Campos finitos y teoría de Galois

José Ibrahim Villanueva Gutiérrez

1. Campos finitos

1.0.1. Campos finitos

Recordemos la siguiente definición.

Definición 1. Un campo K es un conjunto con dos operaciones $+$ y $*$ con las cuales $(K,+)$ y $(K^\times,*)$ son grupos abelianos y la multiplicación distribuye sobre la suma:

$$a*(b+c)=(a*b)+(a*c) \quad \text{para todo} \quad a,b,c\in K.$$

Decimos que un campo es finito si K tiene un número finito de elementos. Generalmente denotamos 0 al neutro de la operación $+$ y 1 al neutro de $*$.

Ejemplo 1.
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son campos infinitos.
- Para p primo $\mathbb{Z}/p\mathbb{Z}$ es un campo finito.

Recordemos la siguiente definición.

Definición 2. Si L y K son campos y $K\subseteq L$, decimos que L es una extensión de K, y escribimos L/K.

Si L es una extensión de K entonces, L es un grupo abeliano con la suma, y los axiomas de espacio vectorial sobre K se satisfacen, al considerar la multiplicación por escalares simplemente como la multiplicación de elementos de K por elementos (¡vectores!) de L. Es decir, una extensión de campos L/K es un espacio vectorial L sobre K. La dimensión de este espacio vectorial es llamada el grado de la extensión y lo denotamos $[L:K]$.

Ejemplo 2.
- $\mathbb{C}/\mathbb{R}$ es una extensión de grado $[\mathbb{C}:\mathbb{R}]=2$.
- Sea Φ_n el n-ésimo polinomio ciclotómico, y α una raíz de Φ_n entonces $\mathbb{Q}(\alpha)$ es un espacio vectorial de dimensión $\varphi(n)$ sobre $\mathbb{Q}$.

Sea F un campo finito. La aplicación

$$\mathbb{Z}\longrightarrow F$$

$$n\mapsto n\cdot 1,$$

es claramente un morfismo de anillos, su kernel no puede ser 0 porque un morfismo de anillos con kernel trivial es inyectivo, entonces tiene que ser un ideal de $\mathbb{Z}$, además este ideal tiene que ser generado por un número primo ya que F es un dominio entero.

Por el teorema de isomorfismo de anillos, tenemos que la imagen del morfismo precedente es isomorfa a $\mathbb{Z}/p\mathbb{Z}$, para algún p primo. El entero p es llamado la característica de F y el subcampo de F que es isomorfo a $\mathbb{Z}/p\mathbb{Z}$ lo denotamos $\mathbb{F}_p$. Toda extensión L de F (o subcampo L de F) contiene a $\mathbb{F}_p$, por lo tanto un tal cuerpo L es un $\mathbb{F}_p$-espacio vectorial, isomorfo a una suma directa de $[L:\mathbb{F}_p]$ copias de $\mathbb{F}_p$. Claramente, L es finito sí y solamente si $[L:\mathbb{F}_p]$ es finito, en este caso tenemos $|L|=p^{[L:\mathbb{F}_p]}$.

Proposición 1. *El número de elementos de un cuerpo finito es una potencia de su característica (que es un número primo).*

Teorema 1. *Todo subgrupo finito del grupo multiplicativo de un campo es cíclico.*

Demostración: Sea G un subgrupo multiplicativo finito de orden n de $K^\times$. Para cada divisor de d de n definimos

$$\rho(d) = |\{x \in G \mid x \text{ tiene orden } d\}|.$$

Claramente tenemos

$$n = \sum_{d|n} \rho(d),$$

además, la ecuación $X^d - 1$ tiene a lo más d raíces en el cuerpo K. Si G contiene un elemento x de orden d, las raíces de $X^d - 1$ son exactamente las potencias de x, y de estas $\varphi(d)$ son exactamente de orden d. Tenemos entonces $\rho(d) = 0$ o $\varphi(d)$ para cada d, y por lo tanto (por el ejercicio 1)

$$\rho(n) = n - \sum_{\substack{d \mid n \\ d \neq n}} \rho(d) \geqslant n - \sum_{\substack{d \mid n \\ d \neq n}} \varphi(d) = \varphi(n) > 0,$$

por lo tanto existe un $x \in G$ de orden n, y todos los demás elementos de G son potencias de x.

■

Corolario 1. *El grupo multiplicativo de un cuerpo finito con q elementos es cíclico de orden $q - 1$.*

Ejercicio 1. Sea $f : \mathbb{N} \to \mathbb{C}$ una función aritmética. Decimos que f es multiplicativa si $f(ab) = f(a)f(b)$ para $(a, b) = 1$.

1. Demuestre que la función

$$F(n) = \sum_{d \mid n} f(d),$$

   es multiplicativa.

2. Sea φ la función de Euler, demuestre que

$$\sum_{d \mid n} \varphi(d) = n.$$

1.0.2. La retícula de las extensiones de $\mathbb{F}_p$

Definición & Proposición 1. *Un campo C es algebraicamente cerrado si satisface alguna de las siguientes condiciones equivalentes:*

1. *Todo polinomio no constante $f \in C[X]$ tiene al menos una raíz en C.*
2. *Todo polinomio no constante $f \in C[X]$ se descompone sobre C.*
3. *Todo polinomio irreducible $f \in C[X]$ es lineal.*
4. *C no tiene extensiones algebraicas propias.*

Demostración:

- (*1.* $\Rightarrow$ *2.*): Podemos escribir $f = (X - \alpha_1)g$, y proceder inductivamente para demostrar que cualquier polinomio no constante es el producto de factores lineales.
- (*2.* $\Rightarrow$ *3.*): Si f es un polinomio irreducible en $C[X]$, entonces f es no constante. Pero un polinomio no constante es producto de factores lineales, y como f es irreducible entonces f mismo tiene que ser lineal.
- (*3.* $\Rightarrow$ *4.*): Sea E una extension algebraica de C. Si $\alpha \in E$, sea f_α el polinomio mínimo de α sobre C. f_α es irreducible, por lo tanto de la forma $X - \alpha$, pero entonces $\alpha \in C$, es decir $E = C$.

- (*4. ⇒ 1.*): Sea f un polinomio no constante en $C[X]$, sea α una raíz de f, entonces $C(\alpha)$ es una extensión algebraica de C, sin embargo C no tiene extensiones algebraicas propias, es decir, $\alpha \in C$.

■

Definición 3. Una extensión C de F es una cerradura algebraica de F, si C es algebraica sobre F y C es algebraicamente cerrado.

Fijemos una cerradura algebraica $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$. Vamos a ver que es posible describir de manera sencilla todas las extensiones finitas de $\overline{\mathbb{F}}_p$:

Teorema 2. *Para todo entero $n \geqslant 1$ existe un subcampo de $\overline{\mathbb{F}}_p$ con $q = p^n$ elementos que denotamos $\mathbb{F}_q$. Este es el campo formado por las raíces en $\overline{\mathbb{F}}_p$ del polinomio separable $\Omega_q(X) = X^q - X$.*

Demostración: Sea F un subcampo de $\overline{\mathbb{F}}_p$ con q elementos. En este caso, $q-1$ elementos del grupo multiplicativo $F^\times$ verifican la identidad $x^{q-1} = 1$; y los q elementos de F son realmente las q raíces del polinomio $\Omega_q(X) = X(X^{q-1} - 1)$.

Ahora consideremos el polinomio $\Omega_q(X)$. Notemos que $\Omega_q(X)$ es separable porque tenemos $\Omega'_q(X) = q-1$, y denotemos F el conjunto de sus q raíces distintas en la cerradura algebraica $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$. Para x y y en F tenemos:

$$(x+y)^q = x^q + y^q = x + y \qquad \text{y} \qquad (xy)^q = x^q y^q = xy,$$

lo que demuestra que, como F es cerrado bajo multiplicación y resta, y además contiene contiene 1: F es un subanillo de $\overline{\mathbb{F}}_p$. Como F es un dominio entero y finito, es un campo con q elementos.

■

Escolio. *Para todo $n \geqslant 1$ existe un único (salvo isomorfismo) campo de p^n elementos: $\mathbb{F}_{p^n}$.*

Demostración: Un campo F de p^n elementos, es algebraico sobre algún campo con un número primo de elementos y este se identifica con $\mathbb{F}_p$, entonces F se encaja en la cerradura algebraica de $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$ y su imagen es claramente $\mathbb{F}_{p^n}$.

■

Proposición 2. *Sean m y n dos números naturales. Tenemos entonces en $\overline{\mathbb{F}}_p$:*

$$\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \;\Leftrightarrow\; n|m.$$

En particular tenemos: $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^{m.c.d.(n,m)}}$ et $\mathbb{F}_{p^n}\mathbb{F}_{p^m} = \mathbb{F}_{p^{m.c.m.(m,n)}}$

Demostración: Si $\mathbb{F}_{p^m}$ contiene $\mathbb{F}_{p^n}$, entonces es un $\mathbb{F}_{p^n}$-espacio vectorial de dimensión finita, digamos k. Se sigue que $p^m = (p^n)^k = p^{nk}$, es decir $m = nk$. Del otro lado, de la igualdad $m = nk$ obtenemos lo siguiente:

$$x^{p^n} = x \;\Rightarrow\; x^{p^m} = x^{p^{nk}} = (\cdots(x^{p^n})^{p^n}\cdots)^{p^n} = x,$$

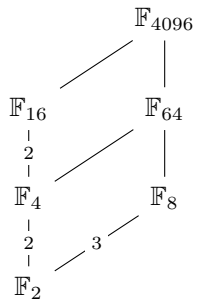
i.e. $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$.

Las identidades de la intersección y de la composición son claras.

■

Ejercicio 2. Demuestre las identidades de la intersección y de la composición.

Ejemplo 3. A continuación presentamos el diagrama de subcampos de $\mathbb{F}_{4096}$:



Notemos que $\mathbb{F}_8$ (extensión cúbica de $\mathbb{F}_2$) no contiene $\mathbb{F}_4$ (extensión cuadrada de $\mathbb{F}_2$).

Para poder tomar en cuenta ahora las extensiones infinitas de $\mathbb{F}_p$ tenemos que introducir el conjunto de los números supernaturales $\mathbb{S}$, i.e. el conjunto de los productos formales

$$\bar{n} = \prod p^{\nu_p(\bar{n})},$$

donde p recorre el conjunto de los números primos, y el exponente $\nu_p(\bar{n})$ toma valores en $\overline{\mathbb{N}} = \mathbb{N} \cup \{0, \infty\}$. Definimos de manera evidente el producto, el máximo común divisor y el mínimo común múltiplo de una familia de elementos en $\mathbb{S}$. Una vez establecido esto, tenemos el siguiente teorema:

Teorema 3. *La aplicación*

$$\mathbb{S} \to \overline{\mathbb{F}}_p$$
$$\bar{n} \mapsto \mathbb{F}_{p^{\bar{n}}} = \bigcup_{n|\bar{n}} \mathbb{F}_{p^n}$$

(donde la unión de la derecha es sobre todos los subcampos finitos de $\overline{\mathbb{F}}_p$ para los cuales n divide $\bar{n}$) es una biyección creciente del conjunto $\mathbb{S}$ de los números supernaturales (ordenada por divisibilidad) sobre el conjunto (ordenado por inclusión) de los subcampos de $\overline{\mathbb{F}}_p$, donde los subcampos finitos corresponden a los números naturales.

Demostración: Primero notemos que $\mathbb{F}_{p^{\bar{n}}}$ es efectivamente, un subcampo de $\overline{\mathbb{F}}_p$: para x y y en $\mathbb{F}_{p^{\bar{n}}}$, tenemos $x \in \mathbb{F}_{p^m}$ y $y \in \mathbb{F}_{p^n}$ para dos naturales m y n que dividen $\bar{n}$, entonces $\mathbb{F}_p[x, y] \subseteq \mathbb{F}_{p^{\mathrm{m.c.m}(m,n)}} \subset \mathbb{F}_{p^{\bar{n}}}$ como esperado, ya que el mínimo común múltiplo de m y n divide $\bar{n}$ (Prop. 2).

De manera explícita, tenemos

$$x \in \mathbb{F}_{p^{\bar{n}}} \quad \Leftrightarrow \quad \exists\, n \,|\, \bar{n} \quad \text{tal que} \quad x \in \mathbb{F}_{p^n} \quad \Leftrightarrow \quad \exists\, n | \bar{n} \quad \text{tal que} \quad \deg(x) \,|\, n,$$

es decir $x \in \mathbb{F}_{p^{\bar{n}}} \Leftrightarrow \deg(x) \,|\, \bar{n}$; de donde deducimos que la aplicación es inyectiva.

Queda verificar que todo subcampo F de $\overline{\mathbb{F}}_p$ es de la forma $\mathbb{F}_{p^{\bar{n}}}$ para algún $\bar{n}$: dado F, definimos $\bar{n}$ como el mínimo común múltiplo $\bar{n} = \mathrm{m.c.m}_{\mathbb{F}_{p^n} \subset F}(n)$. De donde obtenemos que $\mathbb{F}_{p^{\bar{n}}} = \bigcup_{\mathbb{F}_{p^n} \subset F} \mathbb{F}_{p^n} = F$ (ya que F es la unión de sus subcampos finitos).

■

1.1. Teoría de Galois

1.1.1. Extensiones separables

Definición & Proposición 2. *Sea F un campo finito de característica p, y definamos*

$$\begin{aligned} \sigma : F &\longrightarrow F \\ \alpha &\mapsto \sigma(\alpha) = \alpha^p. \end{aligned}$$

Entonces σ es un automorfismo. En particular, si $\alpha \in F$, entonces $\alpha = \beta^p$ para algún $\beta \in F$.

Demostración: Tenemos $\sigma(1) = 1$ y

$$\sigma(\alpha + \beta) = (\alpha + \beta)^p = \alpha^p + \beta^p = \sigma(\alpha) + \sigma(\beta)$$

y además

$$\sigma(\alpha\beta) = (\alpha\beta)^p = \alpha^p \beta^p = \sigma(\alpha)\sigma(\beta),$$

por lo tanto σ es un monomorfismo. Pero una función inyectiva de un conjunto finito a si mismo es automáticamente sobreyectiva, de donde se sigue el resultado.

■

Lema 1. *Sobre un campo* F *de característica* p*, el polinomio irreducible* f *no es separable si y sólo sí* f' *es el polinomio constante 0, equivalentemente* $f \in F[X^p]$.

Demostración: ($\Rightarrow$) Sea f un polinomio irreducible. Si $f' \neq 0$, este es un polinomio de grado menor que f. Como f es irreducible, el máximo común divisor de f y f' es 1 o f, pero esto último no puede pasar por tener grados distintos. Entonces f es separable.

($\Leftarrow$) Si $f' = 0$, entonces m.c.d.$(f, f') = f$, entonces f no es separable.

En característica p, un entero n es cero si y sólo sí es un múltiplo de p, entonces se sigue que $f' = 0$ si y sólo si $f \in F[X^p]$.

■

Proposición 3. *Sobre un campo finito, todo polinomio es separable.*

Demostración: Supongamos que f es un polinomio irreducible sobre el campo F con raíces repetidas en un campo de descomposición. Entonces f es de la forma:

$$f(X) = a_0 + a_1X^p + \ldots + a_nX^{np} \quad \text{con} \quad a_i \in F.$$

Por el resultado precedente (2) para cada i existe un elemento $b_i \in F$ tal que $b_i^p = a_i$. Pero entonces

$$(b_0 + b_1X + \cdots + b_nX^n)^p = b_0^p + b_1^pX^p + \cdots + b_nX^{np} = f(X),$$

lo cual contradice la irreductibilidad de f.

■

Definición 4. Sea E una extensión de F y $\alpha \in E$, decimos que α es separable sobre F si α es algebraico sobre F y el polinomio mínimo f_α de α es un polinomio separable sobre F. Si todo elemento de E es separable sobre F, decimos que E es una extensión separable de F o que E/F es separable.

Ejercicio 3. Demuestre que si $F \leqslant K \leqslant E$ son extensiones de campos y E es separable sobre F, entonces K es separable sobre F y E es separable sobre K.

Nota: Del ejercicio precedente y de la proposición 3 se sigue que toda extensión E/F de subcampos finitos de $\overline{\mathbb{F}}_p$ es separable.

1.1.2. Extensiones normales

Sea E/F una extensión de campos. Ahora estamos interesados en el comportamiento de los monomorfismos definidos en E, especialmente los que fijan puntualmente a F. Tales monomorfismos son llamados F-monomorfismos y queremos ver su acción en las raíces de un polinomio en $F[X]$.

Lema 2. *Sea* $\sigma : E \to E$ *un* F*-monomorfismo, y supongamos que* $f \in F[X]$ *se descompone sobre* E*. Si* α *es una raíz de* f *en* E*, entonces también lo es* $\sigma(\alpha)$*. Por lo tanto* σ *permuta las raíces de* f*.*

Demostración: Sea $f(X) = b_nX^n + \ldots b_1X + b_0$ un polinomio en $F[X]$ y supongamos que $f(\alpha) = 0$. Entonces

$$\begin{aligned} \sigma(f(\alpha)) &= \sigma(b_n\alpha^n) + \ldots \sigma(b_1\alpha) + \sigma(b_0) \\ &= \sigma(b_n)\sigma(\alpha^n) + \ldots \sigma(b_1)\sigma(\alpha) + \sigma(b_0) \\ &= b_n\sigma(\alpha)^n + \ldots \sigma(b_1)\sigma(\alpha) + \sigma(b_0). \end{aligned}$$

■

Definición 5. Decimos que la extensión algebraica E/F es normal, si todo polinomio irreducible sobre F que tiene al menos una raíz en E se descompone sobre E. Es decir, si $\alpha \in E$, entonces todos los conjugados de α sobre F (i.e. todas las raíces del polinomio minimal f_α de α sobre F) pertenecen a E.

Teorema 4. *Una extension finita* E/F *es normal si y sólo si* E *es el campo de descomposición para algún polinomio* $f \in F[X]$.

Demostración: ($\Rightarrow$) Supongamos que E/F es normal. Sea $\alpha_1, \ldots, \alpha_n$ una base de E sobre F, y sea f_i el polinomio mínimo de α_i sobre F para $i = 1, \ldots, n$. Como f_i tiene una raíz α_i en E, f_i se descompone sobre E, entonces pasa lo mismo para $f = f_1 \cdots f_n$. Si f se descompone sobre un campo K tal que $F \subset K \subset E$, entonces cada α_i pertenece a K, y por lo tanto K coincide con E. Por lo tanto E es el campo de descomposición de f sobre F.

($\Leftarrow$) Sea E el campo de descomposición de f sobre F, donde las raíces de f son los α_i con $i = 1, \ldots, n$ (Base de E/F). Sea τ un F-monomorfismo de E en una cerradura algebraica de C de F. Por el Lema 2, τ permuta las raíces de f. Pero $F(\alpha_1, \ldots, \alpha_n) = E$, entonces $\tau(E) = E$. Es decir, τ es un automorfismo de E, por lo tanto E/F es normal.

■

Ejercicio 4. Sea $F \leqslant K \leqslant E$ una extensión de campos, donde E es una extensión finita de F. Demuestre que si E/F es normal, entonces E/K es normal.

Nota: Sabemos que el campo $\mathbb{F}_{p^n}$ de p^n elementos es el campo de descomposición del polinomio $\Omega_{p^n}(X) = X^{p^n} - X$ sobre F, entonces por el teorema 4 $\mathbb{F}_{p^n}/\mathbb{F}_p$ es normal. Esto combinado con el ejercicio anterior demuestra que toda extensión de campos finitos E/F es normal.

1.1.3. Grupo de automorfismos de un campo finito

Definición 6. Si E/F es una extensión de campos normal y separable, decimos que E/F es una extensión de Galois. Además si E/F es una extensión finita de Galois entonces hay exactamente $[E : F]$ F-automorfismos de E.

Definición 7. Si E/F es una extension de campos arbitraria, el grupo de Galois de la extensión, denotado $\mathrm{Gal}(E/F)$, es el conjunto de F-automorfismos de E, es decir

$$\mathrm{Gal}(E/F) = \{\sigma : E \xrightarrow{\sim} E \mid \sigma(x) = x \ \text{ para todo } \ x \in F\}.$$

Sea E/F una extensión de subcampos finitos de $\overline{\mathbb{F}}_p$, digamos $F = \mathbb{F}_q$ (con $q = p^t$) y $E = \mathbb{F}_{q^s}$ (con $s = [E : F]$). Por el Teorema 2, E es el cuerpo de las raíces del polinomio separable $\Omega_{q^s}(X) = X^{q^s} - X$. Vamos a ver que su grupo de Galois es cíclico:

Teorema 5. *Sea* E/F *una extensión de campos finitos, el grupo de Galois* $\mathrm{Gal}(E/F)$ *de los* F*-automorfismos de* E *es el grupo cíclico de orden* $[E : F]$ *generado por el automorfismo de Frobenius*

$$\sigma_q : x \mapsto x^q,$$

donde q *es el cardinal de* F.

Demostración: Tomemos un elemento primitivo x de E/F (por ejemplo, uno de los generadores del grupo cíclico $E^\times$). Su polinomio minimal sobre F, digamos $f_x(X)$, divide $\Omega_{q^s}(X)$ y tiene exactamente $s = [E : F]$ raíces (distintas) en E. Como E es igual a $F[x]$, cada F-automorfismo de E es únicamente determinado por la imagen de x que es una raíz arbitraria dentro de las s raíces de $f_x(X)$. El grupo $\mathrm{Gal}(E/F)$ tiene entonces cardinal s.

Como el operador de Frobenius $\sigma_q : x \mapsto x^q$ es claramente un F-automorfismo de E, todo el problema se convierte en estudiar que σ_q es de orden s. Ahora, para $k = 1, \ldots, s$, el campo invariante de σ_q^k en E es el conjunto de raíces del polinomio $X^{q^k} - X$ en $E = \mathbb{F}_{q^s}$, es decir $\mathbb{F}_{q^s} \cap \mathbb{F}_{q^k}$. Y esto es E solamente en el caso $k = s$.

■

Corolario 2. *Para cada potencia* $\mathfrak{q} = \mathfrak{p}^{\mathfrak{k}}$ *del número primo* $\mathfrak{p}$*, el subcampo de* $\mathfrak{q}$ *elementos de* $\overline{\mathbb{F}}_{\mathfrak{p}}$ *es el campo de invariantes de la potencia* $\mathfrak{k}$*-ésima del Frobenius* $\sigma_{\mathfrak{p}}$*. Además tenemos*

$$\mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}) = \sigma_{\mathfrak{p}}^{\mathbb{Z}}/\sigma_{\mathfrak{p}}^{\mathfrak{k}\mathbb{Z}} \simeq \mathbb{Z}/\mathfrak{k}\mathbb{Z}.$$

1.1.4. Grupo de automorfismos de $\overline{\mathbb{F}}_{\mathfrak{p}}$

Recordemos algunas cosas sobre el grupo $\mathrm{Gal}(\overline{\mathbb{F}}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}})$ de los automorfismos de $\overline{\mathbb{F}}_{\mathfrak{p}}$. Como $\overline{\mathbb{F}}_{\mathfrak{p}}$ es la unión de campos finitos $\mathbb{F}_{\mathfrak{p}^{\mathfrak{n}}}$ (para $\mathfrak{n} \in \mathbb{N}$), el grupo $\mathrm{Gal}(\overline{\mathbb{F}}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}})$ se interpreta como el límite proyectivo de los grupos de Galois finitos $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}^{\mathfrak{n}}}/\mathbb{F}_{\mathfrak{p}})$: Un elemento σ de $\mathrm{Gal}(\overline{\mathbb{F}}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}})$ es determinado por sus restricciones $\sigma_{\mathfrak{n}} = \sigma|_{\mathbb{F}_{\mathfrak{p}^{\mathfrak{n}}}}$; es decir, se expresa como una familia $(\sigma_{\mathfrak{n}})_{\mathfrak{n}} \in \prod_{\mathbb{F}_{\mathfrak{p}^{\mathfrak{n}}} \subset \overline{\mathbb{F}}_{\mathfrak{p}}} \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}^{\mathfrak{n}}}/\mathbb{F}_{\mathfrak{p}})$ de automorfismos finitos que satisfacen las condiciones de coherencia $\sigma|_{\mathbb{F}_{\mathfrak{p}^{\mathfrak{n}}}} = \sigma_{\mathfrak{m}}$, para todas las parejas de índices $(\mathfrak{m}, \mathfrak{n})$ ordenados por divisibilidad.

En nuestro caso, este límite

$$\mathrm{Gal}(\overline{\mathbb{F}}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}}) = \varprojlim_{\mathfrak{n}} \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}^{\mathfrak{n}}}/\mathbb{F}_{\mathfrak{p}})$$

es particularmente simple: El corolario anterior identifica $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}^{\mathfrak{n}}}/\mathbb{F}_{\mathfrak{p}})$ con $\mathbb{Z}/\mathfrak{n}\mathbb{Z}$, entonces $\mathrm{Gal}(\overline{\mathbb{F}}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}})$ con el límite inverso $\varprojlim \mathbb{Z}/\mathfrak{n}\mathbb{Z}$, es decir con el completado $\hat{\mathbb{Z}}$ de $\mathbb{Z}$ con la topología definida por los subgrupos de índice finito. Es decir:

Escolio. *El grupo de Galois* $\mathrm{Gal}(\overline{\mathbb{F}}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}})$ *es el grupo pro-finito isomorfo a* $\hat{\mathbb{Z}}$*, que es engendrado topológicamente por el automorfismo de Frobenius* $\sigma_{\mathfrak{p}}$*.*

Nota. *La teoria de Galois topológica establece una biyección entre las subextensiones de* $\overline{\mathbb{F}}_{\mathfrak{p}}$ *y los subgrupos cerrados de* $\mathrm{Gal}(\overline{\mathbb{F}}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}})$*, es decir los subgrupos cerrados de* $\hat{\mathbb{Z}}$*. Estos están en biyección con los números super naturales.*