El anillo de los enteros algebraicos y dominios de Dedekind

Trabajo de Grado

Autor:

Jorge Eliécer Gómez Ríos

Director:

Dr. Héctor Edonis Pinedo Tapia

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Matemáticas
Bucaramanga, junio de 2015

Enteros algebraicos

La teoría de los números algebraicos se desarrolló en gran parte gracias al Último Teorema de Fermat; éste establece que la ecuación

$$X^n + Y^n = Z^n$$

no tiene soluciones enteras no triviales cuando $n > 2$. El teorema fue conjeturado por Pierre de Fermat en 1637, pero fue demostrado hasta 1995 por Andrew Wiles. Varios matemáticos importantes del siglo XIX, entusiasmados por encontrar la prueba de este teorema (que para entonces era una conjetura), contribuyeron para que la teoría algebraica de números se consolidara como una rama importante de las matemáticas.

En esta presentación se darán las definiciones básicas y se probarán algunos resultados de la teoría de los enteros algebraicos que servirán como herramienta para solucionar algunos problemas que involucran ecuaciones Diofánticas.

Para los detalles de las demostraciones y un amplio estudio del tema, se recomienda consultar la monografía presentada como evidencia del trabajo de grado.

Enteros algebraicos

Definición

Sea $\mathbb{L}$ un cuerpo y R, B anillos tales que $R \subseteq B \subseteq \mathbb{L}$. Diremos que $\alpha \in B$ es un ***entero*** *sobre R si existe $f(X) \in R[X]$ mónico tal que $f(\alpha) = 0$.*
El conjunto

$$I_B(R) := \{\alpha \in B : \text{existe } f(X) \in R[X] \text{ mónico tal que } f(\alpha) = 0\};$$

formado por los elementos de B que son enteros sobre R es llamado la ***clausura entera de R en B****. Cuando $B = \mathbb{L}$ y $R = \mathbb{Z}$, escribiremos simplemente $I_{\mathbb{L}}$, en particular los elementos de $I_{\mathbb{C}}$ son llamados* ***enteros algebraicos****.*

Objetivos

- Probar que $I_B(R)$ es un subanillo de B que contiene a R.
- Probar que el anillo $I_B(R)$ es un dominio de Dedekind.
- Estudiar algunos casos particulares e interesantes, como $R = \mathbb{Z}[i]$, enteros de Gauss, o cuando B es un cuerpo cuadrático.

Enteros algebraicos

Nuestro primer objetivo es probar que los elementos enteros sobre un dominio entero forman un anillo, y para ello usaremos la siguiente caracterización de la integridad:

Teorema

Sean $R \subseteq B \subseteq \mathbb{L}$ con $\mathbb{L}$ un cuerpo, R y B anillos y $\alpha \in B$. Las siguientes proposiciones son equivalentes:

1. *α es entero sobre R.*
2. *$R[\alpha] := \{f(\alpha) | f(X) \in R[X]\}$ es un R-módulo finitamente generado.*
3. *Existe un $R-$módulo finitamente generado M tal que $M \subseteq B$ y $\alpha M \subseteq M$.*

Corolario

Si $\alpha_1, \alpha_2, \cdots, \alpha_m$ son enteros sobre R, entonces $R[\alpha_1, \alpha_2, \cdots, \alpha_m]$ es un $R-$módulo finitamente generado.

Corolario

$I_B(R)$ es un subanillo de B que contiene a R.

Demostración.

$I_B(R)$ es no vacío, ya que R es no vacío y si $a \in R$, entonces $f(X) = X - a \in R[X]$ es un polinomio mónico tal que $f(a) = 0$, esto es $a \in I_B(R)$, en particular $R \subseteq I_B(R)$. Probemos que $I_B(R)$ es cerrado bajo la suma y el producto. Sean $\alpha, \beta \in I_B(R)$, entonces $R[\alpha, \beta]$ es un $R-$módulo finitamente generado por el corolario anterior y tenemos que $\alpha - \beta,\ \alpha\beta \in R[\alpha, \beta]$. Luego,

$$(\alpha - \beta)R[\alpha, \beta] \subseteq R[\alpha, \beta] \text{ y}$$
$$(\alpha\beta)R[\alpha, \beta] \subseteq R[\alpha, \beta]$$

Así, por 3 del Teorema 1 tenemos que $\alpha - \beta$ y $\alpha\beta$ son enteros sobre R, es decir $\alpha - \beta,\ \alpha\beta \in I_B(R)$. □

Enteros algebraicos

Definición

Sean $\mathbb{L}$ un cuerpo y R, B anillos con $R \subseteq B \subseteq \mathbb{L}$.

- *Si $I_B(R) = R$, diremos que R es **integralmente cerrado en** B.*
- *Si R es integralmente cerrado en su cuerpo de fracciones decimos que R es **integralmente cerrado**.*
- *Si $I_B(R) = B$, diremos que B es **entero sobre** R.*

Ejemplo

- Toda extensión algebraica de un cuerpo $\mathbb{K}$ es entera sobre $\mathbb{K}$.
- Todo dominio de factorización única es integralmente cerrado. En consecuencia $I_{\mathbb{Q}} = \mathbb{Z}$.

Traza y Norma

Definición

Sean $\mathbb{L}|\mathbb{K}$ una extensión finita y separable de cuerpos, con $[\mathbb{L}:\mathbb{K}]=n$; $\alpha\in\mathbb{L}$ y $\sigma_1,\sigma_2,\cdots,\sigma_n$ son los $\mathbb{K}-$homomorfismos de $\mathbb{L}$ en $\overline{\mathbb{K}}$. Definimos la ***traza*** *y la* ***norma*** *de α relación a $\mathbb{L}|\mathbb{K}$ como:*

$$N_{\mathbb{L}|\mathbb{K}}(\alpha):=\prod_{i=1}^{n}\sigma_i(\alpha),$$

$$T_{\mathbb{L}|\mathbb{K}}(\alpha):=\sum_{i=1}^{n}\sigma_i(\alpha).$$

Observación: Para todos $\alpha,\beta\in\mathbb{L}$ se cumple que:

$$N_{\mathbb{L}|\mathbb{K}}(\alpha\beta)=N_{\mathbb{L}|\mathbb{K}}(\alpha)N_{\mathbb{L}|\mathbb{K}}(\beta).$$

Enteros algebraicos de cuerpos cuadráticos

Definición

Un ***cuerpo cuadrático*** *es un subcuerpo* $\mathbb{L}$ *de* $\mathbb{C}$ *tal que* $[\mathbb{L} : \mathbb{Q}] = 2$.

Proposición

Sea $\mathcal{D} = \{d \in \mathbb{Z} : d \notin \{0, 1\}$ y d es libre de cuadrados$\}$. La aplicación definida por $d \longmapsto \mathbb{Q}\left(\sqrt{d}\right)$ es una biyección de $\mathcal{D}$ sobre el conjunto de los cuerpos cuadráticos.

Observación:
Si $\mathbb{L} = \mathbb{Q}\left(\sqrt{d}\right)$ es un cuerpo cuadrático, entonces los dos $\mathbb{Q}-$homomorfismos de $\mathbb{L}$ en $\mathbb{C}$, son precisamente $\sigma_1(x) = x$ y $\sigma_2(x) = \overline{x}$, donde $\overline{x}$ denota el conjugado de x; es decir, para $x = a + b\sqrt{d} \in \mathbb{L}$, $\sigma_2(x) = a - b\sqrt{d}$. Así, si $\alpha \in \mathbb{L}$, entonces $\alpha = m + n\sqrt{d}$, con $m, n \in \mathbb{Q}$ y $d \in \mathcal{D}$, por lo tanto:

$$N_{\mathbb{L}|\mathbb{Q}}(\alpha) = \prod_{i=1}^{2} \sigma_i(\alpha) = \left(m + n\sqrt{d}\right)\left(m - n\sqrt{d}\right) = m^2 - n^2 d.$$

Enteros algebraicos de cuerpos cuadráticos

El siguiente teorema caracteriza los enteros algebraicos de un cuerpo cuadrático.

Teorema

Si $\mathbb{L} = \mathbb{Q}\left(\sqrt{d}\right)$, *donde* d *es un entero libre de cuadrados y*

$$\delta = \begin{cases} \sqrt{d}, & \text{si } d \equiv 2, 3 \pmod 4, \\ \dfrac{1+\sqrt{d}}{2}, & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

Entonces, $\{1, \delta\}$ *es una base del* $\mathbb{Z}-$*módulo* $I_{\mathbb{L}}$.

Enteros algebraicos de cuerpos cuadráticos

Ejemplo

Sea $\mathbb{L} = \mathbb{Q}\left(\sqrt{-5}\right)$. El domino $I_{\mathbb{L}}$ no es DFU. De hecho como $-5 \equiv 3 \pmod 4$, entonces $I_{\mathbb{L}} = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Observe que:

$$\left(1 + 2\sqrt{-5}\right)\left(1 - 2\sqrt{-5}\right) = 3 \cdot 7.$$

Basta mostrar que los factores $1 \pm 2\sqrt{-5}$, 3 y 7 son irreducibles en $I_{\mathbb{L}}$. Como ellos tienen norma 21, 21, 9 y 49 respectivamente, tenemos que si $1 + 2\sqrt{-5}$ fuese reducible, existen $\alpha, \beta \in I_{\mathbb{L}} \setminus U(I_{\mathbb{L}})$ tales que $1 + 2\sqrt{-5} = \alpha\beta$, entonces tendríamos que $21 = N_{\mathbb{L}|\mathbb{Q}}(\alpha)N_{\mathbb{L}|\mathbb{Q}}(\beta)$, luego $N_{\mathbb{L}|\mathbb{Q}}(\alpha) \in \{3, -3, 7, -7\}$. Pero esto es imposible, pues $N_{\mathbb{L}|\mathbb{Q}}\left(a + b\sqrt{-5}\right) = a^2 + b^2 5 \notin \{3, -3, 7, -7\}$ para cualesquiera $a, b \in \mathbb{Z}$. La irreducibilidad de $1 - 2\sqrt{-5}$, 3 y 7 se prueba análogamente.

Note que, aunque $\mathbb{Z}$ es un DFU, esto no implica que el anillo de enteros algebraicos de un cuerpo numérico tenga factorización única. A pesar de esto, podemos encontrar ejemplos de cuerpos numéricos $\mathbb{L}$, tales que $I_{\mathbb{L}}$ sea DFU, pero antes necesitamos recordar la noción de dominio Euclidiano.

Enteros algebraicos de cuerpos cuadráticos

Definición

Un dominio integral R es un ***dominio Euclidiano****, si existe una función* $\delta : R \setminus \{0\} \longrightarrow \mathbb{N}$ *con las siguientes propiedades:*

i) *Si* $a, b \in R \setminus \{0\}$, *entonces* $\delta(a) \leq \delta(ab)$.

ii) *Si* $a, b \in R$ *y* $b \neq 0$, *entonces existen* $q, r \in R$ *tales que* $a = qb + r$ *y* $r = 0$ *ó* $\delta(r) < \delta(b)$.

Proposición

Todo dominio Euclidiano es un DIP y por lo tanto un DFU.

Para sacar provecho a este resultado, debemos encontrar cuerpos para los cuales el anillo de enteros sea Euclidiano. Estudiaremos esta propiedad en el anillo $I_{\mathbb{L}}$ de los enteros algebraicos de un cuerpo cuadrático $\mathbb{L} = \mathbb{Q}\left(\sqrt{d}\right)$.

Enteros algebraicos de cuerpos cuadráticos

Un candidato natural a ser la función δ es la norma absoluta, restricta a $I_{\mathbb{L}} \setminus \{0\}$, esto es, la función definida por:

$$\begin{aligned} \delta : I_{\mathbb{L}} \setminus \{0\} &\longrightarrow \mathbb{N} \\ \alpha &\longmapsto \left|N_{\mathbb{L}|\mathbb{Q}}(\alpha)\right|. \end{aligned} \tag{1}$$

Claramente esta función cumple la propiedad $i)$ de la definición de dominio Euclidiano, pues para todo $\alpha, \beta \in I_{\mathbb{L}} \setminus \{0\}$,

$$\left|N_{\mathbb{L}|\mathbb{Q}}(\alpha\beta)\right| = \left|N_{\mathbb{L}|\mathbb{Q}}(\alpha)N_{\mathbb{L}|\mathbb{Q}}(\beta)\right| = \left|N_{\mathbb{L}|\mathbb{Q}}(\alpha)\right|\left|N_{\mathbb{L}|\mathbb{Q}}(\beta)\right| \geq \left|N_{\mathbb{L}|\mathbb{Q}}(\alpha)\right|.$$

La propiedad $ii)$ solo se cumple en ciertos casos, como veremos a continuación.

Ejemplo

El ***anillo de los enteros Gaussianos*** $\mathbb{Z}[i]$ es precisamente el anillo $I_{\mathbb{L}}$ de los enteros algebraicos del ***cuerpo de los números de Gauss*** $\mathbb{L} = \mathbb{Q}(i)$, donde $i = \sqrt{-1}$, es un dominio Euclidiano en relación a la norma $N_{\mathbb{Q}(i)|\mathbb{Q}}(\alpha)$.

Enteros algebraicos de cuerpos cuadráticos

La Proposición 2 y el ejemplo anterior prueban que el dominio $\mathbb{Z}[i]$ de los enteros Gaussianos es un dominio de factorización única. De hecho, para los cuerpos cuadráticos tenemos el siguiente resultado.

Teorema

Sea $d \in \mathcal{D}$.

- *Para* $d < 0$, $I_{\mathbb{Q}(\sqrt{d})}$ *es Euclidiano con relación a la norma, si y solo si,*

$$d \in \{-1,\ -2,\ -3,\ -7,\ -11\}\,.$$

- *Si* $d < -11$, *entonces* $I_{\mathbb{Q}(\sqrt{d})}$ *no es Euclidiano.*
- *Para* $d > 0$, $I_{\mathbb{Q}(\sqrt{d})}$ *es Euclidiano en relación a la norma absoluta, si y solo si,*

$$d \in \{2,\ 3,\ 5,\ 6,\ 7,\ 11,\ 13,\ 17,\ 19,\ 21,\ 29,\ 33,\ 37,\ 41,\ 57,\ 73\}\,.$$

El lector interesado en los detalles de la demostración, puede consultar [6] y [2].

Enteros algebraicos de cuerpos cuadráticos

Sin embargo, no podemos afirmar que para los $d \in \mathcal{D}$ positivos que no están en esta lista $I_{\mathbb{Q}(\sqrt{d})}$ no sea un dominio Euclidiano con alguna función δ diferente a la norma absoluta. Por ejemplo, se puede verificar que para $d = 69$, el anillo $I_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}\left[\frac{1+\sqrt{69}}{2}\right]$ es un dominio Euclidiano con respecto a la función

$$\delta(a+b\omega) = \begin{cases} \left|a^2+ab-17b^2\right|, & \text{si } (a,b) \neq (10,3), \\ 26, & \text{si } (a,b) = (10,3). \end{cases}$$

Donde $\omega = \frac{1+\sqrt{69}}{2}$*

Más aún, el número 26 puede ser reemplazado por cualquier entero mayor que 26, por lo que $\mathbb{Z}\left[\frac{1+\sqrt{69}}{2}\right]$ es un dominio Euclidiano con respecto a infinitas funciones distintas.

*D. A. Clark. *A quadratic field which is Euclidean but not norm-Euclidean*. Manuscripta Mathematica 83 (1994) 327-330.

Enteros algebraicos de cuerpos cuadráticos

Sabemos que para $I_{\mathbb{L}}$ ser un domino de factorización única es suficiente, más no necesario ser un dominio Euclidiano. De hecho, $\{-19,\ -43,\ -67,\ -163\}$ es el conjunto de los $d \in \mathcal{D}$ negativos tales que $I_{\mathbb{Q}(\sqrt{d})}$ es DFU, pero no Euclidiano ([1], Teorema 5.1). Existen también muchos $d \in \mathcal{D}$ positivos con esta propiedad, pero aún es un problema abierto determinar la existencia de infinitos números positivos $d \in \mathcal{D}$ tales que $I_{\mathbb{Q}(\sqrt{d})}$ es DFU (*Conjetura de Gauss*)

Aplicaciones de la factorización única

La factorización única del anillo de los enteros algebraicos de algunos cuerpos cuadráticos es una herramienta muy útil para resolver problemas de Teoría de Números, por ejemplo:

Con la factorización única del anillo de los enteros Gaussianos se prueban los siguientes dos teoremas.

Teorema

La únicas soluciones enteras de la ecuación

$$X^2 + 4 = Z^3,$$

son $(X, Z) = (\pm 11, 5) \quad o \quad (X, Z) = (\pm 2, 2).$

Teorema

(Fermat) *Si* p *es un entero primo de la forma* $4n + 1$, *existen* $a, b \in \mathbb{Z}$ *tales que*

$$p = a^2 + b^2.$$

Aplicaciones de la factorización única

Volviendo al Último Teorema de Fermat, se cree que el primer matemático que consiguió avanzar en su demostración fue el propio Pierre de Fermat, quien demostró el caso $n = 4$. Partiendo de éste, se deduce si p es un primo impar el Último Teorema de Fermat equivale a la no existencia de soluciones enteras no triviales de la ecuación

$$X^p + Y^p = Z^p.$$

En la prueba para $p = 3$, Euler consideró la factorización

$$X^3 + Y^3 = (X + Y)\left(X^2 - XY + Y^2\right),$$

mientras Direchlet y Legendre en sus pruebas para $p = 5$ consideraron

$$X^5 + Y^5 = (X + Y)\left(X^4 - X^3Y + X^2Y^2 - XY^3 + Y^4\right).$$

La estructura de las dos demostraciones es similar, se trata de determinar cuándo los factores son primos relativos, en tal caso argumentar que si el producto es un cubo o una potencia quinta, lo mismo le ha de suceder a cada factor y después analizar las implicaciones de este hecho. Sin embargo, es evidente que la complejidad del segundo factor aumenta a medida que p aumenta lo que hace que los casos de orden superior se vuelvan intratables.

Aplicaciones de la factorización única

En este contexto Lamé, dió un pasó adelante considerando el anillo de los enteros ciclotómicos

$$\mathbb{Z}[\omega] := \left\{ a_{p-1}\omega^{p-1} + \cdots + a_1\omega + a_0 : a_i \in \mathbb{Z}, \text{ para } 0 \leq i \leq p-1 \right\},$$

donde ω es una raíz $p-$ésima primitiva de la unidad. En efecto, sustituyendo X por X/Y y multplicando por $-Y^p$ en

$$X^p + 1 = (X-1)(X-\omega)\cdots(X-\omega^{p-1}),$$

obtenemos la siguiente factorización en $\mathbb{Z}[\omega]$:

$$X^p + Y^p = (X+Y)(X+\omega Y)\cdots(X+\omega^{p-1}Y).$$

Lamé conjeturó que si $\mathbb{Z}[\omega]$ tuviera factorización única sería posible generalizar los argumentos de los casos que hemos comentado para obtener una prueba completa del teorema de Fermat, con la ventaja de trabajar con factores lineales. Más adelante, Kummer descubrió que los anillos de enteros ciclotómicos no siempre tienen factorización única, pero que la conjetura de Lamé era correcta.

Aplicaciones de la factorización única

Buscando contraejemplos de factorización única en los enteros ciclótomicos; Kummer desarrolló una teoría que le permitía establecer un tipo de factorización única en estos anillos, para ello debió introducir la noción de divisores *'ideales'*. Fue Dedekind quien a finales del siglo XIX formalizó la teoría de Kummer identificando sus divisores ideales con los ideales en el sentido usual de la teoría de anillos y probando que los resultados de Kummer son válidos en una clase muy general de anillos que estudiaremos a continuación

Dominios de Dedekind

En general, el anillo de los enteros de un cuerpo numérico no es un DFU. Sin embargo se tiene el resultado, un poco más débil, de que en éste anillo todo ideal propio se factoriza en forma única como producto de ideales primos. Para probar lo anterior, comenzamos introduciendo los conceptos de anillo noetheriano y dominio de Dedekind.

Definición

Un anillo conmutativo R se dice ***noetheriano*** *si satisface la condición de cadena ascendente (CCA) para ideales, esto es, si dada una cadena* $\mathfrak{i}_1 \subseteq \mathfrak{i}_2 \subseteq \ldots \subseteq \mathfrak{i}_m \subseteq \ldots$ *de ideales de R, existe $n \in \mathbb{N}$ tal que $\mathfrak{i}_n = \mathfrak{i}_t$, para todo $t \geq n$.*

Ejemplo

El anillo de los números enteros $\mathbb{Z}$ es noetheriano.

Dominios de Dedekind

El nombre de anillo noetheriano se debe fundamentalmente al artículo *'Idealtheorie...'* [**] de Emmy Noether, allí aparecen por primera vez los conceptos modernos de anillo, ideal y módulo sobre un anillo, pero sin duda, el concepto que más se destaca en este artículo es el de la condición de cadena ascendente para ideales. Esta condición había sido previamente estudiada por Dedekind en 1894 y Lasker en 1905, pero la principal contribución de Noether fue definirla en un contexto abstracto y mostrar su importancia y naturalidad.

El siguiente teorema nos muestra una caracterización de anillos noetherianos.

[**] E. Noether, *Idealtheorie in Ringbereichen, Math. Annalen 83* (1921), 24-66.

Dominios de Dedekind

Teorema

Sea R un anillo. Son equivalentes:

1. *R es noetheriano.*
2. *R verifica la condición de maximalidad: Sea $\mathcal{F}$ una familia no vacía de ideales de R, entonces $\mathcal{F}$ tiene un elemento maximal.*
3. *Todo ideal de R es un R-módulo finitamente generado.*

Ejemplo

Sea $\mathbb{F}$ un cuerpo, entonces los únicos ideales de $\mathbb{F}$ son $\mathbf{0}$ y $\mathbb{F}$, que claramente son $\mathbb{F}-$módulos finitamente generados por 0 y 1 respectivamente, luego $\mathbb{F}$ es noetheriano. En consecuencia $\mathbb{L} := \mathbb{F}_1 \times \mathbb{F}_2 \times \cdots \times \mathbb{F}_n$, donde los $\mathbb{F}_i$ son cuerpos es noetheriano.

Se puede mostrar que si un anillo R es noetheriano, $R[X]$ también es noetheriano, de donde, entonces el anillo de polinomios $R[X_1, \cdots, X_n]$ es noetheriano. Este resultado se conoce como el *Teorema de la base de Hilbert*.

Dominios de Dedekind

Definición

Un dominio R es de Dedekind si:

$i)$ *Es noetheriano.*

$ii)$ *Es integralmente cerrado.*

$iii)$ *Todo ideal primo no nulo es maximal.*

Ejemplo

Todo DIP es un dominio de Dedekind.

A continuación, probaremos un teorema que es clave para el desarrollo de los objetivos propuestos en este trabajo.

Teorema

Sean R un dominio de Dedekind, $\mathbb{K} = Q(R)$, $\mathbb{L}$ una extensión finita y separable de $\mathbb{K}$ y $A = I_{\mathbb{L}}(R)$. Entonces A es un dominio de Dedekind.

Dominios de Dedekind

Para su demostración, necesitamos algunos resultados previos

Lema

Sea R un dominio y $\mathbb{L}$ una extensión de $Q(R)$, entonces $Q(I_{\mathbb{L}}(R)) = \mathbb{L}$, si y solamente si, $\mathbb{L}$ es algebraica sobre $Q(R)$.

Lema

Sean B y S subanillos de un cuerpo, con $B \subseteq S$, entonces $I_S(B) = I_S(I_S(B))$.

- Sean $R,\ A,\ \mathbb{K},\ \mathbb{L}$ como en el Teorema 7, entonces A es integralmente cerrado.
  De hecho, como $\mathbb{L}$ es extensión finita de $\mathbb{K}$, $\mathbb{L}$ es algebraica y por el Lema 1 $Q(A) = Q(I_{\mathbb{L}}(R)) = \mathbb{L}$, entonces

$$I_{Q(A)}(A) = I_{\mathbb{L}}(A) = I_{\mathbb{L}}(I_{\mathbb{L}}(R)) = I_{\mathbb{L}}(R) = A,$$

  donde la penúltima igualdad es consecuencia del Lema 2

Dominios de Dedekind

Lema

Sean B y S dominios tales que $B \subseteq S$ y S es entero sobre B. Entonces:

1. *Si $\mathfrak{u}$ es un ideal no nulo de S, $\mathfrak{u} \cap B$, es un ideal no nulo de B.*
2. *Un ideal primo $\mathfrak{p}$ de S es maximal en S, si y solo si, $\mathfrak{p} \cap B$, es maximal en B.*

- Sean R, A, $\mathbb{K}$, $\mathbb{L}$ como en el Teorema 7, vamos a probar que todo ideal primo no nulo de A es maximal.
  De hecho, si $\mathfrak{p}$ es un ideal primo no nulo de A, entonces, por el ítem 1 del lema anterior, $\mathfrak{p} \cap R$ es un ideal primo no nulo de R. Como R es dominio de Dedekind, $\mathfrak{p} \cap R$ es un ideal maximal de R. Luego por el ítem 2, el ideal $\mathfrak{p}$ de A es maximal.

Dominios de Dedekind

El siguiente lema completa la prueba del Teorema 7.

Lema

A es noetheriano.

En el anillo $\mathbb{Z}$ todo ideal es principal y por el Teorema Fundamental de la Aritmética todo ideal propio lo podemos expresar de manera única como producto de ideales primos. Sin embargo, en general, no cabe esperar dicha descomposición de ideales.
Ser de Dedekind es condición suficiente (y necesaria) para que en un anillo valga dicha descomposición.

Factorización de Ideales

Teorema

Si R es un dominio de Dedekind, entonces todo ideal propio de R puede ser escrito de manera única como producto de ideales primos.

Ejemplo

En $\mathbb{Z}\left[\sqrt{-5}\right]$ el ideal $\langle 6\rangle$ es producto de cuatro ideales primos:

$$\langle 6\rangle = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3.$$

Donde

$$\mathfrak{p}_1 = \left\langle 2, 1+\sqrt{-5}\right\rangle, \quad \mathfrak{p}_2 = \left\langle 3, 1+\sqrt{-5}\right\rangle, \quad \mathfrak{p}_3 = \left\langle 3, 1-\sqrt{-5}\right\rangle.$$

Factorización de Ideales

Definición

Sea R un dominio de Dedekind, $\mathfrak{a}$ y $\mathfrak{b}$ ideales no nulos de R. Decimos que $\mathfrak{a}$ divide a $\mathfrak{b}$ si existe $\mathfrak{j}$ ideal de R tal que $\mathfrak{a}\mathfrak{j} = \mathfrak{b}$, en tal caso escribimos $\mathfrak{a}|\mathfrak{b}$.

En el contexto de los ideales "contener" es equivalente a "dividir".

Proposición

Sea R un dominio de Dedekind, $\mathfrak{a}$ y $\mathfrak{b}$ ideales no nulos de R. Entonces $\mathfrak{a}|\mathfrak{b}$, si y solo si $\mathfrak{a} \supseteq \mathfrak{b}$.

Factorización de Ideales

Probamos que los dominos de ideales principales son dominios de Dedekind, sin embargo existen dominios de Dedekind que no son de ideales principales, es el caso de $\mathbb{Z}\left[\sqrt{-5}\right]$ que por el Teorema 7 es de Dedekind pero vimos que no tiene factorización única.
Para finalizar, tenemos que una condición suficiente para que un dominio de Dedekind tenga factorización única es que tenga un número finito de ideales primos, pues sucede que dichos anillos son siempre dominios de ideales principales.

Teorema

Si R es un dominio de Dedekind con un número finito de ideales primos entonces R es un dominio de ideales principales y por lo tanto tiene factorización única.

La siguiente es una demostración algebraica de que hay infinitos números primos dada por L.C. Washington usando algunos resultados que hemos estudiado.

Factorización de Ideales

Ejemplo

Sabemos que $\mathbb{Z}\left[\sqrt{-5}\right]$ es de Dedekind, pero no DFU, por lo tanto debe tener infinitos ideales primos.

Sea $p \in \mathbb{Z}$ primo, entonces existe $k \in \mathbb{N}$ tal que $\langle p \rangle = \prod_{i=1}^{k} \mathfrak{q}_i^{n_i}$, con $\mathfrak{q}_i$ ideal primo de $\mathbb{Z}\left[\sqrt{-5}\right]$ para cada $i \in \{1, \cdots, k\}$. Supongamos que el número de primos es finito, entonces el conjunto

$$X = \left\{\mathfrak{q} : \mathfrak{q} \text{ es ideal primo de } \mathbb{Z}\left[\sqrt{-5}\right] \text{ y } \mathfrak{q} \mid \langle p \rangle \text{ para algún primo } p \in \mathbb{Z}\right\}$$

es finito. Como $\mathbb{Z}\left[\sqrt{-5}\right]$ tiene infinitos ideales primos podemos escoger a $\mathfrak{q}_1$, un ideal primo de $\mathbb{Z}\left[\sqrt{-5}\right]$ tal que $\mathfrak{q}_1 \notin X$. Pero $\mathbb{Z}\left[\sqrt{-5}\right]$ es entero sobre $\mathbb{Z}$ entonoces, $\mathfrak{q}_1 \cap \mathbb{Z}$ es un ideal primo (maximal) de $\mathbb{Z}$, por el Lema 3, esto es, $\mathfrak{q}_1 \cap \mathbb{Z} = \langle p_1 \rangle$ con p_1 primo. Luego $\mathfrak{q}_1 \mid \langle p_1 \rangle$ pues $\langle p_1 \rangle \subseteq \mathfrak{q}_1$, así $\mathfrak{q}_1 \in X$, contradicción. Por lo tanto existen infinitos números primos.

Referencias

- A. Baker. *Trascendental number theory*. Cambridge University press. 1975.
- E. S. Barnes, H.P.F. Swinnerton-Dyer. *The inhomogeneus minima of binary quadratic forms (I)*. Acta Mathematica 87 (1952), 259-323.
- O. Endler. *Teoria dos números algebráicos*. Segunda edição, Projecto euclides, Rio de Janeiro, IMPA, 2006.
- P. Martin. *Introdução á Teoria dos Grupos e á Teoria de Galois*. Publicações IME-USP.
- K. Spindler. *Abstract Algebra with Applications*. Volume 2: Rings and Fields, Chapman and Hall/CRC Pure and Applied Mathematics, 1993.
- I. Stewart and W. Tall. *Algebraic Number Theory and Fermat's Last Theorem*. Third Edition, AK-Peters, Naticks-Massachusets, 2002.
- O. Zariski, P. Samuel, I. S. Cohen. *Commutative Algebra I: 1 and 2*. Graduate text in methematics, Springer, 1975