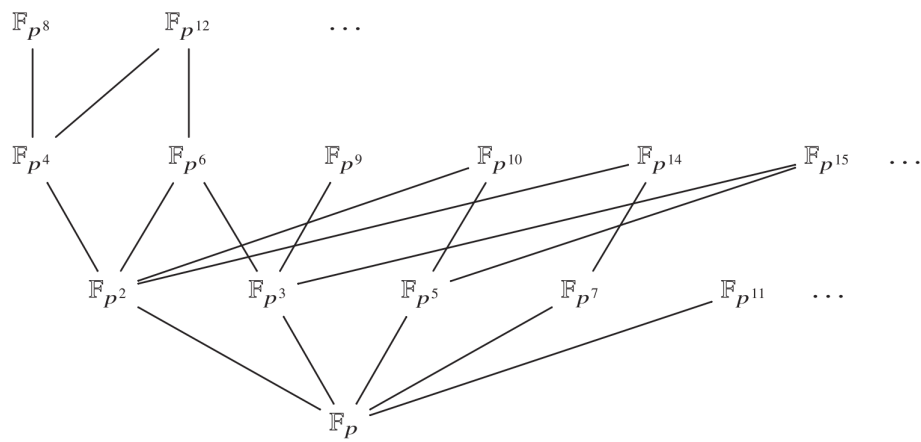


TEORÍA DE GALOIS

SEGUNDO CUATRIMESTRE - 2025



∞ -Galois y la clausura algebraica de cuerpos finitos

Valentín Nico

Índice general

Introducción	3
Capítulo 1. Teoría de Galois para extensiones infinitas	4
1.1. Extensiones de Galois	5
1.2. Espacios de Stone	7
1.3. El grupo profinito de Galois	10
1.4. La correspondencia de Galois	11
Capítulo 2. Aplicaciones a cuerpos finitos	15
2.1. Clasificación de subgrupos cerrados	15
2.2. Clasificación de las subextensiones	17
Bibliografía	20

Introducción

Descubierta por el propio Évariste Galois, la correspondencia que lleva su nombre configura la pieza central de la teoría de extensiones de cuerpos. En su versión clásica, las hipótesis de finitud sobre las extensiones consideradas garantizan que no haya *demasiados* automorfismos de cuerpos que fijen a una dada subextensión. En efecto, al intentar generalizar esta versión para dimensión infinita, uno puede encontrar distintos subgrupos del grupo de automorfismos de una extensión que fijan a un mismo subcuerpo (cf. Ejemplo 1.3). Esto fue descubierto originalmente por Dedekind en 1901, quien sugirió en [Ded01, p.15] que el inconveniente podría solucionarse haciendo del grupo de Galois una *stetige Mannigfaltigkeit*: una variedad topológica. En 1928, Krull propuso en [Kru28] una manera canónica de introducir una topología en el grupo de Galois que distinga a los subgrupos cerrados como a ellos que implementen la Correspondencia de Galois Infinita (cf. Teorema 1.23).



WOLFGANG KRULL
1899-1971, ALEMANIA

En el Capítulo 1, introduciremos la topología de Krull y demostraremos la correspondencia de Galois para extensiones infinitas. Para ello, se supondrán como preliminares nociones básicas de Teoría de Galois en dimensión finita, así como de Topología General y de (co)límites de funtores con valores en la categoría de grupos topológicos.

En el Capítulo 2, aplicaremos lo demostrado en el primer capítulo para describir todas las subextensiones de la clausura algebraica del cuerpo finito de p elementos, para un primo p . En primer lugar, daremos una clasificación de los subgrupos cerrados de los enteros profinitos (cf. Teorema 2.4), cuya demostración adaptamos de la clasificación para subgrupos cerrados de los enteros p -ádicos en el libro de John Wilson [Wil98] sobre grupos profinitos. Luego, utilizaremos esta clasificación para, a través de la correspondencia de Galois, obtener el siguiente teorema que describe todas las subextensiones de $\overline{\mathbb{F}}_p/\mathbb{F}_p$:

Teorema (2.10). Sea p un primo y $\overline{\mathbb{F}}_p/E$ una subextensión de la clausura algebraica de $\mathbb{F}_p$. Entonces, para cada primo q existe $0 \leq i_q \leq \infty$ tal que

$$E = \prod_{q \text{ primo}} \left(\bigcup_{n=0}^{i_q} \mathbb{F}_{p^{q^n}} \right).$$

Teoría de Galois para extensiones infinitas

La teoría de Galois para extensiones infinitas tiene como objetivo generalizar el clásico Teorema de Galois para extensiones finitas, normales y separables:

Teorema 1.1 (Correspondencia de Galois finita, Thm. 3.17 [Mil03]). Sea E/F una extensión de cuerpos normal, separable y de dimensión finita. Hay un isomorfismo de posets contravariante:

$$\begin{aligned} \{\text{subgrupos } H \leq \text{Gal}(E/F)\} &\cong \{\text{subextensiones } E/L/F\} \\ H &\mapsto E^H = \{\alpha \in E : \sigma(\alpha) = \alpha, \forall \sigma \in H\} \\ \text{Gal}(E/L) &\leftarrow L \end{aligned}$$

Además, la correspondencia identifica subgrupos normales con subextensiones normales.

Para comprender la naturaleza de la falla en la correspondencia en dimensión infinita, elaboremos un ejemplo. Comencemos recordando cómo se construye la clausura algebraica de un cuerpo finito:

Teorema 1.2 (Prop. 4.23 [Mil03]). Sea p un primo. Para cada $n \in \mathbb{N}$, clausura algebraica de $\mathbb{F}_{p^n}$ es

$$\overline{\mathbb{F}}_{p^n} = \bigcup_{m \geq 0} \mathbb{F}_{p^m}.$$

Más aún, la extensión $\overline{\mathbb{F}}_{p^n}/\mathbb{F}_{p^n}$ es normal y separable.

Ahora sí, veamos el contraejemplo a la Correspondencia de Galois 1.1 en el caso infinito:

Ejemplo 1.3. Sea p un primo y $\overline{\mathbb{F}}_p$ la clausura algebraica del cuerpo de p elementos. Por el Teorema 1.2, sabemos que la extensión $\overline{\mathbb{F}}_p/\mathbb{F}_p$ es normal y separable, pero es de dimensión infinita pues para cada número natural $n \in \mathbb{N}$ contiene a la extensión $\mathbb{F}_{p^n}/\mathbb{F}_p$, que tiene grado n . Consideremos el $\mathbb{F}_p$ -morfismo de Frobenius:

$$\begin{aligned} \Phi: \overline{\mathbb{F}}_p &\rightarrow \overline{\mathbb{F}}_p \\ \alpha &\mapsto \alpha^p \end{aligned}$$

Como $\Phi \in \text{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, el subgrupo cíclico generado $\langle \Phi \rangle \leq \text{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ determina una subextensión de $\overline{\mathbb{F}}_p$:

$$\overline{\mathbb{F}}_p^{(\Phi)} = \{\alpha \in \overline{\mathbb{F}}_p : \alpha^p = \alpha\} = \mathbb{F}_p.$$

Si la correspondencia fuera cierta, esto implicaría que $\langle \Phi \rangle = \text{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ y por ende el grupo coincidiría con el cíclico infinito. Veamos que hay un elemento de $\text{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ que no es una potencia del endomorfismo de Frobenius. En efecto, consideremos

$$\Phi^\infty = \dots \Phi^{4!} \circ \Phi^{3!} \circ \Phi^{2!} \circ \Phi.$$

Este elemento está bien definido pues, si $n \in \mathbb{N}$, para todo $m \geq n$ se tiene que $\Phi^{m!}|_{\mathbb{F}_{p^n}} = \text{id}_{\mathbb{F}_{p^n}}$ y por lo tanto

$$\Phi^\infty|_{\mathbb{F}_{p^n}} = \Phi^{(n-1)!} \circ \dots \circ \Phi.$$

Sin embargo, Φ^∞ no es potencia del endomorfismo de Frobenius. En efecto, si existe $k \in \mathbb{N}$ tal que $\Phi^\infty = \Phi^k$, para cada $n \in \mathbb{N}$ debería ser que $\Phi^\infty|_{\mathbb{F}_{p^{n!}}} = \Phi^k$ y por tanto que

$$\sum_{j=1}^{n-1} j! \equiv \sum_{j=1}^{n!-1} j! \equiv k \pmod{n!}.$$

Luego, $\sum_{j=1}^{n-1} j! \leq (n-1)(n-1)! < n!$ y por ende para cualquier $n \in \mathbb{N}$:

$$\pm k = \sum_{j=1}^{n-1} j!.$$

En cualquiera de los casos, $|k|$ es arbitrariamente grande lo cual es una contradicción, de modo tal que $\Phi^\infty \notin \langle \Phi \rangle$ ¹. Esto muestra que, en el caso infinito, la correspondencia de Galois 1.1 no vale considerando todo el poset de subgrupos. En efecto, tanto $\langle \Phi \rangle$ como el grupo $\text{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ fijan exactamente a $\mathbb{F}_p$, pero estos no coinciden.

La necesidad de limitar la cantidad de subgrupos considerados en la correspondencia de Galois se soluciona introduciendo una restricción topológica. En efecto, el camino será definir una topología acorde sobre el grupo de automorfismos de las extensiones para así restringir la correspondencia a los subgrupos *cerrados*.

1.1. Extensiones de Galois

El objetivo para lo que sigue será visitar las denominadas *extensiones de Galois*, pero esta vez sin restricciones dimensionales. De este modo, definimos:

Definición 1.4. Sea Ω/F una extensión de cuerpos. Decimos que Ω/F es una **extensión de Galois** si es normal y separable y notamos $\text{Gal}(\Omega/F)$ al grupo de automorfismos.

Nos será de utilidad recordar el siguiente lema sobre extensiones normales:

Lema 1.5. Si Ω/F es una extensión normal y Ω/E es una subextensión, entonces todo F -morfismo $\sigma: E \rightarrow \Omega$ se extiende a un F -automorfismo $\tilde{\sigma} \in \text{Aut}(\Omega/F)$.

DEMOSTRACIÓN. Procedemos por el Lema de Zorn. Consideremos el poset de pares (L, τ) donde $\Omega/L/E$ es una extensión intermedia y $\tau: L \rightarrow \Omega$ una extensión de σ ; ordenado por la inclusión natural. La unión filtrante define una cota superior para cualquier cadena, de modo tal que existe $(\tilde{E}, \tilde{\sigma})$ un elemento maximal. Veamos que $\tilde{E} = \Omega$ y que $\tilde{\sigma}$ es un automorfismo. Si existiera $\alpha \in \Omega \setminus \tilde{E}$, podríamos extender $\tilde{\sigma}$ a un F -morfismo $\tilde{E}[\alpha] \rightarrow \Omega$ enviando α a alguna raíz del minimal $m_{\alpha, F}$ que no esté en la imagen de $\tilde{\sigma}$. Dicha raíz existe pues Ω es normal y, por ende, el minimal tiene todas sus raíces en Ω . Además, $\tilde{\sigma}$ permuta las raíces, de modo tal que si toda raíz estuviera en la imagen de $\tilde{\sigma}$, entonces α debería estar en el dominio, pero por hipótesis no lo está. De esta manera, construimos una extensión a $\tilde{E}[\alpha]$, contradiciendo la maximalidad de $(\tilde{E}, \tilde{\sigma})$; lo cual es un absurdo. De esta forma, obtuvimos una extensión $\tilde{\sigma}: \Omega \rightarrow \Omega$. Basta ver que $\tilde{\sigma}$ es un automorfismo. Si no lo fuera, por el mismo argumento del Lema de Zorn podríamos extender la inversa $\tilde{\sigma}^{-1}: \text{im}(\tilde{\sigma}) \xrightarrow{\cong} \Omega$ a un F -morfismo $\Omega \rightarrow \Omega$, pero si $\text{im}(\tilde{\sigma}) \neq \Omega$,

¹Notar que lo demostrado es equivalente a que el entero profinito $\sum_{k \in \mathbb{N}} k! \in \hat{\mathbb{Z}}$ no es un número natural.

entonces esta extensión no sería inyectiva; lo cual es una contradicción pues todo morfismo de cuerpos es inyectivo. En conclusión, necesariamente tenemos que $\tilde{\sigma} \in \text{Aut}(\Omega/F)$ ■

Observación 1.6. Sea Ω/F una extensión de Galois y $\Omega/E/F$ una subextensión tal que E/F es una extensión de Galois. Entonces para cualquier morfismo $\sigma \in \text{Gal}(\Omega/E)$, la restricción $\sigma|_E$ se correstringe a E , pues todo elemento $\alpha \in E$ tiene como imagen $\sigma(\alpha)$ alguna raíz de su minimal $m_{\alpha,F}$, que por la normalidad de E/F se factoriza linealmente en E . De este modo, hay un morfismo de grupos bien definido

$$\text{res}_E : \text{Gal}(\Omega/F) \rightarrow \text{Gal}(E/F),$$

que por el Lema 1.5 es sobreyectivo.

La manera en que dotaremos de una estructura de grupo topológico al grupo de automorfismos de una extensión Ω/F viene dada por la siguiente construcción:

Construcción 1.7. Consideramos el funtor contravariante $\text{Gal}(-, F)$ que a cada subextensión $\Omega/M/F$ tal que M/F es una extensión de Galois finita le asigna su grupo de Galois $\text{Gal}(M/F)$, y que a cada inclusión $M \hookrightarrow N$ le asigna la restricción $\text{res}_M : \text{Gal}(N/F) \rightarrow \text{Gal}(M/F)$. Dotando a cada grupo de Galois de las extensiones finitas con la topología discreta, este funtor constituye un diagrama cofiltrante en la categoría de grupos topológicos²:

$$(1.8) \quad \begin{array}{ccc} & & \text{Gal}(N, F) \\ & \nearrow \text{res}_N & \\ \text{Gal}(MN, F) & & \\ & \searrow \text{res}_M & \\ & & \text{Gal}(M, F) \end{array}$$

Teorema 1.9. Sea Ω/F una extensión de Galois. Entonces, la restricción $\text{res}_M : \text{Gal}(\Omega/F) \rightarrow \text{Gal}(M, F)$ para cada subextensión de Galois finita M/F induce un isomorfismo de grupos:

$$\begin{aligned} \text{Gal}(\Omega/F) &\cong \varprojlim \text{Gal}(M/F) \\ \sigma &\mapsto (\sigma|_M) \end{aligned}$$

DEMOSTRACIÓN. Es claro que la restricción es un morfismo compatible con el diagrama y por lo tanto induce el morfismo canónico al límite. Veamos que es un isomorfismo de grupos. En efecto, su núcleo viene dado por

$$\bigcap_{\substack{M \subseteq \Omega \\ \text{Galois finita}}} \ker(\text{res}_M) = \bigcap_{\substack{M \subseteq \Omega \\ \text{Galois finita}}} \text{Gal}(\Omega/M).$$

Como todo elemento en Ω está contenido en una subextensión finita, se sigue que el núcleo es trivial y por ende es un monomorfismo. Para ver la sobreyectividad, consideremos $(\sigma_M) \in \varprojlim \text{Gal}(M/F)$. La compatibilidad dice que si M y N son subextensiones de Galois finitas, entonces $\text{res}_{M \cap N}(\sigma_M) = \sigma_{M \cap N} = \text{res}_{M \cap N}(\sigma_N)$. En consecuencia, la propiedad universal

²Recordemos que los límites en la categoría de grupos topológicos se calculan como en la categoría de espacios topológicos.

del colímite induce un F -morfismo

$$\sigma: \bigcup_{\substack{M \subseteq \Omega \\ \text{Galois finita}}} M \rightarrow \Omega$$

$$\alpha \mapsto \sigma_M(\alpha), \text{ si } \alpha \in M$$

Este morfismo $\sigma \in \text{Gal}(\Omega/F)$ verifica que $\text{res}_M(\sigma) = \sigma_M$ para toda subextensión de Galois finita M/F , de modo tal que la aplicación del teorema es un isomorfismo de grupos. ■

Vía el isomorfismo de grupos del Teorema 1.9, definiremos la topología del grupo de Galois de la siguiente manera:

Definición 1.10. Si Ω/F es una extensión de Galois, su **grupo profinito de Galois** es el grupo topológico $\text{Gal}(\Omega/F)$ dotado de la topología que hace de la aplicación del Teorema 1.9 un isomorfismo de grupos topológicos, donde cada $\text{Gal}(M, F)$ tiene la topología discreta.

Notemos que esta construcción recupera la correspondencia de Galois en el caso finito:

Observación 1.11. Si E/F es una extensión de Galois finita, entonces admite finitas subextensiones $E/M/F$ tales que M/F es de Galois y por lo tanto el diagrama del Teorema 1.9 es finito. Esto dice que $\text{Gal}(E/F)$ como grupo profinito es un límite finito de grupos topológicos discretos y por lo tanto discreto. En consecuencia, la topología en el grupo profinito de Galois es trivial y los resultados en dimensión finita se extienden sin modificaciones.

1.2. Espacios de Stone

Dado que los espacios topológicos con los que trabajaremos se presentan como límites de espacios discretos, merece la pena dedicar un apartado a mencionar las propiedades principales de estos espacios

Definición 1.12. Un espacio topológico X se dice **espacio de Stone** si existen

- una categoría cofiltrante I ,
- un funtor $D: I \rightarrow \mathbf{Top}$ tal que D_i es un espacio discreto y finito para todo $i \in I$,
- un homeomorfismo de espacios topológicos $X \cong \lim_{i \in I} D_i$.

Algunos ejemplos notables de espacios de Stone son, por ejemplo, los productos arbitrarios de espacios discretos finitos, el espacio de Cantor o los enteros p -ádicos para un primo $p \in \mathbb{Z}$; algunos de los cuales mencionaremos en detalle a continuación. Los espacios de Stone son ampliamente estudiados en el marco de las álgebras de Boole; es decir, los reticulados distributivos. En particular, un resultado fundamental del área es el siguiente:

Teorema 1.13 ([Joh82, Chapter II, Section 4.4]). La categoría de espacios de Stone junto a las funciones continuas es equivalente a la categoría opuesta de álgebras de Boole.

La siguiente proposición ilustra propiedades topológicas destacables de los espacios de Stone:

Proposición 1.14. Todo espacio de Stone es compacto, Hausdorff y totalmente desconexo.

DEMOSTRACIÓN. Sea $(D_i)_{i \in I}$ una familia de espacios discretos indexados por una categoría cofiltrante I . Es claro que el límite de espacios topológicos discretos es Hausdorff, por ser un subespacio de un producto de espacios T_2 . A su vez, el producto y subespacio de espacios totalmente desconexos es también totalmente desconexo, de modo tal que un espacio de Stone es

totalmente desconexo. Veamos que $\lim_{i \in I} D_i \subseteq \prod_{i \in I} D_i$ es cerrado, y concluyamos por el Teorema de Tychonoff que el límite es compacto. En efecto, si $(x_i)_{i \in I} \notin \lim_{i \in I} D_i$, entonces existen $i, j \in I$ y un morfismo del diagrama $f_{i,j}: D_i \rightarrow D_j$ tales que $f_{i,j}(x_i) \neq x_j$. Consideremos el abierto:

$$\{(y_i)_{i \in I} : y_i = x_i, y_j = x_j\} = \pi_i^{-1}(\{x_i\}) \cap \pi_j^{-1}(\{x_j\}) \subseteq \prod_{i \in I} D_i.$$

Es claro que $(x_i)_{i \in I}$ pertenece a este abierto que está completamente contenido en el complemento del límite, probando lo buscado. ■

El siguiente teorema dice que las propiedades topológicas del resultado anterior caracterizan a los espacios de Stone

Teorema 1.15 ([RZ10, Theorem 1.1.12]). Un espacio topológico X es un espacio de Stone si y solo si es compacto, Hausdorff y totalmente desconexo.

En parte de la literatura, esta clase de espacios recibe el nombre de *espacios profinitos*. El espíritu de este nombre surge de que los límites cofiltrantes de espacios discretos consisten de una generalización intermedia entre los espacios finitos y los espacios compactos.

Definición 1.16. Diremos que un grupo topológico es un **grupo profinito** si su espacio topológico subyacente es un espacio de Stone.

Por lo anterior, el grupo de automorfismos de una extensión de Galois es un grupo profinito. Veamos algunos ejemplos que serán de interés en el Capítulo 2.

Ejemplo 1.17 (Enteros p -ádicos). Fijemos p un número primo y consideremos, para cada $n \in \mathbb{N}$, el grupo topológico discreto $\mathbb{Z}/p^n\mathbb{Z}$. Las proyecciones al cociente $\mathbb{Z}/p^{n+1}\mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z}$ definen un diagrama cofiltrante

$$\cdots \mathbb{Z}/p^4\mathbb{Z} \rightarrow \mathbb{Z}/p^3\mathbb{Z} \rightarrow \mathbb{Z}/p^2\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}.$$

Llamamos **enteros p -ádicos** al grupo topológico que es el límite del diagrama anterior y los notamos $\mathbb{Z}_p$. Explícitamente, un entero p -ádico es una tupla $(a_n)_{n \in \mathbb{N}}$ que verifica la siguiente relación de compatibilidad:

$$a_{n+1} \equiv a_n \pmod{p^n}.$$

Una forma alternativa de caracterizar a los enteros p -ádicos, que en efecto justifica su nombre, viene dada por lo siguiente: cada entero $a \in \mathbb{Z}_p$ es una serie formal en base p

$$a = \sum_{n \in \mathbb{N}} a_n p^n,$$

donde $0 \leq a_n < p$ para cada $n \in \mathbb{N}$ y la suma de dos elementos viene dada por la suma de las series formales, *acarreando* los coeficientes de la expansión en base p . El espacio de Stone de enteros p -ádicos resulta metrizable y, de hecho, es la completación de los números enteros respecto la métrica p -ádica (cf. [Pom20]).

El siguiente ejemplo configura la manera *universal* de embeber a los números enteros en un grupo profinito:

Ejemplo 1.18 (Enteros profinitos). Extendiendo lo realizado en el ejemplo anterior, podemos considerar el diagrama cofiltrante que, para cada $m \in \mathbb{N}$ divisor de $n\mathbb{N}$, tiene la proyección al cociente $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$. En otras palabras, consideramos el diagrama cofiltrante definido por

el funtor de la categoría poset $\mathbb{N}$ con la divisibilidad, que a cada n le asigna el grupo topológico discreto $\mathbb{Z}/n\mathbb{Z}$. Definimos el grupo de **enteros profinitos** como el límite del diagrama:

$$\hat{\mathbb{Z}} := \lim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}.$$

Los números enteros, con la topología discreta, se insertan diagonalmente en el límite por el morfismo de grupos continuo $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, para cada $n \in \mathbb{N}$. Explícitamente, un entero profinito es una tupla $(a_n)_{n \in \mathbb{N}}$ tal que, para cada $m \in \mathbb{N}$ divisor de $n \in \mathbb{N}$, se tiene que

$$a_n \equiv a_m \pmod{m}$$

La universalidad dice que para cualquier morfismo de grupos continuo $\mathbb{Z} \rightarrow H$, con valores en un grupo profinito H , existe un único morfismo de grupos continuo $\hat{\mathbb{Z}} \rightarrow H$ que factoriza al original (cf. [Wil20]).

Veamos la relación entre los enteros profinitos y los enteros p -ádicos, para cada primo p :

Teorema 1.19 (Teorema chino del resto). Hay un isomorfismo de grupos topológicos:

$$\begin{aligned} \hat{\mathbb{Z}} &\cong \prod_{p \text{ primo}} \mathbb{Z}_p \\ (a_n)_{n \in \mathbb{N}} &\mapsto ((a_{p^n})_{n \in \mathbb{N}}) \end{aligned}$$

DEMOSTRACIÓN. Escribiendo a cada número natural $n \in \mathbb{N}$ como

$$n = \prod_{p \text{ primo}} p^{v_p(n)},$$

donde $v_p(n)$ es la valuación p -ádica de n , para cada primo p ; el Teorema Chino del Resto da un isomorfismo de grupos topológicos discretos

$$f_n: \mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} \prod_{p \text{ primo}} \mathbb{Z}/p^{v_p(n)}\mathbb{Z}.$$

Estos morfismos de grupos continuos son compatibles con los diagramas inducidos por las proyecciones $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$, para cada m divisor de n . De esta forma, obtenemos un isomorfismo de grupos topológicos

$$\hat{\mathbb{Z}} \cong \lim_{n \in \mathbb{N}} \prod_{p \text{ primo}} \mathbb{Z}/p^{v_p(n)}\mathbb{Z}.$$

Basta ver que el término de la derecha coincide con el producto de todos los enteros p -ádicos. En efecto, para cada primo p y entero $n \in \mathbb{N}$, la proyección $\mathbb{Z}_p \rightarrow \mathbb{Z}/p^{v_p(n)}\mathbb{Z}$ induce un morfismo continuo

$$f: \prod_{p \text{ primo}} \mathbb{Z}_p \rightarrow \lim_{n \in \mathbb{N}} \prod_{p \text{ primo}} \mathbb{Z}/p^{v_p(n)}\mathbb{Z}.$$

Este morfismo es sobreyectivo pues lo es al componer con cualquier proyección en el límite. A su vez, todo elemento no nulo en $\prod_p \mathbb{Z}_p$ es no nulo al proyectarlo a $\mathbb{Z}/p^v\mathbb{Z}$ para algún p y v suficientemente grandes. Como el producto de los enteros p -ádicos es compacto y f es biyectiva y continua, entonces es un isomorfismo de grupos topológicos y por lo tanto

$$\hat{\mathbb{Z}} \cong \prod_{p \text{ primo}} \mathbb{Z}_p.$$

Es directo verificar que la composición de los isomorfismos coincide con la del enunciado. ■

Gracias al teorema anterior, alternaremos sin ambigüedad entre las dos caracterizaciones de los enteros profinitos.

1.3. El grupo profinito de Galois

Expandamos la descripción de las propiedades topológicas para el grupo profinito de una extensión de Galois Ω/F . Las proposiciones de este apartado están formuladas en base al Capítulo 4 de [Bor24], aunque las demostraciones aquí expuestas no remiten a las de Borceux. Es sabido que un espacio de Stone tiene una base de abiertos y cerrados. Veamos explícitamente cuál es una base de entornos de la identidad para el grupo $\text{Gal}(\Omega/F)$:

Proposición 1.20. Sea Ω/F una extensión de Galois. Entonces

$$\{\text{Gal}(\Omega/M) : \Omega/M/F \text{ Galois y finita}\}$$

es una base de entornos abiertos y cerrados de $\text{id} \in \text{Gal}(\Omega/F)$.

DEMOSTRACIÓN. Comencemos notando que cualquier subextensión $\Omega/E/F$ verifica que Ω/E es de Galois. De este modo, tenemos que si M/F es de Galois finita, entonces

$$\text{Gal}(\Omega/M) = \{\sigma \in \text{Gal}(\Omega/F) : \sigma|_M = \text{id}_M\} = \text{res}_M^{-1}(\{\text{id}\}),$$

de modo que cada $\text{Gal}(\Omega/M)$ es un entorno abierto y cerrado de id . Basta ver que si $\text{id} \in V$ es un entorno abierto básico en $\varprojlim \text{Gal}(M/F)$, entonces V contiene un abierto de la forma $\text{Gal}(\Omega/M)$ para alguna subextensión M/F finita y de Galois. Todo entorno básico de la identidad es de la forma $\text{res}_{M_1}^{-1}(U_1) \cap \dots \cap \text{res}_{M_n}^{-1}(U_n)$, con $M_1, \dots, M_n$ subextensiones de Galois finitas y $U_1, \dots, U_n$ entornos abiertos de la identidad en $\text{Gal}(M_i/F)$, para cada $i = 1, \dots, n$. Consideremos la extensión de Galois finita dada por la composición de extensiones $N = M_1 M_2 \dots M_n / F$. Notemos que $\text{res}_{M_i}(\sigma) = \text{id}_{M_i}$ para todo $1 \leq i \leq n$ si y solamente si $\text{res}_N(\sigma) = \text{id}_N$. En consecuencia, tenemos que

$$\text{id} \in \text{Gal}(\Omega/N) = \text{res}_N^{-1}(\{\text{id}_N\}) = \bigcap_{i=1}^n \text{res}_{M_i}^{-1}(\{\text{id}_{M_i}\}) \subseteq \text{res}_{M_1}^{-1}(U_1) \cap \dots \cap \text{res}_{M_n}^{-1}(U_n),$$

probando que $\{\text{Gal}(\Omega/M) : \Omega/M/F \text{ Galois y finita}\}$ es una base de entornos clopen de $\{\text{id}\}$. ■

Notar que la base anterior es de hecho una base de subgrupos abiertos **normales**, pues cada $\text{Gal}(\Omega/M)$ es el núcleo del morfismo de grupos res_M .

Corolario 1.21. Sea Ω/F una extensión de Galois, entonces todo subgrupo cerrado $H \leq \text{Gal}(\Omega/F)$ es intersección de todos los subgrupos abiertos que lo contienen.

DEMOSTRACIÓN. Es claro que H está contenido en la intersección de todos los abiertos que lo contienen. Como todo subgrupo abierto es cerrado, la intersección de todos los cerrados que contienen a H es también cerrada. Supongamos que existe σ en la intersección de todos los subgrupos abiertos que contienen a H y que $\sigma \notin H$. Esto implica que $\sigma \notin \overline{H} = H$ y por ende existe un abierto $\sigma \in V$ tal que $V \cap H = \emptyset$. Para ese abierto, el abierto $\sigma^{-1}V$ es un entorno de id y por la Proposición 1.20 existe una subextensión de Galois finita M/F tal que $\text{Gal}(\Omega/M) \subseteq \sigma^{-1}V$. En particular, se tiene que $\sigma \text{Gal}(\Omega/M) \cap H = \emptyset$ y por ende $\sigma \notin \text{Gal}(\Omega/M)H$. Como $\text{Gal}(\Omega/M)$ es un subgrupo normal, se sigue que $\text{Gal}(\Omega/M)H$ es un subgrupo abierto que contiene a H , pero que no tiene a σ , lo cual es una contradicción pues σ pertenece por hipótesis a la intersección de todos los subgrupos abiertos que contienen a H . ■

Gracias a la base de entornos abiertos de la identidad, podemos dar una caracterización alternativa de la topología del grupo de Galois profinito:

Proposición 1.22. Sea Ω/F una extensión de Galois. Entonces, la familia de evaluaciones

$$\{\text{ev}_\alpha : \text{Gal}(\Omega/F) \rightarrow \Omega : \alpha \in \Omega\}$$

es una familia inicial para la topología de $\text{Gal}(\Omega/F)$, dotando a Ω de la topología discreta.

DEMOSTRACIÓN. Comencemos viendo que las evaluaciones son continuas. Sea $\alpha \in \Omega$ y consideremos $\text{ev}_\alpha : \text{Gal}(\Omega/F)$. Basta ver que las fibras son abiertas, pues Ω tiene la topología discreta. En primer lugar, notemos que

$$\text{ev}_\alpha^{-1}(\{\alpha\}) = \{\sigma \in \text{Gal}(\Omega/F) : \sigma(\alpha) = \alpha\} = \text{Gal}(\Omega/F[\alpha])$$

es un subgrupo de $\text{Gal}(\Omega/F)$. Además, $\text{Gal}(\Omega/F[\alpha])$ contiene un entorno abierto de la identidad, dado por $\text{Gal}(\Omega/M)$ donde M/F es cualquier subextensión de Galois finita que contenga a α , como por ejemplo el cuerpo de descomposición de $m_{\alpha,F}$. Luego, cualquier subgrupo de un grupo topológico que contenga un entorno abierto del elemento neutro es inmediatamente abierto, de modo tal que $\text{ev}_\alpha^{-1}(\{\alpha\})$ es abierto. Sea $x \in \Omega$ un elemento arbitrario. Si $\text{ev}_\alpha^{-1}(\{x\})$ es vacío, no hay nada que probar. En caso contrario, existe $\sigma \in \text{Gal}(\Omega/F)$ tal que $\sigma(\alpha) = x$, y podemos considerar la composición

$$\text{Gal}(\Omega/F) \xrightarrow{\sigma^*} \text{Gal}(\Omega/F) \xrightarrow{\text{ev}_\alpha} \Omega.$$

Como la multiplicación a derecha por σ es un homeomorfismo, es claro que $\text{ev}_\alpha^{-1}(\{x\})$ es abierto si y solo si $(\sigma^*)^{-1}(\text{ev}_\alpha^{-1}(\{x\}))$ lo es. Este último conjunto coincide con

$$(\sigma^*)^{-1}(\text{ev}_\alpha^{-1}(\{x\})) = \{\tau \in \text{Gal}(\Omega/F) : \tau(\sigma(\alpha)) = x\} = \text{ev}_x^{-1}(\{x\}).$$

Por el mismo argumento que antes, resulta que este conjunto es un abierto de $\text{Gal}(\Omega/F)$, probando que las evaluaciones son continuas. Veamos que es inicial. Para ello, supongamos que $f : X \rightarrow \text{Gal}(\Omega/F)$ es una función tal que $\text{ev}_\alpha \circ f : X \rightarrow \Omega$ es continua para todo $\alpha \in \Omega$. Por la Proposición 1.20, f es continua si y solo si para toda extensión de Galois finita M/F y $\sigma \in \text{Gal}(\Omega/F)$ se tiene que

$$f^{-1}(\sigma \text{Gal}(\Omega/M)) = f^{-1}(\text{res}_M^{-1}(\{\sigma|_M\}))$$

es abierto. En efecto, si $M = F[\alpha_1, \dots, \alpha_n]$, entonces

$$\text{res}_M^{-1}(\{\sigma|_M\}) = \{\tau \in \text{Gal}(\Omega/F) : \tau(\alpha_i) = \sigma(\alpha_i), \forall 1 \leq i \leq n\} = \bigcap_{i=1}^n \text{ev}_{\alpha_i}^{-1}(\{\sigma(\alpha_i)\}),$$

de manera tal que

$$f^{-1}(\sigma \text{Gal}(\Omega/M)) = \bigcap_{i=1}^n (\text{ev}_{\alpha_i} \circ f)^{-1}(\{\sigma(\alpha_i)\})$$

es un clopen porque $\text{ev}_{\alpha_i} \circ f$ es continua para cada $1 \leq i \leq n$. ■

1.4. La correspondencia de Galois

Ya estamos listos para explorar la generalización de la Correspondencia de Galois para dimensión infinita. Comenzaremos enunciando la correspondencia y luego la demostraremos utilizando una serie de lemas, siguiendo la exposición de [Bor24].

Teorema 1.23 (Correspondencia de Galois). Sea Ω/F una extensión de cuerpos de Galois. Hay un isomorfismo de posets contravariante:

$$\begin{aligned} \{\text{subgrupos cerrados } H \leq \text{Gal}(\Omega/F)\} &\cong \{\text{subextensiones } \Omega/E/F\} \\ H &\mapsto \Omega^H = \{\alpha \in \Omega : \sigma(\alpha) = \alpha, \forall \sigma \in H\} \\ \text{Gal}(\Omega/E) &\leftarrow E \end{aligned}$$

Además, la correspondencia identifica subgrupos normales con subextensiones normales y subgrupos abiertos con subextensiones finitas.

Para ver la buena definición del isomorfismo, primero debemos ver que para **cualquier** subextensión $\Omega/E/F$, el grupo de Galois $\text{Gal}(\Omega/E)$. Por la Proposición 1.20 sabemos que el grupo de Galois es clopen cuando M/F es de Galois finita, pero todavía resta ver que el grupo de Galois es cerrado para cuando E/F es arbitraria.

Lema 1.24. Sea Ω/F una extensión de Galois y E/F una subextensión. Entonces $\text{Gal}(\Omega/E) \leq \text{Gal}(\Omega/F)$ es cerrado.

DEMOSTRACIÓN. Veamos primero que es cierto cualquier subextensión finita E/F . En ese caso, existe $E \leq M \leq \Omega$ tal que M/F es de Galois finita, por ejemplo tomando la composición de todos los cuerpos de descomposición de los finitos generadores de E/F . En ese caso, tenemos que $\text{Gal}(\Omega/M) \leq \text{Gal}(\Omega/F)$ es clopen. Más aún, como

$$\text{id} \in \text{Gal}(\Omega/M) \leq \text{Gal}(\Omega/E),$$

esto implica que $\text{Gal}(\Omega/E)$ contiene un subgrupo abierto y por ende es también clopen. En efecto, es abierto pues es unión de los trasladados $\sigma \text{Gal}(\Omega/M)$, para cada $\sigma \in \text{Gal}(\Omega/E)$, y es cerrado pues si $\sigma \notin \text{Gal}(\Omega/E)$, entonces $\sigma \text{Gal}(\Omega/M) \cap \text{Gal}(\Omega/E) = \emptyset$. Finalmente, si E/F es cualquier subextensión, tenemos que

$$\text{Gal}(\Omega/E) = \bigcap_{\alpha \in E} \text{Gal}(\Omega/F[\alpha])$$

y por ende $\text{Gal}(\Omega/E)$ es cerrado. ■

Para probar que las asignaciones son inversas mutuas, usaremos como herramienta el siguiente lema:

Lema 1.25. Sea $H \leq \text{Gal}(\Omega/F)$ un subgrupo y $\sigma \in \text{Gal}(\Omega/F)$ tal que para toda subextensión de Galois finita M/F existe $\tau \in H$ tal que

$$\sigma|_M = \tau|_M.$$

Entonces $\sigma \in \overline{H}$.

DEMOSTRACIÓN. Basta ver que cualquier entorno básico de σ interseca a H no vacío. Por la Proposición 1.22, basta ver que para cualquier colección finita $\alpha_1, \dots, \alpha_n \in \Omega$ se tiene que

$$\left(\text{ev}_{\alpha_1}^{-1}(\sigma(\alpha_1)) \cap \text{ev}_{\alpha_2}^{-1}(\sigma(\alpha_2)) \cap \dots \cap \text{ev}_{\alpha_n}^{-1}(\sigma(\alpha_n)) \right) \cap H \neq \emptyset.$$

Sea M/F una subextensión de Galois finita que contenga a $\alpha_1, \dots, \alpha_n$ y consideremos, por hipótesis, algún $\tau \in H$ tal que $\sigma|_M = \tau|_M$. Como $\tau(\alpha_i) = \sigma(\alpha_i)$ para todo $1 \leq i \leq n$, concluimos que la intersección anterior es no vacía y por ende que $\sigma \in \overline{H}$. ■

En lugar de probar que las asignaciones en la Correspondencia de Galois son inversas mutuas, probaremos una proposición ligeramente más fuerte que resulta de interés por sí sola:

Proposición 1.26. Sea Ω/F una extensión de Galois y $H \leq \text{Gal}(\Omega/F)$ un subgrupo. Entonces

$$\overline{H} = \text{Gal}(\Omega/\Omega^H).$$

En particular, si H es cerrado entonces $H = \text{Gal}(\Omega/\Omega^H)$.

DEMOSTRACIÓN. Es claro que para todo $\sigma \in H$, si $\alpha \in \Omega^H$ entonces $\sigma(\alpha) = \alpha$. En otras palabras, $H \subseteq \text{Gal}(\Omega/\Omega^H)$. Como este último es cerrado por el Lema 1.24, obtenemos la contención $\overline{H} \subseteq \text{Gal}(\Omega/\Omega^H)$. Sea $\sigma \in \text{Gal}(\Omega/\Omega^H)$; es decir, un F -morfismo tal que

$$(\tau(\alpha) = \alpha, \forall \tau \in H) \implies \sigma(\alpha) = \alpha.$$

Por el Lema 1.25, basta probar que para cualquier subextensión de Galois finita M/F , existe $\tau \in H$ tal que $\sigma|_M = \tau|_M$. Consideremos el subgrupo $H_M = \text{res}_M(H) \leq \text{Gal}(M/F)$. Por la Correspondencia de Galois finita 1.1, tenemos que

$$H_M = \text{Gal}(M/M^{H_M}).$$

Por hipótesis, si $\alpha \in M$ es tal que $\tau|_M(\alpha) = \alpha$ para todo $\tau \in H$, entonces $\sigma(\alpha) = \alpha$. En otras palabras, tenemos que $\text{res}_M(\sigma) \in \text{Gal}(M/M^{H_M})$ y por ende existe $\text{res}_M(\tau) \in H_M$, con $\tau \in H$ tal que $\sigma|_M = \tau|_M$. Esto prueba que $\sigma \in \overline{H}$ y por lo tanto la igualdad deseada. ■

El resultado de la proposición anterior no debería sorprendernos, considerando la conclusión del Ejemplo 1.3. Ahora sí, terminemos de demostrar la correspondencia:

DEMOSTRACIÓN. (Teorema 1.23). Es directo verificar que las asignaciones son morfismos de posets contravariantes. Por la Proposición 1.26 ya hemos probado que una de las composiciones en la correspondencia es la identidad. Por otra parte, si $\Omega/E/F$ es una subextensión arbitraria, es claro que

$$E \subseteq \Omega^{\text{Gal}(\Omega/E)}.$$

Si $\alpha \in \Omega^{\text{Gal}(\Omega/E)}$ consideremos M/E una extensión finita (sobre E) de Galois tal que $\alpha \in M$. Por la correspondencia de Galois finita 1.1 tenemos que

$$E = M^{\text{Gal}(M/E)}.$$

Veamos que para todo $\sigma \in \text{Gal}(M/E)$, se tiene que $\sigma(\alpha) = \alpha$ y concluyamos la contención deseada. En efecto, como Ω/E es Galois, por el Lema 1.5 existe $\tilde{\sigma} \in \text{Gal}(\Omega/E)$ tal que $\tilde{\sigma}|_M = \sigma$. Como $\alpha \in \Omega^{\text{Gal}(\Omega/E)}$ y $\tilde{\sigma} \in \text{Gal}(\Omega/E)$, entonces tenemos que

$$\sigma(\alpha) = \tilde{\sigma}|_M(\alpha) = \alpha$$

y por lo tanto que $\alpha \in E$. Para lo que sigue, el mismo argumento que para dimensión finita muestra que los subgrupos normales se corresponden con las subextensiones de Galois (cf. Thm. 3.17 [Mil03]). Finalmente, veamos que los subgrupos abiertos se corresponden con las subextensiones finitas. En efecto, la demostración del Lema 1.24 muestra que si E/F es finita, entonces $\text{Gal}(\Omega/E)$ es clopen, y en particular abierto. Resta ver que si $H \leq \text{Gal}(\Omega/F)$ es un subgrupo abierto, entonces Ω^H/F es una extensión finita. En efecto, como H es un subgrupo abierto, entonces por el Lema 1.20 existe una subextensión Galois finita M/F tal que $\text{Gal}(\Omega/M) \leq H = \text{Gal}(\Omega/\Omega^H)$. Como la correspondencia de Galois es morfismo de posets contravariantes, esto implica que $\Omega^H \subseteq M$ y por lo tanto Ω^H/F es una subextensión finita. Esto concluye la prueba de la Correspondencia de Galois infinita. ■

Hasta el momento, no hemos descartado la posibilidad de que el grupo de Galois de una extensión infinita pueda ser finito. Dicho de otra forma, por la teoría de Galois finita sabemos que si E/F es una extensión de Galois finita entonces $\text{Gal}(E/F)$ es un grupo finito. No obstante, la vuelta de esta afirmación también es cierta, y una posible demostración surge naturalmente utilizando topología:

Corolario 1.27. Si Ω/F es una extensión de Galois infinita, entonces $\text{Gal}(\Omega/F)$ es un grupo infinito.

DEMOSTRACIÓN. En caso contrario, $\text{Gal}(\Omega/F)$ es un espacio topológico Hausdorff finito y por ende es discreto. De este modo, el subgrupo trivial $1 \leq \text{Gal}(\Omega/F)$ es clopen y, por la Correspondencia de Galois 1.23, se corresponde con una extensión finita sobre F . En efecto, dicha extensión es precisamente Ω/F , lo cual demuestra lo buscado por el contrarecíproco. ■

Aplicaciones a cuerpos finitos

Utilizaremos la teoría desarrollada en el Capítulo 1 para clasificar todas las subextensiones de la clausura algebraica de un cuerpo finito. En efecto, como todo cuerpo finito en característica $p > 0$ es una extensión finita de $\mathbb{F}_p$, estudiaremos el poset de subextensiones de $\overline{\mathbb{F}_p}/\mathbb{F}_p$. Comencemos calculando su grupo de Galois.

Teorema 2.1. El grupo de Galois de la extensión $\overline{\mathbb{F}_p}/\mathbb{F}_p$ es el grupo de enteros profinitos:

$$\begin{aligned} \lim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z} &\cong \lim_{n \in \mathbb{N}} \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \\ (a_n)_{n \in \mathbb{N}} &\mapsto (\Phi^{a_n})_{n \in \mathbb{N}} \end{aligned}$$

DEMOSTRACIÓN. Basta probar que el isomorfismo de grupos topológicos definido, para $n \in \mathbb{N}$, por el endomorfismo de Frobenius $\mathbb{Z}/n\mathbb{Z} \cong \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ es compatible con el límite. Eso es consecuencia de que el siguiente diagrama conmuta para cada $m \in \mathbb{N}$ que divide a n :

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\cong} & \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \\ \text{proy} \downarrow & & \downarrow \text{res} \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\cong} & \text{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \end{array}$$

Luego, el resultado se sigue de que, por el Teorema 1.9 el grupo de Galois de $\overline{\mathbb{F}_p}/\mathbb{F}_p$ es el límite sobre las extensiones finitas de $\mathbb{F}_p$, de las cuales hay exactamente una para cada número natural. ■

2.1. Clasificación de subgrupos cerrados

En pos de clasificar todas las subextensiones de $\overline{\mathbb{F}_p}/\mathbb{F}_p$ utilizando la correspondencia de Galois, debemos describir todos los subgrupos cerrados de $\text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$. Veamos una familia de ejemplos de subgrupos cerrados:

Ejemplo 2.2. Para cada primo p , consideremos $i_p \in \mathbb{N} \cup \{\infty\}$ y el subgrupo de los p -ádicos

$$p^{i_p}\mathbb{Z}_p = \{(a_{p^n})_{n \in \mathbb{N}} \in \mathbb{Z}_p : a_{p^j} = 0 \ \forall j \leq i_p\}.$$

Este es un subgrupo cerrado en $\mathbb{Z}_p$ pues desplazar e insertar 0 en las primeras i_p coordenadas define un isomorfismo de grupos topológicos $\mathbb{Z}_p \cong p^{i_p}\mathbb{Z}_p$ (salvo cuando $i_p = \infty$, en donde el anterior es el subgrupo trivial), y por lo tanto $p^{i_p}\mathbb{Z}_p$ es un subespacio compacto en un espacio topológico Hausdorff. Como un producto de subgrupos compactos es subgrupo compacto, obtenemos un subgrupo cerrado de los enteros profinitos:

$$(2.3) \quad \prod_{p \text{ primo}} p^{i_p}\mathbb{Z}_p \leq \hat{\mathbb{Z}}.$$

El siguiente teorema dice que todos los subgrupos cerrados son de la forma anterior:

Teorema 2.4. Todo subgrupo cerrado de $\hat{\mathbb{Z}}$ es de la forma 2.3. Más aún, los subgrupos abiertos son exactamente los subgrupos de índice finito $n \in \mathbb{N}$ y de la forma

$$n\hat{\mathbb{Z}} = \prod_{p \text{ primo}} p^{v_p(n)} \mathbb{Z}_p.$$

La demostración de este resultado está adaptada de [Wil98], donde se prueba un resultado análogo para clasificar subgrupos cerrados de $\mathbb{Z}_p$ para cada primo p .

DEMOSTRACIÓN. Clasifiquemos primero los subgrupos abiertos de $\hat{\mathbb{Z}}$. Como los enteros profinitos son compactos, todo subgrupo abierto tiene índice finito. Dado $H \leq \hat{\mathbb{Z}}$ subgrupo abierto de índice $n \in \mathbb{N}$, tenemos que $\hat{\mathbb{Z}}/H$ es un grupo de orden n , por lo que $n \cdot (\hat{\mathbb{Z}}/H) = 0$ y por ende que $n\hat{\mathbb{Z}} \subseteq H$. Describamos $n\hat{\mathbb{Z}}$. En efecto, para cada primo p tenemos que $n\mathbb{Z}_p = p^{v_p(n)} \mathbb{Z}_p$, donde $v_p(n)$ es la valuación p -ádica de n . Esto es una consecuencia del hecho de que $\mathbb{Z}_p$ es divisible por enteros coprimos con p . Finalmente, se tiene que

$$n\hat{\mathbb{Z}} = \prod_{p \text{ primo}} p^{v_p(n)} \mathbb{Z}_p.$$

Como cada $p^{v_p(n)} \mathbb{Z}_p$ es el núcleo de la proyección canónica en el límite $\mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p^{v_p(n)} \mathbb{Z}$, tenemos que $p^{v_p(n)} \mathbb{Z}_p$ tiene índice $p^{v_p(n)}$ y, por ende, que $n\hat{\mathbb{Z}}$ tiene índice n . Como H también tiene índice n y contiene a $n\hat{\mathbb{Z}}$, entonces

$$H = n\hat{\mathbb{Z}}.$$

Por el Corolario 1.21, cualquier subgrupo cerrado T es la intersección de subgrupos abiertos de la forma de H , y por lo tanto se escribe como

$$T = \prod_{p \text{ primo}} p^{i_p} \mathbb{Z}_p,$$

con $i_p \in \mathbb{N} \cup \{\infty\}$ para cada primo p , donde $p^\infty \mathbb{Z}_p = 0$ denota el subgrupo trivial. ■

Gracias al teorema anterior y la correspondencia de Galois, recuperamos que las subextensiones finitas de $\overline{\mathbb{F}}_p$ son exactamente aquellas de la forma $\mathbb{F}_{p^n}/\mathbb{F}_p$ para cada $n \in \mathbb{N}$:

Observación 2.5. Por el Teorema de Galois 1.23, las subextensiones finitas de $\overline{\mathbb{F}}_p/\mathbb{F}_p$ se corresponden exactamente con los subgrupos abiertos y cerrados de $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. Por el Teorema 2.4, hay exactamente un subgrupo de esa clase para cada $n \in \mathbb{N}$ y es de la forma $n\hat{\mathbb{Z}}$. Por el isomorfismo del Teorema 2.1, un tal subgrupo se corresponde con el subgrupo $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)^n$, con notación multiplicativa. Gracias al Ejemplo 1.3 y a la Proposición 1.26, sabemos que el subgrupo generado por el Frobenius $\langle \Phi \rangle$ es denso en el grupo de Galois y por ende por continuidad que

$$\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)^n = \overline{\langle \Phi \rangle^n} = \overline{\langle \Phi^n \rangle}.$$

De este modo, empleando la correspondencia vemos que el subgrupo clopen $n\hat{\mathbb{Z}}$ se corresponde con la subextensión

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

Es decir, las subextensiones finitas son exactamente las de la forma $\mathbb{F}_{p^n}/\mathbb{F}_p$ para cada $n \in \mathbb{N}$.

2.2. Clasificación de las subextensiones

Antes de caracterizar completamente las subextensiones de Galois, necesitamos el siguiente lema que describe la subextensión fijada por un dado subgrupo del grupo de Galois en términos de las subextensiones de la forma $\mathbb{F}_{p^{q^n}}$, para cada primo q y $n \in \mathbb{N}$.

Lema 2.6. Sea $H \leq \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ un subgrupo. Entonces

$$(\overline{\mathbb{F}}_p)^H = \prod_{\substack{q \text{ primo} \\ n \in \mathbb{N}}} (\mathbb{F}_{p^{q^n}})^{H_{q^n}},$$

donde $H_m \leq \text{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p)$ denota la imagen de H por la restricción $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \rightarrow \text{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p)$.

DEMOSTRACIÓN. Comencemos notando que, para cada $m = q_1^{n_1} \cdots q_k^{n_k}$ escrito en su factorización en primos, por el Teorema Chino del Resto tenemos un isomorfismo que hace conmutar el siguiente diagrama:

$$\begin{array}{ccc} & & \text{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \\ & \nearrow \text{res}_m & \downarrow \cong \\ \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) & & \prod_{j=1}^k \text{Gal}(\mathbb{F}_{p^{q_j^{n_j}}}/\mathbb{F}_p) \\ & \searrow (\text{res}_{q_j^{n_j}}) & \end{array}$$

En consecuencia, por la conmutatividad del diagrama, el subgrupo H_m se escribe como:

$$H_m \cong \prod_{j=1}^k H_{q_j^{n_j}}.$$

Es claro que $\overline{\mathbb{F}}_p^H$ contiene a $(\mathbb{F}_{p^{q^n}})^{H_{q^n}}$ para todo primo q y $n \in \mathbb{N}$, de modo que la composición de extensiones está contenida en $(\overline{\mathbb{F}}_p)^H$. Sea $\alpha \in \overline{\mathbb{F}}_p^H$ tal que $\sigma(\alpha) = \alpha$ para cualquier $\sigma \in H$. Por construcción de la clausura algebraica, existe $m \in \mathbb{N}$ tal que $\alpha \in \mathbb{F}_{p^m}$. Escribamos a $m = q_1^{n_1} \cdots q_k^{n_k}$ en su factorización en primos y notemos que

$$\alpha \in \mathbb{F}_{p^m} = \prod_{j=1}^k \mathbb{F}_{p^{q_j^{n_j}}}.$$

Como $\alpha \in (\mathbb{F}_{p^m})^{H_m}$, basta ver que la siguiente contención es una igualdad

$$\prod_{j=1}^k (\mathbb{F}_{p^{q_j^{n_j}}})^{H_{q_j^{n_j}}} \subseteq (\mathbb{F}_{p^m})^{H_m}.$$

Los términos de la composición tienen órdenes coprimos dos a dos, de modo tal que, por Proposition 3.19 [Mil03], el grupo de Galois (finito) de la composición de extensiones de $\mathbb{F}_p$ es el producto de los grupos de Galois:

$$\text{Gal}\left(\prod_{j=1}^k (\mathbb{F}_{p^{q_j^{n_j}}})^{H_{q_j^{n_j}}}/\mathbb{F}_p\right) \cong \prod_{j=1}^k \text{Gal}\left((\mathbb{F}_{p^{q_j^{n_j}}})^{H_{q_j^{n_j}}}/\mathbb{F}_p\right).$$

Para cada $j = 1, \dots, n$, por torres de extensiones se tiene que

$$\left| \text{Gal} \left((\mathbb{F}_{p^{q_j}})^{H_{q_j}^{n_j}} / \mathbb{F}_p \right) \right| = \frac{\left| \text{Gal}(\mathbb{F}_{p^{q_j}} / \mathbb{F}_p) \right|}{\left| \text{Gal}(\mathbb{F}_{p^{q_j}} / (\mathbb{F}_{p^{q_j}})^{H_{q_j}^{n_j}}) \right|} = \frac{\left| \text{Gal}(\mathbb{F}_{p^{q_j}} / \mathbb{F}_p) \right|}{\left| H_{q_j}^{n_j} \right|} = \frac{q_j^{n_j}}{\left| H_{q_j}^{n_j} \right|}.$$

De esta forma, por el isomorfismo del Teorema Chino del Resto obtenemos que

$$\left| \text{Gal} \left(\prod_{j=1}^k (\mathbb{F}_{p^{q_j}})^{H_{q_j}^{n_j}} / \mathbb{F}_p \right) \right| = \frac{m}{\prod_{j=1}^k \left| H_{q_j}^{n_j} \right|} = \frac{m}{|H_m|}.$$

Nuevamente, por torres de extensiones tenemos que

$$\left| \text{Gal}((\mathbb{F}_{p^m})^{H_m} / \mathbb{F}_p) \right| = \frac{\left| \text{Gal}(\mathbb{F}_{p^m} / \mathbb{F}_p) \right|}{\left| \text{Gal}(\mathbb{F}_{p^m} / (\mathbb{F}_{p^m})^{H_m}) \right|} = \frac{\left| \text{Gal}(\mathbb{F}_{p^m} / \mathbb{F}_p) \right|}{|H_m|} = \frac{m}{|H_m|}.$$

Juntando ambas cosas resulta que

$$\text{Gal} \left(\prod_{j=1}^k (\mathbb{F}_{p^{q_j}})^{H_{q_j}^{n_j}} / \mathbb{F}_p \right) = \text{Gal}((\mathbb{F}_{p^m})^{H_m} / \mathbb{F}_p)$$

y la correspondencia de Galois finita 1.1 implica que

$$\prod_{j=1}^k (\mathbb{F}_{p^{q_j}})^{H_{q_j}^{n_j}} = (\mathbb{F}_{p^m})^{H_m}.$$

Esto dice que α pertenece a la composición de subextensiones y por ende que

$$\alpha \in \prod_{\substack{q \text{ primo} \\ n \in \mathbb{N}}} (\mathbb{F}_{p^{q^n}})^{H_{q^n}}.$$

■

Observación 2.7. Para cada primo q , el morfismo de Frobenius induce un isomorfismo

$$\text{Gal}(\bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{q^n}} / \mathbb{F}_p) = \lim_{n \in \mathbb{N}} \text{Gal}(\mathbb{F}_{p^{q^n}} / \mathbb{F}_p) \cong \mathbb{Z}_q$$

Gracias al lema anterior, podemos describir en función de las subextensiones generadas por los q -ádicos la correspondencia de Galois:

Teorema 2.8. Sea $H \leq \text{Gal}(\overline{\mathbb{F}}_p / \mathbb{F}_p)$ un subgrupo. Entonces

$$(\overline{\mathbb{F}}_p)^H = \prod_{q \text{ primo}} \left(\bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{q^n}} \right)^{\pi_q(H)},$$

donde $\pi_q: \hat{\mathbb{Z}} \rightarrow \mathbb{Z}_q$ es la proyección canónica a los q -ádicos.

DEMOSTRACIÓN. Notar que, por la Observación 2.7, la proyección $\pi_q(H)$ coincide con la restricción de H al grupo de Galois $\text{Gal}(\bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{q^n}} / \mathbb{F}_p)$. Luego, por el Lema 2.6, basta probar la igualdad

$$\prod_{\substack{q \text{ primo} \\ n \in \mathbb{N}}} (\mathbb{F}_{p^{q^n}})^{H_{q^n}} = \prod_{q \text{ primo}} \left(\bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{q^n}} \right)^{\pi_q(H)}.$$

Es claro que el término de la izquierda está contenido en el de la derecha pues

$$(\mathbb{F}_{p^{q^n}})^{H_{q^n}} \subseteq (\bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{q^n}})^{\pi_q(H)},$$

para todo primo q y $n \in \mathbb{N}$. Por otra parte, todo elemento en $(\bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{q^n}})^{\pi_q(H)}$ pertenece a $(\mathbb{F}_{p^{q^n}})^{H_{q^n}}$ para algún $n \in \mathbb{N}$, probando la igualdad deseada. ■

Basta describir las subextensiones de la forma $(\bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{q^n}})^{q^{i_q} \mathbb{Z}_q}$ para cada primo q y cada $0 \leq i_q \leq \infty$.

Lema 2.9. Sea q un primo y $0 \leq i_q \leq \infty$. Entonces

$$(\bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{q^n}})^{q^{i_q} \mathbb{Z}_q} = \bigcup_{n=0}^{i_p} \mathbb{F}_{p^{q^n}}.$$

DEMOSTRACIÓN. Notar que un q -ádico $(a_n)_{n \in \mathbb{N}}$ verifica que $(a_n)_{n \in \mathbb{N}} \in q^{i_q} \mathbb{Z}_q$ si y solo si $a_n = 0$ para todo $0 \leq n \leq i_q$. Si $i_q = \infty$ es claramente cierto el enunciado. En caso contrario, por el isomorfismo de la Observación 2.7, un q -ádico tal que $a_n = 0$ para todo $0 \leq n \leq i_q$ se corresponde unívocamente con un $\mathbb{F}_{p^{q^{i_q}}}$ -automorfismo. En otras palabras, tenemos que

$$q^{i_q} \mathbb{Z}_q = \text{Gal}(\bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{q^n}} / \bigcup_{n=0}^{i_p} \mathbb{F}_{p^{q^n}}),$$

y, como $q^{i_q} \mathbb{Z}_q$ es un subgrupo cerrado, la correspondencia de Galois concluye lo deseado. ■

Obtenemos la siguiente clasificación:

Teorema 2.10 (Subextensiones de $\overline{\mathbb{F}_p}$). Sea p un primo y $\overline{\mathbb{F}_p}/E$ una subextensión de la clausura algebraica de $\mathbb{F}_p$. Entonces, para cada primo q existe $0 \leq i_q \leq \infty$ tal que

$$E = \prod_{q \text{ primo}} (\bigcup_{n=0}^{i_q} \mathbb{F}_{p^{q^n}}).$$

DEMOSTRACIÓN. Por la Correspondencia de Galois 1.23, toda subextensión de la clausura algebraica es el cuerpo fijo por un subgrupo cerrado de $\text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$. Por el Teorema 2.4, todo subgrupo cerrado H es de la forma

$$H = \prod_{q \text{ primo}} q^{i_q} \mathbb{Z}_q,$$

con $0 \leq i_q \leq \infty$ para cada primo q . En particular, se tiene que $\pi_q(H) = q^{i_q} \mathbb{Z}_q$, donde $\pi_q: \hat{\mathbb{Z}} \rightarrow \mathbb{Z}_q$ es la proyección canónica y, por el Teorema 2.8, obtenemos que

$$(\overline{\mathbb{F}_p})^H = \prod_{q \text{ primo}} (\bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{q^n}})^{q^{i_q} \mathbb{Z}_q}.$$

Por el Lema 2.9, cada factor de la composición de subextensiones es de la forma $\bigcup_{n=0}^{i_p} \mathbb{F}_{p^{q^n}}$ y por lo tanto tenemos que

$$(\overline{\mathbb{F}_p})^H = \prod_{q \text{ primo}} (\bigcup_{n=0}^{i_q} \mathbb{F}_{p^{q^n}}),$$

concluyendo lo deseado. ■

Bibliografía

- [Bor24] Francis Borceux. *Galois Theories of Fields and Rings*. Springer, 2024.
- [Ded01] Richard Dedekind. Ueber die permutationen des korpers aller algebraischen zahlen. (*No Title*), 1901.
- [Joh82] Peter T Johnstone. *Stone spaces*, volume 3. Cambridge university press, 1982.
- [Kru28] Wolfgang Krull. Galoissche theorie der unendlichen algebraischen erweiterungen. *Mathematische Annalen*, 100(1):687–698, 1928.
- [Mil03] James S Milne. Fields and galois theory. *Courses Notes, Version*, 4, 2003.
- [Pom20] Alexa Pomerantz. An introduction to the p-adic numbers. *The University of Chicago Mathematics Research Experience for Undergraduates (REU)*, 2020.
- [RZ10] Luis Ribes and Pavel Zalesskii. Profinite groups. In *Profinite Groups*, pages 19–74. Springer, 2010.
- [Wil98] John S Wilson. *Profinite groups*, volume 19. Clarendon Press, 1998.
- [Wil20] Gareth Wilkes. Part iii profinite groups. *Expository notes available online. No date provided. url: <https://www.dpmms.cam.ac.uk/~grw46/LectureNotes.pdf> (visited on 10/27/2023)*, 2020.