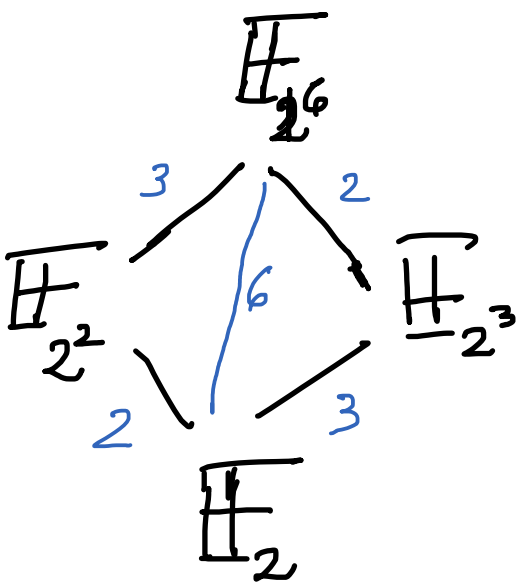
¿Cuáles son los $\alpha \in \mathbb{F}_{q^n}$ t.q. $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$?

Ej. $x^{2^6} - x = \dfrac{(x^{2^2}-x)(x^{2^3}-x)}{x^2-x} \cdot g(x)$,



con g = producto de los polinomios irreducibles mónicos en $\mathbb{F}_2[x]$ de grado 6

En particular. $64 = 10 + \deg(g)$

$\Rightarrow \deg(g) = 54$

$\Rightarrow$ Hay $\frac{54}{6} = 9$ pol's irred mónicos en $\mathbb{F}_2[x]$ de grado 6.

. Observemos que entonces tenemos 54 α's t.q. $\mathbb{F}_{2^6} = \mathbb{F}_2[\alpha]$

. Por otro lado: $\mathbb{F}_{2^6}^{\times} \simeq \mathbb{Z}/63\mathbb{Z}$

y $\varphi(63) = \varphi(7)\varphi(9) = 6 \cdot 6 = 36$

Osea, hay 36 elementos en $\mathbb{F}_{2^6}^{\times}$ que lo generan

como grupo. En particular, para esos α's.

$$\mathbb{F}_{2^6} \underset{(*)}{=} \mathbb{F}_2(\alpha).$$

O sea, no son todos los que cumplen (*)

Afirmo: Dado $\alpha \in \overline{\mathbb{F}}_{q^n}$,

$$\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha) \iff \begin{cases} 1) \ \mathrm{ord}(\alpha) = q^m - 1, \text{ en } \overline{\mathbb{F}}_{q^m}^{\times} \\ 2) \ \mathrm{ord}(\alpha) \nmid q^m - 1, \text{ en } \overline{\mathbb{F}}_{q^m}^{\times} \end{cases}$$

$\forall m \ t.q. \ m \mid n, \ m < m.$

Dem ($\Leftarrow$) 1) ✓

2) Sup. que $\mathbb{F}_{q^m} \neq \mathbb{F}_q(\alpha)$:

$\mathbb{F}_{q^m}$

|

$\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ (con $m \mid n$), entonces,

|

$\mathbb{F}_q$ como $\alpha \in \mathbb{F}_{q^m}$: $\alpha^{q^m} = \alpha$

$\alpha \neq 0$ $\Rightarrow$ $\alpha^{q^m - 1} = 1$

$\Rightarrow \mathrm{ord}(\alpha) \mid q^m - 1$ ▨

⇒) escribirla

Ej: $\overline{\mathbb{F}}_{24}$: Veamos cuántos α's hay en $\overline{\mathbb{F}}_{24}$ tq

$$\overline{\mathbb{F}}_{24} = \overline{\mathbb{F}}_2(\alpha).$$

$\overline{\mathbb{F}}_{24}^{\times} \simeq \mathbb{Z}/15\mathbb{Z}$. Entonces un α cumple lo pedido $\iff$ $\mathrm{ord}(\alpha) = 15$ en $\overline{\mathbb{F}}_{16}^{\times}$

ó $\mathrm{ord}(\alpha) \nmid 2^1 - 1, 2^2 - 1$

$= 1, 3$

O sea: $\mathrm{ord}(\alpha) = 15$ ó $\mathrm{ord}(\alpha) = 5$

$\mathbb{Z}/15\mathbb{Z}$: ~~0~~, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14

↓ orden 3 ↓

Ej: Sea ξ_n raíz n-ésima primitiva de 1 en $\overline{\mathbb{F}}_q$

Sea $\alpha_i = \xi_n + \xi_n^{-1}$.

a) Probar que $\alpha \in \overline{\mathbb{F}}_q \iff q \equiv \pm 1 \ (n)$

b) Calcular en $\xi_7 + \xi_7^{-1}, \overline{\mathbb{F}}_2$

a) $\alpha \in \overline{\mathbb{F}}_q \iff \alpha^q = \alpha \iff \xi_n^q + \xi_n^{-q} = \xi_n + \xi_n^{-1}$

Enlaces $\Rightarrow$) $\xi_n^q + \xi_n^{-q} - \xi_n - \xi_n^{-1} = 0$

$\Rightarrow (\xi_n^{q-1} - 1)(\xi - \xi^{-q}) = 0$

$\Rightarrow \xi_n^{q-1} = 1$ ó $\xi^{-q} = \xi$

$\Rightarrow n \mid q-1$ ó $\underbrace{\xi^{-q-1} = 1}$

$\Rightarrow n \mid q+1$

$\Rightarrow q \equiv \pm 1 \ (n)$

$\Leftarrow$) Si $q \equiv 1(n) \Rightarrow n \mid q-1 \Rightarrow \xi_n^{q-1} = 1$

$\Rightarrow \xi_n \in \mathbb{F}_q \Rightarrow \alpha \in \mathbb{F}_q$

Si $q \equiv -1(n)$ ... lemmon (Nota que la ida ya prueba el $\Leftrightarrow$)

b) $\mathbb{F}_2(\overbrace{\xi_7 + \xi_7^{-1}}^{\alpha}) = \mathbb{F}_{2^r}$

?

$\mathbb{F}_2$

a)

$\alpha \in \mathbb{F}_{2^r} \Leftrightarrow 2^r \equiv \pm 1 \ (7)$

$\boxed{r = 3}$ es el mínimo que lo cumple

$\Rightarrow \alpha \in \mathbb{F}_{2^3}$, con lo cual.

$m_{\alpha, \mathbb{F}_2} = (x-\alpha)(x-\alpha^2)(x-\alpha^4)$

Obs. 1) (ej 13) $\mathrm{car}(k) \nmid n \Rightarrow \Phi_n$ se factoriza en $k[x]$ como producto de polis irreducibles de grado $[k(\xi_n) : k]$

2) (ej 14 ó Visto con Juan)

Si $k = \mathbb{F}_q$ $\quad [k(\xi_n) : k] = \min\{k / n \mid q^k - 1\}$

Conclusión: Ej: ¿cómo se factorizan Φ_8 y Φ_{10} en $\mathbb{F}_9$?

1) Φ_8: $\min\{k / 8 \mid 9^k - 1\} = 1$

(se factoriza linealmente)

2) Φ_{10}: $\min\{k / 10 \mid 9^k - 1\} = 2$

(se factoriza como prod de irred's de grado 2)

Ej: ¿Cuáles son los cuerpos finitos $\mathbb{F}_q$ "$i \in k$"? (-1 es un cuadrado)

Se trata de ver cuando el polinomio $x^2 + 1$ se factoriza en $\mathbb{F}_q = \mathbb{F}_{p^r}$. Sup, $p \neq 2$

"Φ_4" Por lo que vimos, Φ_4 se factoriza en $\mathbb{F}_{p^r}$ como producto de irreducibles de grado $d = \min\{k / 4 \mid (p^r)^k - 1\}$.

En bus buscar los p y r tq $d=1$.

O sea $\cdot\ p^r \equiv 1\ (4)$.

- Si $p \equiv 1\ (4) \Rightarrow p^r \equiv 1\ (4)\ \forall r$
- Si $p \equiv 3\ (4) \Rightarrow p^r \equiv 1\ (4)$ Si r es par

Rta $\mathbb{F}_{p^r}$, con $p \equiv 1\ (4)$ ó $p \equiv 3(4)$ y r par

Si $p=2$: ya tenemos $i \in \mathbb{F}_2$ ✓

Ej a) Factorizar $\Phi_{28}(x^{10})$ en $\mathbb{Q}[x]$

b) ¿Cuántos factores tiene en $\mathbb{F}_{13}$?

a) $\Phi_{2^2.7}(x^{10}) = \Phi_{2.7}(x^{20}) = \Phi_{2.7}((x^5)^4)$

↓ ej 8.2

$= \phi_{2^3.7}(x^5) = \phi_{2^3.7.5}(x) \cdot \Phi_{2^3.7}(x)$ listo

↓ ej 8.2