Dominios de Dedekind, factorización de ideales y aplicaciones.

Alberto Daza Garcia

20 de junio de 2018

Tutorizado por Antonio Rojas León

Índice general

Abstract

In order to study some number theoretical problems, algebraic number fields and their ring of integers have being introduced. In this dissertation rings of integers and their arithmetic properties will be studied. Since they don't have unique factorization, in the second chapter ideals will be used to generalize it as unique factorization of ideals. This will be proved in the more general case of Dedekind domains. Afterwards, it will be given a measure of "how far" they are from being principal ideal domains called the class number.

Since the moment all those concepts are introduced, the objective of this dissertation will be to give a formula which relates the class number with the zeta functions. In order to do this, in chapter 3, it will be proved Minkowski theorem which will be used to find a bound to the discriminant (an invariant of the number fields) and in chapter 4 it will be proved the Dirichlet's unit theorem which gives the structure of the group of units in the ring of integers. Finally, in chapter 5 we get the formula.

Resumen

Para estudiar algunos problemas de teoría de números, se han introducido los cuerpos de números algebraicos y sus anillos de enteros. En esta memoria se estudiarán los anillos de enteros y sus propiedades aritméticas. Como estos no tienen necesariamente factorización única, en el segundo capítulo se usarán los ideales para generalizarlo como factorización única de ideales. Se probará en el caso más general de dominios de Dedekind. Después, se dará una medida de "cómo de lejos" están de ser dominio de ideales principales llamada número de clases.

Desde el momento en el que todos estos conceptos se han introducido, el objetivo de la memoria será el de dar una fórmula que relacione el número de clases con las funciones zeta. Para hacer esto, en el capítulo 3, se probará el teorema de Minkowski que será usado para encontrar una cota del discriminante (un invariante de los cuerpos de números) y en el capítulo 4, se probará el teorema de Dirichlet que da la estructura del grupo de unidades en el anillo de enteros. Finalmente, en el capítulo 5 obtendremos la fórumla.

1 Enteros Algebraicos

1.1. Motivación.

Antes de nada, se definirá que es un cuerpo de números algebraicos y su anillo de enteros comprobándose que efectivamente es un anillo. Luego se estudiarán algunas propiedades.

Definición 1.1.1. *Se llamará cuerpo de números algebraicos a cualquier extensión finita K de $\mathbb{Q}$*

Ejemplos 1.1.2. *1. El caso trivial es $\mathbb{Q}$.*

2. *Sea α solución de un polinomio $f \in \mathbb{Q}[x]$ irreducible de grado 2, entonces $\mathbb{Q}(\alpha)$ es un cuerpo de números algebraicos. Estos cuerpos se llamarán cuadráticos. En este caso $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.*

3. *Sea m un entero positivo y sea $\zeta_m = e^{2\pi i/m}$. Se tiene que ζ_m es raiz de $x^m - 1$. Por tanto, $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] \leq m$. Además $x^m - 1 = (x-1)(x-\zeta_m)...(x-\zeta_m^{m-1})$. Por tanto, es el cuerpo de descomposición del polinómio y por esto $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ es una extensión de Galois. Este tipo de cuerpos se llama cuerpos ciclotómicos.*

El objetivo primero es, dado un cuerpo de números algebraicos K, definir un anillo de enteros $\mathcal{O}_K$ que sea "muy parecido a $\mathbb{Z}$".

Por ejemplo, si $K = \mathbb{Q}(\sqrt{d})$, se podría pensar en usar $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Esto, fue usado con d=-1 por Gauss para estudiar cuándo un número entero se podía escribir como suma de cuadrados [HW, Teorema 366]. Sin embargo, esta forma de definir el anillo, no será siempre la mejor.

Entonces, se buscarán una serie de condiciones que se quiere que cumpla ese anillo de enteros:

1. $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo finitamente generado sobre K
2. El cuerpo de fracciones de $\mathcal{O}_K$ es K
3. $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$

Realmente, estas condiciones no son suficientes para determinar el anillo de forma satisfactoria dado que existen muchos anillos que cumplen esto. Para encontrar el anillo de enteros se prodría pensar de dos formas.

1. $\mathcal{O}_K :=$ el subanillo de K generado por $\bigcup_{\substack{A \subseteq K \\ \text{A cumple 1.,2. y 3.}}} A$
2. $\mathcal{O}_K :=$ el subanillo de K generado por $\bigcap_{\substack{A \subseteq K \\ \text{A cumple 1.,2. y 3.}}} A$

Sin embargo, estos anillos, no cumplen las propiedades anteriores. Para evitar este problema se puede tener en cuenta que si $K/\mathbb{Q}$ es una extensión de Galois y $Gal(K/\mathbb{Q}) = \{\sigma_1, ..., \sigma_n\}$ su grupo de Galois, entonces sería interesante que $\sigma_1(\mathcal{O}_K) = ... = \sigma_n(\mathcal{O}_K) = \mathcal{O}_K$. El próximo lema será buena ayuda para encontrar el anillo de enteros.

Lema 1.1.3. *Sea L/M una extensión de Galois con grupo de Galois $Gal(L/M)$. Sea $R \subseteq L$ un subanillo tal que $\sigma(R) = R$ para todo $\sigma \in Gal(L/M)$. Entonces, el polinomio mínimo de cualquier elemento de R tiene coeficientes en $R \cap M$*

Demostración. Sea $\alpha \in R$, sea $H := \{\sigma \in Gal(L/M) : \sigma(\alpha) = \alpha\}$. Entonces, el número de conjugados distintos en L que tiene α es $s := |Gal(L/M)/H|$. Sean $\alpha_1, ..., \alpha_s$ los conjugados. El polinomio mínimo de α sobre M es:

$$f(x) := \prod_{i=1}^{s} (y - \alpha_i)$$

Además, como $\forall \sigma \in Gal(L/M)\ \sigma(R) = R$, entonces, los coeficientes de f están en R. Por tanto, los coeficientes de f están en $R \cap M$ □

Definición 1.1.4. *Dado un cuerpo K, un subanillo A de K y $\alpha \in K$, se dice que α es **íntegro** sobre A si es la raiz de un polinomio mónico con coeficientes en A. En el caso en el que $A = \mathbb{Z}$ se dice que α es un entero algebraico.*

Definición 1.1.5. *Sea A un subanillo de un anillo C. El anillo C se dice **íntegro** sobre A si cada elemento de C es íntegro sobre A.*

El lema anterior motiva la posibilidad de definir los enteros algebraicos entorno a esta definición. Se plantean dos posibilidades:

1. $\mathcal{O}_K$ es el menor subanillo de K que contiene todos los enteros algebraicos de K

2. $\mathcal{O}_K$ es el menor subanillo de K que contiene todos los subanillos R de K que son íntegros sobre $\mathbb{Z}$

Si definimos R_1 como el anillo descrito en 1. y R_2 como el anillo descrito en 2., demostrando que el conjunto de todos los enteros algebraicos de K forman un anillo, se tiene que $R_1 = R_2$ y por tanto, da una buena motivación para la definición de $\mathcal{O}_K$.

Proposición 1.1.6. *Sea L un cuerpo. Sea A un subanillo de L. Sea $\alpha \in L$. Entonces, son equivalentes:*

1. *α es íntegro sobre A.*

2. *El subanillo $A[\alpha]$ de L es un A-módulo finítamente generado*

3. *Existe un A-Módulo M finitamente generado tal que $\alpha M \subseteq M$*

Demostración. [DL, prop 2.10] □

Corolario 1.1.7. *Sea L un cuerpo. Sea A un subanillo de L. El conjunto B cuyos elementos son los elementos de L íntegros sobre A es un anillo.*

Demostración. [DL, cor 2.11] □

Se puede notar ahora que las dos posibles definiciones anteriores son equivalentes. Por tanto, ya estamos en condiciones de definir anillo de enteros algebraicos

Definición 1.1.8. *Sea L un cuerpo. Sea A un subanillo de L. La **clausura íntegra** de A es el anillo que tiene todos los elementos de L que son íntegros sobre A. Si A es un dominio de integridad y en su cuerpo de fracciones es igual a su clausura íntegra se llama **íntegramente cerrado**.*

Definición 1.1.9. *Dada una extensión finita $K/\mathbb{Q}$, se define el **anillo de enteros** de K (y se denotará $\mathcal{O}_K$) como la clausura íntegra de $\mathbb{Z}$ en K.*

Ahora falta comprobar que efectivamente esta es la definición que nos interesa. Es decir, falta ver que tiene todas las características que buscábamos.

Proposición 1.1.10. *Sean A,B,C tres dominios de integridad tales que $A \subseteq B \subseteq C$. Entonces C es íntegro sobre A si y sólo si C es íntegro sobre B y B es íntegro sobre A*

Demostración. [DL, prop 2.18] □

Ahora, en un caso más general que el de los números algebraicos, se probará que se cumplen las condiciones que queríamos que cumpliesen los anillos de enteros.

Proposición 1.1.11. *Sea A un dominio de integridad. Sea K su cuerpo de fracciones. Sea L/K una extensión finita. Sea B la clausura íntegra de A en L.*

1. *Sea $\alpha \in L$. Existe $b \in B$ y $a \in A$ tales que $\alpha = b/a$. Por tanto, L es el cuerpo de fracciones de B.*

2. *B es íntegramente cerrado.*

3. *Si A es íntegramente cerrado, entonces $B \cap K = A$*

4. *Si L/K es Galois, entonces $\tau(B) = B \ \forall \tau \in G = Gal(L/K)$. De hecho, si A es íntegramente cerrado, $A = B^G$*

Demostración. [DL, prop I 2.19] □

Para ver que los enteros algebraicos son un caso particular de la proposición sólo hay que ver que dada una extensión finita $K/\mathbb{Q}$ se tiene que $\mathbb{Z}$ es dominio de integridad, $\mathbb{Q}$ es su cuerpo de fracciones, que $\mathcal{O}_K$ es la clausura íntegra de $\mathbb{Z}$, y para usar el apartado 3. hay que ver que $\mathbb{Z}$ es íntegramente cerrado. Que $\mathbb{Z}$ es un dominio de integridad es una de las primeras cosas que se demuestran en matemáticas, y el resto de cosas excepto que $\mathbb{Z}$ es íntegramente cerrado son definiciones. Esto último es consecuencia de la siguiente proposición.

Proposición 1.1.12. *Todo dominio de factorización única es íntegramente cerrado*

Demostración. [DL, Lema I 2.16] □

Finalmente, se tiene la siguiente proposición que se demostrará más adelante para el caso de enteros algebraicos.

Proposición 1.1.13. *Sea A un dominio de ideales principales. Sea K su cuerpo de fracciones. Sea L/K una extensión finita y separable. Entonces la clausura íntegra de A en L es un A-módulo finitamente generado.*

Este teorema se puede encontrar con toda su generalidad en [DL, cor 4.9]. La prueba es interesante, pero para los objetivos que tenemos aquí quizás sea más interesante seguir otro camino y dar la demostración en el caso particular de los anillos de enteros.

1.2. Algunas Herramientas.

En esta sección se considerará que K es un cuerpo con característica 0. Se introducirán unas herramientas que servirán para el estudio de propiedades de los enteros algebraicos.

Dada una extensión finita L/K con dimensión $[L\colon K] = n$, se buscarán unas funciones que a cada elemento de L le asigne un elemento de K. Para relacionar L con K se puede usar una base $B = \{\alpha_1, ..., \alpha_n\}$ de L/K.

Sea $\alpha \in L$, se define el automorfismo $\phi\colon L \to L$ dado por $\phi(\beta) = \alpha\beta \forall \beta \in L$.

Sea $\alpha\alpha_i = \sum_{j=i}^{n} a_{ij}\alpha_j \ \forall i = 1, ..., n$. Entonces la matriz de ϕ respecto de la base B es $M = (a_{ij})$. Si $B' = \{\beta_1, ..., \beta_n\}$ es otra base, se llama C a la matriz de cambio de base de B' a B entonces, si $b \in L$ se denota como $b_{B'}$ a b con coordenadas respecto a B' y b_B el mismo vector respecto a la base B. Lo mismo se hace con $\phi(b)$. Entonces, $\phi(b)_B = Mb_B = MCb_{B'}$ y por tanto, $\phi(b)_{B'} = C^{-1}MCb_{B'}$. Así que la matriz de ϕ respecto de la base B' es $C^{-1}MC$.

Como L es un cuerpo ϕ es biyectiva. Por tanto, tanto M como $C^{-1}MC$ son invertibles. Por tanto, su determinante y su traza dependen únicamente de los autovalores, pero los autovalores son los mismos y por tanto ni el determinante ni la traza dependen de la base que se elija.

Definición 1.2.1. *La **norma** de α se define como $N_{L/K}(\alpha) := det(M)$ y la **traza** de α se define como $t_{L/K}(\alpha) := tr(M)$. Si no hay confusión se denotarán $N(\alpha)$ y $t(\alpha)$.*

A continuanción se demostrarán algunas propiedades.

Proposición 1.2.2. *Sean $\alpha, \beta \in L$ y $a \in K$:*

1. *$N(\alpha\beta) = N(\alpha)N(\beta)$ y $t(\alpha + \beta) = t(\alpha) + t(\beta)$*
2. *$N(a\alpha) = a^n N(\alpha)$ y $t(a\alpha) = at(\alpha)$*
3. *si $\alpha \neq 0$, $N(\alpha^{-1}) = N(\alpha)^{-1}$*
4. *N(1)=1 y si $\alpha \neq 0$, entonces $N(\alpha) \neq 0$*
5. *t no es idénticamente 0*

Demostración. [IR] □

El problema de estas definiciones es que no son las más fáciles con las que se puede trabajar en muchos casos. La siguiente proposición proporciona una expresión que puede ser muy útil.

Proposición 1.2.3. *Sea L/K una extensión separable. Sean $\sigma_1, ..., \sigma_n$ los n isomorfismos distintos de L en una clausura algebráica de K que dejan K fijo. Sea $\alpha \in L$. Se denota $\alpha^{(i)} := \sigma_i(\alpha)$. Con esta notación, $t(\alpha) = \alpha^{(1)} + ... + \alpha^{(n)}$ y $N(\alpha) = \alpha^{(1)}...\alpha^{(n)}$*

Demostración. [DL, lema IV 2.5] □

Corolario 1.2.4. *Si $K/\mathbb{Q}$ es una extensión finita sea $\alpha \in \mathcal{O}_K$, entonces $N(\alpha)$, $t(\alpha) \in \mathbb{Z}$.*

Demostración. Como se vio en la demostración del lema 1.1.3 si α tiene s conjugados distintos, siendo estos $\alpha^{(1)}, ..., \alpha^{(s)}$ entonces, el polinómio mínimo de α es $f(x) = \prod_{i=1}^{s}(x - \alpha^{(i)})$. Entonces, si $f(x) = x^s + a_{s-1}x^{s-1} + ... + a_1x + a_0$ se tiene que $a_0 = (-1)^s\alpha^{(1)}...\alpha^{(s)}$ y $a_{s-1} = \alpha^{(1)} + ... + \alpha^{(s)}$ y por tanto $a_0^{n/s} = (-1)^{n/s}N(\alpha)$ y $a_1 \cdot n/s = t(\alpha)$. Como se verá en el lema 1.3.4. como α es íntegro sobre $\mathbb{Z}$ se tiene que $f \in \mathbb{Z}[x]$. □

Se definirá una última herramienta.

Definición 1.2.5. *Sea L/K una extensión finita. Sean $\alpha_1, ..., \alpha_n \in L$. Se define el **discriminante** $\Delta(\alpha_1, ..., \alpha_n) := det(\alpha_i\alpha_j)$.*

Proposición 1.2.6. *Si $\Delta(\alpha_1, ..., \alpha_n) \neq 0$, entonces $\alpha_1, ..., \alpha_n$ es una base de L/K. Además, si L/K es separable y $\alpha_1, ..., \alpha_n$ es una base, entonces $\Delta(\alpha_1, ..., \alpha_n) \neq 0$.*

Demostración. [IR, prop 12.1.1.] □

Proposición 1.2.7. *Sean $\alpha_1, ..., \alpha_n$ y $\beta_1..., \beta_n$ dos bases de L/K. Sea $\alpha_i = \sum_{j=1}^{n} a_{ij}\beta_j$, con $a_{ij} \in K$. Entonces $\Delta(\alpha_1, ..., \alpha_n) = det(a_{ij})^2\Delta(\beta_1, ..., \beta_n)$*

Demostración. [IR, prop 12.1.2.] □

En cuerpos de números se trabaja en extensiones separables. Además, como consecuencia del teorema de Artin las extensiones serán de la forma $\mathbb{Q}(\beta)$ para algún $\beta \in \mathbb{C}$. Así que será interesante tener las siguientes proposiciones que dan expresiones fáciles de calcular para el discriminante.

Proposición 1.2.8. *Sea L/K una extensión separable. Sean $\alpha_1, ..., \alpha_n \in L$. Entonces $\Delta(\alpha_1, ..., \alpha_n) = det(\alpha_i^{(j)})^2$*

Demostración. [IR, prop 12.2.2] □

Proposición 1.2.9. *Sea L/K una extensión separable. Sean $1, \beta, ...\beta^{n-1}$ elementos de L linealmente independientes sobre K. Sea $f \in K[x]$ el polinomio mínimo de β sobre K. Entonces $\Delta(1, \beta, ...\beta^{n-1}) = (-1)^{n(n-1)/2}N(f'(\beta))$*

Demostración. [IR, prop 12.2.4] □

1.3. Números algebraicos

En este apartado, se aplicarán las herramientas anteriores al caso concreto de los números algebraicos. Se demostrará que los anillos de enteros algebraicos son un $\mathbb{Z}$-módulo finitamente generado, se aplicará al caso particular de los cuerpos cuadráticos y estos se determinarán completamente. Finalmente se comprobará que estos no necesariamente tienen las propiedades aritméticas que $\mathbb{Z}$. No tienen factorización única, pero eso se empezará a suplir en el capítulo siguiente.

Dado un cuerpo de números K, como se tiene que K es el cuerpo de fracciones de $\mathcal{O}_K$ si $\alpha_1, ..., \alpha_n$ es una base de K sobre $\mathbb{Q}$, usando el teorema 1.1.11. apartado 1, existe $a \in \mathbb{Z}$ no nulo tal que $a\alpha_1, ..., a\alpha_n \in \mathcal{O}_K$. Además son base de K. El resultado se puede incluso hacer más fuerte. Sea I un ideal no nulo de $\mathcal{O}_K$. Sea $b \in I$. Entonces, por las propiedades del ideal $ab\alpha_i \in I$ para cada $i = 1, ..., n$. Además $ab\alpha_1, ..., ab\alpha_n$ es una base de K sobre $\mathbb{Q}$ dado que es la imagen de $\alpha_1, ..., \alpha_n$ por el homomorfismo $\phi\colon L \to L$ definido por $\phi(\beta) = ab\beta$. Lo interesante, es que para cada ideal I de $\mathcal{O}_K$, una base contenida en I lo genera como $\mathbb{Z}$-módulo. Esto viene dado en la siguiente proposición:

Proposición 1.3.1. *Sea K/$\mathbb{Q}$ una extensión finita. Sea I un ideal en $\mathcal{O}_K$. Sean $\alpha_1, ..., \alpha_n \in I$ elementos que forman una base de K sobre $\mathbb{Q}$ con $|\Delta(\alpha_1, ..., \alpha_n)|$ minimal. Entonces, $\alpha_1, ..., \alpha_n$ genera I como $\mathbb{Z}$-módulo.*

Demostración. [IR, prop 12.2.2] □

A partir de ahora se notará que en concreto $\mathcal{O}_K$ es un ideal de $\mathcal{O}_K$. Por tanto es un $\mathbb{Z}$-módulo fintamente generado. Si $\alpha_1, ..., \alpha_n$ es una base de K/$\mathbb{Q}$ que genera $\mathcal{O}_K$ como $\mathbb{Z}$-módulo, entonces se llamara base íntegra de I. Como $|\Delta(\alpha_1, ..., \alpha_n)|$ da números naturales cuando los α_i están en $\mathcal{O}_K$, entonces siempre se alcanza ese mínimo. A ese valor mínimo de $|\Delta(\alpha_1, ..., \alpha_n)|$ para $\alpha_1, ..., \alpha_n \in I$ se llama discriminante de I y se denota $\Delta(I)$.

Definición 1.3.2. *Dada una extensión finita K/$\mathbb{Q}$, se llamará* ***discriminante de K*** *a $\delta_K := \Delta(\mathcal{O}_K)$*

El lema siguiente, permitirá calcular el discriminante de un ideal conociendo una base íntegra.

Lema 1.3.3. *Dada dos base íntegras $\alpha_1, ..., \alpha_n$ y $\beta_1, ..., \beta_n$ de un ideal I, se tiene que $\Delta(\alpha_1, ..., \alpha_n) = \Delta(\beta_1, ..., \beta_n)$*

Demostración. Sea $\alpha_i = \sum_{j=1}^{n} a_{ij}\beta_j$, con $a_{ij} \in \mathbb{Z}$. Entonces $\Delta(\alpha_1, ..., \alpha_n) = det(a_{ij})^2\Delta(\beta_1, ..., \beta_n)$ por el teorema 1.2.7. Como cada a_{ij} es entero, entonces $det(a_{ij})^2 \geq 1$ por tanto, $\Delta(\alpha_1, ..., \alpha_n) \geq \Delta(\beta_1, ..., \beta_n)$. Análogamente sale la otra desigualdad □

Ahora estamos en disposición de determinar los anillos de enteros en cuerpos cuadráticos y su discriminante. Lo primero es considerar el cuerpo $K := \mathbb{Q}(\sqrt{d})$. Sin pérdida de generalidad y para simplificar la tarea, se considerará $d \in \mathbb{Z}$ y libre de cuadrados. Se buscará una base íntegra de $\mathcal{O}_K$. Para ello, primero se tendrá en cuenta que 1 y $\sqrt{d}$ son una base de $\mathbb{Q}(\sqrt{d})$ sobre $\mathbb{Q}$. Por tanto, existe un sistema generador de $\mathcal{O}_K$ con dos elementos. Sea $\alpha = a + b\sqrt{d}$ con $a, b \in \mathbb{Q}$. El siguiente lema ayudará a ver cómo son a y b.

Lema 1.3.4. *Sea A un dominio de factorización única. Sea K el cuerpo de fracciones de A. Sea L/K una extensión finita. Sea $\alpha \in L$. Sea $g \in K[x]$ el polinomio mínimo de α sobre K. Entonces, α es íntegro sobre A si y sólo si $g \in A[x]$.*

Demostración. [DL, Remark 2.6] □

Corolario 1.3.5. *Sea d un entero libre de cuadrados. Sea $\alpha \in \mathbb{Q}(\sqrt{d})$. α es íntegro sobre $\mathbb{Z}$ si y sólo si $t(\alpha), N(\alpha) \in \mathbb{Z}$*

Usando el corolario anterior, como $t(\alpha) = \alpha^{(1)} + \alpha^{(2)} = 2a$ y $N(\alpha) = \alpha^{(1)}\alpha^{(2)} = a^2 - b^2 d$ entonces $\alpha \in \mathcal{O}_K$ si y sólo si $2a \in \mathbb{Z}$ y $a^2 - b^2 d \in \mathbb{Z}$. Si se multiplica por -4 la segunda condición y se suma $4a^2$, como $\mathbb{Z}$ es un anillo, se tiene que $4b^2 d \in \mathbb{Z}$. Como d es libre de cuadrados, entonces se tiene que cumplir que $2b \in \mathbb{Z}$. Se distinguiran dos casos:

1. Si $d \equiv 1 (\text{mod } 4)$, entonces, $4a^2 - d4b^2 \equiv 4a^2 - 4b^2 \equiv 0 (\text{mod } 4)$. Por tanto 2a y 2b tienen la misma paridad. Entonces, como $\alpha = a + b\sqrt{d} = (2a + 2b)/2 + b((-1 + \sqrt{d})/2) \in \mathbb{Z} + \mathbb{Z}((-1 + \sqrt{d})/2)$. Entonces $\mathcal{O}_K \subseteq \mathbb{Z} + \mathbb{Z}((-1 + \sqrt{d})/2)$. Para la otra contención sólo hay que notar que 1 y $(-1 + \sqrt{d})/2)$ pertenecen a $\mathcal{O}_K$. 1 pertenece claramente, y $(-1 + \sqrt{d})/2)$ es raiz de $x^2 + x + (-1 + d)/4 \in \mathbb{Z}[x]$, por tanto también pertenece a $\mathcal{O}_K$

2. si $d \equiv 2, 3 (\text{mod } 4)$, entonces, o $(4a^2) + 2(4b^2) \equiv 0 (\text{mod } 4)$ o $4a^2 + 4b^2 \equiv 0 (\text{mod } 4)$. Se tiene así que tanto 2a como 2b son pares. Por tanto, a y $b \in \mathbb{Z}$. Así que $\alpha \in \mathbb{Z} + \sqrt{d}\mathbb{Z}$ implicando que $\mathcal{O}_K \subseteq \mathbb{Z} + \sqrt{d}\mathbb{Z}$. Para la otra implicación hay que ver que 1 y $\sqrt{d} \in \mathcal{O}_K$. $1 \in \mathcal{O}_K$ es trivial porque es entero, y $\sqrt{d} \in \mathcal{O}_K$ ya que el polinómio mínimo es $x^2 - d \in \mathbb{Z}[x]$.

Así que se tiene el siguiente resultado

Proposición 1.3.6. *Sea $K = \mathbb{Q}(\sqrt{d})$*

1. *Si $d \equiv 1 (mod\ 4)$ entonces, $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}((-1 + \sqrt{d})/2) = \mathbb{Z}[(-1 + \sqrt{d})/2]$*
2. *Si $d \equiv 2, 3 (mod\ 4)$ entonces, $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d} = \mathbb{Z}[\sqrt{d}]$*

Ahora que se tiene $\mathcal{O}_K$ como $\mathbb{Z}-$módulo, se puede plantear buscar el discriminante.

Proposición 1.3.7. *Sea $K = \mathbb{Q}(\sqrt{d})$. Entonces:*

1. *Si $d \equiv 1 (mod\ 4)$, entonces, $\delta_{\mathcal{O}_K} = d$.*
2. *Si $d \equiv 2, 3 (mod\ 4)$, entonces, $\delta_{\mathcal{O}_K} = 4d$.*

Demostración. [IR, prop 13.1.2] □

2

Propiedades de los ideales

2.1. Factorización de ideales

La mayoría de las facilidades que se tienen al trabajar en $\mathbb{Z}$ vienen de que es un dominio euclideo. Los anillos de enteros no tienen necesariamente esta propiedad. Por ejemplo, el anillo de enteros de $\mathbb{Q}(\sqrt{-5})$ es $\mathbb{Z}[\sqrt{-5}]$.Se puede comprobar que este anillo no tiene factorización única. De hecho, se tiene que $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Si se prueba que $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ son irreducibles y que no son asociados, entonces se tienen dos factorizaciones en irreducibles.

2 es irreducible porque por reducción al absurdo, si 2 lo es, $\exists a, b \in \mathbb{Z}[\sqrt{-5}]$ tal que $2 = ab$. Tomando norma, se tendría $4 = N(2) = N(a)N(b)$. Como a y b son enteros algebraicos, sus normas son números enteros. Por tanto, se tiene que $N(a) = N(b) = \pm 2$. En el capítulo 4 se probará que para a entero algebráico, $N(a) = \pm 1$ si y sólo si a es una unidad. Además, es imposible que la norma de un elemento de $\mathbb{Z}[\sqrt{-5}]$ sea ± 2 dado que $N(x + \sqrt{-5}y) = x^2 + 5y^2 \ \forall x, y \in \mathbb{Z}$. Es facil comprobar que eso no tiene solución probando primero que no tiene solución con y diferente de 0 y luego que 2 no es un cuadrado perfecto.

Las normas de las unidades son ± 1. Por tanto, si $x + \sqrt{-5}y$ es unidad, entonces, $x^2 + 5y^2 = \pm 1$. Las soluciones a esta ecuacion son $x = \pm 1, y = 0$. Ahora, por tanteo, se puede probar que los elementos no son asociados y por tanto 6 tiene dos factorizaciones.

A veces vendría muy bien la factorización única. Un ejemplo de esto es el intento de demostrar el teorema de Fermat de Gabriel Lamé factorizando $x^p + y^p$ en $\mathbb{Z}[\zeta]$ donde $\zeta = e^{2\pi i/p}$ como $x^p + y^p = \prod_{i=1}^{p}(x + \zeta^i y)$. Luego se factoriza z^p y se ve que las factorizaciones son distintas. Por desgracia el anillo en el que se factoriza no siempre tiene factorización única. La pregunta es: ¿Se puede generalizar esto? Aquí aparecen los anillos de Dedekind. Estos anillos solucionan parcialmente este problema con la factorización única de ideales. Próximamente se definiran estos

anillos y se verá cómo se factorizan los ideales en el caso de anillos de enteros algebraicos.

Definición 2.1.1. *Sea A un anillo. Se dice que tiene* ***dimensión*** *1 si no es el anillo trivial y si los ideales primos no nulos son ideales maximales.*

Esta no es la definición de dimensión habitual pero es equivalente para el caso de dimensión 1.

Hay que tener en cuenta que los ideales maximales son primos. Por tanto, esta definición lo que dice es que los ideales maximales y los primos son lo mismo.

Definición 2.1.2. *Sea A un dominio de integridad, se dice que A es un* ***dominio de Dedekind*** *si cumple:*

1. *A es noetheriano*
2. *A tiene dimensión 1*
3. *A es íntegramente cerrado sobre su cuerpo de fracciones.*

Los anillos de enteros son dominios de Dedekind. Lo que nos interesa es ver que eso implica factorización única de ideales.

El resultado se obtendrá poco a poco. Se irán demostrando resultados más débiles y usando estos se llegará a el resultado importante.

Lema 2.1.3. *Sea P un ideal primo. Sea I y J ideales tal que* $P \supseteq IJ$. *Entonces* $P \supseteq I$ *ó* $P \supseteq J$

Demostración. Por reducción al absurdo, si $P \supseteq IJ$ pero $P \not\supseteq I$ y $P \not\supseteq J$, entonces, existen $x \in I \backslash P$, $y \in J \backslash P$. Como $P \supseteq IJ$, entonces, $xy \in P$. Sin embargo $x, y \notin P$ contradiciendo que P sea primo. □

Lema 2.1.4. *Sea A un anillo conmutativo. Sean* $I_1, ..., I_n$ *ideales coprimos dos a dos de A. Entonces:*

1. $I_1 ... I_s$ *es coprimo con* I_{s+1} $\forall s = 1, ..., n-1$
2. $I_1 ... I_n = I_1 \cap ... \cap I_n$

Demostración.

1. Sean $x_j \in I_j$ e $y_j \in I_{s+1}$ con tales que $x_j + y_j = 1$ $\forall j = 1, ..., s$, entonces, $1 = \prod_{j=1}^{s}(x_j + y_j) \in I_{s+1} + I_1 ... I_s$
2. Por inducción en n:

   Si n=2 $I_1 \cdot I_2 \subseteq I_1 \cap I_2$ es claro. Sea $x \in I_1 + I_2$, como I_1 e I_2 son coprimos, sean $y \in I_1$ y $z \in I_2$ tales que $y + z = 1$, entonces, $x = x(y+z) = xy + xz \in I_1 \cdot I_2$.

   Si es cierto para n, entonces $I_1 ... I_n \cdot I_{n+1} = (I_1 ... I_n) \cdot I_{n+1} = (I_1 \cap ... \cap I_n) \cdot I_{n+1} = I_1 \cap ... \cap I_n \cap I_{n+1}$

□

Proposición 2.1.5. *Sea I un ideal no trivial de un anillo noetheriano A. Entonces, existen ideales primos $P_1, ..., P_s$ y enteros positivos $a_1, ..., a_s$ tales que $P_1^{a_1}...P_s^{a_s} \subseteq I \subseteq P_1 \cap ... \cap P_s$.*

Demostración. Por reducción al absurdo, sea Σ el conjunto de ideales que no tienen la propiedad de la proposición, se supondrá que es no vacío. Como A es noetheriano, existe un ideal I maximal en Σ. I no es primo porque entonces $I \subseteq I \subseteq I$ y sería una contradicción. Sean $x, y \in A$ tales que $xy \in I$ pero $x, y \notin I$, sea $I_x = \langle I, x\rangle$ e $I_y = \langle I, y\rangle$. Entonces, $I_x I_y = \langle I^2, \langle x\rangle I, \langle y\rangle I, xy\rangle \subseteq I \subseteq I_x \cap I_y$.

Está claro que $I_x, I_y \notin \Sigma$ dado que entonces I no sería un elemento maximal. Por tanto, existen $P_1, ..., P_s, Q_1, ..., Q_r$ ideales primos y $a_1, ..., a_s, b_1, ..., b_s$ enteros no negativos tales que:

$P_1^{a_1}...P_s^{a_s}Q_1^{b_1}...Q_r^{b_r} \subseteq I_x I_y \subseteq I \subseteq P_1 \cap ... \cap P_s \cap Q_1 \cap ... \cap Q_r$

Contradiciendo la hipótesis de que $I \in \Sigma$. □

Corolario 2.1.6. *Sea A un dominio de integridad de dimensión 1. Sea I un ideal cualquiera no trivial. Entonces, el conjunto de ideales maximales que contienen a I es finito. Sea $M_1, ..., M_s$ ese conjunto, entonces, existen $a_1, ..., a_s$ tales que $M_1^{a_1}...M_s^{a_s} \subseteq I \subseteq M_1 \cap ... \cap M_s$*

Demostración. Por la proposición anterior y dado que la dimensión del anillo es 1, queda demostrada la existencia de ideales maximales $M_1, ..., M_s$ tales que $M_1^{a_1}...M_s^{a_s} \subseteq I \subseteq M_1 \cap ... \cap M_s$.

Por la contención última $M_1, ..., M_s$ es un subconjunto de ideales maximales que contienen a I. Falta ver que son todos. Sea M un ideal maximal que contiene a I, entonces Si se localiza en M la contención $I \subseteq M_1 \cap ... \cap M_s$, se tiene que $I_M \subseteq (M_1 \cap ... \cap M_s)_M = M_{1M} \cap ... \cap M_{sM}$. Como $I \subseteq M$ se tiene que I_M es no vacío. Por tanto, $M_{1M} \cap ... \cap M_{sM}$ es no vacío. Eso sólo puede ser si existe un i con $1 \leq i \leq s$ tal que $M_{iM} \neq \emptyset$ y eso sólo ocurre si $M_i \subseteq M$. Como ambos son ideales maximales, eso sólo ocurre si $M_i = M$. Es decir, si $M \in M_1, ..., M_s$

□

Ahora se estudiará el problema en el caso en el caso particular de que el anillo sea local (es decir, que tenga un sólo ideal maximal) y se generalizará.

Proposición 2.1.7. *Sea A un anillo conmutativo. Son equivalentes:*

1. *A es un dominio de ideales principales*
2. *Todo ideal primo de A es principal*

Demostración. [DL, prop II.8.2] □

Proposición 2.1.8. *Sea A un dominio local de dimensión 1 con ideal maximal M. Son equivalentes:*

1. *A tiene factorización única de ideales.*

2. *A es un dominio de ideales principales.*

3. *A es íntegramente cerrado.*

Demostración. 1 $\implies$ 2 Sea $x \in M \backslash M^2$. Entonces $\langle x \rangle = M^n$ para algún n por la propiedad de factorización única. Como $x \notin M^2$, entonces, $x \notin M^n \ \forall n \geq 2$ dado que $M^n \subseteq M^2 \ \forall n \geq 2$. Por tanto, $\langle x \rangle \neq M^n \ \forall n \geq 2$. La única opción que queda es $\langle x \rangle = M$ Como el único ideal primo es un ideal principal, entonces es un dominio de ideales principales.

2 $\implies$ 1 Dado n, si x no es una unidad, entonces $x \in M^n \backslash M^{n+1}$. Se probará que $M^n = \langle x \rangle$. Sea $M = \langle m \rangle$, entonces, $M^n = \langle m^n \rangle$. Como $x \in \langle m^n \rangle$ entonces $m^n \mid x$. Por tanto, $x = mt$ para algún $t \in A$. Falta ver que t es una unidad. Es decir, que t no está en M. Por reducción al absurdo, $t \in M$ si y sólo si t=mr para algún $r \in A$. Por tanto, $x = m^{n+1}r$ pero esto no puede ser porque $x \notin M^{n+1}$.

2 $\implies$ 3 [DL, lema I2.16]

3 $\implies$ 2 Sea $x \in M$. Si $M = \langle x \rangle$ el resultado es consecuencia de la proposición anterior. Si $M \neq \langle x \rangle$, por el corolario 2.1.6. existe un n natural tal que $M^n \subseteq \langle x \rangle$. Sea $y \in M^{n-1} \backslash \langle x \rangle$ tal que $y \notin \langle x \rangle$. Por tanto, y/x no pertenece a A. Como A es integramente cerrado sobre su cuerpo de fracciones, entonces, y/x no es íntegro sobre A. Como A es noetheriano, entonces M es un A-módulo finítamente generado. Por la proposición 1.1.6. se tiene que $(y/x)M \not\subset M$. Como $y \cdot M \subseteq M^n \subseteq \langle x \rangle$, entonces, se tiene que $(y/x)M$ es un ideal de A que no está contenido en M. Por tanto, $(y/x)M = A$ y eso implica que $M = (x/y)A$ es un ideal principal y por la proposición anterior A es un dominio de ideales principales. □

Proposición 2.1.9. *Sea A un dominio noetheriano de dimensión 1. Son equivalentes.*

1. *A tiene la propiedad de factorización única de ideales.*

2. *A_M tiene la propiedad de factorización única de ideales para todo ideal maximal M de A.*

Demostración. 1 $\implies$ 2 Sea M un ideal maximal de A, se considera la aplicación natural $\phi \colon A \to A_M$. Sea $I \in A_M$ un ideal. Se considera el ideal $J \colon = \phi^{-1}(I)$. Este ideal se puede factorizar como $J = M_1^{a_1} ... M_s^{a_s}$. Ahora bien, como $J \subseteq M$ entonces, existe un i tal que $M_i \subseteq M$. De hecho son iguales por ser maximales. Por tanto, $J_M = (M_i^{a_i})_M$ teniendo así una factorización de I. Para ver que es única, como el ideal maximal de A_M es M_M hay que ver que dado a y b dos naturales distintos entonces $(M_M)^a \neq (M_M)^b$. Esto es por el lema que viene a continuación dado que $M^a \neq M^b$.

$2 \implies 1$ Sea $I \subseteq A$ un ideal no nulo. Sea $M_1, ..., M_s$ el conjunto de ideales maximales que contienen a I, entonces si I_{M_i} se puede factorizar como $I_{M_i} = M_{iM_i}^{a_i}$ para cada $i = 1, ..., s$ con a_i entero no negativo. Se verá que I se factoriza en A de forma única como $I = M_1^{a_1}...M_s^{a_s}$. Está claro que $I \subseteq \phi(M_{1M_1}^{a_1}) \cap ... \cap \phi(M_{iM_s}^{a_s})$. Además, se tiene que $M_i^{a_i} \subseteq \phi_i^{-1}((M_{iM_i})^{a_1})$. Como M_i es el único ideal maximal de A que contiene $M_i^{a_i}$, el lema siguiente implica que $M_i^{a_i} = \phi_i^{-1}(M_{iM_i}^{a_i})$. Como los ideales M^{a_i} son coprimos dos a dos, se tiene que: $M_1^{a_1} \cap ... \cap M_s^{a_s} = M_1^{a_1}...M_s^{a_s}$.

Se sigue que $I \subseteq M_1^{a_1}...M_s^{a_s}$. Por tanto, como $I_{M_i} = M_{iM_i}^{a_i} = (M_1^{a_1}...M_s^{a_s})_{M_i}$ $\forall i = 1, ..., s$, por el lema siguiente se tiene que $I = M_1^{a_1}...M_s^{a_s}$. Para ver que la factorización es única, se supondrá que $I = M_1^{b_1}...M_s^{b_s}$. Localizando en cada M_i, la factorización única de A_{M_i} da que $a_i = b_i$ para todo $i = 1, ..., s$.

□

Lema 2.1.10. *Sean $J \subseteq I$ dos ideales de un anillo A tales que el conjunto de ideales maximales que contienen a J es finito. Entonces J=I si y sólo si $J_{M_i} = I_{M_i}$ para J siendo $M_1, ..., M_s$ el conjunto de ideales maximales que contienen a J.*

Demostración. [DL, lema III 1.3] □

Por fin estamos en disposición de demostrar el teorema que nos interesa.

Teorema 2.1.11. *Sea un dominio noetheriano de dimensión 1. Son equivalentes:*

1. *A es un domino de Dedekind*
2. *A tiene factorización única de ideales*

Demostración. $1 \implies 2$ Sea M un ideal maximal de A, con demostrar que A_M tiene factorización única necesariamente, entonces la implicación es cierta. A_M es un anillo local así que sólo es necesario demostrar que es íntegramente cerrado sobre su cuerpo de fracciones. Los elementos del cuerpo de fracciones de A_M son de la forma a/b con $a \in A_M$ y $b \in M$. Por reducción al absurdo, si $(a/b) \notin A_M$ es íntegro sobre A_M entonces existen $c_1, ..., c_n \in A_M$ tales que $(a/b)^n + c_1(a/b)^{n-1} + ... + c_n = 0$. cada c_i se puede escribir como a_i/m_i con $a_i \in A$ y $m_i \notin M$. Sea m el mínimo común múltiplo de los m_i entonces, multiplicando por m^n se tiene que $(am/b)^n + c_1 m(am/b)^{n-1} + ... + c_n m^n = 0$. Por tanto, am/b es íntegro sobre A. Falta ver que $am/b \notin A$. Eso es porque si $b \mid m$ entonces, como $m \notin M$, entonces b sería una unidad en A_M y por tanto, $a/b \in A_m$

$2 \implies 1$ A tiene factorización única de ideales si y sólo si A_M tiene factorización única de ideales para todo ideal maximal M. Eso es cierto si y sólo si A_M es íntegramente cerrado para todo ideal maximal M. Falta ver que A es íntegramente cerrado si A_M lo es para todo ideal maximal M. Sean $a, b \in A$ tal que $a/b \notin A$ esto implica que b no es una unidad. Si a/b es íntegro sobre A, entonces existen

$a_1, ..., a_n \in A$ tal que $(a/b)^n + a_1(a/b)^{n-1} + ... + a_n$. Como b no es una unidad, entonces, existe un ideal maximal M que contiene a b. Eso implica que $(a/b) \notin A_M$ pero está en su cuerpo de fracciones. Sin embargo esto es una contradicción porque con el mismo polinomio, a/b sería íntegro sobre A_m. □

Conocido que los ideales se pueden factorizar, ahora se estudiará cómo es esa factorización. En el caso de enteros algebraicos, se conoce cómo se factorizan los ideales en $\mathbb{Z}$ dado que es equivalente a la factorización del generador del ideal. Dado un cuerpo de números algebraicos K se intentará exportar ese conocimiento a $\mathcal{O}_K$.

Para hacer el estudio en general se considerará A un dominio de Dedekind, con cuerpo de fracciones F y B la clausura íntegra de A en una extensión finita y separable K de F. Como queremos estudiar la factorización de ideales en B conocida la factorización en A, nos interesaremos por la factorización de los ideales que surgen de extender los ideales maximales de A en B. Para ello, primero nos fijaremos en el siguiente lema:

Lema 2.1.12. *Con la notación anterior, sea P un ideal maximal de A, entonces $PB \neq B$.*

Demostración. [DL, lema III.3.1] □

Este lema, sirve para poder escribir $PB = M_1^{e_1}...M_s^{e_s}$. Y con esta notación, se pueden definir los siguientes términos bastante importantes.

Definición 2.1.13. *Con la notación anterior, se llama* ***indice de ramificación*** *de M_i sobre P al entero $e_{M_i/P} := e_i$*

Como P es un ideal maximal de A, A/P es un cuerpo. Como $M_i \cap A$ es un ideal de A distinto del total que contiene a P y P es maximal, $M_i \cap A = P$. Como además $A \subseteq B$, entonces se define un homomorfismo natural por inclusión $i\colon A/P \to B/M_i$. Como M_i es un ideal maximal, B/M_i es un cuerpo. El homomorfismo, entonces define una extesión de cuerpos. Como B es un A-módulo finitamente generado, entonces, define una extensión finita.

Definición 2.1.14. *Se define el* ***grado residual*** *de M_i sobre P como el entero $f_{M_i/P} := [B/M_i : A/P]$.*

El objetivo será relacionar los indices de ramificación con los grados residuales.

Lo primero que se puede notar es que como los $M_i^{e_i}$ son primos dos a dos, se tiene que, denotando PB a la extensión de P como ideal en B, $B/(PB) \cong B/M_1^{e_1} \times ... \times B/M_s^{e_s}$. La idea es considerar $B/(PB)$ y cada $B/M_i^{e_i}$ como A/P-espacios vectoriales. Por tanto, se tiene que $\dim(B/(PB)) = \dim(B/M_1^{e_1}) + ... + \dim(B/M_s^{e_s})$. El paso lógico ahora sería intentar escribir $\dim(B/M_i^{e_i})$ en función de $\dim(B/M_i)$ para cada $i = 1, ..., s$. Esto nos lo dará el siguiente lema.

Lema 2.1.15. *Sea A un dominio de Dedekind. Sea P un ideal maximal de A. Entonces, $\forall n \in \mathbb{N}$ el A-módulo P^{n-1}/P^n es isomorfo a A/P. En particular, si A/P es finito, se tiene que $\#(A/P^n) = (\#A/P)^n$.*

Demostración. [DL, lema 3.4] □

Corolario 2.1.16. *$dim(B/M_i^{e_i}) = e_i dim(B/M_i)$*

Demostración. Como A/P es finito, sea r el número de elementos, un A/P-espacio vectorial de dimensión d tiene r^d elementos. Por tanto, B/M_i tiene $r^{\dim(B/M_i)}$ elementos. Por tanto, $r^{\dim(B/M_i^{e_i})} = \#(B/M_i^{e_i}) = (\#B/M_i)^{e_i} = r^{e_i \dim(B/M_i)}$. □

Así que se puede escribir $\dim(B/(PB)) = e_1\dim(B/M_1) + ... + e_s\dim(B/M_s)$. Esta expresión se puede mejorar un poco más si se usa el siguiente lema.

Lema 2.1.17. *dim(B/(PB))=[K:F]*

Demostración. Este lema se probará en el caso en el que P sea un ideal principal.

Sea $[K : F] = n$. Como B es un A-módulo libre de rango n [DL, lema I.4.10] entonces, $B \cong A \oplus ... \oplus A$. Si p es un generador de P, entonces $PB \cong PA \oplus ... \oplus PA \cong P \oplus ... \oplus P$. Por tanto, $B/(PB) \cong (A \oplus ... \oplus A)/(P \oplus ... \oplus P) \cong (A/P)^n$. Por tanto, $dim(B/(PB)) = n$ □

Así que se ha demostrado el siguiente resultado:

Proposición 2.1.18. *Sea A un dominio de Dedekind. Sea F su cuerpo de fracciones. Sea L/K una extensión finita de F con [K:F]=n. Sea B la clausura íntegra de A en K. Sea $P \subset A$ un ideal primo tal que en B se cumple que $P = M_1^{e_1}...M_s^{e_s}$. Entonces, $n = e_1f_1 + ... + e_sf_s$ donde $f_i = f_{M_i/P}$.*

Este resultado, ya da información que restringe la factorización y tiene aplicaciones.

Sea A un dominio de Dedekind sea F su cuerpo de funciones. Sea $f \in A[y]$ un polinomio irreducible. Entonces, $K := F[y]/\langle f \rangle$ es una extensión finita de F de grado n. Si f es tal que la clausura íntegra de A en K es $B := A[y]/\langle f \rangle$, entonces, se puede intentar usar la proposición anterior para, dado un ideal primo $P \subseteq A$, factorizar PB. Se llamará $\bar{f}$ a la reducción de f en $(A/P)[y]$

Se tiene $B/PB \cong (A[y]/\langle f \rangle)/PB \cong A[y]/\langle P, f \rangle \cong (A/P)[y]/\langle \bar{f} \rangle$

Como PB no siempre tiene que ser maximal, se tiene que $(A/P)[y]/\langle \bar{f} \rangle$ no siempre será un cuerpo y por tanto, cuando no lo sea, $\bar{f}$ se podrá factorizar. Puesto, el hecho de que PB se pueda factorizar implica que $\bar{f}$ se puede factorizar, sería interesante ver si la factorización de PB tiene que ver con la factorización de $\bar{f}$.

Sean $\bar{g_1}, ..., \bar{g_s} \in (A/P)[y]$ polinomios irreducibles tales que existen enteros $e_1, ..., e_s$ tales que $\prod_{i=1}^{s} \bar{g_i}^{e_i} = \bar{f}$. Sean $g_1, ..., g_s \in A$ polinomios tales que su reducción en $(A/P)[y]$ es $\bar{g_1}, ..., \bar{g_s}$, entonces se tiene que existe $h \in PA[y]$ tal que $f = g_1^{e_1} \cdot ... \cdot g_s^{e_s} + h$.

Como un breve paréntesis, ahora se abusará de la notación y se llamará g_i tanto, al polinomio en $A[y]$ como a su clase en B y se distinguirá por el contexto. También ocurrirá lo mismo con $\bar{g_i}$. Según el contexto denotará al polinomio en $(A/P)[y]$ o a la clase de equivalencia en $(A/P)[y]/\langle \bar{f} \rangle$.

Se considerarán los ideales $M_i = \langle PB, g_i \rangle$. Entonces, se tiene que: $M_1^{e_1} \cdot ... \cdot M_s^{e_s} \subseteq \langle PB, g_1^{e_1} \cdot ... \cdot g_s^{e_s} \rangle$. Como $h \in PA[y]$ entonces su clase en B está en PB. Por tanto, $\langle PB, g_1^{e_1} \cdot ... \cdot g_s^{e_s} \rangle = \langle PB, g_1^{e_1} \cdot ... \cdot g_s^{e_s} - h \rangle = \langle PB, f \rangle = PB$.

Ahora falta ver que $PB = M_1^{e_1} \cdot ... \cdot M_s^{e_s}$. Si $PB = M_1^{a_1} \cdot ... \cdot M_s^{a_s}$. La contención que tenemos antes dice que $a_1 \leq e_1, ..., a_s \leq e_s$.Hay que demostrar la igualdad.

Por la proposición 2.1.18. se tiene que $n = a_1 f_1 + ... + a_s f_s$. Vamos a calcular f_1. $B/M_i = B/\langle PB, g_i \rangle = (A[x]/\langle f \rangle)/\langle PB, g_i \rangle) = A[x]/\langle P, f, g_i \rangle = (A/P)[x]/\langle \bar{f}, \bar{g_i} \rangle = (A/P)[x]/\langle \bar{g_i} \rangle$. Por tanto, $f_i = [B/M_i : A/P] = deg(g_i)$. Como se tiene que $n = deg(f) = e_1 deg(g_1) + ... + e_s deg(g_s) = e_1 f_1 + ... + e_s f_s$, debe ocurrir que $e_i = a_i$ para todo $i = 1, ..., s$.

Esto se puede resumir en la siguiente proposición:

Proposición 2.1.19. *Con la notación anterior* $PB = M_1^{e_1} \cdots M_s^{e_s}$. *Además* $f_i = \deg g_i$

Esto se puede usar por ejemplo para factorizar ideales en cuerpos cuadráticos:

Proposición 2.1.20. *Sea* $K = \mathbb{Q}(\sqrt{d})$.*con* $d \in \mathbb{Z}$ *libre de cuadrados y* $d \neq 1$. *Sea* $p \in \mathbb{Z}$ *un número primo. Entonces* $\langle p \rangle$ *se factoriza en* $\mathcal{O}_K$ *como:*

1. *Si* $p \mid d$ *se tiene que* $\langle p \rangle = \langle p, \sqrt{d} \rangle^2$
2. *Si* $2 \nmid d$

$$\langle 2 \rangle = \begin{cases} \text{es primo si } d \equiv 5 \bmod 8 \\ \langle 2, (1+\sqrt{d})/2 \rangle \langle 2, (1-\sqrt{d})/2 \rangle \text{ si } d \equiv 1 \bmod 8 \\ \langle 2, 1+\sqrt{d} \rangle^2 \text{ si } d \equiv 3 \bmod 4 \end{cases}$$

3. *Si* $p \nmid d$ *y* $p \neq 2$, *entonces:*

$$\langle p \rangle = \begin{cases} \text{es primo si } d \text{ no es un cuadrado mod } p \\ \langle p, \sqrt{d}+n \rangle \langle p, \sqrt{d}-n \rangle \text{ si } n^2 \equiv d \bmod 8 \end{cases}$$

Demostración. El apartado 3 está demostrado en [DL, ejemplo III.4.4]. En general está demostrado en [IR, prop 13.1.3 y prop 13.1.4]. Aquí se demostrará el apartado

3 cuando $d \not\equiv 1 \bmod 4$ usando la idea anterior para ejemplificar cómo se puede aplicar.

Lo primero es que en este caso $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Además $\mathbb{Z}[x]/\langle x^2 - d\rangle \cong \mathcal{O}_K$ via el isomorfismo $\phi\colon \mathbb{Z}[x] \to \mathcal{O}_K$ dado por $\phi(f(x)) = f(\sqrt{d})$. f es irreducible. Para usar la idea anterior se verá cómo se factoriza su clase $(\bar{f})$ en $\mathbb{Z}/\langle p\rangle[x]$. Como $\bar{f}$ es de grado 2 se factoriza si y sólo si tiene una raiz en $\mathbb{Z}/\langle p\rangle$. Es decir, si d es un cuadrado módulo p. Por tanto si d no es un cuadrado módulo p se tiene que $\langle p\rangle$ es primo en $\mathbb{Z}[x]/\langle f\rangle$. Por tanto, $\langle p\rangle$ es primo en $\mathcal{O}_K$. Veamos en el otro caso.

Si $n^2 \cong d \bmod p$ entonces $\bar{f} = (x-n)(x+n)$. Por tanto, en $\mathbb{Z}[x]/\langle f\rangle$ se tiene que $\langle p\rangle = \langle p, x-n\rangle\langle p, x+n\rangle$. El resultado se tiene de aplicar el isomorfismo ϕ. □

2.2. Grupo de clase

Si los anillos de enteros no tienen por qué tener factorización única, entonces, tampoco se puede esperar que sean dominios de ideales principales. El objetivo, a partir de ahora será "medir" cómo de lejos está un anillo de ser dominio de ideales principales. En particular se estudiará el caso de los anillos de enteros.

La idea de esto, será hacer una relación de equivalencia según la cual una de las clases sea la de los ideales principales y se medirá la cantidad de clases que hay.

Definición 2.2.1. *Dado un anillo conmutativo A, que sea dominio de integridad, sea $M(A)$ el conjunto de ideales no nulos. Sean $I, J \in M(A)$ se considera la relación de equivalencia siguiente:*

$I \sim J$ si y sólo si $\exists a, b \in A$ tal que $\langle a\rangle I = \langle b\rangle J$.

Se define $Cl(A)$ como el conjunto de clases de equivalecia junto con la operación siguiente:

Sean $I, J \in M(A)$, sean $\overline{I}, \overline{J}$ la clase de equivalencia de I y de J respectivamente, se define la operación $\bar{I}\bar{J} = \overline{IJ}$.

Cuando sea un grupo se llamará ***grupo de clase****.*

La operación está bien definida y con esa operación $Cl(A)$ es un semigrupo. Ahora se comprobarán algunas cosas para ver que efectivamente, el grupo de clases de ideales es interesante.

Lema 2.2.2. *Sea A un anillo conmutativo y dominio de integridad. Si $I \in M(A)$ entonces $I \sim A$ si y sólo si I es un ideal principal*

Demostración. Si $A \sim I$, entonces, existen $a, b \in A$ tales que $\langle a\rangle A = \langle b\rangle I$. Como $a \in \langle b\rangle I$ entonces, existe $c \in I$ tal que a=bc. Sea $d \in I$, entonces, $bd \in \langle a\rangle$ por tanto, $\exists x \in A$ tal que $bd = ax$. Como$a = bc$, se tiene que $bd = bcx$. Como es un dominio de integridad, se puede cancelar y se tiene: $d = cx$. Por tanto, $I = \langle c\rangle$ y por tanto, es un ideal principal.

Si I es un ideal principal es trivial que $I \sim A$. □

La primera duda que uno puede tener es si dado un anillo dado un ideal I siempre se puede pedir que exista un ideal J tal que IJ es principal. La respuesta es no. Por ejemplo, en el anillo de polinómios en infinitas variables sobre un cuerpo k, es decir $k[\{x_i\}_{i\in\mathcal{N}}]$ tiene un ideal que es el ideal $\langle\{x_i\}_{i\in\mathcal{N}}\rangle$ que vale de contraejemplo. Afortunadamente, en los casos que nos interesan, si ocurre como se puede ver en el siguiente lema.

Lema 2.2.3. *Sea A un dominio de Dedekind. Entonces, $Cl(A)$ es un grupo con elemento neutro $1 := \overline{A}$.*

Demostración. Hay que demostrar que cada elemento tiene inverso. Sea $J \in M(A)$, y sea $a \in J$, entonces como $\langle a\rangle \subseteq J$, y el anillo tiene factorización única de ideales, debe existir $I \in M(A)$ tal que $\langle a\rangle = IJ = JI$. Por tanto, $\bar{I}\bar{J} = \bar{J}\bar{I} = 1$.

Probar que efectivamente 1 es el elemento neutro es trivial puesto que $\bar{A}\bar{I} = \bar{I}\bar{A} = \overline{IA} = \bar{I}$

□

Para entender $Cl(A)$ como una medida de lo lejos que está A de ser dominio de ideales principales, hay que notar que cuando $Cl(A)$ sólo tiene un elemento, entonces A es un dominio de ideales principales. De hecho, por el lema 2.2.2, A es un dominio de ideales principales si y sólo si $Cl(A)$ tiene un elemento. Además, si $Cl(A)$ es finito esa "lejanía"se puede medir por el número de elementos.

Definición 2.2.4. *Sea A un dominio de integridad conmutativo tal que $Cl(A)$ es finito. Entonces, se define el* ***número de clases*** $h_A \colon = \#CL(A)$

Esto, es interesante, dado que si $Cl(A)$ es finito, entonces, el teorema de Lagrange asegura que dado J un ideal de A, entonces $J^{h_A} = 1$.

Para que esto sea útil, será interesante saber si efectivamente $Cl(A)$ es finito o no. De aquí en adelante, nos preocuparemos de ver cuando es finito, se comprobará que este es el caso de los anillos de enteros algebraicos y el objetivo será buscar formas de calcular $h_{\mathcal{O}_K}$ para los distintos cuerpos de números algebraicos K.

Definición 2.2.5. *Sea A un dominio de Dedekind. Se dice que A tiene* ***cocientes finitos*** *si A/M tiene un número finito de elementos para todo ideal maximal M de A.*

Definición 2.2.6. *Sea A un dominio de Dedekind con cocientes finitos, entonces, dado un ideal I, se define su* ***norma*** $\|I\|_A = \#A/I$.

Se ha comprobará que $\#A/I$ es un número entero en el lema 2.2.7 y dado que $A/I \cap J \cong A/I \times A/J$ si I y J son primos entre si. Cuando se sepa por el contexto el anillo en el que se está trabajando solo se escribirá $\|I\|$.

Lema 2.2.7. *Sea A un dominio de Dedekind con cocientes finitos. Entonces, la norma de cualquier ideal no nulo es un número entero y además es una función multiplicativa.*

Demostración. [DL, lema 3.5] □

Ahora, se enunciarán varios lemas con el objetivo de encontrar una propiedad en las normas de ideales para comprobar, en anillos de enteros algebraicos, si el grupo de clase es finito o no.

Lema 2.2.8. *Los enteros algebraicos tienen cocientes finitos.*

Demostración. Dado un cuerpo de números algebraicos K, si M es un ideal maximal entonces, existe un primo $p \in \mathbb{Z}$ tal que $\langle p\rangle = M \cap \mathbb{Z}$ con los M_i ideales maximales. Como $\mathcal{O}_K/M$ es una extensión finita de $\mathbb{Z}/\langle p\rangle$ entonces $\#(\mathcal{O}_K/M) = \#(\mathbb{Z}/\langle p\rangle)[\mathcal{O}_K/M : \mathbb{Z}/\langle p\rangle]$ □

Como los anillos de enteros tienen cocientes finitos, la norma de los ideales es finita. En el siguiente capítulo se comprobara que efectivamente, los anillos de entero tienen grupo de clase finito.

A partir de aquí, se considerará que $K/\mathbb{Q}$ es una extensión finita.

Lema 2.2.9. *Dado $a \in \mathbb{R}$. El número de ideales I de $\mathcal{O}_K$ tal que $\|I\| \leq a$ es finito.*

Demostración. Como $\|\cdot\|$ es multiplicativa, sólo hay que probarlo para los ideales maximales. Sea M un ideal maximal de $\mathcal{O}_K$. Como se tiene que $\|M\|_{\mathcal{O}_K} = \|M \cap \mathbb{Z}\|_{\mathbb{Z}}^{f_{M/M\cap\mathbb{Z}}} \geq \|M \cap \mathbb{Z}\|_{\mathbb{Z}}$, entonces sólo hay que probar el lema para $\mathbb{Z}$.

Sea un ideal primo de $\mathbb{Z}$ es un ideal principal generado por un número primo. Dado un número primo $p \in \mathbb{Z}$, se tiene que $\#(\mathbb{Z}/\langle p\rangle) = p$ por tanto, ya se tiene el lema. □

Lema 2.2.10. *$Cl(\mathcal{O}_K)$ es finito si y sólo si, existe un número $a \in \mathbb{R}$ tal que para toda clase $C \in Cl(\mathcal{O}_K)$ existe un ideal $I \in C$ con $\|I\| \leq a$.*

Demostración. Si $Cl(\mathcal{O}_K)$ es finito, sea $Cl(\mathcal{O}_K) = \{C_1, ..., C_n\}$, se elige un ideal $I_i \in C_i$ para cada $i = 1, ..., n$ y se elige $a = \max\{\|I_1\|, ..., \|I_n\|\}$.

Si existe un a con la propiedad anterior, como sólo hay un número finito de ideales con norma menor que a, entonces el número de clases de equivalencia debe ser finito.

□

Lema 2.2.11. *Dado $a \in \mathbb{R}$ entonces,toda clase de ideales de $\mathcal{O}_K$ contiene un ideal I tal que $\|I\| \leq a$ si todo ideal no nulo J contiene un elemento b tal que $\|\langle b\rangle\| \leq a\|J\|$.*

Demostración. Dado una clase de ideales $C \in Cl(A)$, como $\mathcal{O}_K$ es un dominio de dedekind, tiene inversa C^{-1} sea $J \in C^{-1}$ y sea $B \in J$ tal que $\|\langle b\rangle\| \leq a\|J\|$. Entonces, como $\mathcal{O}_K$ tiene factorización única, debe existir un ideal I tal que $\langle b\rangle = IJ$. Por tanto, $\|I\|\|J\| = \|IJ\| \leq a\|J\|$ teniendose así que $\|I\| \leq a$. Como C es la inversa de C^{-1}, entonces, $I \in C$. □

Finalmente se notará que $\|\langle b\rangle\| = |N(b)|$ para todo $b \in \mathcal{O}_K$ [RIB, capítulo 8 F].

Los esfuerzos en el siguiente capítulo irán dirigidos a encontrar un a tal que cumpla la desigualdad del tema anterior. Existen varias formas de encontrarlo. Esta no será la más directa, pero sin embargo servirá más tarde para encontrar una fórmula asintótica para el número de clases.

3

Teorema de minkowski y cotas del dicriminante.

3.1. Teorema de Minkowski

Definición 3.1.1. *Un **retículo** A en $\mathbb{R}^n$ es el conjunto de todas las combinaciones lineales sobre $\mathbb{Z}$ de n elementos $a_1, ..., a_n$ linealmente independientes*

El paralelotopo fundamental de A es el conjunto $\Pi = \{\sum_{k=1}^{n} x_k a_k \mid x_k \in \mathbb{R}, 0 \leq x_k \leq k = 1, ..., n\}$. Se denotará el volumen de Π por $\mu = \mu(\Pi)$

Definición 3.1.2. *Un subconjunto $S \subseteq \mathbb{R}^n$ es **convexo** si $\forall y, y' \in S$ y $\forall \lambda \in [0, 1]$, se tiene que $\lambda y + (1 - \lambda)y' \in S$*

Definición 3.1.3. *Si $S \subseteq \mathbb{R}^n$ es un conjunto y $a \in \mathbb{R}$, se define la **homotecia** de S con radio a al conjunto $aS = \{ax \mid x \in S\}$.*

Si S es convexo y $x, x' \in aS$ entonces existen $y, y' \in S$ tal que $x = ay$ y $x' = ay'$. Dado $\lambda \in [0, 1]$, se tiene que $\lambda x + (1-\lambda)x' = \lambda ay + (1-\lambda)ay' = a(\lambda y + (1-\lambda)y') \in aS$. Por tanto, aS es convexo $\forall a \in \mathbb{R}$.

Definición 3.1.4. *Si $S \subseteq \mathbb{R}^n$ es convexo, cerrado y acotado, se dirá que es un **cuerpo convexo**.*

Definición 3.1.5. *Si $S \subseteq R^n$ es tal que $y \in S$ si y sólo si $-y \in S$, se dice que S es simétrico.*

Lema 3.1.6. *Sea S un conjunto convexo. Sean $y, y' \in int(S)$, entonces, todo punto del segmento que une y e y' está en el interior de S*

Demostración. Como tanto y como y' están en int(S), existe un $c \in \mathbb{R}_{>0}$ tal que $B(y, c) \subseteq S$ y $B(y', c) \subseteq S$ siendo $B(a, r) = \{x \mid \|x - a\| < r\}$.

Sea y'' un punto del segmento que une y e y', entonces, $\exists\lambda \in [0,1]$ tal que $y'' = \lambda y + (1-\lambda)y'$. Se probará que $B(y'', c) \subseteq S$.

Sea $x \in B(y, c'')$, entonces, $\|x - y''\| \leq c$. Sea $z = x - y''$, entonces, $x = z + y'' = z + \lambda y + (1-\lambda)y' = \lambda(z+y) + (1-\lambda)(z+y')$.

Si se prueba que $z + y \in S$ y $z + y' \in S$, como S es convexo se tiene que $x \in S$. $\|(z+y) - y\| = \|z\| = \|x - y''\| \leq c$. Por tanto, $z + y \in B(y, c) \subseteq S$. Análogamente con z+y'. Por tanto, $x \subseteq S$. □

Teorema 3.1.7. *(Minkowski). Sea $A \subseteq \mathbb{R}^n$ un retículo. Sea μ el volumen del paralelotopo fundamental de A.*

Si S es un cuerpo convexo y simétrico tal que $vol(S) > 2^n\mu$, entonces existe un punto de A distinto del origen que pertenece al interior de S.

Si $vol(S) = 2^n\mu$, no se puede asegurar que el punto esté en el interior pero sí que existe uno.

Demostración. Se supondrá que $S \cap A = \{0\}$.

Sea $y \in A$, se considera $Sy = y + 1/2S = \{y + 1/2x \mid x \in S\}$. Sy es convexo porque es suma de conjuntos convexos.

Si $y, y' \in A$ son distintos y $x \in \text{int}(Sy)$, entonces, $x \notin \text{int}(Sy')$. En otro caso, $x - y \in \text{int}(1/2S)$ y $x - y' \in \text{int}(1/2S)$. Entonces, como $1/2S$ es convexo y simétrico, se tendría que $1/2(x-y) + 1/2(y'-x) \in 1/2S$. Por tanto, $1/2(y'-y) \in 1/2S$. Es decir, $(y'-y) \in S$ siendo esto una contradicción porque $S \cap A = \{0\}$. Por tanto, dados $y, y \in A$, los interiores de Sy y de Sy' son disjuntos.

Sea $a_1, ..., a_n \in \mathbb{R}^n$, los generadores de A. Dado $m \geq 0$ se define $A_m = \{\sum_{i=1}^n y_i a_i \mid -m \leq y_i \leq m, y_i \in \mathbb{Z}, i = 1, ..., n\}$. Claramente, $\#A_m = (2m+1)^n$.

Como S está acotado, existe $\gamma \geq 0$ tal que si $x = \sum_{i=1}^n x_i a_i \in S$, entonces, $|x_i| \leq \gamma\ \forall i = 1, ..., n$. Por tanto, $\forall y \in A_m$, se tiene que $|y_i + 1/2x_i| \leq |y_i| + 1/2|x_i| \leq m + 1/2 \cdot \gamma\ \ \forall x \in S$. Por tanto, $A_m + 1/2S \subseteq \Pi' = \{\sum_{j=1}^n x_j a_j \mid |x_j| \leq m + 1/2 \cdot \gamma\}$.

Entonces, como $A_m + 1/2S = \bigcup_{y \in A_m} [y + 1/2S] = \bigcup_{y \in A_m} Sy$, Como los Sy tienen los interiores disjuntos, y como las translaciones dejan los volúmenes invariantes, se tiene que:

$vol(A_m + 1/2S) = \sum_{y \in A_m} vol(1/2Sy) = \sum_{y \in A_m} (1/2^n) vol(Sy) = \sum_{y \in A_m} vol(S) = \#A_m (1/2^n) vol(S) = ((2m+1)^n/2^n) vol(S) \leq ((2m+\gamma)^n/2^n)\mu$.

Entonces:

$$vol(S) \leq ((2m+\gamma)^n/(2m+1)^n) 2^n \mu \quad \forall m \in \mathbb{Z}_{>0}$$

Si se hace tender m a infinito se tiene que $vol(S) \leq 2^n\mu$. Por tanto, si $vol(S) > 2^n\mu$, entonces tiene un elemento del retículo en su interior.

Para el caso en que $vol(S) = 2^n\mu$, se tiene que $\forall n \geq 1 \quad vol((1+1/n)S) > vol(S) = 2^\mu$. Por tanto $\exists x_n \in (1+1/n)S \cap A$ no nulo. Como cada $(1+1/n)S \subseteq 2S$, entonces, está acotado. Por tanto, $2S \cap A$ es finito. Por tanto, existen $n_1 < n_2 < ....$

tal que $x_{n_k} = x_{n_1} \quad \forall k \in \mathbb{N}$. Entonces, $x_{n_1} \in S$ dado que dado $m \in \mathbb{Z}$, entonces, existe k tal que $n_k \geq m$. Así que $x_{n_1} = x_{n_k} \in (1 + 1/n_k)S \subset (1 + 1/m)S$. Por tanto, como $S = \bigcup_{m\in\mathbb{Z}}(1 + 1/m)S$, se tiene que $x_1 \in S$.

□

Este teorema es muy útil a la hora de demostrar la existencia de soluciones en ecuaciones diofánticas.

Se usará aquí para demostrar la existencia de soluciones en sistemas lineales de desigualdades.

Proposición 3.1.8. *Sea $n \geq 1$. Sea $L_i(x_1, ..., x_n) = \sum_{i=1}^{n} a_{ij}x_i \quad i = 1, ..., n$ con $a_{ij} \in \mathbb{R}\ \forall i = 1, ..., n \quad j = 1, ..., n$, tal que $d = det(a_{ij}) \neq 0$. Sean $t_1, ..., t_n$ números positivos con $t_1, ..., t_n \geq |d|$. Dado i_0 con $1 \leq i_0 \leq n$, entonces, existen $b_1, ..., b_n \in \mathbb{Z}$ no todos nulos, con $|L_i(b_1, ..., b_n)| < t_i$ si $i \neq i_0$ y $|L_{i_0}(b_1, ..., b_n)| \leq t_{i_0}$*

Demostración. Sin pérdida de generalidad $i_0 = n$.

Si n=1 entonces $|L_1(1)| = |a_{11}| = d \leq t_n$.

Si $n > 1$ se hará por reducción al absurdo. Si la proposición no es cierta, entonces $\forall x_1, ..., x_n \in \mathbb{Z}$ se tiene una de las siguientes afirmaciones:

1. $\exists i$ con $1 \leq i \leq n - 1$ tal que $|L_i(x_1, ..., x_n)| \geq t_i$
2. $\forall i$ tal que $1 \leq i \leq n - 1 |L_i(x_1, ..., x_n)| < t_i$ pero $|L_n(x_1, ..., x_n)| > t_n$

Sea $T = \{(x_1, ..., x_n) \mid (x_1, ..., x_n)$ satisfacen 2.$\}$. Si $T \neq \emptyset$, sea $(x_1, ..., x_n) \in T$ y sea t tal que $|L_n(x_1, ..., x_n)| < t$.

Se considera $T' = \{(x_1, ..., x_n) \in T \mid |L_n(x_1, ..., x_n)| < t\}$. Entonces T' es no vacío y T' es finito porque es un subcojunto acotado de $\mathbb{Z}^n$. Por tanto, $A = \{|L_n(x_1, ..., x_n)| \mid (x_1, ..., x_n) \in T'\}$. tiene mínimo.

Sea $\delta = t_n - min(A)$, por la condición 2. se tiene que $\delta > 0$. Si $T = \emptyset$, entonces, δ puede tomar cualquier valor. Por tanto, existe δ tal que $\forall (x_1, ..., x_n) \in \mathbb{Z}^n$ no nulo, se tiene que o bien $|L_i(x_1, ..., x_n)| \geq t_i$ para algún i=1,...,n-1 o bien $|L_n(x_1, ..., x_n)| \geq t_n + \delta$.

Se define el homomorfismo siguiente. Sea $x \in \mathbb{R}^n$, se define $\theta\colon \mathbb{R}^n \to \mathbb{R}^n$ com $\theta(x) = (L_1(x), ..., L_n(x)$. Sea e_i el vector que es 1 en la fila i y 0 en el resto, entonces, θ transforma $e_1, ..., e_n$ en los vectores linealmente independientes $\theta(e_1), ..., \theta(e_n)$. Sea A el retículo definido con estos vectores, entonces, es $\mu = |d|$ el volumen del paralelotopo fundamental.

Sea S el conjunto de los elementos $x = (x_1, ..., x_n) \in \mathbb{R}^n$ tal que $|x_i| \leq t_i$ para $i = 1, .., n-1$ y $|x_n| \leq t_n + \delta$. Entonces, S es un cuerpo convexo simétrico que tiene volumen $\text{vol}(S) = 2t_1..2t_{n-1}2(t_n + \delta) > 2^n t_1...t_n \geq 2^n|d| \geq 2^n\mu$. Por el teorema de Minkiowski, existe un punto $\theta(y) \in A$ no nulo en el interior de S. Es decir, existen $y_1, ..., y_n$, no todos numlos tal que $|L_i(y)| < t_i$ para i=1,...,n-1 y $|L_n(y)| < t_n + \delta$, lo que es una contradicción. □

Proposición 3.1.9. *Sea $n > 1$ y sea $L_i(x_1, ..., x_n) = \sum_{i=1}^{n} a_{ij}x_j$ para todo $i = 1, ..., n$ una forma lineal con $a_{i,j} \in \mathbb{C}$ con $d = det(a_{ij}) \neq 0$. Suponiendo que para todo i existe un índice i' tal que $\overline{L_i}(x_1, ..., x_n) = \sum_{j=1}^{n} \overline{a_{ij}}x_j$ es igual a $L_{i'}$, (si L_i tiene coeficientes reales $i=i'$). Sean $t_1, ..., t_n$ numeros reales positivos con $t_i = t_{i'}$ si $\overline{L_i} = L_{i'}$. Si $t_1, ..., t_n \geq |d|$, dado cualquier indice i_0 tal que $\overline{L_{i_0}} = L_{i_0}$, existen enteros $x_1, ..., x_n$ no todos nulos tal que $\overline{L_i}(x_1, ..., x_n) < t_i$ si $i \neq i_0$ y $|L_{i_0}|(x_1, ..., x_n) \leq t_{i_0}$*

Demostración. [RIB, B cap 9] □

Finalmente, tenemos los resultados para probar la cota que buscábamos.

Proposición 3.1.10. *Dado un cuerpo de números algebraicos, para todo ideal J no nulo de $\mathcal{O}_K$ existe un elemento $a \in J$, $a \neq 0$, tal que $|N(a)| < \|J\|\sqrt{|\delta|}$ siendo δ el discriminante de K.*

Demostración. Sea $a_1, ..., a_n$ una base de K sobre $\mathbb{Q}$ tal que es un sistema generador de J como $\mathbb{Z}$-módulo. Se considera las n forma lineales $L_i = \sum_{j=1}^{n} a_j^{(i)}x_j \quad \forall i = 1, ..., n$.

Como $d = det(a_j^{(i)}) = \|J\|\sqrt{|\delta|}$ se puede coger $t_1 = ... = t_n = d^{1/n}$ para usar la proposición anterior, que dice que existen $x_1, ..., x_n \in \mathbb{Z}$ no todos nulos tal que $\left|\sum_{j=1}^{n} a_j^{(i)}x_j\right| \leq d^{1/n} \quad \forall i = 1, ..., n$. Con al menos una desigualdad estricta.

Sea $a = \sum_{j=1}^{n} x_j a_j \in J$, se tiene que $a \neq 0$ porque no todos los x_j son nulos. Además $N(a) = \prod_{i=1}^{n}(a^{(i)}) = \prod_{i=1}^{n}(\sum_{j=1}^{n} x_j a_j^{(i)}) < d = \|J\|\sqrt{|\delta|}$. □

De aquí ya tenemos que $Cl(\mathcal{O}_K)$ es finito

4 Unidades

4.1. Raices de la unidad.

Ya hemos tenido un contacto con las unidades cuando probamos que $\mathbb{Z}[\sqrt{-5}]$ no tenía factorización única. Para intuir que serán interesantes a la hora de calcular el número de clases, se notará que si K es un cuerpo de números algebraicos, J es un ideal de $\mathcal{O}_K$ y $a, b \in \mathcal{O}_K$ son asociados, es decir, existe una unidad u tal que $a = ub$, entonces, se tiene que $a \in J$ si y sólo si $b \in J$. De hecho, a y b generan el mismo ideal.

Se denotará $U(\mathcal{O}_K)$ (o U si se sobreentiende por el contexto), al grupo de unidades de $\mathcal{O}_K$. De nuevo, nos adelantamos a un resultado diciendo que es un grupo. Pero de hecho, no es complicado probar que lo es con el producto, ya que cada elemento tiene inverso por definición de unidad, si u y v son unidades entonces uv lo es porque su elemento inverso es $v^{-1}u^{-1}$ y hereda el resto de propiedades de que el producto es un grupo en $\mathcal{O}_K$.

En este capítulo se estudiará qué estructura tiene ese grupo.

Las unidades más simples son las raices de la unidad. es decir, las raices de polinomios de la forma $x^m - 1$ donde $m \geq 1$. Estas unidades forman un subgrupo ya que 1 es una raiz de la unidad porque es raiz del polinomio con $m = 1$, si ζ es una raiz de la unidad ζ^{-1} también lo es dado que $(\zeta^{-1})^m = (\zeta^m)^{-1} = 1$ y el producto de raices de a unidad es una raiz de la unidad porque si ζ y ζ' son tales que $\zeta^m = 1$ y $\zeta^n = 1$ entonces, $(\zeta\zeta')^{nm} = 1$. El grupo de raices de la unidad de $\mathcal{O}_K$ se denotará como $W(\mathcal{O}_K)$ y si el contexto es claro, se dejará en W.

La primera pregunta es ¿W es finito o infinito?. Lo primero es caracterizar las raices de unidad de una forma que sea facil de contar. Como si $a \in \mathcal{O}_K$ es raiz de la unidad, entonces, existe m tal que $a^m = 1$, se tiene que $|a^m| = 1$ teniendo que $|a|^m = 1$ y por tanto $|a| = 1$ Hay que notar que un conjugado de a también es raiz de la unidad puesto que si σ es un endomorfismo, entonces, se tiene que

$\sigma(a)^m = \sigma(a^m) = \sigma(1) = 1$. La otra implicación también se tiene. Es decir, a es raiz de la unidad si y sólo si $\left|a^{(i)}\right| = 1$ para todo conjugado $a^{(i)}$ de a. Esto se verá luego, pero antes, veamos la finitud de W con la siguiente proposición.

Proposición 4.1.1. *Sea c un numero real positivo. Sea K un cuerpo de números algebraicos. Entonces, existe un número finito de enteros algebraicos x en K tal que* $\left|x^{(i)}\right| \leq c$ *para todo conjugado* $x^{(i)}$ *de x.*

Demostración. Sea $[K : \mathbb{Q}] = n$. Sean $s_i(x_1, ..., x_n) = \sum_{j_1<...<j_i} x_{j_1}...x_{j_i}$ $\forall i = 1, ..., n$.

La idea será encontrar un conjunto finito de polinomios F tal que si $x \in \mathcal{O}_K$ y $\left|x^{(i)}\right| \leq c$ para todo conjugado $x^{(i)}$ de x, entonces, hay un polinomio del que x es raiz.

Lo primero que se notará es que $f(x) = \prod_{i=1}^{n}(x - x^{(i)}) = x^n + \sum_{i=1}^{n}(-1)^i s_i(x^{(1)}, ..., x^{(n)})x^{n-i}$. Luego, como x es un entero algebraico, cada $s_i(x^{(1)}, ..., x^{(n)})$ es un número entero. Finalmente, $\left|s_i(x^{(1)}, ..., x^{(n)})\right| \leq \binom{n}{i}c^i$. Sea $r = \max\{\binom{n}{i}c^i \mid i = 1, ..., n\}$. Entonces, si F es el conjunto de los polinómios mónicos de grado n con coeficientes enteros que en valor absoluto son menores o iguales que r, entonces F tiene las propiedades que buscamos. Como F es finito, entonces, el conjunto $S = \{x \mid f(x) = 0 f \in F\}$ es finito y el resultado se da. □

Teniendo este resultado y teniendo en cuenta que si x es raiz de la unidad, entonces, $\left|x^{(i)}\right| = 1$ para todo conjugado $x^{(i)}$ de x. Por tanto, hay un número finito de raices de la unidad. Para caracterizarlas completamente, se tiene el siguiente resultado.

Proposición 4.1.2. *Dado un cuerpo de números algebraicos K y* $x \in \mathcal{O}_K$*, entonces,* $x \in W$ *si y sólo si x es un entero algebraico de K tal que* $\left|x^{(i)}\right| = 1$ *para todo conjugado* $x^{(i)}$ *de x*

Demostración. Si $x \in W$, se ha probado que se tiene la implicación.

Para probar la otra implicación, simplemente, hay que notar que si x no es una raiz de la unidad, entonces, suponiendo que $|x| = 1$, se tiene que $|x^r| = 1$ para todo r natural. Por la proposición anterior, deben existir dos exponentes $a > b$ tal que $x^a = x^b$. Esto contradice que no sea raiz de la unidad porque como estamos en un dominio de integridad, se tiene que $x^{a-b} = 1$. □

Usando el teorema de Lagrange, se tiene que si W tiene h elementos, entonces el orden de cada elemento de W divide a h. Por tanto, todo elemento de W es raiz de $x^h - 1$. Como las raices de ese polinomio son el grupo cíclico generado por $e^{2\pi i/h}$, entonces, como todo subgrupo de un grupo cíclico es un grupo cíclico, se tiene que W es un grupo cíclico.

4.2. Caso cuadrático

En esta sección se estudiará el caso particular de los cuerpos cuadráticos. Sea $K = \mathbb{Q}(\sqrt{d})$. Estudiar las unidades no es demasiado complicado dado que una condición suficiente y necesaria para que $u \in \mathcal{O}_K$ sea una unidad es que $N(u) = \pm 1$ dado que $|N(x)| = \|\langle x \rangle\| = \#(\mathcal{O}_K/\langle x \rangle) = 1$ si y sólo si x es una unidad.

Proposición 4.2.1. *Si $d < 0$, entonces:*

1. *Si d=-1, entonces $U(\mathcal{O}_K) = \{1, -1, i, -i\}$*
2. *Si d=-3, entonces $U(\mathcal{O}_K) = \{1, -1, (1+\sqrt{-3})/2, (1-\sqrt{-3})/2, (-1+\sqrt{-3})/2, (-1-\sqrt{-3})/2\}$*
3. *En ontro caso $U(\mathcal{O}_K) = \{1, -1\}$*

Además, todas las unidades son raices de la unidad.

Demostración. Lo primero es notar que como $d \leq 0$ si $x = a + b\sqrt{d} \in K$ con $a, b \in \mathbb{Q}$ entonces $N(x) = a^2 - db^2 = 0$ si y sólo si $a = b = 0$.

Si $d \equiv 2(\text{mod } 4)$ o $d \equiv 3(\text{mod } 4)$, entonces, dado $u \in \mathcal{O}_K$ se tiene que $\exists a, b \in \mathbb{Z}$ tales que $u = a + b\sqrt{d}$. El conjugado es $\bar{u} = a - b\sqrt{d}$. Por tanto, $N(u) = u\bar{u} = a^2 - db^2$ y u es una unidad si y sólo si $a^2 - db^2 = 1$. Si $b = 0$, entonces $a = \pm 1$. Si $b \neq 0$, entonces $1 = a^2 - db^2 > a^2$. Por tanto, $a = 0$ y entonces, se tiene que si d=-1 entonces $b = \pm 1$ y en otro valor de d no hay solución.

Si $d \equiv 1(\text{mod } 4)$ se tiene que si $u \in \mathcal{O}_K$, entonces, $\exists a, b \in \mathbb{Z}$ con la misma paridad tales que $u = (a + b\sqrt{d})/2$. El conjugado de u es $\bar{u} = (a - b\sqrt{d})/2$. Como $N(u) = u\bar{u}$ se tiene que u es unidad si y sólo si $a^2 - db^2 = 4$. Si $a = \pm 1$ entonces hay que resolver $-db^2 = 3$. Si d=-3 entonces, tiene solución para $b = \pm 1$. En otro caso no hay solución. Si a=0, hay que resolver $db^2 = 4$. Esto no tiene solución puesto que $d \equiv 1(\text{mod } 4)$. □

El caso con $d > 0$ se demostrará a la misma vez que el teorema de Dirichlet. Se tendrá que $U \cong W \times C$ con C un grupo cíclico infinito. La forma de encontrar un generador de C y de W se explica en [RIB, capítulo 10]. En concreto se tiene que $W = \{1, -1\}$

4.3. Teorema de Dirichlet

Ahora, el ojetivo, ya se centrará completamente en encontrar la estructura de las unidades. Ya sabemos cómo es W. Antes de nada, hay que introducir algunos conceptos.

Lo primero es notar que como $K/\mathbb{Q}$ es una extensión separable finita, por el teorema de Artin debe existir un $t \in \mathbb{C}$ tal que $K = \mathbb{Q}(t)$. Si [K:Q]=n entonces, t tiene n conjugados. Sean estos $t^{(1)}, ..., t^{(n)}$, entonces, se dirá que los conjugados de K son $K^{(i)}$=$\mathbb{Q}(t^{(i)})$ para i=1,...,n . Se dirá que $K^{(i)}$ es un conjugado real si $t^{(i)}$ es real y si no se dirá que es un conjugado complejo. Hay que notar que si $K^{(i)}$ es un conjugado complejo , entonces existe un $i' \neq i$ tal que $K^{(i)} = K^{(i')}$. Por tanto, el número de conjugados complejos es par. Además, si hay r_1 conjugados reales y $2r_2$ conjugados complejos, entonces, $r_1 + 2r_2 = n$.

Se seguirá la notación en la que $K^{(1)}, ..., K^{(r_1)}$ son los conjugados reales, $\overline{K^{(r_1+1)}}, ..., K^{(n)}$ y además, $K^{(r_1+r_2+j)}$ es el conjugado de $K^{(r_1+j)}$ y se podrá denotar $\overline{K^{(r_1+j)}}$ para todo $j = 1, ..., r_2$. Si $x \in K$, entoces,$\overline{x^{(r_1+j)}} = x^{(r_1+r_2+j)}$ para $j = 1, ..., r_2$.

A partir de ahora se definirá la siguiente aplicación que da una interpretación geométrica a las unidades. $\lambda\colon U \to \mathbb{R}^r$ siendo $r_1 + r_2 - 1$ se define como $\lambda(u) = (\log \left|u^{(1)}\right|, ..., \log \left|u^{(r)}\right|)$

Lo primero es ver dónde manda esta aplicación a los elementos de W que son de los que tenemos más información ahora mismo.

Proposición 4.3.1. *Sea $u \in U$. Entonces, $u \in W$ si y sólo si $\lambda(u) = (0, ..., 0)$.*

Demostración. Si $u \in W$ está claro.

Si $\lambda(u) = (0, ..., 0)$, entonces, $\left|x^{(i)}\right| = 0 \quad \forall i = 1...r$. Se nota que $\left|x^{(r_1+j)}\right| = \left|x^{(r_1+r_2+j}\right| \quad \forall j = 1, ..., r_2$. Por tanto, $\left|x^{(r_1+r_2+j)}\right| = 0 \quad \forall j = 1, ..., r_2 - 1$.

Finalmente, como u es una unidad, $|N(u)| = 1$. Tomando logaritmo, eso queda como $\sum_{i=1}^{n} \log \left|x^{(i)}\right| = 2 \log x^{(r_1+r_2)} = 0$. Por tanto, $\left|x^{(i)}\right| \quad \forall i = 1, ..., n$. Así que u es una unidad. □

Se introducirá el siguiente lema que se usará luego.

Lema 4.3.2. *Sean $u_1, ..., u_k \in U$ tales que $\lambda(u_1), ..., \lambda(u_k)$. Sea $G = \{(a_1, ..., a_k) \mid \exists v \in U$ tal que $\lambda(v) = a_1\lambda(u_1) + ... + a_k\lambda(u_k)\}$. Entonces $\mathbb{Z}^k \subseteq G$ y además $G/\mathbb{Z}^k$ es un grupo finito.*

Demostración. [RIB, lema 5, capítulo 10] □

Si queremos conocer cómo son las unidades de un anillos de enteros habría que ver cómo son los sistemas generadores de U y además, sería interesante comprobar si existe un sistema generador que genere unidades de forma única.

Definición 4.3.3. *Dado un conjunto de unidades $u_1, ..., u_k$, se dice que es un* ***sistema independiente de unidades*** *si no existen $m_1, ..., m_k \in \mathbb{Z}$ no todos nulos tal que $u_1^{m_1}...u_k^{m_k} = 1$.*

Hay que notar que en estos sistemas no hay raices de la unidad.

Lema 4.3.4. *Sean $u_1, ..., u_k$ unidades de $\mathcal{O}_K$. Son equivalentes:*

1. *$u_1, ..., u_k$ son un sistema independiente de unidades*
2. *$\lambda(u_1), ..., \lambda(u_k)$ son linealmente independientes sobre $\mathbb{Q}$*
3. *$\lambda(u_1), ..., \lambda(u_k)$ son linealmente independientes sobre $\mathbb{R}$*

Demostración. $1 \implies 2$ Suponiendo que $\lambda(u_1), ..., \lambda(u_k)$ son linealmente independientes sobre $\mathbb{Q}$. Entonces, existen $t_1, ..., t_k \in \mathbb{Q}$ no todos nulos tal que $t_1\lambda(u_1) + ... + t_k\lambda(u_k) = 0$. Eliminando denominadores, se puede encontrar $m_1, ..., m_k \in \mathbb{Z}$ no todos nulos tal que $m_1\lambda(u_1) + ... + m_k\lambda(u_k) = 0$. Entonces, $\lambda(\prod_{i=1}^k u_i^{m_i}) = 0$. Eso implica que $\prod_{i=1}^k u_i^{m_i}$ es una raiz de la unidad y eso implica que existe un $h \in \mathbb{N}$ tal que $\prod_{i=1}^k u_i^{hm_i}$. Así que $u_1, ..., u_k$ no es un sistema independiente de unidades.

$2 \implies 3$ Sean $\lambda(u_1), ..., \lambda(u_k)$ linealmente independientes sobre $\mathbb{Q}$, por reducción al absurdo se supone que no son linealmente independientes sobre $\mathbb{R}$. Además, sin pérdida de generalidad se puede suponer que $\lambda(u_1), ..., \lambda(u_{k-1})$ son linealmente independientes sobre r porque se puede elegir el mínimo k tal que la implicación no se cumple y $k > 1$. Sin péridida de generalidad existen $a_1, ..., a_{k-1} \in \mathbb{R}$ tales que $\lambda(u_k) = a_1\lambda(u_1) + ... + a_{k-1}\lambda(u_{k-1})$. Por el lema 4.3.2 se tiene que como $\lambda(u_1), ..., \lambda(u_{k-1})$ son linealmente independientes, entonces con la notación del lema $G/\mathbb{Z}^k$ es finito. Por tano, existe un h tal que $a_i h \in \mathbb{Z}$ para todo $i = 1, ..., k-1$. Por tanto $a_i \in \mathbb{Q}$ para todo $i = 1, ..., k-1$ contradiciendo que $\lambda(u_1), ..., \lambda(u_k)$ son linealmente independientes sobre $\mathbb{Q}$.

$3 \implies 1$ Si $u_1, ..., u_k$ no es un sistema independiente, existen $m_1, ..., m_k \in \mathbb{Z}$ no todos nulos tal que $u_1^{m_1}...u_k^{m_k} = 1$. La implicación sales de tomar logaritmos. □

El teorema más importante, que es el que da la existencia de un sistema de generadores como el que buscábamos es el siguiente:

Teorema 4.3.5. *(Teorema de Dirichlet) Dado un cuerpo de números algebraicos K. Entonces se tiene que:*

$$U(\mathcal{O}_K) \cong W \times C_1 \times ... \times C_r.$$

Siendo W el grupo de las unidades, cada C_i un grupo cíclico infinito y $r = r_1 + r_2 - 1$

Demostración. Si r=0, entonces, $r_1 + r_2 = 1$. Eso es posible si o bien $r_1 = 1$, en cuyo caso $[K : \mathbb{Q}] = 1$ y por tanto $K = \mathbb{Q}$ y $\mathcal{O}_K = \mathbb{Z}$ donde $U = \{\pm 1\}$ o bien $r_2 = 1$, teniendose que $[K : \mathbb{Q}] = 2$. Por tanto $K = \mathbb{Q}(\sqrt{d})$ con $d < 0$. Este caso se ha comprobado en la proposición 4.2.1.

Para el resto de casos la prueba de este teorema se basará en los siguientes lemas:

Lema 4.3.6. *Existe $k \leq r$ tal que $U(\mathcal{O}_K) \cong W \times C_1 \times ... \times C_k$*

Demostración. Por el lema 4.3.4. si $u_1, ..., u_k$ es un sistema independiente de unidades, entonces se tiene que $\lambda(u_1), ..., \lambda(u_k) \in \mathbb{R}^r$ son $\mathbb{R}$-linealmente independientes. Por tanto $k \leq r$.

Sea $G = \{(a_1, ..., a_k) \in \mathbb{R} \mid \exists v \in U \text{tal que} \lambda(v) = \sum_{i=1}^{k} a_i \lambda(u_i)\}$. Entonces, G es un grupo con la suma y $\mathbb{Z}^k \subseteq G$ dado que dado $a_1, ..., a_k \in \mathbb{Z}$ se tiene que $u_1^{a_1}...u_k^{a_k}$ es una unidad. Por el lema 4.3.2 $G/\mathbb{Z}^k$ es un grupo finito con h elementos.

Dado $u \in U$ con $u \neq u_i$ para $i = 1, ..., k$, como $u_1, ..., u_k$ es un sistema independiente maximal de unidades se tiene que $u, u_1, ..., u_k$ no es un sistema independiente y por tanto, $\lambda(u), \lambda(u_1), ..., \lambda(u_k)$ son linealmente dependientes sobre $\mathbb{Q}$, Por tanto, existen $a, a_1, ..., a_k \in \mathbb{Q}$ no todos nulos tales que $a\lambda(u) = a_1\lambda(u_1) + ... + a_k\lambda(u_k)$. En concreto $a \neq 0$ dado que $\lambda(u_1), ..., \lambda(u_k)$ son linealmente independientes. Por tanto, sin pérdida de generalidad, se puede suponer que $a = 1$.

Como $(a_1, ..., a_k) \in G$, por el teorema de Lagrange $(ha_1, ..., ha_k)$ es un representante del 0 en $G/\mathbb{Z}^k$. Por tanto, $(ha_1, ..., ha_k) \in \mathbb{Z}^k$. Ahora bien, se tiene $\lambda(u^h) = h\lambda(u) = ha_1\lambda(u_1) + ... + ha_k\lambda(u_k) = \lambda(u_1^{ha_1}...u_k^{ha_k})$. Es decir, $\lambda(u^{-h}u_1^{ha_1}...u_k^{ha_k}) = 0$. Por el lema 4.3.1 ocurre que existe $z \in W$ tal que $u = zu_1^{ha_1}...u_k^{ha_k}$.

Sea z_1 una raiz de $x^h - z$ y sea t_i una raiz de $x^h - u_i$ para cada i=1,...,k y sea $w = \#W$. Se tiene que $u^h = (z_1 \prod_{i=1}^{k} t_i^{ha_i})^h$. Por tanto, existe z_2 tal que $z_2^h = 1$ y $u = z_2 z_1 \prod_{i=1}^{k} t_i^{ha_i}$. Como $z_2^h = 1$ y $z_1^{hw} = 1$, en concreto se tiene $(z_2 z_1)^{hw} = 1$.

Sea z_3 una raiz hw-ésima primitiva de la unidad. Sea U' el grupo generado por $z_3, t_1, ..., t_k$ y W' el subgrupo de unidades se tiene entonces, que $U \subseteq U'$. Si $z \in W$, como z es una raiz w-ésima de la unidad, entonces es una potencia de Z_3 por tanto, está en W'. Por tanto $W \subseteq W' \cap U$. Si $z \in W' \cap U$, por estar en W' es una raiz de la unidad y está en U. Por tanto $z \in W$. Así que $W' \cap U \subseteq W$ teniendo finalmente $W' \cap U = W$. Por tanto, $U/W = U/(W' \cap U) \subseteq U'/W'$. Como U'/W' es un grupo libre de rango k, entonces, U/W es un grupo libre de rango como mucho k. Como $u_1, ..., u_k$ son unidades independientes, entonces es un grupo libre de rango k.

□

Ahora, falta probar que hay un sistema independiente de r unidades. Para ello, se introduce el siguiente lema

Lema 4.3.7. *Si $r >= 0$ $c_1, ..., c_r \in \mathbb{R}$ no son todos nulos, existe $u \in U$ tal que $\sum_{i=0}^{r} c_i \log \left|u^{(i)}\right| \neq 0$*

Demostración. [RIB, teorema 1 capítulo 10] □

Lo que se necesita es encontrar un sistema independiente de r unidades. Eso es equivalente a encontrar $u_1, ..., u_r \in U$ tales que $\lambda(u_1), ..., \lambda(u_r)$ son linealmente independientes sobre $\mathbb{Q}$. Esto es equivalente a que:

$$\begin{vmatrix} \log\left|u_1^{(1)}\right| & \log\left|u_1^{(2)}\right| & ... & \log\left|u_1^{(r)}\right| \\ \log\left|u_2^{(1)}\right| & \log\left|u_2^{(2)}\right| & ... & \log\left|u_2^{(r)}\right| \\ \vdots & \vdots & \ddots & \\ \log\left|u_r^{(1)}\right| & \log\left|u_r^{(2)}\right| & ... & \log\left|u_r^{(r)}\right| \end{vmatrix} \neq 0$$

Se demostrará por inducción en k que para todo $1 \leq k \leq r$ existen k unidades tales que un determinante de ese tipo (sustituyendo r por k)

Si $k = 1$, se elige $c_1 = 1$ y $c_i = 0 \ \forall \ i = 2, ..., r$. Entonces, existe u_1 tal que $\log\left|u_1^{(1)}\right| \neq= 0$. Si para k es cierto, si $k + 1 > r$ entonces, el enunciado es trivialmente cierto. Si $k + 1 \leq r$, entonces, existen k unidades $u_1, ..., u_k$ tales que:

$$\begin{vmatrix} \log\left|u_1^{(1)}\right| & \log\left|u_1^{(2)}\right| & ... & \log\left|u_1^{(k)}\right| \\ \log\left|u_2^{(1)}\right| & \log\left|u_2^{(2)}\right| & ... & \log\left|u_2^{(k)}\right| \\ \vdots & \vdots & \ddots & \\ \log\left|u_k^{(1)}\right| & \log\left|u_k^{(2)}\right| & ... & \log\left|u_k^{(k)}\right| \end{vmatrix} \neq 0$$

Si se elige $c_i = \det((-1)^i A_i)$ donde A_i es la matriz que surge de eliminar la columna i a la matriz

$$A = \begin{pmatrix} \log\left|u_1^{(1)}\right| & \log\left|u_1^{(2)}\right| & ... & \log\left|u_1^{(k+1)}\right| \\ \log\left|u_2^{(1)}\right| & \log\left|u_2^{(2)}\right| & ... & \log\left|u_2^{(k+1)}\right| \\ \vdots & \vdots & \ddots & \\ \log\left|u_k^{(1)}\right| & \log\left|u_k^{(2)}\right| & ... & \log\left|u_k^{(k+1)}\right| \end{pmatrix}.$$

Entonces $c_1 \neq 0$ y se tiene por el lema anterior que $\begin{vmatrix} \log\left|u_1^{(1)}\right| & \log\left|u_1^{(2)}\right| & ... & \log\left|u_1^{(k+1)}\right| \\ \log\left|u_2^{(1)}\right| & \log\left|u_2^{(2)}\right| & ... & \log\left|u_2^{(k+1)}\right| \\ \vdots & \vdots & \ddots & \\ \log\left|u_{k+1}^{(1)}\right| & \log\left|u_{k+1}^{(2)}\right| & ... & \log\left|u_{k+1}^{(k+1)}\right| \end{vmatrix} =$

$(-1)^{k+1} \sum_{i=0}^{k+1} c_i \log\left|u_{k+1}^{(i)}\right| \neq 0$

Como se cumple para k=r se tiene lo que buscábamos.

□

Por tanto, existe una raiz de la unidad ζ y r unidades $u_1, ..., u_r$ tal que cada unidad u se puede escribir de fomra unica como $u = \zeta^{e_0} u_1^{e_1} ... u_r^{e_r}$ donde $0 \leq e_0 < w$ siendo w el orden de ζ y $e_1, ..., e_r \in \mathbb{Z}$.

Definición 4.3.8. *A cualquier conjunto de r unidades $u_1, ..., u_r$ tal que cumple lo anterior, se llama* ***sistema fundamental de unidades****.*

Si $u_1, ..., u_r$ y $v_1, ..., v_r$ son dos sistemas fundamentales de unidades entonces se puede escribir cada v_i en función de los u_j de forma única como $v_i = \zeta^{b_i} u_1^{a_{1i}} ... u_r^{a_{ri}}$. De la misma forma se puede hacer al contrario y tener $u_i = \zeta^{b'_i} v_1^{a'_{1i}} ... v_r^{a'_{ri}}$. Como $u_1, ..., u_r$ y $v_1, ..., v_r$ son conjuntos independientes de unidades, entonces $\lambda(u_1), ..., \lambda(u_r)$ y $\lambda(v_1), ..., \lambda(v_r)$ son linealmente independientso sobre $\mathbb{Q}$. Además generan el mismo espacio vectorial, y la matrices de cambio de base son (a_{ij}) y $(a_{ij})'$, que deben

ser inversas. Por tanto, $det(a_{ij})det(a'_{ij}) = 1$. Teniendo que $|det(a_{ij})|\left|det(a'_{ij})\right| = 1$. Y como $a_{i,j} \in \mathbb{Z}$ se tiene que $|det(a_{ij})| = \left|det(a'_{ij})\right| = 1$. Como además $\log\left|v_j^{(i)}\right| = \sum_{h=1}^{r} a_{hj} \log\left|u_h^{(i)}\right|$. Esto se puede ver de forma matricial como $(\log\left|v_j^{(i)}\right|) = (a_{ij})(\log\left|u_j^{(i)}\right|)$. Y tomando determiante se tiene que:

$$\left|det(\log\left|v_j^{(i)}\right|)\right| = \left|det(\log\left|u_j^{(i)}\right|)\right|$$

.

Entonces, podemos definir una invariante:

Definición 4.3.9. *Sea $u_1, ..., u_r$ un sistema fundamental de unidades de $\mathcal{O}_K$. Se define el **regulador** de $\mathcal{O}_K$ como:*

$R = \left|\det\left(\log\left|u_j^{(i)}\right|\right)\right|$

Como antes habíamos visto, el regulador está bien definido.

5

Expresiones asintóticas.

5.1. Expresiones asintóticas

Durante estos capítulos, hemos profundizado en nuestro conocimiento de los anillos de enteros y encontrado una visión geométrica de ellos. En este capítulo se relacionará el número de clases con las funciones zeta. Hasta ahora, sobre este número sabíamos que era finito y nada más. Antes de nada se darán unas definiciones y se recordarán algunos conceptos previos que se usarán para encontrar estas expresiones.

Definición 5.1.1. *Se define la aplicación* $v\colon \mathbb{R}_{\geq 1} \to \mathbb{N}$ *como*

$$v(m) = \#\{J \text{ ideal de } \mathcal{O}_K \mid \|J\| = m\}$$

Se recuerda que como se probó en el la proposición 4.1.1 $v(m)$ está bien definida.

Sean $C_1, ..., C_h$ las h clases de ideales de K, se demostró en el lema 2.2.10 para todo i=1,...,h existe un ideal $J \in C_i$ tal que $\|J\| < \sqrt{\delta}$. Además los ideales de I C_i cumplen que existen $a, b \in \mathcal{O}_K$ tal que $\langle a\rangle I = \langle b\rangle I$. Por tanto, $\|I\| = |N(a/b)|\|J\|$

Dado un $t \in \mathbb{R}_{>0}$, se define $\sigma(t; C_i) = \#\{I \in C_i \mid \|I\| \leq t\}$. Por la misma razón que v, σ siempre está bien definido (el conjunto siempre es finito).

Se considerará r_1 como el número de conjugados reales de K y $2r_2$ el número de conjugados complejos. Se denotará $r = r_1 + r_2 - 1$ y como siempre $[K : \mathbb{Q}] = n$. Se denotará $l_1 = ... = l_{r_1} = 1$ y $l_{r_1+1} = ... = l_{r_1+r_2} = 2$.

Se denotará $w = \#W$. y será $u_1, ..., u_r$ un sistema fundamental de unidades.

Sea $a_1, ..., a_n$ una base de K sobre $\mathbb{Q}$ que genera $\mathcal{O}_K$ como $\mathbb{Z}$-módulo. Sea $x \in K$, entonces, existen $b_1, ..., b_n \in \mathbb{Q}$ tal que $x = \sum_{i=1}^{n} b_1 a_i$.

Como el sistema de unidades es intependiente, se $x^{(1)}, ..., x^{(n)}$ no son 0, existen

números reales $\alpha_1, ..., \alpha_r$ únicos tal que:

$$\sum_{k=1}^{r} \alpha_k \log \left| u_k^{(i)} \right| = \log \left| x^{(i)} / \left| x^{(1)} \cdots x^{(n)} \right|^{1/n} \right|$$

$\alpha_1, ..., \alpha_r$ se llaman exponentes de $x^{(1)}, ..., x^{(n)}$ con respecto del sistema fundamental de unidades $u_1, ..., u_r$.

Si v es una unidad de $\mathcal{O}_K$ enntonces, se puede escribir $v = \zeta u_1^{m_1} ... u_r^{m_r}$. con los $m_i \in \mathbb{Z}$. En este caso los $m_1, ..., m_r$ son los exponentes de v.

Teorema 5.1.2. *Dada una clase de ideales C, se tiene:*

$$\lim_{t \to \infty} \sigma(t; C)/t = (2^{r_1+r_2} \pi^{r_2} R)/(w\sqrt{|\delta|})$$

Demostración. Sea C^{-1} la inversa de la clase C y sea $J \in C^{-1}$. Entonces, se tiene una correspondecia biunívoca entre: $\epsilon_t = \{I \in C \mid \|I\| \leq t\}$ y $\epsilon'_t = \{\langle x \rangle \mid 0 \neq \langle x \rangle \subseteq J, |N(x)| \leq t\|J\|\}$.

Efectivamente, la aplicación $\phi \colon \epsilon_t \to \epsilon'_t$ dada por $\phi(I) = IJ$ es inyectiva por ser K un dominio de Dedekind. Además está bien definida porque si $IJ = \langle x \rangle$, entonces, $N(x) = \|x\| = \|IJ\| = \|I\|\|J\| \leq t\|J\|$. Además si $\langle x \rangle \in \epsilon'_t$ como $\langle x \rangle \subseteq J$ entonces, existe I tal que $\langle x \rangle = IJ$. La aplicación $\psi \colon \epsilon_t \to \epsilon_t$ que envía $\langle x \rangle$ a ese I es inyectiva también por la factorización única. Por tanto, existe una biyección.

El primer problema para calcular $\#\epsilon'_t$ viene porque cada ideal principal puede generarse por distintos elementos, normalmente infinitos. Dado que $\langle x \rangle = \langle y \rangle$ si y sólo si existe una unidad v tal que $x = vy$. Se intentará asociar a cada ideal un número finito de elementos. La idea será coger de cada ideal un generador y los que se obtienen de él multiplicándolo por una raiz de la unidad.

¿Cómo se hace esto? Se coge un sistema independiente de r unidades $\{u_1, ..., u_r\}$ Se considera $\#\epsilon''_t = \{x \mid \langle x \rangle \in \epsilon'_t$ y si $a_1, ..., a_r$ son los exponentes respecto de$\{u_1, ..., u_r\}$ se tiene que $0 \leq a_i < 1 \ \forall i = 1..., r\}$.

¿Se ha conseguido el objetivo? Si $x, y \in \epsilon''_t$ y $\langle x \rangle = \langle y \rangle$. Entonces, existe una unidad u tal que $x = uy$. Si $a_1, ..., a_r$ son los exponentes de x, $b_1, ..., b_r$ los de y y $m_1, ..., m_r$ los de u. Entonces, para cada $i = 1, ..., r$ se tiene que $0 \leq a_i = b_i + m_i < 1$. Como $0 \leq b_i < 1$ y m_i es entero, entonces $m_i = 0$ para todo $i = 1, ..., r$. Si $x \in \epsilon''_t$ y z es una unidad, entonces $\langle x \rangle = \langle zx \rangle$ y además, como los exponentes de z son todos 0, tienen los mismos exponentes y por tanto, $zx \in \epsilon''_t$. Finalmente, se probará que si $\langle x \rangle \in \epsilon'_t$ entonces, existe un $y \in \epsilon'_t$ que genera $\langle x \rangle$. Si los exponentes de x son $a_1, ..., a_r$, entonces, $u_1^{-\lfloor a_1 \rfloor} ... u_r^{-\lfloor a_r \rfloor} x$ debe estar en ϵ''_t dado que los exponentes son $0 \leq a_i - \lfloor a_i \rfloor < 1$ y además genera $\langle x \rangle \in \epsilon''_t$. Por todo esto se tiene que $\#\epsilon''_t = w\#\epsilon'_t$.

Ahora, hay que buscar una forma de contar el número de elmentos de ϵ''_t. Para ello, se harán corresponder sus elementos con puntos de $\mathbb{R}^n$ y el número de elementos se aproximará.

Sea $\{a_1, ..., a_n\}$ una base de J como $\mathbb{Z}$-módulo. Dada una n-upla $(b_1, ..., b_n) \in \mathbb{R}^n$ se le asocia $x^{(i)} = \sum_{j=1}^{n} b_j a_j^{(i)}$ para cada i=1,...,n.

Se define E_t como el conjunto de n-uplas $(b_1, ..., b_n)$ tales que:

1. $0 < \prod_{j=1}^{n} x^{(j)} \leq \|J\| \cdot t$

2. Los exponentes $\alpha_1, ..., \alpha_r$ cumplen $0 \leq \alpha_k < 1$ para cada $k = 1...n$

E_t es un conjunto acotado. Si $(b_1, ..., b_n) \in E_t$, entonces:
$\left|x^{(i)}\right| = \left|x_{(1)} \cdots x_{(n)}\right|^{1/n} exp(\sum_{k=1}^{r} \alpha_k log\left|u_k^{(i)}\right|) \leq \left|x_{(1)} \cdots x_{(n)}\right|^{1/n} exp(rM) \leq$
$|\|J\| \cdot t|^{1/n} exp(rM)$

Donde $M = \text{máx}\{\log\left|u_k^{(j)}\right| \mid k = 1, \ldots, n; k = 1, \ldots, r\}$.

Si se considera $\theta\colon \mathbb{R}^n \to \mathbb{R}^n$ la el homomorfismo que envía $(b_1, \ldots, b_n)$ en $(x^{(1)}, \ldots, x^{(n)})$, entonces, como $\{a_1, \ldots, a_n\}$ es un conjunto linealmente independiente, se tiene que $\left|det(a_k^{(j)})\right| = |\Delta(a_1, ..., a_n| \neq 0$ y por tanto, θ es invertible. Por esto, como $\theta(E_t)$ está acotado, se tiene que E_t está acotado.

Para conseguir un conjunto cerrado, se considera el conjunto $E'_t = \{(b_1, ..., b_n) \mid \exists i \in \{1 \ldots n\}$ tal que $x^{(i)} = \sum_{k=1}^{n} b_k a_k^{(i)} = 0$ y $\forall j \in \{1 \ldots n\}\ x^{(j)} \leq |\|J\| \cdot t|^{1/n} \exp(rM)\}$ y entonces se usará el conjunto $D_t = E_t \cup E'_t$. Entonces, D_t es cerrado y acotado.

Los elementos de ϵ''_t están en biyección con los puntos no nulos D_t con coordenadas enteras dado que si $x = \sum_{k=1}^{n} m_k a_k \in \epsilon''_t$ entonces, $m_1, \ldots, m_n \in \mathbb{Z}$ por estar x en J. Entonces, se considera la correspondencia $x \to (m_1, ..., m_n)$ es biyectiva. Como $a_1, ..., a_n$ es una base de J como $\mathbb{Z}$-módulo se tiene la inyectividad. Y si $(m_1, ..., m_n) \in D_t$, como $m_1, ..., m_n \in \mathbb{Z}$ entonces $(m_1, ..., m_n) \in E_t$. Por las condiciones 1 y 2 de E_t, $x = \sum_{j=1}^{n} m_j a_j \in \epsilon''_t$.

Por tanto, el número de coordenadas enteras de D_t, que se denotará como $\#D_t$ es $1 + \epsilon''_t$.

Entonces, por lo que tenemos ahora:

$\lim_{t\to\infty} w\sigma(t; C)/t = \lim_{t\to\infty}[1+w\sigma(t; C)]/t = \lim_{t\to\infty}[1+\epsilon t'']/t = \lim_{t\to\infty} \#D_t/t$.

Se probará que $\lim_{t\to\infty} \#D_t/t = \text{vol}(D_1)$.. Para cada $t > 0$ se considera la aplicación lineal definida por $\theta_t(b_1, ..., b_n) = (b_1/\sqrt[n]{t}, ..., b_n/\sqrt[n]{t}$. Entonces, $D_1 = \theta_t(D_t)$. Además, cada hipercubo H con centro en $(m_1, ..., m_n)$ lo manda a un hipercubo de lado $1/\sqrt[n]{t}$, es decir, volumen $1/t$ y centro $\theta_t(m_1, ..., m_n)$. Entonces $1 + \#(\epsilon''_t$ es el número de hipercubos descritos anteriormente con centro en D_1 y lado $1/t$. Por tanto $(1/t)(1 + \#(\epsilon''_t))$ es una aproximación para el volumen de D_1. Por tanto:

$vol(D_1) = \lim_{t\to 1} 1/t\#(D_t)$

Se calculará entonces $\text{vol}(D_1) = \int_{D_1} \mathrm{d}b_1 \ldots \mathrm{d}b_n$. Para ello, se harán cambios de variables.

Primero se usarán las variables $\zeta_1 \dots \zeta_n$ dadas por el cambio:

$$\begin{cases} \sum_{k=1}^{n} b_k a_k^{(j)} = \zeta_j \text{ para } j = 1 \dots r_1 \\ \sum_{k=1}^{n} b_k a_k^{(j)} = \zeta_j + i\zeta_{j+r_2} \text{ para } j = r_1 + 1 \dots r_1 + r_2 \end{cases}$$

Por tanto:
$\zeta_j = \sum_{k=1}^{n} b_k a_k^{(j)} para j = 1 \dots r_1$
$\zeta_j = \sum_{k=1}^{n} b_k((a_k^{(j)} + a_k^{(j+r_2)})/2)$ para $j = r_1 + 1 \dots r_1 + r_2$
$\zeta_{j+r_2} = \sum_{k=1}^{n} b_k((a_k^{(j)} - a_k^{(j+r_2)})/2)$ para $j = r_1 + 1 \dots r_1 + r_2$.

El valor absoluto del Jacobiano es: $\left|\det\left(\frac{\mathrm{d}\zeta_i}{\mathrm{d}b_j}\right)\right| = 2^{-r_2}\left|\det\left(a_i^{(j)}\right)\right| = 2^{-r_2}\|J\|\sqrt{|\delta|}$

Entonces, por el teorema de cambio de variables:

$\int_{D_1} \mathrm{d}b_1 \dots \mathrm{d}b_n = \int_{D_1'} \left|\det\left(\frac{\mathrm{d}b_i}{\mathrm{d}\zeta_j}\right)\right| \mathrm{d}\zeta_1 \dots \mathrm{d}\zeta_n = \int_{D_1'} 2^{r_2}/(\|I\|\sqrt{|\delta|}\mathrm{d}\zeta_1 \dots \mathrm{d}\zeta_n$

Donde D_1' es el conjunto obtenido de D_1 por el cambio de variables.

Ahora, se cambia a polares.

$$\begin{cases} \zeta_j = \rho_j \text{ para } j = 1 \dots r_1 \\ \zeta_j = \rho_j \cos\phi_j \text{ para } j = r_1 + 1 \dots r_1 + r_2 \\ \zeta_{j+r_2} = \rho_j \sin\phi_j \end{cases}$$

El Jacobiano es el determinante de la matriz

$$\left[\begin{array}{c|c} I_{r_1} & 0 \\ \hline 0 & M \end{array}\right]$$

Donde

$$M = \begin{pmatrix} \cos\phi_{r_1+1} & 0 & 0 & \dots & -\rho_{r_1+1}\sin\phi_{r_1+1} & 0 & 0 & \dots \\ 0 & \cos\phi_{r_1+2} & 0 & \dots & 0 & -\rho_{r_1+2}\sin\phi_{r_1+2} & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \sin\phi_{r_1+1} & 0 & 0 & \dots & \rho_{r_1+1}\cos\phi_{r_1+1} & 0 & 0 & \dots \\ 0 & \sin\phi_{r_1+2} & 0 & \dots & 0 & \rho_{r_1+2}\cos\phi_{r_1+2} & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}.$$

E I_{r_1} es la matriz identidad de orden r_1. El valor absoluto del determinante es $\rho_{r_1+1} \cdots \rho_{r_1+r_2}$

Después de este cambio, D_1' se combierte en el conjunto D_1'' dado por:

$$\begin{cases} 0 < \prod_{j=1}^{r_1+r_2} |\rho_j|^{l_j} \leq \|J\| \\ \log|\rho_j| = 1/n \log \prod_{k=1}^{r_1+r_2} |\rho_k|^{l_k} + \sum_{k=1}^{r} \alpha_k \log u_k^{(j)} \text{ con } 0 \leq \alpha_k < 1 \end{cases}$$

Por tanto:

$\mathrm{vol}(D_1) = 2^{r_2}/(\|J\| \cdot \sqrt{|\delta|}) \int_{D_1'} \rho_{r_1+1} \cdot \rho r_1 + r_2 \mathrm{d}\rho_1 \cdots \mathrm{d}\rho_{r_1+r_2} \mathrm{d}\phi_{r_1+1} \cdots \mathrm{d}\phi_{r_1+r_2} =$
$2^{r_2}/(\|J\| \cdot \sqrt{|\delta|}) \int_{D_1''} \mathrm{d}\rho_1 \cdots \mathrm{d}\rho_{r_1+r_2} \mathrm{d}\phi_{r_1+1} \cdots \mathrm{d}\phi_{r_1+r_2} = 2^{r_2}\pi^{r_2}/(\|J\| \cdot \sqrt{|\delta|}) \int_{D_1''} \mathrm{d}\rho_1 \cdots \mathrm{d}\rho_{r_1+r_2}$

Se considera D_1''' a la parte del dominio de integración donde $\rho_1 > 0, \ldots, \rho_{r_1} > 0$. Entonces:

$\int_{D_1''} \mathrm{d}\rho_1 \cdots \mathrm{d}\rho_{r_1+r_2} \mathrm{d}\phi_{r_1+1} \cdots \mathrm{d}\phi_{r_1+r_2} = 2^{r_1} \int_{D_1'''} \mathrm{d}\rho_1 \cdots \mathrm{d}\rho_{r_1+r_2}$.

Se define el cambio de variable $\tau_j = \rho_j^{l_j}$ para $j = 1, ..., r_1 + r_2$ con $l_1 = ... = l_{r_1}$ y $l_{r_1+1} = ... = l_{r_1+r_2}$. El valor absoluto del Jacobiano es $2^{-r_2}\rho_{r_1+1}^{-1} \cdots \rho_{r_1+r_2}^{-1}$. Además, el conjunto D_1''' se convierte en el conjunto D_1^{iv} de los puntos $(\tau_1, ..., \tau_{r_1+r_2}, \phi_{r_1+1}, ..., \phi_{r_1+r_2}$ con $\tau_j > 0$ para $j = 1, ..., r_1 + r_2$, $0 \leq \phi_j < 2\pi$ para $j = r_1 + 1, ..., r_1 + r_2$, $\tau_1 \cdots \tau_{r_1+r_2} \leq \|J\|$ y $\log(\tau_j) = l_j/n \log(\tau_1 \cdots \tau_{r_1+r_2}) + l_j \sum_{k=1}^{r} \alpha_k \log\left(\left|u_k^{(j)}\right|\right)$.

Por tanto:

$\mathrm{vol}(D_1) = 2^{r_1+r_2}\pi^{r_2}/(\|J\| \cdot \sqrt{|\delta|}) \int_{D_1^{iv}} \mathrm{d}\tau_1 \cdots \mathrm{d}\tau_{r_1+r_2}$

Se considera ahora el conjunto de variables $\alpha_1, ..., \alpha_r, \omega = \tau_1 \cdots \tau_{r_1+r_2}, \phi_{r_1+1}, ..., \phi_{r_1+r_2}$. Así se tiene:

$\log \tau_j = l_j/n \log(\omega) + l_j \sum_{k=1}^{r} \alpha_k \log\left(\left|u_k^{(j)}\right|\right)$

Por tanto:

$1/\tau_j \cdot \mathrm{d}\tau_j/\mathrm{d}\alpha_k = l_j \log\left(\left|u_k^{(j)}\right|\right)$ y $1/\tau_j \cdot \mathrm{d}\tau_j/\mathrm{d}\omega = l_j/n \cdot 1/\omega$.

Así que la matriz del jacobiano es:

$$\frac{\mathrm{d}(\tau_1, ..., \tau_{r_1+r_2}, \phi_{r_1+1}, ..., \phi_{r_1+r_2})}{\mathrm{d}(\alpha_1, ..., \alpha_r, \phi_{r_1+1}, ..., \phi_{r_1+r_2})} = \frac{\tau_1 \cdots \tau_{r_1+r_2}}{\omega} \left(\begin{array}{c|c} M & 0 \\ \hline 0 & I \end{array}\right).$$

Donde

$$M = \begin{pmatrix} l_1 \log\left(\left|u_1^{(1)}\right|\right) & \cdots & l_1 \log\left(\left|u_r^{(1)}\right|\right) & l_1/n \\ l_2 \log\left(\left|u_1^{(2)}\right|\right) & \cdots & l_2 \log\left(\left|u_r^{(2)}\right|\right) & l_2/n \\ \cdots & \cdots & \cdots & \cdots \\ l_{r_1+r_2} \log\left(\left|u_1^{(r_1+r_2)}\right|\right) & \cdots & l_{r_1+r_2} \log\left(\left|u_r^{(r_1+r_2)}\right|\right) & l_{r_1+r_2}/n \end{pmatrix}.$$

Como se tiene que $1 = |N(u_l)| = \prod_{j=1}^{r_1+r_2} \left|u_k^{(j)}\right|^{l_j}$, entonces $\sum_{j=1}^{r_1+r_2} l_j \log\left(\left|u_k^{(j)}\right|\right) = 0$. Además $n = \sum_{j=1}^{r_1+r_2} l_j$. Por tanto, el valor absoluto del determinante es igual al regulador. Por tanto:

$\mathrm{vol}(D_1) = 2^{r_1+r_2}\pi^{r_2}R/(\|J\| \cdot \sqrt{|\delta|}) \int_0^{\|J\|} \mathrm{d}\omega \int_0^1 \int_0^1 \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_r$

Por tanto, finalmente se tiene

$\lim_{t\to\infty} \sigma(t; C)/t = (2^{r_1+r_2}\pi^{r_2}R)/(w\sqrt{|\delta|})$

[RIB, A, cap 23.1] □

Corolario 5.1.3. $\lim_{t\to\infty} \sigma(t)/t = h \cdot (2^{r_1+r_2}\pi^{r_2}R)/(w\sqrt{|\delta|})$

Se ha encontrado por fin, una expresión asintótica en la que aparece h multiplicando. Si se consigue calcular el límite, r_1, r_2, R, w y δ, entonces ya se tiene el número de clases. Lo que realmente es complicado de calcular en la mayoría de los casos es el límite.

Lo primero que se nota es que $\sigma(t) = \sum_{m=1}^{\lfloor t \rfloor} v(m)$. Se considera $\delta > 0$ y $s > 1+\delta$, entonces, $\forall n \in \mathbb{N}$, se tiene que $|\sum_{i=1}^{n} v(i)/i^s| =$
$|v(1) + \sum_{i=2}^{n}(\sigma(i) - \sigma(i-1))/i^s| =$
$\left|v(1) + \sigma(n)/n^s - \sigma(1) + \sum_{i=2}^{n-1}(\sigma(i)(1/i^s - 1/(i-1)^s)\right| \leq |v(1)||\sigma(n)/n^s| + |\sigma(1)| +$
$\left|\sum_{i=2}^{n-1}(\sigma(i)(1/i^s - 1/(i-1)^s)\right|$

Se tiene que $|v(1)|$ está acotado, $|\sigma(n)/n^s|$ está acotado puesto que converge cuando n tiende a ∞, $|\sigma(1)|$ también está acotado, así que para ver que $|\sum_{i=1}^{n} v(i)/i^s|$ converge uniformemente para $s \in (1+\delta, \infty)$ $\forall \delta > 0$ hay que comprobar que $\left|\sum_{i=2}^{n-1}(\sigma(i-1)(1/i^s - 1/(i-1)^s))\right|$ está acotado.

Primero se tiene que como $\sigma(n)/n$ converge, entonces existe un $a > 0$ tal que $|\sigma(n)/n| \leq a$ $\forall n \in \mathbb{N}$. A partir de este dato, $\left|\sum_{i=2}^{n-1}(\sigma(i)(1/i^s - 1/(i-1)^s))\right| \leq$
$\sum_{i=2}^{n-1} |(\sigma(i)||(1/i^s - 1/(i-1)^s))| \leq \sum_{i=2}^{n-1} |i|a|(1/i^s - 1/(i-1)^s))| \leq$
$\sum_{i=2}^{n-1} a|(1/i^{s-1} - 1/(i-1)^{s-1}))| \leq \sum_{i=2}^{n-1} \left|\int_{i-1}^{i} -(s-1)(1/t^s)dt\right| \leq$
$\sum_{i=2}^{n-1} \int_{i-1}^{i} |-(s-1)(1/t^s)|dt = \sum_{i=2}^{n-1} \int_{i-1}^{i} (s-1)(1/t^s)dt = \int_{1}^{n-1} (s-1)(1/t^s)dt \leq$
$\int_{1}^{\infty} (s-1)(1/t^s)dt \leq \infty$ dado que $s > 0$.

Entonces, $\sum_{i=1}^{n} v(i)/i^s$ converge uniformemente en $(1+\delta, \infty)$ $\forall \delta > 0$. Se llamará $\zeta_K(s) = \sum_{i=1}^{n} v(i)/i^s$ esta es la función zeta de Dedekind. Se puede notar que $\zeta_{\mathbb{Q}} = \zeta$ (la de Riemman). Para lo que la necesitamos, sólo será necesario que esté definida en $\mathbb{R} > 1$. Por tanto, sólo nos preocuparemos de la serie de Dirichlet.

El siguiente resultado nos dará la relación que tiene con la expresión asintótica anterior.

Proposición 5.1.4. *Dada na sucesión de números reales* $\{a_i\}_{i\in\mathbb{N}}$. *Sea* $S(m) = a_1 + ... + a_m$. *Si* $\lim_{m\to\infty} S(m)/m = c$, *entonces, la serie de dirichlet* $\sum_{n=1}^{\infty} a_n/n^s$ *converge para* $s > 1$ *y además* $\lim_{s\to 1}(s-1)(\sum_{n=1}^{\infty} a_n/n^s) = c$.

Demostración. [RIB, E cap 22] □

Aplicando el resultado para el caso de $a_i = v(i)$ se tiene :

Proposición 5.1.5. $\lim_{s\to 1}(s-1)\zeta_K(s) = h \cdot (2^{r_1+r_2}\pi^{r_2}R)/(w\sqrt{|\delta|})$.

Entonces, ya tenemos una expresión que relaciona la función ζ con el número de clases. Lo que nos interesa finalmente, es encontrar una expresión de la función como producto de Euler.

Se definirá el conjunto $\mathcal{P}$ como el conjunto de ideales primos de $\mathcal{O}_K$ y se definirá $\mathcal{J}$ como el conjunto de ideales no nulos en $\mathcal{O}_K$. Se tiene la última proposición.

Proposición 5.1.6. *Con $\mathcal{P}$ y $\mathcal{J}$ definidos como anteriormente, se tiene que $\prod_{P\in\mathcal{P}}(1-1/\|P\|^s)^{-1}$ converge absolutamente para $s>1$ y se tiene que $\prod_{P\in\mathcal{P}}(1-1/\|P\|^s)^{-1}=\sum_{I\in\mathcal{J}}1/\|I\|^s$*

Demostración. [RIB, D cap 23.2] □

Finalmente, como consecuencia de todo esto, se tiene el siguiente teorema que da h.

Teorema 5.1.7. $h=\frac{w\sqrt{|\delta|}}{2^{r_1+r_2}\pi^{r_2}R}\lim_{s\to1}(s-1)\prod_{P\in\mathcal{P}}(1-1/\|P\|^s)^{-1}$.

Bibliografía

[HW] G.H. Hardy, E.M Wright. *An Introduction to the Theory of Numbers.* Oxford University Press.

[AM] M.F. Atiyah, I.G. MacDonald. *Introduction to Commutative Algebra.* Ed. Reverté.

[IR] Ireland, K., Rosen. *A Classical Introduction to Modern Number Theory.* Springer-Verlag, New York, 1990 (second edition).

[DL] Dino Lorezini *An invitation to Arithmetic Geometry.* American Mathematical Society.

[RIB] Paulo Ribenboim. *Classical Theory of Algebraic Numbers* Springer.

[ByS] Z.I. Borevich, I. R. Shafarevich. *Number Theory* Academic Press Inc.