RAMIFICACIÓN

FERNANDA CARES

El objetivo de esta sección es comprender algunos hechos de la teoría algebráica de números para poder usarlos más adelante en extensiones de cuerpos cuadráticos imaginarios. Estos resultados son más generales así que los enunciaremos de esa forma, sin embargo, varias demostraciones ya están realizadas para este caso en CM3.

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 $\mathbb{Q}$.

Definimos $\mathcal{O}_K$ como el conjunto de enteros algebraícos 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 algebraíco.*
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.*

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 $\mathfrak{a}$. (demostración pendiente), así $m\mathcal{O}_K \subseteq \mathfrak{a}$.

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. En efecto, 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, 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 $\mathbb{Q}[\sqrt{-5}]$.

Pero 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. Si $\alpha \in K$ es 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 $i = 1, 2..., n-1$.
   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 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 que α es entero algebraíco y 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 $\mathfrak{a}$ 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:
$$\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_g^{e_g}$$
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 $\mathcal{B}_i$ 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 el grado inercial de $\mathfrak{p}$ en $\mathfrak{B}_i$ y se denota f_i o $f_{\mathfrak{B}_i|\mathfrak{p}}$.

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 $e_i, i = 1, ..., g$ los índices de ramificación y f_i los grados inerciales, entonces:*

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

Demostraremos para el caso $K = \mathbb{Q}$ que es el que usaremos en adelante. Para ello necesitaremos 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) 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 $\mathfrak{B}^e \subseteq (\alpha) + \mathfrak{B}^{e-1}$, tenemos que este último tiene que ser potencia de $\mathfrak{B}$ (por descomposición en primos). Además tenemos que $(\alpha) + \mathfrak{B}^{e-1} \subseteq \mathfrak{B}^{e-1}$, así que $(\alpha) + \mathfrak{B}^e = \mathfrak{B}^{e-1}$.

con esto podemos definir un homomorfismo sobreyectivo:

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

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 isomorfismo entre $\mathcal{O}_K/\mathfrak{B}$ 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 $p\mathbb{Z}$ 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 $\mathcal{O}_K/\mathfrak{p} = \mathbb{Z}/p\mathbb{Z}$, 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, 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.

□

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*

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

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 separa completamente 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 arriba, tenemos:*

1. *$I_{\mathfrak{B}} \subseteq D_{\mathfrak{B}}$*
2. *Todo elemento $\sigma \in D_{\mathfrak{B}}$ induce un automorfismo 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. Como $\sigma \in \mathrm{Gal}(L/K)$ tenemos que podemos hacer restricción $\hat{\sigma} \colon \mathcal{O}_L \longrightarrow \mathcal{O}_L$ (las raíces de polinomios mónicos con coeficientes enteros son permutadas por σ). Sea $\pi \colon \mathcal{O}_L \longrightarrow \mathcal{O}_L/\mathfrak{B}$ la proyección, consideremos $\hat{\sigma} \circ \pi$:

$$\mathcal{O}_L \xrightarrow{\hat{\sigma}} \mathcal{O}_L \xrightarrow{\pi} \mathcal{O}_L/\mathfrak{B}$$

   Como tenemos que es homomorfismo sobreyectivo y 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, $\tilde{\sigma} \in \tilde{G}$. Demostrar que es homomorfismo quedará pendiente. Se tiene que

$$\tilde{\sigma}(\alpha + \mathfrak{B}) = \alpha + \mathfrak{B} \leftrightarrow \hat{\sigma}(\alpha) + \mathfrak{B} = \alpha + \mathfrak{B} \leftrightarrow \sigma(\alpha) - \alpha \in \mathfrak{B}$$

   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 y las de esta sección:

Teorema 3.6. *Sea $D_{\mathfrak{B}}, I_{\mathfrak{B}}$ y $\tilde{G}$ como arriba.*

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

Demostración: [Idea]: Notemos que si demostramos que $D_{\mathfrak{B}}/I_{\mathfrak{B}}$ tiene caldinalidad $f_{\mathfrak{B}|\mathfrak{p}}$ podemos concluír 1, al ser $D_{\mathfrak{B}}/I_{\mathfrak{B}}$ isomorfo a la imágen que es subgrupo de $\tilde{G}$, ahora tenemos que las cardinalidades de la imágen y $\tilde{G}$ son iguales, así que la función es sobreyectiva.

Para 2 tenemos que $\tilde{G}$ tiene tantos elementos como el grado de la extensión $\mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_L/\mathfrak{B}$, que por definición es $f_{\mathfrak{B}|\mathfrak{p}}$, habría que demostrar que la cantidad de elementos de $I_{\mathfrak{B}}$ es $e_{\mathfrak{B}|\mathfrak{p}}$.

Esto se hace considerando 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. Si quiero factorizar $\mathfrak{B}$ en $\mathcal{O}_L^H$ donde $H = D_{\mathfrak{B}}$ o $H = I_{\mathfrak{B}}$, tenemos que solo hay un primo en la factorización: $\mathfrak{B}^H$ (porque el Galois actúa transitivamente y en este caso es $D_{\mathfrak{B}}$ o $I_{\mathfrak{B}}$).

Se trabaja con estos cuerpos intermedios, anillos intermedios y teoría de Galois hasta llegar a $[L^I : L^D] \geq f$. Como teníamos el homomorfismo sobreyectivo de 3.5, $|D_{\mathfrak{B}}/I_{\mathfrak{B}}| = [L^I : L^D] \leq f$.

Así $|D_{\mathfrak{B}}/I_{\mathfrak{B}}| = f$, que $|I_{\mathfrak{B}}| = e$ sale del trabajo en anillos de números intermedios. □

Tendremos la siguiente proposicicón para ver cuando un primo es ramificado o se separa completamente en una extensión Galois:

Proposición 3.7. *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. *$\mathfrak{p}$ no ramifica en L.*
2. *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*
$$p\mathcal{O}_L = \mathfrak{B}_1 \cdots \mathfrak{B}_g.$$
Más aún, todos los $f_i(x)$ tienen el mismo grado: el grado inercial: f.
3. *$\mathfrak{p}$ se separa completamente en L si y solamente si $f(x) \equiv 0 \pmod{\mathfrak{p}}$ tiene solución en $\mathcal{O}_K$.*

Demostración: Notar que basta demostrar 2, en tal caso vemos que $e = 1$, así que $\mathfrak{p}$ no ramifica en L. Además dado que tenemos que $e = 1$, $\mathfrak{p}$ se separa completamente en L si y solamente si $f = 1$, como los $f_i(x)$ tienen grado f, esto ocurre si y solamente si $f(x)$ tiene solución módulo $\mathfrak{p}$. 2. Version Final. □

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 $d_k = D_{\mathcal{O}_K}$ que 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 primo en $\mathbb{Z}$.*

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

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 $\left(\frac{d_k}{p}\right) = 1$.*

Email address: facares@uc.cl