

Aproximación de Kummer al Teorema de Fermat

Guillermo Mantilla
Director: Xavier Caicedo Ferrer

Universidad de Los Andes
Facultad de Ciencias
Departamento de Matemáticas
Bogotá, Agosto de 2002

Yo, GUILLERMO MANTILLA , manifiesto en este documento mi voluntad de ceder a la Universidad de Los Andes los derechos patrimoniales, consagrados en el artículo 72 de la Ley 23 de 1982, del trabajo final de grado* denominado APROXIMACIÓN DE KUMMER AL TEOREMA DE FERMAT, producto de mi actividad académica, para optar por el título de MATEMÁTICO en la Universidad de Los Andes. La Universidad de Los Andes, entidad académica sin ánimo de lucro, queda por lo tanto facultada para ejercer plenamente los derechos anteriormente cedidos en su actividad ordinaria de investigación, docencia y publicación. La cesión otorgada se ajusta a lo que establece la Ley 23 de 1982. Con todo, en mi condición de autor me reservo los derechos morales de la obra antes citada con arreglo al artículo 30 de la Ley 23 de 1982. En concordancia suscribo este documento en el momento mismo que hago entrega del trabajo final a la Biblioteca General de la Universidad de Los Andes.

<hr/> NOMBRE	<hr/> FIRMA	<hr/> CÉDULA
--------------	-------------	--------------

Santafé de Bogotá, D.C., 12 de julio de 2009

* “Los derechos de autor recaen sobre las obras científicas, literarias y artísticas en las cuales se comprenden las creaciones del espíritu en el campo científico, literario y artístico, cualquiera que sea el modo o forma de expresión y cualquiera que sea su destinación, tales como: los libros, folletos y otros escritos; las conferencias, alocuciones, sermones y otras obras de la misma naturaleza; las obras dramáticas o dramático-musicales; las obras coreográficas y las pantomimas; las composiciones musicales con letra o sin ella; las obras cinematográficas, a las cuales se asimilan las obras expresadas por procedimiento análogo a la cinematografía, inclusive los videogramas, las obras de dibujo, pintura, arquitectura, escultura, grabado, litografía; las obras fotográficas a las cuales se asimilan las expresas por procedimiento análogo a la fotografía; las obras de artes plásticas; las ilustraciones, mapas, planos, croquis y obras plásticas relativas a la geografía, a la topografía, a la arquitectura o a las ciencias, en fin, toda producción del dominio científico, literario o artístico que pueda reproducirse o definirse por cualquier forma de impresión o de reproducción, por fonografía, radiotelefonía o cualquier otro medio conocido o por conocer”. (artículo 2 de la Ley 23 de 1982)

Agradecimientos

Todo este trabajo no hubiese sido posible sin la compañía de mi familia por esto quiero darles gracias. A mi mamá por su paciencia y dedicación, a mi papá por su apoyo y sacrificio, y a mi hermano por ser la alegría y el orgullo en mi vida.

También quiero agradecer a Xavier Caicedo por todas sus enseñanzas e invaluable consejos, especialmente por sus lecciones de humildad; a Carlos Montenegro que aparte de ser un matemático brillante es una gran persona, a Luis Jaime Corredor por su apoyo en la elaboración de este trabajo y a Ahmed quien fue un gran apoyo durante mis primeros años en la universidad.

Especialmente quiero agradecer a German, el mejor de los amigos, aquel que con su talento especial para los grupos me ayudó a entender el álgebra y algunas cosas de la vida y la fe. A Jaime, Andrés y Mauricio toda mi admiración, me siento muy feliz de haber compartido mi carrera con uds, y como alguien dijo una vez. Espero nos veamos entre los grandes.

Finalmente agradezco a la persona mas especial en mi vida, ya que sin ella no podría haber superado esta etapa y mucho menos habría logrado culminar este trabajo. Por esto y por hacer de mi una mejor persona, gracias Andrea.

Índice de contenido

0.1. INTRODUCCIÓN	2
1. Problemas de Fermat	5
1.1. La Ecuación $x^2 + 2 = y^3$	6
1.2. La Ecuación $x^2 + 4 = y^3$	7
1.3. Fermat y el Descenso	9
2. Dominios de Dedekind	11
2.1. Módulos	12
2.2. Clausura Entera.	13
2.3. Localización.	17
2.3.1. Estructuras de los anillos de fracciones.	18
2.3.2. Localización de Módulos	20
2.3.3. Dominios de Factorización Única en Ideales Primos “DFUP”	23
3. Grupo de Clases De Ideales	25
3.1. Pruebas de factorización en dominios de Dedekind.	25
3.2. Normas y Trazas	30
3.3. Normas de Ideales	33
3.4. Primos Regulares	35
4. $\mathfrak{C}(\mathbb{Z})_{\mathbb{Q}(\zeta_p)}$ y Fermat caso I	39
4.1. $\mathbb{Z}[\zeta_p]$ y sus propiedades	39
4.2. Raíces de la unidad en $\mathbb{Q}(\zeta_p)$	41
4.3. Fermat Caso I	44
5. Teoría Analítica de Numeros y Fermat CasoII	46
5.1. Los Numeros de Bernoulli	46
5.2. Congruencias y criterio de regularidad	49
5.3. Fermat Caso II	50
5.4. Irregulares e Infinitud	54
Bibliografía	56

0.1. INTRODUCCIÓN

El matemático Frances Pierre de Fermat¹, mantuvo intrigados durante mas de tres siglos a los matemáticos de todo el mundo a raíz de una nota que dejó en el margen de su copia de la *arithmetic* de Diofanto², un clásico de la matemática griega. En ella, Fermat afirmaba que la ecuación $X^n + Y^n = Z^n$ no tenía soluciones en números enteros X, Y, Z diferentes a cero, salvo para n igual a 1,2. "He encontrado una demostración maravillosa para este problema, pero el margen es muy pequeña para escribirla", anotó.

Todo esto ocurrió a mitades del siglo XVII. Tiempo después, muchos matemáticos se pusieron en la tarea de probar esta afirmación que resistió a ser probada por mas de tres siglos. Esto en realidad es algo asombroso, dado que el enunciado es muy sencillo de entender, hasta para una persona que no este en el ambiente de las matemáticas, para mí lo que hizo interesante el problema fue, precisamente esto: que algo tan sencillo fuera un reto para muchos de los hombres mas brillantes.

Bueno la pregunta que se debe plantear es la siguiente: ¿un problema como este aporta algún conocimiento matemático?, no sólo la satisfacción de resolver un problema difícil, este es el punto más interesante del problema, la riqueza de las teorías dejadas por los hombres que se enfrentaron a este problema, entre ellos Kummer³, quien pensó abstraer las propiedades fundamentales de \mathbb{Z} y crear extensiones de \mathbb{Z} mismo donde se cumplan la mayoría de ellas, para así poder tratar de encontrar soluciones a esta ecuación, en este punto Dedekind⁴ jugó un papel muy especial ya que el desarrolló una teoría completa sobre el comportamiento de estas extensiones. Estas extensiones son las que llamaremos anillos de Dedekind, donde fundamentalmente se cumplen propiedades de factorización única similares “no iguales” a las de \mathbb{Z} .

Para el siglo XVIII se conocía que para $n = 3$ y $n = 4$ la afirmación era cierta,

¹Pierre de Fermat (1601-1675), Frances

²Diofanto de Alejandría Siglo 2 A.C

³Ernst Eduard Kummer (1810-1893), Alemán

⁴Julius Wilhem Richard Dedekind (1831-1916), Alemán

esto gracias a Euler⁵ y el **método del descenso infinito** de Fermat. Fermat comenzó suponiendo una solución hipotética en el caso $n = 4$, examinando las propiedades de esta solución Fermat demostró que existiría otra solución mas pequeña. Luego, examinando esta nueva solución, Fermat podía demostrar que tendría que haber otra solución aún mas pequeña que la anterior, y así sucesivamente, por tanto Fermat logró encontrar una cadena descendiente de enteros positivos lo que es imposible. Esta contradicción muestra que la suposición inicial de solución era falsa. Resueltos los casos 3, 4, se puede ver mediante un razonamiento sencillo es fácil ver que es suficiente probarlo para los primos mayores o iguales a cinco.

La Prueba del caso 3 elaborada por Euler, introducía en el problema extensiones de \mathbb{Z} y numeros complejos, por esto estudiaré los anillos $\mathbb{Z}[\zeta_p]$ extensiones de \mathbb{Z} que son Dedekind, estas extensiones de los enteros no necesariamente cumplen factorización única en irreducibles "DFU", sin embargo muchos matemáticos lo supusieron, entre ellos el más famoso Lamé⁶, quien paso una prueba errónea del teorema de Fermat asumiendo "DFU" lo cual no era cierto. El primer contra-ejemplo fue encontrado por Kummer para $p = 23$ (ver [9] Capitulo 1), así Kummer desarrolló su teoría de las clases de grupos sobre dominios de Dedekind, definidos por una relación de equivalencia sobre los ideales del anillo y una operación con la cual obtenía un grupo. Es muy llamativo el hecho de que para anillos de Dedekind el orden del grupo es finito; que es el gran teorema de Kummer. Ahora, la aplicación de esto es importante para UTF "Ultimo Teorema de Fermat" , ya que si denotamos por H_p el orden del grupo sobre $\mathbb{Z}[\zeta_p]$ si p no divide a H_p se cumple UTF. A esta clase de números se les conoce como primos regulares, sin embargo existe un inconveniente y es que se conoce que hay infinitos primos no regulares, por ejemplo 37, 59, 67 estos sólo en los primeros cien números.

Este documento esta elaborado con el fin de mostrar en un contexto histórico como con las ideas desarrolladas por Euler y la teoría desarrollada por Kummer, se puede

⁵Leonard Euler (1701-1783), Suizo

⁶Gabriel Lamé (1795-1890), Frances

abrir un camino totalmente algebraico para llegar a la demostración de UTF para primos regulares.

En el capítulo uno, se dan pruebas algunas de las preguntas que Fermat dejó sin resolver. Esto, con el fin de ilustrar al lector como se tratará el UTF en los capítulos finales.

En los capítulos dos y tres se elabora con todo el detalle (esperando complementar los textos actuales), toda la maquinaria necesaria en pruebas posteriores. En los capítulos finales es presentada una clasificación muy detallada del anillo $\mathbb{Z}[\zeta_p]$, aclarando cualquier duda que el lector haya podido encontrar en otros textos. Todo esto para al final mostrar pruebas de UTF en el caso regular.

Finalmente se introducen los numeros de Bernoulli, para con estos dar una herramienta sencilla de verificación de cuando un primo es regular o no.

1. Problemas de Fermat

Mirando en el pasado podemos ver que el UTF no fue el único problema que hizo celebre a Fermat, su fama se vio verdaderamente confirmada gracias a una serie de retos matemáticos. Por ejemplo, Fermat observo que el número 26 se halla entre los números 25 y 27, uno de los cuales es un cuadrado y el otro un cubo. Buscó otros números en medio de un cuadrado y un cubo pero no halló ninguno, y sospecho que 26 era el único. Esta propiedad de 26 se puede expresar fácilmente como $25+2=27$ es la única solución en números enteros de $x^2 + 2 = y^3$, años después esta ecuación se le conocería con el nombre de ecuación de Bachet. Al parecer como en UTF Fermat no dió prueba alguna de haber encontrado una demostración a su afirmación de 26, sin embargo Fermat comunicó esta propiedad única del número 26 a la comunidad matemática y luego los retó a demostrar que era cierta. Abiertamente Fermat afirmó que él mismo tenía una demostración; la pregunta era, sin embargo, ¿tenían otros el ingenio para encontrarla también? A pesar de la simplicidad del enunciado, parecía ser que la demostración era bastante complicada, y Fermat se deleitó especialmente desafiando al matemático inglés Wallis, quien finalmente tuvo que declararse derrotado, no solo con este problema si no además, con uno muy similar también propuesto por Fermat; 6 esta dos adelante de 4 y dos atrás de 8, un cuadrado y un cubo, al igual que 6, 123 también cumple esta propiedad según Fermat 6 y 123 son los únicos con esta propiedad.

En este capítulo se elaboran pruebas a los retos que Fermat propuso a Wallis, muy seguramente el estilo de estas pruebas no sería el utilizado por Fermat, si él en verdad resolvió estos problemas. Si no mas bien algo al estilo de Euler quién introdujo los complejos con el caso $n = 3$ de UTF.

1.1. La Ecuación $x^2 + 2 = y^3$

Nótese que $x^2 + 2 = (x - \sqrt{-2})(x + \sqrt{-2})$, así pues lo mas lógico para estudiar esta ecuación sería considerar el anillo $\mathbb{Z}[\sqrt{-2}] := \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}$. Lo primero es verificar si es dominio Euclidiano. Sea $\alpha = a + b\sqrt{-2}$ un elemento de nuestro anillo y definimos la valuación $N(\alpha) = \alpha\bar{\alpha} \in \mathbb{Z}$, claramente N es multiplicativa, ahora veamos que N es una valuación euclidiana. Sean $\alpha = a + b\sqrt{-2}$, $\gamma = c + d\sqrt{-2}$, γ no cero, a, b, c, d enteros. Sea $\frac{\alpha}{\gamma} = r + s\sqrt{-2}$ y encuéntrense dos enteros m y n tales que $|r - m| \leq \frac{1}{2}$ y $|s - n| \leq \frac{1}{2}$. Es claro que siempre se les puede encontrar tomando parte entera de r o $r + 1$. Sea $\beta = m + n\sqrt{-2}$ y considérese $N(\frac{\alpha}{\gamma} - \beta) = (r - m)^2 + 2(s - n)^2 \leq \frac{1}{2} + \frac{1}{4} = \frac{3}{4} < 1$, de aquí y por N ser multiplicativa se puede concluir que $N(\alpha - \gamma\beta) < N(\gamma)$, por lo tanto N es una valuación euclidiana. Con un poco de congruencias básicas se puede ver que si (x, y) son solución a nuestra ecuación los dos deben ser impares¹, por otro lado si $N(\lambda)$ es primo entonces λ es irreducible, así que $\sqrt{-2}$ es irreducible en $\mathbb{Z}[\sqrt{-2}]$, y dado que este es un D.I.P, $\langle \sqrt{-2} \rangle$ es maximal. Lo siguiente a probar es que si (x, y) es solución entonces $(x - \sqrt{-2})$ y $(x + \sqrt{-2})$ son coprimos, para ver esto sea π un divisor irreducible de ambos, entonces π divide a $2\sqrt{-2} = -(\sqrt{-2})^3$ como π es irreducible que equivale a primo en D.F.U entonces $\pi|\sqrt{-2}$ con lo que obtendríamos $\langle \sqrt{-2} \rangle \subseteq \langle \pi \rangle$ y entonces π y $\sqrt{-2}$ son asociados, por tanto $N(\pi) = N(\sqrt{-2})^2$. Puesto que $\pi|y^3$ tomando normas se obtendría $2|y^6$ lo que es una contradicción, así que $(x - \sqrt{-2})$ y $(x + \sqrt{-2})$ son coprimos y como estamos en un D.F.U y están igualados a un cubo cada uno debe ser un cubo, así que existen enteros p, q tales que $(x + \sqrt{-2}) = (p + q\sqrt{-2})^3$. Resolviendo este cubo, $(p + q\sqrt{-2})^3 = (p^2 + 2pq\sqrt{-2} - 2q^2)(p + q\sqrt{-2}) = (p^3 + 2pq^2\sqrt{-2} - 2pq^2 + qp^2\sqrt{-2} - 4pq^2 - 2q^3) = p^3 - 2pq^2 - 4pq^2 + (2p^2q + p^2q - 2q^3)\sqrt{-2} = p(p^2 - 6q^2) + q(3p^2 - 2q^2)\sqrt{-2}$ que igualando las correspondientes partes dá:

$$x = p(p^2 - 6q^2) \tag{1.1}$$

$$1 = q(3p^2 - 2q^2) \tag{1.2}$$

¹tome congruencias módulo dos y después modulo cuatro

²si α es unidad $N(\alpha) = 1$

De (1.2), q es 1 o -1 , pero si fuera -1 p no sería entero, así que $q = 1$ de donde p es 1 o -1 , y así x toma los valores 5 o -5 . Reemplazando en la ecuación original vemos que solo existen las soluciones $(5, 3)$ y $(-5, 3)$.

1.2. La Ecuación $x^2 + 4 = y^3$

Se puede probar que $\mathbb{Z}[\sqrt{-1}]$ es un dominio euclidiano siguiendo un procedimiento similar al utilizado con $\mathbb{Z}[\sqrt{-2}]$.

Supongamos que x, y son soluciones enteras de $x^2 + 4 = y^3$, por el pequeño teorema de Fermat, tenemos que $x \equiv y \pmod{2}$.

Caso 1: x, y impares.

$x^2 + 4 = y^3$, muestra que x, y deben ser primos relativos, es decir $\langle x, y \rangle = 1$. Notese que en $\mathbb{Z}[i]$ el lado izquierdo de la ecuación se puede factorizar como $(x + 2i)(x - 2i)$.

Afirmación 1.2.1. $x + 2i, x - 2i$ son primos relativos.

Demostración. Sea π irreducible que divide a los dos entonces $\pi|4i$. Como $4i = (1 - i)^4(-i)$ y π es irreducible $\pi|(1 - i)$ entonces $\langle 1 - i \rangle \subseteq \langle \pi \rangle$ y como $1 - i$ es primo³ entonces $\langle 1 - i \rangle$ es maximal; por lo tanto $\langle 1 - i \rangle = \langle \pi \rangle$. Así que $1 - i|x + 2i$ y entonces $1 - i|x$. Tomando normas, $2|x^2$, lo cual contradice la paridad de x . Por tanto $x + 2i$ y $x - 2i$ son primos relativos. Como $\mathbb{Z}[i]$ es DFU y su producto es un cubo cada uno es un cubo, pues toda unidad es un cubo en $\mathbb{Z}[i]$ ($i = (-i)^3$, $-i = (i)^3$, $-1 = (-1)^3$, $1 = (1)^3$), así que existen $a, b \in \mathbb{Z}$ tales que $(x + 2i) = (a + ib)^3$. Desarrollando el cubo:

$$x = a(a^2 - b^2) - 2ab^2 \tag{1.3}$$

$$2 = b(3a^2 - b^2) \tag{1.4}$$

En (1.4) hay solo cuatro posibilidades para b que son $\{2, -2, 1, -1\}$.

i) Si $b = 2$, $3a^2 = 5$, contradicción.

³ $N(1 - i) = 2$

ii) Si $b = -2$, $a = \{1, -1\}$.

iii) Si $b = 1$, $a = \{1, -1\}$.

iv) Si $b = -1$, $3a^2 = -1$, contradicción.

Así los únicos casos posibles son (ii), (iii).

Reemplazando en (1.3) lo obtenido en el caso (ii), $x = \pm 11$, y reemplazando en (1.3) lo obtenido en el caso (iii) $x = \pm 2$, lo cual contradice la paridad.

Se sigue que las únicas soluciones para esta caso son: $(11, 5), (-11, 5)$. †

Caso 2: x, y pares.

Entonces $x = 2x_0$ $y = 2y_0$ para algunos enteros x_0, y_0 tales que $x_0^2 + 1 = 2y_0^3$. Claramente x_0 es impar, y y_0 también, de lo contrario -1 sería un cuadrado modulo 4. Entonces $x_0 = 2k + 1$ para algún entero k , como $(x_0 + i)(x_0 - i) = 2y_0^3$ se tiene que $(2k + 1 + i)(2k + 1 - i) = 2y_0^3$, entonces $(1 - i)(1 + i)((1 - i)k + 1)((1 + i)k + 1) = 2y_0^3$, cancelando el 2 $((1 - i)k + 1)((1 + i)k + 1) = y_0^3$. Haciendo $\alpha = ((1 - i)k + 1)$ $\beta = ((1 + i)k + 1)$ se tiene que $\beta + i\alpha = 1 - i$, como $\langle 1 - i \rangle$ es maximal entonces $\langle \alpha, \beta \rangle = \langle 1 \rangle$ o $\langle \alpha, \beta \rangle = \langle 1 - i \rangle$. Si $\langle \alpha, \beta \rangle = \langle 1 - i \rangle$, $1 - i | y_0^3$. Tomando normas $2 | y_0^6$ entonces $2 | y_0$ contradicción. $\langle \alpha, \beta \rangle = \langle 1 \rangle$ implica que cada uno es un cubo, así que existen $(a, b) \in \mathbb{Z}$ tales que $(1 - i)k + 1 = (a + ib)^3$ y $k + 1 - ki = (a + ib)^3$. Igualando parte real e imaginaria:

$$k + 1 = a(a^2 - 3b^2) \quad (1.5)$$

$$k = b(3a^2 - b^2) \quad (1.6)$$

Restando las ecuaciones,

$$a^3 - 3ab^2 - 3ba^2 + b^3 = 1$$

$$a^3 + b^3 - 3ab(a + b) = 1$$

$$(a + b)(a^2 - ab + b^2 - 3ab) = 1$$

$$(a + b)[(a + b)^2 - 6ab] = 1$$

Dado que a, b son enteros $a + b = \pm 1$ en cuyo caso $(a + b)^2 = 1$

i) Si $(a + b) = 1$, $1 - 6ab = 1$ entonces $ab = 0$

ii) Si $(a + b) = -1$, $6ab - 1 = 1$ entonces $6ab = 2$, contradicción.

así lo único que nos queda es $ab = 0$, $a = b = 0$ es imposible ya que $a + b = 1$.

Si $b = 0$ por (1.6) $k = 0$, reemplazando en (1.5), $a^3 = 1$ entonces $a = 1$.

Si $a = 0$ por (1.5) $k = -1$, reemplazando en (1.6), $-b^3 = -1$ entonces $b = 1$. Así los únicos valores posibles para k son $-1, 0$, de donde $x_0 = \pm 1$ y $x = \pm 2$, reemplazando en la ecuación original $4 + 4 = y^3$ y $y = 2$. Así en general las únicas soluciones en enteros de $x^2 + 4 = y^3$ son $(\pm 11, 5), (\pm 2, 2)$.

1.3. Fermat y el Descenso

Ahora pensando en el UTF, aunque Fermat no probó su afirmación, si abrió un camino con su prueba para la ecuación $x^4 + y^4 = z^4$, dando a conocer su método del **descenso infinito**. Este método consiste en suponer una solución ligada a un natural y mostrar que si esta existe existiría otra en la cual el natural sería menor, esto implicaría una sucesión decreciente infinita de números naturales, lo que es imposible.

Notese que dados n, m enteros tales que $n|m$ si $x^n + y^n = z^n$ no tiene solución en enteros x, y, z diferentes a cero, tampoco la ecuación $x^m + y^m = z^m$. Dado lo anterior y que todo entero $n > 2$ se factoriza como producto de primos impares o múltiplos de 4 es claro que UTF es equivalente a que

$$x^p + y^p = z^p \tag{1.7}$$

no tenga soluciones no triviales con p primo impar. En este punto, por simplificar el trabajo, es conveniente separar el problema en 2 casos:

Caso I: $p \nmid xyz$.

Caso II: $p \mid z$ y $p \nmid xy$.

El caso I es mucho más sencillo que el II. Esto es claro en el caso de la ecuación

$$x^3 + y^3 = z^3, \tag{1.8}$$

ya que todo cubo no congruente a cero módulo 3 es congruente a ± 1 módulo 9. Por tanto si 3 no divide a ninguno de x, y, z al cumplirse (1.8) claramente tendríamos una contradicción.

2. Dominios de Dedekind

Gracias a la fama que había tomado el UTF a inicios del siglo XIX la Academia matemática Francesa ofreció una serie de premios, entre ellos una medalla de oro y una gran cantidad de francos a aquel que pudiese demostrar o refutar el UTF. Así París se llenó de rumores de quién podría estar tratando y que estrategia estaría utilizando para resolver el problema. Luego, en marzo de 1847, se celebró en la Academia una reunión que pasaría a la historia.

Gabriel Lamé, que unos años antes había demostrado el caso 7, tomó el estrado frente a los más eminentes matemáticos de la época y proclamó que estaba a punto de demostrar el UTF, tan pronto como Lamé abandonó el estrado, Cauchy¹, otro de los grandes matemáticos de su época anunció que él también estaba muy cerca de lograr una demostración.

Luego unos pocos meses después, se hizo un anuncio que puso fin a toda especulación. Joseph Liouville² sorprendió a toda la audiencia al leer el contenido de una carta elaborada por Kummer quien llevaba algún tiempo estudiando los métodos que utilizaban Lamé y Cauchy. Para Kummer los estudios de ambos hombres los estaban dirigiendo al mismo callejón sin salida, y en su carta explicaba sus razones.

De acuerdo con Kummer, el problema fundamental de Cauchy y Lamé, era que ellos asumieron que las propiedades de factorización de los enteros seguían siendo válidas en extensiones de ellos. Kummer logró demostrar que esto no era necesariamente cierto, esto se convirtió en un error fatal para Cauchy y Lamé.

Debido a su descubrimiento, Kummer entendió que era importante estudiar el com-

¹Agustín Lois Cauchy(1789-1857) Frances

²Joseph Liouville(1809-1882) Frances

portamiento de las extensiones de los enteros. Por tanto, en este capítulo se presenta un resumen de muchos de los resultados del álgebra conmutativa que se necesitarán en capítulos posteriores. Resultados sobre módulos, localizaciones, dimensión de Krull³, anillos de Dedekind y en estos principalmente se da una prueba de **factorización única de ideales**.

2.1. Módulos

Definición 2.1.1. Si \mathcal{A} es un anillo, un \mathcal{A} -módulo \mathcal{M} es un grupo abeliano que se comporta en forma semejante a un espacio vectorial donde \mathcal{A} hace las veces de campo escalar. Siendo precisos, \mathcal{M} es un \mathcal{A} -módulo si para todas α, β en \mathcal{A} y todas m, n en \mathcal{M}

$$1m = m$$

$$(\alpha\beta)m = \alpha(\beta m)$$

$$(\alpha + \beta)m = (\alpha m) + (\beta m)$$

$$\alpha(m + n) = (\alpha m) + (\alpha n)$$

Ejemplo 2.1.2. *Todo grupo abeliano es un \mathbb{Z} -módulo, todo \mathbb{K} -espacio vectorial es un \mathbb{K} -módulo.*

Definición 2.1.3. Un \mathcal{A} -módulo se dice *libre* si tiene una **base**, donde base es un conjunto generador \mathcal{A} -linealmente independiente. Se puede probar que el cardinal de la base es único, así podemos hablar de la **dimensión** del \mathcal{A} -módulo libre como el cardinal de la base.

Definición 2.1.4. Un **homomorfismo** de \mathcal{A} -módulos es un morfismo F de grupos tal que $F(\alpha m) = \alpha F(m)$ para todas α en \mathcal{A} y m en \mathcal{M}

Definición 2.1.5. Dados tres \mathcal{A} -módulos $\mathcal{M}, \mathcal{M}^1, \mathcal{M}^2$, una sucesión de homomorfismos $f, g \mathcal{M}^1 \xrightarrow{f} \mathcal{M} \xrightarrow{g} \mathcal{M}^2$ se dice exacta si $Ker(g) = Im(f)$ y semi-exacta si $Im(f) \subseteq Ker(g)$.

³Wolfgang Krull (1899-1970) Alemán

Definición 2.1.6. Un anillo \mathcal{A} se dice **Noetheriano**⁴ si cumple cualquiera de las siguientes equivalencias:

1. Todo ideal de \mathcal{A} es finitamente generado.
2. Cualquier cadena creciente de ideales es estacionaria (condición de cadena ascendente)
3. Todo conjunto de ideales no vacío tiene un elemento maximal.

Definición 2.1.7. Un \mathcal{A} -módulo \mathcal{M} se dice **Noetheriano** si todo \mathcal{A} -submódulo de \mathcal{M} es finitamente generado.

La siguiente proposición es una generalización de un hecho de la teoría de grupos: todo subgrupo de un grupo abeliano finitamente generado es finitamente generado. Para una prueba de esta ver ([1], Capítulo2)

Proposición 2.1.8. *Dado \mathcal{A} un anillo Noetheriano, si \mathcal{M} es un \mathcal{A} -módulo finitamente generado, entonces \mathcal{M} es Noetheriano.*

Corolario 2.1.9. *Dados $\mathcal{A} \subseteq \mathcal{B}$ dos anillos, si \mathcal{A} es Noetheriano y \mathcal{B} es finitamente generado como \mathcal{A} módulo entonces \mathcal{B} es un anillo Noetheriano*

Demostración. Tome \mathcal{I} un ideal en \mathcal{B} , éste es claramente un \mathcal{A} -submódulo del \mathcal{A} -módulo \mathcal{B} . Por la proposición anterior \mathcal{I} es un \mathcal{A} -submódulo finitamente generado y como $\mathcal{A} \subseteq \mathcal{B}$ entonces \mathcal{I} es un ideal finitamente generado. †

2.2. Clausura Entera.

Definición 2.2.1. Sea \mathbb{D} un subanillo de un anillo \mathbb{R} . Un elemento $r \in \mathbb{R}$ se dice **entero sobre \mathbb{D}** si existe $p(x) \in \mathbb{D}[X]$ mónico tal que $p(r) = 0$

Definición 2.2.2. Sea \mathbb{D} un subanillo de un anillo \mathbb{R} , \mathbb{R} es una **extensión entera** de \mathbb{D} si solo sí todo elemento de \mathbb{R} es entero sobre \mathbb{D} .

⁴Amalie (Emmy) Noether (1882,1935) Alemana

Proposición 2.2.3. Sea \mathbb{D} un subanillo de un campo \mathbb{K} . Sea $k \in \mathbb{K}$. Las siguientes son equivalentes:

1. El elemento k es entero sobre \mathbb{D} .
2. El subanillo $\mathbb{D}[k]$ de \mathbb{K} , es un \mathbb{D} -módulo finitamente generado.
3. Existe un \mathbb{D} -submódulo \mathcal{M} de \mathbb{K} finitamente generado tal que $k\mathcal{M} \subset \mathcal{M}$.

Demostración. $1 \Rightarrow 2$, $2 \Rightarrow 3$ son claros. Ahora $3 \Rightarrow 2$: Sea $(e_i)_{i=\{1,2,\dots,n\}}$ un conjunto generador para \mathcal{M} , como por hipótesis $k\mathcal{M} \subset \mathcal{M}$ se tiene que ke_i pertenece a \mathcal{M} para todo $i \in \{1, 2, \dots, n\}$ así

$$\left[ke_i = \sum d_{ij}e_j \right] \quad (2.1)$$

, $d_{ij} \in \mathbb{D}$ $1 \leq i, j \leq n$. Sea \mathcal{D} la matriz (d_{ij}) y sea \mathcal{N} la matriz (e_i) , en notación matricial (2.1) dice que $k\mathcal{N}^T = \mathcal{M}\mathcal{N}^T$. Así la matriz $kI - \mathcal{M}$ es singular “ I es la matriz identidad” por esto $\det(kI - \mathcal{M}) = 0$, luego si tomamos $p(x) = \det(xI - \mathcal{M}) \in \mathbb{D}[X]$ obtenemos un polinomio mónico con coeficientes en \mathbb{D} que anula a k de donde se sigue el resultado. †

Corolario 2.2.4. Sea \mathbb{D} un subanillo de un campo \mathbb{K} , el conjunto de los elementos de \mathbb{K} enteros sobre \mathbb{D} forman un anillo.

Demostración. Las únicas propiedades no triviales de probar son la cerradura bajo suma y producto. Así, sean r, s en \mathbb{K} enteros sobre \mathbb{D} , por la proposición anterior $\mathbb{D}[r]$, $\mathbb{D}[s]$ son \mathbb{D} -módulos finitamente generados por esto, el \mathbb{D} -módulo $\mathbb{D}[r, s]$ será también finitamente generado. Entonces utilizando que $rs\mathbb{D}[r, s] \subseteq \mathbb{D}[r, s]$ y que $(r + s)\mathbb{D}[r, s] \subseteq \mathbb{D}[r, s]$ obtenemos que $(r + s)$ y rs son enteros sobre \mathbb{D} . †

Definición 2.2.5. Sea \mathbb{D} un subdominio de un campo \mathbb{K} . El anillo $\mathfrak{C}(\mathbb{D})_{\mathbb{K}}$ de elementos enteros de \mathbb{K} sobre \mathbb{D} se conoce como la **clausura entera** de \mathbb{D} sobre \mathbb{K} . Cuando $\mathbb{K} = \mathbb{Q}(\alpha)$, para algún α algebraico $\mathfrak{C}(\mathbb{Z})_{\mathbb{K}}$ se denomina el **anillo de enteros** de \mathbb{K} .

Definición 2.2.6. Un dominio \mathbb{D} es **íntegramente cerrado** si y sólo si $\mathbb{D} = \mathfrak{C}(\mathbb{D})_{\mathbb{Q}(\mathbb{D})}$

Lema 2.2.7. Si \mathbb{D} es un DFU entonces \mathbb{D} es íntegramente cerrado.

Demostración. Sea $f(x) \in \mathbb{D}[x]$ con $f(x) = \sum_{i=0}^n f_i x^i$ mónico, y supongamos $p, q \neq 0$ elementos de \mathbb{D} sin factores en común tales que $f(\frac{p}{q}) = 0$. Así tendríamos que $\sum_{i=0}^n f_i (\frac{p}{q})^i = 0$, multiplicando todo por q^n obtenemos $-p^n = q \sum_{i=0}^{n-1} f_i p^i q^{(n-1)-i}$ así q dividiría a p^n . Pero como q y p son primos relativos q tiene que ser un invertible, de donde $\frac{p}{q} \in \mathbb{D}$. †

Lema 2.2.8. Sea $\mathbb{D}_1, \mathbb{D}_2, \mathbb{D}_3$ tres dominios encadenados. \mathbb{D}_3 es entera sobre \mathbb{D}_1 si y solo si \mathbb{D}_3 es entera sobre \mathbb{D}_2 y \mathbb{D}_2 es entera sobre \mathbb{D}_1 .

Demostración. La parte no trivial es el "sólo si". Supongamos que \mathbb{D}_3 es entera sobre \mathbb{D}_2 y \mathbb{D}_2 es entera sobre \mathbb{D}_1 . Sea $\lambda \in \mathbb{D}_3$, como \mathbb{D}_3 es entera sobre \mathbb{D}_2 existe un polinomio mónico en $\mathbb{D}_2[x]$ que se anula en λ . Sean d_0, \dots, d_{n-1} los coeficientes de este polinomio, por la proposición (2.2.3-2) utilizada inductivamente tenemos que $\mathbb{B} := \mathbb{D}_1[d_0, \dots, d_{n-1}]$ es un \mathbb{D}_1 -módulo finitamente generado. Por la construcción de \mathbb{B} es sencillo verificar que $\lambda \mathbb{B}[\lambda] \subseteq \mathbb{B}[\lambda]$, así por (2.2.3-2) λ es entero sobre \mathbb{D}_1 . †

Proposición 2.2.9. Sea \mathbb{D} un dominio y sea \mathbb{K} una extensión algebraica de $\mathbb{Q}(\mathbb{D})$, entonces:

1. $\mathbb{Q}(\mathfrak{C}(\mathbb{D})_{\mathbb{K}}) = \mathbb{K}$, más aún, dado $\lambda \in \mathbb{K}$ existen $\gamma \in \mathfrak{C}(\mathbb{D})_{\mathbb{K}}$ y $\alpha \in \mathbb{D}$ tales que $\lambda = \frac{\gamma}{\alpha}$.
2. Si \mathbb{D} es íntegramente cerrado entonces $\mathbb{D} = \mathbb{Q}(\mathbb{D}) \cap \mathfrak{C}(\mathbb{D})_{\mathbb{K}}$.
3. $\mathfrak{C}(\mathbb{D})_{\mathbb{K}}$ es íntegramente cerrado.
4. Si la extensión \mathbb{K} de $\mathbb{Q}(\mathbb{D})$ es de Galois con grupo de Galois G , se tiene que para todo $\sigma \in G$ $\sigma(\mathfrak{C}(\mathbb{D})_{\mathbb{K}}) = \mathfrak{C}(\mathbb{D})_{\mathbb{K}}$, y si \mathbb{D} es íntegramente cerrado, $\mathbb{D} = (\mathfrak{C}(\mathbb{D})_{\mathbb{K}})^G := \{d \in \mathfrak{C}(\mathbb{D})_{\mathbb{K}} : \sigma(d) = d \forall \sigma \in G\}$.

Demostración. 1. Sea $\lambda \in \mathbb{K}$, sea $p(x) \in \mathbb{Q}(\mathbb{D})[x]$, $p(x) = \sum_{i=0}^n p_i x^i$ polinomio mónico mínimo de λ , como $p(x) \in \mathbb{Q}(\mathbb{D})[x]$ existe $\alpha \in \mathbb{D}^*$ tal que $\alpha p(x) \in \mathbb{D}[x]$. Como $\alpha^n p(\lambda) = 0$ podemos construir un polinomio mónico $q(x) = \sum_{i=0}^n q_i x^i$ en $\mathbb{D}[x]$ que se anula en $\alpha\lambda$, donde $q_i = p_i \alpha^{n-i}$; $0 \leq i \leq n$. Así podemos ver que $q(\alpha\lambda) = \alpha^n p(\lambda)$ lo cual implica que $\alpha\lambda = \gamma$ para algún $\gamma \in \mathfrak{C}(\mathbb{D})_{\mathbb{K}}$.

2. Trivialmente de la definición,
3. Ya que $\mathfrak{C}(\mathfrak{C}(\mathbb{D})_{\mathbb{K}})_{\mathbb{K}}$ es entera sobre $\mathfrak{C}(\mathbb{D})_{\mathbb{K}}$ que a su vez es entera sobre \mathbb{D} , por (2.2.8) $\mathfrak{C}(\mathfrak{C}(\mathbb{D})_{\mathbb{K}})_{\mathbb{K}}$ es entera sobre \mathbb{D} pero esto implica que $\mathfrak{C}(\mathfrak{C}(\mathbb{D})_{\mathbb{K}})_{\mathbb{K}} = \mathfrak{C}(\mathbb{D})_{\mathbb{K}}$ lo cual unido a (1) implica que $\mathfrak{C}(\mathbb{D})_{\mathbb{K}}$ es íntegramente cerrado.
4. Sea $p(x) \in \mathbb{D}[x]$ mónico, $\sigma(p(x)) = p(\sigma(x))$ para todo $\sigma \in G$, así los elementos de G llevan enteros en enteros. Por otro lado sabemos que $\mathbb{K}^G = \mathbb{Q}(\mathbb{D})$ así que $(\mathfrak{C}(\mathbb{D})_{\mathbb{K}})^G = \mathfrak{C}(\mathbb{D})_{\mathbb{K}} \cap \mathbb{Q}(\mathbb{D}) = \mathbb{D}$ si \mathbb{D} es íntegramente cerrado. †

Lema 2.2.10. *Dado \mathbb{D} un dominio y sea \mathbb{K} extensión finita de $\mathbb{Q}(\mathbb{D})$ sea $\mathbb{B} = \mathfrak{C}(\mathbb{D})_{\mathbb{K}}$. Si \mathbb{B} es un \mathbb{D} -módulo libre finitamente generado, entonces la dimensión de \mathbb{B} es $[\mathbb{K} : \mathbb{Q}(\mathbb{D})]$.*

Demostración. Dada $\{v_1, \dots, v_n\}$ una base para \mathbb{B} sobre \mathbb{D} , por esto este conjunto es linealmente independiente sobre $\mathbb{Q}(\mathbb{D})$ ya que puedo quitar los denominadores, por la parte 1 de la proposición anterior este conjunto genera a \mathbb{K} sobre $\mathbb{Q}(\mathbb{D})$ †

Proposición 2.2.11. *Sea \mathcal{A} un dominio en el que ideal primo no trivial y maximal son equivalentes. Sea \mathcal{B} un dominio, extensión entera de \mathcal{A} . Entonces en \mathcal{B} ideal primo no trivial y maximal son equivalentes.*

Demostración. Ver ([8] Capitulo 1 Proposición 5.6) †

Proposición 2.2.12. *Sea \mathbb{K} extensión finita de \mathbb{Q} . Sea $\{v_1, \dots, v_n\} \subseteq \mathbb{B} = \mathfrak{C}(\mathbb{Z})_{\mathbb{K}}$ una base para \mathbb{K} sobre \mathbb{Q} , entonces existe $d \in \mathbb{Z}^*$ tal que el \mathbb{Z} -módulo \mathbb{B} está contenido en el \mathbb{Z} -módulo libre generado por $\{(v_1)/d, \dots, (v_n)/d\}$*

Demostración. Ver ([9] Capitulo 3) †

Corolario 2.2.13. *Sea \mathbb{K} extensión finita de \mathbb{Q} . Sea $\mathbb{B} = \mathfrak{C}(\mathbb{Z})_{\mathbb{K}}$. Entonces \mathbb{B} es un \mathbb{Z} -módulo libre finitamente generado.*

Demostración. Por la proposición anterior \mathbb{B} es subgrupo de un grupo abeliano finitamente generado, así \mathbb{B} también es finitamente generado y como \mathbb{B} es dominio es libre de torsión se sigue de la clasificación de los grupos abelianos finitamente generados que \mathbb{B} es suma directa de \mathbb{Z} . †

Definición 2.2.14. Sea A un dominio. El anillo A se dice **dominio de Dedekind** si cumple.

1. \mathcal{A} es Noetheriano.
2. En \mathcal{A} ideal primo no trivial y maximal son equivalentes⁵.
3. \mathcal{A} es íntegramente cerrado.

Teorema 2.2.15. Sea \mathbb{A} un dominio Noetheriano en el que ideal primo no trivial y maximal son equivalentes. Sea \mathbb{K} una extensión algebraica de $\mathbb{Q}(\mathbb{A})$, si $\mathfrak{C}(\mathbb{A})_{\mathbb{K}}$ es un \mathbb{A} -módulo finitamente generado se tiene que $\mathfrak{C}(\mathbb{A})_{\mathbb{K}}$ es un dominio de Dedekind.

Demostración. Corolario 2.1.9 , proposición 2.2.9-3 y proposición 2.2.11 muestran que $\mathfrak{C}(\mathbb{A})_{\mathbb{K}}$ es un dominio de Dedekind. †

2.3. Localización.

El concepto de localización es una herramienta que generaliza el campo de cocientes de un dominio cualquiera. Hablando rústicamente lo que se hace es tomar un subconjunto adecuado de un anillo y dar inversos a estos elementos, en el caso del campo de cocientes de un dominio el conjunto son todos menos el cero.

Definición 2.3.1. Sea A un anillo. Un subconjunto S de A se dice **multiplicativo** si:

1. $0 \notin S$ y $1 \in S$.
2. $a, b \in S \Rightarrow ab \in S$.

Ejemplo 2.3.2.

1. Sea \mathcal{P} ideal primo de \mathcal{A} , $\mathcal{S} := \mathcal{A} \setminus \mathcal{P}$.
2. Si A es dominio $\mathcal{S} := \mathcal{A} \setminus \{0\}$ un caso particular del anterior.

⁵Dimensión de Krull igual a 1

Dado un anillo A y un subconjunto multiplicativo \mathcal{S} de A se define una relación sobre el conjunto $\mathcal{A} \times \mathcal{S}$, de la siguiente forma: $(a, s) \sim (b, t)$ si existe $\sigma \in \mathcal{S}$ tal que $\sigma(at - bs) = 0$. Nótese que si A es un dominio como \mathcal{S} es multiplicativo tendríamos que $(at - bs) = 0$ que es la relación para construir el campo de cocientes de \mathcal{A} cuando \mathcal{S} es $\mathcal{A} \setminus \{0\}$

Afirmación 2.3.3. \sim es una relación de equivalencia sobre $\mathcal{A} \times \mathcal{S}$:

El conjunto de clases de equivalencia se denotará por $\mathcal{S}^{-1}\mathcal{A}$ y las clases se escribirán de la manera usual $[(a, s)] := \frac{a}{s}$, a este conjunto lo podemos dotar de dos operaciones $+$, \cdot .

definidas a partir de la suma y el producto del anillo de la siguiente manera:

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

Es sencillo ver que están bien definidas y que $\langle \mathcal{S}^{-1}\mathcal{A}, +, \cdot, [(0, 1)], [(1, 1)] \rangle$ es un anillo.

Afirmación 2.3.4. Sea $\Gamma_{\mathcal{S}} : \mathcal{A} \mapsto \mathcal{S}^{-1}\mathcal{A}$
 $a \mapsto \frac{a}{1}$

- a) $\Gamma_{\mathcal{S}}$ es un homomorfismo de anillos.
- b) $\forall s \in \mathcal{S}$ $\Gamma_{\mathcal{S}}(s)$ es invertible y su inverso es $\frac{1}{s}$.
- c) Si \mathcal{A} es un dominio $\Gamma_{\mathcal{S}}$ es inyectiva.
- d) Si A es dominio entonces $\mathcal{S}^{-1}\mathcal{A}$ es dominio.
- e) Si A es dominio y $\mathcal{S} := \mathcal{A} \setminus \{0\}$ entonces $\mathcal{S}^{-1}\mathcal{A}$ es $\mathbb{Q}(\mathcal{A})$.

Para un estudio detallado véase ([1] Capitulo 4)

2.3.1. Estructuras de los anillos de fracciones.

En esta sección se estudiará la estructura de ideales de $\mathcal{S}^{-1}\mathcal{A}$, para analizar ciertas propiedades del anillo \mathcal{A} que se conservan en el anillo $\mathcal{S}^{-1}\mathcal{A}$, donde normalmente el trabajo será mucho mas sencillo.

Lema 2.3.5. Sea \mathcal{A} un anillo, $\mathcal{S} \subseteq \mathcal{A}$ multiplicativo, \mathcal{I} un ideal en \mathcal{A} y $\mathcal{S}^{-1}\mathcal{I} := \langle \Gamma_{\mathcal{S}}(\mathcal{I}) \rangle$ entonces $\mathcal{S}^{-1}\mathcal{I} = \{ \frac{x}{s} : x \in \mathcal{I}, s \in \mathcal{S} \}$, en particular: $\mathcal{S}^{-1}\mathcal{I} = \mathcal{S}^{-1}\mathcal{A} \iff \mathcal{I} \cap \mathcal{S} \neq \emptyset$.

Demostración. $\{ \frac{x}{s} : x \in \mathcal{I}, s \in \mathcal{S} \} \subseteq \mathcal{S}^{-1}\mathcal{I}$ es claro. Sea $z \in \mathcal{S}^{-1}\mathcal{I}$ entonces $z = \sum_{i=1}^n \left(\frac{a_i}{s_i} \right) \left(\frac{x_i}{1} \right)$ con $a_i \in \mathcal{A}$, $s_i \in \mathcal{S}$ y $x_i \in \mathcal{I}$. Reescribiendo $z = \sum_{i=1}^n \left(\frac{x_i a_i}{s_i} \right)$, si definimos $s := \prod_{i=1}^n s_i$, $\sigma_i := \frac{s}{s_i}$, $a_i x_i := y_i$ tenemos entonces $z = \sum_{i=1}^n \left(\frac{y_i \sigma_i}{s} \right)$ de donde $z = \frac{y}{s}$ con $y \in \mathcal{I}$, $s \in \mathcal{S}$.

Ahora si $\mathcal{I} \cap \mathcal{S} \neq \emptyset$, $\frac{1}{1} \in \mathcal{S}^{-1}\mathcal{I}$ lo que implica que $\mathcal{S}^{-1}\mathcal{I} = \mathcal{S}^{-1}\mathcal{A}$.

Si $\mathcal{S}^{-1}\mathcal{I} = \mathcal{S}^{-1}\mathcal{A}$, existen $x \in \mathcal{I}$, $s \in \mathcal{S}$ tales que $\frac{x}{s} = \frac{1}{1}$, lo cual por definición significa que existe $\sigma \in \mathcal{S}$ tal que $\sigma(x - s) = 0$, así que $\sigma x = \sigma s$, entonces $\mathcal{I} \cap \mathcal{S} \neq \emptyset$. †

Observación 2.3.6. En general no siempre es cierto que si tengo un homomorfismo de anillos $\Gamma : \mathcal{A} \rightarrow \mathcal{B}$ y \mathcal{J} un ideal de \mathcal{B} entonces $\langle \Gamma^{-1}(\mathcal{J}) \rangle = \mathcal{J}$. La inclusión que siempre se tiene es \subseteq , pero en el caso de $\Gamma_{\mathcal{S}}$ es muy sencillo verificar la igualdad.

Corolario 2.3.7. Si \mathcal{A} es un anillo noetheriano, $\mathcal{S} \subseteq \mathcal{A}$ multiplicativo entonces $\mathcal{S}^{-1}\mathcal{A}$ es noetheriano.

Demostración. Se sigue de que $\langle \Gamma_{\mathcal{S}}^{-1}(\mathcal{J}) \rangle = \mathcal{J}$, para todo ideal \mathcal{J} en $\mathcal{S}^{-1}\mathcal{A}$. †

Definición 2.3.8. Sea \mathcal{A} un anillo, $SPEC(\mathcal{A}) :=$ ideales primos no triviales de \mathcal{A} .

Definición 2.3.9. Sea \mathcal{A} un anillo y $\mathcal{P} \in SPEC(\mathcal{A})$. Si $\mathcal{S} := \mathcal{A} \setminus \mathcal{P}$ a $\mathcal{S}^{-1}\mathcal{A}$ se le llama la **localización** de \mathcal{A} en \mathcal{P} y la denotamos $\mathcal{A}_{\mathcal{P}}$.

Lema 2.3.10. Sea \mathcal{A} un anillo, $\mathcal{S} \subseteq \mathcal{A}$ multiplicativo y $\mathcal{P} \in SPEC(\mathcal{A})$ tal que $\mathcal{P} \cap \mathcal{S} = \emptyset$. Entonces $\mathcal{S}^{-1}\mathcal{P} \in SPEC(\mathcal{S}^{-1}\mathcal{A})$.

Demostración. Como $\mathcal{P} \cap \mathcal{S} = \emptyset$ entonces $\mathcal{S}^{-1}\mathcal{P} \subsetneq \mathcal{S}^{-1}\mathcal{A}$. Sean $\frac{a}{s}, \frac{b}{t} \in \mathcal{S}^{-1}\mathcal{A}$, supongamos que $\frac{ab}{st} \in \mathcal{S}^{-1}\mathcal{P}$, entonces existen $r \in \mathcal{S}$ $c \in \mathcal{P}$ con $\frac{ab}{st} = \frac{c}{r}$. Lo que implica que existe $\sigma \in \mathcal{S}$ con $\sigma(abr - cst) = 0$, como \mathcal{P} es primo $abr - cst \in \mathcal{P}$ y puesto que $c \in \mathcal{P}$ y $r \notin \mathcal{P}$ se sigue que $ab \in \mathcal{P}$ entonces $a \in \mathcal{P}$ ó $b \in \mathcal{P}$ de lo que se concluye que $\frac{a}{s} \in \mathcal{S}^{-1}\mathcal{P}$ ó $\frac{b}{t} \in \mathcal{S}^{-1}\mathcal{P}$. †

De los resultados anteriores nos queda como corolario una proposición muy interesante. Existe una correspondencia biyectiva entre el retículo de ideales primos de \mathcal{A} que no intersecan a \mathcal{S} y el retículo de ideales primos de $\mathcal{S}^{-1}\mathcal{A}$.

Proposición 2.3.11. *Sea A un anillo y $S \subseteq A$ multiplicativo el homomorfismo Γ_S induce una biyección $\Gamma_S^* : \text{SPEC}(S^{-1}A) \Rightarrow \{\mathcal{P} \in \text{SPEC}(A) : \mathcal{P} \cap S = \emptyset\}$; con $\Gamma_S^*(\mathcal{J}) := \Gamma_S^{-1}(\mathcal{J})$. De hecho, Γ_S^* respeta inclusiones.*

Corolario 2.3.12. *Sea A un anillo en el que ideal primo y maximal son equivalentes. Sea $S \subseteq A$ multiplicativo, tal que existe $\mathcal{P} \in \text{SPEC}(A)$ con $\mathcal{P} \cap S = \emptyset$, entonces en $S^{-1}A$ primo y maximal también son conceptos equivalentes.*

Lema 2.3.13. *Sea A íntegramente cerrado. Dado $S \subseteq A$ multiplicativo. Entonces $S^{-1}A$ es íntegramente cerrado.*

Demostración. Es claro que $\mathbb{Q}(A) = \mathbb{Q}(S^{-1}A)$. Sea $\frac{a}{b} \in \mathbb{Q}(A)$, suponga que existe polinomio mónico $f(x)$ en $S^{-1}A[x]$ de grado n tal que $f(\frac{a}{b}) = 0$. Sean s_0, \dots, s_{n-1} los denominadores de los coeficientes del polinomio. Si definimos $s := \prod_{i=0}^{n-1} s_i$, y hacemos $s^n f(\frac{a}{b}) = 0$, asociando adecuadamente obtendremos un polinomio mónico en $A[x]$ con raíz $\frac{sa}{b}$, como A es íntegramente cerrado existe $c \in A$ tal que $\frac{a}{b} = \frac{c}{s}$. †

Corolario 2.3.14. *Sea A un dominio de Dedekind. Sea $S \subseteq A$ multiplicativo, tal que existe $\mathcal{P} \in \text{SPEC}(A)$ con $\mathcal{P} \cap S = \emptyset$ entonces en $S^{-1}A$ es dominio de Dedekind.*

Corolario 2.3.15. *Sea A un dominio de Dedekind entonces $\mathcal{A}_{\mathcal{P}}$ es dominio de Dedekind para todo $\mathcal{P} \in \text{SPEC}(A)$.*

2.3.2. Localización de Módulos

En esta sección se generaliza la noción de anillo de fracciones a **módulo de fracciones**, esto para probar hechos sobre la clausura entera de un dominio, por medio de las clausuras de sus localizaciones.

Dado un anillo A , un A -módulo M y $S \subseteq A$ multiplicativo, definimos una relación sobre $M \times S$, de la siguiente forma: $(m, s) \sim (n, t)$ si existe $\sigma \in S$ tal que $\sigma(mt - ns) = 0$. Esta es una relación de equivalencia y notamos al conjunto de clases como $S^{-1}M$ (**Módulo de fracciones** de M), este sera un $S^{-1}A$ -Módulo con la definición obvia de suma y producto.

Dado un homomorfismo de \mathcal{A} -módulos $f : \mathcal{M} \rightarrow \mathcal{N}$, f induce un homomorfismo de $\mathcal{S}^{-1}\mathcal{A}$ -módulos,

$$\begin{aligned} \mathcal{S}^{-1}(f) : \mathcal{S}^{-1}\mathcal{M} &\rightarrow \mathcal{S}^{-1}\mathcal{N} \\ \frac{m}{s} &\mapsto \frac{f(m)}{s} \end{aligned}$$

si g es otro \mathcal{A} -homomorfismo, $g : \mathcal{N} \rightarrow \mathcal{R}$ se tiene que: $\mathcal{S}^{-1}(g) \circ (f) = \mathcal{S}^{-1}(g) \circ \mathcal{S}^{-1}(f)$

⁶

Definición 2.3.16. Sea $\mathcal{P} \in \text{SPEC}(\mathcal{A})$. Si $\mathcal{S} = \mathcal{A} \setminus \mathcal{P}$, notamos a $\mathcal{S}^{-1}\mathcal{M}$ por $\mathcal{M}_{\mathcal{P}}$ y a $\mathcal{S}^{-1}(f)$ como $f_{\mathcal{P}}$.

Proposición 2.3.17. Sea $\mathcal{M}^1 \xrightarrow{f} \mathcal{M} \xrightarrow{g} \mathcal{M}^2$ una sucesión exacta de \mathcal{A} -módulos y sea $\mathcal{S} \subseteq \mathcal{A}$ multiplicativo. La sucesión de $\mathcal{S}^{-1}\mathcal{A}$ -módulos $\mathcal{S}^{-1}\mathcal{M}^1 \xrightarrow{\mathcal{S}^{-1}(f)} \mathcal{S}^{-1}\mathcal{M} \xrightarrow{\mathcal{S}^{-1}(g)} \mathcal{S}^{-1}\mathcal{M}^2$ es exacta.

Demostración. Sea $\frac{m}{s}$ en $\mathcal{S}^{-1}\mathcal{M}^1$. Entonces $(\mathcal{S}^{-1}(g) \circ \mathcal{S}^{-1}(f))(\frac{m}{s}) = \mathcal{S}^{-1}((g) \circ (f))(\frac{m}{s}) = \frac{(g) \circ (f)(m)}{s} = 0$ por lo tanto $\text{Imagen}(\mathcal{S}^{-1}(f)) \subseteq \text{Kernel}(\mathcal{S}^{-1}(g))$. Sea m/s en $\text{Kernel}(\mathcal{S}^{-1}(g))$ entonces $\frac{g(m)}{s} = 0$ así que existe σ en \mathcal{S} tal que $g(m)\sigma = 0$, como g es homomorfismo $m\sigma$ esta en $\text{Kernel}(g)$ que es igual a $\text{Imagen}(f)$, por lo que hay un n en \mathcal{M}^1 tal que $f(n) = m\sigma$. $\mathcal{S}^{-1}(f)(\frac{n}{s\sigma}) = \frac{m}{s}$. †

Corolario 2.3.18. Sea $0 \rightarrow \mathcal{M}^1 \xrightarrow{f} \mathcal{M} \xrightarrow{g} \mathcal{M}^2 \rightarrow 0$ una sucesión exacta de \mathcal{A} -módulos y sea $\mathcal{S} \subseteq \mathcal{A}$ multiplicativo. La sucesión de $\mathcal{S}^{-1}\mathcal{A}$ -módulos $0 \rightarrow \mathcal{S}^{-1}\mathcal{M}^1 \xrightarrow{\mathcal{S}^{-1}(f)} \mathcal{S}^{-1}\mathcal{M} \xrightarrow{\mathcal{S}^{-1}(g)} \mathcal{S}^{-1}\mathcal{M}^2 \rightarrow 0$ es exacta.

Corolario 2.3.19. Sea $\mathcal{S} \subseteq \mathcal{A}$ multiplicativo. Dado un homomorfismo de \mathcal{A} -módulos $f : \mathcal{M} \rightarrow \mathcal{N}$ se tiene:

$$\mathcal{S}^{-1}(\text{Imagen}(f)) = \text{Imagen}(\mathcal{S}^{-1}(f))$$

$$\mathcal{S}^{-1}(\text{Kernel}(f)) = \text{Kernel}(\mathcal{S}^{-1}(f))$$

⁶ \mathcal{S}^{-1} es un Functor de la Categoría de \mathcal{A} -módulos en la Categoría de $\mathcal{S}^{-1}\mathcal{A}$ -módulos.

Lema 2.3.20. *Sea \mathcal{M} un \mathcal{A} -módulo. Las siguientes son equivalentes:*

1. $\mathcal{M} = (0)$
2. $\mathcal{M}_P = (0)$ para todo $P \in \text{Spec}(\mathcal{A})$
3. $\mathcal{M}_P = (0)$ para todo $P \in \text{Max}(\mathcal{M})$

Demostración. Veamos $(3 \Rightarrow 1)$. Sea $m \in \mathcal{M}$, entonces $\frac{m}{1} = 0$ en \mathcal{M}_P para todo $P \in \text{Max}(\mathcal{M})$, así para cada P existe $x_P \in \mathcal{A} \setminus P$ tal que $mx_P = 0$. Sea $I(m)$ el ideal generado por los x_P . Por su definición $I(m)$ no está contenido en ningún ideal maximal, por lo tanto $I(m) = \langle 1 \rangle$ y así $1 = \sum_{i=1}^n a^i x_{P_i}$. Entonces $m = \sum_{i=1}^n a^i m x_{P_i} = 0$. Las otras implicaciones son triviales. †

Proposición 2.3.21. *Sea $\mathcal{M}^1 \xrightarrow{f} \mathcal{M} \xrightarrow{g} \mathcal{M}^2$ una sucesión semi-exacta de \mathcal{A} -módulos.*

Las siguientes son equivalentes:

1. $\mathcal{M}^1 \xrightarrow{f} \mathcal{M} \xrightarrow{g} \mathcal{M}^2$ es exacta en \mathcal{M} .
2. $\mathcal{M}_P^1 \xrightarrow{f_P} \mathcal{M}_P \xrightarrow{g_P} \mathcal{M}_P^2$ es exacta en \mathcal{M}_P para todo $P \in \text{Spec}(\mathcal{A})$.
3. $\mathcal{M}_P^1 \xrightarrow{f_P} \mathcal{M}_P \xrightarrow{g_P} \mathcal{M}_P^2$ es exacta en \mathcal{M}_P para todo $P \in \text{Max}(\mathcal{A})$.

Demostración. Veamos $(3 \Rightarrow 1)$, consideremos la sucesión exacta $0 \rightarrow \text{Im}(f) \xrightarrow{i} \text{Ker}(g) \xrightarrow{\pi} \text{Ker}(g)/\text{Im}(f) \rightarrow 0$ por el corolario 2.3.14 $0 \rightarrow (\text{Im}(f))_P \xrightarrow{i} (\text{Ker}(g))_P \xrightarrow{\pi} (\text{Ker}(g)/\text{Im}(f))_P \rightarrow 0$ Es una sucesión exacta de \mathcal{A}_P -módulos, para todo $P \in \text{Max}(\mathcal{A})$. Dado que $(\text{Im}(f))_P = \text{Im}(f_P)$, $(\text{Ker}(g))_P = \text{Ker}(g_P)$ y que la localización respeta cocientes $(\text{Ker}(g)/\text{Im}(f))_P = \text{Ker}(g_P)/\text{Im}(f_P)$, del lema 2.3.16 se sigue que $\text{Ker}(g)/\text{Im}(f) = (0)$ si y solo si $\text{Ker}(g_P)/\text{Im}(f_P) = (0)$ para todo $P \in \text{Max}(\mathcal{A})$.

$(1 \Rightarrow 2)$ es la proposición 2.3.13

$(2 \Rightarrow 3)$ es trivial. †

Corolario 2.3.22. *Sea \mathcal{A} un dominio. Entonces:*

$$\mathcal{A} = \bigcap_{P \in \text{Spec}(\mathcal{A})} \mathcal{A}_P = \bigcap_{P \in \text{Max}(\mathcal{A})} \mathcal{A}_P$$

Demostración. Considere la sucesión semi-exacta $\mathcal{A} \xrightarrow{i} \bigcap_{P \in \text{Spec}(\mathcal{A})} \mathcal{A}_P \Rightarrow 0$ sea $Q \in \text{Spec}(\mathcal{A})$, $\mathcal{A}_Q \xrightarrow{i_Q} \left(\bigcap_{P \in \text{Spec}(\mathcal{A})} \mathcal{A}_P \right)_Q = \bigcap_{P \in \text{Spec}(\mathcal{A})} (\mathcal{A}_P)_Q \subseteq \mathcal{A}_Q$ así i_Q es sobre para todo $Q \in \text{Spec}(\mathcal{A})$ así la inclusión ya era sobre por lo tanto $\mathcal{A} = \bigcap_{P \in \text{Spec}(\mathcal{A})} \mathcal{A}_P$ y como $\bigcap_{P \in \text{Max}(\mathcal{A})} \mathcal{A}_P \subseteq \bigcap_{P \in \text{Spec}(\mathcal{A})} \mathcal{A}_P$ se sigue la otra igualdad. †

Corolario 2.3.23. *Sea \mathcal{A} un dominio, las siguientes son equivalentes:*

1. \mathcal{A} es íntegramente cerrado
2. \mathcal{A}_P es íntegramente cerrado para todo $P \in \text{Spec}(\mathcal{A})$
3. \mathcal{A}_P es íntegramente cerrado para todo $P \in \text{Max}(\mathcal{A})$

Demostración. Sea $p(x)$ polinomio mónico en $A[x]$ con una raíz α en $\mathbb{Q}(\mathcal{A})$. $p(x)$ es también un polinomio mónico en $\mathcal{A}_P[x]$, para todo $P \in \text{Max}(\mathcal{A})$ como $\mathbb{Q}(\mathcal{A}) = \mathbb{Q}(\mathcal{A}_P)$ y \mathcal{A}_P es íntegramente cerrado para todo $P \in \text{Max}(\mathcal{A})$ tenemos que $\alpha \in \bigcap_{P \in \text{Max}(\mathcal{A})} \mathcal{A}_P = \mathcal{A}$. †

2.3.3. Dominios de Factorización Única en Ideales Primos “DFUI”

La siguiente proposición es una aplicación estandar del lema de Zorn, esta junto a lo desarrollado en este capítulo traen como consecuencia el teorema 2.3.27. Para una explicación detallada ver ([1]Teo 9.3 pg 106).

Proposición 2.3.24. *Dado I un ideal no trivial en un anillo Noetheriano \mathcal{A} , existen finitos ideales primos P_1, \dots, P_n y finitos enteros a_1, \dots, a_n tales que $P_1^{a_1} \dots P_n^{a_n} \subseteq I \subseteq P_1 \dots P_n$*

Corolario 2.3.25. *Sea \mathcal{A} un dominio Noetheriano en el que primo y maximal son equivalentes y sea I un ideal no trivial. El conjunto de ideales maximales que contienen a I es finito. Sea M_1, \dots, M_n este conjunto entonces existen enteros a_1, \dots, a_n tales que $M_1^{a_1} \dots M_n^{a_n} \subseteq I \subseteq M_1 \dots M_n$*

Definición 2.3.26. Un dominio \mathcal{A} tiene la propiedad de **factorización única de ideales**, si todo ideal propio no trivial se escribe como producto finito de ideales primos y su representación es única.

Teorema 2.3.27. *Sea \mathcal{A} un dominio Noetheriano en el que primo y maximal son equivalentes. Entonces las siguientes son equivalentes.*

- i) \mathcal{A} tiene la propiedad de factorización única de ideales.*
- ii) \mathcal{A}_M tiene la propiedad de factorización única de ideales para todo M en $\text{Max}(\mathcal{A})$.*
- iii) \mathcal{A} es un dominio de Dedekind.*

3. Grupo de Clases De Ideales

Después que Kummer se diera cuenta que la falla de Cauchy y Lamé era la suposición de factorización única, Kummer se puso en la tarea de desarrollar algún método para saber cuando una extensión de los enteros tenía o no esta propiedad. Así fue como Kummer desarrolló su teoría del grupo de clases de ideales y con ella, por primera vez se abría un camino claro hacia UTF.

En este capítulo se expone en forma muy detallada todo el desarrollo de la teoría del grupo de clases de ideales iniciada por Kummer, esto con el animo de resolver cualquier duda que el lector haya podido encontrar consultando otros textos sobre el tema.

3.1. Pruebas de factorización en dominios de Dedekind.

Definición 3.1.1. Sea A un dominio, sean I, J ideales propios no triviales, se dice que I divide a J , $I \mid J$, si y solo si existe un ideal M tal que $IM = J$.

Proposición 3.1.2. Sea A un dominio de Dedekind, sean I, J ideales propios no triviales entonces $J \subseteq I$ si y sólo si $I \mid J$.

Demostración. (\Leftarrow) claro. (\Rightarrow) Si $J \subseteq I$ todo maximal que contiene a I contiene a J , de esta forma si $I = M_1^{a_1} \dots M_m^{a_m} \Rightarrow J = M_1^{b_1} \dots M_m^{b_m} M_{m+1}^{b_{m+1}} \dots M_n^{b_n}$ donde $b_i \geq a_i$; $i = 1, \dots, m$. Para esto consideremos $I \cap J = (M_1^{a_1} \cap M_1^{b_1}) \cap (M_2^{a_2} \cap M_2^{b_2}) \cap \dots \cap (M_m^{a_m} \cap M_m^{b_m}) \cap (M_{m+1}^{b_{m+1}}) \cap \dots \cap (M_n^{b_n})$ ahora $M_i^{a_i} \cap M_i^{b_i} = M_i^{\max(a_i, b_i)}$, entonces reescribiendo tenemos $I \cap J = M_1^{\max(a_1, b_1)} \dots M_m^{\max(a_m, b_m)} M_{m+1}^{b_{m+1}} \dots M_n^{b_n} = J = M_1^{b_1} \dots M_m^{b_m} M_{m+1}^{b_{m+1}} \dots M_n^{b_n}$ luego por unicidad $\max(a_i, b_i) = b_i$ de donde se sigue que $I \mid J$. †

Corolario 3.1.3. Sea A un dominio de Dedekind, I un ideal propio no trivial. Existe un ideal J tal que $IJ = \langle \alpha \rangle$ para algún $\alpha \in A \setminus \{0\}$.

Demostración. Sea $\alpha \in I$ no cero $\Rightarrow \langle \alpha \rangle \subseteq I \Rightarrow I \mid \langle \alpha \rangle$. †

Definición 3.1.4. Sea A un dominio de Dedekind y $P \in \text{Max}(A)$, dado un ideal I propio no trivial, se define $\text{ord}_P(I) := n$, como el único entero n no negativo tal que $P^n \supseteq I$ y $P^{n+1} \not\supseteq I$

Proposición 3.1.5. Sea A un dominio de Dedekind, sean $P \in \text{Max}(A)$, I, J ideales propios no triviales

1. $\text{ord}_P(P) = 1$.
2. $Q \in \text{Max}(A), Q \neq P \Rightarrow \text{ord}_P(Q) = 0$.
3. $\text{ord}_P(IJ) = \text{ord}_P(I) + \text{ord}_P(J)$.

Demostración. 1. Es claro.

$$2. \text{ord}_P(Q) > 0 \Rightarrow P \supseteq Q \Rightarrow P = Q.$$

3. Sea $r = \text{ord}_P(I)$ y sea $t = \text{ord}_P(J)$, por la factorización debemos tener $I = P^r I_1$ y $J = P^t J_1$ donde $P \nmid I_1$ y $P \nmid J_1$ o equivalentemente $P \not\supseteq I_1$ y $P \not\supseteq J_1$, por tanto $IJ = P^{r+t} I_1 J_1$. Supongamos $P^{r+t+1} \supseteq IJ$, entonces $IJ = P^{r+t+1} D$ para algún ideal D , esto implica debido a la representación única que $I_1 J_1 = PD$ por tanto $P \supseteq I_1 J_1$ que por ser P primo implica $P \supseteq I_1$ o $P \supseteq J_1$ que es una contradicción. Entonces $P^{r+t+1} \not\supseteq IJ$ así que $\text{ord}_P(IJ) = r+t = \text{ord}_P(I) + \text{ord}_P(J)$

†

Lema 3.1.6. Sea A un dominio de Dedekind. Sea $K = \mathbb{Q}(A)$ sea $B = \mathfrak{C}(A)_L$ donde L es una extensión finita de K . Sea $P \in \text{Max}(A)$ entonces $P^e \neq B$, donde P^e es el ideal generado por P en B .

Demostración. Supongamos que primero P principal, $P = \langle p \rangle$ con $p \in A$. Si $P^e = B$ existe $b \in B \setminus A$ tal que $pb = 1$. Sea $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ el polinomio minimal de b sobre $A[x]$. Como $b \in B \setminus A$ $\text{grado}(f) > 1$ sea $g(x) = x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1 + a_0p$, $g(b) = b^{n-1} + a_{n-1}b^{n-2} + \dots + a_1 + a_0p = pbb^{n-1} + a_{n-1}pbb^{n-2} + \dots + a_1pb + a_0p = pf(b) = 0$, así g anula a b , contradiciendo la minimalidad de f . Ahora para P en general sea $S = A \setminus P$, este es un subconjunto multiplicativo tanto de A como de B y P_P es un ideal primo

de A_P , además como $S^{-1}B = \mathfrak{C}(A_P)_L$ por la parte inicial tenemos que $(P_P)^e \neq S^{-1}B$ ya que en A_P todo ideal es principal, por otro lado es fácil ver que $(P_P)^e \neq S^{-1}B$ si y solo si $P^e \neq B$. †

Ahora dada una extensión finita L de \mathbb{Q} . Sea $B = \mathfrak{C}(\mathbb{Z})_L$ y sea $P \in \text{Max}(\mathbb{Z})$, $P^e = M_1^{r_1} \dots M_n^{r_n}$ donde definiremos $r_{M_i/P} := r_i$ como el **índice de ramificación** de M_i sobre P . Como $M_i \cap \mathbb{Z}$ es un ideal maximal de \mathbb{Z} y contiene a P tenemos que $M_i \cap \mathbb{Z} = P$ por esto podemos ver a B/M_i como un \mathbb{Z}/P -espacio vectorial el cual gracias a que B es un \mathbb{Z} -módulo finitamente generado es de dimensión finita $[B/M_i : \mathbb{Z}/P] := s_{M_i/P}$, la que denotaremos por **grado residual** de M_i sobre P .

Teorema 3.1.7. *Sea L una extensión finita de \mathbb{Q} y sea $B = \mathfrak{C}(\mathbb{Z})_L$. Dado $P \in \text{Max}(\mathbb{Z})$ entonces $[L : \mathbb{Q}] = \sum_{i=1}^n r_i \cdot [B/M_i : \mathbb{Z}/P]$ donde $P^e = M_1^{r_1} \dots M_n^{r_n}$.*

Demostración. Por el teorema chino del residuo (ver [1] Capítulo 1)

$$B/P^e \cong \prod_{i=1}^n B/M_i^{r_i} \quad (3.1)$$

Por otra parte como $P^e \cap \mathbb{Z} = P$ tenemos una función inyectiva $\Phi : \mathbb{Z}/P \rightarrow B/P^e$ tal que $[a]_P \mapsto [a]_{P^e}$, por tanto podemos ver a B/P^e como un \mathbb{Z}/P -espacio vectorial, de manera similar podemos ver a $B/M_i^{r_i}$ como \mathbb{Z}/P -espacios vectoriales. Se probarán $[B/P^e : \mathbb{Z}/P] = [L : \mathbb{Q}]$ y $[B/M_i^{r_i} : \mathbb{Z}/P] = r_i [B/M_i : \mathbb{Z}/P]$, claramente esto y (3.1) concluye la demostración.

Del Corolario (2.2.9) se tiene que $B = \bigoplus_{i=1}^n \mathbb{Z}$, donde por el lema (2.2.6) $n = [L : \mathbb{Q}]$.

El final de la demostración está dado por la siguiente proposición. †

Proposición 3.1.8. *Sea L una extensión finita de \mathbb{Q} y sea $B = \mathfrak{C}(\mathbb{Z})_L$. Sea $P \in \text{Max}(\mathbb{Z})$ y $M \in \text{Max}(B)$ con $P \subseteq M$, $r \in \mathbb{N}$. Entonces B/M es un \mathbb{Z}/P -espacio vectorial de dimensión finita y $[B/M^r : \mathbb{Z}/P] = r [B/M : \mathbb{Z}/P]$*

Demostración. Igual que antes se puede ver a B/M como un \mathbb{Z}/P -espacio vectorial, dado que B es un \mathbb{Z} -módulo libre finitamente generado la dimensión de B/M como un \mathbb{Z}/P -espacio vectorial es finita.

Ahora para la segunda parte se procederá por inducción en r . Si $r=1$ es claro. Supongámoslo para $r-1$ y veámoslo para r . $P \subseteq M^r \subseteq M^{r-1}$ por esto B/M^{r-1} es también un

\mathbb{Z}/P -espacio vectorial, también podemos ver Que M^{r-1}/M^r es un \mathbb{Z}/P -espacio vectorial definiendo el producto por escalar $(a + P)(\alpha + M^r) := (a\alpha + M^r)$ donde $a \in \mathbb{Z}$, $\alpha \in M^{r-1}$. Dado esto podemos definir la siguiente sucesión exacta de \mathbb{Z}/P -espacios vectoriales

$$0 \longrightarrow M^{r-1}/M^r \longrightarrow B/M^r \longrightarrow B/M^{r-1} \longrightarrow 0$$

con esto

$$[B/M^r : \mathbb{Z}/P] = [B/M^{r-1} : \mathbb{Z}/P] + [M^{r-1}/M^r : \mathbb{Z}/P] \quad (3.2)$$

Afirmación 3.1.9. M^{r-1}/M^r es un B/M -espacio vectorial de dimension 1.

Sea $\alpha \in M^{r-1} \setminus M^r$ existe ya que B es dominio de Dedekind, definase $\Phi : B/M \rightarrow M^{r-1}/M^r$ tal que $[b]_M \mapsto [b\alpha]_{M^r}$. No es difícil ver que Φ es un morfismo de B/M -espacios vectoriales. Para ver que es inyectivo sean b, c en B tales que $\Phi(b) = \Phi(c)$ entonces $(b-c)\alpha \in M^r$ así $\text{ord}_M(\langle (b-c)\alpha \rangle) \geq r$, como $\text{ord}_M(\langle (b-c)\alpha \rangle) = \text{ord}_M(\langle b-c \rangle) + \text{ord}_M(\langle \alpha \rangle)$ y $\text{ord}_M(\langle \alpha \rangle) = r-1$, se tiene que $\text{ord}_M(\langle b-c \rangle) \geq 1$ entonces $(b-c) \in M$. Para la sobreyectividad solo hay que mostrar que $\langle \alpha \rangle + M^r = M^{r-1}$, ya que $M^r \subseteq \langle \alpha \rangle + M^r$ entonces $(\langle \alpha \rangle + M^r) | M^r$ así $\langle \alpha \rangle + M^r$ debe ser una potencia de M, dado que $\alpha \notin M^r$ y $\langle \alpha \rangle + M^r \subseteq M^{r-1}$ se tiene Que $\langle \alpha \rangle + M^r = M^{r-1}$ por esto Φ es un isomorfismo.

De la afirmación se puede concluir que

$$[M^{r-1}/M^r : \mathbb{Z}/P] = [B/M : \mathbb{Z}/P] \quad (3.3)$$

Ahora por hipótesis de inducción

$$[B/M^{r-1} : \mathbb{Z}/P] = (r-1) [B/M : \mathbb{Z}/P] \quad (3.4)$$

El resultado se obtiene al reemplazar (3.3) y (3.4) en (3.2) †

Sea L una extensión de Galois de \mathbb{Q} con grupo de Galois G y sea $B = \mathfrak{C}(\mathbb{Z})_L$, sabemos por la proposición (2.2.5) que $\sigma(B) = B$ para todo σ en G. Sea $P \in \text{Max}(\mathbb{Z})$ y

sean M_1, M_2, \dots, M_t los finitos elementos de $\text{Max}(B)$ tales que $M_i \cap \mathbb{Z} = P$, se define $E(P) := \{M_1, M_2, \dots, M_t\}$, como $\sigma(P) = P$ para todo σ en G entonces $\sigma(E(P)) = E(P)$ para todo σ en G

Lema 3.1.10. Sean $L, B, P, G, M_1, M_2, \dots, M_t$ como arriba. Entonces $r_{M_1/P} = r_{M_2/P} = \dots = r_{M_t/P} = r$ y $s_{M_1/P} = s_{M_2/P} = \dots = s_{M_t/P} = s$, con lo cual $P^e = (M_1 M_2 \dots M_t)^r$ con $rs | E(P)| = [L : Q]$, mas aun el grupo G actúa sobre $E(P)$ y la acción es transitiva.

Demostración. Sin perdida de generalidad es suficiente mostrar Que existe $\sigma \in G$ tal que $\sigma(M_1) = M_t$. Supongamos que $\sigma(M_1) \neq M_t$ para todo σ en G , entonces los ideales maximales $\{\sigma(M_1) : \sigma \in G\} \cup \{M_t\}$ son coprimos dos a dos, por el teorema chino del residuo existe $x \in B$ tal que $x \equiv 1 \pmod{\sigma(M_1)}$ para todo σ en G y $x \equiv 0 \pmod{M_t}$, sea $y = \prod_{\sigma \in G} \sigma(x)$, como $\sigma(B) = B$ para todo σ en G y esta en B , además claramente $\sigma(y) = y$ por esto $y \in \mathbb{Q}$, así que $y \in B \cap \mathbb{Q} = \mathbb{Z}$. Ahora $y \notin M_1$ de lo contrario existiría $\sigma^{-1} \in G$ tal que $\sigma^{-1}(x) \in M_1$ esto ya que M_1 es primo, pero esto contradice el hecho $x \equiv 1 \pmod{\sigma(M_1)}$ para todo σ en G , por esto $y \notin M_1$ entonces $y \notin M_1 \cap \mathbb{Z} = P$. Por otro lado $x \equiv 0 \pmod{M_t}$ entonces $y \equiv 0 \pmod{M_t}$, dado que la identidad esta en G , así $y \in M_t \cap \mathbb{Z} = P$ contradicción. Entonces existe σ en G tal Que $\sigma(M_1) = M_t$. Por el primer teorema del isomorfismo existe $\Gamma_\sigma : B/M_1 \rightarrow B/\sigma(M_1)$ isomorfismo con $\Gamma_\sigma |_{\mathbb{Z}/P} = \text{identidad}$ por lo tanto $s_{M_1/P} = s_{M_{\sigma(1)}/P}$ para todo σ en G . Como $E(P) = \{\sigma(M_1) : \sigma \in G\}$ tenemos que $s_{M_1/P} = s_{M_i/P}$ $i = 1, \dots, t$ entonces $s_{M_1/P} = s_{M_2/P} = \dots = s_{M_t/P} = s$. Por otro lado $\sigma(P^e) = P^e$ para todo σ en G se sigue Que $P^e = \sigma(M_1)^{r_{M_1/P}} \dots \sigma(M_t)^{r_{M_t/P}} = \sigma(M_1)^{r_{\sigma(M_1)/P}} \dots \sigma(M_t)^{r_{(M_t)/P}}$ lo cual implica $r_{M_1/P} = r_{\sigma(M_1)/P}$ entonces $r_{M_1/P} = r_{M_i/P}$ $i = 1, \dots, t$ por lo tanto $r_{M_1/P} = r_{M_2/P} = \dots = r_{M_t/P} = r$. †

Lema 3.1.11. Sea L, B y G como antes, sea $M \in \text{Max}(B)$. Si $P := M \cap \mathbb{Z}$ entonces

$$\prod_{\sigma \in G} \sigma(M) = (P^e)^{s_{M/P}}. \quad (3.5)$$

Demostración. Sea, r índice de ramificación y $s = s_{M/P}$, podemos hacer actuar a G sobre $Max(B)$ de la forma $\sigma.M = \sigma(M)$. Ya que G actúa transitivamente sobre $E(P)$ “ $Stab(M) := \{\sigma \in G : \sigma(M) = M\}$ ” sabemos de la teoría de grupos que $|G/Stab(M)| = |E(P)|$, por lo tanto $[L : Q] = |Stab(M)| |E(P)|$ con esto obtenemos $|Stab(M)| = rs$. Sea $M_i \in E(P)$ y $S_M(M_i) := \{\sigma \in G : \sigma(M) = M_i\} = \{\tau \in G : M = \tau(M_i)\}$. Aver : $|Stab(M)| = |S_M(M_i)|$, dado $\tau \in S_M(M_i)$ definase $H_\tau : Stab(M) \rightarrow S_M(M_i)$ tal que $\sigma \mapsto \sigma \circ \tau$, claramente es inyectiva, como $\tau \in S_M(M_i)$, $M_i = \tau^{-1}(M)$, sea $\rho \in S_M(M_i)$ entonces $\rho\tau^{-1}(M) = M$ así $\rho\tau^{-1} = \sigma$ para algún $\sigma \in Stab(M)$ entonces $H_\tau(\sigma) = \rho$. por lo tanto

$$\prod_{\sigma \in G} \sigma(M) = \prod_{E(P)} M_i^{|S_M(M_i)|} = \prod_{E(P)} M_i^{|Stab(M)|} = \prod_{E(P)} M_i^{rs} = \left(\prod_{E(P)} M_i^r \right)^s = (P^e)^s.$$

†

3.2. Normas y Trazas

Definición 3.2.1. Un campo \mathbb{K} se llama de **números**, si es una extensión finita de \mathbb{Q} , en otras palabras si $\mathbb{K} = \mathbb{Q}(\alpha)$ para algún $\alpha \in \mathbb{Q}$.

El propósito inicial es definir dos funciones, $N_{\mathbb{K}/\mathbb{Q}} : \mathbb{K} \rightarrow \mathbb{Q}$, $Tr_{\mathbb{K}/\mathbb{Q}} : \mathbb{K} \rightarrow \mathbb{Q}$, tales que $N_{\mathbb{K}/\mathbb{Q}} \upharpoonright \mathfrak{C}(\mathbb{Z})_{\mathbb{K}} : \mathfrak{C}(\mathbb{Z})_{\mathbb{K}} \rightarrow \mathbb{Z}$, lo mismo para $Tr_{\mathbb{K}/\mathbb{Q}}$, que sean multiplicativas y aditivas para así poder dar algunos criterios de irreducibilidad y demás en el anillo $\mathfrak{C}(\mathbb{Z})_{\mathbb{K}}$, (Anillo de enteros de \mathbb{K}).

Sea un campo de números \mathbb{K} y $\alpha \in \mathbb{K}$, la función $T : \mathbb{K} \rightarrow \mathbb{K}$ tal que $T_\alpha(y) = \alpha y$ es claramente una transformación \mathbb{Q} -lineal. Por medio de esta transformación se definen las siguientes funciones:

$$\begin{aligned} N_{\mathbb{K}/\mathbb{Q}} : \mathbb{K} &\rightarrow \mathbb{Q} & Tr_{\mathbb{K}/\mathbb{Q}} : \mathbb{K} &\rightarrow \mathbb{Q} \\ \alpha &\mapsto \det(T_\alpha) & \alpha &\mapsto \text{traza}(T_\alpha) \end{aligned}$$

Claramente $N_{\mathbb{K}/\mathbb{Q}}$ es multiplicativa y $Tr_{\mathbb{K}/\mathbb{Q}}$ es aditiva.

Lema 3.2.2. Sea $\alpha \in \mathbb{K}$ tal que $[\mathbb{K} : \mathbb{Q}] = n$ y $[\mathbb{Q}(\alpha) : \mathbb{Q}] = m$, y sea $f(x) \in \mathbb{Q}(x)$ $f(x) = x^m + f_{m-1}x^{m-1} + \dots + f_0$ el polinomio mínimo de α sobre \mathbb{Q} entonces se tienen las siguientes:

1. $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha) = -\frac{n}{m}f_{m-1}$
2. $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = ((-1)^n f_0)^{\frac{n}{m}}$

Demostración. Sea $\{1, \alpha, \dots, \alpha^{m-1}\}$ una base para $\mathbb{Q}(\alpha)$ sobre \mathbb{Q} y $\{t_1, t_2, \dots, t_{\frac{n}{m}}\}$ una base para \mathbb{K} sobre $\mathbb{Q}(\alpha)$; consideremos la siguiente base de \mathbb{K} sobre \mathbb{Q} , $B = \{t_1, t_{1\alpha}, \dots, t_{1\alpha^{m-1}}, t_2, t_{2\alpha}, \dots, t_{2\alpha^{m-1}}, \dots, \alpha^{m-1}t_{\frac{n}{m}}\}$, entonces $B = \{e_1, e_2, \dots, e_n\}$ donde

$$T_\alpha(e_k) = \begin{cases} -f_0 e_{k-(m-1)} - f_1 e_{k-m+2} - \dots - f_{m-1} e_k, & \text{si } m|k, \\ e_{k+1}, & \text{en otro caso.} \end{cases}$$

Así T_α , en la base B , será:

$$\begin{pmatrix} B_\alpha & 0 & \cdot & 0 \\ 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 0 \\ 0 & \cdot & 0 & B_\alpha \end{pmatrix}$$

Donde B_α es la matriz

$$\begin{pmatrix} 0 & 0 & \cdot & \cdot & -f_0 \\ 1 & 0 & & & -f_1 \\ 0 & 1 & & & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & & 1 & -f_{m-1} & \cdot \end{pmatrix}$$

Entonces $\det(T_\alpha) = (\det(B_\alpha))^{\frac{n}{m}} = [(-f_0)(-1)^{m+1}]^{\frac{n}{m}} = [(-1)^m f_0]^{\frac{n}{m}}$

$Traza(T_\alpha) = \frac{n}{m} Traza(B_\alpha) = -\frac{n}{m} f_{m-1}$. †

Lema 3.2.3. Sean $\alpha \in \overline{\mathbb{Q}}$ y $f(x) = x^m + f_{m-1}x^{m-1} + \dots + f_0$, polinomio mínimo de α sobre \mathbb{Q} . Si se define

$$\begin{aligned} T_\alpha : \mathbb{Q}_\alpha &\longrightarrow \mathbb{Q}_\alpha \\ y &\longmapsto \alpha y \end{aligned}$$

entonces $\det(xI - T_\alpha) = f(x)$.

Demostración. $\text{grad}(\det(xI - T_\alpha)) = \text{grad}(f(x))$ y $\det(xI - T_\alpha)$ es un polinomio mónico en $\mathbb{Q}[x]$ que anula a α . †

Corolario 3.2.4. $(-1)^m f_0 = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$; $-f_{m-1} = \text{tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$.

Corolario 3.2.5. Sea \mathbb{K} un campo de números de dimensión n sobre \mathbb{Q} y sea $\alpha \in \mathbb{K}$ de grado m sobre \mathbb{Q} entonces $\text{Tr}_{\mathbb{K}/\mathbb{Q}} = \frac{n}{m} \text{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$, $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = [N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)]^{\frac{n}{m}}$.

Corolario 3.2.6. Sea \mathbb{K} como antes, si $\alpha \in C(\mathbb{Z})_{\mathbb{K}}$ entonces $\text{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ y $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

Demostración. Si $\alpha \in \mathfrak{C}(\mathbb{Z})_{\mathbb{K}}$ su polinomio mínimo está en $\mathbb{Z}[x]$. †

Lema 3.2.7. Sea \mathbb{K} como antes y sean $\sigma_1, \sigma_2, \dots, \sigma_n$, los automorfismos de \mathbb{K} que fijan a \mathbb{Q} entonces

1. $\forall \alpha \in \mathbb{K} \quad N_{\mathbb{K}/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$
2. $\forall \alpha \in \mathbb{K} \quad \text{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$

Demostración. Considere $\mathbb{Q}(\alpha)$ y sean s_1, s_2, \dots, s_m , los automorfismos de $\mathbb{Q}(\alpha)$ que fijan \mathbb{Q} . Para cada i , s_i es exactamente la restricción de $[\mathbb{K} : \mathbb{Q}(\alpha)]$ automorfismos de \mathbb{K} que fijan \mathbb{Q} , así $\sum_{i=1}^n \sigma_i(\alpha) = [\mathbb{K} : \mathbb{Q}(\alpha)] \sum_{j=1}^m s_j(\alpha)$ y $\prod_{i=1}^n \sigma_i(\alpha) = (\prod_{j=1}^m s_j(\alpha))^{[\mathbb{K} : \mathbb{Q}(\alpha)]}$. Ahora sea $f(x) = x^m + f_{m-1}x^{m-1} + \dots + f_0$, el polinomio mínimo de α sobre \mathbb{Q} , como $f(x) = (x - s_1(\alpha))(x - s_2(\alpha)) \dots (x - s_m(\alpha))$ se rompe en $\overline{\mathbb{Q}}[x]$, es fácil ver que $-f_{m-1} = \sum_{i=1}^m s_i(\alpha)$, $(-1)^m f_0 = \prod_{i=1}^m s_i(\alpha)$. Por lo anterior y por el lema (3.2.2), $\sum_{i=1}^m \sigma_i(\alpha) = -\frac{n}{m} f_{m-1} = \text{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha)$ y $\prod_{i=1}^m \sigma_i(\alpha) = [(-1)^m f_0]^{\frac{n}{m}} = N_{\mathbb{K}/\mathbb{Q}}(\alpha)$. †

3.3. Normas de Ideales

Sea \mathbb{K} un campo de números tal que la extensión \mathbb{K}/\mathbb{Q} es de Galois, con grupo de Galois $G = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ y sea $B := \mathfrak{C}(\mathbb{Z})_{\mathbb{K}}$. Del capítulo 2 de la proposición (2.2.9-4), sabemos que $B^G = \mathbb{Z}$ y $\sigma_i(B) = B$, $i = 1, 2, \dots, n$, con esto se puede definir la función:

$$N_{B/\mathbb{Z}} : Id(B) \longrightarrow Id(\mathbb{Z})$$

$$I \longmapsto \left[\prod_{i=1}^n \sigma_i(I) \right]^c$$

donde J^c es la contracción de el homomorfismo $i : \mathbb{Z} \hookrightarrow B, I^e$ sera la extension de este. Se denotará a una extension de Galois \mathbb{K} de \mathbb{Q} con $B = \mathfrak{C}(\mathbb{Z})_{\mathbb{K}}$ como $\langle \mathbb{Z}, \mathbb{Q}, B, \mathbb{K} \rangle$

Lema 3.3.1. Dada $\langle \mathbb{Z}, \mathbb{Q}, B, \mathbb{K} \rangle$, sea $i : \mathbb{Z} \hookrightarrow B$, dado $I \in Id(\mathbb{Z})/\langle 1 \rangle \Rightarrow (I^e)^c = I$.

Demostración. Siempre tenemos $I \subseteq (I^e)^c$. Dado que I es propio y por el lema (3.1.6) I^e es propio, por lo mismo $(I^e)^c$ será propio ya que \mathbb{Z} es de Dedekind, así existe $I' \in Id(\mathbb{Z})$ tal que $I = I'(I^e)^c$. Extendiendo nuevamente $I^e = (I')^e((I^e)^c)^e = (I')^e I^e$ entonces $I^e = (I')^e I^e$. Como B es de Dedekind, por cancelatividad $(I')^e = \langle 1 \rangle_B$ así $I' = \mathbb{Z}$; por tanto $I = (I^e)^c$. †

Proposición 3.3.2. Dada $\langle \mathbb{Z}, \mathbb{Q}, B, \mathbb{K} \rangle$, sea $\alpha \in B \Rightarrow N_{B/\mathbb{Z}}(\langle \alpha \rangle_B) = \langle N_{\mathbb{K}/\mathbb{Q}}(\alpha) \rangle_{\mathbb{Z}}$.

Demostración. Sea $Gal(\mathbb{K}/\mathbb{Q}) = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$, note que $\sigma_i(\langle \alpha \rangle_B) = \langle \sigma_i(\alpha) \rangle_B$ ya que $\sigma_i(B) = B$

$$N_{B/\mathbb{Z}}(\langle \alpha \rangle_B) = \left[\prod_{i=1}^n \sigma_i(\langle \alpha \rangle_B) \right]^c = \left[\prod_{i=1}^n \langle \sigma_i(\alpha) \rangle_B \right]^c = \left[\langle \prod_{i=1}^n \sigma_i(\alpha) \rangle_B \right]^c = \left[\langle N_{\mathbb{K}/\mathbb{Q}}(\alpha) \rangle_{\mathbb{Z}} \right]^c = \langle N_{\mathbb{K}/\mathbb{Q}}(\alpha) \rangle_{\mathbb{Z}}.$$

†

Lema 3.3.3. Sea $\langle \mathbb{Z}, \mathbb{Q}, B, \mathbb{K} \rangle$, $Gal(\mathbb{K}/\mathbb{Q}) = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$. Sea $M \in Max(B)$, $P := M^c \Rightarrow N_{B/\mathbb{Z}}(M) = P^{D_{M/P}}$, donde, $D_{M/P} = [B/M : \mathbb{Z}/P]$.

Demostración. Sea $D = D_{M/P}$. Por lema(3.1.9), $\prod_{i=1}^m \sigma_i(M) = (P^e)^D = (P^D)^e$, tomando contracción a ambos lados del igual se obtiene $N_{B/\mathbb{Z}}(M) = (P^D)^{e^c} = P^D$. †

Proposición 3.3.4. Sea $\langle \mathbb{Z}, \mathbb{Q}, B, \mathbb{K} \rangle$ y $Gal(\mathbb{K}/\mathbb{Q}) = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$. Dado un ideal I en B tal que $I = M_1^{a_1} \dots M_s^{a_s}$, con $M_i \in Max(B)$, y $a_i \in \mathbb{N}$ entonces $N_{B/\mathbb{Z}}(I) = \prod_{i=1}^s N_{B/\mathbb{Z}}^{a_i}(M_i)$, "por tanto $N_{B/\mathbb{Z}}(\cdot)$ es multiplicativa ".

Demostración. Si $I = \prod_{i=1}^s M_i^{a_i}$ si asocio este producto de modo que queden juntos los que sus restricciones a \mathbb{Z} son iguales obtengo que

$$I = \prod_{p \in Max(\mathbb{Z})} \left(\prod_{\{j: M_j \cap \mathbb{Z} = P\}} M_j^{a_j} \right). \quad (3.6)$$

Evaluando en los automorfismos y haciendo el producto.

$$\prod_{i=1}^n \sigma_i(I) = \prod_{p \in Max(\mathbb{Z})} \left(\prod_{\{j: M_j \cap \mathbb{Z} = P\}} \left(\prod_{i=1}^n \sigma_i(M_i) \right)^{a_j} \right) \quad (3.7)$$

Debido al lema (3.1.9) tenemos que $\prod_{i=1}^n \sigma_i(M_i) = (P^e)^{D_{M_i/P}}$ así reemplazando en (3.7) se obtiene

$$\prod_{i=1}^n \sigma_i(I) = \prod_{p \in Max(\mathbb{Z})} \left(\prod_{\{j: M_j \cap \mathbb{Z} = P\}} (P^e)^{a_j D_{M_i/P}} \right). \quad (3.8)$$

Si se definen $J_P = \{j : M_j \cap \mathbb{Z} = P\}$ y $n_P = \sum_{j \in J_P} a_j D_{M_i/P}$,

$$\prod_{i=1}^n \sigma_i(I) = \prod_{p \in Max(\mathbb{Z})} (P^e)^{n_P}. \quad (3.9)$$

Ahora si $P_i, P_j \in Max(\mathbb{Z}), i \neq j$ sus extensiones serán coprimos y así mismo sus potencias entonces

$$\prod_{p \in Max(\mathbb{Z})} (P^e)^{n_P} = \bigcap_{p \in Max(\mathbb{Z})} (P^e)^{n_P} \quad (3.10)$$

reemplazando en (3.9) y aplicando contracción se tiene que

$$\left(\prod_{i=1}^n \sigma_i(I) \right)^c = \bigcap_{p \in Max(\mathbb{Z})} P^{n_P} \quad (3.11)$$

por otra parte aplicando el mismo truco de (3.6) se tiene que:

$$\prod_{p \in \text{Max}(\mathbb{Z})} P^{n_P} = \prod_{p \in \text{Max}(\mathbb{Z})} \left(\prod_{\{j: M_j \cap \mathbb{Z} = P\}} (P^{d_{M_j/p}})^{a_j} \right) \quad (3.12)$$

y además observando la ecuación

$$\prod_{p \in \text{Max}(\mathbb{Z})} \left(\prod_{\{j: M_j \cap \mathbb{Z} = P\}} N_{B/\mathbb{Z}}(M_j)^{a_j} \right) = \prod_{i=1}^s N_{B/\mathbb{Z}}^{a_i}(M_i). \quad (3.13)$$

Notando que el lado derecho de (3.11) es igual al izquierdo de (3.12) y a su vez el lado derecho de (3.12) es igual al izquierdo de (3.13) (lema (3.1.9)) se obtiene el resultado.

†

3.4. Primos Regulares

Sea A un dominio de Dedekind, considérese la siguiente relación \sim sobre $I(A) :=$ conjunto de ideales de A , $I \sim J$ si y solo si existen $\alpha, \beta \in A \setminus \{0\}$ tal que $I\alpha = J\beta$, es claro que es de equivalencia, el propósito es dar una estructura de grupo a $I(A)/\sim$ que permita ver cuan lejos esta A de ser DIP.

Definición 3.4.1. Sea $Cl(A) := I(A)/\sim$ definimos la siguiente operación

$$\begin{aligned} \cdot : Cl(A) \times Cl(A) &\longrightarrow Cl(A) \\ (\bar{I}, \bar{J}) &\longmapsto \overline{IJ} \end{aligned}$$

donde \bar{I} es la clase de I .

Lema 3.4.2. *Dado A un dominio de Dedekind, entonces \cdot esta bien definida y $\langle \bar{1} \rangle$ es un grupo con $\overline{\langle 1 \rangle}$ como identidad.*

Demostración. Sean I_1, I_2, J_1, J_2 ideales de A tales que $\bar{I}_1 = \bar{I}_2$ y $\bar{J}_1 = \bar{J}_2$ entonces existen $\alpha_1, \alpha_2 \in A \setminus \{0\}$ tales que $I_1\alpha_1 = I_2\alpha_2$ y existen $\beta_1, \beta_2 \in A \setminus \{0\}$ tales que $J_1\beta_1 = J_2\beta_2$; por tanto $\overline{I_1 J_1} = \overline{I_2 J_2}$ ya que $I_1 J_1 \alpha_1 \beta_1 = I_2 J_2 \alpha_2 \beta_2$ y $\alpha_i \beta_i \neq 0$ $i = 1, 2$, así la operación esta bien definida. De otro lado, $\overline{\langle 1 \rangle} = \overline{\langle 1 \rangle} = \bar{I}$ para todo I ideal. Entonces $\overline{\langle 1 \rangle}$ es identidad y para todo $\alpha \in A \setminus \{0\}$ $\overline{\langle \alpha \rangle} = \overline{\langle 1 \rangle}$, por esto y por colorario (3.1.3) todo \bar{I} tiene un inverso \bar{J} tal que $\overline{IJ} = \overline{\langle 1 \rangle}$. †

Definición 3.4.3. Sea A un dominio de Dedekind, $Cl(A)$ es el **grupo de clases de ideales** de A .

Lema 3.4.4. Sea A un dominio de Dedekind, el grupo $Cl(A)$ es trivial $\Leftrightarrow A$ es un DIP.

Demostración. (\Leftarrow) es trivial.

(\Rightarrow) Sea I un ideal propio no trivial de A , por hipótesis $\exists \alpha, \beta \in A \setminus \{0\}$ tales que $I\langle \alpha \rangle = \langle \beta \rangle$ en particular $\beta = \alpha\gamma$ para algún $\gamma \in I$. Sea $\xi \in I$ entonces $\alpha\xi = \beta\delta$ para algún $\delta \in A$, si multiplicamos por γ obtenemos $\beta\xi = \beta\delta\gamma$, como $\beta \neq 0$ y A es un dominio $\xi = \beta\delta$, así $I = \langle \beta \rangle$. †

Dado esto tenemos una herramienta importante para ver cuando un dominio de Dedekind es DIP.

Ahora el paso siguiente es ver que pasa con extensiones del tipo $\langle \mathbb{Z}, \mathbb{Q}, B, \mathbb{K} \rangle$. La meta en esta parte es mostrar que $Cl(B)$ es finito y para esto se utilizarán las normas de ideales.

Definición 3.4.5. Sea A un dominio de Dedekind, se dice que A tiene la **propiedad de cocientes finitos** si para todo $I \in Max(A)$, A/I es finito.

Definición 3.4.6. Sea A un dominio de Dedekind con la propiedad de cocientes finitos, se define la norma de un ideal no trivial por $\|I\|_A :=$ cardinal de A/I .

Nota: $\|I\|_A$ no tiene por que ser finita, mas adelante se probará que lo es.

Lema 3.4.7. Sea A un dominio de Dedekind. Sea $P \in Max(A)$. Entonces $\forall n \in \mathbb{N}$ $P^{n-1}/P^n \cong A/P$ como A/P espacios vectoriales. En particular si A/P es finito A/P^n es finito, y $|A/P^n| = |A/P|^n$.

Demostración. La afirmación (3.1.9) implica que $P^{n-1}/P^n \cong_{A/P} A/P$. Supóngase ahora que A/P es finito, entonces A/P^{n-1} es isomorfo a $(A/P^n)/(P^{n-1}/P^n)$ como A -módulos, con lo cual $|A/P^n| = |P^{n-1}/P^n| \cdot |A/P^{n-1}| = |A/P| \cdot |A/P^{n-1}|$, se sigue por inducción $|A/P^n| = |A/P|^n$. †

Corolario 3.4.8. Sea A un dominio de Dedekind con cocientes finitos, la norma de cualquier ideal no trivial es finita y es una función multiplicativa: $\|IJ\|_A = \|I\|_A \|J\|_A$.

Demostración. Sea I un ideal no trivial de A entonces $I = P_1^{\alpha_1} \dots P_s^{\alpha_s}$ con $P_i \in \text{Max}(A)$ y $\alpha_i \in \mathbb{N}$, $i = 1, \dots, s$. Por el teorema chino del residuo $A/I \cong \prod_{i=1}^s A/P_i^{\alpha_i}$, así por (3.4.3) $\|I\|_A = \prod_{i=1}^s \|P_i\|_A^{\alpha_i}$. Entonces para cualesquiera ideales I, J en A $\|IJ\|_A = \|I\|_A \|J\|_A$ †

Proposición 3.4.9. *Dada $\langle \mathbb{Z}, \mathbb{Q}, B, \mathbb{K} \rangle$, B tiene la propiedad de los cocientes finitos. Mas aún si $I \subseteq B$ es un ideal no trivial entonces $\|I\|_B = \|N_{B/\mathbb{Z}}(I)\|_{\mathbb{Z}}$. Esto da un criterio para verificar maximalidad para ideales en B : I es maximal $\Leftrightarrow \|I\|_B$ es primo.*

Demostración. Sea $M \in \text{Max}(B)$, sea $\langle P \rangle = M^C$, "la contracción de M " entonces B/M es un \mathbb{Z}_p -espacio vectorial finito $\|M\|_B = |B/M| = |\mathbb{Z}/\langle P \rangle|^{D_{M/p}} = \|\langle P \rangle^{D_{M/p}}\|_{\mathbb{Z}} = |P|^{D_{M/p}} = \|\langle P \rangle^{D_{M/p}}\|_{\mathbb{Z}} = N_{B/\mathbb{Z}}$ es multiplicativa y tenemos que $\|I\|_A = \|N_{B/\mathbb{Z}}(I)\|_{\mathbb{Z}}$. †

Lema 3.4.10. *Dado $\lambda \in \mathbb{R}$ un número real fijo, dado $\langle \mathbb{Z}, \mathbb{Q}, B, \mathbb{K} \rangle$. Existen solo finitos ideales I de B tal que $\|I\|_B \leq \lambda$.*

Demostración. Es suficiente mostrar que hay solo finitos ideales maximales con $\|M\|_B \leq \lambda$. Suponga que existen infinitos ideales $\{I_\alpha\}_{\alpha \in \Lambda}$ con Λ infinito tales que $\|I_\alpha\|_B \leq \lambda$ y finitos maximales M_i , $i = 1, \dots, n$, $\|M_i\| \leq \lambda$. Un subconjunto de los M_i , contendrá todos los I_α , dado que si $J \supseteq I$ ideales entonces $\|J\|_B \leq \|I\|_B$. Como son infinitos I_α , tendríamos infinitas combinaciones de potencias de los M_i y como un ideal J , tiene norma 1 si y solo si $J = \langle 1 \rangle$ es imposible que todos los I_α cumplan $\|I_\alpha\| \leq \lambda$. Ya que un ideal maximal de \mathbb{Z} esta contenido sólo en finitos maximales de B y como $\|M\|_B = \|M \cap \mathbb{Z}\|_{\frac{D_M}{M \cap \mathbb{Z}}} \geq \|M \cap \mathbb{Z}\|_{\mathbb{Z}}$, es suficiente probar que solo hay finitos P ideales maximales de \mathbb{Z} con $\|P\|_{\mathbb{Z}} \leq \lambda$, pero esto es claro. †

Lema 3.4.11. *Dado B como antes. El grupo $Cl(B)$ es finito si y sólo si existe $\lambda \in \mathbb{R}$ dependiendo de B tal que toda clase en $Cl(B)$ contiene un ideal I con $\|I\|_B \leq \lambda$.*

Demostración. Si $Cl(B)$ es finito, sea n el numero de clases, tome elementos I_i $i = 1, \dots, n$ en cada clase y $\lambda = \max_i \{\|I_i\|\}$. Supóngase que existe λ tal que toda clase en $Cl(B)$ contiene un ideal I tal que $\|I\|_B \leq \lambda$, por el lema (3.4.10) solo hay finitas clases. †

Lema 3.4.12. *Dado $\lambda \in \mathbb{R}$, si todo ideal I no trivial, contiene un elemento α con $\|\langle \alpha \rangle\|_B \leq \lambda \|I\|$ entonces toda clase en $Cl(B)$ contiene un ideal I con $\|I\|_B \leq \lambda$.*

Demostración. Dado $C \in Cl(B)$, distinto de la identidad, fije J un ideal en la clase inversa de C . Dado $\alpha \in J$ tal que $\|\langle \alpha \rangle\|_B \leq \lambda \|J\|_B$, como $\langle \alpha \rangle \subseteq J$, $IJ = \langle \alpha \rangle$ para algún I de B , I esta en la clase C . Como $\|\cdot\|_B$ es multiplicativa $\|I\|_B \|J\|_B \leq \lambda \|J\|_B$ de donde se sigue el resultado. †

Teorema 3.4.13. *Dado $\langle \mathbb{Z}, \mathbb{Q}, B, \mathbb{K} \rangle$. Entonces existe $\lambda \in \mathbb{R}$ dependiendo de B tal que ideal no trivial I contiene un elemento $\alpha \neq 0$ con $\|\langle \alpha \rangle\|_B \leq \lambda \|I\|_B$. En particular $Cl(B)$ es finito.*

Demostración. Como B es un \mathbb{Z} -módulo libre finitamente generado, podemos fijar una base para B sobre \mathbb{Z} , $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$, y sean $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$ los monomorfismos de K en C . Si definimos $\lambda := \prod_{i=1}^n (\sum_{j=1}^n |\sigma_i(\alpha_j)|)$, donde $|\cdot|$ es valor absoluto complejo, se mostrará que todo ideal no trivial I de B contiene un elemento $\alpha \neq 0$ tal que $\|\langle \alpha \rangle\|_B \leq \lambda \|I\|_B$.

Sea I un ideal no trivial de B , sea $m = \max\{j \in \mathbb{N} : j^n \leq \|I\|_B\} \Rightarrow m^n \leq \|I\|_B < (m+1)^n$, consideremos el siguiente conjunto de $(n+1)^n$ elementos de B , $\Gamma := \{\sum_{j=1}^n m_j \alpha_j$ con $m_i \in \mathbb{Z}, 0 \leq m_i \leq m, j = 1, \dots, n\}$. Como $(m+1)^n > \|I\|_B$, dos elementos de Γ son congruentes modulo I , sean β_1, β_2 estos dos. Se define $\alpha = \beta_1 - \beta_2 = \sum_{i=1}^n a_i \alpha_i$ con $a_i \in \mathbb{Z}$ y $|a_i| \leq m$ para todo i , así que $\|\langle \alpha \rangle\|_B = \|N_{B/\mathbb{Z}}(\langle \alpha \rangle)\|_{\mathbb{Z}} = |N_{K/\mathbb{Q}}(\alpha)| = \prod_{i=1}^n |\sigma_i(\alpha)| \leq \prod_{i=1}^n (\sum_{j=1}^n |m_j| |\sigma_i(\alpha_j)|) \leq m^n \prod_{i=1}^n (\sum_{j=1}^n |\sigma_i(\alpha_j)|) = m^n \lambda \leq \|I\|_B \lambda$. †

Definición 3.4.14. Un primo p impar se dice **regular** si $p \nmid |Cl(\mathbb{Z}[\zeta_p])|$

4. $\mathfrak{C}(\mathbb{Z})_{\mathbb{Q}(\zeta_p)}$ y Fermat caso I

4.1. $\mathbb{Z}[\zeta_p]$ y sus propiedades

Sea p un primo impar y $\zeta_p := e^{\frac{2\pi i}{p}}$ una raíz p -ésima de la unidad, sabemos de la teoría de campos que $\mathbb{Q}(\zeta_p) := \{a_0 + a_1\zeta_p + \dots + a_{p-2}\zeta_p^{p-2} : a_i \in \mathbb{Q}\}$ es una extensión de Galois de \mathbb{Q} de grado $p-1$. Para una explicación detallada ver ([5]).

Sea $\mathbb{Z}[\zeta_p] := \{a_0 + a_1\zeta_p + \dots + a_{p-2}\zeta_p^{p-2} : a_i \in \mathbb{Z}\}$, se puede verificar que $\mathbb{Z}[\zeta_p]$ es un dominio.

El propósito de la primera parte de este capítulo es conocer las propiedades más importantes de $\mathbb{Z}[\zeta_p]$, como que es un dominio de Dedekind y más aún probar que $\mathbb{Z}[\zeta_p] = \mathfrak{C}(\mathbb{Z})_{\mathbb{Q}(\zeta_p)}$, esto para así poder mostrar la imposibilidad de solución de la ecuación $x^p + y^p = z^p$, en el caso 1 para p un primo regular.

Sea $\lambda_p = 1 - \zeta_p$, este elemento será muy importante en el desarrollo de este capítulo.

Lema 4.1.1. $-\lambda_p$ es raíz del polinomio $p(x) = x^{p-1} + x^{p-2} + \dots + p$ que es irreducible de grado $p-1$. Así pues $\mathbb{Q}(\lambda_p) = \mathbb{Q}(\zeta_p)$.

Demostración. Dado $\Phi_p(x) = \frac{x^p-1}{x-1}$ el polinomio mínimo de ζ_p , si denotamos $p(x) = \Phi_p(x+1)$, es claro que $p(-\lambda_p) = 0$. Para la irreducibilidad ver ([3] Capítulo 5). †

Si se define $\mathbb{Z}[\lambda_p] = \{a_0 + a_1\lambda_p + \dots + a_{p-2}\lambda_p^{p-2} : a_i \in \mathbb{Z}\}$, por el lema anterior es sencillo ver que $\mathbb{Z}[\lambda_p] = \mathbb{Z}[\zeta_p]$.

Lema 4.1.2. $\prod_{i=1}^{p-1} (1 - \zeta_p^i) = p$, es decir $(N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\lambda_p) = p)$

Demostración. Sea $\Phi_p(x) = \frac{x^p-1}{x-1}$, las raíces de este polinomio son las raíces p -ésimas de la unidad $\{\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\}$, así que $\Phi_p(x) = (x - \zeta_p)(x - \zeta_p^2) \dots (x - \zeta_p^{p-1}) \prod_{i=1}^{p-1} (1 - \zeta_p^i) = \Phi_p(1) = \lim_{x \rightarrow 1} \frac{x^p-1}{x-1} = p$. †

Lema 4.1.3. Sea $\varphi_i = \frac{1-\zeta_p^i}{1-\zeta_p}$ $1 \leq i \leq p-1 \Rightarrow \varphi_i$ es un invertible en $\mathbb{Z}[\zeta_p]$.

Demostración. Dado que $p \nmid i \Rightarrow \exists j \in \mathbb{Z}^+$ tal que $ij \equiv 1 \pmod{p} \Rightarrow \zeta_p = \zeta_p^{ij}$, pero $\nu_i := \frac{1-\zeta_p^{ij}}{1-\zeta_p^i} = 1 + \zeta_p^i + \zeta_p^{2i} + \dots + \zeta_p^{(j-1)i} \in \mathbb{Z}[\zeta_p]$ y $\varphi_i \nu_i = 1$. †

Corolario 4.1.4. Existe u invertible en $\mathbb{Z}[\zeta_p]$ tal que $u\lambda_p^{p-1} = p$, ($\langle \lambda_p \rangle^{p-1} = \langle p \rangle$).

Demostración. $p = \prod_{i=1}^{p-1} (1 - \zeta_p^i) = (\prod_{i=1}^{p-1} u_i) \lambda_p^{p-1} = u \lambda_p^{p-1}$. †

Afirmación 4.1.5. Sea $\alpha \in \mathbb{Q}(\zeta_p)$, $\alpha = a_0 + a_1 \zeta_p + \dots + a_{p-2} \zeta_p^{p-2}$, $a_i \in \mathbb{Q}$, $i = 0, \dots, p-2$.

$$1. \quad \text{tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^j) = \begin{cases} -1, & p \nmid j; \\ p-1, & \text{de lo contrario.} \end{cases}$$

$$2. \quad \text{tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\alpha \zeta_p^{-s}) = -a_0 - a_1 - \dots - a_{s-1} + (p-1)a_s - a_{s+1} - \dots - a_{p-2}.$$

Demostración. Si $p \mid j \Rightarrow \zeta_p^j = 1 \Rightarrow \text{tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^j) = \text{tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1) = \sum_{i=1}^{p-1} \sigma_i(1) = p-1$, $\sigma_i \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, $i = 1, \dots, p-1$.

Si $p \nmid j \Rightarrow \text{tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^j) = \sum_{i=1}^{p-1} \zeta_p^{ij} = \frac{(\zeta_p^j)^p - \zeta_p^j}{\zeta_p^j - 1} = -1$.

(2) se deduce de (1). †

Teorema 4.1.6. $\mathbb{Z}[\zeta_p] = \mathfrak{C}(\mathbb{Z})_{\mathbb{Q}(\zeta_p)}$.

Demostración. Sea $\alpha \in \mathfrak{C}(\mathbb{Z})_{\mathbb{Q}(\zeta_p)}$, $\alpha = a_0 + a_1 \zeta_p + \dots + a_{p-2} \zeta_p^{p-2}$, $a_i \in \mathbb{Q}$, $i = 0, \dots, p-2$.

Sea $\beta_s = \alpha \zeta_p^{-s}$, $\gamma = \alpha \zeta_p$, $s = 0, \dots, p-2$, $\beta_s - \gamma \in \mathfrak{C}(\mathbb{Z})_{\mathbb{Q}(\zeta_p)} \Rightarrow \text{tr}(\beta_s - \gamma) \in \mathbb{Z}$

Ahora $\text{tr}(\beta_s) - \text{tr}(\gamma) = -a_0 - a_1 - \dots - a_{s-1} + (p-1)a_s - a_{s-1} - \dots - a_{p-2} + a_0 + a_1 + \dots + a_{p-2} = pa_s$ por lo tanto $pa_s \in \mathbb{Z}$ $s = 0, \dots, p-2$ así $p\alpha \in \mathbb{Z}[\zeta_p] = \mathbb{Z}[\lambda_p]$. Entonces existen $b_0, b_1, \dots, b_{p-2} \in \mathbb{Z}$ tales que $p\alpha = b_0 + b_1 \lambda_p + \dots + b_{p-2} \lambda_p^{p-2}$, puesto que $\lambda_p \mid p$ $\lambda_p \mid b_0$, tomando normas, como $b_0 \in \mathbb{Z}$ se tiene $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(b_0) = b_0^{p-1}$ así $p \mid b_0^{p-1}$ en \mathbb{Z} , entonces $b_0 = b_0^* p$ donde $b_0^* \in \mathbb{Z}$, por esto $\lambda_p^{p-1} \mid b_0$, de esto se deduce que $\lambda^2 \mid \lambda b_1$ entonces $\lambda \mid b_1$, de nuevo tomando normas se obtiene $b_1^* \in \mathbb{Z}$ tal que $b_1 = b_1^* p$. Así sucesivamente se pueden encontrar $b_i^* \in \mathbb{Z}$ tales que $b_i = b_i^* p$, $i = 0, \dots, p-2$. Entonces $\alpha = b_0^* + b_1^* \lambda_p + \dots + b_{p-2}^* \lambda_p$ que es un elemento de $\mathbb{Z}[\lambda_p]$.

Claramente $\mathbb{Z}[\zeta_p] \subseteq \mathfrak{C}(\mathbb{Z})_{\mathbb{Q}(\zeta_p)}$. †

Proposición 4.1.7. *El ideal $\langle \lambda_p \rangle$ en $\mathbb{Z}[\lambda_p]$ es maximal, mas aún $\mathbb{Z}[\lambda_p]/\langle \lambda_p \rangle \cong \mathbb{Z}_p$.*

Demostración. Ya que $\mathbb{Z}[\lambda_p] = \mathfrak{C}(\mathbb{Z})_{\mathbb{Q}(\zeta_p)}$, $\|\langle \lambda_p \rangle\|_{\mathbb{Z}[\zeta_p]} = \|\langle N_{\mathbb{Z}[\zeta_p]/\mathbb{Z}}(\lambda_p) \rangle\|_{\mathbb{Z}} = \|\langle p \rangle\|_{\mathbb{Z}} = p$
 $\Rightarrow \mathbb{Z}[\lambda_p]/\langle \lambda_p \rangle \cong \mathbb{Z}_p$. †

4.2. Raíces de la unidad en $\mathbb{Q}(\zeta_p)$

Definición 4.2.1. Sea G un grupo finito, el **exponente** $e(G)$ de G es el mínimo entero positivo tal que $g^{e(G)} = e$ para todo $g \in G$. Sea $o(g)$ el orden del elemento g .

Proposición 4.2.2. *Suponga G un grupo abeliano finito entonces $\exists g \in G$ tal que $o(g) = e(G)$.*

Demostración. Por el teorema de grupos abelianos finitamente generados, ver ([5] Teo 9.3), $G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \times \mathbb{Z}_{d_s}$, $d_j \mid d_k$ $j \leq k$, entonces si $g \in G$ $g^{d_s} = \text{identidad}$, así $e(G) \leq d_s$. Por otro lado G tiene un subgrupo isomorfo a \mathbb{Z}_{d_s} , si h es un generador de este $\Rightarrow o(h) = d_s$, como $o(h) \leq e(G)$ se sigue el resultado. †

Lema 4.2.3. *Sea K un campo y sea K^* , el grupo multiplicativo de K . Si G es un subgrupo finito de K^* entonces G es cíclico.*

Demostración. Sea $n = e(G)$ entonces $\alpha^n = 1 \forall \alpha \in G$, como $x^n - 1$, tiene a lo mas n raíces por tanto $|G| \leq e(G)$ entonces $|G| = e(G)$, por el lema anterior $\exists g \in G$ tal que $o(g) = e(G) = |G| \Rightarrow G = \langle g \rangle$. †

Lema 4.2.4. *Sea c un real positivo y K un campo de números, entonces existe sólo un número finito de enteros algebraicos α en K tales que $|\alpha^{(i)}| \leq c$ para todos los conjugados $\alpha^{(i)}$ de α .*

Demostración. Sea $n = [K : \mathbb{Q}]$, sea

$$s_1(x_1, x_2, \dots, x_n) = x_1 + x_2 + \dots + x_n$$

$$s_2(x_1, x_2, \dots, x_n) = \sum_{i < j} x_i + x_j$$

.

.

$$s_n(x_1, x_2, \dots, x_n) = x_1 x_2 \dots x_n$$

las funciones simétricas elementales en n -variables.

Sea α un entero algebraico tal que $|\alpha^{(i)}| \leq c$ para todos sus conjugados $\alpha^{(i)}$, sea $p_\alpha(x) = (x - \alpha^{(1)})(x - \alpha^{(2)}) \dots (x - \alpha^{(n)})$ el polinomio con raíces los conjugados de α en K .

No es difícil ver que $p_\alpha(x) = x^n - s_1(\alpha^1, \alpha^2, \dots, \alpha^n)x^{n-1} + \dots + (-1)^i s_i(\alpha^1, \alpha^2, \dots, \alpha^n)x^{n-i} + \dots + (-1)^n x_1 x_2 \dots x_n$.

Ahora $|s_i(\alpha^1, \alpha^2, \dots, \alpha^n)| \leq (\max_{i=1, \dots, n} \{|\alpha^{(i)}|\})^i \leq c^i$. Como α es un entero algebraico, $s_i(\alpha^1, \alpha^2, \dots, \alpha^n) \in \mathbb{Z}$ para todo $i = 1, \dots, n$. Sea $m = \max_{i=1, \dots, n} \{c^i\}$, sólo existen finitos polinomios en $\mathbb{Z}[x]$ tales que el valor absoluto de sus coeficientes es menor que m , por tato sólo existen finitos enteros algebraicos tal que $|\alpha^{(i)}| \leq c$ para todos sus conjugados.

†

Lema 4.2.5. *Sea K un campo de números y sea $\alpha \in K$, α es raíz de la unidad si y solo si $|\alpha^{(i)}| = 1$, para todos los conjugados $\alpha^{(i)}$ de α en K .*

Demostración. (\Rightarrow) es claro.

(\Leftarrow) Si $|\alpha^{(i)}| = 1$ para todos los conjugados de α , por el lema anterior el conjunto $\Gamma = \{\alpha, \alpha^2, \dots, \alpha^n, \dots\}$ debe ser finito, así que existen $n > m$ tales que $\alpha^n = \alpha^m \alpha^{n-m} = 1$, así que α es raíz de la unidad. †

Corolario 4.2.6. *Sea K como antes, el grupo de las raíces de la unidad es un grupo cíclico finito.*

Definición 4.2.7. Dado n un entero positivo, definimos $\Phi(n) = \sum_{d \leq n, (d, n) = 1} 1$.

Dos propiedades importantes que se necesitarán de la función Φ son las siguientes:

1. $(n, m) = 1 \Rightarrow \Phi(nm) = \Phi(n)\Phi(m)$. Ver ([11] cap 4 Teo 20).
2. $\omega \in \mathbb{C}$, una raíz m -ésima de la unidad $\Rightarrow [\mathbb{Q}(\omega) : \mathbb{Q}] = \Phi(m)$. Ver ([2] corolario 1 pg 195).

Proposición 4.2.8. *Sea R el grupo multiplicativo de raíces de la unidad de $\mathbb{Q}(\zeta_p)$, entonces*

$$R = \{\pm 1, \pm \zeta_p, \pm \zeta_p^2, \dots, \pm \zeta_p^{p-1}\}.$$

Demostración. R es un grupo cíclico de orden r , como $-\zeta_p$ tiene orden $2p$, $2p \mid r$. Sea $\alpha \in R$ un elemento de orden r , $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta_p)$ entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] \mid [\mathbb{Q}(\zeta_p) : \mathbb{Q}]$ entonces $\Phi(r) \mid p-1$. Ahora $r = p^k m$ $k \geq 1, m \geq 2$ y $(p^k, m) = 1$, $\Phi(r) = p^{k-1}(p-1)\Phi(m)$, por lo tanto $\Phi(m) = 1$, $k-1 = 0$, así que $m = 2, k = 1$ y $r = 2p$. †

Lema 4.2.9. Sea $\alpha \in \mathbb{Z}[\zeta_p]$, $\alpha = a_0 + a_1\zeta_p + a_2\zeta_p^2 + \dots + a_{p-2}\zeta_p^{p-2}$, $a_i \in \mathbb{Z}$, $i = 0, 1, \dots, p-2$, $p \mid \alpha \Rightarrow p \mid a_i \forall i = 0, 1, \dots, p-2$.

Demostración. Si $p \mid \alpha$ $\alpha = p(b_0 + b_1\zeta_p + b_2\zeta_p^2 + \dots + b_{p-2}\zeta_p^{p-2}) (a_0 - pb_0) + (a_1 - pb_1)\zeta_p + \dots + (a_{p-2} - pb_{p-2})\zeta_p^{p-2} = 0$, como $\{1, \zeta_p, \dots, \zeta_p^{p-2}\}$ son una base para $\mathbb{Q}(\zeta_p)$, como \mathbb{Q} -espacio vectorial $a_i - pb_i = 0$. †

Lema 4.2.10. Dados $\alpha, \beta \in \mathbb{Z}[\zeta_p]$ si $p \mid (\alpha - \beta) \Rightarrow p \mid \bar{\alpha} - \bar{\beta}$, en otras palabras $\alpha \equiv \beta \pmod{p} \iff \bar{\alpha} \equiv \bar{\beta} \pmod{p}$.

Demostración. La conjugación compleja deja invariante a p . †

Lema 4.2.11. Sean $\alpha_1, \alpha_2, \dots, \alpha_n$ finitos elementos de $\mathbb{Z}[\zeta_p]$ $(\alpha_1 + \alpha_2 + \dots + \alpha_n)^p \equiv \alpha_1^p + \alpha_2^p + \dots + \alpha_n^p \pmod{p}$.

Demostración. Es suficiente mostrarlo para dos. $(\alpha + \beta)^p = \alpha^p + \beta^p + \sum_{n=1}^{p-1} C_n^p \alpha^{p-n} \beta^n$, es fácil ver que $p \mid C_n^p$ para todo $n = 1, \dots, p-1$ donde C_k^m denota $\frac{m!}{(m-k)!k!}$. entonces $(\alpha + \beta)^p \equiv \alpha^p + \beta^p \pmod{p}$. †

Lema 4.2.12. Sea $\alpha \in \mathbb{Z}[\zeta_p]$ entonces $\alpha^p \equiv a \pmod{p}$, para algún $a \in \mathbb{Z}$.

Demostración. Sea $\alpha = a_0 + a_1\zeta_p + \dots + a_{p-2}\zeta_p^{p-2}$ $\alpha^p \equiv a_0^p + a_1^p\zeta_p^p + \dots + a_{p-2}^p(\zeta_p^p)^{p-2} \pmod{p} \Rightarrow \alpha^p \equiv a_0^p + a_1^p + \dots + a_{p-2}^p \pmod{p}$. †

Proposición 4.2.13. Sea u unidad en $\mathbb{Z}[\zeta_p]$, $\frac{u}{\bar{u}} = \zeta_p^k$ para algún $k \in \{1, \dots, p-1\}$.

Demostración. Dado que $\alpha = \frac{u}{\bar{u}}$ tiene norma 1, igual que todos sus conjugados, debemos tener que $\frac{u}{\bar{u}}$ es una raíz de la unidad entonces $\frac{u}{\bar{u}} = \pm \zeta_p^k$ donde $k \in \{1, \dots, p-1\}$. Supongamos $u = -\bar{u}\zeta_p^k$ tomando potencias $u^p = -\bar{u}^p$, haciendo congruencias modulo p , existe $a \in \mathbb{Z}$ tal que $a \equiv -a \pmod{p}$ entonces $p \mid 2a$, como $p \neq 2$, $p \mid a$ entonces $a \equiv 0 \pmod{p}$ por tanto $u^p \equiv 0 \pmod{p}$, así p sería una unidad de donde λ_p , sería una unidad, contradiciendo el hecho de $\mathbb{Z}[\zeta_p]/\langle \lambda_p \rangle \cong \mathbb{Z}_p$. †

4.3. Fermat Caso I

Teorema 4.3.1. *Dados $x, y, z \in \mathbb{Z}$ tales que $(x, y) = (x, z) = (y, z) = 1$ y dado $p > 3$ un primo regular, si $p \nmid xyz \Rightarrow x^p + y^p \neq z^p$.*

Demostración. Supongamos que $x^p + y^p = z^p$, esta ecuación puede ser reescrita en $\mathbb{Z}[\zeta_p]$ como:

$$(x + y)(x + \zeta_p y)(x + \zeta_p^2 y) \dots (x + \zeta_p^{p-1} y) = z^p \quad (4.1)$$

ahora escribiendo (4.1) en términos de ideales

$$\langle x + y \rangle \langle x + y\zeta_p \rangle \langle x + y\zeta_p^2 \rangle \dots \langle x + y\zeta_p^{p-1} \rangle = \langle z \rangle^p. \quad (4.2)$$

Afirmación 4.3.2. *No existe $M \in \text{Max}(\mathbb{Z}[\zeta_p])$ tal que $\forall k \in \{0, 2, \dots, p-1\} \langle x + y\zeta_p \rangle \subseteq M$ y $\langle x + y\zeta_p^k \rangle \subseteq M$.*

Si este M existiera entonces $y(\zeta_p^k - \zeta_p) \in M$ por tanto $-\zeta_p y(1 - \zeta_p^{k-1}) \in M$ y por (4.1.3) $y\lambda_p \in M$, por otro lado $\langle x + y\zeta_p \rangle \subseteq M$ entonces $M \mid \langle x + y\zeta_p \rangle$ así $M \mid \langle z \rangle^p$, como M es maximal $M \mid \langle z \rangle$, así $z \in M$. Ahora yp, z son primos relativos por hipótesis, por tanto existen $m, n \in \mathbb{Z}$ tales que $nyp + mz = 1$, $p = \lambda^{p-1}u_1$, u_1 invertible de $\mathbb{Z}[\zeta_p]$ entonces $ny\lambda_p u_1 \lambda_p^{p-2} + mz = 1$ entonces $1 \in M$, que es una contradicción por lo tanto M no existe.

Por lo anterior y por la factorización única en dominios de Dedekind se sigue que $\langle x + y\zeta_p \rangle = I^p$ para algún ideal I en $\mathbb{Z}[\zeta_p]$. Como I^p es la identidad en $Cl(\mathbb{Z}[\zeta_p])$ y p es regular, I tiene que ser la identidad, entonces existe $\alpha \in \mathbb{Z}[\zeta_p]$ tal que $I = \langle \alpha \rangle$. Luego $\langle x + y\zeta_p \rangle = \langle \alpha^p \rangle$, así que existe u invertible en $\mathbb{Z}[\zeta_p]$ tal que $x + y\zeta_p = u\alpha^p$. Por (4.2.12) $x + y\zeta_p \equiv ua \pmod{p}$ para algún $a \in \mathbb{Z}$. Tomando conjugación compleja $x + y\zeta_p^{-1} \equiv \bar{u}a \pmod{p}$ entonces $x + y\zeta_p = \frac{u}{\bar{u}}(x + y\zeta_p^{-1}) \pmod{p}$ así por (4.2.13) $x + y\zeta_p = \zeta_p^k(x + y\zeta_p^{-1}) \pmod{p}$ para algún $k \in \{0, 1, \dots, p-1\}$. Entonces $x + y\zeta_p \equiv x\zeta_p^k + y\zeta_p^{k-1} \pmod{p}$. Si $k \neq 1$ $p \mid x$ y $p \mid y$, por lo tanto $k = 1$ entonces $x \equiv y \pmod{p}$.

Siguiendo un razonamiento totalmente análogo y notando que $x^p + y^p = z^p$ implica que $x^p + (-z)^p \equiv (-y)^p$, obtenemos que $x \equiv -z(\text{mod } p)$, como $x \equiv y(\text{mod } p)$, $x^p \equiv y^p(\text{mod } p)$, $2x^p \equiv x^p + y^p(\text{mod } p)$ entonces $2x^p \equiv z^p(\text{mod } p)$ así $2x^p \equiv -x(\text{mod } p)$ lo cual implica que $3x^p \equiv 0(\text{mod } p)$, como $p > 3$, $x^p \equiv 0(\text{mod } p)$ entonces $x \equiv 0(\text{mod } p)$, que contradice las hipótesis. †

5. Teoría Analítica de Numeros y Fermat CasoII

5.1. Los Numeros de Bernoulli

Este capitulo se inicia discutiendo dos antiguos problemas, el primero de ellos trata de encontrar una formula para la suma de las potencias k -ésimas de los primeros n naturales. Es bien sabido que :

$$\sum_{i=1}^{n-1} i = \frac{n(n-1)}{2}, \sum_{i=1}^{n-1} i^2 = \frac{n(n-1)(2n-1)}{6}, \sum_{i=1}^{n-1} i^3 = \left(\frac{n(n-1)}{2}\right)^2,$$

así la suma de las potencias k -ésimas de los primeros $n - 1$ naturales es un polinomio en n , de grado $k + 1$. El problema era encontrar los coeficientes de este polinomio, Jacob Bernoulli encontró estos coeficientes, debido esto son llamados **los números de Bernoulli**.

Otro problema interesante era el siguiente: Si definimos para $s > 1$ $Z(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, entonces ¿cual es el valor de $Z(2m)$, $m \in \mathbb{N}$?. En 1734 Euler mostró que $Z(2) = \frac{\pi^2}{6}$, más adelante logró encontrar el valor de $Z(2m)$ para todo m , sin embargo el valor en $2m + 1$ todavía es desconocido. Hay una relación directa entre los numeros Bernoulli y $Z(2m)$. Mejor aún es que estos números dan las herramientas necesarias para determinar por un cálculo sencillo cuando un primo p es regular o no.

Definición 5.1.1. La sucesión B_0, B_1, B_2, \dots , se define inductivamente de la siguiente forma: $B_0 = 1, (m + 1)B_m = -\sum_{k=0}^{m-1} C_k^{m+1} B_k$, donde C_k^m denota $\frac{m!}{(m-k)!k!}$. Los B_m se conocen como los números de Bernoulli.

Lema 5.1.2. Si $\sum_{m=0}^{\infty} b_m \frac{t^m}{m!}$ es la serie de potencias de $f(t) = \frac{t}{e^t - 1}$ entonces $\forall m \in \mathbb{N}$ $b_m = B_m$.

Demostración.

$$t = (e^t - 1) \sum_{m=0}^{\infty} b_m \frac{t^m}{m!}$$

$$t = \sum_{n=1}^{\infty} \frac{t^n}{n!} \sum_{m=0}^{\infty} b_m \frac{t^m}{m!}$$

$$t = \sum_{n=0}^{\infty} \frac{t^{k+1}}{(k+1)!} \sum_{m=0}^{\infty} b_m \frac{t^m}{m!}$$

$$1 = \sum_{n=0}^{\infty} \frac{t^k}{(k+1)!} \sum_{m=0}^{\infty} b_m \frac{t^m}{m!}$$

$$1 = \sum_{m=0}^{\infty} \left(\sum_{k=0}^m \frac{b_k}{(m-k+1)!k!} \right) t^m$$

$$1 = \sum_{m=0}^{\infty} \frac{1}{(m+1)!} \left(\sum_{k=0}^m C_k^{m+1} b_k \right) t^m$$

igualando término a término obtenemos que $b_0 = 1$ y para todo $m \geq 1$ $\frac{1}{(m+1)!} \left(\sum_{k=0}^m C_k^{m+1} b_k \right) = 0$ entonces $\sum_{k=0}^m C_k^{m+1} b_k = 0$, por esto los b_n satisfacen la misma recursión de B_m y $b_0 = B_0 \dagger$

Definición 5.1.3. $S_m(n) = \sum_{i=1}^{n-1} (i)^m$, $m, n \in \mathbb{N}^*$.

Teorema 5.1.4. Dados $m, n \in \mathbb{N}$ $(m+1)S_m(n) = \sum_{k=0}^m C_k^{m+1} B_k n^{m+1-k}$.

Demostración.

$$\sum_{k=0}^{n-1} e^{kt} = \sum_{k=0}^{n-1} \left(\sum_{m=0}^{\infty} k^m \frac{t^m}{m!} \right) = \sum_{m=0}^{\infty} \left(\sum_{k=0}^{n-1} k^m \right) \frac{t^m}{m!} = \sum_{m=0}^{\infty} S_m(n) \frac{t^m}{m!}.$$

Ahora

$$\sum_{k=0}^{n-1} e^{kt} = \frac{e^{nt} - 1}{e^t - 1} = \frac{e^{nt} - 1}{t} \frac{t}{e^t - 1} = \sum_{k=1}^{\infty} \frac{n^k t^{k-1}}{k!} \left(\sum_{m=0}^{\infty} B_m \frac{t^m}{m!} \right) =$$

$$\sum_{k=0}^{\infty} \frac{n^{k+1}t^k}{(k+1)!} \sum_{m=0}^{\infty} B_m \frac{t^m}{m!} = \sum_{m=0}^{\infty} \left(\sum_{k=0}^m \frac{b_k n^{m-k+1}}{(m-k+1)!k!} \right) t^m = \sum_{m=0}^{\infty} \frac{1}{(m+1)!} \left(\sum_{k=0}^m C_k^{m+1} B_k n^{m+1-n} \right) t^m$$

Igualando el coeficiente de t^m se obtiene $\frac{S_m(n)}{m!} = \frac{1}{(m+1)!} \sum_{k=0}^m C_k^{m+1} B_k n^{m+1-n}$ †

Definición 5.1.5. Dados $r \in \mathbb{Q} \setminus \{0\}$, $r = \frac{a}{b}$ ($a, b = 1$) y $p \in \mathbb{Z}$ primo definimos $O_p(r) := \text{ord}_p(a) - \text{ord}_p(b)$ donde $\text{ord}_p(a) = \text{ord}_{\langle p \rangle}(\langle a \rangle)$.

Lema 5.1.6. Dados $r, s \in \mathbb{Q} \setminus \{0\}$, $O_p(rs) = O_p(r) + O_p(s)$.

Demostración. Se sigue del hecho $\text{ord}_{ab}(rs) = \text{ord}_p(a) + \text{ord}_p(b)$ $a, b \in \mathbb{Z} \dagger$

Definición 5.1.7. Sea p un primo en \mathbb{Z} , un racional r se dice **p-entero** si $r \in \mathbb{Z}_{(p)}$, la localización de \mathbb{Z} en p .

Note que r es p -entero si y solo si $O_p(r) \geq 0$

Definición 5.1.8. Dado un primo p y r, s en el anillo de los p -enteros: $r \equiv s \pmod{p^n} \Leftrightarrow O_p(r - s) \geq n$, $n \in \mathbb{N}$.

Lema 5.1.9. $S_m(n) = \sum_{k=0}^m C_k^m B_{m-k} \frac{n^{k+1}}{k+1}$.

Demostración. Por el teorema (5.1.4) $(m+1)S_m(n) = \sum_{i=0}^m C_i^{m+1} B_i n^{m+1-i}$, dado que $C_i^{m+1} = \frac{m+1}{m-i+1} C_i^m$ entonces $S_m(n) = \sum_{i=0}^m C_i^m \frac{B_i n^{m+1-i}}{m+1-i}$ haciendo la sustitución $k = m - i$, en la última suma se obtiene el resultado. †

Lema 5.1.10. Sea p primo y k un entero positivo, entonces

1. $\frac{p^k}{k+1}$ es un p -entero.
2. $\frac{p^k}{k+1} \equiv 0 \pmod{p}$ para $k \geq 2$.
3. $\frac{p^{k-2}}{k+1}$ es un p -entero si $k \geq 3$ y $p \geq 5$.

Demostración. (1) Para probar 1 es suficiente ver que $p^k \geq k+1$ esto se hará por inducción en k . Si $k = 1$ es claro.

Supóngase $p^k \geq k+1 \Rightarrow k+2 \leq p^k + 1 < 2p^k \leq p^{k+1}$.

(2) Si $k \geq 2$ entonces $p^k > k + 1$. Si $k + 1 = p^n q$ (p, q) = 1 $n \geq 0$ entonces $\frac{p^{k-n}}{q} > 1$ por tanto $k > n$ así $k - n \geq 1$ $k - n = o_p(\frac{p^k}{k+1})$ entonces $\frac{p^k}{k+1} \equiv 0(\text{mod } p)$.

(3) Inductivamente se puede ver que $k + 1 < p^{k-2}$ si $k \geq 3$ y $p \geq 5$, a su vez se concluye que $k - 2 > n$ entonces $\frac{p^{k-2-n}}{q}$ es p -entero y $\frac{p^{k-2-n}}{q} \equiv 0(\text{mod } p)$. †

Proposición 5.1.11. *Sea p un primo y m un entero positivo. Entonces pB_m es un p -entero. Si m es par mayor o igual que 2, $pB_m \equiv S_m(n)(\text{mod } p)$.*

Demostración. Como $S_m(p) = pB_m + \sum_{k=1}^m C_k^m B_{m-k} \frac{p^{k+1}}{k+1}$ para probar que pB_m es p -entero es suficiente probar que $C_k^m pB_{m-k} \frac{p^k}{k+1}$ es p -entero para todo $k = 1, \dots, m$.

Probemos por inducción en m que pB_m es p -entero. El caso base claramente se cumple, ahora supóngase que pB_k es p -entero para $1 \leq k \leq m$, por la parte 1 del lema anterior $\frac{p^k}{k+1}$ es p -entero entonces $C_k^m pB_{m-k} \frac{p^k}{k+1}$ es p -entero para $1 \leq k \leq m$.

Para establecer la congruencia es suficiente mostrar que $O_p(C_k^m pB_{m-k} \frac{p^k}{k+1}) \geq 1$ para $1 \leq k \leq m$.

Si $k = 1$ $O_p(\frac{m}{2} pB_{m-1} p) = O_p(\frac{m}{2}) + O_p(pB_{m-1}) + 1 \geq O_p(\frac{m}{2}) + 1$, como m es par esto es mayor o igual a 1.

Si $k \geq 2$ $O_p(C_k^m pB_{m-k} \frac{p^k}{k+1}) \geq O_p(\frac{p^k}{k+1}) \geq 1$ por la parte 3 del lema anterior. †

5.2. Congruencias y criterio de regularidad

Lema 5.2.1. *Sea p un primo. Entonces $S_m(p) \equiv 0(\text{mod } p)$ si $p - 1 \nmid m$ y $S_m(p) \equiv -1(\text{mod } p)$ si $p - 1 \mid m$.*

Demostración. $S_m(p) = \sum_{k=1}^{p-1} k^m$, si $p - 1 \mid m$ entonces $k^{p-1} \equiv 1(\text{mod } p) \forall 1 \leq k \leq m$ por tanto $S_m(p) \equiv p - 1(\text{mod } p)$ entonces $S_m(p) \equiv p - 1(\text{mod } p)$.

Sea g un generador del grupo cíclico \mathbb{Z}_{p^*} tal que $1 < g < p$, $\sum_{k=1}^{p-1} k^m \equiv \sum_{k=1}^{p-1} g^{km}(\text{mod } p)$ entonces $(g^m - 1)S_m(p) \equiv g^{m(p-1)} - 1 \equiv 0(\text{mod } p)$, si $p - 1 \nmid m$, $g^m - 1 \not\equiv 0(\text{mod } p)$ entonces $S_m(p) \equiv 0(\text{mod } p)$.

Teorema 5.2.2. *(Claussen, Staudt) Sea m un entero positivo $B_{2m} = A_{2m} - \sum_{p-1 \mid 2m} \frac{1}{p}$ donde $A_{2m} \in \mathbb{Z}$ y la suma es sobre los primos p tales que $p - 1 \mid 2m$.*

Demostración. Sea n un entero positivo par y definamos $A_n := B_n + \sum_{p-1|n} \frac{1}{p}$, p primos.

Caso 1: Sea q primo tal que $q-1 \nmid B_n$, entonces B_n es un q -entero ya que $qB_n \equiv S_n(q) \equiv 0 \pmod{q}$, de otro lado $\frac{1}{p}$ es q -entero para todo primo p tal que $p \neq q$. Así A_n es q -entero para todo q tal que $q-1 \nmid n$.

Caso 2: Sea q primo tal que $q-1 \mid n$ entonces $A_n := B_n + \frac{1}{q} + \sum_{p-1|n, p \neq q} \frac{1}{p}$, como $q-1 \mid n$, $S_n(q) \equiv -1 \pmod{q}$, y como $qB_n \equiv S_n(q) \pmod{q}$, $qB_n \equiv -1 \pmod{q}$, así por definición $O_q(qB_n + 1) \geq 1$. Ahora $O_q(B_n + \frac{1}{q}) = O_q(qB_n + 1) + O_q(\frac{1}{q}) = O_q(qB_n + 1) - 1 \geq 1 - 1 = 0 \Rightarrow B_n + \frac{1}{q}$ es un q -entero entonces A_n es un p -entero para todo primo $p \Rightarrow A_n \in \bigcap_{p \in \text{Spec}(\mathbb{Z})} \mathbb{Z} \dagger$

Siguiendo en el camino de las propiedades de los números de Bernoulli se tiene la **congruencia de Kummer**, llamada así debido a su autor.

Teorema 5.2.3. *Si p es un primo impar y $p-1 \nmid m$, m un entero positivo par entonces*

$$\frac{B_m}{m} \text{ es un } p\text{-entero y } \frac{B_{m+p-1}}{m+p-1} \equiv \frac{B_m}{m} \pmod{p}.$$

Ver ([2] Teo 5 pg 239).

Los siguientes resultados, también de Kummer, permiten relacionar íntimamente los primos regulares con los números de Bernoulli, sus pruebas requieren sofisticados métodos del análisis complejo los cuales no son el propósito de este trabajo, si se quiere profundizar en el tema puede remitirse a ([4] Corolario al Teorema 2, Teorema 3 pg 377).

Teorema 5.2.4. *(Kummer) Un primo $p \geq 3$ es regular si y sólo si el numerador de los números de Bernoulli $\{B_2, B_4, \dots, B_{p-3}\}$ no es divisible por p .*

Teorema 5.2.5. *(Lema de Kummer) Sea p primo regular, dada una unidad $\epsilon \in \mathbb{Z}[\zeta_p]$, si $\epsilon \equiv a \pmod{p}$ para algún $a \in \mathbb{Z}$ existe $\epsilon_0 \in \mathbb{Z}[\zeta_p]$ tal que $\epsilon = \epsilon_0^p$.*

5.3. Fermat Caso II

Después que Kummer desarrollara su teoría del grupo de clases de ideales y con esta pudiera inventar los primos regulares, Kummer llegó lo mas cerca que ninguno antes

de el hubiese logrado en la búsqueda de respuesta al UTF, lamentablemente el mismo habría de demostrar que a su avance le faltaban infinitos casos por cubrir.

Teorema 5.3.1. *Dado un numero primo $p \geq 3$, si p es regular $x^p + y^p \neq z^p$, para numeros x, y, z todos distintos de cero.*

Demostración. Supongamos que existen $x, y, z \in \mathbb{Z}$ tales que $x^p + y^p = z^p$ y $xyz \neq 0$. Asumamos que x, y, z son primos relativos, dado que el caso 1, ya se ha probado, podemos asumir que uno y sólo uno de x, y, z es divisible por p , sin perdida de generalidad, supongamos z . Por lo tanto existe $z_0 \in \mathbb{Z}$ tal que $z = z_0 p^n$, con $n \geq 1$ y $(z_0, p) = 1$ entonces $x^p + y^p = z_0^p p^{np}$. Sabemos que en $\mathbb{Z}[\zeta_p]$, $p = \lambda_p^{p-1} u$ u invertible en $\mathbb{Z}[\zeta_p]$. Por lo tanto $x^p + y^p = z_0^p (\lambda_p)^{np(p-1)} u_p$. Notese que $(p-1)n \geq 1$ así en $\mathbb{Z}[\zeta_p]$ tenemos una ecuación del tipo

$$x^p + y^p = z_0^p (\lambda_p)^m u_p \quad (5.1)$$

u invertible, x, y, z_0 no divisibles por λ_p y $m \geq 1$. Tomemos una de estas ecuaciones tal que m sea mínimo, sabemos que en $\mathbb{Z}[\zeta_p]$ esta ecuación puede ser escrita como

$$\prod_{i=0}^{p-1} (x + y \zeta_p^i) = z_0^p \lambda_p^m u_p, \quad (5.2)$$

pasando a ideales tenemos

$$\prod_{i=0}^{p-1} \langle x + y \zeta_p^i \rangle = \langle z_0 \rangle^p \langle \lambda_p \rangle^m \quad (5.3)$$

como $mp > 0$, $\langle \lambda_p \rangle$ divide al menos algún $\langle x + y \zeta_p^i \rangle$, como $x + y \zeta_p^i = x + y \zeta_p^j - \zeta_p^j (1 - \zeta_p^{i-j}) y$, $\langle \lambda_p \rangle$ divide a todos los términos en el producto.

Afirmación 5.3.2. *Sea $0 \leq j < i \leq p-1$ entonces la clase de $\frac{x + y \zeta_p^j}{\lambda_p}$ es diferente a la de $x + y \zeta_p^j$ modulo $\langle \lambda_p \rangle$.*

Demostración. Si las clases fueran iguales se tendría que $\lambda_p^2 \mid \zeta_p^j(1 - \zeta_p^{i-j})y$ por tanto $\lambda_p \mid y$, contradiciendo las hipótesis. †

Con esto y ya que $\mathbb{Z}[\zeta_p]/\langle \lambda_p \rangle \cong \mathbb{Z}_p$ tenemos que uno y sólo uno entre $\frac{x+y\zeta_p^i}{\lambda_p}$; $i = 0, \dots, p-1$ es divisible por λ_p o, equivalentemente, uno y sólo uno entre $x + y\zeta_p^i$ es divisible por λ_p^2 . Sin perder generalidad podemos suponer que es $x + y$, ya que en la ecuación original puedo cambiar y por $y\zeta_p^i$.

De la afirmación se deduce que:

$$\begin{aligned} ord_{\lambda_p}(\prod_{i=0}^{p-1} \langle x + y\zeta_p^i \rangle) &= ord_{\lambda_p}(\langle x + y \rangle) + ord_{\lambda_p}(\prod_{i=0}^{p-1} \langle x + y\zeta_p^i \rangle) = ord_{\lambda_p}(\langle x + y \rangle) + \\ \sum_{i=0}^{p-1} ord_{\lambda_p}(\langle x + y\zeta_p^i \rangle) &= ord_{\lambda_p}(\langle x + y \rangle) + p - 1 \geq 2 + p - 1 = p + 1 \\ \text{como } ord_{\lambda_p}(\langle \lambda_p \rangle^{mp} \langle z_0 \rangle^p) &= mp \text{ entonces } m > 1 \end{aligned}$$

Sea $M = \langle x \rangle + \langle y \rangle$, se tiene que $M \not\subseteq \langle \lambda_p \rangle$ ya que $\langle x \rangle \not\subseteq \langle \lambda_p \rangle$ y $\langle y \rangle \not\subseteq \langle \lambda_p \rangle$. Como $M + \langle \lambda_p \rangle = \langle 1 \rangle$ y $\langle x + y\zeta_p^i \rangle \subset M$ se cumple que $\langle \lambda_p \rangle M \supseteq \langle x + y\zeta_p^i \rangle$ por tanto $\langle x + y\zeta_p^i \rangle = \langle \lambda_p \rangle M A_i$ para $i = 1, \dots, p-1$ y A_i ideales tales que $A_i + \langle \lambda_p \rangle = \langle 1 \rangle$. Como $ord_p(\langle z_0 \rangle^p \langle \lambda_p \rangle^{mp}) = mp$ y $ord_p(\prod_{i=1}^{p-1} \langle x + y\zeta_p^i \rangle) = p-1$ tenemos que $\langle x + y \rangle = \langle \lambda_p \rangle^{p(m-1)+1} M A_0$ con $A_0 + \langle \lambda_p \rangle = \langle 1 \rangle$.

Afirmación 5.3.3. $A_i + A_j = \langle 1 \rangle$, $i \neq j$

Demostración. Supongamos que existen ideales $M_{ij} = A_i + A_j$, $i > j$. Entonces $x + y\zeta_p^i$, $x + y\zeta_p^j$ pertenecerían a $\langle \lambda_p \rangle M M_{ij}$ así $x(1 - 1\zeta_p^{i-j})$ y $y\lambda_p^j(1 - 1\zeta_p^{i-j})$ estarían en $\langle \lambda_p \rangle M M_{ij}$ entonces $\langle \lambda_p \rangle M M_{ij}$ dividiría a $\langle x \rangle \langle \lambda_p \rangle$ y $\langle y \rangle \langle \lambda_p \rangle$ por tanto $M M_{ij}$ dividiría tanto a $\langle x \rangle$ como a $\langle y \rangle$ entonces $M M_{ij} = M$ por lo tanto $M_{ij} = \langle 1 \rangle$. †

De lo anterior obtenemos $M^p \langle \lambda_p \rangle^{mp} \prod_{i=0}^{p-1} A_i = \langle \lambda_p \rangle^{pm} \langle z_0 \rangle^p$ como los A_i son coprimos existen B_i ideales tales que $A_i = B_i^p$ para todo i , $i = 0, 1, \dots, p-1$

$$\langle x + y \rangle = \langle \lambda_p \rangle^{p(m-1)+1} M B_0^p \quad (5.4)$$

$$\langle x + y\lambda_p^i \rangle = \langle \lambda_p \rangle M B_i^p \quad (5.5)$$

Sea C_0 ideal tal que B_0C_0 es principal, multiplicando (5.4) por $(C_0B_i)^p$ y (5.5) por $\langle \lambda_p \rangle^{p(m-1)} \langle \alpha_0 \rangle^p$ donde $\langle \alpha_0 \rangle = C_0B_0$ obtenemos

$$\langle x + y\zeta_p^i \rangle \langle \lambda_p \rangle^{p(m-1)} \langle \alpha_0 \rangle^p = \langle x + y \rangle (B_iC_0)^p \quad (5.6)$$

,para $i = 1, \dots, p-1$.

Entonces $(B_iC_0)^p$ es principal, como el primo p es regular (B_iC_0) es principal entonces $(B_iC_0) = \langle \alpha_i \rangle$. Notese que $\alpha_i \notin \langle \lambda_p \rangle$ con $i = 0, \dots, p-1$. Así obtenemos

$$(x + y\zeta_p^i)(\lambda_p)^{p(m-1)} \alpha_0^p = (x + y) \alpha_i^p u_i \quad (5.7)$$

con u_i invertibles para $i = 1, \dots, p-1$.

Consideremos la siguiente ecuación que es claramente cierta

$$(x + y\zeta_p)(1 + \zeta_p) - (x + y\zeta_p^2) = \zeta_p(x + y) \quad (5.8)$$

si multiplicamos esta ecuación por $\lambda_p^{p(m-1)} \alpha_0^p$ y utilizamos (5.7) con $i = 1, 2$ llegamos a

$$(1 + \zeta_p)(x + y) \alpha_1^p u_1 - (x + y) \alpha_2^p u_2 = \zeta_p(x + y) \lambda_p^{p(m-1)} \alpha_0^p \quad (5.9)$$

que es equivalente a

$$(1 + \zeta_p) \alpha_1^p u_1 - \alpha_2^p u_2 = \zeta_p \lambda_p^{p(m-1)} \alpha_0^p \quad (5.10)$$

reescribiendo obtenemos

$$\alpha_1^p + u_3 \alpha_2^p = u_4 \lambda_p^{p(m-1)} \alpha_0^p \quad (5.11)$$

donde $u_3 = \frac{-u_2}{u_1(\zeta_p+1)}$ y $u_4 = \frac{\zeta_p}{u_1(\zeta_p+1)}$. Dado que $p(m-1) \geq p$, $\alpha_1^p + u_3 \alpha_2^p \equiv 0 \pmod{\langle \lambda_p \rangle^p}$ como $\alpha_2 \notin \langle \lambda_p \rangle$ y $\langle \lambda_p \rangle$ es maximal, $\langle \alpha_2 \rangle + \langle \lambda_p \rangle^p = \langle 1 \rangle$ entonces $\alpha_1^p + u_3 \equiv 0 \pmod{\langle \lambda_p \rangle^p}$

$0(\text{mod}\langle p\lambda_p\rangle)$ por tanto $u_3 \equiv -\alpha_1^p(\text{mod}p)$ y $u_3 \equiv a(\text{mod}p)$ para algún a en \mathbb{Z} , se sigue del lema de Kummer que existe $u_5 \in \mathbb{Z}[\zeta_p]$ tal que $u_3 = u_5^p$ por tanto

$$\alpha_1^p + (u_5\alpha_2)^p = u_4\lambda_p^{p(m-1)}\alpha_0^p \quad (5.12)$$

que es una ecuación del tipo (5.1), pero con el exponente de λ_p^p igual a $m-1$, contradiciendo la minimalidad de m . †

5.4. Irregulares e Infinitud

Habiendo mostrado la validez de UTF en el caso de los primos regulares, Kummer se encuentra con que hay infinitos primos no regulares, peor aún no logra demostrar si hay infinitos regulares o no. Hasta el momento esta es una pregunta sin respuesta.

Teorema 5.4.1. $B_{2m} = (-1)^{m+1} 2 \frac{(2m)!}{(2\pi)^{2m}} Z(2m)$

Demostración. La prueba de esto necesita un resultado clásico del análisis:

$$\cot(x) = \frac{1}{x} - 2 \sum_{n=1}^{\infty} \frac{x}{n^2\pi^2 - x^2} \quad (5.13)$$

multiplicando por x

$$x \cot(x) = 1 - 2 \sum_{n=1}^{\infty} \frac{x^2}{n^2\pi^2 - x^2} = 1 - 2 \sum_{n=1}^{\infty} \frac{\left(\frac{x}{n\pi}\right)^2}{1 - \left(\frac{x}{n\pi}\right)^2} \quad (5.14)$$

utilizando la expansión en serie geométrica

$$x \cot(x) = 1 - 2 \sum_{n=1}^{\infty} \left(\sum_{m=1}^{\infty} \frac{x^{2m}}{n^{2m}\pi^{2m}} \right) = 1 - 2 \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \left(\frac{1}{n^{2m}} \right) \frac{x^{2m}}{\pi^{2m}} = 1 - 2 \sum_{m=1}^{\infty} Z(2m) \frac{x^{2m}}{\pi^{2m}} \quad (5.15)$$

de otro lado como $\cos(x) = \frac{e^{ix} + e^{-ix}}{2}$, $\sin(x) = \frac{e^{ix} - e^{-ix}}{2}$ podemos ver que $x \cot(x) = ix + \frac{2ix}{e^{2ix} - 1} = ix + \sum_{n=0}^{\infty} B_n \frac{(2ix)^n}{n!} = 1 + \sum_{n=2}^{\infty} B_n \frac{(2ix)^n}{n!}$ lo que implica

$$-2 \sum_{m=1}^{\infty} Z(2m) \frac{x^{2m}}{\pi^{2m}} = \sum_{n=2}^{\infty} B_n \frac{(2ix)^n}{n!} \quad (5.16)$$

comparando los coeficientes de x^{2m} en ambas series obtenemos el resultado †

Corolario 5.4.2. $|\frac{B_{2m}}{2m}| \rightarrow \infty$ si $m \rightarrow \infty$.

Demostración. Claramente $z(2m) > 1$ entonces $|B_{2m}| > \frac{2(2m)!}{(2\pi)^{2m}}$ de la expresión en serie de e^x es obvio que $e^n > \frac{n^n}{n!} \forall n \geq 1$ por tanto $|B_{2m}| > \frac{2(2m)^{2m}}{(2\pi e)^{2m}} = 2(\frac{m}{\pi e})2m \rightarrow \infty$ si $m \rightarrow \infty$. †

Definición 5.4.3. Un primo p es irregular si no es regular.

Teorema 5.4.4. *El conjunto de los primos irregulares es infinito.*

Demostración. Supongamos que este conjunto es finito, sean p_1, p_2, \dots, p_k sus elementos. Sea $n = m(p_1 - 1)(p_2 - 1)\dots(p_k - 1)$ con m par, como $\frac{B_{2r}}{2r} \rightarrow \infty$ cuando $r \rightarrow \infty$, podemos escoger m lo suficientemente grande para que $|\frac{B_n}{n}| > 1$. Sean u_n, v_n enteros tales que $\frac{B_n}{n} = \frac{u_n}{v_n}$ y $(u_n, v_n) = 1$ encojase un primo p tal que $p | u_n$, si $p - 1 | n$, por (claussen, staud) $p | v_n$, contradiciendo que $(u_n, v_n) = 1$ entonces $p - 1 \nmid n$ y $p \neq p_i, i = 1, 2, \dots, k$ y $p \neq 2$.

Dado $s \equiv n \pmod{p-1}$ con $0 \leq s < p-1$ por lo anterior s es par entonces $2 \leq s \leq p-3$, por la congruencia de Kummer $\frac{B_n}{n} \equiv \frac{B_s}{s} \pmod{p}$, ya que $O_p(\frac{B_n}{n} - \frac{B_m}{m}) > 0$ entonces $O_p(\frac{B_m}{m}) > 0$, $O_p(\frac{B_m}{m}) = O_p(B_m) > 0$ como $2 \leq m \leq p-3$ por el lema de Kummer p es irregular entonces no pueden haber finitos irregulares.

†

Bibliografía

- [1] M.F.Atiyah and I.G.Macdonald, Introduction to Commutative Algebra Addison-Wesley 1969
- [2] Kenneth Ireland and Michael Rosen, A Classical Introduction to Modern Number Theory 2nd. edition, Springer-Verlag 1972
- [3] D.J.H.Garling, A Course in Galois Theory, Cambridge University Press 1986
- [4] Z.I. Borevich and I.R. Shafarevich, Number Theory , Academi Press Inc, 1966
- [5] John B.Fraleigh, A First Course in Abstract Algebra, Addison-Wesley, 1982
- [6] P.Ribenboim. Algebraic Numbers, Wiley, 1972
- [7] H.M. Edwards, Fermat´s Last Theorem, Springer, 1977
- [8] Dino Lorenzini, An Invitation to Arithmetic Geometry, AMS, 1996
- [9] Daniel A. Marcus, Number Fields, Springer-Verlag, 1977
- [10] Harry Pollard, The theory of Algebraic Numbers, The Mathematical Associaton of America, 1950
- [11] Emil Grosswald, Topics From the Theory of Numbers, 2nd. edition, birkhäuser, 1984.