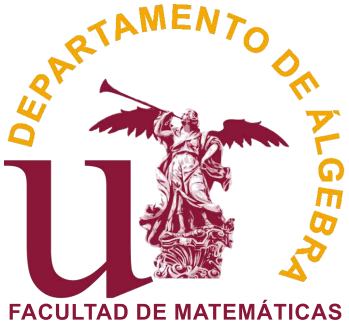
Cálculo Explícito de Elementos de Frobenius en Grupos de Galois

Garrido López, Verónica



Cálculo Explícito de Elementos de Frobenius en Grupos de Galois

Memoria presentada como parte de los requisitos para la obtención del título de Grado en Matemáticas por la Universidad de Sevilla.

Realizada por
Garrido López, Verónica

Tutorizada por
Arias de Reyna Domínguez, Sara

“ *Just a moment, Mary Poppins. What is the meaning of this outrage?*

I beg your pardon?

Will you be good enough to explain all this?

First of all, I would like to make one thing quite clear

Yes?

I never explain anything ”

Mary Poppins, George Banks

——Mary Poppins (1964)

Índice general

Sumario

English Abstract

In the XIX century David Hilbert proposed a problem in Galois Theory that remains unanswered today,
"Every finite group appears as the Galois group of some Galois extension of the rational numbers"
A related question that arose as result of it is if, given a finite group G, we can find families of parametric polynomials with coefficients in $\mathbb{Q}$ whose finite Galois extension $K/\mathbb{Q}$ has its Galois group isomorphic to G for almost every value of the parameters.

The goal of this dissertation is, given a known family of parametric polynomials $f_a(x)$ with Galois group G and K its splitting field over $\mathbb{Q}$ for some value of a, take a prime $p \in \mathbb{Q}$ that doesn't ramify in the Galois extension $K/\mathbb{Q}$ and find the associated Frobenius element Frob_p which meets

$$\mathrm{Frob}_p(x) \equiv x^p \bmod \mathfrak{p}$$

for all integral x in K and $\mathfrak{p}$ prime ideal in the ring of integers of K such that $\mathfrak{p} \cap \mathbb{Z}$ matches the ideal generated by p.

To reach this objective we have to elaborate the results on Dedekind domains and ideal ramification leading to the definition of the Frobenius element. Once the groundwork is laid we proceed to expound the method of the Dokchitser brothers for the identification of the element for almost every prime ideal $\mathfrak{p}$.

We will see that it suffices to check if

$$\Gamma_C\left(Tr_{\frac{\mathbb{F}_q[x]}{f_a(x)}/\mathbb{F}_q}(h(x)x^p)\right) = 0 \bmod \mathfrak{p}$$

Then we would have $\mathrm{Frob}_p \in C$, where C is a conjugacy class of G and Γ_C a polynomial that we will define in section 2.2.

We will also make some examples applying the previous procedure as well as add in theorems such as Chevotarev's Density theorem that will widen our conlclusions.

Resumen

En el siglo XIX David Hilbert propuso un problema en teoría de Galois que sigue sin tener respuesta a día de hoy,
"Todo grupo finito es el grupo de Galois de alguna extensión de los numeros racionales"
Una pregunta relacionada que surgió a raíz de ello es si, dado un grupo finito G, podemos encontrar familias de polinomios paramétricos con coeficientes en $\mathbb{Q}$ cuya extensión finita de Galois $K/\mathbb{Q}$ tenga su grupo de Galois isomorfo a G para casi todos los valores de los parámetros.

El objetivo de este trabajo es, dada una familia conocida de polinomios paramétricos $f_a(x)$ con grupo de Galois G y K su cuerpo de descomposición sobre $\mathbb{Q}$ para algún valor de a, tomar un primo $p \in \mathbb{Q}$ que no ramifique en la extensión de Galois $K/\mathbb{Q}$ y encontrar el elemento de Frobenius Frob_p asociado que cumple

$$\mathrm{Frob}_p(x) \equiv x^p \bmod \mathfrak{p}$$

para todo x íntegro en K y $\mathfrak{p}$ ideal primo del anillo de enteros de K tal que $\mathfrak{p} \cap \mathbb{Z}$ coincide con el ideal generado por p.

Para lograr este objetivo tenemos que desarrollar resultados sobre dominios de Dedekind y ramificación de ideales que nos llevarán a la definición del elemento de Frobenius. Una vez sentadas estas bases procederemos a explicar el método de los hermanos Dokchitser para la identificación del elemento para casi todo ideal primo $\mathfrak{p}$.

Veremos que nos basta comprobar si

$$\Gamma_C\left(Tr_{\frac{\mathbb{F}_q[x]}{f_a(x)}/\mathbb{F}_q}(h(x)x^p)\right) = 0 \bmod \mathfrak{p},$$

entonces tendríamos que $\mathrm{Frob}_p \in C$. Siendo C una clase de conjugación de G y Γ_C un polinomio para cada clase que definiremos en la sección 2.2.

Realizaremos también algún ejemplo para aplicar el procedimiento anterior además de añadir algún teorema como el teorema de Densidad de Chevotarev que ampliarán las conclusiones que podremos obtener.

1 Introducción

> " *Well, first things first. I always say, the place to hang a hat is on a hat stand.* "
>
> Mary Poppins
>
> ——Mary Poppins(1964)

Antes de meternos en la cuestión principal es esencial que nos hagamos algunas preguntas necesarias para que todos los pasos que demos lleguen a tener sentido cuando estamos en una extensión finita L/K ¿Existe factorización única en L para los elementos de K? ¿cómo se comportan estos elementos?

Una vez satisfecha nuestra curiosidad sabremos que los pasos que demos más adelante son rígidos, con sentido, y con el mismo ritmo de baile que unos serviciales pingüinos.

Un ejemplo del objetivo de esta primera parte sería la descomposición en $\mathbb{Z}[\sqrt{-5}]$ de 21. Tenemos que $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$ y además todos estos elementos son irreducibles y no asociados. En nuestro caso trabajaremos con los ideales generados por estos elementos, entonces los factores que han surgido antes estarían formados por el producto de unos ideales primos $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$, sujetos a

$$\langle 3 \rangle = \mathfrak{p}_1\mathfrak{p}_2, \quad \langle 7 \rangle = \mathfrak{p}_3\mathfrak{p}_4, \quad \langle 1 + 2\sqrt{-5} \rangle = \mathfrak{p}_1\mathfrak{p}_3, \quad \langle 1 - 2\sqrt{-5} \rangle = \mathfrak{p}_2\mathfrak{p}_4$$

Esto resolvería la no unicidad anterior implicando que

$$\langle 21 \rangle = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4)$$

Este proceso lo podremos aplicar a $\mathcal{O}_L$, un subanillo muy especial de L llamado el anillo de enteros del que veremos sus propiedades en esta sección.

1.1 Conceptos Previos

En esta sección nos basaremos principalmente en resultados que aparecen en los libros *Algebraic number theory-Neukirck*[4], *Introductory algebraic number theory-Alaca y Williams*[1] y *Algebraic number theory-Mollin*[3], y planteamos los pilares sobre los que vamos a desarrollar nuestra teoría.

Dominios Noetherianos

Lo primero que necesitamos es algún tipo de factorización de los elementos que podremos encontrarnos en nuestro trabajo, puede que esta no sea única en un principio. El concepto de un Dominio Noetheriano nos permitirá encontrar una manera debido a la condición de la cadena ascendente.

Definición 1.1.1.1. *Una secuencia de ideales* $\{I_n\}_{n\in\mathbb{N}}$ *en un dominio de integridad se dice que es una cadena ascendente si*

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

Y se dice que dicha cadena es estacionaria si $\exists n_0 \in \mathbb{N}$ *tal que* $I_n = I_{n_0}\ \forall N \geq n_o$.

Definición 1.1.1.2 (Dominio Noetheriano). *Sea un dominio de integridad* D. *Si toda cadena de ideales en* D *es estacionaria se dice que cumple la condición de cadena ascendente y, en este caso,* D *es un dominio Noetheriano.*

Ejemplo 1.1.1.3. $\mathbb{F}[x_1, x_2, \ldots]$ no es Noetheriano. Encontramos la cadena de ideales $\langle x_1\rangle \subseteq \langle x_1, x_2\rangle \subseteq \cdots$ que no es estacionaria.

Proposición 1.1.1.4. Sea D un dominio de integridad. Entonces D es Noetheriano si y sólo si todo ideal de D es finitamente generado.

Demostración. *La prueba puede encontrarse en [1, Página 55]*

Corolario 1.1.1.5. Sea D un dominio de ideales principales. Entonces D es un dominio Noetheriano.

Definición 1.1.1.6. *Sea* D *un dominio de integridad. Se dice que* D *cumple la condición maximal si todo conjunto* S *de ideales no vacío de* D *contiene un ideal* I *tal que si* J *es un ideal de* S *con* $I \subseteq J$ *entonces* $I = J$.

Proposición 1.1.1.7. Sea D un dominio de integridad. Entonces D es Noetheriano si y sólo si D satisface la condición maximal.

Demostración. Supongamos que D es Noetheriano y no satisface la condición maximal. Entonces existe S conjunto no vacío de ideales de D tal que $\forall I \in S\ \exists J \in S$ tal que $I \subsetneq J$. Esto nos permite construir por inducción una cadena ascendente infinita de ideales de S, que contradice que D sea Noetheriano.

Sea ahora un dominio de integridad D que satisface la condición maximal. Sea

$$I_1 \subseteq I_2 \subseteq \dots$$

una cadena ascendente de ideales de D, llamamos $S = \{I_n | n \in \mathbb{N}\}$. Por satisfacer D la condición maximal $\exists I_m \in S$ tal que $I_m = I_k\ \forall m \leq k$, y por lo tanto la cadena es estacionaria. ∎

Vista esta propiedad nos podemos aventurar a decir que si D es un dominio Noetheriano entonces su anillo de polinomos, $D[x]$, también lo es. Este es el llamado *Teorema de la Base de Hilbert* cuya prueba se basa en la construcción de un conjunto de polinomios de grado creciente y comprobar que este cumple la condición maximal observando sus coeficientes líderes en D que ya es un dominio Noetheriano.

Este resultado nos proporciona la *herencia* de la propiedad y veremos su utilidad a la hora de realizar extensiones de cuerpo.

Definición 1.1.1.8 (Dominio de Factorización). *Sea D un dominio de integridad. Entonces D se dice que es un dominio de factorización si todo elemento de D que no sea cero o unidad puede expresarse como producto finito de elementos irreducibles de D.*

Proposición 1.1.1.9. Si D es Noetheriano entonces D es dominio de factorización.

Demostración. Sea D un dominio Noetheriano, supongamos que D no es un dominio de factorización. Entonces $\exists a \in D$ que no es cero ni unidad y no es producto finito de elementos irreducibles de D. Llamemos A al conjunto de todos estos elementos, A es no vacío y sea $S = \{\langle a \rangle | a \in A\}$.

Evidentemente, S es un conjunto no vacío de ideales principales de D. Al ser D Noetheriano, por la condición maximal existe un elemento $\langle b \rangle$ maximal en S. Como $\langle b \rangle \in S$, $b \in A$ no es cero, ni unidad ni producto finito de irreducibles. Por consiguiente b no es irreducible, es decir, podemos escribir $b = cd$ donde c y d no son cero ni unidades de D. Así tenemos que $\langle b \rangle = \langle cd \rangle \subseteq \langle c \rangle$, como d no es unidad, b y c no son asociados, por lo tanto $\langle b \rangle \neq \langle c \rangle$. Análogamente $\langle b \rangle \subsetneq \langle d \rangle$. Tenemos pues que $\langle c \rangle, \langle d \rangle \notin S$, y eso implica que son producto finito de irreducibles, contradiciendo que b no lo es. ∎

Ejemplo 1.1.1.10. $\mathbb{Z}[x]$ es dominio de factorización, de hecho por inducción se ve que $\mathbb{Z}[x_1, x_2, \dots, x_n]$ es dominio de factorización.

Corolario 1.1.1.11. Sea D un dominio de ideales principales. Entonces D es un dominio de factorización.

Definición 1.1.1.12 (Dominio de Factorización Única). *Sea D un dominio de factorización. Si todo elemento de D que no sea cero o unidad tiene una única factorización como producto de elementos irreducibles de D entonces D es dominio de factorización única.*

Proposición 1.1.1.13. Sea D un dominio de ideales principales. Entonces D es dominio de factorización única.

Demostración. Supongamos que D es dominio de ideales principales y por lo tanto dominio de factorización, pero no es dominio de factorización única. Entonces existiría un elemento $d \in D$ que tiene dos factorizaciones distintas. El conjunto de los ideales generados por estos elementos tiene un elemento maximal $\langle a \rangle$, por lo tanto

$$a = ub_1^{k_1} \cdots b_n^{k_n} = vc_1^{j_1} \cdots c_m^{j_m}$$

donde u, v son unidades, b_i, c_l son elementos irreducibles distintos dos a dos en cada factorización y $k_i, j_l > 0$.

Ya que D es dominio de ideales principales, todo irreducible es primo, por lo que b_1 ha de dividir únicamente a un c_i, supongamos c_1. Obtenemos que $b_1 = wc_1$, siendo w una unidad. El resultado es análogo para c_1, de ahí $k_1 = j_1$. Por inducción llegamos a que $n = m$, $b_i = w_i c_i$ con w_i una unidad de D y $k_i = j_i$ $\forall 1 \leq i \leq n$. ∎

Ejemplo 1.1.1.14. $\mathbb{Z}[i]$ es dominio Euclídeo, que es dominio de ideales principales y por lo tanto dominio de factorización única.

Ejemplo 1.1.1.15. Sea $\mathbb{F}$ un cuerpo, $\mathbb{F}[x]$ es un dominio Euclídeo, es decir, es dominio de factorización única.

Ejemplo 1.1.1.16. $\mathbb{Z}[x]$ es dominio de factorización única, de aquí se sigue que $\mathbb{Z}[x_1, x_2, \dots, x_n]$ también lo es, ya que el anillo de polinomios de un dominio de factorización única también lo es.

Como podemos observar muchos de los dominios que están basados en el anillo $\mathbb{Z}$ comparten sus propiedades, pero no todos. Nos interesa saber cuando ocurre para darle un buen empleo a nuestros dos peniques, es decir, como llegar a generalizar las propiedades de $\mathbb{Z}$, no sólo a sus extensiones, si no a otros anillos también.

Un primer paso son los dominios de ideales principales que hemos estado viendo previamente. Resulta sencillo relacionar la divisibilidad de sus elementos con la de sus ideales y es lo que vamos a buscar en este primer capítulo, aunque sigue siendo un concepto muy rígido que tendremos que ir relajando para nuestro objetivo.

Definición 1.1.1.17 (Módulo Noetheriano). *Sea A un anillo con unidad. Un $A-$módulo M se dice Noetheriano si toda cadena ascendente de submódulos de M es estacionaria.*

Proposición 1.1.1.18. Sea A un anillo con unidad. Sea M un $A-$módulo y N un submódulo de M. Entonces M es Noetehriano si y sólo si N y M/N son Noetherianos.

Demostración. *La prueba puede encontrarse en [1, Página 67]*

Proposición 1.1.1.19. Si A es Noetheriano, cualquier $A-$módulo finitamente generado es un módulo Noetheriano.

Demostración. Sea M un $A-$módulo finitamente generado.
Entonces $\exists m_1, \dots, m_n \in M$ tales que

$$M = Am_1 + Am_2 + \cdots + Am_n$$

donde cada Am_i es un $A-$módulo. Sean $N_i = \{a \in A | am_i = 0\}$, son submódulos de A. Dado que los submódulos de A son sus ideales y es Noetheriano, A es un módulo Noetheriano. por la proposición 1.1.1.18 A/N_i es Noetheriano, además $A/N_i \simeq Am_i$. En particular Am_i es un módulo Noetheriano.

Definimos M_k para $1 \leq k \leq n$ al $A-$módulo

$$M_k = Am_1 + \cdots + Am_k.$$

y supongamos que $M_1, \dots, M_{k-1}$ son módulos Noetherianos. Puesto que Am_k es Noetheriano, el cociente $Am_k/(Am_k \cap M_{k-1})$ también lo es. En consecuencia

$$M_k/M_{k-1} = (M_{k-1} + Am_k)/M_{k-1} \simeq Am_k/(Am_k \cap M_{k-1})$$

es Noetheriano y de nuevo por la proposición 1.1.1.18 vemos que M_k es Noetheriano, concretamente $M = M_n$ es un módulo Noetheriano.

Corolario 1.1.1.20. Sean D y E dominios de integridad tales que $D \subseteq E$. Si D Noetheriano y E es un $D-$módulo finitamente generado entonces E es un dominio Noetheriano.

Demostración. Sea $I_1 \subseteq I_2 \subseteq \dots$ una cadena ascendente de ideales de E. Por la proposición 1.1.1.19, como D es Noetheriano y E es un $D-$módulo finitamente generado, E es un $D-$módulo Noetheriano. Cada ideal I_i es un $D-$submódulo de E, por lo que la cadena es estacionaria y por tanto E es domino Noetheriano.

Integralidad

A continuación queremos aprender la manera en la que se comportan ciertos elementos de nuestro anillo, como hemos visto somos capaces de factorizar en muchos casos, pero queremos construir un subanillo dentro de la extensión finita L/K sobre la que trabajaremos en el que encontramos una condición necesaria para la unicidad, aquí es donde entran en juego los anillos íntegramente cerrados.

Definición 1.1.2.1 (Elemento Íntegro). *Sean A y B dominios de integridad con $A \subseteq B$. Un elemento $b \in B$ se dice íntegro sobre A si es el cero de un polinomio mónico de grado $n \geq 1$ con coeficientes en A.*

El anillo B se dice íntegro sobre A si todo elemento $b \in B$ es entero sobre A.

Definición 1.1.2.2 (Elementos Algebraicos). *Sean A y B dominios de integridad tales que $A \subseteq B$. Si A es cuerpo y $b \in B$ es íntegro sobre A entonces se dice que b es algebraico sobre A.*

Proposición 1.1.2.3. Sean $A \subseteq B \subseteq C$ una torre de dominios de integridad. Si $c \in C$ es íntegro sobre A entonces $c \in C$ es íntegro sobre B.

Proposición 1.1.2.4. Sean A y B dominios de integridad con $A \subseteq B$. Sea $b \in B$. Entonces son equivalentes:

1. b es íntegro sobre A
2. El subanillo $A[b]$ es un $A-$módulo finitamente generado

Demostración. Sea $b \in B$ un elemento íntegro sobre A y un polinomio mónico $f(x) \in A[x]$ de grado $n \geq 1$ tal que $f(b) = 0$. Sea $g(x) \in A[x]$ entonces $g(x) = f(x)q(x) + r(x)$ donde $q(x), r(x) \in A[x]$ y $\deg(r(x)) < n$.

Tenemos que $g(b) = r(b) = a_0 + a_1 b + \cdots + a_{n-1} b^{n-1}$, en consecuencia $A[b]$ es un $A-$módulo generado por $1, b, \ldots, b^{n-1}$.

Si partimos ahora de ser $A[b]$ un $A-$módulo finitamente generado y $w_1, \ldots, w_n$ un sistema de generadores. Entonces para cualquier elemento $c \in A[b]$

$$w_i c = w_1 a_{i1} + \cdots + w_n a_{in}, \quad 1 \leq i \leq n, \quad a_{ij} \in A$$

$$((a_{ij}) - Ic)w = \begin{pmatrix} a_{11} - c & \cdots & a_{1i} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{i1} & \cdots & a_{ii} - c & \cdots & a_{in} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{ni} & \cdots & a_{nn} - c \end{pmatrix} \begin{pmatrix} w_1 \\ \vdots \\ w_i \\ \vdots \\ w_n \end{pmatrix} = 0$$

Esto implica que $det((a_{ij}) - Ic) = 0$, lo que nos da un polinomio mónico de grado $n \geq 1$ que se anula para c, por lo tanto es un elemento íntegro. haciendo los ajustes necesarios se ve que b es íntegro sobre A.

Corolario 1.1.2.5. Sean A y B dominios de integridad con $A \subseteq B$. Sean $b_1, \dots, b_n \in B$. Entonces son equivalentes:

1. $b_1, \dots, b_n$ son íntegros sobre A
2. $A[b_1, \dots, b_n]$ es un $A-$módulo finitamente generado

Proposición 1.1.2.6. Sean $A \subseteq B \subseteq C$ una torre de dominios de integridad. Si B es íntegro sobre A y $c \in C$ es íntegro sobre B entonces $c \in C$ es íntegro sobre A.

Demostración. Dado $c \in C$ íntegro sobre B, existen $b_1, \dots, b_n \in B$ tales que

$$c^n + b_n c^{n-1} + \cdots + b_2 c + b_1 = 0$$

De este modo probamos que c es íntegro en $A[b_1, \dots, b_n]$, que es un $A-$módulo finitamente generado, por lo tanto $A[b_1, \dots, b_n][c] = A[b_1, \dots, b_n, c]$ es $A-$módulo finitamente generado, que por el corolario 1.1.2.5 implica que c es íntegro sobre A.

Definición 1.1.2.7 (Clausura Íntegra). *Sean A y B dominios de integridad con $A \subseteq B$. Entonces el conjunto de todos los elementos de B que son íntegros sobre A se llama la clausura íntegra de A en B y se denota $\overline{A}^B$.*

Si la clausura íntegra de A resulta ser él mismo en B se dice que es íntegramente cerrado sobre B. En el caso en el que $B = Q(A)$ se dice sencillamente que A es íntegramente cerrado.

Observación 1.1.2.8. La clausura íntegra de A en B es un dominio de integridad contenido en B y que contiene a A.

Definición 1.1.2.9 (Anillo de Enteros). *Sea K un cuerpo de números algebraicos sobre $\mathbb{Q}$. El anillo de enteros de K, denotado $\mathcal{O}_K$, es la clausura íntegra de $\mathbb{Z}$ en K.*

Estas dos definiciones serán la base sobre la que vamos a trabajar. Los elementos de un anillo de enteros son un primer acercamiento a la idea de factorización más genérica que queremos desarrollar. Veremos que ser íntegramente cerrado es una condición necesaria para la factorización única de elementos.

Proposición 1.1.2.10. Sea D un dominio de factorización única y $K = Q(D)$ su cuerpo de fracciones. Entonces $k \in K$ es íntegro sobre D si y sólo si $k \in D$.

Demostración. Si $k \in D$ no es necesario probar nada ya que todos los elementos de D son íntegros sobre él.

Si $k \in K \setminus D$ y suponemos que es íntegro sobre D entonces satisface la ecuación

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

Donde $a_i \in A,\ 0 \leq i \leq n-1$. Como $k \in K$ podemos expresarlo como $k = r/s$ con $r, s \in A,\ s \neq 0$ y $\gcd(r, s) = 1$, así llegamos a

$$r^n + a_{n-1}r^{n-1}s + \cdots + a_1 r s^{n-1} + s^n = 0$$

Si s no es una unidad en D entonces es divisible por algún primo p. Según la ecuación anterior r también sería divisible por p. Esto contradice que $\gcd(r, s) = 1$ y por lo tanto $k = rs^{-1} \in D$.

Corolario 1.1.2.11. La clausura íntegra de D un dominio de factorización única sobre K, su cuerpo de fracciones, es $\overline{D}^K = D$ y por consiguiente es íntegramente cerrado.

Corolario 1.1.2.12. Sea D un dominio de factorización única. Entonces D es íntegramente cerrado.

Ejemplo 1.1.2.13. $\mathbb{Z}[\sqrt{-3}]$ no es íntegramente cerrado. Su cuerpo de fracciones es $\mathbb{Q}(\sqrt{-3})$, si tomamos $\alpha = \frac{1+\sqrt{-3}}{2}$ está claro que $\alpha \in \mathbb{Q}(\sqrt{-3})$ y $\alpha \notin \mathbb{Z}[\sqrt{-3}]$, sin embargo se tiene que $\alpha^2 - \alpha + 1 = 0$, por lo tanto es íntegro sobre $\mathbb{Z}[\sqrt{-3}]$. Por el contrarecíproco del corolario 1.1.2.12 obtenemos que $\mathbb{Z}[\sqrt{-3}]$ no es dominio de factorización única, esto se ve en que $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ siendo todos irreducibles.

Traza y Norma

Ahora nos disponemos a definir dos conceptos que nos van a ayudar a identificar de una forma mucho más sencilla los elementos íntegros y su reducibilidad vistos en una extensión finita de cuerpos L/K. La traza nos será de especial utilidad en el siguiente capítulo, ya que nos va a definir la clase del elemento X en dicha extensión en el lema 2.2.2.1 de la sección 2.2.

Definición 1.1.3.1. *Sea L/K una extensión de cuerpos finita, la traza y la norma de un elemento $x \in L$ se definen respectivamente como la traza y el determinante del endomorfismo del $K-$espacio vectorial L:*

$$T_x : L \to L, \quad T_x(a) = xa,$$

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(T_x), \qquad \mathrm{N}_{L/K}(x) = \det(T_x).$$

Observación 1.1.3.2. En el polinomio característico de T_x

$$f_x(t) = \det(t \cdot \mathrm{I} - T_x) = t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n \in K[t], \quad n = [L : K]$$

podemos reconocer la traza y la norma como

$$a_1 = \mathrm{Tr}_{L/K}(x) \quad \text{y} \quad a_n = \mathrm{N}_{L/K}(x).$$

Además se tiene que $T_{x+y} = T_x + T_y$ y $T_{xy} = T_x \circ T_y$

Proposición 1.1.3.3. Sea L/K una extensión de cuerpos. Si L/K es una extensión separable, $x \in L$ y $\sigma : L \to \overline{K}^L$ varía por las diferentes $K-$inmersiones de L en la clausura algebraica $\overline{K}^L$ entonces tenemos

1. $f_x(t) = \prod_\sigma (t - \sigma x)$
2. $Tr_{L/K}(x) = \sum_\sigma \sigma x$
3. $N_{L/K}(x) = \prod_\sigma \sigma x$

Demostración. Sea $K(x)/K$ una de las extensiones algebraicas, vamos a ver que el polinomio característico es una potencia del polinomio mínimo de x

$$p_x(t) = t^m + c_1 t^{m-1} + \cdots + c_m, \quad m = [K(x) : K]$$

Como hemos visto en la proposición 1.1.2.4, $1, x, \ldots x^{m-1}$ es una base de $K(x)/K$ y $\alpha_1, \ldots, \alpha_d$ lo es de $L/K(x)$, donde $d = [L : K(x)]$. Entonces

$$\alpha_1, \alpha_1 x, \ldots \alpha_1 x^{m-1}, \ldots, \alpha_d, \alpha_d x, \ldots \alpha_d x^{m-1}$$

es base de L/K. La matriz de la transformación lineal $T_x : y \to xy$ con respecto a esta base tiene únicamente bloques en la diagonal de la forma

$$\begin{pmatrix} & & -c_0 \\ 1 & & -c_1 \\ & \ddots & \vdots \\ & 1 & -c_{m-1} \end{pmatrix}$$

Es fácil comprobar que el polinomio característico de cada bloque es $p_x(t)$, luego, el polinomio característico de T_x es $f_x(t) = p_x(t)^d$.

El conjunto $Hom_K(L, \overline{K}^L)$ de $K-$inmersiones de L está particionado por la relación de equivalenca $\sigma \sim \tau \iff \sigma x = \tau x$ en m clases de equivalencia de d elementos cada una. Si $\sigma_1, \dots, \sigma_m$ son representantes, entonces

$$p_x(t) = \prod_{i=1}^{m}(t - \sigma_i x)$$

Y por lo tanto

$$f_x(t) = \prod_{i=1}^{m}(t - \sigma_i x)^d = \prod_{i=1}^{m}\prod_{\sigma\sim\sigma_i}(t - \sigma x) = \prod_{\sigma}(t - \sigma x)$$

Con esto concluye la prueba del primer punto, y por la observación 1.1.3.2 se sigue el resto.

Corolario 1.1.3.4. En una torre de de extensiones separables $K \subseteq M \subseteq L$ se tiene que

$$\mathrm{Tr}_{M/K} \circ \mathrm{Tr}_{L/M} = \mathrm{Tr}_{L/K}, \quad \mathrm{N}_{M/K} \circ \mathrm{N}_{L/M} = \mathrm{N}_{L/K}$$

Demostración. *La prueba puede encontrarse en [4, Página 10]*

Las funciones Traza y Norma evaluadas en elemento íntegros pertenecen a la clausura íntegra base en una extensión, esto se puede ver fácilmente en la observación 1.1.3.2

Con un simple chasquido, comprobar si elementos de la extensión son íntegros o no con unas simples ecuaciones se convierte en un juego.

Definición 1.1.3.5. *Sea una base $\alpha_1, \dots, \alpha_n$ de una extensión separable L/K. El disciminante de dicha base se define como*

$$\mathrm{d}(\alpha_1, \dots, \alpha_n) = det((\sigma_i \alpha_j))^2,$$

donde $\sigma_i : L \to \overline{K}^L$ varía por las diferentes $K-$inmersiones de L en la clausura algebraica $\overline{K}^L$.

Observación 1.1.3.6. Sea la matriz $A = (\sigma_i \alpha_j)_{ij}$, por la relación dada en 1.1.3.3(2.)

$$\mathrm{Tr}_{L/K}(\alpha_i \alpha_j) = \sum_k (\sigma_k \alpha_i)(\sigma_k \alpha_j) = (\sigma_i \alpha_j)^t_{ij}(\sigma_i \alpha_j)_{ij} = A^t A.$$

Lo cual hace que

$$\mathrm{d}(a_1, \dots, a_n) = \det\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right).$$

En el caso concreto de una base del tipo $1, \theta, \dots, \theta^{n-1}$ se tiene que

$$\mathrm{d}(1, \theta, \dots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2, \quad \theta_k = \sigma_k \theta$$

Proposición 1.1.3.7. Sea L/K una extensión separable y $\alpha_1, \dots, \alpha_n$ una base, entonces $\mathrm{d}(\alpha_1, \dots, \alpha_n) \neq 0$ y la aplicación bilineal del $K-$espacio vectorial L $(x, y) = \mathrm{Tr}_{L/K}(xy)$ no es degenerada.

Demostración. Sea θ un elemento primitivo para L/K, es decir, $L = K(\theta)$. Entonces $1, \theta, \dots, \theta^{n-1}$ es una base con la que la forma (x, y) viene dada por la matriz $M = \mathrm{Tr}_{L/K}(\theta^{i-1}\theta^{j-1})$ no es degenerada porque para cada $\theta_i = \sigma_i \theta$

$$\det(M) = d(1, \theta, \dots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \neq 0$$

Si $\alpha_1, \dots, \alpha_n$ es otra base de L/K, entonces la forma bilineal (x, y) vendrá dada por $M = \mathrm{Tr}_{L/K}(\alpha_i \alpha_j)$ que por lo anterior se sigue que $\mathrm{d}(\alpha_1, \dots, \alpha_n) = \det(M) \neq 0$. ∎

Corolario 1.1.3.8. Sea A un dominio de integridad con cuerpo de fracciones K, L/K una extensión separable y B la clausura íntegra de A en L/K. Sea $\alpha_1, \dots, \alpha_n$ una base de L/K que está contenida en B de discriminante $d = d(\alpha_1, \dots, \alpha_n)$. Entonces se tiene que

$$d\,B \subseteq A\alpha_1 + \cdots + A\alpha_n$$

Ejemplo 1.1.3.9. Consideremos $m \in \mathbb{Z}$ libre de cuadrados distinto de 0 y 1, y la extensión $\mathbb{Q}(\sqrt{m})$. Sea $\alpha = \dfrac{a + b\sqrt{m}}{c}$ un elemento íntegro con $a, b, c \in \mathbb{Z}$ tales que $\gcd(a, c) = \gcd(b, c) = 1$ y $c \neq 0, 1, -1$.

$$\begin{aligned} \mathrm{Tr}_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) &= \tfrac{a+b\sqrt{m}}{c} + \tfrac{a-b\sqrt{m}}{c} = \tfrac{2a}{c} \in \mathbb{Z} \quad \Rightarrow \quad c = 2 \\ \mathrm{N}_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(\alpha) &= \tfrac{a+b\sqrt{m}}{2} \cdot \tfrac{a-b\sqrt{m}}{2} = \tfrac{a^2-b^2m}{4} \in \mathbb{Z} \quad \Rightarrow \quad a^2 \equiv b^2 m \bmod 4 \end{aligned}$$

Distinguiremos los casos en los que $m \equiv 1, 2, 3 \bmod 4$.

a	0	1	2	3
a^2	0	1	0	1
b^2	0	1	0	1
$2b^2$	0	2	0	2
$3b^2$	0	3	0	3

$$\Rightarrow \begin{cases} m \equiv 1 \bmod 4 & \begin{cases} \frac{a+b\sqrt{m}}{2} \text{ es íntegro si } a \text{ y } b \text{ tienen} \\ \text{la misma paridad} \end{cases} \\ m \equiv 2, 3 \bmod 4 & \begin{cases} a + b\sqrt{m} \text{ es íntegro} \end{cases} \end{cases}$$

Entonces, si $m \equiv 1 \bmod 4$, $\{1, \frac{1+\sqrt{m}}{2}\}$ es base de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})} = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ y $\mathrm{d}(1, \frac{1+\sqrt{m}}{2}) = m$.
Si $m \equiv 2, 3 \bmod 4$, $\{1, \sqrt{m}\}$ es base de de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})} = \mathbb{Z}[\sqrt{m}]$ y $\mathrm{d}(1, \sqrt{m}) = 4m$.

1.2 Teoría de Ramificación

Aquí desarrollaremos las secciones 3, 8 y 9 del capítulo 1 del libro *Algebraic number theory-Neukirck*[4], en la que veremos la factorización de ideales en cuerpos que yacen sobre ellos y otros resultados interesantes como nuestro viejo amigo el Teorema Chino del Resto.

Dominios de Dedekind

Consideremos un cuerpo de números algebraicos K sobre un dominio Noetheriano, y en él su anillo de enteros $\mathcal{O}_K$. Nuestro objetivo es generalizar la factorización que existe en $\mathbb{Z} \subset \mathbb{Q}$ para elementos que no son unidades, o en cualquier dominio de ideales principales, ya que aquí podemos observar indistintamente ideales y elementos. Tal y como hemos visto en el primer ejemplo no siempre es posible, pero si en lugar de en sus elementos nos fijamos en sus ideales es cuando todo empieza a cobrar sentido.

Definición 1.2.1.1 (Dominio de Dedekind). *Un dominio de Dedekind es un dominio de integridad que satisface la siguientes propiedades:*

1. *Todo ideal es finitamente generado.*
2. *Todo ideal primo no trivial es maximal.*
3. *Es íntegramente cerrado en su cuerpo de fracciones.*

Lema 1.2.1.2. Sea K un cuerpo, y α un elemento íntegro sobre K. La extensión finita $K(\alpha) \supset K$ de grado n, formada al añadir el elemento α, es cuerpo.

Demostración. Sea α un elemento íntegro sobre K entonces existe un polinomio mónico $f(x) \in K[x]$ de grado $n \geq 1$ tal que $f(\alpha) = 0$. Tomemos f de grado mínimo y supongamos que es reducible. En este caso existen $g(x), h(x) \in K[x]$ no unidades tales que $f(x) = g(x)h(x)$. Esto implica que $f(\alpha) = g(\alpha)h(\alpha) = 0$ y por tanto $g(\alpha) = 0$ o $h(\alpha) = 0$, pero no es posible ya que $f(x)$ es de grado mínimo, es decir, $g(x)$ o $h(x)$ es una unidad. De aquí $f(x)$ es irreducible y $\langle f(x) \rangle$ es maximal en $K[x]$, por ende $K[X]/\langle f \rangle = K(\alpha)$ es cuerpo. ∎

Proposición 1.2.1.3. Tomemos el dominio $\mathbb{Z}$, y sea K un cuerpo de números algebraicos sobre $\mathbb{Z}$. Si $\mathcal{O}_K$ el anillo de enteros de K entonces $\mathcal{O}_K$ es un dominio de Dedekind.

Demostración. Por la propia definición de anillo de enteros $\mathcal{O}_K$ es íntegramente cerrado y también es un $\mathbb{Z}-$módulo finitamente generado por el corolario1.1.2.5. Aplicando el corolario 1.1.1.20 a lo anterior vemos que $\mathcal{O}_K$ es Noetheriano. Tomemos un ideal primo $\mathfrak{p} \in \mathcal{O}_K$, $\mathfrak{p} \neq 0$, y consideremos $(p) = \mathfrak{p} \cap \mathbb{Z}$ que es un ideal primo en $\mathbb{Z}$. Sea $x \in \mathfrak{p}$, $x \neq 0$, se tiene el polinomio

$$x^n + a_{n-1}x^{n-1} + \cdots + xa_1 + a_0 = 0,\ a_i \in D\ 1 \leq i \leq n-1,\ a_0 \in \mathfrak{p} \cap \mathbb{Z},\ a_0 \neq 0.$$

Con esto se prueba que $(p) \neq 0$. Entonces el dominio de integridad $\overline{\mathcal{O}} = \mathcal{O}_K/\mathfrak{p}$ se levanta desde $\mathbb{Z}/(p) \simeq \frac{\mathbb{Z}+\mathfrak{p}}{\mathfrak{p}}$ añadiendo elementos algebraicos. Por el lema 1.2.1.2 $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo, y de aquí $\mathfrak{p}$ es ideal maximal. ∎

Podemos considerar los dominios de Dedekind como una generalización de $\mathbb{Z}$ en cuanto al trato con sus ideales. Sean I y J ideales de un dominio de Dedekind se tiene que

1. La divisibilidad, $I \mid J$, está definida por la contención $J \subseteq I$
2. El mayor común divisor de I y J es la suma$I + J = \{a + b \mid a \in I, b \in J\}$
3. El menor común múltiplo de I y J es la multiplicación $IJ = \left\{ \sum_i a_i b_i \mid a_i \in I, b_i \in J \right\}$

Observación 1.2.1.4. Dados dos ideales, I y J, decimos que son relativamente primos si $\gcd(I, J) = \langle 1 \rangle = \mathcal{O}_K$

Proposición 1.2.1.5. En un dominio Noetheriano todo ideal no trivial contiene un producto de ideales primos.

Demostración. Sea D un dominio Noetheriano que contiene al menos un ideal no trivial que no contiene un producto de ideales primos. LLamemos S al conjunto de estos ideales, $S \neq \emptyset$, como D es Noetheriano cumple la condición maximal, es decir, $\exists I \in S$ maximal con respecto a dicha propiedad.

Puesto que I no es primo $\exists a_1, a_2 \notin I$ tales que $a_1 a_2 \in I$. Sean $J_1 = \langle a_1 \rangle + I$ y $J_2 = \langle a_2 \rangle + I$, se tiene que $I \subsetneq J_1, J_2$ por lo que no están en S. Esto significa que ambos contienen un producto de ideales primos. Ahora bien

$$J_1 J_2 = (\langle a_1 \rangle + I)(\langle a_2 \rangle + I) \subset I$$

y por lo tanto existe un producto de ideales primo contenido en I, lo que contradice que $I \in S$. ∎

Lema 1.2.1.6. Sea $\mathcal{O}_K$ un dominio de Dedekind, y $\mathfrak{p} \subset \mathcal{O}_K$ es un ideal primo. Definamos

$$\mathfrak{p}^{-1} = \{x \in K | x\mathfrak{p} \subseteq \mathcal{O}_K\}.$$

Entonces, $\forall I \subset \mathcal{O}_K$ ideal no trivial, se tiene que

$$I\mathfrak{p}^{-1} = \left\{ \sum_i a_i x_i \mid a_i \in I,\ x_i \in \mathfrak{p}^{-1} \right\} \neq I$$

Demostración. Sea $a \in \mathfrak{p}$ no nulo, y $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \langle a \rangle \subset \mathfrak{p}$, con r tan pequeño como sea posible. Entonces, por ser $\mathfrak{p}$ ideal primo, uno de los $\mathfrak{p}_i$, digamos $\mathfrak{p}_1$, está contenido en $\mathfrak{p}$, por lo que $\mathfrak{p}_1 = \mathfrak{p}$ ya que ambos son maximales.

Como $\mathfrak{p}_2 \cdots \mathfrak{p}_r \nsubseteq \langle a \rangle$, $\exists b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ tal que $b \notin a\mathcal{O}_K$, es decir, $a^{-1}b \notin \mathcal{O}_K$. Por otro lado tenemos que $b\mathfrak{p} \subseteq a\mathcal{O}_K$, lo que es los mismo que $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}_K$, de aquí $a^{-1}b \in \mathfrak{p}^{-1}$. Se sigue que $\mathfrak{p}^{-1} \neq \mathcal{O}_K$.

Sea ahora $I \neq 0$ un ideal de $\mathcal{O}_K$ y $a_1, \ldots, a_n$ un sistema de generadores. Supongamos que $I\mathfrak{p}^{-1} = I$, entonces para cualquier $x \in \mathfrak{p}^{-1}$

$$xa_i = \sum_j c_{ij} a_j, \quad c_{ij} \in \mathcal{O}_K, \quad 1 \leq i, j \leq n$$

Siguiendo el ritmo de la de la proposición 1.1.2.4 obtendíamos un polinomio en $\mathcal{O}_K[x]$ dado por el determinante de una matriz, lo cual diría que $x \in \mathcal{O}_K$. De aquí $\mathfrak{p}^{-1} = \mathcal{O}_K$, una contradicción con lo anterior.

Teorema 1.2.1.7 (Factorización Ideales). *Todo ideal $I \subset \mathcal{O}_K$ distinto de $\langle 0 \rangle$ y $\langle 1 \rangle$ admite una factorización $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ en ideales primos $\mathfrak{p}_i$ de $\mathcal{O}_K$ que es única salvo por el orden de los factores.*

Demostración (Existencia). Sea S el conjunto de todos los ideales distintos de $\langle 0 \rangle$ y $\langle 1 \rangle$ que no admiten descomposición en ideales primos. Si S no es vacío, por el mismo razonamiento que en la proposición 1.2.1.5 debe existir un elemento maximal I en S. Éste está contenido en un ideal maximal $\mathfrak{p}$, así que

$$I \subseteq I\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$$

Por el lema 1.2.1.6 se tiene que $I \subsetneq I\mathfrak{p}^{-1}$ y $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$. Al set $\mathfrak{p}$ ideal maximal sigue que $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$. En vista a la maximalidad de I en S, $I \neq \mathfrak{p}$ y $I\mathfrak{p}^{-1} \neq \mathcal{O}_K$. Entonces el ideal $I\mathfrak{p}^{-1}$ admite una descomposición en ideales primos $I\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, y también lo hace $I = I\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{p}$, en contradicción ya que $I \in S$.

Demostración (Unicidad). Sea I un ideal tal que tiene dos factorizaciones distintas en ideales primos

$$I = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

Entonces $\mathfrak{p}_1$ divide algún factor $\mathfrak{q}_i$, digamos $\mathfrak{q}_1$, y siendo maximales $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplicamos por $\mathfrak{p}_1^{-1}$ y obtenemos

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$$

Continuando este proceso llegamos a que $r = s$ y que $\mathfrak{p}_i = \mathfrak{q}_i \forall 1 \leq i \leq r$. ∎

Observación 1.2.1.8. Agrupando las ocurrencias de algunos ideales primos obtenemos la descomposición $I = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_r^{v_r}$, $v_i > 0$.

A continuación nos reencontramos con un viejo amigo. Dado un producto $I = I_1 \cdots I_n$ de ideales relativamente primos podemos obtener un análogo al *Teorema chino del Resto* que ya conocemos para comprobar si un elemento pertenece o no a I.

Teorema 1.2.1.9 (Teorema Chino del Resto). *Sean $I_1, \ldots, I_n$ ideales en un dominio de Dedekind $\mathcal{O}$ tales que $I_i + I_j = \mathcal{O}$ para todo $i \neq j$. Entonces, si $I = \bigcap_{i=1}^{n} I_i$, se tiene*

$$\mathcal{O}/I \cong \bigoplus_{i=1}^{n} \mathcal{O}/I_i.$$

Demostración. El homomorfismo canónico

$$\mathcal{O} \to \bigoplus_{i=1}^{n} \mathcal{O}/I_i, \quad a \to \bigoplus_{i=1}^{n} a \bmod I_i$$

tiene kernel $I = \bigcap_{i=1}^{n}$, lo que nos da inyectividad, luego nos basta probar la sobreyectividad. Sean $x_i \bmod I_i \in \mathcal{O}/I_i$ dados para $1 \leq i \leq n$. Si $n = 2$ podemos escribir $1 = a_1 + a_2$, $a_i \in I_i$, y tomando $x = x_1a_2 + x_2a_1$ tenemos que $x \equiv x_i \bmod I_i$, $i = 1, 2$.

Si $n > 2$, podemos encontrar elementos $y_1, y_2, \ldots, y_n$ tales que

$$y_i \equiv 1 \bmod I_i, \quad y_i \equiv 0 \bmod \bigcap_{j \neq i} I_j.$$

Tomando $x = x_1y_1 + x_2y_2 + \cdots + x_ny_n$ nos encontramos con que $x \equiv x_i \bmod I_i$, $1 \leq i \leq n$. De aquí sacamos la sobreyectividad. ∎

Definición 1.2.1.10 (Ideal Fraccionario). *Sea D un dominio de integridad con cuerpo de fracciones K. Un subconjunto I no vacío de K se llama $D-$ideal fraccionario si satisface las siguientes propiedades:*

1. *Si $a, b \in I$, entonces $a + b \in I$*
2. *Si $a \in I$ y $d \in D$, entonces $ad \in I$*
3. *Existe $\gamma \in D$ tal que $\gamma I \subseteq D$*

Ejemplo 1.2.1.11. Sea $D = \mathbb{Z}$ y $K = \mathbb{Q}$ entonces los $\mathbb{Z}$-ideales fraccionarios son $I_q = \{q\mathbb{Z} | q \in \mathbb{Q}^+\}$. De hecho forman un grupo multiplicativo con $\mathbb{Z}$ como unidad.

Proposición 1.2.1.12. Sea K un cuerpo de números, los $\mathcal{O}_K-$ideales fraccionarios de K forman un grupo abeliano. La identidad es $\mathcal{O}_K$ y el inverso de un ideal I es

$$I^{-1} = \{x \in K \mid xI \subseteq \mathcal{O}_K\}.$$

Demostración. Fácilmente se tiene la asociatividad y la conmutatividad, y además $I\mathcal{O}_K = I$. Sea $\mathfrak{p}$ un ideal primo, el lema 1.2.1.6 nos dice que $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$ y por tanto $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$ porque $\mathfrak{p}$ es maximal. Del mismo modo, si $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ es un ideal en $\mathcal{O}_K$, $J = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$ es un inverso. $IJ = \mathcal{O}_K$ implica que $J \subseteq I^{-1}$. Por otro lado, si $xI \subseteq \mathcal{O}_K$, entonces $xIJ \subset J$, así $x \in J$, ya que $IJ = \mathcal{O}_K$. Por lo tanto tenemos que $J = I^{-1}$. Finalmente, si I es un $\mathcal{O}_K-$ideal fraccionario arbitrario y $a \in \mathcal{O}_K$, no nulo, es tal que $aI \subseteq \mathcal{O}_K$, entonces $(aI)^{-1} = a^{-1}I^{-1}$ es el inverso de aI, así que $I^{-1}I = \mathcal{O}_K$.

Extensiones de Dominios de Dedekind

Supongamos que partimos desde un dominio de Dedekind y realizamos un extensión finita de su cuerpo de fracciones. Nos preguntamos si, evidentemente, todo lo que acabamos de ver sigue funcionando. La respuesta es que sí, aunque tendremos que ser algo selectivos en cuanto a los ideales que consideramos para aplicar nuestros conocimientos.

Veremos que tan sólo una cantidad finita de ideales son los conflictivos, con esta súbita suerte deberíamos preguntarnos cuantas manos hemos estrechado hoy.

Proposición 1.2.2.1. Sea $\mathfrak{o}$ un dominio de Dedekind con cuerpo de fracciones K, sea L/K una extensión separable K y $\mathcal{O}$ la clausura íntegra de $\mathfrak{o}$ en L. Entonces $\mathcal{O}$ es de nuevo dominio de Dedekind.

Demostración. Puesto que $\mathcal{O}$ la clausura íntegra de $\mathfrak{o}$ es íntegramente cerrado. Sea $\mathfrak{P}$ un ideal primo de $\mathcal{O}$, $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}$ es ideal primo de $\mathfrak{o}$ no nulo. De aquí, el dominio de integridad $\mathcal{O}/\mathfrak{P}$ es una extensión del cuerpo $\mathfrak{o}/\mathfrak{p}$, por lo tanto también es cuerpo por el lema 1.2.1.2, por ende $\mathfrak{P}$ es ideal maximal. Nos queda probar que $\mathcal{O}$ es Noetheriano. Sea $a_1, \dots, a_n$ una base de L/K contenida en $\mathcal{O}$ de discriminante $d = d(a_1, \dots, a_n) \neq 0$ por la proposición 1.1.3.7 y por el corolario 1.1.3.8 obtenemos que $\mathcal{O}$ está contenido en el $\mathfrak{o}-$módulo $Aa_1/d + \cdots + Aa_n/d$ finitamente generado. Tenemos que $\mathfrak{o}$ es un dominio Noetheriano y que $\mathcal{O} \supseteq \mathfrak{o}$ es un $\mathfrak{o}-$módulo finitamente generado, por lo tanto, por el corolario1.1.1.20, $\mathcal{O}$ es Noetheriano.

Trasladando lo visto para dominios de Dedekind, si tomamos un ideal primo $\mathfrak{p}$ en el anillo $\mathfrak{o}$ se descompone en $\mathcal{O}$ de manera única en un producto de ideales primos

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

Siendo estos ideales $\mathfrak{P}_i$ los que yacen sobre $\mathfrak{p}$ en el sentido en que $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}$.

Definición 1.2.2.2 (Índice de Ramificación y Grado de Inercia). *Sea $\mathfrak{p}$ un ideal primo de $\mathfrak{o}$ y $\mathfrak{P}$ un ideal primo de $\mathcal{O}$ que aparece en la descomposición de $\mathfrak{p}$. Llamamos índice de ramificación de $\mathfrak{P}$ al exponente e con el que aparece en la descomposición de $\mathfrak{p}$ y el grado de la extensión $f = [\mathcal{O}/\mathfrak{P} : \mathfrak{o}/\mathfrak{p}]$ se llama grado de inercia de $\mathfrak{P}$ sobre $\mathfrak{p}$.*

Proposición 1.2.2.3. Sea L/K una extensión separable de grado n y la descomposición $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ del ideal primo $\mathfrak{p}$ en $\mathcal{O}$. Entonces se tiene la identidad fundamental

$$\sum_{i=i}^{r} e_i f_i = n.$$

Demostración. La prueba se basa en el Teorema Chino del Resto

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \bigoplus_{i=1}^{r} \mathcal{O}/\mathfrak{P}_i^{e_i}.$$

Teniendo en cuenta que $\mathcal{O}/\mathfrak{p}\mathcal{O}$ y $\mathcal{O}/\mathfrak{P}_i^{e_i}$ son espacios vectoriales sobre el cuerpo $k = \mathfrak{o}/\mathfrak{p}$ nos basta comprobar que

$$\dim_{\mathfrak{o}/\mathfrak{p}}(\mathcal{O}/\mathfrak{p}\mathcal{O}) = n \quad \text{y} \quad \dim_{\mathfrak{o}/\mathfrak{p}}(\mathcal{O}/\mathfrak{P}_i^{e_i}) = e_i f_i$$

Sean $b_1, \dots, b_m \in \mathcal{O}$ representantes de una base $\overline{b}_1, \dots, \overline{b}_m$ de $\mathcal{O}/\mathfrak{p}\mathcal{O}$ sobre k, nos basta con probar que $b_1, \dots, b_m$ es una base de L/K. Supongamos que $b_1, \dots, b_m$ son linealmente dependientes sobre K, y por tanto también sobre $\mathfrak{o}$. Entonces existen elementos $a_1, \dots, a_m \in \mathfrak{o}$ no todos nulos tales que

$$a_1 b_1 + \cdots a_m b_m = 0.$$

Consideremos el ideal $J = \langle a_1, \dots, a_m \rangle$ de $\mathfrak{o}$ y un elemento $a \in J^{-1}$ tal que $a \notin J^{-1}\mathfrak{p}$, así $aJ \nsubseteq \mathfrak{p}$. Entonces los elementos $aa_1, \dots, aa_m$ están en $\mathfrak{o}$ pero no todos en $\mathfrak{p}$ llegando a la congruencia

$$aa_1b_i + \cdots + aa_mb_m \equiv 0 \bmod \mathfrak{p}$$

que resulta en la dependencia lineal de $\overline{b}_1, \dots, \overline{b}_m$ en k, que es una contradicción. Por lo que $b_1, \dots, b_m$ son linealmente independientes sobre K.

Para ver que los b_i forman una base de L/K consideramos los $\mathfrak{o}-$módulos $M = \mathfrak{o}b_1 + \cdots + \mathfrak{o}b_m$ y $N = \mathcal{O}/M$. Dado que $\mathcal{O} = M + \mathfrak{p}\mathcal{O}$, tenemos que $N = \mathfrak{p}N$, y como L/K es separable, $\mathcal{O}$ y N son $\mathfrak{o}-$módulos finitamente generados. Si $c_1, \dots, c_s$ es un sistema de generadores de N, entonces

$$c_i = \sum_{j=1}^{s} a_{ij}c_j, \quad a_{ij} \in \mathfrak{p}.$$

Sea A la matriz $(a_{ij} - I)$, y sea B la matriz adjunta de A. Entonces se da que $A(c_1, \dots, c_n)^t = 0$ y $BA = dI$, donde $d = det(A)$. Por consiguiente

$$0 = BA(c_1, \dots, c_n)^t = (dc_1, \dots, dc_n)^t,$$

Y por tanto $dN = 0$, es decir, $d\mathcal{O} \subseteq M = \mathfrak{o}b_1 + \cdots + \mathfrak{o}b_m$. Nos encontramos con que $d = (-1)^s \bmod \mathfrak{p}$ ya que $a_{ij} \in \mathfrak{p}$. Se sigue que $L = dL = Kb_1 + \cdots + kb_m$ y de aquí, $b_1, \dots, b_m$ es una base de L/K.

Para probar la segunda identidad, consideremos la cadena descendiente de $k-$espacios vectoriales

$$\mathcal{O}/\mathfrak{P}_i^{e_i} \supseteq \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \supseteq \cdots \supseteq \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i} \supseteq \langle 0 \rangle$$

Los cocientes sucesivos tomados como $\mathfrak{P}_i^v/\mathfrak{P}_i^{v+1}$ en esta cadena son todos isomorfos a $\mathcal{O}\mathfrak{P}_i$, ya que para $b \in \mathfrak{P}_i^v \backslash \mathfrak{P}_i^{v+1}$ podemos definir el homomorfismo

$$\mathcal{O} \to \mathfrak{P}_i^v/\mathfrak{P}_i^{v+1}, \quad a \to ab,$$

con kernel $\mathfrak{P}_i$. Este es sobreyectivo ya que $\mathfrak{P}_i^v$ es el máximo común divisor entre $\mathfrak{P}_i^{v+1}$ y $\langle b \rangle = b\mathcal{O}$ por tanto $\mathfrak{P}_i^v = b\mathcal{O} + \mathfrak{P}_i^{v+1}$. Al ser $f_i = [\mathcal{O}/\mathfrak{P}_i : k]$, obtenemos que $\dim_k(\mathfrak{P}_i^v/\mathfrak{P}_i^{v+1}) = f_i$ y de aquí

$$\dim_k(\mathcal{O}/\mathfrak{P}_i^{e_i}) = \sum_{v=0}^{e_i-1} \dim_k(\mathfrak{P}_i^v/\mathfrak{P}_i^{v+1}) = e_if_i.$$

Definición 1.2.2.4 (Conductor). *Sea L/K una extensión separable, $\theta \in \mathcal{O}$ un elemento primitivo tal que $L = K(\theta)$. Definimos el conductor $\mathfrak{F}$ del anillo $o[\theta]$ como el mayor ideal de $\mathcal{O}$ contenido en $o[\theta]$*

$$\mathfrak{F} = \{a \in \mathcal{O} \mid a\mathcal{O} \subseteq o[\theta]\}.$$

En este caso podremos ver, salvo para una cantidad finita de ideales que no son relativamente primos con el conductor, la descomposición de un ideal primo $\mathfrak{p}$ dentro de $\mathcal{O}$, y resultados muy interesantes que derivan de esta.

Proposición 1.2.2.5. Sea $\mathfrak{p}$ un ideal primo en o que es relativamente primo al conductor $\mathfrak{F}$ de $o[\theta]$ y sea $\overline{p}(x) = \overline{p}_1(x)^{e_1} \cdots \overline{p}_r(x)^{e_r}$ la factorización de $\overline{p}(x) \equiv p(x) \bmod \mathfrak{p}$, el polinomio mínimo de θ en irreducibles $\overline{p}_i(x) \equiv p_i(x) \bmod \mathfrak{p}$ sobre el cuerpo $o/\mathfrak{p}$ con todos los $p_i(x) \in o[x]$ mónicos. Entonces

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O}, \quad 1 \leq i \leq r,$$

son distintos ideales primos de $\mathcal{O}$ sobre $\mathfrak{p}$. El grado de inercia f_i de $\mathfrak{P}_i$ es el grado de $\overline{p}_i(x)$ y se tiene que

$$\mathcal{O}\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

Demostración. Sea $\mathcal{O}' = o[\theta]$ y $\overline{o} = o/\mathfrak{p}$, tenemos los siguientes isomorfismos

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \mathcal{O}'/\mathfrak{p}\mathcal{O}' \cong \overline{o}[x]/\langle \overline{p}(x) \rangle.$$

El primero surge del homomorfismo $\mathcal{O}' \to \mathcal{O}/\mathfrak{p}\mathcal{O}$, que es sobreyectivo, ya que $\mathfrak{p}\mathcal{O} + \mathfrak{F} = \mathcal{O}$ y de aquí $\mathfrak{p}\mathcal{O} + \mathcal{O}' = \mathcal{O}$, y tiene kernel $\mathfrak{p}\mathcal{O} \cap \mathcal{O}' = \mathfrak{p}\mathcal{O}'$ al ser $\mathfrak{p} + (\mathfrak{F} \cap o) = o$.

El segundo se deduce del homomorfismo sobreyectivo $o \to \overline{o}[x]/\langle \overline{p}(x) \rangle$, cuyo kernel es el ideal generado por $\mathfrak{p}\mathcal{O}$ y $\langle p(x) \rangle$. Puesto que $\mathcal{O}' = o[\theta] \cong o[x]/\langle p(x) \rangle$, se tiene que $\mathcal{O}'/\mathfrak{p}\mathcal{O}' \cong \overline{o}[x]/\langle \overline{p}(x) \rangle$.

Como $\overline{p}(x) = \prod_{i=1}^{r} \overline{p}_i(x)^{e_i}$, el Teorema Chino del Resto nos da el isomorfismo

$$\overline{o}[x]/\langle \overline{p}(x) \rangle \cong \bigoplus_{i=1}^{r} \overline{o}[x]/\langle \overline{p}_i(x) \rangle^{e_i}.$$

Esto muestra que los ideales primos del anillo $R = \overline{o}[x]/\langle \overline{p}(x) \rangle$ son los ideales principales $\langle \overline{p}_1 \rangle$ generados por $\overline{p}_i(x) \bmod \overline{p}(x)$ para $1 \leq i \leq r$, que el grado de extensión $[R/\langle \overline{p}_i \rangle : \overline{o}] = \deg(\overline{p}_i(x))$, y que $\langle 0 \rangle = \langle \overline{p} \rangle = \bigcap_{i=1}^{r} \langle \overline{p}_i \rangle^{e_i}$.

Vistos los isomorfismos anteriores, nos encontramos con la misma situación en $\overline{\mathcal{O}} = \mathcal{O}/\mathfrak{p}\mathcal{O}$. Por lo que los ideales $\overline{\mathfrak{P}}_i$ se corresponden con los ideales primos $\langle \overline{p}_i \rangle$, que son ideales principales generados por $\overline{p}_i(\theta) \bmod \mathfrak{p}\mathcal{O}$. El grado de la extensión $[\overline{\mathcal{O}}/\overline{\mathfrak{P}}_i : \overline{o}]$ es el grado del polinomio $\overline{p}_i(x)$, y tenemos que $\langle 0 \rangle = \bigcap_{i=1}^{r} \overline{\mathfrak{P}}_i^{e_i}$.

Sea ahora $\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O}$, la preimagen del ideal $\overline{\mathfrak{P}}_i$ del homomorfismo $\mathcal{O} \to \mathcal{O}/\mathfrak{p}\mathcal{O}$. Entonces $\mathfrak{P}_i$, para $1 \leq i \leq r$ varía por los ideales primos de $\mathcal{O}$ que se levantan sobre $\mathfrak{p}$. Se da que $f_i = [\mathcal{O}/\mathfrak{P}_i : o/\mathfrak{p}]$ es el grado del polinomio $\overline{p}_i(x)$. Es más, $\mathfrak{P}_i^{e_i}$ es la preimagen de $\overline{\mathfrak{P}}_i^{e_i}$, y $\mathfrak{p}\mathcal{O} \supseteq \bigcap_{i=1}^{r} \mathfrak{P}_i^{e_1}$, de manera que $\mathfrak{p}\mathcal{O} \mid \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$, y en consecuencia

$$\mathfrak{p}\mathcal{O} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i} \text{ porque } \sum_{i=1}^{r} e_i f_i = n.$$

Definición 1.2.2.6. *Sea un ideal primo en o, este se dice que descompone completamente en L si en su descomposición $\mathcal{O}\mathfrak{p} = \mathfrak{P}_i^{e_1} \cdots \mathfrak{P}_r^{e_r}$ se tiene que $r = n = [L : K]$, de forma que $f_i = e_i = 1$.*

Del mismo modo, se dice que que el ideal no descompone si $r = 1$.

Definición 1.2.2.7. *Sea $\mathfrak{P}_i$ un ideal que aparece en la descomposición $\mathcal{O}\mathfrak{p} = \mathfrak{P}_i^{e_1} \cdots \mathfrak{P}_r^{e_r}$. Se dice que no ramifica en o si $e_i = 1$ y si la extensión residual de cuerpo $(\mathcal{O}/\mathfrak{P}_i)/(o/\mathfrak{p})$ es separable. Si no, se dice que es ramificado, si además se tiene que $f_i = 1$ es completamente ramificado.*

Si ninguno los $\mathfrak{P}_i$ es ramificado, entonces se dice que $\mathfrak{p}$ no es ramificado. De otro modo es ramificado.

La extensión L/K se dice no ramificada si ninguno de los ideales primos de K es ramificado en L.

Proposición 1.2.2.8. Si L/K es separable, entonces tan sólo hay un número finito de ideales primos que ramifiquen en L.

Demostración. Sea $\theta \in \mathcal{O}$ un elemento primitivo para L , y $p(x) \in o[x]$ su polinomio mínimo. Sea el discriminante de $p(x)$

$$d = d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \in o.$$

Entonces todo ideal $\mathfrak{p}$ de K que sea relativamente primo a d y al conductor $\mathfrak{F}$ de $o[\theta]$ no ramifica. De hecho, por la proposición 1.2.2.5, cuando algún factor de $\overline{p}(x) \equiv p(x) \bmod \mathfrak{p}$ tenga exponente 1 en $o/\mathfrak{p}$ el índice de ramificación $e_i = 1$, es decir, si $\overline{p}(x)$

no tiene raíces múltiples, entonces $\mathfrak{p}$ no es ramificado. Pero en este caso $\overline{d} \equiv d \bmod \mathfrak{p}$, discriminante de $\overline{p}(x)$, no es nulo. Las extensiones residuales de cuerpo $(\mathcal{O}/\mathfrak{P}_i)/(\mathcal{O}/\mathfrak{p})$ están generados por $\overline{\theta} \equiv \theta \bmod \mathfrak{P}_i$ y son, por tanto, separables. De aquí $\mathfrak{p}$ no es ramificado.

A continuación vamos a ver una pequeña condición en el caso de añadir una raíz cuadrada a $\mathbb{Q}$ para comprobar de una manera relativamente sencilla si un primo en $\mathbb{Z}$ descompone completamente (o no ramifica) en estas extensiones.

Definición 1.2.2.9 (Símbolo de Legendre). *Sea $p \in \mathbb{Z}$ un primo impar y $a \in \mathbb{Z}$ definimos el símbolo de Legendre como*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ es un residuo cuadrático} \\ -1 & \text{si } a \text{ no es residuo cuadrático} \\ 0 & \text{si } p \mid a \end{cases}$$

Observación 1.2.2.10. El símbolo de Legendre se puede definir equivalentemente sel siguiente modo

$$\left(\frac{a}{p}\right) = a^{(\frac{p-1}{2})} \bmod p$$

Proposición 1.2.2.11 (Criterio de Euler). Sea $a \in \mathbb{Z}$ libre de cuadrados y $p \in \mathbb{Z}$ un número primo tales que $\gcd(p, 2a) = 1$. Entonces

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow p \text{ descompone completemente en } \mathbb{Q}(\sqrt{a}).$$

Teoría de Ramificación

A continuación vamos a aplicar los resultados en una extensión de Galois y veremos que la actuación de su grupo de Galois nos facilita la factorización de ideales primos ya que tan sólo tendremos que estar pendientes de las clases de conjugación.

Proposición 1.2.3.1. Sea L/K una extensión de Galois y G su grupo de Galois. Entonces G actúa transitivamente en el conjunto de todos los primos $\mathfrak{P}$ de $\mathcal{O}$ que se levantan sobre $\mathfrak{p}$, es decir, son conjugados unos de otros.

Demostración. Sean $\mathfrak{P}$ y $\mathfrak{P}'$ dos ideales primos sobre $\mathfrak{p}$. Supongamos que $\mathfrak{P}' \neq \sigma\mathfrak{P}$ para todo $\sigma \in G$. Por el teorema Chino del Resto existe $x \in \mathcal{O}$ tal que

$$x \equiv 0 \bmod \mathfrak{P}' \quad \text{y} \quad x \equiv 1 \bmod \sigma\mathfrak{P} \ \forall \sigma \in G.$$

Entonces la norma $N_{L/K}(x) = \prod_{\sigma\in G} \sigma x \in \mathfrak{P}' \cap \mathfrak{o} = \mathfrak{p}$. Por otro lado $x \notin \sigma\mathfrak{P}$ para ningún $\sigma \in G$, así que $\sigma x \notin \mathfrak{P}$ para ningún $\sigma \in G$. Consecuentemente $\prod_{\sigma\in G} \sigma x \notin \mathfrak{P} \cap \mathfrak{o} = \mathfrak{p}$, contradicción.

Definición 1.2.3.2. *Sea L/K una extensión de Galois con grupo de Galois G. Si $\mathfrak{P}$ es un ideal de $\mathcal{O}$, entonces el subgrupo $G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$ se llama el grupo de descomposición de $\mathfrak{P}$sobre K.*

El cuerpo fijo $Z_{\mathfrak{P}} = \{x \in L \mid \sigma x = x \ \forall \sigma \in G_{\mathfrak{P}}\}$ se llama el cuerpo de descomposición de $\mathfrak{P}$ sobre K .

El grupo de descomposición nos deja entrever en cuantos ideales primos factoriza el ideal $\mathfrak{p} \subseteq \mathfrak{o}$ en $\mathcal{O}$. Si tomamos un representante de las clases que hay en $G/G_{\mathfrak{P}}$, entonces $\sigma\mathfrak{P}$ varía por los distintos primos sobre $\mathfrak{p}$, y la cantidad es $(G : G_{\mathfrak{P}})$.

Tenemos entonces los casos particulares

1. $G_{\mathfrak{P}} = 1 \Leftrightarrow Z_{\mathfrak{P}} = L \Leftrightarrow \mathfrak{p}$ descompone completamente
2. $G_{\mathfrak{P}} = G \Leftrightarrow Z_{\mathfrak{P}} = K \Leftrightarrow \mathfrak{p}$ no descompone

Lema 1.2.3.3. En una extensión de Galois los grados de inercia $f_1, \dots, f_r$ y los índices de ramificación $e_1, \dots, e_r$ de la descomposición en primos no dependen del subíndice ya que son iguales.

Demostración. Sean $\mathfrak{p} \subseteq \mathfrak{o}$ un ideal primo cuya factoización en $\mathcal{O}$ es $\mathcal{O}\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. Sea $\mathfrak{P} = \mathfrak{P}_1$ un ideal de $\mathcal{O}$ y $\sigma_i\mathfrak{P} = \mathfrak{P}_i$ para un $\sigma_i \in G = \mathrm{Gal}(L/K)$ adecuado. Entonces se induce un isomorfismo

$$\mathcal{O}/\mathfrak{P} \xrightarrow{\sigma_i} \mathcal{O}/\mathfrak{P}_i, \quad a \bmod \mathfrak{P} \to \sigma_i a \bmod \mathfrak{P}_i$$

De este modo obtenemos que $f_i = [\mathcal{O}/\mathfrak{P}_i : \mathfrak{o}/\mathfrak{p}] = [\mathcal{O}/\mathfrak{P} : \mathfrak{o}/\mathfrak{p}] = f$.

Ahora, como $\sigma_i(\mathfrak{p}\mathcal{O}) = \mathfrak{p}\mathcal{O}$, y además

$$\mathfrak{P}^v \mid \mathfrak{p}\mathcal{O} \Leftrightarrow \sigma_i(\mathfrak{P}^v) \mid \sigma_i(\mathfrak{p}\mathcal{O}) \Leftrightarrow (\sigma_i\mathfrak{P})^v \mid \mathfrak{p}\mathcal{O}$$

se deduce que la descomposición de $\mathfrak{p}$ en $\mathcal{O}$ es tal que $\mathfrak{p}\mathcal{O} = \left(\prod_{\sigma\in G/G_{\mathfrak{P}}} \sigma\mathfrak{P}\right)^e$.

Proposición 1.2.3.4. Sea L/K una extensión de Galois y sea $\mathfrak{P}_Z = \mathfrak{P} \cap Z_{\mathfrak{P}}$ el ideal primo en $Z_{\mathfrak{P}}$ bajo $\mathfrak{P}$. Entonces se tiene que

1. $\mathfrak{P}_Z$ no descompone en L, es decir, $\mathfrak{P}$ es el único ideal primo sobre $\mathfrak{P}_Z$ en L
2. $\mathfrak{P}$ tiene índice de ramificación e y grado de inercia f sobre $\mathfrak{P}_Z$
3. El índice de ramificación y el grado de inercia de $\mathfrak{P}_Z$ sobre K son ambos 1

Demostración. Puesto que $\mathrm{Gal}(L/Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$, los ideales primos sobre $Z_{\mathfrak{P}}$ son los $\sigma\mathfrak{P}$ para $\sigma \in G_{\mathfrak{P}}$ y todos estos son $\mathfrak{P}$.

Como acabamos de ver en el lema 1.2.3.3, los índices de ramificación y los grados de inercia en una extensión de Galois son independientes del divisor primo. En este caso la identidad fundamental es $n = efr$ donde $n = \#\mathrm{Gal}(L/K) = G$ y $r = (G : G_{\mathfrak{P}})$.

Vemos por tanto que $\#G_{\mathfrak{P}} = [L : Z_{\mathfrak{P}}] = ef$. Sean e' y e'' los índices de ramificación de $\mathfrak{P}$ sobre $Z_{\mathfrak{P}}$ y de $\mathfrak{P}_Z$ sobre K respectivamente. Tenemos que para un ideal primo $\mathfrak{p}\mathcal{O} = \mathfrak{P}_Z^{e''} \cdots$ en $Z_{\mathfrak{P}}$, ahora bien, $\mathfrak{P}_Z = \mathfrak{P}^{e'}$ en L, así que $\mathfrak{p} = \mathfrak{P}^{e'e''} \cdots$, es decir, $e = e'e''$. Análogamente podemos obtener la identidad $f = f'f''$ para los grados de inercia. La identidad fundamental para $\mathfrak{P}_Z$ en L es $[L : Z_{\mathfrak{P}}] = e'f'$, y de aquí $ef = e'f'$, es decir $e = e'$ y $f = f'$ y $f'' = e'' = 1$.

Proposición 1.2.3.5. Sea L/K una extensión de Galois con grupo de Galois G. Si llamamos $k(\mathfrak{P}) = \mathcal{O}/\mathfrak{P}$ y $k(\mathfrak{p}) = \mathfrak{o}/\mathfrak{p}$, entonces la extensión $k(\mathfrak{P})/k(\mathfrak{p})$ es normal y admite un homomorfismo sobreyectivo.

$$G_{\mathfrak{P}} \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$$

Demostración. El grado de inercia de $\mathfrak{P}_Z$ sobre K es 1 por la proposición 1.2.3.4 y tiene el mismo cuerpo cociente, $k(\mathfrak{p})$, que K respecto a $\mathfrak{p}$. Así que vamos a asumir que $K = Z_{\mathfrak{P}}$ y que $G_{\mathfrak{P}} = G$. Sea $\theta \in \mathcal{O}$ un representante de $\overline{\theta} \in k(\mathfrak{p})$ y, $f(x)$ y $\overline{g}(x)$ polinomios mínimos de θ y $\overline{\theta}$ respectivamente. Entonces $\overline{\theta} \equiv \theta \bmod \mathfrak{P}$ es un cero del polinomio $\overline{f}(x) \equiv f(x) \bmod \mathfrak{p}$, se da que $\overline{g}(x)$ divide a $\overline{f}(x)$. Al ser L/K una extensión normal, $f(x)$ se descompone en factores lineales, lo mismo ocurre con $\overline{f}(x)$ y consecuentemente con $\overline{g}(x)$. Es decir, $k(\mathfrak{P})/k(\mathfrak{p})$ es una extensión normal.

Sea $\overline{\theta}$ un elemento primitivo de la subextensión separable maximal de $k(\mathfrak{P})/k(\mathfrak{p})$ y $\overline{\sigma} \in \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) = \mathrm{Gal}(k(\mathfrak{p})(\overline{\theta})/k(\mathfrak{p}))$. Entonces $\overline{\sigma}\overline{\theta}$ es una raíz de $\overline{g}(x)$, y por tanto de $\overline{f}(x)$, así que existe una raíz $\theta' \equiv \overline{\sigma}\overline{\theta} \bmod \mathfrak{P}$ que es conjugada de θ para

algún $\sigma \in G$, $\theta' = \sigma\theta$. Como $\sigma\theta \equiv \overline{\sigma}\overline{\theta} \bmod \mathfrak{P}$, el automorfismo σ se lleva por el homomorfismo en cuestión a $\overline{\sigma}$, lo que hace que sea sobreyectivo.

Definición 1.2.3.6. *En las condiciones anteriores, se llama grupo de inercia de $\mathfrak{P}$ sobre K a $I_{\mathfrak{P}} \subseteq G_{\mathfrak{P}}$, el kernel del homomorfismo $G_{\mathfrak{P}} \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$. Se define el cuerpo de inercia de $\mathfrak{P}$ sobre K como $T_{\mathfrak{P}} = \{x \in L \mid \sigma x = x \ \forall \sigma \in I_{\mathfrak{P}}\}$, al cuerpo fijo por $I_{\mathfrak{P}}$.*

Corolario 1.2.3.7. La extensión $T_{\mathfrak{P}}/Z_{\mathfrak{P}}$ es normal y se tiene que

$$\mathrm{Gal}(T_{\mathfrak{P}}/Z_{\mathfrak{P}}) \cong \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})), \quad \mathrm{Gal}(L/T_{\mathfrak{P}}) = I_{\mathfrak{P}}.$$

Si la extensión de cuerpos $k(\mathfrak{P})/k(\mathfrak{p})$ es separable, entonces

$$\#I_{\mathfrak{P}} = [L : T_{\mathfrak{P}}] = e, \quad (G_{\mathfrak{P}} : I_{\mathfrak{P}}) = [T_{\mathfrak{P}} : Z_{\mathfrak{P}}] = f$$

y además, para un ideal $\mathfrak{P}_T$ en $T_{\mathfrak{P}}$ debajo de $\mathfrak{P}$

1. El índice de ramificación de $\mathfrak{P}$ sobre $\mathfrak{P}_T$ es e y el grado de inercia 1
2. El índice de ramificación de $\mathfrak{P}_T$ sobre $\mathfrak{P}_Z$ es 1 y el grado de inercia f

Demostración. *La prueba puede encontrarse en [4, Página 57]*

Definición 1.2.3.8 (Elemento de Frobenius). *Si L/K es una extensión de Galois, y $\mathfrak{P}$ es un ideal primo que no ramifica en L/K, entonces existe un único automorfismo $Frob_{\mathfrak{P}} \in \mathrm{Gal}(L/K)$, llamado automorfismo de Frobenius, tal que*

$$\sigma_{\mathfrak{P}}(x) = x^q \bmod \mathfrak{P} \ \forall x \in \mathcal{O}, \quad q = \#k(\mathfrak{p}).$$

Diremos que $\sigma_{\mathfrak{P}}$ pertenece a la clase de conjugación del elemento de Frobenius, que reúne a los automorfismos de los conjugados de $\mathfrak{P}$.

Observación 1.2.3.9. Si $L/\mathbb{Q}$ es una extensión de Galois, $p \in \mathbb{Q}$ es un número primo que no ramifica en L, y $\mathfrak{p}$ es un ideal primo en O_L por encima de p, entonces tenemos que la acción por el elemento de Frobenius es

$$\mathrm{Frob}_p(x) = x^p \bmod \mathfrak{p}, \ \forall x \in \mathcal{O}_L.$$

Con esta última observación es con la que vamos a trabajar de aquí en adelante. Nos interesa el estudio de los elementos de Frobenius para los números primos en $\mathbb{Z}$, es donde encontraremos los resultados más interesantes y con los que estamos más habituados a trabajar.

2 | Identificación del Frobenius

> " *Though you can't see it, there's a little country fair down that road and uh, over the hill.*
>
> *I don't see any road.*
>
> *What? No road? Just wants a bit of somethin' here, and a bit of somethin' there. There. A country road suitable for travel and high adventure.* "
>
> Bert, Michael Banks
>
> ——Mary Poppins (1964)

Ahora que contamos con las herramientas necesarias podemos comenzar con el tema principal de este estudio, la identificación de los elementos de Frobenius dada por los hermanos Tim y Vladimir Dokchitser[2].

Nos hará falta construir los polinomios Γ_C que mencionamos al principio tales que

$$\Gamma_C\left(Tr_{\frac{\mathbb{F}_q[x]}{f_a(x)}/\mathbb{F}_q}(h(x)x^q)\right) = 0 \bmod \mathfrak{p} \Leftrightarrow \mathrm{Frob}_{\mathfrak{P}} \in C$$

Veremos que $Tr_{\frac{\mathbb{F}_q[x]}{f_a(x)}/\mathbb{F}_q}(h(x)x^p)$ se comporta como la clase de un elemento íntegro que es raíz del polinomio Γ_C al tomar módulo por $\mathfrak{P}$, por eso se debe anular, tal y como se ha visto en la demostración de la proposición 1.2.3.5. La traza que estamos considerando podemos mirarla como la traza de la matriz vista en la demostración de la proposición 1.1.3.3 tras la operación $h(x)x^q$ y módulo q.

Dependiendo que para qué clase de conjugación resulte ser la traza un raíz podremos saber con qué clase coincide el elemento de Frobenius.

2.1 Acciones de Grupo

Isomorfismos entre Extensiones

Vamos a considerar un polinomio $f \in K[x]$ y sus raíces $[a_1, \dots, a_n] = a$. La extensión L/K por dicho polinomio con grupo de Galois $G_a < S_n$ puede ser alcanzada por distintos caminos según se ordenen las raíces. Si $[b_1, \dots, b_n] = b$ son también raíces de f, nuestro objetivo será encontrar una biyección entre a y b, para ello necesitamos de un isomorfismo entre $K(a)$ y $K(b)$.

Definición 2.1.1.1. *Sea $F \in K[x_1, \dots, x_n]$. Definimos la aplicación de evaluación $S_n \to K(a)$ como*

$$e_a^F(\sigma) = F([a_1, \dots, a_n]^\sigma) = F(\sigma^{-1}(a_1), \dots, \sigma^{-1}(a_n)).$$

Definición 2.1.1.2. *Sea X un conjunto, $x \in X$ uno de sus elementos y G un grupo de permutaciones que actúa sobre X, se define el estabilizador de x como $G_x = \{g \in G \mid g(x) = x\}$.*

Sea T un subgrupo de S_n. Un elemento $F \in K[x_1, \dots, x_n]$ se dice $T-$invariante si su estabilizador es precisamente T, es decir,

$$\tau(F(x_1, \dots, x_n)) = F(\tau(x_1), \dots, \tau(x_n)) = F(x_1, \dots, x_n)\ \forall \tau \in T.$$

Lema 2.1.1.3. Sean $T < S_n$ y $F \in K[x_1, \dots, x_n]$ un $T-$invariante $\sigma, \tau \in S_n$. Entonces

1. $e_{a^\tau}^F(\sigma) = e_a^F(\sigma\tau)$
2. $g(e_a^F(\sigma)) = e_a^F(\sigma g^{-1})$ para $g \in G_a$
3. La aplicación $e_a^F : S_n \to K(a)$ es constante para la clase a derecha $T\sigma$

Demostración.

1. Sea un $\tau \in S_n$

$$e_{a^\tau}^F(\sigma) = F((a^\tau)^\sigma) = F(a^{\sigma\tau}) = e_a^F(\sigma\tau)$$

2. Tomemos $g \in G_a$

$$\begin{aligned} g(e_a^F(\sigma)) &= g(F([a_1, \dots, a_n]^\sigma)) = F([g(a_1), \dots, g(a_n)]^\sigma) \\ &= F(([a_1, \dots, a_n]^{g^{-1}})^\sigma) = e_a^F(\sigma g^{-1}) \end{aligned}$$

3. Para un $\tau \in T$

$$\begin{aligned} e_a^F(\tau\sigma) &= F([a_1, \dots, a_n]^{\tau\sigma}) = F(([a_1, \dots, a_n]^{\sigma})^{\tau}) \\ &= F^{\tau^{-1}}([a_1, \dots, a_n]^{\sigma}) = F([a_1, \dots, a_n]^{\sigma}) = e_a^F(\sigma) \end{aligned}$$

Definición 2.1.1.4. *Para una clase de conjugación $D = T\sigma_0 G_a$ en S_n y un polinomio $F \in K[x_1, \dots, x_n]$, definimos el polinomio mínimo correspondiente*

$$\Gamma^F_{a,\sigma_0} = \Gamma^F_{a,D}(X) = \prod_{\sigma \in T\backslash D} (X - e_a^F(\sigma)) \in K[X].$$

Donde $T\backslash D$ denota al conjunto cociente.

Observación 2.1.1.5. Vemos por el lema 2.1.1.3(2.) que G_a permuta únicamente los factores lineales, por lo que $\Gamma^F_{a,D}$ es producto de irreducibles en $K[X]$. Además, si la aplicación $e_a^F : T\backslash S_n \to K(a)$ es inyectiva, entonces $\Gamma^F_{a,D}(X)$ es irreducible y polinomio mínimo de $e_a^F(\sigma_0)$.

Proposición 2.1.1.6. Sean a, b distintas ordenaciones de las raíces de $f(x) \in K[x]$ en dos cuerpos de descomposición de f, y sea $\phi : K(a) \to K(b)$ un isomorfismo. Si $e_a^F : T\backslash S_n \to K(a)$ es una aplicación inyectiva, entonces para toda clase de conjugación $D \in T\backslash S_n/G_a$,

$$\Gamma^F_{a,D}(F(b)) = 0 \Leftrightarrow b = [\phi(a_1), \dots, \phi(a_n)]^{\sigma}, \text{ para algún } \sigma \in D.$$

Demostración. Tenemos que $\Gamma^F_{a,D}(F(b)) = 0$ si y sólo si $F(b) = \phi(e_a^F(\sigma))$ para algún $\sigma \in D$ como se puede ver por la definición anterior.

$$\begin{aligned} \Gamma^F_{a,D}(F(b)) = 0 &\Leftrightarrow F(b) = \phi(e_a^F(\sigma)), \text{ para algún } \sigma \in D \\ &\Leftrightarrow F(\phi^{-1}(b)) = e_a^F(\sigma) = F(a^{\sigma}) \\ &\Leftrightarrow \phi^{-1}(b) = (a^{\sigma})^{\tau} = a^{\tau\sigma}, \text{ para algún } \tau \in T \\ &\Leftrightarrow b = \phi(a)^{\sigma'}, \text{ para algún } \sigma' \in D \end{aligned}$$

Teorema 2.1.1.7. *Sea $F \in K[x_1, \dots, x_n]$ un G_a-invariante, y supongamos que la evaluación $e_a^F : G_a\backslash S_n \to K(a)$ es inyectiva. Si $F(b) = F(a) \in K$, entonces la aplicación $a_i \to b_i$ define un isomorfismo $K(a) \to K(b)$.*

Demostración. Utilizando la proposición anterior, si tomamos $T = G_a$ y como D a la clase principal $G_a e G_a$, siendo e el elemento neutro, se tiene que $\Gamma^F_{a,D}(X) = X - F(a)$ y por tanto $\Gamma^F_{a,D}(F(b)) = 0$. De aquí $b = \phi(a)^{\sigma}$ para algún $\sigma \in G_a$ y ϕ algún isomorfismo $K(a) \to K(b)$. Entonces $\phi \circ \sigma$ es el isomorfismo que buscamos.

Observación 2.1.1.8. La inyectividad se pide para asegurar que no hay más repeticiones de las que debería. Para un F que sea G_a-invariante tendremos $\dfrac{|S_n|}{|G_a|}$ valores distintos para $e_A^F(\sigma)$ que se repetirán $|G_a|$ veces.

Reconocer Clases de Conjugación

Ahora que hemos visto que no nos importa en que orden tomar las raíces en nuestra extensión queremos saber como se conservan las clases de conjugación de los automorfismos que hay en G_a. De este modo podremos más adelante diferenciar las distintas clases del elemento de Frobenius.

Definición 2.1.2.1. *Sea $\xi \in S_n$. El centralizador de este elemento es Z_ξ, el conjunto de todas las permutaciones que conmutan con ξ.*

A partir de ahora fijemos un $\xi \in S_n$ y llamemos Z_ξ a su centralizador.

Definición 2.1.2.2. *Sea $\Psi \in S_n$ un conjugado de ξ, $\xi = \sigma_0 \Psi \sigma_0^{-1}$ para algún $\sigma_0 \in S_n$. Para una F que sea $T-$invariante y una ordenación a de las raíces de f, definimos el polinomio*

$$M^F_{a,\Psi}(X) = \prod_{\sigma \in (Z_\xi \cap T)\backslash Z_\xi \sigma_0} \Gamma^F_{a,\sigma}(X).$$

Está bien definido por el lema 2.1.1.3(3.) y además es independiente de la elección de σ_0.

Lo que queremos a partir de esto es, sin conocer el isomorfismo $\phi : K(a) \to K(b)$, saber si los automorfismos $\alpha \in G_a$ y $\beta \in G_b$, que actúan como Ψ y ξ respectivamente. Si se corresponden a través ϕ veremos que $M^F_{a,\Psi}(F(b)) = 0$. Más adelante en la proposición 2.2.1.1(3.) comprobaremos que es una condición necesaria y suficiente tomando $T = Z_\xi$.

Lema 2.1.2.3. Sea $\phi : K(a) \to K(b)$ un isomorfismo entre dos cuerpos de descomposición de f, y sea $\rho \in S_n$ tal que $b = \phi(a^\rho)$. Entonces $M^F_{a,\rho^{-1}\Phi\rho} = M^F_{b,\Phi}$.

Demostración. Sea $\Psi = \rho^{-1}\Phi\rho$, escogemos σ_Φ tal que $\xi = \sigma_\Phi \Phi \sigma_\Phi^{-1}$, y sea $\sigma_\Psi = \sigma_\Phi \rho$ de tal forma que

$$\sigma_\Psi \Psi \sigma_\Psi^{-1} = \sigma_\Phi \rho \Psi (\sigma_\Phi \rho)^{-1} = \sigma_\Phi \Phi \sigma_\Phi^{-1} = \xi.$$

Por definición

$$M^F_{b,\Phi}(X) = \prod_{\sigma \in (Z_\xi \cap T)\backslash Z_\xi \sigma_\Phi} \Gamma^F_{b,\sigma}(X), \quad M^F_{a,\Psi}(X) = \prod_{\sigma \in (Z_\xi \cap T)\backslash Z_\xi \sigma_\Psi} \Gamma^F_{a,\sigma}(X).$$

Afirmamos que $\Gamma^F_{a,s\sigma_\Psi} = \Gamma^F_{b,s\sigma_\Phi}$ para $s \in Z_\xi$. Primero vemos que tienen el mismo grado porque $G_b = \rho G_a \rho^{-1}$,

$$\begin{aligned} \deg(\Gamma^F_{a,s\sigma_\Psi}) &= |T\backslash T s\sigma_\Psi G_a| = |T\backslash T s\sigma_\Psi G_a \rho^{-1}| \\ &= |T\backslash T s\sigma_\Phi \rho G_a \rho^{-1}| = |T\backslash T s\sigma_\Phi G_b| \\ &= \deg(\Gamma^F_{b,s\sigma_\Phi}). \end{aligned}$$

Puesto que ambos polinomios son potencias de irreducibles, nos basta con identificar una de as raíces

$$\begin{aligned} e_a^F(s\sigma_\Psi) = e_a^F(s\sigma_\Phi\rho) = F(a^{s\sigma_\Phi\rho}) = F(\phi^{-1}(b)^{s\sigma_\Phi}) \\ = F(\phi^{-1}(b^{s\sigma_\Phi})) = \phi^{-1}(F(b^{s\sigma_\Phi})) \\ = \phi^{-1}(e_b^F(s\sigma_\Phi)). \end{aligned}$$

Corolario 2.1.2.4. La aplicación $\Psi \to M_{a,\Psi}^F$ es constante en toda clase de conjugación de ξ en G_a.

Demostración. Por el lema anterior se puede ver fácilmente que $M_{a,\Psi}^F = M_{a,g\Psi g^{-1}}^F$ para todo $g \in G_a$

Proposición 2.1.2.5. Sean a, b dos ordenaciones de las raíces del polinomio f en dos cuerpos de descomposición distintos. Sean $\Psi \in G_a$ y $\Phi \in G_b$ con el mismo tipo de ciclo que ξ. Si los polinomios $M_{a\psi}^F$ son distintos para cada clase de conjugación en G_a con tipo de ciclo que ξ, entonces existe un isomorfismo $K(a) \to K(b)$ por el que Ψ se corresponde con Φ si y sólo si $M_{a,\Psi}^F = M_{b,\Phi}^F$.

Si además los $M_{a,\psi}^F$ son coprimos dos a dos, entonces esto ocurre justamente cuando $M_{a,\Psi}^F(F(b^\sigma)) = 0$ para cualquier $\sigma \in S_n$ tal que $\sigma\Phi\sigma^{-1} = \xi$.

Demostración. Hacia derecha, si existe un isomorfismo $K(a) \to K(b)$ por el que Ψ se corresponde con Φ, nos encontramos en las condiciones del lema 2.1.2.3 que acabamos de ver.

Sea $\phi : K(a) \to K(b)$ un isomorfismo. Puesto que el polinomio $M_{b,\Phi}^F$ coincide con algún $M_{a,\psi}^F$, por el corolario 2.1.2.4 y nuestra hipótesis vemos que ψ debe caer en la clase de conjugación de Ψ. Componiendo ϕ con elementos de G_a para conjugar ψ hacia Ψ obtenemos el isomorfismo que queremos.

Con esta última proposición conseguimos despegarnos del uso de los isomorfismos que hay entre las distintas ordenaciones de las raíces que podemos considerar para, sencillamente, observar lo que ocurre con estos mismos polinomios.

2.2 Elementos de Frobenius

Polinomios Invariantes

A continuación nos disponemos a ver las propiedades de los polinomios $M^F_{a,\Psi}(X)$ de la definición 2.1.2.2. En el caso $T = Z_\xi$ queremos poder tomar de una manera cómoda el polinomio F que sea $T-$invariante y de este modo formalizar los polinomios $\Gamma_C(X)$.

Proposición 2.2.1.1. Sea $\xi \in S_n$ y sea Z_ξ su centralizador. Sea $F \in K[x_1 \dots, x_n]$ un $Z_\xi-$invariante tal que $e^F_a : Z_\xi \backslash S_n \to K(a)$ es inyectiva. Si Ψ y Ψ' son dos elementos de G_a con el mismo tipo de ciclo que ξ, entonces

1. $M^F_{a,\Psi}$ es irreducible, y es igual a $\Gamma^F_{a,\sigma}$ para cualquier $\sigma \in S_n$ tal que $\xi = \sigma\Psi\sigma^{-1}$
2. $M^F_{a,\Psi}$ tiene grado $|(\Psi)|$, siendo (Ψ) la clase de conjugación de Ψ en G_a
3. $M^F_{a,\Psi} = M^F_{a,\Psi'}$ si y sólo si Ψ y Ψ' son conjugados en G_a

Demostración.

1. Por definición se tiene que
$$M^F_{a,\Psi} = \prod_{\tau \in (Z_\xi \cap Z_{\xi})\backslash Z_\xi \sigma} \Gamma^F_{a,\tau} = \Gamma^F_{a,\sigma}.$$
Además, una vez asumida la inyectividad se tiene que es irreducible como se ha visto en la observación 2.1.1.5.

2. De nuevo por propia definición
$$\begin{aligned}\deg(\Gamma^F_{a,\sigma}) = |Z\backslash Z\sigma G_a| = \frac{|Z\sigma G_a|}{|Z|} = \frac{|\sigma^{-1}Z\sigma G_a|}{Z} \\ = \frac{|G_a|}{|G_a \cap \sigma^{-1}Z\sigma|} = \frac{|G_a|}{|G_a \cap Z_\Psi|} = |(\Psi)|.\end{aligned}$$

3. Si Ψ y Ψ' son conjugados, entonces, por el corolario 2.1.2.4, $M^F_{a,\Psi} = M^F_{a,\Psi'}$. Por otro lado, si $M^F_{a,\Psi} = M^F_{a,\Psi'}$, al ser e^F_a inyectiva, $Z\sigma G_a = Z\sigma' G_a$, de forma que $\sigma' = s\sigma g$ para algún $s \in Z$ y $g \in G_a$. Entonces
$$\Psi' = \sigma'^{-1}\xi\sigma' = (s\sigma g)^-1\xi s\sigma g = (\sigma g)^-1\xi\sigma g = g^{-1}\Psi g,$$
por lo que $[\Psi'] = [\Psi]$.

Observación 2.2.1.2. Si tomamos un $\xi \in S_n$ y definimos $F(x_1, \dots, x_n) = \sum_{j=1}^{n} h(x_j)\xi(x_j)$ para algún polinomio $h(x) \in K[X]$ con $2 \leq \deg(h) \leq n-1$, entonces puede verse que F es Z_ξ−invariante.

Definición 2.2.1.3. *Sea un polinomio $h(x) \in K[x]$ fijo tal que $2 \leq \deg(h) \leq n-1$. Definimos para cada clase de conjugación C en G_a*

$$\Gamma_C(X) = \prod_{\sigma \in C} \big(X - \sum_{j=1}^{n} h(a_j)\sigma(a_j)\big).$$

Proposición 2.2.1.4. Sea $F \in K[x_1, \dots x_n]$ como en la observación 2.2.1.2. Entonces para todo $\Psi \in G_a$,

$$M^F_{a,\Psi}(X) = \Gamma_{[\Psi]}(X).$$

Demostración. Tomemos un $\sigma \in S_n$ tal que $\sigma\Psi\sigma^{-1} = \xi$. Sean $\tau \in [\Psi]$ y $u_\tau \in S_n$ satisfaciendo $u_\tau^{-1}\xi u_\tau = \tau$. Entonces

$$e^F_a(u_\tau) = F(a^{u_\tau}) = \sum_i h(u_\tau^{-1}(a_i))u_\tau^{-1}\xi(a_i) = \sum_j h(a_j)u_\tau^{-1}\xi u_\tau(a_j) = \sum_j h(a_j)\tau(a_j).$$

Por otro lado, para $t \in Z_\xi$ y $g \in G_a$,

$$(t\sigma g)^{-1}\xi(t\sigma g) = (\sigma g)^{-1}\xi(\sigma g) = g^{-1}\Psi g.$$

Entonces para $\tau = g^{-1}\Psi g \in [\Psi]$, $\{u_\tau \in S_n \mid u_\tau^{-1}\xi u_\tau = \tau\} = Z_\xi \sigma g$.

Esta igualdad nos da una correspondencia ente $[\Psi]$ y $Z_\xi \backslash Z_\xi \sigma G_a$, por lo que

$$M^F_{a,\Psi}(X) = \Gamma^F_{a,\sigma}(X) = \prod_{u \in Z_\xi \backslash Z_\xi \sigma G_a} (X - e^F_a(u)) = \prod_{\tau \in [\Psi]} \big(X - \sum_{j=1}^{n} h(a_j)\tau(a_j)\big) = \Gamma_{[\Psi]}(X).$$

Corolario 2.2.1.5. Sean a, b ordenaciones de las raíces de f en dos cuerpos de descomposición distintos, y sean $\Psi \in G_a$ y $\Phi \in G_b$. Si los $\Gamma_C(X)$ son coprimos dos a dos para las distintas clases de conjugación de G_a, entonces hay un isomorfismo $K(a) \to K(b)$ por el que Ψ está en correspondencia con Φ si y sólo si $\Gamma_{[\Psi]}\big(\sum_j (b_j)\Phi(b_j)\big) = 0$.

Demostración. La equivalencia se sigue a raíz de la proposición 2.1.2.5 y la proposición anterior.

Observación 2.2.1.6. En general nos bastará con tomar $h(x) = x^m$ con $2 \leq m \leq n-1$.

Reconocer Elementos de Frobenius

Por fin llegamos a nuestro objetivo. Tras poner en pie todo lo necesario nos disponemos a dar un criterio para reconocer a los elementos de Frobenius. Nos basaremos también en una generalización del Criterio de Euler (Corolario 1.2.2.11) y la función traza como mencionamos anteriormente.

Lema 2.2.2.1. Sea K un cuerpo y $f(x) \in K[x]$ un polinomio con raíces $a_1, \dots, a_n \in L$ contadas con multiplicidad. Entonces para todo $H(x) \in K[x]$,

$$\sum_{j=1}^{n} H(a_j) = \mathrm{Tr}_{A/K}(H(X)),$$

Donde X es la clase de x en $A = K[x]/\langle f \rangle$.

Demostración. Sea $f(x) \in K[x]$ con raíces $a_1, \dots, a_n$ contadas con multiplicidad, entonces $f(x) = f(x)_1 \cdots f_k(x) = p_1^{d_1}(x) \cdots p_k^{d_k}(x)$ para ciertos $p_i \in K[x]$ irreducibles y mónicos. Denotamos X a la clase de x en $A = K[x]/\langle f(x) \rangle$.

El polinomio mínimo de la aplicación $T_X : A \to A : Y \to XY$ descrita en la definición 1.1.3.1 es, efectivamente, $f(x)$, ya que ninguna combinación lineal de $1, X, \dots, X^{n-1}$ se anula en A, esto lo podemos ver en la forma de Jordan del siguiente modo.

Cada $p_i(x)$ es de la forma $c_{i,0}+c_{i,1}x+\ldots+c_{i,m_i-1}x^{m_i-1}+x^{m_i}$ y podemos plantear la matriz asociada que se ha visto en la demostración de la proposición 1.1.3.3, cuya diagonal está formada por los bloques C_i repetidos d_i veces y la parte inferior es nula, donde

$$C_i = \begin{pmatrix} & & -c_{i,0} \\ 1 & & -c_{i,1} \\ & \ddots & \vdots \\ & 1 & -c_{i,m_i-1} \end{pmatrix}.$$

La matriz resultante tiene como autovalores los a_j que son raíces de $f(x)$ contadas con multiplicidad, de este modo

$$\sum_{j=1}^{n} a_j = \mathrm{Tr}_{A/K}(X).$$

Este mismo procedimiento se lo podemos aplicar al elemento $H(X)$, y trivialmente se sigue que

$$\sum_{j=1}^{n} H(a_j) = \mathrm{Tr}_{A/K}(H(X)).$$

Proposición 2.2.2.2. Sea $q = p^r$. Sea $f(x) \in \mathbb{F}_q[x]$ un polinomio con raíces $a_1, \dots, a_n \in \mathbb{F}_q(a)$ contadas con multiplicidad, y sea $\phi = \mathrm{Frob}_p \in \mathrm{Gal}(\mathbb{F}_q(a)/\mathbb{F}_q)$. Para todo polinomio $h(x) \in \mathbb{F}_q[x]$,

$$\sum_{j=1}^{n} h(a_j)\phi(a_j) = \mathrm{Tr}_{A/\mathbb{F}_q}(h(X)X^q)$$

, donde X es la clase de x en el álgebra $A = \mathbb{F}_q[x]/\langle f \rangle$.

Demostración. Es una consecuencia inmediata del lema anterior tomando $H(x) = h(x)x^q$.

Teorema 2.2.2.3 (Criterio de Euler General). *Sea K un cuerpo de números algebraicos y sea $f(x) \in K(x)$ un polinomio separable con raíces $a_1, \dots, a_n \in L$ con grupo de Galois G. Si fijamos $h(x) \in K[x]$, y para cada clase de conjugación C de G,*

$$\Gamma_C(X) = \prod_{\sigma \in C} \Big(X - \sum_{j=1}^{n} h(a_j)\sigma(a_j)\Big).$$

1. *Los polinomios $\Gamma_C(X)$ tienen coeficientes en K*

2. *Sea $\mathfrak{p}$ un primo de K con cuerpo residual $\mathbb{F}_q$, y C una clase de conjugación de G. Si $\mathfrak{p}$ no divide a los denominadores de los coeficientes de f y h, al coeficiente líder de f, ni a las resultantes $\mathrm{Res}(\Gamma_C, \Gamma_{C'})$ para $C \neq C'$, entonces los coeficientes de $\Gamma_C(X)$ son íntegros en el localizado de $\mathfrak{p}$, y*

$$Frob_{\mathfrak{p}} \in C \Leftrightarrow \Gamma_C\Big(\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{\langle f \rangle}/\mathbb{F}_q}(h(x)^q)\Big) = 0 \bmod \mathfrak{p}.$$

Demostración.

1. Por la proposición 2.2.1.4 vemos que $M^F_{a,\Psi} = \Gamma_{[\Psi]}$ y éstos tienen coeficientes en K por definición

2. Podemos ver fácilmente que las condiciones sobre $\mathfrak{p}$ implican que los $\Gamma_C(X)$ son íntegros.

   Ahora hacia derecha, si $\mathrm{Frob}_{\mathfrak{p}} \in C$, entonces $\sum_{j=1}^{n} h(a_j)\mathrm{Frob}_{\mathfrak{p}}(a_j)$ es una raíz de $\Gamma_C(X)$ por definición, y se reduce módulo $\mathfrak{p}$ a $\mathrm{Tr}_{\mathbb{F}_q[x]/\langle f \rangle/\mathbb{F}_q}(h(x)x^q)$ por la proposición 2.2.2.2.

   En la implicación a izquierda el polinomio Γ_C se distingue del resto por cualquiera de sus raíces módulo $\mathfrak{p}$, ya que estamos tomando $\mathfrak{p} \nmid \mathrm{Res}(\Gamma_c, \Gamma_{C'})$ para $C \neq C'$

Observación 2.2.2.4. La condición de que $\mathfrak{p}$ no divida a la resultante $\mathrm{Res}(\Gamma_C, \Gamma_{C'})$ excluye a los primos que ramifican en el cuerpo de descomposición de f sobre K.

Observación 2.2.2.5. Con el criterio de Euler estándar buscamos conocer si un elemento tiene raíz cuadrada módulo p. Esto lo podemos extender también a comprobar si $x^3 - a$ tiene raíz módulo $p \equiv 1 \bmod 3$ mirando si $a^{\frac{p-1}{3}} \equiv 1 \bmod 3$.

Esto puede reformularse con las matrices vistas en la demostración de la proposición 1.1.3.3. Sea $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$, la traza del Criterio de Euler General puede interpretarse como

$$\left(\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{\langle f\rangle}/\mathbb{F}_q}(x^d)\right) = \mathrm{Tr}\begin{pmatrix} & & & -c_0 \\ 1 & & & -c_1 \\ & \ddots & & \vdots \\ & & 1 & -c_{n-1} \end{pmatrix}^d \bmod q.$$

3 Ejemplos

> " *All right, I'll do it myself.*
>
> *Do what?*
>
> *Bit of magic. It's easy. Let's see. You think. You wink. You do a double blink. You close your eyes and jump.* "
>
> Bert, Mary Poppins
>
> ——Mary Poppins (1964)

A continuación expondremos algunos ejemplos que aparecen en el artículo de los hermanos Tim y Vladimir Dokchitser[2] y otros que hemos hecho por nuestra mano aplicando el método que se ha expuesto en el teorema 2.2.2.3.

3.1 Grupo Cíclico

El ejemplo se encuentra en [2, páginas 17∼18].

Pongámonos en $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, y sea $\zeta = \zeta_m$ para algún primo $m > 2$. El polinomio mínimo de ζ es

$$f(x) = x^{m-1} + \cdots + x + 1 \quad \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/\mathbb{Z}m).$$

Los automorfismos del grupo de Galois se aplican de forma que $\sigma_i : \zeta \to \zeta^i$ para $1 \leq i < m$, las clases $[\sigma_i]$ son unitarias. Tomando $h(x) = x^2$

$$\Gamma_{[\sigma_i]}(X) = X - \sum_{j=1}^{m-1} (\zeta^j)^2 \sigma_i(\zeta^j) = X - \sum_{j=1}^{m-1} \zeta^{j(2+i)} = \begin{cases} X - (-1) & \text{si } i \neq m-2 \\ X - (m-1) & \text{si } i = m-2 \end{cases}$$

Para un primo $p \in \mathbb{Q}$,

$$\mathrm{Tr}_{\frac{\mathbb{F}_p[x]}{\langle f \rangle}/\mathbb{F}_p}(X^{p+2}) = \mathrm{Tr}_{\frac{\mathbb{Z}[x]}{\langle f \rangle}/\mathbb{Z}}(X^{p+2}) \bmod p = \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^{p+2}) = \begin{cases} -1 & \bmod p, \text{ si } m \nmid p+2 \\ m-1 & \bmod p, \text{ si } m \mid p+2 \end{cases}$$

Por el teorema 2.2.2.3(2.) vemos que para todo primo $p \neq m$ se tiene

$$\mathrm{Frob}_p = \sigma_{m-2} \Leftrightarrow p \equiv -2 \bmod m.$$

Observamos que nuestra elección del polinomio $h(x)$ no es la mejor posible, ya que tan sólo logramos identificar una de las clases, sin embargo simplifica mucho los cálculos y, además, podemos ver que variando la potencia del polinomio entre 2 y $m-1$ somos capaces de ver una condición similar para el resto.

3.2 Extensiones de Kummer

Este ejemplo se puede encontrar en [2, página 17].

Sea $\zeta = \zeta_n$ una raíz primitiva $n-$ésima de la unidad que está en $K = \mathbb{Q}(\zeta)$ y sea $L = K(\sqrt[n]{m})$ una extensión de Kummer de grado n. El polinomio mínimo de $\zeta^j \sqrt[n]{m}$, $1 \leq j \leq n$ es

$$f(x) = x^n - m$$

Consideramos el grupo $\mathrm{Gal}(K(\sqrt[n]{m})/K)$. los automorfismos del grupo de Galois se aplican de manera tal que

$$\sigma_i : \sqrt[n]{m} \to \zeta^i \sqrt[n]{m} \quad \text{para } 1 \leq i \leq n.$$

Si tomamos $h(x) = x^{n-1}$, entonces los polinomios Γ_C son

$$\Gamma_{[\sigma_i]} = X - \sum_{j=1}^{n} h(\zeta^j \sqrt[n]{m})\sigma_i(\zeta^j \sqrt[n]{m}) = X - m \sum_{j=1}^{n} \zeta^{j(n-1)} \zeta^{j+i} = X - nm\zeta^i.$$

Para un primo $\mathfrak{p}$ con cuerpo residual $\mathbb{F}_q$ tenemos que

$$\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{\langle f \rangle}/\mathbb{F}_q}(h(X)X^q) = \mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{\langle f \rangle}/\mathbb{F}_q}(X^{n+q-1}) = \mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{\langle f \rangle}/\mathbb{F}_q}(m^{(q-1)/n+1}) = (nm)m^{(q-1)/n},$$

entonces vemos que para un $\mathfrak{p} \nmid nm$

$$\mathrm{Frob}_{\mathfrak{p}} = \sigma_i \Leftrightarrow m^{(q-1)/n} \equiv \zeta^i \bmod \mathfrak{p}.$$

3.3 Grupo Diédrico D_8

Consideremos el polinomio $f(x) = x^4 - m$ en $\mathbb{Q}[x]$, donde $m \in \mathbb{N}$ no presenta en su descomposición potencias de grado mayor a 3.

Sea $L = \mathbb{Q}(i, \sqrt[4]{m}) = \mathbb{Q}[x]/\langle f(x)\rangle$ con grupo de Galois $\mathrm{Gal}(L/\mathbb{Q}) = D_8$, vemos que el grupo de los automorfismos está generado por los siguientes

$$\tau : i \to -i, \quad \sigma : \sqrt[4]{m} \to i\sqrt[4]{m}$$

Las clases de conjugación son $[e]$, $[\tau]$, $[\sigma]$, $[\sigma^2]$ y $[\tau\sigma]$. De nuevo, para simplificar los cálculos, vamos tomar $h(x) = x^3/m$, entonces los polinomios Γ_C son

$$\begin{aligned}
\Gamma_{[e]} =& X - \frac{1}{m}\sum_{j=1}^{4}(i^j\sqrt[4]{m})^3(i^j\sqrt[4]{m}) = X - \sum_{j=1}^{4} i^{4j} = X - 4,\\
\Gamma_{[\sigma^2]} =& X - \frac{1}{m}\sum_{j=1}^{4}(i^j\sqrt[4]{m})^3\sigma^2(i^j\sqrt[4]{m}) = X - (i^{4+2} + i^{8+2} + i^{12+2} + i^{16+2}) = X + 4,\\
\Gamma_{[\sigma]} =& \prod_{\gamma\in[\sigma]}\left(X - \frac{1}{m}\sum_{j=1}^{4}(i^j\sqrt[4]{m})^3\gamma(i^j\sqrt[4]{m})\right) =\\
&= \left(X - (i^{4+1} + i^{8+1} + i^{12+1} + i^{16+1})\right)\left(X - (i^{4+3} + i^{8+3} + i^{12+3} + i^{16+3})\right) = X^2 + 16,\\
\Gamma_{[\tau]} =& \prod_{\gamma\in[\tau]}\left(X - \frac{1}{m}\sum_{j=1}^{4}(i^j\sqrt[4]{m})^3\gamma(i^j\sqrt[4]{m})\right) =\\
&= \left(X - (i^{3+3} + i^{6+6} + i^{9+9} + i^{12+12})\right)\left(X - (i^{3+9} + i^{6+12} + i^{9+15} + i^{12+18})\right) = X^2,\\
\Gamma_{[\tau\sigma]} =& \prod_{\gamma\in[\tau\sigma]}\left(X - \frac{1}{m}\sum_{j=1}^{4}(i^j\sqrt[4]{m})^3\gamma(i^j\sqrt[4]{m})\right) =\\
&= \left(X - (i^{3+6} + i^{6+9} + i^{9+12} + i^{12+15})\right)\left(X - (i^{3+4} + i^{6+7} + i^{9+10} + i^{12+13})\right) = X^2.
\end{aligned}$$

Entonces, para un primo $\mathfrak{p}$ con cuerpo residual $\mathbb{F}_q$ y que no divida a m ni a 8, se da que

$$\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{\langle f(x)\rangle}/\mathbb{F}_q}(h(X)X^q) = \mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{\langle f(x)\rangle}/\mathbb{F}_q}(X^{q+3}/m) = \mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{\langle f(x)\rangle}/\mathbb{F}_q}(m^{(q-1)}) = \begin{cases} m^{\frac{q-1}{4}}, \text{ si } q \equiv 1 \bmod 4\\ 0, \text{ en caso contrario.}\end{cases}$$

Con esto se puede ver que, si $q \equiv 1 \bmod 4$, entonces para $q = 4p + 1$,

$$\begin{aligned}
\mathrm{Frob}_{\mathfrak{p}} \in [e] &\Leftrightarrow m^p \equiv 4 \bmod \mathfrak{p}\\
\mathrm{Frob}_{\mathfrak{p}} \in [\sigma^2] &\Leftrightarrow m^p \equiv -4 \bmod \mathfrak{p}\\
\mathrm{Frob}_{\mathfrak{p}} \in [\sigma] &\Leftrightarrow m^p \equiv \pm 4i \bmod \mathfrak{p}.
\end{aligned}$$

3.4 Polinomio Cúbico

El ejemplo puede verse también en [2, página 21].

Sean K un cuerpo de números algebraico. Sean $a, b \in K$ tales que el polinomio $f(x) = x^3 + bx + c$ es irreducible sobre $K[x]$, con raíces α_1, α_2 y α_3, y sea $L = K(\alpha_1, \alpha_2, \alpha_3)$ el cuerpo de descomposició de $f(x)$, el grupo de Galois $\mathrm{Gal}(L/K) = S_3$ con clases de conjugación $[e]$, $[(12)]$ y $[(123)]$.

Expresamos los coeficientes de $f(x)$ en función de sus raíces como $c = -\alpha_1\alpha_2\alpha_3$, $b = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3$ y $0 = \alpha_1 + \alpha_2\alpha_3$, y tomamos $h(x) = x$. Entonces los polinomios Γ_C son los siguientes

$$\begin{aligned}
\Gamma_{[e]} =& X - (\alpha_1^2 + \alpha_2^2 + \alpha_3^2) = X - (\alpha_1 + \alpha_2 + \alpha_3)^2 + 2(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3) = X + 2b,\\
\Gamma_{[(12)]} =& (X - (\alpha_1\alpha_2 + \alpha_2\alpha_1 + \alpha_3^2))(X - (\alpha_1^2 + \alpha_2\alpha_3 + \alpha_3\alpha_2))(X - (\alpha_1\alpha_3 + \alpha_2^2 + \alpha_3\alpha_1)) =\\
=& X^3 - 3b^2X - 2b^3 - 27c^2,\\
\Gamma_{[(123)]} =& (X - (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1))(X - (\alpha_1\alpha_3 + \alpha_2\alpha_1 + \alpha_3\alpha_2)) = (X - b)^2.
\end{aligned}$$

Si tomamos un primo $\mathfrak{p} \in K$ con cuerpo residual $\mathbb{F}_q$ que no divida a $3b(4b^3 + 27c^2)$, la traza queda

$$T = \mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{\langle f(x)\rangle}/\mathbb{F}_q}(h(X)X^q) = \mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{\langle f(x)\rangle}/\mathbb{F}_q}(X^{q+1}) = \mathrm{Tr}\begin{pmatrix} 0 & 0 & -c \\ 1 & 0 & -b \\ 0 & 1 & 0 \end{pmatrix}^{q+1} \mod \mathfrak{p}$$

De aquí obtenemos las equivalencias siguientes

$$\begin{aligned}
&\mathrm{Frob}_{\mathfrak{p}} \in [e] \Leftrightarrow T \equiv -2b \bmod \mathfrak{p}\\
&\mathrm{Frob}_{\mathfrak{p}} \in [(123)] \Leftrightarrow T \equiv b \bmod \mathfrak{p}\\
&\mathrm{Frob}_{\mathfrak{p}} \in [(12)] \Leftrightarrow T^3 - 3b^2T - 2b^3 - 27c^2 \equiv 0 \bmod \mathfrak{p}.
\end{aligned}$$

3.5 Projective Special Linear Group (2,3)

Vamos a partir desde el grupo $\mathrm{PLS}(2,3) \cong A_4$. Buscamos un polinomio paramétrico cuyo grupo de Galois sobre $\mathbb{Q}$ sea $\mathrm{PLS}(2,3)$ para casi todos los valores.

Trabajaremos con el polinomio $f_a(x) = 3x^4 - 4x^3 + 1 + 3a^2$ que se puede encontrar en [6, Ch.4, párrafo 5, página 44] con la ayuda de la herramienta *SAGE* para llevar a cabo, de un modo más sencillo, los cálculos durante el proceso.

Lo primero es comprobar qué valores de a nos son válidos, es decir, comprobar su irreducibilidad. Analíticamente es fácil ver que, salvo para $a = 0$, todos los $f_a(x)$ tienen 4 raíces complejas, y por lo tanto son irreducibles en $\mathbb{Q}[x]$.

Al igual que en el ejemplo anterior sustituiremos las expresiones simétricas en función de las raíces por los coeficientes de $f_a(x)$ siempre que se pueda.

Fijamos el valor $a = 1$ y llamamos $f(x) = \frac{f_1(x)}{3} = x^4 - \frac{4}{3}x^3 + \frac{4}{3}$. Las raíces α_1 y α_3 son conjugadas de α_2 y α_4 respectivamente. Además consideramos las relaciones

$$\prod_j \alpha_j = \frac{4}{3}, \quad \sum_{i<j<k} \alpha_i\alpha_j\alpha_k = 0, \quad \sum_{i<j} \alpha_i\alpha_j = 0, \quad \sum_i \alpha_i = \frac{4}{3}.$$

Las clases de conjugación de $\mathrm{PLS}(2,3) \cong A_4$ son $[e]$, $[(12)(34)]$, $[(123)]$ y $[(124)]$. Procedemos entonces al cálculo de los polinomios Γ_C tomando $h(x) = x^2$,

$$\begin{aligned}
\Gamma_{[e]} &= \prod_{\sigma\in[e]} \left(X - \sum_{j=1}^{4} h(\alpha_j)\sigma(\alpha_j) \right) = X - \frac{64}{27} \\
\Gamma_{[(12)(34)]} &= \prod_{\sigma\in[(12)(34)]} \left(X - \sum_{j=1}^{4} h(\alpha_j)\sigma(\alpha_j) \right) = X^3 - \frac{832}{27}X - \frac{13312}{729} \\
\Gamma_{[(123)]} &= \prod_{\sigma\in[(123)]} \left(X - \sum_{j=1}^{4} h(\alpha_j)\sigma(\alpha_j) \right) \\
&= X^4 - \frac{64}{27}X^3 - \frac{2704}{27}X^2 + \frac{7728414251067}{56430428576}X + \frac{75904192}{19683} \\
\Gamma_{[(124)]} &= \prod_{\sigma\in[(124)]} \left(X - \sum_{j=1}^{4} h(\alpha_j)\sigma(\alpha_j) \right) \\
&= X^4 - \frac{64}{27}X^3 + \frac{137014274378515}{773282903056}X^2 - \frac{15490546004027}{80790751180}X + \frac{270937982197}{55017487}
\end{aligned}$$

Sea ahora un primo $\mathfrak{p}$ con cuerpo residual $\mathbb{F}_p$ que no divida a 3, al discriminante de f, ni al mínimo común múltiplo de las resultantes de los Γ_C dos a dos. Definimos la traza de $h(X)X^p$ como

$$\mathrm{Tr}_{\frac{\mathbb{F}_p[x]}{\langle f(x)\rangle}/\mathbb{F}_q}(h(X)X^q) = \mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{\langle f(x)\rangle}/\mathbb{F}_q}(X^{q+2}) = \mathrm{Tr}\begin{pmatrix} 0 & 0 & 0 & -\frac{4}{3} \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \frac{4}{3} \end{pmatrix}^{q+2} \mod \mathfrak{p}$$

De este modo obtenemos la equivalencia $\mathrm{Frob}_{\mathfrak{p}} \in C \Leftrightarrow \Gamma_C(\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{\langle f(x)\rangle}/\mathbb{F}_q}(X^{q+2})) \equiv 0 \bmod \mathfrak{p}$.
Vamos a ilustrarlo con una tabla

p	5	7	23	31	47	53	59	71	73
$\mathrm{Frob}_{\mathfrak{p}}$	(123)	e	(12)(34)	e	(123)	(12)(34)	(124)	(123)	(124)
p	83	101	103	107	113	137	139	149	157
$\mathrm{Frob}_{\mathfrak{p}}$	e	(12)(34)	(12)(34)	e	(12)(34)	(12)(34)	e	e	e
$\vdots$									$\vdots$

Aquí vemos una pequeña muestra de como se distribuye el elemento de Frobenius por las distintas clases de equivalencia de PSL(2, 3) al hacer variar un primo p.

4 Resultados de Interés

> " *Speaking of names, I know a man with a wooden leg named Smith.*
> *What's the name of his other leg?* "
>
> Bert, Uncle Albert
> ——Mary Poppins (1964)

Por último comentaremos un par de resultados que han captado nuestra atención a la hora de estudiar el elemento de Frobenius, como es la factorización de un polinomio al tomar módulo, o el Teorema de Densidad de Tchevotarev.

La curiosidad por estas materias surgió al leer la tesis de *Van Bommel*[7] y el paper de *Sun Woo Park*[5]. en los que buscan ciertas aplicaciones y propiedades del elemento de Frobenius.

4.1 Factores de un Polinomio en Módulo

El elemento de Frobenius está estrechamente ligado a la forma que tiene un polinomio al tomar módulo.

Sea $f(x)$ un polinomio con coeficientes en el cuerpo base $\mathbb{Q}$, consideramos el cuerpo de descomposición de $f(x)$, L. Si p es un primo en $\mathbb{Q}$ y $\mathfrak{p}$ un primo en L por encima de p, el elemento de Frobenius actúa de forma que $\mathrm{Frob}_{\mathfrak{p}} : x \to x^p \bmod \mathfrak{p}$ como se ha visto en la observación 1.2.3.9.

El elemento $\mathrm{Frob}_{\mathfrak{p}}$ puede verse también como una permutación de las raíces de $f(x) \bmod p$ en la extensión $(\mathcal{O}/\mathfrak{p})/(\mathcal{o}/p)$, visto en la demostración de la proposición 1.2.3.5.

Entonces, el polinomio $f(x) \bmod p$ tiene grado el orden de $\mathrm{Frob}_{\mathfrak{p}}$ y relaciona sus raíces según sus ciclos disjuntos, por lo que los factores irreducibles tienen grado la longitud de los ciclos de $\mathrm{Frob}_{\mathfrak{p}}$.

4.2 Teorema de Densidad de Tchevotarev

Una pregunta que nos surge al estudiar como varía el elemento de Frobenius al movernos entre distintos primos es la frecuencia con la que ocurre un cierto elemento.

Sea $\mathcal{P} \subset \mathbb{Z}$ el conjunto de los números primos, definimos las siguientes densidades para los subconjuntos de $\mathcal{P}$.

Definición 4.2.0.1 (Densidad Natural). *Sea $A \subset \mathcal{P}$ un subconjunto, supongamos que el siguiente límite existe*

$$\mathrm{D}(A) := \lim_{x\to\infty} \frac{|\{p \in A : p \leq x\}|}{|\{p \in \mathcal{P} : p \leq x\}|}.$$

Entonces se llama $\mathrm{D}(A)$ a la densidad natural de A.

Esta es una noción bastante intuitiva de densidad y que, de existir, coincide con la siguiente definición, que es un acercamiento más analítico al concepto de densidad de un conjunto.

Definición 4.2.0.2 (Densidad de Dirichlet). *Sea $A \subset \mathcal{P}$ un subconjunto, supongamos que existe el límite*

$$\delta(A) := \lim_{s\downarrow 1} \frac{\sum_{p\in A} \frac{1}{p^s}}{\sum_{p\in\mathcal{P}} \frac{1}{p^s}}$$

Entonces se llama $\delta(A)$ a la densidad de Dirichlet de A.

Teorema 4.2.0.3 (Teorema de Densidad de Tchevotarev). *Sea L/K una extensión finita de cuerpos con grupo de Galois $G = \mathrm{Gal}(L/K)$. Sea C una de las clases de conjugación de G. Entonces*

$$\mathrm{D}(\{p \in \mathcal{P} : p \text{ no ramificado}, Frob_p = C\}) = \frac{|C|}{|G|},$$

$$\delta(\{p \in \mathcal{P} : p \text{ no ramificado}, Frob_p = C\}) = \frac{|C|}{|G|}.$$

5 | Apéndice

5.1 Código de *SAGE*

> " *What did I tell ya? There's the whole world at your feet. And who gets to see it? But the birds, the stars and the chimney sweeps.* "
>
> Bert
>
> ——Mary Poppins(1964)

Este es el código que se ha elaborado y usado para el ejemplo de la sección §3.5 Projective Special Linear Group (2,3).

Comenzamos definiendo una funciones básicas que nos ayudarán en la obtención de una base de Gröbner para aplicar teoría de eliminación y sustituir las expresiones en las que aparecen las raíces por sus funciones elementales.

```
 def Anillo(n):
     x = ['x%s'%p for p in range(n)]
     y = ['y%s'%p for p in range(n)]
     variables = x+y

     Q = PolynomialRing(QQ, 2*n, variables, order='lex')
    return Q

def elementales(n,Anillo):
    X = Anillo.gens()[0:n]
```

```
    I = [0]*n
    I[n-1] = prod(X)
    for k in range(1,n):
        I[n-1-k] = sum([I[n-k] // x for x in X])/k
    return I

def base(n, Polinomios, Anillo):
    Y = Anillo.gens()[n:2*n]

    G = [0]*n
    for k in range(n):
        G[k] = Polinomios[k]-Y[k]

    G = Anillo.ideal(G).groebner_basis()
    #print 'Base de Groebner'
    #for g in G:
    #    print g, '\n'

    return G
```

Ahora pasamos a usar teoría de eliminación para obtener las expresiones que queremos, pero antes es necesario implementar el algoritmo de división de Euclides.

```
def div( f, g, ring ):
    m = len(g)
    p, r, q = f, 0,  [0 for _ in range(m)]

    count = 0
    while p != 0:
        count += 1
        i, divisionoccured = 0, False

        while i < m and not divisionoccured:
```

```
            glt, plt = g[i].lt(), p.lt()

            if glt and plt / glt in ring:
                q[i] = q[i] + plt // glt
                p    =    p - plt // glt * g[i]
                divisionoccured = True
            else:
                i = i + 1
        if not divisionoccured:
            r = r + p.lt()
            p = p - p.lt()

    return r

def divide(f,n):
    K = Anillo(n)
    PolElemental = elementales(n,K)
    B = base (n, PolElemental, K)
    #print 'Cambio de variables'
    S = div(f, B, K)
    return S
```

El siguiente paso es el cálculo de los polinomios Γ_C para las distintas clases de conjugación del grupo de Galois.

```
C = AlternatingGroup(n).conjugacy_classes()

def Anillo_X(n):
    Qx, x = Anillo(n), Anillo(n).gens()
    QX, X = PolynomialRing(Qx, 1, 'X', order='lex').objgens()
    return QX, X+x
L, x = Anillo_X(4)
```

```
def gamma(n,j,x,C):
    m = len(C)+1; L = m*[0]
    g = 1
    for sigma in C:
        f = x[0]-sum((x[p]^j)*x[sigma(p)] for p in range(1,n+1))
        g = g*f

    for i in range(m):
        L[i] = g[i]
    return L

def Cambio(n,L,a):
    m = len(L); H = m*[0]
    x = QQ['x'].0
    f = 3*x^4-4*x^3+1+3*a^2
    F = f.complex_roots()
    for i in range(m):
        h = divide(L[i],n)
        h = h(F[0],F[1],F[2],F[3],4/3,0,0,1/3+a^2)
        if abs(h.imag())<0.0001:
            H[i] = h.real()
        else:
            print 'No está en Q'
            return
    QY = PolynomialRing(QQ, 'X')
    return QY(H)

G = []
for c in C:
    Ga = gamma(4,2,x,c)
    Gamma = Cambio(4,Ga,2)
    G = G+[Gamma]
    print c,'\n'
    print Gamma
    print '_____________\n'
```

A continuación hemos de comprobar que son válidos estos polinomios, para ello habría que comprobar que no tienen resultante nula dos a dos, pero nos basta con ver que son coprimos por el mayor común divisor.

```
def valido(n,G):
    C = An(n); l = len(C)

    k = 0
    for i in range(l):
        for j in range(i+1,l):
            if gcd(G[i],G[j]) != 1:
                print i, ' y ', j, ' tienen reultante nula'
                k = 0
                break
            else:
                k = 1
    if k == 1:
        print 'Los polinomios Gamma son validos'
```

Por último, antes de aplicar el teorema 2.2.2.3 definimos la matriz asociada al polinomio $f_a(x)$ de la sección 3.5 y calculamos la traza como se muestra en la observación 2.2.2.5. Tras esto la evaluamos en los polinomios Γ_C que ya tenemos calculados y tomamos módulo por los ideales $\mathfrak{p}$ que se encuentren por encima de p y que satisfagan las condiciones del teorema 2.2.2.3(2.).

```
Qa = PolynomialRing(QQ, 'a, b', order='lex')
A = Qa.gens()
MQ = MatrixSpace(Qa, 4, 4)
M = MQ.matrix([0,0,0,-1/3-A[0]^2,1,0,0,0,0,0,1,0,0,0,0,1,-A[1]])
M(1,-4/3)

def traza(a,p,M):
```

```
J = M(a,-4/3)

if a != A[0]:
  divison = True
  x = QQ['x'].0
  f = 3*x^4-4*x^3+1+3*a^2
  r1 = f.complex_roots()[0]
  k.<z> = NumberField(f,embedding=r1)

  if a.is_integer(): n , m = a.numerator() , 0
  else: n , m = a.numerator() , a.denominator()

else: n , m , divison = 0 , 0, False

for q in range(0,p+1):
  J = J*M(a,-4/3)

  if is_prime(q):

    t = sum(J.eigenvalues())
    if abs(t.imag())<0.0001:
      print 'Para q =', q
      print '-----------------------'
      print 'La traza ->', t.real() , '\n'
    else:
      print  'Para q =', q
      print '-----------------------'
      print  'La traza -> No esta en Q'
    if divison:
    #    LCMgamma = 1 #con la definición actual
     #   for i in range(3):#no es necesario
      #    for j in range(i+1,4):
       #     LCMgamma = lcm(LCMgamma,G[i].resultant(G[j]))
        if m!=0:
          D = list(factor(k.ideal(3))) + list(factor(k.ideal(m)))
              + list(factor(k.ideal(f.discriminant())))
              #+ list(factor(k.ideal(LCMgamma)))
```

```
          else:
            D = list(factor(k.ideal(3)))
                + list(factor(k.ideal(f.discriminant())))
                #+ list(factor(k.ideal(LCMgamma)))
          D = sorted(set([d[0] for d in D]))
          I = list(factor(k.ideal(q)))
          P0 = 0
          for j in I:
            P1 = 0
            if j[1] == 1:
              print 'se toma', j
              for d in D:
                if not j[0]==d:
                  P1 = P1+1
                  T = t - (t // CC(j[0].gens_reduced()[0]))
                       *CC(j[0].gens_reduced()[0])
                  print 'mod', d, '->','Traza=' ,T
                  Pw = 0
                  for w in range(4):
                    if G[w](t) - (G[w](t)
                      // CC(j[0].gens_reduced()[0]))
                      * CC(j[0].gens_reduced()[0])==0:
                        Pw = Pw+1
                        W = w
                if Pw==1:
                    print 'mod', d, '->','Traza=' ,T
                    print 'Frob ->',C[W]
                    break
                  else: print 'El primo no es bueno'
                  print '\n'
                if  P1: P0 = P0+1
              if not P0: print 'no da'
              print '-----------------------\n'
      else: print '-----------------------\n'
```

Bibliografía

[1] Alaca, S., and Williams, K. S. *Introductory algebraic number theory.* Cambridge University Press, 2004.

[2] Dokchitser, T., and Dokchitser, V. Identifying frobenius elements in galois groups. *Algebra & Number Theory 7*, 6 (2013), 1325–1352.

[3] Mollin, R. A. *Algebraic number theory.* Chapman and Hall/CRC, 2011.

[4] Neukirch, J. *Algebraic number theory*, vol. 322. Springer Science & Business Media, 2013.

[5] PARK, S. Existence of the frobenius element and its applications.

[6] Serre, J.-P. Topics in galois theory, volume 1 of research notes in mathematics. ak peters ltd., wellesley, ma, 2008. *With notes by Henri Darmon 4*, 3.

[7] van Bommel, R. Using the chebotarev density theorem to calculate the size of galois groups.