Álgebra III - 2do C. 2020 - Clase 13 - 13/10/2020

9.3 Cuerpos de Galois y elementos primitivos

Todo cuerpo *finito* de característica p es algún $\mathbb{F}_{p^n} = \mathbb{F}_p(X^{p^n} - X)$, que es Galois sobre $\mathbb{F}_p$, y por lo tanto es una extensión simple de $\mathbb{F}_p$, que tiene elementos primitivos.

¿Cómo se determinan elementos primitivos?
Busco $\theta \in \overline{\mathbb{F}_p}$ tal que $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$.

Podemos conseguir θ por ejemplo usando el hecho que $\mathbb{F}_{p^n}^\times = \langle\theta\rangle$ es un grupo cíclico, y entonces

$$\mathbb{F}_{p^n} = \{0, 1, \theta, \ldots, \theta^{p^n-2}\} = \mathbb{F}_p(\theta).$$

Pero esto es matar una hormiga con un camión, además de que hay muchos más elementos primitivos para $\mathbb{F}_{p^n}/\mathbb{F}_p$ que generadores del grupo cíclico $\mathbb{F}_{p^n}^\times$, y además, no sabemos quién es realmente ese θ ya que no sabemos bien quienes son los elementos de $\mathbb{F}_{p^n}$ ...

Ejemplo $(\mathbb{F}_9)$

- $\mathbb{F}_9^\times \simeq \mathbb{Z}/8\mathbb{Z}$ que tiene 4 generadores: 1,3,5 y 7.
- Pero $\mathbb{F}_9$ tiene 9 elementos y una única subextensión que es $\mathbb{F}_3$.

  Por lo tanto los 6 elementos de $\mathbb{F}_9 \setminus \mathbb{F}_3$ generan $\mathbb{F}_9$ sobre $\mathbb{F}_3$:

  hay entonces 6 elementos primitivos.

  ¿Cuáles son?

  En $\mathbb{F}_3[X]$,

  $X^9 - X = (X^3 - X)(X^6 + X^4 + X^2 + 1) = (X^3 - X)(X^2 + 1)(X^2 + X + 2)(X^2 + 2X + 2)$.

  El primer polinomio $X^3 - X$ define $\mathbb{F}_3$ dentro de $\mathbb{F}_9$ y los otros 3 polinomios son irreducibles de grado 2, y por lo tanto cada una de sus raíces genera $\mathbb{F}_9$, i.e. para cada θ raiz de $X^2 + 1$ o de $X^2 + X + 2$ o de $X^2 + 2X + 2$, se tiene que

  $$\mathbb{F}_9 = \mathbb{F}_3(\theta).$$

  Fijarse que efectivamente aunque no esté presentado en forma normal, $\mathbb{F}_3(\theta)$ es normal, pues (además de ser una extensión de grado 2) si θ es raíz de $X^2 + X + 2$ por ejemplo, la otra es $2\theta + 2$ ...

Observación 9.3.1 (Elementos primitivos en $\mathbb{F}_{p^n}$)
Sea $f \in \mathbb{F}_p[X]$ *un polinomio* irreducible *de grado* n *y sea* $\alpha \in \overline{\mathbb{F}_p}$ *raíz de* f. *Entonces*

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha).$$

En particular $f \mid X^{p^n} - X$ *en* $\mathbb{F}_p[X]$.

Prueba.–
$\mathbb{F}_p(\alpha)$ es un cuerpo finito, extensión de $\mathbb{F}_p$ de grado n, y por lo tanto tiene p^n elementos.
Como hay un único cuerpo finito de p^n elementos, $\mathbb{F}_{p^n} = \mathbb{F}_p(X^{p^n} - X)$, se tiene que $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$, y además $f \mid X^{p^n} - X$.

■

¡Acabamos de decir que todo polinomio irreducible de grado n es un divisor de $X^{p^n} - X$ en $\mathbb{F}_p[X]$!
Más aún ¿podemos sacar de esto como se factoriza $X^{p^n} - X$ en $\mathbb{F}_p[X]$?

Ejemplo ($\mathbb{F}_{25}$)
¿Cuántos elementos primitivos tiene $\mathbb{F}_{25}$?
¿Cuántos polinomios mónicos de grado 2 hay en $\mathbb{F}_5[X]$?
¿Cuántos son irreducibles?

$$X^{25} - X = (X^5 - X)q$$

donde q de grado 20 se factoriza como ¿cuántos polinomios de qué grado en $\mathbb{F}_5[X]$?
¿Por qué sólo esos grados?

Otro ejemplo ($\mathbb{F}_{5^6}$)
¿Cuáles son las subextensiones de $\mathbb{F}_{5^6}$?
¿Cuántos elementos primitivos tiene $\mathbb{F}_{5^6}$?
¿Cuántos polinomios mónicos de grado 6 hay en $\mathbb{F}_5[X]$?
¿Cuántos son irreducibles?

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

donde q tiene grado

Las raíces de q no pertenecen ni a $\mathbb{F}_5$, ni a $\mathbb{F}_{25}$ ni a $\mathbb{F}_{125}$.

Por lo tanto q es el producto de polinomios irreducibles de grado ,
y hay polinomios irreducibles mónicos de grado 6 en $\mathbb{F}_5[X]$.

Observación 9.3.2 *Sea $n \in \mathbb{N}$ y sea q_d el producto de todos los polinomios irreducibles mónicos de grado d en $\mathbb{F}_p[X]$. Entonces*

$$X^{p^n} - X = \prod_{d \,|\, n} q_d.$$

Ejercicio
El polinomio $X^4 + 1$ es irreducible en $\mathbb{Q}[X]$, pues $X^4 + 1 = \Phi_8(X)$.

¿Para qué primos p es $X^4 + 1$ irreducible en $\mathbb{F}_p[X]$?

$X^4 + 1$ irreducible en $\mathbb{F}_p[X]$ define el cuerpo $\mathbb{F}_{p^4} = \mathbb{F}_p(X^{p^4} - X)$,
o sea $X^4 + 1 \,|\, X^{p^4} - X$ pero además $X^4 + 1$ no define una subextensión propia de $\mathbb{F}_{p^4}$: $X^4 + 1 \nmid X^{p^2} - X$.
Para $p = 2$, $X^4 + 1 = (X + 1)^4$ no es irreducible.
Para p impar,

$$p \equiv 1 \ (2) \quad \Longrightarrow \quad p^2 \equiv 1 \ (8) \quad \Longrightarrow \quad p^2 - 1 = 8k.$$

Esto implica

$$X^4 + 1 \,|\, X^8 - 1 \,|\, X^{8k} - 1 = X^{p^2-1} - 1 \quad \Longrightarrow \quad X^4 + 1 \,|\, X^{p^2} - X$$

siempre. O sea que $X^4 + 1$ no es irreducible en ningún $\mathbb{F}_p[X]$.

■

Ejercicio
Probar que para todo $p \neq 2, 3$, el polinomio $X^4 - X^2 + 1$ es reducible en $\mathbb{F}_p[X]$.

9.4 El grupo de Galois de $\mathbb{F}_{p^n}$

Observación-Definición 9.4.1 (El automorfismo de Frobenius)
Sea K cuerpo con $\mathrm{car}(K) = p$, y sea

$$\begin{array}{rccc} \Phi_p : & K & \longrightarrow & K \\ & \alpha & \longmapsto & \alpha^p. \end{array}$$

Resulta que $\Phi_p \in \mathrm{End}(K/\mathbb{F}_p)$:

Y por lo tanto, $\forall\, k \in \mathbb{N}$, $\Phi_p^k \in \mathrm{End}(K/\mathbb{F}_p)$ *también.*
Se tiene $\Phi_p^k(\alpha) = \alpha^{p^k}$, $\forall\, k \in \mathbb{N}$.

Más aún, si K *es finito o algebraico sobre* $\mathbb{F}_p$, *entonces* Φ_p *y* Φ_p^k *para* $k \in \mathbb{N}$ *son* $\mathbb{F}_p$-automorfismos *de* K.
En ese caso Φ_p *se llama el* automorfismo de Frobenius *de* K, *por Ferdinand Georg Frobenius, matemático alemán, 1849-1917.*

¿Por qué tan importante ese automorfismo? ¡Porque genera $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$!

Teorema 9.4.2 *Sea* $n \in \mathbb{N}$. *Entonces* $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ *es un grupo cíclico de orden* n *generado por el automorfismo de Frobenius:*

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

donde recuerdo que $\Phi_p(\alpha) = \alpha^p$.
En particular, $\Phi_p^n = \{\mathrm{id}_{\mathbb{F}_{p^n}}\}$.

Prueba.–
Sabemos que $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ es un grupo de orden n pues $\mathbb{F}_{p^n}/\mathbb{F}_p$ Galois implica $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.
Para probar que $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \Phi_p \rangle$, probemos que

$$\{\mathrm{id}, \Phi_p, \Phi_p^2, \ldots, \Phi_p^{n-1}\}$$

son todos automorfismos distintos.
Para ello se los aplicamos a un generador θ del grupo multiplicativo $\mathbb{F}_{p^n}^\times$ que sabemos que es cíclico. O sea

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

Se tiene $\Phi_p^k(\theta) = \theta^{p^k}$ para $0 \leq k < n$, y se puede verificar que el conjunto

$$\{\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}}\}$$

es un subconjunto de elementos distintos en $\mathbb{F}_{p^n}$, pues $p^{n-1} \leq p^n - 2$ para $n \geq 2$.
■

9.5 El polinomio $X^p - X - a \in \mathbb{F}_p[X]$

Sabemos que para $a = 0$ el polinomio $X^p - X$ define $\mathbb{F}_p$:

$$X^p - X = \prod_{\alpha \in \mathbb{F}_p} (X - \alpha).$$

Y para $a \in \mathbb{F}_p$, $a \neq 0$, $X^p - X - a$ no tiene raíces en $\mathbb{F}_p$ y es separable: tiene p raíces distintas en $\overline{\mathbb{F}_p}$.

Proposición 9.5.1 (Irreducibilidad de $X^p - X - a$ para $a \neq 0$ en $\mathbb{F}_p[X]$)
Sea $a \in \mathbb{F}_p$, $a \neq 0$. Entonces el polinomio $X^p - X - a$ es irreducible en $\mathbb{F}_p[X]$, y por lo tanto define la extensión $\mathbb{F}_{p^p}$.

Prueba.–
Sea $\alpha \in \overline{\mathbb{F}_p}$ raíz de $X^p - X - a \in \mathbb{F}_p[X]$ con $a \neq 0$. Entonces $\alpha \notin \mathbb{F}_p$ y

$$2 \leq [\mathbb{F}_p(\alpha) : \mathbb{F}_p] \leq p \quad \text{pues} \quad f(\alpha, \mathbb{F}_p) \mid X^p - X - a.$$

Recordando que $\mathbb{F}_p(\alpha)$ es Galois sobre $\mathbb{F}_p$, esto implica que

$$|\mathrm{Gal}(F_p(\alpha)/\mathbb{F}_p)| \leq p$$

y por otro lado, $\mathrm{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_p) = \langle \Phi_p \rangle$.
¿Qué orden tiene el automorfismo de Frobenius Φ_p?

- $\Phi_p(\alpha) = \alpha^p = \alpha + a$ pues α es raíz de $X^p - X - a$.
- $\Phi_p^2(\alpha) = \Phi_p(\alpha + a) = \Phi_p(\alpha) + a = \alpha + 2\,a$, y así sucesivamente
- $\Phi_p^k(\alpha) = \alpha + k\,a$ para $k \in \mathbb{N}$.

Se tiene

$$\begin{aligned} \Phi_p^k(\alpha) = \Phi_p^j(\alpha) \quad &\iff \quad \alpha + k\,a = \alpha + j\,a \\ &\iff \quad k\,a = j\,a \ \text{ en } \mathbb{F}_p \\ &\underset{a \neq 0 \ (p)}{\iff} \quad k \equiv j \ (p). \end{aligned}$$

Por lo tanto

$$\Phi_p(\alpha) = \alpha + a, \ldots, \Phi_p^{p-1}(\alpha) = \alpha + (p-1)\,a, \Phi_p^p(\alpha) = \alpha$$

son todos distintos:

$$\mathrm{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_p) = \langle \Phi_p \rangle = \{\mathrm{id}_{\mathbb{F}_p(\alpha)}, \Phi_p, \ldots, \Phi_p^{p-1}\}$$

tiene orden p, y

$$\begin{aligned} f(\alpha, \mathbb{F}_p) &= \prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_p)} \big(X - \sigma(\alpha)\big) \\ &= \prod_{0 \le k < p} \big(X - \Phi_p^k(\alpha)\big) \\ &= \prod_{0 \le k < p} \big(X - (\alpha + k\,a)\big) \end{aligned}$$

es un polinomio irreducible en $\mathbb{F}_p[X]$, que divide a $X^p - X - a$, y como tienen mismo grado (y son ambos mónicos) son iguales.
Así

$$X^p - X - a \;=\; \prod_{0 \le k < p} \big(X - (\alpha + k\,a)\big)$$

es irreducible en $\mathbb{F}_p[X]$ y

$$\mathbb{F}_p(\alpha) = \mathbb{F}_{p^p}.$$

Notar que si $a \neq b \in \mathbb{F}_p$, ambos no nulos, entonces $X^p - X - a$ y $X^p - X - b$ son irreducibles distintos, y como la única subextensión de $\mathbb{F}_{p^p}$ es $\mathbb{F}_p$, Se tiene que

$$X^{p^p} - X = (X^p - X)(X^p - X - 1) \cdots (X^p - X - (p-1))q(X)$$

donde q es el producto de $p^{p-1} - p$ polinomios irreducibles de grado p.

■