FACULTAD DE MATEMÁTICAS

FACTORIZACIÓN DE IDEALES Y ÚLTIMO TEOREMA DE FERMAT

Trabajo realizado por:

Fernando López Díaz-Jorge

Dirigido por:

Dr. Antonio Rojas León

Índice general

Summary

The objective in the present work is to explain the proof of the famous Fermat's Last Theorem in the particular case of the regular primes when $gcd(xyz, p) = 1$. Before of this, we need to know some important theorems about factorization of ideals, ideal class group or cyclotomic fields, because this results will be fundamental in the proof of the theorem. Finally, we will give a characterization of the regular primes based in Bernoulli's numbers.

Introducción

La motivación de este trabajo es el teorema conjeturado por el matemático Pierre de Fermat en 1637 conocido como **último teorema de Fermat** y que dice lo siguiente:

La ecuación $x^n + y^n = z^n$ *no tiene soluciones con* $x, y, z \in \mathbb{Z}$ *y* $xyz \neq 0$, *cuando* $n \geq 3$.

Basta demostrar que no hay soluciones en el caso $n = 4$ y cuando $n = p \geq 3$ es un número primo (pues en otro caso si tenemos la igualdad $x^{a \cdot b} + y^{a \cdot b} = z^{a \cdot b}$, cualquier solución con exponente $n = a \cdot b$ nos daría una solución con exponente a y otra con exponente b). La prueba del caso $n = 4$ fue proporcionada por Fermat mediante el método del descenso y además, mencionó que tenía la prueba del caso general aunque nunca llegó a mostrarla. Para $p \geq 3$, a la hora de tratar el problema, algunos matemáticos empezaron a considerar dos casos:

1. Cuando $\text{mcd}(xyz, p) = 1$, y

2. cuando $\text{mcd}(xyz, p) = p$.

Nosotros, en concreto, trataremos el primero de los casos, el segundo es técnicamente algo más complicado.

En 1847, Gabriel Lamé presentó una posible demostración del último teorema de Fermat. Dicha demostración consistía en la factorización de $x^p + y^p$ usando números complejos (nos restingimos al primero de los casos como hemos referido antes aunque la demostración de Lamé trataba ambos casos). Esta factorización consistía en lo siguiente:

$$x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta_p^i y),$$

donde ζ_p es una raíz p-ésima de la unidad. A partir de esta factorización, del hecho de que los factores de la derecha son primos entre sí y de la suposición de factorización única en los anillos de la forma $\mathbb{Z}[\zeta_p]$, Lamé conluyó que cada elemento de la factorización era una potencia p-ésima. Es decir, que existe $\beta_i \in \mathbb{Z}[\zeta_p]$ tal que $x + \zeta_p^i y = \beta_i^p$, y después deduciría una contradicción con la existencia de tales β_i.

Dos meses despúes de esta presentación, Ernst Kummer puso de manifiesto un gran error en la demostración de Lamé. Publicó una carta en la que explicaba que tres años antes había demostrado que la factorización única supuesta por Lamé no se daba, en general, en anillos de ese tipo. Pero en esa misma carta, decía que el problema de la factorización se podía *salvar* introduciendo una nueva clase de números complejos que llamó *números complejos ideales*. Estos *nuevos* números complejos son lo que hoy en día llamamos ideales de un anillo.

En lugar de un producto de elementos, Kummer definió los ideales y consideró en la factorización anterior el ideal generado por cada elemento del producto. Comprendió que cada ideal tiene una factorización única como producto de ideales primos (con lo que *salvaba el problema anterior*) y pudo concluir que el ideal generado por cada elemento era una potencia p-ésima.

Si estos ideales encontrados eran principales, Kummer llegaba a una contradicción con su existencia, lo que probaba el teorema.

Pero se encontró con el problema de que dichos ideales no tenían que ser necesariamente principales, lo que supuso la demostración del teorema para una determinada *clase* de números primos (primos regulares). Para el resto de primos no se encontró una demostración hasta 1995 (Andrew Wiles) y se llegó a ella por métodos totalmente distintos.

En el trabajo veremos los detalles de la demostración de Kummer para el caso uno, cuyo enunciado dice:

Para un primo regular $p \geq 3$, la ecuación $x^p + y^p = z^p$ tal que p no divide a x, y o z, no tiene solución en los enteros positivos.

Capítulo 1

Teoría General

Antes de abordar la demostración del teorema, necesitamos ver todo lo que concierne a la factorización de ideales. Además, necesitamos definir *el grupo de clases* que será fundamental para describir los números primos para los que probaremos el último teorema de Fermat.

Por último, veremos como ejemplo la factorización de ideales en cuerpos cuadráticos, y trataremos también los cuerpos ciclotómicos que serán con los que trabajemos en la demostración.

1.1. Anillo de enteros

Antes que nada, veamos el concepto de *anillo de enteros*, pues será donde tendremos la factorización de ideales.

Definición 1.1.1 Sea A un dominio de integridad y sea L un cuerpo conteniendo A. Un elemento α de L es **entero** sobre A si es raíz de un polinomio mónico con coeficientes en A, es decir, satisface una ecuación

$$\alpha^n + a_1\alpha^{n-1} + ... + a_n = 0, a_i \in A$$

Para demostrar que estos elementos forman un anillo, necesitamos la siguiente proposición.

Proposición 1.1.2 *Sea L un cuerpo conteniendo a A. Un elemento $\alpha \in L$ es entero sobre $A \Leftrightarrow$ existe un A-submódulo M de L finitamente generado no nulo tal que $\alpha M \subset M$.*

Demostración: $\Rightarrow$ Supongamos

$$\alpha^n + a_1\alpha^{n-1} + ... + a_n = 0, a_i \in A.$$

Entonces el A-submódulo M de L generado por $1, \alpha, ..., \alpha^{n-1}$ tiene la propiedad de que $\alpha M \subset M$.

$\Leftarrow$ Necesitamos aplicar la regla de Cramer como usualmente la conocemos, es decir, si

$$\sum_{j=1}^{m} c_{ij}x_j = d_i, i = 1, .., m,$$

entonces

$$x_j = \det(C_j)/\det(C)$$

donde $C = (c_{ij})$ y C_j se obtiene de C cambiando los elementos de la columna j-ésima por los d_i. Escribiendo la ecuación de la forma

$$x_j \cdot \det(C) = \det(C_j),$$

esto es cierto sobre cualquier anillo (sea o no $\det(C)$ invertible). La prueba de esto consiste en utilizar la igualdad $\sum_{j=1}^{m} c_{ij}x_j = d_i, i = 1, .., m$ para sustituir en el $\det(C_j)$ los d_i y una vez sustituidos, desarrollando $\det(C_j)$, obtenemos el resultado.

Ahora sea M un A-módulo en L tal que $\alpha M \subset M$, y sean $v_1, ..., v_n$ un conjunto finito de generadores para M. Entonces, para cada i,

$$\alpha v_i = \sum a_{ij}v_j, a_{ij} \in A.$$

Podemos escribir el sistema de ecuaciones como

$$(\alpha - a_{11})v_1 - a_{12}v_2 - a_{13}v_3 - ... = 0$$

$$-a_{21}v_1 + (\alpha - a_{22})v_2 - a_{23}v_3 - ... = 0$$

$$\vdots$$

$$-a_{n1}v_1 - a_{n2}v_2 - ... + (\alpha - a_{nn})v_n = 0$$

Sea C la matriz de coeficientes del lado izquierdo de las igualdades, entonces la regla de Cramer nos dice que $\det(C) \cdot v_i = 0, \forall i$. Como al menos un v_i es no nulo ya que hemos supuesto que $M \neq \emptyset$ y estamos trabajando dentro

del cuerpo L, esto implica que $\det(C) = 0$. Desarrollando el determinante obtenemos la ecuación

$$\alpha^n + a_1\alpha^{n-1} + ... + a_n = 0, a_i \in A,$$

lo que implica que α es entero sobre A. □

Teorema 1.1.3 *Los elementos de L enteros sobre A forman un anillo.*

Demostración: Sean α y β dos elementos de L enteros sobre A, y sean M y N A-módulos en L finitamente generados tal que $\alpha M \subset M$ y $\beta N \subset N$. Definimos MN como el submódulo generado por

$$\{m_i n_i | m_i \in M, n_i \in N\}.$$

Entonces:

(a) MN es un A-submódulo de L (por definición);

(b) MN es finitamente generado ya que, si $e_1, ..., e_m$ generan M y $f_1, ..., f_n$ generan N, entonces $\{e_i f_j\}$ genera MN.

(c) Es cerrado bajo la multiplicación por $\alpha\beta$ y $\alpha \pm \beta$.

Aplicando ahora la proposición (1.1.2) con el A-submódulo MN, deducimos que $\alpha\beta$ y $\alpha \pm \beta$ son enteros sobre A y por tanto, A es un anillo. □

Definición 1.1.4 El anillo formado por los elementos de L enteros sobre A se llama la **clausura entera** de A en L. La clausura entera de $\mathbb{Z}$ en una extensión finita L de $\mathbb{Q}$ se llama el **anillo de enteros** $\mathcal{O}_L$ de L.

Proposición 1.1.5 *Sea K el cuerpo de fracciones de A y sea L un cuerpo conteniendo a K. Si $\alpha \in L$ es algebraico sobre K, entonces existe $d \in A$ tal que $d\alpha$ es entero sobre A.*

Demostración: Como α es algebraico sobre K satisface una ecuación del tipo

$$\alpha^n + a_1\alpha^{n-1} + ... + a_n = 0, a_i \in K.$$

Sea d un común denominador para los a_i, entonces $da_i \in A$ para todo i y la ecuación anterior al multiplicarla por d^n queda:

$$d^n\alpha^n + a_1 d^n\alpha^{n-1} + ... + a_n d^n = 0.$$

Podemos reescribir esa ecuación de la forma:

$$(d\alpha)^n + a_1 d(d\alpha^{n-1}) + ... + a_n d^n = 0.$$

Como $a_1 d, ..., a_n d^n \in A$ se tiene que α es entero sobre A. □

Corolario 1.1.6 *Sea A un dominio de integridad con cuerpo de fracciones K, y sea B la clausura entera de A en un cuerpo L conteniendo a K. Si L es algebraico sobre K, entonces es el cuerpo de fracciones de B.*

Demostración: La proposición (1.1.5) muestra que todo $\alpha \in L$ puede ser escrito como $\alpha = \beta/d$ con $\beta \in B$, $d \in A$. □

Definición 1.1.7 Un dominio de integridad A se dice **íntegramente cerrado** si coincide con su clausura entera en su cuerpo de fracciones K, es decir si $\alpha \in K$, α entero sobre $A \Rightarrow \alpha \in A$.

1.2. Factorización de ideales

En esta sección veremos que en un cierto tipo de anillo todo ideal se puede escribir como producto de ideales primos de forma única, pero antes veamos el concepto de *dominio de Dedekind* ya que será ahí donde tengamos dicha factorización.

Definición 1.2.1 Un **dominio de Dedekind** es un dominio de integridad A, que no es un cuerpo, tal que:

(a) A es noetheriano,
(b) A es íntegramente cerrado, y
(c) todo ideal primo no nulo es maximal

Proposición 1.2.2 *$\mathbb{Z}$ es un dominio de Dedekind.*

Demostración: Sabemos que $\mathbb{Z}$ es un dominio de ideales principales, en particular, todo ideal es finitamente generado, luego es noetheriano.

Sea $p/q \in \mathbb{Q}$ entero sobre $\mathbb{Z}$ con $\gcd(p,q) = 1$, se tiene que $(\frac{p}{q})^n + a_{n-1}(\frac{p}{q})^{n-1} + \cdots + a_0 = 0$, $a_i \in \mathbb{Z} \Rightarrow p^n + a_{n-1}qp^{n-1} + \cdots + a_0q^n = 0$ $\Rightarrow p^n = -a_{n-1}qp^{n-1} - \cdots - a_0q^n \Rightarrow q$ divide a p^n, pero como son primos entre sí, $q = \pm 1 \Rightarrow \frac{p}{q} = \pm p \in \mathbb{Z}$. Esto prueba que $\mathbb{Z}$ es íntegramente cerrado.

Por último, que todo ideal no nulo primo en $\mathbb{Z}$ es maximal se tiene a partir de que un ideal no nulo es primo en $\mathbb{Z}$ si y solo si está generado por un número primo, y sabemos que los ideales generados por estos números son maximales. □

Proposición 1.2.3 *Sea A dominio íntegramente cerrado con cuerpo de fracciones K, y sea B la clusura entera de A en una extensión separable L de K*

de grado m. Entonces existe un A-submódulo M de L finitamente generado tal que $B \subset M$. Por tanto, B es finitamente generado como A-módulo si A es noetheriano.

Demostración: Sea $\{\beta_1, ..., \beta_m\}$ una base de L sobre K, existe $d \in A$ tal que $d \cdot \beta_i \in B$ para todo i. El conjunto $\{d \cdot \beta_1, ..., d \cdot \beta_m\}$ es todavía una base de L como espacio vectorial sobre K, luego podemos suponer que los $\beta_i \in B$. Veamos ahora cómo podemos coger la base dual.

Una forma bilineal se dice no degenerada si verifica las siguientes condiciones equivalentes: tiene discriminante no nulo respecto a una base del espacio vectorial, el núcleo en la primera componente es cero y el núcleo en la segunda componente es cero. A partir de una base $\{e_i\}$ del espacio vectorial y la base dual $\{f_i\}$ ($f_i(e_j) = \delta_{ij}$), podemos usar el isomorfismo $V \to V^\vee$ dado por una forma bilineal no degenerada ψ para pasar de $\{f_i\}$ a una base e_i' de V con la propiedad: $\psi(e_i', e_j) = \delta_{ij}$.

En nuestro caso la forma bilineal no degenerada será la Traza del producto, por lo que tenemos una base dual $\{\beta_1', ..., \beta_m'\}$ de L sobre K tal que Traza$(\beta_i \cdot \beta_j')= \delta_{ij}$. Vamos a mostrar que

$$B \subset A\beta_1' + \cdots + A\beta_m'.$$

Sea $\beta \in B$, entonces β puede ser escrito de forma única como una combinación lineal $\beta = \sum b_j \beta_j'$ con $b_j \in K$. Veamos que cada $b_j \in A$. Como β_i y β están en B, $\beta_i \cdot \beta$ también está, por tanto Traza$(\beta_i \cdot \beta)\in A$. Pero

$$Tr(\beta_i \cdot \beta) = Tr(\sum_j b_j \beta_j' \cdot \beta_i) = \sum_j b_j Tr(\beta_j' \cdot \beta_i) = \sum_j b_j \cdot \delta_{ij} = b_i.$$

Se tiene entonces que $b_i \in A$.

Si A es noetheriano, entonces M es un A-módulo noetheriano, y por tanto B es finitamente generado como A-módulo. □

Puesto que trabajaremos en el anillo de enteros, necesitamos que sea un dominio de Dedekind. Eso es lo que nos dice el siguiente resultado.

Proposición 1.2.4 *Sea A un dominio de Dedekind con cuerpo de fracciones K, y sea B la clausura entera de A en una extensión separable L de K. Entonces B es un dominio de Dedekind. En particular, tomando $A = \mathbb{Z}$ y $K = \mathbb{Q}$, se tiene que el anillo de enteros $\mathcal{O}_L$ en un cuerpo de números L es un dominio de Dedekind.*

Demostración: Veamos primero que B es noetheriano. Por (1.2.3) sabemos que B está contenido en un A-módulo finitamente generado. Se sigue entonces que todo ideal en B es finitamente generado cuando se lo considera A-módulo (siendo un submódulo de un A-módulo noetheriano) y con mayor razón como un ideal.

Lo siguiente es probar que B es íntegramente cerrado. Tenemos que B es la clausura entera de A en L. Sea C la clausura entera de B en L. Claramente $B \subset C$. Sabemos que C es entero sobre B y que B es entero sobre A, por tanto, por la transitividad de la dependencia entera tenemos que C es entero sobre A, lo que implica que $C \subset B$.

Falta probar que todo ideal primo no nulo $\mathfrak{q}$ de B es maximal. Sea $\beta \in \mathfrak{q}$, $\beta \neq 0$, entonces β es entero sobre A y por tanto verifica una ecuación de la forma

$$\beta^n + a_1\beta^{n-1} + \cdots + a_n = 0, a_i \in A,$$

la cual podemos suponer que tiene el mínimo grado posible, entonces $a_n \neq 0$. Como $a_n \in \beta B \cap A$, tenemos que $\mathfrak{q} \cap A \neq (0)$. Pero $\mathfrak{q} \cap A$ es un ideal primo, lo que implica que es un ideal maximal $\mathfrak{p}$ de A (pues A es dominio de Dedekind) y que $A/\mathfrak{p}$ es un cuerpo. Como $\mathfrak{q}$ es primo sabemos que $B/\mathfrak{q}$ es un dominio de integridad, y la aplicación

$$a + \mathfrak{p} \mapsto a + \mathfrak{q}$$

identifica $A/\mathfrak{p}$ con un subcuerpo de $B/\mathfrak{q}$. Dado que B es íntegro sobre A, $B/\mathfrak{q}$ es algebraico sobre $A/\mathfrak{p}$. Si probamos que $B/\mathfrak{q}$ es un cuerpo, tendremos que $\mathfrak{q}$ es maximal. Veamos esto.

Sea c un elemento no nulo de $B/\mathfrak{q}$, tenemos que probar que tiene inverso en $B/\mathfrak{q}$. Como c es algebraico sobre $A/\mathfrak{p}$, el anillo $A/\mathfrak{p}[c]$ tiene dimensión finita como $A/\mathfrak{p}$ espacio vectorial y la aplicación

$$x \mapsto cx : A/\mathfrak{p}[c] \to A/\mathfrak{p}[c]$$

es inyectiva. Por las propiedades del álgebra lineal deducimos que es también sobreyectiva, y por tanto existe un elemento $c' \in A/\mathfrak{p}[c]$ tal que $cc' = 1$. □

Para demostrar el resultado de factorización de ideales necesitamos varios lemas previos.

Lema 1.2.5 *Sea A un anillo noetheriano. Todo ideal I en A contiene un producto de ideales primos no nulos.*

Demostración: Supongamos que no, y sea entonces I un contraejemplo maximal (que existe porque A es noetheriano). Entonces I no puede ser primo, y por tanto, existen elementos x, y de A tal que $xy \in I$ pero ni x ni y pertenecen a I. Los ideales $I + (x)$, $I + (y)$ contienen estrictamente a I, pero su producto está contenido en I. Entonces, como cada uno de los dos ideales $I+(x)$, $I+(y)$ contiene un producto de ideales primos, se tiene que I contiene un producto de ideales primos. Pero eso contradice lo que habíamos supuesto. □

Lema 1.2.6 *Sea A un anillo, y sean I y J ideales primos entre sí en A, es decir, si $I + J = A$. Para cualquier $n \in \mathbb{N}$, I^n y J^m son primos entre sí.*

Demostración: si I^n y J^m no son primos entre sí, entonces ambos están contenidos en algún ideal primo $\mathfrak{p}$. Pero al ser un ideal primo, si contiene un producto de dos ideales debe contener a uno de los dos ideales. Tenemos entonces que como I^n está, se deduce que I también está. Para J se tiene el mismo razonamiento.

Por tanto, $I \subset \mathfrak{p}$ y $J \subset \mathfrak{p}$ lo que contradice la hipótesis de que I y J sean primos entre sí ya que los dos están contenidos en un mismo ideal primo. □

Nota 1.2.7 Si $\mathfrak{p}$ y $\mathfrak{p}'$ son ideales primos distintos no nulos de un dominio de Dedekind, entonces la condición (c) de la definición (1.2.1) implica que $\mathfrak{p}$ y $\mathfrak{p}'$ son primos entre sí, y junto con el lema anterior, que $\mathfrak{p}^n$ y $\mathfrak{p}'^m$ también son primos entre sí.

Lema 1.2.8 *Sea $\mathfrak{p}$ un ideal maximal de un anillo A, sea $A_\mathfrak{p}$ el anillo de fracciones localizado en $\mathfrak{p}$ y sea $\mathfrak{q}$ el ideal que genera $\mathfrak{p}$ en $A_\mathfrak{p}$: $\mathfrak{q} = \mathfrak{p}A_\mathfrak{p}$. La aplicación*

$$a + \mathfrak{p}^n \mapsto a + \mathfrak{q}^n : A/\mathfrak{p}^n \to A_p/\mathfrak{q}^n$$

es un isomorfismo.

Demostración: Primero vemos que es una aplicación inyectiva. Para esto tenemos que probar que $\mathfrak{q}^n \cap A = \mathfrak{p}^n$. Pero notemos que $\mathfrak{q}^n = S^{-1}\mathfrak{p}^n$ donde $S = A - \mathfrak{p}$ luego lo que hay que probar en realidad es que $(S^{-1}\mathfrak{p}^n) \cap A = \mathfrak{p}^n$. Un elemento de $(S^{-1}\mathfrak{p}^n) \cap A$ puede ser escrito de la forma $a = b/s$ con $b \in \mathfrak{p}^n$, $s \in S$ y $a \in A$. Entonces $sa \in \mathfrak{p}^n$ lo que implica que $sa = 0$ en $A/\mathfrak{p}^n$. El único ideal maximal que contiene a $\mathfrak{p}^n$ es $\mathfrak{p}$ porque si $m \supset \mathfrak{p}^n \Rightarrow m \supset \mathfrak{p}$, y por tanto, el único ideal maximal en $A/\mathfrak{p}^n$ es $\mathfrak{p}/\mathfrak{p}^n$. En particular, $A/\mathfrak{p}^n$ es

un anillo local. Como $s + \mathfrak{p}^n$ no está en $\mathfrak{p}/\mathfrak{p}^n$, es una unidad en $A/\mathfrak{p}^n$, luego $sa = 0$ en $A/\mathfrak{p}^n \Rightarrow a = 0$ en $A/\mathfrak{p}^n$, es decir, $a \in \mathfrak{p}^n$.

Veamos ahora que es una aplicación sobreyectiva. Sea $\frac{a}{s} \in A_\mathfrak{p}$. Como s no pertenece a $\mathfrak{p}$ que es maximal, tenemos que $(s) + \mathfrak{p} = A$, es decir, (s) y $\mathfrak{p}$ son primos entre sí. De esta manera, (s) y $\mathfrak{p}^n$ igualmente son primos entre sí, y por tanto, $1 \in (s) + \mathfrak{p}^n$ luego existe $b \in A$ y $q \in \mathfrak{p}^n$ tal que $bs + q = 1$. Entonces b va en s^{-1} en $A_\mathfrak{p}/\mathfrak{q}^n$ y por tanto ba va en $\frac{a}{s}$. Más precisamente, como s es invertible en $A_\mathfrak{p}/\mathfrak{q}^n$, $\frac{a}{s}$ es el único elemento de este anillo tal que $s\frac{a}{s} = a$. Como $s(ba) = a(1 - q)$, la imagen de ba en $A_\mathfrak{p}$ también tiene esta propiedad y así es igual a $\frac{a}{s}$. □

Ahora ya tenemos las herramientas necesarias para demostrar el teorema que nos da la factorización única de ideales.

Teorema 1.2.9 *Sea A un dominio de Dedekind. Todo ideal propio no nulo I de A puede ser escrito de la forma:*

$$I = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$$

donde los $\mathfrak{p}_i$ son ideales primos distintos y los $r_i > 0$. Los $\mathfrak{p}_i$ y los r_i están unívocamente determinados.

Demostración: Aplicando el lema (1.2.6) a A, tenemos que el ideal I contiene un producto de ideales primos no nulos:

$$J = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_n^{s_n}.$$

Podemos suponer que los $\mathfrak{p}_i$ son distintos. Entonces

$$A/J \simeq A/\mathfrak{p}_1^{s_1} \times \cdots \times A/\mathfrak{p}_n^{s_n} \simeq A_{\mathfrak{p}_1}/\mathfrak{q}_1^{s_1} \times \cdots \times A_{\mathfrak{p}_n}/\mathfrak{q}_n^{s_n}$$

donde $\mathfrak{q}_i = \mathfrak{p}_i A_{\mathfrak{p}_i}$ es el ideal maximal del anillo local $A_{\mathfrak{p}_i}$. El primer isomorfismo es consecuencia del Teorema Chino del Resto y del lema (1.2.6) mientras que el segundo isomorfismo viene dado por el lema (1.2.8). Bajo este isomorfismo, I/J corresponde a $\mathfrak{q}_1^{r_1}/\mathfrak{q}_1^{s_1} \times \cdots \times \mathfrak{q}_n^{r_n}/\mathfrak{q}_n^{s_n}$ para algunos $r_i \leq s_i$. Como este ideal es también la imagen de $\mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_n^{s_n}$ bajo el isomorfismo, vemos que

$$I = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$$

en A/J. Ambos ideales contienen a J, lo que implica que

$$I = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$$

en A ya que existe una correspondecia biyectiva entre los ideales de A/J y los ideales de A que contienen a J. Para completar la demostración faltaría ver que la factorización es única, pero en el transcurso de la prueba hemos mostrado que r_i está determinado por la condición:

$$IA_{\mathfrak{p}_i} = \mathfrak{q}_i^{r_i}$$

$\mathfrak{q}_i$ el ideal maximal en $A_{\mathfrak{p}_i}$. □

Es conveniente recordar la relación que existe entre divisibilidad de ideales y contención. Por ejemplo, un ideal I está contenido en otro ideal J si y sólo si existe un ideal K tal que $I = JK$. Además, dicha contención, también es equivalente a que los exponentes de la descomposición de I sean mayores que los de J.

Corolario 1.2.10 *Sea I un ideal en un dominio de Dedekind A, entonces existe un ideal no nulo I^* en A tal que II^* es principal. Además, I^* puede ser elegido tal que $II^* = (a)$ con a un elemento de I que puede ser elegido de forma arbitraria.*

Demostración: Sea $a \in I$, $a \neq 0$, entonces $I \supset (a)$ y por tanto, tenemos

$$(a) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$$

$$I = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_n^{s_n}$$

$s_i \leq r_i$. Si $I^* = \mathfrak{p}_1^{r_1 - s_1} \cdots \mathfrak{p}_n^{r_n - s_n}$, entonces $II^* = (a)$. □

1.3. Grupo de clases de ideales

Los siguiente conceptos necesarios son los de *ideal fraccionario* y *grupo de clases de ideales*.

Definición 1.3.1 Sea A un dominio de Dedekind, un **ideal fraccionario** de A es un sub-A-módulo $\mathfrak{m}$ no nulo de K tal que

$$dm = \{da | a \in m\}$$

está contenido en A para algún $d \in A$ no nulo. Es decir, un sub-A-módulo no nulo de K cuyos elementos tienen un común denominador. Al conjunto de los ideales fraccionarios de A lo denotamos por $Id(A)$.

Esta definición de un ideal fraccionario I es equivalente a decir que existe un ideal J de A y una elemento $a \in A$ tal que $I = \{\frac{b}{a} | b \in J\}$, por lo que existe $d \in A$ tal que dI es un ideal entero.

Nótese que un ideal fraccionario no es un ideal a menos que esté contenido en A. Cuando sea necesario para evitar confusión, nos referiremos a los ideales en A como ideales enteros.

Todo elemento no nulo $b \in K$ define un ideal fraccional

$$(b) =^{def} bA =^{def} \{ba | a \in A\}.$$

Un ideal fraccionario de este tipo se dice **principal**.

El producto de ideales fraccionarios se define de la misma forma que para ideales enteros:

$$\mathfrak{a} \cdot \mathfrak{b} = \{\sum a_i b_i | a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}.$$

Lema 1.3.2 *El producto de ideales fraccionarios es un ideal fraccionario.*

Demostración: Sean $\mathfrak{a}$, $\mathfrak{b}$ dos ideales fraccionarios, el producto de ambos

$$\mathfrak{a} \cdot \mathfrak{b} = \{\sum a_i b_i | a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$$

es claramente un A-módulo. Sean $d, e \in A$ tal que $d\mathfrak{a} \subset A$ y $e\mathfrak{b} \subset A$, que sabemos que existen por definición. Entonces $de\mathfrak{ab} \subset A$, luego por definición se tiene que $\mathfrak{ab}$ es un ideal fraccionario. □

Teorema 1.3.3 *Sea A un dominio de Dedekind, $Id(A)$ es un grupo con el producto de ideales fraccionarios. De hecho, es el grupo abeliano libre en el conjunto de los ideales primos.*

Demostración: Cumple claramente la propiedad asociativa y conmutativa pues

$$(\mathfrak{ab})\mathfrak{c} = \{\Sigma a_i b_i c_i | a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, c_i \in \mathfrak{c}\} = \mathfrak{a}(\mathfrak{bc}).$$

El anillo A juega el papel de elemento unidad. Veamos la existencia de elemento inverso. Sea I un ideal entero no nulo. Por (1.2.10) sabemos que existe un ideal I^* y $a \in A$ tal que $II^* = (a)$. Claramente $I \cdot (a^{-1}I^*) = A$, y por tanto, $a^{-1}I^*$ es un inverso de I. Si I es un ideal fraccionario, entonces dI es un ideal entero para algún d y para un ideal entero sabemos ya que existe inverso. Luego el elemento $d \cdot (dI)^{-1}$ será un inverso de I.

Falta ver que $Id(A)$ es el grupo abeliano libre en el conjunto de los ideales primos, es decir, que cada ideal fraccional puede ser expresado de forma única como producto de potencias de ideales primos. Sea $\mathfrak{a}$ un ideal fraccional, entonces $d\mathfrak{a}$ es un ideal entero para algún $d \in A$ por lo que puede ser escrito como

$$d\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m},$$

$$(d) = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}.$$

Así, $\mathfrak{a} = \mathfrak{p}_1^{r_1 - s_1} \cdots \mathfrak{p}_m^{r_m - s_m}$, y la unicidad se sigue de la unicidad que tenemos para la factorización de ideales primos enteros. □

Definición 1.3.4 El **grupo de clases de ideales** $Cl(A)$ de A es el cociente $Cl(A) = Id(A)/P(A)$ donde $P(A)$ es el subgrupo de los ideales principales. El **número de clases** de A es el orden de $Cl(A)$. En el caso de que A sea el anillo de enteros de un cuerpo K, a menudo nos referimos a $Cl(A)$ como el grupo de clases de ideales de K y a su orden como el número de clases de K.

Teorema 1.3.5 *El número de clases h_K de un cuerpo de números K es finito.*

Demostración: Vamos a utilizar la norma de un ideal I, que viene dada por $N(I) = \#(A/I)$ donde A es el anillo.

Veamos ahora que dado un entero m, existe un número finito de ideales con norma m. Sea J tal que $N(J) = m$. Así, en el grupo cociente A/J el orden de todo elemento divide a m y por tanto, si $x \in A \Rightarrow mx \in J$. En particular, $m = m \cdot 1 \in J$, lo que implica que J divide a Am. Como Am tiene un número finito de divisores (por los resultados de factorización de ideales que hemos visto anteriormente), concluimos que existe un número finito de ideales J con norma m.

Definimos ahora el siguiente número real. Sea $\{x_1, ..., x_n\}$ una base de K y sean para cada $i = 1, ..., n$, $x_i^{(1)} = x_i, x_i^{(2)}, ..., x_i^{(n)}$ los conjugados de x_i.

$$\mu = \prod_{j=1}^{n} \sum_{i=1}^{n} |x_i^{(j)}|,$$

por lo que μ es un número real positivo dependiente de K y la base dada.

Vamos a aplicar ahora lo anterior. La norma de todo ideal fraccionario no nulo es un entero positivo, ya que es $N(J) = \#(A/J)$. Dado, el número μ

definido antes, hemos visto que existe una cantidad finita de ideales no nulos $J_1, ..., J_k$ tal que $N(J_i) \leq \mu$.

Veamos que si I es un ideal no nulo de A, entonces I es equivalente a algún ideal J_i, y por lo tanto el número de clases de ideales es como máximo k, un número finito.

Para ello necesitamos mostrar primero que para todo ideal entero J de A existe un elemento $a \in J$, $a \neq 0$, tal que

$$|N_{K|\mathbb{Q}}(a)| \leq N(J) \cdot \mu,$$

donde $N_{K|\mathbb{Q}}(a)$ es el producto de todos los conjugados de a. Veamos esto.

Si J es un ideal entero no nulo de A, sea k el entero tal que $k^n \leq N(J) < (k+1)^n$. Consideramos el conjunto S de todos los elementos $\sum_{i=1}^n d_i x_i$ donde $0 \leq d_i \leq k$. Como $\#(S) = (k+1)^n > \#(A/J)$, deben existir elementos $b, c \in S$, $b \neq c$, tal que $a = b - c = \sum_{i=1}^n a_i x_i \in J$. Notemos que $|a_i| \leq k$ para cada $i = 1, ..., n$. Se sique que

$$|N_{K|\mathbb{Q}}(a)| = \prod_{j=1}^n \left| \sum_{i=1}^n a_i x_i^{(j)} \right| \leq \prod_{j=1}^n k \left(\sum_{i=1}^n |x_i^{(j)}| \right) = k^n \mu \leq N(J)\mu.$$

Una vez visto esto, denotemos por I^{-1} el ideal fraccionario inverso de I, existe entonces un elemento $c \in A$, $c \neq 0$, tal que cI^{-1} es un ideal entero. Por lo que acabamos de mostrar, existe un elemento $b \in cI^{-1}$, $b \neq 0$, tal que $N(Ab) \leq N(cI^{-1}) \cdot \mu$. Multiplicando por $N(I)$ y teniendo en cuenta que $Ibc^{-1} \subseteq A$, obtenemos

$$N(Ibc^{-1}) \cdot N(Ac) = N(Ibc^{-1} \cdot Ac) = N(Ib),$$

$$N(Ibc^{-1}) \cdot N(Ac) = N(Ab) \cdot N(I) \leq N(cI^{-1}) \cdot N(I)\mu = N(Ac)\mu.$$

Se tiene que $N(Ibc^{-1}) \leq \mu$, y por tanto, $Ibc^{-1} = J_i$ para algún i. □

1.4. Factorización en extensiones

Sea A un dominio de Dedekind con cuerpo de fracciones K y sea B la clausura entera de A en una extensión finita separable L de K. En esta sección mostraremos el teorema que nos da explícitamente la factorización de un ideal en B y trataremos el caso especial en el que la extensión es de Galois.

Un ideal primo $\mathfrak{p}$ de A factorizará en B

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}, e_i \geq 1.$$

Si cualquiera de los $e_i > 1$, diremos que $\mathfrak{p}$ es **ramificado** en B (o L) y el número e_i se llama **índice de ramificación**. Decimos que $\mathfrak{P}$ divide a $\mathfrak{p}$ si $\mathfrak{P}$ aparece en la factorización de $\mathfrak{p}$ en B. Escribiremos $e(\mathfrak{P}/\mathfrak{p})$ para el índice de ramificación y $f(\mathfrak{P}/\mathfrak{p})$ para el grado de la extensión $[B/\mathfrak{P} : A/\mathfrak{p}]$. Un primo se dice **totalmente descompuesto** en L si $e_i = f_i = 1$ para todo i, y se dice **inerte** en L si $\mathfrak{p}B$ es un ideal primo ($g = 1 = e$).

Teorema 1.4.1 *Supongamos que $B = A[\alpha]$ y sea $f(x)$ el polinomio mínimo de α sobre K. Sea p un ideal primo en A. Elegimos polinomios mónicos $g_1(x), ..., g_r(x)$ en $A[x]$ que son distintos e irreducibles módulo p y tales que $f(x) = \Pi g_i(x)^{e_i}$ módulo p. Entonces*

$$pB = \Pi(p, g_i(\alpha))^{e_i}$$

es precisamente la factorización de pB como producto de potencias de ideales primos distintos.

Demostración: Partiendo de que $B = A[\alpha]$, como el homomorfismo

$$A[x] \to B$$

$$x \mapsto \alpha$$

es claramente sobreyectivo, por el primer teorema de isomorfía tenemos el siguiente isomorfismo:

$$A[x]/(f(x)) \to B.$$

Ahora tomamos cociente por el ideal p en los dos lados. En el primer lado queda lo siguiente:

$$A[x]/(f(x), p) = (A[x]/pA[x])/(\bar{f}(x)) = k[x]/(\bar{f}(x))$$

donde $k[x] = A/p$ y $\bar{f}(x)$ es el polinomio $f(x)$ módulo p. El isomorfismo que tenemos ahora por tanto es:

$$k[x]/(\bar{f}(x)) \to B/pB$$

$$x \mapsto \alpha.$$

Los ideales maximales del anillo $k[x]/(\bar{f}(x))$ son los generados por los $g_i(x)$ irreducibles tales que $g_i(x)|\bar{f}(x)$. Esto se debe a la correspondencia biyectiva que hay entre los ideales maximales de $k[x]/(\bar{f}(x))$ y los ideales maximales de $k[x]$ (los generados por polinomios irrreducibles) que contienen a $(\bar{f}(x))$, es decir, que dividen a $\bar{f}(x)$.

Estos ideales, mediante el isomorfismo, se corresponden con los ideales maximales de B/pB, es decir, los generados por $g_i(\alpha)$. Al igual que antes, estos ideales de B/pB están en correspondencia con los ideales maximales de B que contienen a pB, que son los

$$(g_i(\alpha), p).$$

Por otro lado, como

$$\bar{f}(x) = g_1(x)^{e_1} \cdots g_r(x)^{e_r}$$

tenemos que en $k[x]/(\bar{f}(x))$,

$$g_1(x)^{e_1} \cdots g_r(x)^{e_r} = 0.$$

Por tanto, mediante el isomorfismo, en B/pB

$$g_1(\alpha)^{e_1} \cdots g_r(\alpha)^{e_r} = 0.$$

Por último, pasando a B, tenemos que

$$pB = (g_1(\alpha), p)^{e_1} \cdots (g_r(\alpha), p)^{e_r}.$$

□

Proposición 1.4.2 *Seaa m el grado de L sobre K, y sean $\mathfrak{P}_1, ..., \mathfrak{P}_g$ ideales primos dividiendo a $\mathfrak{p}$, entonces:*

$$\sum_{i=1}^{g} e_i f_i = m.$$

Demostración: Vamos a mostrar que ambos lados de la igualdad anterior se corresponden con $[B/\mathfrak{p}B : A/\mathfrak{p}]$.

Notemos que $B/\mathfrak{p}B = B/\prod \mathfrak{P}_i^{e_i} \simeq \prod B/\mathfrak{P}_i^{e_i}$ por el Teorema Chino del Resto, y por tanto, basta demostrar que $[B/\mathfrak{P}_i^{e_i} : A/\mathfrak{p}]$=$e_i f_i$. De la definición de f_i, sabemos que $B/\mathfrak{P}_i$ es un cuerpo de grado f_i sobre $A/\mathfrak{p}$. Para cada r_i, $\mathfrak{P}_i^{r_i}/\mathfrak{P}_i^{r_{i+1}}$ es un $B/\mathfrak{P}_i$-módulo, y como no existe un ideal entre $\mathfrak{P}_i^{r_i}$ y

$\mathfrak{P}_i^{r_{i+1}}$ (si existiera tal ideal J tendríamos que $\mathfrak{P}_i^i|J$ y que $J|\mathfrak{P}_i^{i+1}$, pero por la factorización de ideales vista anteriormente llegaríamos a que J debe ser uno de los dos ideales), debe tener dimensión uno como $B/\mathfrak{P}_i$-espacio vectorial por lo que tiene dimensión f_i como $A/\mathfrak{p}$ espacio vectorial. Luego cada cociente en la cadena

$$B \supset \mathfrak{P}_i \supset \mathfrak{P}_i^2 \supset \cdots \mathfrak{P}_i^{e_i}$$

tiene dimensión f_i sobre $A/\mathfrak{p}$, y por ello, la dimensión de $B/\mathfrak{P}_i^{e_i}$ es $e_i f_i$.

La prueba de que $[B/\mathfrak{p}B : A/\mathfrak{p}]=m$ es fácil cuando B es un A-módulo libre, porque un isomorfismo $A^n \to B$ de A-módulos cuando tensorizamos con K, nos da un isomorfismo $K^n \to L$ lo que muestra que $n = m$, y cuando tensorizamos con $A/\mathfrak{p}$, nos da un isomorfismo $(A/\mathfrak{p})^n \to B/\mathfrak{p}B$ lo que muestra que $n=[B/\mathfrak{p} : A/\mathfrak{p}B]$.

Si B no es un A-módulo libre, al tomar el subconjunto multiplicativamente cerrado $S = A - \mathfrak{p}$ de A se obtiene que $S^{-1}A$ es principal. Consideramos $B' = S^{-1}B$ y $A' = S^{-1}A$. Entonces $\mathfrak{p}B' = \prod(\mathfrak{P}_i B')^{e_i}$ y por tanto, $\sum e_i f_i=[B'/\mathfrak{p}B' : A'/\mathfrak{p}A']$. Pero A' es principal, por lo que se tiene que $[B'/\mathfrak{p}B' : A'/\mathfrak{p}A']=m$. □

Proposición 1.4.3 *Supongamos que la extensión $L|K$ es de Galois. Entonces, si Q,Q' son ideales primos de B tal que $Q \cap A = Q' \cap A \neq \{0\}$, existe $\sigma \in G$ tal que $\sigma(Q) = Q'$ donde G es el grupo de Galois de la extensión $L|K$.*

Demostración: Sea $G = \{\sigma_1, ..., \sigma_n\}$ el grupo de Galois de $L|K$ y supongamos que $Q' \neq \sigma_i(Q)\ \forall \sigma_i \in G$. Por el Teorema Chino del Resto, existe un elemento $x \in B$ tal que $x \notin \sigma_i(Q)\ \forall i = 1, ..., n$, $x \in Q'$. Sea

$$a = \prod_{i=1}^{n} \sigma_i(x),$$

entonces $a \in A \cap Q'$. Sin embargo, $a \notin Q$ ya que cada $\sigma_i(x) \notin Q\ \forall i = 1, ..., n$ (en otro caso $x = \sigma_i^{-1}\sigma_i(x) \in \sigma_i^{-1}(Q)$, para algún i). Esto es una contradicción, por lo que existe $\sigma_i \in G$ tal que $\sigma_i(Q) = Q'$. □

Corolario 1.4.4 *Si $L|K$ es una extensión de Galois de grado n, $Bp = \prod_{i=1}^{g} Q_i^{e_i}$ y $[B/Q_i : A/p] = f_i$, entonces $e_1 = \cdots = e_g$, $f_1 = \cdots = f_g$.*

Demostración: sea $Bp = \prod_{i=1}^{g} Q_i^{e_i}$, $\forall j$, $1 \leq j \leq g$, por (1.4.3) tenemos que existe $\sigma \in G$ tal que $\sigma(Q_1) = Q_j$. A partir de que $Bp = \sigma(Bp) = \prod_{i=1}^{g} \sigma(Q_i)^{e_i}$ y de la unicidad en la descomposición de Bp en producto de ideales primos,

se sigue que $e_j = e_1 \ \forall j,\ 1 \leq j \leq g$. De forma similar, a partir de que $B/Q_j = B/\sigma(Q_1) \cong B/Q_1$ se sigue que $f_i = f_1 \ \forall j,\ 1 \leq j \leq g$. □

1.5. Cuerpos cuadráticos

Como ejemplo, veamos la factorización de ideales en los cuerpos cuadráticos. Para ellos lo primero es conocer el anillo de enteros.

Proposición 1.5.1 *Sea d un entero libre de cuadrados, el anillo de enteros de $K = \mathbb{Q}(\sqrt{d})$ es:*
(a) $\mathcal{O}_k = \mathbb{Z}[\sqrt{d}]$ si $d \equiv 2, 3 \ mod\ 4$
(b) $\mathcal{O}_k = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ si $d \equiv 1 \ mod\ 4$.

Demostración: Sea $x = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ con $b \neq 0$, el polinomio mínimo es

$$(x - (a + b\sqrt{d}))(x - (a - b\sqrt{d})) = x^2 - 2ax + (a^2 - b^2 d).$$

Para que $x \in \mathcal{O}_K \Rightarrow 2a \in \mathbb{Z}$ y $(a^2 - b^2 d) \in \mathbb{Z}$.

$$2a \in \mathbb{Z} \Rightarrow a = \frac{A}{2}, A \in \mathbb{Z}$$

$$(\frac{A^2}{4} - b^2 m) \in \mathbb{Z} \Rightarrow (A^2 - 4b^2 d) \in 4\mathbb{Z} \Rightarrow 4b^2 d = (2b)^2 d \in \mathbb{Z}$$

y como d es libre de cuadrados

$$2b \in \mathbb{Z} \Rightarrow b = \frac{B}{2}, B \in \mathbb{Z}.$$

Queda entonces:

$$\frac{A^2}{4} - \frac{B^2}{4} d \in \mathbb{Z} \Rightarrow A^2 - B^2 d \in 4\mathbb{Z} \Rightarrow A^2 \equiv B^2 d, \quad \text{mód } 4.$$

A partir de esto conlcuimos lo siquiente:

Si $d \equiv 3 \mod 4 \Rightarrow A \equiv B \mod 2$. Si A y B fueran impares, tendríamos que $1 \equiv 3 \mod 4$ (ya que un número impar al cuadrado es congruente con uno módulo cuatro), lo que es una contradicción. Por tanto, A y B son pares, luego $a = \frac{A}{2}$ y $b = \frac{B}{2}$ están en $\mathbb{Z}$.

Si $d \equiv 2 \mod 4 \Rightarrow A^2 \equiv 0 \mod 2 \Rightarrow A$ es par. Si B fuera impar, quedaría $A^2 \equiv 2 \mod 4$ (por el mismo razonamiento que antes para un número impar

al cuadrado módulo cuatro). Pero esto no se puede dar, pues un número par al cuadrado es congruente con cero módulo cuatro. Esto implica que B también es par y al igual que antes, $a, b \in \mathbb{Z}$.

Si $d \equiv 1 \mod 4 \Rightarrow$ o bien A y B son pares, o bien A y B son impares $\Rightarrow$ $A \equiv B \mod 2$. Aparecen aquí dos posiblidades: $a, b \in \mathbb{Z}$ o $a, b \in \mathbb{Z} + \frac{1}{2}$. $\square$

Sea p un número primo, vamos a determinar la descomposición de Ap en producto de ideales primos de A donde $A = \mathcal{O}_K$. Para ellos utilizamos el teorema (1.4.1) además de tener en cuenta que si $d \equiv 2, 3 \mod 4$ el polinomio mínimo de $\sqrt{d}$ es $x^2 - d$, y si $d \equiv 1 \mod 4$ el polinomio mínimo de $\frac{1+\sqrt{d}}{2}$ es $x^2 - x + \frac{1-d}{4}$.

Tenemos cuatro posibilidades en la factorización de Ap:

1. Si $p|d \Rightarrow$ al reducir el polinomio módulo p vemos que obtenemos x^2 por un lado y $x^2 - x + \frac{1}{4}$ por otro. En ambos casos tenemos una raíz doble, luego Ap factoriza como producto de dos ideales primos iguales.

2. Si p es un primo impar que no divide a d tenemos:

   En el caso en que d es un cuadrado $\mod p$, por ejemplo $d \equiv a^2 \mod p$, los polinomios al tomar módulo p quedan $x^2 - a^2$ y $x^2 - x + \frac{1-a^2}{4}$. En el primer caso es claro que tiene dos soluciones distintas y en el segundo basta ver que el discriminante del polinomio es a^2 para confirmar que sucede lo mismo. Esto conlleva que Ap es el producto de dos ideales primos distintos.

   En cambio, cuando d no es un cuadrado módulo p, en el primer caso de nuevo es obvio que el polinomio es irreducible módulo p. En el segundo caso nos fijamos en que el discriminante es d y como estamos suponiendo que d no es un cuadrado módulo p, llegamos a que el polinomio es irreducible módulo p. Por tanto, Ap es un ideal primo.

3. Veamos el caso en el que $p = 2$ y $d \equiv 1 \mod 4$. Entonces tenemos:

   Ap es el producto de dos ideales primos distintos $\Leftrightarrow d \equiv 1 \mod 8$. Esto se debe a que como $d \equiv 1 \mod 8$ el polinomio mínimo mod 2 factoriza como $x^2 + x \equiv x(x + 1)$ y por tanto, $A2 = (2, \alpha)(2, 1 + \alpha)$ donde $\alpha = \frac{1+\sqrt{d}}{2}$.

Ap es un ideal primo $\Leftrightarrow d \equiv 5 \bmod 8$. Esto es consecuencia de que si $d \equiv 5 \bmod 8$ el polinomio mínimo mod 2 factoriza como $x^2 + x + 1$, el cual es irreducible.

4. Por último falta ver cuando $p = 2$ y $d \equiv 3 \mod 4$. Este caso es sencillo ya que el polinomio es $x^2 - d$ y al reducir módulo p nos queda $x^2 - 1$ pues nótese que si $d \equiv 3 \mod 4 \Rightarrow d \equiv 1 \mod 2$. Sólo falta observar que el polinomio $x^2 - 1$ tiene una raíz doble en $\mathbb{Z}/\mathbb{Z}2$, lo que implica que Ap factoriza como producto de dos ideales primos iguales.

1.6. Cuerpos ciclotómicos

Por último en este capítulo, vamos a tratar el caso de los cuerpos ciclotómicos, que son los que verdaderamente nos interesan de cara a la prueba del teorema.

Sea $K = \mathbb{Q}(\zeta)$, donde ζ es una raíz p-ésima de la unidad siendo p un número primo impar. Veamos que el polinomio mínimo de ζ sobre $\mathbb{Q}$ es

$$\Phi_p = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + ... + x + 1.$$

Basta ver que es irreducible y que tiene a ζ como raíz. Lo segundo se observa fácilmente. Para ver que es irreducible, hacemos el cambio de variable $x \to x + 1$:

$$\widetilde{\Phi_p} = \frac{(x+1)^p - 1}{x}$$

Por las propiedades de los coeficientes binomiales, tenemos que $(x+1)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k}$. Queda pues

$$\widetilde{\Phi_p} = \frac{(\sum_{k=0}^{p} \binom{p}{k} x^{p-k}) - 1}{x} = \frac{\sum_{k=0}^{p-1} \binom{p}{k} x^{p-k}}{x} = \sum_{k=0}^{p-1} \binom{p}{k} x^{p-k-1}.$$

El polinomio es mónico, el término independiente es p y los demás coeficientes son de la forma $\frac{p!}{(p-k)!k!}$ con $1 \leq k \leq p-2$ claramente divisibles por p. Aplicando el criterio de Eisenstein, obtenemos que $\widetilde{\Phi_p}$ es irreducible, lo que implica que Φ_p también lo es.

Como $\zeta^p - 1 = 0$, tenemos que ζ pertenece al anillo A de los enteros de $\mathbb{Q}(\zeta)$. Las raíces de Φ_p son $\zeta, \zeta^2, ..., \zeta^{p-1}$, así

$$\Phi_p = \prod_{i=1}^{p-1}(x - \zeta^i).$$

En particular, $p = \Phi_p(1) = \prod_{i=1}^{p-1}(1 - \zeta^i)$. Notemos que los elementos $1 - \zeta, 1 - \zeta^2, ..., 1 - \zeta^{p-1}$ son asociados. En efecto, si $1 \leq i, j \leq p - 1$ entonces existe un entero k tal que $j \equiv ik \bmod(p)$. Así,

$$\frac{1 - \zeta^j}{1 - \zeta^i} = \frac{1 - \zeta^{ik}}{1 - \zeta^i} = 1 + \zeta^i + \zeta^{2i} + ... + \zeta^{(k-1)i} \in A.$$

De forma similar, $(1-\zeta^i)/(1-\zeta^j) \in A$, por tanto $1-\zeta^j = u_j(1-\zeta)$ donde u_j es una unidad de A. Luego concluimos que $p = u(1-\zeta)^{p-1}$ donde $u = u_1 \cdots u_{p-1}$ es una unidad de A.

El elemento $1-\zeta$ no es invertible en A, pues en otro caso p tendría inverso, el cual pertenece a $A \cap \mathbb{Q} = \mathbb{Z}$. Por tanto, $A(1 - \zeta) \cap \mathbb{Z} = \mathbb{Z}p$ ya que el ideal $A(1 - \zeta) \cap \mathbb{Z}$ contiene a p y no es igual al ideal unidad.

Primero veamos cuál es el anillo de enteros de un cuerpo ciclotómico y luego mostraremos la forma que tiene la descomposición en ideales primos del ideal Aq donde q es un primo cualquiera.

Proposición 1.6.1 *$\mathcal{O}_K$ es un grupo libre abeliano con base $\{1, \zeta, ..., \zeta^{p-2}\}$, y por tanto, $\mathcal{O}_K = \mathbb{Z}[\zeta]$.*

Demostración: $1, \zeta, ..., \zeta^{p-2}$ son linealmente independientes sobre $\mathbb{Q}$, pues si no lo fueran, ζ sería raíz de un polinomio de grado $p - 2$ a lo más, contradiciendo que Φ_p es el polinomio mínimo.

Si $x \in \mathcal{O}_K \Rightarrow$ existen números racionales $a_0, a_1, ..., a_{p-2}$ definidos de forma única tal que $x = a_0 + a_1\zeta + ... + a_{p-2}\zeta^{p-2}$. Veamos que $a_i \in \mathbb{Z}$ con lo que se tendrá el resultado.

Observemos qué pasa con las trazas en $\mathbb{Q}(\zeta)|\mathbb{Q}$ (recordemos que la traza de un elemento es la suma de los conjugados de Galois de ese elemento en la extensión en cuestión). Tenemos

$$Tr(x(1 - \zeta)) = Tr(a_0(1 - \zeta)) = a_0 \cdot Tr(1 - \zeta) = a_0[(p - 1) + 1] = a_0p.$$

Para mostrar que $a_0 \in \mathbb{Z}$, calculamos $Tr(x(1 - \zeta))$.

Sean $x_1 = x, x_2, ..., x_{p-1} \in \mathcal{O}_K$ los conjugados de x:

$$Tr(x(1-\zeta)) = x_1(1-\zeta)+x_2(1-\zeta^2)+...+x_{p-1}(1-\zeta^{p-1}) = (1-\zeta)x' \in \mathcal{O}_K(1-\zeta),$$

ya que $(1-\zeta^{j-1})/(1-\zeta) = 1+\zeta+...+\zeta^j \in \mathcal{O}_K$. Pero $Tr(x(1-\zeta)) \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, luego $Tr(x(1-\zeta)) \in \mathcal{O}_K(1-\zeta) \cap \mathbb{Z} = p\mathbb{Z}$, es decir, $a_0 \in \mathbb{Z}$.

Ahora por inducción se prueba que $a_1, ..., a_{p-2} \in \mathbb{Z}$. Para probar que $a_j \in \mathbb{Z}$, multiplicamos por ζ^{p-j} obteniendo $x\zeta^{p-j} = a_0\zeta^{p-j} + a_1\zeta^{p-j+1} + ... + a_{j-1}\zeta^{p-1} + a_j + a_{j+1}\zeta + ... + a_{p-2}\zeta^{p-2}$, y expresando $\zeta^p - 1$ en términos de potencias inferiores de ζ, podemos escribir $x\zeta^{p-j}$ de la forma

$$x\zeta^{p-j} = (a_j - a_{j-1}) + a'_1\zeta + a'_2\zeta^2 + ... + a'_{p-2}\zeta^{p-2}.$$

Por inducción $a_{j-1} \in \mathbb{Z}$, luego aplicando el mismo argumento que antes, $(a_j - a_{j-1}) \in \mathbb{Z} \Rightarrow a_j \in \mathbb{Z}$. □

Proposición 1.6.2 *Sea $\xi = 1-\zeta \in A$, entonces el ideal principal $A\xi$ es primo y $Ap=(A\xi)^{p-1}$.*

Demostración: Sabemos que $p = u\xi^{p-1}$, donde u es una unidad de A. Así, $Ap=(A\xi)^{p-1}$. Tomando normas tenemos que $p^{p-1}=N(Ap)=(N(A\xi)^{p-1})$, y por tanto, $N(A\xi)=p$. Como conlusión se tiene que $A\xi$ tiene que ser un ideal primo de A. □

El siguiente resultado nos muestra la factorización en este tipo de cuerpos.

Teorema 1.6.3 *Sea q un primo distinto de p, sea $f \geq 1$ el menor entero tal que $q^f \equiv 1$ mod p y sea $g = (p-1)/f$. Entonces $\mathcal{O}_K q = Q_1 \cdots Q_g$ donde $Q_1, ..., Q_g$ son ideales primos distintos de $\mathcal{O}_K$.*

Demostración: Denotemos $A = \mathcal{O}_K$. Por la teoría desarrollada hasta aquí, $Aq = (Q_1 \cdots Q_g)^e$ (pues se trata de una extensión de Galois) donde $Q_1, ..., Q_g$ son ideales primos distintos, $e \geq 1$ y $efg = p-1$. Así, $f = [A/Q_i|\mathbb{Z}/q\mathbb{Z}]$ para cada $i = 1, ..., g$.

Nos fijamos ahora en el ideal primo $Q = Q_1$. Sea $\mathcal{G}$ el grupo de Galois, definimos $\mathcal{Z} = \{\sigma \in \mathcal{G} | \sigma(Q) = Q\}$. Entonces $\mathcal{Z}$ es un subgrupo de $\mathcal{G}$ y su índice es $(\mathcal{G}:\mathcal{Z}) = g$. En efecto, si $\sigma, \tau \in \mathcal{G} \Rightarrow \sigma\mathcal{Z} = \tau\mathcal{Z} \Leftrightarrow \sigma(Q) = \tau(Q)$. Por otro lado, por (1.4.4), para cada $i = 1, .., g$, existe $\sigma \in \mathcal{G}$ tal que $\sigma(Q) = Q_i$. Así $g = (\mathcal{G}:\mathcal{Z})$, por tanto $\sharp(\mathcal{Z}) = ef$ pues $efg = |G| = |\mathcal{Z}||G : \mathcal{Z}| = |\mathcal{Z}|g$.

Con todos los $\sigma \in \mathcal{Z}$ tenemos la aplicación $\bar{\sigma} : A/Q \to A/Q$ definida como $\bar{\sigma}(\bar{x}) = \overline{\sigma(x)}$ donde $\bar{t}$ denota $t+Q \in A/Q$ para cada $t \in A$. Tenemos que $\bar{\sigma} \in G(A/Q|\mathbb{F}_q)$ y la aplicación $\mathcal{Z} \Rightarrow G(A/Q|\mathbb{F}_q)$ así definida es un homomorfismo de grupos. El núcleo es el subgrupo normal $\Gamma = \{\sigma \in \mathcal{Z} | \sigma(x) \equiv x \bmod Q \ \forall x \in A\}$. Veamos que Γ se reduce a la identidad por lo que la aplicación $\mathcal{Z} \Rightarrow G(A/Q|\mathbb{F}_q)$ es inyectiva. En efecto, $\sigma(\zeta)$ es también una raíz p-ésima de la unidad (pues lleva raíces en raíces) por lo que $\sigma(\zeta) = \zeta^s$ donde $1 \leq s \leq p$ y $\gcd(s,p) = 1$.

Si $\sigma \in \Gamma$ entonces Q contiene el elemento $\sigma(\zeta) - \zeta = \zeta^s - \zeta = -\zeta(1-\zeta^{s-1})$. Como $\gcd(s-1,p) = 1$ entonces hemos visto que $1-\zeta^{s-1}$ y $1-\zeta$ son elementos asociados, por tanto $\xi = 1-\zeta \in Q$ por ser Q ideal primo, esto es, $Q = A\xi$ (ya que $A\xi$ es un ideal primo por (1.6.2)) y Q divide a Ap que no es el caso.

Como conclusión se tiene que la aplicación de $\mathcal{Z}$ a $G(A/Q|\mathbb{F}_q)$ es inyectiva y $ef = \sharp(\mathcal{Z}) \leq \sharp(G(A/Q|\mathbb{F}_q)) = [A/Q : \mathbb{F}_q] = f$, implicando ya que $e = 1$. Ahora veamos que $f \geq 1$ es el menor entero tal que $q^f \equiv 1 \bmod(p)$.

Sea σ_q el *automorfismo de Frobenius* del grupo de Galois, esto es, $\bar{\sigma_q}(\bar{x}) = \bar{x}^q$ para cada $\bar{x} \in A/Q$. Entonces $(\bar{\sigma}_q)^f$ es el automorfismo identidad, por tanto σ_q^f es el automorfismo identidad ya que la aplicación $\mathcal{Z} \to G(A/Q|\mathbb{F}_q)$ es inyectiva.

Así $\sigma_q^f(\zeta) = \zeta^{q^f}$ es igual a $\zeta \Rightarrow \zeta^{q^f-1} = 1 \Rightarrow p$ divide a $q^f - 1$.

Si $1 \leq f' \leq f$ y p divide a $q^{f'} - 1$, entonces $\sigma_q^{f'}$ es la identidad, y por tanto $\bar{\sigma}_q^{f'}$ es la identidad, lo cual fuerza que $f = f'$, porque $\bar{\sigma_q}$ es un generador de $G(A/Q|\mathbb{F}_q)$, lo que prueba que tienen orden f. □

Antes de pasar a la ecuación de Fermat nos falta por ver cómo son las unidades en los cuerpos ciclotómicos. Para ello necesitamos un lema previo.

Lema 1.6.4 (Kronecker) *Sea $\alpha \in \mathbb{C}$ entero sobre $\mathbb{Q}$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$ y tal que todos sus conjugados tienen módulo uno, entonces α es una raíz de la unidad.*

Demostración: Por las hipótesis sabemos que α satisface una ecuación del tipo

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, a_i \in \mathbb{Z}.$$

Podemos factorizar el polinomio de la siguiente forma

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \prod (x - \alpha_i)$$

donde α_i son los conjugados de α. Notemos que para todo i, α_i tiene módulo uno por ser conjugado de α.

Veamos ahora que los coeficientes del polinomio están acotados.

$$a_{n-1} = -\sum \alpha_i \Rightarrow |a_{n-1}| \leq n$$

$$a_{n-2} = \sum \alpha_i\alpha_j \Rightarrow |a_{n-2}| \leq \binom{n}{2}$$

$$a_{n-3} = -\sum \alpha_i\alpha_j\alpha_k \Rightarrow |a_{n-3}| \leq \binom{n}{3}$$

$$\vdots$$

$$a_0 = (-1)^n\alpha_1 \cdots \alpha_n \Rightarrow |a_0| = \binom{n}{n} = 1.$$

Como α tiene módulo uno y los conjugados de α^k son los α_i^k, α^k también tiene esa propiedad, con $k \geq 1$. Se tiene entonces que el polinomio mínimo de α^k cumple las mismas condiciones que el polinomio de α, es decir, los coeficientes están acotados, luego existe un número finito de polinomios de este tipo. Obtenemos como conclusión que hay un número finito de elementos en $\mathbb{Q}(\alpha)$ tales que todos sus conjugados tengan módulo uno (pues son raíces de un número finito de polinomios).

Existen por tanto, k, l con $k > l$, tal que $\alpha^k = \alpha^l \Rightarrow \alpha^{k-l} = 1 \Rightarrow \alpha$ es una raíz de la unidad. □

Proposición 1.6.5 *Toda unidad u de $\mathbb{Q}(\zeta)$ se puede escribir de la forma $u = \pm\zeta^k v$ donde v es una unidad positiva real de A.*

Demostración: sea u una unidad de $\mathbb{Q}(\zeta) \Rightarrow$ por lo que hemos visto del anillo de enteros,

$$u = a_0 + a_1\zeta + a_2\zeta^2 + ... + a_{p-2}\zeta^{p-2}$$

con $a_i \in \mathbb{Z}$. El conjugado complejo de u, el cual es una unidad también (porque $uv = 1$ implica que $\bar{u}\bar{v} = 1$), viene dado por

$$\bar{u} = a_0 + a_1\zeta^{-1} + a_2\zeta^{-2} + ... + a_{p-2}\zeta^{-(p-2)}.$$

Entonces $u' = u\bar{u}^{-1}$ es una unidad también. Además, si

$$u^{(k)} = a_0 + a_1\zeta^k + a_2\zeta^{2k} + ... + a_{p-2}\zeta^{k(p-2)}$$

para $k = 1, ..., p-1$ son los conjugados de u, entonces $\overline{u^{(k)}} = \bar{u}^{(k)}$ son los conjugados de $\bar{u}$, por lo que los de u' son $u'^{(k)} = u^{(k)} \cdot \overline{u^{(k)-1}}$. Se tiene pues, que $|u'^{(k)}| = 1$. Entonces el elemento u' es una raíz de la unidad y es de la forma $u' = \pm\zeta^h$ con $0 \leq h \leq p-1$.

Debemos tener el signo positivo. Si no fuera así y $u' = \pm\zeta^h$, entonces $u = -\zeta^h\bar{u}$. Consideramos el anillo $R = A/A(1-\zeta)$ y sea θ:$A \to R$ el homomorfismo canónico. Entonces $\theta(\zeta) = 1$ y por tanto $\theta(\zeta^k) = 1 \ \forall \ k = 1, ..., p-2$ y $\theta(u) = a_0 + a_1 + \cdots + a_{p-2} = \theta(\bar{u})$. Como $u = -\zeta^h\bar{u}$ tenemos que $\theta u = -\theta(\bar{u}) \Rightarrow \theta(2\bar{u}) = 0 \Rightarrow 2\bar{u} \in A(1-\zeta) \Rightarrow (1-\zeta)$ divide a $2\bar{u}$, y como $\bar{u}$ es unidad $\Rightarrow 1-\zeta$ divide a 2. Partiendo de que p es asociado con $(1-\zeta)^{p-1}$ $\Rightarrow p$ divide a $2 \Rightarrow p = 2$, lo que contradice la hipóetesis de que p es un primo impar. Luego $u = \zeta^h\bar{u}$

Sea k tal que $2k = h \pmod{p} \Rightarrow \zeta^h = \zeta^{2k}$ y por tanto

$$\frac{u}{\zeta^k} = \zeta^k\bar{u} = \frac{\bar{u}}{\zeta^{-k}} = \overline{\left(\frac{u}{\zeta^k}\right)}.$$

Elegimos ahora $v = u/\zeta^k = u\zeta^{p-k}$, vemos que v es unidad real positiva y $u = \zeta^k v$. □

Capítulo 2

Aplicación a la ecuación de Fermat

Una vez desarrollada toda la teoría previa necesaria, estamos en disposición de abordar la demostración del último teorema de Fermat en el primer caso que dio Ernst Kummer.

Para ello, necesitaremos definir *los primos regulares* que serán aquellos números primos para los que será válida la demostración, y después daremos una caracterización de tales números.

2.1. Ecuación de Fermat

Definición 2.1.1 Dado un primo p, decimos que es **regular** si el número de clases de $\mathbb{Q}(\zeta)$ denotado por h_p no es divisible por p, donde ζ es un raíz p-ésima de la unidad. En caso contrario se dirá que es **irregular**.

Observación 2.1.2 La importancia de que un primo p sea regular radica en que si la potencia p-ésima de un ideal $\mathfrak{a}$ en $\mathbb{Z}[\zeta]$ es principal, entonces $\mathfrak{a}$ tiene que ser principal. Veamos esto.

Si $\mathfrak{a}^p$ es principal, entonces es trivial en el grupo de clases de $\mathbb{Q}(\zeta)$ (el cociente del grupo de los ideales fraccionarios del anillo de enteros entre el subgrupo de los ideales principales). Como p no divide a h_p y el orden de todo elemento tiene que dividir al orden del grupo, se tiene que $\mathfrak{a}$ es trivial en el grupo de clases y por tanto, $\mathfrak{a}$ es principal.

Nota 2.1.3 El conjugado complejo de α en $\mathbb{Q}(\zeta)$ es $\bar{\alpha}$. Como el conjugado complejo es un automorfismo de este cuerpo, cuyo grupo de Galois sobre $\mathbb{Q}$ es abeliano, $\sigma(\bar{\alpha}) = \overline{\sigma(\alpha)}$ para cualquier α en $\mathbb{Q}(\zeta)$ y para cualquier $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

Teorema 2.1.4 *Para un primo regular $p \geq 3$, la ecuación $x^p + y^p = z^p$ tal que p no divide a x ,y o z, no tiene solución en los enteros positivos.*

Demostración: Supongamos que existe una solución en los enteros positivos para dicha ecuación. Podemos suponer que x, y y z son primos entre ellos pues si dos de ellos tienen un primo como factor común, también es factor del tercero y por tanto se pueden dividir todos los términos por ese número primo. Llegaremos a una contradicción con que p es regular.

En $\mathbb{Z}[\zeta]$, la ecuación de Fermat factoriza como

$$z^p = x^p + y^p = \prod_{j=0}^{p-1}(x + \zeta^j y).$$

Veamos que los factores de la derecha de la igualdad generan ideales relativamente primos. Para $0 \leq j < j' \leq p-1$ y cualquier ideal $\mathfrak{o}$ factor común de $(x + \zeta^j y)$ y $(x + \zeta^{j'} y)$, se tiene que $x + \zeta^j y$ y $x + \zeta^{j'} y$ están en $\mathfrak{o}$, por tanto su diferencia

$$x + \zeta^j y - x - \zeta^{j'} y = y\zeta^j(1 - \zeta^{j'-j}) = vy(1 - \zeta)$$

donde v es una unidad, también estará en $\mathfrak{o}$ (hemos utilizado que los elementos $1 - \zeta^{j'-j}$ y $1 - \zeta$ son asociados, y cómo son las unidades). Como $p = u(1-\zeta)^{p-1}$ con u una unidad, tenemos que $y(1-\zeta)$ divide a yp, luego $\mathfrak{o}|(yp)$. Además, a partir de la factorización de la ecuación de Fermat, sabemos que $\mathfrak{o}$ divide a $(z)^p$. Partiendo de que yp y z^p son enteros relativamente primos, tenemos que $\mathfrak{o}$ es el ideal unidad, por lo que los ideales $(x + \zeta^j y)$ son relativamente primos.

El producto de los ideales generados por estos elementos es la potencia p-ésima $(z)^p$, lo que implica que cada factor es una potencia p-ésima. Tomando $j = 1$:

$$(x + \zeta y) = \mathfrak{a}^p$$

para algún ideal $\mathfrak{a}$. Así, $\mathfrak{a}^p$ es principal, luego es trivial en el grupo de clases de $\mathbb{Q}(\zeta)$. Como p es regular, sabemos que $\mathfrak{a}$ es trivial en el grupo de clases, lo

que implica que es un ideal principal. Tenemos pues, que $\mathfrak{a} = (t)$ con $t \in \mathbb{Z}[\zeta]$. Así,

$$x + \zeta y = ut^p$$

para alguna unidad u en $\mathbb{Z}[\zeta]$.

Por (1.6.1), podemos escribir

$$t = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2},$$

con $b_j \in \mathbb{Z}$. Observemos ahora que al calcular t^p, todos los coeficientes que quedan multiplicados por términos de la forma $\binom{p}{i}, i < p$ son múltiplos de p y por tanto son cero módulo $p\mathbb{Z}[\zeta]$. Luego los únicos términos no nulos son los $b_i^p\zeta^{i\cdot p}$, que al tomar módulo $p\mathbb{Z}[\zeta]$ quedan b_i por el pequeño teorema de Fermat. Obtenemos entonces

$$t^p \equiv b_0 + b_1 + \cdots + b_{p-2} \quad \text{mód } p\mathbb{Z}[\zeta].$$

Como los $b_i \in \mathbb{Z}$ tenemos que

$$\bar{t} = b_0 + b_1\bar{\zeta} + \cdots + b_{p-2}\overline{\zeta^{p-2}},$$

lo que conlleva que $t^p \equiv \bar{t}^p$ mód $p\mathbb{Z}[\zeta]$ pues al elevar a p y tomar módulo $p\mathbb{Z}[\zeta]$ sucede lo mismo que antes. Por la nota (2.1.3) sabemos que $\sigma(\bar{u}) = \overline{\sigma(u)}$ para todo $\sigma \in Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$, luego $u/\bar{u}$ y todos sus conjugados tienen valor absoluto uno. Aplicando ahora (1.6.4), tenemos que $u/\bar{u}$ es una raíz de la unidad y por tanto $u/\bar{u} = \pm\zeta^j$ para algún j entre 0 y $p-1$. Si $u/\bar{u} = \zeta^j$, entonces

$$x + \zeta y = ut^p$$

$$x + \zeta y = \zeta^j\bar{u}t^p$$

$$x + \zeta y \equiv \zeta^j\bar{u}\bar{t}^p \quad \text{mód } p\mathbb{Z}[\zeta]$$

$$x + \zeta y \equiv \zeta^j(x + \bar{\zeta}y) \quad \text{mód } p\mathbb{Z}[\zeta].$$

Así,

$$u/\bar{u} = \zeta^j \Rightarrow x + y\zeta - y\zeta^{j-1} - x\zeta^j \equiv 0 \quad \text{mód } p\mathbb{Z}[\zeta]. \tag{2.1.1}$$

De forma similar,

$$u/\bar{u} = -\zeta^j \Rightarrow x + y\zeta + y\zeta^{j-1} + x\zeta^j \equiv 0 \quad \text{mód } p\mathbb{Z}[\zeta]. \tag{2.1.2}$$

Vamos a comprobar ahora que ninguna de estas congruencias puede darse cuando $0 \leq j \leq p-1$ y x,y enteros primos con p.

Supongamos que tenemos

$$a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \equiv 0 \quad \text{mód } p\mathbb{Z}[\zeta],$$

entonces

$$a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \in p\mathbb{Z}[\zeta].$$

Se tiene pues, que

$$a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} = p\alpha$$

con $\alpha \in \mathbb{Z}[\zeta]$. Por (1.6.1) podemos escribir

$$\alpha = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2}.$$

Así, queda entonces

$$a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} = pb_0 + pb_1\zeta + \cdots + pb_{p-2}\zeta^{p-2},$$

lo que implica que

$$a_i \equiv 0 \quad \text{mód } p, \forall i = 0, ..., p-2.$$

En nuestro caso los coeficientes asociados a los elementos $1, \zeta, \zeta^2, ..., \zeta^{p-2}$ son $1, \pm x, \pm y$ y sabemos que x, y no son divisibles por p, por lo que tenemos que no se pueden dar ninguna de las dos congruencias (2.1.1) y (2.1.2) para $3 \leq j \leq p-2$.

El resto de la prueba consiste en comprobar los casos $j = 0, 1, 2, p-1$.

Veamos que podemos suponer $p \geq 5$ ya que la ecuación $x^3 + y^3 = z^3$ no tiene soluciones en los enteros primos con 3. Como x es primo con 3, tenemos que $x \equiv \pm 1, \pm 2, \pm 4 \mod 9$. Esto nos lleva a que $x^3 \equiv \pm 1 \mod 9$ ya que $2^3 = 8 \equiv -1 \mod 9$ y $4^3 = 4 \cdot 16 \equiv 1 \mod 9$. Lógicamente para y y z se tienen las mismas conclusiones ya que también son primos con 3. Queda entonces que $x^3 + y^3 \equiv 0, \pm 2 \mod 9$ y $z^3 \equiv \pm 1 \mod 9$, lo que demuestra que no existe solución.

Una vez que podemos suponer $p \geq 5$, veamos primero el caso $j = p-1$. Como

$$1 + \zeta + \cdots + \zeta^{p-1} = 0$$

(polinomio mínimo), tenemos que

$$1 - \zeta^{p-1} = 1 + (1 + \zeta + \cdots + \zeta^{p-2}).$$

Por tanto, el lado izquierdo de la congruencia (2.1.1) quedaría

$$x(1 - \zeta^{p-1}) + y(\zeta - \zeta^{p-2}) = 2x + (x + y)\zeta + x(\zeta^2 + \cdots + \zeta^{p-3}) + (x - y)\zeta^{p-2},$$

pero todos los coeficientes tienen que ser divisibles por p, en particular $2x$. Como sabemos que p no divide a x, estamos de nuevo ante una congruencia que no se puede dar. Para la congruencia (2.1.2) tenemos una contradicción similar pues el lado izquierdo quedaría

$$x(1 + \zeta^{p-1}) + y(\zeta + \zeta^{p-2}) = (y - x)\zeta - x(\zeta^2 + \cdots + \zeta^{p-3}) + (y - x)\zeta^{p-2}.$$

Consideremos ahora el caso $j = 0$. En este caso, la congruencia (2.1.1) queda de la forma

$$y(\zeta - \zeta^{-1}) \equiv 0 \mod p\mathbb{Z}[\zeta].$$

Como y no es divisible por p, podemos dividir por y y obtenemos

$$\zeta - \zeta^{-1} \equiv 0 \mod p \Rightarrow \zeta^2 - 1 \equiv 0 \mod p,$$

lo cual contradice la independencia lineal de 1 y $\zeta^2 \mod p$ ya que $p \geq 5$. Similarmente, la congruencia (2.1.2) para $j = 0$ implica que

$$2x\zeta + y\zeta + y \equiv 0 \mod p$$

llegando de nuevo a una contradicción.

Para el caso $j = 2$, la congruencia (2.1.1) queda

$$x - x\zeta^2 \equiv 0 \mod p\mathbb{Z}[\zeta],$$

mientras que (2.1.2) sería

$$x + 2y\zeta + x\zeta^2.$$

Es fácil observar que en ambos casos nos encontramos con sendas contradicciones.

Por último veamos qué ocurre con $j = 1$. La congruencia (2.1.2) implica que

$$(x + y)(1 + \zeta) \equiv 0 \mod p$$

y por tanto,

$$x + y \equiv 0 \mod p\mathbb{Z}$$

pues sabemos que $1 - \zeta^j$ y $1 - \zeta$ son asociados lo que implica que $1 - \zeta^2 = (1-\zeta)(1+\zeta) = v(1-\zeta)$ donde v es una unidad, es decir, $1+\zeta$ es una unidad. Así, tendríamos que

$$z^p = x^p + y^p \equiv (x + y)^p \equiv 0 \mod p,$$

luego p dividiría a z, algo que hemos supuesto que no pasa. Queda entonces la congruencia (2.1.1) en el caso $j = 1$:

$$x(1 - \zeta) + y(1 - \zeta) \equiv 0 \mod p.$$

Escribiendo $p = u(1 - \zeta)^{p-1}$, tendríamos que

$$x \equiv y, \mod (1 - \zeta)^{p-2}.$$

Como $p - 2 \geq 1$ (pues $p \geq 5$) y $x, y \in \mathbb{Z}$, esto fuerza que $x \equiv y \mod p\mathbb{Z}$. Recorriendo la demostración análogamente con y y $-z$ intercambiados, obtenemos que $x \equiv -z \mod p\mathbb{Z}$, llegando a que

$$0 = x^p + y^p - z^p \equiv 3x^p \mod p.$$

Como $p \neq 3$ y x es primo con p, tenemos una contradicción. □

2.2. Números de Bernoulli

Nuestro interés en los números de Bernouilli se debe a que nos proporcionan una caracterización de los números primos regulares para los cuales hemos demsotrado la ecuación de Fermat.

Definición 2.2.1 Los **números de Bernoulli** se definen a partir de la siguiente serie:

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$$

donde los B_n denotan los números de Bernouilli.

Proposición 2.2.2 *Los números de Bernoulli son números racionales.* $B_0 = 1$, $B_1 = -\frac{1}{2}$ *y para todo* $k \geq 1$ *se tiene la siguiente relación de recurrencia:*

$$\binom{k+1}{1} B_k + \binom{k+1}{2} B_{k-1} + \cdots + B_1 + 1 = 0.$$

Demostración:

$$x = (e^x - 1)\left(\frac{x}{e^x - 1}\right) = \left(\sum_{n=1}^{\infty} \frac{x^n}{n!}\right)\left(\sum_{n=0}^{\infty} \frac{B_n}{n!} B_n\right)$$

$$= (x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 + \cdots)(B_0 + \frac{B_1}{1!}x + \frac{B_2}{2!}x^2 + \frac{B_3}{3!}x^3 \cdots).$$

A partir de esta igualdad sabemos que en el producto de la derecha se tienen que anular todos los coeficientes de las potencias de x excepto el de x, luego en primer lugar obtenemos que $B_0 = 1$. Para $k \geq 1$ queda

$$B_1 + \frac{1}{2} = 0,$$

$$\frac{B_2}{2!} + \frac{B_1}{1!2!} + \frac{B_0}{3!} = 0,$$

$$\frac{B_3}{3!} + \frac{B_2}{2!2!} + \frac{B_1}{1!3!} + \frac{B_0}{4!} = 0,$$

$$\vdots$$

$$\frac{B_k}{k!} + \frac{B_{k-1}}{2!(k-1)!} + \frac{B_{k-2}}{3!(k-2)!} + \cdots + \frac{B_1}{k!} + \frac{1}{(k+1)!}.$$

Si multiplicamos la expresión resultante por $(k+1)!$, obtenemos

$$\binom{k+1}{1} B_k + \binom{k+1}{2} B_{k-1} + \cdots + B_1 + 1 = 0.$$

Ahora por inducción en k podemos comprobar fácilmente que los B_k son números racionales. Ya sabemos que $B_1 = -\frac{1}{2}$ es racional. Spongamos ahora que hasta B_{k-1} son racionales, entonces tendríamos

$$(k+1)B_k + q = 0 \Rightarrow B_k = -\frac{q}{k+1}$$

donde q es un número racional por hipótesis. Por tanto, B_k es racional al ser cociente de dos números racionales. □

Proposición 2.2.3 *Para todo $k \geq 3$ impar se tiene que $B_k = 0$.*

Demostración: Consideremos la serie

$$S(x) = \frac{x}{2} + \frac{x}{e^x - 1} = \frac{x}{2} + \sum_{k=0}^{\infty} \frac{B_k}{k!} x^k = 1 + \sum_{k=2}^{\infty} \frac{B_k}{k!} x^k.$$

Al cambiar x por $-x$ queda

$$S(x) = -\frac{x}{2} - \frac{x}{e^{-x} - 1} = \frac{xe^x}{e^x - 1} - \frac{x}{2}.$$

Restamos ahora ambas expresiones

$$S(-x) - S(x) = \frac{x}{e^x - 1}(e^x - 1) - \frac{2x}{2} = 0.$$

Si tomamos los k impares

$$S(-x) - S(x) = \sum_{k=2n+1, n\geq 1}^{\infty} \frac{B_k}{k!}(-x)^k - \sum_{k=2n+1, n\geq 1}^{\infty} \frac{B_k}{k!} x^k =$$

$$= -2 \sum_{k=2n+1, n\geq 1}^{\infty} \frac{B_k}{k!} x^k = 0,$$

lo que demuestra que $B_k = 0$ para todo $k \geq 3$ impar. □

Los primeros números de Bernoulli son:

$$B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_4 = -\frac{1}{30}, B_6 = \frac{1}{42}, B_8 = -\frac{1}{30}, B_{10} = \frac{5}{66}, B_{12} = -\frac{691}{2730}.$$

Teorema 2.2.4 *[1, 19.1]*

Para un número primo $p > 2$, las siguientes condiciones son equivalentes:
(1) p es un primo regular;
(2) p no divide los numeradores de los números de Bernoulli:

$$B_2, B_4, ..., B_{p-3}$$

.

Nota 2.2.5 En la práctica, es esta caracterización la que se utiliza para comprobar si un primo es regular o no. Por ejemplo, a partir de que $B_{12} = -\frac{691}{2730}$, podemos deducir que 691 es un primo irregular utilizando dicha caracterización.

No ha sido probado que existan infinitos primos regulares. Por otro lado, las evidencias numéricas indican que aproximadamente el sesenta por ciento de los primos deberían ser regulares, es decir, no solo que hay infinitos primos regulares sino que son mucho más numerosos que los primos irregulares. Sin embargo, si ha sido probado que existen infintos primos irregulares[2].

Los primeros primos irregulares son:

$$37, 59, 67, 101, 103, 131, 149.$$

Bibliografía

[1] Paulo Ribenboim. *Classical Theory of Algebraic Numbers*. Springer-Verlag, New York, 2001.

[2] James S.Milne. *Algebraic Number Theory*. September 28, 2008. *http://www.jmilne.org/math/CourseNotes/ANT301.pdf*

[3] Keith Conrad. *Fermat's Last Theorem for Regular Primes*. *http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/fltreg.pdf*