Apuntes: Elementos de Frobenius

Rocío Belén Sepúlveda Manzo

Resumen. Esta es una transcripción y completación de contenidos con referencias de la charla de Benjamín Castillo para el Seminario de representaciones de Galois cuyo resumen es: Revisaremos algunas construcciones básicas de la teoría algebraica de números para poder hablar sobre el elemento de Frobenius de un ideal primo en el anillo de enteros de un campo de números.

1. Introducción

Un *domino de Dedekind* es un dominio íntegro tal que todo ideal no nulo se puede factorizar de manera única en ideales primos. Por ejemplo, dado K un campo de números, el anillo de enteros $\mathcal{O}_K$ es un dominio de Dedekind (véase Neukirch [2, págs. 44-45]).

> Es relevante notar que en la literatura se suele definir el dominio de Dedekind como un anillo noetheriano, íntegramente cerrado donde cada ideal no nulo es maximal. A partir de esta definición, se deduce la equivalencia con la anterior definición. Puede ver la sección de dominios de Dedekind en Janusz [1].

Sea $p \in \mathbb{Z}$ un primo racional, su ideal generado en $\mathcal{O}_K$ se factoriza

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_{\mathfrak{p}_1}} \cdot \ldots \cdot \mathfrak{p}_g^{e_{\mathfrak{p}_g}},$$

donde $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ son los ideales primos distintos de $\mathcal{O}_K$ que contienen a p.

Definición 1. Dado $\mathfrak{p} \subseteq \mathcal{O}_K$ primo tal que $p\mathcal{O}_K \subseteq \mathfrak{p}$ se tiene:

(i) El valor $e_{\mathfrak{p}}$ es el *índice de ramificación* de $\mathfrak{p}$.
(ii) El campo residual $\mathcal{O}_K/\mathfrak{p}$ es finito de característica p, donde $f_{\mathfrak{p}} := [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$ es el *grado residual* de $\mathfrak{p}$.
(iii) El valor g es la cantidad de primos distintos que aparecen en la factorización, a éste se le denomina como *índice de descomposición*.

Estos tres valores se relacionan mediante la siguiente fórmula:

$$[K : \mathbb{Q}] = \sum_{i=1}^{g} e_{\mathfrak{p}_i} f_{\mathfrak{p}_i}. \tag{1}$$

Ejemplo. Sea $K = \mathbb{Q}(i)$ y $\mathcal{O}_K = \mathbb{Z}[i]$, considere $p = 2$, luego $p = (1+i)(1-i)$. Luego,

$$p\mathbb{Z}[i] = (1+i)(1-i).$$

Fecha: 4 de octubre de 2023.

Nótese que $-i(1-i) = 1+i$, por tanto, $p\mathbb{Z}[i] = (1+i)^2$. Además, el ideal $(1+i)$ es primo, pues su norma $N(1+i) = (1+i)(1-i) = 2$ es un valor primo. Por lo tanto $g = 1$, $e = 2$. Por otro lado, $[K : \mathbb{Q}] = 2$, así que $f = 1$; ésto quiere decir que el campo residual es $\mathbb{F}_2$.

2. Campos de números de Galois

En esta parte trabajaremos con campos de números F tales que su extensión $F/\mathbb{Q}$ es de Galois. Estos campos serán denotados por F en vez de K para enfatizar que cumplen un rol diferente a los campos de números en general. El propósito a futuro es ilustrar algunos resultados de la teoría algebraica de números en el caso Galois dando ejemplos específicos para ganar intuición.

Teorema 2 (La acción del grupo de Galois)**.** *Sea $F/\mathbb{Q}$ una extensión de Galois, y sea p un primo racional. Luego*

(i) El grupo de Galois $\mathrm{Gal}(F/\mathbb{Q})$ actúa transitivamente sobre los primos en F tales que contienen a $p\mathcal{O}_F$, i.e., para $\mathfrak{p}$ y $\mathfrak{p}'$ ideales primos tales que contienen a $p\mathcal{O}_K$, entonces existe $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ tal que $\sigma(\mathfrak{p}) = \mathfrak{p}'$.

(ii) Los ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ de $\mathcal{O}_K$ tales que contienen a $p\mathcal{O}_K$ tienen el mismo índice de ramificación e y el mismo grado residual f, y la fórmula (1) se convierte en:

$$[F : \mathbb{Q}] = efg.$$

Aquel teorema se encuentra demostrado en Neukirch [2, págs. 54-55].

Definición 3. Dado una extensión de Galois $F/\mathbb{Q}$, para p primo racional, diremos que p *ramifica* en F si existe algún ideal primo $\mathfrak{p}$ tal que contiene a $p\mathcal{O}_K$ con índice de ramificación $e > 1$. Diremos que p *no ramifica* si $e = 1$. Si p satisface $e = f = 1$, entonces diremos que p *escinde completamente* en F.

Observación. Los primos que ramifican son los que dividen al discriminante D_K y, en particular, son finitos (ver apéndice A).

Ejemplo (Campos ciclotómicos). Sea n un entero positivo, considere el campo de números $F = \mathbb{Q}(\zeta_n)$. Sabemos que existe un isomorfismo $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \cong \mu_n$. En particular, $[F : \mathbb{Q}] = \phi(n)$. Luego, se tiene:

(i) El anillo de enteros $\mathcal{O}_K$ es $\mathbb{Z}[\zeta_n]$.
(ii) Un primo p ramifica en $\mathbb{Z}[\zeta_n]$ si y solamente si $p \mid n$.
(iii) El grado residual f_p es el orden multiplicativo de p en $(\mathbb{Z}/n\mathbb{Z})^\times$.

Puede ver Washington [3, págs. 10 - 14] prop. 2.3, thm. 25 y thm. 26.

3. Grupo de descomposición e inercia

Seguiremos trabajando sobre una extensión de campos $F/\mathbb{Q}$ finita de Galois. Sea p un primo racional, para cada ideal maximal $\mathfrak{p}$ de $\mathcal{O}_F$ que contiene a $p\mathcal{O}_F$ se define el *grupo de descomposición* de $\mathfrak{p}$ como el subgrupo del grupo de Galois que fija a $\mathfrak{p}$ como conjunto, es decir,

$$D_\mathfrak{p} = \{\sigma \in \mathrm{Gal}(F/Q) : \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

El orden del grupo de descomposición es ef, así que el índice $[\mathrm{Gal}(F/\mathbb{Q}) : D_{\mathfrak{p}}]$ es, en efecto, el índice de descomposición g. Por definición, este grupo actúa sobre el campo residual $\mathcal{O}_F/\mathfrak{p}$:

$$\sigma(x+\mathfrak{p}) = \sigma(x) + \mathfrak{p}, \quad x \in \mathcal{O}_F,\ \sigma \in D_{\mathfrak{p}}.$$

Además, se define el *grupo de inercia* de $\mathfrak{p}$ como el kernel de la acción $D_{\mathfrak{p}} \times \mathcal{O}_F/\mathfrak{p} \to \mathcal{O}_F/\mathfrak{p}$, dado por $(\sigma, [x]) \mapsto [\sigma(x)]$, es decir,

$$I_{\mathfrak{p}} = \{\sigma \in D_g : \sigma(x) \equiv x \mod \mathfrak{p} \text{ para cada } x \in \mathcal{O}_F\}.$$

Observación. El orden del grupo de inercia es e, así que el grupo es trivial para cada $\mathfrak{p}$ en cualquier p no ramificado y $D_{\mathfrak{p}} \cong \mathrm{Gal}((\mathcal{O}_F/\mathfrak{p})/\mathbb{F}_p)$. En casos más generales, se tiene

$$D_{\mathfrak{p}}/I_{\mathfrak{p}} \cong \mathrm{Gal}((\mathcal{O}_F/\mathfrak{p})/\mathbb{F}_p).$$

para cualquier p primo racional.

4. Elementos de Frobenius

Sea p primo racional. Recordemos que el automorfismo de Frobenius sobre $\overline{\mathbb{F}_p}$ es $\sigma_p : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$, dado por $x \mapsto x^p$. Para $\mathfrak{p}$ ideal maximal de $\mathcal{O}_F$ tal que contiene a $p\mathcal{O}_F$ se tiene que el automorfismo de Frobenius genera:

$$D_{\mathfrak{p}}/I_{\mathfrak{p}} \cong \mathrm{Gal}((\mathcal{O}_F/\mathfrak{p})/\mathbb{F}_p) = \langle \sigma_p \rangle.$$

Cualquier representante en $D_{\mathfrak{p}}$ de este generador se le denomina *un elemento de Frobenius* de $\mathrm{Gal}(F/\mathbb{Q})$ y se denotará por $\mathrm{Frob}_{\mathfrak{p}}$. Si p no ramifica, entonces $I_{\mathfrak{p}}$ es trivial, por tanto, $\mathrm{Frob}_{\mathfrak{p}}$ es único.

Observación. La condición que se pide explícitamente es: $\mathrm{Frob}_{\mathfrak{p}}(x) \equiv x^p \mod \mathfrak{p}$ para cada $x \in \mathcal{O}_F$.

Para $F/\mathbb{Q}$ una extensión de Galois y cualquier par de ideales primos $\mathfrak{p}$ y $\mathfrak{p}'$ tales que contienen a $p\mathcal{O}_F$ se tiene $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ tal que $\sigma(\mathfrak{p}) = \mathfrak{p}'$. Luego, el grupo de descomposición y el de inercia asociados satisfacen

$$D_{\mathfrak{p}'} = \sigma^{-1} D_{\mathfrak{p}} \sigma, \qquad I_{\mathfrak{p}'} = \sigma^{-1} I_{\mathfrak{p}} \sigma.$$

Definición 4. Se dice que una extensión F/K de Galois es *abeliana* si el grupo de Galois es abeliano. Se dice que una extensión L/K es *abeliana* si es una subextensión de una extensión de Galois abeliana.

Proposición 5. *Sea p un primo racional que no ramifica. Entonces para cada ideal maximal $\mathfrak{p}$ tal que contiene a $p\mathcal{O}_F$, se tiene:*

(i) $\mathrm{Frob}_{\mathfrak{p}'} = \sigma^{-1} \mathrm{Frob}_{\mathfrak{p}}\, \sigma$,
(ii) *El orden de* $\mathrm{Frob}_{\mathfrak{p}}$ *es el grado residual* f,
(iii) $\mathrm{Frob}_{\mathfrak{p}} = \mathrm{Id}_F$ *si y solamente si* p *escinde completamente en* K.
(iv) *Si la extensión $F/\mathbb{Q}$ es abeliana, entonces tanto $D_{\mathfrak{p}}$ como $\mathrm{Frob}_{\mathfrak{p}}$ no dependen de la elección de $\mathfrak{p}$, y se pueden anotar como D_p y Frob_p.*

Ejemplo. Considere el n-ésimo campo ciclotómico $F := \mathbb{Q}(\zeta_n)$ y sea $p \nmid n$ primo (el cual no se ramifica). Luego para cada $x \in \mathbb{Z}[\zeta_n]$, se tiene que $\mathrm{Frob}_p(x) \equiv x^p \mod \mathfrak{p}$. En particular, $\mathrm{Frob}_p(\zeta_n) \equiv \zeta_n^p \mod \mathfrak{p}$ y, viendo a Frobenius como automorfismo, $\mathrm{Frob}_p(\zeta_n) = \zeta_n^m$ para algún m entero positivo. Así que: si $m \not\equiv p \mod n$ entonces $\mathfrak{p}$ no contiene a $(\zeta_n^m - \zeta_n^p)\mathcal{O}_F$, pues

$\zeta_n^m - \zeta_n^p = \zeta^m(1-\zeta^{m-p})$ y $(1-\zeta^{m-p})$ es, o bien, una unidad (cuando n tiene al menos dos factores primos distintos, ver Washington [3], prop. 2.8), o bien, es un primo que divide a n (cuando n es potencia de algún primo, ver Washington [3], lemma 1.4).

Por tanto, $m \equiv p \mod n$. Entonces Frob_p es el automorfismo determinado por $\zeta_n \mapsto \zeta_n^p$.

Observación. Por el Teorema de Dirichlet en Progresión Aritmética, para cada $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ existe infinitos primos p tales que $p \equiv a \mod n$. Por lo tanto, cada elemento del grupo de Galois de F toma la forma de Frob_p para infinitos p, y el isomorfismo que fue enunciado en el ejemplo de campos ciclotómicos (2) es

$$\mathrm{Gal}(F/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times, \qquad \mathrm{Frob}_p \mapsto p \mod n, \text{ para } p \nmid n.$$

El Teorema de Dirichlet en Progresión Aritmética es un caso especial de

Teorema 6 (Teorema de densidad de Chebotarev, versión débil)**.** *Sea F un campo de números de Galois. Entonces cada elemento del grupo $\mathrm{Gal}(F/\mathbb{Q})$ toma la forma de $\mathrm{Frob}_\mathfrak{p}$ para infinitos ideales maximales $\mathfrak{p}$ de $\mathcal{O}_F$.*

Esta versión débil aparece en Janusz [1] como el Teorema de Densidad del Frobenius (thm. 5.2). Para revisar la versión general puede ver Neukirch [2] thm. 13.4.

A. Discriminante y ramificación

Sea L/K una extensión de campos separable finita de grado n y sean $x_1, \ldots, x_n \in L$ una K-base. Sea L' la clausura normal de L sobre K y sean $\sigma_1, \ldots, \sigma_n : L \to L'$ monomorfismos de K-álgebras. Se define el discriminante como:

$$\mathrm{Disc}_{L/K}(x_1, \ldots, x_n) := \det[\sigma_i(x_j)]_{ij}^2$$

Proposición 7. *Sea $K/\mathbb{Q}$ extensión finita de campos y sea $B := \mathcal{O}_K$. Entonces todo B-submódulo finitamente generado M no nulo de K es un $\mathbb{Z}$-módulo libre de rango $[K : \mathbb{Q}]$. En particular, B admite una base entera sobre $\mathbb{Z}$.*

El discriminante $\mathrm{Disc}_{K/\mathbb{Q}}(x_1, \ldots, x_n)$ es independiente a la elección de una $\mathbb{Z}$-base. Así que, si consideramos una base entera $y_1, \ldots, y_n$ de $\mathcal{O}_K$ obtenemos el *discriminante del campo de números algebraico* K,

$$D_K := \mathrm{Disc}_{K/\mathbb{Q}}(y_1, \ldots, y_n).$$

Para profundizar más, véase Neukirch [2, págs. 11-15].

Teorema 8 (Janusz [1], thm. 7.3)**.** *Sea K un campo de números y sea p un primo racional. Tenemos que $p \mid D_K$ si y solo si existe un primo $\mathfrak{p}$ de $\mathcal{O}_K$ sobre p con $e(\mathfrak{p}) > 1$, i.e. si ramifica en K.*

Corolario 9. *Los primos que ramifican son finitos.*

Ejemplo. Sea $K = \mathbb{Q}(i)$ tenemos que su anillo de enteros es $O_K = \mathbb{Z}[i]$, anteriormente vimos que $2\mathcal{O}_K = \mathfrak{p}^2$ con $\mathfrak{p} = (1+i)$. Así que $p = 2$ ramifica en K. Calculando el discriminante respecto a la base entera $\{1, i\}$ de $\mathcal{O}_K$, y los automorfismos en $\mathrm{Gal}(K/\mathbb{Q})$: σ_1 la identidad y σ_2 la conjugación, luego

$$D_K = \det[\sigma_i(x_j)]_{ij} = \det \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}^2 = (-2i)^2 = -4.$$

Por tanto, el único primo que ramifica en $K = \mathbb{Q}(i)$ es 2.

Referencias

1. Janusz, G. *Algebraic number theory* 2.ª ed. doi:10.1090/gsm/007 (Academic Press, 1973).
2. Neukirch, J. *Algebraic number theory* (Springer-Verlag, 1999).
3. Washington, L. C. *Introduction to Cyclotomic Fields* (Springer-Verlag, 1982).

Correo electrónico: rseplveda@uc.cl