Recordemos que un grupo era un conjunto con una operación $(G, *)$ que es asociativa, tiene un elemento neutro y todo elemento tiene un inverso u opuesto.

Para un grupo, si usamos una notación aditiva entonces representamos al neutro con 0 y al inverso (opuesto) de $a \in G$ por $-a$.

En este caso podemos escribir, para algún $n \in \mathbb{N}$

$$n \cdot a = \underbrace{a + a + \dots + a}_{n \text{ veces}} \quad \text{para } a \in G.$$

En cambio, si usamos una notación multiplicativa en general denotamos a la identidad por 1 y al inverso de $a \in G$ por a^{-1}. En este caso podemos escribir, para algún $n \in \mathbb{N}$

$$a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ veces}}$$

Las notaciones anteriores pueden extenderse para agregar $0 \in \mathbb{Z}$ adoptando las convenciones

$0 \cdot a = 0$ ($0 \in \mathbb{Z}$; el neutro de la suma)

$a^0 = 1$ ($0 \in \mathbb{Z}$; el neutro de la multiplicación)

Def: Si R es un anillo arbitrario y existe un entero positivo n tal que

$$n \cdot r = 0$$

para $r \in R$, entonces el entero positivo n más pequeño con esta propiedad se llama **característica del anillo**; y en este caso decimos que R es un anillo de **característica positiva**. Si no existe ningún tal n, se dice que R tiene **característica cero**.

Ejemplo:

- El anillo de enteros módulo p, $\mathbb{Z}_p$ tiene característica positiva p;

$$a \in \mathbb{Z}_p \qquad \underbrace{a+a+\dots+a}_{p \text{ veces}} = p \cdot a = 0$$

- Los enteros $(\mathbb{Z}, +, \cdot)$ o $(\mathbb{Q}, +, \cdot)$ tienen característica cero.

Ejercicio: ¿Existe un anillo con característica 1?

$R \neq \{0\}$ $\qquad$ $R = \{0\}$

Teorema: Un anillo $R \neq \{0\}$ de característica positiva, que tenga una identidad y que no tenga divisores propios de cero, debe tener característica prima.

Dem.

Como R tiene algún elemento no nulo (pues $R \neq \{0\}$) y tiene característica positiva, entonces la característica del anillo n, debe ser $n \geq 2$. Si n no es primo, entonces existen $m, k \in \mathbb{N}$ $1 < m < n$ y $1 < k < n$ y $n = m \cdot k$.

Si $e \in R$ es la identidad en R (de la multiplicación) entonces

$$0 = \overbrace{n \cdot e}^{e+e+\dots+e} = (m \cdot k)\, e = (m.e) \overset{\text{producto en } R}{!} (k.e)$$

n es la característica

$$(m.k)\, e = \underbrace{e+e+\dots+e}_{m.k \text{ veces}} =$$

$$m.(k.e)$$

$$= m \underbrace{(e+\dots+e)}_{k \text{ veces}}$$

$$= \underbrace{(e+e+\dots+e) + \dots + (e+\dots+e)}_{m \text{ veces}}$$

$$= \underbrace{(e+\dots+e)}_{k \text{ veces}} \cdot \underbrace{(e+\dots+e)}_{m \text{ veces}} = (k.e) \cdot (m.e)$$

propiedad distributiva en R

Como $0 = (k.e) \cdot (m.e)$ y R no tiene divisores propios de cero, debe ser que

o bien $k.e = 0$ o bien $m.e = 0$.

Supongamos que $k.e = 0$. Pero entonces, para cualquier $r \in R$ tenemos que

$$0 = 0 \cdot r = (k.e) \cdot r = \overbrace{(e + \dots + e)}^{k \text{ veces}} \cdot r = \overbrace{e \cdot r + \dots + e r}^{k \text{ veces}}$$

$$= \underbrace{r + \dots + r}_{k \text{ veces}} = k.r$$

(e es neutro de $\cdot$)

Pero entonces k tiene la propiedad de la característica del anillo y $1 < k < n$, y esto es un absurdo pues n es el más chico con esta propiedad.

∎

Corolario: Un cuerpo finito F tiene característica prima.

Dem.

Como es un cuerpo, es un anillo $\neq\{0\}$ con identidad y sin divisores propios de cero. Para usar el teorema anterior sólo me falta probar que tiene característica positiva.

Sea e la identidad del cuerpo, y consideremos

$e+e$ $\quad$ $e+e+e$

$2\cdot e$, $3\cdot e$, $4e$, ...

Como es finito, deben existir dos naturales k, m tales que $k\cdot e = m\cdot e$ con $1 \leq k < m$

Entonces $0 = \underbrace{(m-k)}_{\in \mathbb{N}} e$

Con la misma idea que antes tenemos que para cualquier $a \in F$ satisface $0 = (m-k)\cdot a$

$$\left(0 = 0\cdot a = (m-k)\cdot e \cdot a = \dots = (m-k)\cdot a \right)$$

Entonces $m-k > 0$ es la característica o hay uno menor, pero F tiene característica positiva.

Una propiedad interesante de un anillo de característica 2 es que $\forall r \in R$

$$r + r = 2 \cdot r = 0$$

Como el opuesto es único, tenemos que $-r = r$.

En particular en cualquier anillo de característica par todo elemento es su propio opuesto.

Otra propiedad importante de todos los cuerpos de característica prima es la siguiente:

Teorema: En un anillo conmutativo R con característica prima p se cumple que

$$\underline{(a+b)^{p^n} = a^{p^n} + b^{p^n}} \quad \text{y} \quad \underline{(a-b)^{p^n} = a^{p^n} - b^{p^n}};$$

para $a, b \in R$ $\quad n \in \mathbb{N}$.

Demostración (por inducción en n)

Para $n = 1$ vamos a ver que $(a+b)^p = a^p + b^p$.

Por el teorema del binomio.

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i$$

$$= \overbrace{\binom{p}{0}}^{1} a^p \overbrace{b^0}^{e} + \binom{p}{1} a^{p-1} \cdot b^1 + \cdots + \overbrace{\binom{p}{p}}^{1} \overbrace{a^0}^{e} \cdot b^p$$

Recordar $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ es un número entero positivo que cuenta la cantidad de maneras de elegir subconjuntos de k elementos en un tomados de un total de n.

donde

$n! = 1.2.\ldots.n \quad n \in \mathbb{N}$

Notar que

$\binom{p}{i}$ es multiplo de p para $1 \leq i \leq p-1$. en este anillo

$\binom{p}{i} a^{p-i} \cdot b^i = 0$ ✓ neutro de la suma

$\binom{p}{i}$ es un número natural

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{1.2\ldots(p-i)(p-i+1)\ldots(p)}{1.2\ldots i \cdot 1.2\ldots(p-i)}$$

$$= \frac{(p-i+1)\ldots\ldots(p)}{1.2\ldots\ldots i}$$

$$= \left(\frac{(p-i+1)\ldots(p-1)}{1.2\ldots i}\right) \cdot p$$

Entonces $\binom{p}{i} a^{p-i} b^i = 0$ y

$(a+b)^p = a^p + b^p$

Supongamos ahora que vale para n, y veamos que se cumple para $n+1$.

$$(a+b)^{p^{n+1}} = \left((a+b)^{p^n}\right)^p \overset{\text{H.I}}{=} \left(a^{p^n} + b^{p^n}\right)^p \overset{\text{H.I.}}{=} \left(a^{p^n}\right)^p + \left(b^{p^n}\right)^p$$

$$= a^{p^{n+1}} + b^{p^{n+1}}.$$

$$a^{p^n} = \left((a-b)+b\right)^{p^n} = (a-b)^{p^n} + b^{p^n}$$

$$a^{p^n} - b^{p^n} = (a-b)^{p^n}$$