Teorema: Para $f \in F[x]$ el anillo de clases residuales $F[x]/(f)$ es un cuerpo si y solo si f es irreducible en $F[x]$.

Como las clases $[g(x)] \in F[x]/(f)$ corresponden a

$$[g(x)] = \{ g(x) + p(x) \cdot f(x) : p(x) \in F[x] \}$$

hay un único representante $r(x) \in F[x]$ con $\deg r < \deg f$ que es justamente el resto de dividir a $g(x)$ por $f(x)$.

(algoritmo de la división)

Entonces podemos "describir" a $F[x]/(f)$ como el conjunto de polinomios en $F[x]$ de grado menor al grado de f.

Entonces si $\deg f = n \geq 0$ y $F = \mathbb{F}_p$ entonces el número de elementos de $\mathbb{F}_p[x]/(f)$ es el número de polinomios de la forma

$$a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \qquad a_0, \dots, a_{n-1} \in \mathbb{F}_p$$

es decir hay p^n elementos.

$p=2$

Ejemplo: Consideremos $F=\mathbb{F}_2=\{0,1\}$ y $f(x)=x+1$

$2^1=2$ elementos. $n=\deg f=1$

$\mathbb{F}_2[x]/(x+1)$ es un cuerpo.

$\deg(x+1)=1$ entonces si $[g(x)]\in \mathbb{F}_2[x]/(x+1)$ debe ser que $\deg g<0$.

Luego $[0]=\{p(x)(x+1) : p(x)\in\mathbb{F}_2[x]\}$

$[1]=\{p(x)(x+1)+1 : p(x)\in\mathbb{F}_2[x]\}$

Entonces $\mathbb{F}_2[x]/(x+1) \underset{\text{isomorfo}}{\simeq} \mathbb{F}_2$.

Ejemplo: $F = \mathbb{F}_2$ y $f(x) = x^3 + x^2 + 1$ $p=2$ $n=3$

$\mathbb{F}_2[x]/(f)$ un cuerpo con $2^3 = 8$ elementos.

$[g(x)] \in \mathbb{F}_2[x]/(f)$ si $g(x) = a_0 + a_1 x + a_2 x^2$

$a_0, a_1, a_2 \in \mathbb{F}_2$.

$$\{ [0], [1], [x], [x+1], [x^2], [x^2+1], [x^2+x], [x^2+x+1] \}$$

(x^3 sobre $[x^2+1]$; x^4 sobre $[x^2+x+1]$)

Ejercicio: construir las tablas de la suma y producto y verificar que $\mathbb{F}_2[x]/(f)$ es un cuerpo y por lo tanto que f es irreducible.

Ejemplo: $[x^2+1] + [x^2+x+1] =$

$= [x^2+1+x^2+x+1] =$

$= [\underbrace{2}_{0}x^2 + x + \underbrace{2}_{0}] = [x]$

$\mathbb{F}_2$: $1+1 = 2 = 0$

$[x^2+1] \cdot [x^2+x+1] = [(x^2+1)\cdot(x^2+x+1)] =$

$= [x^4 + x^3 + x^2 + x^2 + x + 1] =$

$= [x^4 + x^3 + x + 1]$

$[x^3] = [x^2+1]$ $\qquad f(x) = x^3+x^2+1$

$x^3 - (x^2+1) = x^3 - x^2 - 1 = x^3 + x^2 + 1 = 1 \cdot f(x)$

$\mathbb{F}_2 = \{0, 1\}$

$[x^4] = [x^3+x] = [x^2+1+x] =$ $\qquad -1 = 1$

$[x^2+1] \cdot [x^2+x+1] = [(x^2+1)\cdot(x^2+x+1)] =$

$= [x^4 + x^3 + x^2 + x^2 + x + 1] =$

$= [x^4 + x^3 + x + 1]$

$= [x^2 + x + 1 + x^2 + 1 + x + 1]$

$= [2\cdot x^2 + 2\cdot x + 3] = [1]$

($2 \to 0$, $2 \to 0$, $3 \to 1$)

$p(x) = x^2+1$ $\qquad p(x)\,(p(x))^{-1} \equiv 1 \quad (f)$

$(p(x))^{-1} = x^2+x+1$

$\mathbb{F}_7$

$[15] = [1]$ $\qquad$ $a = b \ (p)$ si $a-b$ es divisible por p.

$15 = 2 \cdot 7 + 1$

$15 \equiv 1 \pmod 7$

$15 - 1$ es divisible por 7

$\mathbb{F}_2 = \{0, 1\}$

$[g(x)] = [h(x)]$ $\qquad$ $g(x) \equiv h(x) \pmod{f(x)}$ cuando $g(x) - h(x)$ divisible por $f(x)$.

$x^3 - (x^2+1) =$

$= x^3 - x^2 - 1$

$= x^3 + (-1)x^2 + (-1)x$

$= x^3 + 1 \cdot x^2 + 1 \cdot x$

$= f(x)$

$f(x) = \underline{x^3 + x^2 + 1} = 0$

$[x^3] = [x^2+1]$ en $\mathbb{F}_2[x]/(f)$

$x \cdot x^3 \equiv x(x^2+1) \pmod f$

$x^4 \equiv x^3 + x \equiv \underline{x^2 + 1 + x} \pmod f$

$\equiv x^2 + 1$

+	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	. . .			
$x+1$								
x^2								
x^2+1								
x^2+x								
x^2+x+1								

$[x^3] = [x^2+1]$

•	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x			x^2	x^2+x	x^3	x^3+x	x^3+x^2	
$x+1$					x^2+1	x^2+x+1	1	
x^2								
x^2+1								
x^2+x								
x^2+x+1								

$15 = 1$

$15 \mid 7$

1 2

x^3+x | x^3+x^2+1

x^2+x+1

$f(x) = x^3+x^2+1$

$= x^3-x^2-1$

$\mathbb{F}_2$.

$(f) = x^3+x+1 = 0$

$x^3 = x+1$

$x^4 = x^2+x$

$x^5 = x^3+x^2 = x+1+x^2$

$x^6 =$

$\mathbb{F}_3$ $-1 \equiv 2$

$x^3 = -x-1 = 2x+2$ $f = x^3+x+1$

$\mathbb{F}_3$.

$x^4 = 2x^2+2x$

$x^5 = 2x^3+2x^2 = 2(2x+2)+2x^2$

$= x+1+2x^2 = 2x^2+x+1$

x^3 | x^3+x^2+1

x^2+1 | 1.

$x^3 = x^2+1$

1. $(x^3+x^2+1) + (x^2+1) = x^3+2x^2+2$

$= x^3$.

$[x^3] = [x^2+1]$.

x^5 | x^3+x^2+1

$-(x^5+x^4+x^2)$ | x^2-x+1

$-(-x^4-x^3-x)$

x^3-x^2+x

$-(x^3+x^2+1)$

$x+1$

$x^3 = x^2+1$

$x^4 = x^3+x = x^2+1+x$

$x^5 = x^3+x+x^2 = x^2+1+x+x^2 = x+1$

Si F es un cuerpo arbitrario y $f(x) \in F[x]$ entonces al remplazar la indeterminada x en $f(x)$ por cualquier elemento $b \in F$ obtenemos otro elemento de F. En detalle si

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \in F[x]$$

y $b \in F$

$$f(b) = a_0 + a_1 \cdot b + \dots + a_n b^n \in F$$

Además si tenemos cualquier identidad polinomial en $F[x]$ y remplazamos x por $b \in F$ obtenemos una identidad válida en F. (Principio de sustitución)

Def: Un elemento $b \in F$ se llama una raíz o un cero de $f(x) \in F[x]$ si $f(b) = 0$ ← neutro de + en F.

Teorema: Un polinomio $f \in F[x]$ de grado 2 o 3 es irreducible en $F[x]$ si y sólo si f no tiene raíces en F.

f irreducible $\Rightarrow$ no tiene raíces

no tiene raíces $\Rightarrow$ f irreducible

$\deg(f) \leq 3$

$f(x) = x^4 + 1$ en $\mathbb{F}_3[x]$ $\quad f(x) = (x^2+x+2)(x^2+2x+2)$