Prerequisitos y preliminares
Hungerford

Pablo Brianese

28 de agosto de 2021

Teorema 1 (4.1)**.** *Sea A un conjunto novacio. Dada una relación de equivalencia $R \subseteq A \times A$, definimos sus clases de equivalencia como $\bar{a} = \{b \in A : (a, b) \in R\}$ para cada $a \in A$, y definimos el cociente de A por R como $A/R = \{\bar{a} : a \in A\}$. La asignación $R \mapsto A/R$ define una biyección entre el conjunto $E(A)$, formado por todas las relaciones de equivalencia R sobre A, y el conjunto $Q(A)$, formado por todas las parciones de A.*

Teorema 2 (5.2)**.** *Sea $\{A_i : i \in I\}$ una familia de conjuntos indexada por I. Entonces existe un conjunto D, junto con una familia de aplicaciones $\{\pi_i : D \to A_i | i \in I\}$ con la siguiente propiedad: para cualquier conjunto C y familia de aplicaciones $\{\phi_i : C \to A_i | i \in I\}$, existe una única aplicación $\psi : C \to D$ tal que $\pi_i \phi = \phi_i$ para todo $i \in I$. Más aún, D queda determinado univocamente salvo una biyección.*

$$\begin{tikzcd}
C \arrow[d, dotted, "\phi"] \arrow[dr, "\phi_i"] & \\
D \arrow[r, "\pi_i"] & A_i
\end{tikzcd}$$

Teorema 3 (6.2 Recursion)**.** *Si S es un conjunto, $a \in S$ y para cada $n \in \mathbb{N}$, $f_n : S \to S$ es una función, entonces existe una única función $\phi : \mathbb{N} \to S$ tal que $\phi(0) = a$ y $\phi(n+1) = f_n(\phi(n))$ para todo $n \in \mathbb{N}$.*

Para cada $N \in \mathbb{Z}$, denotamos $[N] = \{n \in \mathbb{N} : 0 \leq n \leq N\}$.

Demostración. Sea $\mathcal{N}$ el conjunto de los $N \in \mathbb{N}$ tales que existe una única función $\phi_N : [N] \to S$ que verifica la *condición recursiva* $\phi_N(n+1) = f_n(\phi_N(n))$ para todo $n \in [N-1]$, y la condición base $\phi_N(0) = a$.

En un principio $0 \in \mathcal{N}$. En efecto, aquí la condición $\phi_0(0) = a$ determina unívocamente a la función $\phi_0 : \{0\} \to S$; y la condición recursiva sobre ϕ_0 es vacua porque $[-1] = \emptyset$.

Supongamos, inductivamente, que $N \in \mathcal{N}$. Entonces existe una única función $\phi_N : [N] \to S$ tal que $\phi_N(0) = a$ y verifica la condición recursiva. Definimos $\phi_{N+1} : [N+1] \to S$ como $\phi_{N+1}(n) = \phi_N(n)$ para $n \in [N]$, e imponemos $\phi_{N+1}(N+1) = f_N(\phi_N(N))$. Entonces por construcción $\phi_{N+1}(0) = a$, y ϕ_{N+1} verifica la condición recursiva. Para probar la unicidad de ϕ_{N+1} suponemos que $\psi : [N+1] \to S$ es cualquier función que verifique la condición recursiva y la condición base. Si restringimos ψ al conjunto $[N]$ obtenemos una función que satisface la condición recursiva y la condición base. Por hipótesis inductiva $\psi|_{[N]} = \phi_N$. La condición recursiva para ψ dice que $\psi(N+1) = f_N(\psi(N))$. Pero probamos $\psi(N) = \phi_N(N)$. Entonces $\psi(N+1) = f_N(\phi_N(N))$. Por lo tanto $\psi = \phi_{N+1}$. En conclusión $N + 1 \in \mathcal{N}$.

Por inducción, para todo $N \in \mathbb{N}$ existe una única función $\phi_N : [N] \to S$ tal que $\phi_N(0) = a$ y $\phi_N(n+1) = f_n(\phi_N(n))$ para todo $n \in [N-1]$. La propiedad de unicidad las hace compatibles, es decir que $\phi_N|_{[M]} = \phi_M$ si $M \leq N$. Esta compatibilidad nos permite afirmar que la unión de sus gráficas, $\bigcup_{N \in \mathbb{N}} \mathrm{gr}(\phi_N)$, es la gráfica de una función $\phi : \mathbb{N} \to S$ tal que $\phi(0) = a$ y $\phi(n+1) = f_n(\phi(n))$ para todo $n \in \mathbb{N}$. La unicidad de esta gran ϕ es consecuencia de la unicidad de las pequeñas ϕ_N con $N \in \mathbb{N}$. $\square$

Teorema 4 (6.3 Algoritmo de la División)**.** *Si $a, b \in \mathbb{Z}$ y $a \neq 0$, entonces existen enteros q y r, únicos tales que $b = aq + r$ y $0 \leq r < |a|$.*

Demostración. Siendo que $a \neq 0$, el conjunto $a\mathbb{Z}$ no está acotado inferiormente. Luego, existe un entero en $a\mathbb{Z}$ menor o igual a b. Por eso el conjunto $S = (b - a\mathbb{Z}) \cap \mathbb{N}$ no vacío. En tanto es un subconjunto novacío de $\mathbb{N}$, S contiene un elemento mínimo $r = b - aq$ (para algún $q \in \mathbb{Z}$).

Tenemos, en primer lugar, que $b = aq + r$. También sabemos $0 \leq r$ porque $r \in \mathbb{N}$.

Supongamos, para llegar a un absurdo, que $r \geq |a|$. Escribimos $|a| = a\sigma$ con $\sigma = \pm 1$. Así, $\sigma \in \mathbb{Z}$ implica que $q' = q + \sigma$, $r' = r - a\sigma$ son números enteros tales que $b = aq + r = a(q + \sigma) + (r - a\sigma) = aq' + r'$. Más aún, $r \geq |a|$ implica $r' \geq 0$. Luego $r' \in S$, conjunto que tiene a r como elemento mínimo. Se sigue que $r \leq r'$. Pero $a\sigma > 0$ porque $a \neq 0$, luego $r' = r - a\sigma < r$. Esto es absurdo. Por lo tanto $r < |a|$.

Para probar la unicidad de q, r, suponemos que q', r' son enteros tales que $b = aq' + r'$ y $0 \leq r' < |a|$. Luego, las ecuaciones $b = aq + r$ y $b = aq' + r'$ implican $-a(q' - q) = r' - r$; y las desigualdades $0 \leq r < |a|$ y $0 \leq r' < |a|$ implican $-|a| < r' - r < |a|$. Juntas, permiten deducir que $|-a(q' - q)| < |a|$ y $|q' - q| < 1$. Pero $|q' - q| \in \mathbb{N}$, y el menor número natural positivo es 1, por lo tanto $|q' - q| = 0$. Concluímos $q' - q = 0$, y $r' - r = -a \cdot 0 = 0$. □

Teorema 5 (Existencia del máximo común divisor)**.** *Si $a_1, a_2, \ldots, a_n$ son enteros, no todos nulos, entonces $(a_1, a_2, \ldots, a_n)$ existe. Más aún, existen enteros $k_1, k_2, \ldots, k_n$ tales que $(a_1, a_2, \ldots, a_n) = k_1 a_1 + k_2 a_2 + \cdots + k_n a_n$.*

Demostración. Consideremos el conjunto $C = a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z}$. Este contiene al menos a un elemento positivo $|a_1| + |a_2| + \cdots + |a_n|$ porque $a_1, a_2, \ldots, a_n$ no son todos nulos y $|a_i| \in a_i\mathbb{Z}$ para todo i. Luego el conjunto $S = C \cap \mathbb{Z}^+$, en tanto subconjunto de $\mathbb{N}$, tiene un elemento mínimo que denotamos por d. Además, este mínimo puede escribirse como $d = k_1 a_1 + k_2 a_2 + \cdots + k_n a_n$ para unos $k_1, k_2, \ldots, k_n \in \mathbb{Z}$.

Dado a_i con $i \in \{1, 2, \ldots, n\}$, por el teorema del Algoritmo de la División, existen enteros q, r tales que $a_i = dq + r$ con $0 \leq r < d$. La ecuación $r = a_i - dq$ implica $r \in C$. Y la desigualdad $0 \leq r$ implica $r \in \mathbb{N}$. Si fuera el caso que $r \in \mathbb{Z}^+$, entonces sería $r \in S$ y $d \leq r$ (porque $d = \min S$). Pero $r < d$ por el Teorema del Algoritmo de la División. Luego $r = 0$. Esto prueba que $d \mid a_i$.

Sea d' un entero que divide a cada $a_1, a_2, \ldots, a_n$. Luego existen enteros $q_1, q_2, \ldots, q_n$ tales que $a_i = d' q_i$ para todo $i \in \{1, 2, \ldots, n\}$. Por eso

$$d = \sum_{i=1}^{n} k_i a_i = \sum_{i=1}^{n} k_i d' q_i = d' \left(\sum_{i=1}^{n} k_i q_i \right) \tag{1}$$

resulta que $d' \mid d$. □

Teorema 6 (Fundamental de la Aritmética)**.** *Cualquier entero positivo $n > 1$ puede ser escrito de forma única en la forma $n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$, donde $p_1 < p_2 < \ldots < p_k$ son primos y $t_i > 0$ para todo i.*