Teoría de números algebraicos
Tarea 7

Alexey Beshenov (alexey.beshenov@cimat.mx)

14 de octubre de 2020

Ejercicio 7.1. Demuestre que para una extensión de Galois L/K, primos $\mathfrak{q} \subset \mathcal{O}_L$, $\mathfrak{p} \subset \mathcal{O}_K$, tales que $\mathfrak{q} \mid \mathfrak{p}$, y $\sigma \in \mathrm{Gal}(L/K)$ se tiene

$$D(\sigma(\mathfrak{q})|\mathfrak{p}) = \sigma\, D(\mathfrak{q}|\mathfrak{p})\, \sigma^{-1}, \quad I(\sigma(\mathfrak{q})|\mathfrak{p}) = \sigma\, I(\mathfrak{q}|\mathfrak{p})\, \sigma^{-1}.$$

Además, si $\mathfrak{p}$ no se ramifica, entonces el Frobenius cumple

$$\mathrm{Frob}_{\sigma(\mathfrak{q})|\mathfrak{p}} = \sigma\ \mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}\ \sigma^{-1}.$$

Solución. Recordemos que $D(\mathfrak{q}|\mathfrak{p})$ es el grupo estabilizador de $\mathfrak{q}$ respecto a la acción del grupo de Galois $\mathrm{Gal}(L/K)$ sobre los primos $\mathfrak{q}_1, \ldots, \mathfrak{q}_g$ que están sobre $\mathfrak{p}$. Es un cálculo general que para un G-conjunto X se cumple $\mathrm{Stab}_{\sigma x} = \sigma\, \mathrm{Stab}_x\, \sigma^{-1}$.

Para el grupo de inercia, podemos considerar el diagrama

$$\begin{array}{ccccccccc}
1 & \longrightarrow & I(\sigma(\mathfrak{q})|\mathfrak{p}) & \longrightarrow & D(\sigma(\mathfrak{q})|\mathfrak{p}) & \longrightarrow & \mathrm{Gal}(\kappa(\sigma(\mathfrak{q}))/\kappa(\mathfrak{p})) & \longrightarrow & 1 \\
 & & \| & & \| & & \| & & \\
1 & \longrightarrow & \sigma I(\mathfrak{q}|\mathfrak{p})\sigma^{-1} & \longrightarrow & \sigma D(\mathfrak{q}|\mathfrak{p})\sigma^{-1} & \longrightarrow & \overline{\sigma}\,\mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))\overline{\sigma}^{-1} & \longrightarrow & 1
\end{array}$$

Aquí $\sigma \in \mathrm{Gal}(L/K)$ induce un isomorfismo $\overline{\sigma}\colon \kappa(\mathfrak{q}) \to \kappa(\sigma(\mathfrak{q}))$.
De allí también se sigue la afirmación sobre el Frobenius.

$$\begin{array}{ccc}
D(\sigma(\mathfrak{q})|\mathfrak{p}) & \xrightarrow{\cong} & \mathrm{Gal}(\kappa(\sigma(\mathfrak{q}))/\kappa(\mathfrak{p})) \\
\| & & \| \\
\sigma D(\mathfrak{q}|\mathfrak{p})\sigma^{-1} & \xrightarrow{\cong} & \overline{\sigma}\,\mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))\overline{\sigma}^{-1}
\end{array}$$

□

Ejercicio 7.2. Sea F un campo de números, y $L/K/F$ una torre de extensiones tal que L/K es una extensión normal. Sean $\mathfrak{p} \subset \mathcal{O}_F$, $\mathfrak{q} \in \mathcal{O}_K$, $\mathfrak{Q} \subset \mathcal{O}_L$ ideales primos tales que $\mathfrak{Q} \mid \mathfrak{q}$ y $\mathfrak{q} \mid \mathfrak{p}$.

1) Demuestre que $D(\mathfrak{Q}|\mathfrak{q})$ se identifica con un subgrupo de $D(\mathfrak{Q}|\mathfrak{p})$ e $I(\mathfrak{Q}|\mathfrak{q})$ con un subgrupo de $I(\mathfrak{Q}|\mathfrak{p})$.

2) Si $\mathfrak{p}$ no se ramifica en L, demuestre que $\mathrm{Frob}_{\mathfrak{Q}|\mathfrak{q}} = (\mathrm{Frob}_{\mathfrak{Q}|\mathfrak{p}})^{f(\mathfrak{q}|\mathfrak{p})}$.

3) Si la extensión K/F es normal, demuestre que $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$ es la restricción de $\mathrm{Frob}_{\mathfrak{Q}|\mathfrak{p}}$.

Solución. Estamos en la siguiente situación:

$$\begin{array}{ccc} \mathcal{O}_L & \twoheadrightarrow & \kappa(\mathfrak{Q}) \\ | & & | \\ \mathcal{O}_K & \twoheadrightarrow & \kappa(\mathfrak{q}) \\ | & & | \\ \mathcal{O}_F & \twoheadrightarrow & \kappa(\mathfrak{p}) \end{array}$$

Tenemos inclusiones naturales $\mathrm{Gal}(L/K) \subset \mathrm{Gal}(L/F)$ y $\mathrm{Gal}(\kappa(\mathfrak{Q})/\kappa(\mathfrak{q})) \subset \mathrm{Gal}(\kappa(\mathfrak{Q})/\kappa(\mathfrak{p}))$, y estas nos dan el diagrama conmutativo

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I(\mathfrak{Q}|\mathfrak{q}) & \longrightarrow & D(\mathfrak{Q}|\mathfrak{q}) & \longrightarrow & \mathrm{Gal}(\kappa(\mathfrak{Q})/\kappa(\mathfrak{q})) & \longrightarrow & 1 \\ & & \vdots\downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & I(\mathfrak{Q}|\mathfrak{p}) & \longrightarrow & D(\mathfrak{Q}|\mathfrak{p}) & \longrightarrow & \mathrm{Gal}(\kappa(\mathfrak{Q})/\kappa(\mathfrak{p})) & \longrightarrow & 1 \end{array}$$

Aquí la flecha punteada existe por la conmutatividad del segundo cuadrado, y es un monomorfismo porque la flecha en el medio lo es. Si $\mathfrak{p}$ no se ramifica, se obtiene

$$\begin{array}{ccc} D(\mathfrak{Q}|\mathfrak{q}) & \xrightarrow{\cong} & \mathrm{Gal}(\kappa(\mathfrak{Q})/\kappa(\mathfrak{q})) \\ \downarrow & & \downarrow \\ D(\mathfrak{Q}|\mathfrak{p}) & \xrightarrow{\cong} & \mathrm{Gal}(\kappa(\mathfrak{Q})/\kappa(\mathfrak{p})) \end{array}$$

Tenemos

$$\mathrm{Frob}_{\mathfrak{Q}|\mathfrak{p}} \colon \alpha \mapsto \alpha^{\#\kappa(\mathfrak{p})} = \alpha^{p^{f(\mathfrak{p}|p)}}$$

y

$$\mathrm{Frob}_{\mathfrak{Q}|\mathfrak{q}} \colon \alpha \mapsto \alpha^{\#\kappa(\mathfrak{q})} = \alpha^{p^{f(\mathfrak{q}|p)}} = \left(\alpha^{p^{f(\mathfrak{p}|p)}}\right)^{f(\mathfrak{q}|\mathfrak{p})}.$$

Si K/F es también una extensión normal, entonces tiene sentido considerar el diagrama

$$\begin{array}{ccc} D(\mathfrak{Q}|\mathfrak{p}) & \xrightarrow{\cong} & \mathrm{Gal}(\kappa(\mathfrak{Q})/\kappa(\mathfrak{p})) \\ \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow \\ D(\mathfrak{q}|\mathfrak{p}) & \xrightarrow{\cong} & \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) \end{array}$$

inducido por $\mathrm{Gal}(L/F) \twoheadrightarrow \mathrm{Gal}(K/F)$, y $\mathrm{Gal}(\kappa(\mathfrak{L})/\kappa(\mathfrak{p})) \twoheadrightarrow \mathrm{Gal}(\kappa(\mathfrak{L})/\kappa(\mathfrak{p}))$. Estas son las restricciones de automorfismos, con el núcleo $\mathrm{Gal}(L/K)$ y $\mathrm{Gal}(\kappa(\mathfrak{L})/\kappa(\mathfrak{q}))$ respectivamente. □

Ejercicio 7.3. Sea K el campo de descomposición del polinomio

$$f = x^4 + 8x + 12.$$

Calcule $\mathrm{Gal}(K/\mathbb{Q})$, las clases de conjugación, los tipos de descomposición que corresponden a cada $\mathrm{Frob}_{\mathfrak{p}|p}$, y las densidades que nos da el teorema de Chebotarëv.

Solución. Podemos ocupar la reducción módulo p. Para un polinomio mónico $f \in \mathbb{Z}[x]$ y un primo p, supongamos que el polinomio correspondiente $\overline{f} \in \mathbb{F}_p[x]$ no tiene raíces múltiples en $\overline{\mathbb{F}_p}$. En este caso el grupo de Galois de $\overline{f}$ se encaja en el grupo de Galois de f. Para las pruebas, véanse por ejemplo §§VI.2 + VII.2 en el libro de Lang. Aquí me gustaría usar nuestro polinomio particular para explicar el uso de este resultado.

El polinomio $f = x^4+8x+12$ tiene factores múltiples al factorizarlo módulo $p = 2$ y 5. La factorización módulo $p = 5$ nos da

$$\overline{f} = (x + 1)\,(x^3 + 4x^2 + x + 2).$$

El grupo de Galois de $\overline{f}$ será $\mathrm{Gal}(\mathbb{F}_{p^3}/\mathbb{F}_p) \cong C_3$, lo que nos dice que el grupo de Galois de f contiene un elemento de orden 3.

El grupo de Galois de f se realiza como un subgrupo transitivo de S_4, y las únicas posibilidades para este son

$$C_4,\ V_4,\ D_8,\ A_4,\ S_4.$$

Sabiendo que tenemos un elemento de orden 3, nos quedan solamente dos posibilidades: A_4 y S_4. Calculamos el discriminante

$$\Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

En este caso particular $\Delta(f) = 2^{12} \cdot 3^4$ es un cuadrado. Entonces,

$$\prod_{i<j} (\alpha_i - \alpha_j) \in \mathbb{Q},$$

y por lo tanto este número es fijo respecto a la acción del grupo de Galois. Notamos que la transposición que intercambia dos raíces α_i y α_j no está en el grupo de Galois: esta transposición cambia el signo de $\prod_{i<j}(\alpha_i - \alpha_j)$. Entonces, el grupo de Galois es A_4.

Ahora bien, las clases de conjugación en A_4 son las siguientes.

- $C_1 = \{id\}$. En este caso el Frobenius es trivial, así que p se escinde completamente en 12 ideales primos. La densidad correspondiente será $\frac{1}{12}$.

- $C_2 = \{(1\,2)\,(3\,4),\ (1\,3)\,(2\,4),\ (1\,4)\,(2\,3)\}$. En este caso el Frobenius tiene orden 2, lo que corresponde a descomposiciones de la forma $\mathfrak{p}_1 \cdots \mathfrak{p}_6$. La densidad correspondiente es $\frac{1}{4}$.
- $C_3 = \{(1\,2\,3),\ (1\,3\,4),\ (1\,4\,2),\ (2\,4\,3)\}$. En este caso el Frobenius tiene orden 3, lo que corresponde a las factorizaciones de la forma $\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$. La densidad correspondiente es $\frac{1}{3}$.
- $C_4 = \{(1\,2\,4),\ (1\,3\,2),\ (1\,4\,3),\ (2\,3\,4)\}$. Este caso es similar al anterior.

En particular, podemos concluir que hay tres tipos de factorizaciones: en 4 ideales primos (densidad $\frac{2}{3}$), en 6 ideales primos (densidad $\frac{1}{4}$), y en 12 ideales primos (densidad $\frac{1}{12}$). □

Ejercicio 7.4. Para $K = \mathbb{Q}(\sqrt[4]{2})$ consideremos la cerradura de Galois $L = \mathbb{Q}(\sqrt[4]{2}, i)$.

1) Demuestre que el único primo racional p que se ramifica en L es $p = 2$.
2) Para p impar sea $\mathfrak{p} \subset \mathcal{O}_L$ un primo tal que $\mathfrak{p} \mid p$. Determine cómo el tipo de factorización de p en $\mathcal{O}_K$ para toda posibilidad para $\mathrm{Frob}_{\mathfrak{p}|p}$.

Solución. Tenemos $L = KF$, donde $F = \mathbb{Q}(i)$. La extensión $F/\mathbb{Q}$ es de Galois. Dado un primo racional p, sean $\mathfrak{P} \subset \mathcal{O}_L$ un ideal primo tal que $\mathfrak{P} \mid p$ y $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ y $\mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_F$.

Se puede ver que en esta situación la restricción de automorfismos induce inclusiones $D(\mathfrak{P}|\mathfrak{p}) \hookrightarrow D(\mathfrak{q}|p)$ e $I(\mathfrak{P}|\mathfrak{p}) \hookrightarrow I(\mathfrak{q}|p)$. El único primo p que se ramifica en F es $p = 2$. Entonces, para todo p impar se tiene $I(\mathfrak{P}|\mathfrak{p}) = I(\mathfrak{q}|p) = 1$. Esto implica que

$$e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p})\, e(\mathfrak{p}|p) = e(\mathfrak{p}|p).$$

Tenemos $\Delta(x^4 - 2) = -2^{11}$, así que en K también se ramifica solamente $p = 2$. Entonces, $e(\mathfrak{P}|p) = 1$ para todo p impar. Esto verifica la parte 1).

Ahora K es el subcampo fijo por la conjugación compleja, que bajo el isomorfismo $\mathrm{Gal}(L/\mathbb{Q}) \cong D_4$ corresponde al subgrupo $H = \{1, f\}$. Las clases laterales correspondientes son

$$H,\ Hr,\ Hr^2,\ Hr^3.$$

La siguiente tabla nos da las acciones del Frobenius $\mathrm{Frob}_{\mathfrak{p}|p}$ sobre las clases laterales y las descomposiciones correspondientes de p en K.

$\mathrm{Frob}_{\mathfrak{p}\mid p}$	órbitas	descomposición	densidad
1	$\{H\},\ \{Hr\},\ \{Hr^2\},\ \{Hr^3\}$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	$\frac{1}{8}$
r	$\{H \to Hr \to Hr^2 \to Hr^3\}$	inerte, $f = 4$	$\frac{1}{4}$
r^3	$\{H \to Hr^3 \to Hr^2 \to Hr\}$		
r^2	$\{H \to Hr^2\},\ \{Hr \to Hr^3\}$	$\mathfrak{p}_1\mathfrak{p}_2$, $f_1 = f_2 = 2$	$\frac{3}{8}$
$rf = fr^3$	$\{H \to Hr^3\},\ \{Hr \to Hr^2\}$		
$r^3f = fr$	$\{H \to Hr\},\ \{Hr^2 \to Hr^3\}$		
f	$\{H\},\ \{Hr \to Hr^3\},\ \{Hr^2\}$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, $f_1 = f_2 = 1$, $f_3 = 2$	$\frac{1}{4}$
$r^2f = fr^2$	$\{H \to Hr^2\},\ \{Hr\},\ \{Hr^3\}$		

□

Ejercicio 7.5. Para la extensión ciclotómica $L = \mathbb{Q}(\zeta_n)$ determine cómo los primos no ramificados $p \nmid n$ se descomponen en el subcampo $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Solución. Para $p \nmid n$ el automorfismo de Frobenius sobre $\mathbb{Q}(\zeta_n)$ viene dado por $\zeta_n \mapsto \zeta_n^p$. El grado de campos residuales f es el orden del Frobenius; es decir, el orden de p en el grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Ahora $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ es el subcampo fijo por la conjugación compleja $\zeta_n \mapsto \zeta_n^{-1}$ y $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times/\{\pm 1\}$. El Frobenius corresponde a la clase de p en el cociente $(\mathbb{Z}/n\mathbb{Z})^\times/\{\pm 1\}$, y el grado del campo residual será el orden de p en ese grupo.

He aquí un ejemplo particular para el campo $\mathbb{Q}(\zeta_7)$.

p mód 7:	1	2	3	4	5	6
orden en $(\mathbb{Z}/7\mathbb{Z})^\times$:	1	3	6	3	6	2
orden en $\frac{(\mathbb{Z}/7\mathbb{Z})^\times}{\{\pm 1\}}$:	1	3	3	3	3	1
desc. en $\mathbb{Q}(\zeta_7)$:	$\mathfrak{P}_1 \cdots \mathfrak{P}_6$	$\mathfrak{P}_1\mathfrak{P}_2$	inerte	$\mathfrak{P}_1\mathfrak{P}_2$	inerte	$\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$
desc. en $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$:	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	inerte	inerte	inerte	inerte	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$

Otro ejemplo: $p = 2$ tiene orden 4 en $(\mathbb{Z}/15\mathbb{Z})^\times$ y también en $(\mathbb{Z}/15\mathbb{Z})^\times/\{\pm 1\}$. Entonces, p se descompone en $2 = \phi(15)/4$ ideales primos en $\mathbb{Q}(\zeta_{15})$, y es inerte en el subcampo $\mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1})$. □