Introducción a los Números Algebraicos

Clase 11: Descomposición e inercia

Gonzalo Tornaría

24 de abril, 2007

4 Descomposición e inercia

4.1 Grupo de descomposición y grupo de inercia

Sea K un cuerpo de números de grado n, y asumamos que $K/\mathbb{Q}$ es normal. En tal caso denotaremos $G = \mathrm{Gal}(K/\mathbb{Q})$ su grupo de Galois. Sea p un primo racional, y fijemos $\mathfrak{p}$ un primo de K sobre p. Recordemos que, por tratarse de una extensión normal, $e = e(\mathfrak{p}|p)$ y $f = f(\mathfrak{p}|p)$ son independientes de $\mathfrak{p}$ (3.5.7), y tenemos $n = efg$ donde g es el número de distintos primos de K sobre p (3.5.3).

Definición 4.1.1. El *grupo de descomposición* de $\mathfrak{p}$ es

$$D_\mathfrak{p} := \{\sigma \in G \;:\; \sigma\mathfrak{p} = \mathfrak{p}\}.$$

El *grupo de inercia* de $\mathfrak{p}$ es

$$I_\mathfrak{p} := \{\sigma \in G \;:\; \sigma\alpha \equiv \alpha \pmod{\mathfrak{p}} \quad \forall\alpha \in \mathcal{O}_K\}.$$

Como G actúa transitivamente en los g ideales primos sobre p (3.5.6), se sigue que $[G : D_\mathfrak{p}] = g$, o lo que es lo mismo, $\#D_\mathfrak{p} = ef$. En efecto, hay una correspondencia biyectiva entre las coclases de $D_\mathfrak{p}$ y los ideales primos sobre p dada por $\sigma D_\mathfrak{p} \mapsto \sigma\mathfrak{p}$ (verificar que es una biyección).

Denotaremos $k_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$ al *cuerpo residual* en $\mathfrak{p}$, que es una extensión de grado f sobre $\mathbb{F}_p := \mathbb{Z}/p$. Como los automorfismos $\sigma \in D_\mathfrak{p}$ dejan fijo $\mathfrak{p}$, hay un mapa natural

$$D_\mathfrak{p} \longrightarrow \overline{G} := \mathrm{Gal}(k_\mathfrak{p}/\mathbb{F}_p),$$

cuyo núcleo es justamente $I_\mathfrak{p}$ (es fácil ver que $I_\mathfrak{p} \subseteq D_\mathfrak{p}$). En particular $I_\mathfrak{p} \lhd D_\mathfrak{p}$.

Se sigue que $D_\mathfrak{p}/I_\mathfrak{p}$ es isomorfo a un subgrupo de $\overline{G}$. Veremos que, en efecto $D_\mathfrak{p}/I_\mathfrak{p} \cong \overline{G}$; equivalentemente, dado que $\#\overline{G} = f$, que $\#I_\mathfrak{p} = e$.

Extensiones relativas

Hasta ahora hemos trabajado con cuerpos de números pensados como extensiones de $\mathbb{Q}$. Resulta natural extender la teoría de normas y trazas, bases enteras, discriminantes, descomposición de primos, etc. al caso de extensiones relativas de cuerpos de números K/L. No desarrollaremos la teoría en general, que podría tomarse como un ejercicio (con dificultades técnicas) a partir de la teoría para extensiones de $\mathbb{Q}$, pero veremos algunas definiciones y un pequeño resultado que nos serán de utilidad.

Sea K/L una extensión de cuerpos de números, y sean $\mathfrak{p} \mid \mathfrak{q}$ primos de $\mathcal{O}_K$ y $\mathcal{O}_L$ respectivamente (necesariamente $\mathfrak{q} = \mathfrak{p} \cap L$). Podemos estudiar la factorización de $\mathfrak{q}$ en $\mathcal{O}_K$ (en realidad, se trata de la factorización de $\mathfrak{q}\mathcal{O}_K$, para que sea ideal de $\mathcal{O}_K$).

El exponente de $\mathfrak{p}$ en dicha descomposición será el *índice de ramificación* de $\mathfrak{p}$ sobre $\mathfrak{q}$, denotado $e(\mathfrak{p}|\mathfrak{q})$. Por otra parte, existe una extensión natural de los cuerpos residuales $k_\mathfrak{p}/k_\mathfrak{q}$ (donde $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ y $k_\mathfrak{q} = \mathcal{O}_L/\mathfrak{q}$). El grado de dicha extensión será el *grado de inercia* o *grado residual* de $\mathfrak{p}$ sobre $\mathfrak{q}$, denotado $f(\mathfrak{p}|\mathfrak{q})$. Notar que $N(\mathfrak{p}) = N(\mathfrak{q})^f$.

Proposición 4.1.2. *Sea $K/L/M$ una torre de cuerpos, y sean $\mathfrak{p}|\mathfrak{q}|\mathfrak{r}$ respectivos primos. Entonces*

$$e(\mathfrak{p}|\mathfrak{r}) = e(\mathfrak{p}|\mathfrak{q})\,e(\mathfrak{q}|\mathfrak{r}), \qquad y \qquad f(\mathfrak{p}|\mathfrak{r}) = f(\mathfrak{p}|\mathfrak{q})\,f(\mathfrak{q}|\mathfrak{r}).$$

Demostración. Para la primer parte, escribir $\mathfrak{r} = \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{r})}\cdots$, y $\mathfrak{q} = \mathfrak{p}^{e(\mathfrak{p}|\mathfrak{q})}\cdots$, sustituir, y usar factorización única para concluir que $\mathfrak{r} = \mathfrak{p}^{e(\mathfrak{p}|\mathfrak{q})e(\mathfrak{q}|\mathfrak{r})}\cdots$.

Para la segunda parte, observar que hay una torre de cuerpos residuales $k_\mathfrak{p}/k_\mathfrak{q}/k_\mathfrak{r}$ y usar la correspondiente propiedad del grado en torres. $\square$

Ahora volvemos a los grupos de descomposición e inercia. Denotemos K^I al cuerpo fijo por $I_\mathfrak{p}$, y K^D al cuerpo fijo por $D_\mathfrak{p}$ (ambos dependen de $\mathfrak{p}$, aunque la notación no lo indique), y denotemos $\mathfrak{p}^I := \mathfrak{p} \cap K^I$, y $\mathfrak{p}^D := \mathfrak{p} \cap K^D$. Entonces tenemos una torre de cuerpos $K/K^I/K^D/\mathbb{Q}$, con correspondientes ideales primos $\mathfrak{p} \mid \mathfrak{p}^I \mid \mathfrak{p}^D \mid p$.

Teorema 4.1.3. *Los grados de las extensiones en la torre $K/K^I/K^D/\mathbb{Q}$ son $[K:K^I]=e$, $[K^I:K^D]=f$, y $[K^D:\mathbb{Q}]=g$. Además, $\mathfrak{p}|\mathfrak{p}^I$ es totalmente ramificado, y $\mathfrak{p}^I|\mathfrak{p}^D$ es inerte.*

Demostración. Ya observamos que $[G:D_\mathfrak{p}]=g$, de modo que $[K^D:\mathbb{Q}]=g$. Además, como $D_\mathfrak{p}=\mathrm{Gal}(K/K^D)$ deja fijo $\mathfrak{p}$ se sigue que $\mathfrak{p}$ es el único primo de K arriba de $\mathfrak{p}^D$, y por lo tanto $e(\mathfrak{p}|\mathfrak{p}^D)=e$, $f(\mathfrak{p}|\mathfrak{p}^D)=f$.

Para terminar la demostración consideremos $k_\mathfrak{p}:=\mathcal{O}_K/\mathfrak{p}$ como extensión de $k_{\mathfrak{p}^I}:=\mathcal{O}_{K^I}/\mathfrak{p}^I$ de grado $f(\mathfrak{p}|\mathfrak{p}^I)$. Necesitamos probar que dicha extensión es trivial, pues esto implica que $f(\mathfrak{p}|\mathfrak{p}^I)=1\Rightarrow f(\mathfrak{p}^I|\mathfrak{p}^D)=f$, luego $\#(D_\mathfrak{p}/I_\mathfrak{p})=[K^D:K^I]\geq f$, pero como $D_\mathfrak{p}/I_\mathfrak{p}\hookrightarrow\overline{G}$, que tiene orden f, se sigue que . $\#(D_\mathfrak{p}/I_\mathfrak{p})=[K^D:K^I]=f$, y $e(\mathfrak{p}^I|\mathfrak{p}^D)=1\Rightarrow e(\mathfrak{p}|\mathfrak{p}^I)=e$.

Sea entonces $\alpha\in\mathcal{O}_K$, y consideremos $g(X)=\prod_{\sigma\in I}(X-\sigma\alpha)$, que tiene coeficientes en $\mathcal{O}_{K^I}$ y anula α. Reduciendo módulo $\mathfrak{p}$ tenemos la factorización $\overline{g}=(X-\overline{\alpha})^{\#I_\mathfrak{p}}$ en $k_\mathfrak{p}$, y como $k_\mathfrak{p}/k_{\mathfrak{p}^I}$ es separable (cuerpos finitos son perfectos) se sigue que $\overline{\alpha}\in k_{\mathfrak{p}^I}$. □

Corolario 4.1.4. *El mapa natural $D_\mathfrak{p}\to\overline{G}$ induce un isomorfismo*

$$D_\mathfrak{p}/I_\mathfrak{p}\xrightarrow{\sim}\overline{G}.$$

Demostración. Es un mapa inyectivo entre grupos de igual orden. □

Corolario 4.1.5. *Supongamos que $D_\mathfrak{p}\lhd G$. Entonces p descompone completamente en K^D.*

Demostración. Pues $e(\mathfrak{p}^D|p)=f(\mathfrak{p}^I|p)=1$, y como $D_\mathfrak{p}\lhd G$ lo mismo vale para cualquier primo arriba de p (pues $D_\mathfrak{p}$ es siempre el mismo). □

Ejemplo 4.1.6. $\mathbb{Q}[\sqrt{-23}]\subseteq K_{23}$, $p=2$. Sabemos que p descompone en $\mathbb{Q}[\sqrt{-23}]$ como producto de dos primos de grado 1, pues $\left(\frac{-23}{2}\right)=1$.

Otra forma de verlo es observar que $2 \bmod 23$ tiene orden 11 (el orden divide a 22, y $\left(\frac{2}{23}\right)=1$, se sigue que el orden es 1 o 11). Entonces $2=\mathfrak{p}_1\mathfrak{p}_2$ en K_{23}, donde $\mathfrak{p}_i$ son primos de grado 11. Por lo tanto $D_{\mathfrak{p}_1}=D_{\mathfrak{p}_2}$ es el único subgrupo de $(\mathbb{Z}/23)^\times$ de índice 2, y $K_D=\mathbb{Q}[\sqrt{-23}]$.

Ejemplo 4.1.7. $K=\mathbb{Q}[i,\sqrt{2},\sqrt{5}]$, de grado 8 normal sobre $\mathbb{Q}$, con grupo de Galois $G\cong(\mathbb{Z}/2)^3$, donde los automorfismos están dados por

$$i,\sqrt{2},\sqrt{5}\mapsto\pm i,\pm\sqrt{2},\pm\sqrt{5}.$$

Consideramos $p=5$. Conocemos la descomposición de p en cuerpos cuadráticos, a saber:

- p descompone en $\mathbb{Q}[\sqrt{i}]$ pues $\left(\frac{-1}{5}\right)=1$,
- p es inerte en $\mathbb{Q}[\sqrt{2}]$ pues $\left(\frac{2}{5}\right)=-1$,
- p ramifica en $\mathbb{Q}[\sqrt{5}]$.

Entonces, en K, necesariamente p descompone con $e=f=g=2$. Ahora es claro que $K^D=\mathbb{Q}[i]$ (pues es un cuerpo intermedio de grado $g=2$ en el que p descompone completamente) y K^I (pues es un cuerpo intermedio de grado $fg=2$ donde 5 no ramifica).

Ejemplo 4.1.8. $K=\mathbb{Q}[\alpha,\zeta_3]$, con $\alpha=\sqrt[3]{19}$, normal sobre $\mathbb{Q}$, grupo de Galois $G\cong S_3$ que actúa como permutaciones del conjunto $\{\alpha,\zeta_3\alpha,\zeta_3^2\alpha\}$ de raíces de X^3-19. Consideremos $p=3$. Sabemos que $(p)=(1-\zeta_3)^2$ en $\mathbb{Q}[\zeta_3]$, y puede verse que $(p)=\mathfrak{p}^2\mathfrak{q}$ en $\mathbb{Q}[\alpha]$, donde $\mathfrak{p}=(3,\beta)$, $\mathfrak{q}=(3,\beta-1)$, con $\beta=\frac{1+\alpha+\alpha^2}{3}\in\mathcal{O}_K$.

Entonces, en K, necesariamente la descomposición de p tiene e par, y $g\geq2$, luego $e=2$, $g=3$, $f=1$, y se tiene $\mathfrak{p}=\mathfrak{p}_1\mathfrak{p}_2$ y $\mathfrak{q}=\mathfrak{p}_3^2$, con $(1-\zeta_3)=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

Luego $\#D_{\mathfrak{p}_i}=ef=2$, generado por un automorfismo que deja fijo $\mathfrak{p}_i$ e intercambia los otros primos de K arriba de p. Entonces $K^D=K^I$ es un cuerpo de grado 3 sobre $\mathbb{Q}$, para cada $\mathfrak{p}_i$, pero son todos distintos.

Además, se ve que (3) no descompone completamente en ninguno de los K^D. Por ejemplo, el cuerpo de descomposición correspondiente a $\mathfrak{p}_3$ es $\mathbb{Q}[\alpha]$, por cuanto el automorfismo de K no trivial que fija $\mathbb{Q}[\alpha]$ deja fijo $\mathfrak{q}$ (por ser primo de $\mathbb{Q}[\alpha]$) y por lo tanto deja fijo $\mathfrak{p}_3$ también. A posteriori, se ve que el mismo automorfismo intercambia $\mathfrak{p}_1$ y $\mathfrak{p}_2$.