Introducción a los Números Algebraicos
Clase 12: Descomposición e inercia II

Gonzalo Tornaría

26 de abril, 2007

Podemos caracterizar el cuerpo de descomposición K^D y el cuerpo de inercia K^I de la siguiente manera:

Teorema 4.1.8. *Las subextensiones K^D y K^I están caracterizadas por*

1. *K^D es la subextensión más grande tal que $e(\mathfrak{p}^D|p) = f(\mathfrak{p}^D|p) = 1$.*
2. *K^D es la subextensión más chica tal que $\mathfrak{p}$ es el único primo de K arriba de $\mathfrak{p}^D$.*
3. *K^I es la subextensión más grande tal que $e(\mathfrak{p}^I|p) = 1$.*
4. *K^I es la subextensión más chica tal que $\mathfrak{p}$ es totalmente ramificado sobre $\mathfrak{p}^I$.*

Corolario 4.1.9. *Supongamos que $D_\mathfrak{p} \lhd G$, y sea $L \subseteq K$. Entonces p descompone completamente en L si y solo si $L \subseteq K^D$.*

Las siguientes proposiciones permiten hacer razonamientos de inducción en cuerpos compuestos y clausuras normales, respectivamente.

Proposición 4.1.10. *Sean K y L cuerpos de números, y sea p un primo racional.*

1. *Si p no ramifica en K ni en L, entonces p no ramifica en el cuerpo compuesto KL.*
2. *Si p descompone completamente en K y en L, entonces p descompone completamente en el cuerpo compuesto KL.*

Proposición 4.1.11. *Sea K un cuerpo de números, y sea L su clausura normal.*

1. *Si p no ramifica en K, entonces p no ramifica en L.*
2. *Si p descompone completamente en K, entonces p descompone completamente en L.*

4.2 Raíces d-ésimas y reciprocidad

Sea p un primo impar, y consideremos el cuerpo ciclotómico $\mathbb{Q}[\zeta_p]$, cuyo grupo de Galois $\mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q})$ es cíclico de orden $p-1$. Se sigue que para todo $d \mid p-1$ existe una única subextensión $F_d \subseteq \mathbb{Q}[\zeta_p]$ de grado d sobre $\mathbb{Q}$. Además, $F_{d_1} \subseteq F_{d_2} \Leftrightarrow d_1 \mid d_2$.

Teorema 4.2.1. *Sea $q \neq p$ primo impar, y sea $d \mid p-1$. Entonces q es una potencia d-ésima módulo p sii q descompone completamente en F_d.*

Demostración. Sabemos que q descompone en $\mathbb{Q}[\zeta_p]$ como producto de g primos distintos de grado f, donde f es el orden de q módulo p. Por otra parte, como $(\mathbb{Z}/p)^\times$ es cíclico de orden $p-1$, las potencias d-ésimas módulo p son exactamente aquellos elementos cuyo orden es un divisor de $(p-1)/d$. Entonces las siguientes afirmaciones son equivalentes:

$$\begin{aligned} &q \text{ es potencia } d\text{-ésima módulo } p,\\ &f \mid \frac{p-1}{d},\\ &d \mid g,\\ &F_d \subseteq F_g. \end{aligned}$$

Pero F_g es la única subextensión de $\mathbb{Q}[\zeta_p]/\mathbb{Q}$ de grado g, así que es el cuerpo de descomposición de q, y por 4.1.9 la última afirmación es equivalente a que q descomponga completamente en F_d. □

Corolario 4.2.2 (Ley de Reciprocidad Cuadrática)**.** *Sean $q \neq p$ primos racionales impares. Entonces*

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{si } p \equiv 1 \pmod 4 \text{ o si } q \equiv 1 \pmod 4,\\ -\left(\frac{p}{q}\right) & \text{si } p \equiv q \equiv 3 \pmod 4 a. \end{cases}$$

Demostración. $\left(\frac{q}{p}\right) = 1 \overset{4.2.1}{\iff} q$ descompone completamente en $F_2 = \mathbb{Q}[\sqrt{p^*}]$ $\overset{5.2}{\iff} \left(\frac{p^*}{q}\right) = 1$, etc. □

4.3 Cuerpos finitos

Sea $\mathbb{F}$ un cuerpo finito (en 2.5.7 vimos que todo dominio integral finito es un cuerpo). El subcuerpo primo de $\mathbb{F}$, es necesariamente $\mathbb{F}_p := \mathbb{Z}/p$ donde p es el menor entero positivo tal que $\underbrace{1+1+\ldots+1=0}_{p \text{ veces}}$. Es claro que p tiene que ser primo, pues $\mathbb{F}$ no tiene divisores de cero. Se sigue que $\mathbb{F}$ tiene p^f elementos, donde $f = [\mathbb{F} : \mathbb{F}_p]$.

El grupo multiplicativo $\mathbb{F}^\times$ es cíclico, pues lo es cualquier subgrupo finito del grupo multiplicativo de un cuerpo. A saber, sea d el *exponente* de $\mathbb{F}^\times$ (el menor $d > 0$ tal que $x^d = 1$ para todo x). Como $X^d - 1 = 0$ es un polinomio de grado d, tiene a lo sumo d raíces; se sigue que $\mathbb{F}^\times$ es cíclico de orden $d = p^f - 1$.

Todo elemento de $\mathbb{F}$ es raíz del polinomio $X^{p^f} - X$, que es separable (su derivada es -1), y como $\mathbb{F}$ tiene p^f elementos se sigue que $X^{p^f} - X$ descompone totalmente en $\mathbb{F}$. Es decir que $\mathbb{F}$ es el cuerpo de descomposición de $X^{p^f} - X$ sobre $\mathbb{F}_p$, por lo tanto $\mathbb{F}$ es el único cuerpo de orden p^f salvo isomorfismo, y además es Galois sobre $\mathbb{F}_p$.

El *automorfismo de Frobenius* de $\mathbb{F}$ es un automorfismo τ dado por $\tau(x) = x^p$. Hay que verificar que τ es un automorfismo, utilizando el teorema del binomio (ver que τ es uno a uno, por lo tanto también sobreyectivo).

Observar que, como $\mathbb{F}^\times$ es cíclico de orden $p^f - 1$, se sigue que τ^f es la identidad pero ninguna otra potencia de τ lo es. En otras palabras, τ genera un grupo cíclico de orden f. En particular $\mathbb{F}$ tiene al menos f automorfismos diferentes, pero $[\mathbb{F} : \mathbb{F}_p] = f$; entonces $\mathbb{F}/\mathbb{F}_p$ es Galois, con grupo de Galois cíclico generado por τ. Una consecuencia de esto es que para cada $d \mid f$ existe un único subcuerpo de grado d sobre $\mathbb{F}_p$.

4.4 El símbolo de Artin

Como antes, sea K una cuerpo de números normal sobre $\mathbb{Q}$, y supongamos que p es un primo racional no ramificado, y sea $\mathfrak{p} \mid p$. Por 4.1.4 tenemos un isomorfismo canónico $D_\mathfrak{p} \xrightarrow{\sim} \overline{G}$, donde $\overline{G} = \mathrm{Gal}(k_\mathfrak{p}/\mathbb{F}_p)$ es el grupo de Galois de una extensión de grado f de cuerpos finitos; luego $\overline{G}$ es cíclico de orden

f, con el automorfismo de Frobenius como generador canónico. Entonces tenemos

Proposición 4.4.1. *Existe un único automorfismo $\sigma = \sigma_\mathfrak{p} \in G$ tal que*

$$\sigma(\alpha) \equiv \alpha^p \pmod{\mathfrak{p}},$$

para todo $\alpha \in \mathcal{O}_K$.

El automorfismo $\sigma_\mathfrak{p}$ del lema se llama *automorfismo de Frobenius* en $\mathfrak{p}$. Es un generador canónico del grupo de descomposición $D_\mathfrak{p}$, y lo denotaremos $\left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right]$.

Proposición 4.4.2. *Sea $\sigma\mathfrak{p}$ otro primo arriba de p. Entonces*

$$D_{\sigma\mathfrak{p}} = \sigma D_\mathfrak{p} \sigma^{-1}, \qquad y \qquad \left[\frac{K/\mathbb{Q}}{\sigma\mathfrak{p}}\right] = \sigma \left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right] \sigma^{-1}.$$

Concluimos que, si bien el automorfismo de Frobenius varía con $\mathfrak{p}$, su clase de conjugación no.

Definición 4.4.3. El *símbolo de Artin*

$$\left(\frac{K/\mathbb{Q}}{p}\right)$$

es la clase de conjugación de $\left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right]$ para cualquier $\mathfrak{p} \mid p$.

La clase de conjugación $\left(\frac{K/\mathbb{Q}}{p}\right)$ tiene una gran relación con la forma de la descomposición de p en K. Por ejemplo, si K es un cuerpo cuadrático, ya hemos visto que $\left(\frac{K/\mathbb{Q}}{p}\right)$ es trivial si p descompone y no trivial si p es inerte. Más en general

Proposición 4.4.4. *Sea $K/\mathbb{Q}$ normal, y sea p un primo racional. Entonces p descompone completamente en K sii $\left(\frac{K/\mathbb{Q}}{p}\right) = 1$.*

Demostración. $\left(\frac{K/\mathbb{Q}}{p}\right) = 1$ es equivalente a $D_\mathfrak{p} = 1$ para todo $\mathfrak{p} \mid p$; en otras palabras $K^D = K$ y por lo tanto p descompone completamente en K. □

En los ejercicios 51, 52 se estudia la relación entre $\left(\frac{K/QQ}{p}\right)$ y la descomposición de p en cuerpos cúbicos, y en los ejercicios 53, 56, 57, es necesario entender dicha relación en el caso de cuerpos de grado 4 y 5, dependiendo del grupo de Galois de la clausura normal.

Uno de los temas centrales en la Teoría de Cuerpos de Clases es entender el mapa

$$\{\text{ideales primos no ramificados}\} \longrightarrow G$$

dado por el símbolo de Artin, llamado *mapa de reciprocidad de Artin*. En particular se trata de entender su imágen y núcleo, y encontrar extensiones especiales (*cuerpos de clases*) donde dicho mapa tenga propiedades particularmente importantes que permitan relacionar el grupo de Galois G con el grupo de clases de ideales, etc.

Como muestra enunciaremos (sin demostración) un teorema muy importante que explica la imágen del mapa de reciprocidad de Artin.

Teorema 4.4.5 (Cebotarev)**.** *Sea $K/\mathbb{Q}$ normal, y sea $\langle\sigma\rangle$ la clase de conjugación de $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Entonces $\left(\frac{K/\mathbb{Q}}{p}\right) = \langle\sigma\rangle$ para infinitos primos racionales p. Más aún,*

$$S = S_\sigma := \left\{p \ : \ \left(\frac{K/\mathbb{Q}}{p}\right) = \langle\sigma\rangle\right\},$$

entonces S tiene densidad de Dirichlet

$$\frac{\#\langle\sigma\rangle}{\#\,\mathrm{Gal}(K/\mathbb{Q})}.$$

Corolario 4.4.6. *La densidad de los primos racionales p que descomponen completamente en K es $1/[K:\mathbb{Q}]$.*

Interpretemos el Teorema de Cebotarev en el caso de cuerpos ciclotómicos. Si $K = K_m$ es el m-ésimo cuerpo ciclotómico, entonces $\mathrm{Gal}(K_m/\mathbb{Q}) = (\mathbb{Z}/m)^\times$, y el símbolo de Artin $\left(\frac{K_m/\mathbb{Q}}{p}\right)$ no es más que $p \bmod m$. Entonces el Teorema de Cebotarev dice que, dado $a \in (\mathbb{Z}/m)^\times$, los primos racionales $p \equiv a \pmod m$ son infinitos y tienen densidad $1/\varphi(m)$. En otras palabras, el Teorema de Cebotarev es una generalización del Teorema de Dirichlet de primos en progresiones aritméticas.