RAMIFICACIÓN

FERNANDA CARES

El objetivo de esta sección es comprender algunos hechos y conceptos de la teoría algebraica de números para utilizarlos como herramienta para las siguientes secciones. Esta sección está basada en el capítulo 5, sección A del libro de Cox [Cox13] y resultados de los capítulos 2, 3 y 4 del libro de Marcus [Mar18].

1. Cuerpos de Números

Definición 1.1. Un cuerpo de números K es un subcuerpo de los números complejos que tiene grado finito sobre $\mathbb{Q}$. Denotamos como $[K:\mathbb{Q}]$ el grado de K como espacio vectorial sobre $\mathbb{Q}$.

Denotaremos como $\mathcal{O}_K$ al conjunto de enteros algebraicos de K, es decir, el conjunto de elementos de K tales que son raíz de un polinomio mónico con coeficientes enteros.

Teorema 1.2. *Sea K un cuerpo de números.*

1. *$\mathcal{O}_K$ es un subanillo de $\mathbb{C}$ con cuerpo de fracciones K.*
2. *$\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre de rango $[K:\mathbb{Q}]$.*

La demostración de 1. es consecuencia de la siguiente proposición:

Proposición 1.3. *Los siguientes son equivalentes para $\alpha \in \mathbb{C}$:*

1. *α es entero algebraico.*
2. *El grupo aditivo del anillo $\mathbb{Z}[\alpha]$ es finitamente generado.*
3. *α está en algún subanillo de $\mathbb{C}$ con grupo aditivo finitamente generado.*

Demostración: [de la Proposición 1.3] Si α es entero algebraico entonces es raíz de un polinomio $a_0 + a_1x + ... + a_{n-1}x^{n-1} + x^n$. Así $\alpha^n = -a_0 - a_1\alpha - a_{n-1}\alpha^{n-1}$ y el grupo aditivo del anillo $\mathbb{Z}[\alpha]$ está generado por $\{1, \alpha, ..., \alpha^{n-1}\}$.

Para 2. implica 3. tomamos el subanilo $\mathbb{Z}[\alpha]$ que está finitamente generado y en el que está α.

Para 3. implica 1., llamemos C el subanillo de $\mathbb{C}$ con grupo aditivo finitamente generado. Así C es un $\mathbb{Z}$-módulo finitamente generado y consideramos el endomofismo de C (como $\mathbb{Z}$-módulo) $\phi(x) = \alpha x$, tenemos que cumple una ecuación de forma:

$$\phi^n + a_{n-1}\phi^{n-1} + ... + a_0 = 0$$

con $a_i \in \mathbb{Z}$. Evaluando en 1, obtenemos que:

$$\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_0 = 0.$$

Así que α es entero algebraico.

□

Para el item 2. del Teorema 1.2 podemos encontrar una demostración en [Mar18] (Theorem 9).

Ahora ya podemos definir $\mathcal{O}_K$ de la siguiente manera:

Definición 1.4. Le llamaremos a $\mathcal{O}_K$ el anillo de números de K.

Los siguientes resultados ya los teníamos para el caso cuadrático en CM3, pero se pueden generalizar:

Corolario 1.5. *Si K es un cuerpo de números y $\mathfrak{a}$ es un ideal no cero de $\mathcal{O}_K$, entonces el anillo cuociente $\mathcal{O}_K/\mathfrak{a}$ es finito.*

Demostración: Si $\mathfrak{a}$ es ideal no cero, entonces existe $m \in \mathbb{Z}$ no cero en $\mathfrak{a}$. En efecto, sea $\alpha \in \mathfrak{a}$ no cero, como $\alpha \in \mathcal{O}_K$ consideramos su polinomio minimal. Al evualuar en α obtenemos: $\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_0 = 0$ para algunos enteros a_i. Como α está en el ideal $\mathfrak{a}$, tenemos que $a_0 \in \mathfrak{a}$. Así a_0 es un entero en $\mathfrak{a}$ y no cero por minimalidad. Por lo tanto, para $m = a_0$, tenemos que $m\mathcal{O}_K \subseteq \mathfrak{a}$.

Al igual que en la demostración del Lema 2.3 del CM3 tenemos que hay homomorfismo sobreyectivo $\mathcal{O}_K/m\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}$, así que basta demostrar que $\mathcal{O}_K/m\mathcal{O}_K$ es finito. De hecho, si $\{\alpha_1, ..., \alpha_n\}$ es base de $\mathcal{O}_K$ como $\mathbb{Z}$-módulo (existe y es finita por 1.2), tenemos que un conjunto de representantes de $\mathcal{O}_K/m\mathcal{O}_K$ sería

$$\{\alpha_1 x_1 + ... + \alpha_n x_n : 0 \leq x_i < m \text{ enteros}\},$$

así $|\mathcal{O}_K/m\mathcal{O}_K| = m^n$ así que es finito. □

Definición 1.6. Dado un ideal no cero $\mathfrak{a}$ de $\mathcal{O}_K$, su norma se define como $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$ y es finita por el Corolario 1.5.

De hecho en la demostración anterior ya calculamos una norma:

Ejemplo 1.7. Sea m un entero no cero, tenemos que $N(m\mathcal{O}_K) = m^n$ donde $n = [K : \mathbb{Q}]$.

Queremos hablar de factorización en $\mathcal{O}_K$ por lo que nos gustaría que fueran dominios de factorización única, sin embargo sabemos que por ejemplo $\mathbb{Z}[\sqrt{-5}]$ no es DFU y es el anillo de enteros de $\mathbb{Q}[\sqrt{-5}]$.

Aún así tenemos una condición que nos permite hablar de factorización:

Teorema 1.8. *Sea $\mathcal{O}_K$ el anillo de números de K. Entonces $\mathcal{O}_K$ es un Dominio de Dedekind, es decir cumple:*

1. *$\mathcal{O}_K$ es integralmente cerrado en K, es decir, si $\alpha \in K$ es raíz de un polinomio mónico con coeficientes en $\mathcal{O}_K$, entonces $\alpha \in \mathcal{O}_K$.*
2. *$\mathcal{O}_K$ es Noetheriano.*
3. *Todo ideal primo no nulo de $\mathcal{O}_K$ es maximal.*

Demostración:

1. Sea $\alpha \in K$ tal que $\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0$ para algunos $a_i \in \mathcal{O}_K$. Por Proposición 1.3 el grupo aditivo de $\mathbb{Z}[a_i]$ es finitamente generado para todo $i = 0, 1, ..., n-1$.
   Luego, como
   $$-\alpha^n = a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0,$$
   tenemos que el grupo aditivo de $\mathbb{Z}[a_0, a_1, ..., a_{n-1}, \alpha]$ es finitamente generado. De hecho está generado por los productos de la forma:
   $$a_0^{m_0} \cdots a_{n-1}^{m_{n-1}} \alpha^{m_n}$$
   donde los m_i varían entre 0 y el grado del polinomio minimal de a_i (sin considerar este último) y $m \in \{0, 1, ..., n-1\}$.
   Luego, como $\alpha \in \mathbb{Z}[a_0, a_1, ..., a_{n-1}, \alpha]$ que tiene grupo aditivo finitamente generado, concluímos por Propiedad 1.3 que α es entero algebraico y así está en $\mathcal{O}_K$.
2. Es exactamente la misma de la Proposición 2.1 del CM3 (dado que es consecuecia del mismo hecho: $\mathcal{O}_K/\mathfrak{a}$ es finito para todo ideal $\mathfrak{a}$ no nulo de $\mathcal{O}_K$).
3. Sea $\mathfrak{p}$ un ideal primo no nulo de $\mathcal{O}_K$, tenemos que $O_k/\mathfrak{p}$ es un dominio y es finito por el Corolario 1.5, por lo tanto es cuerpo y $\mathfrak{p}$ es maximal.

□

Como consecuencia de ser un dominio de Dedekind tenemos lo siguiente:

Corolario 1.9. *Si K es un cuerpo de números, todo ideal no cero $\mathfrak{a}$ de $\mathcal{O}_K$ se puede escribir como producto de ideales primos, es decir,*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

Esta descomposición es única salvo orden. Más aún, los $\mathfrak{p}_i$ son los ideales primos de $\mathcal{O}_K$ conteniendo a $\mathfrak{a}$.

De ahora en adelante podemos usar el termino "primo de K" para referirnos a un ideal primo no nulo de $\mathcal{O}_K$.

Definición 1.10. Si $\mathfrak{p}$ es primo de K, el cuerpo residual de $\mathfrak{p}$ es el anillo cuociente $\mathcal{O}_K/\mathfrak{p}$.

Esta definición tiene sentido por el punto 3 del Teorema 1.8.

Definición 1.11. Un ideal fraccional de $\mathcal{O}_K$ es un $\mathcal{O}_K$-submódulo de K no cero y finitamente generado.

Algunas propiedades básicas de los ideales fraccionales son:

Proposición 1.12. *Sea $\mathfrak{a}$ un ideal fraccional de $\mathcal{O}_K$.*

1. *$\mathfrak{a}$ es invertible, es decir, existe un ideal fraccional de $\mathcal{O}_K$ $\mathfrak{b}$ tal que $\mathfrak{ab} = \mathcal{O}_K$.*
2. *$\mathfrak{a}$ puede escribirse de manera única como un producto $\prod_{i=1}^{r} \mathfrak{p}_i^{r_i}$ con r_i enteros, tal que los $\mathfrak{p}_i$ son distintos ideales primos de $\mathcal{O}_K$.*

Al igual que en el caso cuadrático:

Proposición 1.13. *Sea I_K el conjunto de todos los ideales fraccionales, es cerrado bajo multiplicación de ideales y es grupo por la Proposición 1.12.*
El conjunto de ideales principales, denotado P_K, es subgrupo de I_k y I_K/P_K es finito.

Definición 1.14. El cuociente P_K/O_K es el grupo de clases de ideales y se denota $C(\mathcal{O}_K)$.

2. Descomposición Prima de ideales

Definición 2.1. Sea K un cuerpo de números y L una extensión finita de K. Si $\mathfrak{p}$ es ideal primo de $\mathcal{O}_K$, entonces $p\mathcal{O}_L$ es ideal de $\mathcal{O}_L$. Por Corolario 1.9, tenemos que existe descomposición:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_g^{e_g}, \tag{2.1}$$

donde los $\mathfrak{B}_i$ son primos distintos de L conteniendo a $\mathfrak{p}$.
El entero e_i es llamado el índice de ramificación de $\mathfrak{p}$ en $\mathfrak{B}_i$ y lo podemos denotar $e_{\mathfrak{B}_i|\mathfrak{p}}$.
Cada primo $\mathfrak{B}_i$ nos da una extensión del cuerpo residual $\mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_L/\mathfrak{B}_i$, el grado de la extensión es denominado el grado inercial de $\mathfrak{p}$ en $\mathfrak{B}_i$ y se denota f_i o $f_{\mathfrak{B}_i|\mathfrak{p}}$.
Además se dice que el primo $\mathfrak{B}_i$ está sobre $\mathfrak{p}$ o que $\mathfrak{p}$ está bajo $\mathfrak{B}_i$, pues $\mathfrak{B}_i$ aparece en la descomposición de $\mathfrak{p}\mathcal{O}_L$.

Tenemos relación entre los e_i y los f_i:

Teorema 2.2. *Sea $K \subseteq L$ cuerpos de números y $\mathfrak{p}$ un primo de K. Sean e_i los índices de ramificación y f_i los grados inerciales para $i = 1, ..., g$, entonces:*

$$\sum_{i=1}^{g} e_i f_i = [L : K].$$

Demostraremos para el caso $K = \mathbb{Q}$ para tener una idea más concreta basándonos en [IR82], para una demostración en el caso general se puede consultar el Teorema 21 del capítulo 3 de [Mar18].
Antes de demostrar el teorema nos será de utilidad el siguiente lema:

Lema 2.3. *Sea $\mathfrak{B}$ primo de L y supongamos que $\mathcal{O}_L/\mathfrak{B}$ tiene p^f elementos para un primo entero p. Entonces $\mathcal{O}_L/\mathfrak{B}^e$ tiene p^{ef} elementos.*

Demostración: [del Lema 2.3] La realizaremos por inducción sobre e.
Si $e = 1$ se verifica por hipótesis. Supongamos que se verifica para $e-1$ y demostremos para e:
Tenemos que $\mathfrak{B}^e \subseteq \mathfrak{B}^{e-1}$, así que por teorema de isomorfismo:

$$(\mathcal{O}_L/\mathfrak{B}^e)/(\mathfrak{B}^{e-1}/\mathfrak{B}^e) \cong \mathcal{O}_L/\mathfrak{B}^{e-1}.$$

Por hipótesis inductiva el cuociente de la derecha tiene $p^{f(e-1)}$ elementos, así que basta demostrar que $\mathfrak{B}^{e-1}/\mathfrak{B}^e$ tiene p^f elementos.
En primer lugar, tenemos que $\mathfrak{B}^e \subsetneq \mathfrak{B}^{e-1}$ así que tomemos $\alpha \in \mathfrak{B}^{e-1}$ tal que $\alpha \notin \mathfrak{B}^e$. Vamos a demostrar que $(\alpha) + \mathfrak{B}^e = \mathfrak{B}^{e-1}$.
De hecho, como $\mathfrak{B}^e \subseteq (\alpha) + \mathfrak{B}^e$, tenemos que este último tiene que ser potencia de $\mathfrak{B}$ (por descomposición en primos). Además tenemos que $(\alpha) + \mathfrak{B}^e \subseteq \mathfrak{B}^{e-1}$, así que $(\alpha) + \mathfrak{B}^e = \mathfrak{B}^{e-1}$.
Con esto podemos definir un homomorfismo sobreyectivo:

$$\mathcal{O}_L \longrightarrow \mathfrak{B}^{e-1}/\mathfrak{B}^e$$
$$\gamma \longmapsto \gamma\alpha + \mathfrak{B}^e$$

El kernel de este homomorfismo es

$$\{\gamma \in \mathcal{O}_L : \gamma\alpha + \mathfrak{B}^e = \mathfrak{B}^e\} = \{\gamma \in \mathcal{O}_L : \gamma\alpha \in \mathfrak{B}^e\} = \{\gamma \in \mathcal{O}_L : \gamma \in \mathfrak{B}\} = \mathfrak{B},$$

donde en la penúltima igualdad usamos que $\alpha \in \mathfrak{B}^{e-1}$ pero $\alpha \notin \mathfrak{B}^e$.

Así tenemos que induce un isomorfismo entre $\mathcal{O}_L/\mathfrak{B}$ y $\mathfrak{B}^{e-1}/\mathfrak{B}^e$, así que este último tiene p^f elementos por hipotesis. □

Demostración: [del Teorema 2.2]

En nuestro caso un primo de $K = \mathbb{Q}$ es uno de la forma (p) para un número p primo. Consideremos la descomposición de $(p)\mathcal{O}_L$ en primos de L:

$$(p)\mathcal{O}_L = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_g^{e_g}$$

donde los $\mathfrak{B}_i$ contienen a (p).

Se tiene que para $i \neq j$, $\mathfrak{B}_i^{e_i} + \mathfrak{B}_j^{e_j} = \mathcal{O}_L$, así que usando teorema chino del resto tenemos:

$$\mathcal{O}_L/(p)\mathcal{O}_L \cong (\mathcal{O}_L/\mathfrak{B}_1^{e_1}) \times ... \times (\mathcal{O}_L/\mathfrak{B}_g^{e_g}).$$

Por un lado, en el cuociente de la izquierda hay p^n elementos donde $n = [L : \mathbb{Q}]$ por el ejemplo 1.7.

Por otro lado, cada $\mathcal{O}_L/\mathfrak{B}_i$ tiene dimensión f_i como espacio vectorial sobre $\mathcal{O}_K/(p) = \mathbb{Z}/p\mathbb{Z}$, así tiene p^{f_i} elementos. Por el lema 2.3 tenemos que $\mathcal{O}_L/\mathfrak{B}_i^{e_i}$ tiene $p^{f_i e_i}$ elementos.

Igualando cardinalidades, tenemos:

$$p^n = p^{e_1 f_1} \cdots p^{e_g f_g} = p^{\sum_{i=1}^g e_i f_i}.$$

Así concluímos lo pedido.

□

La siguiente definición le da el nombre a la sección:

Definición 2.4. Un primo $\mathfrak{p}$ de K ramifica en L si alguno de sus índices de ramificación e_i es mayor que 1.

3. Teoría de Galois aplicada a descomposición prima

Cuando trabajamos en extensiones de Galois tenemos propiedades más interesantes:

Teorema 3.1. *Sea $K \subseteq L$ una extensión de Galois y $\mathfrak{p}$ un primo de K.*

1. *El grupo de Galois $\mathrm{Gal}(L/K)$ actúa transitivamente en los primos de L conteniendo a $\mathfrak{p}$, es decir, si $\mathfrak{B}$ y $\mathfrak{B}'$ son primos de L conteniendo a $\mathfrak{p}$, entonces existe un $\sigma \in \mathrm{Gal}(L/K)$ tal que $\sigma(\mathfrak{B}) = \mathfrak{B}'$.*
2. *Los primos $\mathfrak{B}_1, ..., \mathfrak{B}_g$ de L conteniendo a $\mathfrak{p}$ tiene todos el mismo índice de ramificación e y grado inercial f. Así la fórmula del teorema 2.2 se transforma en*

$$efg = [L : K].$$

Una demostración de este Teorema se puede encontrar en el Teorema 23 de [Mar18].

Observación 3.2. En el caso Galois, un primo $\mathfrak{p}$ de K ramifica si $e > 1$.

Definición 3.3. Un primo $\mathfrak{p}$ de K se escinde en L si $e = f = 1$, o equivalentemente, si $g = [L : K]$.

Hay subgrupos de $\mathrm{Gal}(L/K)$ que será importante estudiar:

Definición 3.4. Sea $K \subseteq L$ una extensión de Galois y $\mathfrak{B}$ un primo de L.

El grupo de descomposición de $\mathfrak{B}$ se define como:

$$D_{\mathfrak{B}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{B}) = \mathfrak{B}\}$$

El grupo de inercia de $\mathfrak{B}$ se define como:

$$I_{\mathfrak{B}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{B}} \text{ para todo } \alpha \in \mathcal{O}_L\}$$

.

Proposición 3.5. *Sean $D_{\mathfrak{B}}, I_{\mathfrak{B}}$ como en la defínción anterior, tenemos:*

1. $I_{\mathfrak{B}} \subseteq D_{\mathfrak{B}}$.
2. *Todo elemento $\sigma \in D_{\mathfrak{B}}$ induce un automorfismo $\tilde{\sigma}$ de $\mathcal{O}_L/\mathfrak{B}$ que es la identidad en $\mathcal{O}_K/\mathfrak{p}$ donde $\mathfrak{p} = \mathfrak{B} \cap \mathcal{O}_K$.*
3. *Sea $\tilde{G} = \mathrm{Gal}((\mathcal{O}_L/\mathfrak{B})/(\mathcal{O}_K/\mathfrak{p}))$, tenemos que $\tilde{\sigma} \in \tilde{G}$ y la función $\sigma \mapsto \tilde{\sigma}$ define un homomorfismo $D_{\mathfrak{B}} \longrightarrow \tilde{G}$ cuyo kernel es $I_{\mathfrak{B}}$.*

Demostración:

1. De la definición de $I_{\mathfrak{B}}$, si $\sigma \in I_{\mathfrak{B}}$ y $\alpha \in \mathfrak{B}$ tenemos que $\sigma(\alpha) \equiv \alpha \equiv 0 \pmod{\mathfrak{B}}$, así $\sigma(\mathfrak{B}) = \mathfrak{B}$ y $\sigma \in D_{\mathfrak{B}}$.
2. Sea $\sigma \in D_{\mathfrak{B}}$, como $\sigma \in \mathrm{Gal}(L/K)$ y las raíces de polinomios mónicos con coeficientes enteros son permutadas por σ, podemos hacer restricción $\hat{\sigma}\colon \mathcal{O}_L \longrightarrow \mathcal{O}_L$.
   Sea $\pi\colon \mathcal{O}_L \longrightarrow \mathcal{O}_L/\mathfrak{B}$ el homomorfismo de proyección, consideremos $\hat{\sigma} \circ \pi$:
   $$\mathcal{O}_L \xrightarrow{\hat{\sigma}} \mathcal{O}_L \xrightarrow{\pi} \mathcal{O}_L/\mathfrak{B},$$
   tenemos que es un homomorfismo sobreyectivo ($\hat{\sigma}$ isomorfismo y π sobreyectivo). Su kernel es:
   $$\{\alpha \in \mathcal{O}_L : \pi \circ \hat{\sigma}(\alpha) = \mathfrak{B}\} = \{\alpha \in \mathcal{O}_L : \sigma(\alpha) \in \mathfrak{B}\} = \mathfrak{B},$$
   donde en la última igualdad usamos que $\sigma \in D_{\mathfrak{B}}$.
   Así induce un isomorfismo $\tilde{\sigma}\colon \mathcal{O}_L/\mathfrak{B} \longrightarrow \mathcal{O}_L/\mathfrak{B}$ tal que $\tilde{\sigma}(\alpha + \mathfrak{B}) = \pi \circ \hat{\sigma}(\alpha)$.
   Como σ fija a K (y por lo tanto a $\mathcal{O}_K$), tenemos que $\tilde{\sigma}$ es la identidad en $\mathcal{O}_K/\mathfrak{p}$.
3. Por 2, $\tilde{\sigma} \in \tilde{G}$. Para ver que es homomorfismo, sean $\sigma, \tau \in D_{\mathfrak{B}}$ notemos que por el siguiente diagrama:
   $$\begin{array}{ccccc} \mathcal{O}_L & \xrightarrow{\hat{\sigma}} & \mathcal{O}_L & \xrightarrow{\hat{\tau}} & \mathcal{O}_L \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{O}_L/\mathfrak{B} & \xrightarrow{\tilde{\sigma}} & \mathcal{O}_L/\mathfrak{B} & \xrightarrow{\tilde{\tau}} & \mathcal{O}_L/\mathfrak{B} \end{array}$$
   tenemos que $(\tau \tilde{\circ} \sigma) = \tilde{\tau} \circ \tilde{\sigma}$.
   Además se tiene que para $\alpha \in \mathcal{O}_L$:
   $$\tilde{\sigma}(\alpha + \mathfrak{B}) = \alpha + \mathfrak{B} \leftrightarrow \hat{\sigma}(\alpha) + \mathfrak{B} = \alpha + \mathfrak{B} \leftrightarrow \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{B}}.$$
   Así, $\tilde{\sigma}$ es la identidad si y solamente si $\sigma \in I_{\mathfrak{B}}$.

□

Con estos preliminares podemos hacer conexión entre las definiciones de la sección anterior (índice de ramificicación y grado inercial) y las definciones recientes:

Teorema 3.6. *Sea $D_{\mathfrak{B}}, I_{\mathfrak{B}}$ y $\tilde{G}$ como en la Proposición 3.5, entonces:*

1. $|I_{\mathfrak{B}}| = e_{\mathfrak{B}|\mathfrak{p}}$ *y* $|D_{\mathfrak{B}}| = e_{\mathfrak{B}|\mathfrak{p}} f_{\mathfrak{B}|\mathfrak{p}}$.
2. *El homomorfismo $D_{\mathfrak{B}} \longrightarrow \tilde{G}$ es sobreyectivo. Entonces $D_{\mathfrak{B}}/I_{\mathfrak{B}} \cong \tilde{G}$.*

Para demostrarlo usaremos los siguientes resultados de libro de Marcus [Mar18] (Theorem 20):

Teorema 3.7. *Todo primo $\mathfrak{B}$ de L está sobre un único primo de K : $\mathfrak{B} \cap \mathcal{O}_K$. Todo primo $\mathfrak{p}$ de K esta bajo al menos un primo de L.*

Proposición 3.8. *Sean $\mathfrak{p} \subseteq \mathfrak{B} \subseteq \mathfrak{Q}$ primos de tres cuerpos de números $K \subseteq L \subseteq F$, entonces:*

$$e_{\mathfrak{Q}|\mathfrak{p}} = e_{\mathfrak{Q}|\mathfrak{B}} e_{\mathfrak{B}|\mathfrak{p}}.$$

Similarmente,

$$f_{\mathfrak{Q}|\mathfrak{p}} = f_{\mathfrak{Q}|\mathfrak{B}} f_{\mathfrak{B}|\mathfrak{p}}.$$

Demostración: [Del Teorema 3.6]

1. Consideremos los cuerpos fijos L^I, L^D de $I_{\mathfrak{B}}$ y $D_{\mathfrak{B}}$, respectivamente.
   Sea H un subgrupo de $\mathrm{Gal}(L/K)$, consideramos $\mathcal{O}_L^H = L^H \cap \mathcal{O}_L$, el anillo de enteros de L^H.
   Tenemos el siguiente diagrama:

$$\begin{array}{ccc} \{e\} & L & \mathcal{O}_L \\ | & | & | \\ I_{\mathfrak{B}} & L^I & (\mathcal{O}_L)^I \\ | & | & | \\ D_{\mathfrak{B}} & L^D & (\mathcal{O}_L)^D \\ | & | & | \\ \mathrm{Gal}(L/K) & K & \mathcal{O}_K \end{array}$$

Donde en la primera columna tenemos subgrupos del grupo $\mathrm{Gal}(L/K)$, en la segunda tenemos sus correspondentes cuerpos fijos y en la tercera los anillos de números de cada cuerpo.

Sea $\mathfrak{B}$ primo de L, para efectos de la demostración denotaremos $D = D_{\mathfrak{B}}$, $I = I_{\mathfrak{B}}$, $e = e_{\mathfrak{B}|\mathfrak{p}}$ y $f = f_{\mathfrak{B}|\mathfrak{p}}$.

Primero notemos que por Teorema 3.7 existe único primo $\mathfrak{B}_I$ de L^I bajo $\mathfrak{B}$, único primo $\mathfrak{B}_D$ de L^D bajo $\mathfrak{B}$ y único primo $\mathfrak{p}$ de K bajo $\mathfrak{B}$, además cumplen

$$\mathfrak{p} \subseteq \mathfrak{B}_D \subseteq \mathfrak{B}_I \subseteq \mathfrak{B}.$$

Demostraremos que $[L^D : K] = g$, donde g es el número de primos de L que aparecen en la descomposición de $\mathfrak{p}\mathcal{O}_L$ (como en 2.1). Por correspondencia de Galois $[L^D : K] = [G : D]$, así basta estudiar las clases laterales de D. Notemos que σ, τ están en la misma clase lateral si y solamente si $\sigma(\mathfrak{B}) = \tau(\mathfrak{B})$ (pues los elementos de D dejan $\mathfrak{B}$ fijo). Así tenemos una correspondencia entre clases laterales de D y posibles imágenes de $\mathfrak{B}$ por elementos de $\mathrm{Gal}(L/K)$. Por 3.1, $\mathrm{Gal}(L/K)$ actúa de manera transitiva en los primos sobre $\mathfrak{p}$, es decir, las posibles imágenes de $\mathfrak{B}$ corresponden exactamente a la cantidad de primos que aparecen en la descomposición de $\mathfrak{p}\mathcal{O}_L$.

Luego, veremos que $e_{\mathfrak{B}_D|\mathfrak{p}} = f_{\mathfrak{B}_D|\mathfrak{p}} = 1$. Sabemos que $\mathfrak{B}_D$ es primo de L^D bajo $\mathfrak{B}$, además el grupo D actúa transitivamente en los primos de L sobre $\mathfrak{B}_D$. Notemos que $\mathfrak{B}$ es un primo sobre L y los elementos de D lo dejan fijo $\mathfrak{B}$, así es el único primo de L sobre $\mathfrak{B}_D$. Usando la formula del Teorema 3.1 tenemos que

$$[L : L^D] = e_{\mathfrak{B}|\mathfrak{B}_D} f_{\mathfrak{B}|\mathfrak{B}_D}. \tag{3.2}$$

Por Proposición 3.8, tenemos que

$$e_{\mathfrak{B}|\mathfrak{p}} = e_{\mathfrak{B}|\mathfrak{B}_D} e_{\mathfrak{B}_D|\mathfrak{p}} \text{ y } f_{\mathfrak{B}|\mathfrak{p}} = e_{\mathfrak{B}|\mathfrak{B}_D} f_{\mathfrak{B}_D|\mathfrak{p}},$$

así $e_{\mathfrak{B}|\mathfrak{B}_D} \leq e$, $f_{\mathfrak{B}|\mathfrak{B}_D} \leq f$. Además el lado izquierdo de 3.2 lo podemos calcular por la ley de las torres y el Teorema 3.1: como $[L : K] = efg$ y $[L^D : K] = g$ obtenemos que $[L : L^D] = ef$. Para que se cumplan las desigualdades recién descritas, se debe cumplir $e_{\mathfrak{B}|\mathfrak{B}_D} = e$ y $f_{\mathfrak{B}|\mathfrak{B}_D} = f$. Así $e_{\mathfrak{B}_D|\mathfrak{p}} = f_{\mathfrak{B}_D|\mathfrak{p}} = 1$.

Ahora demostraremos que $f_{\mathfrak{B}|\mathfrak{B}_I} = 1$, es decir, que $\mathcal{O}_L/\mathfrak{B}$ es extensión trivial de $(\mathcal{O}_L)^I/\mathfrak{B}_I$. Para ello, demostraremos que $\sigma \in \mathrm{Gal}((\mathcal{O}_L/\mathfrak{B})/((\mathcal{O}_L)^I/\mathfrak{B}_I))$ arbitrario actúa como la identidad. Sea $\alpha \in \mathcal{O}_L$ y $\theta = \alpha + \mathfrak{B} \in \mathcal{O}_L/\mathfrak{B}$, definimos

$$g(x) = \prod_{\tau \in I} (x - \tau(\alpha)),$$

notemos que tiene coeficientes en $\mathcal{O}_L \cap L^I = (\mathcal{O}_L)^I$ y es un polinomio pues los elementos de I son finitos. Reduciendo módulo $\mathfrak{B}$ obtenemos

$$\bar{g}(x) = (x - \theta)^m \in ((\mathcal{O}_L)^I/\mathfrak{B})[x],$$

donde $m = |I|$. Esto pues para todo $\tau \in I$ se tiene $\tau(\alpha) + \mathfrak{B} = \alpha + \mathfrak{B} = \theta$. Ahora sea $\sigma \in \mathrm{Gal}((\mathcal{O}_L/\mathfrak{B})/((\mathcal{O}_L)^I/\mathfrak{B}_I))$, σ envía a θ a otra raíz de $\bar{g}(x) : \theta$. Así, actúa como la identidad.

Uniendo todo lo anterior: como $f_{\mathfrak{B}_D|\mathfrak{p}} = 1$ y $f_{\mathfrak{B}|\mathfrak{B}_I} = 1$, tenemos que

$$f = f_{\mathfrak{B}|\mathfrak{B}_I} f_{\mathfrak{B}_I|\mathfrak{B}_D} f_{\mathfrak{B}_D|\mathfrak{p}} = f_{\mathfrak{B}_I|\mathfrak{B}_D}.$$

Por formula del teorema 3.1, tenemos que $[D : I] = [L^I : L^D] \geq e_{\mathfrak{B}_I|\mathfrak{B}_D} f_{\mathfrak{B}_I|\mathfrak{B}_D} \geq f$.

Por otro lado, por Teorema 3.5 tenemos que hay un homomorfismo inyectivo de $D|I$ en $\tilde{G}$, donde este último tiene f elementos. Así que $[D:I] \leq f$.

Así $[D:I] = [L^I : L^D] = f$, y por ley de torres:

$$efg = [L:K] = [L:L^I][L^I:L^D][L^D:K] = [L:L^I]fg.$$

Así $|I| = [L:L^I] = e$.

2. El homomorfismo inducido $D|I \longrightarrow \tilde{G}$ es inyectivo y, por parte 1., dominio y codominio son finitos y tienen igual cardinalidad. Así es sobreyectivo.

□

Tendremos la siguiente proposición para ver cuando un primo es ramificado o se escinde en una extensión Galois:

Proposición 3.9. *Sea $K \subseteq L$ una extensión de Galois, donde $L = K(\alpha)$ para algún $\alpha \in \mathcal{O}_L$. Sea $f(x)$ un polinomio mónico minimal para α sobre K, luego $f(x) \in \mathcal{O}_K[x]$. Si $\mathfrak{p}$ es primo de $\mathcal{O}_K$ y $f(x)$ es separable módulo $\mathfrak{p}$, entonces:*

1. *Si $f(x) \equiv f_1(x) \cdots f_g(x) \pmod{\mathfrak{p}}$, donde los $f_i(x)$ son irreduccibles y distintos módulo $\mathfrak{p}$, entonces $\mathfrak{B}_i = \mathfrak{p}\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L$ es ideal primo de $\mathcal{O}_L$, $\mathfrak{B}_i \neq \mathfrak{B}_j$ si $i \neq j$, y*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1 \cdots \mathfrak{B}_g.$$

   Más aún, todos los $f_i(x)$ tienen el mismo grado: el grado inercial: f.
2. *$\mathfrak{p}$ no ramifica en L.*
3. *$\mathfrak{p}$ se escinde en L si y solamente si $f(x) \equiv 0 \pmod{\mathfrak{p}}$ tiene solución en $\mathcal{O}_K$.*

Demostración:

1. Esta demostración es el ejercicio 5.6 de [Cox13].
2. Es implicancia directa de 1.
3. Por 2., $e = 1$. Así $\mathfrak{p}$ se escinde en L si y solo si $f = 1$. Como los $f_i(x)$ tienen grado f, esto ocurre si y solamente si $f(x)$ tiene solución módulo $\mathfrak{p}$.

□

4. El caso extensión cuadrática

Vamos a aplicar todo lo anterior al caso $K = \mathbb{Q}(\sqrt{d})$, donde $d \neq 0, 1$ es entero libre de cuadrados.

Recordemos que definimos el discriminante $d_k = D_{\mathcal{O}_K}$ en CM3, el cual toma el valor de d cuando $d \equiv 1 \pmod 4$ y $4d$ en otro caso.

Proposición 4.1. *Sea K cuerpo cuadrático de discriminante d_k, sea el automorfismo no trivial de K denotado como $\alpha \mapsto \alpha'$. Sea p un número primo.*

1. *Si $\left(\frac{d_k}{p}\right) = 0$, entonces $p\mathcal{O}_K = \mathfrak{p}^2$ para un primo $\mathfrak{p}$ de K.*
2. *Si $\left(\frac{d_k}{p}\right) = 1$, entonces $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, donde $\mathfrak{p} \neq \mathfrak{p}'$ primos de K.*
3. *Si $\left(\frac{d_k}{p}\right) = -1$, entonces $p\mathcal{O}_K$ es primo en K.*

Demostración: La haremos para el caso p primo impar, el caso $p = 2$ es similar.

1. Sea $I = (p, d_k)$ en $\mathcal{O}_K$. Notemos que $I^2 = p^2\mathcal{O}_K + d_k\mathcal{O}_K + p\sqrt{d_k}\mathcal{O}_K$. Como $(p^2, d_k) = p$, tenemos que $p\mathcal{O}_K \subseteq I^2$. Además, como p divide a d_k, $I^2 \subseteq p\mathcal{O}_K$. Así $I^2 = p\mathcal{O}_K$.

   Por fórmula del Teorema 3.1: $efg = 2 = [K:\mathbb{Q}]$, por lo que tenemos que I debe ser ideal primo de $\mathcal{O}_K$.
2. Notemos que el polinomio minimal de $\sqrt{d_k}$ sobre $\mathbb{Q}$ es $f(x) = x^2 - d_k$. Si $p \nmid d_k$, entonces $f(x)$ es separable módulo p. Por la Proposición 3.9, p no ramifica en K. Además si $\left(\frac{d_k}{p}\right) = 1$, $f(x)$ tiene solución módulo p, así que p se separa completamente en K:

$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$$

   con $\mathfrak{p}_1$, $\mathfrak{p}_2$ primos distintos de K. Como $\mathrm{Gal}(K/\mathbb{Q})$ actúa de manera transitiva, tenemos que $\mathfrak{p}_2 = \mathfrak{p}_1'$.
3. Al igual que antes, tenemos que p no ramifica en K. Pero ahora, $f(x) = x^2 - d_k$ es irreducible módulo p. Así que por Proposición 3.9 tenemos que $g = 1$ y $p\mathcal{O}_K$ es primo de K.

□

Gracias a esto podemos resumir el comportamiento de los primos de $\mathbb{Z}$ en la extensión K:

Corolario 4.2. *Sea K un cuerpo cuadrático de discriminante d_k y p un entero primo. Entonces:*

1. *p ramifica en K si y solamente si p divide a d_k.*
2. *p se separa completamente en K si y solamente si $\left(\frac{d_k}{p}\right) = 1$.*

Referencias

[Cox13] David A. Cox. *Primes of the form $x2 + ny2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013.

[IR82] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics 84. Springer New York, second edition, 1982.

[Mar18] Daniel A. Marcus. *Number fields*. Universitext. Springer International Publishing, second edition, 2018. (document), 1

2

(document), 1, 2, 3, 3

Email address: facares@uc.cl