UNIVERSIDAD AUTÓNOMA METROPOLITANA-IZTAPALAPA

DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA

INERCIA EN CAMPOS CUADRÁTICOS

Tesis que presenta
Edgar Pacheco Castán
Para obtener el grado de
Maestro en Ciencias (Matemáticas)

Asesor: Dr. Mario Pineda Ruelas

Jurado calificador:

Presidente: Dra. Rita Esther Zuazua Vega

Secretario: Dr. Rogelio Fernández-Alonso González

Vocal: Dr. Mario Pineda Ruelas

Ciudad de México, Mayo 2016

UNIVERSIDAD AUTÓNOMA METROPOLITANA-IZTAPALAPA

DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA

INERCIA EN CAMPOS CUADRÁTICOS

Tesis que presenta
Edgar Pacheco Castán
Para obtener el grado de
Maestro en Ciencias (Matemáticas)

Asesor: Dr. Mario Pineda Ruelas

Jurado calificador:

Presidente: Dra. Rita Esther Zuazua Vega

Secretario: Dr. Rogelio Fernández-Alonso González

Vocal: Dr. Mario Pineda Ruelas

Ciudad de México, Mayo 2016

UNIVERSIDAD AUTÓNOMA METROPOLITANA
Iztapalapa

Departamento de Matemáticas

Inercia en Campos Cuadráticos

Proyecto Terminal de la Maestría en Ciencias (Matemáticas)
que se llevó a cabo en los cursos de Introducción a la investigación I, II y III

Presenta

Edgar Pacheco Castán

Asesor

Dr. Mario Pineda Ruelas

México
20 de Mayo de 2016

Agradecimientos

Cuando se tiene en las manos el fruto del trabajo y tras el recuento de los años invertidos en este, las horas dedicadas a pensar e imaginar, incluyendo los desvelos así como los ratos en que abandonaba todo para aclarar la mente y recuperar las fuerzas necesarias para continuar cuando todo lucía nebuloso, es imprescindible detenerme en las parsonas que me ayudaron a hacerlo posible, aquellos que por su mano dura o su sonrisa le dieron sentido a continuar.

Primero quiero mencionar a mis padres, Salvador Pacheco y Elizabeth Castán, quienes me brindaron la oportunidad de retomar el rumbo de mi vida y a pesar de no entender qué hace un matemático, no dudaron en dejarme forjar un camino, mi camino y hoy pueden ver los resultados, gracias por permitirme volar alto, tanto como yo quiera. No tengo hermanos pero hay una personita muy especial en mi vida, que desde hace muchos años ha jugado ese papel, además de ayudarme a ser verdaderamente humano, mi tía *Doña Ena* por enseñarme que siempre se puede ser un adulto y conservar el alma de niño.

Siguiendo con mi famila quiero agradecer a mi tío Hernándo Castán, por mostrarme que la gracia y la cultura son perfectamente compatibles y que abrir la mente es lo más sano que podemos hacer por mejorar al mundo. A mi prima Geovanna Barajas, *Yovis* y su familia por siempre hacerme sentir querido y especial. A mi sobrina Paulina Pacheco, *Pau*, por ser más una amiga y confindente que pariente, sus regaños siempre me ayudaron a enfocarme, gracias muchacha. A mi sobrino y ahijado Emiliano Olvera por enseñarme la responsabilidad que conlleva ser admirado y querido por alguien pequeño. A mis primos, hermanos de diferente mamá, Alfonso Santín y Ena Elizabeth Gatell por ser, válgase la redundancia, los mejores hermanos que no tuve. A mis dos segundas madres, mi tía Eunice Castán, *Niche* por sus inagotables esfuerzos por enseñarnos con su ejemplo a reirnos con la vida y a Celedonia López, *Cele* por no desistir en recordarme que el amor fraternal se cultiva aún con personas nacidas en otra familia.

Continuo con una lista de amigos y ofrezco una disculpa de antemano por si omito a alguno: A Romy Clemente, por ser una gran amiga y tener siempre una sonrisa contagiosa que ayudaba a aliviar momentos aciagos. A Lorena Morales, *Lore* por siempre escuchar mis tonterías con entusiasmo y aconsejarme con cariño. Una mención especial para Janette Ramos *La Boloncha*, por haberme acogido como alguien entrañable desde que pisé esta ciudad y haberme acompañado con gusto por este largo transitar que hoy culmina un paso más, muchas gracias. A José Luis González, *Huicho* y Juan de Dios Carvajal por siempre estar al pendiente de mis progresos y siempre estar dispuestos a recordarme que debo tomarme la vida

menos en serio de lo que yo me exijo. A Jorge Tello por recordarme que tengo sentimientos y sentido del humor. A César Augusto Arroyo por sus muchas inquietudes sobre mi manera de pensar y por mostrarme que el diálogo siempre es la solución.

Desde luego a alguien especial en mi vida, mi pareja, Ilse Valeria Pérez, *Valerita* quien comenzó siendo esa amiga que siempre me decía lo que pensaba, por duro o desagradable que fuera y me escuchaba con ahínco cuando algo me agobiaba y hoy en día es la mujer con quien mejor me entiendo. Gracias loquilla.

Así mismo, quiero agradecer a alguien que se ha convertido en una persona muy especial en mi vida, pues pasó de ser un profesor a ser un gran amigo, confidente, consejero, guía, apoyo, psicólogo y tantas otras cosas, el doctor Mario Pineda por haberme brindado su confianza y sus muchos cuestionamientos que me siguen haciendo crecer como profesional y como persona. Gracias profe, no me alcanza este espacio para mostrarle mi profundo agradecimiento y deuda que tengo con usted por ello.

Finalmente, quiero agradecer a algunas personas más que hicieron posible que culminara mi maestría con un panorama amplio del futuro. A los sinodales, la doctora Rita Zuazua y al doctor Rogelio Fernández-Alonso por el tiempo que se tomaron para evaluar mi trabajo y sus invaluables comentarios para hacerlo más pulcro. Al doctor Gabriel Villa, por haberme aceptado para crecer como profesional y siempre estar dispuesto a brindarme su ayuda en mis planes a mediano plazo. A las doctoras Patricia Saavedra y Shirley Bromberg por ser mujeres tan dedicadas y que pusieron énfasis en que los alumnos avanzaran siempre. Al doctor Luis Casián por brindarme toda la información necesaria para seguir con mis estudios a futuro. A special mention to professor Matt Baker by helping me to clarify my perspectives and his invaluable help in the understanding of some gaps in this thesis. A todos mis compañeros, profesores, secretarias y demás personal de mi muy amada alma mater. Gracias a todos ustedes, pues cada uno jugó un papel importante para estar parado justo donde me encuentro ahora.

Índice general

Introducción

La ramificación es un tema de investigación en la teoría de números que ha llamado la atención de destacados matemáticos durante cientos de años. A manera de introducción al tema comentaremos un ejemplo conocido. El campo gaussiano $\mathbb{Q}(i)$ tiene como anillo de enteros a los enteros gaussianos $\mathbb{Z}[i]$. Este anillo tiene la propiedad que sus elementos pueden escribirse en forma única como producto de primos gaussianos (salvo asociados), tal como sucede en $\mathbb{Z}$. Sin embargo, no todos los primos en $\mathbb{Z}$ siguen siendo primos al ser vistos en $\mathbb{Z}[i]$. Por ejemplo, es fácil ver que $5 = (2+i)(2-i)$ y $(2+i), (2-i)$ son primos no asociados en $\mathbb{Z}[i]$. De hecho, en el anillo de los enteros gaussianos ocurre una y solo una de las siguientes afirmaciones:

1. Un primo $p \in \mathbb{Z}$ se descompone como producto de dos primos gaussianos distintos si y solo si $p = 4k + 1$.
2. Un primo $p \in \mathbb{Z}$ se mantiene primo en $\mathbb{Z}[i]$ si y solo si $p = 4k + 3$.
3. Si $p = 2$, entonces $2 = i(1-i)^2$ y $1 - i$ es primo en $\mathbb{Z}[i]$ (en este caso particular, solamente el 2 tiene esta cualidad).

El que únicamente el 2 tenga tal propiedad en $\mathbb{Z}[i]$ es porque el discriminante del campo $\mathbb{Q}(i)$ es 4 (véase teorema 1.4.9). Los primos racionales de la forma $p = 4k + 3$ siguen siendo primos en $\mathbb{Z}[i]$ (primos inertes) y no tienen un análogo geométrico, seguramente por esto no son considerados en la literatura. De hecho, en la literatura referente a los fenómenos que se desprenden de la ramificación, la carga fuerte se halla en los primos ramificados, quizá porque este es un aspecto de índole geométrico, ya que como lo señala Lorenzini en el capítulo 3, sección 5 de [**21**], existe una correspondencia directa entre un punto de ramificación de una curva proyectiva y el índice de ramificación de un ideal primo en un campo de números. Esta es una buena razón por lo cual se puede ubicar el origen del estudio de la ramificación en la geometría.

El interés de desarrollar el presente trabajo es precisamente el estudio de los primos inertes en el anillo de enteros $\mathcal{O}_K$ de un campo cuadrático $K = \mathbb{Q}(\sqrt{d}\,)$. A lo largo del primer capítulo se presentan las herramientas teóricas aritméticas necesarias para determinar la forma que debe poseer un primo racional q, tal que $q\mathcal{O}_K$ sea un ideal primo de $\mathcal{O}_K$. Así mismo, se presentan todas los fundamentos algebraicos que sostienen el trabajo desarrollado en el capítulo 2 de esta tesis y es precisamente en este capítulo donde se dan de manera explícita la forma de los primos racionales inertes cuando se extienden al anillo $\mathcal{O}_K$, en los casos en que $d = p$, $d = p_1p_2$ y $d = p_1p_2p_3$. En los dos primeros casos el análisis para

determinar cuáles y cómo son los primos inertes es exhaustivo, para el último caso, se dá solamente un bosquejo, puesto que las ideas vistas en los dos primeros son las mismas que se utilizan para este último, con la salvedad que las complicaciones que parecen presentar los primeros se simplifican enormemente y es aquí donde se asoma con claridad la naturaleza combinatoria en la construcción de los primos inertes.

Capítulo 1

Antecedentes

1.1. Resultados sobre teoría básica de números

A continuación presentamos algunas definiciones y resultados de la teoría de números básica de suma importancia en el desarrollo de este trabajo.

Definición 1.1.1. *Sean p un primo impar y $a \in \mathbb{Z}$ tales que $mcd(a,p) = 1$. Se define el símbolo de Legendre como*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & si \quad x^2 \equiv a \pmod{p} \quad \text{para alguna } a \in \mathbb{Z} \\ -1 & si \quad x^2 \not\equiv a \pmod{p} \quad \text{para ninguna } a \in \mathbb{Z} \end{cases}$$

Teorema 1.1.2. *Sean $a, b \in \mathbb{Z}$, p primo impar con $mcd(ab,p) = 1$. Entonces:*

1. $\left(\frac{a^2}{p}\right) = 1, \quad \left(\frac{1}{p}\right) = 1.$
2. *Si* $a \equiv b \pmod{p}$, *entonces* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
4. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

DEMOSTRACIÓN. Véase teorema 3.1.1 de [25]. □

De singular importancia tenemos el siguiente resultado. el cual es una alternativa teórica bastante útil:

Teorema 1.1.3 (Teorema de Euler)**.** *Sean a, p como en el teorema anterior. Entonces*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

DEMOSTRACIÓN. Véase teorema 3.1.1 de [25]. □

Teorema 1.1.4. *(Teorema Chino del Residuo). Sean $m_1, \ldots, m_r \in \mathbb{N}$, tal que $mcd(m_i, m_j) = 1$ para $i \neq j$. Si $a_1, \ldots, a_r \in \mathbb{Z}$, entonces el sistema de congruencias*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

tiene solución única, es decir, cualquier par de soluciones son congruentes módulo $mcm(m_1, \ldots, m_r)$ *y tal solución está dada por* $x = \sum_{i=1}^{r} \frac{m}{m_i} s_i a_i$, *con* $m = \prod_{i=1}^{r} m_i$ *y* s_i *tal que* $\frac{m}{m_i} s_i \equiv 1 \pmod{m_i}$.

DEMOSTRACIÓN. Véanse teorema 2.3.1 y corolario 2.3.2 de [25]. □

Notemos que en el Teorema Chino del Residuo, al cual en adelante denotaremos **TCR**, la condición $mcd(m_i, m_j) = 1$ para $i \neq j$ es crucial; existen sistemas que no cumplen esta condición y son solubles. Para esos casos, requerimos del siguiente resultado.

Teorema 1.1.5. *(Teorema Chino del Residuo Generalizado). Sean* $m_1, \ldots, m_r \in \mathbb{N}$ *y* $\{a_1, \ldots, a_r\} \subset \mathbb{Z}$. *Entonces el sistema*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

es soluble si y solo si $mcd(m_i, m_j) | (a_i - a_j)$.

DEMOSTRACIÓN. Véase teorema 2.3.7 de [25]. □

Para fines de este trabajo, es suficiente trabajar con sistemas de dos congruencias y las soluciones están dadas por $x_{12} = a_1 - \alpha m_1 t = a_2 + \beta m_2 t$, para algún $t \in \mathbb{Z}$. Con esto, cualquier otra solución X del sistema de dos congruencias, cumple $X \equiv x_{12} \pmod{mcm(m_1, m_2)}$(véase lema 2.3.4 de [25]). En adelante, denotaremos al teorema anterior **TCRG**.

El estudio de los valores del símbolo de Legendre se divide en tres casos:

$$\left(\frac{-1}{p}\right), \quad \left(\frac{2}{p}\right), \quad \left(\frac{q}{p}\right)$$

El primero corresponde al inciso 4 del teorema 1.1.2, el segundo viene dado por el siguiente resultado (véase teorema 3.2.1 de [25]) :

Proposición 1.1.6. *Sea* $p \in \mathbb{Z}$ *primo. Entonces*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & si \quad p \equiv 1 \text{ o } 7 \pmod{8} \\ -1 & si \quad p \equiv 3 \text{ o } 5 \pmod{8} \end{cases}$$

DEMOSTRACIÓN. Véase corolario 3.2.4 de [25] □

El tercer caso es la célebre Ley de Reciprocidad Cuadrática (**LRC**)

Teorema 1.1.7. *(Ley de reciprocidad cuadrática). Sean p, q primos impares tales que $p \neq q$. Entonces*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \textit{si} \quad p \textit{ o } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \textit{si} \quad p \textit{ y } q \equiv 3 \pmod 4 \end{cases}$$

DEMOSTRACIÓN. Véanse Teorema 3.2.6 y Corolario 3.2.8 de [25] □

1.2. Resultados sobre campos de números

Sean $K \mid \mathbb{Q}$ un campo de números, con $[K : \mathbb{Q}] = n$. El anillo de enteros de K es

$$\mathcal{O}_K = \{\alpha \in K : f(\alpha) = 0 \text{ para algún } f(x) \in \mathbb{Z}[x] \text{ mónico}\}.$$

Más adelante veremos algunas de las propiedades sobresalientes del anillo $\mathcal{O}_K$. Recordemos que para cualquier campo de números existe $\theta \in \mathbb{C}$ algebraico tal que $K = \mathbb{Q}(\theta)$ es una extensión simple.

Para $\alpha \in K$, se define la función multiplicación por α de la siguiente manera:

$$\begin{aligned} m_\alpha : K &\longrightarrow K \\ x &\mapsto \alpha x \end{aligned}$$

la cual es fácil ver que es $\mathbb{Q}-$lineal. Por tanto, dada una base $\{\omega_1, \ldots, \omega_n\}$ de K sobre $\mathbb{Q}$ es posible representar a m_α con una matríz $A \in M_{n\times n}(\mathbb{Q})$ y esto da lugar a la siguiente definición.

Definición 1.2.1. *Se definen la norma y la traza de α respectivamente como el determinante y la traza de la matríz A y se denotan $N_{K|\mathbb{Q}}(\alpha)$, $T_{K|\mathbb{Q}}(\alpha)$ (si el contexto es claro, las denotaremos simplemente como $N(\alpha), T(\alpha)$).*

En la literatura es común encontrar la definición de norma y traza en términos de las inmersiones de K en $\mathbb{C}$.

Definición 1.2.2. *Sean $\alpha \in K$ y $\sigma_1, \ldots, \sigma_n$ las inmersiones de K en $\mathbb{C}$. Definimos la norma y la traza de α como:*

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \quad y \quad T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

Estas dos definiciones son equivalentes (ver [19] proposición 3.16 página 47) y cada una de ellas ofrece ventajas. Por ejemplo, a partir de la definición 1.2.2 se puede verificar fácilmente que si $\alpha \in \mathcal{O}_K$, entonces $N(\alpha)$ y $T(\alpha)$ son enteros algebraicos y por la definición 1.2.1 son tambien números racionales, asi que a final de cuentas son enteros racionales.

Otra ventaja que ofrece la definición 1.2.2 es que las propiedades fundamentales de la norma y la traza son casi inmediatas.

Proposición 1.2.3. *Sea K un campo de números tal que $[K:\mathbb{Q}]=n$. Si $\alpha,\beta\in K$ y $c\in\mathbb{Q}$, entonces:*

1. $T(\alpha+\beta)=T(\alpha)+T(\beta)$.
2. $N(a\beta)=a^nN(\beta)$.
3. $T(a\alpha)=a\,T(\alpha)$.
4. $N(\alpha\beta)=N(\alpha)N(\beta)$.
5. $N(1)=1$.
6. $N(\alpha^{-1})=N(\alpha)^{-1}$, *si* $\alpha\neq 0$.

DEMOSTRACIÓN. Se siguen directamente de la definición 1.2.2. □

Definición 1.2.4. *Dadas $n\geq 2$ variables $x_1,\ldots,x_n$ sobre un campo L, definimos el discriminante de $x_1,\ldots,x_n$ como:*

$$\Delta_L(x_1,\ldots,x_n):=\prod_{1\leq i<j\leq n}(x_i-x_j)^2\in L[x_1,\ldots,x_n]$$

Definición 1.2.5. *Sea L un campo $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0\in L[x]$ mónico. Definimos el discriminante de $f(x)$ como:*

$$\Delta(f):=\Delta(-a_{n-1},\ldots,(-1)^{n-i}a_i,\ldots,(-1)^na_0).$$

Si $grad(f)=1$, entonces definimos $\Delta(f)=1$.

Proposición 1.2.6. *Sea $f(x)\in L[x]$ mónico con $grad(f)\geq 2$ y $\alpha_1,\ldots,\alpha_n$ las raices de $f(x)$ en su campo de descomposición F. Entonces*

$$\Delta(f)=\prod_{i<j}(\alpha_i-\alpha_j)^2.$$

DEMOSTRACIÓN. Véase proposición 2.4.3 de [10] □

Definición 1.2.7. *Sea $\{\omega_1,\ldots,\omega_n\}$ una base de $K=\mathbb{Q}(\theta)$. Se define el discriminante de $\{\omega_1,\ldots,\omega_n\}$ como:*

$$\Delta(\omega_1,\ldots,\omega_n):=|M|^2,$$

donde $M=\begin{pmatrix}\sigma_1(\omega_1) & \cdots & \sigma_1(\omega_n)\\ \vdots & \ddots & \vdots\\ \sigma_n(\omega_1) & \cdots & \sigma_n(\omega_n)\end{pmatrix}$ *y σ_i son las inmersiones de K en $\mathbb{C}$.*

Proposición 1.2.8. *Sea $\{\omega_1,\ldots,\omega_n\}$ una base de $K=\mathbb{Q}(\theta)$ y $\left(T_{ij}\right)$ la matríz dada por $T_{ij}=T_{K|\mathbb{Q}}(\omega_i\omega_j)$. Entonces $\Delta(\omega_1,\ldots,\omega_n)=\left|\left(T_{ij}\right)\right|$.*

DEMOSTRACIÓN. Observemos el siguiente producto de matrices:

$$\left(M^tM\right)_{ij}=\sum_{k=1}^{n}M^t_{ik}M_{kj}=\left(M^tM\right)_{ij}=\sum_{k=1}^{n}M_{ki}M_{kj}=$$

$$\sum_{k=1}^{n}\sigma_k(\omega_i)\sigma_k(\omega_j)=\sum_{k=1}^{n}\sigma_k(\omega_i\omega_j)=T_{K|\mathbb{Q}}(\omega_i\omega_j).$$

Así, por la definición 1.2.7 se tiene que

$$\Delta(\omega_1,\ldots,\omega_n) = |M|^2 = |M||M| = |M^t||M| = |M^tM| = \big|\big(T_{ij}\big)\big|.$$

□

Notemos que la demostración del resultado anterior permite intercambiar la definición de discriminante en términos de la traza y caracterizarla en términos de las inmersiones $\sigma_i : K \to \mathbb{C}$.

Definición 1.2.9. *Sea $\{\omega_1,\ldots,\omega_n\}$ una base de $K|\mathbb{Q}$. Se dice que $\{\omega_1,\ldots,\omega_n\}$ es una base entera si las siguientes condiciones se cumplen:*

1. $\{\omega_1,\ldots,\omega_n\} \subseteq \mathcal{O}_K$.
2. $\mathcal{O}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$.

OBSERVACIÓN. Las bases enteras se caracterizan por tener discriminante mínimo en valor absoluto. Por lo anterior, cualesquiera dos bases enteras de $\mathcal{O}_K$ tiene el mismo discriminante el cual denotaremos por Δ_K. En adelante, al hablar del discriminante Δ_K, estaremos haciendo referencia a la definición 1.2.7 o a la caracterización dada por la proposición anterior.

Proposición 1.2.10. *Para cualquier ideal $I \neq \{0\}$ de $\mathcal{O}_K$, $\mathcal{O}_K/I$ es finito.*

DEMOSTRACIÓN. Sea I ideal de $\mathcal{O}_K$. Sabemos que existe $\alpha \in I \cap \mathbb{Z}$, tal que $\alpha > 0$. Considere el ideal principal $\langle\alpha\rangle = \alpha\mathcal{O}_K$ y ϕ definida como:

$$\phi\colon \mathcal{O}_K/\langle\alpha\rangle \to \mathcal{O}_K/I$$
$$\delta + \langle\alpha\rangle \mapsto \delta + I.$$

Afirmamos que ϕ es un epimorfismo de grupos, pues:

1. ϕ está bien definida. Si $a + \langle\alpha\rangle = b + \langle\alpha\rangle$, entonces, $a - b \in \langle\alpha\rangle$ y así $\phi(a+\langle\alpha\rangle) = a+I$ y $\phi(b+\langle\alpha\rangle) = b+I$. Como $\langle\alpha\rangle \subseteq I$, esto implica que $a - b \in I$, es decir $a + I = b + I$, y por tanto $\phi(a + \langle\alpha\rangle) = \phi(b + \langle\alpha\rangle)$.
2. ϕ es un morfismo de grupos pues
$$\phi((a + \langle\alpha\rangle) + (b + \langle\alpha\rangle)) = \phi((a + b) + \langle\alpha\rangle) = (a + b) + I =$$
$$(a + I) + (b + I) = \phi(a + \langle\alpha\rangle) + \phi(b + \langle\alpha\rangle)$$
3. ϕ es suprayectiva por definición.

Así, basta demostrar que $\mathcal{O}_K/\langle\alpha\rangle$ es finito. Sea $\delta = \sum_i z_i\omega_i$, con $z_i \in \mathbb{Z}$ y $\{\omega_1,\ldots,\omega_n\}$ base entera de $\mathcal{O}_K$. Como $z_i = q_i\alpha + \gamma_i$, con $0 \leq \gamma_i < \alpha$, se tiene que $\delta = \alpha\sum_i q_i\omega_i + \sum_i \gamma_i\omega_i$, esto implica que $\sum_i \gamma_i\omega_i \in \mathcal{O}_K$, entonces $\delta - \sum_i \gamma_i\omega_i = \alpha\sum_i q_i\omega_i \in \langle\alpha\rangle$ y por tanto $\delta \equiv \sum_i \gamma_i\omega_i \pmod{\langle\alpha\rangle}$ y así

$$\phi(\delta + \langle\alpha\rangle) = \phi(\sum_i \gamma_i\omega_i + \langle\alpha\rangle) = \sum_i \gamma_i\omega_i + I.$$

Por lo anterior $\sum_i \gamma_i\omega_i \in I$. Sea $S = \{\sum_i \gamma_i\omega_i : 0 \leq \gamma_i < \alpha\}$. Como $\sum_i \gamma_i\omega_i = \gamma_1\omega_1 + \cdots + \gamma_n\omega_n$ con α posibles valores para cada γ_i, hay por lo menos α^n elementos en S, pero como $\{\omega_1,\cdots,\omega_n\}$ es una base, S no tiene elementos repetidos, por lo tanto $|S| = \alpha^n$ y $|\mathcal{O}_K/\langle\alpha\rangle| = \alpha^n$. □

Corolario 1.2.11. *$\mathcal{O}_K$ es un anillo Noetheriano.*

DEMOSTRACIÓN. Se sigue directamente de la proposición 1.2.10. □

Puesto que $\mathcal{O}_K$ es integramente cerrado, noetheriano y los ideales primos $\neq 0$ son máximos, entonces $\mathcal{O}_K$ es un dominio de Dedekind.

Definición 1.2.12. *Se define la norma de un ideal $I \neq \{0\}$ de $\mathcal{O}_K$, denotada $N_{K|\mathbb{Q}}(I)$ como*

$$N_{K|\mathbb{Q}}(I) = |\mathcal{O}_K/I|.$$

OBSERVACIÓN. Las dos proposiciones siguientes son consecuencia de la finitud del *grupo de clases de ideales*. Véase el capítulo 12 de [17] páginas 178 - 179.

Proposición 1.2.13. *Sean $H, I, J \neq \{0\}$ ideales de $\mathcal{O}_K$ tales que $HI = HJ$. Entonces $I = J$.*

DEMOSTRACIÓN. Véase proposición 12.2.6 de [17]

Proposición 1.2.14. *Sean I, J ideales de $\mathcal{O}_K$, tales que $I \subset J$. Entonces, existe un ideal H de $\mathcal{O}_K$, tal que $I = JH$.*

DEMOSTRACIÓN. Existe $k \in \mathbb{N}$ tal que $J^k = \langle j \rangle$. Puesto que $I \subset J$, se tiene que $J^{k-1}I \subset J^k = \langle j \rangle$. Por tanto, tomando $H = \left\langle \frac{1}{j} \right\rangle J^{k-1}I$, se tiene el resultado. □

Definición 1.2.15. *Sea D un dominio entero. Un ideal P de D se dice primo si:*

1. *$P \neq D$.*
2. *Si $xy \in P$, entonces $x \in P$ ó $y \in P$.*

OBSERVACIÓN. Si P es un ideal $\neq \{0\}$, entonces $\mathcal{O}_K/P$ es un campo finito y por lo tanto, la definición de ideal primo e ideal máximo coinciden.

Lema 1.2.16. *Un ideal P de D es primo si y solo si, siempre que: para I, J ideales de D, tales que $IJ \subseteq P$, entonces $I \subseteq P$ ó $J \subseteq P$.*

DEMOSTRACIÓN. Sea P un ideal primo de D y supongamos que existen I, J ideales tales que $IJ \subseteq P$, pero $I, J \nsubseteq P$. Entonces, existen $i \in I$, $j \in J$ tales que $i, j \notin P$, sin embargo $ij \in P$, que es primo, lo cual implica que $i \in P$ ó $j \in P$, que contradice la hipótesis. Por lo tanto $I \subseteq P$ ó $I \subseteq P$ si $IJ \subseteq P$. Ahora, supongamos que para I, J ideales de D, tales que $IJ \subseteq P$, se cumple que $I \subseteq P$ ó $J \subseteq P$. Sean $i, j \in D$ no nulos, tales que $ij \in P$. De esta manera $\langle i \rangle$ $\langle j \rangle = \langle ij \rangle \subseteq P$ y de esto se sigue que $\langle i \rangle \subseteq P$ ó $\langle j \rangle \subseteq P$ y por ende $i \in P$ ó $j \in P$, es decir, P es un ideal primo de D. □

Proposición 1.2.17. *Para todo ideal $I \neq \{0\}$ de $\mathcal{O}_K$, $I = P_1 \cdots P_r$, con P_i ideal primo, no todos distintos.*

DEMOSTRACIÓN. Se tiene que I está contenido en un ideal máximo P_1. Por la proposición 1.2.14, se tiene que $I = P_1 B_1$, para algún ideal B_1. Si ocurre que $B_1 \neq \mathcal{O}_K$, de nuevo, B_1 está contenido en un ideal máximo P_2 y por lo tanto

$I = P_1P_2B_2$. Si continuamos con el proceso, se observa que $I \subseteq B_1 \subseteq B_2 \subseteq \cdots$, que es una cadena ascendente y por el corolario 1.2.11, en un número finito de pasos se obtiene que $B_i = \mathcal{O}_K$, es decir, $I = P_1 \cdots P_r$. □

Teorema 1.2.18. *Para I como en la proposición anterior, su factorización en ideales primos es única.*

DEMOSTRACIÓN. Supongamos que

$$I = P_1P_2 \cdots P_r = Q_1Q_2 \cdots Q_s$$

con $r < s$. Entonces $P_1P_2 \cdots P_r = P_1(P_2 \cdots P_r) = Q_1Q_2 \cdots Q_s$ y por 1.2.14 ocurre que $Q_1Q_2 \cdots Q_s \subset P_1$. Como P_1 es un ideal primo, entonces por 1.2.16 podemos suponer que $Q_1 = P_1$ y aplicando 1.2.13 a

$$P_1P_2 \cdots P_r = Q_1Q_2 \cdots Q_s$$

llegamos a que

$$P_2 \cdots P_r = Q_2 \cdots Q_s.$$

Repetimos este proceso r-veces para llegar a que $P_i = Q_i$ para $i = 1, \ldots, r$ y

$$\langle 1 \rangle = Q_{r+1} \cdots Q_s.$$

lo cual implicaría que $1 \in Q_m$, con $r + 1 \leq m \leq s$, lo cual es imposible. Si suponemos ahora que $r > s$, procedemos de manera análoga y se obtiene que $\langle 1 \rangle = P_{s+1} \cdots P_r$ y de nuevo no es posible, por lo tanto $r = s$ y $P_i = Q_i$, es decir, la factorización en ideales primos es única. □

Teorema 1.2.19. *(Teorema Chino del Residuo para Anillos). Sea A un anillo conmutativo con 1, sean $I_1, \ldots, I_n$ ideales de A tales que $I_j + I_k = A$ para $j \neq k$ y sea $I = I_1 \cdots I_n$. Entonces*

$$A/I \cong \prod_{j=1}^{n} A/I_j.$$

DEMOSTRACIÓN. La función:

$$\psi : A \to A/I_1 \times A/I_2$$

$$a \mapsto (a + I_1, a + I_2)$$

es un epimorfismo y $Ker\ \psi = I_1 \cap I_2 = I_1I_2$. Esto implica que

$$A/I_1I_2 \cong A/I_1 \times A/I_2.$$

Ahora consideremos los ideales $I = I_1$ y $J = I_2 \times \cdots \times I_n$ y por el primer caso se sigue el resultado. □

OBSERVACIÓN. Como una aplicación del Teorema Chino del Residuo para Anillos, que en adelante se denotará **TCRA** y de la factorización única de un ideal como producto de ideales primos, es posible demostrar que la norma es una función multiplicativa, es decir, para cualesquiera ideales $I, J \neq 0$ de $\mathcal{O}_K$, se tiene que $N(IJ) = N(I)N(J)$, véase la sección 5.3 de [28].

1.3. El teorema de Dedekind-Kummer

En la sección anterior, vimos que la factorización de un ideal I como producto de ideales primos es única. Agrupando los ideales que se repiten en la factorización resulta que $I = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}$. Con esto, damos paso a las siguientes definiciones.

Definición 1.3.1. *Sea $p \in \mathbb{Z}$ primo y sea $\langle p \rangle = P_1^{e_1} \cdots P_r^{e_r}$. A cada exponente e_i que aparecen en la factorización del ideal $\langle p \rangle \in \mathcal{O}_K$ se le llama el índice de ramificación de P_i sobre p.*

OBSERVACIÓN. Los ideales primos P_i que aparecen en la factorización de $\langle p \rangle$ son los únicos ideales primos de $\mathcal{O}_K$ que contienen al primo racional p.

Para P ideal primo de $\mathcal{O}_K$ y $p \in \mathbb{Z} \cap P$ primo, se tiene que $N(P) = p^f$, por la proposición 1.2.10, para algún $f \in \mathbb{N}$.

Definición 1.3.2. *Al número f de la discusión anterior se le llama el grado de inercia del ideal primo P.*

Si P es un ideal primo de $\mathcal{O}_K$, entonces para $\sigma \in \mathrm{Aut}(K : \mathbb{Q})$ claramente se tiene que $\sigma(P)$ es un ideal primo.

Lema 1.3.3. *Sea $p \in \mathbb{Z}$ primo y sean P_i, P_j ideales primos de $\mathcal{O}_K$, tales que $p \in P_i \cap P_j$. Entonces existe $\sigma \in \mathrm{Aut}(K : \mathbb{Q})$ tal que $\sigma(P_i) = P_j$.*

DEMOSTRACIÓN. Sea $P_G = \{\sigma(P_i) : \sigma \in \mathrm{Aut}(K : \mathbb{Q})\}$ y supongamos que $P_j \notin P_G$. Existe $\alpha \in \mathcal{O}_K$ tal que $\alpha \equiv 0 \pmod{P_j}$, $\alpha \equiv 1 \pmod{\sigma(P_i)}$. Como $N(\alpha) = \prod_{\sigma \in \mathrm{Aut}(K:\mathbb{Q})} \sigma(\alpha)$ y $\alpha \in P_j$, se tiene que $N(\alpha) \in P_j$, y para $\alpha \in \mathcal{O}_K$, $N(\alpha) \in \mathbb{Z}$ y por lo tanto $N(\alpha) \in \mathbb{Z} \cap P_j = \langle p \rangle = P_i \cap \mathbb{Z}$, pues $p \in P_i \cap P_j$ y por tanto $N(\alpha) \in P_i$. Como P_i es primo, para algún $\sigma \in \mathrm{Aut}(K : \mathbb{Q})$, $\sigma(\alpha) \in P_i$, es decir $\alpha \in \sigma^{-1}(P_i)$, pero esto no es posible, pues si lo fuera, como $\alpha \equiv 1 \pmod{\sigma^{-1}(P_i)}$, se tendría que $1 \in \sigma^{-1}(P_i)$, pero por el comentario previo al lema, $\sigma^{-1}(P_i)$ es primo. Por lo tanto $P_j \in P_G$, es decir $\sigma(P_i) = P_j$ para algún $\sigma \in \mathrm{Aut}(K : \mathbb{Q})$. □

Definición 1.3.4. *Un campo de números algebráicos K de grado n sobre $\mathbb{Q}$ se dice monogénico si existe $\theta \in \mathcal{O}_K$ tal que $\{1, \theta, \ldots, \theta^{n-1}\}$ es base entera de $K|\mathbb{Q}$.*

Lema 1.3.5. *Supongamos que $K = \mathbb{Q}(\theta)$ y $F = \mathbb{Q}(\beta)$ donde $f(\beta) = 0$, con $f(x) = Irr_{\mathbb{Q}}(\theta)$. Si K es monogénico, entonces F es monogénico.*

DEMOSTRACIÓN. El isomorfismo:

$$\mathcal{O}_K \longrightarrow \mathcal{O}_F$$

$$\sum_{i=0}^{n-1} z_i \theta^i \mapsto \sum_{i=0}^{n-1} z_i \beta^i$$

implica que $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\beta + \cdots + \mathbb{Z}\beta^{n-1}$, y por lo tanto F es monogénico. □

Lema 1.3.6. *Sean $d_i > 0$ y $a_i \geq 0$, para $i = 1, \ldots, r$. Si $\sum_{i=1}^{r} d_i a_i = 0$, entonces $a_i = 0$, para $i = 1, \ldots, r$.*

DEMOSTRACIÓN. Procedemos por inducción sobre r. Supongamos primero $r = 2$. Entonces $d_1 a_1 + d_2 a_2 = 0$, si digamos $a_1 > 0$, esto implica que $-d_1 a_1 = d_2 a_2 < 0$ y por ende $a_2 < 0$ lo cual no es posible y por tanto $a_1, a_2 = 0$.
Ahora supongamos cierto para $r - 1$. Entonces

$$\sum_{i=1}^{r} d_i a_i = \sum_{i=1}^{r-1} d_i a_i + d_r a_r = 0 + d_r a_r,$$

por lo tanto $a_i = 0$. □

Teorema 1.3.7. *(Teorema de Dedekind-Kummer).*[1] *Sean $K = \mathbb{Q}(\theta)$ monogénico de grado n, $f(x) = Irr_{\mathbb{Q}}(\theta) \in \mathbb{Z}[x]$ y $p \in \mathbb{Z}$ primo. Sea*

$$^{-} : \mathbb{Z} \longrightarrow \mathbb{F}_p$$

$$\overline{f}(x) = g_1(x)^{e_1} \ldots g_r(x)^{e_r}$$

con $g_i(x) \in \mathbb{F}_p[x]$ mónicos irreducible distintos, $e_i \geq 0$ y sean $f_i(x) \in \mathbb{Z}[x]$ mónicos tales que $\overline{f}_i(x) = g_i(x)$, $i = 1, \ldots, r$. Definimos $P_i = \langle p, f_i(\theta) \rangle$. Entonces $P_i, \ldots, P_r$ son ideales primos distintos de $\mathcal{O}_K$ tales que $\langle p \rangle = P_1^{e_1} \cdots P_1^{e_r}$.

DEMOSTRACIÓN. Para $i = 1, \ldots, r$, sea θ_i raíz de $g_i(x) \in \mathbb{F}_p[\theta_i]$ con $\mathbb{F}_p[\theta_i] \simeq \mathbb{F}_p[x]/\langle g_i(x) \rangle$, el cual es un campo finito. Sea $\nu_i : \mathbb{Z} \longrightarrow \mathbb{F}_p[\theta_i]$ el epimorfismo dado por $\nu_i(h(\theta)) = \overline{h}(\theta_i)$. Entonces $\mathbb{Z}[\theta]/Ker(\nu_i) \cong \nu_i(\mathbb{Z}[\theta]) = \mathbb{F}_p[\theta_i]$ es un campo y por tanto $Ker(\nu_i)$ es un ideal primo de $\mathbb{Z}[\theta] = \mathcal{O}_K$.

Es claro que $\nu_i(p) = 0$ y $\nu_i(f_i(\theta)) = 0$, por lo tanto $p, f_i(\theta) \in Ker(\nu_i)$ y con esto $\langle p, f_i(\theta) \rangle \subseteq Ker(\nu_i)$. Ahora, si $g(\theta) \in Ker(\nu_i)$, se tiene que $\overline{g}(\theta_i) = \nu_i(g(\theta)) = 0$ y con ello $g_i(x) | \overline{g}(x)$ en $\mathbb{F}_p[x]$. Así, $\overline{g}(x) = g_i(x)\overline{h}(x) = \overline{f}(x)\overline{h}(x)$ para algún $\overline{h}(x) \in \mathbb{F}_p[x]$. Como $grad(g_i(x)) = grad(\overline{f_i}(x)\overline{h}(x))$, se tiene que $grad(\overline{g}(x) - \overline{f_i}(x)\overline{h}(x)) < grad(g_i(x))$ y $(g - f_i h)(x) = 0$, por tanto, los coeficientes de $(g - f_i h)(x)$ son divisibles por p. Con lo anterior,

$$g(\theta) = (g(\theta) - f_i(\theta)h(\theta)) + f_i(\theta)h(\theta) \in \langle p \rangle + \langle f_i(\theta) \rangle = \langle p, f_i(\theta) \rangle,$$

y así $Ker(\nu_i) \subseteq \langle p, f_i(\theta) \rangle$, es decir, $Ker(\nu_i) = \langle p, f_i(\theta) \rangle = P_i$, con P_i ideal primo de $\mathcal{O}_K$, $i = 1, \ldots, r$.

Ahora veamos que $P_i \neq P_j$ si $i \neq j$. Supongamos que $P_i = P_j$, para $i, j \in \{1, \ldots, r\}$, es decir, $\langle p, f_i(\theta) \rangle = \langle p, f_j(\theta) \rangle$. Por tanto $f_j = pg(\theta) + f_i(\theta)h(\theta)$, para algunos $g(x), h(x) \in \mathbb{Z}[x]$. Aplicando ν_i a esta última ecuación se tiene

$$g_j(\theta) = \overline{f}_j(\theta) = \nu_i(f_j(\theta)) = \nu_i(f_i(\theta)h(\theta)) = g_i(\theta_i)\overline{h}(\theta_i) = 0,$$

[1] Este resultado es nombrado por algunos autores como teorema de Kummer. De acuerdo a Alaca-Williams [3], el resultado es atribuido a Dedekind. Nosotros hemos decidido llamarlo teorema de Dedekind-Kummer.

lo cual implica que $g_i(x)|g_j(x)$ en $\mathbb{F}_p[x]$, es decir, $g_j(x) = g_i(x)l(x)$, para algún $l(x) \in \mathbb{F}_p[x]$. Pero $g_i(x)$ y $g_j(x)$ son mónicos irreducibles en $\mathbb{F}_p[x]$, por lo tanto $l(x) = 1$ y con ello $g_i(x) = g_j(x)$ y por ende $i = j$.

Solo resta ver que $\langle p\rangle = P_1^{e_1} \cdots P_1^{e_r}$. Primero, es fácil ver que para cualesquiera ideales A, B, C se tiene que $(A+B)(A+C) \subseteq A+BC$, con esto, se tiene la contención $\langle p\rangle \supseteq P_1^{e_1} \cdots P_1^{e_r}$, pues

$$P_1^{e_1} \cdots P_1^{e_r} = \langle p, f_1(\theta)\rangle^{e_1} \cdots \langle p, f_r(\theta)\rangle^{e_r} =$$
$$(\langle p\rangle + \langle f_1(\theta)\rangle)^{e_1} \cdots (\langle p\rangle + \langle f_r(\theta)\rangle)^{e_r} \subseteq$$
$$\langle p\rangle + (\langle f_1(\theta)\rangle^{e_1} \cdots \langle f_r(\theta)\rangle^{e_r}) =$$
$$\langle p\rangle + \langle f_1(\theta)^{e_1} \cdots f_r(\theta)^{e_r}\rangle = \langle p\rangle + \langle f(\theta)\rangle = \langle p\rangle.$$

Para la otra contención, notemos que $P_i = \langle p, f_i(\theta)\rangle \supseteq \langle p\rangle$, para $i = 1, \ldots, r$, es decir $P_i|\langle p\rangle$. Por tanto $\langle p\rangle = P_1^{k_1} \cdots P_r^{k_r}$. De hecho, éstos son los únicos ideales en tal factorización pues si P es algún ideal primo distinto de P_i tal que $P|\langle p\rangle$, entonces por el lema 1.3.3, $P = \sigma(P_i)$, para algún $\sigma \in \mathrm{Aut}(K : \mathbb{Q})$ y en consecuencia

$$P = \sigma(\langle p, f_i(\theta)\rangle) = \langle p, f_i(\sigma(\theta))\rangle = \langle p, f_i(\beta)\rangle$$

y por el lema 1.3.5, se puede elegir desde el principio $\theta = \beta$ y con esto $P = P_i$, para algún $i \in \{1, \ldots, r\}$. Ahora, $k_i \leq e_i$, $i = 1, \ldots, r$, pues como $P_1^{e_1} \cdots P_r^{e_r} \subseteq P_1^{k_1} \cdots P_r^{k_r}$, por la proposición 1.2.14, existe un ideal C de $\mathcal{O}_K$ tal que

$$P_1^{e_1} \cdots P_r^{e_r} = P_1^{k_1} \cdots P_r^{k_r} C$$

y por la factorización única de $\langle p\rangle$, se tiene que $C = P_1^{t_1} \cdots P_r^{t_r}$ con $t_i \geq 0$, $i = 1, \ldots, r$, así $P_1^{e_1} \cdots P_r^{e_r} = P_1^{k_1+t_1} \cdots P_r^{k_r+t_r}$. Observemos que

$$\mathcal{O}_K/P_i = \mathbb{Z}[\theta]/P_i = \mathbb{Z}[\theta]/Ker(\nu_i) \simeq \nu_i(\mathbb{Z}[\theta]) = \mathbb{F}_p[\theta_i]$$

Por lo tanto

$$N(P_i) = \left|\mathcal{O}_K/P_i\right| = \left|\mathbb{F}_p[\theta_i]\right| = p^{d_i}$$

donde $d_i = grad(\overline{f}_i)$. Así, por el teorema 1.2.10 y como la norma es multiplicativa, se tiene

$$p^n = N(\langle p\rangle) = N(P_1^{k_1} \cdots P_r^{k_r}) =$$
$$N(P_1^{k_1}) \cdots N(P_r^{k_r}) = (p^{d_1})^{k_1} \cdots (p^{d_r})^{k_r} = p^{\sum_{i=1}^r d_i k_i}$$

y con esto $n = \sum_{i=1}^{r} d_i k_i$. Por otro lado $n = grad(f(x)) = grad(\overline{f}(x))$ por ser mónico, con lo cual $n = \sum_{i=1}^{r} d_i e_i$ ya que $\overline{f}(x) = \overline{f}_1(x)^{e_1} \ldots \overline{f}_(x)^{e_r}$. Por lo tanto

$$\sum_{i=1}^{r} d_i e_i = n = \sum_{i=1}^{r} d_i k_i,$$

lo cual es equivalente a afirmar que $\sum_{i=1}^{r} d_1(e_i - k_1) = 0$. Como $d_i > 0$, $i = 1, \ldots, r$ y $(e_i - k_i) \geq 0$, resulta $e_i = k_i$, $i = 1, \ldots, r$ y con esto se tiene que

$$\langle p \rangle = P_1^{e_1} \cdots P_1^{e_r}.$$

□

Esta última parte de la demostración del teorema de Dedekind-Kummer es de hecho la demostración del siguiente resultado general que relaciona el grado de la extensión $n = [K : \mathbb{Q}]$, con el índice de ramificación e y el grado de inercia f.

Teorema 1.3.8. *Sea K un campo de números de grado n sobre $\mathbb{Q}$, $p \in \mathbb{Z}$ primo y sean e_i, f_i como en las definiciones* 1.3.1 *y* 1.3.2 *respectivamente. Entonces*

$$n = \sum_{i=1}^{r} e_i f_i.$$

DEMOSTRACIÓN. Sean $p \in \mathbb{Z}$ y $\langle p \rangle = P_1^{e_1} \cdots P_r^{e_r}$. Por el **TCRA** (1.2.19) se tiene que

$$\mathcal{O}_K/\langle p \rangle = \mathcal{O}_K/P_1^{e_1} \times \cdots \times \mathcal{O}_K/P_r^{e_r}.$$

Por la parte final en la demostración de la proposición 1.2.10 tenemos $|\mathcal{O}_K/\langle p \rangle| = p^n$. Haciendo uso de la multiplicatividad de la norma

$$p^n = |\mathcal{O}_K/\langle p \rangle| = |\mathcal{O}_K/P_1^{e_1} \times \cdots \times \mathcal{O}_K/P_r^{e_r}| = |\mathcal{O}_K/P_1|^{e_1} \cdots |\mathcal{O}_K/P_r|^{e_r} =$$
$$(p^{f_1})^{e_1} \cdots (p^{f_r})^{e_r} = p^{e_1 f_1} \cdots p^{e_r f_r} = p^{e_1 f_1 + \cdots + e_r f_r} = p^{\sum_{i=1}^{r} e_i f_i}.$$

□

En el caso que la extensión $K|\mathbb{Q}$ es Galois, el resultado anterior se puede reinterpretar de la siguiente manera:

Teorema 1.3.9. *Sean $p \in \mathbb{Z}$ primo y $\langle p \rangle = P_1^{e_1} \cdots P_r^{e_r}$ su factorización como en el teorema 1.3.7 y e_i, f_i como en las definiciones* 1.3.1 *y* 1.3.2 *respectivamente. Entonces $f_1 = \cdots = f_r$, $e_1 = \cdots = e_r$ y $n = ref$.*

DEMOSTRACIÓN. Véase teorema 3', capítulo 12 de [17] □

1.4. Ramificación en un anillo de enteros

El teorema de Dedekind-Kummer nos muestra la forma en que se factoriza el ideal principal $\langle p \rangle$ de $\mathcal{O}_K$. Recordando las definiciones de grado de inercia e índice de ramificación se puede clasificar el comportamiento de tales ideales en tres formas: el ideal $\langle p \rangle$ se descompone, se ramifica o es inerte, dependiendo de qué valores tomen tales exponentes.

Definición 1.4.1. *Sea p un primo racional y consideremos la factorización en $\mathcal{O}_K$:$\langle p\rangle = P_1^{e_1}\cdots P_r^{e_r}$. Diremos que p se ramifica en $\mathcal{O}_K$ si algún $e_i > 1$. Diremos que p se descompone totalmente en $\mathcal{O}_K$ si $e_i = 1$ para $i = 1,\ldots,r$. Diremos que p se ramifica totalmente si $\langle p\rangle = P_1^n$, donde $n = [K:\mathbb{Q}]$. Finalmente, diremos que p es inerte si $\langle p\rangle = P_1$.*

Con ayuda de las ideas desarrolladas en la prueba del Teorema de Dedekind-Kummer, se demostrará un resultado que sirve como criterio para saber si un primo $p \in \mathbb{Z}$ se ramifica o no. Con este resultado, tendremos también un punto de partida hacia el estudio de los primos inertes, pues como veremos, el número de primos ramificados es finito, por tanto, los restantes solo podrán descomponerse o ser inertes.

Proposición 1.4.2. *Sea $K = \mathbb{Q}(\theta)$ un campo de números monogénico y sean $\theta_1,\ldots,\theta_n$ los conjugados de θ. Entonces $\Delta(1,\ldots,\theta^{n-1}) = \Delta(f)$, con $f(x) = Irr_{\mathbb{Q}}(\theta)$.*

DEMOSTRACIÓN. Sea $\{1,\ldots,\theta^{n-1}\}$ base entera de $K|\mathbb{Q}$. Entonces

$$\Delta(1,\ldots,\theta^{n-1}) = \begin{vmatrix} \sigma_1(1) & \cdots & \sigma_1(\theta)^{n-1} \\ \vdots & \ddots & \vdots \\ \sigma_n(1) & \cdots & \sigma_n(\theta)^{n-1} \end{vmatrix}^2 = \begin{vmatrix} 1 & \cdots & \theta_1^{n-1} \\ \vdots & \ddots & \vdots \\ 1 & \cdots & \theta_n^{n-1} \end{vmatrix}^2.$$

Esta última matríz es de tipo Van Der Monde, por lo tanto su discriminante está dado por

$$\prod_{i<j}(\theta_i - \theta_j)^2.$$

Por la proposición 1.2.6, se tiene el resultado. □

Lema 1.4.3. *Sean $K = \mathbb{Q}(\theta)$ un campo de números monogénico y $p \in \mathbb{Z}$ primo. Entonces p se ramifica en $\mathcal{O}_K$ si y solo si $p|\Delta(1,\ldots,\theta^{n-1})$.*

DEMOSTRACIÓN. Sea $f(x) = Irr_{\mathbb{Q}}(\theta)$. Por definición, un primo p se ramifica si y solo si $e_i > 1$ para algún i. Tomando la reducción módulo p de $f(x)$, tenemos

$$\bar{f}(x) = \bar{f}_1^{e_1}(x)\cdots\bar{f}_r^{e_r}(x) \in \mathbb{F}_p[x],$$

con $\bar{f}_i^{e_i}(x)$ mónico irreducible y por lo tanto separable. Esto implica que $e_i > 1$ si y solo si $\bar{f}(x)$ tiene una raíz repetida en algún campo de descomposición sobre $\mathbb{F}_p[x]$ si y solo si $\Delta(\bar{f}) = \bar{0} \in \mathbb{F}_p$.

Por la definición 1.2.4, se tiene que $\Delta(\bar{f}) = \Delta(f) \pmod p$, con lo cual $\Delta(\bar{f}) = \bar{0}$ si y solo si $\Delta(f) \equiv 0 \pmod p$. Así, por la proposición anterior, se tiene que p se ramifica si y solo si $p|\Delta(1,\ldots,\theta^{n-1})$. □

El resultado anterior es válido para campos de números que no son monogénicos y es lo que veremos a continuación (aunque para las necesidades del presente trabajo, basta con el lema 1.4.3). Para ello, primero requerimos algunos hechos y resultados importantes que ahora se presentan.

Por el **TCRA**, tenemos

$$\mathcal{O}_K/\langle p\rangle \cong \mathcal{O}_K/P_1^{e_1} \times \cdots \times \mathcal{O}_K/P_r^{e_r}.$$

Además, si $e_i > 1$ para algún i, entonces $\mathcal{O}_K/P_i^{e_i}$ tiene un elemento nilpotente $\alpha \neq 0$, pues $P_i^{e_i} \subset P_i^{e_i-1} \subset P_i$. Entonces, si $0 \neq \alpha \in P_i$ tenemos que $\alpha^{e_i} \in P_i^{e_i}$, así

$$(\alpha + P_i^{e_i})^{e_i} = \alpha^{e_i} + P_i^{e_i} = P_i^{e_i}$$

y $\alpha \in P_i \setminus P_i^{e_i}$.

Esto implica que la clase de α en $\mathcal{O}_K/\langle p\rangle$ es nilpotente. Si $e_i = 1$, para $i = 1, \ldots, r$, entonces $\mathcal{O}_K/\langle p\rangle$ es un producto de campos y estos no poseen elementos nilpotentes distintos de cero. Así, p se ramifica en K si y solo si $\mathcal{O}_K/\langle p\rangle$ tiene un elemento nilpotente no trivial.

La definición para campos de números de norma, traza y discriminante de una base se puede extender a una extensión de dominios enteros $A \subset B$ con 1 en donde B es un A-módulo libre finitamente generado, es decir $B = Ae_1 \oplus \cdots \oplus Ae_r$, para ciertos elementos $e_1, \cdots, e_r \in B$.

Definición 1.4.4. *Sean A un anillo conmutativo y B una extensión de A tal que $B = Ae_1 \oplus \cdots \oplus Ae_r$. Entonces se define*

$$\Delta_A(e_1, \ldots, e_r) = \left|\left(T_{B|A}(e_ie_j)\right)\right| \in A.$$

Proposición 1.4.5. *Sean $A \subset B$ dominios enteros con 1 tal que B es un A-módulo libre finitamente generado. Si $\{e_1, \ldots, e_r\}$ y $\{e'_1, \ldots, e'_r\}$ son A-bases de B, entonces*

$$\Delta_A(e'_1, \ldots, e'_r) = |(a_{ij})|^2 \Delta_A(e_1, \ldots, e_r),$$

con $a_{ij} \in A$.

En particular,

$$\Delta_A(e'_1, \ldots, e'_r) = \Delta_A(e_1, \ldots, e_r) = 0$$

ó

$$\Delta_A(e'_1, \ldots, e'_r) = u\Delta_A(e_1, \ldots, e_r).$$

para algún u unidad de A.

DEMOSTRACIÓN. Dadas dos A-bases distintas $\{e_1, \ldots, e_r\}$, $\{e'_1, \ldots, e'_r\}$ de B, siempre es posible expresar cada elemento de una en términos de la otra, es decir

$$e'_j = \sum_{i=1}^{r} a_{ij}e_i,$$

donde los $a_{ij} \in A$. Entonces, la traza de productos de los e'_i es

$$T_{B|A}(e'_ie'_j) = T_{B|A}\left[\left(\sum_{k=1}^{r} a_{ki}e_k\right)\left(\sum_{l=1}^{r} a_{li}e_l\right)\right] = \sum_{k=1}^{r}\sum_{l=1}^{r} a_{ki}a_{li}T(e_ie_j),$$

por los incisos 1 y 3 de la proposición 1.2.3.

Así, tomando la matriz de trazas, ocurre que

$$\Big(T_{B|A}(e_i'e_j')\Big) = \Big(a_{ij}\Big)\Big(T_{B|A}(e_ie_j)\Big)\Big(a_{ji}\Big),$$

y por tanto, tomando el determinante a ambos lados de la igualdad anterior, se obtiene

$$\Big|\Big(T_{B|A}(e_i'e_j')\Big)\Big| = \Big|\Big(a_{ij}\Big)\Big(T_{B|A}(e_ie_j)\Big)\Big(a_{ji}\Big)\Big|$$

$$= |(a_{ij})||(a_{ji})|\Delta_A(e_1,\ldots,e_r) = |(a_{ij})|^2\Delta_A(e_1,\ldots,e_r).$$

Para la segunda parte del resultado, notemos que la matriz (a_{ij}), es justamente la matriz cambio de base de $\{e_1',\ldots,e_r'\}$ a $\{e_1,\ldots,e_r\}$ y por ende, es invertible. Así, $|(a_{ij})|$ es una unidad en A y de aquí se sigue que ambos discriminantes o bien son cero o bien son asociados en A. □

Por lo tanto, sin ambigüedad, se puede dar la siguente definición.

Definición 1.4.6. *Dada una base «adecuada» $\{e_1,\ldots,e_r\}$ del A-módulo libre finitamente generado B, se define el discriminante de la extensión B como*

$$\Delta_A(B) := \Delta_A(e_1,\ldots,e_r).$$

Regresamos ahora al anillo de enteros $\mathcal{O}_K$. Si $\{\omega_1,\ldots,\omega_n\}$ es una base entera de $\mathcal{O}_K$ y p es un primo racional, se define el homomofismo

$$\mathcal{O}_K \to \mathcal{O}_K/\langle p\rangle$$

$$y \mapsto y + \langle p\rangle.$$

Para un $y \in \mathcal{O}_K$ arbitrario, existen $z_1,\ldots z_n \in \mathbb{Z}$ tales que

$$y + \langle p\rangle = (z_1\omega_1 + \cdots + z_n\omega_n) + \langle p\rangle =$$

$$(z_1 + \langle p\rangle)(\omega_1 + \langle p\rangle) + \cdots + (z_n + \langle p\rangle)(\omega_n + \langle p\rangle).$$

Si escribimos $z_i = pt_i + r_i$, con $0 \leq r_i < p$, entonces

$$z_i + \langle p\rangle = pt_i + r_i + \langle p\rangle = r_i + \langle p\rangle.$$

Además, es claro que el conjunto $\{\overline{\omega}_i\} = \{\omega_i + \langle p\rangle\}$ forma una base del cociente.

Por lo tanto, la reducción módulo $\langle p\rangle$ de $\mathcal{O}_K$ está dada por

$$\mathcal{O}_K/\langle p\rangle = \bigoplus_{i=1}^{n} \mathbb{F}_p\overline{\omega}_i.$$

Lema 1.4.7. *Para una base entera de $\mathcal{O}_K$ y p un primo racional se tiene*

$$\Delta_{\mathbb{Z}}(\mathcal{O}_K) \pmod p = \Delta_{\mathbb{F}_p}(\mathcal{O}_K/\langle p\rangle).$$

DEMOSTRACIÓN. Sea $\{\omega_1, \ldots, \omega_r\}$ una $\mathbb{Z}$-base de $\mathcal{O}_K$. Entonces, por el comentario previo a este lema, $\{\overline{\omega}_1, \ldots, \overline{\omega}_r\}$ es una $\mathbb{F}_p$-base de $\mathcal{O}_K/\langle p\rangle$. Sean ahora $x \in \mathbb{Z}$ y (m_x) la representación matricial de la transformación lineal m_x respecto a la base $\{\omega_1, \ldots, \omega_r\}$. Entonces, la reducción módulo p de (m_x) es $(m_{\overline{x}})$ respecto a la base $\{\overline{\omega}_1, \ldots, \overline{\omega}_r\}$, para el elemento $\overline{x} \in \mathcal{O}_K/\langle p\rangle$. Por lo tanto tomando la traza correspondiente se tiene

$$T_{\mathcal{O}_K/\langle p\rangle|\mathbb{F}_p}(\overline{x}) = T((m_{\overline{x}})) = T((m_x)) \pmod p = T_{\mathcal{O}_K|\mathbb{Z}}(x) \pmod p$$

y tomando los determinantes se obtiene

$$\Delta_{\mathbb{Z}}(\mathcal{O}_K) \pmod p = \Delta_{\mathbb{F}_p}(\mathcal{O}_K/\langle p\rangle).$$

□

OBSERVACIÓN. Para dominios enteros unitarios A y B,C extensiones de A, se tiene que los elementos $b \in B$ y $c \in C$ se identifican en $B \times C$ como $(b, 0_C)$ y $(0_B, c)$ respectivamente. Por lo tanto, se tiene

$$b \cdot c = (b, 0_C) \cdot (0_B, c) = (0_B, 0_C) = 0_{(B\times C)}.$$

Lema 1.4.8. *Para dominios enteros unitarios A y B_1,B_2 extensiones de A tales que B_1 y B_2 son $A-$módulos libres finitamente generados, entonces, para bases «apropiadas» $\{e_1, \ldots, e_m\}$ y $\{f_1, \ldots, f_n\}$ de B_1 y B_2 respectivamente, se tiene*

$$\Delta_A(B_1 \times B_2) = \Delta_A(B_1)\Delta_A(B_2).$$

DEMOSTRACIÓN. Puesto que $B_1 = \bigoplus_{i=1}^{m} Ae_i \quad y \quad B_2 = \bigoplus_{i=1}^{n} Af_j$, se observa que $\{e_1, \ldots, e_m, f_1, \ldots, f_n\}$ es una base de $B_1 \times B_2$ y además $e_i \cdot f_j = 0$ por la observación previa al enunciado del lema. Esto implica que

$$T_{\mathcal{O}_K/\langle p\rangle|\mathbb{F}_p}(e_i \cdot f_j) = 0 \quad \text{y} \quad T_{\mathcal{O}_K/\langle p\rangle|\mathbb{F}_p}(f_j \cdot e_i) = 0.$$

Por lo tanto

$$\Delta_A(B_1 \times B_2) = \begin{vmatrix} T_{B_1\times B_2|A}(e_i \cdot e_k) & 0 \\ 0 & T_{B_1\times B_2|A}(f_j \cdot f_l) \end{vmatrix}.$$

Además, para $x \in B_i$

$$T_{B_1\times B_2|A}(x) = T_{B_1|A}(x) \quad \text{y} \quad T_{B_1\times B_2|A}(x) = T_{B_2|A}(x).$$

Por lo anterior

$$\Delta_A(B_1 \times B_2) = |T_{B_1|A}(e_i \cdot e_k)||T_{B_2|A}(f_j \cdot f_l)| = \Delta_A(B_1)\Delta_A(B_2).$$

□

Notemos ahora que si un elemento $x \neq 0$ es nilpotente, es decir, $x^r = 0$ para algún $r \in \mathbb{N}$, entonces $(xy)^r = x^r y^r = 0$ y por lo tanto la transformación m_{xy} es nilpotente y por ende su matriz asociada (m_{xy}) también lo es.

Del álgebra lineal sabemos que para una matriz cuadrada A, su polinomio característico tiene la forma $c(\lambda) = \lambda^n - T(A)\lambda^{n-1} + \cdots + (-1)^n|A|$. Además, dadas todas las raices $\lambda_1, \ldots, \lambda_n$ (incluidas sus multiplicidades) de $c(\lambda)$, se tiene que

$$T(A) = \sum_{i=1}^{n} \lambda_i.$$

En particular, si A es nilpotente, el polinomio característico correspondiente es

$$c(\lambda) = (-1)^n \lambda^n$$

y esto implica que $c(\lambda) = 0$ si y solo si $\lambda = 0$ y por lo tanto $T(A) = 0$.

Procedamos a demostrar el resultado general sobre la ramificación de los primos en relación al discriminante.

Teorema 1.4.9. *(Ramificación). Sea $K = \mathbb{Q}(\theta)$ un campo de números de grado n y sea $p \in \mathbb{Z}$ primo. Entonces p se ramifica en $\mathcal{O}_K$ si y solo si $p|\Delta_{\mathbb{Z}}(\mathcal{O}_K)$.*

DEMOSTRACIÓN. Sea $p \in \mathbb{Z}$ y sea $\{\omega_1, \ldots, \omega_n\}$ una base de $\mathcal{O}_K$. Entonces $p|\Delta_{\mathbb{Z}}(\mathcal{O}_K)$ si y solo si $\Delta_{\mathbb{Z}}(\mathcal{O}_K) \equiv 0 \pmod{p}$.

Por el lema 1.4.7 se tiene que

$$\Delta_{\mathbb{Z}}(\mathcal{O}_K) \pmod{p} = \Delta_{\mathbb{F}_p}(\mathcal{O}_K/\langle p\rangle),$$

por lo tanto

$$p|\Delta_{\mathbb{Z}}(\mathcal{O}_K) \text{ si y solo si } \Delta_{\mathbb{F}_p}(\mathcal{O}_K/\langle p\rangle) = \overline{0} \in \mathbb{F}_p.$$

En la descomposición de $\mathcal{O}_K/\langle p\rangle$ mencionada, cada $\mathcal{O}_K/P_i^{e_i}$ es un $\mathbb{F}_p$-espacio vectorial, pues $p \in P_i^{e_i}$, para cada i. Ahora, por el lema 1.4.8, se tiene que

$$\Delta_{\mathbb{F}_p}(\mathcal{O}_K/\langle p\rangle) = \prod_{i=1}^{r} \Delta_{\mathbb{F}_p}(\mathcal{O}_K/P_i^{e_i}).$$

Por tanto, basta probar que para cualquier primo $p \in \mathbb{Z}$ y un ideal P^e tal que $P^e|\langle p\rangle$,

$$\Delta_{\mathbb{F}_p}(\mathcal{O}_K/\langle p\rangle) = \overline{0} \in \mathbb{F}_p \text{ si y solo si } e > 1.$$

Supongamos primero que $e > 1$ y sea $x \in P \setminus P_i^{e_i}$, el cual es un elemento nilpotente no trivial de $\mathcal{O}_K/P_i^{e_i}$. Sea $\{\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n\}$ una base de $\mathcal{O}_K/P_i^{e_i}$ sobre $\mathbb{F}_p$, tal que $\overline{x}_1 = \overline{x}$ es la reducción módulo p de x.

Por los comentarios posteriores al lema 1.4.8,

$$T_{\mathcal{O}_K/\langle p\rangle}(\overline{x}_1\overline{x}_j) = \overline{0},$$

para $j = 1, \ldots, n$ y esto implica que el primer renglón de la matriz

$$(T_{\mathcal{O}_K/\langle p\rangle}(\overline{x}_i\overline{x}_j))$$

está conformado de ceros, con lo cual

$$\Delta_{\mathbb{F}_p}(\mathcal{O}_K/\langle p\rangle) = |(T_{\mathcal{O}_K/\langle p\rangle}(\overline{x}_i\overline{x}_j))| = \overline{0}.$$

Supongamos ahora que $e = 1$. Entonces $\mathcal{O}_K/P^e = \mathcal{O}_K/P$ es un campo finito de característica p donde $|\mathcal{O}_K/P| = p^s$. Por lo tanto, la traza está dada por el polinomio

$$T(t) = t + t^p + t^{p^2} + \cdots + t^{p^{s-1}},$$

donde $grad(T(t)) < |\mathcal{O}_K/P|$ y esto obliga a que $T \neq \overline{0}$ en $\mathcal{O}_K/P$. Con esto queda demostrado el resultado. □

Corolario 1.4.10. *El número de primos ramificados en el anillo de enteros de un campo de números es finito.*

DEMOSTRACIÓN. Para una base entera de $\mathcal{O}_K$, por los comentarios posteriores a la definición 1.2.2 y el teorema fundamental de la aritmética, Δ_K tiene un número finito de divisores, por ende, únicamente lo divide un número finito de primos racionales. □

1.5. El teorema de Dirichlet

En ésta última sección se muestra el célebre resultado conocido como Teorema de Dirichlet para primos en progresión aritmética, mismo que nos asegura que en cada clase $\overline{a} \in \mathbb{F}_p^*$, existe una infinidad de primos $q \neq p$. Para ello se requieren herramientas de la teoría analítica de números y se debe aclarar que el tratamiento que se dará, está lejos del tratamiento algebraico que se ha usado en las otras partes de este capítulo. Los resultados siguientes esencialmente se encuentran en la parte cuatro de Ribenboim [26][2].

Definición 1.5.1. *Sea $(G, \cdot)$ un grupo abeliano finito de orden n y $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Un homomorfismo de grupos*

$$\chi : G \longrightarrow \mathbb{C}^*$$

se le llama caracter de G con valores complejos.

Si $\chi, \chi^{`}$ son caracteres de G, entonces la operación $(\chi \cdot \chi')(a) = \chi(a) \cdot \chi'(a)$ hace que el conjunto de caracteres $\widehat{G}$ de G sea un grupo multiplicativo. Si $o(G) = n$ y $\chi \in \widehat{G}$, entonces para $a \in G$ se tiene $\chi(a^n) = \chi(a)^n = 1$, así que $\chi(G)$ es subgrupo del grupo cíclico de las raíces n-ésimas de 1. Si G es cíclico finito de orden n y $\langle a \rangle = G$, entonces $\chi(a)$ es un generador del grupo de las raíces n-ésimas de 1. Si $\langle \mu \rangle$ es el grupo de las raíces n-ésimas de 1, entonces $\chi(a) = \mu^j$ con $\mathrm{mcd}(j, n) = 1$. Por lo anterior, $\chi(a^r) = \mu^{rj}$ y de esta manera queda caracterizado el caracter χ. Así que $o(\widehat{G}) = n$. La función $f : \widehat{G} \to G$ definida como $f(\chi) = a^j$ es un isomorfismo de grupos. Con ésto, es fácil mostrar que si G es abeliano finito, entonces $\widehat{G} \cong G$.

Definición 1.5.2. *Sea $m \in \mathbb{Z}$, con $m > 1$. Un mapeo $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ se llama caracter modular (módulo m) si satisface lo siguiente:*

1. $\chi(a) = 0$ *si y solo si* $mcd(a, m) > 1$.
2. *Si* $a \equiv b \pmod{m}$, *entonces* $\chi(a) = \chi(b)$.

[2]Complementos esenciales para leer la parte 4 de Ribenboim son [5] y [18].

3. $\chi(ab) = \chi(a)\chi(b)$.

En particular, existe un caracter modular denotado χ_0 definido como:

$$\chi_0(a) = \begin{cases} 1 & \text{si} \quad mcd(a,m) = 1 \\ 0 & \text{si} \quad mcd(a,m) > 1 \end{cases}$$

Si χ es un caracter modulo m y $P(m) = \{a_1, \ldots, a_{\varphi(m)}\}$ son las unidades de $\mathbb{Z}_m$, entonces la función $\widehat{\chi} : P(m) \to \mathbb{C}$ definida como $\widehat{\chi}(a) = \chi(a)$ está bien definida por la condición anterior 2 y $\widehat{\chi}$ es un caracter del grupo abeliano $P(m)$. El mapeo $\chi \to \widehat{\chi}$ es inyectivo.

Definición 1.5.3. *Para $s > 0$ y $a_n \in \mathbb{C}$, se define la serie de Dirichlet como*

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

Se sabe que para cualquier $\delta > 0$, la serie $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ converge uniformemente en el intervalo $[1+\delta, \infty)$ y define una función continua en el intervalo $(1, \infty)$. La función $\zeta(s)$ se conoce como la *función zeta de Riemann* (véase [26] página 489).

Definición 1.5.4. *Sea χ un caracter módulo $m > 1$ y $s > 1$. Se define una L-serie de Dirichlet con respecto a χ como*

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Lema 1.5.5. *El cociente $\dfrac{\zeta(s) - 1}{(s-1)}$ se mantiene acotado cuando $s \to 1^+$ y esto se denota*

$$\zeta(s) \approx \frac{1}{s-1}, \quad \textit{cuando} \quad s \to 1^+.$$

En particular $\lim_{s \to 1^+} (s-1)\zeta(s) = 1$.

DEMOSTRACIÓN. Véase 22.1 D de [26]. □

Proposición 1.5.6. *Sea χ un caracter módulo $m > 1$. Entonces, la L-serie asociada a χ, converge absolutamente para todo $s > 1$. Para todo $\delta > 0$, la L-serie respecto a χ, converge uniformemente en el intervalo $[1+\delta, \infty)$. Por lo tanto, se define una función continua $L(s, \chi)$ de s en $(1, \infty)$:*

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad s > 1.$$

Más aún, $L(s, \chi)$ admite la siguiente representación:

$$L(s, \chi) = \prod_{p} \frac{1}{1 - \frac{\chi(p)}{p^s}}, \quad s > 1.$$

En particular, para el caracter χ_0 módulo m se tiene:

$$L(s,\chi_0)=\prod_{p|m}\left(1-\frac{1}{p^s}\right)\zeta(s),\quad s>1$$

y por tanto, la serie $\displaystyle\sum_{n=1}^{\infty}\frac{\chi_0(n)}{n^s}$ *diverge cuando* $0<s\leq 1$.

DEMOSTRACIÓN. Véase 22.2 G de [26]. □

Así mismo, son hechos conocidos que para $|x|<1$, entonces

$$\log\frac{1}{1-x}=\sum_{n=1}^{\infty}\frac{x^n}{n}$$

y que si el producto infinito de funciones $\prod f_n(s)$ es absolutamente convergente para $s>1$, se tiene

$$\log\prod_n f_n(s)=\sum_n \log f_n(s).$$

En consecuencia, dado un caracter modular χ, cuando $s\to 1^+$, ocurre que

$$\log L(s,\chi)\approx\sum_p\frac{\chi(p)}{p^s}.$$

Lema 1.5.7. *Sea χ un caracter módulo m tal que $\chi\neq\chi_0$. Entonces, para todo $\delta>0$, la serie*

$$\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$$

converge uniformemente en $[\delta,\infty)$. Por lo anterior, la serie define una función continua $L(s,\chi)$ en $(0,\infty)$.

DEMOSTRACIÓN. Véase 21.1 K de [26]. □

Lema 1.5.8. *Sean $G=\{a_0,\ldots,a_{n-1}\}$ y $\widehat{G}=\{\chi_0,\ldots,\chi_{n-1}\}$. Entonces, el sistema de ecuaciones lineales:*

$$\sum_{j=0}^{n-1}\chi_i(a_j)x_j=\beta_i,$$

con $\beta_i\in\mathbb{C}$, $i=0,\ldots,n-1$, tiene solución única y está dada por

$$x_j=\frac{1}{n}\sum_{i=0}^{n-1}\overline{\chi}_i(a_j)\beta_i,$$

donde $\overline{\chi}$ es el conjugado complejo de χ.

DEMOSTRACIÓN. Véase 22.2 I de [26]. □

Lema 1.5.9. *Sea $m \in \mathbb{Z}$. Entonces existe una infinidad de primos p tales que $p \equiv 1 \pmod{m}$. Además, si $s \to 1^+$, se tiene que*

$$\varphi(m) \sum_{p \equiv 1 \pmod{m}} \frac{1}{p^s} \approx \log \frac{1}{s-1},$$

DEMOSTRACIÓN. Véase 24.1 A de [26]. □

Con los resultados anteriores, finalmente podemos dar un paseo por la prueba del célebre Teorema de Dirichlet. Antes reflexionemos un poco sobre lo que establece el enunciado. Consideremos el grupo de unidades del anillo $\mathbb{Z}/m\mathbb{Z}$:

$$\mathcal{U}_m = \{\overline{a} \in \mathbb{Z}/m\mathbb{Z} : mcd(a, m) = 1\},$$

el cual tiene cardinalidad $|\mathcal{U}_m| = \varphi(m)$. El teorema de Dirichlet, establece que siempre que un entero b sea tal que $mcd(b, m) = 1$, este será congruente con una infinidad de primos, es decir, que cada clase de $\mathcal{U}_m$ contiene una infinidad de primos. En particular, cuando la congruencia es respecto a un primo p, entonces $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ es un campo y con ello, cada clase de $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{\overline{0}\}$ es una unidad.

Teorema 1.5.10. *(Teorema de Dirichlet para primos en progresión aritmética). Sean a, $m \in \mathbb{Z}$ tales que $1 \leq a \leq m$ y $mcd(a, m) = 1$. Entonces la progresión aritmética*

$$\{a, a + m, a + 2m, \ldots, a + km, \ldots\}$$

contiene una infinidad de números primos.

DEMOSTRACIÓN. Primero notemos que el caso $a = m$ implica $a = m = 1$, esto es el Teorema Fundamental de la Aritmética.

La idea de la demostración es la siguiente: Dada una clase $\overline{a} \in \mathcal{U}_m$, entonces la serie

$$\sum_{p \in \overline{a}} \frac{1}{p}$$

es divergente, donde la serie corre sobre todos los primos p que hay en la clase $\overline{a}$, lo cual es equivalente a que la clase $\overline{a}$ contiene una infinidad de primos.

Observemos que por 1.5.5 y 1.5.6 se tiene lo siguiente:

$$\log L(s, \chi_0) \approx \log \zeta(s) \approx \sum_p \frac{1}{p^s} \approx \log \frac{1}{1-s}, \quad s \to 1^+.$$

Ahora, si se hace variar $\overline{a}$ sobre las clases de $\mathcal{U}_m$, resulta que

$$\sum_p \frac{\chi(p)}{p^s} = \sum_{\overline{a}} \chi(\overline{a}) \left[\sum_{p \in \overline{a}} \frac{1}{p^s} \right],$$

lo cual podemos interpretar de la siguiente manera:

Para $\mathcal{U}_m = \{\overline{a}_1, \ldots, \overline{a}_{\varphi(m)}\}$, sea $\{\chi_0, \ldots, \chi_{\varphi(m)-1}\}$ el conjunto de los correspondientes caracteres modulares módulo m. Entonces, para $i = 0, \ldots, \varphi(m) - 1$ se tiene

$$\sum_p \frac{\chi_i(p)}{p^s} = \sum_{j=1}^{\varphi(m)} \chi_i(a_j) \left[\sum_{p \equiv a_j \pmod{m}} \frac{1}{p^s} \right]$$

y por 1.5.8, este sistema de ecuaciones tiene por solución

$$\sum_{p \equiv a_j \pmod{m}} \frac{1}{p^s} = \frac{1}{\varphi(m)} \sum_{i=0}^{\varphi(m)-1} \overline{\chi_i(a_j)} \left[\sum_p \frac{\chi_i(p)}{p^s} \right],$$

para $j = 1, \ldots, \varphi(m)$, cuando $s \to 1^+$. Basta ahora probar que el lado derecho de la ecuación anterior no está acotado cuando $s \to 1^+$. Para $i = 0$ se tiene

$$\log L(s, \chi_0) \approx \log \frac{1}{s-1}$$

es decir, el término correspondiente al caracter principal χ_0 no está acotado cuando $s \to 1^+$, por lo tanto, es suficiente mostrar que si $\chi_i \neq \chi_0$, entonces $\log L(s, \chi_i)$ está acotado cuando $s \to 1^+$.

El lema 1.5.7 asegura que si $\chi_i \neq \chi_0$, entonces $\log L(s, \chi_i)$ es una función continua en $(0, \infty)$, con esto

$$\lim_{s \to 1} \log L(s, \chi_i) = \log L(1, \chi_i).$$

Afirmamos que si χ_i es un caracter módular tal que $\chi_i \neq \chi_0$, entonces $L(1, \chi_0) \neq 0$. Consideremos $a_j \equiv 1 \pmod{m}$ en las soluciones del sistema de ecuaciones anterior. Entonces se tiene

$$\sum_{p \equiv 1 \pmod{m}} \frac{1}{p^s} \approx \frac{1}{\varphi(m)} \sum_{i=0}^{\varphi(m)-1} \log L(s, \chi_i),$$

y por 1.5.9

$$\log \frac{1}{s-1} \approx \sum_{i=0}^{\varphi(m)-1} \log L(s, \chi_i), \quad s \to 1^+.$$

De la observación al principio de la demostración, se concluye que

$$\log \frac{1}{s-1} \approx \log \zeta(s) \approx \log L(s, \chi_0), \quad s \to 1^+.$$

Si escribimos $H(s) = \sum_{\chi_i \neq \chi_0} \log L(x, \chi_i)$, observamos que $H(s)$ permanece acotado cuando $s \to 1^+$ y por lo tanto

$$\prod_{\chi_i \neq \chi_0} L(1,\chi_i) = \lim_{s\to 1} \prod_{\chi_i \neq \chi_0} \log L(s,\chi_i) = \lim_{s\to 1} e^{H(s)} \neq 0,$$

lo cual obliga que $L(1,\chi_i) \neq 0$ si $\chi_i \neq \chi_0$.

Por lo tanto, como $\sum_{p\in\overline{a}} \frac{1}{p^s}$ diverge, se tiene que $\sum_{p\in\overline{a}} \frac{1}{p}$ diverge y por ende, hay una infinidad de primos en cada clase $\overline{a} \in \mathcal{U}_m$. □

El teorema anterior es de suma importancia, pues nos asegura que en cualquier clase $\mathbb{F}_p^*$, siempre podremos encontrar primos, lo cual es indispensable para el desarrollo del siguiente capítulo

Capítulo 2

Inercia en extensiones cuadráticas

En el presente captítulo se darán condiciones explícitas para encontrar primos inertes en el anillo de enteros de un campo cuadrático con base en la teoría desarrollada en la primera parte de este trabajo. Una extensión cuadrática es una extensión de grado 2 y es Galois. De acuerdo al teorema 1.3.9, es claro que solo hay tres posibles arreglos de los valores de r, e, f:

r	e	f
2	1	1
1	2	1
1	1	2

Nuestro interés está en el último renglón, es decir, cuando $r = 1$, $e = 1$ y $f = 2$. En adelante se denotará al discriminante de un campo cuadrático por δ_K, por R_p al grupo de residuos cuadráticos de $\mathbb{F}_p^*$ y por N_p a $\mathbb{F}_p^* \setminus R_p$.

2.1. Campos cuadráticos

Cualquier campo cuadrático es de la forma $\mathbb{Q}(\sqrt{d})$ para algún $d \in \mathbb{Z}$ libre de cuadrados. Si $d < 0$, al campo se le llama imaginario y si $d > 0$, al campo se le llama real. Es relativamente fácil mostrar la caracterización del anillo de enteros en el caso cuadrático:

Proposición 2.1.1. *Sea $K = \mathbb{Q}(\sqrt{d})$ un campo cuadrático. Entonces:*

1. *Si $d \equiv 2, 3 \pmod 4$, $\mathcal{O}_K = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$.*
2. *Si $d \equiv 1 \pmod 4$, $\mathcal{O}_K = \{a + b\left(\frac{1+\sqrt{d}}{2}\right) : a, b \in \mathbb{Z}\}$.*

DEMOSTRACIÓN. Véase el teorema 4.2.2 de [29]. □

Proposición 2.1.2. *Sea $K = \mathbb{Q}(\sqrt{d})$ un campo cuadrático y sea δ_K su discriminante. Entonces:*

1. *Si $d \equiv 2, 3 \pmod 4$, entonces $\delta_K = 4d$.*
2. *Si $d \equiv 1 \pmod 4$, entonces $\delta_K = d$.*

DEMOSTRACIÓN. Se sigue de la proposición 1.2.8, utilizando las bases $\{1, \sqrt{d}\}$ y $\{1, \frac{1+\sqrt{d}}{2}\}$ respectivamente. □

El siguiente cuadro resume información importante sobre el anillo de enteros $\mathcal{O}_K$ con $K = \mathbb{Q}(\sqrt{d})$:

$d \pmod 4$	$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}(\rho)$	$Pol.Irred.$	δ_K
2,3	$\rho = \sqrt{d}$	$x^2 - d$	$4d$
1	$\rho = \left(\frac{1+\sqrt{d}}{2}\right)$	$x^2 - x + \frac{1-d}{4}$	d

CUADRO 1. Parámetros para $\mathcal{O}_K$

2.2. Ramificación en una extensión cuadrática

Dado un primo p en $\mathbb{Z}$, por el teorema de Dedekind-Kummer (teorema 1.3.7) conocemos explícitamente la forma de un ideal primo P de $\mathcal{O}_K$ tal que $p \in P$.

El siguente resultado muestra la factorización del ideal $\langle p \rangle$ en $\mathcal{O}_K$, únicamente tengamos presentes los polinomios irreducibles que aparecen en el cuadro 1.

Teorema 2.2.1. *Sea $p \in \mathbb{Z}$ un primo impar.*

1. *Si $p \mid \delta_K$, entonces $\langle p \rangle = P^2$.*
2. *Si $p \nmid \delta_K$ y $x^2 \equiv d \pmod p$ no es soluble en $\mathbb{Z}$, entonces $\langle p \rangle = P$.*
3. *Si $p \nmid \delta_K$ y $x^2 \equiv d \pmod p$ es soluble en $\mathbb{Z}$, entonces $\langle p \rangle = P_1 P_2$, $P_1 \neq P_2$.*

DEMOSTRACIÓN. Supongamos $\delta_K = 4d$, así, la afirmación 1 es inmediata pues $\langle p \rangle$ se ramifica totalmente en $\mathcal{O}_K$. En este caso, notemos que la reducción módulo p de $f(x)$ es $\overline{f}(x) = x \cdot x$. Del teorema de Dedekind-Kummer se tiene que

$$\langle p \rangle = P^2 = \langle p, \sqrt{d} \rangle^2.$$

Supongamos ahora que $p \nmid \delta_K$ y $x^2 \equiv d \pmod p$ no es soluble. Entonces la reducción de $f(x)$ módulo p es $\overline{f}(x) = x^2 - d$ y por Dedekind-Kummer, se tiene que

$$\langle p \rangle = P,$$

es decir, $\langle p \rangle$ es inerte.

Si $p \nmid \delta_K$ y $a^2 \equiv d \pmod p$ para alguna $a \in \mathbb{Z}$, entonces la reducción de $f(x)$ módulo p es $\overline{f}(x) = (x - \sqrt{d})(x + \sqrt{d})$ y evaluando cada factor en $x = \sqrt{d} = a$, se obtiene

$$\langle p \rangle = P_1 P_2 = \langle p, a - \sqrt{d} \rangle \langle p, a + \sqrt{d} \rangle,$$

por lo tanto, $\langle p \rangle$ se descompone totalmente.

Ahora supongamos que $\delta_K = d$. Para la afirmación 1, si $p \mid \delta_K$, la reducción de $f(x)$ módulo p es $\overline{f}(x) = (x - \frac{1}{2})(x - \frac{1}{2})$ pues $p \mid d$ y $\sqrt{d} \equiv 0 \pmod p$. En este caso, evaluando cada factor en $\frac{1+\sqrt{d}}{2}$ obtenemos

$$\langle p \rangle = P^2 = \left\langle p, \frac{\sqrt{d}}{2} \right\rangle^2.$$

Ahora, si $p \nmid \delta_K$ y $x^2 \equiv d \pmod p$ no es soluble, entonces la reducción módulo p de $f(x)$ es $\overline{f}(x) = x^2 - x + \frac{1-d}{4}$, que al evaluarlo en $\frac{1+\sqrt{d}}{2}$ se anula. Lo anterior significa que el ideal $\langle p \rangle$ solo tiene un generador; él mismo. Así $\langle p \rangle = P$ es principal e inerte.

Por último, si $p \nmid \delta_K$ y $a^2 \equiv d \pmod{p}$ para alguna $a \in \mathbb{Z}$, entonces la reducción de $f(x)$ módulo p es $\overline{f}(x) = (x - \frac{1+a}{2})(x - \frac{1-a}{2})$ y de nuevo, al evaluar $\frac{1+\sqrt{d}}{2}$ en cada factor de $\overline{f}(x)$ resulta que

$$\langle p \rangle = P_1 P_2 = \Big\langle p, \frac{a - \sqrt{d}}{2} \Big\rangle \Big\langle p, \frac{a + \sqrt{d}}{2} \Big\rangle.$$

□

El teorema anterior establece que en un campo cuadrático ocurre una y sólo una de las siguientes tres posibilidades:

1. Si $p \mid \delta_K$, entonces $\langle p \rangle$ se ramifica totalmente.
2. Si $p \nmid \delta_K$ y $d \in N_p$, entonces $\langle p \rangle$ es inerte.
3. Si $p \nmid \delta_K$ y $d \in R_p$, entonces $\langle p \rangle$ se descompone totalmente.

2.3. Inercia en una extensión cuadrática $\mathbb{Q}(\sqrt{d})$

Ahora estudiaremos los primos racionales inertes en el anillo de enteros $\mathcal{O}_K$ de una extensión cuadrática $K = \mathbb{Q}(\sqrt{d})$, con $d \in \mathbb{Z} \setminus \{1, 0\}$ libre de cuadrados.

Por el teorema 2.2.1, la condición de solubilidad o insolubilidad de la congruencia $x^2 \equiv d \pmod{p}$ es de vital importancia pues es una de las condiciones para conocer la factorización de un ideal $\langle p \rangle$. Con los resultados siguientes, se tendrá un criterio para determinar si un primo $q \neq p$ en alguna clase de $\mathbb{F}_p^*$ (una vez excluidos los ramificados) es inerte o se descompone totalmente.

2.3.1. Inercia en $\mathbb{Q}(\sqrt{d})$ cuando $d = p$

En esta sección vamos a encontrar los primos inertes en el caso $d = p$ primo. Tengamos presentes las condiciones sobre la ramificación de un primo q impar. Si $p = 2$, entonces $K = \mathbb{Q}(\sqrt{2})$ y $\delta_K = 8$. Por tanto, 2 se ramifica totalmente en $\mathcal{O}_K$ y es el único primo ramificado. Si consideramos ahora $p = -2$, entonces $K = \mathbb{Q}(\sqrt{-2})$ y $\delta_K = -8$, por tanto 2 es el único primo que se ramifica totalmente en $\mathcal{O}_K$. Del análisis anterior, la multiplicatividad del símbolo de Legendre y la proposición 1.1.6, es claro que un primo q impar que no divide a δ_K es inerte en $K = \mathbb{Q}(\sqrt{2})$ si y solo si $q \equiv 3, 5 \pmod{8}$ y es inerte en $K = \mathbb{Q}(\sqrt{-2})$ si y solo si $q \equiv 5, 7 \pmod{8}$.

En adelante supondremos que $d = p$ primo impar, a menos que se indique lo contrario.

Teorema 2.3.1. *Sea $K = \mathbb{Q}(\sqrt{p})$ una extensión cuadrática. Entonces un primo impar q tal que $q \nmid \delta_K$ es inerte en $\mathcal{O}_K$ si ocurre una de las siguientes afirmaciones:*

1. *Si $p \equiv 1 \pmod{4}$, entonces $\left(\frac{p}{q}\right) = -1$ si y solo si $q \equiv s \pmod{p}$ para algún $s \in N_p$.*
2. *Si $p \equiv 3 \pmod{4}$, entonces:*

a) $\left(\frac{p}{q}\right) = -1$ *si y solo si* $q \equiv 3 \pmod 4$ *y* $q \equiv r \pmod p$, *para algún* $r \in R_p$.

b) $\left(\frac{p}{q}\right) = -1$ *si y solo si* $q \equiv 1 \pmod 4$ *y* $q \equiv s \pmod p$, *para algún* $s \in N_p$.

DEMOSTRACIÓN. La afirmación 1 se sigue directamente del *Teorema de Euler* 1.1.3 y la *Ley de reciprocidad cuadrática* 1.1.7. Para la afirmación 2 a), tenemos que el siguiente sistemas de congruencias

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv r \pmod p \end{aligned}$$

es soluble por el **TCR**. Podemos dar explícitamente la forma que debe tener la solución general:

$$x_1 = 4r_i y_1 + 3py_2, r_i \in R_p. \tag{1}$$

Por el teorema de Dirichlet, elegimos q cualquier primo en la clase de x_1 módulo $4p$. Análogamente, para la afirmación 2 b), tenemos el siguiente sistema:

$$\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv s \pmod p \end{aligned}$$

en donde la solución general tiene la forma

$$x_2 = 4s_i w_1 + pw_2, s_i \in N_p. \tag{2}$$

Por el teorema de Dirichlet, elegimos q, cualquier primo en la clase de x_2 módulo $4p$. □

Notemos que en el caso $q = 2$ se tiene que 2 se descompone totalmente si $p \equiv 1 \pmod 4$ pues $\delta_K = p$ y la congruencia $x^2 \equiv p \pmod 2$ siempre es soluble y 2 se ramifica totalmente si $p \equiv 3 \pmod 4$, pues $\delta_K = 4p$.

Las ideas de la prueba del teorema anterior pueden ser usadas si buscamos primos que se descomponen totalmente: resolvemos $\left(\frac{p}{q}\right) = 1$ simplemente cambiando las congruencias del primo q con los elementos de R_p y N_p respectivamente.

Teorema 2.3.2. *Sea* $K = \mathbb{Q}(\sqrt{p})$ *una extensión cuadrática. Entonces un primo* q *se descompone totalmente en* $\mathcal{O}_K$ *si ocurre una de las siguientes afirmaciones:*

1. *Si* $p \equiv 1 \pmod 4$, *entonces* $\left(\frac{p}{q}\right) = 1$ *si y solo si* $q \equiv r \pmod p$ *para algún* $r \in R_p$.
2. *Si* $p \equiv 3 \pmod 4$, *entonces:*

a) $\left(\frac{p}{q}\right) = 1$ *si y solo si* $q \equiv 3 \pmod 4$ *y* $q \equiv s \pmod p$, *para algún* $s \in N_p$.

b) $\left(\frac{p}{q}\right) = 1$ *si y solo si* $q \equiv 1 \pmod 4$ *y* $q \equiv r \pmod p$, *para algún* $r \in R_p$.

DEMOSTRACIÓN. La forma general de q en la afirmación 1 es $q \equiv r \pmod p$ para $r \in R_p$. La solución para la afirmación 2 a) es

$$x_3 = 4r_i\overline{y}_1 + p\overline{y}_2, r_i \in R_p. \tag{3}$$

La solución para la afirmación 2 b) es

$$x_4 = 4s_i\overline{w}_1 + 3p\overline{w}_2, s_i \in N_p. \tag{4}$$

Por lo tanto, tomando a un primo q en la clase de x_3 ó x_4 módulo $4p$, este es inerte. □

En general, es claro que $\mathbb{F}_p^* = \mathbb{F}_{-p}^*$, así que es de esperarse que los resultados conocidos para $p > 0$ son válidos para $-p$, pero no es así. Por ejemplo, en el campo $\mathbb{F}_{-7}$, la congruencia $x^2 \equiv -1 \pmod{-7}$ no es soluble y debería serlo porque $-7 \equiv 1 \pmod 4$. Tenemos la siguiente versión de un resultado conocido, pero para primos $p < 0$:

Teorema 2.3.3. *Sea* $p < 0$ *un número primo. Entonces* $-1 \in R_p$ *si y solo si* $p = -2$ *ó* $p \equiv 3 \pmod 4$.

DEMOSTRACIÓN. Es inmediata. □

Con el teorema anterior, ahora es claro que $\left(\frac{a}{p}\right) = \left(\frac{a}{-p}\right)$, sin embargo, los primos ramificados en $\mathbb{Q}(\sqrt{p})$ no son los mismos que en $\mathbb{Q}(\sqrt{-p})$; la diferencia está marcada por el primo 2: el comentario posterior a la demostración del teorema 2.3.1 asegura que cuando el primo 2 no se ramifica, se descompone totalmente.

Lema 2.3.4. *Sea* $q \in \mathbb{Z}$ *un primo impar. Entonces:*

1. *Si* $q \equiv 1 \pmod 4$, *entonces* $\left(\frac{p}{q}\right) = \left(\frac{-p}{q}\right)$.
2. *Si* $q \equiv 3 \pmod 4$, *entonces* $\left(\frac{p}{q}\right) = -\left(\frac{-p}{q}\right)$.

DEMOSTRACIÓN. Si $q \equiv 1 \pmod 4$, entonces se tiene

$$\left(\frac{-p}{q}\right) = \left(\frac{q}{-p}\right) = \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right).$$

Supongamos ahora que $q \equiv 3 \pmod 4$. Si $-p \equiv 3 \pmod 4$, se tiene

$$\left(\frac{-p}{q}\right) = -\left(\frac{q}{-p}\right) = -\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right),$$

y si $-p \equiv 1 \pmod 4$, se tiene

$$\left(\frac{-p}{q}\right) = \left(\frac{q}{-p}\right) = \left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).$$

□

Teorema 2.3.5. *Sean $K = \mathbb{Q}(\sqrt{p})$, $F = \mathbb{Q}(\sqrt{-p})$ y sea $q \in \mathbb{Z}$ primo racional tal que $q \nmid \delta_K$ y $q \nmid \delta_F$. Entonces:*

1. *Si $q \equiv 1 \pmod 4$, entonces q se comporta del mismo modo en $\mathcal{O}_F$ y en $\mathcal{O}_K$.*
2. *Si $q \equiv 3 \pmod 4$, entonces:*
   a) Si q es inerte en $\mathcal{O}_K$, q se descompone totalmente en $\mathcal{O}_F$.
   b) Si q se descompone totalmente en $\mathcal{O}_K$, q es inerte en $\mathcal{O}_F$.

DEMOSTRACIÓN. Se sigue de los teoremas 2.3.1 al 2.3.3 y el lema anterior. □

Ejemplo 2.3.6. *Sean $K = \mathbb{Q}(\sqrt{5})$ y $F = \mathbb{Q}(\sqrt{-5})$. Entonces $5 \equiv 1 \pmod 4$ y por ende $-5 \equiv 3 \pmod 4$. Lo primero que se obtiene es que en $\mathcal{O}_K$, 2 se descompone totalmente mientras que en $\mathcal{O}_F$, 2 se ramifica totalmente. Los residuos y no residuos cuadráticos en $\mathbb{F}_5^* = \mathbb{F}_{-5}^*$ son $R_5 = \{1, 4\}$ y $N_5 = \{2, 3\}$. Por el teorema 2.3.1, un primo impar $q \in \mathbb{Z}$ es inerte en $\mathcal{O}_K$ si $q \equiv 2, 3 \pmod 5$ y se descompone totalmente si $q \equiv 1, 4 \pmod 5$. Por ejemplo, $17, 47 \equiv 2 \pmod 5$ y $13, 23 \equiv 3 \pmod 5$, por tanto $13, 17, 23, 47$ son inertes en $\mathcal{O}_K$. Ahora, por el teorema 2.3.5, vemos que $13, 17 \equiv 1 \pmod 4$ y por ende, también son inertes en $\mathcal{O}_F$, mientras que $23, 47 \equiv 3 \pmod 4$ y por tanto, por 2.3.2, se descomponen totalmente en $\mathcal{O}_F$. Si $q = 11$, se tiene $11 \equiv 1 \pmod 5$, es decir, se descompone totalmente en $\mathcal{O}_K$ y además $11 \equiv 3 \pmod 4$, por lo tanto, 11 es inerte en $\mathcal{O}_F$.*

Con lo anterior queda completamente determinado el criterio para que un primo $q \neq p$ sea inerte (o totalmente descompuesto) en los respectivos anillos de enteros de $K = \mathbb{Q}(\sqrt{p})$ y $F = \mathbb{Q}(\sqrt{-p})$.

2.3.2. Inercia en $\mathbb{Q}(\sqrt{d})$ cuando $d = p_1p_2$

Por los teoremas 2.2.1, 2.3.1 y 2.3.2, podemos conocer detalladamente la factorización del ideal $\langle q \rangle$, para un primo racional $q \neq p$, en el anillo de enteros $\mathcal{O}_K$ con $K = \mathbb{Q}(\sqrt{p})$. Ahora consideremos el caso $d = p_1p_2$ con p_1, p_2 primos distintos. Siguiendo las ideas de la sección anterior y observando que

$$\left(\frac{d}{q}\right) = \left(\frac{p_1p_2}{q}\right) = \left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right) = -1,$$

determinar la factorización del ideal $\langle q \rangle$ en $\mathcal{O}_K$, con $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{p_1p_2})$, es equivalente a estudiar las condiciones bajo las cuales

$$\left(\frac{p_1}{q}\right) = 1 \;\; y \;\; \left(\frac{p_2}{q}\right) = -1$$

ó

$$\left(\frac{p_1}{q}\right) = -1 \;\; y \;\; \left(\frac{p_2}{q}\right) = 1$$

Con este análisis y el **TCR** (en su versión simple como en la generalizada) es posible encontrar un criterio para determinar cuándo un primo $q \neq p_1, p_2$ es inerte en $\mathcal{O}_K$. Comencemos el estudio de la inercia con el caso más simple; $p_1, p_2 \equiv 1 \pmod 4$.

Teorema 2.3.7. *Sean $d = p_1p_2$, con $p_1, p_2 \equiv 1 \pmod 4$, $p_1 \neq p_2$ y q un primo tal que $q \nmid \delta_K$. Entonces*

$$\left(\frac{d}{q}\right) = -1 \quad \textit{si y solo si} \quad q \equiv x_{j,i} \pmod{p_1p_2}$$

donde

$$x_{1,i} = p_1 s_{i,2} y_2 + p_2 r_{i,1} y_1$$

y

$$x_{2,i} = p_1 r_{i,2} y_2 + p_2 s_{i,1} y_1,$$

con $r_{i,j} \in R_{p_i}$ y $s_{i,j} \in N_{p_i}$, $j = 1, 2$.

DEMOSTRACIÓN. El primer caso de estudio es $\left(\frac{p_1}{q}\right) = 1$ y $\left(\frac{p_2}{q}\right) = -1$. Puesto que $p_1, p_2 \equiv 1 \pmod 4$, tenemos

$$\left(\frac{p_i}{q}\right) = \left(\frac{q}{p_i}\right).$$

Buscamos que el primo q sea descomponga totalmente en $\mathbb{Q}(\sqrt{p_1})$ e inerte respecto a $\mathbb{Q}(\sqrt{p_2})$. Así, por los teoremas 2.3.1 y 2.3.2, se obtiene el siguiente sistema de congruencias:

$$\begin{cases} x \equiv r_{i,1} \pmod{p_1} & \text{con } r_{i,1} \in R_{p_1} \\ x \equiv s_{i,2} \pmod{p_2} & \text{con } s_{i,2} \in N_{p_2}, \end{cases}$$

el cual es soluble por el **TCR** pues $mcd(p_1, p_2) = 1$. Cualquier solución del sistema es de la forma $x_{1,i} = p_1 s_{i,2} y_2 + p_2 r_{i,1} y_1$. Por el Teorema de Dirichlet, elegimos cualquier primo q en la clase de $x_{1,i}$ módulo p_1p_2.

Si ahora pedimos que q se descomponga totalmente en $\mathbb{Q}(\sqrt{p_2})$ y sea inerte en $\mathbb{Q}(\sqrt{p_1})$, entonces el sistema de congruencias

$$\begin{cases} x \equiv s_{i,1} \pmod{p_1} & \text{con } s_{i,1} \in N_{p_1} \\ x \equiv r_{i,2} \pmod{p_2} & \text{con } r_{i,2} \in R_{p_2}, \end{cases}$$

tiene como solución general $x_{2,i} = p_1 r_{i,2} y_2 + p_2 s_{i,1} y_1$. Nuevamente, por el teorema de Dirichlet, elegimos cualquier primo q en la clase de $x_{2,i}$ módulo p_1p_2.

Por lo anterior, si $\left(\frac{d}{q}\right) = -1$, entonces $q \equiv x_{1,i}$ ó $x_{2,i} \pmod{p_1p_2}$.

Inversamente, queremos asegurar la existencia de un primo q que satisfaga

$$\left(\frac{d}{q}\right) = \left(\frac{q}{p_1}\right)\left(\frac{q}{p_2}\right) = -1.$$

Sea $x = p_1 r_{i,2} y_2 + p_2 s_{i,1} y_1$ en donde $r_{i,2} \in R_{p_2}$ y $s_{i,1} \in N_{p_1}$. Primero veamos el caso $p_2 \in R_{p_1}$. Aquí elegimos $y_1 = y_2 = 1$. Se tiene

$$\left(\frac{p_1 r_{i,2} + p_2 s_{i,1}}{p_1}\right) = \left(\frac{p_2 s_{i,1}}{p_1}\right) = \left(\frac{p_2}{p_1}\right)\left(\frac{s_{i,1}}{p_1}\right) = -1.$$

Ahora calculemos el otro símbolo:

$$\left(\frac{p_1 r_{i,2} + p_2 s_{i,1}}{p_2}\right) = \left(\frac{p_1 r_{i,2}}{p_2}\right) = \left(\frac{p_1}{p_2}\right)\left(\frac{r_{i,2}}{p_2}\right) = 1.$$

Por lo anterior

$$\left(\frac{x}{p_1}\right)\left(\frac{x}{p_2}\right) = -1$$

Aplicando el Teorema de Dirichlet, elegimos cualquier primo q en la clase de x módulo $p_1 p_2$.

Ahora veamos el caso $p_2 \in N_{p_1}$. En la expresión $x = p_1 r_{i,2} y_2 + p_2 s_{i,1} y_1$ elegimos $y_1 \in N_{p_1}$ y $y_2 \in N_{p_2}$. Así

$$\left(\frac{p_1 r_{i,2} y_2 + p_2 s_{i,1} y_1}{p_1}\right) = \left(\frac{p_2 s_{i,1} y_1}{p_1}\right) = \left(\frac{p_2}{p_1}\right)\left(\frac{s_{i,1}}{p_1}\right)\left(\frac{y_1}{p_1}\right) = -1.$$

Ahora calculemos el otro símbolo:

$$\left(\frac{p_1 r_{i,2} y_2 + p_2 s_{i,1} y_1}{p_2}\right) = \left(\frac{p_1 r_{i,2} y_2}{p_2}\right) = \left(\frac{p_1}{p_2}\right)\left(\frac{r_{i,2}}{p_2}\right)\left(\frac{y_2}{p_2}\right) = 1.$$

Por lo anterior

$$\left(\frac{x}{p_1}\right)\left(\frac{x}{p_2}\right) = -1.$$

Aplicando el Teorema de Dirichlet, elegimos cualquier primo q en la clase de x módulo $p_1 p_2$.

Finalmente, si consideramos $x' = p_1 s_{i,2} y_2 + p_2 r_{i,1} y_1$, con un argumento casi idéntico al anterior y una elección adecuada de y_1, y_2, aseguramos que existe un número primo q en la clase de x' módulo $p_1 p_2$ que satisface

$$\left(\frac{q}{p_1}\right)\left(\frac{q}{p_2}\right) = -1.$$

Por lo tanto, si $q \equiv x, x' \pmod{p_1 p_2}$, entonces $\left(\frac{d}{q}\right) = -1$. □

Ahora, recordemos que por la ley de reciprocidad cuadrática, si alguno de los elementos involucrados es congruente con 3 módulo 4, es necesario conocer la forma del otro, pues este caso tiene una sutileza importante la cual hay que tratar con sumo cuidado y es la siguiente:

Para un primo q, si p_1, p_2 y $q \equiv 3 \pmod 4$, entonces se tiene

$$\left(\frac{d}{q}\right) = \left(\frac{p_1p_2}{q}\right) = \left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right) = \left(-\left(\frac{q}{p_1}\right)\right)\left(-\left(\frac{q}{p_2}\right)\right) = \left(\frac{q}{p_1}\right)\left(\frac{q}{p_2}\right),$$

mientras que si $p_1, p_2 \equiv 3 \pmod 4$ y $q \equiv 1 \pmod 4$, se tiene

$$\left(\frac{d}{q}\right) = \left(\frac{p_1p_2}{q}\right) = \left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right) = \left(\frac{q}{p_1}\right)\left(\frac{q}{p_2}\right),$$

lo cual aparenta que se comportan igual, sin embargo, la forma del primo q es un factor determinante. Con esta discusión y siguiendo argumentos semejantes al teorema anterior, se obtiene el siguiente resultado.

Teorema 2.3.8. *Sea $d = p_1p_2$, con $p_1, p_2 \equiv 3 \pmod 4$ y $p_1 \neq p_2$. Entonces:*
Si $q \equiv 3 \pmod 4$

$$\left(\frac{d}{q}\right) = -1 \ \textit{ si y solo si } \ q \equiv x_{j,i} \pmod{4p_1p_2},$$

donde

$$x_{1,i} = 3p_1p_2y_1 + 4p_1r_{i,2}y_3 + 4p_2s_{i,1}y_2$$

y

$$x_{2,i} = 3p_1p_2w_1 + 4p_1s_{i,2}w_3 + 4p_2r_{i,1}w_2,$$

con $r_{i,j} \in R_{p_i}$ y $s_{i,j} \in N_{p_i}$.

Si $q \equiv 1 \pmod 4$, entonces

$$\left(\frac{d}{q}\right) = -1 \ \textit{ si y solo si } \ q \equiv \overline{x}_{j,i} \pmod{4p_1p_2},$$

donde

$$\overline{x}_{1,i} = p_1p_2\overline{y}_1 + 4p_1r_{i,2}\overline{y}_3 + 4p_2s_{i,1}\overline{y}_2$$

y

$$\overline{x}_{2,i} = p_1p_2\overline{w}_1 + 4p_1s_{i,2}\overline{w}_3 + 4p_2r_{i,1}\overline{w}_2,$$

con $r_{i,j} \in R_{p_i}$ y $s_{i,j} \in N_{p_i}$

DEMOSTRACIÓN. Necesitamos primero que el primo buscado, sea de la forma $4k+3$, con $k \in \mathbb{Z}$. Con esta restricción y por un argumento análogo al de la demostración del teorema anterior, obtenemos los siguientes sistemas de congruencias:

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv s_{i,1} \pmod{p_1} & \text{con } s_{i,1} \in N_{p_1} \\ x \equiv r_{i,2} \pmod{p_2} & \text{con } r_{i,2} \in R_{p_2} \end{cases}$$

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv r_{i,1} \pmod{p_1} & \text{con } r_{i,1} \in R_{p_1} \\ x \equiv s_{i,2} \pmod{p_2} & \text{con } s_{i,2} \in N_{p_2} \end{cases}$$

Observe que ambos sistemas son solubles por el **TCR**. Para el primero, se obtiene la solución $x_{1,i} = 3p_1p_2y_1 + 4p_1r_{i,2}y_3 + 4p_2s_{i,1}y_2$, cualquier otra solución, es congruente con ésta módulo $4p_1p_2$. Por lo tanto, por el Teorema de Dirichlet, un primo q en la clase de $x_{1,i}$ es inerte.

Procediendo de este mismo modo, con el otro sistema de congruencias, se obtiene la solución $x_{2,i} = 3p_1p_2w_1 + 4p_1s_{i,2}w_3 + 4p_2r_{i,1}w_2$ y por los mismos argumentos un primo q es inerte si está en la case de $x_{2,i}$ módulo $4p_1p_2$.

Por ello, siempre que $\left(\dfrac{d}{q}\right) = -1$, entonces $q \equiv x_{1,i}, x_{2,i} \pmod{4p_1p_2}$.

Ahora, sea $x = 3p_1p_2y_1 + 4p_1r_{i,2}y_3 + 4p_2s_{i,1}y_2$, con $r_{i,2} \in R_{p_2}$ y $s_{i,1} \in N_{p_1}$. Determinaremos el valor del símbolo de Legendre de $\left(\dfrac{x}{p_j}\right)$ del mismo modo que se hizo en el teorema anterior. Supongamos primero que $p_2 \in R_{p_1}$. Si elegimos $y_2 = 1$ y $y_3 \in N_{p_2}$, se tiene que

$$\left(\frac{3p_1p_2y_1 + 4p_1r_{i,2}y_3 + 4p_2s_{i,1}y_2}{p_2}\right) = \left(\frac{4p_1r_{i,2}y_3}{p_2}\right) = 1,$$

$$\left(\frac{3p_1p_2y_1 + 4p_1r_{i,2}y_3 + 4p_2s_{i,1}y_2}{p_1}\right) = \left(\frac{4p_2s_{i,1}y_2}{p_1}\right) = -1.$$

De nueva cuenta, por el Teorema de Dirichlet, si q es un primo en la clase de x módulo $4p_1p_2$, éste es inerte.

Si ahora suponemos que $p_2 \in N_{p_1}$, se tiene que para $y_2 \in N_{p_1}$ y $y_3 = 1$ ocurre

$$\left(\frac{3p_1p_2y_1 + 4p_1r_{i,2}y_3 + 4p_2s_{i,1}y_2}{p_2}\right) = \left(\frac{4p_1r_{i,2}y_3}{p_2}\right) = 1,$$

$$\left(\frac{3p_1p_2y_1 + 4p_1r_{i,2}y_3 + 4p_2s_{i,1}y_2}{p_1}\right) = \left(\frac{4p_2s_{i,1}y_2}{p_1}\right) = -1.$$

y por el mismo argumento, si q es un primo que está en la misma clase de x módulo $4p_1p_2$, éste es inerte.

Análogamente, si consideramos ahora $x' = 3p_1p_2w_1 + 4p_1s_{i,2}w_3 + 4p_2r_{i,1}w_2$, eligiendo w_2 y w_3 de manera adecuada respecto a p_1 y p_2, se tiene

$$\left(\frac{x'}{p_1}\right)\left(\frac{x'}{p_2}\right) = -1.$$

Por lo tanto, si q es un primo en la clase de x' módulo $4p_1p_2$, éste es inerte.

Ahora supongamos que el primo q que buscamos sea de la forma $4k + 1$. Se obtienen los siguientes sistemas de congruencias:

$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv r_{i,1} \pmod{p_1} & \text{con } r_{i,1} \in R_{p_1} \\ x \equiv s_{i,2} \pmod{p_2} & \text{con } s_{i,2} \in N_{p_2} \end{cases}$$

$$\begin{cases} x & \equiv & 1 & (\text{mód } 4) & & \\ x & \equiv & r_{i,1} & (\text{mód } p_1) & \text{con } r_{i,1} & \in R_{p_1} \\ x & \equiv & s_{i,2} & (\text{mód } p_2) & \text{con } s_{i,2} & \in N_{p_2} \end{cases}$$

La demostración es completamente análoga al primer caso de este teorema, eligiendo adecuadamente los correspondientes parámetros $\overline{y}_i$ y $\overline{w}_i$, respecto a p_1 y p_2. Por lo tanto, $\left(\frac{d}{q}\right) = -1$ si y solo si el primo q está en la misma clase de

$$\overline{x}_{1,i} = p_1p_2\overline{y}_1 + 4p_1r_{i,2}\overline{y}_3 + 4p_2s_{i,1}\overline{y}_2$$

o en la clase de

$$\overline{x}_{2,i} = p_1p_2\overline{w}_1 + 4p_1s_{i,2}\overline{w}_3 + 4p_2r_{i,1}\overline{w}_2$$

módulo $4p_1p_2$. □

Con los teoremas 2.3.7 y 2.3.8 se obtienen los primos q inertes en $K = \mathbb{Q}(\sqrt{d})$ cuando $d = p_1p_2$ y ambos primos p_1, p_2 son de la misma forma. Estudiemos ahora que sucede en el caso que $p_1 \equiv 1 \pmod 4$ y $p_2 \equiv 3 \pmod 4$.

Comencemos observando que por los teoremas 2.3.1 y 2.3.2, conocemos la inercia cuando $d = p$. Como veremos, con esto es inmediata la forma de obtener los primos inertes en $K = \mathbb{Q}(\sqrt{p_1p_2})$, con $p_1 \equiv 1 \pmod 4$ y $p_2 \equiv 3 \pmod 4$ y así se obtienen los siguientes resultados.

Teorema 2.3.9. *Sea $d = p_1p_2$, con $p_1 \equiv 1 \pmod 4$ y $p_2 \equiv 3 \pmod 4$. Si $q \equiv 1 \pmod 4$, entonces $\left(\frac{d}{q}\right) = -1$ si y solo si q se encuentra en alguna de las clases*

$$x_{1,i} = p_1p_2y_1 + 4r_{i,1}p_2y_2 + 4s_{i,2}p_1y_3$$

ó

$$x_{2,i} = p_1p_2w_1 + 4s_{i,1}p_2w_2 + 4r_{i,2}p_1w_3$$

módulo $4p_1p_2$, para $r_{i,j} \in R_{p_j}$, $s_{i,j} \in N_{p_j}$.

DEMOSTRACIÓN. Puesto que $\left(\frac{p_1}{q}\right) = \left(\frac{q}{p_1}\right)$ y $\left(\frac{p_2}{q}\right) = \left(\frac{q}{p_2}\right)$, es suficiente que $q \in R_{p_1} \cap N_{p_2}$ ó $q \in N_{p_1} \cap R_{p_2}$. En el primer caso debemos resolver el sistema

$$\begin{cases} x & \equiv & 1 & (\text{mód } 4) & & \\ x & \equiv & r_{i,1} & (\text{mód } p_1) & \text{con } r_{i,1} & \in R_{p_1} \\ x & \equiv & s_{i,2} & (\text{mód } p_2) & \text{con } s_{i,2} & \in N_{p_2} \end{cases}$$

y en el segundo caso debemos resolver

$$\begin{cases} x & \equiv & 1 & (\text{mód } 4) & & \\ x & \equiv & s_{i,1} & (\text{mód } p_1) & \text{con } s_{i,1} & \in N_{p_1} \\ x & \equiv & r_{i,2} & (\text{mód } p_2) & \text{con } r_{i,2} & \in R_{p_2} \end{cases}$$

Es claro que ambos sistemas son solubles y las soluciones respectivas son

$$x_{1,i} = p_1p_2y_1 + 4r_{i,1}p_2y_2 + 4s_{i,2}p_1y_3$$

y

$$x_{2,i} = p_1p_2w_1 + 4s_{i,1}p_2w_2 + 4r_{i,2}p_1w_3.$$

Inversamente, como en los teoremas 2.3.7 y 2.3.8 , eligiendo adecuadamente los y_i, w_i respecto a los p_j correspondientes, cualquier primo q en la clase de $x_{j,i}$ módulo $4p_1p_2$, es inerte en $\mathbb{Q}(\sqrt{p_1p_2})$. □

Teorema 2.3.10. *Sea $d = p_1p_2$, con $p_1 \equiv 1 \pmod 4$ y $p_2 \equiv 3 \pmod 4$. Si $q \equiv 3 \pmod 4$, entonces $\left(\frac{d}{q}\right) = -1$ si y solo si q se encuentra en alguna de las clases*

$$x_{1,i} = 4p_1y_3r_{i,1} + 4p_2y_2r_{i,2} + 3p_1p_2y_1$$

ó

$$x_{2,i} = 4p_1w_3s_{i,1} + 4p_2w_2s_{i,2} + 3p_1p_2w_1,$$

con $r_{i,j} \in R_{p_j}$, $s_{i,j} \in N_{p_j}$.

DEMOSTRACIÓN. Puesto que $\left(\frac{p_1}{q}\right) = \left(\frac{q}{p_1}\right)$ y $\left(\frac{p_2}{q}\right) = -\left(\frac{q}{p_2}\right)$, es suficiente que $q \in R_{p_1} \cap R_{p_2}$ ó $q \in N_{p_1} \cap N_{p_2}$. En el primer caso debemos resolver el sistema:

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv r_{i,1} \pmod{p_1} & \text{con } r_{i,1} \in R_{p_1} \\ x \equiv r_{i,2} \pmod{p_2} & \text{con } r_{i,2} \in R_{p_2} \end{cases}$$

y para el segundo caso, el sistema:

$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv s_{i,1} \pmod{p_1} & \text{con } s_{i,1} \in N_{p_1} \\ x \equiv s_{i,2} \pmod{p_2} & \text{con } s_{i,2} \in N_{p_2} \end{cases}$$

donde la primera y tercera congruencia en cada sistema son las condiciones para el los valores $-1, 1$, respectivamente, del símbolo de Legendre de $\left(\frac{p_2}{q}\right)$, cuando $p_2 \equiv 3 \pmod 4$. De nueva cuenta, ambos sistemas son solubles por el **TCR**. Por lo tanto, cualquier primo q que esté en la clase de las respectivas soluciones $x_{j,i}$, es inerte.

En el otro sentido de las implicaciones simplemente hay que elegir de forma adecuada los valores de y_i y w_i respecto a p_1 y p_2 en las x y x' propuestas. Con esto, el símbolo de Legendre $\left(\frac{d}{q}\right) = -1$, siempre que el primo q esté en la clase correspondiente módulo $4p_1p_2$. □

Con este último teorema, se tiene explícitamente la forma de los primos q inertes en $K = \mathbb{Q}(\sqrt{p_1p_2})$, cuando $p_1, p_2 > 0$. Resta ver como deben ser los primos q inertes en $K = \mathbb{Q}(\sqrt{-d})$, con $-d < 0$, lo cual haremos a continuación.

Ahora estudiemos el caso $d = p_1p_2 < 0$. Notemos primero que $-d < 0$ implica que $-p_1 < 0$ y $p_2 > 0$, ó $p_1 > 0$ y $-p_2 < 0$. Analizando el símbolo de Legendre tenemos lo siguiente:

$$\left(\frac{-d}{q}\right) = \left(\frac{-(p_1p_2)}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right),$$

y por otro lado se tiene

$$\left(\frac{-1}{q}\right)\left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right) = \left(\frac{-p_1}{q}\right)\left(\frac{p_2}{q}\right) = \left(\frac{p_1}{q}\right)\left(\frac{-p_2}{q}\right).$$

Este análisis, nos dice que buscar los primos q inertes en $K = \mathbb{Q}(\sqrt{-d})$ es equivalente a encontrar las condiciones bajo las cuales

$$\left(\frac{-1}{q}\right)\left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right) = -1.$$

Esta última observación nos permite discriminar los casos que son posibles. Se necesita o bien que los tres símbolos tomen el valor de -1 o únicamente uno de ellos. Sin embargo, notemos que cuando $\left(\frac{-1}{q}\right) = 1$, entonces $q \equiv 1 \pmod 4$, mientras que si $\left(\frac{-1}{q}\right) = -1$, se tiene $q \equiv 3 \pmod 4$ y por el teorema 2.3.2 y su observación posterior, se tienen todos los ingredientes para determinar las condiciones de inercia en $\mathcal{O}_K$ cuando $d < 0$.

Proposición 2.3.11. *Sean $K = \mathbb{Q}(\sqrt{-p_1p_2})$ y $q \in \mathbb{Z}$ primo, tal que $q \equiv 1 \pmod 4$ y $p_1, p_2 > 0$ primos racionales. Entonces las condiciones de inercia para q son las mismas que en los teoremas 2.3.7, 2.3.8, 2.3.9 según la forma de p_i.*

DEMOSTRACIÓN. Puesto que $q \equiv 1 \pmod 4$, entonces el factor

$$\left(\frac{-1}{q}\right) = 1,$$

y por ende

$$\left(\frac{-1}{q}\right)\left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right) = \left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right).$$

Por tanto, todo se reduce a estudiar $\left(\frac{p_1p_2}{q}\right) = -1$, lo cual ya hicimos en los teoremas 2.3.7, 2.3.8, 2.3.9. Si $p_1, p_2 \equiv 1 \pmod 4$, aplicamos el teorema 2.3.7. Si $p_1, p_2 \equiv 3 \pmod 4$, aplicamos la segunda parte del teorema 2.3.8. Si $p_1 \equiv 1 \pmod 4$, $p_2 \equiv 3 \pmod 4$, aplicamos el teoema 2.3.9. Por tanto q es inerte en $\mathbb{Q}(\sqrt{-p_1p_2})$ dependiendo de la forma de p_1 y p_2.

□

Ahora estudiemos el caso $q \equiv 3 \pmod 4$. Notemos primero que:

1. Cuando $p_1, p_2 \equiv 1 \pmod 4$, entonces
$$\left(\frac{-1}{q}\right)\left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right) = -\left(\left(\frac{q}{p_1}\right)\left(\frac{q}{p_2}\right)\right) = -\left(\frac{q}{p_1}\right)\left(\frac{q}{p_2}\right).$$
2. Cuando $p_1, p_2 \equiv 3 \pmod 4$, entonces
$$\left(\frac{-1}{q}\right)\left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right) = -\left(-\left(\frac{q}{p_1}\right)\right)\left(-\left(\frac{q}{p_2}\right)\right) = -\left(\frac{q}{p_1}\right)\left(\frac{q}{p_2}\right).$$
3. Cuando $p_1 \equiv 1 \pmod 4$ y $p_2 \equiv 3 \pmod 4$, entonces
$$\left(\frac{-1}{q}\right)\left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right) = -\left(\left(\frac{q}{p_1}\right)\left(-\left(\frac{q}{p_2}\right)\right)\right) = \left(\frac{q}{p_1}\right)\left(\frac{q}{p_2}\right).$$

Por lo tanto, se necesita que los símbolos tengan el mismo valor en todos los casos y para ello, recurrimos a los teoremas 2.3.1 y 2.3.2 que establecen los valores adecuados de los respectivos símbolos. Para la afirmación 1 anterior, por un argumento análogo al del teorema 2.3.7, se tiene que

$$\left(\frac{d}{q}\right) = -1 \quad \text{si y solo si} \quad q \equiv x_{j,i} \pmod{4p_1p_2}$$

donde

$$x_{1,i} = 3p_1p_2y_1 + 4p_1r_{i,2}y_3 + 4p_2r_{i,1}y_2$$

y

$$x_{2,i} = 3p_1p_2w_1 + 4p_1s_{i,2}w_3 + 4p_2s_{i,1}w_2,$$

con $r_{i,j} \in R_{p_i}$ y $s_{i,j} \in N_{p_i}$. En la forma de $x_{1,i}$ y $x_{2,i}$ ya está impuesta la condición $q \equiv 3 \pmod 4$.

Para el caso 2, por un argumento análogo a la primera afirmación del teorema 2.3.8, se tiene que

$$\left(\frac{d}{q}\right) = -1 \text{ si y solo si } q \equiv x_{j,i} \pmod{4p_1p_2},$$

donde

$$x_{1,i} = 3p_1p_2y_1 + 4p_1s_{i,2}y_3 + 4p_2s_{i,1}y_2$$

y

$$x_{2,i} = 3p_1p_2w_1 + 4p_1r_{i,2}w_3 + 4p_2r_{i,1}w_2,$$

con $r_{i,j} \in R_{p_i}$ y $s_{i,j} \in N_{p_i}$, con las adecuadas elecciones de y_i, w_i.

Finalmente, para la afirmación 3, primero notemos que

$$\left(\frac{d}{q}\right) = -1 \quad \text{si y solo si} \quad \left(\frac{p_1}{q}\right) = \left(\frac{p_2}{q}\right).$$

por un argumento similar al usado en la prueba del teorema 2.3.10, se tiene que

$$\left(\frac{d}{q}\right) = -1 \text{ si y solo si } q \equiv x_{j,i} \pmod{4p_1p_2},$$

donde

$$x_{1,i} = 3p_1p_2y_1 + 4p_1s_{i,2}y_3 + 4p_2r_{i,1}y_2$$

y

$$x_{2,i} = 3p_1p_2w_1 + 4p_1r_{i,2}w_3 + 4p_2s_{i,1}w_2,$$

con $r_{i,j} \in R_{p_i}$ y $s_{i,j} \in N_{p_i}$, con las adecuadas elecciones de y_i, w_i.

De esta manera, queda demostrado el siguiente resultado:

Proposición 2.3.12. *Sean $K = \mathbb{Q}(\sqrt{-p_1p_2})$ y $q \in \mathbb{Z}$ primo, tal que $q \equiv 3 \pmod 4$ y $p_1, p_2 > 0$ primos racionales.. Entonces, el primo racional q es inerte si y sólo si $q \equiv x_{j,i} \pmod{4p_1p_2}$ como en el análisis previo.*

□

Solo resta estudiar el caso $d = 2p$ y el estudio de la inercia estará completo. Se aprovechará la proposición 1.1.6 (que nos describe la naturaleza cuadrática del primo 2), junto con los teoremas 2.3.1 y 2.3.2 , para conocer explícitamente la inercia de un primo q, cualquiera que sea su residuo módulo 4. Primero analicemos el caso $p \equiv 1 \pmod 4$.

Teorema 2.3.13. *Sea $K = \mathbb{Q}(\sqrt{d})$, con $d = 2p$ y $2 \neq p \in \mathbb{N}$ primo. Entonces, si $p \equiv 1 \pmod 4$, $\left(\frac{d}{q}\right) = -1$ si y solo si $q \equiv x_j \pmod{8p}$, con*

$$x_1 = 8s_iy_1 + py_2 \quad y \quad x_2 = 8s_i\overline{y}_1 + 7p\overline{y}_2, s_i \in N_p$$

$$x_3 = 8r_iw_1 + 3pw_2 \quad y \quad x_4 = 8r_i\overline{w}_1 + 5p\overline{y}_2, r_i \in R_p.$$

DEMOSTRACIÓN. Simplemente consideremos los siguientes sistemas:

$$\begin{cases} x \equiv s_i \pmod p & \text{con } s_i \in N_p \\ x \equiv 1,7 \pmod 8 \end{cases}$$

$$\begin{cases} x \equiv r_i \pmod p & \text{con } r_i \in R_p \\ x \equiv 3,5 \pmod 8 \end{cases}$$

Por el **TCR**, se tienen las respectivas soluciones x_j descritas en el enunciado del teorema y con ello se tiene una implicación. En el otro sentido, la demostración es como en los resultados anteriores, simplemente eligiendo de manera adecuada los $y_i, \overline{y_i}, w_i, \overline{w_i}$ en las soluciones propuestas. Por tanto, q es inerte en $\mathcal{O}_K$ si y solo si $q \equiv x_j \pmod{8p}$. □

El caso $p \equiv 3 \pmod 4$, es un poco delicado pues las ecuaciones (1), (2) que aparecen en la prueba del teorema 2.3.1 y las ecuaciones (3) y (4) en la demostración del teorema 2.3.2, combinadas con las condiciones de la proposición 1.1.6 adecuadas, llevan a establecer los siguientes sistemas de congruencias:

$$\begin{cases} x \equiv 7 \pmod 8 \\ x \equiv x_2 \pmod{4p} \end{cases}, \quad \begin{cases} x \equiv 1 \pmod 8 \\ x \equiv x_1 \pmod{4p} \end{cases}$$

$$\begin{cases} x \equiv 5 \pmod 8 \\ x \equiv x_3 \pmod{4p} \end{cases}, \quad \begin{cases} x \equiv 3 \pmod 8 \\ x \equiv x_4 \pmod{4p} \end{cases}$$

$$\begin{cases} x \equiv 7 \pmod 8 \\ x \equiv x_1 \pmod{4p} \end{cases}, \quad \begin{cases} x \equiv 1 \pmod 8 \\ x \equiv x_2 \pmod{4p} \end{cases}$$

$$\begin{cases} x \equiv 5 \pmod 8 \\ x \equiv x_4 \pmod{4p} \end{cases}, \quad \begin{cases} x \equiv 3 \pmod 8 \\ x \equiv x_3 \pmod{4p} \end{cases}$$

Por el teorema **TCRG** (1.1.5) los primeros cuatro sistemas no son solubles y por lo tanto, los únicos sistemas solubles son los siguientes:

$$\begin{cases} x \equiv 7 \pmod 8 \\ x \equiv x_1 \pmod{4p} \end{cases}, \quad \begin{cases} x \equiv 1 \pmod 8 \\ x \equiv x_2 \pmod{4p} \end{cases}$$

$$\begin{cases} x \equiv 5 \pmod 8 \\ x \equiv x_4 \pmod{4p} \end{cases}, \quad \begin{cases} x \equiv 3 \pmod 8 \\ x \equiv x_3 \pmod{4p} \end{cases}$$

y las soluciones obtenidas por el mismo teorema 1.1.5 son:

$$\hat{x}_1 = x_1 + 4p\beta t \qquad y \qquad \hat{x}_2 = x_2 + 4p\beta' t'.$$

$$\hat{x}_3 = x_3 + 4p\overline{\beta}\overline{t} \qquad y \qquad \hat{x}_4 = x_4 + 4p\overline{\beta}'\overline{t}'.$$

Por argumentos análogos a los resultados previos, estas son las únicas soluciones.

Por tanto, q es un primo inerte en el anillo de enteros correspondiente si y solo si $q \equiv \hat{x}_j \pmod{32p}$, con lo cual se demuestra el siguiente resultado:

Teorema 2.3.14. *Sea $K = \mathbb{Q}(\sqrt{d})$, con $d = 2p$ y $2 < p \equiv 3 \pmod 4$ primo. Entonces, $\left(\frac{d}{q}\right) = -1$ si y solo si $q \equiv \hat{x}_j \pmod{32p}$, donde*

$$\hat{x}_1 = x_1 + 4p\beta t, \quad \hat{x}_2 = x_2 + 4p\beta' t', \quad \hat{x}_3 = x_3 + 4p\overline{\beta}\overline{t}, \quad \hat{x}_4 = x_4 + 4p\overline{\beta}'\overline{t}'.$$

□

2.3.3. Inercia en $\mathbb{Q}(\sqrt{d})$ cuando $d = p_1p_2p_3$

Para esta última parte del presente trabajo, se dará únicamente un bosquejo de la forma que deben tener los primos inertes en $\mathbb{Q}(\sqrt{d})$ cuando $d = p_1p_2p_3$ y $d > 0$. La razón de esto es que durante el desarrollo de esta parte, se encontró que la forma de tales soluciones permiten proyectar las soluciones para el caso general:

$$d = \prod_{i=1}^{m} p_i, \text{ para } p_i \neq p_j \text{ y } m < \infty.$$

Así mismo, se verá con claridad que para $m \geq 3$, este es un problema de naturaleza puramente combinatoria.

Veamos qué sucede en el caso más simple, cuando $p_i \equiv 1 \pmod 4$. Este análisis es suficiente para vislumbrar la forma de las soluciones para cualquier caso. Siguiendo las ideas desarrolladas en los casos anteriores, para que un primo racional q sea inerte en $\mathbb{Q}(\sqrt{d})$, se necesita que ocurra lo siguiente:

$$\left(\frac{d}{q}\right) = \left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right)\left(\frac{p_3}{q}\right) = -1.$$

Claramente, existen solo cuatro posibilidades para que esto ocurra y éstas son:

$\left(\frac{p_1}{q}\right)$	$\left(\frac{p_2}{q}\right)$	$\left(\frac{p_3}{q}\right)$
-1	-1	-1
-1	1	1
1	-1	1
1	1	-1

Es decir, o bien el primo q está en N_{p_i}, para todo i o bien es un no residuo respecto a solamente uno de ellos. Como hemos hecho antes, estas condiciones están ligadas a sistemas de congruencias, mismos que son siempre solubles y las soluciones obtenidas tienen la forma

$$x = p_2p_3\gamma_1w_1 + p_1p_3\gamma_2w_2 + p_1p_2\gamma_3w_3,$$

donde la variable γ_j es o bien un elemento $r_j \in R_{p_j}$ o bien un elemento $s_j \in N_{p_j}$, según sea el caso. Fijémonos en algún renglón de la tabla anterior, digamos, en el primero, i.e., cuando q está en N_{p_i}, para todo i. La solución al sistema correspondiente es

$$x = p_2p_3s_1w_1 + p_1p_3s_2w_2 + p_1p_2s_3w_3.$$

Por tanto, si $q \equiv x \pmod{p_1p_2p_3}$, este debe ser inerte y por lo tanto debe satisfacer

$$\left(\frac{p_2p_3s_1w_1 + p_1p_3s_2w_2 + p_1p_2s_3w_3}{p_i}\right) = -1,$$

es decir

$$\left(\frac{p_2p_3s_1w_1}{p_1}\right) = -1, \left(\frac{p_1p_3s_2w_2}{p_2}\right) = -1, \left(\frac{p_1p_2s_3w_3}{p_3}\right) = -1.$$

Consideremos el primer símbolo de los tres anteriores y analicémoslo con cuidado

$$\left(\frac{p_2p_3s_1w_1}{p_1}\right) = \left(\frac{p_2}{p_1}\right)\left(\frac{p_3}{p_1}\right)\left(\frac{s_1}{p_1}\right)\left(\frac{w_1}{p_1}\right) = -1.$$

Notemos primero que el factor $\left(\frac{s_1}{p_1}\right)$ es siempre -1. Por lo tanto, determinar el valor del último factor en la descomposición anterior y mantenener el valor global de -1 es equivalente a conocer el comportamiento de los símbolos $\left(\frac{p_2}{p_1}\right)$ y $\left(\frac{p_3}{p_1}\right)$. Recordando que $p_i \equiv 1 \pmod 4$, la **LRC** nos dice que en automático conocemos el valor de los siímbolos $\left(\frac{p_1}{p_2}\right)$ y $\left(\frac{p_1}{p_3}\right)$. Por lo tanto, la elección adecuada de w_1 depende de lo siguiente:

$\left(\frac{p_2}{p_1}\right)$	$\left(\frac{p_3}{p_1}\right)$	$\left(\frac{w_1}{p_1}\right)$
1	1	$w_1 \in R_{p_1}$
-1	-1	$w_1 \in R_{p_1}$
1	-1	$w_1 \in N_{p_1}$
-1	1	$w_1 \in N_{p_1}$

Si ahora tomamos el siímbolo $\left(\frac{p_1p_3s_2w_2}{p_2}\right)$, procediendo de forma análoga a la anterior, encontramos que en su factorización, para determinar dónde tomar w_2 basta ver el comportamiento de $\left(\frac{p_3}{p_2}\right)$, pues el otro símbolo ya está determinado como lo mencionamos en el análisis previo y de nuevo, también está determinado el valor de $\left(\frac{p_2}{p_3}\right)$. De esta forma se tiene que

$\left(\frac{p_1}{p_2}\right)$	$\left(\frac{p_3}{p_2}\right)$	$\left(\frac{w_2}{p_2}\right)$
1	1	$w_2 \in R_{p_2}$
-1	-1	$w_2 \in R_{p_2}$
1	-1	$w_2 \in N_{p_2}$
-1	1	$w_2 \in N_{p_2}$

Para el símbolo que nos resta procedemos de manera análoga. De esta manera se obtiene

$\left(\frac{p_1}{p_3}\right)$	$\left(\frac{p_2}{p_3}\right)$	$\left(\frac{w_3}{p_3}\right)$
1	1	$w_3 \in R_{p_3}$
-1	-1	$w_3 \in R_{p_3}$
1	-1	$w_3 \in N_{p_3}$
-1	1	$w_3 \in N_{p_3}$

Si elegimos otra solución, digamos $x' = p_2p_3s_1w_1 + p_1p_3r_2w_2 + p_1p_2r_3w_3$, y tomamos $q \equiv x' \pmod{p_1p_2p_3}$, el análisis es idéntico, simplemente recordando que $\left(\frac{r_i}{p_i}\right) = 1$ y eso nos lleva a obtener las tablas adecuadas semejantes a las previas, con w_i en el conjunto adecuado y con ello, la forma del primo racional inerte q.

Pasemos ahora al caso $p_i \equiv 3 \pmod 4$. De forma semejante a como hicimos en el caso anterior, es posible determinar la forma de las soluciones a los sistemas correspondientes, que son las mismas que se listaron antes. En consecuencia, las soluciones obtenidas son de la forma:

$$x = \alpha p_1p_2p_3w + 4(p_2p_3\gamma_1w_1 + p_1p_3\gamma_2w_2 + p_1p_2\gamma_3w_3),$$

con γ_i como en el caso anterior y $\alpha = 1$ ó 3. Así, tomando $q \equiv x \pmod{4p_1p_2p_3}$, éste debe ser inerte.

De nuevo, consideremos el caso en que $q \in N_{p_i}$, entonces se debe satisfacer que

$$\left(\frac{3p_1p_2p_3w + 4(p_2p_3r_1w_1 + p_1p_3r_2w_2 + p_1p_2r_3w_3)}{p_i}\right) = -1.$$

Lo primero que debemo notar es que el sumando $3p_1p_2p_3w$ no tiene injerencia en el valor global del símbolo, por ello podemos considerar $w = 1$, entonces, el símbolo a estudiar es

$$\left(\frac{4(p_2p_3r_1w_1 + p_1p_3r_2w_2 + p_1p_2r_3w_3)}{p_i}\right) = -1.$$

Ahora, notemos que si factorizamos el símbolo anterior, resulta

$$\left(\frac{4}{p_i}\right)\left(\frac{p_2p_3r_1w_1 + p_1p_3r_2w_2 + p_1p_2r_3w_3}{p_i}\right) = -1,$$

y con ello, éste se reduce a

$$\left(\frac{p_2p_3r_1w_1 + p_1p_3r_2w_2 + p_1p_2r_3w_3}{p_i}\right) = -1,$$

es decir, el análisis correspondiente es idéntico al caso en que los primos en la descomposición de d dejan residuo 1 módulo 4, solo hay que tener presente la **LRC** para determinar en dónde se deben tomar los w_i respectivos.

Resta por analizar lo que ocurre cuando exactamente un p_i deja un residuo distinto módulo 4 a los otros dos. Esto significa, combinar los resultados obtenidos en las dos secciones anteriores, cuando $d = p$ y $d = p_1p_2$, únicamente hay que tener cuidado con cuál primo es el que deja residuo distinto para elegir las condiciones adecuadas. Notemos primero que los dos únicos casos posibles son $p_1, p_2 \equiv 1 \pmod 4, p_3 \equiv 3 \pmod 4$ y $p_1, p_2 \equiv 3 \pmod 4, p_3 \equiv 1 \pmod 4$, pues cualquier otra combinación es equivalente a estas dos. Si consideramos cualquiera de los dos casos anteriores, con un análisis similar, también obtenemos soluciones de la forma

$$x = \alpha p_1p_2p_3w + 4(p_2p_3\gamma_1w_1 + p_1p_3\gamma_2w_2 + p_1p_2\gamma_3w_3),$$

con γ_i como antes y $\alpha = 1$ ó 3. De este modo, queda completamente descrita la forma que debe tener un primo inerte cuando $d = p_1p_2p_3 > 0$.

Conclusiones

Se ha encontrado explícitamente la forma que debe tener un primo $q \in \mathbb{Z}$ si deseamos que el ideal $q\mathcal{O}_K$ sea un ideal primo en $\mathcal{O}_K$, cuando $K = \mathbb{Q}(\sqrt{d})$ y $d = p$, $d = p_1p_2$ ó $d = p_1p_2p_3$. El caso $d = p$ fue la base de las siguientes construcciones, considerando que el primo fuera tanto positivo como negativo. Se encontró que cuando el primo p deja residuo 1 módulo 4, la forma de los primos inertes es inmediata. Cuando el primo p deja residuo 3 módulo 4, encontrar la forma de los primos inertes es equivalente a estudiar un sistema de dos congruencias lineales debido a la **LRC**. En la caracterización de la construcción de q se vislumbra la forma en que se comportará el caso siguiente, cuando la factorización de d está dada como el producto de dos primos p_1 y p_2.

En el caso $d = p_1p_2p_3$ se ve claramente en la construcción la naturaleza combinatoria de la forma de los primos racionales inertes en $\mathcal{O}_K$. La parte que hay que rescatar de este último análisis es que todo queda bien determinado una vez que se conocen todas las posibilidades válidas de los símbolos $\left(\frac{p_j}{p_i}\right)$, cuando $p_i \neq p_j$ y sus respectivos productos. Ésta parece ser la parte medular para cualquier factorización de d. De hecho, los resultados obtenidos permiten conjeturar el caso general cuando $d = \prod_{i=1}^{t} p_i$, con $p_i \neq p_j$ si $i \neq j$. Se puede conjeturar además que esta forma general de los primos inertes está determinada por la paridad de los factores en que se descompone d.

Bibliografía

[1] Adhikari M.R., Adhikari A., *Basic Modern Algebra with Applications*, Springer India, 2014.

[2] Aguilar-Zavoznik A., Pineda-Ruelas M., *Introducción a los campos de números y campos de funciones*, Departamento de matemáticas UAM-I, 2014.

[3] Alaca S., Williams K.S., *Introductory algebraic number theory*, Cambridge University Press, 2004.

[4] Andrews G.E., *Number Theory*, W.B. Saunders Company, 1971.

[5] Apostol T.M., *Introduction to Analytic Number Theory*, Springer Verlag, 1976.

[6] Ash R., *A course in algebraic number theory*. Publicación electrónica `http://www.math.uiuc.edu/ r-ash/ANT.html`.

[7] Baker A., *A Comprehensive Course in Number Theory*, Cambridge University Press, 2012.

[8] Baker M., *Algebraic Number Theory Course Notes*, Publicación electrónica `http://people.math.gatech.edu/ mbaker/pdf/ANTBook.pdf`, 2006.

[9] Conrad K., Discriminants and ramified primes. Publicación electrónica `http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy`.

[10] Cox D.A., *Galois Theory*, John Wiley & Sons, 2012.

[11] Davenport H., *The Higher Aritmetic: an introduction to the theory of numbers*, Cambride University Press, 2008.

[12] Dummit D., Foote R., *Abstract algebra*, John Wiley and Sons, 2004.

[13] Duverney D., *Number Theory: An elementary introduction through diophantine problems*, World Scientific, 2010.

[14] Friedberg S., Insel A., Spence L., *Linear algebra*, Prentice Hall, 2003.

[15] Halmos P.R., *Linear Algebra Problem Book*, Dolciani Mathematical Exposition Number 16, 1995.

[16] Hernández-Magdaleno A.M., *Álgebra moderna: Anillos y campos*, Universidad de Guadalajara, 2012.

[17] Ireland, K., Rosen, M.. *A classical introduction to modern number theory*. GTM **84** Springer Verlag, 1990.

[18] Ivorra-Castillo, C., *Funciones de variable compleja con aplicaciones a la teoría de números*. Publicación electrónica `https://www.uv.es/ivorra/Libros/Varcom.pdf`.

[19] Jarvis F., *Algebraic number theory*. SUMS Springer International Publishing, 2014.

[20] Lidl R., Niederreiter H., *Introduction to finite fields and their applications*. Cambride University Press, 1986.

[21] Lorenzini D., *An inivitation to Arithmetic Geometry*. GSM American Mathematical Society, 1996.

[22] McCarthy P., *Algebraic extensions of fields*. Dover, 1990.

[23] Narkiewicz, W. *Elementary and Analytic Theory of Algebraic Numbers*. Springer Verlag Universitext, 2004.

[24] Pacheco-Castán E. Proyecto Terminal de la Licenciatura en Matemáticas de la Universidad Autónoma Metropolitana-Iztapalapa, 2012.

[25] Pineda-Ruelas M., *Enteros, aritmética modular y grupos finitos*. Universidad Autónoma Metropolitana, 2014.

[26] Ribenboim P., *Classical Theory of Algebraic Numbers*, Springer Verlag, 2001.

[27] Robinson D. J., *A Course in Linear Algebra with applications*. World Scientific Publishing, 2006.

[28] Stewart, I., Tall, D.. *Algebraic number theory and Fermat's last theorem*. A K Peters, 2002.

[29] Trifković M. *Algebraic Theory of Quadratic Numbers*. Universitext Springer Science + Business Media, 2013.

[30] Weintraub S.H., *Factorization: Unique and Otherwise*. A K Peters, 2008

[31] Wyman B.F., *What is a reciprocity law*. American Mathematical Monthly, Vol. 79, No. 6, 1972

[32] Yang Y., *A Concise Text on Advanced Linear Algebra*. Cambridge University Press, 2015.

Índice alfabético