MATÍAS ALVARADO TORRES

1. MOTIVACIÓN

La idea de esta charla es introducir dos nociones y herramientas muy importantes en la teoría de multiplicación compleja, el cuerpo de clases de Hilbert y la función de Artin. El cuerpo de clases de Hilbert es un objeto muy estudiado en teoría de cuerpos de clases y teoría de números, pues nos permite entender las extensiones abelianas de un cuerpo de números. En nuestro caso tomará un rol protagónico, pues relacionaremos estos cuerpos con retículos con multiplicación compleja y más específicamente con el invariante j. Por otro lado la función de Artin es una herramienta que por sí misma es de mucha importancia en teoría de números, ya que, esta nos permite generalizar la nociones de leyes de reciprocidad. En nuestro caso la usaremos cómo herramienta para entender algunas propiedades del cuerpo de clases. En esta ocasión definiremos la función de Artin solo para extensiones que son no ramificadas, pero en la siguiente charla se hará en un contexto mucho más general.

2. PRELIMINARES

Antes de definir el cuerpo de clases de Hilbert de un cuerpo de números necesitamos algunas definiciones básicas. A continuación introduciremos cierto lenguaje.

Definición 2.1. Una extensión de cuerpos L/K es **abeliana** si es una extensión galoisiana con grupo de Galois abeliano.

En adelante supondremos que lo cuerpos que consideramos son cuerpos de números a menos que se especifique lo contrario.

Para definir el objeto principal debemos extender la noción de primos en K. Recordemos que un primo (o lugar) de K es un ideal primo del anillo de enteros $\mathcal{O}_K$ de K. A estos ideales primos le llamaremos **primos finitos** de K. A continuación daremos la noción de primo infinito.

Definición 2.2. Un primo infinito de un cuerpo de números K es una incrustación $\sigma\colon K \hookrightarrow \mathbb{C}$.

Recordemos que si la extensión $K/\mathbb{Q}$ es de grado n, entonces existen n incrustaciones de K en $\mathbb{C}$. Además hay r_1 de estas incrustaciones que tienen imagen contenida en $\mathbb{R}$, las cuales llamaremos **primos infinitos reales** mientras que $2r_2$ de ellas son complejas. Otro hecho importante de recordar es que estas últimas vienen de a pares, ya que, si σ no tiene imagen en $\mathbb{R}$, entonces $\overline{\sigma}$ define una incrustación y es diferente a σ.

Al igual que en el caso de primos finitos, existe una noción de ramificación en primos infinitos. Si L/K es una extensión de cuerpos de números, esta se dice **ramificada en** σ, si σ es un primo infinito real de K el cual tiene una extensión a L que no sea real, es decir, existe una extensión de σ a L tal que $\sigma(L) \nsubseteq \mathbb{R}$. Si σ es un lugar real de L cuando extendemos la función, entonces diremos que la extensión L/K es no ramificada en σ.

Definición 2.3. Una extensión L/K se dice **no ramificada** si es no ramificada en primos finitos e infinitos.

Ejemplo 2.4. La incrustación natural $\mathbb{Q} \hookrightarrow \mathbb{C}$ la denotaremos simplemente como ∞. Observamos que esta incrustación es real. De este modo vemos que la extensión $\mathbb{Q}(i)/\mathbb{Q}$ es ramificada en ∞, pues las dos extensiones de esta incrustación a $\mathbb{Q}(i)$ toma valores no reales.

Ejemplo 2.5. La extensión $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ es no ramificada en ∞, pues las extensiones de esta incrustación a $\mathbb{Q}(\sqrt{5})$ vienen dadas por $\sigma_1\colon a+\sqrt{b} \mapsto a+\sqrt{b} \in \mathbb{R}$ y $\sigma_2\colon a+\sqrt{b} \mapsto a-\sqrt{b} \in \mathbb{R}$

Ejemplo 2.6. Sea ζ una raíz primitiva n-ésima de la unidad, para $n > 2$. La extensión $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta+\zeta^{-1})$ ramifica en cada primo infinito de $\mathbb{Q}(\zeta+\zeta^{-1})$. Para ver esto observamos que cada incrustación de $\mathbb{Q}(\zeta+\zeta^{-1})$ en $\mathbb{C}$ viene dada por la restricción de las incrustaciones de $\mathbb{Q}(\zeta)$. Cada incrustación de $\mathbb{Q}(\zeta)$ en $\mathbb{C}$ es compleja, pues la imagen de ζ debe ser una raíz n-ésima de la unidad en $\mathbb{C}$. Por otro lado, cuando restringimos una incrustación σ a $\mathbb{Q}(\zeta+\zeta^{-1})$

observamos que $\sigma(\zeta+\zeta^{-1}) = \sigma(\zeta)+\overline{\sigma(\zeta)} \in \mathbb{R}$, donde la barra denota la multiplicación compleja. Luego como la imagen de $\mathbb{Q}$ y del generador vía σ son reales, se tiene que la restricción de σ es real. Lugo cada lugar infinito de $\mathbb{Q}(\zeta+\zeta^{-1})$ ramifica en la extensión $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta+\zeta^{-1})$.

Ahora que tenemos la noción de ramificación en infinito estamos en condiciones de dar la definición del cuerpos de clases de Hilbert.

Definición 2.7. Si K es un cuerpo de números, el **cuerpo de clases de Hilbert** de K se define como la extensión finita L/K tal que:

(i) L/K es abeliana y no ramificada.
(ii) Cualquier extensión abeliana no ramificada de K es una subextensión de L/K.

Observación 2.8. Es usual encontrar en la literatura la notación $H(K)$, para denotar el cuerpo de clases de Hilbert de K.

De la definición es dificil tener certeza de como debe ser el cuerpo de Hilbert ¿será una extensión no trivial?, ¿será una extensión finita? ¿es único?. Lo que podemos responder ahora es la maximalidad suponiendo la existencia de extensiones abelianas y no ramificadas. SI L/K y F/K son extensiones abelianas no ramificadas, veamos entonces LF/K es abeliana no ramificada.

- **Abeliana:** Sea ϕ: $\mathrm{Gal}(LF/K) \to \mathrm{Gal}(L/K) \times \mathrm{Gal}(F/K)$ el morfismo de grupos dado por la ley $\sigma \mapsto (\sigma|_L, \sigma|_F)$. ϕ es inyectivo, pues si ϕ es la identidad en L y F entonces será la identidad en LF. De este modo existe una inclusión de $\mathrm{Gal}(LF/K)$ en un grupo abeliano.
- **No ramificada:** Si $\mathfrak{p}$ es un primo finito de K, entonces sabemos que es no ramificado en L y en F. Sea M la clausura normal de LF y sea $\wp$ un primo en M sobre $\mathfrak{p}$. Sea $I = I_{\wp/\mathfrak{p}}$ el grupo de inercia, y M^I la máxima subextensión de M/K no ramificada en $\mathfrak{p}$. Como suponemos que L y F son no ramificadas en $\mathfrak{p}$ concluimos que $L \subseteq M^I$ y $F \subseteq M^I$, por lo tanto $LF \subseteq M^I$, es decir, LF es no ramificada en $\mathfrak{p}$. De este modo concluimos que LF/K es no ramificada en primos finitos. Para los primos infinitos observamos que $L = K(\alpha)$ y $F = K(\beta)$ para ciertos $\alpha, \beta \in K$, luego si una incrustación real de K se extiende a una incrustación compleja de LF es porque la imagen de α o β es compleja, pero eso contradice el hecho que L y F sean no ramificadas al infinito.

Ejemplo 2.9. Del hecho que $\mathbb{Q}$ no tenga extensiones no ramificadas se deduce que el cuerpo de Hilbert de $\mathbb{Q}$ es $\mathbb{Q}$.

En este punto es dificil dar ejemplos de cuerpos de Hilbert porque no tenemos herramientas para argumentar que alguna extensión L/K es maximal dentro de las no ramificadas abelianas. Por ese motivo es que introduciremos el simbolo de Artín, el cual nos ayudará a resolver este problema, en particular podremos relacionar el grado de la extensión $H(K)/K$ con información intrinseca de K. Antes de introducir esta nueva herramienta necesitaremos el siguiente lema.

Lema 2.10. *Sea L/K una extensión de Galois y $\mathfrak{p}$ un lugar finito de K no ramificado en L. Si $\mathfrak{P}$ es un primo de L sobre $\mathfrak{p}$, entonces existe un único elemento $\sigma \in Gal(L/K)$ tal que para todo $\alpha \in \mathcal{O}_L$*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \ mod\ \mathfrak{P}$$

Demostración: Por proposición 3.5 de la charla 12 sabemos que existe una sucesión exacta corta

$$1 \longrightarrow I_{\mathfrak{P}} \longrightarrow D_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \longrightarrow 1$$

Como en este caso sabemos que $\mathfrak{p}$ es no ramificado en L, tenemos que $I_{\mathfrak{P}}$ es trivial, luego vemos que $D_{\mathfrak{P}} \simeq \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$. Recordemos que este isomorfismo está dado por reducir módulo $\mathfrak{P}$ la restricción $\psi|_{\mathcal{O}_L}$ para $\psi \in D_{\mathfrak{P}}$. Tomemos $\sigma \in D_{\mathfrak{P}}$ como la preimagen de Frob $\in \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ vía el isomorfismo anterior. Observemos que Frob es el morfismo dado por la asignación $x \mapsto x^{N(\mathfrak{p})}$. De este modo, por como está construido el isomorfismo y por como fue tomado σ, concluimos que

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P} \quad \forall \alpha \in \mathcal{O}_L$$

□

Definición 2.11. Sea L/K una extensión de Galois y $\mathfrak{p}$ un lugar finito de K no ramificado en L. El **símbolo de Artin** es el único elemento $\sigma \in \mathrm{Gal}(L/K)$ tal que para todo $\alpha \in \mathcal{O}_L$ $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}$. Al elemento σ lo denotaremos por $\left(\dfrac{L/K}{\mathfrak{P}}\right)$.

Observación 2.12. La definición 2.11 está bien definida gracias al lema 2.10.

Para familiarizarnos con el símbolo de Artin, veremos un ejemplo para extensiones cuadráticas, y concluiremos que en algún sentido el símbolo de Artin es una generalización del símbolo de Legendre.

Ejemplo 2.13. Sean p, q primos impares diferentes, y sea $\mathfrak{p}$ un primo de $\mathbb{Q}(\sqrt{q})$ sobre p.

- Si $\left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{\mathfrak{p}}\right) = Id \in \mathrm{Gal}(\mathbb{Q}(\sqrt{q})/\mathbb{Q})$, entonces $\sqrt{q} \equiv \sqrt{q}^p \bmod \mathfrak{p}$, luego $\overline{\sqrt{q}} \in \mathbb{F}_p$, pues es fijado por el Frobenius. Con lo que concluimos que q es un cuadrado módulo p. Por lo tanto
$$\left(\frac{q}{p}\right) = 1$$
- Si $\left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{\mathfrak{p}}\right)$ es el elemento no trivial en $\mathrm{Gal}(\mathbb{Q}(\sqrt{q})/\mathbb{Q})$, entonces $-\sqrt{q} \equiv \sqrt{q}^p \bmod \mathfrak{p}$. Por lo tanto $\overline{\sqrt{q}} \notin \mathbb{F}_p$, pues no es fijado por Frobenius. De este modo vemos que q no es un cuadrado módulo p. En terminos del simbolo de Legendre tenemos que
$$\left(\frac{q}{p}\right) = -1$$
Lo que concluimos es que podemos interpretar el simbolo de Artin como el simbolo de Legendre en este caso.

Veamos ahora algunas propiedades

Proposición 2.14. *Sea L/K una extensión de Galois y $\mathfrak{p}$ un primo finito de K no ramificado en L y $\mathfrak{P}$ un lugar en L sobre $\mathfrak{p}$.*

(i) *Si $\sigma \in Gal(L/K)$, entonces*
$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}.$$

(ii) *El orden de $\left(\frac{L/K}{\mathfrak{P}}\right)$ en $Gal(L/K)$ es el grado de inercia de $\mathfrak{p}$ en L/K.*

(iii) *$\mathfrak{p}$ escinde completamente en L si y slo si $\left(\frac{L/K}{\mathfrak{P}}\right)$ es la identidad.*

Demostración:

(i) Sea $\alpha \in \mathcal{O}_L$. Usemos la propiedad de $\left(\frac{L/K}{\mathfrak{P}}\right)$ evaluando el elemento $\sigma^{-1}(\alpha)$. Asi obtenemos
$$\left(\frac{L/K}{\mathfrak{P}}\right)(\sigma^{-1}(\alpha)) \equiv \sigma^{-1}(\alpha)^{N(\mathfrak{p})} \bmod \mathfrak{P}$$
De este modo tenemos que
$$\left(\frac{L/K}{\mathfrak{P}}\right)(\sigma^{-1}(\alpha)) - \sigma^{-1}(\alpha)^{N(\mathfrak{p})} \in \mathfrak{P}$$
$$\sigma\left(\frac{L/K}{\mathfrak{P}}\right)(\sigma^{-1}(\alpha)) - \sigma\sigma^{-1}(\alpha)^{N(\mathfrak{p})} \in \sigma(\mathfrak{P})$$
$$\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}(\alpha) - \alpha^{N(\mathfrak{p})} \in \sigma(\mathfrak{P})$$
Como esto es para todo $\alpha \in \mathcal{O}_L$, concluimos el resultado por la unicidad del símbolo de Artin, ya que $\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}$ cumple la propiedad de $\left(\frac{L/K}{\sigma(\mathfrak{P})}\right)$.

(ii) Por construcción, el símbolo de Artin tiene el mismo orden que el elemento Frobenius de la extensión residual, y el orden de este es por definición el grado de inercia en $\mathfrak{p}$.

(iii) Sea $n = \deg(L/K)$. $\mathfrak{p}$ escinde completamente si y solo si, descompone en n primos diferentes en L. Luego por el teorema 2.2 de la charla 12 concluimos que el grado de inercia debe ser igual a 1. Usando la parte (ii) concluimos que esto es equivalente a que $\left(\frac{L/K}{\mathfrak{P}}\right)$ sea la identidad.

□

Por definición, el símbolo de Artin depende de una extensión L/K y un primo finito $\mathfrak{P}$ en L. Una pregunta interesante es como varia el simbolo de Artin sobre los diferentes primos $\mathfrak{P}_1, ..., \mathfrak{P}_r$ sobre algún primo $\mathfrak{p}$ en K no ramificado en L. A priori la respuesta no es clara, de hecho podemos encontrar extensiones en donde los grados de inercia sean diferentes para los distintos primos $\mathfrak{P}_i$, lo cual implicaria que los simbolos de Artin sean distintos. Un caso importante en donde sí podemos dar una respuesta concreta es en el caso en que la extensión L/K sea abeliana. Supongamos que este sea el caso y sean $\mathfrak{P}, \mathfrak{P}'$ primos en L sobre el primo $\mathfrak{p}$ en K, el cual es no ramificado en L. Por teorema 3.1 de la charla 12 $\mathrm{Gal}(L/K)$ actúa de forma transitiva en el conjunto de los lugares de L que están sobre $\mathfrak{p}$. De este modo existe $\sigma \in \mathrm{Gal}(L/K)$ tal que $\mathfrak{P}' = \sigma(\mathfrak{P})$. Por la proposición 2.14 tenemos

$$\left(\frac{L/K}{\mathfrak{P}'}\right) = \left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1} = \left(\frac{L/K}{\mathfrak{P}}\right)$$

Vemos que el simbolo de Artin será igual para cualquier primo sobre $\mathfrak{p}$, por lo tanto esto solo depende del primo en el cuerpo base. La observación hecha recientemente nos permite escribir simplemente $\left(\frac{L/K}{\mathfrak{p}}\right)$.

A continuación veremos otro ejemplo de símbolo de Artin. Este ejemplo es expuesto en [Cox13], pero para entenderlo es necesario manejar una generalización del simbolo de Legendre en el anillo $\mathbb{Z}[\omega]$. Una pequeña introducción a esta materia se encuentra en el apéndice.

Ejemplo 2.15. Sea $K = \mathbb{Q}(\sqrt{-3})$ y $L = K(\sqrt[3]{2})$. Observamos que $\mathcal{O}_K = \mathbb{Z}[\omega]$, el cual es un dominio de ideales principales, por lo tanto cualquier ideal primo $\mathfrak{p}$ de K se puede escribir como (π) o $\pi\mathbb{Z}[\omega]$. La extensión $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})/\mathbb{Q}$ es ramificada en 2 y en 3, por lo tanto la extensión L/K es no ramificada en primos π que no contegan a 2 o 3. Sea entonces π un primo de K no ramificado en L. Probemos que

$$\left(\frac{L/K}{\pi}\right) = \left(\frac{2}{\pi}\right)_3$$

Sea $\mathfrak{P}$ un primo de L sobre π, entonces

$$\begin{aligned}\left(\frac{L/K}{\pi}\right)(\sqrt[3]{2}) &\equiv \sqrt[3]{2}^{N(\pi)} \bmod \mathfrak{P} \\ &\equiv 2^{(N(\pi)-1)/3} \cdot \sqrt[3]{2} \bmod \mathfrak{P}\end{aligned}$$

Como sabemos que

$$2^{(N(\pi)-1)/3} \cdot \sqrt[3]{2} \equiv \left(\frac{2}{\pi}\right)_3 \sqrt[3]{2} \bmod \pi$$

y ademas $\mathfrak{P}$ está sobre π, concluimos que

$$\left(\frac{L/K}{\pi}\right)(\sqrt[3]{2}) \equiv \left(\frac{2}{\pi}\right)_3 \sqrt[3]{2} \bmod \mathfrak{P}$$

Como $\sqrt[3]{2}$ genera la extensión L/K concluimos que el simbolo de Artin coincide con el simbolo de Legendre.

3. Función de Artin

La idea a continuación es definir la función de Artin en el caso particular de una extensión abeliana L/K no ramificada. En general uno puede definir una función de Artin para cualquier extensión de cuerpos teniendo el debido cuidado en los primos ramificados. Esto tomará mayor sentido en la siguiente charla cuando se defina esto. Por el momento estamos interesados en el caso no ramificado, pues es lo que necesitamos para enunciar el teorema principal sobre el cuerpo de clases de Hilbert. Lo primero que haremos será extender la definición del simbolo de Artin, permitiendo definirlo no solo para ideales ideales primos, sino que para cualquier ideal fraccionario de K. Si $\mathfrak{a}$ es un ideal fraccionario de K, entonces podemos factorizar de forma única $\mathfrak{a}$ como producto de ideales primos

$$\mathfrak{a} = \prod_{1 \le i \le r} \mathfrak{p}_i^{r_i}, \ r_i \in \mathbb{Z}$$

Así definimos el simbolo de Artin en el ideal $\mathfrak{a}$ como

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{1 \le i \le r} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}$$

Ahora ya tenemos todos los ingredientes para definir la función de Artin.

Definición 3.1. Sea L/K una extensión abeliana no ramificada, I_K denota el grupo de ideales fraccionarios de K, entonces la **función de Artin** es la aplicación

$$\left(\frac{L/K}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K)$$
$$\mathfrak{a} \mapsto \left(\frac{L/K}{\mathfrak{a}}\right)$$

Observaciones 3.2.

- Usamos el hecho que L/K sea abeliana para que el simbolo de Artin solo dependa del primo en el cuerpo base.
- Estamos usando que la extensión es no ramificada pues el simbolo de Artin se define sobre esos primos.
- El homomorfismo está bien definido, pues está definido en los generadores.

Ahora enunciaremos el teorema principal de esta charla, que relaciona el cuerpo de clases de Hilbert con el número de clases del cuerpo de números.

Teorema 3.3. *Si L el cuerpo de clases de K, entonces la función de Artin $\left(\frac{L/K}{\cdot}\right)$ induce un isomorfismo entre $C(\mathcal{O}_K)$ y $Gal(L/K)$.*

En particular el teorema nos dice que tan grande es el cuerpo de Hilbert, lo cual es muy útil, pues nos permite decidir si una extensión F/K abeliana no ramificada es o no el cuerpo de clases de Hilbert solo mirando el grado de la extensión. Por otro lado automaticamente nos dice que si el anillo de enteros de un cuerpo de numeros K es un dominio de factorización única, entonces el cuerpo de clases de Hilbert es solo K, es decir $H(K)/K$ es una extensión de grado 1. Podemos deducir también un corolario que caracteriza las extensiones abelianas no ramificadas mediante una biyección con los subgrupos del grupo de clases.

Corolario 3.4. *Existe una biyección entre las extensiones abelianas no ramificadas M/K y subgrupos H de $C(\mathcal{O}_K)$. Además la función de Artin induce el isomorfismo*

$$C(\mathcal{O}_K)/H \simeq Gal(M/K)$$

Demostración: Esto es simplemente la correspondencia de Galois y el hecho que todas las subextensiones son de Galois sobre K por ser $H(K)/K$ una extensión abeliana. □

Observación 3.5. El teorema 3.3 le da sentido a la palabra "clases" cuando decimos cuerpo de clases de Hilbert, pues viene del hecho que el grupo de Galois $\mathrm{Gal}(H(K)/K)$ se realiza como un grupo de clases.

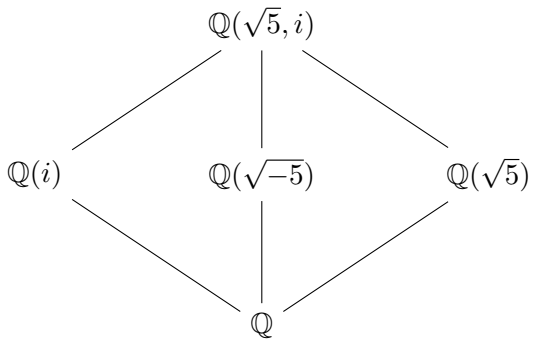
Corolario 3.6. *Si $H(K)$ es el cuerpo de clases de Hilbert de K y $\mathfrak{p}$ un primo finito de K. Entonces $\mathfrak{p}$ escnde completamente en $H(K)$ si y solo si $\mathfrak{p}$ es principal.*

Demostración: Por 2.14 sabemos que $\mathfrak{p}$ escinde completamente en $H(K)$ si y solo si $\left(\frac{H(K)/K}{\mathfrak{p}}\right) = Id$, y a su vez esto es equivalente a que la clase de $\mathfrak{p}$ sea trivial en $C(\mathcal{O}_K)$ por el teorema 3.3, luego concluimos que es equivalente a que $\mathfrak{p}$ sea principal. □

Ahora que sabemos el grado de la extensión $H(K)/K$ podemos dar ejemplos no triviales.

Ejemplo 3.7. Veamos nuevamente el ejemplo de $\mathbb{Q}$, pero desde otro punto de vista. Como el número de clases de $\mathbb{Q}$ es 1, entonces su cuerpo de clases de Hilbert es $\mathbb{Q}$.

Ejemplo 3.8. Sea $K = \mathbb{Q}(\sqrt{-5})$. Para estudiar $H(K)$ primero debemos encontrar el número de clases de K. Sabemos que $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ y con esto deducimos que $d_K = -20$. Luego, el número de clases de K es $h(-20)$. De la charla 1 y 2 (sección 2.2) sabemos que $h(-20) = 2$ y de hecho $C(-20) = \{[x^2 + 5y^2], [2x^2 + 2xy + 3y^2]\}$. Por Teorema 3.3 $[H(K) : K] = 2$. Afirmamos que $\mathbb{Q}(\sqrt{5}, i)$ es el cuerpo de clases de Hilbert de $\mathbb{Q}(\sqrt{-5})$. Observamos que $[\mathbb{Q}(\sqrt{5}, i) : \mathbb{Q}(\sqrt{-5})] = 2$, por lo tanto abeliana. $\mathbb{Q}(\sqrt{5}, i)/\mathbb{Q}(\sqrt{-5})$ es no ramificada al infinito, pues la ramificación en los primos infinitos solo puede aparecer en primos reales, mientras que las incrustaciones de $\mathbb{Q}(\sqrt{-5})$ son complejas. Solo nos falta verificar que $\mathbb{Q}(\sqrt{5}, i)/\mathbb{Q}(\sqrt{-5})$ es no ramificada en los primos finitos. Veamos la siguiente torre de cuerpos.



La extensión $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ es ramificada solo en 5, mientras que la extensión $\mathbb{Q}(\sqrt{5},i)/\mathbb{Q}(\sqrt{5})$ es solo ramificada en 2, pues la extensión está generada por una raíz del polinomio x^2+1, el cual es separable sobre cualquier cuerpos de caracteristica diferente de 2. Por la proposición 3.7 de la charla 12 concluimos que la extensión es no ramificada en primos diferentes de 2. Por otro lado vemos que la extensión ramifica en 2, pues $\mathbb{Q}(i)/\mathbb{Q}$ ramifica en 2, luego $\mathbb{Q}(\sqrt{5},i)/\mathbb{Q}$ lo hace. De este modo $\mathbb{Q}(\sqrt{5},i)/\mathbb{Q}$ ramifica en los primos 2 y 5. Otra cosa que podemos observar del diagrama es que el indice de ramificación de ambos primos es 2. Por otro lado la extensión $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$ es ramificada solo en 2 y 5. $\mathbb{Q}(\sqrt{5},i)/\mathbb{Q}(\sqrt{-5})$ es no ramificada en primos sobre 2 y 5, pues $\mathbb{Q}(\sqrt{5},i)/\mathbb{Q}$ no ramifica en 2 y 5. Además no puede ramificar en primos sobre 2 o 5, pues en ese caso el indice de ramificación de $\mathbb{Q}(\sqrt{5},i)/\mathbb{Q}$ en esos primos sería mayor a 2. De este modo concluimos que $\mathbb{Q}(\sqrt{5},i)/\mathbb{Q}(\sqrt{-5})$ es no ramificada y con eso que $\mathbb{Q}(\sqrt{5},i)$ es el cuerpo de clases de Hilbert de $\mathbb{Q}(\sqrt{-5})$.

4. Apéndice

Nociones de reciprocidad cúbica. La idea de esta sección es entender la aritmética del cuerpo de números $\mathbb{Q}(\sqrt{-3})$ y de su anillo de enteros $\mathbb{Z}[\omega]$(los enteros de Eisenstein) y poder definir el simbolo de Legendre.

Partamos viendo la factorización de los primos de $\mathbb{Z}$ en $\mathbb{Z}[\omega]$, para eso enunciaremos la siguiente proposición

Lema 4.1. *Sea $D \equiv 0,1$ mod 4, y sea m un entero impar coprimo a D. Si D es residuo cuadrático módulo m, entonces m es representado por una forma cudrática de discriminante D.*

Demostración: Supongamos que $D \equiv b^2 \bmod m$. Por ser m impar podemos suponer que D y b tienen igual paridad (reemplazando b por $b+m$ de ser necesario). Por otro lado como $D \equiv 0,1$ mod 4, tenemos que $D \equiv b^2 \bmod 4m$. Luego $D = b^2 - 4mc$ para algún c. Finalizamos fijandonos que $mx^2+bxy+cy^2$ representa a m y tiene discriminante D. □

Proposición 4.2. *Sea p un primo en $\mathbb{Z}$, entonces:*

(i) *Si $p=3$, entonces $1-\omega$ es primo en $\mathbb{Z}[\omega]$ y $3 = -\omega^2(1-\omega)^2$.*
(ii) *Si $p \equiv 1$ mod 3, entonces existe un primo $\pi \in \mathbb{Z}[\omega]$ tal que $p = \pi\overline{\pi}$, y los primos π y $\overline{\pi}$ son no asociados en $\mathbb{Z}[\pi]$*
(iii) *Si $p \equiv 2$ mod 3, entonces p sigue siendo primo en $\mathbb{Z}[\omega]$*

Demostración:

(i) Observamos que $N(1-\omega) = 3$, luego como $N(1-\omega)$ es primo en $\mathbb{Z}$ tenemos que $1-\omega$ es primo en $\mathbb{Z}[\omega]$
(ii) Si $p \equiv 1 \bmod 3$, entonces -3 es cuadrado módulo p, entonces por 4.1 p es repsentado por una forma cuadrática reducida, luego como existe una única forma reducida de discriminante -3, a saber x^2+xy+y^2, concluimos que existen $a,b \in \mathbb{Z}$ tal que $p = a^2 - ab + b^2$, es decir $p = N(\pi)$ con $\pi = a + b\omega \in \mathbb{Z}[\omega]$. De este modo concluimos que $p = \pi\overline{\pi}$, con $\overline{\pi} = a + b\omega^2$
(iii) Fijemonos en el grado de inercia. Como $p \equiv 2 \bmod 3$, tenemos que -3 no es un cuadrado mod p, luego x^2+3 es irreducible en $\mathbb{F}_p[x]$. Así concluimos que sobre p hay solo un primo con indice de ramificación 1 y grado de inercia 2.

□

Antes de continuar observamos que si $\pi\mathbb{Z}[\omega]$ que no divide a $\alpha \in \mathbb{Z}[\omega]$, entonces $\alpha^{N(\pi)-1} \equiv 1$ mod π, lo cual es simplemente la traducción del hecho que en un grupo todo elementos es

anulado cuando lo elevamos al orden del grupo, en este caso el grupo es el grupo multiplicativo del cuerpo residualasociado al primo π.

en este punto estamos en condiciones de definir el simbolo de Legendre.

Lo primero que debemos notar que si π es primo en $\mathbb{Z}[\omega]$, entonces $3|1 - N(\pi)$, lo cual sale de hecho que $N(\pi) = p$ si π está sobre el primo p con $p \equiv 1 \mod 3$, mientras que si $p \equiv 2 \mod 3$ entonces $N(\pi) = p^2$. De este modo vemos que para α no divisidble por π, el elemento $x = \alpha^{N(\pi)-1}/3$ tiene sentido y cumple con $x^3 \equiv 1 \mod \pi$. Es decir, es una raíz de la unidad en el cuerpo residual. por lo tanto

$$\alpha^{(N(\pi)-1)/3} \equiv 1, \omega, \omega^2 \mod \pi$$

Definición 4.3. El **símbolo de Legendre** $\left(\frac{\alpha}{\pi}\right)_3$ como la raíz de la unidad tal que

$$\alpha^{(N(\pi)-1)/3} \equiv \left(\frac{\alpha}{\pi}\right)_3$$

Referencias

[Cox13] David A. Cox. *Primes of the form x^2+ny^2*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication. 2