Cuerpos con pocos elementos

16 de abril, 2020

1 Un cuerpo con dos elementos

De la definición, sabemos que un cuerpo $\Bbbk$ tiene un elemento 0, un elemento 1, y que esos dos elementos son distintos: esto significa que un cuerpo tiene *al menos* dos elementos. Tratemos de construir un cuerpo $\Bbbk$ que tenga la menor cantidad de elementos posible, es decir, dos.

Los elementos del cuerpo van a ser 0, el cero de la suma, y 1, el elemento neutro de la multiplicación, así que

$$\Bbbk = \{0, 1\}.$$

Para hacer del conjunto $\Bbbk$ un cuerpo, tenemos que describir las dos operaciones de suma $+$ y de multiplicación $\cdot$ de $\Bbbk$. Una forma de hacerlo —conveniente en este caso en el que hay pocos elementos— es dar las tablas de las dos operaciones. Tenemos entonces que ver de qué manera conpletar las siguientes dos tablas:

$+$	0	1
0		
1		

$\cdot$	0	1
0		
1		

Empecemos con la suma. El cero 0 es el elemento neutro de la suma: esto significa que para todo $x \in \Bbbk$ se tiene que $x+0 = x$ y que $0+x = x$. Si tomamos $x = 0$, esto nos dice que $0 + 0 = 0$ y otra vez que $0 + 0 = 0$; si tomamos $x = 1$, lo que tenemos es que $1 + 0 = 1$ y que $0 + 1 = 1$. De esta forma vemos que tres de las cuatro entradas de la tabla de la suma están bien determinadas:

$+$	0	1
0	0	1
1	1	

Ahora bien, todo elemento de $\Bbbk$ tiene que tener un opuesto aditivo. Esto significa lo siguiente: para cada elemento $x \in \Bbbk$ existe otro $y \in \Bbbk$ tal que $x + y = 0$ e $y + x = 0$. En particular, si tomamos $x = 1$, esto nos dice que tiene que haber en $\Bbbk$ un elemento y tal que $1 + y = 0$. Ese elemento y es o 0 o 1, y ya sabemos que $1 + 0 = 1 \neq 0$, así que no puede ser que sea $y = 0$: vemos de esta forma que necesariamente debe ser $y = 1$ y, por lo tanto, que $1 + 1 = 0$. Con esto vemos

que la tabla de la operación de suma de $\Bbbk$ está completamente determinada: tiene que ser

$+$	0	1
0	0	1
1	1	0

Ocupémonos ahora de la multiplicación: tenemos que ver si podemos completar la tabla

$\cdot$	0	1
0		
1		

Sabemos que el elemento 1 es el neutro de la multiplicación. Esto significa que para todo $x \in \Bbbk$ tenemos que $x \cdot 1 = x$ y que $1 \cdot x = x$. Tomando $x = 0$, estas igualdades nos dicen que $0 \cdot 1 = 0$ y que $1 \cdot 0 = 0$; tomando, en cambio, $x = 1$, nos dicen que $1 \cdot 1 = 1$. Podemos así completar tres entradas de la tabla:

$\cdot$	0	1
0		0
1	0	1

Nos queda por ver qué valor puede tener el producto $0 \cdot 0$. Para eso hacemos unas observaciónes que valen, de hecho, en cualquier cuerpo.

Lema 1. *Sea $\mathbb{K}$ un cuerpo. Es $0 \cdot 0 = 0$ y, más generalmente, es $x \cdot 0 = 0$ para cualquier $x \in \mathbb{K}$.*

Proof. Sea $x \in \mathbb{K}$. Sabemos que $0 = 0 + 0$, así que

$$x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0 \tag{1}$$

gracias a la distributividad. El elemento $x \cdot 0$ tiene un opuesto aditivo en $\mathbb{K}$, es decir, existe un elemento $y \in \mathbb{K}$ tal que

$$x \cdot 0 + y = 0. \tag{2}$$

Sumando y a cada lado de la igualdad (1) deducimos que

$$x \cdot 0 + y = (x \cdot 0 + x \cdot 0) + y = x \cdot 0 + (x \cdot 0 + y)$$

y, usando ahora (2), que

$$0 = x \cdot 0 + y = x \cdot 0 + (x \cdot 0 + y) = x \cdot 0 + 0 = x \cdot 0,$$

que es la igualdad que afirma el enunciado. □

La conclusión de todo esto es que si hay un cuerpo $\mathbb{k}$ con dos elementos 0 y 1, entonces sus dos operaciones están necesariamente dadas por las siguientes tablas:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Esto no implica que efectivamente exista un cuerpo con dos elementos: para saber eso necesitamos verificar que $\mathbb{k}$ dotado de estas dos operaciones satisface las condiciones de la definición.

- Las condiciones (K2) y (K6) de conmutatividad de la suma y del producto se satisfacen: para verlo, basta observar que la tablas de las dos operaciones son simétricas con respecto a la diagonal principal.

- La condición (K3) se cumple: hay un elemento neutro para la suma, que es el 0: eso es fácil de determinar en la tabla de la suma. De manera similar, la condición (K7) se cumple: hay un elemento neutro para el producto, el 1.

- La condición (K4) se cumple: todo elemento tiene un upuesto aditivo. Para verlo, es suficiente con ver que en la tabla de la suma en cada columna hay al menos un 0.

- La condición (K8) se cumple: todo elemento no nulo tiene un inverso multiplicativo. En este caso, hay exactamente un elemento no nulo, el 1, y sabemos que $1 \cdot 1 = 1$, así que 1 es su propio inverso multiplicativo.

- La condición (K10) se cumple tautológicamente en este ejemplo, ya que 0 y 1 son dos elementos distintos de $\mathbb{k}$.

- Veamos que se cumple la condición (K1), es decir, que la suma es asociativa. Tenemos que mostrar que para cualquier elección de x, y y z en $\mathbb{k}$ se tiene que
$$(x + y) + z = x + (y + z). \tag{3}$$
Para cada una de x, y y z hay dos posibles valores, así que en principio deberíamos verificar $2^3 = 8$ igualdades. Sin embargo, podemos disminuir el número de casos a considerar.

  - Si $x = 0$, entonces la igualdad vale. En efecto, el valor del lado izquierdo de (3) es
  $$(0 + y) + z = y + z,$$
  mientras que el del lado derecho es
  $$0 + (y + z) = y + z,$$
  así que la igualdad vale.

– Si $y = 0$, entonces la igualdad también vale. El lado izquierdo es ahora

$$(x + 0) + z = x + z$$

mientras que el derecho es

$$x + (0 + z) = x + z.$$

– Finalmente, si $z = 0$, la igualdad vale: el lado izquierdo es en este caso

$$x + (y + 0) = x + y$$

y el derecho

$$(x + y) + 0 = x + y.$$

Hecho esto, vemos que es suficiente probar la igualdad (3) cuando ningun de x, y o z es igual a 0. Esto significa, ya que $\mathbb{k}$ tiene dos elementos, que basta considerar el caso en el que $x = y = z = 1$, y entonces basta calcular que

$$(1 + 1) + 1 = 0 + 1 = 1$$

y que

$$1 + (1 + 1) = 1 + 0 = 1.$$

- Veamos ahora que la multiplicación es asociativa, esto es, que se cumple la condición (K3): hay que mostrar que para cada elección de x, y y z en $\mathbb{k}$ se tiene que

$$(x \cdot y) \cdot z = x \cdot (y \cdot z). \tag{4}$$

Como para la suma, hay dos posibles valores para cada una de las tres letras, así que hay en principio 8 igualdad que considerar, pero podemos hacer una observación similar a la que hicimos arriba: si alguna de las tres letras es igual a 1, elemento neutro de la multiplicación, entonces la igualdad (4) vale. Esto implica que basta verificar que (4) vale cuando $x = y = z = 1$, y para hacerlo es suficiente con calcular que

$$(1 \cdot 1) \cdot 1 = 1 \cdot 1 = 1$$

y que

$$1 \cdot (1 \cdot 1) = 1 \cdot 1 = 1.$$

- Para terminar las verificaciones, tenemos que mostrar que se satisface la condición (K9), es decir, que la multiplicación se distribuye sobre la suma: que cada vez que x, y y z están en $\mathbb{k}$ vale que

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

Ahora bien, si $x = 0$, entonces de acuerdo al Lema 1 el lado izquierdo de esta igualdad es

$$0 \cdot (y + z) = 0$$

y el derecho es

$$0 \cdot y + 0 \cdot z = 0 + 0 = 0.$$

Si, en cambio, es $x = 1$, el lado izquierdo de la igualdad es

$$1 \cdot (y + z) = y + z$$

mientras que el derecho es

$$1 \cdot y + 1 \cdot z = y + z.$$

En cualquier caso, entonces, la igualdad que queremos vale.

La conclusión de todo esto es la siguiente:

Proposición 2. *Hay un cuerpo $\mathbb{k} = \{0, 1\}$ con dos elementos, con operaciones dadas por las siguientes tablas:*

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Más aún, nuestro razonamiento muestra que hay *esencialmente* un único cuerpo con dos elementos: esto es consecuencia de que no tuvimos ninguna opción al construirlo.

2 Un cuerpo con tres elementos

Supongamos que $\mathbb{k}$ es un cuerpo con exactamente tres elementos. Sabemos que en $\mathbb{k}$ hay un elemento 0, neutro para la suma, y un elemento 1, neutro para el producto, y que además, $0 \neq 1$. Como $\mathbb{k}$ tiene tres elementos, entonces sabemos que en $\mathbb{k}$ hay exactamente un elemento que no es ni 0 ni 1: llamémoslo α. Nos proponemos ver qué podemos decir de la suma y de la multiplicación de $\mathbb{k}$.

$+$	0	1	α
0			
1			
α			

$\cdot$	0	1	α
0			
1			
α			

Empezamos estudiando la operación de suma. Como 0 es el elemento neutro de la suma, podemos completar la primera fila y la primera columna:

$+$	0	1	α
0	0	1	α
1	1		
α	α		

Observemos que $1+\alpha$ es distinto de 1 y de α: no es igual a 1, porque de $1+\alpha = 1$ se deduce que $\alpha = 0$, lo que es falso, y de $1 + \alpha = \alpha$ se deduce que $1 = 0$, lo que también es falso. Vemos así que

$$1 + \alpha = 0.$$

Con esto, la tabla queda en la forma

$+$	0	1	α
0	0	1	α
1	1		0
α	α	0	

(5)

Para completarla, hacemos la siguiente observación:

Lema 3. *Sea $\mathbb{K}$ un cuerpo.*

(*i*) *Si x, x', $y \in \mathbb{K}$ son tales que $x + y = x' + y$, entonces $x = x'$.*

(*ii*) *En la tabla de la operación $+$ no hay elementos repetidos en ninguna columna ni en ninguna fila.*

Proof. Si x, x', $y \in \mathbb{K}$ son tales que $x + y = x' + y$ y z es el opuesto de y, de manera que $y + z = 0$, entonces

$$\begin{aligned} x = x + 0 = x + (y + z) = (x + y) + z = (x' + y) + z \\ = x' + (y + z) = x' + 0 = x'. \end{aligned}$$

Esto prueba la primera afirmación del lema. La segunda es simplemente una forma alternativa de enunciarla. □

Si miramos ahora la segunda columna de la tabla (5), vemos que el ligar vacío no pude ser llenado con 1 o con 0, porque eso iría en contra de la conclusión del lema que acabamos de probar, así que tiene que ir ahí α. De la misma forma, el ligar vacío de la tercera columna necesariamente tiene que estar ocupado con un 1. Como conclusión de esto, la tabla de la suma es

$+$	0	1	α
0	0	1	α
1	1	α	0
α	α	0	1

Veamos ahora la tabla de la multiplicación. Sabemos que 1 es el elemento neutro del producto y tenemos el Lema 1, así que podemos completar hasta obtener

$\cdot$	0	1	α
0	0	0	0
1	0	1	α
α	0	α	

(6)

Nos queda solamente ver qué podemos decir del valor de $\alpha \cdot \alpha$. Podemos hacer una observación parecida a la que hicimos para la suma:

Lema 4. *Sea $\mathbb{K}$ un cuerpo.*

(*i*) *Si x e y son elementos de $\mathbb{K}$ distintos de 0, entonces $x \cdot y$ es distinto de 0.*

(*ii*) *Si x, x', $y \in \mathbb{K}$ son distintos de 0 y tales que $x \cdot y = x' \cdot y$, entonces $x = x'$.*

(*iii*) *En la tabla de la operación* $\cdot$*, una vez que sacamos la fila y la columna que corresponden al* 0*, no hay elementos repetidos en ninguna columna ni en ninguna fila.*

Proof. (*i*) Supongamos que x e y son elementos de $\mathbb{K}$ distintos de 0 y sea z el inverso de y, de manera que $y \cdot y = 1$. Si fuese $x \cdot y = 0$ tendríamos que

$$0 = 0 \cdot z = (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot 1 = x,$$

lo que es absurdo.

(*ii*) Si x, x', $y \in \mathbb{K}$ son no nulos y tales que $x \cdot y = x' \cdot y$ y z es el inverso de y, de manera que $y \cdot z = 1$, entonces

$$\begin{aligned} x &= x \cdot 1 = x \cdot (y \cdot z) = (x \cdot y) \cdot z = (x' \cdot y) \cdot z \\ &= x' \cdot (y \cdot z) = x' \cdot 1 = x'. \end{aligned}$$

(*iii*) Esta afirmación es simplemente una forma alternativa de enunciar la parte (*ii*). □

Usando este lema, vemos que hay una única forma posible de completar la tabla (6): como $\alpha \neq 0$, la primera parte del lema nos dice que $\alpha \cdot \alpha \neq 0$ y como no puede haber repeticiones, vemos que necesariamente $\alpha \cdot \alpha = 1$. Vemos así que la tabla completa es:

$\cdot$	0	1	α
0	0	0	0
1	0	1	α
α	0	α	1

Esto nos lleva al siguiente resultado:

Proposición 5. *Hay un cuerpo* $\Bbbk = \{0, 1, \alpha\}$ *con tres elementos, con operaciones dadas por las siguientes tablas:*

$+$	0	1	α
0	0	1	α
1	1	α	0
α	α	0	1

$\cdot$	0	1	α
0	0	0	0
1	0	1	α
α	0	α	1

Proof. Hay que mostrar que efectivamente el conjunto $\{0, 1, \alpha\}$ de tres elementos y esas dos operaciones es un cuerpo. Que la suma es conmutativa, posee un elemento neutro, y que cada elemento posee un opuesto, por un lado, y que la multiplicación es conmutativa, posee un elemento neutro, y que cada elemento no nulo posee un inverso puede verificarse inmediatamente mirando las tablas de las dos operaciones. Que las dos operaciones son asociativas y que la multiplicación se distribuye sobre la suma es algo que puede verse por un cálculo directo. □

3 Un cuerpo con cuatro elementos

Empecemos con un par de observaciones sencillas.

Lema 6. *Sea $\mathbb{K}$ un cuerpo.*
(i) Si $u \in \mathbb{K}$, entonces $-(-u) = u$.
(ii) Si $u \in \mathbb{K}$ no es nulo, entonces $-u$ tampoco lo es.

Proof. (i) Sea $u \in \mathbb{K}$. Queremos mostrar que $-(-u) = u$, esto es, que u es el elemento opuesto de $-u$ y para ello es suficiente con probar que la suma de u y $-u$ es nula: esto es evidente, porque el segundo de estos elementos es el opuesto del primero.

(ii) Si $u \in \mathbb{K}$ es tal que $-u = 0$, entonces $0 = u + (-v) = u + 0 = u$. □

Supongamos ahora que $\Bbbk$ es un cuerpo con 4 elementos. Dos de ellos son el cero 0, neutro de la suma, y el 1, neutro del producto, y sabemos que $1 \neq 0$. Queremos ver que en $\Bbbk$ se tiene que

$$1 + 1 = 0. \tag{7}$$

Supongamos que no es así. Esto significa, precisamente, que $-1 \neq 1$. Sabemos que 1 y -1 son elementos no nulos de $\Bbbk$ y $\Bbbk$ tiene exactamente *tres* elementos no nulos: sea x el restante elemento no nulo de $\Bbbk$, de manera que los elementos no nulos de $\Bbbk$ son 1, -1 y x.

Ahora bien, como x no es nulo, su opuesto $-x$ tampoco lo es, y debe ser igual a alguno de 1, -1 o x.

- Si fuese $-x = 1$, entonces $x = -(-x) = -1$, contra la forma en que elegimos a y.
- De manera similar, si fuese $-x = -1$, entonces $x = -(-x) = -(-1) = 1$, lo que es absurdo.

Vemos de esta forma que necesariamente se tiene que $-x = x$ o, en otras palabras, que $x + x = 0$. Ahora bien, esto implica que

$$0 = x + x = x \cdot 1 + x \cdot 1 = x \cdot (1 + 1).$$

Como x no es nulo y el producto $x \cdot (1+1)$ sí lo es, vemos que necesariamente se tiene que $1+1 = 0$: esto contradice nuestra hipótesis. Esto implica que vale (7), como queríamos.

Más generalmente, de (7) se deduce fácilmente que

$$\textit{para cada } u \in \mathbb{K} \textit{ se tiene que } u + u = 0.$$

En efecto, si $u \in \mathbb{K}$, entonces podemos calcular que

$$u + u = u \cdot 1 + u \cdot 1 = u \cdot (1 + 1) = u \cdot 0 = 0.$$

Llamemos α y β a los dos elementos de $\mathbb{k}$ que no son 0 ni 1. Con la información que tenemos hasta ahora más el hecho de que 0 es el elemento neutro de la suma, podemos completar la tabla de la suma hasta obtener lo siguiente:

$+$	0	1	α	β
0	0	1	α	β
1	1	0		
α	α		0	
β	β			0

Queremos ahora saber saber el valor de $1+\alpha$: en la fila del 1 en esta tabla aparecen 0 y 1, y en la columna de α aparece α, así que ninguno de esos tres elementos puede ser igual a $1+\alpha$. La única posibilidad que queda, entonces, es que sea $1+\alpha=\beta$.

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	
α	α		0	
β	β			0

Mirando ahora la fila del 1, vemos que el lugar vacío sólo puede ser completado con α, porque en esa fila no puede haber repeticiones.

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α		0	
β	β			0

Ahora mirando la columna correspondiente a β y porque no puede haber allí repeticiones, el lugar vacío claramente tiene que ser ocupado con 1. Hecho eso y usando la conmutatividad de la suma podemos completar la tabla:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

Pasemos ahora a la multiplicación. Usando el Lema 1 y el hecho de que 1 es el elemento neutro para el producto, llegamos a lo siguiente:

$+$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α		
β	0	β		

Veamos cuánto puedo valer $\alpha\cdot\alpha$. Como $\alpha\neq 0$, ese producto no es nulo y entonces es o 1, o α, o β.

- Si es igual a 1, entonces

$$\begin{aligned}\beta \cdot \beta = (1+\alpha)(1+\alpha) &= 1 \cdot 1 + 1 \cdot \alpha + \alpha \cdot 1 + \alpha \cdot \alpha \\ &= 1 + \alpha + \alpha + 1 = 0,\end{aligned}$$

  lo que es absurdo porque $\beta \neq 0$.

- Si es igual a α, entonces

$$\alpha \cdot \beta = \alpha \cdot (\alpha + 1) = \alpha \cdot \alpha + \alpha \cdot 1 = \alpha + \alpha = 0,$$

  lo que es absurdo ya que $\alpha \neq 0$ y $\beta \neq 0$.

La única posibilidad, entonces, es que sea $\alpha \cdot \alpha = \beta$.

$+$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	
β	0	β		

Miremos ahora la tabla que queda cuando borramos la fila y la columna que corresponden a 0: sabemos que las filas y columnas de esa subtabla ni tienen repeticiones. Es claro, entonces, que tiene que ser $\alpha \cdot \beta = 1$ y, usando eso, que $\beta \cdot \beta = \alpha$. Estas observaciones y la conmutatividad del producto completan la tabla. Haciendo eso, llegamos al siguiente resultado:

Proposición 7. *Hay un cuerpo $\Bbbk = \{0, 1, \alpha, \beta\}$ con cuatro elementos, con operaciones dadas por las siguientes tablas:*

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$+$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Proof. Hay que verificar que efectivamente estas tablas hacen del conjunto $\Bbbk$ un cuerpo. Todas las condiciones se verificar inmediatamente mirándolas salvo, como siempre, la asociatividad de la suma y del producto, y la ley distributiva, que requieren una verificación directa. □

4 Un cuerpo con cinco elementos

Sea $\Bbbk$ un cuerpo con 5 elementos. Para cada $n \in \mathbb{N}$ consideremos en $\Bbbk$ el elemento

$$u_n = \underbrace{1 + \cdots + 1}_{n \text{ sumandos}}$$

que se obtiene sumando n veces el elemento 1 con si mismo, y pongamos además $u_0 = 0$. Podemos armar sucesión

$$u_1, u_2, u_3, u_4, \dots \tag{8}$$

Como $\Bbbk$ tiene solo 5 elementos y esta sucesión tiene infinitos términos, es claro que en la sucesión tiene que haber repeticiones: esto es, existen dos enteros distintos r, $s \in \mathbb{N}$ tales que $u_r = u_s$, y sin pérdida de generalidad podemos suponer que $r < s$. En ese caso, tenemos que

$$0 = u_s - u_r = \underbrace{(1 + \cdots + 1)}_{s \text{ sumandos}} - \underbrace{(1 + \cdots + 1)}_{r \text{ sumandos}} = \underbrace{(1 + \cdots + 1)}_{s - r \text{ sumandos}} = u_{s-r}.$$

Esto nos dice que el elemento 0 de $\Bbbk$ aparece por lo menos una vez en la sucesión (8). Escribamos p al *menor* elemento de $\mathbb{N}$ tal que $u_p = 0$ y consideremos los p elementos de $\Bbbk$

$$u_0, u_1, u_2, \dots, u_{p-1}. \tag{9}$$

Estos p elementos son distintos dos a dos. En efecto, si no fuese ese el caso, habría dos enteros i y j tales que $0 \leq i < j < p$ tales que $u_i = u_j$. Por la forma en que elegimos p, sabemos que los elementos u_1, …, u_{p-1} no son nulos, así que tiene que ser $i > 0$ y entonces tenemos que

$$0 = u_j - u_i = \underbrace{(1 + \cdots + 1)}_{j \text{ sumandos}} - \underbrace{(1 + \cdots + 1)}_{i \text{ sumandos}} = -\underbrace{(1 + \cdots + 1)}_{j - i \text{ sumandos}} = u_{j-i}.$$

Esto es absurdo, ya que $0 < j - i < p$ y ninguno de los últimos $p - 1$ elemetos de la lista (9) es nulo.

Si $i \in \{0, \dots, p-1\}$, entonces

$$u_i + u_{p-i} = \underbrace{(1 + \cdots + 1)}_{i \text{ sumandos}} + \underbrace{(1 + \cdots + 1)}_{p - i \text{ sumandos}} = \underbrace{1 + \cdots + 1}_{p \text{ sumandos}} = u_p = 0,$$

así que

$$-u_i = u_{p-i}.$$

Esto nos dice que el opuesto de un elemento de la lista (9) aparece en esa misma lista. Vamos a usar esto más abajo.

Supongamos que los p elementos de $\Bbbk$ listados en (9) no son todos los elementos de $\Bbbk$. Esto implica que existe un elemento $x_1 \in \Bbbk$ que no aparece en la lista (9). Más aún, en vista de nuestra observación de arriba, $-x_1$ tampoco aparece en esa lista: si apareciese, entonces $-(-x_1)$ también estaría en la lista y este elemento es x_1.

Afirmamos que los $2p$ elementos

$$\begin{array}{llllll} u_0, & u_1, & u_2, & \dots, & u_{p-1} \\ x_1 + u_0, & x_1 + u_1, & x_1 + u_2, & \dots, & x_1 + u_{p-1}. \end{array} \tag{10}$$

son distintos dos a dos.

- Sabemos ya que los primeros p son distintos dos a dos.
- Supongamos dos de los elementos del segundo renglón son iguales entre sí, de manera que hay enteros i y j tale que $0 \leq i < j < p$ y $x_1 + u_i = x_1 + u_j$. Claramente se tiene entonces que $u_i = u_j$ y sabemos que esto es imposible.
- Finalmente, supongamos que un elemento del primer renglón es igual a alguno del segundo, de manera que existen enteros i, $j \in \{0, \ldots, p-1\}$ tales que $u_i = x_1 + u_j$. Si $i > j$, esto nos dice que $x_1 = u_j - u_i = u_{j-i}$, lo que es absurdo porque elegimos a x_1 de manera que no aparezca en la lista (9). Si en cambio es $i < j$, tenemos que $x_1 = u_i - u_j = -u_{j-i}$, lo que también es imposible.

En la lista (10) hay $2p$ elementos distintos dos a dos: no pueden ser todos los de $\Bbbk$, porque $\Bbbk$ tiene 5 elementos y $2p \neq 5$: esto implica que existe un elemento x_2 en $\Bbbk$ que no aparece en la lista (10). Razonando exactamente como antes podemos verificar ahora que los $3p$ elementos de la lista

$$\begin{array}{llll} u_0, & u_1, & u_2, & \ldots, \quad u_{p-1} \\ x_1 + u_0, & x_1 + u_1, & x_1 + u_2, & \ldots, \quad x_1 + u_{p-1}, \\ x_2 + u_0, & x_2 + u_1, & x_2 + u_2, & \ldots, \quad x_2 + u_{p-1} \end{array}$$

son distintos dos a dos. Otra vez, como $3p \neq 5$, estos $3p$ elementos no pueden ser todos los de $\Bbbk$ y tiene que existir un elemento $x_3 \in \Bbbk$ que no está lista aquí... Claramente este procedimiento puede continuarse indefinidamente: esto es absurdo, ya que $\Bbbk$ tiene solamente 5 elementos!

Esta contradicción nos dice que nuestra hipótesis no puede ser cierta y, por lo tanto, que los p elementos

$$u_0, u_1, u_2, \ldots, u_{p-1},$$

que son distintos dos a dos, son *todos* los elementos de $\Bbbk$. En particular, vemos de esta forma que $p = 5$, claro.

Con esta información podemos determinar completamente la tabla de sumar de $\Bbbk$. Supongamos que i y j son dos elementos de $\{0, \ldots, 4\}$. Es claro que $u_i + u_j = u_{i+j}$. Si $0 \leq i+j < 5$, entonces u_{i+j} es uno de los 5 elementos listados arriba. Si no, entonces claramente $5 \leq i+j < 9$, de manera que $0 \leq i+j-5 < 4$ y

$$u_i + u_j = u_5 + u_{i+j-5} = u_{i+j-5}$$

es otra vez uno de los 5 elementos de nuestra lista. La tabla de sumar de $\Bbbk$ debe ser, entonces, la siguiente:

$+$	u_0	u_1	u_2	u_3	u_4
u_0	u_0	u_1	u_2	u_3	u_4
u_1	u_1	u_2	u_3	u_4	u_0
u_2	u_2	u_3	u_4	u_0	u_1
u_3	u_3	u_4	u_0	u_1	u_2
u_4	u_4	u_0	u_1	u_2	u_3

De manera similar, la información que tenemos determina de manera completa la tabla de multiplicar de $\Bbbk$. Veamos un ejemplo: calculemos $u_3 \cdot u_4$. Es

$$u_3 \cdot u_4 = (\underbrace{1 + \cdots + 1}_{3 \text{ sumandos}})(\underbrace{1 + \cdots + 1}_{4 \text{ sumandos}})$$

Si distribuimos este producto y luego agrupamos convenientemente términos, vemos que

$$u_3 \cdot u_4 = \underbrace{1 + \cdots + 1}_{12 \text{ sumandos}} = u_{12} = u_5 + u_5 + u_2 = u_2$$

ya que $u_5 = 0$. Procediendo de esta forma, obtenemos la siguiente tabla.

$+$	u_0	u_1	u_2	u_3	u_4
u_0	u_0	u_0	u_0	u_0	u_0
u_1	u_0	u_1	u_2	u_3	u_4
u_2	u_0	u_2	u_4	u_1	u_3
u_3	u_0	u_3	u_1	u_4	u_2
u_4	u_0	u_4	u_3	u_2	u_1

Todo esto nos dice que hay a lo sumo *un* cuerpo de 5 elementos, ya que no hubo ninguna alternativa en el proceso de determinación de estas dos tablas. Puede verificarse que efectivamente de esta forma obtenemos un cuerpo.

5 Un cuerpo con un número primo de elementos

Lo que hicimos en la sección anterior no dependió demasiado de que el cuerpo tuviera exactamente 5 elementos sino más bien de que el número 5 es primo.

Supongamos que $\Bbbk$ es un cuerpo con ℓ elementos y que el número ℓ es primo. Como antes, para cada $n \in \mathbb{N}$ escribamos

$$u_n = \underbrace{1 + \cdots + 1}_{n \text{ sumandos}}$$

al elemento de $\Bbbk$ que se obtiene sumando n veces a 1 con sí mismo, y pongamos $u_0 = 0$. La lista

$$u_1, u_2, u_3, u_4, \ldots \tag{11}$$

es infinita y sus elementos son todos elementos de $\Bbbk$, así que tiene que haber repeticiones: existen dos enteros r y s tales que $1 \leq r < s$ y $u_r = u_s$, y entonces

$$u_{r-s} = \underbrace{1 + \cdots + 1}_{r-s \text{ sumandos}} = (\underbrace{1 + \cdots + 1}_{r \text{ sumandos}}) - (\underbrace{1 + \cdots + 1}_{s \text{ sumandos}}) = u_r - u_s = 0.$$

Esto significa que en la lista (11) aparece el cero de $\Bbbk$: llamemos p al *menor* entero positivo tal que $u_p = 0$. Podemos entonces considerar los p elementos

$$u_0, u_1, \ldots, u_{p-1} \tag{12}$$

de $\Bbbk$. Estos son distintos dos a dos, y el opuesto de cada uno de ellos aparece también en la lista: la verificación de estas dos afirmaciones puede hacerse exactamente igual que en la sección anterior. Más aún, veamos que la suma de dos elementos de la lista (12) también aparece en esa lista. Sean i y j dos enteros tales que $0 \leq i, j < p$. Si alguno de i o j es igual a 0, digamos i, entonces $u_i = 0$ y $u_i + u_j = u_j$, que aparece en la lista. Supongamos entonces que tanto i como j son distintos de 0. En ese caso tenemos que

$$u_i + u_j = (\underbrace{1 + \cdots + 1}_{i \text{ sumandos}}) + (\underbrace{1 + \cdots + 1}_{j \text{ sumandos}}) = \underbrace{1 + \cdots + 1}_{i+j \text{ sumandos}}$$

Si $i + j < p$, entonces claramente tenemos que $u_i + u_j = u_{i+j}$, que aparece en (12). Si $i + j \geq p$, en entonces como tanto i como j son menores que p tenemos que $i + j - p < p$, y

$$\begin{aligned} u_i + u_j &= \underbrace{1 + \cdots + 1}_{i+j \text{ sumandos}} = (\underbrace{1 + \cdots + 1}_{p \text{ sumandos}}) + (\underbrace{1 + \cdots + 1}_{i+j-p \text{ sumandos}}) \\ &= u_p + u_{i+j-p} = u_{i+j-p}, \end{aligned}$$

ya que $u_p = 0$.

Queremos ahora mostrar que los p elementos listados en (12) son todos los elementos de $\Bbbk$. Con ese fin, y para llegar a una contradicción, supondremos que, por el contrario, no es ese el caso.

Para cada entero positivo $m \in \mathbb{N}$ sea $P(m)$ la afirmación

«existen elementos $x_1, \ldots, x_m$ en $\Bbbk$ tales que los $m \cdot p$ elementos

$$\begin{array}{llllll} x_1 + u_0, & x_1 + u_1, & x_1 + u_2, & \ldots, & x_1 + u_{p-1}, \\ x_2 + u_0, & x_2 + u_1, & x_2 + u_2, & \ldots, & x_2 + u_{p-1}, \\ x_3 + u_0, & x_2 + u_3, & x_3 + u_2, & \ldots, & x_3 + u_{p-1}, \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_m + u_0, & x_m + u_3, & x_m + u_2, & \ldots, & x_m + u_{p-1} \end{array}$$

son distintos dos a dos pero no son todos los elementos de $\Bbbk$».

Observemos que la afirmación $P(1)$ vale: si tomamos $x_1 = 0$, entonces sabemos que los $1 \cdot p$ elementos

$$x_1 + u_0, \quad x_1 + u_1, \quad x_1 + u_2, \quad \ldots, \quad x_1 + u_{p-1}$$

son distintos dos a dos y estamos suponiendo que no son todos los elementos del cuerpo $\Bbbk$.

Supongamos ahora que m es un elemento arbitrario de $\mathbb{N}$ y que vale la afirmación $P(m)$, de manera que hay elementos $x_1, \ldots, x_n$ en $\Bbbk$ tales que los

$m \cdot p$ elementos

$$\begin{array}{lllll} x_1+u_0, & x_1+u_1, & x_1+u_2, & \ldots, & x_1+u_{p-1}, \\ x_2+u_0, & x_2+u_1, & x_2+u_2, & \ldots, & x_2+u_{p-1}, \\ x_3+u_0, & x_2+u_3, & x_3+u_2, & \ldots, & x_3+u_{p-1}, \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_m+u_0, & x_m+u_3, & x_m+u_2, & \ldots, & x_m+u_{p-1} \end{array}$$

son distintos dos a dos pero no son todos los elementos de $\Bbbk$. En particular, existe un elemento de $\Bbbk$ que no está en esta lista: llamémoslo x_{m+1}. Consideremos ahora los $(m+1)p$ elementos

$$\begin{array}{lllll} x_1+u_0, & x_1+u_1, & x_1+u_2, & \ldots, & x_1+u_{p-1}, \\ x_2+u_0, & x_2+u_1, & x_2+u_2, & \ldots, & x_2+u_{p-1}, \\ x_3+u_0, & x_2+u_3, & x_3+u_2, & \ldots, & x_3+u_{p-1}, \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_m+u_0, & x_m+u_3, & x_m+u_2, & \ldots, & x_m+u_{p-1}, \\ x_{m+1}+u_0, & x_{m+1}+u_3, & x_{m+1}+u_2, & \ldots, & x_{m+1}+u_{p-1}. \end{array} \tag{13}$$

Sabemos que entre los pm elementos de las primeras m filas de esta lista no hay repeticiones. Por otro lado, dos elementos de la última fila no pueden ser iguales: si hubiera enteros i y j tales que $0 \leq i < j < p$ y $x_{m+1}+u_i = x_{m+1}+u_j$, entonces tendríamos que $u_i = u_j$, lo que es imposible, ya que sabemos que en la lista (12) no hay repeticiones.

Queda la posibilidad que un elemento de las primeras m filas de a tabla sea igual a alguno de la última fila, es decir, que existan i, j y k tales que $0 \leq i, j < p$ y $1 \leq k \leq m$ tales que $x_k + u_i = x_{m+1} + u_j$. Pero en ese caso tendríamos que

$$x_{m+1} = x_k + (u_i - u_j),$$

Sabemos que $-u_j$ es uno de los elementos de la lista (12) y, entonces, que tambiñen lo es la suma $u_i+(-u_j) = u_i-u_j$: esto significa que existe $l \in \{0, \ldots, p-1\}$ tal que $u_i - u_j = u_l$. Pero entonces lo que tenemos es que $x_{m+1} = x_k + u_l$, lo que es absurdo en vista de la forma en que elegimos al elemento x_{m+1}.

Vemos de esta forma que los $(m+1)p$ elementos listados en (13) son distintos dos a dos. Como el número $(m+1)p$ no es primo, no puede ser igual a ℓ, el cardinal de $\Bbbk$: esto significa que es *menor* que ℓ y, por lo tanto, que los $(m+1)p$ elementos listados en (13) no son todos los elementos de $\Bbbk$.

Hemos probado con todo esto que para cada $m \in \mathbb{N}$ vale la implicación $P(m) \implies P(m+1)$. Como además vale la afirmación $P(1)$, el principio de inducción nos dice que vale la afirmación $P(m)$ cualquiera sea el elemento m de $\mathbb{N}$. Esto es absurdo: en efecto, existe $n \in \mathbb{N}$ tal que $np > \ell$, y como la

afirmación $P(n)$ vale sabemos que los np elementos

$$\begin{array}{llllll} x_1+u_0, & x_1+u_1, & x_1+u_2, & \dots, & x_1+u_{p-1}, \\ x_2+u_0, & x_2+u_1, & x_2+u_2, & \dots, & x_2+u_{p-1}, \\ x_3+u_0, & x_2+u_3, & x_3+u_2, & \dots, & x_3+u_{p-1}, \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n+u_0, & x_n+u_3, & x_n+u_2, & \dots, & x_n+u_{p-1} \end{array}$$

de $\Bbbk$ son distintos dos a dos. Por supuesto, esto implica que, en particular, el cuerpo $\Bbbk$ tiene al menos np elementos: esto es imposible, ya que $np > \ell$.

Esta contradicción provino de haber supuesto, como hicimos arriba, que los elementos listados en (12) no son todos los elementos de $\Bbbk$. Vemos así que sí, son todos. Como además en esa lista no hay repeticiones, es claro que el número p tiene que coincidir con el cardinal ℓ de $\Bbbk$.

La conclusión de todo esto es que los elementos del cuerpo $\Bbbk$ son precisamente los ℓ elementos

$$u_0, u_1, \dots, u_{\ell-1}.$$

Procediendo ahora como en la sección anterior podemos determinar completamente las operaciones de $\Bbbk$. Si i y j son elementos de $\{0, \dots, \ell-1\}$, entonces sabemos que existen enteros r y s, también elementos de $4\{0, \dots, \ell-1\}$, tales que

$$i + j \equiv r \mod \ell, \qquad i \cdot j \equiv s \mod \ell$$

y, más aún, que r y s están unívocamente determinados por i y j. Es fácil verificar que en $\Bbbk$ se tiene que

$$u_i + u_j = u_r, \qquad u_i \cdot u_j = u_s.$$

Esto muestra —ya que toda la estructura del cuerpo está completamente determinada una vez que conocemos su cardinal ℓ— que hay esencialmente *a lo sumo* un cuerpo con ℓ elementos. Podría pasar, sin embargo, que no haya ninguno! La siguiente proposición nos dice que esto, en realidad, no ocurre:

Proposición 8. *Para cada número primo ℓ existe un cuerpo $\Bbbk$ con exactamente ℓ elementos.*

Proof. Sea ℓ un número primo y sea $\equiv$ la relación de congruencia módulo ℓ en $\mathbb{Z}$, de manera que si a y b son dos elementos de $\mathbb{Z}$ se tiene que

$$a \equiv b \iff \exists c \in \mathbb{Z} : a - b = \ell c.$$

Para cada $a \in \mathbb{Z}$ escribamos $[a]$ a la clase de equivalencia de a co respecto a esta relación y escribamos $\Bbbk$ al conjunto de todas las clases de equivalencia de $\equiv$ en $\mathbb{Z}$. Sabemos que $\Bbbk$ tiene exactamente ℓ elementos, a saber, las clases de equivalencia

$$[0], [1], [2], \dots, [\ell-1].$$

Es fácil verificar que hay dos operaciones $\oplus, \otimes : \Bbbk \times \Bbbk \to \Bbbk$ tales que para cada para de elementos a y b de $\mathbb{Z}$ se tiene que

$$[a] \oplus [b] = [a + b], \qquad [a] \otimes [b] = [ab].$$

Afirmamos que $(\Bbbk, \oplus, \otimes)$ es un cuerpo, en el que el cero y el uno son, respectivamente, las clases $[0]$ y $[1]$. Todas las condiciones necesarias para establecer esta afirmación se verifican de manera casi inmediata, salvo la aquella que pide la existencia de inversos multiplicativos. Ocupémonos de ella.

Sea α un elemento de $\Bbbk$ distinto del 0. Como α es una clase de equivalencia, existe $a \in \mathbb{Z}$ ta que $\alpha = [a]$. Más aún, como $\alpha \neq [0]$, tenemos que $a \not\equiv 0$, es decir, que ℓ no divide a a o, como ℓ es un número primo, que a y ℓ son coprimos. existen entonces enteros r y s tales que $ra + s\ell = 1$. Se sigue de esa igualdad inmediatamente que $ra \equiv 1$ y, por lo tanto, que

$$\alpha \otimes [r] = [a] \otimes [r] = [ra] = [1],$$

de manera que la clase $[r]$ es un inverso para α en $\Bbbk$. □

Esta proposición nos da cuerpos de cardinal primo, pero vimos en la Sección 3 que también hay cuerpos de cardinales que no son primos. El resultado final en esta dirección es el siguiente:

Proposición 9.

(*i*) *Para cada número primo p y cada entero positivo n existe un cuerpo $\mathbb{F}_{p^n}$ con p^n elementos, y esencialmente uno solo.*

(*ii*) *Si $\Bbbk$ es un cuerpo con finitos elementos y ℓ es su cardinal, entonces hay un número primo p y un entero positivo n tales que $\ell = p^n$.*

La prueba de esto requiere herramientas que todavía no tenemos.