



Universidad Autónoma del Estado de Hidalgo
Instituto de Ciencias Básicas e Ingeniería
Área Académica de Matemáticas y Física

Bases enteras y número de clase en extensiones radicales

Tesis que para obtener el grado de

Maestra en Matemáticas

presenta

Betzabé Topete Galván

bajo la dirección de

Dr. Fernando Barrera Mora

PACHUCA, HIDALGO, NOVIEMBRE DE 2018.



UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO
 Instituto de Ciencias Básicas e Ingeniería
School of Engineering and Applied Sciences

Mineral de la Reforma, Hgo., a 26 de octubre de 2018

Número de control: ICBI-D/840/2018

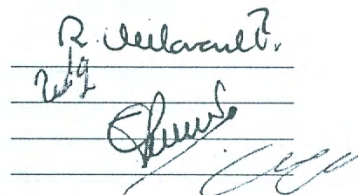
Asunto: Autorización de impresión de tesis.

MTRO. JULIO CÉSAR LEINES MEDECÍGO
DIRECTOR DE ADMINISTRACIÓN ESCOLAR

Por este conducto le comunico que el comité revisor asignado a la C. Betzabé Topete Galván, alumna de la Maestría en Matemáticas con número de cuenta 202441, autoriza la impresión del proyecto de tesis titulado "Bases enteras y número de clase en extensiones radicales" en virtud de que se han efectuado las revisiones y correcciones pertinentes.

A continuación se registran las firmas de conformidad de los integrantes del comité revisor.

- PRESIDENTE Dr. Rafael Villarroel Flores
- SECRETARIO Dr. Víctor Cuauhtémoc García Hernández
- VOCAL Dr. Fernando Barrera Mora
- SUPLENTE Dr. Rubén Alejandro Martínez Avendaño



Sin otro particular reitero a Usted la seguridad de mi atenta consideración.

Atentamente
 "Amor, Orden y Progreso"



Dr. Óscar Rodolfo Suárez Castillo
 Director del ICBI



ORSC/POJM

Ciudad del Conocimiento
 Carretera Pachuca-Tulancingo km 4.5 Colonia
 Carboneras, Mineral de la Reforma, Hidalgo,
 México. C.P. 42164
 Teléfono: +52 (771) 71 720 00 ext. 2231
 Fax 2109
 direccion.icbi@uaeh.edu.mx



A mi mamá, hermanos y Lalo.

Agradecimientos

Agradezco primeramente a mi mamá, hermanos y a Eduardo, ya que gracias a ellos este camino fue más diferenciable, pues me apoyaron primordialmente con su tiempo, para que yo pudiera terminar este trabajo. Le doy gracias a mi abuela materna por preocuparse de mí y ayudarme hasta el día de hoy. Quiero agradecer mucho a mi asesor, el Dr. Fernando Barrera Mora, por seguir enseñándome matemáticas y lecciones de vida. También, quiero agradecer especialmente a mi amiga Annel Ayala Velasco, por dedicarle tiempo a este trabajo y hacer observaciones importantes para que éste fuera mejor. Agradezco a cada uno de los profesores de la Maestría en Matemáticas por haberme compartido sus conocimientos. Por último, quiero agradecer a mis sinodales, los doctores Rafael Villarroel Flores y Víctor C. García Hernández, por las observaciones realizadas que ayudaron a mejorar este trabajo.

Resumen

Conocer la estructura y las propiedades de objetos matemáticos, en muchas ocasiones, resulta complicado. Quizá porque no se han desarrollado suficientes herramientas o tal vez por la propia naturaleza de los objetos. En este trabajo buscamos comprender un poco más a los enteros algebraicos, en especial a aquellos que provienen de extensiones que son radicales, esto a través de su estructura como \mathbb{Z} -módulo, donde tiene lugar el concepto de base entera, y el hecho de que el Teorema Fundamental de la Aritmética se puede extender a los enteros algebraicos, dando paso a los conceptos de grupo y número de clase.

El tiempo fue limitado, por lo que únicamente obtuvimos algunos resultados sobre bases enteras, más concretamente, mejoramos un resultado que denominamos “método de mínimos enteros”. También introducimos los conceptos de parejas semi-pares y semi-impares, los cuales nos permitirán construir una base entera para campos de la forma $\mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_m]{a_m})$, bajo ciertas hipótesis sobre los a_i y n_i . Asimismo, damos condiciones suficientes para que el campo $\mathbb{Q}(\sqrt[n]{a})$ sea monogénico, considerando algunas restricciones sobre a y n . Finalmente, aplicamos los resultados que obtuvimos para mostrar algunos ejemplos.

Knowing the structure and properties of mathematical objects, in some cases, is complicated. Perhaps, it is due to the little developed of tools, or maybe it is due to the very nature of the mathematical objects. In this work we try to comprehend a little more of the structure of algebraic integers, especially those that arise from radical extensions, this is done by using its structure as \mathbb{Z} -module. Here, the concept of integral basis appears, as well as the fact that the Fundamental Theorem of Arithmetic can be extended to the group of fractional ideals, given rise to the concepts of class group and class number.

For time pressure, we only obtained some results concerning integral bases, more specifically, we improved a result that we call “the method of minimal integers”. We also introduce the concepts of semi-even and semi-odd couples, which will allow us to construct an integral base for fields of the form $\mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_m]{a_m})$, under certain assumptions related to the a_i and n_i . Likewise, we give sufficient conditions so that the field $\mathbb{Q}(\sqrt[n]{a})$ be monogenic, considering some restrictions on a and n . Finally, we apply the obtained results to present some examples.

Índice general

Resumen	I
Agradecimientos	III
Introducción	4
1. Preliminares, notación y terminología	5
1.1. Notación	6
1.2. Anillos	7
1.3. Módulos	9
1.4. Campos	10
1.5. Localización	12
1.6. Normas y trazas	15
2. Campos numéricos	18
2.1. Dependencia entera	18
2.2. Anillos Dedekind	22
2.3. Discriminante	36
2.4. Norma de ideales	39
2.5. Grupo de clase	41
3. Bases enteras	47
3.1. Mínimos enteros	48
3.2. Bases enteras de extensiones radicales	57
4. Ejemplos	63
4.1. Conclusiones	76
Bibliografía	77

Introducción

Recuerdo que mi asesor de tesis, desde el primer curso que tomé con él, constantemente nos decía a mí y a mis compañeros de clase la siguiente frase: “en matemáticas la diversión nunca termina”. Para mí esta frase tiene total sentido, ya que siempre existen caminos que nos invitan a buscar nuevos resultados, y uno de estos senderos resulta ser el de la generalización. Esta última fue la ruta que intentamos seguir para la elaboración del presente trabajo, por lo que considero que los dos tópicos que aquí abordamos tienen como motivación principal aquella frase que se quedó tan grabada en mi mente. Tanto la construcción de bases enteras, como la determinación del número de clase de un campo numérico, son dos temas estudiados desde hace tiempo, sin embargo aún no existen, en ambos casos, resultados generales para poder determinarlos. Una base para el anillo de enteros, visto como \mathbb{Z} -módulo, de un campo numérico es la definición de base entera, ésta fue propuesta por Dedekind [13], sin embargo, para que pudiera nacer este concepto el Último Teorema de Fermat jugó un rol decisivo, pues gracias a éste se desarrollaron nuevas herramientas que tenían como propósito ayudar en su demostración, y a lo largo de este camino se profundizó en el estudio de los enteros algebraicos; por ejemplo [13], para los casos donde en la ecuación de Fermat los exponentes son 3, 5 y 14, los enteros de $\mathbb{Q}(\zeta_3)$, usados por Euler, y los de $\mathbb{Q}(\sqrt{5})$ y $\mathbb{Q}(\sqrt{-7})$, usados por Dirichlet, sirvieron para la demostración de cada caso, y aunque no desarrollaron nuevas propiedades de los enteros algebraicos, sí hicieron uso de algunas de éstas.

Otra manera de ver la ecuación de Fermat es de la siguiente forma:

$$(x + y)(x + \zeta y) \cdots (x + \zeta^{n-1}y) = z^n, \quad (1)$$

donde ζ_n es una raíz n -ésima primitiva de la unidad, por lo que podemos considerar esta factorización en los enteros de $\mathbb{Q}(\zeta_n)$. Ahora bien, si los enteros de $\mathbb{Q}(\zeta_n)$ fueran de factorización única, se podría concluir que la Ecuación

1 no tiene solución, como lo hizo Lamé [16]. No obstante Kummer encontró que para el caso $n = 23$, la factorización única falla, lo que implica que hay un error en la demostración que Lamé propuso. Es aquí donde Kummer introduce el concepto de “números ideales” con el fin de obtener una nueva forma de factorización única y, así, poder demostrar el Último Teorema de Fermat para una gran cantidad de números primos.

El hecho de que se tenga o no factorización única está estrechamente relacionado con el concepto de número de clase, ya que, como discutiremos más adelante, el número de clase “mide” qué tan lejos está un anillo de enteros de ser de factorización única. Se sabe que el número de clase es finito, y este resultado, para el caso cuadrático, se le atribuye a Lagrange, mientras que el caso cúbico fue establecido por Eisenstein; además, Kummer lo probó para campos ciclotómicos, y el caso general se debe a Dedekind y Kronecker [13]. En este trabajo presentamos la demostración de Minkowski. Ahora bien, es sabido que en matemáticas son comunes los enunciados que garantizan la existencia de ciertos objetos matemáticos, mas en su demostración no encontramos un método para construirlos, y tal es el caso tanto de las bases enteras como del número de clase de un campo numérico; no obstante, contamos con resultados parciales para ambos casos: si la extensión es cuadrática o ciclotómica, el problema de encontrar una base entera está resuelto [10]; también, en [12] se propone una base entera para $K = \mathbb{Q}(\theta)$, donde θ es raíz del polinomio $x^3 - m$, con m entero libre de cubo. Notemos que los ejemplos anteriores son casos especiales de extensiones radicales. Centraremos la discusión en tales extensiones, ya que en el intento de abordar estos problemas, las extensiones radicales son, en principio, un poco más sencillas, pues éstas se obtienen de adjuntar a \mathbb{Q} raíces de polinomios irreducibles muy simples, a saber, los que son de la forma $x^n - a$, con a un entero libre de raíz n -ésima. Ejemplos de trabajos más recientes son [17], [6] y [8], donde proponen una base entera para $\mathbb{Q}(\sqrt{m}, \sqrt{n})$, $\mathbb{Q}(\sqrt[4]{m})$ y $\mathbb{Q}(\sqrt{c}, \sqrt{a + b\sqrt{c}})$, respectivamente. En este punto, cabe mencionar que hicimos un intento por generalizar las ideas que proponen en [17], es decir, quisimos aplicar la misma técnica con $\mathbb{Q}(\sqrt{m}, \sqrt{n}, \sqrt{l})$, pero, como sucedió en repetidas ocasiones a lo largo de este trabajo, los cálculos se complicaron y no pudimos concluir nada. Ahora bien, un ejemplo donde se discuten algunos casos de extensiones de grado 6 se encuentra en [7], donde se hace uso del concepto de índice de un elemento para determinar si un campo no es monogénico. Tocado ya el tema del índice de un elemento, es conveniente mencionar que en [1] encontramos un resultado

que será de suma importancia en este trabajo, ya que proponen una manera de construir una base entera a través de un conjunto de mínimos enteros (de los cuales daremos todos los detalles en la Sección 3.1), y cada elemento de este conjunto es de forma particular, pues sus denominadores están relacionados con el índice del elemento primitivo que estaremos considerando, y éste, a su vez, con el discriminante de tal elemento. Como veremos más adelante, inmediatamente nos damos cuenta que existe un problema, y es que las posibilidades que aparecen para cada mínimo entero pueden ser demasiadas, ya que esto depende del número de factores primos que aparecen en el discriminante del elemento que tomamos, y a pesar de que nos apoyamos de SageMath para realizar los cálculos, consideramos que este método, el cual llamamos “método de mínimos enteros”, no es muy óptimo; sin embargo, pudimos mejorarlo para aquellos campos que cuentan con subcampos propios, y la manera en que lo hicimos fue mediante el uso de un resultado que relaciona el discriminante de un campo intermedio con el del campo que estamos estudiando, de ahí que se pueden descartar varias posibilidades en la construcción de cada mínimo entero. En este trabajo mostramos algunas bases enteras de extensiones radicales de grado 4 y 6, aplicando el método de mínimos enteros “mejorado”. En [14] el autor expone una base entera para $\mathbb{Q}(\sqrt[n]{a})$, con $\text{mcd}(a, n) = 1$. Por falta de tiempo no nos fue posible revisarlo con detalle pues es un compendio de 5 artículos, sin embargo, creemos que es relevante mencionarlo ya que es un trabajo que está muy relacionado con el que presentamos aquí. Respecto a lo anterior, en [15, páginas 272 y 274] encontramos el caso particular cuando n es un primo impar, para el cual se dan condiciones necesarias y suficientes para decidir si el anillo de enteros del campo $\mathbb{Q}(\sqrt[n]{a})$ es $\mathbb{Z}[\sqrt[n]{a}]$, y en caso de no ser de esta manera, propone una base entera. Con este resultado nosotros hacemos dos cosas: la primera es dar algunas condiciones para que $\mathbb{Q}(\sqrt[n]{a})$, con n libre de cuadrado, $\text{mcd}(a, n) = 1$ y unas hipótesis extras sobre a , sea monogénico; la segunda es proponer bases enteras formadas a partir de las de algunos subcampos del campo que estamos tratando, aplicando también [13, Teorema 4.26]. Aquí introducimos los conceptos de parejas *semi-pares* y *semi-impares*, los cuales son de gran utilidad en el resultado que proponemos para $\mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_m]{a_m})$, ¡claro!... bajo algunas hipótesis sobre los a_i y n_i .

Comentemos brevemente la estructura de la tesis. En el Capítulo 1 introducimos notación, terminología y resultados básicos de anillos, módulos y campos para que este trabajo sea lo más autocontenido posible. En esta parte la bibliografía que más consideramos la encontramos en [3] y [9]. Dado

que los anillos con los que trabajamos son los anillos de enteros de campos numéricos y como éstos son dominios Dedekind, entonces en este tipo de anillos es posible establecer un resultado equivalente al Teorema Fundamental de la Aritmética por medio de los ideales, como lo hemos mencionado anteriormente. Por lo que de forma natural tuvimos la necesidad que discutir propiedades de estos anillos, pues estamos interesados en conocer cómo son sus elementos y su grupo de clase. Por tal motivo, en el Capítulo 2, nos enfocamos en mostrar algunos resultados de los anillos que son Dedekind. Además, incluimos los dos teoremas que mencionamos de [15] y [13] ya que éstos sirven de herramienta para poder establecer los Teoremas 3.2.1 y 3.2.2, que forman parte de las aportaciones de este trabajo.

Uno de nuestros objetivos era poder desarrollar ejemplos del grupo de clase en una extensión radical sobre los racionales, como lo hacemos con las bases enteras, sin embargo, una vez más por limitaciones de tiempo en el Capítulo 2 sólo incluimos resultados estándar sobre el grupo de clase y mostramos que éste es finito. Consideraremos este tema como posible trabajo para futuro, ya que si tuvimos algo de éxito con las bases enteras, confiamos en que con más tiempo también lo hubiéramos tenido con este tópico.

Pusimos especial atención al método de mínimos enteros, por lo que en el Capítulo 3 primero hacemos una discusión lo más detallada posible al respecto, ya que consideramos que la manera en que lo mejoramos es nuestro aporte principal y, en la segunda parte, incluimos todos los resultados que obtuvimos a partir de los teoremas que encontramos en [15] y [13].

En el Capítulo 4 incluimos aplicaciones de lo que desarrollamos en el Capítulo 3. Mostramos algunos ejemplos donde hacemos uso del método de mínimos enteros, en éstos es importante resaltar nuestra aportación, es decir, simplificamos el número de casos que en principio aparecen al determinar cada mínimo entero. Igualmente aplicamos los Teoremas 3.2.1 y 3.2.2 para proponer bases enteras. Además, en cada ejemplo, mostramos las bases que SageMath propone, encontramos una matriz de cambio de base y también pedimos a SageMath que calculara el número de clase.

CAPÍTULO 1

Preliminares, notación y terminología

La teoría de números es una de las ramas de la matemática que, por lo menos desde Diofanto, ha cautivado la atención de los más ilustres geómetras, hablando en términos no muy de moda para referirse a los profesionales de la matemática. A lo largo de la historia, la teoría de números ha jugado un rol importante en diversas áreas de la matemática y sus aplicaciones. Por mencionar solamente una, nos referiremos a la teoría de números algebraicos. El primer gran impulso de esta área tiene lugar desde los años 1840's, con las importantes contribuciones de Kummer, Dirichlet, Dedekind y Kronecker. Es precisamente con el trabajo de Kummer que se inicia una rama del álgebra, que tiene como eje el concepto de ideal, que para Kummer eran los “números ideales”, cuando pensaba subsanar el “defecto” que se tiene en los enteros ciclotómicos al no cumplirse el Teorema Fundamental de la Aritmética.

Los expertos dicen [16] que una de las consecuencias más importantes del Último Teorema de Fermat es la gran cantidad de áreas de la matemática que se desarrollan en el proceso de su demostración.

En este trabajo abordaremos algunos de los temas centrales de la teoría algebraica de números, particularmente centramos la discusión en dos conceptos importantes: bases enteras y número de clase. Ambos son definidos en el anillo de enteros de un campo numérico K , denotado por \mathcal{O}_K . El concepto de base entera se origina al mostrar que \mathcal{O}_K es un \mathbb{Z} -módulo libre de rango finito, mientras que el de número de clase es resultado de definir el grupo libre abeliano generado por los ideales de \mathcal{O}_K , llamado grupo de ideales fraccionarios, y considerar el cociente con los ideales fraccionarios principales, que da como resultado el grupo de clase de \mathcal{O}_K , el cual es finito. Es por eso que en este capítulo presentamos algunos resultados básicos de anillos, módulos

y campos. También agregamos la notación y terminología de los conceptos que se irán definiendo en cada capítulo, todo esto con el fin de que el trabajo sea lo más autocontenido posible.

Cabe mencionar que omitiremos las demostraciones de resultados que son estándar y aparecen en libros de texto a nivel licenciatura. Habrá excepciones a esta regla, si consideramos que los métodos de prueba ilustran ideas cercanas a lo que se discute en el trabajo.

1.1. Notación

En esta sección describimos la notación que representa términos, algunos propios de la teoría algebraica de números.

Como es usual, para denotar al anillo de los enteros racionales, al campo de los números racionales y al campo de los números complejos les denotaremos con \mathbb{Z} , \mathbb{Q} y \mathbb{C} , respectivamente. También aclaramos acá, porqué se usa el término “enteros racionales”, esto se debe a que los números enteros son el anillo de enteros, a definirse más adelante, en el campo de los números racionales.

Se usarán símbolos usuales de teoría de conjuntos para denotar pertenencia de un elemento a un conjunto y la inclusión de conjuntos.

Para denotar que a divide a b usamos la representación: $a|b$.

El máximo común divisor entre un par de enteros a y b lo denotamos por $\text{mcd}(a, b)$.

Dado un entero positivo n , se define la función de Euler $\phi(n)$, como la cardinalidad del conjunto $\{1 \leq a \leq n : \text{mcd}(a, n) = 1\}$.

Con $\binom{n}{k}$ nos referimos al coeficiente binomial.

Una raíz fija del polinomio $x^m - 1$, que genera a todas las demás, en el sentido de grupo cíclico, la denotaremos por ζ_m y se le llama *raíz primitiva de la unidad*.

Cuando haya una función inyectiva $f : A \rightarrow B$, esto se denotará por $A \hookrightarrow B$ y se dirá que A está insertado en B o que hay una inclusión de A en B .

Para nosotros en este trabajo, el término anillo significará que es un anillo conmutativo, con identidad. Si además no tiene divisores de cero, se le llama dominio entero.

Si R es un anillo, para denotar al grupo que tiene a R como conjunto soporte, escribiremos $(R, +)$.

Usaremos $I \leq R$ cuando nos refiramos a un ideal I de un anillo R .

Para denotar el ideal generado por un conjunto finito de elementos escribiremos $\langle a_1, \dots, a_n \rangle$ o $\langle a_1, \dots, a_n \rangle$ y, en caso de que se trate del ideal generado por un sólo elemento, usamos también Ra .

Si K y F son campos tales que $K \subseteq F$, diremos que F es una extensión de K y lo denotaremos F/K .

Si F/K es una extensión de campos, F adquiere estructura de K -espacio vectorial y a la dimensión de F como tal le llamaremos el grado de F/K , denotado $[F : K]$.

Por un campo numérico entenderemos una extensión finita de \mathbb{Q} .

Si R es un anillo, $R[x]$ denotará el anillo de los polinomios con coeficientes en R , en la indeterminada x . Si F/K es una extensión de campos y $\alpha \in F$, $K(\alpha)$ denota al mínimo subcampo de F que contiene a K y a α . Por R_S nos referimos al anillo localizado de R en S (Definición 1.5.2).

Para la extensión, F/K , con $T_{F/K}(\alpha)$ y $N_{F/K}(\alpha)$ denotamos las importantes funciones traza y norma, respectivamente, del elemento α (Definición 1.6.1). Tanto la norma como la norma absoluta de un ideal I la denotaremos por $\mathcal{N}(I)$.

Cuando $\{\alpha_1, \dots, \alpha_n\}$ es un subconjunto de un campo numérico de grado n sobre \mathbb{Q} , denotaremos por $\Delta(\alpha_1, \dots, \alpha_n)$ al discriminante de dicho subconjunto. En particular, para simplificar notación, pondremos $\Delta(1, \theta, \dots, \theta^{n-1}) := \Delta(\theta)$.

Al discriminante de un campo numérico lo denotaremos por δ_K .

Con Δ_F nos referimos al ideal discriminante.

Escribimos f.g. para abreviar el término: finitamente generado.

El símbolo \square indica el fin de una prueba.

1.2. Anillos

Discutimos brevemente los conceptos concernientes a ideal y anillo que utilizamos a lo largo de este trabajo.

Definición 1.2.1. *Por un dominio de ideales principales R , entenderemos un dominio entero en el cual todo ideal es principal, es decir, todo ideal I de R es de la forma $I = Ra$, para algún $a \in R$.*

Definición 1.2.2. *Sean R un anillo e I un ideal distinto de R . Se dice que:*

- *el ideal I es primo, si cuando $ab \in I$ implica que al menos uno de a o b pertenece a I ,*

- el ideal I es maximal, si para cualquier otro ideal J tal que $I \subseteq J$, se debe cumplir una de las condiciones, $I = J$ o $J = R$.

Definición 1.2.3. Si I y J son ideales de R , se define el ideal producto como: $IJ := \left\{ \sum_{i=1}^n a_i b_i \mid a_i \in I, b_i \in J, n \in \mathbb{N} \right\}$.

Teorema 1.2.1. [5, Teorema 1.2.8] Si R es un anillo e I es un ideal de R , entonces las siguientes condiciones son equivalentes.

- (i) El ideal I es primo.
- (ii) Si J_1 y J_2 son ideales tales que $J_1 J_2 \subseteq I$, entonces $J_1 \subseteq I$ o $J_2 \subseteq I$.
- (iii) El anillo $\frac{R}{I}$ es un dominio entero.

Demostración. Esta demostración la podemos encontrar en [4, Teorema 1.2.8]. \square

Si R es un anillo e I es un ideal de R , por definición, I es un subgrupo de $(R, +)$, entonces podemos hablar del grupo cociente $\frac{R}{I}$ ya que, por hipótesis, I es un subgrupo normal de R .

Ahora, si $a + I, b + I \in \frac{R}{I}$, se verifica que la multiplicación de $a + I$ y $b + I$, dada por $(a + I)(b + I) := ab + I$ está bien definida y que $\frac{R}{I}$ resulta ser un anillo con la multiplicación definida antes.

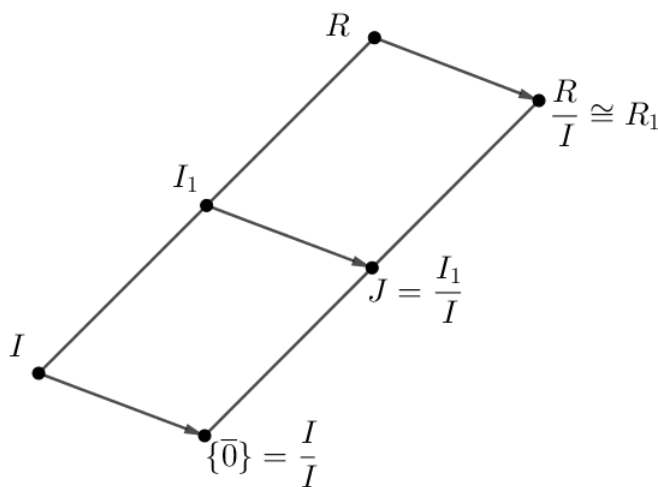
El siguiente resultado es de gran importancia por establecer una relación “natural” entre los ideales de R y los de $\frac{R}{I}$.

Teorema 1.2.2. (Teorema de la correspondencia [4, Teorema 1.2.2]) Sean R y R_1 anillos. Si $f : R \rightarrow R_1$ un epimorfismo con núcleo I , entonces R_1 es isomorfo a $\frac{R}{I}$. Además, hay una correspondencia biyectiva entre el conjunto de ideales de R_1 y el conjunto de ideales de R que contienen a I . Esta correspondencia puede obtenerse asociando a cada ideal $J \subseteq R_1$, el ideal $I_1 \subseteq R$ definido por $I_1 = f^{-1}(J)$. Con I_1 así definido, se tiene el isomorfismo:

$$\frac{R}{I_1} \cong \frac{R_1}{J}.$$

Demostración. El enunciado de este teorema puede ser encontrado en la referencia mencionada. \square

El siguiente diagrama ilustra la situación en el Teorema 1.2.2.



1.3. Módulos

El anillo de enteros de un campo numérico K , que definiremos más adelante, es un \mathbb{Z} -módulo libre de rango $[K : \mathbb{Q}]$. Por esta razón, en esta sección presentamos algunos resultados básicos de módulos.

Definición 1.3.1. *Sea R un anillo y M un R -módulo.*

1. *Un subconjunto S de M se dice linealmente independiente, si todo subconjunto finito de S es linealmente independiente. Cuando S también genera, es decir, cuando todo elemento de M es combinación lineal de elementos de S , se le llama una base. Si M admite una base, se dice que es libre.*
2. *Se dice que M es finitamente generado, si existe un subconjunto finito de M que lo genera.*

Teorema 1.3.1. [4, Teorema 3.1.2] *Sea R un anillo. Si M es un R -módulo libre, entonces las cardinalidades de cualesquiera dos bases son iguales.*

Demostración. La demostración de este teorema puede ser consultada en la referencia citada. \square

Definición 1.3.2. Si M es un R -módulo libre, se define su rango, denotado $\text{rank}(M)$, como la cardinalidad de una base de M .

Teorema 1.3.2. [4, Teorema 3.1.3] Sea R un anillo. Entonces R es un dominio de ideales principales si y sólo si todo submódulo E de un R -módulo libre M es libre y $\text{rank}(E) \leq \text{rank}(M)$.

Demostración. Esta demostración puede ser consultada en la referencia mencionada. \square

1.4. Campos

Presentamos algunas propiedades generales de extensiones de campos que utilizaremos más adelante.

Definición 1.4.1. Si K y F son campos tales que $K \subseteq F$, diremos que F es una extensión de K y lo denotaremos por F/K . A la dimensión de F como K -espacio vectorial le llamaremos el grado de F/K , denotado $[F : K]$. Cuando $[F : K] \in \mathbb{N}$, diremos que la extensión es finita.

Teorema 1.4.1. [4, Teorema 6.1.2] Sea F/K una extensión de campos, $\alpha \in F$ algebraico sobre K , entonces existe un único polinomio mónico e irreducible $m_\alpha(x)$ tal que $m_\alpha(\alpha) = 0$ y si $f(x)$ es otro polinomio que satisface $f(\alpha) = 0$, entonces $m_\alpha(x) | f(x)$.

Demostración. Como α es algebraico entonces es raíz de un polinomio $f(x) = a_n x^n + \dots + a_1 x + a_0$ con $a_n \neq 0$. También es raíz de $x^n + \dots + \frac{a_1}{a_n} x + \frac{a_0}{a_n}$, el cual se obtiene dividiendo por el coeficiente principal de $f(x)$. De todos los polinomios mónicos que tienen a α por raíz elegimos uno de menor grado, sea $m_\alpha(x)$ dicho polinomio.

El polinomio $m_\alpha(x)$ es único ya que si $g(x)$ es otro polinomio mónico del mismo grado que $m_\alpha(x)$ que tiene a α por raíz, entonces α es raíz de $(m_\alpha - g)(x)$, y como el término principal de m_α se cancela con el de g , el grado de $m_\alpha - g$ es menor que el de m_α ó g . Si $m_\alpha - g \neq 0$ entonces podemos dividir por el coeficiente principal y tendríamos que α es raíz de un polinomio mónico con grado menor y eso contradice la elección de $m_\alpha(x)$.

Ahora, supongamos que $m_\alpha(x)$ se puede factorizar como producto de dos polinomios de grado menor, es decir, $m_\alpha(x) = f(x)g(x)$. Como $m_\alpha(\alpha) = 0$ entonces $f(\alpha)g(\alpha) = 0$ de lo que tendríamos que α es raíz de f ó g lo cual contradeciría la elección de m_α como el polinomio de menor grado que tiene a α por raíz.

Finalmente, si $f(\alpha) = 0$, por el algoritmo de la división existen $q(x), r(x) \in K[x]$ tales que $f(x) = m_\alpha(x)q(x) + r(x)$, donde $r(x)$ es el polinomio cero o su grado es menor que el grado de $m_\alpha(x)$. Evaluando a $f(x)$ en α tenemos:

$$f(\alpha) = m_\alpha(\alpha)q(\alpha) + r(\alpha),$$

como $f(\alpha) = m_\alpha(\alpha) = 0$, entonces $r(\alpha) = 0$. Si $r(x)$ no es el polinomio cero, lo podemos hacer mónico y α , por lo anterior, será raíz de $r(x)$, es decir, hemos encontrado un polinomio mónico de grado menor que el de $m_\alpha(x)$ que tiene a α por raíz lo cual contradice la elección de $m_\alpha(x)$. Por lo que $r(x)$ debe ser el polinomio cero y $f(x) = m_\alpha(x)q(x)$. \square

Teorema 1.4.2. [4, Teorema 6.1.3] *Si L/F y F/K son extensiones finitas, entonces $[L : K] = [L : F][F : K]$.*

Demostración. Esta demostración se encuentra en la referencia citada. \square

Corolario 1.4.1. *Si L/K es una extensión finita de campos y $K \subseteq F \subseteq L$, con F campo, entonces $[F : K][L : K]$.*

Demostración. Se sigue directamente del Teorema 1.4.2. \square

Definición 1.4.2. *Sean $F/K, L/K$ y M/K extensiones de campos tales que $L, M \subseteq F$. Definimos el campo compuesto de L y M por:*

$$LM := \left\{ \sum_{finita} \alpha_i \beta_i : \alpha_i \in L, \beta_i \in M \right\}.$$

Teorema 1.4.3. [4, Teorema 6.1.5] *Sean F/K y L/K extensiones finitas. Entonces $[LF : K] \leq [F : K][L : K]$, con igualdad si $\text{mcd}([F : K], [L : K]) = 1$.*

Demostración. La demostración se encuentra en la referencia citada. \square

Definición 1.4.3. *Si F/K es una extensión de campos y $\alpha \in F$, diremos que α es algebraico sobre K si existe un polinomio $f(x) \in K[x] \setminus \{0\}$ tal que $f(\alpha) = 0$. La extensión F/K se dice algebraica si todo $\alpha \in F$ es algebraico.*

Definición 1.4.4. Sea F/K una extensión de campos, $\alpha \in F$ algebraico sobre K . Diremos que α es separable sobre K , si el polinomio irreducible de α sobre K tiene raíces simples. Si F/K es algebraica y todo elemento de F es separable sobre K , se dice que F/K es una extensión separable.

Definición 1.4.5. Dada una extensión F/K , se dice que F contiene un elemento primitivo, si existe $\alpha \in F$ tal que $F = K(\alpha)$.

Teorema 1.4.4. (Teorema del elemento primitivo [4, Teorema 7.1.2]) Si F/K es finita y separable, entonces $F = K(\alpha)$ para algún $\alpha \in F$.

Demostración. Este enunciado lo podemos encontrar en la referencia mencionada. \square

Definición 1.4.6. Una extensión F/K se llama normal si satisface que para todo polinomio irreducible $f(x) \in K[x]$ que tiene una raíz en F , implica que F contiene todas las raíces de $f(x)$.

Teorema 1.4.5. [4, Corolario 8.1.1] Si F/K es una extensión finita, entonces existe una única extensión normal mínima N_F/K tal que $K \subseteq F \subseteq N_F$ y $[N_F : K] < \infty$.

Demostración. La demostración de este teorema la podemos encontrar en la referencia citada. \square

Definición 1.4.7. Al campo N_F del Teorema 1.4.5 se le llama la cerradura normal de F/K .

Teorema 1.4.6. [4, Teorema 8.1.5] Sean, F/K una extensión finita y separable de grado n y N/K una extensión normal tal que $F \subseteq N$. Entonces hay exactamente n K -isomorfismos $\sigma_i : F \rightarrow N$, donde $i = 1, \dots, n$.

Demostración. La demostración puede ser consultada en la referencia dada. \square

1.5. Localización

En esta sección presentamos algunos resultados sobre localización con el fin de mostrar propiedades que utilizaremos en anillos Dedekind, además veremos que la localización es la generalización de construir el campo de cocientes de un dominio entero.

Definición 1.5.1. Sea R un anillo y $S \subseteq R$. Se dice que S es multiplicativamente cerrado, si $1 \in S$ y para todos $a, b \in S$ se tiene que $ab \in S$.

Si R es un dominio entero y $S = R \setminus \{0\}$, entonces S es multiplicativamente cerrado. Esto es consecuencia inmediata de la definición de un dominio entero. Sean R un anillo y $S \subseteq R$ multiplicativamente cerrado. Se define en $R \times S$ la relación: $(r, s) \sim (r_1, s_1)$ si existe $t \in S$ tal que $t(rs_1 - sr_1) = 0$.

Proposición 1.5.1. [3, pág. 5] Si R es un anillo, entonces la relación anterior, $(r, s) \sim (r_1, s_1)$ es de equivalencia.

Demostración. Esta demostración se encuentra en la referencia citada. \square

Notación: Al conjunto de clases de equivalencia en la Proposición 1.5.1 lo denotaremos por R_S y la clase de (r, s) será representada por $[(r, s)] := \frac{r}{s}$.

Teorema 1.5.1. [9, Proposición 1.1] El conjunto R_S es un anillo con las operaciones

$$\frac{a}{s} + \frac{b}{t} := \frac{at + sb}{st} \quad y \quad \frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}.$$

Más aún, si $0 \notin S$, entonces todo elemento en S tiene inverso multiplicativo en R_S .

Demostración. La demostración la podemos encontrar en la referencia dada. \square

Observación 1.5.1. [3, Observación 1] Si $0 \in S$, entonces R_S es un anillo con un solo elemento.

Definición 1.5.2. Si $S \subseteq R$ es multiplicativamente cerrado, el anillo R_S es llamado el anillo localizado de R en S .

Las siguientes dos proposiciones son estándar en la teoría algebraica de números.

Proposición 1.5.2. Si R es un dominio entero y $S = R \setminus \{0\}$, entonces $R_S = K$ es campo, el cual es llamado campo de cocientes de R .

Demostración. Se verifica sin dificultad que R_S es anillo conmutativo con identidad. Vamos a mostrar que para todo $a \in R_S \setminus \{0\}$, existe $x \in R_S$ tal

que $ax = 1$. Como $a \in R_S$, entonces $a = \frac{b}{c}$, con $b \in R \setminus \{0\}$ y $c \in S$. De esto, si $x = \frac{c}{b}$ tenemos que $ax = 1$, como se quería. \square

El campo de cocientes de R es único y es el campo más pequeño que contiene a R en el siguiente sentido; si F es un campo que contiene una copia isomorfa de R , entonces también contiene una copia isomorfa de R_S .

Proposición 1.5.3. *Sean R un anillo, \mathfrak{p} un ideal de R y $S = R \setminus \mathfrak{p}$, entonces S es multiplicativamente cerrado si y sólo si \mathfrak{p} es primo.*

Demostración. Supongamos que S es multiplicativamente cerrado y sea $ab \in \mathfrak{p}$. Mostraremos que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$. Argumentemos por contradicción, es decir, supongamos que a y b no pertenecen a \mathfrak{p} , entonces a y b son elementos de S , y como S es multiplicativamente cerrado $ab \in S$. Por la hipótesis sobre ab , esto es imposible. Así, \mathfrak{p} es primo.

Recíprocamente, supongamos ahora que \mathfrak{p} es primo y sean $a, b \in S$. Vamos a mostrar que $ab \in S$. Si $ab \notin S$, entonces $ab \in \mathfrak{p}$, y como \mathfrak{p} es primo, entonces $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$, lo cual es imposible. Por lo que S es multiplicativamente cerrado. \square

Teorema 1.5.2. [3, Teorema 3] *Si R un dominio entero y $S \subseteq R$ multiplicativamente cerrado, entonces existe una biyección entre los ideales primos de R tales que su intersección con S es vacía y los ideales primos de R_S . La correspondencia está dada por $\mathfrak{p} \rightarrow \mathfrak{p}R_S = \left\{ \frac{a}{b} : a \in \mathfrak{p}, b \in S \right\}$.*

Demostración. Observemos primero que, como R es un dominio entero, entonces $R \hookrightarrow R_S$ por medio de la función $x \mapsto \frac{x}{1}$.

Si $\mathfrak{P} \subseteq R_S$ es un ideal primo, entonces $\mathfrak{p} = \mathfrak{P} \cap R$ es ideal primo en R . Mostremos que $\mathfrak{P} = \mathfrak{p}R_S$. Por definición de \mathfrak{p} , tenemos $\mathfrak{p}R_S \subseteq \mathfrak{P}$, por lo que resta mostrar la inclusión recíproca. Para esto, sea $\frac{x}{t} \in \mathfrak{P}$, entonces

$t \left(\frac{x}{t} \right) = x \in \mathfrak{P} \cap R = \mathfrak{p}$, por ende, $\frac{x}{t} \in \mathfrak{p}R_S$. Más aún, hemos probado que todo ideal de R_S es de la forma IR_S , con I ideal de R .

Ahora, dado \mathfrak{P} ideal primo en R_S tenemos $\mathfrak{P} \cap S = \emptyset$, ya que los elementos de S son unidades en R_S y \mathfrak{P} es ideal primo. De lo anterior obtenemos que $\mathfrak{p} \cap S = (\mathfrak{P} \cap R) \cap S = \emptyset$.

Dado un ideal primo \mathfrak{p} en R tal que $\mathfrak{p} \cap S = \emptyset$, vamos a probar que $\mathfrak{p}R_S$ es primo. Para esto, sean $\frac{a}{t}, \frac{b}{t_1} \in R_S$ tales que $\frac{a}{t} \cdot \frac{b}{t_1} \in \mathfrak{p}R_S$, entonces $\frac{ab}{tt_1} = \frac{x}{s}$ con $x \in \mathfrak{p}$ y $s \in S \setminus \mathfrak{p}$. De la igualdad anterior tenemos que existe $t_2 \in S \setminus \mathfrak{p}$ tal que $t_2(abs - xtt_1) = 0 \in \mathfrak{p}$ y, como $t_2 \notin \mathfrak{p}$, entonces $abs - xtt_1 \in \mathfrak{p}$. Ahora, dado que $x \in \mathfrak{p}$, el elemento xtt_1 pertenece a \mathfrak{p} y por lo cual $abs \in \mathfrak{p}$. Como $s \notin \mathfrak{p}$ obtenemos que $ab \in \mathfrak{p}$, lo que implica las siguientes posibilidades: $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$. Luego $\frac{a}{t}$ o $\frac{b}{t_1}$ pertenecen a $\mathfrak{p}R_S$.

Por último, nos resta probar que $\mathfrak{p} = \mathfrak{p}R_S \cap R$. Por definición de $\mathfrak{p}R_S$, tenemos que $\mathfrak{p} \subseteq \mathfrak{p}R_S \cap R$. Sea $x \in \mathfrak{p}R_S \cap R$, entonces $x = \frac{a}{t}$ con $a \in \mathfrak{p}$, luego $tx = a \in \mathfrak{p}$ y, como $t \notin \mathfrak{p}$, concluimos que $x \in \mathfrak{p}$. \square

Observación 1.5.2. [3, Observación 3] *Los ideales primos en R_S , con $S = R \setminus \mathfrak{p}$, provienen de ideales contenidos en \mathfrak{p} .*

Observación 1.5.3. [3, Observación 4] *Si R es un anillo, \mathfrak{p} es un ideal primo de R y $S = R \setminus \mathfrak{p}$, entonces la localización de R en S se denotará por $R_{\mathfrak{p}}$. Este anillo tiene un único ideal maximal: $\mathfrak{p}R_{\mathfrak{p}}$, es decir, $R_{\mathfrak{p}}$ es un anillo local.*

1.6. Normas y trazas

Si L/K es una extensión finita, podemos definir dos funciones que juegan un rol muy importante desde el punto de vista aritmético, éstas son la norma y la traza. Ambas son homomorfismos, una de la parte multiplicativa y la otra de la aditiva y entre sus aplicaciones encontramos que, mediante la traza, se puede definir el discriminante de un campo numérico. Por otra parte, con la norma es posible definir la norma de un ideal y utilizar este concepto para mostrar que el número de clase de un campo numérico es finito, como se discutirá más adelante.

Definición 1.6.1. *Sea L/K una extensión finita. Dado $\alpha \in L$, α define una transformación K -lineal dada por $r_{\alpha}(\beta) = \alpha\beta$, con $\beta \in L$. Se definen la norma y la traza de α por*

$$T_{L/K}(\alpha) = \text{traza}(r_{\alpha}), \quad N_{L/K}(\alpha) = \det(r_{\alpha}).$$

Teorema 1.6.1. [3, Teorema 25] *Sea L/K una extensión finita de campos. Entonces*

- (i) $T_{L/K}$ es K -lineal.
- (ii) Para todos $\alpha, \beta \in L$, $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$.
- (iii) Si $\alpha \in K$ y $n = [L : K]$, entonces $N_{L/K}(\alpha) = \alpha^n$.
- (iv) Sea E un subcampo de L que contiene a K . Entonces $T_{L/K}(\alpha) = T_{E/K}(T_{L/E}(\alpha))$.

Demostración. La demostración se encuentra en la referencia citada. \square

Proposición 1.6.1. [10, Proposición 3.14] Sean L/K una extensión finita, $\alpha \in L$ algebraico con polinomio mínimo $m(x) \in K[x]$ y r_α como antes. Entonces el polinomio característico de r_α es $m(x)$.

Demostración. Sean $m(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$ el polinomio mínimo de α y $\{1, \alpha, \dots, \alpha^{m-1}\}$ base de $K(\alpha)/K$. Como $\alpha^m = -a_{m-1}\alpha^{m-1} - \cdots - a_1\alpha + a_0$, entonces

$$\begin{aligned} r_\alpha(b_0 + b_1\alpha + \cdots + b_{m-1}\alpha^{m-1}) &= b_0\alpha + b_1\alpha^2 + \cdots + b_{m-1}\alpha^m \\ &= b_0\alpha + b_1\alpha^2 + \cdots + b_{m-1}(-a_{m-1}\alpha^{m-1} - \\ &\quad \cdots - a_1\alpha - a_0) \\ &= -a_0b_{m-1} + (b_0 - b_{m-1}a_1)\alpha + \\ &\quad \cdots + (b_{m-2} - b_{m-1}a_{m-1})\alpha^{m-1}. \end{aligned}$$

Luego, la matriz asociada a r_α , de acuerdo a la base dada, es

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{m-1} \end{pmatrix}.$$

Se verifica que esta matriz tiene a $m(x)$ como polinomio característico y mínimo. \square

De la discusión anterior hemos encontrado algo más, es decir, que $T_{L/K}(\alpha) = -a_{m-1}$ y $N_{L/K}(\alpha) = (-1)^m a_0$.

Teorema 1.6.2. [10, Proposición 3.16] Sea L/K una extensión finita y separable de grado n . Sean $\sigma_1, \dots, \sigma_n$ las diferentes inmersiones de L en una cerradura normal de L/K . Entonces

$$(i) \quad T_{L/K}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha).$$

$$(ii) \quad N_{L/K}(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha).$$

Demostración. Sea $m(x) \in K[x]$ el polinomio mínimo de α . Supongamos que $m(x) = (x - \alpha)(x - \alpha_2) \cdots (x - \alpha_d)$, donde para cada $i = 2, 3, \dots, d$, α_i se encuentra en la cerradura de Galois de L/K . Entonces tenemos que $[K(\alpha) : K] = d$. Sea $\{\beta_1, \dots, \beta_r\}$ una base de L sobre $K(\alpha)$, donde $r = [L : K(\alpha)] = \frac{n}{d}$. Como $\{1, \alpha, \dots, \alpha^{d-1}\}$ es una base de $K(\alpha)/K$, entonces $\{\beta_i \alpha^j : 1 \leq i \leq r, 0 \leq j \leq d-1\}$ es una base de L/K . Para cada $i = 1, \dots, r$, sea W_i al espacio vectorial generado por $\{\beta_i, \beta_i \alpha, \dots, \beta_i \alpha^{d-1}\}$. Es claro que cada W_i es r_α -invariante y $L = W_1 \oplus \cdots \oplus W_r$. Por la Proposición 1.6.1, la matriz que representa a la restricción de r_α a $K(\alpha)$ tiene por polinomio característico a $m(x)$. También se tiene que en cada W_i , la matriz que representa a la restricción de r_α es la misma, más aún, es la que representa a r_α sobre $K(\alpha)$. De todo esto, el polinomio característico de r_α sobre K es $f(x) = m(x)^r$. Ahora, como la extensión $L/K(\alpha)$ tiene grado r y es separable, entonces cada inmersión de $K(\alpha)$, en una extensión normal que contiene a L , se puede extender en r formas distintas y, por definición, cada inmersión de estas queda definida por la acción en α . Más preciso, si estas inmersiones son $\sigma_1 = \text{id}, \sigma_2, \dots, \sigma_d$, entonces $\sigma_j(\alpha) = \alpha_j$, con $\alpha = \alpha_1$. El resultado se obtiene recordando que el determinante de r_α es el producto de las raíces de $f(x)$ y que la traza de r_α es la suma de las raíces de $f(x)$. \square

CAPÍTULO 2

Campos numéricos

A un campo numérico K lo podemos considerar como un espacio vectorial de dimensión finita sobre los números racionales, por consiguiente éste tiene una \mathbb{Q} -base la cual es, en teoría, relativamente sencilla de construir. Por ejemplo, si θ es un elemento primitivo, entonces una \mathbb{Q} -base para K es $\{1, \theta, \dots, \theta^{n-1}\}$, donde $n = [K : \mathbb{Q}]$.

Junto con el campo numérico, se tiene una nueva estructura de anillo denominado el *anillo de enteros* de K sobre \mathbb{Q} y denotado por \mathcal{O}_K . En este capítulo vamos a demostrar que este anillo tiene rango n , es decir, lo podemos considerar como un \mathbb{Z} -módulo libre de rango n , es aquí en donde aparece el concepto de base entera, que es el tópico central de la discusión que estamos realizando. Asimismo, mostraremos que en anillos Dedekind tenemos un resultado análogo al del Teorema Fundamental de la Aritmética, visto ahora en los ideales del anillo, con el cual definiremos el grupo y número de clase del campo numérico K , ya que \mathcal{O}_K resulta ser un anillo Dedekind.

Finalmente, incluimos resultados que hemos encontrado en [13] y [15], éstos jugarán un rol importante ya que son parte fundamental de algunos resultados que hemos obtenido en este trabajo.

2.1. Dependencia entera

En esta sección desarrollamos propiedades con el fin de extender al anillo de los enteros racionales.

Definición 2.1.1. Sean R y R' anillos tales que $R \subseteq R'$. Un elemento $b \in R'$ se dice entero sobre R , si existe $f(x) \in R[x]$, mónico tal que $f(b) = 0$.

Como mencionamos antes, buscamos que este trabajo sea lo más autocontenido posible, así que enunciamos la Regla de Cramer, la cual utilizaremos en distintas ocasiones.

Teorema 2.1.1 (Regla de Cramer). *Sea A una matriz $n \times n$, entonces $\text{Adj}(A) \cdot A = A \cdot \text{Adj}(A) = |A|I_n$, donde $\text{Adj}(A)$ es la matriz adjunta clásica de A .*

Teorema 2.1.2. [3, Teorema 6] *Sean $R \subseteq R'$ anillos y $b \in R'$. Entonces las siguientes condiciones son equivalentes.*

- (i) *El elemento $b \in R'$ es entero sobre R .*
- (ii) *El anillo $R[b]$ es un R -módulo finitamente generado.*
- (iii) *Existe B , R -módulo finitamente generado tal que $R[b] \subseteq B \subseteq R'$.*
- (iv) *Existe $M \subseteq R'$, $R[b]$ -módulo finitamente generado como R -módulo, y el único elemento $y \in R[b]$ tal que $yM = 0$ es $y = 0$.*

Demostración.

(i) \Rightarrow (ii) Como b es entero, entonces existe $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$ tal que $f(b) = b^n + a_{n-1}b^{n-1} + \cdots + a_1b + a_0 = 0$. De esto se tiene que $b^n \in R + Rb + \cdots + Rb^{n-1}$. Inductivamente se prueba que $b^{n+i} \in R + Rb + \cdots + Rb^{n-1}$, para todo $i \geq 1$, por lo que $R[b] = R + Rb + \cdots + Rb^{n-1}$, es decir, es generado por $\{1, b, \dots, b^{n-1}\}$.

(ii) \Rightarrow (iii) Basta con tomar $B = R[b]$.

(iii) \Rightarrow (iv) Para la primera parte tomemos $M = B$. Luego, como $1 \in M$, si $yM = 0$, entonces $y \cdot 1 = y = 0$

(iv) \Rightarrow (i) Sea $b \in R'$. Vamos a mostrar que existe $f(x) \in R[x]$ tal que $f(b) = 0$. Para esto, sea $M = Rm_1 + \cdots + Rm_n$. Como M es un $R[b]$ -módulo, entonces $bM \subseteq M$, por lo que existen $a_{ij} \in R$ tales que

$$bm_i = a_{i1}m_1 + \cdots + a_{in}m_n, \quad \text{para todo } i = 1, \dots, n.$$

Así, si $A = (a_{ij})$ es la matriz de coeficientes del sistema, entonces

$$(A - bI_n) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad (2.1)$$

Multiplicando por la matriz adjunta clásica de $A - bI_n$ y usando la Regla de Cramer obtenemos

$$|A - bI_n|I_n \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

con I_n la matriz identidad. De esto se obtiene que $|A - bI_n|m_i = 0$, para todo $i = 1, \dots, n$. En consecuencia $|A - bI_n| = 0$ ya que, por hipótesis, el único elemento y tal que $yM = 0$ es $y = 0$.

Por último, sea $f(x) = |xI_n - A|$, entonces $f(x) \in R[x]$, es mónico y $f(b) = |bI_n - A| = 0$, como se quería. \square

Teorema 2.1.3. [3, Teorema 7] *Si R y R' son anillos tales que $R \subseteq R'$ y $b_1, \dots, b_n \in R'$ son enteros sobre R , entonces $R[b_1, \dots, b_n]$ es un R -módulo finitamente generado.*

Demostración. Se argumentará por inducción sobre n . Si $n = 1$, el resultado se tiene por el Teorema 2.1.2.

Supongamos que $n > 1$ y el resultado cierto para $n - 1$. Vamos a mostrar que $R[b_1, \dots, b_n]$ es un R -módulo finitamente generado. Por hipótesis de inducción, existen $a_1, \dots, a_r \in R[b_1, \dots, b_{n-1}]$ generadores de $R[b_1, \dots, b_{n-1}]$ como R -módulo. Puesto que b_n es entero sobre R , entonces también es entero sobre $R[b_1, \dots, b_{n-1}]$. Luego, para algún entero positivo k , $R[b_1, \dots, b_{n-1}, b_n]$ es generado sobre $R[b_1, \dots, b_{n-1}]$ por $\{1, b_n, \dots, b_n^k\}$. La conclusión se obtiene tomando como generadores a $\{a_i b_n^j\}$ con $1 \leq i \leq r$ y $1 \leq j \leq k$. \square

Corolario 2.1.1. [3, Corolario 4] *Si $R \subseteq R'$ son anillos y $R_c = \{b \in R' : b \text{ es entero sobre } R\}$, entonces R_c es un subanillo de R' que contiene a R .*

Demostración. Sean $x, y \in R'$ enteros sobre R . Por el Teorema 2.1.3, $R[x, y]$ es finitamente generado como R -módulo. Luego, por el Teorema 2.1.2, $x \pm y$ y xy son enteros sobre R . Lo que implica que R_c es un subanillo de R' , además todo elemento $b \in R$ es entero sobre R , pues $f(x) = x - b \in R[x]$, es mónico y $f(b) = 0$. \square

Definición 2.1.2. *Sean $R \subseteq R'$ y R_c como en el Corolario 2.1.1.*

Al anillo R_c se le llama la cerradura entera de R en R' . Si $R' = R_c$, se dice que R' es entero sobre R .

Cuando R es un dominio entero, R' es el campo de cocientes de R y $R_c = R$, se dice que R es íntegramente cerrado.

Definición 2.1.3. Sean $\bar{\mathbb{Q}}$ la cerradura algebraica de \mathbb{Q} en \mathbb{C} y \mathcal{O} la cerradura entera de \mathbb{Z} en $\bar{\mathbb{Q}}$. Al anillo \mathcal{O} le llamaremos el anillo de los enteros en $\bar{\mathbb{Q}}$.

Observación 2.1.1. [3, Observación 10] Se cumple que $\bar{\mathbb{Q}}$ es el campo de cocientes de \mathcal{O} .

Demostración. Esta demostración la podemos encontrar en la referencia mencionada. \square

Definición 2.1.4. Dado un campo numérico K , se define el anillo de enteros \mathcal{O}_K en K como $\mathcal{O}_K = K \cap \mathcal{O}$.

Observación 2.1.2. Si R es un dominio de factorización única, entonces R es íntegramente cerrado.

Demostración. Sean R' el campo de cocientes de R y $y \in R' \cap R_c$, entonces $y = \frac{a}{b}$ con $a, b \in R$. Queremos mostrar que $y \in R$. Como R es dominio de factorización única, podemos suponer que a y b no tienen factores en común, salvo unidades. Como y es entero, existe un polinomio mónico $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$ tal que $f(y) = 0$. De esto tenemos que

$$\left(\frac{a}{b}\right)^n = \sum_{i=0}^{n-1} -a_i \left(\frac{a}{b}\right)^i.$$

Multiplicando en la igualdad anterior por b^n obtenemos

$$a^n = b \sum_{i=0}^{n-1} -a_i a^i b^{n-i-1}. \quad (2.2)$$

De la Ecuación 2.2, llegamos a que b divide a a^n . Ahora, si y no fuera una unidad, tendríamos que b divide a a , pero esto no puede ser, ya que supusimos que a y b no tienen factores en común. Así, y es unidad de R y $y = ab^{-1} \in R$. \square

Teorema 2.1.4. [3, Teorema 8] Sean $R \subseteq R' \subseteq R''$ anillos tales que R' es entero sobre R y R'' es entero sobre R' . Entonces R'' es entero sobre R .

Demostración. Sea $\alpha \in R''$, entonces existen $a_0, \dots, a_{n-1} \in R'$ tales que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Como R' es entero sobre R entonces, por el Teorema 2.1.3, $R[a_0, a_1, \dots, a_{n-1}]$ es finitamente generado como

R -módulo. Por otro lado, como α es entero sobre $R[a_0, \dots, a_{n-1}]$, entonces $R[a_0, \dots, a_{n-1}, \alpha]$ es finitamente generado sobre $R[a_0, \dots, a_{n-1}]$. De donde $R[a_0, \dots, a_{n-1}, \alpha]$ es finitamente generado sobre R y de esto, α es entero sobre R .

Observación 2.1.3. [10, Corolario 3.17] *Sean R un dominio íntegramente cerrado, K su campo de cocientes, L/K una extensión finita y separable y R' la cerradura entera de R en L , entonces para todo R' se tiene que $T_{L/K}(\alpha), N_{L/K}(\alpha) \in R$.*

Demostración. La demostración puede ser consultada en la referencia dada. \square

2.2. Anillos Dedekind

El Teorema Fundamental de la Aritmética es un resultado que se cumple en \mathbb{Z} y es piedra angular en la aritmética, sin embargo, al considerar anillos más generales, éstos no necesariamente son de factorización única, por ejemplo, si $R = \mathbb{Z}[\sqrt{-5}]$, podemos observar que $6 = 2 \times 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$ y se muestra que ambas factorizaciones son diferentes, como producto de irreducibles. Ahora bien, vamos a mostrar que los anillos de enteros son Dedekind (Definición 2.2.6) y que en éstos anillos se tiene un resultado análogo al Teorema Fundamental de la Aritmética, para ideales, el cual a su vez es utilizado para definir el grupo de clase, cuya cardinalidad es el número de clase de un campo numérico.

Definición 2.2.1. *Un dominio entero se dice anillo de valuación discreta si es de ideales principales con un solo ideal primo no cero.*

Teorema 2.2.1. [3, Teorema 4] *Sea R un anillo, entonces los siguientes enunciados son equivalentes.*

- (i) *Todo ideal de R es finitamente generado.*
- (ii) *Todo ideal primo de R es finitamente generado.*
- (iii) *Toda sucesión $I_1 \subseteq \dots \subseteq I_n \subseteq \dots$ de ideales de R se estaciona, es decir, existe un entero m tal que $I_m = I_{m+j}$ para todo $j \geq 1$.*
- (iv) *Toda familia no vacía de ideales tiene elementos maximales con el orden dado por la inclusión.*

Demostración.

(i) \Rightarrow (iii) Sea $I_1 \subseteq \cdots I_n \subseteq \cdots$ una familia ascendente de ideales y pongamos $J = \bigcup_{j=1}^{\infty} I_j$. Se verifica que J es un ideal. Por hipótesis, J es finitamente generado, es decir, $J = \langle a_1, \dots, a_r \rangle$. Luego, existe un m tal que $\{a_1, \dots, a_r\} \subseteq I_m$ y por tanto $J = \langle a_1, \dots, a_r \rangle \subseteq I_m$. Así $I_{m+j} = I_m$, para todo $j \geq 1$.

(iii) \Rightarrow (iv) Sea $F \neq \emptyset$ una familia de ideales. Entonces existe $I_1 \in F$ ideal. Si I_1 es maximal, hemos terminado, de lo contrario existe $I_2 \in F$ ideal tal que $I_1 \subsetneq I_2$ y la inclusión es propia. Por hipótesis, esta construcción no puede continuar indefinidamente, por lo que F admite elementos maximales.

(iv) \Rightarrow (i) Sea I ideal de R y $F = \{J \subseteq I : J \text{ es f.g.}\}$. Como $(0) \subseteq I$, entonces $F \neq \emptyset$ y, por hipótesis, existe un elemento maximal $I_0 \in F$. Mostremos que $I = I_0$ y para esto argumentaremos por contradicción. Sea $a \in I \setminus I_0$, entonces $I_0 \subsetneq I_0 + (a) \subseteq I$. Como I_0 es finitamente generado, entonces $I_0 + (a)$ también lo es y por tanto $I_0 + (a) \in F$, pero esto es imposible. Así $I = I_0$ y es finitamente generado.

(i) \Rightarrow (ii) Claramente se cumple.
(ii) \Rightarrow (i) Sea $F = \{I \leq R : I \text{ no es f.g.}\}$. Si F es no vacío, entonces se ordena con la inclusión y aplicando el lema de Zorn se prueba que F admite elementos maximales. Sea $\mathfrak{M} \in F$ maximal en el sentido del orden. Mostraremos que $\mathfrak{M} \in F$ es primo. Sean $a, b \in R$ tales que $ab \in \mathfrak{M}$. Si $a, b \notin \mathfrak{M}$, entonces $J = \mathfrak{M} + (a) \notin F$ y por tanto $\mathfrak{M} + (a) = \langle b_1, \dots, b_n \rangle$ para algunos $b_i = m_i + r_i a$, con $m_i \in \mathfrak{M}$, $r_i \in R$ y $1 \leq i \leq n$. Sea $I = \{y \in R : ya \in \mathfrak{M}\}$. Así $I \notin F$, pues se verifica que I es ideal de R , además $\mathfrak{M} \subseteq I$ y $(b) \subseteq I$ (ya que $ab \in \mathfrak{M}$). Mostremos ahora que $\mathfrak{M} = \langle m_1, \dots, m_n \rangle + aI$. Como $m_i \in \mathfrak{M}$ y $aI \subseteq \mathfrak{M}$, se cumple que $\langle m_1, \dots, m_n \rangle + aI \subseteq \mathfrak{M}$. Sea $x \in \mathfrak{M} \subseteq J$, entonces $x = z_1 b_1 + \cdots + z_n b_n = z_1(m_1 + r_1 a) + \cdots + z_n(m_n + r_n a)$, de esto tenemos $x - z_1 m_1 - \cdots - z_n m_n = (z_1 r_1 + \cdots + z_n r_n) a \in \mathfrak{M}$ y por tanto $z_1 r_1 + \cdots + z_n r_n \in I$, es decir, $\mathfrak{M} = \langle m_1, \dots, m_n \rangle + aI$, pero esto implica que \mathfrak{M} es finitamente generado, lo cual es imposible. Luego, $a \in \mathfrak{M}$ o $b \in \mathfrak{M}$, es decir, \mathfrak{M} es primo, contradiciendo que $\mathfrak{M} \in F$. Así F debe ser vacío. \square

(i) \Rightarrow (ii) Claramente se cumple.

(ii) \Rightarrow (i) Sea $F = \{I \leq R : I \text{ no es f.g.}\}$. Si F es no vacío, entonces se ordena con la inclusión y aplicando el lema de Zorn se prueba que F admite elementos maximales. Sea $\mathfrak{M} \in F$ maximal en el sentido del orden. Mostraremos que $\mathfrak{M} \in F$ es primo. Sean $a, b \in R$ tales que $ab \in \mathfrak{M}$. Si $a, b \notin \mathfrak{M}$, entonces $J = \mathfrak{M} + (a) \notin F$ y por tanto $\mathfrak{M} + (a) = \langle b_1, \dots, b_n \rangle$ para algunos $b_i = m_i + r_i a$, con $m_i \in \mathfrak{M}$, $r_i \in R$ y $1 \leq i \leq n$. Sea $I = \{y \in R : ya \in \mathfrak{M}\}$. Así $I \notin F$, pues se verifica que I es ideal de R , además $\mathfrak{M} \subseteq I$ y $(b) \subseteq I$ (ya que $ab \in \mathfrak{M}$). Mostremos ahora que $\mathfrak{M} = \langle m_1, \dots, m_n \rangle + aI$. Como $m_i \in \mathfrak{M}$ y $aI \subseteq \mathfrak{M}$, se cumple que $\langle m_1, \dots, m_n \rangle + aI \subseteq \mathfrak{M}$. Sea $x \in \mathfrak{M} \subseteq J$, entonces $x = z_1 b_1 + \cdots + z_n b_n = z_1(m_1 + r_1 a) + \cdots + z_n(m_n + r_n a)$, de esto tenemos $x - z_1 m_1 - \cdots - z_n m_n = (z_1 r_1 + \cdots + z_n r_n) a \in \mathfrak{M}$ y por tanto $z_1 r_1 + \cdots + z_n r_n \in I$, es decir, $\mathfrak{M} = \langle m_1, \dots, m_n \rangle + aI$, pero esto implica que \mathfrak{M} es finitamente generado, lo cual es imposible. Luego, $a \in \mathfrak{M}$ o $b \in \mathfrak{M}$, es decir, \mathfrak{M} es primo, contradiciendo que $\mathfrak{M} \in F$. Así F debe ser vacío. \square

Definición 2.2.2. Se dice que R es un anillo noetheriano si satisface cualquiera de las 4 condiciones del Teorema 2.2.1.

Definición 2.2.3. Sean R un dominio entero noetheriano, K su campo de cocientes, M un R -módulo no cero contenido en K . Se dice que M es un

ideal fraccionario de R si M es finitamente generado sobre R .

Teorema 2.2.2. [3, Teorema 21] Sean R un dominio entero noetheriano, K su campo de cocientes, M un R -módulo no cero contenido en K , entonces M es un ideal fraccionario de R si y sólo si existe $r \in R \setminus \{0\}$ tal que $rM \subseteq R$.

Demostración. Supongamos que M es un ideal fraccionario, entonces $M = \frac{a_1}{b_1}R + \cdots + \frac{a_n}{b_n}R$. Si $r = \prod_{i=1}^n b_i$, se tiene $rM \subseteq R$. Recíprocamente, supongamos ahora que existe $r \in R \setminus \{0\}$ tal que $rM \subseteq R$, entonces rM es un ideal de R y es finitamente generado, ya que R es noetheriano. De esto $rM = a_1R + \cdots + a_nR$, lo que implica $M = \frac{a_1}{r}R + \cdots + \frac{a_n}{r}R$. \square

Definición 2.2.4. Dado un ideal fraccionario M , se define $M^{-1} = \{x \in K : xM \subseteq R\}$.

Observación 2.2.1. [9, Observación, página 17] Si M es un ideal fraccionario, entonces M^{-1} también lo es.

Demostración. Por definición tenemos que M^{-1} es un subconjunto de K y se verifica sin dificultad que es un R -módulo no cero. Falta mostrar que es finitamente generado sobre R . Para esto, sea $m \in M$, con $m \neq 0$. Entonces $M^{-1}m \subseteq R$ y es finitamente generado como R -módulo, ya que R es noetheriano. Así $M^{-1}m = a_1R + \cdots + a_nR$, lo que implica $M^{-1} = \frac{a_1}{m}R + \cdots + \frac{a_n}{m}R$, como se quería. \square

Definición 2.2.5. Un ideal fraccionario M se dice invertible si $MM^{-1} = R$.

Observación 2.2.2. [3, Observación 8] Si R es de valuación discreta, entonces

- (i) El anillo R es íntegramente cerrado.
- (ii) El anillo R es noetheriano.
- (iii) Todo elemento $\alpha \in R \setminus \{0\}$ es de la forma $u\pi^n$, con $n \geq 0$, u unidad y π irreducible que genera al único primo no cero de R .
- (iv) Los ideales no cero en R son de la forma $R\pi^n$, con $n \geq 1$.

Demostración.

(i) Como R es un dominio de valuación discreta, entonces es de ideales principales y por tanto de factorización única, luego por la Observación 2.1.2, R es íntegramente cerrado.

(ii) El anillo R es noetheriano, pues es de ideales principales.

(iii) Como R es de factorización única y tiene un único ideal maximal no cero, entonces existe, salvo asociados un único elemento irreducible π .

(iv) Este hecho se sigue de (iii) y de que R es de ideales principales.

Teorema 2.2.3. [3, Teorema 10] *Si R es un dominio entero, entonces R es de valuación discreta si y sólo si R es noetheriano, íntegramente cerrado y con un único ideal primo no cero.*

Demostración. Si R es de valuación discreta, por la Observación 2.2.2, R es noetheriano, íntegramente cerrado y con un único ideal primo no cero.

Para probar el recíproco, debemos mostrar que R es de ideales principales. Para esto, mostremos primero que si \mathfrak{p} es el ideal primo no cero de R , entonces es principal. Sean $a \in \mathfrak{p} \setminus \{0\}$, $b \in R$ y consideremos el conjunto $(a : b) = \{r \in R : rb \in Ra\}$, el cual resulta ser un ideal, como se puede verificar sin dificultad. Definamos $F = \{(a : b) : b \notin Ra\}$ y notemos que $F \neq \emptyset$, pues $(a : 1) \in F$. Dado que R es noetheriano, entonces F admite elementos maximales. Sea $\mathfrak{M} = (a : b) \in F$ maximal, en el sentido de orden. Mostraremos que \mathfrak{M} es primo no cero. Como $a \neq 0$ y $a \in \mathfrak{M}$, entonces $\mathfrak{M} \neq (0)$, además si $xy \in \mathfrak{M}$ y $x, y \notin \mathfrak{M}$, entonces

$$\mathfrak{M} = (a : b) \subsetneq \mathfrak{M} + (x) \subseteq (a : yb),$$

contradiciendo la elección de \mathfrak{M} . Luego, como \mathfrak{p} es el único primo no cero, entonces $\mathfrak{p} = (a : b) = \mathfrak{M}$.

Por la elección de b , se tiene $\frac{b}{a} \notin R$. Observemos que $\mathfrak{M}\frac{b}{a} \subseteq R$ y es un ideal, entonces se cumple una de las posibilidades: $\mathfrak{M}\frac{b}{a} \subseteq \mathfrak{M}$ o $\mathfrak{M}\frac{b}{a} = R$, pues \mathfrak{M} es maximal. Si $\mathfrak{M}\frac{b}{a} \subseteq \mathfrak{M}$, entonces \mathfrak{M} es un $R\left[\frac{b}{a}\right]$ -módulo finitamente generado sobre R .

Aplicando el Teorema 2.1.2, y que R es íntegramente cerrado, tenemos que $\frac{b}{a} \in R$, lo cual es imposible. De esto, $\mathfrak{M}\frac{b}{a} = R$ y $\mathfrak{M} = R\frac{a}{b} = R\pi$.

Ahora mostremos que R es de ideales principales, para esto primero probemos que

$$\bigcap_{n \geq 1} (\pi^n) = (0). \quad (2.3)$$

Sea $a \in \bigcap_{n \geq 1} (\pi^n)$, entonces $a = b_n \pi^n = b_{n+1} \pi^{n+1}$ para todo $n \geq 1$. De lo anterior tenemos $(b_1) \subseteq (b_2) \subseteq \cdots \subseteq (b_n) \subseteq \cdots$ y, como R es noetheriano, entonces existe n tal que $(b_n) = (b_{n+1})$. Así $b_{n+1} = t_n b_n$ y, de la igualdad $a = b_n \pi^n = b_{n+1} \pi^{n+1}$, tenemos que $a = b_n \pi^n = b_n t_n \pi^{n+1}$ lo que implica $b_n(t_n \pi - 1) = 0$. Como R es un dominio entero y π no es unidad, entonces $b_n = 0$, probando que $a = 0$. Por último, sea I ideal de R no cero. De la Ecuación 2.3 concluimos que existe n tal que $I \subseteq (\pi^n)$ e $I \not\subseteq (\pi^{n+1})$. Sea $a \in I \setminus (\pi^{n+1})$, entonces $a = t \pi^n$ y π no divide a t , por que t es unidad. Así $\pi^n = t^{-1} a \in I$. Luego $I = (\pi^n)$, como se quería. \square

Definición 2.2.6. *Un dominio entero R se dice anillo Dedekind si es noetheriano y $R_{\mathfrak{p}}$ es anillo de valuación discreta para todo ideal primo $\mathfrak{p} \neq (0)$.*

Teorema 2.2.4. [3, Teorema 11] *Si R es un dominio Dedekind y S es un subconjunto multiplicativamente cerrado de R , entonces:*

- (i) *todo ideal primo no cero de R es un ideal maximal,*
- (ii) *el anillo R_S es Dedekind.*

Demostración.

(i) Si \mathfrak{p} es un ideal primo de R , entonces existe \mathfrak{M} , ideal maximal de R , tal que $\mathfrak{p} \subseteq \mathfrak{M}$. Como \mathfrak{M} es maximal, entonces es primo. Si localizamos a R en \mathfrak{M} tenemos que $\mathfrak{p}R_{\mathfrak{M}} \subseteq \mathfrak{M}R_{\mathfrak{M}}$. Dado que $R_{\mathfrak{M}}$ es un dominio de valuación discreta, entonces tiene un único ideal primo. Luego, por el Teorema 1.5.2, necesariamente se cumple que $\mathfrak{p} = \mathfrak{M}$.

(ii) Primero mostremos que R_S es noetheriano. Como R lo es, entonces todo ideal de R es finitamente generado, además todo ideal de R_S es de la forma IR_S , con $I \leq R$. Así IR_S es finitamente generado y por tanto R_S es noetheriano. Ahora probemos que $(R_S)_{\mathfrak{p}R_S}$ es de valuación discreta. Un ideal primo en R_S tiene la forma $\mathfrak{p}R_S$, con $\mathfrak{p} \leq R$ y $\mathfrak{p} \cap S = \emptyset$. Como $S \subseteq R \setminus \mathfrak{p}$, entonces $R_S \hookrightarrow R_{\mathfrak{p}}$. Se verifica que

$$(R_S)_{\mathfrak{p}R_S} = \left\{ \frac{\frac{r}{t}}{\frac{a}{s}} : \frac{a}{s} \notin \mathfrak{p}R_S \right\} \cong R_{\mathfrak{p}}.$$

Por tanto R_S es Dedekind. □

Teorema 2.2.5. (Teorema Chino del Residuo [3, Teorema 12]) Sean R un anillo conmutativo con identidad e I_1, \dots, I_n ideales de R tales que $I_i + I_j = R$

para $i \neq j$. Si $I = \bigcap_{j=1}^n I_j$, entonces:

$$(i) \quad \frac{R}{I} \cong \frac{R}{I_1} \times \cdots \times \frac{R}{I_n}$$

$$(ii) \quad I = \bigcap_{j=1}^n I_j = I_1 \cdots I_n$$

Demostración.

(i) Sea $\varphi : R \rightarrow \frac{R}{I_1} \times \cdots \times \frac{R}{I_n}$ dada por $\varphi(r) = (r + I_1, \dots, r + I_n)$.

Se verifica que φ es un homomorfismo y $\text{Ker}\varphi = I$. Mostremos que φ es suprayectiva. Para esto, definamos $e_i := (0, \dots, 0, 1 + I_i, 0, \dots, 0) \in \frac{R}{I_1} \times$

$\cdots \times \frac{R}{I_n}$. Observemos que, como $(r_1 + I_1, \dots, r_n + I_n) = r_1 e_1 + \cdots + r_n e_n$, es suficiente justificar que existe $x_i \in R$ tal que $\varphi(x_i) = e_i$, pues si definimos $x = r_1 x_1 + \cdots + r_n x_n$ tenemos que $\varphi(x) = (r_1 + I_1, \dots, r_n + I_n)$.

Fijemos un índice i . Entonces para cada $j \neq i$, existen $x_{ij} \in I_i$ y $y_j \in I_j$ tales que $x_{ij} + y_j = 1$, pues $I_i + I_j = R$. Sea $x_i = \prod_{j \neq i} y_j = \prod_{j \neq i} (1 - x_{ij}) = 1 - x$

con $x \in I_i$. De esto tenemos que $x_i \equiv 1 \pmod{I_i}$, $x_i \equiv 0 \pmod{I_j}$ para $j \neq i$ y por tanto $\varphi(x_i) = e_i$. Ahora, por el primer teorema de isomorfismo

$$\frac{R}{I} \cong \frac{R}{I_1} \times \cdots \times \frac{R}{I_n}.$$

(ii) Para esta parte, argumentaremos por inducción sobre n . Supongamos que $n = 2$. Sabemos que $I_1 I_2 \subseteq I_1 \cap I_2$. Mostraremos la otra inclusión. Como $I_1 + I_2 = R$, entonces existen $a_1 \in I_1$ y $a_2 \in I_2$ tales que $a_1 + a_2 = 1$. Así, si $r \in I_1 \cap I_2$, entonces $r = r a_1 + r a_2 \in I_1 I_2$.

Supongamos que $n > 2$ y el resultado cierto para $n - 1$. Sea $J = I_1 \cdots I_{n-1}$. Por hipótesis tenemos que para cada $1 \leq j \leq n - 1$, existen $x_j \in I_n$ y

$y_j \in I_j$ tales que $1 = x_j + y_j$. Si $y = \prod_{j=1}^{n-1} y_j = \prod_{j=1}^{n-1} (1 - x_j) = 1 - x \in J$,

entonces $1 - x = y \in J$ y $x \in I_n$. Luego, como $x + y = 1$, tenemos que

$J + I_n = R$. Aplicando hipótesis inductiva y el caso $n = 2$ concluimos que

$$(I_1 \cdots I_{n-1}) \cdot I_n = J \cap I_n = (I_1 \cap \cdots \cap I_{n-1}) \cap I_n = \bigcap_{j=1}^n I_j. \quad \square$$

Teorema 2.2.6. [3, Teorema 14] *Si R un anillo noetheriano, entonces todo ideal de R contiene un producto finito de ideales primos.*

Demostración. Sea $F = \{I \leq R : I \text{ no contiene un producto finito de ideales primos}\}$. Si $F \neq \emptyset$, entonces por el Teorema 2.2.1, F tiene elementos maximales. Sean $\mathfrak{p} \in F$ maximal y $a, b \in R$ tales que $ab \in \mathfrak{p}$, entonces $\mathfrak{p} \subsetneq \mathfrak{p} + (a)$ y $\mathfrak{p} \subsetneq \mathfrak{p} + (b)$ y por tanto $\mathfrak{p} + (a), \mathfrak{p} + (b) \notin F$. Así, existen $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_t$, ideales primos de R , tales que $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{p} + (a)$ y $\mathfrak{q}_1 \cdots \mathfrak{q}_t \subseteq \mathfrak{p} + (b)$. Tomando producto obtenemos $\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_t \subseteq (\mathfrak{p} + (a))(\mathfrak{p} + (b)) \subseteq \mathfrak{p}$, lo cual no es posible, pues $\mathfrak{p} \in F$. En consecuencia $F = \emptyset$. \square

Observación 2.2.3. [3, Observación 11] *Si M_1 y M_2 son ideales maximales diferentes de R , entonces $M_1^n + M_2^m = R$, para todos $n, m \geq 1$.*

Demostración. Sean $n, m \geq 1$. Como $M_1 \neq M_2$ y son maximales, existen $x \in M_1$ y $y \in M_2$ tales que $x + y = 1$. De esto $x^n = (1 - y)^n = 1 - z$, con $z \in M_2$. De lo anterior tenemos $z^m = (1 - x^n)^m = 1 - w$, con $w \in M_1^n$. Así, $M_1^n + M_2^m = R$ para todos $n, m \geq 1$. \square

Corolario 2.2.1. [3, Corolario 5] *Si M_1, \dots, M_n son ideales maximales de R , entonces para todo $e_i \geq 1$*

$$\frac{R}{\bigcap_{i=1}^n M_i^{e_i}} = \frac{R}{\prod_{i=1}^n M_i^{e_i}} \cong \frac{R}{M_1^{e_1}} \times \cdots \times \frac{R}{M_n^{e_n}}.$$

Demostración. La conclusión se tiene del Teorema 2.2.5 y de la Observación 2.2.3. \square

Corolario 2.2.2. [3, Corolario 6] *Si R es un anillo noetheriano, entonces existen ideales primos tales que $(0) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Adicionalmente, si todo ideal primo no cero es maximal, entonces*

$$R \cong \frac{R}{\mathfrak{p}_1^{e_1}} \times \cdots \times \frac{R}{\mathfrak{p}_r^{e_r}}$$

Demostración. La primera parte se obtiene del Teorema 2.2.6. Para la segunda parte usamos el Teorema Chino del Residuo, es decir,

$$R \cong \frac{R}{(0)} = \frac{R}{\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}} \cong \frac{R}{\mathfrak{p}_1^{e_1}} \times \cdots \times \frac{R}{\mathfrak{p}_r^{e_r}}.$$

□

Teorema 2.2.7. [3, Teorema 15] *Sea R un anillo en el que todo ideal primo no cero es maximal. Adicionalmente, supongamos que $(0) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, con $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ ideales primos no cero. Entonces estos son los únicos ideales primos de R .*

Demostración. Sea \mathfrak{Q} un ideal primo no cero de R . Entonces $(0) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \subseteq \mathfrak{Q}$. Como \mathfrak{Q} es primo, entonces $\mathfrak{p}_i \subseteq \mathfrak{Q}$, para algún $i = 1, \dots, r$. Luego, como todo ideal primo es maximal, necesariamente $\mathfrak{p}_i = \mathfrak{Q}$. □

Corolario 2.2.3. [3, Corolario 7] *Si R es un dominio Dedekind e I es un ideal no cero de R , entonces existe solamente un número finito de ideales primos $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ que contienen a I y $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \subseteq I$, para algunos $e_i > 0$.*

Demostración. Sea $B = \frac{R}{I}$, entonces los únicos ideales en B son los que se corresponden con los ideales que contienen a I . Además, como R es noetheriano, entonces B también lo es y por el Teorema 2.2.6, todo ideal de B contiene un producto finito de ideales primos. Luego, por el Corolario 2.2.2, $\{\bar{0}\} = \bar{\mathfrak{p}}_1^{e_1} \cdots \bar{\mathfrak{p}}_r^{e_r}$, es decir,

$$\frac{I}{I} = \left(\frac{\mathfrak{p}}{I}\right)^{e_1} \cdots \left(\frac{\mathfrak{p}}{I}\right)^{e_r} = \frac{\mathfrak{p}^{e_1} + I}{I} \cdots \frac{\mathfrak{p}^{e_r} + I}{I} = \frac{\mathfrak{p}^{e_1} \cdots \mathfrak{p}^{e_r} + I}{I}.$$

Por el teorema de la correspondencia para ideales tenemos $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} + I = I$ y en consecuencia $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \subseteq I$. □

Teorema 2.2.8. [3, Teorema 16] *Si R es un dominio Dedekind, \mathfrak{p} es un ideal primo no cero de R y $a \in \mathbb{N}$, entonces*

$$\frac{R}{\mathfrak{p}^a} \cong \frac{R_{\mathfrak{p}}}{\mathfrak{p}^a R_{\mathfrak{p}}}.$$

Demostración. Definamos $f : \frac{R}{\mathfrak{p}^a} \longrightarrow \frac{R_{\mathfrak{p}}}{\mathfrak{p}^a R_{\mathfrak{p}}}$, dada por $f(r + \mathfrak{p}^a) = r + \mathfrak{p}^a R_{\mathfrak{p}}$. Se verifica que f está bien definida y que es homomorfismo. Mostremos que

es inyectiva. Para esto, si $f(r + \mathfrak{p}^a) = r + \mathfrak{p}^a R_{\mathfrak{p}} = \mathfrak{p}^a R_{\mathfrak{p}}$, entonces $r \in \mathfrak{p}^a R_{\mathfrak{p}}$ y de esto $\frac{r}{1} = \frac{b}{t}$, con $b \in \mathfrak{p}^a$, $t \in R \setminus \mathfrak{p}$, consecuentemente $tr = b \in \mathfrak{p}^a$. Ahora, como $t \notin \mathfrak{p}$, se cumple que $(t) + \mathfrak{p} = R$. Luego, usando un argumento similar al de la Observación 2.2.3, $(t) + \mathfrak{p}^a = R$. En consecuencia, existen $x \in R$ y $y \in \mathfrak{p}^a$ tales que $xt + y = 1$. Si multiplicamos la ecuación anterior por r obtenemos que $xrt + yr = xb + yr = r \in \mathfrak{p}^a$, ya que xb y yr son elementos de \mathfrak{p}^a .

Mostremos que f es suprayectiva. Sea $\frac{b}{c} + \mathfrak{p}^a R_{\mathfrak{p}}$, con $b \in R$ y $c \notin \mathfrak{p}$. Entonces $(c) + \mathfrak{p} = R$, lo que implica $(c) + \mathfrak{p}^a = R$, de lo cual existen $x \in R$ y $y \in \mathfrak{p}^a$ tales que $xc + y = 1$. De esto $x + \frac{y}{c} = \frac{1}{c}$ y así $bx + \frac{by}{c} = \frac{b}{c}$. Luego $f(bx + \mathfrak{p}^a) = \frac{b}{c} + \mathfrak{p}^a R_{\mathfrak{p}}$, como se quería. \square

Corolario 2.2.4. [3, Corolario 8] *Si R y a son como en el Teorema 2.2.8, entonces los ideales en $\frac{R}{\mathfrak{p}^a}$ son potencia de $\frac{\mathfrak{p}}{\mathfrak{p}^a}$, el cual es principal.*

Demostración. Como $R_{\mathfrak{p}}$ es de ideales principales, entonces $\frac{R_{\mathfrak{p}}}{\mathfrak{p}^a R_{\mathfrak{p}}}$ también lo es. Luego, de $\frac{R}{\mathfrak{p}^a} \cong \frac{R_{\mathfrak{p}}}{\mathfrak{p}^a R_{\mathfrak{p}}}$, tenemos que $\frac{R}{\mathfrak{p}^a}$ es de ideales principales. Por el teorema de la correspondencia y dado que $\frac{\mathfrak{p}}{\mathfrak{p}^a}$ es principal, todo ideal en $\frac{R}{\mathfrak{p}^a}$ es potencia de $\frac{\mathfrak{p}}{\mathfrak{p}^a}$. \square

Teorema 2.2.9. [3, Teorema 17] *Si R es un dominio Dedekind e I es un ideal no cero de R , entonces $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, para algunos $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ ideales primos y $e_i > 0$, $i = 1, 2, \dots, r$. La factorización de I es única salvo orden.*

Demostración. Primero mostremos la existencia. Por el Corolario 2.2.3, tenemos que existen $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ tales que $\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r} \subseteq I$ con $a_i > 0$. Como R es Dedekind, por la Observación 2.2.3 y el Teorema Chino del Residuo (Teorema 2.2.5) obtenemos:

$$B = \frac{R}{\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}} \cong \frac{R}{\mathfrak{p}_1^{a_1}} \times \cdots \times \frac{R}{\mathfrak{p}_r^{a_r}}.$$

Ahora, por el isomorfismo anterior, el ideal $\frac{I}{\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}}$ tiene una representación en $\frac{R}{\mathfrak{p}_1^{a_1}} \times \cdots \times \frac{R}{\mathfrak{p}_r^{a_r}}$ de la forma $\frac{\mathfrak{p}_1^{e_1}}{\mathfrak{p}_1^{a_1}} \times \cdots \times \frac{\mathfrak{p}_r^{e_r}}{\mathfrak{p}_r^{a_r}}$, es decir, existe una función $f : \frac{I}{\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}} \rightarrow \frac{\mathfrak{p}_1^{e_1}}{\mathfrak{p}_1^{a_1}} \times \cdots \times \frac{\mathfrak{p}_r^{e_r}}{\mathfrak{p}_r^{a_r}}$, dada por $f(y) = (y + \mathfrak{p}_1^{a_1}, \dots, y + \mathfrak{p}_r^{a_r})$. Por el isomorfismo f , existen $y_i \in \mathfrak{p}_i^{e_i}$ tales que $(y + \mathfrak{p}_1^{a_1}, \dots, y + \mathfrak{p}_r^{a_r}) = (y_1 + \mathfrak{p}_1^{a_1}, \dots, y_r + \mathfrak{p}_r^{a_r})$. De la igualdad anterior tenemos que $y - y_i \in \mathfrak{p}_i^{a_i} \subseteq \mathfrak{p}_i^{e_i}$ y de esto, $y \in \mathfrak{p}_i^{e_i}$, es decir, $y \in \bigcap_{i=1}^r \mathfrak{p}_i^{e_i} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, para todo $i = 1, \dots, r$. Con esto se ha probado que $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$.

Mostremos unicidad. Supongamos que $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} = \mathfrak{q}_1^{a_1} \cdots \mathfrak{q}_s^{a_s}$, con \mathfrak{p}_i y \mathfrak{q}_j ideales primos para todos $i = 1, \dots, r$ y $j = 1, \dots, s$. Entonces $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \subseteq \mathfrak{q}_i$ para todo i . De esto $\mathfrak{p}_j \subseteq \mathfrak{q}_i$. Luego, como R es Dedekind y por el Teorema 2.2.4, se cumple que todo ideal primo es maximal y en consecuencia $\mathfrak{p}_j = \mathfrak{q}_i$, para algún i y algún j . Así $r \leq s$. Análogamente se prueba que $s \leq r$ y por tanto $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$. Para cada $i = 1, \dots, r$ considere el ideal $IR_{\mathfrak{p}_i} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} R_{\mathfrak{p}_i} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r} R_{\mathfrak{p}_i}$. Entonces $\mathfrak{p}_i^{e_i} R_{\mathfrak{p}_i} = \mathfrak{p}_i^{a_i} R_{\mathfrak{p}_i}$ y, como $\mathfrak{p}_i R_{\mathfrak{p}_i}$ es principal, se tiene que es generado por un elemento, digamos π . Así $\pi^{e_i} R_{\mathfrak{p}_i} = \pi^{a_i} R_{\mathfrak{p}_i}$, lo que implica que $\pi^{e_i} = \pi^{a_i} u$, con u unidad en $R_{\mathfrak{p}_i}$ y $e_i = a_i$, como se quería. \square

Teorema 2.2.10. [3, Teorema 18] *Si R es un dominio Dedekind el cual tiene sólo un número finito de ideales primos, entonces R es un dominio de ideales principales.*

Demostración. Como R es Dedekind, entonces todo ideal no cero se puede factorizar como producto de ideales primos. Por esto, basta mostrar el resultado para los ideales primos. Sean $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ los ideales primos de R . Entonces, por el Corolario 2.2.4, sabemos que $\frac{\mathfrak{p}_i}{\mathfrak{p}_i^2}$ es principal para todo $i = 1, \dots, r$.

Así $\frac{\mathfrak{p}_i}{\mathfrak{p}_i^2} = \pi_i + \mathfrak{p}_i^2$, con $\pi_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$. Luego, por el Teorema Chino del Residuo, tenemos $\frac{R}{\mathfrak{p}_1 \cdots \mathfrak{p}_i^2 \cdots \mathfrak{p}_r} \cong \frac{R}{\mathfrak{p}_1} \times \cdots \times \frac{R}{\mathfrak{p}_i^2} \times \cdots \times \frac{R}{\mathfrak{p}_r}$. Así, existe $x_i \in R$ tal que $x_i \equiv \pi_i \pmod{\mathfrak{p}_i^2}$ y $x_i \equiv 1 \pmod{\mathfrak{p}_j}$ con $j \neq i$. De esto, $x_i \in \mathfrak{p}_i$ y $x_i \notin \mathfrak{p}_j$. Por consiguiente $x_i R \not\subseteq \mathfrak{p}_j$ y, como $x_i R$ se factoriza como producto de primos en R , necesariamente $x_i R = \mathfrak{p}_i$. \square

Teorema 2.2.11. [3, Teorema 19] Sean R un dominio íntegramente cerrado, K su campo de cocientes, L/K una extensión finita y separable de grado n , A la cerradura entera de R en L . Entonces existen R -módulos M y M' de rango n tales que $M' \subseteq A \subseteq M$. Explícitamente, si $L = K(\alpha)$, $\alpha \in A$, entonces $M' = R \oplus R\alpha \oplus \cdots \oplus R\alpha^{n-1} = R[\alpha]$ y $M = \frac{1}{\delta}R[\alpha]$, con

$$\delta = \prod_{i < j} (\alpha_i - \alpha_j)^2,$$

en donde $\alpha = \alpha_1, \dots, \alpha_n$ son los conjugados de α .

Demostración. Como $[L : K] < \infty$ y L/K es separable, entonces por el Teorema del elemento primitivo, existe $\beta \in L$ tal que $L = K(\beta)$. Se verifica que existen $\alpha \in A$ y $b \in R$ tales que $\beta = \frac{\alpha}{b}$. Por tanto $L = K(\alpha)$ y $\{1, \alpha, \dots, \alpha^{n-1}\}$ es una K -base de L . Si $M' = R \oplus R\alpha \oplus \cdots \oplus R\alpha^{n-1} = R[\alpha]$ tenemos la primera parte del teorema, es decir, $M' \subseteq A$. Mostremos ahora que $A \subseteq \frac{1}{\delta}R[\alpha]$. Para esto, sea $y \in A$, entonces existen c_1, \dots, c_n elementos de K tales que

$$y = \sum_{j=0}^{n-1} c_j \alpha^j. \quad (2.4)$$

Reescribiendo la Ecuación 2.4 tenemos

$$y = \sum_{j=0}^{n-1} \delta c_j \frac{\alpha^j}{\delta}.$$

Como $\delta \in R$, (Observación 2.3.1) y dado que $c_j \in K$, entonces $\delta c_j \in K$, para todo $j = 0, \dots, n-1$.

Debemos probar que $\delta c_j \in R$. Sean N la cerradura normal de L/K , A' la cerradura entera de R en N y $\sigma_1, \dots, \sigma_n$ los K -monomorfismos de L en N , entonces los conjugados de y son $\sigma_1(y) = y_1, \dots, \sigma_n(y) = y_n$ y pertenecen a A .

Aplicando σ_i en la Ecuación 2.4 obtenemos

$$y_i = \sum_{j=0}^{n-1} c_j \alpha_i^j,$$

con $\alpha_i = \sigma_i(\alpha)$. Entonces c_0, \dots, c_{n-1} pueden ser considerados como soluciones del sistema

$$y_i = \sum_{j=0}^{n-1} \alpha_i^j x_j, \quad \text{con } i = 0, \dots, n-1. \quad (2.5)$$

El determinante del Sistema 2.5 es

$$D = \det(\alpha_i^j) = \begin{vmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & & \vdots \\ \alpha_1^{n-1} & \cdots & \alpha_n^{n-1} \end{vmatrix} = \prod_{i < j} (\alpha_i - \alpha_j),$$

el cual es un determinante de Vandermonde y $D^2 = \delta$.

Por la Regla de Cramer tenemos que $Dc_j = \det(A_j)$, en donde A_j es la matriz de coeficientes obtenida al reemplazar la columna j -ésima por las variables y_1, \dots, y_n . Así $Dc_j = \det(A_j) \in A'$, lo que implica que $D^2c_j \in A'$ y, dado que $D^2c_j \in K$, entonces $\delta c_j = D^2c_j \in K \cap A' = R$. \square

Corolario 2.2.5. [3, Corolario 9] *Si K es un campo numérico, \mathcal{O}_K el anillo de enteros en K , entonces \mathcal{O}_K es un \mathbb{Z} -módulo libre de rango $[K : \mathbb{Q}]$.*

Demostración. Por el Teorema 2.2.11 y dado que \mathbb{Z} es un dominio de ideales principales, el resultado se sigue tomando $R = \mathbb{Z}$, $K = \mathbb{Q}$ y $L = K$. \square

Proposición 2.2.1. [3, Corolario 10] *Si K es un campo numérico, \mathcal{O}_K es el anillo de enteros de K , entonces:*

- (i) *el anillo \mathcal{O}_K es íntegramente cerrado y noetheriano,*
- (ii) *todo ideal primo en \mathcal{O}_K es maximal.*

Demostración.

(i) Sea $\alpha \in K$ entero sobre \mathcal{O}_K . Entonces existe $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathcal{O}_K[x]$ tal que $f(\alpha) = 0$, por lo que α es entero sobre $\mathbb{Z}[a_0, \dots, a_{n-1}]$. Por el Teorema 2.1.2, $\mathbb{Z}[a_0, \dots, a_{n-1}, \alpha]$ es finitamente generado como $\mathbb{Z}[a_0, \dots, a_{n-1}]$ -módulo. Como $a_i \in \mathcal{O}_K$, para $i = 0, \dots, n-1$, entonces, por el Teorema 2.1.3, $\mathbb{Z}[a_0, \dots, a_{n-1}]$ es finitamente generado como \mathbb{Z} -módulo y por el Teorema 2.1.4 $\mathbb{Z}[a_0, \dots, a_{n-1}, \alpha]$ también es entero sobre \mathbb{Z} . Luego, $\mathbb{Z}[\alpha]$ es un \mathbb{Z} -módulo finitamente generado y por ende, α es entero.

Luego, \mathcal{O}_K es noetheriano y esto se sigue del hecho de que \mathcal{O}_K es un \mathbb{Z} -módulo libre de rango $[K : \mathbb{Q}]$ y de que \mathbb{Z} es dominio de ideales principales.

(ii) Sea \mathfrak{p} un ideal primo no cero de \mathcal{O}_K , entonces existe un número primo $p \in \mathbb{Z}$ tal que $\mathfrak{p} \cap \mathbb{Z} = (p)$. Como (p) es maximal, entonces \mathfrak{p} también lo es. \square

Mostraremos otras formas útiles para caracterizar a los dominios Dedekind, para esto necesitaremos los siguientes lemas.

Lema 2.2.1. [9, Lema 3.17] *Si R un dominio entero, entonces*

$$R = \bigcap_{\mathfrak{M} \text{ maximal}} R_{\mathfrak{M}},$$

donde la intersección es tomada sobre todos los ideales maximales de R .

Demostración. Pongamos $R_1 = \bigcap_{\mathfrak{M} \text{ maximal}} R_{\mathfrak{M}}$. Como $R \hookrightarrow R_{\mathfrak{M}}$ para todo \mathfrak{M} ideal maximal de R , podemos considerar que $R \subseteq R_1$.

Sea $x \in R_1$, entonces $x = \frac{a}{b}$. Consideremos

$$\mathfrak{A} = \{y \in R : ya \in Rb\}.$$

Se verifica que \mathfrak{A} es un ideal de R . Ahora, para todo ideal maximal \mathfrak{M} de R tenemos que $x = \frac{a}{b} = \frac{r}{s}$, con $r \in R$ y $s \notin \mathfrak{M}$. Luego, como $sa = rb$, entonces $s \in \mathfrak{A}$. Por tanto, para todo \mathfrak{M} maximal, \mathfrak{A} no está contenido en \mathfrak{M} y de esto $\mathfrak{A} = R$. Así $Ra \subseteq Rb$, $a = bt$ y $x = \frac{a}{b} = \frac{bt}{b} = t \in R$. \square

Lema 2.2.2. [3, Teorema 20] *Si K es un campo y $\{R_i\}_{i \in \Omega}$ es una familia de subanillos de K íntegramente cerrados, con Ω un conjunto de índices, entonces $\bigcap_{i \in \Omega} R_i$ es íntegramente cerrado.*

Demostración. Sean $A = \bigcap_{i \in \Omega} R_i$, L el campo de cocientes de A y K_i el campo de cocientes de cada R_i , entonces $L \subseteq \bigcap_{i \in \Omega} K_i$. Sea $a \in L$ entero sobre A , entonces $a \in \bigcap_{i \in \Omega} K_i$ y por tanto es entero sobre cada R_i . Como cada R_i es íntegramente cerrado, $a \in R_i$ para todo $i \in \Omega$, como se quería. \square

Lema 2.2.3. [9, Lema 3.19] *Si R es un dominio entero, \mathfrak{A} y \mathfrak{B} son dos ideales de R , entonces $\mathfrak{A} = \mathfrak{B}$ si y sólo si $\mathfrak{A}R_{\mathfrak{M}} = \mathfrak{B}R_{\mathfrak{M}}$ para todo ideal maximal \mathfrak{M} de R .*

Demostración. Si $\mathfrak{A} = \mathfrak{B}$, entonces $\mathfrak{A}R_{\mathfrak{M}} = \mathfrak{B}R_{\mathfrak{M}}$. Supongamos que $\mathfrak{A}R_{\mathfrak{M}} = \mathfrak{B}R_{\mathfrak{M}}$ y sea $b \in \mathfrak{B}$, entonces para todo ideal maximal \mathfrak{M} de R tenemos que $b \in \mathfrak{A}R_{\mathfrak{M}}$. De esto $b = \frac{a}{c}$ con $a \in \mathfrak{A}$ y $c \notin \mathfrak{M}$. Consideremos $\mathfrak{C} = \{r \in R : br \in \mathfrak{A}\}$. Se verifica que \mathfrak{C} es un ideal de R y, como $c \in \mathfrak{C}$, entonces \mathfrak{C} no está contenido en \mathfrak{M} , por tanto $\mathfrak{C} = R$. De esto, $b \cdot 1 = b \in \mathfrak{A}$. Análogamente se prueba que $\mathfrak{A} \subseteq \mathfrak{B}$. \square

Teorema 2.2.12. [3, Teorema 20] *Sea R un dominio entero el cual no es campo. Entonces las siguientes condiciones son equivalentes.*

- (i) *El dominio R es Dedekind.*
- (ii) *Para cada ideal maximal \mathfrak{M} de R , $R_{\mathfrak{M}}$ es de valuación discreta y para todo $a \in R \setminus \{0\}$, a está contenido solamente en un número finito de ideales primos.*
- (iii) *El dominio R es íntegramente cerrado, noetheriano y cada ideal primo no cero es maximal.*

Demostración.

(i) \Rightarrow (ii) Como todo ideal maximal es primo, entonces por definición de R , $R_{\mathfrak{M}}$ es de valuación discreta. En el Corolario 2.2.3, ya probamos que todo ideal no cero está contenido en una cantidad finita de ideales primos, en particular tenemos el resultado para el ideal generado por a .

(ii) \Rightarrow (iii) Mostremos primero que todo ideal primo no cero es maximal. Para esto, sean \mathfrak{p} un ideal primo no cero y \mathfrak{M} un ideal maximal tal que \mathfrak{p} está contenido en \mathfrak{M} . Como $\mathfrak{p}R_{\mathfrak{M}}$ es un ideal primo en $R_{\mathfrak{M}}$ y $R_{\mathfrak{M}}$ es de valuación discreta, necesariamente $\mathfrak{p}R_{\mathfrak{M}} = \mathfrak{M}R_{\mathfrak{M}}$. Luego, por el Teorema 1.5.2 (página 14), $\mathfrak{p} = \mathfrak{M}$.

Probemos ahora que R es íntegramente cerrado. Por la Observación 2.2.2, para todo ideal maximal \mathfrak{M} , $R_{\mathfrak{M}}$ es íntegramente cerrado. Por el Lema 2.2.1, $R = \bigcap R_{\mathfrak{M}}$, donde la intersección se toma sobre todos los ideales maximales de R y, por el Lema 2.2.2, el resultado se tiene, es decir, R es íntegramente cerrado. Falta probar que R es noetheriano, para esto sean \mathfrak{A} un ideal no cero de R , $a \in \mathfrak{A} \setminus \{0\}$ y $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ los únicos ideales primos que contienen a

a. Por hipótesis, $R_{\mathfrak{p}_i}$ es de valuación discreta, entonces para todo $i = 1, \dots, r$, $\mathfrak{A}R_{\mathfrak{p}_i}$ es principal, es decir, $\mathfrak{A}R_{\mathfrak{p}_i} = xR_{\mathfrak{p}_i}$, con $x = \frac{c_i}{t_i}$, $c_i \in \mathfrak{A}$. Observemos que $xR_{\mathfrak{p}_i} = c_iR_{\mathfrak{p}_i}$, por lo que desde un principio podemos suponer que $\mathfrak{A}R_{\mathfrak{p}_i} = c_iR_{\mathfrak{p}_i}$. Sea $\mathfrak{B} = (a, c_1, \dots, c_r) \subseteq \mathfrak{A}$. Sea \mathfrak{M} un ideal maximal de R tal que $\mathfrak{M} \neq \mathfrak{p}_i$, entonces para toda $i = 1, \dots, r$ se tiene que $\frac{1}{a} \in R_{\mathfrak{M}}$, pues $a \notin \mathfrak{M}$, lo que implica $\mathfrak{B}R_{\mathfrak{M}} = \mathfrak{A}R_{\mathfrak{M}} = R_{\mathfrak{M}}$. Ahora, si $\mathfrak{M} = \mathfrak{p}_i$, obtenemos

$$\mathfrak{A}R_{\mathfrak{p}_i} = c_iR_{\mathfrak{p}_i} \subseteq \mathfrak{B}R_{\mathfrak{p}_i} \subseteq \mathfrak{A}R_{\mathfrak{p}_i}.$$

Así $\mathfrak{A}R_{\mathfrak{p}_i} = \mathfrak{B}R_{\mathfrak{p}_i}$. Luego, por el Lema 2.2.3, $\mathfrak{A} = \mathfrak{B}$, es decir, \mathfrak{A} es finitamente generado y por tanto R es noetheriano.

(iii) \Rightarrow (i) Por hipótesis R es noetheriano, falta mostrar que para todo ideal primo $\mathfrak{p} \neq 0$, $R_{\mathfrak{p}}$ es de valuación discreta. Para esto, sea \mathfrak{p} ideal primo no cero de R , entonces como R es noetheriano, $R_{\mathfrak{p}}$ es noetheriano y como R es íntegramente cerrado, $R_{\mathfrak{p}}$ también es íntegramente cerrado, además tiene un único ideal primo no cero, pues \mathfrak{p} es maximal. Luego, por el Teorema 2.2.3, página 25, $R_{\mathfrak{p}}$ es de valuación discreta. \square

Corolario 2.2.6. [3, Corolarios 9 y 11] *Si K es un campo numérico, entonces \mathcal{O}_K , el anillo de enteros de K , es un dominio Dedekind, más aún, es un \mathbb{Z} -módulo libre de rango $[K : \mathbb{Q}]$.*

Demostración. En la Proposición 2.2.1 mostramos que \mathcal{O}_K satisface la condición (iii) del Teorema 2.2.12, por consiguiente \mathcal{O}_K es un dominio Dedekind. \square

Teorema 2.2.13. [9, Teorema 6.1] *Si R un dominio Dedekind, K su campo de cocientes, L una extensión finita y separable de K y R' la cerradura entera de R en L , entonces R' es Dedekind.*

Demostración. La prueba de este teorema la podemos encontrar en la referencia citada, en ésta se muestra que R' satisface la condición (iii) del Teorema 2.2.12. \square

2.3. Discriminante

El discriminante de un campo numérico es muy importante, ya que está estrechamente relacionado con el concepto de base entera desde su definición.

En los siguientes resultados encontramos ciertas relaciones entre discriminantes de subcampos de un campo y el del propio campo, es por eso que los consideramos de gran utilidad para encontrar, por ejemplo, bases enteras en extensiones de la forma $K = \mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_m]{a_m})$, para algunos a_i enteros y n_i naturales.

Definición 2.3.1. Sean R un dominio Dedekind, K su campo de cocientes, L/K una extensión de grado n y separable, R' la cerradura entera de R en L y $\{\alpha_1, \dots, \alpha_n\} \subseteq L$. Se define el discriminante de $\{\alpha_1, \dots, \alpha_n\}$ como

$$\Delta(\alpha_1, \dots, \alpha_n) = \det(T_{L/K}(\alpha_i \alpha_j)).$$

Observación 2.3.1. [10, Corolario 3.20] Si $\{\alpha_1, \dots, \alpha_n\} \subseteq R'$, entonces $\Delta(\alpha_1, \dots, \alpha_n) \in R$.

Demostración. Por la Observación 2.1.3, página 22, y dado que $\alpha_i \in R'$, para cada $i = 1, \dots, n$, tenemos que $\alpha_i \alpha_j \in R'$ y esto implica que $T_{L/K}(\alpha_i \alpha_j) \in R$. Luego, $\det(T_{L/K}(\alpha_i \alpha_j)) = \Delta(\alpha_1, \dots, \alpha_n) \in R$. \square

Ahora, sean $R = \mathbb{Z}$, $K = \mathbb{Q}$ y L un campo numérico, R' el anillo de enteros de L ($R' = \mathcal{O}_L$). Por el Corolario 2.2.6, \mathcal{O}_L es un \mathbb{Z} -módulo libre de rango $n = [L : K]$. Sean $\{\alpha_1, \dots, \alpha_n\}$ y $\{\beta_1, \dots, \beta_n\}$ \mathbb{Z} -bases de \mathcal{O}_L , entonces

$$\alpha_j = \sum_{i=1}^n a_{ij} \beta_i, \quad \text{con } a_{ij} \in \mathbb{Z} \quad \text{y} \quad \det(a_{ij}) = \pm 1,$$

de esto

$$\Delta(\alpha_1, \dots, \alpha_n) = \det(T_{L/K}(\alpha_i \alpha_j)) = \det(a_{ij})^2 \Delta(\beta_1, \dots, \beta_n).$$

De lo anterior se concluye:

$$\Delta(\alpha_1, \dots, \alpha_n) = \Delta(\beta_1, \dots, \beta_n).$$

Observación 2.3.2. [5, Teorema 1] Sean $K = \mathbb{Q}(\theta)$, con $\theta \in \mathcal{O}_K$, y $f(x) = x^n - a$ el polinomio mínimo de θ . Entonces $\Delta(1, \theta, \dots, \theta^{n-1}) = (-1)^{\binom{n}{2}} n^n a^{n-1}$.

Demostración. La demostración de esta observación la podemos encontrar en la referencia dada. \square

Definición 2.3.2. Se define el discriminante de \mathcal{O}_L (o de L) y se denota $\delta_L = \Delta(\alpha_1, \dots, \alpha_n)$, en donde $\{\alpha_1, \dots, \alpha_n\}$ es una \mathbb{Z} -base de \mathcal{O}_L .

Definición 2.3.3. Sean R un dominio Dedekind, K su campo de cocientes, L/K una extensión finita y separable de grado n y R' la cerradura entera de R en L . El ideal discriminante de R' en R , denotado $\Delta_{L/K}$, es el ideal de R generado por los elementos $\Delta(\alpha_1, \dots, \alpha_n)$, donde $\{\alpha_1, \dots, \alpha_n\} \subseteq R'$ es una base de L/K .

Teorema 2.3.1. [3, Teorema 33] Si R' es un R -módulo libre con base $\{\alpha_1, \dots, \alpha_n\}$ y es como en la Definición 2.3.3, entonces $\Delta_{L/K} = \Delta_L = R\Delta(\alpha_1, \dots, \alpha_n)$.

Demostración. Como $\{\alpha_1, \dots, \alpha_n\}$ es una base de R' sobre R , entonces es linealmente independiente sobre K y esto implica que $\Delta(\alpha_1, \dots, \alpha_n) \in \Delta_L$. Ahora, si consideramos $\beta_1, \dots, \beta_n \in R'$, donde $\{\beta_1, \dots, \beta_n\}$ es una base de L sobre K , para cada $i = 1, \dots, n$, tenemos que existen $a_{ij} \in R$ tales que $\beta_i = \sum_{j=1}^n a_{ij}\alpha_j$. Al definir la matriz $A = (a_{ij})$ y realizando los cálculos correspondientes obtenemos

$$\Delta(\beta_1, \dots, \beta_n) = (\det(A))^2 \Delta(\alpha_1, \dots, \alpha_n),$$

de esto concluimos que $\Delta(\beta_1, \dots, \beta_n) \in R\Delta(\alpha_1, \dots, \alpha_n)$. \square

Proposición 2.3.1. [13, Corolario 1, pág. 150] Si $\mathbb{Q} \subset K \subset L$, entonces el discriminante $\Delta_{L/\mathbb{Q}}$ es dividido por $\Delta_{K/\mathbb{Q}}^{[L:K]}$.

Demostración. Esta demostración puede ser consultada en la referencia mencionada. \square

Proposición 2.3.2. [13, Proposición 4.25] Sean K un campo numérico, K_1 y K_2 dos extensiones finitas de K . Si $L = K_1K_2$, entonces el conjunto de ideales primos que dividen a Δ_L y $\Delta_{K_1}\Delta_{K_2}$ coinciden.

Demostración. La demostración de este resultado se encuentra en la referencia citada. \square

Las Proposiciones 2.3.1, 2.3.2 y todas las siguientes donde hacemos referencia a alguna propiedad de los ideales discriminante, también se pueden aplicar a los discriminantes del campo.

Teorema 2.3.2. [13, Teorema 4.26] Para $i = 1, 2$ sean K_i/\mathbb{Q} extensiones finitas de grado n_i con ideal discriminante Δ_i , y supongamos que $\text{mcd}(\Delta_{L_1}, \Delta_{L_2}) = 1$. Entonces el grado de la extensión $K = K_1K_2$ es n_1n_2 y

$$\Delta_K = \Delta_{K_1}^{n_2} \Delta_{K_2}^{n_1}.$$

Adicionalmente, si $\{\omega_1, \dots, \omega_{n_1}\}$ y $\{\alpha_1, \dots, \alpha_{n_2}\}$ son bases enteras de K_1 y K_2 , respectivamente, entonces $\{\omega_i \alpha_j\}$ es base entera de K .

Demostración. La demostración puede ser consultada en la referencia dada. \square

Corolario 2.3.1. [13, Corolario, pág.160] Para $i = 1, 2, \dots, r$ sean K_i/\mathbb{Q} extensiones finitas de grado n_i y sean $\{\alpha_{ij}\}$ bases enteras de cada K_i . Si para $i \neq j$ tenemos $\text{mcd}(\Delta_{K_i}, \Delta_{K_j}) = 1$, entonces el ideal discriminante de $K = K_1 K_2 \cdots K_r$ es igual a

$$\prod_{i=1}^r \Delta_{K_i}^{\frac{n}{n_i}},$$

con $n = n_1 n_2 \cdots n_r$ y una base entera es formada por el producto de los elementos de las bases enteras $\{\alpha_{ij}\}$.

Demostración. El resultado se sigue del Teorema 2.3.2 usando inducción sobre r . \square

Tanto los enunciados, como las demostraciones de las siguientes proposiciones las podemos encontrar en [15, páginas 272 y 274]. Se está considerando $f(x) = x^p - a \in \mathbb{Z}[x]$, donde p es un primo distinto de 2, a un entero libre de cuadrado tal que $\text{mcd}(a, p) = 1$ y $K = \mathbb{Q}(\sqrt[p]{a})$.

Proposición 2.3.3. El ideal discriminante de K es $\Delta_K = \mathbb{Z}p^{p-2j}a^{p-1}$, con $2j < p$.

Demostración. La demostración de esta proposición se encuentra en la referencia mencionada. \square

Proposición 2.3.4. Sea j como en la Proposición 2.3.3, entonces las siguientes condiciones son equivalentes:

- (i) el anillo \mathcal{O}_K tiene una base de potencias, más aún, $\mathcal{O}_K = \mathbb{Z}[\sqrt[p]{a}]$,
- (ii) se cumple que $a^{p-1} \not\equiv 1 \pmod{p^2}$ y $j = 0$.

2.4. Norma de ideales

Más adelante mostraremos que el número de clase de un campo numérico es finito, y esto lo haremos utilizando la cota de Minkowski la cual involucra la norma de un ideal.

Definición 2.4.1. Sean R un dominio Dedekind, K su campo de cocientes, L/K una extensión finita y separable, R' la cerradura entera de R en L y $N_{L/K}$ la norma de L en K . Dado un ideal I de R' , se define la norma de I como

$$\mathcal{N}(I) := \langle N_{L/K}(a) : a \in I \rangle,$$

esto es, el ideal generado por $N_{L/K}(a)$, $a \in I$.

Teorema 2.4.1. [3, Teorema 37] Con las condiciones de la Definición 2.4.1 se tiene:

(i) $\mathcal{N}(aR') = N_{L/K}(a)R$.

(ii) Si $S \subseteq R$ es un conjunto multiplicativamente cerrado, entonces $\mathcal{N}(I)_S = \mathcal{N}(I_S)$, con I ideal de R' .

(iii) $\mathcal{N}(IJ) = \mathcal{N}(I)\mathcal{N}(J)$.

Demostración.

(i) Observemos primero que $\mathcal{N}(R') = R$, pues $N_{L/K}(1) = 1$.

Ahora, como $a \in aR'$, entonces $N_{L/K}(a)R \subseteq \mathcal{N}(aR')$. La otra inclusión se tiene de la definición de $\mathcal{N}(aR')$.

(ii) Sea $x = \frac{a}{s} \in I_S$, entonces $N_{L/K}(x) = \frac{N_{L/K}(a)}{N_{L/K}(s)} = \frac{N_{L/K}(a)}{s^n}$, con $n = [L : K]$, por lo que $\mathcal{N}(I_S) \subseteq \mathcal{N}(I)_S$.

Mostremos ahora la otra inclusión. Sea $\frac{b}{s} \in \mathcal{N}(I)_S$, dado que $b \in \mathcal{N}(I)$, tenemos que $\frac{b}{s} = \frac{r_1 N_{L/K}(b_1) + \cdots + r_m N_{L/K}(b_m)}{s}$, con $b_i \in I$ y $r_i \in R$. Así

$$\begin{aligned} \frac{b}{s} &= \frac{r_1 N_{L/K}(b_1) + \cdots + r_m N_{L/K}(b_m)}{s} \\ &= r_1 s^{n-1} N_{L/K}\left(\frac{b_1}{s}\right) + \cdots + r_m s^{n-1} N_{L/K}\left(\frac{b_m}{s}\right) \in \mathcal{N}(I_S), \end{aligned}$$

de donde la igualdad se tiene.

(iii) La idea para demostrar este punto es utilizar el Lema 2.2.3, página 35. La demostración completa puede ser consultada en [3, Teorema 37]. \square

Ahora, notemos que si ponemos $R = \mathbb{Z}$, $K = \mathbb{Q}$ y L un campo numérico, entonces $\mathcal{N}(I) = m\mathbb{Z}$, con $m > 0$, $I \neq (0)$. De esto tenemos la siguiente definición.

Definición 2.4.2. *Se define la norma absoluta de I como m y si no hay confusión se denotará también por $\mathcal{N}(I) = m$.*

2.5. Grupo de clase

En repetidas ocasiones mencionamos que en anillos Dedekind se cumple un resultado análogo al Teorema Fundamental de la Aritmética. Expondremos la manera de conseguir dicho resultado, es decir, mostraremos que los ideales fraccionarios de un dominio Dedekind se representan de manera única como producto de ideales primos con exponentes enteros. A partir de lo anterior, definiremos el grupo y el número de clase de un dominio Dedekind y mostraremos que el número de clase es finito, mediante el Teorema de la cota de Minkowski.

Teorema 2.5.1. [9, Lema 4.1] *Si R es un dominio Dedekind y \mathfrak{p} es un ideal no cero de R , entonces \mathfrak{p} es invertible.*

Demostración. Sea $\mathfrak{p}^{-1} = \{x \in K : x\mathfrak{p} \subseteq R\}$. Se verifica que $\mathfrak{p}\mathfrak{p}^{-1}$ es un ideal de R . Sean $I = \mathfrak{p}\mathfrak{p}^{-1}$ y \mathfrak{M} un ideal máximo de R . Como R es Dedekind, entonces $R_{\mathfrak{M}}$ es un dominio de valuación discreta, particularmente es de ideales principales. Así $IR_{\mathfrak{M}} = \mathfrak{p}\mathfrak{p}^{-1}R_{\mathfrak{M}} = \mathfrak{p}R_{\mathfrak{M}}\mathfrak{p}^{-1}R_{\mathfrak{M}}$. Como $\mathfrak{p}R_{\mathfrak{M}}$ es principal, entonces es invertible y su inverso es $\mathfrak{p}^{-1}R_{\mathfrak{M}}$. Por tanto $IR_{\mathfrak{M}} = R_{\mathfrak{M}}$ y para todo ideal maximal \mathfrak{M} de R tenemos que $I \not\subseteq \mathfrak{M}$, lo que implica $I = \mathfrak{p}\mathfrak{p}^{-1} = R$. \square

El siguiente resultado es al que hemos hecho alusión en repetidas ocasiones, es decir, el resultado análogo al Teorema Fundamental de la Artimética en los ideales fraccionarios de un anillo Dedekind, el cual podremos aplicar a los anillos de enteros, pues ya mostramos que éstos son Dedekind.

Teorema 2.5.2. [9, Teorema 4.2] *Si R es un dominio Dedekind, entonces todo ideal fraccionario de R se representa de manera única como producto de ideales primos con exponentes enteros.*

Demostración. Sea M un ideal fraccionario, entonces existe $a \in R \setminus \{0\}$ tal que $aM \subseteq R$ es un ideal y por tanto $aM = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$, con \mathfrak{p}_i ideal primo de R para toda $i = 1, \dots, r$. También tenemos que $Ra = \mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_n^{b_n}$ con \mathfrak{q}_i ideales primos de R para toda $i = 1, \dots, n$. De esto

$$M = (Ra)^{-1}\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r} = \mathfrak{q}_1^{-b_1} \cdots \mathfrak{q}_n^{-b_n}\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}.$$

La unicidad se obtiene de la unicidad en la representación de ideales en dominios Dedekind. \square

Por el Teorema 2.5.2 el conjunto de los ideales fraccionarios en un dominio Dedekind forman un grupo libre abeliano generado por los ideales primos de R . Este grupo lo denotaremos por $I(R)$ y se llama el *grupo de ideales fraccionarios*.

Consideremos ahora a $P(R) = \{Rx : x \in K^*\}$. Se verifica que $P(R)$ es un subgrupo de $I(R)$ el cual es llamado *grupo de ideales fraccionarios principales*.

Definición 2.5.1. *El cociente*

$$C(R) = \frac{I(R)}{P(R)}$$

es llamado el *grupo de clase de R* . Si $C(R)$ es finito, se define el número de clase de R como $h_R = |C(R)|$.

Notemos que si R es de ideales principales, entonces todo ideal fraccionario de R es principal. De esto $I(R) = P(R)$ y $h_R = 1$, más aún, tenemos el siguiente resultado.

Observación 2.5.1. [9, pág. 19] *Si R es un dominio Dedekind, entonces R es un dominio de ideales principales si y sólo si $h_R = 1$.*

Introduciremos el concepto de red en \mathbb{R}^n , esto con el fin de mostrar que el número de clase de un campo numérico es finito.

Definición 2.5.2. *Una red en \mathbb{R}^n es un subgrupo $\mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_r$, con $\alpha_i \in \mathbb{R}^n$. Si $r = n$ la red se dice completa. Al grupo $\mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_r$ lo denotaremos por \mathfrak{L} .*

Definición 2.5.3. *Si \mathfrak{L} es una red completa, se define el paralelogramo fundamental T determinado por la base $\{\alpha_1, \dots, \alpha_n\}$ de \mathfrak{L} , como $T = \left\{ \sum_{i=1}^n r_i \alpha_i : 0 \leq r_i \leq 1 \right\}$.*

Teorema 2.5.3. (Teorema del cuerpo convexo de Minkowski [9, Teorema 12.3, pág 65]) *Sean \mathfrak{L} una red completa, $\Delta = \text{Vol}(T)$ el volumen del paralelogramo fundamental de \mathfrak{L} y $X \subseteq \mathbb{R}^n$ tal que para todo $x_1, x_2 \in X$ se tiene $\frac{x_1+x_2}{2} \in X$ y $\text{Vol}(X) > 2^n \Delta$. Entonces $X \cap (\mathfrak{L} \setminus \{0\}) \neq \emptyset$.*

Demostración. La demostración completa se encuentra en [9, Teorema 12.3, pág 65], sin embargo se basa en el siguiente hecho: si $Y \subseteq \mathbb{R}^n$ tiene volumen acotado y $(\lambda + Y) \cap (\mu + Y) = \emptyset$ para todo $\lambda, \mu \in \mathcal{L}$ distintos, entonces $Vol(T) \geq Vol(Y)$. \square

Todo polinomio de grado n con coeficientes racionales tiene n raíces en los complejos, de las cuales $r \geq 0$ son reales y las demás, que son un número par, son complejas. Si K es un campo numérico tal que $[K : \mathbb{Q}] = n$, por el teorema del elemento primitivo, sabemos que $K = \mathbb{Q}(\theta)$, y por tanto K posee n inmersiones en \mathbb{C} , r de las cuales son reales y $2s$ son complejas. A partir de esto escribiremos $n = r + 2s$, con r, s enteros no negativos.

Sean $\sigma_1, \dots, \sigma_n$ las n inmersiones de K en \mathbb{C} que dividiremos de la forma: $\sigma_1, \dots, \sigma_r$ tales que $\sigma_i(K) \subseteq \mathbb{R}$, con $i = 1, \dots, r$, y $\sigma_i(K) \not\subseteq \mathbb{R}$ para cada $i > r$. Así las podemos enumerar de tal manera que $\sigma_1, \dots, \sigma_r, \sigma_{r+1}, \dots, \sigma_{r+s}, \bar{\sigma}_{r+1}, \dots, \bar{\sigma}_{r+s}$ son todas las inmersiones de $K \in \mathbb{C}$.

Definamos $\varphi : K \rightarrow \mathbb{R}^r \times \mathbb{C}^s$ dada por

$$\varphi(\alpha) = (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \sigma_{r+1}(\alpha), \dots, \sigma_{r+s}(\alpha)).$$

Se verifica que φ es un monomorfismo de $(K, +)$ en $\mathbb{R}^r \times \mathbb{C}^s$, más aún, cumple el siguiente resultado.

Teorema 2.5.4. [3, Teorema 48] *Sea K un campo numérico de grado $n = r + 2s$. Si I es un ideal no cero de \mathcal{O}_K , entonces $\varphi(I)$ es una red completa en $\mathbb{R}^s \times \mathbb{C}^s \cong \mathbb{R}^n$.*

Demostración. La demostración completa de este Teorema se encuentra en [3, Teorema 48], sin embargo, la idea se basa en probar que si $\{\alpha_1, \dots, \alpha_n\}$ es una \mathbb{Z} -base de I , entonces $\{\varphi(\alpha_1), \dots, \varphi(\alpha_n)\}$ es \mathbb{R} -linealmente independiente. \square

Sea $T = \left\{ \sum_{i=1}^n r_i \varphi(\alpha_i) : 0 \leq r_i < 1 \right\}$. Se verifica que el volumen de T es igual al valor absoluto del determinante de la matriz que cambia la base canónica a $\{\varphi(\alpha_1), \dots, \varphi(\alpha_n)\}$ y es independiente de la base que se elija en $\varphi(I)$.

Corolario 2.5.1. [3, Corolario 19] *Sean I un ideal no cero de \mathcal{O}_K y Δ el discriminante de alguna base de I . Entonces el paralelogramo fundamental T de $\varphi(I)$ tiene volumen*

$$Vol(T) = \frac{\sqrt{|\Delta|}}{2^s}.$$

Demostración. Sea D como en el Teorema 2.5.4, entonces $\Delta(\alpha_1, \dots, \alpha_n) = (\det(D))^2 = (-2i)^{2s}(\det(M))^2$. Por tanto $\text{Vol}(T) = |\det(M)| = \frac{\sqrt{|\Delta|}}{2^s}$. \square

Definición 2.5.4. Si I es un ideal no cero de \mathcal{O}_K , se define el discriminante de I denotado por $\delta_I = \Delta(\alpha_1, \dots, \alpha_n)$, con $\{\alpha_1, \dots, \alpha_n\}$ base de I .

Teorema 2.5.5. [9, Proposición 13.4] Sean K un campo numérico, \mathcal{O}_K su anillo de enteros, I un ideal no cero de \mathcal{O}_K y δ_K el discriminante de K . Entonces $\delta_I = \mathcal{N}(I)^2 \delta_K$.

Demostración. La demostración de este teorema puede ser consultada en la referencia mencionada. \square

Corolario 2.5.2. [3, Corolario 20] Si I es un ideal no cero de \mathcal{O}_K y δ_K el discriminante de K , entonces el volumen del paralelogramo fundamental T de $\varphi(I)$ es

$$\text{Vol}(T) = 2^{-s} \mathcal{N}(I) \sqrt{|\delta_K|}.$$

Demostración. Aplique el Corolario 2.5.1 y el Teorema 2.5.5. \square

Proposición 2.5.1. [9, Proposición 12.4] Sean $n = r + 2s$, c_1, \dots, c_{r+s} y t números reales positivos, definamos

$$X_t = \{(x_1, \dots, x_r, y_1, z_1, \dots, y_s, z_s) \in \mathbb{R}^n : \sum_{i=1}^r |x_i| + 2 \sum_{j=1}^s \sqrt{y_j^2 + z_j^2} < t\},$$

entonces

$$\text{Vol}(X_t) = \frac{2^{r-s} \pi^s t^n}{n!}.$$

Demostración. La demostración de esta proposición puede ser encontrada en la referencia dada. \square

Teorema 2.5.6. [3, Teorema 50] Sea I un ideal no cero de \mathcal{O}_K . Entonces existe $a \in I \setminus \{0\}$ tal que $|N(a)| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \mathcal{N}(I) \sqrt{|\delta_K|}$.

Demostración. Considere el conjunto $X_t \subseteq \mathbb{R}^r \times \mathbb{C}^s$, con $X_t = \{(x_1, \dots, x_r, x_{r+1}, \dots, x_{r+s}) : \sum_{i=1}^r |x_i| + 2 \sum_{j=1}^s \|x_{r+j}\| < t\}$. Por la Proposición 2.5.1,

$Vol(X_t) = \frac{2^{r-s}\pi^s t^n}{n!}$. Queremos encontrar a t de tal manera que podamos aplicar el Teorema 2.5.3, es decir, se requiere que $Vol(X_t) = \frac{2^{r-s}\pi^s t^n}{n!} > 2^n Vol(T) = 2^{n-s}\mathcal{N}(I)\sqrt{|\delta_K|}$ o equivalentemente, $t^n > \frac{2^{n-r}n!\mathcal{N}(I)\sqrt{|\delta_K|}}{\pi^s}$. Dado $\epsilon > 0$, pongamos $t^n = \epsilon + 2^{n-r}n!\pi^{-s}\mathcal{N}(I)\sqrt{|\delta_K|}$. Por el Teorema 2.5.3 tenemos $(\varphi(I) \setminus \{0\}) \cap X_{t(\epsilon)} \neq \emptyset$, además la intersección es finita. Así, existe $a \in I \setminus \{0\}$ tal que

$$\varphi(a) = (\sigma_1(a), \dots, \sigma_r(a), \sigma_{r+1}(a), \dots, \sigma_{r+s}(a)) \in X_{t(\epsilon)}$$

Como $N(a) = \prod_{i=1}^{r+s} \sigma_i(a) = \prod_{i=1}^r \sigma_i(a) \prod_{j=r+1}^{r+s} \sigma_j(a)$, entonces $|N(a)| = \prod_{i=1}^r |\sigma_i(a)| \prod_{j=1}^s |\sigma_{r+j}(a)|^2$.

Usando la desigualdad entre la media geométrica y aritmética tenemos

$$n^n |N(a)| \leq \left[\sum_{i=1}^r |\sigma_i(a)| + 2 \sum_{j=1}^s |\sigma_{r+j}(a)| \right]^n < t^n.$$

Como $t^n = 2^{n-r}n!\pi^{-s}\mathcal{N}(I)\sqrt{|\delta_K|}$, entonces

$$|N(a)| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \mathcal{N}(I)\sqrt{|\delta_K|}.$$

□

Teorema 2.5.7. (Teorema de la cota de Minkowski [3, Teorema 51]) *Sea M un ideal fraccionario de \mathcal{O}_K , entonces existe un ideal entero I , es decir, un ideal de \mathcal{O}_K , tal que $I \in [M]$ y*

$$\mathcal{N}(I) \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\delta_K|}.$$

Demostración. Como M es ideal fraccionario, entonces M^{-1} también lo es, por tanto existe $a \neq 0$ tal que $aM^{-1} \subseteq R$ es un ideal entero. Sean $J = aM^{-1}$ y $m(K) = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\delta_K|}$. Como $aM^{-1}M = aR = JM$, tenemos que $[J] = [M^{-1}]$. Así, podemos suponer que M^{-1} es un ideal entero. Luego, por el Teorema 2.5.6, existe $b \in M^{-1}$ tal que $|N(b)| \leq \mathcal{N}(M^{-1})m(K)$, por lo que $|N(b)|\mathcal{N}(M) \leq m(K)$. Sea $I = bM$ ideal de \mathcal{O}_K , entonces

$$\mathcal{N}(I) = \mathcal{N}(b)\mathcal{N}(M) = |N(b)|\mathcal{N}(M) \leq m(K).$$

□

Teorema 2.5.8. (Finitud del grupo de clase [3, Teorema 52]) *Si K es un campo numérico con anillo de enteros R y $C_R = \frac{I(R)}{P(R)}$ es el grupo de clase de K , entonces $|C_R| < \infty$.*

Demostración. Sea $[M] \in C_R$, entonces por el Teorema 2.5.7 existe $I \in [M]$ ideal entero de R que representa a $[M]$ y $\mathcal{N}(I) \leq m(K)$. Como $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ con \mathfrak{p}_i ideales primos de R y para cada \mathfrak{p}_i existe un $p_i \in \mathbb{Z}$ tal que $(p_i) = \mathfrak{p}_i \cap \mathbb{Z}$, entonces

$$\mathcal{N}(I) = p_1^{f_1 e_1} \cdots p_r^{f_r e_r} \leq m(K). \quad (2.6)$$

Observemos que $m(K)$ no depende de M ni de I , por lo que existen un número finito de primos en \mathbb{Z} y exponentes e_i 's tales que cumplen la desigualdad 2.6, además sobre cada primo $p_i \in \mathbb{Z}$ hay un número finito de ideales primos en R y por tanto hay una cantidad finita de ideales primos en R y exponentes tales que $\mathcal{N}(I) \leq m(K)$. De lo anterior, podemos concluir que C_R tiene una cantidad finita de elementos, de lo contrario tendríamos que existen infinitos ideales de R con norma mayor que $m(K)$. □

CAPÍTULO 3

Bases enteras

En muchas ocasiones nos encontramos con resultados que garantizan la existencia de ciertos objetos matemáticos, sin embargo, sus demostraciones no muestran una manera de construirlos. Este es el caso de los resultados que involucran a las bases enteras ya que, en el Corolario 2.2.5, se demuestra su existencia, pero no una construcción, aunque hay resultados parciales. Por ejemplo, si consideramos una extensión de grado 2, se sabe con precisión cómo es una base entera [10, Proposición 2.34], es decir, si $K = \mathbb{Q}(\sqrt{d})$ con d entero libre de cuadrado, una base entera para K está dada por

$$\begin{cases} \{1, \sqrt{d}\}, & \text{si } d \equiv 2 \text{ o } 3 \pmod{4}, \\ \left\{1, \frac{1 + \sqrt{d}}{2}\right\}, & \text{si } d \equiv 1 \pmod{4}. \end{cases}$$

Ahora, para el campo ciclotómico $K = \mathbb{Q}(\zeta_m)$, donde m es un entero positivo y es ζ_m una raíz primitiva de $x^m - 1$, de acuerdo con [1, Teorema 7.5.1], una base entera para K es de la forma

$$\{1, \zeta_m, \dots, \zeta_m^{\phi(m)-1}\}.$$

Los dos ejemplos anteriores son bien conocidos, sin embargo, es natural preguntarse, ¿qué se ha dicho en el caso de extensiones de grado 3? En [1, Teorema 7.3.2] encontramos una respuesta a esta pregunta cuando $K = \mathbb{Q}(\sqrt[3]{m})$, con $m = ab^2$, a y b enteros libres de cuadrado y primos relativos. Para este

caso, una base entera está dada por

$$\begin{cases} \left\{ 1, \theta, \frac{\theta^2}{b} \right\}, & \text{si } m^2 \not\equiv 1 \pmod{9}, \\ \left\{ 1, \theta, \frac{b^2 \pm b^2\theta + \theta^2}{3b} \right\}, & \text{si } m \equiv \pm 1 \pmod{9}, \end{cases}$$

donde $\theta = \sqrt[3]{m}$.

En este capítulo discutimos, con suficiente detalle, el concepto de mínimo entero de grado i , pues en el Capítulo 5 propondremos ejemplos donde, por medio de los mínimos enteros, construiremos bases enteras. Además veremos que, gracias al uso de los discriminantes de algunos subcampos del campo a considerar, los cálculos necesarios para dicha construcción se simplifican.

Asimismo, obtuvimos algunas consecuencias del Teorema 2.3.2 y de las Proposiciones 2.3.3 y 2.3.4, es decir, bajo ciertas hipótesis sobre los a_i , n_i y los discriminantes de los subcampos de K , donde $K = \mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r})$, podemos construir bases enteras.

Definición 3.0.1. *Sea K un campo numérico. Una \mathbb{Z} -base para \mathcal{O}_K es llamada una base entera para K .*

Definición 3.0.2. *Sea K un campo numérico de grado n . Si existe un elemento $\theta \in \mathcal{O}_K$ tal que $\mathcal{O}_K = \mathbb{Z}[\theta]$ diremos que K es monogénico y al conjunto $\{1, \theta, \dots, \theta^{n-1}\}$ lo llamaremos base de potencias para K .*

3.1. Mínimos enteros

Una manera de obtener bases enteras es mediante la construcción de un conjunto de mínimos enteros de grado i . En esta sección presentamos este concepto que será de gran utilidad para mostrar ejemplos.

Las demostraciones que no presentamos en esta sección pueden ser encontradas en [1, Capítulo 7] y [12, Capítulo 4].

Consideremos un campo numérico K de grado n sobre \mathbb{Q} , entonces existe $\theta \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\theta)$. Sea $\{\alpha_1, \dots, \alpha_n\}$ una base entera de \mathcal{O}_K y, como θ es entero, existen $c_{ij} \in \mathbb{Z}$ tales que

$$\theta^{i-1} = \sum_{j=1}^n c_{ij} \alpha_j, \quad i = 1 \dots, n,$$

y en consecuencia

$$\Delta(1, \theta, \dots, \theta^{n-1}) = (\det(c_{ij}))^2 \Delta(\alpha_1, \dots, \alpha_n) = (\det(c_{ij}))^2 \delta_K.$$

Definición 3.1.1. Sea $m = |\det(c_{ij})|$, el entero positivo m es llamado el índice de θ y se denota por $\text{ind}(\theta)$.

Teorema 3.1.1. [12, Teorema 4.22] Si $\{\alpha_1, \dots, \alpha_n\}$ es un conjunto de generadores de un \mathbb{Z} -módulo libre N y M es un submódulo de N , entonces se cumplen las siguientes condiciones.

(i) Existen β_1, \dots, β_m , con $m \leq n$ tales que

$$M = \mathbb{Z}\beta_1 + \dots + \mathbb{Z}\beta_m$$

$$\text{y } \beta_i = \sum_{j \geq i}^n p_{ij} \alpha_j, \text{ con } 1 \leq i \leq n \text{ y } p_{ij} \in \mathbb{Z}.$$

(ii) Si $n = m$, entonces $[N : M] = p_{11} \cdots p_{nn}$.

Demostración. Esta demostración puede ser consultada en [12, Teorema 4.2.2]. \square

Observación 3.1.1. [12, Ejercicio 4.2.8] Se cumple que $\text{ind}(\theta) = [\mathcal{O}_K : \mathbb{Z}[\theta]]$.

Demostración. Se sigue del Teorema 3.1.1. \square

Observación 3.1.2. [1, Teorema 7.1.8] Sean K un campo numérico de grado n sobre \mathbb{Q} y $\theta \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\theta)$. Si $\Delta(1, \theta, \dots, \theta^{n-1})$ es libre de cuadrado, entonces $\{1, \theta, \dots, \theta^{n-1}\}$ es una base entera de \mathcal{O}_K .

Demostración. Por hipótesis $\Delta(1, \theta, \dots, \theta^{n-1})$ es libre de cuadrado y como $\Delta(1, \theta, \dots, \theta^{n-1}) = \text{ind}^2(\theta) \delta_K$, necesariamente se cumple que $\text{ind}(\theta) = 1$. \square

Proposición 3.1.1. [12, Ejemplo 4.3.1] Supongamos que el polinomio mínimo de θ es Eisenstein con respecto del primo p , entonces $p \nmid \text{ind}(\theta)$.

Demostración. La demostración de esta proposición se encuentra en la referencia citada. \square

El siguiente teorema es un resultado clásico en teoría de números y en ocasiones resulta útil en la construcción de bases enteras.

Teorema 3.1.2. [1, Teorema 7.1.14] *Si K es un campo numérico, entonces*

$$\delta_K \equiv 0 \text{ o } 1 \pmod{4}.$$

Demostración. Este resultado lo podemos encontrar en la referencia mencionada. \square

De aquí en adelante vamos a considerar un campo numérico K de grado $n \geq 3$ sobre \mathbb{Q} tal que $K = \mathbb{Q}(\theta)$, con $\theta \in \mathcal{O}_K$ y, para simplificar notación, escribiremos $\Delta(\theta)$ para referirnos a $\Delta(1, \theta, \dots, \theta^{n-1})$.

Para todo $\alpha \in \mathcal{O}_K$ existen $a_0, \dots, a_{n-1} \in \mathbb{Q}$ tales que

$$\alpha = a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}.$$

Si $i \in \{0, 1, \dots, n-1\}$ es tal que $a_i \neq 0$ y $a_{i+j} = 0$ para todo $j \geq 1$, entonces $\alpha = a_0 + a_1\theta + \dots + a_i\theta^i$ es llamado *entero de grado i en θ* .

Vamos a mostrar que los denominadores de los a_j son acotados. Por ejemplo, si $\{1, \theta, \dots, \theta^{n-1}\}$ es una base de potencias, entonces los denominadores son iguales a 1.

Teorema 3.1.3. [1, Teorema 7.2.1] *Si K es un campo numérico de grado n y $\omega_1, \dots, \omega_n \in \mathcal{O}_K$ son tales que $\Delta(\omega_1, \dots, \omega_n) \neq 0$, entonces para todo $\alpha \in \mathcal{O}_K$ existen únicos enteros racionales x_1, \dots, x_n tales que*

$$\alpha = \sum_{j=1}^n \frac{x_j}{\Delta(\omega_1, \dots, \omega_n)} \omega_j$$

y

$$\Delta(\omega_1, \dots, \omega_n) | x_j^2, \quad j = 1, 2, \dots, n.$$

Demostración. Como $\Delta(\omega_1, \dots, \omega_n) \neq 0$, entonces $\{\omega_1, \dots, \omega_n\}$ forma una \mathbb{Q} -base para K . Además, por la Observación 2.3.1, $\Delta(\omega_1, \dots, \omega_n) \in \mathbb{Z}$.

Por lo que, existen únicos $y_1, \dots, y_n \in \mathbb{Q}$ tales que

$$\alpha = \sum_{j=1}^n y_j \omega_j. \tag{3.1}$$

Sean $\sigma_1, \dots, \sigma_n$ las n \mathbb{Q} -inmersiones de K en una cerradura normal. Si aplicamos los n monomorfismos a la Ecuación 3.1 obtenemos un sistema de n ecuaciones lineales en las indeterminadas y_i , el cual es el siguiente

$$\sigma_r(\alpha) = \sum_{j=1}^n y_j \sigma_r(\omega_j), \quad r = 1, \dots, n. \tag{3.2}$$

Aplicando la regla de Cramer al Sistema 3.2 y elevando al cuadrado obtenemos que

$$y_j^2 \Delta(\omega_1, \dots, \omega_n) = \left| \begin{array}{ccccccc} \sigma_1(\omega_1) & \cdots & \sigma_1(\omega_{j-1}) & \sigma_1(\alpha) & \sigma_1(\omega_{j+1}) & \cdots & \sigma_1(\omega_n) \\ & & \cdots & & & & \cdots \\ \sigma_n(\omega_1) & \cdots & \sigma_n(\omega_{j-1}) & \sigma_n(\alpha) & \sigma_n(\omega_{j+1}) & \cdots & \sigma_n(\omega_n) \end{array} \right|^2.$$

La parte de la derecha, en la igualdad anterior, es un entero algebraico para $j = 1, \dots, n$ y, como $y_j^2 \Delta(\omega_1, \dots, \omega_n) \in \mathbb{Q}$, entonces $y_j^2 \Delta(\omega_1, \dots, \omega_n) \in \mathbb{Z}$.

Pongamos $y_j = \frac{r_j}{s_j}$, donde $r_j \in \mathbb{Z}$, $s_j \in \mathbb{N}$ y $\text{mcd}(r_j, s_j) = 1$. De esto

$$\frac{r_j^2}{s_j^2} \Delta(\omega_1, \dots, \omega_n) \in \mathbb{Z}, \quad j = 1, \dots, n.$$

Como $\text{mcd}(r_j, s_j) = 1$, tenemos que $s_j^2 | \Delta(\omega_1, \dots, \omega_n)$ para $j = 1, \dots, n$.

Sean $x_j = y_j \Delta(\omega_1, \dots, \omega_n) = \frac{r_j}{s_j} \Delta(\omega_1, \dots, \omega_n) \in \mathbb{Z}$, con $j = 1, \dots, n$.

Entonces, de la Ecuación 3.1, obtenemos

$$\alpha = \sum_{j=1}^n \frac{x_j}{\Delta(\omega_1, \dots, \omega_n)} \omega_j.$$

Dado que $s_j^2 | \Delta(\omega_1, \dots, \omega_n)$, concluimos que

$$\Delta(\omega_1, \dots, \omega_n) | x_j^2, \quad j = 1, 2, \dots, n.$$

La unicidad de los x_i se debe a que están unívocamente determinados por los y_i , los cuales son únicos. \square

Teorema 3.1.4. [1, Teorema 7.2.2] *Si $\alpha \in \mathcal{O}_K$, entonces existen únicos racionales $\frac{r_j}{s_j}$, con $\text{mcd}(r_j, s_j) = 1$ y $s_j > 0$ tales que*

$$\alpha = \sum_{j=1}^n \frac{r_j}{s_j} \theta^{j-1}$$

y

$$1 \leq s_j \leq |\Delta(\theta)|, \quad s_j^2 | \Delta(\theta).$$

Demostración. Dado que $\theta \in \mathcal{O}_K$, tenemos que $\Delta(\theta) \in \mathbb{Z}$. Además, como θ es un elemento primitivo, entonces $\Delta(\theta) \neq 0$.

Luego, por el Teorema 3.1.3, existen únicos enteros racionales x_1, \dots, x_n tales que

$$\alpha = \sum_{j=1}^n \frac{x_j}{\Delta(\theta)} \theta^{j-1}$$

y

$$\Delta(\theta) | x_j^2, \quad j = 1, \dots, n.$$

Para $j = 1, \dots, n$ definamos

$$r_j = \frac{\text{sgn}(\Delta(\theta))x_j}{\text{mcd}(x_j, \Delta(\theta))}, \quad s_j = \frac{|\Delta(\theta)|}{\text{mcd}(x_j, \Delta(\theta))}.$$

Observemos que $\text{mcd}(r_j, s_j) = 1$, $s_j > 0$,

$$\frac{r_j}{s_j} = \frac{x_j}{\Delta(\theta)}, \quad \alpha = \sum \frac{r_j}{s_j} \theta^{j-1}$$

y

$$1 \leq s_j \leq |\Delta(\theta)|.$$

También, para $j = 1, \dots, n$ tenemos

$$\frac{r_j^2}{s_j^2} \Delta(\theta) = \frac{x_j^2}{\Delta(\theta)} \in \mathbb{Z}$$

y, como $\text{mcd}(r_j, s_j) = 1$, entonces $s_j^2 | \Delta(\theta)$. □

Para cada $i = 0, 1, \dots, n - 1$, definamos el conjunto

$$S_i = \{a_i \in \mathbb{Q} | a_0 + a_1\theta + \dots + a_i\theta^i \in \mathcal{O}_K, \text{ para algunos } a_0, a_1, \dots, a_{i-1} \in \mathbb{Q}\}.$$

Observemos que $S_0 = \mathbb{Z}$ y $\mathbb{Z} \subseteq S_i$ para $i = 1, \dots, n - 1$. Además, por el Teorema 3.1.4, sabemos que los denominadores de los elementos en S_i son acotados. Por tanto, S_i tiene un elemento a_i^* positivo el cual es mínimo. Por ejemplo $a_0^* = 1$, pues $S_0 = \mathbb{Z}$.

Siguiendo con la notación anterior, obtenemos la siguiente definición.

Definición 3.1.2. *Todo entero algebraico α de K que es de la forma*

$$\alpha = a_0 + a_1\theta + \dots + a_{i-1}\theta^{i-1} + a_i^*\theta^i,$$

donde $a_0, a_1, \dots, a_{i-1} \in \mathbb{Q}$, es llamado un mínimo entero de grado i en θ .

Teorema 3.1.5. [1, Teorema 7.2.3] *Con la notación anterior, $S_i = a_i^* \mathbb{Z}$.*

Demostración. Como $a_i^* \in S_i$, entonces $a_i^* \mathbb{Z} \subseteq S_i$.

Mostremos la otra inclusión. Para esto sean $a \in S_i$ y m el menor entero positivo tal que $ma \in \mathbb{Z}$ y $a_i^* m \in \mathbb{N}$. Por el algoritmo de la división, existen $q, r \in \mathbb{Z}$ tales que

$$ma = a_i^* mq + r, \quad 0 \leq r < a_i^* m.$$

Ahora, como $a, a_i^* \in S_i$, existen $b_0, b_1, \dots, b_{i-1}, c_0, c_1, \dots, c_{i-1} \in \mathbb{Q}$ tales que

$$b_0 + b_1 \theta + \dots + b_{i-1} \theta^{i-1} + a \theta^i \in \mathcal{O}_K$$

y

$$c_0 + c_1 \theta + \dots + c_{i-1} \theta^{i-1} + a_i^* \theta^i \in \mathcal{O}_K.$$

Haciendo algunos cálculos utilizando las dos ecuaciones anteriores tenemos

$$(b_0 - qc_0) + (b_1 - qc_1) \theta + \dots + (b_{i-1} - qc_{i-1}) \theta^{i-1} + (a - qa_i^*) \theta^i \in \mathcal{O}_K,$$

y esto implica que $a - qa_i^* \in S_i$. Por otro lado, como $ma = a_i^* mq + r$, tenemos que $\frac{r}{m} = a - a_i^* q$, con $0 \leq \frac{r}{m} < a_i^*$. Lo cual contradice la elección de a_i^* . Así $\frac{r}{m} = 0$ y $a = a_i^* q$, como se quería. \square

Teorema 3.1.6. [1, Teorema 7.2.4] *Para $i = 0, 1, \dots, n-1$, se cumple que*

$$a_i^* = \frac{1}{d_i},$$

con d_i algún entero positivo.

Demostración. En la demostración de este teorema se argumenta por inducción y se hace uso del Teorema 3.1.5. Los detalles de la prueba pueden encontrarse en la referencia dada, sin embargo es importante mencionar que en el proceso de la demostración se obtiene que $a_{i-1}^* \in S_i$. \square

Teorema 3.1.7. [1, Teorema 7.2.5] *Para $i = 1, \dots, n-1$*

$$d_{i-1} | d_i.$$

Demostración. En el Teorema 3.1.6 se demuestra que $a_{i-1}^* \in S_i$. Dado que $S_i = a_i^* \mathbb{Z}$, entonces existe $m \in \mathbb{Z}$ tal que $a_{i-1}^* = ma_i^*$. Como $a_{i-1}^* = \frac{1}{d_{i-1}}$ y $a_i^* = \frac{1}{d_i}$, para algunos d_{i-1} y d_i enteros positivos, se sigue que $d_i = d_{i-1} m$. \square

Teorema 3.1.8. [1, Teorema 7.2.6] *Si α es un entero algebraico de grado i en θ , entonces existen $a_0, a_1, \dots, a_i \in \mathbb{Z}$ tales que*

$$\alpha = \frac{a_0 + a_1\theta + \dots + a_{i-1}\theta^{i-1} + a_i\theta^i}{d_i}.$$

En particular, si α es un mínimo entero de grado i en θ , entonces existen $a_0, a_1, \dots, a_{i-1} \in \mathbb{Z}$ tales que

$$\alpha = \frac{a_0 + a_1\theta + \dots + a_{i-1}\theta^{i-1} + \theta^i}{d_i}.$$

Demostración. Argumentemos usando inducción sobre $i \in \{0, 1, \dots, n-1\}$. Sea α un entero de grado 0 en θ . Entonces $\alpha = a_0 \in \mathbb{Z}$. Como $d_0 = 1$, entonces $\alpha = \frac{a_0}{d_0}$ y el enunciado es cierto para $i = 0$. Supongamos que el resultado se cumple para todos los enteros de grado hasta $j-1$ en θ , donde $j \in \{1, 2, \dots, n-1\}$. Sea α un entero de grado j en θ . De los Teoremas 3.1.5 y 3.1.6 tenemos que existen $r_0, r_1, \dots, r_{j-1} \in \mathbb{Q}$ y $a_j \in \mathbb{Z}$ tales que

$$\alpha = r_0 + r_1\theta + \dots + r_{j-1}\theta^{j-1} + \frac{a_j}{d_j}\theta^j.$$

Sea β un mínimo entero de grado $j-1$ en θ . Por hipótesis de inducción, existen $s_0, s_1, \dots, s_{j-2} \in \mathbb{Z}$ tales que

$$\beta = \frac{s_0 + s_1\theta + \dots + s_{j-2}\theta^{j-2} + \theta^{j-1}}{d_{j-1}}.$$

Como $d_{j-1} | d_j$, entonces

$$\frac{d_j}{d_{j-1}}\alpha - a_j\theta\beta = \frac{d_j}{d_{j-1}}r_0 + \sum_{l=1}^{j-1} \frac{d_j r_l - a_j s_{l-1}}{d_{j-1}} \theta^l$$

es un entero algebraico de grado $j-1$ en θ . Por hipótesis de inducción, existen $c_0, c_1, \dots, c_{j-1} \in \mathbb{Z}$ tales que

$$\frac{d_j}{d_{j-1}}r_0 + \sum_{l=1}^{j-1} \frac{d_j r_l - a_j s_{l-1}}{d_{j-1}} \theta^l = \sum_{l=0}^{j-1} \frac{c_l}{d_{j-1}} \theta^l.$$

Igualando coeficientes tenemos

$$r_0 = \frac{c_0}{d_j}, \quad r_l = \frac{c_l + a_j s_{l-1}}{d_j}, \quad l = 1, 2, \dots, j-1,$$

como se quería. \square

El siguiente resultado es importante para el desarrollo de este trabajo ya que, como hemos mencionado antes, mostraremos ejemplos de bases enteras usando el concepto de mínimos enteros y algunos discriminantes de subcampos del campo a considerar.

Teorema 3.1.9. [1, Teorema 7.2.7] *Para $i = 0, 1, \dots, n-1$ sea α_i un mínimo entero de grado i en θ . Entonces $\{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$ es una base entera para K .*

Demostración. Primero observemos que cualquier base entera para K debe tener al menos un elemento de la forma $a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}$ con $a_0, a_1, \dots, a_{n-1} \in \mathbb{Q}$ y $a_{n-1} \neq 0$, de lo contrario dicha base no podría representar al elemento θ^{n-1} . Sin pérdida de generalidad podemos suponer que $a_{n-1} > 0$ ya que, si es necesario, lo podemos cambiar por su negativo. Ahora, sea $\{\omega_1, \dots, \omega_n\}$ una base entera para K con

$$\omega_n = a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}$$

donde $a_{n-1} > 0$ y mínimo.

Sea $i \in \{1, 2, \dots, n-1\}$, entonces

$$\omega_i = b_0 + b_1\theta + \dots + b_{n-1}\theta^{n-1}, \quad b_0, b_1, \dots, b_{n-1} \in \mathbb{Q}.$$

Reemplazando a ω_i por su negativo, si es necesario, podemos suponer que $0 \leq b_{n-1}$. Sea m el único entero no negativo tal que

$$\frac{b_{n-1}}{a_{n-1}} - 1 < m \leq \frac{b_{n-1}}{a_{n-1}}.$$

Efectuando algunos cálculos llegamos a

$$0 \leq b_{n-1} - ma_{n-1} < a_{n-1}.$$

Si $b_{n-1} - ma_{n-1} \neq 0$, pongamos $\omega'_i = \omega_i - m\omega_n$. Consideremos al conjunto $\{\omega_1, \dots, \omega_{i-1}, \omega'_i, \omega_{i+1}, \dots, \omega_n\}$ el cual también forma una base entera para K , sin embargo, esto contradice la minimalidad de a_{n-1} . Así, $b_{n-1} - ma_{n-1} = 0$, es decir, b_{n-1} es un múltiplo entero de a_{n-1} . Por tanto, existen $m_1, \dots, m_{n-1} \in \mathbb{Z}$ tales que $\omega'_j = \omega_j - m_j\omega_n$ con $j = 1, \dots, n-1$ son enteros de grado a lo más $n-2$ en θ . Más aún, $\{\omega'_1, \dots, \omega'_{n-1}, \omega_n\}$ es

una base entera para K . Consideremos todas las bases enteras de la forma $\{\omega_1, \dots, \omega_{n-1}, \omega_n\}$ de tal forma que $\omega_1, \dots, \omega_{n-1}$ son enteros de grado a lo más $n-2$ en θ , elijamos una donde el coeficiente de θ^{n-2} es positivo y mínimo y continuemos la construcción hasta obtener una base entera $\{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$, donde cada α_i es de grado i en θ . Mostremos ahora que cada α_i es mínimo entero de grado i . Para esto, debido a que

$$\alpha_i = \sum_{j=0}^i a_{ij}\theta^j, \quad a_{ij} \in \mathbb{Q},$$

tenemos

$$\delta_K = \Delta(\alpha_0, \alpha_1, \dots, \alpha_{n-1}) = (a_{00}a_{11} \cdots a_{n-1n-1})^2 \Delta(\theta).$$

Ahora, para $i = 0, 1, \dots, n-1$ sea β_i un mínimo entero de grado i . De esto

$$\Delta(\beta_0, \dots, \beta_{n-1}) = (a_0^* a_1^* \cdots a_{n-1}^*)^2 \Delta(\theta).$$

Como $|\delta_K| \leq |\Delta(\beta_0, \dots, \beta_{n-1})|$, entonces

$$a_{00}a_{11} \cdots a_{n-1n-1} \leq a_0^* a_1^* \cdots a_{n-1}^*$$

y por tanto

$$\frac{a_{00}}{a_0^*} \cdot \frac{a_{11}}{a_1^*} \cdots \frac{a_{n-1n-1}}{a_{n-1}^*} \leq 1.$$

Finalmente, como $a_{ii} \in S_i$ para $i = 0, 1, \dots, n-1$, tenemos que $a_{ii} = a_i^* m_i$, con $m_i \in \mathbb{Z}$. De esto, cada $\frac{a_{ii}}{a_i^*}$ es un entero positivo, por lo que $a_{ii} = a_i^*$. \square

El siguiente teorema nos brinda información sobre los d_i , la cual será de gran utilidad para construir ejemplos de bases enteras.

Teorema 3.1.10. [1, Teorema 7.2.8] *Para $i = 0, 1, \dots, n-1$ sea*

$$\alpha_i = \frac{a_{i0} + a_{i1}\theta + \cdots + a_{ii-1}\theta^{i-1} + \theta^i}{d_i},$$

con $a_{i0}, \dots, a_{ii-1} \in \mathbb{Z}$, un mínimo entero de grado i en θ , de modo que $\alpha_0 = d_0 = 1$. Entonces

$$d_0 d_1 \cdots d_{n-1} = \text{ind}(\theta)$$

y

$$d_i^{2(n-i)} |\Delta(\theta)|, \quad i = 0, 1, \dots, n-1.$$

Demostración. Ya mostramos que $\{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$ es una base entera para K . Por tanto $\delta_K = \Delta(\alpha_0, \alpha_1, \dots, \alpha_{n-1})$. Como $\Delta(\theta) = \text{ind}^2(\theta)\delta_K$ y $\Delta(\theta) = (d_0d_1 \cdots d_{n-1})^2\Delta(\alpha_0, \alpha_1, \dots, \alpha_{n-1})$, entonces

$$\delta_K = \Delta(\alpha_0, \alpha_1, \dots, \alpha_{n-1}) = \frac{\Delta(\theta)}{(d_0d_1 \cdots d_{n-1})^2} = \frac{\text{ind}^2(\theta)\delta_K}{(d_0d_1 \cdots d_{n-1})^2}.$$

Dado que d_0, d_1, \dots, d_{n-1} e $\text{ind}(\theta)$ son entero positivos, tenemos que

$$d_0d_1 \cdots d_{n-1} = \text{ind}(\theta).$$

También

$$\frac{\Delta(\theta)}{(d_0d_1 \cdots d_{n-1})^2} = \delta_K \in \mathbb{Z},$$

lo que implica

$$(d_0d_1 \cdots d_{n-1})^2 | \Delta(\theta),$$

y, como $d_{i-1} | d_i$, entonces $d_i^{2(n-i)} | \Delta(\theta)$. □

Definición 3.1.3. *Al proceso de encontrar una base de elementos que son como en el Teorema 3.1.9 le llamaremos método de mínimos enteros.*

3.2. Bases enteras de extensiones radicales

Recordemos que uno de nuestros objetivos es poder construir bases enteras en extensiones radicales. Nosotros encontramos en el Teorema 2.3.2 y la Proposición 2.3.4, página 38, algunas condiciones que nos ayudan en gran medida a lograr este objetivo.

Comenzaremos con los resultados que nos fueron dando ideas para llegar al Teorema 3.2.1, el cual es el más importante de esta sección.

Definición 3.2.1. *Una extensión F/K se dice:*

- (i) *radical si existe $\alpha \in F$ $F = K(\alpha)$ y $\alpha^n \in K$ para algún $n \geq 1$,*
- (ii) *radical repetida si existe una sucesión de campos $K \subseteq K_1 \subseteq \cdots \subseteq K_r = F$, tales que K_i/K_{i-1} es radical para todo $i = 1, \dots, r$.*

El término de extensión radical, lo usaremos indistintamente para referirnos a una extensión radical o radical repetida.

Proposición 3.2.1. *Para $i = 1, \dots, r$, sean $K_i = \mathbb{Q}(\sqrt{a_i})$, con a_i enteros y libres de cuadrado. Si $\text{mcd}(a_i, a_j) = 1$, para $i \neq j$, y $a_i \equiv 2$ o $3 \pmod{4}$, para a lo más un i , entonces $\text{mcd}(\delta_{K_i}, \delta_{K_j}) = 1$.*

Demostración. Recordemos que el discriminante en extensiones de la forma $\mathbb{Q}(\sqrt{d})$ es: d , si $d \equiv 1 \pmod{4}$ o $4d$, si $d \equiv 2$ o $3 \pmod{4}$.

Para demostrar la proposición argumentemos por contradicción, es decir, supongamos que $a_i \equiv 2$ o $3 \pmod{4}$ y $a_j \equiv 2$ o $3 \pmod{4}$ con $i \neq j$. Como K_i y K_j tienen discriminantes $\delta_{K_i} = 4a_i$ y $\delta_{K_j} = 4a_j$, respectivamente, entonces $\text{mcd}(\delta_{K_i}, \delta_{K_j}) \neq 1$. Así, si $a_i \equiv 2$ o $3 \pmod{4}$ para a lo más un i , y el resultado se tiene ya que $\text{mcd}(a_i, a_j) = 1$ cuando $i \neq j$. \square

Proposición 3.2.2. *Para $i = 1, \dots, r$, sean K_i como el la Proposición 3.2.1. Si $K = K_1 \cdots K_r$, entonces K satisface las hipótesis del Corolario 2.3.1 (página 39) y una base entera para K es producto de bases enteras de sus subcampos K_i .*

Demostración. El resultado se tiene ya que los discriminates de cada K_i son primos relativos a pares. \square

Proposición 3.2.3. *Sean m y d enteros, $K_1 = \mathbb{Q}(\sqrt[3]{m})$, $K_2 = \mathbb{Q}(\sqrt{d})$, $K = K_1 K_2$, δ_{K_1} y δ_{K_2} los discriminantes de K_1 y K_2 , respectivamente. Adicionalmente, supongamos que $3 \nmid d$ y $\text{mcd}(m, d) = 1$. Si alguna de las condiciones*

$$(a) \ d \equiv 1 \pmod{4},$$

$$(b) \ d \equiv 2 \text{ o } 3 \pmod{4} \text{ y } 2 \nmid m,$$

se cumple, entonces $\text{mcd}(\delta_{K_1}, \delta_{K_2}) = 1$ y una base entera para K se obtiene mediante el producto de una base entera de K_1 con una base entera de K_2 .

Demostración. Sea $m = ab^2$, con a y b enteros, primos relativos y libres de cuadrado. En [1, Teorema 7.3.2] encontramos que

$$\delta_{K_1} = \begin{cases} -27a^2b^2, & \text{si } m^2 \not\equiv 1 \pmod{9}, \\ -3a^2b^2, & \text{si } m \equiv \pm 1 \pmod{9}. \end{cases}$$

Por otro lado, en [3, página 47] podemos encontrar que el discriminante de K_2 es

$$\delta_{K_2} = \begin{cases} 4d, & \text{si } d \equiv 2 \text{ o } 3 \pmod{4}, \\ d, & \text{si } d \equiv 1 \pmod{4}. \end{cases}$$

Supongamos que $d \equiv 1 \pmod{4}$, entonces $\delta_{K_1} = d$. Como $3 \nmid d$ y $\text{mcd}(m, d) = 1$ tenemos que $\text{mcd}(\delta_{K_1}, \delta_{K_2}) = 1$. Ahora, si $d \equiv 2$ o $3 \pmod{4}$ y $2 \nmid m$ de igual manera, por las hipótesis sobre d y m tenemos que $\text{mcd}(\delta_{K_1}, \delta_{K_2}) = 1$. Por tanto K satisface las condiciones del Teorema 2.3.2 y una base entera para K es formada por el producto de una base entera de K_1 y otra de K_2 . \square

Proposición 3.2.4. *Para cada $i = 1, \dots, r$, si $K_i = \mathbb{Q}(\sqrt[p]{a_i})$, con p un primo impar y a_i un entero libre de cuadrado tal que $p \nmid a_i$, entonces los discriminantes de cada K_i no son primos relativos a pares.*

Demostración. Por las Proposiciones 2.3.3 y 2.3.4, página 39, para todo $i = 1, \dots, r$ tenemos que $p \mid \delta_{K_i}$, entonces $p \mid \text{mcd}(\delta_{K_1}, \dots, \delta_{K_r})$. \square

Las Proposiciones 3.2.2, 3.2.3 y 3.2.4 nos permiten notar que, bajo ciertas condiciones, podemos obtener un resultado más general, es decir, para extensiones de la forma $K = \mathbb{Q}(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r})$. Para esto, introduciremos la siguiente definición con el fin de dar condiciones sobre los discriminantes de los subcampos de K de la forma $\mathbb{Q}(\sqrt[n]{a_i})$, para así poder aplicar el Corolario 2.3.1.

Definición 3.2.2. *Sean n un entero positivo y a un entero libre de cuadrado tales que $\text{mcd}(a, n) = 1$. Diremos que la pareja (a, n) es*

- *semi-impar si $n \equiv 1 \pmod{2}$ ó $n \equiv 2 \pmod{4}$ y $a \equiv 1 \pmod{4}$.*
- *semi-par si $n \equiv 0 \pmod{4}$ ó $n \equiv 2 \pmod{4}$ y $a \equiv 3 \pmod{4}$.*

Lema 3.2.1. *Sea $K = \mathbb{Q}(\sqrt[n]{a})$ con a entero libre de cuadrado. Si $\text{mcd}(a, n) = 1$ y $n = 2^{e_0} q_1^{e_1} \cdots q_r^{e_r}$, entonces*

$$\delta_K = \begin{cases} (-1)^{\binom{n}{2}} a^{n-1} q_1^{a_1} \cdots q_r^{a_r}, & \text{si } (a, n) \text{ es semi-impar,} \\ (-1)^{\binom{n}{2}} a^{n-1} 2^{a_0} q_1^{a_1} \cdots q_r^{a_r}, & \text{si } (a, n) \text{ es semi-par.} \end{cases}$$

Donde $1 \leq a_i \leq e_i$, para $i = 0, 1, \dots, r$.

Demostración. Pongamos $\theta = \sqrt[n]{a}$ y mostremos primero que $a^{n-1} \mid \delta_K$. De la ecuación

$$\Delta(\theta) = (-1)^{\binom{n}{2}} n^n a^{n-1} = \text{ind}^2(\theta) \delta_K \quad (3.3)$$

y, dado que el polinomio irreducible de θ es Eisenstein para cada divisor primo de a , tenemos, por la Proposición 3.1.1, página 49, que $a \nmid \text{ind}(\theta)$, lo que implica $a^{n-1} \mid \delta_K$.

También, observemos que para cada divisor primo de n , $\mathbb{Q}(\sqrt[q]{a}) \subseteq K$, con $q \in \{2, q_1, \dots, q_r\}$.

Supongamos primero que q es impar y mostremos que $q|\delta_K$ para todo $q \in \{q_1, \dots, q_r\}$. Por las Proposiciones 2.3.3 y 2.3.4, página 39, tenemos que el discriminante de $\mathbb{Q}(\sqrt[q]{a})$ es

$$\begin{cases} (-1)^{\binom{q}{2}} q^q a^{q-1}, & \text{si } a^{q-1} \not\equiv 1 \pmod{q^2}, \\ (-1)^{\binom{q}{2}} q^{q-2j} a^{q-1}, & \text{si } a^{q-1} \equiv 1 \pmod{q^2}, \end{cases}$$

con $2j < q$. En cualquier caso $q|\delta_{\mathbb{Q}(\sqrt[q]{a})}$ y como $\delta_{\mathbb{Q}(\sqrt[q]{a})}|\delta_K$, entonces $q|\delta_K$ para cada $q \in \{q_1, \dots, q_r\}$.

Hasta aquí, hemos mostrado que $a^{n-1} q_1^{a_1} \dots q_r^{a_r} |\delta_K$, con $1 \leq a_i \leq e_i$ para $i = 1, \dots, r$. Además si $(-1)^{\binom{n}{2}} = -1$, de la Ecuación 3.3, necesariamente $\delta_K < 0$.

Supongamos que (a, n) es semir-impar y estudiemos cada subcaso. Si $n \equiv 1 \pmod{2}$ notemos que, si $2|a$, entonces $2|\delta_K$. En caso de que $n \equiv 2 \pmod{4}$ y $a \equiv 1 \pmod{4}$, entonces $\delta_{\mathbb{Q}(\sqrt{a})} \subseteq K$, sin embargo, como $a \equiv 1 \pmod{4}$ y $\delta_K = a$, tenemos que $2 \nmid \delta_K$.

Ahora, si (a, n) es semir-par, de nuevo, veamos qué sucede en cada caso. Cuando $n \equiv 2 \pmod{4}$ y $a \equiv 3 \pmod{4}$, la situación es similar a la anterior, la diferencia es que $\delta_{\mathbb{Q}(\sqrt{a})} = 4a$ y por tanto $2|\delta_K$. Por último, si $n \equiv 0 \pmod{4}$, entonces $\mathbb{Q}(\sqrt[4]{a}) \subseteq K$ y en [6] encontramos que $2|\delta_{\mathbb{Q}(\sqrt[4]{a})}$, implicando que $2|\delta_K$. \square

Lema 3.2.2. *Sean a y b enteros libres de cuadrado, n y m naturales tales que el máximo común divisor a pares es 1 excepto $\text{mcd}(n, m) \leq 2$. Sean $K_1 = \mathbb{Q}(\sqrt[n]{a})$ y $K_2 = \mathbb{Q}(\sqrt[m]{b})$. Si a lo más una de las parejas (a, n) ó (b, m) es semi-par, entonces $\text{mcd}(\delta_{K_1}, \delta_{K_2}) = 1$.*

Demostración. Si (a, n) y (b, m) son semi-pares, entonces $2|\delta_{K_1}$ y $2|\delta_{K_2}$, en consecuencia $\text{mcd}(\delta_{K_1}, \delta_{K_2}) \neq 1$. Ahora, notemos que, por las hipótesis sobre a, b, n y m , este es el único caso donde 2 divide a los discriminantes de K_1 y K_2 , además es el único posible factor primo que puede dividir a ambos. Así, si a lo más una de las parejas (a, n) o (b, m) es semi-par, entonces $\text{mcd}(\delta_{K_1}, \delta_{K_2}) = 1$. \square

Teorema 3.2.1. *Sean a, b, n y m como en el Lema 3.2.2, $K_1 = \mathbb{Q}(\sqrt[n]{a})$ y $K_2 = \mathbb{Q}(\sqrt[m]{b})$. Si las parejas (a, n) y (b, m) satisfacen las hipótesis del Lema 3.2.2, entonces una base entera para $K = K_1 K_2$ es de la forma $\{\alpha_i \beta_j\}_{i \in I, j \in J}$,*

con $\{\alpha_i\}_{i \in I}$ y $\{\beta_j\}_{j \in J}$ bases de K_1 y K_2 , respectivamente, donde $I = \{1, \dots, n\}$ y $J = \{1, \dots, m\}$.

Demostración. Como K_1 y K_2 satisfacen las hipótesis del Teorema 2.3.2, página 38, el resultado se sigue. \square

Corolario 3.2.1. *Para $i = 1, \dots, r$, sean a_i y n_i enteros tales que a_i es libre de cuadrado, el máximo común divisor a pares es 1 excepto $\text{mcd}(n_i, n_j) \leq 2$, cuando $i \neq j$, y $K_i = \mathbb{Q}(\sqrt[n_i]{a_i})$. Si a lo más una de las parejas (a_i, n_i) es semi-par, entonces $\text{mcd}(\delta_{K_i}, \delta_{K_j}) = 1$ para cada $i \neq j$.*

Demostración. El resultado se sigue usando el mismo argumento del Lema 3.2.2. \square

Corolario 3.2.2. *Para $i = 1, \dots, r$, sean $a_i, n_i, K_i = \mathbb{Q}(\sqrt[n_i]{a_i})$ y (a_i, n_i) como en el Corolario 3.2.1. Entonces una base entera para $K = K_1 \cdots K_r$ puede ser obtenida del producto de bases enteras de cada K_i .*

Demostración. Por el Corolario 3.2.1 tenemos que K satisface las hipótesis del Corolario 2.3.1, página 39, y el resultado se sigue. \square

Por el Teorema 2.3.4, página 39, sabemos exactamente cuándo el anillo de enteros de $K = \mathbb{Q}(\sqrt[p]{a})$ es $\mathbb{Z}[\sqrt[p]{a}]$, bajo ciertas hipótesis sobre a y p . Por otro lado, si consideramos campos de la forma $L = \mathbb{Q}(\sqrt[n]{a})$, con n libre de cuadrado, entonces para cada divisor primo de n encontramos que L contiene campos como K . En el siguiente resultado damos ciertas condiciones para que el campo L , con $n = pq$, tenga una base de potencias.

Teorema 3.2.2. *Sean p y q primos distintos, a entero libre de cuadrado tal que $pq \nmid a$ y $K = \mathbb{Q}(\sqrt[pq]{a})$. Si $a^{q-1} \not\equiv 1 \pmod{q^2}$ y $a^{p-1} \not\equiv 1 \pmod{p^2}$, entonces K tiene una base de potencias.*

Demostración. Pongamos $\theta = \sqrt[pq]{a}$, entonces

$$\Delta(\theta) = (-1)^{\binom{qp}{2}} (qp)^{qp} a^{qp-1} = \text{ind}^2(\theta) \delta_K.$$

Vamos a mostrar que $\text{ind}(\theta) = 1$. Para esto, sean $K_1 = \mathbb{Q}(\sqrt[q]{a})$ y $K_2 = \mathbb{Q}(\sqrt[p]{a})$ subcampos de K . Por las Proposiciones 2.3.3 y 2.3.4, página 39, $\delta_{K_1} = (-1)^{\binom{q}{2}} q^q a^{q-1}$ y $\delta_{K_2} = (-1)^{\binom{p}{2}} p^p a^{p-1}$. De la Proposición 2.3.1, página 38, tenemos que $\delta_{K_1}^p | \delta_K$ y $\delta_{K_2}^q | \delta_K$, lo que implica que $(qp)^{qp} | \delta_K$. Luego, como $f(x) = x^{qp} - a$ es el irreducible de θ y éste es Eisenstein para cada divisor

primo de a , entonces, por la Proposición 3.1.1, página 49, $a \nmid \text{ind}(\theta)$, por lo que $a^{qp-1} \mid \delta_K$. Así, $\text{ind}(\theta) = 1$ y $\{1, \theta, \theta^2, \dots, \theta^{p^q-1}\}$ es una base entera para K . \square

Corolario 3.2.3. Sean $n = p_1 \cdots p_r$, con p_i primos distintos, a entero libre de cuadrado y $K = \mathbb{Q}(\sqrt[n]{a})$. Si $\text{mcd}(a, n) = 1$ y $a^{q_i-1} \not\equiv 1 \pmod{q_i^2}$, para $i = 1, \dots, r$, entonces K es monogénico.

Demostración. El resultado se sigue del Teorema 3.2.2 y usando inducción sobre r . \square

CAPÍTULO 4

Ejemplos

En la primera parte vamos a considerar ejemplos usando mínimos enteros. Para esto observemos que si $\Delta(\theta)$ tiene muchos factores primos a potencias altas, las posibilidades para los d_i aumentan y los cálculos resultan más complicados, sin embargo, si conocemos algunos divisores del discriminante de K , estas posibilidades disminuyen. Así, mediante los ejemplos que proponemos, mostraremos una mejora del método de mínimos enteros y compararemos las bases que obtenemos con las que SageMath muestra.

Por último presentaremos un ejemplo utilizando el Teorema 3.2.1, página 60, y lo compararemos también con el que SageMath propone.

Consideremos p un primo impar tal que $q = 2p - 1$ no es un cuadrado y $1 - 4p^2$ es libre de cuadrado. Sean θ raíz del polinomio $f(x) = x^4 + x^2 + p^2$, $K = \mathbb{Q}(\theta)$ y $L = \mathbb{Q}(\sqrt{1 - 4p^2})$. En [2] encontramos que $f(x)$ es irreducible, por la condición sobre q .

Mediante el método de mínimos enteros, encontraremos una base entera de K . Para esto, calculamos el discriminante de θ y obtuvimos:

$$\Delta(\theta) = 2^4(1 - 4p^2)^2 p^2 = \text{ind}^2(\theta)\delta_K. \quad (4.1)$$

Por el Teorema 3.1.10, página 56, se cumple que $d_i^{2(n-i)}|\Delta(\theta)$ para todo $i = 0, 1, 2, 3$, y la igualdad: $\text{ind}(\theta) = d_0 d_1 d_2 d_3$.

Ya sabemos que $d_0 = 1$, así que procedamos a encontrar las posibilidades para los otros d_i . Como $d_1^6|\Delta(\theta)$, necesariamente $d_1 = 1$. Ahora $d_2^4|\Delta(\theta)$, por lo que d_2 es: 1 o 2. Por último, $d_3^2|\Delta(\theta)$ así que, en principio, d_3 es: 1, 2, 2^2 , p , $1 - 4p^2$, $2p$, $2(1 - 4p^2)$, $4p$, $4(1 - 4p^2)$, $p(1 - 4p^2)$, $2p(1 - 4p^2)$ o $4p(1 - 4p^2)$. Para

d_3 resultaron muchas posibilidades y recordemos que para cada i , estamos buscando $\alpha = \frac{a_0 + a_1\theta + \cdots + a_{i-1}\theta^{i-1} + \theta^i}{d_i} \in \mathcal{O}_K$, con d_i máximo.

Por otro lado, como L es un subcampo de K y $[K : L] = 2$, entonces $\delta_L^2 | \delta_K$, además se cumple la congruencia $1 - 4p^2 \equiv 1 \pmod{4}$, lo que implica que $\delta_L = 1 - 4p^2$. De lo anterior y por la Ecuación 4.1, obtenemos que el factor $(1 - 4p^2)^2$ no divide al índice de θ , así que en las posibilidades para d_3 descartamos a aquellas en donde aparece $1 - 4p^2$.

Con lo que obtuvimos anteriormente busquemos un mínimo entero de grado i para cada $i = 0, 1, 2, 3$. Como $d_0 = d_1 = 1$, entonces 1 y θ son mínimos enteros de grado 0 y 1, respectivamente. Prosigamos con d_2 , si $d_2 = 2$, veamos si existe $\alpha \in \mathcal{O}_K$ tal que $\alpha = \frac{a_0 + a_1\theta + \theta^2}{2}$. De ser así, α debe satisfacer un polinomio mónico con coeficientes enteros y, haciendo algunos cálculos en SageMath, encontramos que las expresiones de los coeficientes del polinomio que α satisface son complicadas de tratar, es por eso que hicimos algunos casos particulares poniendo $p = 3, 7, 11, 17$, y encontramos que si $a_0 = a_1 = 1$, entonces $\alpha \in \mathcal{O}_K$. De lo anterior, si ponemos $a_0 = a_1 = 1$ y consideramos a p como en las hipótesis, mediante el uso de SageMath, encontramos que α es solución de la ecuación

$$x^4 - x^3 + \frac{p^2 + 1}{2}x^2 + \frac{p^2 - 1}{4}x + \frac{p^4 - 2p^2 + 1}{16} = 0.$$

Se verifica sin dificultad que cada coeficiente de la ecuación anterior es entero.

Consecuentemente $d_2 = 2$ y $\frac{1 + \theta + \theta^2}{2}$ es un mínimo entero de grado 2.

Finalmente, dado que $d_2 | d_3$ y por la relación entre el índice y los d_i , tenemos que $2 | d_3$ y las posibilidades restantes para d_3 son 2 o $2p$. Para encontrar un mínimo entero de grado 3, hicimos algunos casos particulares tomando $p = 3, 7, 11$, y esto nos permitió encontrar que $\alpha = \frac{\theta + p\theta^2 + \theta^3}{2p} \in \mathcal{O}_K$, ya que α satisface la ecuación

$$x^4 + x^3 + \frac{p^2 + 1}{2}x^2 - \frac{p^2 - 1}{4}x + \frac{p^4 - 2p^2 + 1}{16} = 0,$$

y se verifica que cada coeficiente del polinomio anterior es entero, lo que implica que un mínimo entero de grado 3 es $\frac{\theta + p\theta^2 + \theta^3}{2p}$.

Con lo hecho anteriormente y por el Teorema 3.1.9, página 55, obtenemos el siguiente resultado para K .

Teorema 4.0.1. Sean p un primo impar tal que $2p - 1$ no es un cuadrado y $1 - 4p^2$ es libre de cuadrado y θ raíz del polinomio $f(x) = x^4 + x^2 + p^2$. Si $K = \mathbb{Q}(\theta)$, entonces una base entera para K es

$$\left\{ 1, \theta, \frac{1 + \theta + \theta^2}{2}, \frac{\theta + p\theta^2 + \theta^3}{2p} \right\}.$$

Demostración. El resultado se sigue de la discusión anterior. \square

Ejemplo 4.0.1. Sean $f(x) = x^4 + x^2 + 9$ y θ una raíz de $f(x)$. Como $2 \cdot 3 - 1 = 5$ no es un cuadrado y $1 - 4 \cdot 9 = -35$ es libre de cuadrado, por el Teorema 4.0.1, si $K = \mathbb{Q}(\theta)$, entonces una base entera para K es

$$A = \left\{ 1, \theta, \frac{1 + \theta + \theta^2}{2}, \frac{\theta + 3\theta^2 + \theta^3}{6} \right\}.$$

Ahora, SageMath cuenta con una función que calcula bases enteras y, para el mismo ejemplo, la base que SAGE propone es

$$B = \left\{ \frac{1 + \theta^3}{2}, \frac{\theta + 3\theta^2 + \theta^3}{6}, \theta^2, \theta^3 \right\}.$$

Haciendo algunos cálculos, obtenemos que la matriz que cambia la base B a la base A está dada por

$$\begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 6 & 3 & 1 \\ 0 & -3 & -1 & 0 \\ -1 & -1 & -1 & 0 \end{pmatrix},$$

la cual tiene determinante 1.

También preguntamos a SageMath sobre el número de clase de este campo y resulta que es 1. Así que para este caso \mathcal{O}_K es un dominio de ideales principales y por tanto es de factorización única.

Apliquemos una vez más el “método de mínimos enteros mejorado” para construir una base entera de $K = \mathbb{Q}(\theta)$, donde θ es raíz del polinomio irreducible $f(x) = x^4 + px^2 + p$ y p es un primo impar tal que $p - 4$ es libre de cuadrado. Si $L = \mathbb{Q}(\sqrt{p^2 - 4p})$, entonces $L \subseteq K$ y, haciendo unos cálculos, obtenemos:

$$\Delta(\theta) = 2^4(p - 4)^2 p^3 = \text{ind}^2(\theta) \delta_K. \quad (4.2)$$

Comencemos por determinar las posibilidades para cada d_i . De nuevo, recordemos que del Teorema 3.1.10 tenemos que $d_i^{2(n-i)}|\Delta(\theta)$ y la igualdad: $\text{ind}(\theta) = d_0 d_1 d_2 d_3$.

Como $d_0 = 1$, prosigamos con d_1 . Para éste, dado que $d_1^6|\Delta(\theta)$ y por la Ecuación 4.2, tenemos que $d_1 = 1$. Ahora, encontramos que d_2 puede ser: 1 o 2 ya que $d_2^4|\Delta(\theta)$. Por último, como $d_3^2|\Delta(\theta)$, las posibilidades para d_3 son: 1, 2, 4, p , $p-4$, $2p$, $4p$, $2(p-4)$, $4(p-4)$, $p(p-4)$, $2p(p-4)$ o $4p(p-4)$.

Luego, como $f(x)$ es p -Eisenstein, entonces por la Proposición 3.1.1, página 49, $p \nmid \text{ind}(\theta)$ y en consecuencia $p^3|\delta_K$.

Por otro lado, $\delta_L = p^2 - 4p$, ya que $p^2 - 4p \equiv p^2 \equiv 1 \pmod{4}$. Así, $(p^2 - 4p)^2|\delta_K$ y el factor $p^3(p-4)$ no divide al índice de θ , por lo que en las posibilidades para d_3 descartamos a aquellas que son divididas por p y $(p-4)$.

Hasta aquí, hemos obtenido que 1 y θ son mínimos enteros de grado 0 y 1, respectivamente. También que las posibilidades para d_2 son: 1 o 2, y las de d_3 son: 1, 2 o 4.

Veamos si $d_2 = 2$. De ser así existe un elemento $\alpha \in \mathcal{O}_K$ tal que $\alpha = \frac{a_0 + a_1\theta + \theta^2}{2}$. Haciendo cálculos, usando SageMath, encontramos que α satisface la ecuación $x^4 + Ax^3 + Bx^2 + Cx + D = 0$, donde

$$A = -2a_0 + p,$$

$$B = \frac{1}{4}[6a_0^2 + (a_1^2 - 6a_0 + 2 + p)p],$$

$$C = -\frac{1}{4}[2a_0^3 + (a_0 - 1)p^2 + ((a_0 - 2)a_1^2 - 3a_0^2 + 2a_0)p],$$

$$D = \frac{1}{16}[a_0^4 + (a_0^2 + a_1^2 - 2a_0 + 1)p^2 + (a_1^4 - 2a_0^3 + (a_0^2 - 4a_0)a_1^2 + 2a_0^2)p].$$

De B , si tomamos congruencia módulo 2 en el numerador, tenemos que a_1 debe ser impar y, si tomamos congruencia módulo 4 de nuevo en el numerador de B , obtenemos:

$$6a_0^2 + (a_1^2 - 6a_0 + 2 + p)p \equiv 2a_0^2 + p + 2a_0p + 2p + 1 \pmod{4}.$$

Ahora, si $p \equiv 1 \pmod{4}$, de la congruencia anterior tenemos que se cumple:

$$2a_0^2 + 1 + 2a_0p + 2 + 1 \equiv 2a_0^2 + 2a_0 \equiv 0 \pmod{4}.$$

Sin embargo, si $p \equiv 3 \pmod{4}$, entonces

$$2a_0^2 + p + 2a_0p + 2p + 1 \equiv 2a_0^2 + 3 + 2a_0 + 2 + 1 \equiv 2a_0^2 + 2a_0 + 2 \not\equiv 0 \pmod{4},$$

es decir, para este caso, $d_2 = 1$.

Supongamos primero que $p \equiv 1 \pmod{4}$. Después haremos el caso cuando $p \equiv 3 \pmod{4}$.

Si $a_0 = a_1 = 1$, entonces α es solución de la ecuación

$$x^4 + (p-2)x^3 + \frac{p^3 - 3p + 6}{4}x^2 + \frac{p-1}{2}x + \frac{p^2 - 2p + 1}{16} = 0.$$

Como $p \equiv 1 \pmod{4}$, se verifica sin dificultad que cada coeficiente de la ecuación anterior es entero. Por consiguiente, $d_2 = 2$ y $\frac{1 + \theta + \theta^2}{2}$ es mínimo entero de grado 2. Además, como $d_2 | d_3$ entonces $d_3 = 2$ y existe $\alpha = \frac{a_0 + a_1\theta + a_2\theta^2 + \theta^3}{2} \in \mathcal{O}_K$ el cual es un mínimo entero de grado 3. Poniendo $a_0 = 0$, $a_1 = 1$ y $a_2 = 2$, encontramos que α satisface la ecuación

$$x^4 + px^3 + \frac{p^3 - 4p^2 + 7p}{4}x^2 + \frac{(p^2 - 3p + 2)p}{4}x + \frac{(p^2 - 2p + 1)p}{16} = 0.$$

De igual manera, se verifica sin dificultad que cada coeficiente de la ecuación anterior es entero. En consecuencia, un mínimo entero de grado 3 es $\frac{\theta + \theta^2 + \theta^3}{2}$.

Ahora, supongamos que $p \equiv 3 \pmod{4}$. Anteriormente obtuvimos que $d_2 = 1$. Como las posibilidades para d_3 son 1, 2 o 2^2 . Veamos si existe $\alpha \in \mathcal{O}_K$ tal que $\alpha = \frac{a_0 + a_1\theta + a_2\theta^2 + \theta^3}{4}$. Mediante el uso de SageMath, encontramos que α debe satisfacer la ecuación $x^4 + Ax^3 + Bx^2 + Cx + D = 0$, donde

$$A = \frac{a_2p - 2a_0}{2},$$

$$B = \frac{1}{16}[(a_2^2 - 2a_1 - 3)p^2 + p^3 + 6a_0^2 + (a_1^2 - 6a_0a_2 + 2a_2^2 + 4a_1)p],$$

$$C = -\frac{1}{32}[(a_0 - a_2)p^3 + 2a_0^3 + (a_0a_2^2 - a_2^3 - 2a_0a_1 + 2(a_1 + 1)a_2 - 3a_0)p^2 + (a_0a_1^2 + 2a_0a_2^2 + 4a_0a_1 - (3a_0^2 + 2a_1^2)a_2)p],$$

$$D = \frac{1}{256}[a_0^4 + (a_0^2 + a_1^2 - 2a_0a_2 + a_2^2 - 2a_1 + 1)p^3 - (2a_0a_2^3 - a_2^4 + 2a_0^2a_1 + 2a_1^3 - (a_0^2 + a_1^2 - 4a_1)a_2^2 + 3a_0^2 - 2a_1^2 - 4(a_0a_1 + a_0)a_2)p^2 + (a_0^2a_1^2 + a_1^4 + 2a_0^2a_2^2 + 4a_0^2a_1 - 2a_2(a_0^3 + 2a_0a_1^2))p].$$

De A , tenemos que a_2 debe ser par. Además, si tomamos congruencia módulo 2 en el numerador de B , encontramos que a_1 también debe ser par. Asimismo y por la información que hemos obtenido sobre a_1 y a_2 se verifica sin dificultad que, si en el numerador de B tomamos congruencia módulo 4, a_0 es par. Luego, del numerador de D , como deseamos que 256 lo divida, en particular el 2 lo debe dividir y, al tomar congruencia módulo 2 en el numerador de D , obtenemos que éste es impar. Consecuentemente $d_3 \neq 4$ y las posibilidades restantes para d_3 son 1 o 2. Análogamente se muestra que $d_3 \neq 2$, lo que implica que $d_3 = 1$ y, para este caso, K tiene una base de potencias.

De la discusión anterior hemos obtenido el siguiente resultado.

Teorema 4.0.2. *Sean p un primo impar y θ raíz de $f(x) = x^4 + px^2 + p$. Si $p - 4$ es libre de cuadrado y $K = \mathbb{Q}(\theta)$, entonces una base entera para K es*

$$\{1, \theta, \theta^2, \theta^3\}, \quad \text{si } p \equiv 3 \pmod{4},$$

$$\left\{1, \theta, \frac{1 + \theta + \theta^2}{2}, \frac{\theta + \theta^2 + \theta^3}{2}\right\}, \quad \text{si } p \equiv 1 \pmod{4}.$$

Demostración. El resultado se sigue de la discusión anterior. \square

Ejemplo 4.0.2. Sean $f(x) = x^4 + 7x^2 + 7$ y θ una raíz de $f(x)$. Debido a que $7 - 4 = 3$ es libre de cuadrado, entonces $K = \mathbb{Q}(\theta)$ es como en el Teorema 4.0.2 y tiene una base de potencias, ya que $7 \equiv 3 \pmod{4}$.

Comparamos con SageMath y, como era de esperarse, él propone la misma base que nosotros. Además calculó que el número de clase es 4 y más aún, dice que su grupo de clase es cíclico.

Ejemplo 4.0.3. Consideremos al polinomio $f(x) = x^4 + 17x^2 + 17$ y θ una raíz de $f(x)$. De nuevo, si $K = \mathbb{Q}(\theta)$, tenemos que K es como en el Teorema 4.0.2 y una base entera para K está dada por

$$A = \left\{1, \theta, \frac{1 + \theta + \theta^2}{2}, \frac{\theta + \theta^2 + \theta^3}{2}\right\},$$

pues $17 \equiv 1 \pmod{4}$. Por otro lado, la base entera que SageMath propone para este ejemplo es

$$B = \left\{\frac{1 + \theta^3}{2}, \frac{\theta + \theta^2 + \theta^3}{2}, \theta^2, \theta^3\right\},$$

y la matriz que cambia la base B a la base A es

$$\begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 2 & 1 & 1 \\ 0 & -1 & 0 & 0 \\ -1 & -1 & -1 & 0 \end{pmatrix},$$

la cual tiene determinante 1.

En este caso, con SageMath encontramos que el número de clase es 8 y que su grupo de clase es $C_4 \times C_2$.

En [17] encontramos la construcción de una base entera para campos de la forma $\mathbb{Q}(\sqrt{n}, \sqrt{m})$, para n y m enteros libres de cuadrado, sin embargo, en el ejemplo que presentamos a continuación, nosotros utilizamos el método de mínimos enteros y el hecho de que conocemos los discriminantes de los subcampos $\mathbb{Q}(\sqrt{n})$ y $\mathbb{Q}(\sqrt{m})$. Es importante mencionar que no presentamos un resultado más general como lo hacen en [17] ya que, por el método que utilizamos, obtendríamos un factor de la forma $(m - n)^2$ y, como m y n son enteros arbitrarios, no tenemos control de sus divisores primos. Sin embargo, recordemos que nuestro propósito principal en este tipo de ejemplos es mostrar una mejora del método de mínimos enteros por medio de los discriminantes de algunos subcampos.

Consideremos el campo $K = \mathbb{Q}(\sqrt{2}, \sqrt{n})$, con n entero libre de cuadrado tal que $n \equiv 1 \pmod{4}$ y supongamos que $q = n - 2$ también es libre de cuadrado. Entonces $K = K_1 K_2$, donde $K_1 = \mathbb{Q}(\sqrt{2})$ y $K_2 = \mathbb{Q}(\sqrt{n})$. Sea $\theta = \sqrt{2} + \sqrt{n}$, se verifica sin dificultad que θ es un elemento primitivo de K .

Calculando el discriminante de θ obtenemos:

$$\Delta(\theta) = 2^{14} n^2 (n - 2)^2 = \text{ind}^2(\theta) \delta_K. \quad (4.3)$$

Por otro lado, determinemos las posibilidades para cada d_i . Como $d_1^6 | \Delta(\theta)$, entonces d_1 puede ser: 1, 2 o 2^2 . Ahora, dado que $d_2^4 | \Delta(\theta)$, encontramos que d_2 es: 1, 2, 2^2 o 2^3 . Por último, ya que $d_3^2 | \Delta(\theta)$, tenemos que las posibilidades para d_3 son: 1, 2, 2^2 , 2^3 , 2^4 , 2^5 , 2^6 , 2^7 , n , $(n - 2)$, $2n$, $2^2 n$, $2^3 n$, $2^4 n$, $2^5 n$, $2^6 n$, $2^7 n$, $2(n - 2)$, $2^2(n - 2)$, $2^3(n - 2)$, $2^4(n - 2)$, $2^5(n - 2)$, $2^6(n - 2)$, $2^7(n - 2)$, $n(n - 2)$, $2n(n - 2)$, $2^2 n(n - 2)$, $2^3 n(n - 2)$, $2^4 n(n - 2)$, $2^5 n(n - 2)$, $2^6 n(n - 2)$, $2^7 n(n - 2)$. Notemos que en el último caso obtenemos demasiadas posibilidades, es por eso que una vez más, si involucramos la información que conocemos sobre los discriminantes de algunos subcampos de K , vamos a obtener menos casos.

Sean δ_{K_1} y δ_{K_2} los discriminantes de K_1 y K_2 , respectivamente. Por la Proposición 2.3.1, página 38, tenemos que $\delta_{K_1}^2 | \delta_K$ y $\delta_{K_2}^2 | \delta_K$. Además, dado que $\delta_{K_1} = 2^3$, $\delta_{K_2} = n$ y por la Proposición 2.3.2, página 38, los únicos primos que dividen a δ_K son 2 y n . De lo dicho anteriormente y de la Ecuación 4.3 tenemos que 2^6 y n^2 son factores de δ_K y que $(n-2)$ divide al índice de θ , por lo que las posibilidades de cada d_i han cambiado y ahora son menos, es decir, hemos obtenido que d_1 es: 1 o 2, d_2 es: 1, 2 o 2^2 , y d_3 es: $(n-2)$, $2(n-2)$, $2^2(n-2)$, $2^3(n-2)$ o $2^4(n-2)$.

Encontremos primero un mínimo entero de grado 1. Si $d_1 = 2$, buscamos $\alpha = \frac{a_0 + \theta}{2} \in \mathcal{O}_K$ tal que sea solución de la ecuación

$$x^4 - 2a_0x^3 + \frac{3a_0^2 - n - 2}{2}x^2 - \frac{a_0(a_0^2 - n - 2)}{2}x + \frac{a_0^4 - 4a_0^2 - 2(a_0^2 + 2)n + n^2 + 4}{16} = 0.$$

Como $\alpha \in \mathcal{O}_K$, entonces cada coeficiente de la ecuación anterior debe ser entero, en particular el de x^2 , de esto, a_0 debe ser impar, sin embargo, con esta condición y dado que $n \equiv 1 \pmod{4}$, si ponemos $a_0 = 2b_0 + 1$ y $n = 4r + 1$, donde b_0 y r pertenecen a \mathbb{Z} , y sustituimos en el término constante obtenemos:

$$a_0^4 - 4a_0^2 - 2(a_0^2 + 2)n + n^2 + 4 = 16(b_0^4 + 2b_0^3 - 2b_0^2r - 2b_0r - b_0 + r^2 - r) + 4 \not\equiv 0 \pmod{16}.$$

Por tanto $d_1 = 1$ y θ es un mínimo entero de grado 1.

Calculemos ahora a un mínimo entero de grado 2. Para esto, tomemos la posibilidad mayor, es decir, pongamos $d_2 = 4$ y veamos si existe $\alpha = \frac{a_0 + a_1\theta + \theta^2}{4}$ que pertenezca a \mathcal{O}_K . En este caso, α satisface la ecuación $x^4 + Ax^3 + Bx^2 + Cx + D = 0$, donde

$$A = -(a_0 + n + 2),$$

$$B = \frac{1}{8}[3a_0^2 - 2a_1^2 - (a_1^2 - 6a_0 - 4)n + 3n^2 + 12a_0 + 12],$$

$$C = -\frac{1}{16}[a_0^3 - 2(a_0 + 2)a_1^2 - (a_1^2 - 3a_0 + 2)n^2 + n^3 + 6a_0^2 - ((a_0 - 4)a_1^2 - 3a_0^2 - 4a_0 + 4)n + 12a_0 + 8],$$

$$D = \frac{1}{256}[a_0^4 + 8a_0^3 + 24a_0^2 + 32a_0 + 4a_1^4 - 2(a_1^2 - 2a_0 + 4)n^3 + n^4 - 4(a_0^2 + 4a_0 + 4)a_1^2 + (a_1^4 - 4(a_0 - 1)a_1^2 + 6a_0^2 - 8a_0 + 24)n^2 - 2(2a_1^4 - 2a_0^3 + (a_0^2 - 8a_0 - 4)a_1^2 - 4a_0^2 + 8a_0 + 16)n + 16].$$

Sin embargo, dado que en los coeficientes encontramos expresiones un tanto complicadas de tratar, hicimos casos particulares tomando $n = 5, 13, 17, 21$. En tales casos, encontramos que si $a_0 = 3$ y $a_1 = 2$, α es raíz de un polinomio mónico con coeficientes enteros. Por tanto, conjeturamos que si tomamos $a_0 = 3$ y $a_1 = 2$, entonces A, B, C, D pertenecen a \mathbb{Z} .

Si consideramos esos valores y poniendo $n = 4r + 1$, obtenemos (usando SageMath) que α es solución de la ecuación

$$x^4 - 2(2r+3)x^3 + (6r^2+12r+11)x^2 - 2(2r^3+3r^2+6r+4)x + r^4 + 2r^2 + 4r + 2 = 0,$$

como se quería. Así $d_2 = 2^2$ y $\frac{3 + 2\theta + \theta^2}{4}$ es un mínimo entero de grado 2.

Ahora, recordemos que $d_2 = 2^2 | d_3$, por lo que necesariamente se debe cumplir que $d_3 = 2^2 q$. Ahora sólo resta encontrar $a_0, a_1, a_2 \in \mathbb{Z}$, tales que $\alpha = \frac{a_0 + a_1\theta + a_2\theta^2 + \theta^3}{4q} \in \mathcal{O}_K$. Sin embargo, una vez más encontramos que α debe ser raíz de un polinomio cuyos coeficientes son complicados de tratar. Es por eso que también calculamos algunos casos particulares considerando $n = 5, 13, 17, 21, 29, 33, 37, 41$, y observamos que si $a_0 = 0$, $a_1 = n - 10$ y $a_2 = 2n - 4$, α pertenecía a \mathcal{O}_K . Así, mediante el uso de SageMath, pudimos encontrar que el polinomio

$$f(x) = x^4 - 2(4r + 3)x^3 + (24r^2 + 18r + 5)x^2 - 2(16r^3 - 3 - 2)x + 16r^4 - 24r^3 + 25r^2 - 12r - 4,$$

tiene coeficientes enteros y $f(\alpha) = 0$, con $\alpha = \frac{(n - 10)\theta + (2n - 4)\theta^2 + \theta^3}{4q}$.

De la discusión anterior obtenemos el siguiente Teorema.

Teorema 4.0.3. *Si $K = \mathbb{Q}(\sqrt{2}, \sqrt{n})$, n y $q = n - 2$ enteros libres de cuadrado donde $n \equiv 1 \pmod{4}$, entonces $\delta_K = 2^6 n^2$ y una base entera para K es*

$$\left\{ 1, \theta, \frac{3 + 2\theta + \theta^2}{4}, \frac{(n - 10)\theta + (2n - 4)\theta^2 + \theta^3}{4q} \right\}.$$

Demostración. El resultado se sigue de la discusión anterior. □

Notemos que, si K es como en el Teorema 4.0.3, K satisface las condiciones del Teorema 2.3.2, es decir, $K = K_1 K_2$ con $K_1 = \mathbb{Q}(\sqrt{2})$ y $K_2 = \mathbb{Q}(\sqrt{n})$.

Como $\delta_{K_1} = 8$ y $\delta_{K_2} = n$, entonces $\text{mcd}(\delta_{K_1}, \delta_{K_2}) = 1$, por lo que, si $\{1, \sqrt{2}\}$ y $\left\{1, \frac{1 + \sqrt{n}}{2}\right\}$ son bases enteras de K_1 y K_2 respectivamente, tenemos que otra base entera para K está dada por el producto de las bases enteras anteriores, es decir, otra base entera para K es

$$B = \left\{1, \sqrt{2}, \frac{1 + \sqrt{n}}{2}, \frac{\sqrt{2} + \sqrt{2n}}{2}\right\},$$

y la matriz que cambia la base B en la base que obtuvimos en el Teorema 4.0.3 es

$$\begin{pmatrix} 1 & -1 & \frac{n+3}{4} & \frac{n+1}{2} \\ 0 & 1 & 0 & 0 \\ 0 & 2 & 1 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix}.$$

Ejemplo 4.0.4. Sea $K = \mathbb{Q}(\sqrt{2}, \sqrt{13})$. Como 13 y $13 - 2 = 11$ son libres de cuadrado y $13 \equiv 1 \pmod{4}$, entonces K satisface las hipótesis del Teorema 4.0.3. Así, una base entera para K es

$$\left\{1, \theta, \frac{3 + 2\theta + \theta^2}{4}, \frac{3\theta + 22\theta^2 + \theta^3}{44}\right\},$$

donde $\theta = \sqrt{2} + \sqrt{13}$.

SageMath dice que para este caso el número de clase es 1. De lo que podemos concluir que el anillo de enteros de K es un dominio de ideales principales o equivalentemente, que es de factorización única.

En los siguientes dos ejemplos hacemos uso del Teorema 3.2.2, página 61, observemos que el primero sí cumple con todas las hipótesis, pero el segundo no. Así que para el Ejemplo 4.0.6, una vez más nos apoyamos del método de mínimos enteros para mostrar una base entera.

Ejemplo 4.0.5. Sean $n = 2 \cdot 3 \cdot 5$, $a = 11$ y pongamos $K = \mathbb{Q}(\sqrt[n]{a})$, entonces por el Corolario 3.2.3, K es monogénico, ya que $11 \equiv 3 \pmod{4}$, $11^2 \equiv 4 \pmod{9}$ y $11^4 \equiv 6 \pmod{25}$.

Ejemplo 4.0.6. Sea $K = \mathbb{Q}(\sqrt[6]{5})$, observemos que K no es como en el Teorema 3.2.2, ya que $5 \equiv 1 \pmod{4}$.

Calculemos una base entera para K mediante el método de mínimos enteros. Para esto, sea $\theta = \sqrt[6]{5}$. Entonces

$$\Delta(\theta) = 6^6 5^5 = \text{ind}^2(\theta) \delta_K. \quad (4.4)$$

Como $f(x) = x^6 - 5$ es el irreducible de θ y éste es 5-Eisenstein, por la Proposición 3.1.1, 5 no divide al índice y por tanto 5^5 es un factor de δ_K . Por otro lado, $L = \mathbb{Q}(\sqrt[3]{5})$ es un subcampo de K con discriminante $\delta_L = -3^3 5^2$. Como $\delta_L^2 | \delta_K$, tenemos que 3^6 es otro factor de δ_K , de esto y de lo anterior, encontramos que $3^6 5^5 | \delta_K$.

Calculemos cada d_i . Sabemos, por el Teorema 3.1.10, que $d_i^{2(6-i)}$ debe dividir a $\Delta(\theta)$ para cada $i = 0, 1, \dots, 5$. Así que, como d_0^{12} , d_1^{10} y d_2^8 dividen a $\Delta(\theta)$, entonces $d_0 = d_1 = d_2 = 1$. Asimismo, las posibilidades para d_3 son: 1, 2, 3 o 6, las de d_4 son: 1, 2, 3, 5, 6, 10, 15 o 30, y las de d_5 son: 1, 2, 2^2 , 2^3 , 3, 3^2 , 3^3 , 5, 5^2 , $2 \cdot 3$, $2^2 \cdot 3$, $2^3 \cdot 3$, $2 \cdot 3^2$, $2^2 \cdot 3^2$, $2^3 \cdot 3^2$, $2 \cdot 3^3$, $2^2 \cdot 3^3$, $2^3 \cdot 3^3$, $2 \cdot 5$, $2^2 \cdot 5$, $2^3 \cdot 5$, $2 \cdot 5^2$, $2^2 \cdot 5^2$, $2^3 \cdot 5^2$, $3 \cdot 5$, $3^2 \cdot 5$, $3^3 \cdot 5$, $3 \cdot 5^2$, $3^2 \cdot 5^2$, $3^3 \cdot 5^2$, $2 \cdot 3 \cdot 5$, $2^2 \cdot 3 \cdot 5$, $2^3 \cdot 3 \cdot 5$, $2 \cdot 3^2 \cdot 5$, $2^2 \cdot 3^2 \cdot 5$, $2^3 \cdot 3^2 \cdot 5$, $2 \cdot 3^3 \cdot 5$, $2^2 \cdot 3^3 \cdot 5$, $2^3 \cdot 3^3 \cdot 5$, $2 \cdot 3 \cdot 5^2$, $2^2 \cdot 3 \cdot 5^2$, $2^3 \cdot 3 \cdot 5^2$, $2 \cdot 3^2 \cdot 5^2$, $2^2 \cdot 3^2 \cdot 5^2$, $2^3 \cdot 3^2 \cdot 5^2$, $2 \cdot 3^3 \cdot 5^2$, $2^2 \cdot 3^3 \cdot 5^2$ o $2^3 \cdot 3^3 \cdot 5^2$. Sin embargo, como notamos anteriormente, tenemos que $3^6 5^5 | \delta_K$, lo que implica que debemos descartar todas aquellas posibilidades para los d_i que tengan de factor a 3 y a 5, lo cual simplifica mucho los casos.

En resumen, hemos obtenido que $1, \theta, \theta^2$ son mínimos enteros de grado 0, 1 y 2, respectivamente, y que ahora las posibilidades para d_3 son: 1 o 2, las de d_4 son: 1 o 2, y las de d_5 se simplificaron únicamente a: 1, 2, 2^2 o 2^3 .

Calculemos los restantes mínimos enteros. Empecemos por un mínimo entero de grado 3, para esto, primero observemos que, como $F = \mathbb{Q}(\sqrt{5})$ es subcampo de K , el elemento $\beta = \frac{1 + \sqrt{5}}{2} = \frac{1 + \theta^3}{2}$ es un elemento entero en F y por tanto también es entero en K , más aún, es un mínimo entero de grado 3. Luego, como $d_3 | d_4$, $d_4 | d_5$ y $d_3 = 2$, y de la Ecuación 4.4 obtenemos que $d_4 = d_5 = 2$.

Ahora, como β y θ son elementos de \mathcal{O}_K , entonces $\theta\beta = \frac{\theta + \theta^4}{2} \in \mathcal{O}_K$, más aún, éste es un mínimo entero de grado 4. De la misma manera, $\theta^2\beta = \frac{\theta^2 + \theta^5}{2}$ es un mínimo entero de grado 5.

Así, una base entera para $K = \mathbb{Q}(\sqrt[6]{5})$ es

$$A = \left\{ 1, \theta, \theta^2, \frac{1 + \theta^3}{2}, \frac{\theta + \theta^4}{2}, \frac{\theta^2 + \theta^5}{2} \right\}.$$

Para este ejemplo, la base entera que propone SageMath es

$$B = \left\{ \frac{1 + \theta^3}{2}, \frac{\theta + \theta^4}{2}, \frac{\theta^2 + \theta^5}{2}, \theta^3, \theta^4, \theta^5 \right\},$$

y la matriz que cambia la base B en la base A es

$$\begin{pmatrix} 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \end{pmatrix},$$

con determinante igual a -1 .

En este ejemplo, resulta que K también tiene número de clase 1, por lo que una vez más, el anillo de enteros de K es de factorización única.

Proposición 4.0.1. Sean $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{m})$ y m entero impar, libre de cuadrado tal que $m^2 \not\equiv 1 \pmod{9}$ y $d = 2^9 + 3^3 m^2$ es libre de cuadrado. Si $\theta = \sqrt{2} + \sqrt[3]{m}$, entonces $K = \mathbb{Q}(\theta)$ e $\text{ind}(\theta) = d$.

Demostración. Se verifica sin dificultad que θ es un elemento primitivo, es decir, $K = \mathbb{Q}(\theta)$. Por otro lado, tenemos lo siguiente, $K_1 = \mathbb{Q}(\sqrt{2}) \subseteq K$, $K_2 = \mathbb{Q}(\sqrt[3]{m}) \subseteq K$, $\delta_{K_1} = 2^3$ y $\delta_{K_2} = -3^3 m^2$. Además,

$$\Delta(\theta) = 2^9 3^6 m^4 d^2 = \text{ind}^2(\theta) \delta_K.$$

Por la Proposición 2.3.1, $\delta_{K_1}^3 | \delta_K$ y $\delta_{K_2}^2 | \delta_K$, lo que implica $2^9 3^6 m^4 | \delta_K$. Luego, por la Proposición 2.3.2, los únicos primos que dividen a δ_K son 2, 3 y divisores primos de m . Como d es primo relativo con 2, 3 y m , necesariamente $\text{ind}(\theta) = d$. \square

Observación 4.0.1. Si K , θ y d son como en la Proposición 4.0.1, entonces una base entera para K es de la forma

$$\left\{ 1, \theta, \theta^2, \theta^3, \theta^4, \frac{a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + \theta^5}{d} \right\},$$

para algunos $a_i \in \mathbb{Z}$ e $i = 0, 1, 2, 3, 4$.

Demostración. Recordemos que en la Proposición 4.0.1, por hipótesis, d es libre de cuadrado y encontramos que $\text{ind}(\theta) = d$. Por otro lado, como $d_0 d_1 d_2 d_3 d_4 = \text{ind}(\theta) = d$ y $d_i | d_{i+1}$, necesariamente $d_0 = d_1 = d_2 = d_3 = 1$ y $d_4 = d$, es decir, de acuerdo con el Teorema 3.1.10, una base entera para K es $\left\{ 1, \theta, \theta^2, \theta^3, \theta^4, \frac{a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + \theta^5}{d} \right\}$, para algunos $a_i \in \mathbb{Z}$. \square

En el intento de construir un ejemplo utilizando la Observación 4.0.1, tuvimos algunas dificultades en los cálculos, sin embargo, nos fue posible encontrar una base con la ayuda de la que SageMath propone a través de la construcción de una matriz de cambio de base. De acuerdo con la notación utilizada en la Observación 4.0.1, si $m = 3$, entonces $d = 755$, recordemos que queremos determinar valores de a_0, a_1, a_2, a_3 y a_4 enteros para que $\alpha_5 = \frac{a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + \theta^5}{755} \in \mathcal{O}_K$. Hallamos que, si $a_0 = 166$, $a_1 = -312$, $a_2 = 179$, $a_3 = 245$ y $a_4 = 614$, α_5 es un mínimo entero de grado 5 y una base entera para K es como en la Observación 4.0.1.

En el siguiente ejemplo obtenemos, mediante la aplicación del Teorema 3.2.1, una base entera para un campo numérico compuesto. Además, para este mismo ejemplo, escribimos la base entera que SageMath propone y encontramos una matriz de cambio de base entre la que proponemos nosotros y la de SageMath.

Ejemplo 4.0.7. Sean $K_1 = \mathbb{Q}(\sqrt[5]{3})$ y $K_2 = \mathbb{Q}(\sqrt{7})$. Para simplificar, pongamos $\alpha = \sqrt[5]{3}$ y $\beta = \sqrt{7}$. Por la Proposición 2.3.4, página 39, una base entera para K_1 está dada por $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$, por otro lado, una base entera para K_2 es $\{1, \beta\}$. Luego, como la pareja $(3, 5)$ es semi-impar y la pareja $(7, 2)$ es semi-par, por el Teorema 3.2.1, una base entera para $K = K_1 K_2$ es

$$\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3, \beta\alpha^4\}.$$

Como $K = \mathbb{Q}(\gamma)$ con $\gamma = \sqrt[5]{3} + \sqrt{7}$, SageMath propone que una base entera para K sea

$$\{\eta, \gamma, \gamma^2, \dots, \gamma^9\},$$

donde $\eta = 9320 + 9511\alpha + 7217\alpha^2 + 11717\alpha^3 + 2311\alpha^4 + \beta(1824 + 2772\alpha + 5114\alpha^2 + 1914\alpha^3 + 2485\alpha^4)$.

Haciendo algunos cálculos, encontramos que la matriz que cambia la base que obtenemos nosotros a la base que propone SageMath es

$$\begin{pmatrix} 9320 & 0 & 7 & 0 & 49 & 3 & 343 & 441 & 2401 & 18522 \\ 9511 & 1 & 0 & 21 & 0 & 245 & 3 & 2401 & 588 & 21609 \\ 7217 & 0 & 1 & 0 & 42 & 0 & 735 & 3 & 9604 & 756 \\ 11717 & 0 & 0 & 1 & 0 & 70 & 0 & 1715 & 3 & 28812 \\ 2311 & 0 & 0 & 0 & 1 & 0 & 105 & 0 & 3430 & 3 \\ 1824 & 1 & 0 & 7 & 0 & 49 & 18 & 343 & 1176 & 2401 \\ 2772 & 0 & 2 & 0 & 28 & 0 & 294 & 21 & 2744 & 1764 \\ 5114 & 0 & 0 & 3 & 0 & 70 & 0 & 1029 & 24 & 12348 \\ 1914 & 0 & 0 & 0 & 4 & 0 & 140 & 0 & 2744 & 27 \\ 2485 & 0 & 0 & 0 & 0 & 5 & 0 & 245 & 0 & 6174 \end{pmatrix},$$

la cual tiene determinante 1.

El número de clase en este ejemplo, según SageMath, es 1, así que \mathcal{O}_K es de ideales principales.

4.1. Conclusiones

El objetivo de este trabajo fue presentar métodos para construir bases enteras y grupos de clase en ciertas extensiones radicales y con éstos mostrar ejemplos. Durante la revisión de la literatura nos encontramos con el Teorema 3.1.9, página 55, en el cual identificamos un método para construir bases enteras y creímos que serviría para presentar algunos ejemplos, sin embargo, al efectuar los cálculos para calcular los coeficientes de algunos elementos que buscábamos fueran enteros, tuvimos muchas dificultades, a pesar de que nos apoyamos de SageMath para realizarlos, por lo que una pregunta que surgió fue, ¿podemos mejorar el método? Como los numerosos casos que aparecieron resultaron ser un obstáculo, buscamos reducir la cantidad de posibilidades,

y observamos que conocer factores del discriminante del campo era de gran utilidad. Lo que hicimos fue aplicar las Proposiciones 2.3.1 y 3.1.1, páginas 38 y 49, respectivamente, en el método de mínimos enteros para construir ejemplos de bases enteras, donde se nota que los casos se simplifican demasiado. Es importante resaltar que aunque mostramos una mejora, el método tiene bastantes limitaciones, ya que determinar los polinomios de los elementos que forman la base en extensiones de grado más alto, parece ser un problema mayor, pues el número de operaciones e incógnitas con las que hay que tratar resultan ser demasiadas. Así que sería interesante buscar otra manera de optimizarlo.

Por otro lado, para proponer bases enteras en $K = \mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_m]{a_m})$ introducimos los conceptos de pareja semi-par y semi-impar. Estos conceptos hicieron que pudiéramos aplicar exitosamente el Teorema 2.3.2 a K , donde a K lo vemos como el campo compuesto $K_1 \cdots K_m$, con $K_i = \mathbb{Q}(\sqrt[n_i]{a_i})$, y planteamos el Teorema 3.2.1, es decir, obtuvimos una base entera para K a partir de bases enteras de sus subcampos K_i .

En la Proposición 2.3.4 se dan condiciones necesarias y suficientes para determinar si el campo $\mathbb{Q}(\sqrt[p]{a})$ tiene como anillo de enteros a $\mathbb{Z}[\sqrt[p]{a}]$, con p primo impar y bajo ciertas hipótesis sobre a . Nosotros hicimos uso de este resultado para obtener el Teorema 3.2.2, donde damos condiciones suficientes sobre a y n para que $\mathbb{Q}(\sqrt[n]{a})$ también tenga una base de potencias.

A pesar de los resultados obtenidos, las condiciones que pedimos en los Teoremas 3.2.1 y 3.2.2 son muy restrictivas, por lo que una posible ruta para continuar se obtiene a través de pedir menos condiciones a a_i y n_i o a a y n , respectivamente.

En el último capítulo, donde desarrollamos ejemplos aplicando cada uno de los resultados que obtuvimos, también pedimos a SageMath que calculara bases enteras para cada caso, las incluimos y encontramos matrices de cambio de base. Dado que estas matrices deben tener entradas enteras y determinante ± 1 , creemos que sería conveniente estudiar más a fondo el grupo lineal general sobre \mathbb{Z} para tener una visión más amplia sobre las matrices de cambio de base y ver si es posible aplicar algunos resultados de estas matrices en la construcción de bases enteras.

Por limitaciones de tiempo y ya que nos sumergimos demasiado en la parte de bases enteras, no pudimos discutir como hubiéramos querido el grupo de clase, sin embargo, lo consideraremos como trabajo para futuro.

Bibliografía

- [1] ALACA S. Y WILLIAMS K. *Introductory Algebraic Number Theory*. Cambridge University Press, 2004.
- [2] AYALA-VELASCO A. *Polígono de Newton e irreducibilidad de polinomios*. En edición, 2018.
- [3] BARRERA-MORA F. *Notas de campos numéricos*. No publicado, 1995-1996, revisado 2017.
- [4] BARRERA-MORA F. *Notas de campos y anillos*. No publicado, 2015.
- [5] BARRERA-MORA F., GARCÍA A., MANCIO R. Y TORRES C., *The discriminant of a trinomial*. International Journal of Pure and Applied Mathematics, 2012.
- [6] FUNAKURA T. *On integral bases of pure quartic fields*. Math. J. Okayama Univ., 1984.
- [7] GAÁL I., OLAJOS P. Y POHST M. *Power integral bases in orders of composite fields*. Experimental Mathematics, 2002.
- [8] HUARD J., SPEARMAN B. Y WILLIAMS K. *Integral Bases for Quartic Fields with Quadratic Subfields*. Journal of number theory, 1995.
- [9] JANUSZ G. *Algebraic Number Fields*. American Mathematical Soc., 1991.
- [10] JARVIS F. *Algebraic Number Theory*. Editorial Springer, 2014.
- [11] JHORAR, B. Y KHANDUJA, S. *On power basis of a class of algebraic number fields*. International Journal of Number Theory, 2016.

- [12] MURTY R. Y ESMONDE J. Problems in algebraic number theory (Vol. 190). Springer Science & Business Media, 2005.
- [13] NARKIEWICZ W. Elementary and analytic theory of algebraic numbers. Springer Science & Business Media, 2013.
- [14] OKUTSU K. Integral basis of the field $\mathbb{Q}(\sqrt[n]{a})$. Proceedings of the Japan Academy, Series A, Mathematical Sciences, 1982.
- [15] RIBENBOIM P. Algebraic numbers. John Wiley & Sons, 1972.
- [16] STEWART I. Y TALL D. Algebraic number theory and Fermat's last theorem. AK Peters/CRC Press, 2001.
- [17] WILLIAMS K. Integers of biquadratic fields. *Canad. Math. Bull.*, 1970.