Juan Manuel Mateos Pérez

Cuerpo con 9 elementos y tabla de multiplicar

Si nos damos cuenta, $9 = 3^2$, donde:

- El 3 nos indica que debemos trabajar en $\mathbb{Z}_3[x]$
- El 2 nos indica el grado del polinomio irreducible $r(x) = x^2 - x - 1$. (Me he tomado este polinomio en lugar de tomarme x^2+1 o x^2+x-1, perfectamente válidos, ya que estos polinomios No tienen raices $\Rightarrow$irreducibles)

Para definir un cuerpo necesitamos un conjunto y 2 operaciones.

- El conjunto está formado por polinomios de $\mathbb{Z}_3[x]$ con grado menor o igual que 2.

$$K_9 = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$$

- La primera operación es la suma habitual de polinomios, definida como:

$$+ : K_9 \times K_9 \longrightarrow K_9$$
$$(p(x), q(x)) \longmapsto p(x) + q(x)$$

Veamos ahora que cumple las propiedades necesarias para ser grupo:

1) Es una operación binaria interna: la suma de dos elementos pertenece al conjunto tal y como vamos a ver.
2) Es asociativa: al ser la suma habitual de polinomios.
3) Existe elemento neutro: al ser la suma habitual, el el neutro es el 0 y este elemento, está en K_9.
4) Existe elemento simétrico: veamos mediante la tabla que todos los elementos tienen simétricos.
5) Es conmutativo: al ser suma habitual de polinomios.

Por tanto $(K_9, +)$ es un grupo conmutativo.

+	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
1		2	3	x+1	x+2	x	2x+1	2x+2	2x
2			1	x+2	x	x+1	2x+2	2x	2x+1
x				2x	2x+1	2x+2	0	1	2
x+1					2x+2	2x	1	2	0
x+2						2x+1	2	0	1
2x							x	x+1	x+2
2x+1								x+2	x
2x+2									x+1

•) Definimos el producto como:

$$\odot : K_q \times K_q \longrightarrow K_q$$
$$(p(x), q(x)) \longmapsto p(x)\cdot q(x) \bmod r(x)$$

$r(x) = x^2 - x - 1$

El producto No puede ser el producto de polinomios usual ya que no es interno.

Veamos ahora que $(K_q, \odot)$ es un monoide:

1) Asociatividad:

$(p(x) \odot q(x)) \odot s(x) = (p(x)\cdot q(x) \bmod r(x)) \odot s(x)$

$= (p(x)\cdot q(x) \bmod r(x))\cdot s(x) \bmod r(x)$

$= p(x)\, q(x)\cdot s(x) \bmod r(x)$

$= p(x)\cdot (q(x)\cdot s(x) \bmod r(x)) \bmod r(x)$

$= p(x) \odot (q(x) \odot r(x))$

2) Es una operación interna tal y como podemos ver en la tabla de multiplicación.

3) El neutro: el elemento neutro es el 1 y pertenece a K_q

Veamos que es un anillo:

$$s(x) \odot (p(x) + q(x)) = s(x)(p(x)+q(x)) \bmod r(x)$$

$$= (s(x)\cdot p(x) + s(x)\,q(x)) \bmod r(x)$$

$$= s(x)\,p(x) \bmod r(x) + s(x)\,q(x) \bmod r(x)$$

$$= s(x) \odot p(x) + s(x) \odot q(x)$$

Analogamente

$$(p(x) + q(x)) \odot s(x) = p(x) \odot s(x) + q(x) \odot s(x)$$

Por lo que la prop. distributiva también se da.

Así, $(K_q, +, \odot)$ es un anillo, y como ahora veremos, todo elemento tiene inverso, por tanto $(K_q, +, \odot)$ es un cuerpo.

$\odot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1		1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2			1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x				$x+1$	$x+2$	1	$2x+2$	2	$x+2$
$x+1$					2	x	$x+2$	$2x$	1
$x+2$						$2x+2$	2	$x+1$	$2x$
$2x$							$x+1$	1	$2x+1$
$2x+1$								$2x+1$	x
$2x+2$									2