S tal que $f(g(y)) = y$. Esto define una tal aplicación g , claramente verificando que $fg = id_T$. Además, para cualquier $x \in S$, como obviamente $x \mapsto f(x)$, es $g(f(x)) = x$, así que $gf = id_S$. Esto prueba que

Proposición 1.2.3. *Una aplicación $f : S \rightarrow T$ es biyectiva si y solo si existe una aplicación $g : T \rightarrow S$ tal que $gf = id_S$ y $fg = id_T$.*

Para $f : S \rightarrow T$ una biyección, solo existe una aplicación $g : T \rightarrow S$ tal que $gf = id_S$ y $fg = id_T$: Si $g' : T \rightarrow S$ es otra con $g'f = id_S$ y $fg' = id_T$, entonces

$$g' = g'id_T = g'fg = id_Sg = g.$$

Esa única g es llamada la *inversa* de f y es denotada por f^{-1} . Si $f : S \rightarrow T$ es biyectiva, entonces su inversa $f^{-1} : T \rightarrow S$ es la única aplicación tal que $f^{-1}f = id_S$ y $ff^{-1} = id_T$. Observar que f^{-1} también es biyectiva y $(f^{-1})^{-1} = f$.

Como una primera aplicación del criterio de biyectividad anterior, podemos dar una demostración del hecho (bastante obvio) de que la composición de dos aplicaciones biyectivas es biyectiva: Sean $f : S \rightarrow T$ y $g : T \rightarrow U$ biyecciones, y consideremos su composición $gf : S \rightarrow U$. Entonces, tenemos sus inversas $g^{-1} : U \rightarrow T$ y $f^{-1} : T \rightarrow S$, y su compuesta $f^{-1}g^{-1} : U \rightarrow S$. Además

$$\begin{aligned}(f^{-1}g^{-1})(gf) &= f^{-1}(g^{-1}(gf)) = f^{-1}((g^{-1}g)f) = f^{-1}(id_Tf) = f^{-1}f = id_S, \\ (gf)(f^{-1}g^{-1}) &= g(f(f^{-1}g^{-1})) = g((ff^{-1})g^{-1}) = g(id_Tg^{-1}) = gg^{-1} = id_U.\end{aligned}$$

Así que gf es biyectiva, con inversa

$$(gf)^{-1} = g^{-1}f^{-1}.$$

La siguiente observación para conjuntos finitos es útil en muchas ocasiones

Lema 1.2.4. *Sea S un conjunto finito. Las siguientes propiedades para $f : S \rightarrow S$ son equivalentes:*

1. f es biyectiva.
2. f es inyectiva.
3. f es sobreyectiva.

DEMOSTRACIÓN. Supongamos que $|S| = n$. Si f es inyectiva, entonces $|Im(f)| = n$, luego $Im(f) = S$ y f es sobreyectiva. Recíprocamente, si f no es inyectiva, entonces $|Im(f)| < n$, luego f no es sobreyectiva. \square

1.2.1 Imágenes directas e inversas

Toda aplicación $f : S \rightarrow T$ determina otras

$$f_* : \mathcal{P}(S) \rightarrow \mathcal{P}(T), \quad f^* : \mathcal{P}(T) \rightarrow \mathcal{P}(S),$$

llamadas las aplicaciones *imagen* e *imagen inversa* por f , respectivamente, que están definidas, para cada $A \subseteq S$ y $X \subseteq T$, por

$$f_*(A) = \{f(a) \mid a \in A\}, \quad f^*(X) = \{a \in S \mid f(a) \in X\}.$$

Dejaremos como ejercicios las siguientes propiedades de las imágenes directas o inversas. Dada una aplicación $f : S \rightarrow T$, $A, B \subseteq S$ subconjuntos de S y $X, Y \subseteq T$ son subconjuntos de T .

1. Probar que $f^*(X \cup Y) = f^*(X) \cup f^*(Y)$ y $f_*(A \cup B) = f_*(A) \cup f_*(B)$.
2. Probar que $f^*(X \cap Y) = f^*(X) \cap f^*(Y)$ y $f_*(A \cap B) \subseteq f_*(A) \cap f_*(B)$.
3. Demostrar que si f es inyectiva, entonces $f_*(A \cap B) = f_*(A) \cap f_*(B)$.
4. Demostrar con el siguiente ejemplo que, en general, $f_*(A \cap B) \neq f_*(A) \cap f_*(B)$: Sea $f = |\cdot| : \mathbb{R} \rightarrow \mathbb{R}$ la aplicación “valor absoluto”, $A = (0, 1)$ y $B = (-1, 0)$.
5. $f_*(f^*(X)) \subseteq X$, y se da la igualdad si f es sobreyectiva.
6. $A \subseteq f^*(f_*(A))$, y se da la igualdad si f es inyectiva.
7. Probar que, si f es una biyección entonces las aplicaciones $f_* : \mathcal{P}(S) \rightarrow \mathcal{P}(T)$ y $f^* : \mathcal{P}(T) \rightarrow \mathcal{P}(S)$ son biyecciones e inversas una de la otra.

EJERCICIOS

1. Sean $f : S \rightarrow T$ y $g : T \rightarrow U$ aplicaciones.
 - (a) Probar que si ambas son inyectivas, entonces su composición $gf : S \rightarrow U$ es también inyectiva.
 - (b) Probar que si ambas son sobreyectivas, entonces su composición $gf : S \rightarrow U$ es también sobreyectiva.
 - (c) Si su compuesta $gf : S \rightarrow U$ es inyectiva o sobreyectiva ¿qué podemos decir sobre f y g ?
2. Sea $f : S \rightarrow T$ una aplicación.
 - (a) Probar que f es inyectiva si y solo si tiene una *inversa por la izquierda*, es decir, existe una aplicación $g : T \rightarrow S$ tal que $gf = id_S$.
 - (b) Dar un ejemplo de una aplicación inyectiva con dos diferentes inversas por la izquierda.
 - (c) Probar que f es sobreyectiva si y solo si tiene una *inversa por la derecha*, es decir, existe una aplicación $g : T \rightarrow S$ tal que $fg = id_T$.
 - (d) Dar un ejemplo de una aplicación sobreyectiva con dos diferentes inversas por la derecha.

3. En los siguientes ejercicios S y T son dos conjuntos arbitrarios, A, A' son subconjuntos de S y B, B' son subconjuntos de T .
- (a)
 - i. Probar $A \times B$ es un subconjunto de $S \times T$.
 - ii. Probar, con el siguiente ejemplo, que no todo subconjunto X de $S \times T$ es de la forma $X = A \times B$: $S = T = \{0, 1\}$, $X = \{(0, 0), (1, 1)\} \subseteq S \times T$.
 - (b) Probar las siguientes igualdades:
 - i. $c(A \times B) = c(A) \times T \cup S \times c(B)$.
 - ii. $(A \cup A') \times B = (A \times B) \cup (A' \times B)$.
 - iii. $(A \cap A') \times B = (A \times B) \cap (A' \times B)$.
 - iv. $(A \cap A') \times (B \cap B') = (A \times B) \cap (A' \times B')$.
 - v. $(A \cup A') \times (B \cup B') = (A \times B) \cup (A' \times B) \cup (A \times B') \cup (A' \times B')$.
4. Se consideran los subconjuntos de \mathbb{R} , $S = [-1, 1]$, $T = [-3, 4]$. Describir en dibujo los siguientes recintos de \mathbb{R}^2 : $S \times T$, $T \times S$, $(S \times T) \cup (T \times S)$, $(S \times T) \cap (T \times S)$, $(S \times T) - (T \times S)$, $(T \times S) - (S \times T)$.