Extensiones de Galois

Facultad de Ciencias UNAM

Introducción

En la sección anterior vimos que los campos de descomposición de polinomios separables son especialmente agradables desde el punto de vista de teoría de Galois. El objetivo de esta sección es caracterizar estas extensiones en términos de normalidad y separabilidad. Después, ocuparemos esto para estudiar a las extensiones separables; pero antes que nada, introducimos una definición que es central en la teoría de Galois.

El campo fijo

Definición

Supongamos que L/F es una extensión de campos y que $H \leq \mathrm{Gal}(L/F)$ es un subgrupo de $\mathrm{Gal}(L/F)$. Denotamos

$$L_H := \{\alpha \in L \mid \sigma\alpha = \alpha \text{ para toda } \sigma \in H\}$$

y decimos que L_H es el **campo fijo de** H.

Es fácil verificar que L_H es un subcampo de L que contiene a F. Cabe recalcar que la L en L_H es independiente de la L en L/F pero que la escribimos de esa manera porque en el caso general se ve bonita esta notación. Por ejemplo, si $H \leq \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, entonces escribimos L_H para denotar a el campo fijo de H, no escribimos $\mathbb{Q}(\sqrt{2})_H$.

$\mathrm{Gal}(L/F) = \mathrm{Gal}(L/L_{\mathrm{Gal}(L/F)})$

Lema 1

Supongamos que L/F es una extensión de campos. Entonces

$$\mathrm{Gal}(L/F) = \mathrm{Gal}(L/L_{\mathrm{Gal}(L/F)}).$$

Demostración.

$\supset$) Es consecuencia inmediata de que $F \subset L_{\mathrm{Gal}(L/F)}$.
$\subset$) Antes que nada, notemos que

$$\alpha = L_{\mathrm{Gal}(L/F)} \iff \sigma\alpha = \alpha \text{ para toda } \sigma \in \mathrm{Gal}(L/F). \tag{1}$$

Ahora si, supongamos que $\sigma \in \mathrm{Gal}(L/F)$. Queremos ver que $\sigma \in \mathrm{Gal}(L/K)$. Como σ es un automorfismo de L, entonces $\sigma \in \mathrm{Gal}(L/K)$ si y solo si σ fija a K. Es decir, $\sigma \in \mathrm{Gal}(L/K)$ si y solo si

$$\sigma\alpha = \alpha \text{ para toda } \alpha \in K.$$

Sin embargo, esto es consecuencia inmediata de (1).

□

Un campo intermedio en una extensión que es campo de descomposición

Lema 2

Supongamos que F, K, L son campos tales que $F \subset K \subset L$ y sea $f(x) \in F[x]$. Si L es campo de descomposición de $f(x)$ sobre F, entonces L también es campo de descomposición de $f(x)$ sobre K.

Demostración. Supongamos que L es el campo de descomposición de $f(x)$ sobre F. Veamos que L es el campo de descomposición de $f(x)$ sobre K.

- *$f(x)$ se descompone en L/K*: Esto es consecuencia inmediata de que L es el campo de descomposición de $f(x)$ sobre F.
- *No existe E campo tal que $K \subset E \subsetneq L$ y $f(x)$ se descompone en E/K*: Procedemos por contradicción, es decir, supongamos que E es un campo tal que $K \subset E \subsetneq L$ y $f(x)$ se descompone en E/K.

  Como $F \subset K$ lo anterior implica que existe un campo E tal que $F \subset E \subsetneq L$ y $f(x)$ se descompone en[1] E/F. Contradiciendo el hecho de que L es campo de descomposición de $f(x)$ sobre F.

□

[1] Esto es consecuencia de que si $f(x) \in F[x]$ y $f(x) = c \cdot g(x)$ con $c \in K$ y $g(x) \in E[x]$ mónico, entonces $c \in F$ (demuéstralo por contradicción).

El polinomio mínimo en una extensión finita L/F que satisface $F = L_{\mathrm{Gal}(L/F)}$

Lema 3

Supongamos que L/F es una extensión finita y que $\alpha \in L$. Denotemos por $\alpha_1, \ldots, \alpha_n$ a los distintos elementos del conjunto finito[2] $\{\sigma\alpha \mid \sigma \in \mathrm{Gal}(L/F)\}$. Es decir, denotemos

$$\{\sigma\alpha \mid \sigma \in \mathrm{Gal}(L/F)\} = \{\alpha_1, \ldots, \alpha_n\}$$

donde $\alpha_i \neq \alpha_j$ para $i \neq j$.

Si $F = L_{\mathrm{Gal}(L/F)}$ (es decir, F es el campo fijo de $\mathrm{Gal}(L/F)$), entonces

$$m_{\alpha,F}(x) = \prod_{i=1}^{n}(x - \alpha_i).$$

En particular, tenemos el siguiente resultado: Si L/F es finita y $F = L_{\mathrm{Gal}(L/F)}$, entonces L/F es separable.

[2] Este conjunto es finito porque $\mathrm{Gal}(L/F)$ es finito (recuerda que el grupo de Galois de una extensión finita es finito).

Demostración. Denotemos

$$h_\alpha(x) = \prod_{i=1}^{n}(x - \alpha_i)$$

Queremos ver que $h_\alpha(x)$ es el polinomio mínimo de α sobre F. El lector podrá fácilmente verificar que para esto basta probar que $h_\alpha(x)$ tiene coeficientes en F y que $h_\alpha(x)$ es irreducible en $F[x]$.

Empecemos por ver que $h_\alpha(x)$ tiene coeficientes en F. Como $F = L_{\mathrm{Gal}(L/F)}$, basta probar que los coeficientes de $h_\alpha(x)$ son fijos bajo cualquier elemento de $\mathrm{Gal}(L/F)$. Supongamos que

$$h_\alpha(x) = a_m x^m + \cdots + a_1 x + a_0$$

Entonces para toda $\sigma \in \mathrm{Gal}(L/F)$ tenemos

$$\sigma(a_m)\sigma(x)^m + \cdots + \sigma(a_1)\sigma(x) + \sigma(a_0) = \sigma\left(a_m x^m + \cdots + a_1 x + a_0\right)$$
$$= \sigma\left(\prod_{i=1}^{n}(x - \alpha_i)\right) = \prod_{i=1}^{n}\left(\sigma(x) - \sigma(\alpha_i)\right) = \prod_{i=1}^{n}(\sigma(x) - \alpha_i)$$
$$= a_m\sigma(x)^m + \cdots + a_1\sigma(x) + a_0 = h_\alpha(\sigma(x))$$

Mas aun, si definimos $g_\alpha(x) = \sigma(a_m)x^m + \cdots + \sigma(a_1)x + \sigma(a_0) \in L[x]$, entonces la ecuación anterior implica que

$$g_\alpha(\sigma(x)) = \sigma(a_m)\sigma(x)^m + \cdots + \sigma(a_1)\sigma(x) + \sigma(a_0) = h_\alpha(\sigma(x))$$

Como σ es un automorfismo de L, entonces lo anterior implica que $g_\alpha(x) = h_\alpha(x)$. Comparando sus coeficientes obtenemos $\sigma(\alpha_i) = \alpha_i$ para toda $i \in \{1, \ldots, n\}$ y como σ es un elemento arbitrario de $\mathrm{Gal}(L/F)$, lo anterior implica que $\alpha_i \in L_{\mathrm{Gal}(L/F)} = F$. Por lo tanto $h_\alpha(x)$ tiene coeficientes en F.

Ahora, veamos que $h_\alpha(x)$ es irreducible en $F[x]$.

Supongamos que

$$h_\alpha(x) = p_1(x) \cdots p_l(x) \text{ con } p_j(x) \in F[x] \text{ para toda } j = 1, \ldots, l$$

es la factorización en irreducibles de $h_\alpha(x)$ en $F[x]$ (cabe recalcar que esta factorización es posible porque $h_\alpha(x)$ tiene coeficientes en $F[x]$).

Como α es raíz de $h_\alpha(x)$, entonces α también es raíz de alguno de los $p_j(x)$, digamos $p_1(x)$. Pero $\alpha_1 = \sigma_1\alpha, \ldots, \alpha_n = \sigma_n\alpha$ también son raíces de $p_1(x)$ (c.f. proposición 2.18.4) y por lo tanto,

$$\prod_{i=1}^{n}(x - \alpha_i) \text{ divide a } p_1(x) \text{ en } F[x].$$

Como $p_1(x)$ es irreducible, acabamos de demostrar que $h_\alpha(x) = \prod_{i=1}^{n}(x - \alpha_i)$ divide (en $F[x]$) a un polinomio irreducible en $F[x]$ y por lo tanto, $h_\alpha(x)$ también es irreducible en $F[x]$. $\square$

Comentario

En lo que sigue, demostraremos una equivalencia muy importante. Específicamente, demostraremos que si L/F es una extensión finita, entonces las siguientes tres condiciones son equivalentes:

1. L es el campo de descomposición sobre F de un polinomio separable.
2. F es el campo fijo de $\mathrm{Gal}(L/F)$ o equivalentemente, $F = L_{\mathrm{Gal}(L/F)}$.
3. L/F es una extensión normal y separable.

Como es usual, demostraremos que (1) $\implies$ (2), que (2) $\implies$ (3), y que (3) $\implies$ (1). Como la demostración de cada una de estas implicaciones es un poco larga, las enunciamos como lemas.

Lema 4

(1) $\implies$ (2): Supongamos que L/F es una extensión finita. Si L es el campo de descomposición sobre F de un polinomio separable, entonces F es el campo fijo de $\mathrm{Gal}(L/F)$ (o equivalentemente, $F = L_{\mathrm{Gal}(L/F)}$).

Demostración. Supongamos que L es el campo de descomposición sobre F de un polinomio separable $f(x) \in F[x]$ y denotemos por K al campo fijo de $\mathrm{Gal}(L/F)$, es decir, $K = L_{\mathrm{Gal}(L/F)}$. Queremos demostrar que $F = K$.

Anteriormente mencionamos que si $H \leq \mathrm{Gal}(L/F)$, entonces L_H es un subcampo de L que contiene a F. En particular, $F \subset K \subset L$. Como L es el campo de descomposición de $f(x)$ sobre F, entonces el lema 2 implica que L también es el campo de descomposición de $f(x)$ sobre K. En particular, como $f(x)$ es separable, el corolario 2.19.2 implica que

$$[L : F] = \left|\mathrm{Gal}(L/F)\right| \quad \text{y} \quad [L : K] = \left|\mathrm{Gal}(L/K)\right|. \tag{2}$$

Pero por el lema 1, $\mathrm{Gal}(L/F) = \mathrm{Gal}(L/L_{\mathrm{Gal}(L/F)}) = \mathrm{Gal}(L/K)$ y por lo tanto

$$[L : F] = \left|\mathrm{Gal}(L/F)\right| = \left|\mathrm{Gal}(L/K)\right| = [L : K] \tag{3}$$

Por otro lado, como $F \subset K \subset L$ también tenemos que $[L : F] = [L : K][K : F]$. Usando esto y (3) es fácil ver que $[K : F] = 1$ o equivalentemente, $K = F$. $\square$

Lema 5

(2) $\implies$ (3): Supongamos que L/F es una extensión finita. Si F es el campo fijo de $\mathrm{Gal}(L/F)$, entonces L/F es una extensión normal y separable.

Demostración. Supongamos que $F = L_{\mathrm{Gal}(L/F)}$. En el lema 3 vimos que en este caso L/F es separable. Resta probar que L/F es normal (es decir, que todo polinomio irreducible en $F[x]$ que tenga una raíz en L se descompone en L/F). Para esto, supongamos que $f(x) \in F[x]$ es un polinomio irreducible en $F[x]$ que tiene una raíz en L, digamos $\alpha \in L$. Es fácil ver que esto implica que $f(x) =^3 c \cdot m_{\alpha,F}(x)$ para alguna $c \in F$ y que por lo tanto $f(x)$ es separable[4]. $\square$

[3] La parte de que c esta en F y no en L es porque si $c \in L \setminus F$ entonces $c \cdot m_{\alpha,F}(x)$ no pertenece a $F[x]$ porque es mónico y lo anterior implicaría que su primer coeficiente no pertenece a F.

[4] Recuerda que $m_{\alpha,F}(x)$ es separable porque L/F es separable.

Lema 6

(3) $\implies$ (1): Supongamos que L/F es una extensión finita. Si L/F es una extensión normal y separable, entonces L es el campo de descomposición sobre F de un polinomio separable.

Demostración. Como L/F es finita, existen $\alpha_1, \ldots, \alpha_n \in F$ algebraicos sobre L tales que $L = F(\alpha_1, \ldots, \alpha_n)$. Usando esto, supongamos que

$$\{m_{\alpha_1,F}(x), \ldots, m_{\alpha_n,F}(x)\} = \{f_1(x), \ldots, f_l(x)\} \text{ donde } f_i(x) \neq f_j(x) \text{ si } i \neq j$$

En palabras, $f_1(x), \ldots, f_l(x)$ son todos los distintos elementos de $\{m_{\alpha_1,F}(x), \ldots, m_{\alpha_n,F}(x)\}$. Con esta notación, definimos

$$f(x) = f_1(x)f_2(x)\cdots f_l(x) \in F[x].$$

Veamos que $f(x)$ es separable. Como L/F es separable, entonces cada uno de los $m_{\alpha_i,F}(x)$ es separable. Usando esto y la definición de $f(x)$ es fácil ver que para demostrar que $f(x)$ es separable, basta probar que $f_i(x)$ y $f_j(x)$ no comparten raíces si $i \neq j$.

A manera de contradicción, supongamos que existen i, j distintos tales que $f_i(x)$ y $f_j(x)$ que comparten una raíz, llamémosle β. Esto implicaría que $f_i(x) = m_{\beta,F}(x)$ y $f_j(x) = m_{\beta,F}(x)$ de donde $f_i(x) = f_j(x)$, contradiciendo nuestra elección de los $f_i(x)$'s. Por lo tanto, $f(x)$ es separable.

Finalmente, veamos que $L = F(\alpha_1, \ldots, \alpha_n)$ es el campo de descomposición de $f(x)$ sobre F verificando las dos condiciones de la definición de campo de descomposición:

- *$f(x)$ se descompone en L/F*: Como L/F es normal y $f(x)$ es un polinomio irreducible[5] en $F[x]$ que tiene una raíz en L (cualquiera de las α_i), entonces $f(x)$ se descompone en L/F.
- *No existe E campo tal que $F \subset E \subsetneq L = F(\alpha_1, \ldots, \alpha_n)$ y $f(x)$ se descompone en E/F*: Supongamos lo contrario. Como $F \subset E \subsetneq F(\alpha_1, \ldots, \alpha_n)$, entonces existe $i \in \{1, \ldots, n\}$ tal que $\alpha_i \notin E$; y como $f(x)$ se descompone en E/F, entonces existen $c \in F$ y $\beta_1, \ldots, \beta_m \in E$ tales que

$$f(x) = c \cdot (x - \beta_1)(x - \beta_2) \cdots (x - \beta_m). \tag{4}$$

  Por otro lado, como $\alpha_i \in L$ es raíz de $f(x)$, existe $g(x) \in L[x]$ tal que

$$f(x) = (x - \alpha_i)g(x). \tag{5}$$

  Usando (4), (5), y el hecho de que $E[x]$ es un DFU, obtenemos que $x - \alpha_i = x - \beta_j$ para alguna $j \in \{1, \ldots, m\}$. Esto implica $\alpha_i = \beta_j \in E$, contradiciendo $\alpha_i \notin E$. Por lo tanto, no existe E campo tal que $F \subset E \subsetneq L = F(\alpha_1, \ldots, \alpha_n)$ y $f(x)$ se descompone en E/F.

□

[5] Es fácil verificar que el producto de polinomios irreducibles es un polinomio irreducible.

Una equivalencia muy importante

Ahora si, estamos listos para presentar la (muy importante) equivalencia mencionada anteriormente:

Teorema 7

Supongamos que L/F es una extensión finita. Son equivalentes:

1. L es el campo de descomposición sobre F de un polinomio separable.
2. F es el campo fijo de $\mathrm{Gal}(L/F)$ o equivalentemente, $F = L_{\mathrm{Gal}(L/F)}$.
3. L/F es una extensión normal y separable.

Extensiones de Galois

Definición

Supongamos que L/F es una extensión finita. Decimos que L/F es una **extensión de Galois** si L/F satisface cualquiera de las siguientes (equivalentes) condiciones.

- L es el campo de descomposición de un polinomio separable en $F[x]$.
- F es el campo fijo de $\mathrm{Gal}(L/F)$ o equivalentemente, $F = L_{\mathrm{Gal}(L/F)}$.
- L/F es una extensión normal y separable.

Por ejemplo,

- $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ es de Galois porque es el campo de descomposición de $(x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$.
- $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es de Galois porque no es normal: $x^3 - 2 \in \mathbb{Q}[x]$ es un polinomio que tiene una raíz en $\mathbb{Q}(\sqrt[3]{2})$ pero no se descompone en $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

El polinomio mínimo en una extensión de Galois

Corolario 8

Supongamos que L/F es una extensión finita y que $\alpha \in L$. Si L/F es de Galois y $\alpha_1, \ldots, \alpha_n$ son los distintos elementos de $\{\sigma\alpha \mid \sigma \in \mathrm{Gal}(L/F)\}$, entonces

$$m_{\alpha,F}(x) = \prod_{i=1}^{n}(x - \alpha_i).$$

Demostración. En el lema 3 vimos que si $F = L_{\mathrm{Gal}(L/F)}$ (es decir, F es el campo fijo de $\mathrm{Gal}(L/F)$), entonces

$$m_{\alpha,F}(x) = \prod_{i=1}^{n}(x - \alpha_i).$$

Como L/F es Galois si y solo si $F = L_{\mathrm{Gal}(L/F)}$, obtenemos lo deseado. $\square$

$L/L_{\mathrm{Gal}(L/F)}$ es una extensión de Galois

Corolario 9

Si L/F es una extensión finita, entonces $L/L_{\mathrm{Gal}(L/F)}$ es de Galois.

Demostración. Usaremos la equivalencia

$$E/K \text{ es de Galois } \iff K = L_{\mathrm{Gal}(E/K)}.$$

Como en nuestro caso $E = L$ y $K = L_{\mathrm{Gal}(L/F)}$, queremos ver que

$$\underbrace{L_{\mathrm{Gal}(L/F)}}_{K} = \underbrace{L_{\mathrm{Gal}(L/L_{\mathrm{Gal}(L/F)})}}_{L_{\mathrm{Gal}(E/K)}}.$$

Sin embargo, esto es consecuencia inmediata de que

$$\mathrm{Gal}(L/F) = \mathrm{Gal}(L/L_{\mathrm{Gal}(L/F)}).$$

□

Un campo intermedio en una extensión de Galois

Corolario 10

Supongamos que F, K, L son campos tales que $F \subset K \subset L$. Si L/F es de Galois, entonces

1. L/K también es de Galois
2. K/F no necesariamente es de Galois
3. K/F es de Galois $\iff$ K/F es normal

Demostración.

1. Supongamos que L/F es de Galois. Usando la equivalencia "L/F es de Galois $\iff$ L es el campo de descomposición sobre F de un polinomio separable" y el lema 2 obtenemos que L/K también es de Galois.

2. Considera

$$F = \mathbb{Q}, \quad K = \mathbb{Q}(\sqrt[4]{2}), \quad L = \mathbb{Q}(i, \sqrt[4]{2}).$$

L/F es una extensión de Galois porque es el campo de descomposición de $x^4 - 2$. Sin embargo, K/F no es de Galois porque no es normal: $x^4 - 2$ es un polinomio que tiene una raíz en K pero no se descompone en K/F.

3. $\Longrightarrow$) Si K/F es de Galois, en particular K/F es normal.

   $\Longleftarrow$) Supongamos que L/F es de Galois y que K/F es normal. Para ver que K/F es de Galois, basta probar que K/F es separable. Es decir, basta probar que todo $\alpha \in K$ es separable sobre F. Sin embargo, esto es consecuencia inmediata de que L/F es separable (pues es de Galois) y de que $F \subset K \subset L$.

□

Comentario

Una consecuencia inmediata del corolario anterior es el siguiente resultado:

Supongamos que F, K, L son campos tales que $F \subset K \subset L$.

- Si $F = L_{\mathrm{Gal}(L/F)}$, entonces $K = L_{\mathrm{Gal}(K/F)}$.
- Si L/F es normal y separable, entonces L/K también es normal y separable.

Notemos que si hubiéramos intentado demostrar esto sin ocupar el material presentado anteriormente, nuestra tarea seria mas complicada que la demostración del lema 2.

Por otro lado, recordemos que si L es un campo de descomposición sobre F de un polinomio separable, entonces $\mathrm{Gal}(L/F) = [L : F]$ (c.f. corolario 2.19.2). En particular,

$$L/F \text{ es de Galois } \implies \left|\mathrm{Gal}(L/F)\right| = [L : F].$$

En lo que sigue veremos que la implicación conversa también es cierta.

$\left|\mathrm{Gal}(L/F)\right|$ divide a $[L:F]$

Corolario 11

Si L/F es una extensión finita, entonces

$$[L:F] = \left|\mathrm{Gal}(L/F)\right| [L_{\mathrm{Gal}(L/F)} : F].$$

En particular, $\left|\mathrm{Gal}(L/F)\right|$ divide a $[L:F]$.

Demostración. Denotemos $K = L_{\mathrm{Gal}(L/F)}$. Entonces

$$[L:K] = \left|\mathrm{Gal}(L/K)\right|$$

porque $L/K = L/L_{\mathrm{Gal}(L/F)}$ es de Galois y

$$\left|\mathrm{Gal}(L/K)\right| = \left|\mathrm{Gal}(L/F)\right|$$

porque $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/L_{\mathrm{Gal}(L/F)}) = \mathrm{Gal}(L/F)$. Por lo tanto,

$$[L:F] = [L:K][K:F] = \left|\mathrm{Gal}(L/K)\right| [K:F] = \left|\mathrm{Gal}(L/F)\right| [K:F].$$

Otra caracterización de las extensiones de Galois

Proposición 12

Supongamos que L/F es una extensión finita. Entonces

$$L/F \text{ es de Galois } \iff \left|\mathrm{Gal}(L/F)\right| = [L:F].$$

Demostración. Por el comentario anterior, basta ver la implicación "$\Longleftarrow$". Por eso, supongamos que L/F es tal que $\left|\mathrm{Gal}(L/F)\right| = [L:F]$. Para ver que L/F es de Galois veremos que $F = L_{\mathrm{Gal}(L/F)}$.

Por la proposición anterior,

$$[L:F] = \left|\mathrm{Gal}(L/F)\right| [L_{\mathrm{Gal}(L/F)} : F].$$

Juntando esto con $\left|\mathrm{Gal}(L/F)\right| = [L:F]$ obtenemos $[L_{\mathrm{Gal}(L/F)} : F] = 1$ o equivalentemente, $F = L_{\mathrm{Gal}(L/F)}$. □

Comentario

Por lo anterior, tenemos que una extensión finita L/F es de Galois si y solo si L/F satisface cualquiera de las siguientes (equivalentes condiciones)

- L es el campo de descomposición de un polinomio separable en $F[x]$.
- F es el campo fijo de $\mathrm{Gal}(L/F)$ o equivalentemente, $F = L_{\mathrm{Gal}(L/F)}$.
- L/F es una extensión normal y separable.
- $\left|\mathrm{Gal}(L/F)\right| = [L : F]$.

Finalizamos esta sección con una aplicación de la proposición anterior.

$\mathbb{F}_{p^n}/\mathbb{F}_p$ desde el punto de vista de teoría de Galois

Supongamos que $p \in \mathbb{Z}_{\geq 0}$ es primo y que $n \in \mathbb{Z}_{\geq 0}$. Por la proposición 2.13.8, $\mathbb{F}_{p^n}$ es el campo de descomposición de $x^{p^n} - x$ sobre $\mathbb{F}$. En particular, $\mathbb{F}_{p^n}/\mathbb{F}_p$ es de Galois y

$$\left|\mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)\right| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n.$$

Por otro lado, recuerda que la sección 2.13 introdujimos al *homomorfismo de Frobenius* dado por

$$\begin{aligned} \sigma : \mathbb{F}_{p^n} &\to \mathbb{F}_{p^n} \\ \alpha &\mapsto \alpha^p \end{aligned}$$

Es trivial verificar que σ es inyectivo; y como $\mathbb{F}_{p^n}$ es finito, entonces también es suprayectivo. Por lo tanto, σ es un automorfismo y como $\alpha^p = \alpha$ para toda $\alpha \in \mathbb{F}_p$, entonces $\sigma \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

En lo que sigue, veremos que $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ es un grupo cíclico generado por σ.

Primero, notemos que

$$\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\alpha^p) = (\alpha^p)^p = \alpha^{p^2}$$

y en general,

$$\sigma^k(\alpha) = \alpha^{p^k} \text{ para toda } k \in \mathbb{Z}_{>0}. \tag{6}$$

Por otro lado, notemos que si $F^\times$ es el grupo multiplicativo de F, entonces $|F^\times| = p^n - 1$ y por lo tanto, (por un resultado básico de teoría de grupos)

$$\alpha^{p^n-1} = 1 \text{ para toda } \alpha \in F^\times.$$

Multiplicando por α y observando que esta ecuación también se satisface para $\alpha = 0$, obtenemos que

$$\alpha^{p^n} = \alpha \text{ para toda } \alpha \in F. \tag{7}$$

Juntado (6) y (7) obtenemos que $\sigma^n = \mathrm{id}_{\mathbb{F}_{p^n}}$.

Veamos que si $k \in \mathbb{Z}$ es tal que $1 \leq k < n$, entonces $\sigma^k \neq \mathrm{id}$.

Procedamos por contradicción, es decir, supongamos que existe $k \in \mathbb{Z}$ tal que $1 \leq k < n$ y $\sigma^k = \mathrm{id}_{\mathbb{F}_{p^n}}$. Entonces

$$\alpha^{p^k} = \sigma^k(\alpha) = \alpha \text{ para toda } \alpha \in \mathbb{F}_{p^n}$$

Como $|\mathbb{F}_{p^n}| = p^n$, lo anterior implica que el polinomio $x^{p^k} - x$ tiene p^n distintas raíces, lo cual es imposible.

Ahora bien, acabamos de demostrar que $\sigma^n = \mathrm{id}_{\mathbb{F}_{p^n}}$ y $\sigma^k \neq \mathrm{id}$ para $k \in \{1, \ldots, n-1\}$. Como $\left|\mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)\right| = n$, entonces lo anterior implica[6] que $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ es un grupo cíclico generado por σ.

En resumen,

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\sigma\rangle \cong \mathbb{Z}_n \text{ donde } \sigma(\alpha) = \alpha^p.$$

Cabe recalcar que el isomorfismo $\langle\sigma\rangle \cong \mathbb{Z}_n$ es consecuencia de que (i) $\sigma^n = \mathrm{id}_{\mathbb{F}_{p^n}}$, (ii) $\sigma^k \neq \mathrm{id}$ para $k \in \{1, \ldots, n-1\}$, y (iii) un resultado básico de teoría de grupos.

[6] Por un resultado básico de teoría de grupos.