CUERPOS FINITOS (Cuerpos de Galois)

ALGEBRA 3 2017
Clase 12
29/9/17 ①

Rdo

① K cpo finito $\Rightarrow$ car$(K) = p$ para algún primo p

② K es una $\mathbb{F}_p$-e.v. para algún $n \in \mathbb{N}$,

y por lo tanto $|K| = p^n$

③ Miremos el cuerpo finito $\mathbb{F}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ con las operaciones de resto módulo p

Todo elto de $\mathbb{F}_p$ satisface el Pequeño Teorema de Fermat (PTF)

$a^p = a$, $\forall a \in \mathbb{F}_p$ (pues $a^p \equiv a \pmod p$)

O sea $\mathbb{F}_p = \{a \in \overline{\mathbb{F}_p} : a$ es raíz de $X^p - X\}$

$\subseteq$ por el PTF

y la igualdad vale porque $X^p - X$ tiene $\leq p$ raíces $\neq$ en $\overline{\mathbb{F}_p}$

(en realidad exactamente p pues $X^p - X$ es separable:

$(X^p - X)' = -1 \neq 0$)

y todos los eltos de $\mathbb{F}_p$, que son exactamente p, son raíces

También se puede ~~caracterizar~~, observar, una vez definido $\overline{\mathbb{F}_p}$, que

$$\mathbb{F}_p = \mathbb{F}_p(X^p - X) \subseteq \overline{\mathbb{F}_p}$$

Los cuerpos de Galois

Proposición: Sea p primo y $n \in \mathbb{N}$

El conjunto

$$K := \{\alpha \in \overline{\mathbb{F}_p} : \alpha \text{ es raíz de } X^{p^n} - X\} \subseteq \overline{\mathbb{F}_p}$$
$$= \{\alpha \in \overline{\mathbb{F}_p} : \alpha^{p^n} = \alpha\}$$

es un cuerpo que tiene exactamente p^n eltos.

Se tiene $K = \mathbb{F}_p(X^{p^n} - X)$, cuerpo de descomposición del polinomio $X^{p^n} - X$ sobre $\mathbb{F}_p$

Demostración

- Para probar que K es cpo, probemos que si $car(K) = p$, $\forall n \in \mathbb{N}$ se tiene $\underline{(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} \quad \forall \alpha, \beta \in K}$ $(*)$

Por inducción en n:

$n = 1$: $(\alpha+\beta)^p = \alpha^p + \beta^p$ pues $p \mid \binom{p}{k}$ para $1 \leq k \leq p-1$

$n > 1$: $(\alpha+\beta)^{p^n} = [(\alpha+\beta)^p]^{p^{n-1}} = (\alpha^p + \beta^p)^{p^{n-1}}$

$$\underset{HI}{=} (\alpha^p)^{p^{n-1}} + (\beta^p)^{p^{n-1}} = \alpha^{p^n} + \beta^{p^n}$$

$(*)$ es importante! Lo retomamos después.

Así, K es cpo pues

- $0, 1 \in K$
- $\alpha, \beta \in K \Rightarrow \alpha \pm \beta \in K$ pues

  $(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta$
- $\alpha, \beta \in K \Rightarrow \alpha\beta \in K$ pues $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$
- $\alpha \in K^\times \Rightarrow 1/\alpha \in K$ pues $\left(\frac{1}{\alpha}\right)^{p^n} = \frac{1}{\alpha^{p^n}} = \frac{1}{\alpha}$

- $\mathbb{F}_p \subseteq K$ pues $\alpha^p = \alpha \Rightarrow \alpha^{p^n} = \alpha$
- $K = \mathbb{F}_p(X^{p^n} - X)$: Valen las 2 inclusiones
- $|K| = p^n$ pues $X^{p^n} - X$ es un polinomio <u>separable</u>:

  $(X^{p^n} - X)' = -1$ en característica p
  $\neq 0$

Vale una recíproca:

<u>PROPOSICIÓN</u>: Sea K un cuerpo de característica p, <u>finito</u> con p^n elementos. Entonces $K = \mathbb{F}_p(X^{p^n} - X)$ es cuerpo de descomposición de $X^{p^n} - X$ sobre $\mathbb{F}_p$.

<u>Demostración</u>:

Ya sabemos que al ser K cuerpo finito, $K^\times$ es un grupo multiplicativo finito ~~cíclico~~ de orden $p^n - 1$ si $|K| = p^n$. Así, $\forall \alpha \in K^\times$ se tiene

$$\alpha^{p^n - 1} = 1 \text{ en } K \underset{\text{mult.} \times \alpha}{\Rightarrow} \alpha^{p^n} = \alpha \text{ en } K$$

y como para $\alpha = 0$,

también vale $\alpha^{p^n} = \alpha$, se tiene

$$\forall \alpha \in K, \ \alpha^{p^n} = \alpha, \text{ i.e. } \alpha \text{ es raíz de } X^{p^n} - X$$

$$\Rightarrow \quad K \subseteq \mathbb{F}_p(X^{p^n} - X)$$

y también vale la recíproca

$\mathbb{F}_p \subseteq K$ y las raíces de $X^{p^n} - X$ están incluidas

en K, y K es cpo:

$$\mathbb{F}_p(X^{p^n} - X) \subseteq K.$$

Por lo tanto $K = \mathbb{F}_p(X^{p^n}-X)$

pues $K \subseteq \mathbb{F}_p(X^{p^n}-X)$ y $\mathbb{F}_p(X^{p^n}-X) \subseteq K$ como antes

Conclusión - Notación - Teorema

- Dado $n \in \mathbb{N}$, existe un único cuerpo de característica p con p^n elementos. Este es

$$\mathbb{F}_{p^n} := \mathbb{F}_p(X^{p^n}-X)$$

En particular $\mathbb{F}_{p^n}$ es Galois sobre $\mathbb{F}_p$, y todo cuerpo finito de característica p es $\mathbb{F}_{p^n}$ para algún n, extensión Galois / $\mathbb{F}_p$.

Notar que $X^{p^n}-X = \prod_{\alpha \in \mathbb{F}_{p^n}} (X-\alpha)$.

Subextensiones de $\mathbb{F}_{p^n}$:

Proposición:

① $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^{(n:m)}}$

② $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \iff n \mid m$

Demostración

① $(X^{p^n}-X : X^{p^m}-X) = X^{p^{(n:m)}}-X$

por el algoritmo de Euclides:

$$a^{dq+r}-1 = a^{dq+r}-a^r+a^r-1$$
$$= a^r\left[a^{dq}-1\right]+a^r-1 = *\cdot(a^q-1)+a^r-1$$

$$\Rightarrow \quad (a^{dq+r}-1 : a^{q}-1) = (a^{q}-1 : a^{r}-1)$$

$$(p^{n}-1 : p^{m}-1) = (p^{m}-1 : p^{r}-1) = \dots$$
$$= p^{(n:m)}-1$$

y $(X^{p^{n}-1}-1 : X^{p^{m}-1}-1) = X^{p^{(n:m)}-1}-1$

$$\Rightarrow (X^{p^{n}}-X : X^{p^{m}}-X) = X(X^{p^{n}-1}-1 : X^{p^{m}-1}-1)$$
$$= X(X^{p^{(n:m)}-1}-1) = X^{p^{(n:m)}}-X.$$

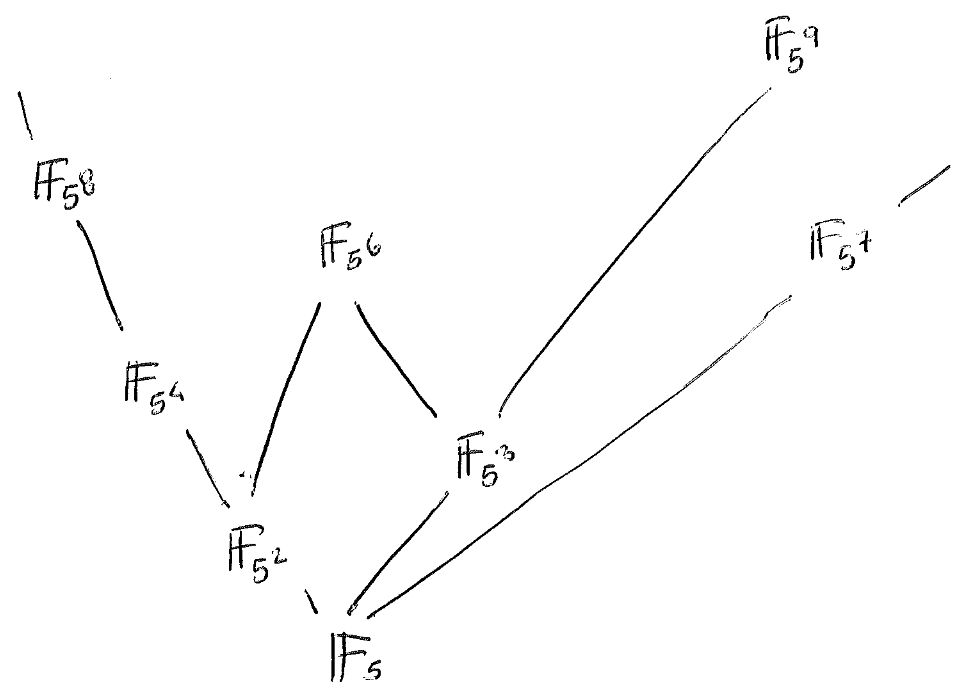
Así: $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_p(X^{p^n}-X) \cap \mathbb{F}_p(X^{p^m}-X)$

$$= \{\alpha \in \overline{\mathbb{F}}_p : \alpha^{p^n}-\alpha = 0 \text{ y } \alpha^{p^m}-\alpha = 0\}$$
$$= \{\alpha \in \overline{\mathbb{F}}_p : \alpha^{p^{(n:m)}}-\alpha = 0\} = \mathbb{F}_p(X^{p^{(n:m)}}-X).$$

(2) $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \iff \mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^n}$

$\iff \mathbb{F}_{p^{(n:m)}} = \mathbb{F}_{p^n} \iff (n:m) = n \iff n \mid m$

<u>Ejemplos</u>



Elementos primitivos

Todo cuerpo finito de característica p es Galois/ $\mathbb{F}_p$.

Por lo tanto admite eltos primitivos.

¿Cómo se construyen eltos primitivos?

Quiero θ / $\mathbb{F}_{p^n} = \mathbb{F}_p[\theta]$

Como $\theta \in \mathbb{F}_{p^n}$, θ satisface $\theta^{p^n} - \theta = 0$

y $f(\theta, \mathbb{F}_p) \mid X^{p^n} - X$ tiene grado n y es irreducible

pero $\theta \notin \mathbb{F}_{p^m}$ para $m \mid n$, o sea

$f(\theta, \mathbb{F}_p) \nmid X^{p^m} - X$ para ningún $m \mid n$

Sabemos

$$f(\theta, \mathbb{F}_p) = \prod_{\sigma \in Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)} (X - \sigma(\theta))$$

Podemos conseguir θ usando por ejemplo que $\mathbb{F}_{p^n}^{\times}$ es <u>cíclico</u>

$\exists\, \theta \in \mathbb{F}_{p^n}^{\times}$ / $\mathbb{F}_{p^n}^{\times} = \{1, \theta, .., \theta^{p^n-2}\}$

y en particular $\mathbb{F}_{p^n} = \{0, 1, \theta, .., \theta^{p^n-2}\}$

$= \mathbb{F}_p[\theta]$

Pero eso es pedir mucho. Hay más eltos primitivos que generadores del grupo cíclico

Por ejemplo $\mathbb{F}_9^{\times} \simeq \mathbb{Z}/8\mathbb{Z}$ tiene 4 generadores: $\bar{1}, \bar{3}, \bar{5}, \bar{7}$

pero admite 6 eltos primitivos divididos entre 3 pols irreducibles de grado 2:

$$\mathbb{F}_{3^2} = \mathbb{F}_9 = \mathbb{F}_3(X^{3^2} - X) = (\underbrace{X^3 - \cancel{X}}_{\text{en } \mathbb{F}_3})(X^6 + X^4 + X^2 + 1)$$

$$= (X^3 - X)\cancel{(\ldots)}(X^2+1)\overbrace{(X^2+X+2)(X^2+2X+2)}^{X^4+1}$$

El automorfismo de Frobenius y el generador de $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$

Proposición: Sea K con $car(K)=p$.

Entonces $\phi_p : K \to K$, $\alpha \mapsto \alpha^p$ es una $\mathbb{F}_p$-inmersión de K y por lo tanto $\forall k \in \mathbb{N}$, ϕ_p^k también lo es.

Satisface $\phi_p^k(\alpha) = \alpha^{p^k}$, $\forall \alpha \in K$.

En particular si K es finito o algebraico$/\mathbb{F}_p$,

ϕ_p y ϕ_p^k, $k \in \mathbb{N}$, son $\mathbb{F}_p$-automorfismos de K.

ϕ_p se llama en ese caso el automorfismo de Frobenius

Teorema Sea $n \in \mathbb{N}$. $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$ es un grupo cíclico generado por el automorfismo de Frobenius:

$$Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \phi_p \rangle$$

(y en particular $\phi_p^n = id$ en $\mathbb{F}_{p^n}$)

Demostración: Sea $\theta \in \mathbb{F}_p$ generador del grupo cíclico multiplicativo $\mathbb{F}_{p^n}^{\times}$, o sea $\mathbb{F}_{p^n} = \{0, 1, \theta, \theta^2, .., \theta^{p^n-2}\}$

Sabemos que $|Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$ pues $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ y la extensión es Galois.

Probemos que $\{id, \Phi_p, \Phi_p^2, .., \Phi_p^{n-1}\}$ son todos $\neq$ en $\mathbb{F}_{p^n}$:

$\Phi_p^k(\theta) = \theta^{p^k}$ pero $\{\theta, \theta^p, \theta^{p^2}, .., \theta^{p^{n-1}}\}$ son todos $\neq$ pues se puede verificar que son un subcjto de eltos $\neq$ de $\mathbb{F}_{p^n} = \{0, 1, \theta, .., \theta^{p^n-2}\}$ $\forall p, \forall n$.

$\boxtimes$

Cantidad de pols irreducibles de grado dado / $\mathbb{F}_p$

¡Gracias a la teoría!

$\mathbb{F}_{5^2} = \mathbb{F}_5(X^{25}-X)$

$| 2$

$\mathbb{F}_5 = \mathbb{F}_5(X^5-X)$

$$X^{25}-X = (X^5-X)\,q \qquad \left(X^5-X = X(X-1)(X-2)(X-3)(X-4)(X-5)\right)$$

donde $gr(q)=20$ y q se descompone como 10 pols irreducibles de grado $2/\mathbb{F}_5$ que son todos los que definen $\mathbb{F}_{5^2}$

(Justificar xq no puede haber factores irreducibles de otro grado que 2 en q)

$$\begin{tikzcd}
\mathbb{F}_{5^6} = \mathbb{F}_5(X^{5^6}-X) \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{F}_{5^2} = \mathbb{F}_5(X^{25}-X) \arrow[d, dash] & \mathbb{F}_{5^3} = \mathbb{F}_5(X^{125}-X) \arrow[dl, dash] \\
\mathbb{F}_5 = \mathbb{F}_5(X^5-X) &
\end{tikzcd}$$

$$X^{5^6}-X = (X^5-X)\left(\frac{X^{25}-X}{X^5-X}\right)\left(\frac{X^{125}-X}{X^5-X}\right) q$$

$\Rightarrow gr(q) = 5^6 - [5+20+120] = 6(\#\text{ pols irred de grado } 6)$

O mejor aún, todo elto que no genera $\mathbb{F}_{5^2}$ y $\mathbb{F}_{5^3}$ y $\mathbb{F}_5$ genera $\mathbb{F}_{5^6}$. Luego

$\#$ eltos primitivos de $\mathbb{F}_{5^6} = \cancel{5^6}.\ |\mathbb{F}_{5^6}| - |\mathbb{F}_{5^2} \cup \mathbb{F}_{5^3}|$

$\Rightarrow \quad = 5^6 - [5^2+5^3-5]$

Y esa cantidad $/6 = \#$ pols irred de grado 6