CYN. CAPÍTULO V: RELACIONES DE EQUIVALENCIA PRIMER CURSO DE MATEMÁTICAS, 2008-09

José García-Cuerva

Universidad Autónoma de Madrid

1 de octubre de 2015

1. RELACIONES DE EQUIVALENCIA
   - Clases de equivalencia.
   - Conjunto cociente
   - Grupo cociente
   - Ideales. Anillo cociente

2. TEORÍA AXIOMÁTICA DE CONJUNTOS

3. CARDINALES
   - Conjuntos infinitos
   - Conjuntos numerables
   - Conjuntos no numerables
   - Comparación de cardinales
   - El teorema de Cantor-Schröder-Bernstein
   - Aritmética de cardinales

Relaciones de equivalencia

Definición

Una relación de equivalencia en el conjunto X es una relación binaria en X que sea REFLEXIVA, SIMÉTRICA y TRANSITIVA.

Ejemplos:

1. Sea $X \xrightarrow{f} Y$. Definimos, para $x, x' \in X$, $x\mathcal{R}_f x' \Leftrightarrow f(x) = f(x')$. Claramente, $\mathcal{R}_f$ es una relación de equivalencia en X.
2. Si $X = \biguplus_{\alpha \in J} A_\alpha$, definimos, para $x, x' \in X$, $x\mathcal{R}x' \Leftrightarrow \exists \alpha \in J \ni x, x' \in A_\alpha$. $\mathcal{R}$ es rel. de equivalencia en X.
3. Sea $X \xrightarrow{f} Y$ y sea $\mathcal{R}$ una relación de equivalencia en Y. Si definimos en $x\mathcal{S}x', x, x' \in X, \Leftrightarrow f(x)\mathcal{R}f(x')$, obtenemos una relación de equivalencia $\mathcal{S}$ en X, a la que se llama imagen recíproca de $\mathcal{R}$ mediante f. Se escribe $\mathcal{S} = f^\star(\mathcal{R})$. El primer ejemplo es un caso particular de éste: $\mathcal{R}_f = f^\star(\Delta)$, siendo $\Delta = \{(y, y) : y \in Y\}$, la relación de igualdad, mínima relación de equivalencia o relación de equivalencia trivial.

Observaciones:

- El primer ejemplo es un caso particular del segundo.

  En efecto: Dada $X \xrightarrow{f} Y$, tenemos una descomposición, clasificación o partición $X = \biguplus_{y \in Y} f^{-1}(y)$, que, según el ejemplo 2, nos da una relación de equivalencia $x \mathcal{R} x' \Leftrightarrow \exists y \in Y \ni x, x' \in f^{-1}(y)$; pero esto es lo mismo que decir que $x \mathcal{R} x' \Leftrightarrow f(x) = f(x')$, de forma que $\mathcal{R} = \mathcal{R}_f$. Pero

- También el segundo ejemplo es un caso particular del primero. En efecto, si tenemos una descomposición, clasificación o partición $X = \biguplus_{\alpha \in J} A_\alpha$, consideramos $X \xrightarrow{f} J$ definida como $f(x) = \alpha$ si $x \in A_\alpha$. Entonces $\mathcal{R}_f$ es, precisamente, la relación asociada a la partición en el ejemplo 2.

Clases de equivalencia.

Definición

Sea $\mathcal{R}$ una relación de equivalencia en X. Para cada $x \in X$, se llama clase de equivalencia de x al conjunto $\mathcal{R}(x) = \{x' \in X : x\mathcal{R}x'\}$.

Proposición

Las clases de equivalencia dadas por la relación de equivalencia $\mathcal{R}$ en X forman una partición, clasificación o descomposición de X, es decir:$\forall x_1, x_2 \in X, \mathcal{R}(x_1) = \mathcal{R}(x_2) \vee \mathcal{R}(x_1) \cap \mathcal{R}(x_2) = \emptyset$.

Demostración

Si $\mathcal{R}(x_1) \cap \mathcal{R}(x_2) \neq \emptyset$, existirá $x' \in X \ni x_1\mathcal{R}x' \wedge x'\mathcal{R}x_2$; pero, entonces, $x_1\mathcal{R}x_2$ y, por lo tanto, $\mathcal{R}(x_1) = \mathcal{R}(x_2)$.

Otra forma de expresar lo que acbamos de ver es decir que cualquier relación de equivalencia queda comprendida con el ejemplo 2.

Conjunto cociente

Como el ejemplo 1 y el ejemplo 2 no son más que dos formas de ver la misma cosa, también se podrá ver cualquier relación de equivalencia como un caso particular del ejemplo 1. Esto se hace a través del conjunto cociente que es un concepto básico que aparece en todas las ramas de las Matemáticas.

Definición

Si $\mathcal{R}$ es una relación de equivalencia en X,

- Se llama conjunto cociente de X por $\mathcal{R}$ y se denota como $X/\mathcal{R}$ al conjunto de las clases de equivalencia, es decir: $X/\mathcal{R} = \{\mathcal{R}(x) : \ x \in X\}$.
- La aplicación $X \stackrel{\pi}{\to} X/\mathcal{R}$ definida por $\pi(x) = \mathcal{R}(x)$ es una aplicación sobreyectiva que se conoce como proyección natural.

Desde luego la relación de equivalencia asociada a π según el ejemplo 1 es $\mathcal{R}$.

Acción de un grupo sobre un conjunto

Definición

- Una acción por la izquierda del grupo $(G, \circ)$ sobre el conjunto $X \neq \emptyset$ es una aplicación $G \times X \to X$ que asigna a cada $(g, x) \in G \times X$ un elemento de X al que llamaremos gx, sujeto a las condiciones
  - I) $ex = x \forall x \in X$ y
  - II) $\forall g, h \in G$ y $\forall x \in X,\ h(gx) = (h \circ g)x$.
- Una acción por la derecha del grupo $(G, \circ)$ sobre el conjunto $X \neq \emptyset$ es una aplicación $X \times G \to X$ que asigna a cada $(x, g) \in X \times G$ un elemento de X al que llamaremos xg, sujeto a las condiciones
  - I') $xe = x \forall x \in X$ y
  - II') $\forall g, h \in G$ y $\forall x \in X,\ (xg)h = x(g \circ h)$.

Proposición

Si $G \times X \to X$ es una acción por la izquierda del grupo G sobre el conjunto X, la relación $x\mathcal{R}y \Leftrightarrow \exists g \in G \ni gx = y$ es una relación de equivalencia en X para la que el conjunto cociente $X/\mathcal{R}$ está formado por las órbitas $Gx = \{gx : g \in G\}$, para $x \in X$.

Demostración

- $\mathcal{R}$ es reflexiva, pues $\forall x \in X,\ ex = x$.
- $\mathcal{R}$ es simétrica, ya que
  $x\mathcal{R}y \Rightarrow \exists g \in G \ni gx = y \Rightarrow x = g^{-1}y \Rightarrow y\mathcal{R}x$.
- Y, finalmente, $\mathcal{R}$ es transitiva: $x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow gx = y \wedge hy = z \Rightarrow (h \circ g)x = h(gx) = hy = z \Rightarrow x\mathcal{R}z$.

Por otro lado
$\mathcal{R}(x) = \{y \in X : x\mathcal{R}y\} = \{y \in X : \exists g \in G : gx = y\} = Gx$.

Del mismo modo se demuestra

PROPOSICIÓN

Si $X \times G \to X$ es una acción por la derecha del grupo G sobre el conjunto X, la relación $x \mathcal{S} y \Leftrightarrow \exists g \in G \ni xg = y$ es una relación de equivalencia en X para la que el conjunto cociente $X/\mathcal{S}$ está formado por las órbitas $xG = \{xg : \ g \in G\}$, para $x \in X$.

EJEMPLO:

- Si H es un subgrupo de G, H actúa sobre G por la izquierda de la manera natural $(h, g) \in H \times G \mapsto hg = h \circ g$. La correspondiente relación de equivalencia es
  $g \mathcal{R}_H g' \Leftrightarrow \exists h \in H \ni hg = g' \Leftrightarrow g \circ g'^{-1} \in H$. Las clases de equivalencia son las órbitas Hg, $g \in G$.
- Pero también H actúa sobre G por la derecha, de la forma natural $(g, h) \in G \times H \mapsto gh = g \circ h$. La correspondiente relación de equivalencia es ahora
  $g \mathcal{S}_H g' \Leftrightarrow \exists h \in H \ni gh = g' \Leftrightarrow g^{-1} \circ g' \in H$. Y las clases de equivalencia son, ahora, las órbitas gH, $g \in G$.

Si G es abeliano, $\mathcal{R}_H$ y $\mathcal{S}_H$ coinciden. Un ejemplo importante para $G = \mathbb{Z}$: es la relación de congruencia módulo un cierto $n \in \mathbb{N},\ n \geq 2$.

DEFINICIÓN

Sea $n \in \mathbb{N},\ n \geq 2$. Se dice que los enteros a y b son congruentes módulo n, y se escribe $a \equiv b (\mathrm{mod}.n)$ si $n|a-b$.

PROPOSICIÓN

La relación de congruencia módulo n es una relación de equivalencia para la que las clases de equivalencia son $a + \mathbb{Z}n,\ a \in \mathbb{Z}$. El conjunto cociente, al que llamaremos $\mathbb{Z}_n$ está formado por n elementos, que se corresponden con los n restos que puede dar la división de un número entero por n. Se suele escribir $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$, donde $\overline{j} = \{j + \mathbb{Z}n\},\ 0 \leq j < n$.

Demostración

Observamos que el subconjunto $H = \mathbb{Z}n = \{xn : \ x \in \mathbb{Z}\} \subset \mathbb{Z}$ es un subgrupo de $\mathbb{Z}$ y que la relación $\mathcal{R}_H$ es, precisamente, la relación de congruencia módulo n. Una clase de equivalencia será $a + \mathbb{Z}n$ y todos sus miembros dan el mismo resto al dividirlos por n. Así, hay sólo n clases de equivalencia.

Y si G no es abeliano ¿es posible que sea $\mathcal{R}_H = \mathcal{S}_H$?

Proposición

Sea G un grupo y sea H un subgrupo de G. Las siguientes condiciones son equivalentes

- $\mathcal{R}_H = \mathcal{S}_H$
- $\forall g \in G, \ gH = Hg$.
- $\forall g \in G, gHg^{-1} = H$.
- $\forall g \in G, gHg^{-1} \subset H$.

DEFINICIÓN

Un subgrupo H del grupo G que cumple alguna, y por lo tanto, todas las propiedades de la proposición anterior se llama subgrupo normal. Escribiremos, en ese caso $H \lhd G$.

EJEMPLO: Sea $G = \{T_{a,b} : \mathbb{R} \to \mathbb{R}, a, b \in \mathbb{R}, a \neq 0 \ni T_{a,b}(x) = ax + b\}$. Es fácil ver que G es un grupo no conmutativo con la operación de composición de aplicaciones. En efecto
$T_{c,d}T_{a,b}x = T_{c,d}(ax+b) = c(ax+b)+d = cax+cb+d = T_{ca,cb+d}(x)$.
Y $T_{a,b}T_{c,d} = T_{ac,ad+b}$. El elemento neutro es la identidad $\mathrm{id}_{\mathbb{R}} = T_{1,0}$. Y el elemento inverso de $T_{a,b}$ es $T_{a^{-1},-a^{-1}b}$. Se ve, entonces que el subgrupo $H = \{T_{1,b} : \ b \in \mathbb{R}\}$ de las traslaciones, es un subgrupo normal de G : $T_{c,d}^{-1} \circ T_{1,b} \circ T_{c,d} = T_{c^{-1},-c^{-1}d} \circ T_{c,d+b} = T_{1,c^{-1}b} \in H$. Sin embargo, $K = \{T_{a,0} : \ a \in \mathbb{R} \setminus \{0\}\}$ es un subgrupo ($T_{c,0} \circ T_{a,0} = T_{ca,0}$); pero no es normal: $T_{c,d}^{-1} \circ T_{a,0} \circ T_{c,d} = T_{a,c^{-1}ad-c^{-1}d}$.

Morfismos de grupos

Definición

Si $(G_1, \star)$ y $(G_2, \circ)$ son grupos, una aplicación $\varphi : G_1 \to G_2$ se llama morfismo de grupos si $\forall x, y \in G_1,\ \varphi(x \star y) = \varphi(x) \circ \varphi(y)$.

Proposición

- Si $\varphi : G_1 \to G_2$ es morfismo de grupos y llamamos e_1 al elemento neutro de G_1 y e_2 al elemento neutro de G_2, resulta que $\varphi(e_1) = e_2$.
- También $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Demostración

- $\varphi(e_1) = \varphi(e_1 \star e_1) = \varphi(e_1) \circ \varphi(e_1)$. Por tanto $e_2 = \varphi(e_1) \circ \varphi(e_1)^{-1} = \varphi(e_1) \circ \varphi(e_1) \circ \varphi(e_1)^{-1} = \varphi(e_1)$.
- $\varphi(x) \circ \varphi(x^{-1}) = \varphi(x \star x^{-1}) = \varphi(e_1) = e_2$.

Ejemplos

- En general, en un grupo $(xy)^{-1} = y^{-1}x^{-1}$, de modo que sólo si G es conmutativo podemos afirmar que la aplicación $x \mapsto x^{-1}$ es un morfismo de grupos.
- La aplicación $z \mapsto |z|$ es un morfismo del grupo $\mathbb{C} \setminus \{0\}$ con la multiplicación, en sí mismo.
- $x \mapsto e^x$ es un morfismo de $(\mathbb{R}, +)$ en $(\mathbb{R}_+, \cdot)$.
- En cualquier grupo G, dado $g \in G$ consideramos $\varphi_g : G \to G$ dada por $\varphi_g(x) = gxg^{-1}$. Resulta que φ_g es un morfismo de grupos que se llama conjugación por g.

Definición

Si $\varphi : G_1 \to G_2$ es un morfismo de grupos, se llama núcleo de φ al conjunto $\mathrm{nuc}(\varphi) = \{x \in G_1 : \ \varphi(x) = e_2\}$, donde e_2 es el elemento neutro de G_2.

PROPOSICIÓN

El núcleo de un morfismo de grupos $\varphi : G_1 \to G_2$ es un subgrupo normal de G_1.

DEMOSTRACIÓN

Hemos de ver que $\varphi(x) = \varphi(y) = e_2 \Rightarrow \varphi(xy^{-1}) = e_2$ y que, además, $\forall y \in G_1, \varphi(x) = e_2 \Rightarrow \varphi(yxy^{-1}) = e_2$. Ambas son inmediatas a partir de la definición de morfismo de grupos.

EJEMPLO: En el grupo $G = \{T_{a,b} : \mathbb{R} \to \mathbb{R}, a, b \in \mathbb{R}, a \neq 0 \ni T_{a,b}(x) = ax + b\}$, el subgrupo de las traslaciones $H = \{T_{1,b} : b \in \mathbb{R}\}$ es, precisamente, el núcleo del morfismo $T_{a,b} \mapsto a$ del grupo G en el grupo multiplicativo $\mathbb{R} \setminus \{0\}$.

Veremos más adelante que, recíprocamente, todo subgrupo normal es el núcleo de un morfismo de grupos. Esto requerirá construir, primero, el GRUPO COCIENTE

Paso al cociente de aplicaciones

Sean X un conjunto y $\mathcal{R}$ una relación de equivalencia en X. La proyección natural $X \xrightarrow{\pi} X/\mathcal{R}$ manda cada $x \in X$ a su clase de equivalencia $\pi(x) = \mathcal{R}(x)$. Supongamos una aplicación $X \xrightarrow{g} Y$. Nos preguntamos cuando es posible pasar al cociente la aplicación g. En otras palabras

¿Cuándo $\exists \tilde{g} : X/\mathcal{R} \to Y \ni \tilde{g} \circ \pi = g$?

Teorema

$\exists \tilde{g} \ni \tilde{g} \circ \pi = g \Leftrightarrow (\forall x, x' \in X,\ x\mathcal{R}x' \Rightarrow g(x) = g(x'))$

Demostración

- $\Rightarrow$ Si $\exists \tilde{g} \ni \tilde{g} \circ \pi = g$, será $x\mathcal{R}x' \Rightarrow \pi(x) = \pi(x') \Rightarrow g(x) = \tilde{g}(\pi(x)) = \tilde{g}(\pi(x')) = g(x')$.
- $\Leftarrow$ Basta definir $\tilde{g}(\mathcal{R}(x)) = g(x)$ y ver que, gracias a la hipótesis, g está bien definida, pues $\mathcal{R}(x) = \mathcal{R}(x') \Rightarrow g(x) = g(x')$.

EJEMPLO: Sea $f : \mathbb{Z} \to \mathbb{Z}_2$ la proyección canónica dada por $f(n) = \begin{cases} \overline{0} \text{ si } n \text{ es par} \\ \overline{1} \text{ si } n \text{ es impar} \end{cases}$. Y sea también $\pi : \mathbb{Z} \to \mathbb{Z}_4$ la correspondiente proyección canónica

Pregunta: ¿Será posible pasar f al cociente $\mathbb{Z}_4$? En otras palabras: ¿$\exists \tilde{f} : \mathbb{Z}_4 \to \mathbb{Z}_2 \ni \tilde{f} \circ \pi = f$?

La respuesta es afirmativa, ya que $\pi(n) = \pi(m) \Rightarrow n - m = 4k = 2 \cdot 2k \Rightarrow f(n) = f(m)$. Basta definir $\tilde{f}(j + 4\mathbb{Z}) = f(j) = j + 2\mathbb{Z}$.

Paso al cociente de operaciones

Sean X_1, X_2, X_3 conjuntos y sea $X_1 \times X_2 \xrightarrow{f} X_3$. Supongamos que, para cada $j = 1, 2, 3$, $\mathcal{R}_j$ es una relación de equivalencia en X_j y tenemos las proyecciones naturales $\pi_j : X_j \to X_j/\mathcal{R}_j$.

Nos preguntamos cómo tiene que ser f para que exista F que haga conmutativo el siguiente diagrama:

$$\begin{array}{ccc} X_1 \times X_2 & \xrightarrow{f} & X_3 \\ \downarrow{\scriptstyle \varphi=\pi_1\times\pi_2} & & \downarrow{\scriptstyle \pi_3} \\ X_1/\mathcal{R}_1 \times X_2/\mathcal{R}_2 & \xrightarrow{F} & X_3/\mathcal{R}_3 \end{array}$$

Si existe F, será $F(\mathcal{R}_1(x_1), \mathcal{R}_2(x_2)) = F(\varphi(x_1, x_2)) = \pi_3(f(x_1, x_2)) = \mathcal{R}_3(f(x_1, x_2))$. Así pues, para que exista F, es condición necesaria que se cumpla $(x_1 \mathcal{R}_1 x_1' \wedge x_2 \mathcal{R}_2 x_2') \Rightarrow f(x_1, x_2) \mathcal{R}_3 f(x_1', x_2')$. Es inmediato ver que la condición es también suficiente.

Grupo cociente

Como aplicación estudiemos cómo puede pasarse al cociente la operación de un grupo $(G, \star)$. Sea H un subgrupo y consideremos la relación $\mathcal{R}_H$, definida por $g\mathcal{R}_H g' \Leftrightarrow g \star g'^{-1} \in H$, que da lugar a las clases por la izquierda $Hg,\ g \in G$. La condición para poder pasar al cociente la operación del grupo es que $g_1\mathcal{R}_H g_1' \wedge g_2\mathcal{R}_H g_2' \Rightarrow g_1 \star g_2 \mathcal{R}_H g_1' \star g_2'$. En otras palabras, se necesita que $g_1 \star g_1'^{-1} \in H \wedge g_2 \star g_2'^{-1} \in H \Rightarrow g_1 \star g_2 \star (g_1' \star g_2')^{-1} \in H$. Como $g_1 \star g_2 \star (g_1' \star g_2')^{-1} = g_1 \star g_2 \star g_2'^{-1} \star g_1'^{-1} = (g_1 \star g_1'^{-1}) \star (g_1' \star (g_2 \star g_2'^{-1}) \star g_1'^{-1})$, vemos que basta que H sea NORMAL para poder pasar al cociente. En ese caso $\mathcal{R}_H = \mathcal{S}_H$ y $\forall g \in G$, $Hg = gH$. Escribiremos, simplemente G/H para el conjunto de las clases $Hg = gH$. La operación que resulta de pasar al cociente $(Hg_1, Hg_2) \mapsto H(g_1 \star g_2)$ convierte a G/H en un grupo al que llamaremos GRUPO COCIENTE. La proyección natural $G \overset{\pi_H}{\to} G/H$ es morfismo de grupos. Por ser sobreyectiva se le suele llamar EPIMORFISMO NATURAL. El núcleo de π_H es H. Así pues,

todo subgrupo normal es núcleo de un morfismo.

SUMA DE CONGRUENCIAS

EJEMPLO Si en el grupo aditivo $\mathbb{Z}$ consideramos el subgrupo $\mathbb{Z}n = \{kn : \ k \in \mathbb{Z}\}$ para algún $n \in \mathbb{Z}, n \geq 2$, el correspondiente grupo cociente es $\mathbb{Z}/\mathbb{Z}n = \mathbb{Z}_n$. La condición para pasar al cociente la suma es el hecho de que las congruencias pueden sumarse, es decir

$$(k \equiv k' (\mathrm{mod} n) \wedge j \equiv j' (\mathrm{mod} n)) \Rightarrow k + j \equiv k' + j' (\mathrm{mod} n).$$

Podemos, entonces, definir la suma en $\mathbb{Z}_n$ como $\overline{k} + \overline{j} = \overline{k + j}$ y obtenemos el siguiente diagrama conmutativo

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow{+} & \mathbb{Z} \\ \downarrow{\scriptstyle \varphi = \pi \times \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{Z}_n \times \mathbb{Z}_n & \xrightarrow{+} & \mathbb{Z}_n \end{array}$$

Sea G un grupo y sea H un subgrupo normal de G. Consideramos el epimorfismo natural $G \overset{\pi_H}{\to} G/H$. Si G' es otro grupo y $G \overset{f}{\to} G'$ es un morfismo de grupos, la condición necesaria y suficiente para que f se pueda factorizar a través de G/H, es decir, para que exista $\widetilde{f} : G/H \to G' \ni f = \widetilde{f} \circ \pi_H$ es que $x \star y^{-1} \in H \Rightarrow f(x) = f(y)$. Claramente, esta condición equivale a $H \subset \operatorname{nuc}(f)$. Si esta condición se cumple, basta definir $\widetilde{f}(xH) = f(x)$. Es inmediato que $\widetilde{f}$ es morfismo de grupos y que $\operatorname{nuc}(\widetilde{f}) = \{xH : f(x) = 0\} = \pi_H(\operatorname{nuc}(f)) = \operatorname{nuc}(f)/H$. En particular, si $H = \operatorname{nuc}(f)$, será $\operatorname{nuc}(\widetilde{f}) = 0$, de modo que $\widetilde{f}$ es un monomorfismo y un isomorfismo con el subgrupo $\operatorname{im}(f)$.
Destacamos que hemos obtenido el siguiente

Teorema de isomorfía de grupos

Cada morfismo de grupos $G \overset{f}{\to} G'$ determina un isomorfismo $G/\operatorname{nuc}(f) \overset{\widetilde{f}}{\approx} \operatorname{im}(f)$ definido de la manera natural: $\widetilde{f}(x \operatorname{nuc}(f)) = f(x)$.

Paso al cociente del producto en un anillo

Sea $(A,+,\cdot)$ un anillo y sea $(B,+)$ un subgrupo aditivo de $(A,+)$. Ya sabemos que la suma de A se puede pasar al cociente por B obteniendo el grupo cociente A/B, en el que la suma es $(a+B)+(c+B)=(a+c)+B$. Inmediatamente surgen algunas preguntas

- ¿Será posible pasar al cociente por B la multiplicación de A?
- ¿Necesitaremos imponer alguna restricción a B?

Para poder pasar la multiplicación al cociente por B ha de cumplirse que $(a-a'\in B)\wedge(c-c'\in B)\Rightarrow a\cdot c-a'\cdot c'\in B$. Si intentamos verificar esta propiedad, haciendo, por ejemplo $a\cdot c-a'\cdot c'=a\cdot c-a\cdot c'+a\cdot c'-a'\cdot c'=a\cdot(c-c')+(a-a')\cdot c'$, pronto nos damos cuenta de que el hecho de que B sea un subgrupo con la suma, resulta insuficiente. La condición que hay que pedir está contenida en la siguiente

IDEALES. ANILLO COCIENTE

DEFINICIÓN

Un subgrupo aditivo B del anillo A se dice que es

- un IDEAL POR LA IZQUIERDA si $\forall c \in B$ y $\forall a \in A,\ a \cdot c \in B$.
- un IDEAL POR LA DERECHA si $\forall c \in B$ y $\forall a \in A,\ c \cdot a \in B$.
- Un IDEAL BILÁTERO si es, a la vez. ideal por la izquierda e ideal por la derecha.

En efecto, si B es un ideal bilátero, tanto $a \cdot (c - c')$ como $(a - a') \cdot c'$ pertenecen a B y, así, $a \cdot c - a' \cdot c' \in B$. De hecho, eligiendo $a' = 0$ o $c' = 0$, vemos que la condición de que B sea ideal bilátero es también necesaria.

PROPOSICIÓN

Si B es ideal bilátero del anillo A, se puede definir el producto en A/B haciendo $(a + B) \cdot (c + B) = (a \cdot c) + B$, obteniéndose un anillo $(A/B, +, \cdot)$ al que se llama anillo cociente.

PRODUCTO DE CONGRUENCIAS

EJEMPLO Si tomamos como anillo los enteros $\mathbb{Z}$, con sus operaciones de suma y producto naturales, observamos que $\forall n \in \mathbb{N},\ \mathbb{Z}n$ es un ideal bilátero. La consecuencia es que las congruencias módulo n se pueden multiplicar, es decir
$(a \equiv b\ (\mathrm{mod} n)) \wedge (c \equiv d\ (\mathrm{mod} n)) \Rightarrow ac \equiv bd\ (\mathrm{mod} n)$ y, por lo tanto, se puede definir el producto en $\mathbb{Z}_n$ haciendo $\bar{j} \cdot \bar{k} = \overline{j \cdot k}$. De este modo se convierte a $\mathbb{Z}_n$ en un anillo conmutativo con unidad, el anillo de la clases de restos módulo n. Las operaciones en $\mathbb{Z}_n$ constituyen lo que se llama aritmética modular. Fueron usadas por primera vez de manera sistemática por C. F. Gauss en su obra monumental Disquisiciones Arithmeticae, que publicó en 1801, cuando sólo contaba 24 años.

Ejemplos

Escribimos las tablas de multiplicar de $\mathbb{Z}_6$ y $\mathbb{Z}_7$ (sin el $\overline{0}$ ni el $\overline{1}$) para comparar estos dos anillos.

$\mathbb{Z}_6$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Observamos que $\mathbb{Z}_6$ no es un anillo entero, ya que $\overline{2}$ y $\overline{3}$ son divisores de cero.
El grupo de unidades es $\mathbb{Z}_6^\star = \{\overline{1}, \overline{5}\}$.

$\mathbb{Z}_7$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Vemos que $\mathbb{Z}_7$ no sólo no tiene divisores de cero, sino que es un cuerpo.
El grupo de unidades es $\mathbb{Z}_7^\star = \mathbb{Z}_7 \setminus \{\overline{0}\}$.

Definición

Sea A un anillo conmutativo con unidad y sea $B \subset A$ un ideal.

- Se dice que B es un ideal primo si sólo si $B \underset{\neq}{\subset} A$ y $\forall x, y \in A,\ x \cdot y \in B \Rightarrow (x \in B) \vee (y \in B)$.
- Se dice que B es un ideal maximal si sólo si $B \underset{\neq}{\subset} A$ y $\nexists C$ ideal tal que $B \underset{\neq}{\subset} C \underset{\neq}{\subset} A$.

Ejemplo En $\mathbb{Z}$, el ideal
$\mathbb{Z} \cdot n$ es maximal $\Leftrightarrow$ es primo $\Leftrightarrow$ n es un número primo.
En efecto, veremos en seguida que todo ideal maximal es primo. Por otro lado, si el ideal $\mathbb{Z} \cdot n$ es primo, n tiene que ser primo, pues, en caso contrario, se podría poner $n = x \cdot y$ y tendríamos $x \cdot y \in \mathbb{Z} \cdot n$, sin que sea ni $x \in \mathbb{Z} \cdot n$ ni $y \in \mathbb{Z} \cdot n$. Finalmente, si n es un número primo y tenemos un ideal $C \underset{\neq}{\supset} \mathbb{Z} \cdot n$, si $x \in C \setminus \mathbb{Z} \cdot n$, será $1 = a \cdot x + b \cdot n \in C$ y entonces, $C = \mathbb{Z}$.

Proposición

Todo ideal maximal es primo; pero un ideal primo no tiene que ser, necesariamente, maximal.

Demostración

Sea B ideal maximal del anillo A, (conmutativo y con unidad). Si $x \cdot y \in B$; pero $x \notin B$, el conjunto $B + A \cdot x$ es un ideal de A. Como $B + A \cdot x \supsetneq B$ y B es maximal, tendrá que ser $B + A \cdot x = A$. En particular $\exists a \in A, b \in B \ni 1 = b + a \cdot x$. Y, multiplicando ambos lados por y, resulta $y = b \cdot y + a \cdot x \cdot y \in B$. Así queda visto que B es un ideal primo.

Por otro lado $\{0\}$ es un ideal primo de $\mathbb{Z}$ que no es maximal.

Proposición

Sea A un anillo conmutativo con unidad y sea $B \subset A$ un ideal. Entonces

- A es un anillo entero $\Leftrightarrow$ $\{0\}$ es un ideal primo.
- A/B es un anillo entero $\Leftrightarrow$ B es un ideal primo. y
- A es un cuerpo $\Leftrightarrow$ $\{0\}$ es un ideal maximal.
- A/B es un cuerpo $\Leftrightarrow$ B es un ideal maximal.

Proposición

Sea A un anillo con un número finito de elementos. Entonces
A es un anillo entero $\Leftrightarrow$ A es un cuerpo.

Demostración

$\Rightarrow$. Sea A un anillo entero finito. Para un $a \in A \setminus \{0\}$, la aplicación $\varphi_a : A \to A$ dada por $\varphi_a(x) = a \cdot x$ es un morfismo de grupos con núcleo $\{0\}$, y por tanto, es inyectiva. Por ser A finito φ_a es sobre. En particular $\exists b \in A \ni a \cdot b = \varphi_a(b) = 1$.

Esto explica que los anillos $\mathbb{Z}_n$, que son finitos, sean, o bien no enteros si n es compuesto, o bien, cuerpos si n es primo. Un resultado que se basa en ideas parecidas es éste

PROPOSICIÓN

Sea A un anillo entero y sea K un subcuerpo de A tal que A es un espacio vectorial de dimensión finita sobre K. Entonces A es un cuerpo.

DEMOSTRACIÓN

Dado $a \in A \setminus \{0\}$, consideramos la aplicación

$$\begin{array}{ccc} A & \to & A \\ x & \mapsto & ax \end{array}$$

que es, claramente, un morfismo de $K-$espacios vectoriales. Además, como A no tiene divisores de cero, se trata de un monomorfismo, es decir, es inyectiva. Pero en un espacio de dimensión finita todo monomorfismo es epimorfismo, es decir, aplicación sobreyectiva. Por tanto, existe $b \in A \ni ab = 1$.

La teoría de ideales extiende muchos aspectos de la divisibilidad en $\mathbb{Z}$ a anillos más generales. Por ejemplo, el hecho de que todo entero $\neq 1, -1$ tiene algún divisor primo, se extiende al siguiente resultado de W. Krull

Teorema

Si A es un anillo conmutativo con unidad y tenemos un ideal $B \underset{\neq}{\subset} A$, entonces existe un ideal maximal $M \underset{\neq}{\subset} A \ni B \subset M$.

Demostración

Sea $\mathcal{I}$ la colección formada por todos los ideales distintos de A y que contienen a B. $\mathcal{I} \neq \emptyset$, ya que $B \in \mathcal{I}$. Vemos que $\mathcal{I}$ con la inclusión de conjuntos, se convierte en un conjunto ordenado inductivo. Según el lema de Zorn, tendrá un elemento maximal, que es el ideal M que buscábamos.

Definición

Sean A y B dos anillos. Diremos que $A \xrightarrow{\varphi} B$ es un morfismo de anillos si se cumplen las dos condiciones siguientes

- $\forall a, c \in A,\ \varphi(a+c) = \varphi(a) + \varphi(c)$ y
- $\forall a, c \in A,\ \varphi(a \cdot c) = \varphi(a) \cdot \varphi(c)$.

Se llama núcleo de φ al conjunto $\mathrm{nuc}(\varphi) = \{a \in A :\ \varphi(a) = 0\}$.

Proposición

Si A es un anillo y $B \subset A$, entonces, B es un ideal bilátero de $A \Leftrightarrow$ B es el núcleo de algún morfismo de anillos definido en A.

Sea A un anillo y sea I un ideal bilátero de A. Consideramos el epimorfismo natural $A \stackrel{\pi_I}{\to} A/I$. Si A' es otro anillo y $A \stackrel{f}{\to} A'$ es un morfismo de anillos, la condición necesaria y suficiente para que f se pueda factorizar a través de A/I, es decir, para que exista $\widetilde{f} : A/I \to A' \ni f = \widetilde{f} \circ \pi_I$ es que $x - y \in I \Rightarrow f(x) = f(y)$. Claramente, esta condición equivale a $I \subset \mathrm{nuc}(f)$. Si esta condición se cumple, basta definir $\widetilde{f}(x + I) = f(x)$. Es inmediato que $\widetilde{f}$ es morfismo de anillos y que $\mathrm{nuc}(\widetilde{f}) = \{x + I : f(x) = 0\} = \pi_I(\mathrm{nuc}(f)) = \mathrm{nuc}(f)/I$. En particular, si $I = \mathrm{nuc}(f)$, será $\mathrm{nuc}(\widetilde{f}) = 0$, de modo que $\widetilde{f}$ es un monomorfismo y un isomorfismo con el subanillo $\mathrm{im}(f)$.
Destacamos que hemos obtenido el siguiente

Teorema de isomorfía de anillos

Cada morfismo de anillos $A \stackrel{f}{\to} A'$ determina un isomorfismo $A/\mathrm{nuc}(f) \stackrel{\widetilde{f}}{\approx} \mathrm{im}(f)$ definido de la manera natural: $\widetilde{f}(x + \mathrm{nuc}(f)) = f(x)$.

Teoría axiomática de conjuntos

Los términos no definidos en esta teoría axiomática son los de clase y la relación binaria entre clases $\in$. Todas las variables $(\mathcal{A}, \mathcal{A}, x, \cdots)$ representarán clases y, dadas dos clases $\mathcal{A}, \mathcal{B}$, el enunciado $\mathcal{A} \in \mathcal{B}$ es verdadero o falso. Una propiedad P significará una fórmula construida con enunciados $\mathcal{A} \in \mathcal{B}$ por negación, conjunción, disyunción y cuantificación de las variables de clase por medio del cálculo de proposiciones.

Definición

$(\mathcal{A} \subset \mathcal{B}) \Leftrightarrow (\forall x : x \in \mathcal{A} \Rightarrow x \in \mathcal{B})$ y $(\mathcal{A} = \mathcal{B}) \Leftrightarrow (\mathcal{A} \subset \mathcal{B}) \wedge (\mathcal{B} \subset \mathcal{A})$.

Esta definición permite sustituir la segunda variable de clase en la relación $x \in \mathcal{A}$; es decir $(x \in \mathcal{A}) \wedge (\mathcal{A} = \mathcal{B}) \Rightarrow (x \in \mathcal{B})$. Para hacer lo mismo con la primera variable necesitamos el

I. Axioma de individualidad

$(x \in \mathcal{A}) \wedge (x = y) \Rightarrow (y \in \mathcal{A})$.

Ahora distinguimos entre clases y conjuntos

Definición

La clase A se llama conjunto si existe alguna clase $\mathcal{A} \ni A \in \mathcal{A}$.

II. Axioma de formación de clases

Para cada propiedad P en la que solamente variables de conjunto son cuantificadas y en la que no aparece la variable $\mathcal{A}$ de clase, existe una clase $\mathcal{A}$ cuyos miembros son, precisamente, los conjuntos que cumplen la propiedad P; en símbolos:
$(x \in \mathcal{A}) \Leftrightarrow (x \text{ es un conjunto}) \wedge P(x)$.

Por el axioma I, la clase $\mathcal{A}$ queda unívocamente determinada por la propiedad P que la define. Escribiremos
$\mathcal{A} = \{x|(x\text{es un conjunto}) \wedge P(x)\} = \mathcal{A}(P)$. Con esta terminología la paradoja de Russell se convierte en el siguiente enunciado inofensivo:
La clase de Russell $\mathcal{R}(P)$, determinada por la propiedad
$P(x) = (x \text{ es un conjunto}) \wedge (x \notin x)$ NO ES UN CONJUNTO.

Usando el axioma II, las operaciones $\mathcal{A} \cup \mathcal{B} = \{x|(x \in \mathcal{A} \vee (x \in \mathcal{B})\}$ y $\mathcal{A} \cap \mathcal{B} = \{x|(x \in \mathcal{A} \wedge (x \in \mathcal{B})\}$ con clases, así como el producto cartesiano $\mathcal{A} \times \mathcal{B}$ de clases, están bien definidas y son clases. La clase universal es $\{x|(x \text{ es un conjunto}) \wedge (x = x)\}$, y la clase nula es $\emptyset = \{x|(x \text{ es un conjunto}) \wedge (x \neq x)\}$. $\emptyset$ es única y es una subclase de cada clase. Las relaciones de equivalencia en las clases se definen como en los conjuntos. Y se tiene

Proposición

Una relación de equivalencia en una clase $\mathcal{A}$ determina una partición de $\mathcal{A}$ en subclases disjuntas dos a dos.

III. Axioma del conjunto vacío

$\emptyset$ es un conjunto.

IV. Axioma de los pares

Si a y B son conjuntos distintos, $\mathcal{A} = \{x|(x = A) \vee (x = B)\}$ es un conjunto (que contiene exactamente dos elementos). Se denota $\{A, B\}$.

V. Axioma de la unión

Si $(A_\alpha)_{\alpha\in\mathcal{A}}$ es una familia de conjuntos, lo cual implica, por definición que tanto $\mathcal{A}$ como cada A_α son conjuntos, entonces $\bigcup_{\alpha\in\mathcal{A}} A_\alpha = \{x|\exists\alpha\in\mathcal{A}\ni x\in A_\alpha\}$ es un conjunto.

VI. Axioma de reemplazamiento

Si A es un conjunto y si $f : A \to \mathcal{A}$ es una aplicación, entonces, $f(A)$ es un conjunto.

El siguiente axioma trata de la formación de subconjuntos

VII. Axioma de la criba

Si A es un conjunto, entonces, para cualquier clase $\mathcal{A}$, $A\cap\mathcal{A}$ es un conjunto.

En particular, si A es un conjunto y P es una propiedad en la que sólo variables de conjunto son cuantificadas, entonces $\{x|(x \in A) \wedge P(x)\}$ es un conjunto, ya que, si $\mathcal{A}$ es la clase determinada por P, $A \cap \mathcal{A} = \{x|(x \in A) \wedge \ x \text{ es un conjunto} \wedge P(x)\}$ y el que $x \in A$ hace que "x es un conjunto"sea redundante.
Puesto que los miembros de una clase son, necesariamente conjuntos, para una clase $\mathcal{A}$ la clase $\mathcal{P}(\mathcal{A})$ de las partes de $\mathcal{A}$, también llamada potencia de A, se define como $\mathcal{P}(\mathcal{A}) = \{\mathcal{B}|(\mathcal{B} \text{ es un conjunto}) \ \wedge \mathcal{B} \subset \mathcal{A}\}$. Así, aunque A sea un conjunto, sólo pertenecen a $\mathcal{P}(\mathcal{A})$ las subclases de A que sean conjuntos.

VIII. Axioma del conjunto potencia

Si A es un conjunto, $\mathcal{P}(A)$ también es un conjunto.

Para ver como se usan estos axiomas, vamos a establecer ahora que algunas construcciones con conjuntos que se usan con frecuencia, dan lugar a conjuntos.

Proposición

$(A_\alpha)_{\alpha\in\mathcal{A}}$ familia de conjuntos $\Rightarrow \bigcap_{\alpha\in\mathcal{A}} A_\alpha$ es un conjunto.

Demostración

Por el axioma V, $S = \bigcup_{\alpha\in\mathcal{A}} A_\alpha$ es un conjunto. Ahora consideramos la propiedad $P(x) = [\forall\alpha \in \mathcal{A} : a \in A_\alpha]$ en la que sólo la variable de conjunto α es cuantificada. Como $\bigcap_{\alpha\in\mathcal{A}} A_\alpha = \{x \in S | P(x)\}$, por la observación que sigue al axioma VII, $\bigcap_{\alpha\in\mathcal{A}} A_\alpha$ es un conjunto.

Proposición

Si A es un conjunto, también lo es $\{A\}$.

Demostración

Si $A = \emptyset$, III y VIII dan, inmediatamente, que $\{\emptyset\}$ es un conjunto. Si $A \neq \emptyset$, entonces, por IV, $\{A, \emptyset\}$ es un conjunto. Llamando $\mathcal{A}$ a la clase determinada por la propiedad $P(x) = (x = A)$, resulta, de nuevo por la observación que sigue a VII, que $\{A, \emptyset\} \cap \mathcal{A} = \{A\}$ es un conjunto.

Proposición

A, B conjuntos $\Rightarrow A \times B$ es un conjunto.

Demostración

Dado $a \in A$, sea $\begin{array}{ccc} B & \xrightarrow{f} & A \times B \\ b & \mapsto & (a, b) \end{array}$. Por VI, $f(B) = \{a\} \times B$ es un conjunto. $A \times B = \bigcup_{a \in A} \{a\} \times B$, luego, por V $A \times B$ es un conjunto.

Proposición

Si A y B son conjuntos, la clase $B^A = \{f : A \to B\}$ es un conjunto.

Demostración

Como $A \times B$ es un conjunto, se sigue de VIII que $\mathcal{P}(A \times B)$ es un conjunto. Cada aplicación es una subclase de $A \times B$ dada por una cierta propiedad, luego, por VII, es un miembro del conjunto $\mathcal{P}(A \times B)$. La clase B^A viene dada por una cierta propiedad aplicada a los miembros de $\mathcal{P}(A \times B)$. De nuevo por VII, B^A es un conjunto.

Proposición

La clase de todos los conjuntos no es un conjunto.

Demostración

Si la clase de todos los conjuntos fuera un conjunto, digamos A, entonces $A \cap \mathcal{R}(P)$ sería un conjunto. Pero $A \cap \mathcal{R}(P) = \mathcal{R}(P)$, que ya hemos visto que no es un conjunto.

Necesitamos, al menos, un par de axiomas más.

IX. Axioma de la base o los cimientos

$\forall A$ conjunto no vacío $\exists u \in A \ni u \cap A = \emptyset$, es decir, $\forall x : x \in A \Rightarrow x \notin u$.

Corolario

$\forall A$ conjunto $\neq \emptyset$, $A \notin A$.

Demostración

Si $A \neq \emptyset \wedge A \in A$, $\{A\}$ es un conjunto y $\nexists u \in \{A\} \ni u \cap \{A\} = \emptyset$.

Corolario

Si tenemos dos conjuntos $A \neq \emptyset$ y $B \neq \emptyset$, entonces, no es posible que sea $A \in B \wedge B \in A$.

Demostración

Si fuera verdad que $A \in B \wedge B \in A$, entonces el conjunto $\{A, B\}$ no tendría ningún elemento $u \ni u \cap \{A, B\} = \emptyset$.

Necesitamos un axioma que garantice la existencia de conjuntos infinitos.

X. Axioma del infinito

Existe un conjunto A con las propiedades siguientes

1. $\emptyset \in A$.
2. $a \in A \Rightarrow a \cup \{a\} \in A$.

Corolario

La clase $\mathbb{Z}_+$ de los números enteros no negativos es un conjunto.

Demostración

Sea A un conjunto con las dos propiedades del axioma X. Sea $\mathcal{B} = \{B \in \mathcal{P}(A) | B$ tiene las dos propiedades del axioma X$\}$. Cada B es un conjunto y, por VII y VIII, $\mathcal{B}$ es un conjunto. Sea $E = \bigcap_{B \in \mathcal{B}} B$. Como cada $B \in \mathcal{B}$ cumple las dos propiedades del axioma X, E también las cumplirá. Si ponemos $x^\star = x \cup \{x\}\ \forall x \in E$, vamos a ver que E cumple las siguientes propiedades:

P1 $\emptyset \in E$.

P2 $x \in E \Rightarrow x^\star \in E$.

P3 $x \in E \Rightarrow x^\star \neq \emptyset$.

P4 $S \subset E\ \ni (\emptyset \in S) \wedge ((x \in S) \Rightarrow (x^\star \in S)) \Rightarrow S = E$.

P5 $(x, y \in E) \wedge (x^\star = y^\star) \Rightarrow x = y$.

Estas cinco propiedades son los llamados axiomas de Peano que, como veremos en el capítulo VI, caracterizan él conjunto $\mathbb{Z}_+$ de los números enteros no negativos. A continuación probamos que E cumple estas cinco propiedades.

Demostración de que E cumple los cinco axiomas de Peano

P1 y P2 son las dos propiedades del axioma X y , como $x \in x^\star$, P3 es evidente. P4 es el Principio de Inducción y para demostrarlo, basta observar que $S \in \mathcal{B}$, de modo que $E \subset S$, que, junto con $S \subset E$ da $S = E$. Sólo queda probar P5. Antes vemos el siguiente

Lema

$\forall x \in E,\ z \in x^\star \Rightarrow z \subset x.$

Demostración

Sea $S = \{x \in E : z \in x^\star \Rightarrow z \subset x\}$. Si vemos que S satisface las hipótesis de P4, tendremos $S = E$. Desde luego $\emptyset \in S$, pues $z \in \emptyset' = \{\emptyset\} \Rightarrow z = \emptyset$.
Veamos ahora que $x \in S \Rightarrow x^\star \in S$. Si $z \in (x^\star)^\star = x^\star \cup \{x^\star\}$, será $z \in x^\star$ o $z = x^\star$. Si $z \in x^\star$, como $x \in S$, será $z \subset x$ y, como $x \subset x^\star$, tendremos $z \subset x^\star$. Por otro lado, si $z = x^\star$, desde luego $z \subset x^\star$.

Demostración de P5

Sean $x, y \in E \ni x^\star = y^\star$. Entonces $x \in x^\star = y^\star \Rightarrow x \subset y$ por el lema. Análogamente, $y \subset x$. En definitiva $x = y$.

Para obtener la versión familiar de los enteros no negativos sólo hay que rebautizar a $\emptyset$ como 0, a $\{\emptyset\}$ como 1, a $\{\emptyset, \{\emptyset\}\}$ como 2, etc. Con esta axiomática, la única forma de obtener subconjuntos de un conjunto dado es utilizar una propiedad y formar la intersección con la clase correspondiente, como indicamos después del axioma VII. Para ver que hay subconjuntos que nos gustaría considerar y que no podemos obtener de esta forma, podemos pensar en este ejemplo de Bertrand Russell: Si tenemos una colección infinita de pares de zapatos, podemos definir un subconjunto que tenga un zapato de cada par mediante la propiedad "zapato derecho". Pero si queremos hacer lo mismo con una colección infinita de pares de calcetines, no tenemos ninguna propiedad que nos permita distinguir un miembro de otro en cada par y no podríamos llamar conjunto a una colección de calcetines que contiene uno de cada par. Por eso se introduce un último axioma que da otra forma de producir subconjuntos.

XI. Axioma de elección

Dada una familia no vacía $(A_\alpha)_{\alpha\in\mathcal{A}}$ de conjuntos no vacíos disjuntos dos a dos, existe un conjunto S que contiene exactamente un elemento de cada A_α.

Este es el único axioma existencial. En contra de lo que ocurre con los otros axiomas, un conjunto obtenido por aplicación del axioma de elección no está, en general, unívocamente determinado por las condiciones dadas. En 1938, Kurt Gödel demostró que si la teoría de conjuntos basada en los axiomas I a X es consistente, entonces, la teoría de conjuntos basada en los axiomas I a XI es también consistente. El resultado de Gödel dejaba abierta la posibilidad de que el axioma de elección pudiera deducirse de los diez axiomas anteriores. Sin embargo Paul Cohen demostró en 1963 que esto no es así, de modo que el axioma de elección es, de hecho, independiente de los otros axiomas.

Cardinales infinitos

Para un conjunto finito X, hemos definido el cardinal de X, que hemos denotado $|X|$, como un número $n \in \mathbb{N} \cup \{0\}$ tal que existe una biyección entre X y $\mathbb{N}_n$ si $n > 0$, o bien $X = \emptyset$ si $n = 0$. Pero ¿Qué hacer con los conjuntos infinitos, o sea, los que no son finitos? ¿ Es posible asignarles un número cardinal? Podemos dar la siguiente

Definición

Dos conjuntos X e Y tienen el mismo cardinal si existe una biyección entre ellos. Pondríamos, entonces $|X| = |Y|$. A veces, en lugar de $|X|$, pondremos $\mathrm{card}(X)$.

Hay que reconocer que esta definición todavía deja un halo de misterio en torno a lo que es, en realidad, el cardinal de un conjunto infinito. Antes que nada demos algunos ejemplos de conjuntos infinitos y sus cardinales.

Ejemplos de conjuntos infinitos

1. Es claro que el conjunto $\mathbb{N}$ de los números naturales, es infinito (¿por qué?). Además si escribimos $\mathbb{N} = \mathbb{P} \biguplus \mathbb{I}$, la descomposición en pares e impares, tenemos que $|\mathbb{P}| = |\mathbb{I}|$, ya que, por ejemplo, $j \mapsto j - 1$ es una biyección de $\mathbb{P}$ sobre $\mathbb{I}$ con inversa $k \mapsto k + 1$.
2. De hecho, $|\mathbb{P}| = |\mathbb{N}|$, como se ve con la aplicación $n \mapsto 2n$, que es una biyección de $\mathbb{N}$ sobre $\mathbb{P}$ con inversa $k \mapsto k/2$. Este hecho sorprendente de que exista una biyección entre el conjunto y una parte propia, veremos que caracteriza a los conjuntos infinitos.
3. Veremos ahora que $|\mathbb{Z}| = |\mathbb{N}|$. Para ello consideramos las aplicaciones $\mathbb{Z} \xrightarrow{f} \mathbb{N}$, dada por $f(j) = \begin{cases} -(2j+1) \text{ si } j < 0 \\ 2j + 2 \text{ si } j \geq 0 \end{cases}$ y

   $\mathbb{N} \xrightarrow{g} \mathbb{Z}$, dada por $g(n) = \begin{cases} (-n-1)/2 \text{ si } n \in \mathbb{I} \\ (n-2)/2 \text{ si } n \in \mathbb{P}. \end{cases}$ Si $j < 0$,

   $g(f(j)) = g(-(2j+1)) = j$ y si $j \geq 0$,

   $g(f(j)) = g(2j+2) = j$, $\therefore g \circ f = \mathrm{id}_{\mathbb{Z}}$. Además, $f \circ g = \mathrm{id}_{\mathbb{N}}$.

Conjuntos numerables

Definición

Los conjuntos biyectivos con $\mathbb{N}$ se llamarán infinitos numerables y a su cardinal se le denotará $\aleph_0$. Se dirá que un conjunto es numerable si es finito o infinito numerable.

Proposición

Si X es infinito numerable e $Y \subset X$, entonces Y es numerable, es decir, Y es finito o infinito numerable.

Demostración

Sea $X = \{x_1, x_2, \cdots, x_n, \cdots\}$. Entonces, o bien es $Y = \emptyset$, en cuyo caso, Y es finito, o si no, podemos ir definiendo $j_1 = \min\{j \ni x_j \in Y\}, j_2 = \min\{j > j_1 \ni x_j \in Y\}, \cdots, j_n = \min\{j > j_{n-1} \ni x_j \in Y\}, \cdots$. Si la sucesión j_n termina, o sea, si es finita, el conjunto Y es finito. En caso contrario $k \mapsto x_{j_k}$ es una biyección entre $\mathbb{N}$ y Y, de forma que Y es infinito numerable.

El mismo argumento demuestra que

PROPOSICIÓN

X finito $\wedge$ $Y \subset X \Rightarrow$ Y finito.

PROPOSICIÓN

Todo conjunto infinito contiene un conjunto infinito numerable.

DEMOSTRACIÓN

Usamos (AE). Elegimos $x_1 \in X$ y, por inducción, si ya tenemos $x_1, x_2, \cdots, x_n \in X$, como $X \setminus \{x_1, x_2, \cdots, x_n\} \neq \emptyset$, elegimos $x_{n+1} \in X \setminus \{x_1, x_2, \cdots, x_n\}$, etc.. Así consegimos $S = \{x_j\}_{j \in \mathbb{N}} \subset X$ con $|S| = \aleph_0$.

TEOREMA

X es infinito $\Leftrightarrow \exists Y \underset{\neq}{\subset} X \ni |X| = |Y|$.

Demostración

- $\Leftarrow$ Veamos que, si X es finito, entonces no existe biyección entre X y una parte propia. Lo hacemos por inducción en $|X|$. Si $|X| = 0,\ X = \emptyset$, de forma que X no tiene partes propias. Si suponemos que ningún conjunto de cardinal n tiene biyección con una parte propia, inmediatamente vemos que lo mismo sucede para los de cardinal $n+1$, pues si existiera una biyección $\mathbb{N}_{n+1} \to A \underset{\neq}{\subset} \mathbb{N}_{n+1}$, podríamos suponer que $A \subset \mathbb{N}_n$ y, eliminando $n+1$ y su imagen, tendríamos una biyección de $\mathbb{N}_n$ con una parte propia.
- $\Rightarrow$ Si X es infinito, sabemos que $X \supset Y$ con $|Y| = \aleph_0$. Si $Y = \{y_n\}_{n\in\mathbb{N}}$, consideramos $S = \{y_{2n}\}_{n\in\mathbb{N}}$ y tenemos una biyección entre X y $X \setminus S$.

Conjuntos no numerables

G. Cantor (1845-1918) demostró que existen conjuntos no numerables, lo que da lugar a distintos cardinales infinitos.

Teorema

El conjunto $\{0,1\}^{\mathbb{N}}$ formado por las sucesiones de 0's y 1's es un conjunto infinito NO NUMERABLE.

Demostración(Cantor)

Lo que hace Cantor es demostrar que ninguna aplicación de $\mathbb{N}$ en $\{0,1\}^{\mathbb{N}}$ es sobre.. Utiliza lo que se ha dado en llamar "proceso diagonal de Cantor", que es como sigue. Sea $\mathbb{N} \xrightarrow{f} \{0,1\}^{\mathbb{N}}$. Escribimos $f(i) = x^i = (x_j^i)_{j=1}^{\infty}$. Definimos ahora $y = (y_j)_{j=1}^{\infty} \in \{0,1\}^{\mathbb{N}}$ de la siguiente forma: $y_j = \begin{cases} 0 \text{ si } x_j^j = 1 \text{ y} \\ 1 \text{ si } x_j^j = 0. \end{cases}$. Vemos que $\forall j \in \mathbb{N}, y \neq f(j)$, pues $y_j \neq x_j^j$. Así pues, $y \notin f(\mathbb{N})$ y f no es sobre..

Definición(Comparación de cardinales)

Se define $|X| < |Y|$ si $\exists f : X \to Y$, inyectiva; pero $\nexists$ biyección $X \to Y$.

El teorema de Cantor implica $|\mathbb{N}| < |\{0,1\}^{\mathbb{N}}|$. Esto vale para cualquier conjunto y se prueba igual.

Teorema

$|X| < |\{0,1\}^X|$, donde hemos usado la notación $\{0,1\}^X$ para designar al conjunto de las aplicaciones de X en $\{0,1\}$.

Demostración

La aplicación $X \xrightarrow{\varepsilon} \{0,1\}^X$ dada por $\varepsilon(x)(y) = \begin{cases} 1 \text{ si } x = y, \\ 0 \text{ si } x \neq y \end{cases}$ es inyectiva. Además, si $X \xrightarrow{f} \{0,1\}^X$, vemos, con el método de Cantor, que f nunca es sobre.. En efecto, definiendo $g : X \to \{0,1\}$ de modo que sea $g(x) = 0$ si $f(x)(x) = 1$ y $g(x) = 1$ si $f(x)(x) = 0$, nos aseguramos que $g \neq f(x) \forall x \in X$, ya que $g(x) \neq f(x)(x) \forall x \in X$.

Corolario

$|X| < |\mathcal{P}(X)|$.

Demostración

Vemos que $|\{0,1\}^X| = |\mathcal{P}(X)|$ con las aplicaciones $\{0,1\}^X \xrightarrow{\varphi} \mathcal{P}(X) \ni \varphi(f) = f^{-1}(1)$ y $\mathcal{P}(X) \xrightarrow{\psi} \{0,1\}^X \ni \psi(A) = \chi_A$, donde $\chi_A(x) = 1 \Leftrightarrow x \in A$, que son inversas una de la otra.
Con estas dos aplicaciones se puede traducir la prueba de que $|X| < |\{0,1\}^X|$ obteniendo $|X| < |\mathcal{P}(X)|$. En concreto $j = \varphi \circ \varepsilon : X \to \mathcal{P}(X)$ es inyectiva. De hecho, $j(x) = \varphi(\varepsilon(x)) = \{x\}$. Por otro lado, dada $X \xrightarrow{F} \mathcal{P}(X)$, pasamos a $f = \psi \circ F : X \to \{0,1\}^X$ y usamos f para construir, como en la prueba del teorema $g : X \to \{0,1\} \ni g(x) = 1 \Leftrightarrow f(x)(x) = 0 \Leftrightarrow x \notin F(x)$. Entonces $g \neq f(x) \forall x \in X$ y $A = \varphi(g) \neq \varphi(f(x)) = F(x) \forall x \in X$. Traduciendo, tenemos $A = g^{-1}(1) = \{x \in X : x \notin F(x)\}$. Sabemos que $A \neq F(x) \forall x \in X$. Lo comprobamos directamente. Si fuera $A = F(x)$, tendríamos $x \in A \Rightarrow x \notin F(x) \Rightarrow x \notin A$ y $x \notin A \Rightarrow x \in F(x) \Rightarrow x \in A$.

Proposición

Si $f : X \to Y$ es sobreyectiva, entonces $|Y| \leq |X|$.

Demostración

Sabemos que existe $g : Y \to X$, tal que $f \circ g = \mathrm{id}_Y$. Por otro lado, también sabemos que la aplicación g es inyectiva y esto nos da lo que queremos.

Hemos de abordar cuanto antes la siguiente PREGUNTA: ¿Es la relación $|X| \leq |Y|$ entre cardinales, una relación de orden ? Dejando aparte el problema de que nunca hemos visto que los cardinales formen un conjunto, lo que queremos dilucidar es si se cumple que $|X| \leq |Y| \wedge |Y| \leq |X| \Rightarrow |X| = |Y|$. La respuesta es positiva y constituye el Teorema de Cantor-Schröder-Bernstein.

El teorema de Cantor-Schröder-Bernstein

Teorema de Cantor-Schröder-Bernstein

$X \xrightarrow{f} Y$ inyectiva $\wedge$ $Y \xrightarrow{g} X$ inyectiva $\Rightarrow \exists X \xrightarrow{h} Y$ biyectiva.

Daremos una prueba basada en el siguiente

Lema

Sea $\mathcal{P}(X) \xrightarrow{\varphi} \mathcal{P}(X)$ ə $A \subset B \Rightarrow \varphi(A) \subset \varphi(B)$ Entonces $\exists U \subset X$ ə $\varphi(U) = U$.

Demostración del lema

Sea $\mathcal{F} = \{S \subset X : \ S \subset \varphi(S)\}$. $\mathcal{F} \neq \emptyset$ (por ejemplo $\emptyset \in \mathcal{F}$).
Consideremos $U = \bigcup_{S \in \mathcal{F}} S$. Sea $S \in \mathcal{F}$. Entonces $S \subset \varphi(S)$ y $S \subset U$.
Por lo tanto $S \subset \varphi(S) \subset \varphi(U)$. Se sigue que $U \subset \varphi(U)$ y, aplicando de nuevo φ, $\varphi(U) \subset \varphi(\varphi(U))$, es decir, $\varphi(U) \in \mathcal{F}$, de modo que $\varphi(U) \subset U$. En definitiva $\varphi(U) = U$.

Demostración del teorema de Cantor-Schröder-Bernstein

Demostración

Definimos $\mathcal{P}(X) \xrightarrow{\varphi} \mathcal{P}(X)$ mediante $\varphi(A) = \complement g(\complement f(A))$. Claramente $A \subset B \Rightarrow \varphi(A) \subset \varphi(B)$. Por el lema, $\exists U \subset X \ni \varphi(U) = U$, o sea $U = \complement g(\complement f(U))$, o, lo que es lo mismo, $\complement(U) = g(\complement f(U))$. Entonces, tenemos $X = U \biguplus \complement U = U \biguplus g(\complement f(U))$ y también $Y = f(U) \biguplus \complement f(U)$.

Definimos $h(x) = \begin{cases} f(x) \text{ si } x \in U. \\ g^{-1}(x) \text{ si } x \notin U. \end{cases}$

- h es inyectiva por serlo $f|_U$ y $g^{-1}|_{g(\complement f(U))}$ y tener imágenes disjuntas, respectivamente $f(U)$ y $\complement f(U)$.
- h es sobre.: si $y \in Y$, o bien $y \in f(U)$, en cuyo caso $\exists x \in U \ni y = f(x) = h(x)$, o bien $y \in \complement f(U)$ y, entonces, $g(y) = x \in \complement(U)$, de modo que $y = g^{-1}(x) = h(x)$.

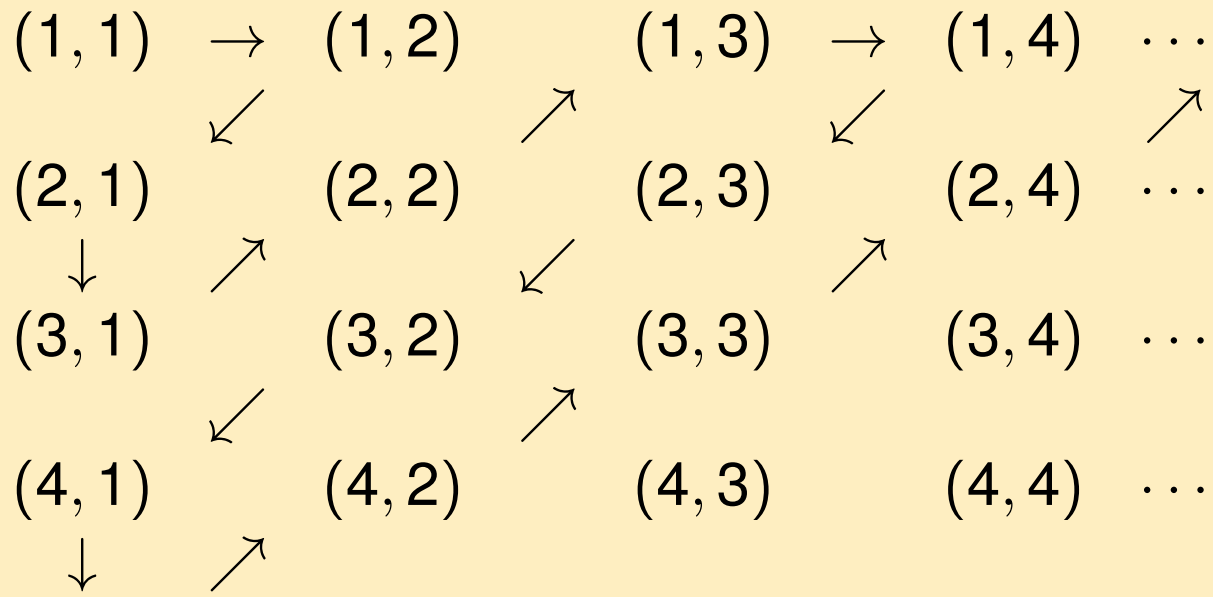
Más conjuntos numerables

Proposición

$\mathbb{N} \times \mathbb{N}$ es infinito numerable, es decir: $|\mathbb{N} \times \mathbb{N}| = \aleph_0$.

Primera prueba

Basta enumerar los elementos del modo siguiente:



Utilizamos el teorema de Cantor-Schröder-Bernstein.

$$\begin{array}{ccc} \mathbb{N} & \to & \mathbb{N}\times\mathbb{N} \\ j & \mapsto & (j,1) \end{array} \quad \text{es inyectiva.}$$

Sólo necesitamos una aplicación inyectiva de $\mathbb{N}\times\mathbb{N}$ en $\mathbb{N}$. Por ejemplo

$$\begin{array}{ccc} \mathbb{N}\times\mathbb{N} & \to & \mathbb{N} \\ (j,k) & \mapsto & 2^j 3^k \end{array}$$

es inyectiva, pues $2^j 3^k = 2^{j'} 3^{k'} \Rightarrow 1 = 2^{j'-j} 3^{k'-k} \Rightarrow j = j' \wedge k = k'$.
Otra posibilidad es

$$\begin{array}{ccc} \mathbb{N}\times\mathbb{N} & \to & \mathbb{N} \\ (j,k) & \mapsto & j10^{j+k} + k. \end{array}$$

La imagen consiste en la expresión decimal de j, seguida por la de k, separadas por una cantidad de ceros (¿cuantos?). Así se ve que es inyectiva.

Suma de cardinales

Definición

Si $\alpha = |A|$ y $\beta = |B|$ y $A \cap B = \emptyset$, definimos $\alpha + \beta = |A \cup B|$.

Hay que ver que
$|A| = |A'| \wedge |B| = |B'| \wedge A' \cap B' = \emptyset \Rightarrow |A \cup B| = |A' \cup B'|$; pero es pura rutina. Veamos como funciona la suma de cardinales infinitos.

Proposición

$\aleph_0 + \aleph_0 = \aleph_0$.

Demostración

Veremos que $|A| = \aleph_0 \wedge |B| = \aleph_0 \Rightarrow |A \cup B| = \aleph_0$. Como $A \cup B \supset A$, desde luego, tenemos $|A \cup B| \geq \aleph_0$. La desigualdad contraria puede obtenerse como sigue: Sean $\mathbb{N} \xrightarrow{\varphi} A$ y $\mathbb{N} \xrightarrow{\varphi} B$ biyectivas. Definimos $\mathbb{N} \times \{1,2\} \xrightarrow{F} A \cup B$ haciendo $F(n,1) = \varphi(n)$ y $F(n,2) = \psi(n)$. F es sobre, de forma que $|A \cup B| \leq |\mathbb{N} \times \{1,2\}| \leq |\mathbb{N} \times \mathbb{N}| = \aleph_0$.

Proposición

$\forall \alpha,$ cardinal infinito, $\alpha + \aleph_0 = \alpha$.

Demostración

Basta ver que si A es un conjunto infinito y B es un conjunto infinito numerable, entonces $|A \cup B| = |A|$. Sabemos que $A \supset A_0$, donde A_0 es infinito numerable. La proposición anterior nos dice que $|A_0 \cup B| = |A_0|$, de modo que existe una biyección entre $A_0 \cup B$ y A_0. Como $A \cup B = (A \setminus A_0) \uplus (A_0 \cup B)$ y $A = (A \setminus A_0) \uplus A_0$, podemos extender la biyección entre $A_0 \cup B$ y A_0 a una biyección de $A \cup B$ sobre A.

Observación: Se sigue que $\forall \alpha,$ cardinal infinito, $\wedge \forall \beta \leq \aleph_0,\ \alpha + \beta = \alpha$.

Corolario

$|A| > \aleph_0 \ \wedge \ A_0 \subset A \ni |A_0| \leq \aleph_0 \Rightarrow \ |A \setminus A_0| = |A|$.

Demostración

$|A| = |A \setminus A_0| + |A_0| = |A \setminus A_0|$, ya que $|A \setminus A_0| > \aleph_0$.

Producto de cardinales

Definición

Si $\alpha = |A|$ y $\beta = |B|$ definimos $\alpha\beta = |A \times B|$. No depende de los conjuntos elegidos.

Proposición

Ya vimos que $\aleph_0\aleph_0 = \aleph_0$.

Proposición

Si $\forall n \in \mathbb{N},\ |A_n| = \aleph_0$, entonces $\left|\bigcup_{n\in\mathbb{N}} A_n\right| = \aleph_0$.

Demostración

$\forall j \in \mathbb{N}$, tenemos una biyección $\mathbb{N} \xrightarrow{\varphi_j} A_j$. Definimos $\Phi : \mathbb{N} \times \mathbb{N} \to \bigcup_{n\in\mathbb{N}} A_n$ haciendo $\Phi(j,k) = \varphi_j(k)$. Vemos que Φ es sobre, con lo cual $\left|\bigcup_{n\in\mathbb{N}} A_n\right| \leq |\mathbb{N} \times \mathbb{N}| = \aleph_0$. La desigualdad contraria es obvia.

La prueba anterior puede adaptarse para demostrar que

Proposición

La unión de cualquier colección numerable de conjuntos numerables es numerable.

Cardinales de algunos conjuntos de números

- $|\mathbb{Z}| = \aleph_0$, pues $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$.
- $|\mathbb{Q}| = \aleph_0$, pues la aplicación $\Psi : \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Q}$, dada por $\Psi(n, m) = \frac{n}{m}$ es sobre, de modo que $|\mathbb{Q}| \leq |\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})| = \aleph_0$. La desigualdad contraria es obvia.
- Sea $\mathcal{P} = \mathbb{Z}[X]$ el anillo de los polinomios con coeficientes enteros. Escribiendo $\mathcal{P} = \bigcup_{j=0}^{\infty} \mathcal{P}_j$, donde $\mathcal{P}_j$ denota el conjunto de los polinomios de grado $\leq j$ y observando que $\mathcal{P}_j$ es biyectivo con $\overbrace{\mathbb{Z} \times \cdots\cdots\cdots \times \mathbb{Z}}^{j+1 \text{ FACTORES}}$, que es numerable, obtenemos que $|\mathcal{P}| = \aleph_0$.

DEFINICIÓN

- Dados un cuerpo L y un subcuerpo K de L, se dice que un elemento $a \in L$ es algebraico sobre K si existe un polinomio $P \in K[X] \ni P(a) = 0$.
- Un número real o complejo se dice que es algebraico si es algebraico sobre $\mathbb{Q}$. Notemos que
  $a \in \mathbb{C}$ es algebraico $\Leftrightarrow \exists P \in \mathbb{Z}[X] \ni P(a) = 0$.
- Escribiremos $\mathcal{A}$ para el conjunto de todos los números complejos algebraicos y $\mathcal{A}_{\mathbb{R}}$ para el conjunto de todos los números reales algebraicos.

Ejemplos: $a \in \mathbb{Q} \Rightarrow a \in \mathcal{A}$, pues $P(a) = 0$ para $P(X) = X - a \in \mathbb{Q}[X]$; pero también son algebraicos $\sqrt{2}, \sqrt{5}, \imath = \sqrt{-1}$ o la razón áurea $\tau = \frac{1+\sqrt{5}}{2}$, ya que todos ellos satisfacen ecuaciones algebraicas con coeficientes enteros. Por ejemplo τ es raíz del polinomio $X^2 - X - 1$. Entonces, tiene sentido plantear la pregunta siguiente

¿Cuántos números algebraicos hay?

Proposición

$|\mathcal{A}_{\mathbb{R}}| = |\mathcal{A}| = \aleph_0$.

Demostración

$\mathbb{Q} \subset \mathcal{A}_{\mathbb{R}} \subset \mathcal{A}$. Además $\mathcal{A} = \bigcup_{P \in \mathbb{Z}[X]} P^{-1}(0)$ y, para cada $P \in \mathbb{Z}[X]$, $P^{-1}(0)$, el conjunto de las raíces de P, es un conjunto finito, con cardinal que no supera al grado de P.

Ahora la pregunta que surge es

¿hay algún número que no sea algebraico?

Veremos que la respuesta es SÍ. Los números no algebraicos se llamarán trascendentes y también veremos que

forman un CONJUNTO NO NUMERABLE

Teorema

Todo conjunto infinito X se puede poner como unión de una colección de conjuntos infinitos numerables que son disjuntos dos a dos.

Demostración

Si $B \subset X$, llamamos descomposición apropiada de S a una familia $\mathcal{B}$ de conjuntos infinitos numerables de X disjuntos dos a dos con unión B. Sea $\mathcal{S} = \{(B, \mathcal{B}) : B \subset X \wedge \mathcal{B}$ descomposición apropiada de $B\}$. En $\mathcal{S}$ damos la relación de orden: $(B, \mathcal{B}) \prec (C, \mathcal{C}) \Leftrightarrow B \subset C \wedge \mathcal{B} \subset \mathcal{C}$. El conjunto ordenado $(\mathcal{S}, \prec)$ es inductivo ya que si $\mathcal{K} = \{(B_\alpha, \mathcal{B}_\alpha\}_{\alpha \in J}$ es una cadena de $(\mathcal{S}, \prec)$, tomando $B = \bigcup_{\alpha \in J} B_\alpha$ y $\mathcal{B} = \bigcup_{\alpha \in J} \mathcal{B}_\alpha$, obtenemos $(B, \mathcal{B}) \in \mathcal{S}$ que es cota superior de $\mathcal{K}$. Por el lema de Zorn, existe $(M, \mathcal{M})$ elemento maximal de $(\mathcal{S}, \prec)$. Si $M = X$, hemos terminado. Si $X \setminus M \neq \emptyset$ fuera infinito, tendría un subconjunto infinito numerable que, añadido a M y a la descomposición apropiada $\mathcal{M}$ daría un elemento de $\mathcal{S}$ mayor estrictamente que $(M, \mathcal{M})$. Así pues, $X \setminus M$ sólo puede ser finito; y basta añadirlo a cualquier conjunto de $\mathcal{M}$ para tener una descomposición apropiada de X.

Corolario

α y β cardinales $\ni \alpha$ infinito y $0 < \beta \leq \aleph_0 \Rightarrow \alpha\beta = \alpha$.

Demostración

Lo que hay que ver es que si A es un conjunto infinito y B es un conjunto numerable, entonces $|A \times B| = |A|$. Usando el teorema, escribimos $A = \biguplus_{j \in J} B_j$, con $|B_j| = \aleph_0 \forall j \in J$. Se sigue que $A \times B = \biguplus_{j \in J} (B_j \times B)$. Como cada $B_j \times B$ es biyectivo con B_j,tenemos una biyección

$$A \times B = \bigbiguplus_{j \in J} (B_j \times B) \leftrightarrow \bigbiguplus_{j \in J} B_j = A.$$

Proposición

Si α y β son cardinales, con α infinito y $\beta \leq \alpha$, entonces $\alpha + \beta = \alpha$.

Demostración

Vamos a ver que si tenemos dos conjuntos A y B, con A infinito y $|B| \leq |A|$, entonces $|A \cup B| = |A|$. En efecto $A \cup B = A \uplus C$ con $C \subset B$. Desde luego $|C| \leq |B| \leq |A|$. Po tanto, existe $\varphi : C \to A$ inyectiva.

Ahora definimos $A \uplus C \overset{\Phi}{\to} A \times \{1, 2\}$ haciendo $\forall a \in A, \Phi(a) = (a, 1)$ y $\forall c \in C, \Phi(c) = (\varphi(c), 2)$. Claramente Φ es inyectiva y, por lo tanto $|A \cup B| = |A \uplus C| \leq |A \times \{1, 2\}| = |A|$.

Proposición

Sea $A = \bigcup_{n \in \mathbb{N}} A_n \ni \forall n \in \mathbb{N},\ |A_n| = \alpha$ infinito. Entonces $|A| = \alpha$.

Demostración

Sea $B \ni |B| = \alpha$. Entonces $\forall n \in \mathbb{N},\ \exists \varphi_n : B \to A_n$ biyectiva. Definimos $\Psi : B \times \mathbb{N} \to A = \bigcup_{n \in \mathbb{N}} A_n$ haciendo $\Psi(a, n) = \varphi_n(a)$. Se trata de una aplicación sobre, de modo que $|A| \leq |B \times \mathbb{N}| = \alpha$.

Potencias

Definición

Dados dos conjuntos A y B, denotaremos por A^B el conjunto de todas las aplicaciones de B en A.
Dados dos cardinales α y β, tomamos dos conjuntos $A \ni |A| = \alpha$ y $B \ni |B| = \beta$ y definimos $\alpha^\beta = |A^B|$.
Hay que ver que la definición no depende de los conjuntos elegidos, lo cual es muy sencillo.

Proposición

$\alpha^\beta \alpha^\gamma = \alpha^{\beta+\gamma}$.

Demostración

Si $|A| = \alpha, |B| = \beta, |C| = \gamma$ y $B \cap C = \emptyset$, hemos de encontrar una biyección $A^B \times A^C \xrightarrow{\Phi} A^{B \uplus C}$. Sea $\Phi(f, g) = h \ni h|_B = f \wedge h|_C = g$. Es claro que Φ es una biyección con inversa $\Phi^{-1}(f) = (f|_B, f|_C)$.

El cardinal del continuo

Proposición

$(\gamma^\alpha)^\beta = \gamma^{\alpha\beta}$.

Demostración

Si $|A| = \alpha, |B| = \beta \ \wedge \ |C| = \gamma$, buscamos $\left(C^A\right)^B \xrightarrow{\Phi} C^{A\times B}$ biyectiva.
$\Phi(f)(a,b) = f(b)(a)$ es biyectiva con inversa $\Psi \ni \Psi(g)(b)(a) = g(a,b)$.

Ejemplo: Vimos que $\forall X,$ conjunto, $|\mathcal{P}(X)| = |\{0,1\}^X| = 2^{|X|}$.
Ya estamos en condiciones de contestar a la siguiente

Pregunta: ¿Cual es el cardinal de $\mathbb{R}$?

$\mathbb{R}$ es biyectivo con cualquier intervalo no trivial. Por ejemplo

$$\begin{array}{ccc}]-\frac{\pi}{2},\frac{\pi}{2}[& \to & \mathbb{R} \\ t & \mapsto & \tan t \end{array}$$

es una biyección y dilatar o contraer el intervalo no cambia el cardinal ni tampoco añadir uno o los dos extremos.

Teorema(El cardinal del continuo)

$|\mathbb{R}| = 2^{\aleph_0}$.

Demostración

La aplicación $\begin{array}{ccc} \{0,1\}^{\mathbb{N}} & \xrightarrow{\Sigma} & [0,1] \\ x = (x_j)_{j=1}^{\infty} & \mapsto & \sum_{j=1}^{\infty} \frac{x_j}{2^j} \end{array}$ es sobre; pero no es inyectiva.

Sea $\prec$ el orden lexicográfico en $\{0,1\}^{\mathbb{N}}$ y $\leq$ el orden usual de $[0,1]$.
$x \prec y \Rightarrow \Sigma(x) \leq \Sigma(y)$; pero puede ser $\Sigma(x) = \Sigma(y)$, sólo cuando, si llamamos j_0 al primer índice $\ni\ x_j \neq y_j$, se tiene que

$\forall j > j_0, x_j = 1 \wedge y_j = 0$. En ese caso $\sum_{j=j_0+1}^{\infty} \frac{1}{2^j} = \frac{1}{2^{j_0}}$, de modo que

$\Sigma(x) = \Sigma(y)$. Sean
$\mathcal{E}_0 = \{x \in \{0,1\}^{\mathbb{N}} : \exists j_0 \in \mathbb{N} : \forall j > j_0 x_j = 0 \vee \forall j > j_0, x_j = 1\}$ y
$\Sigma(\mathcal{E}_0) = \mathbb{D}$. Entonces $|\mathcal{E}_0| = |\mathbb{D}| = \aleph_0$ y Σ es una biyección de $\{0,1\} \setminus \mathcal{E}_0$ sobre $[0,1] \setminus \mathbb{D}$. Por tanto
$|[0,1]| = |[0,1] \setminus \mathbb{D}| = |\{0,1\}^{\mathbb{N}} \setminus \mathcal{E}_0| = |\{0,1\}^{\mathbb{N}}| = 2^{\aleph_0}$.

Hemos visto que $|\mathbb{R}| = 2^{\aleph_0} > \aleph_0$. A veces se suele utilizar la notación $\mathbf{c} = 2^{\aleph_0}$ y a $\mathbf{c}$ se le suele llamar el cardinal del continuo. Una observación interesante de Cantor es que

PROPOSICIÓN

$\forall n \in \mathbb{N},\ |\mathbb{R}^n| = \mathbf{c}$.

DEMOSTRACIÓN

Basta demostrar que si ponemos $I = [0, 1]$, entonces $|I \times I| = |I|$. En realidad, basta exhibir una aplicación inyectiva $I \times I \to I$. Por ejemplo si $x \in I$ tiene expresión decimal $0, x_1 x_2 \cdots x_n \cdots$ e $y \in I$ tiene expresión decimal $0, y_1 y_2 \cdots y_n \cdots$, podemos obtener una aplicación inyectiva de $I \times I$ en I mandando (x, y) al punto de expresión decimal $0, x_1 y_1 x_2 y_2 \cdots$. Esto nos da que $|I \times I| \leq |I|$ y la desigualdad al revés es sencilla. Por ejemplo, a partir de la aplicación inyectiva $x \mapsto (x, 0)$ de I en $I \times I$.

La hipótesis del continuo

El propio Cantor planteó hacia 1880 una famosa pregunta

$$¿\exists A \subset \mathbb{R} \ni \aleph_0 < |A| < 2^{\aleph_0}?$$

El creía que no; pero no consiguió demostrarlo. Quedó como la

HIPÓTESIS DEL CONTÍNUO: $$\nexists A \subset \mathbb{R} \ni \aleph_0 < |A| < 2^{\aleph_0}$$

David Hilbert encabezó con ella la famosa lista de 23 problemas que presentó al Congreso Internacional de Matemáticos de París en 1900. El desarrolllo posterior fue sorprendente y tuvo un enorme impacto en la fundamentación de las Matemáticas.

- En 1938 Kurt Gödel demostró la hipótesis del continuo es consistente con los axiomas de Zermelo-Fraenkel.
- Pero en 1963 Paul Cohen demostró que la negación de la hipótesis del continuo también es compatible con los axiomas de Zermelo-Fraenkel.

Números trascendentes

Con la desigualdad $2^{\aleph_0} > \aleph_0$, Cantor pudo establecer la existencia de números trascendentes, de hecho, la de una cantidad no numerable de ellos

Proposición

$|\mathbb{C} \setminus \mathcal{A}| = |\mathbb{R} \setminus \mathcal{A}_{\mathbb{R}}| = 2^{\aleph_0}|$.

Demostración

Basta observar que $|\mathcal{A}| = |\mathcal{A}_{\mathbb{R}}| = \aleph_0$, mientras que $|\mathbb{C}| = |\mathbb{R}| = 2^{\aleph_0} > \aleph_0$.

Notas históricas sobre los números trascendentes

En realidad, Cantor no fue el primero en demostrar la existencia de números trascendentes. Este honor es para Liouville, quien demostró en 1851 que el número $0,1100010000000000000000010\cdots$, que tiene en su expresión decimal un 1 en la posición $n!$ y un cero en todas las demás, es trascendente. El mérito de Cantor es, desde luego, el método, que es completamente diferente al de Liouville, y la posibilidad de contestar a la pregunta de cuántos números trascendentes hay. En todo caso, Cantor, que publicó su hallazgo en 1874, no puede dar explícitamente con su método ningún número trascendente. Curiosamente, en 1873, Charles Hermite probó que e es trascendente y, con el mismo método de Hermite, Lindemann, el director de tesis de Hilbert, estableció en 1882 que π es trascendente, lo cual implica la imposibilidad de realizar la cuadratura del círculo con regla y compás, como pretendían los griegos clásicos.

Orden total

Proposición

Si α y β son cardinales, entonces $\alpha \leq \beta \vee \ \beta \leq \alpha$.

Demostración

Si $|A| = \alpha$ y $|B| = \beta$, sea $\mathcal{I} = \{(X, f) \ni \ X \subset A \wedge \ f : X \to B \text{ inyectiva}\}$. Suponemos $\beta \neq 0$. Entonces $\mathcal{I} \neq \emptyset$. Definimos un orden $\prec$ en $\mathcal{I}$: $(X, f) \prec (Y, g) \Leftrightarrow X \subset Y \wedge g|_X = f$. $(\mathcal{I}, \prec)$ es un conjunto ordenado inductivo. En efecto, si $\mathcal{K} = \{(X_\alpha, f_\alpha)\}_{\alpha \in J}$ es una cadena, entonces, definiendo $X = \bigcup_{\alpha \in J} X_\alpha \subset A$ y $f : X \to B$ como $f(x) = f_\alpha(x)$ si $x \in X_\alpha$, tenemos (X, f) cota superior de $\mathcal{K}$. El lema de Zorn implica que $(\mathcal{I}, \prec)$ tiene un elemento maximal (M, h). Ahora, o bien $M = A$, en cuyo caso $\alpha \leq \beta$, o bien $h(M) = B$, en cuyo caso, $\beta \leq \alpha$. En efecto, si $M \neq A$ y $h(M) \neq B$, tomamos $a \in A \setminus M$ y $b \in B \setminus h(M)$. Definimos $X = M \cup \{a\}$ y $k : X \to B \ni \ k(x) = \begin{cases} h(x) \text{ si } x \in M \\ b \text{ si } x = a. \end{cases}$ $(M, h) \underset{\neq}{\prec} (X, k)$ ¡imposible!

Teorema

$\forall A$, conjunto infinito, $|A \times A| = |A|$, es decir, si $\alpha = |A|$, $\alpha\alpha = \alpha$.

Demostración

Sea $\mathcal{Y} = \{(B, \varphi) : B \subset A \wedge B \times B \overset{\varphi}{\to} B \text{ biyectiva}\}$. $A \supset D \ni |D| = \aleph_0 \Rightarrow \mathcal{Y} \neq \emptyset$. En $\mathcal{Y}$ damos $(B, \varphi) \prec (C, \psi) \Leftrightarrow B \subset C \wedge \psi|_{B \times B} = \varphi$. $(\mathcal{Y}, \prec)$ es conjunto ordenado inductivo (se omite la prueba, que ya es rutina). Por el lema de Zorn, $\exists (M, \mu)$ maximal en $(\mathcal{Y}, \prec)$. Si $M = A$, hemos terminado. Si $M \underset{\neq}{\subset} A$, será $|A \setminus M| \leq |M| \ \vee |A \setminus M| > |M|$. Si $|A \setminus M| \leq |M|$, tenemos $|A| = |M \cup (A \setminus M)| = |M| = |M \times M| = |A \times A|$ y terminamos. Por último, si $|A \setminus M| > |M|$, existirá $M_0 \subset A \setminus M \ni |M_0| = |M|$. Sea $M_1 = M \uplus M_0$. Tenemos $M_1 \times M_1 = (M \times M) \uplus S$, donde $S = (M \times M_0) \uplus (M_0 \times M) \uplus (M_0 \times M_0)$. Pero, como $|M \times M_0| = |M_0 \times M| = |M_0 \times M_0| = |M|$, resulta $|S| = |M_0|$, y así, existe una biyección $S \overset{\mu_0}{\to} M_0$, que podemos usar para extender $M \times M \overset{\mu}{\to} M$ a una biyección $M_1 \times M_1 \overset{\mu_1}{\to} M_1$, ¡imposible!. El último caso no puede darse y la prueba está completa.

Teorema

Sea $A = \bigcup_{j \in J} A_j \ni |A_j| \leq \alpha \forall j \in J \wedge |J| \leq \alpha$, cardinal infinito. Entonces, $|A| \leq \alpha$.

Demostración

Podemos suponer $|J| = \alpha \wedge |A_j| = \alpha \forall j \in J$. Tendremos, entonces, biyecciones $J \overset{\varphi_j}{\to} A_j$. Si definimos

$$\begin{array}{ccc} J \times J & \to & \bigcup_{j \in J} A_j = A \\ (j,k) & \mapsto & \varphi_j(k) \end{array},$$

tenemos una aplicación sobre.. Se sigue que $|A| \leq |J \times J| = \alpha\alpha = \alpha$.

Aplicación: Dimensión de un espacio vectorial

Proposición

Sea E un $\mathbb{K}-$espacio vectorial. Sea B una base, que suponemos infinita. Sea V un sistema de generadores de E tal que $|V| > |B|$. Entonces, los vectores de V no son linealmente independientes.

Demostración

$\forall b \in B,\ \exists V_b,$ conjunto finito $\subset V \ni b = \sum_{x \in V_b} \lambda_x x$. Vemos que, entonces $W = \bigcup_{b \in B} V_b \subset V$ es un sistema de generadores de E. Pero $|W| \leq |B| < |V|$, de modo que existe algún $v \in V$ que es combinación lineal de los vectores de W. Así pues, los vectores de V no son linealmente independientes.

Corolario

Dos bases cualesquiera de E tienen el mismo cardinal, al que llamaremos dimensión de E.

TEOREMA

$2 \leq \alpha \leq \beta \ \wedge \ \beta$ infinito $\Rightarrow \ \alpha^\beta = 2^\beta$.

DEMOSTRACIÓN

$$2^\beta \leq \alpha^\beta \leq (2^\alpha)^\beta = 2^{\alpha\beta} = 2^\beta \ \Rightarrow \ \alpha^\beta = 2^\beta.$$

Por ejemplo, esto nos dice que $\aleph_0^{\aleph_0} = 2^{\aleph_0}$, o sea, que hay tantas aplicaciones de $\mathbb{N}$ en $\mathbb{N}$ como partes de $\mathbb{N}$ y como números reales.