Ring Class Field y Teorema Principal

Jerson Caro

July 9, 2020

Contenido

El objetivo de esta charla es demostrar el siguiente teorema

Teorema

Sea $\mathcal{O}$ un orden en un campo cuadratico imaginario K, y sea $\mathfrak{a}$ un $\mathcal{O}$-ideal fraccional propio. Entonces el j invariantes $j(\mathfrak{a})$ es un entero algebraico y $K(j(\mathfrak{a}))$ es el ring class field del orden $\mathcal{O}$.

Definición

Recordamos que para K un campo de números, su anillo de enteros $\mathcal{O}_K$ y para un modulo $\mathfrak{m}$ sobre K definimos $I_K(\mathfrak{m})$ y $P_{K,1}(\mathfrak{m})$. A lo largo de esta sección nuestro modulo $\mathfrak{m}$ será un ideal principal $\alpha\,\mathcal{O}_K$.
Considere $\mathcal{O}$ un orden de conductor f en un cuerpo cuadrático imaginario K. Por la Proposition 7.22 el ideal class group $C(\mathcal{O})$ puede ser escrito como

$$C(\mathcal{O}) \cong I_K(f)/P_{K,\mathbb{Z}}(f), \tag{1}$$

(aquí $P_{K,\mathbb{Z}}(f)$ es generado por los ideales principales $\alpha\,\mathcal{O}_K$, donde $\alpha \equiv a (\text{mod } f\,\mathcal{O}_K)$ para algún entero a con $gcd(a, f) = 1$). Es claro que

$$P_{K,1}(f) \subset P_{K,\mathbb{Z}}(f) \subset I_K(f).$$

Por el teorema de existencia (Teorema de existencia Charla 14), esta información determina una única extensión abeliana L de K, la cual es llamada el ring class field del orden $\mathcal{O}$. Las propiedades básicas del ring class field L son: (a)Todos los primos de K ramificados en L deben dividir a $f\,\mathcal{O}_K$, y (b) El mapa de Artin y (1) nos dan los isomorfismos

$$C(\mathcal{O}) \cong I_K(f)/P_{K,\mathbb{Z}}(f) \cong Gal(L/K).$$

En particular $[L : K] = h(\mathcal{O})$. Note además que el Hilbert class field de K es el ring class field del orden $\mathcal{O}_K$.

Propiedades del Ring Class Field

Primero que todo, clasificaremos el grupo de Galois de la extensión $L/\mathbb{Q}$.

Lema 1.1

Sea L el ring class field de un orden $\mathcal{O}$ en un campo imaginario K. Entonces L es una extensión de Galois de $\mathbb{Q}$, y su grupo puede ser escrito como el producto semidirecto

$$Gal(L/\mathbb{Q}) \cong Gal(L/K) \rtimes (\mathbb{Z}/2\mathbb{Z})$$

donde el elemento no trivial de $\mathbb{Z}/2\mathbb{Z}$ actúa sobre $Gal(L/K)$ enviando σ a su inverso σ^{-1}.

Prueba

Primero que todo vamos a demostrar que $\tau(L) = L$, donde τ denota la conjugación compleja. Denotemos por $\mathfrak{m}$ el módulo $f\,\mathcal{O}_K$, y notamos que $\tau(\mathfrak{m}) = \mathfrak{m}$. Del hecho que $\ker(\Phi_{L/K,\mathfrak{m}}) = P_{K,\mathbb{Z}}(f)$, vemos entonces que

$\ker(\Phi_{\tau(L)/K,\mathfrak{m}}) = \tau(\ker(\Phi_{L/K,\mathfrak{m}})) = \tau(P_{K,\mathbb{Z}}(f)) = P_{K,\mathbb{Z}}(f)$. De aquí que $\ker(\Phi_{\tau(L)/K,\mathfrak{m}}) = \ker(\Phi_{L/K,\mathfrak{m}})$ entonces $\tau(L) = L$ sigue desde el Corolario 8.7. Esto, en particular, muestra que todos los embeddings de L en $\overline{\mathbb{Q}}$ caen en L, por lo que $L/\mathbb{Q}$ es Galois, tenemos entonces la siguiente secuencia exacta:

$$1 \to Gal(L/K) \to Gal(L/\mathbb{Q}) \to Gal(K/\mathbb{Q})(\cong \mathbb{Z}/2\mathbb{Z}) \to 1.$$

Del hecho que $\tau \in Gal(L/\mathbb{Q})$, $Gal(L/\mathbb{Q})$ es el producto semidirecto $Gal(L/\mathbb{Q}) \cong Gal(L/K) \rtimes (\mathbb{Z}/2\mathbb{Z})$, donde el elemento no trivial de $\mathbb{Z}/2\mathbb{Z}$ actúa como conjugación por τ. Además, para un primo $\mathfrak{p}$ de K, tenemos que:

$$\tau \left(\frac{L/K}{\mathfrak{p}} \right) \tau^{-1} = \left(\frac{L/K}{\tau(\mathfrak{p})} \right) = \left(\frac{L/K}{\overline{\mathfrak{p}}} \right).$$

Así que bajo el isomorfismo $I_K(f)/P_{K,\mathbb{Z}}(f) \cong Gal(L/K)$, conjugar por τ in $Gal(L/K)$ corresponde a la acción usual de τ sobre $I_K(f)$. Pero si $\mathfrak{a}$ es un ideal de $I_K(f)$, Entonces $\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}_K$ vive en $P_{K,\mathbb{Z}}(f)$ del hecho que $N(\mathfrak{a})$ es primo a f. Así que $\overline{\mathfrak{a}}$ es el inverso de $\mathfrak{a}$ en $I_K(f)/P_{K,\mathbb{Z}}(f)$.

En aras de caracterizar el ring class field de un orden $\mathcal{O}$, usaremos la siguiente proposición, aquí el conjunto $S_{L/K}$ es el conjunto de primos de K que descomponen completamente en L.

Proposición 1.2

Sean L y M extensiones finitas de K.

(i) Si M es una extensión de Galois sobre K, entonces $L \subset M \iff S_{M/K} \dot{\subset} S_{L/K}$

(ii) Si L es una extensión de Galois sobre K, entonces $L \subset M \iff \widetilde{S}_{M/K} \dot{\subset} S_{L/K}$ donde $\widetilde{S}_{M/K}$ es definido por

$$\widetilde{S}_{M/K} = \{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} \text{ es no ramificado y } f_{\mathfrak{P}|\mathfrak{p}} = 1 \text{ para algún } \mathfrak{P} \in \mathcal{P}_M\}.$$

Ahora, como ya sabemos que el ring class field es una extensión de Galois, esta está caracterizada por el conjunto de los primos que descomponen completamente. Por esta razón el siguiente Teorema es muy importante.

Teorema 1.3

Sea $n > 0$ un entero, y L el ring class field del orden $\mathbb{Z}[\sqrt{-n}]$ en el campo cuadrático imaginario $K = \mathbb{Q}(\sqrt{-n})$. Si p es un primo impar que no divide a n, entonces

$$p = x^2 + ny^2 \iff p \text{ se descompone completamente en} L.$$

Prueba

Sea $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$. El discriminante de $\mathcal{O}$ es $-4n$, y entonces $-4n = f^2 d_K$, donde $\mathcal{O}$ es el conductor de $\mathcal{O}$ (Lema 7.2). Sea p un primo impar que no divide a n. Entonces $p \nmid f^2 d_K$, lo cuál implica que p es no ramificado en K. Dadas estas condiciones probaremos este teorema demostrando las siguientes equivalencias:

$$
\begin{aligned}
p = x^2 + ny^2 &\iff p\,\mathcal{O}_K = \mathfrak{p}\,\overline{\mathfrak{p}},\ \overline{\mathfrak{p}} \neq \mathfrak{p},\ \text{y}\ \ \mathfrak{p} = \alpha\,\mathcal{O}_K, \alpha \in \mathcal{O} \\
&\iff p\,\mathcal{O}_K = \mathfrak{p}\,\overline{\mathfrak{p}},\ \overline{\mathfrak{p}} \neq \mathfrak{p},\ \text{y}\ \ \mathfrak{p} \in P_{K,\mathbb{Z}}(f) \\
&\iff p\,\mathcal{O}_K = \mathfrak{p}\,\overline{\mathfrak{p}},\ \overline{\mathfrak{p}} \neq \mathfrak{p},\ \text{y}\ ((L/K)/\mathfrak{p}) = 1 \\
&\iff p\,\mathcal{O}_K = \mathfrak{p}\,\overline{\mathfrak{p}},\ \overline{\mathfrak{p}} \neq \mathfrak{p},\ \text{y}\ \ \mathfrak{p}\ \text{se desc. complet. en}\ L \\
&\iff p\ \text{se descompone completamente en}\ L.
\end{aligned}
$$

Para probar la primera equivalencia, supongamos que $p = x^2 + ny^2 = (x + y\sqrt{-n}y)(x - y\sqrt{-n}y)$. Si $\mathfrak{p} = x + y\sqrt{-n}y$ tenemos que $p\,\mathcal{O}_K = \mathfrak{p}\,\overline{\mathfrak{p}}$ es la factorización en primos de $p\,\mathcal{O}_K$. Para el converso, si $p\,\mathcal{O}_K = \mathfrak{p}\,\overline{\mathfrak{p}}$, donde $\mathfrak{p} = (x + \sqrt{-n}y)\,\mathcal{O}_K$, se sigue que $p = x^2 + ny^2$. Del hecho que $p \nmid f$, la segunda equivalencia viene de la proposición 7.22. La tercera y cuarta equivalencia viene del hecho que $P_{K,\mathbb{Z}}(f) = \ker(\Phi_{L/K,\mathfrak{m}})$. Mientras que la última equivalencia viene del hecho que ambas son equivalente a tener $[L : \mathbb{Q}]$ primos sobre p en L.

Ejemplo

El ring class field del orden $\mathbb{Z}[\sqrt{-27}] \subset K := \mathbb{Q}(\sqrt{-3})$ es $L = K(\sqrt[3]{2})$. Sea L el ring class field de $\mathbb{Z}[\sqrt{-27}]$. Tenemos la siguiente información de L:

(i) L es una extensión de Galois cubica de $K = \mathbb{Q}(\sqrt{-3})$, esto pasa pues

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p|f} \left(1 - \left(\frac{d_k}{p}\right)\frac{1}{p}\right)$$
$$= \frac{6}{3}\left(\left(1 - 0\frac{1}{3}\right)\left(1 - (-1)\frac{1}{2}\right)\right) = 3.$$

(ii) Por el lema anterior el grupo de Galois $Gal(L/\mathbb{Q}) \cong S_3$.

(iii) Todos los primos de K que ramifican en L deben dividir a $6\,\mathcal{O}_K$.

Vamos a demostrar que sólo hay 4 casos posibles. Primero notamos por teoría de Kummer que $L = K(\sqrt[3]{u})$ con $u \in K$. Pero además de esto tenemos el siguiente Lema.

Lema 4

Si M es una extensión cúbica de $K = \mathbb{Q}(\sqrt{-3})$ con $Gal(M/\mathbb{Q}) \cong S_3$, entonces $M = K(\sqrt[3]{m})$ para algún entero positivo m libre de cubos.

Luego de tener esto, notamos que para que L solo ramifique en 2 y 3, estos deben ser los únicos números que dividan a m. Tenemos entonces la siguiente lista de posibilidades para m

$$2, 3, 4, 6, 9, 12, 18, 36,$$

esto implica que L es uno de los siguientes 4 campos:

$$K(\sqrt[3]{2}),\ K(\sqrt[3]{3}),\ K(\sqrt[3]{6}),\ K(\sqrt[3]{12})$$

Todos estos campos cumplen las condiciones (i)-(iii), así que necesitamos algo más sobre L. La manera de decir que es el primer campo es como sigue, por ejemplo para descartar el segundo caso, notemos que $31 = 2^2 + 27 \cdot 1^2$, luego 31 debe descomponer completamente en L, sin embargo $x^3 \equiv 3 (\text{mod } 31)$ no tiene solución.

Teorema Principal

Antes de demostrar el teorema importante, debemos definir y demostrar un resultado con respecto a un caso especial de subretículos cíclicos. Dado un orden $\mathcal{O}$, decimos que un $\mathcal{O}$-ideal propio es primitivo si no es de la forma $d\,\mathfrak{a}$, donde $d > 1$ es un entero y $\mathfrak{a}$ es un $\mathcal{O}$-ideal propio. Tenemos el siguiente resultado:

Lema

Sea $\mathcal{O}$ un orden en un campo cuadrático imaginario, y sea $\mathfrak{b}$ un $\mathcal{O}$-ideal fraccionario. Entonces, dado un $\mathcal{O}$-ideal propio $\mathfrak{a}$, $\mathfrak{a}\,\mathfrak{b}$ es un subretículo de $\mathfrak{b}$ de índice $N(\mathfrak{a})$, y $\mathfrak{a}\,\mathfrak{b}$ es un subretículo cíclico si y sólo si $\mathfrak{a}$ es un ideal primitivo.

Prueba

Podemos asumir (reemplazando $\mathfrak{b}$ por un multiplo si es necesario) que $\mathfrak{b} \subset \mathcal{O}$. Note que tenemos la siguiente secuencia exacta:

$$0 \to \mathfrak{b} / \mathfrak{a}\,\mathfrak{b} \to \mathcal{O} / \mathfrak{a}\,\mathfrak{b} \to \mathcal{O} / \mathfrak{b} \to 0,$$

la cual implica que $[b : \mathfrak{a}\,\mathfrak{b}]N(\mathfrak{b}) = N(\mathfrak{a}\,\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$, y $[\mathfrak{b} : \mathfrak{a}\,\mathfrak{b}] = N(\mathfrak{a})$ se sigue. Asuma hacia una contradicción que $\mathfrak{b} / \mathfrak{a}\,\mathfrak{b}$ no es cíclico. De aquí que existe $d > 1$ tal que $(\mathbb{Z}/d\,\mathbb{Z})^2 \subset \mathfrak{b} / \mathfrak{a}\,\mathfrak{b}$. De aquí que existe un subretículo tal que $\mathfrak{b} \supset \mathfrak{b}' \supset \mathfrak{a}\,\mathfrak{b}$. Como $\mathfrak{b}'$ es de rango 2 tenemos que $\mathfrak{a}\,\mathfrak{b} = d\,\mathfrak{b}'$, luego $\mathfrak{a} = d\,\mathfrak{b}'\,\mathfrak{b}^{-1}$ y como $\mathfrak{b}' \subset \mathfrak{b}$ se tiene que $\mathfrak{b}'\,\mathfrak{b}^{-1} \subset \mathcal{O}$, de aquí que $\mathfrak{a}$ no es primitivo.
Si $\mathfrak{a}$ no es primitivo es claro que un cociente de $\mathfrak{b} / \mathfrak{a}\,\mathfrak{b}$ es isomorfo a $(\mathbb{Z}/d\,\mathbb{Z})^2$. Luego $\mathfrak{b} / \mathfrak{a}\,\mathfrak{b}$ no es cíclico.

Este lema será aplicado con $\mathfrak{a} = \alpha\,\mathcal{O}$, con $\alpha \in \mathcal{O}$. En este caso, $\alpha\,\mathcal{O}$ es primitivo si y sólo si α es primitivo como elemento de $\mathcal{O}$ (esto es α no es de la forma $d\beta$ donde $d > 1$ y $\beta \in \mathcal{O}$). Del hecho que $N(\alpha) = N(\alpha\,\mathcal{O})$, tenemos entonces el siguiente Corolario del Lema 2.1:

Corolario 2.2

Sea $\mathcal{O}$ y $\mathfrak{b}$ como antes. Entonces, dado $\alpha \in \mathcal{O}$, $\alpha\,\mathfrak{b}$ es un subretículo de $\mathfrak{b}$ de indice $N(\alpha)$, y $\alpha\,\mathfrak{b}$ es un subretículo cíclico si y sólo si α es primitivo.

Prueba

(Demostración Teorema 0.1) Sea $\mathfrak{a}$ un $\mathcal{O}$-ideal propio, donde $\mathcal{O}$ es un orden en un campo cuadrático imaginario K. Lo primero que vamos a demostrar es que $j(\mathfrak{a})$ es un entero algebraico.
Sea $\alpha \in \mathcal{O}$ un elemento primitivo, de aquí que $\alpha\,\mathfrak{a}$ es un subretículo cíclico de $\mathfrak{a}$ es de indece $m = N(\alpha)$. Entonces por teorema 11.23, sabemos que

$$0 = \Phi_m(j(\alpha\,\mathfrak{a}), j(\mathfrak{a})) = \Phi_m(j(\mathfrak{a}), j(\mathfrak{a})) = 0$$

pues $j(\alpha\,\mathfrak{a}) = j(\mathfrak{a})$. Así que $j(\mathfrak{a})$ es una raíz de $\Phi_m(X, X)$, y como este polinomio tiene coeficientes en $\mathbb{Z}$ (parte (i) del Teorema 11.18) $j(\mathfrak{a})$ es algebraico. Además si podemos escoger α de tal forma que no sea un cuadrado perfecto el término lider de $\Phi_m(X, X)$ será ± 1, (parte (iv) of Teorema 11.18), y así $j(\mathfrak{a})$ es un entero algebraico. Por Lema 7.2, $\mathcal{O} = [1, fw_K]$, con $w_k = (d_K + \sqrt{d_K})/2$. Entonces si tomamos $\alpha = fw_K$, tenemos que $N(\alpha) = f^2((d_K^2 - d_K)/4) = (f/2)^2 d_K(d_K - 1)$ es cuál no es un cuadrado.

Ahora probaremos que si L es el ring class field de $\mathcal{O}$, entonces $L = K(j(\mathfrak{a}))$. Para ello usaremos la Proposición 1.2, por tal razón debemos estudiar $S_{L/\mathbb{Q}}$ el conjunto de primos que descomponen completamente en L. Vamos a mostrar que

$$S_{L/\mathbb{Q}} \doteq \{p \text{ primo} : p = N(\alpha) \text{ para algún } \alpha \in \mathcal{O}\}. \tag{2}$$

Cuando $D \equiv 0 \bmod 4$, se tiene que $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ para algun entero positivo n. Así que $N(\alpha) = N(x + y\sqrt{-n}) = x^2 + ny^2$, por el Teorema 1.3 tenemos la igualdad (2) para casi todo primo. El caso $D \equiv 1 \bmod 4$ es la misma idea sólo que teniendo en cuanta que la norma es $x^2 + xy + ((1 - D)/4)y^2$. Esto prueba (2).
Sea $M = K(j(\mathfrak{a}))$. Del hecho que L sobre $\mathbb{Q}$ es Galois por Lema 1.1. Por Proposición 1.2 tenemos que $M \subset L$ es igual a

$$S_{L/\mathbb{Q}} \dot{\subset} S_{M/\mathbb{Q}}, \tag{3}$$

Tome $p \in S_{L/\mathbb{Q}}$, y asuma que p es no ramificado en M (esto excluye solo a finitos primos). Por (2), $p = N(\mathfrak{a})$ para algún $\alpha \in \mathcal{O}$. Entonces $\alpha\,\mathfrak{a} \subset \mathfrak{a}$ es un subretículo de índice $N(\alpha) = p$, y es cíclico pues p es primo. Así

$$0 = \Phi_p(j(\alpha\,\mathfrak{a}), j(\mathfrak{a})) = \Phi_p(j(\mathfrak{a}), j(\mathfrak{a})).$$

Usando Teorema 2.1 (5) charla 10 (Congruencia de Kronecker), tenemos que

$$0 = \Phi_p(j(\alpha\,\mathfrak{a}), j(\mathfrak{a})) = (j(\mathfrak{a})^p - j(\mathfrak{a}))^2 + p\beta$$

para algún $\beta \in \mathcal{O}_M$. Ahora tomemos $\mathfrak{P}$ un primo sobre p de M. Entonces tenemos

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \bmod \mathfrak{P}\,. \tag{4}$$

Antes de seguir con la prueba vamos a demostrar el siguiente Lema:

Lema

(i) $\mathcal{O}_K[j(\mathfrak{a})] \subset \mathcal{O}_M$ tiene índice finito,

(ii) Si $p \nmid [\mathcal{O}_M; \mathcal{O}_K[j(\mathfrak{a})]]$ entonces (4) implica que $\alpha^p \equiv \alpha \bmod \mathfrak{P}$ para todo $\alpha \in \mathcal{O}_M$.

Prueba

Para la parte (i) es bien conocido que $\mathcal{O}_M$ y $\mathcal{O}_K[j(\mathfrak{a})]$ son $\mathbb{Z}$-módulos de rango $[M : \mathbb{Q}]$. Para la parte (ii), note que como p descompone completamente en L, así lo hace en K, y de aquí que existe un ideal $\mathfrak{p}$ sobre p, de norma p. Esto implica que $\alpha^p \equiv \alpha \bmod \mathfrak{P}$ se cumple para todo $\alpha \in \mathcal{O}_K$ y consecuentemente se cumple para todo $\alpha \in \mathcal{O}_K[j(\mathfrak{a})]$ por (4). Si $N = [\mathcal{O}_L : \mathcal{O}_K[j(\mathfrak{a})]]$, entonces la multiplicacón por N es un automorfismo (de grupos abelianos) de $\mathcal{O}_L / \mathfrak{P}$.

Desde (ii) obtenemos que $\mathcal{O}_M / \mathfrak{P} = \mathbb{F}_p$, luego $f_{\mathfrak{P}|p} = 1$, y como esto se cumple para todo primo $\mathfrak{P}$ sobre p, tenemos que p descompone completamente. Note que esto pasa para todo primo p que descompone completamente en L (salvo los primos que ramifican en M y que dividen a $[\mathcal{O}_M; \mathcal{O}_K[j(\mathfrak{a})]]$). Esto prueba (3), luego $M \subset L$ se sigue.
La inclusión $M = K(j(\mathfrak{a})) \subset L$ muestra que los j-invariantes de todos los $\mathcal{O}$-ideales fraccionarios propios pertenecen a L. Sea $h = h(\mathcal{O})$, y sean $\mathfrak{a}_i$, con $i = 1 \ldots, h$ una lista completa de representantes para $C(\mathcal{O})$. Se sigue que cualquier $j(\mathfrak{a})$ es igal a algún $j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_h)$ y ademaás ellos son todos distintos. De aquí que

$$\Delta = \prod_{i<j} (j(\mathfrak{a}_i) - j(\mathfrak{a}_j)) \tag{5}$$

es un elemento distinto de cero en $\mathcal{O}_L$.

Ahora vamos a demostrar que $L \subset M$. Para ello vamos a demostrar que $\widetilde{S}_{M/\mathbb{Q}} \dot{\subset} S_{L/\mathbb{Q}}$, donde $p \in \widetilde{S}_{M/\mathbb{Q}}$ significa que p es no ramificado en M y $f_{\mathfrak{P}|p} = 1$ para algún primo $\mathfrak{P}$ de M sobre p. Esto en particular implica que p se descompone completamente en K, y de aquí que $p = N(\mathfrak{p})$ para algún primo en $\mathcal{O}_K$. Por Proposición 7.20 y asumiendo $p \nmid f$ (lo cuál excluye finitos primos)) nos dice que $p = N(\mathfrak{p} \cap \mathcal{O})$. *vamos ahora a demostrar que* $\mathfrak{p} \cap \mathcal{O}$ *es un ideal principal* $\alpha\,\mathcal{O}$, entonces $p = N(\alpha)$, lo que implica que $p \in S_{L/\mathbb{Q}}$ por (2). Vamos además a asumir que p es primo relativo a Δ de (5).

Definamos $\mathfrak{a}' = (\mathfrak{p} \cap \mathcal{O})\,\mathfrak{a}$. Del hecho que $\mathfrak{p} \cap \mathcal{O}$ tiene norma p, es un subretículo de índice p en $\mathfrak{a}$ por Lema (2.1) y de aquí que es cíclico. Así que $\Phi_p(j(\mathfrak{a}'), j(\mathfrak{a})) = 0$. Usando de nuevo la congruencia de Kronecker tenemos que

$$0 = \Phi_p(j(\mathfrak{a}'), j(\mathfrak{a})) = (j(\mathfrak{a}')^p - j(\mathfrak{a}))(j(\mathfrak{a}') - j(\mathfrak{a})^p) + pQ(j(\mathfrak{a}'), j(\mathfrak{a}))$$

para algún polinomio $Q(X, Y) \in \mathbb{Z}[X, Y]$.

Sea $\mathfrak{O}$ un primo L sobre $\mathfrak{P}$. Del hecho que $j(\mathfrak{a}')$ y $j(\mathfrak{a})$ son enteros algebraicos en L, tenemos que $pQ(j(\mathfrak{a}'), j(\mathfrak{a})) \in \mathfrak{O}$. Así

$$j(\mathfrak{a}')^p \equiv j(\mathfrak{a}) \bmod \mathfrak{O} \qquad \text{o} \qquad j(\mathfrak{a}') \equiv j(\mathfrak{a})^p \bmod \mathfrak{O}\,. \tag{6}$$

Por otra parte, como $f_{\mathfrak{P}|p} = 1$, nos dice que $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \bmod \mathfrak{P}$, y como $\mathfrak{P} \subset \mathfrak{O}$, tenemos que

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \bmod \mathfrak{O}\,. \tag{7}$$

Del hecho que $j(\mathfrak{a}')^p \equiv j(\mathfrak{a})^p \bmod \mathfrak{O}$ implica que $j(\mathfrak{a}') \equiv j(\mathfrak{a}) \bmod \mathfrak{O}$, entonces juntando (6) y (7) tenemos:

$$j(\mathfrak{a}') \equiv j(\mathfrak{a}) \bmod \mathfrak{O}\,.$$

Basta mostrar que $\mathfrak{a}'$ y $\mathfrak{a}$ estan en la misma clase en $C(\mathcal{O})$. Si no estan en la misma clase $j(\mathfrak{a}') = j(\mathfrak{a})$ divide a Δ en 5. Sin embargo escogimos p primo relativo a Δ.

Gracias.