UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

FACTORIZACION EN POLINOMIOS CON COEFICIENTES ENTEROS ALGEBRAICOS

T E S I S

PARA OBTENER EL TITULO DE

M A T E M A T I C O

P R E S E N T A :

JOHN WALKER HART JR.

FACULTAD DE CIENCIAS
UNAM

DIRECTOR DE TESIS: DR. FRANCISCO MARMOLEJO RIVAS

A

DRA. MARÍA DE LOURDES ESTEVA PERALTA
Jefa de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo escrito:
Factorización en polinomios con coeficientes enteros algebraicos

realizado por John Walker Hart Jr.

con número de cuenta 09977002-4 , quien cubrió los créditos de la carrera de matemáticas

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Propietario	Dr. Francisco Marmolejo Rivas
Propietario	Dr. Alejandro Diaz Barriga Casales
Propietario	Dr. Ma. del Carmen Gómez Laveaga
Suplente	M.C. Angel M. Carrillo Hoyo
Suplente	Dr. Adalberto Garcia Maynez Cervantes

Consejo Departamental de Matemáticas

M. en C. José Antonio Gómez Ortega

FACULTAD DE CIENCIAS
CONSEJO DEPARTAMENTAL
DE
MATEMÁTICAS

B

FACTORIZACIÓN EN POLINOMIOS CON COEFICIENTES ENTEROS ALGEBRAICOS

Contenido

Agradeciementos

Gracias, me parace que ni siquiera empieza a decir ni describir la gratitud que siento con mis amigos y profesores (los cuales considero amigos también). Pero aquí está, gracias.....

El siguiente conjunto es bien ordenado (más ó menos por tiempo).

A mi mejor amiga Liliana Danea: GRACIAS, gracias por todo. Gracias por ayudarme cuando I was broke, gracias por apoyarme cuando empezaba a estudiar, cuando estaba enojado, triste, feliz, enamorado siempre estabas conmigo, gracias. How about a game of connect four?

Al Queso: gracias Rodrigo por darme chamba y después el GMAT que nunca funcionó pero me permitió llegar hasta aquí. Dominos?

Gene: the loans, the beer, more beer. Cheers. Thanks man. More cheers.

Nacho: Gracias por toda tu ayuda. Go GreenBay.

Tere: Gracias por todo, en especial la comida.

Alex, Laura, Laurita, y Francisca: Gracias por dejarme ser parte de la familia.

Tio Carlos y Tia Ana: Gracias por cuidar a Lili y por el dominó.

Juan R.: Gracias por tu ayuda.

Cesar G.: por todo tu ayuda cuando entre aqui.

A mi maestra Carmen Gómez, gracias más que nada por tu paciencia con todas mis preguntas locas.

Lisa: Thanks for being such a great sis.

Tim: Let's go skiing bro.

Olmo: gracias por tu ayuda.

Leo: por ser un chingón ayudante de álgebra.

Rolando: por tu ayuda en álgebra. ¿Qué tal un Cohiba?

Tito: también por tu ayuda en álgebra.

José Luis: también por tu ayuda en álgebra. Does anyone see a pattern here?

Algebra: por ser tan buena onda.

A mi maestro Angel Carillo. Gracias por tu paciencia y por hacer el análisis más interesante. Y gracias a mandarme con Díaz Barriga.

Eric: por ser un chingón ayudante de análisis.

Parmi: GRE, Subject test.... blah, blah. Thanks for being my friend.

Alex: por ser tan buen pedo. Gracias por todo.

Julio: también por ser buen pedo.

Pablo: por ser el único actuario en análisis tres, y por ser buen pedo.

A mi maestro Adalberto García Maynez, gracias por todo topo. (También paciencia, you thought I was going to forget, didn't you?)

Ferran: gracias por tu ayuda en topo 1.

Adela: por ser una chingona ayudante de topo.

Artico: por ser un buen amigo, por fumar puros y pipa, y las chelas.

A Díaz Barriga: gracias por tu ayuda al principio y por mandarme con Quico.

Manny: gracias por tu entusiasmo en análisis. ¿Luna llena?

Sandino: también por tu entusiasmo en análisis.

Quico: you thought I had forgotten you eh... Gracias por tanto trabajo y paciencia. It turned out pretty good. Gracias.

Introducción

Casi cualquier joven en secundaria sabe factorizar un polinomio cuadrático con coeficientes reales usando el famoso chicharronero (la fórmula para resolver ecuaciones de segundo grado). En esta tesis tratamos algo un poquito distinto: factorizar un polinomio con coeficientes enteros en un producto de polinomios lineales con coeficientes enteros algebraicos. Mientras que el chicharronero tiene años, la nuestra es mucho más joven. El chicharonero no requiere mucha álgebra, mientras que nosotros estamos suponiendo que el lector tiene como mínimo nivel de álgebra la teoría de Galois.

Para una breve historia del problema hay que leer el artículo de Arturo Magidin y David McKinnon [M-M], del cual mucho del capítulo 3 está tomado. Arturo, quien fue mi maestro de teoría de los números clásica, me planteó el problema citado arriba.

La parte realmente bonita del problema es la mezcla de álgebra que usamos en encontrar el algoritmo: Grupos, anillos, teoría de Galois, teoría de números clásica, teoría de números algebraicos y un poco de combinatoria.

La tesis está organizada en forma tal que si uno no sabe nada de teoría de los números y tiene una buena idea de la teoría de Galois, se pueda learla sin mucha dificultad.

En el primer capítulo empezamos con algunas definiciones, por ejemplo, las de entero algebraico y campo cuadrático, y construimos las herramientas básicas como la norma, la traza y el discriminante, culminando en corolario 1.17 que dice que cada anillo numérico visto como grupo aditivo es un grupo abeliano

libre. La mayoría del capítulo uno viene del Marcus [Mar].

En el segundo capítulo definimos dominio de **Dedekind**. Primero demostramos que si I es un ideal no cero en un anillo numérico R, entonces R/I es de orden finito, lo cual permite la demostración de que todo anillo numérico sobre $\mathbb{Q}$ es un anillo de **Dedekind**. Después definimos una relación de equivalencia y desarrollamos el álgebra de esta clase. Terminamos el capítulo dos con los teoremas 2.17 y 2.18, los cuales nos permiten demostrar, en el capítulo tres, que bajo esta relación, las clases forman un grupo finito. Igual que en el primer capítulo, la mayor parte viene del Marcus [Mar].

El tercer capítulo está dedicado a demostrar que dado cualquier polinomio (no constante) con coeficientes enteros algebraicos es posible factorizarlo en un producto de factores lineales, cada uno con coeficientes enteros algebraicos. La mayor parte viene de Arturo Magidin y David McKinnon, "Gauss's Lemma for number fields" [M-M], que se encuentra en proceso de arbitraje en este momento. Se puede conseguir en

`http://www.math.umt.edu/~magidin/preprints/gauss.pdf`

El capítulo cuatro es el algoritmo que estabamos buscando desde el principio. Aquí es donde los teoremas demuestran su poder. El algoritmo es original con esta tesis, aunque usamos muy fuertemente algunas técnicas del libro **Algorithmic Algebraic Number Theory** [P-Z] de M. Pohst y H. Zassenhaus.

Capítulo 1

Herramientas básicas

1.1 Nociones básicas

Definición 1.1. *Un* ***campo numérico*** *es un subcampo de* $\mathbb{C}$ *que es una extensión finita de* $\mathbb{Q}$.

Definición 1.2. *Un número complejo es un* ***número algebraico*** *si es una raíz de un polinomio con coeficientes en* $\mathbb{Z}$. *Vamos a denotar el campo de números algebraicos como* $\overline{\mathbb{Q}}$, *que es un campo es un resultado de teoría de Galois, ver por ejemplo [Fra].*

Definición 1.3. *Un número complejo es un* ***entero algebraico*** *si es una raíz de un polinomio mónico con coeficientes en* $\mathbb{Z}$. *Vamos a denotar el anillo de enteros algebraicos como* $\mathbb{A}$ *que es anillio es resultado de corolario 1.6.*

Definición 1.4. *Un* ***campo cuadrático*** *es un campo de la forma* $\mathbb{Q}(\sqrt{m})$, *donde* m *es un entero libre de cuadrados. Un campo cuadrático es una extensión de grado dos sobre* $\mathbb{Q}$.

Notación: Cuando decimos **encaje** nos estamos referiendo a un $\mathbb{Q}$-*monomorfismo.*

Lema 1.1. *Sea f un polinomio mónico con coeficientes en $\mathbb{Z}$ y supongamos que $f = gh$ donde g y h son polinomios mónicos con coficientes en $\mathbb{Q}$. Entonces g y h realmente tienen coeficientes en $\mathbb{Z}$.*

Demostración. Sea m el mínimo entero positivo tal que mg tiene coeficientes en $\mathbb{Z}$ (n el mínimo entero positivo tal que nh tiene coeficientes en $\mathbb{Z}$). Entonces los coeficientes de mg tienen máximo factor común 1 (ya que si el factor común d es más grande que 1, entonces m no es mínimo, $\frac{m}{d}$ sería un entero positivo menor que m, con $\frac{mg}{d} \in \mathbb{Z}[x]$ una contradicción). (Hacemos lo mismo para n). Supongamos que $mn > 1$ y tomamos cualquier primo p que divida a mn. Consideramos la ecuación $mnf = (mg)(nh)$. Reduciendo mod p, obtenemos $0 = (\overline{mg})(\overline{nh})$. Entonces $0 = \overline{mg}$ o bien $0 = \overline{nh}$. Esto implica que p divide a todos los coeficientes de mg o de nh; lo cual es una contradicción. Entonces tenemos que $m = n = 1$ y que $g, h \in \mathbb{Z}[x]$. □

Teorema 1.2. *Sea α un entero algebraico y sea f un polinomio mónico sobre $\mathbb{Z}$ de grado mínimo que tiene a α como raíz. Entonces f es irreducible sobre $\mathbb{Q}$.*

Demostración. Si f no es irreducible, entonces $f = gh$ donde g y h son polinomios no constantes en $\mathbb{Q}[x]$. Sin perdida de generalidad podemos suponer que g y h son mónicos. Entonces por el lema 1.1, $g, h \in \mathbb{Z}[x]$. Pero α es una raíz de g o de h y los dos tienen grado menor que f, lo cual es una contradicción. □

Corolario 1.3. *Los únicos enteros algebraicos en $\mathbb{Q}$ son los enteros usuales.*

Demostración. Directamente del teorema ya que el polinomio mínimo de cualquier entero algebraico es irreducible sobre $\mathbb{Q}$. □

Corolario 1.4. *Sea m un entero libre de cuadrados. El conjunto de los enteros algebraicos en el campo cuadrático $\mathbb{Q}(\sqrt{m}\,)$ coincide con:*

$$\{a + b\sqrt{m} : a, b \in \mathbb{Z}\} \text{ si } m \equiv 2 \text{ o } 3 \pmod 4$$

$$\left\{\frac{a + b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod 2\right\} \text{ si } m \equiv 1 \pmod 4.$$

Demostración. Si $\alpha \in \mathbb{Q}(\sqrt{m}), \alpha = r + s\sqrt{m}$ donde $r, s \in \mathbb{Q}$, i.e. $\alpha = \frac{a+b\sqrt{m}}{c}$ donde $a, b, c \in \mathbb{Z}, (a, b, c) = 1$. $\mathbb{Q}(\sqrt{m})$ es un extensión de grado dos sobre $\mathbb{Q}$ con base $\{1, \sqrt{m}\}$. Entonces el polinomio mínimo de α es de grado dos. α es un entero algebraico sii su polinomio irreducible está en $\mathbb{Z}[x]$, i.e. $\left(x - (\frac{a+b\sqrt{m}}{c})\right)\left(x - (\frac{a-b\sqrt{m}}{c})\right) \in \mathbb{Z}[x]$. Tenemos esto sii $\frac{2a}{c}, \frac{a^2-b^2m}{c^2} \in \mathbb{Z}$.

Nota: Sabemos que $m \equiv 0 \ (mod\ 4)$ no es posible ya que m es libre de cuadrados.

Si $c = 1$ no hay nada que demostrar.

Supongamos que $c > 1$. Si p es un primo tal que $p|c$ y $p|a$ entonces, como $c^2|(a^2 - mb^2)$, tenemos $p^2|(a^2 - mb^2)$ y como $p|a, p^2|a^2$. Por lo tanto $p^2|mb^2$ y como m es libre de cuadrados $p|b$, lo cual contradice $(a, b, c) = 1$. Esto implica que $(a, c) = 1$.

Entonces como $(a, c) = 1$ y $c|2a$ tenemos que $c|2$. Ya que $c > 1$ tenemos que $c = 2$. Como $(a, c) = 1$, a es impar. Si b es par, entonces, como $4|(a^2 - mb^2)$ tenemos que $4|a^2$, lo cual es una contradicción ya que entonces $2|a$. Entonces a y b son impares, lo cual implica $a \equiv b \ (mod\ 2)$, $a^2 \equiv 1 \ (mod\ 4)$ y $b^2 \equiv 1 \ (mod\ 4)$. Finalmente $mb^2 \equiv 1 \ (mod\ 4)$ lo cual implica que $m \equiv 1 \ (mod\ 4)$.

Ahora si $m \equiv 1 \ (mod\ 4)$ y $c = 2$ entonces $\frac{2a}{2} \in \mathbb{Z}$. Como a, b son impares y $m \equiv 1 \ (mod\ 4)$ tenemos $a^2 - mb^2 \equiv 0 \ (mod\ 4)$ lo cual implica que $\frac{a^2-mb^2}{4} \in \mathbb{Z}$. □

Teorema 1.5. *Las siguientes afirmaciones son equivalentes para $\alpha \in \mathbb{C}$:*

(1) α es un entero algebraico;

(2) El grupo aditivo del anillo $\mathbb{Z}[\alpha]$ es finitamente generado;

(3) α es miembro de algún subanillo de $\mathbb{C}$ que tiene grupo aditivo finitamente generado;

(4) $\alpha A \subset A$ para algún subgrupo $A \subset \mathbb{C}$ finitamente generado.

Demostración. (1)⇒(2): Si α es una raíz de un polinomio mónico sobre $\mathbb{Z}$ de grado n, entonces el grupo aditivo de $\mathbb{Z}[\alpha]$ está generado por $1, \alpha, \ldots, \alpha^{n-1}$.

(2)⇒(3)⇒(4) trivialmente.

(4)⇒(1): Sea $a_1, \ldots, a_n$ un conjunto de generadores de A. Expresando cada αa_i como combinación lineal de $a_1, \ldots, a_n$ con coeficientes en $\mathbb{Z}$, obtenemos

$$\begin{pmatrix} \alpha a_1 \\ \vdots \\ \alpha a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix},$$

donde M es un matriz $n \times n$ sobre $\mathbb{Z}$, i.e,

$$(\alpha I - M) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

donde I es la matriz identidad $n \times n$. Como no todos los a_i son cero, se sigue que $\alpha I - M$ tiene determinante 0. Expresando este determinante en términos de las n^2 coordenadas de $\alpha I - M$, obtenemos α^n + términos de grado menor.

Entonces hemos producido un polinomio mónico sobre $\mathbb{Z}$ que tiene a α como raíz. □

Corolario 1.6. *Si α y β son enteros algebraicos, también lo son $\alpha + \beta$ y $\alpha\beta$.*

Demostración. Sabemos que $\mathbb{Z}[\alpha]$ y $\mathbb{Z}[\beta]$ tienen grupos aditivos finitamente generados. Entonces también $\mathbb{Z}[\alpha, \beta]$ (si $\alpha_1, \ldots, \alpha_m$ generan $\mathbb{Z}[\alpha]$ y $\beta_1, \ldots, \beta_n$ generan $\mathbb{Z}[\beta]$, entonces los mn productos $\alpha_i\beta_j$ generan $\mathbb{Z}[\alpha, \beta]$). Finalmente, $\mathbb{Z}[\alpha, \beta]$ contiene $\alpha + \beta$ y $\alpha\beta$. Por (3) del teorema 1.5, esto implica que son enteros algebraicos. □

1.2 Campos ciclotómicos

Recordamos que si L es una extensión del campo K y $\alpha \in L$ es algebraico sobre K entonces β es un **conjugado** de α sii es raíz del polinomio irreducible de α sobre K.

Sea $\omega = e^{\frac{2\pi i}{m}}$, donde $m \in \mathbb{N}$. Decimos que $\mathbb{Q}(\omega)$ es el **m-ésimo campo ciclotómico**. Los dos primeros campos ciclotómicos son $\mathbb{Q}$ ya que ω es igual a 1 y -1 respectivamente. Más aún, el tercer campo ciclotómico es igual al sexto: sea $\omega = e^{\frac{2\pi i}{6}}$, entonces $\omega = -\omega^4 = -(\omega^2)^2$, lo cual muestra que $\mathbb{Q}(\omega) = \mathbb{Q}(\omega^2)$. En general, para m impar, el m-ésimo campo ciclotómico es igual al $2m$-ésimo campo ciclotómico ya que siempre es verdad que si $\omega = e^{\frac{2\pi i}{2m}}$, con m impar, entonces $\mathbb{Q}(\omega^2) \subset \mathbb{Q}(\omega)$. Para la otra contención basta notar que $\omega = -\omega^{m+1} \in \mathbb{Q}(\omega^2)$, ya que m es impar.

Cada conjugado de ω es también una raíz m-ésima de 1 y no es una raíz n-ésima de 1 para $n < m$. Se sigue que los únicos candidatos para los conjugados son ω^k donde $1 \leq k \leq m$, $(k, m) = 1$.

Teorema 1.7. *Todo ω^k, $1 \leq k \leq m$, $(k, m) = 1$, es conjugado de ω.*

Demostración. Es suficiente demostrar que para cada $\theta = \omega^k$ y para cada primo p que no divide a m, θ^p es un conjugado de θ. Sea $\theta = \omega^k$ y sea p un primo que no divide a m. Sea f el polinomio mónico irreducible de θ sobre $\mathbb{Q}$. Entonces $x^m - 1 = f(x)g(x)$ para algún polinomio mónico $g \in \mathbb{Q}[x]$ y por el lema 1.1 sabemos que $f, g \in \mathbb{Z}[x]$. Obviamente θ^p es raíz de $x^m - 1$, entonces θ^p es raíz de f o g; tenemos que mostrar que θ^p es raíz de f. Supongamos que no, entonces $g(\theta^p) = 0$. Entonces θ es una raíz del polinomio $g(x^p)$. Se sigue que $g(x^p)$ es divisible por $f(x)$ en $\mathbb{Q}[x]$. Aplicando el lema otra vez, tenemos que $g(x^p)$ es divisible por $f(x)$ en $\mathbb{Z}[x]$. Ahora reducimos *mod* p y obtenemos que $\overline{g(x^p)}$ es divisible por $\overline{f(x)}$ en $\mathbb{Z}_p[x]$. Pero *mod* p, $\overline{g(x^p)} = \overline{g(x)}^p$ y $\mathbb{Z}_p[x]$ es un dominio de factorizacion única, entonces $\overline{f}$ y $\overline{g}$ tienen un factor común, $h(x) \in \mathbb{Z}_p[x]$. Entonces $h^2 | \overline{fg} = x^m - 1$. Esto implica que h divide a la derivada de $x^m - 1$, la cual es $\overline{mx^{m-1}}$. Como $p \nmid m$, $\overline{m} \neq 0$; entonces $h(x)$ es un monomio, pero esto contradice el hecho de que $h | x^m - 1$. □

Corolario 1.8. *$\mathbb{Q}(\omega)$ tiene grado $\varphi(m)$, donde $\varphi(m)$ es la φ de Euler, sobre $\mathbb{Q}$.*

Demostración. ω tiene $\varphi(m)$ conjugados, entonces el polinomio irreducible de ω sobre $\mathbb{Q}$ tiene grado $\varphi(m)$. □

1.3 La traza y la norma

Sea K un campo numérico. Definimos dos funciones T y N (la **traza** y la **norma**) en K, como sigue: sean $\sigma_1, \ldots, \sigma_n$ los encajes de K en $\mathbb{C}$, donde $n = [K : \mathbb{Q}]$. Para cada $\alpha \in K$, definimos

$$T(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_n(\alpha),$$

$$N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)\ldots\sigma_n(\alpha).$$

Es obvio que $T(\alpha)$ y $N(\alpha)$ dependen tanto del campo K como de α. De la definición obtenemos $T(\alpha + \beta) = T(\alpha) + T(\beta)$ y $N(\alpha\beta) = N(\alpha)N(\beta)$ para toda $\alpha, \beta \in K$. También, si $\alpha \in \mathbb{Q}$, entonces $T(\alpha) = n\alpha$ y $N(\alpha) = \alpha^n$. Cuando hay más de un campo en juego vamos a escribir T^K y N^K para evitar confusión.

En lo que sigue supongamos que α tiene grado d sobre $\mathbb{Q}$. Denotamos $t(\alpha)$ y $n(\alpha)$ la suma y producto, respectivamente, de los d conjugados de α sobre $\mathbb{Q}$. Entonces tenemos

Teorema 1.9.

$$T(\alpha) = \frac{n}{d}t(\alpha), \qquad N(\alpha) = (n(\alpha))^{\frac{n}{d}}$$

donde $n = [K : \mathbb{Q}]$. *Notamos que* $\frac{n}{d}$ *es un entero: de hecho, es el grado de* $[K : \mathbb{Q}(\alpha)]$.

Demostración. $t(\alpha)$ y $n(\alpha)$ son la traza y la norma de α sobre $\mathbb{Q}$. Cada encaje de $\mathbb{Q}(\alpha)$ en $\mathbb{C}$ se extiende a exactamente $\frac{n}{d}$ encajes de K en $\mathbb{C}$. □

Corolario 1.10. *Para todo* $\alpha \in K$, $T(\alpha)$ *y* $N(\alpha)$ *son racionales.*

Demostración. Es suficiente demostrar que $t(\alpha)$ y $n(\alpha)$ son racionales. Pero esto es obvio ya que $-t(\alpha)$ es el coeficiente del x^{n-1}, si $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \kappa$ del polinomio irreducible de α sobre $\mathbb{Q}$ y $\pm n(\alpha)$ es el término constante. □

Si α es un entero algebraico, entonces su polinomio mónico irreducible sobre $\mathbb{Q}$ tiene coeficientes en $\mathbb{Z}$; entonces

Corolario 1.11. *Si α es un entero algebraico, entonces $T(\alpha)$ y $N(\alpha)$ son enteros.*

Demostración. Directamente de los comentarios previos. □

Ejemplo:
Para el campo cuadrático $\mathbb{Q}(\sqrt{m}\,)$, tenemos

$$T(a + b\sqrt{m}\,) = 2a$$

$$N(a + b\sqrt{m}\,) = a^2 - mb^2$$

para $a, b \in \mathbb{Q}$. Si $\alpha = a + b\sqrt{m}$, con $a, b \in \mathbb{Q}$, $b \neq 0$, entonces el polinomio mónico irreducible sobre $\mathbb{Q}$ que tiene a α como raíz es

$$x^2 - 2ax + a^2 - mb^2$$

Entonces α es un entero algebraico sii $2a$ y $a^2 - mb^2$ son enteros. Entonces $a + b\sqrt{m}$ es entero algebraico sii la traza y norma son enteros.

Ejemplo:
Supongamos que queremos determinar las unidades en el anillo $\mathcal{O}_K$ de enteros algebraicos de K, K un campo numérico. Notamos que para $\alpha \in K$, $N(\alpha) = 0$ sii $\alpha = 0$. También, ya que la norma es multiplicativa, tenemos $N(\alpha) = N(1 \cdot \alpha) = N(1)N(\alpha)$ por lo tanto $N(1) = 1$. Si α es unidad, existe α^{-1} tal que $\alpha \cdot \alpha^{-1} = 1$. Por el corolario 1.11 tenemos que $N(\alpha) = \pm 1$. Si α es un entero algebraico que tiene norma ± 1, entonces por el teorema 1.9, $\frac{1}{\alpha}$ es un entero algebraico, ya que $n(\alpha) = \pm 1$. Esto muestra que las unidades en $\mathcal{O}_K$ son los elementos con norma ± 1.

Ejemplo:

Consideramos el campo cuadrático $\mathbb{Q}(\sqrt{m})$ pero con la restricción $m \leq -5$. Afirmamos que las únicas unidades en $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ son ± 1. Sea $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{m})}$, i.e $\alpha = a + b\sqrt{m}$ con $a, b \in \mathbb{Q}$. $N(a + b\sqrt{m}) = a^2 - b^2 m$, entonces, si α es unidad, tenemos que $a^2 - b^2 m = \pm 1$. También, gracias al corolario 1.4, tenemos que $a, b \in \mathbb{Z}$ o $a = \frac{c}{2}, b = \frac{d}{2}$ con $c, d \in \mathbb{Z}$. Si $a, b \in \mathbb{Z}$, es imposible que $a^2 - b^2 m = -1$ por lo que $a^2 - b^2 m = 1$. Si $b \neq 0$ entonces $a^2 - b^2 m \geq 5$, entonces $b = 0$, por lo que $a = \pm 1$. En el otro caso tenemos $\frac{c^2}{4} - \frac{d^2 m}{4} = \pm 1$. Otra vez es imposible que $\frac{c^2}{4} - \frac{d^2 m}{4} = -1$, entonces $\frac{c^2}{4} - \frac{d^2 m}{4} = 1$, i.e $c^2 - d^2 m = 4$. Si $d \neq 0$, $c^2 - d^2 m \geq 5$ lo cual implica que $d = 0$ y que $c = \pm 2$. Otra vez $\alpha = \pm 1$. Es fácil verificar que las unidades en el caso en que $m = -1$ son $\{\pm 1, \pm i\}$ y cuando $m = -3$ son $\pm 1, \pm\omega, \pm\omega^2$ donde $\omega = e^{\frac{2\pi i}{3}}$.

Ejemplo:

Como arriba pero con $m = 2$. Consideramos la ecuación $a^2 - 2b^2 = \pm 1$. $1 + \sqrt{2}$ es unidad en $\mathbb{Z}[\sqrt{2}\,]$ (con inverso $-1 + \sqrt{2}$) y no es raíz de uno. Entonces hay un número infinito de unidades en $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$, lo cual implica que hay un número infinito de soluciones enteros a la ecuación $a^2 - 2b^2 = \pm 1$.

1.4 Discriminante

Notación: vamos a escribir $[a_{ij}]$ para denotar la matriz que tiene a_{ij} en el i-ésimo renglón y j-ésima columna y $|a_{ij}|$ para denotar su determinante.

Sea K un campo numérico de grado n sobre $\mathbb{Q}$. Sean $\sigma_1, \ldots, \sigma_n$ los n encajes de K en $\mathbb{C}$. Para cualquier n-ada de elementos $\alpha_1, \ldots, \alpha_n \in K$, definimos el **discriminante** de $\alpha_1, \ldots, \alpha_n$ como:

$$disc(\alpha_1, \ldots, \alpha_n) = |\sigma_i(\alpha_j)|^2$$

i.e., el cuadrado del determinante de la matriz que tiene $\sigma_i(\alpha_j)$ en el i-ésimo renglón y j-ésima columna.

Notamos que el cuadrado hace que el discriminante sea independiente del orden de los σ_i y de los α_i.

Teorema 1.12. $disc(\alpha_1, \ldots, \alpha_n) = |T(\alpha_i\alpha_j)|$.

Demostración. Esto se sigue de inmediato de la ecuación matricial

$$[\sigma_j(\alpha_i)][\sigma_i(\alpha_j)] = [\sigma_1(\alpha_i\alpha_j) + \cdots + \sigma_n(\alpha_i\alpha_j)] = [T(\alpha_i\alpha_j)]$$

y de las propiedades del determinante:
$|a_{ij}| = |a_{ji}|$ y $|AB| = |A||B|$ para las matrices A y B. □

Corolario 1.13. $disc(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$ *; y si todo* α_i *es entero algebraico, entonces* $disc(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$

Demostración. Directamente del teorema ya que si α_i y α_j son enteros algebraicos sabemos, por el corolario 1.6, que $\alpha_i\alpha_j$ es un entero algebraico, lo cual implica que $T(\alpha_i\alpha_j)$ está en $\mathbb{Z}$ y un determinante de enteros es entero. □

Teorema 1.14. $disc(\alpha_1, \ldots, \alpha_n) = 0$ *sii* $\alpha_1, \ldots, \alpha_n$ *son linealmente dependientes sobre* $\mathbb{Q}$

Demostración. Si los α_j son linealmente dependientes sobre $\mathbb{Q}$, entonces también lo son las columnas de lo matriz $[\sigma_i(\alpha_j)]$; por lo tanto el discriminante es 0.

Ahora, si $disc(\alpha_1, \ldots, \alpha_n) = 0$, entonces los renglones R_i de la matriz $[T(\alpha_i\alpha_j)]$ son linealmente dependientes. Supongamos que $\alpha_1, \ldots, \alpha_n$ son linealmente independientes sobre $\mathbb{Q}$. Fijando números racionales $a_1, \ldots, a_n$ (no todos cero) tales que $a_1R_1 + \cdots + a_nR_n = 0$ (vector), consideramos $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$. Necesariamente $\alpha \neq 0$ (ya que $\alpha_1, \ldots, \alpha_n$ son linealmente independientes sobre $\mathbb{Q}$ y al menos un $a_i \neq 0$). Considerando la j-ésima coordenada de cada renglón, obtenemos que $T(\alpha\alpha_j) = 0$ para cada j. Como los α_i son linealmente independientes sobre $\mathbb{Q}$, forman una base de K sobre $\mathbb{Q}$; se sigue (ya que $\alpha \neq 0$) que lo mismo es verdad de los $\alpha\alpha_j$. Pero esto implica que $T(\beta) = 0$ para todo $\beta \in K$, ya que $(\alpha\alpha_1, \ldots, \alpha\alpha_n)$ es base de K sobre $\mathbb{Q}$ y que T es aditivo. Esto es una contradicción ya que $T(1) = n$. □

1.5 Estructura aditiva de un anillo numérico

Sea K un campo numérico de grado n sobre $\mathbb{Q}$ y sea $\mathcal{O}_K$ el anillo de enteros algebraicos en K, es decir, $\mathbb{A} \cap K = \mathcal{O}_K$.

Un **grupo abeliano libre** de rango finito n es cualquier grupo que es la suma directa de n subgrupos, cada uno isomorfo a $\mathbb{Z}$. Sabemos de la teoría de grupos que cada subgrupo de un grupo abeliano libre de rango n es también un grupo abeliano libre de rango $\leq n$. De esto se sigue que si un grupo está entre dos grupos que son abelianos libres del mismo rango, el grupo también es abeliano libre del mismo rango.

Lema 1.15. *Existe una base de K sobre $\mathbb{Q}$ formada por enteros algebraicos.*

Demostración. Para ver esto es suficiente ver que dado $\alpha \in K$ existe $m \in \mathbb{Z}$, $m \neq 0$, tal que $m\alpha$ es un entero algebraico. Si α es raíz del polinomio $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_i \in \mathbb{Z}$, entonces el polinomio $g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_n^{n-2}x + a_1 a_n^{n-1} a_0 = x^n + \sum_{i=1}^{n} a_{n-i} a_n^{i-1} x^{n-i}$ tiene raíz $a_n\alpha$. □

Fijando tal base $\{\alpha_1, \ldots, \alpha_n\} \subset \mathcal{O}_K$ de K sobre $\mathbb{Q}$, tenemos un grupo abeliano libre de rango n dentro de $\mathcal{O}_K$, a saber

$$A = \left\{ m_1\alpha_1 + \cdots + m_n\alpha_n | m_i \in \mathbb{Z} \right\},$$

el cual se puede ser expresado como:

$$A = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$$

Teorema 1.16. *Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base de K sobre $\mathbb{Q}$ formada por enteros algebraicos y sea $d = disc(\alpha_1, \ldots, \alpha_n)$. Entonces cada $\alpha \in \mathcal{O}_K$ se puede expresar en la forma*

$$\frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d}$$

con todos los $m_j \in \mathbb{Z}$ y todos $m_j{}^2$ divisibles por d.

Notamos que $d \neq 0$ porque los α_i forman una base y $d \in \mathbb{Z}$ porque los α_i son enteros algebraicos.

Demostración. Sea $\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n$ con $x_j \in \mathbb{Q}$. Sean $\sigma_1, \ldots, \sigma_n$ los encajes de K en $\mathbb{C}$. Si aplicamos cada σ_i a α obtenemos

$$\sigma_i(\alpha) = x_1\sigma_i(\alpha_1) + \cdots + x_n\sigma_i(\alpha_n).$$

Usando la regla de Cramer, $x_j = \frac{\gamma_j}{\delta}$ donde δ es el determinante $|\sigma_i(\alpha_j)|$ y γ_j se obtiene de δ remplazando la j-ésima columna por $\sigma_i(\alpha)$. Es claro que γ_j y δ son enteros algebraicos y, de hecho, $\delta^2 = d$. Entonces $dx_j = \delta\gamma_j$, lo cual demuestra que el número racional dx_j es un entero algebraico, lo cual implica que $dx_j \in \mathbb{Z}$. Sea $dx_j = m_j$. Por tanto, $\frac{m_j^2}{d} = dx_j^2 = d(\frac{\gamma_j^2}{\delta^2}) = \gamma_j{}^2$. □

El teorema 1.16 muestra que $\mathcal{O}_K$ está contenido en el grupo abeliano libre

$$\frac{1}{d}A = \mathbb{Z}\frac{\alpha_1}{d} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha_n}{d}.$$

Entonces:

Corolario 1.17. *$\mathcal{O}_K$ es un grupo abeliano libre de rango n.*

Demostración. Directamente de arriba. □

Equivalentemente, $\mathcal{O}_K$ tiene base sobre $\mathbb{Z}$: existen $\beta_1, \ldots, \beta_n \in \mathcal{O}_K$ tales que cada $\alpha \in \mathcal{O}_K$ tiene representación única de la forma

$$m_1\beta_1 + \cdots + m_n\beta_n, m_i \in \mathbb{Z}$$

$(\beta_1, \ldots, \beta_n)$ se llama **base entera** sobre $\mathcal{O}_K$.

Ejemplo:

Consideramos el campo cuadrático $\mathbb{Q}(\sqrt{m})$. Si $m \equiv 2$ o 3 $(mod\ 4)$ entonces $\{1, \sqrt{m}\}$ es base entera de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$, gracias a corolario 1.4. Notamos en cualquier caso que el discriminate es igual a $4m$. Si $m \equiv 1$ $(mod\ 4)$ entonces una base entera de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ es $\{1, \frac{1+\sqrt{m}}{2}\}$.

Proposición 1.18. *El campo de fracciones de $\mathcal{O}_K$ es K.*

Demostración. Es suficiente demostrar que $K \subset$ campo de fracciones de $\mathcal{O}_K$, ya que $\mathcal{O}_K \subset K$ implica que el campo de fracciones de $\mathcal{O}_K$ está contenido en K. Si $\alpha \in K$, es suficiente demostrar que existe $b \in \mathcal{O}_K$, no cero, tal que $\alpha b \in \mathcal{O}_K$. Pero como $\alpha \in K$, α es un número algebraico, entonces existe $b \in \mathbb{Z}$, no cero, tal que αb es un entero algebraico y claramente $b \in \mathcal{O}_K$. □

Notamos que esto implica que cualquier base entera de $\mathcal{O}_K$ es una base de K sobre $\mathbb{Q}$.

Teorema 1.19. *Sean $(\beta_1, \ldots, \beta_n)$ y $(\gamma_1, \ldots, \gamma_n)$ dos bases enteras de $\mathcal{O}_K$. Entonces $disc(\beta_1, \ldots, \beta_n) = disc(\gamma_1, \ldots, \gamma_n)$.*

Demostración. Escribiendo β_i en términos de los γ_j, tenemos

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = M \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix}$$

donde M es una matriz $n \times n$ sobre $\mathbb{Z}$.

Aplicando cada σ_j a cada una de las n ecuaciones, llegamos a que $[\sigma_j(\beta_i)] = M[\sigma_j(\gamma_i)]$. Tomando el cuadrado de los determinantes, obtenemos

$$disc(\beta_1, \ldots, \beta_n) = |M|^2 disc(\gamma_1, \ldots, \gamma_n).$$

Claramente $|M| \in \mathbb{Z}$, lo cual implica que $disc(\gamma_1, \ldots, \gamma_n)$ es un divisor de $disc(\beta_1, \ldots, \beta_n)$ y que los dos tienen el mismo signo. Un argumento similar demustra que $disc(\beta_1, \ldots, \beta_n)$ divide a $disc(\gamma_1, \ldots, \gamma_n)$. □

Capítulo 2

Primos

Definición 2.1. *Decimos que un anillo R es* ***enteramente cerrado*** *en su campo de fracciones K, si cualquier $\gamma \in K$ que sea raíz de un polinomio mónico sobre R, pertenece a R.*

Definición 2.2. *Un* ***Dominio de Dedekind*** *es un dominio entero R tal que:*

(1) Cada ideal es finitamente generado;

(2) Cada ideal primo no cero es maximal;

(3) R es enteramente cerrado en su campo de fracciones $K = \{\frac{\alpha}{\beta} | \alpha, \beta \in R, \beta \neq 0\}$.

Recordamos que un anillo que satisface la condición (1) se llama un anillo Noeteriano y que la condición (1) es equivalente a:

(1') Cada cadena ascendente de ideales se estaciona.

(1") Cada conjunto no vacío S de ideales tiene un elemento maximal.

Proposición 2.1. *Si I es cualquier ideal no cero en el anillo numérico $\mathcal{O}_K$, entonces $\mathcal{O}_K / I$ es finito.*

Demostración. Sea α un elemento no cero en I y sea $m = N^K(\alpha)$. Sabemos que $m \in \mathbb{Z}$ y que $m \neq 0$. De hecho $m \in I$: de la definición de la norma tenemos que $m = \alpha\beta$, donde β es el producto de los conjugados de α distintos

de α. Estos conjugados no tienen por qué estar en $\mathcal{O}_K$, pero β está porque $\beta = \frac{m}{\alpha} \in K$. Ademas $\beta \in \mathbb{A}$ ya que cada conjugado es un entero algebraico y ya hemos visto que el producto de dos enteros algebraicos es un entero algebraico. Entonces $m \in I$. Obviamente $\mathcal{O}_K/(m)$ es finito, ya que es $\mathcal{O}_K/(m\mathcal{O}_K)$ que tiene orden m^n, esto de un resultado de grupos que dice que si G es un grupo abeliano libre de rango n entonces para $m \in \mathbb{Z}$, G/mG es la suma directa de n grupos cíclicos de orden m. Como $m\mathcal{O}_K \subset I$ sabemos que $\mathcal{O}_K/I$ es finito. □

Teorema 2.2. *Cada anillo numérico es un dominio de Dedekind.*

Demostración. Sea $\mathcal{O}_K$ el anillo numérico correspondiente a la extensión $K/\mathbb{Q}$. Ya hemos visto que cada anillo numérico es un grupo (aditivamente) abeliano libre de rango finito; un ideal es un subgrupo (aditivamente), entonces es abeliano libre de rango finito también y, por tanto, es finitamente generado.

Para demostrar que cada ideal primo P no cero es maximal, es suficiente demostrar que el dominio entero $\mathcal{O}_K/P$ es un campo, para lo cual es suficiente demostrar que $\mathcal{O}_K/P$ es finito, lo cual tenemos de la proposición 2.1.

Finalmente observemos que $\mathcal{O}_K$ es enteramente cerrado en K: Si $\alpha \in K$ es raíz de un polinomio mónico sobre $\mathcal{O}_K$, i.e si

$$\alpha^n + a_{n-1}\alpha^{n-1} \cdots a_1\alpha + a_0 = 0$$

con $a_i \in \mathcal{O}_K$, entonces $\mathbb{Z}[a_0, \cdots, a_{n-1}, \alpha]$ es finitamente generado como grupo aditivo. Para ver esto consideramos los productos $a_0^{m_0} a_1^{m_1} \cdots a_{n-1}^{m_{n-1}} \alpha^m$ y notamos que solamente un número finito de valores para los m_i son necesarios ya que,

$$\alpha^n = -(a_{n-1}\alpha^{n-1} \cdots a_1\alpha + a_0),$$

entonces podemos generar cualquier potencia de α con esto. Para los demás es suficiente aplicar el teorema 1.5 ya que los a_i son enteros algebraicos. Esto implica α es entero algebraico, lo cual implica que $\alpha \in \mathcal{O}_K$. □

NOTA: En lo que sigue, **ideal** siempre significa **ideal no cero**.

Ejemplo:
Consideramos el campo cuadrático $\mathbb{Q}(\sqrt{-3})$. Como $-3 \equiv 1 \ mod\ 4$,

$$\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \left\{ \frac{a + b\sqrt{m}}{2} : a, b \in \mathbb{Z},\ a \equiv b \ (mod\ 2) \right\}.$$

lo cual es un dominio de Dedekind. Afirmamos que $\mathbb{Z}[\sqrt{-3}]$ no lo es. Esto es fácil de ver si consideramos $I = (2,\ 1 + \sqrt{-3})$. Obviamente $I \neq (2)$ y $I^2 = 2I$, entonces no tenemos factorizacion única en ideales primos. (Ver teorema 2.10 m ás adelante.)

Teorema 2.3. *Sea I un ideal en un dominio de Dedekind R. Entonces existe un ideal J tal que IJ es principal.*

Demostración. Sea α cualquier elemento no cero de I y sea

$$J = \{\beta \in R | \beta I \subset (\alpha)\}.$$

Entonces $\alpha \in J$ y J es un ideal ya que es trivialmente un grupo aditivo y cerrado bajo multiplicación. Si $a \in J$ y $b \in R$, entonces $aI \subset (\alpha)$ entonces, como (α) es un ideal, $baI \subset (\alpha)$. Ademaś, $IJ \subset (\alpha)$.

Para demostrar igualdad necesitamos dos lemas:

Lema 2.4. *En un dominio de Dedekind, cada ideal (no cero) contiene un producto de ideales primos (no cero).*

Demostración. Supongamos que no; entonces el conjunto de los ideales que no contienen tales productos es no vacío, y por la condición (1") tiene un miembro maximal M. M no es primo, entonces existen $r, s \in R - M$ tales que $rs \in M$. Los ideales $M + (r)$ y $M + (s)$ contienen propiamente a M y por lo tanto contienen un producto de primos; pero entonces el producto $(M + (r))(M + (s)) \subset M$ y contiene un producto de primos. □

Lema 2.5. *Sea A un ideal propio en un dominio de Dedekind R con campo de fracciones K. Entonces existe un elemento $\gamma \in K - R$ tal que $\gamma A \subset R$.*

Demostración. Fijamos cualquier elemento $\alpha \in A$ no cero. Por el lema 2.4, existen primos $P_1, P_2, \ldots, P_r$ tales que $P_1P_2 \ldots P_r \subset (\alpha)$ y podemos suponer que r es mínimo con esta propiedad. Cada ideal propio está contenido en un ideal maximal (por el lema de Zorn) y sabemos que todo ideal maximal es primo; entonces $A \subset P$ para algún ideal primo P. Entonces P contiene el producto $P_1P_2 \ldots P_r$. Se sigue que P contiene algún P_i (si esto no fuera verdad, entonces fijamos elementos $a_i \in P_i - P$; P contiene el producto $a_1a_2 \ldots a_r$, entonces P contiene uno de los a_i, lo cual es una contradicción). Sin pérdida de generalidad supongamos que $P_1 \subset P$. Por la condición (2) de dominios de Dedekind, tenemos que $P_1 = P$. Finalmente, como (α) no contiene un producto con menos de r primos; existe $b \in (P_2P_3 \ldots P_r) - (\alpha)$. Entonces $\gamma = \frac{b}{\alpha} \in K - R$ y $\gamma A \subset R$. Para ver esto, si $\gamma \in R$, entonces multiplicando por α tenemos $b \in \alpha R$ lo cual es una contradicción. Ahora $\frac{b}{\alpha}A \subset \frac{b}{\alpha}P_1$ y como $P_1P_2 \ldots P_r \subset (\alpha)$, entonces $\frac{b}{\alpha}P_1 \subset R$. □

Continuando con la desmostración del teorema 2.3, consideramos el conjunto $A = \frac{1}{\alpha}IJ$. Esto está contenido en R, ya que $IJ \subset (\alpha)$. También A es un ideal, ya que IJ lo es y $A \subset R$. Si $A = R$ entonces $IJ = (\alpha)$ y ya hemos terminado; si no, A es un ideal propio y por el lema 2.5 existe $\gamma \in K - R$ tal que $\gamma A \subset R$. Buscamos una contradicción. Como R es enteramente cerrado en K, es suficiente demostrar que γ es raíz de un polinomio mónico sobre R.

Como $\alpha \in I$, $A = \frac{1}{\alpha}IJ$ contiene J, entonces $\gamma J \subset \gamma A \subset R$. Se sigue que $\gamma J \subset J$; ya que $\alpha\gamma J \subset \gamma JI \subset (\alpha)$.

Finalmente, fijamos un conjunto de generadores $(\alpha_1, \ldots, \alpha_m)$ para el ideal J y usamos la relación $\gamma J \subset J$ para obtener la ecuación

$$\gamma \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

donde M es una matriz $m \times m$ sobre R. Como en la demostración del teorema 1.5, obtenemos un polinomio mónico sobre R que tiene a γ como raíz. □

Ejemplo:

Consideramos el anillo numérico $R = \mathbb{Z}[\sqrt{-5}\,]$. No es un anillo de factorización única ($2 \times 3 = (1+\sqrt{-5}\,)(1-\sqrt{-5}\,)$). El ideal $(2, 1+\sqrt{-5}\,) = I$ es maximal y $I^2 = (2)$. Para ver esto, observamos que $|R/(2)| = 4$, entonces $R/(2, 1+\sqrt{-5}\,)$ tiene orden que divide a 4. Tiene que ser 2 ya que contiene (2) propiamente y no es R, ya que si fuera R, entonces $I^2 = R$. Entonces $(2, 1+\sqrt{-5}\,) = I$ es maximal como subgrupo aditivo, i.e. maximal como ideal, y por lo tanto, primo.

Proposición 2.6. *Definimos una relación para los ideales de un dominio entero R, como sigue: para I, J ideales de R, $I \sim J$ sii existen $a, b \in R - \{0\}$ tales que $aI = bJ$. Entonces $\sim$ es una relación de equivalencia y los ideales principales forman una sola clase.*

Demostración. Es claro que $\sim$ es un relación de equivalencia. Ahora, si A es un ideal en R y si αA es principal para algún $\alpha \in R$, demostraremos que A es principal, lo cual implica que los ideales principales forman una clase. Ahora, como αA es principal, sea $\alpha A = (b)$. Sea $d \in A$ tal que $\alpha d = b$. Afirmamos que $A = (d)$. Sea $a \in A$. Entonces $\alpha a = br$ para algún $r \in R$. Entonces tenemos que $\alpha a = \alpha dr$ y como R es un dominio entero $a = dr$, lo cual implica que $A = (d)$. □

Corolario 2.7. *Las clases de ideales en un dominio de Dedekind forman un grupo.*

Demostración. Definimos la multiplicación de dos representantes en forma natural, i.e. si I_1, I_2 son dos ideales su producto es $I_1 I_2$. Hay que demostrar que la multiplicación entre clases está bien definida. Si $I_1 \sim I_2$ y $J_1 \sim J_2$, existen $a_1, a_2, b_1, b_2 \in R$ tales que $a_1 I_1 = a_2 I_2$ y $b_1 J_1 = b_2 J_2$. Multiplicando las dos igualdades tenemos $a_1 b_1 I_1 J_1 = a_2 b_2 I_2 J_2$ lo cual muestra que la multiplación está bien definida, ya que $I_1 J_1 \sim I_2 J_2$. Gracias al teorema 2.3 y la proposición 2.6 tenemos inversos y la clase de los ideales principales es unidad. □

Corolario 2.8. *(Ley de cancelación) Si A,B,C son ideales en un dominio de Dedekind y $AB = AC$ entonces $B = C$.*

Demostración. Existe un ideal J tal que $AJ = (\alpha)$. Entonces $JAB = JAC$, i.e. $\alpha RB = \alpha RC$, i.e. $\alpha B = \alpha C$, por lo tanto $B = C$. □

Definición 2.3. *Decimos que el ideal A divide al ideal B si existe un ideal C tal que $B = AC$. Notación: $A|B$.*

Corolario 2.9. *Si A y B son ideales en un dominio de Dedekind R, entonces $A|B$ sii $B \subset A$.*

Demostración. $\Rightarrow$ Trivial.

$\Leftarrow$ Si $B \subset A$, fijamos J tal que AJ es principal, $AJ = (\alpha)$. El conjunto $C = \frac{1}{\alpha}JB$ es un ideal de R y $AC = B$ ya que $AC = \frac{1}{\alpha}AJB = \frac{1}{\alpha}\alpha RB = RB = B$. □

Teorema 2.10. *Cada ideal en un dominio de Dedekind R tiene una única representación como un producto de ideales primos.*

Demostración. Supongamos que el conjunto de ideales propios que no tienen representación como producto de ideales primos es no vacío. Entonces por la condición (1''), tiene un elemento maximal M, $M \neq R$ y $M \subset P$ para algún ideal primo (maximal) P. Entonces $M = PI$ para algún ideal I. Entonces $M \subset I$ propiamente ya que si $M = I$ entonces $R = P$, una contradicción. Entonces I es un producto de ideales primos, pero entonces M también lo es, lo cual es una contradicción.

Falta demostrar unicidad. Si $P_1P_2 \dots P_r = Q_1Q_2 \dots Q_s$, donde P_i y Q_i son primos. Entonces $Q_1Q_2 \dots Q_s \subset P_1$ y hemos visto que esto implica que $Q_i \subset P_1$ para algún i. Cambiando la numeración si es necesario, podemos suponer que tenemos que $Q_1 \subset P_1$. Pero como todo ideal primo es maximal, $Q_1 = P_1$. Por la ley de cancelación tenemos que $P_2 \dots P_r = Q_2 \dots Q_s$. Entonces vemos que $r = s$ y reenumerando, si es necesario, que $P_i = Q_i$. □

De esto observamos que cada ideal en un anillo numérico se factoriza de manera única en ideales primos.

También, gracias al teorema 2.10, es posible definir, para dos ideales I y J en $\mathcal{O}_K$, el máximo común divisor y el mínimo común multiplo (lo cual denotamos como $mcd(I,J)$ y $mcm(I,J)$ respectivamente). Por el corolario 2.9 vemos que el $mcd(I,J)$ es realmente el ideal más pequeño que contiene I y J, y que el $mcm(I,J)$ es el ideal más grande contenido en ambos I y J. Entonces, tenemos;

$$mcd(I,J) = I + J$$

$$mcm(I,J) = I \cap J.$$

Dos ideales I y J de un anillo R se llaman **coprimos** sii $I + J = R$.

Proposición 2.11. *Si I es coprimo con cada uno de $J_1, \ldots, J_n$ entonces I es coprimo con $\bigcap_{i=1}^{n} J_i$.*

Demostración. Para cada i escribimos $a_i + b_i = 1$ con $a_i \in I$ y $b_i \in J_i$. Multiplicando las ecuaciones, vemos que $1 = a + b_1 b_2 \ldots b_n$, donde $a \in I$ y $b_1 b_2 \ldots b_n \in \bigcap_{i=1}^{n} J_i$. También notamos que si I y J son coprimos, entonces $IJ = I \cap J$, ya que la contención de la izquierda es trivial y si $x \in I \cap J$ y si escribimos $1 = i + j$ con $i \in I$, $j \in J$, multiplicando por x tenemos $x = xi + xj$, lo cual está en IJ. □

Teorema 2.12. *Teorma Chino.*

Sean $I_1, \ldots, I_n$ ideales coprimos dos a dos en un anillo R. Entonces la función canónica

$$R/\bigcap_{i=1}^{n} I_i \to R/I_1 \times \cdots \times R/I_n$$

es un isomorfismo.

Demostración. Es suficiente demostrar el caso $n = 2$, ya que el caso general se desprende de éste porque I_1 es coprimo a $\bigcap_{i=2}^{n} I_i$

Supongamos que $n = 2$. El núcleo del mapeo es obviamente trivial, por lo cual la función es inyectiva. Para ver que es sobre, fijamos r_1 y $r_2 \in R$. Queremos encontrar $r \in R$ tal que

$$r \equiv r_1 (mod\ I_1)$$

$$r \equiv r_2 (mod\ I_2).$$

Como I_1 es coprimo con I_2 existen $a_1 \in I_1$ y $a_2 \in I_2$ tales que $a_1 + a_2 = 1$. Sea $r = a_1 r_2 + a_2 r_1$. Un simple cálculo demuestra que r satisface las condiciones de arriba. □

Teorema 2.13. *Sea I un ideal en un dominio de Dedekind R y sea α un elemento no cero de I. Entonces existe $\beta \in I$ tal que $I = (\alpha, \beta)$.*

Demostración. Es suficiente demostrar que existe $\beta \in R$ tal que

$$I = mcd((\alpha), (\beta)),$$

ya que esto implica que $\beta \in I$.

Sea $P_1^{n_1} P_2^{n_2} \dots P_r^{n_r}$ la descomposición de I en producto de primos, donde los P_i son distintos. Como $(\alpha) \subset I$, $(\alpha) \subset P_i^{n_i}$ para cada i, i.e. $P_i^{n_i} | (\alpha)$ para cada i. Sean $Q_1, \dots, Q_s$ los otros primos, si los hay, que dividen a (α). Tenemos que construir β tal que ningún Q_j divida a (β) y para cada i, $P_i^{n_i}$ sea la potencia exacta de P_i que divide (β). i.e.

$$\beta \in \bigcap_{i=1}^{r} (P_i^{n_i} - P_i^{n_i+1}) \cap \bigcap_{j=1}^{s} (R - Q_j).$$

Usamos el teorema Chino: fijamos $\beta_i \in P_i^{n_i} - P_i^{n_i+1}$, que existe por factorización única y sea β tal que satisface las congruencias

$$\beta \equiv \beta_i\ (mod\ P_i^{n_i+1}), i = 1, \dots, r$$

$$\beta \equiv 1 \ (mod\ Q_j), j = 1, \ldots, s.$$

Tal β existe porque las potencias de P_i y los Q_j son coprimos dos a dos, puesto que su mcd es (1), i.e. R. □

Si K es un campo numérico, P es cualquier ideal primo en el anillo numérico $\mathcal{O}_K$ y si L es un campo numérico que contiene a K, consideramos la descomposición del ideal generado por P en el anillo numérico $\mathcal{O}_L$. Dicho ideal es $P\mathcal{O}_L$.

En lo que sigue, K y L son campos numéricos con $K \subset L$ y $\mathcal{O}_K = \mathbb{A} \cap K$, $\mathcal{O}_L = \mathbb{A} \cap L$. El término **primo** se refire a **ideal primo no cero**.

Teorema 2.14. *Sean P un primo de $\mathcal{O}_K$ y Q un primo de $\mathcal{O}_L$. Entonces las siguientes afirmaciones son equivalentes:*

(1) $Q|P\mathcal{O}_L$
(2) $P\mathcal{O}_L \subset Q$
(3) $P \subset Q$
(4) $Q \cap \mathcal{O}_K = P$
(5) $Q \cap K = P$.

Demostración. (1) $\Longleftrightarrow$ (2) se deduce del corolario 2.9. (2)⇒(3) Como $1 \in \mathcal{O}_L$, $P \subset P\mathcal{O}_L$. (3)⇒(2) Si multiplicamos $P \subset Q$ por $\mathcal{O}_L$ obtenemos (ya que Q es un ideal en $\mathcal{O}_L$) $P\mathcal{O}_L \subset Q$. (4)⇒(3) Trivial. (4) $\Longleftrightarrow$ (5) Es claro que $P = Q \cap \mathcal{O}_K = Q \cap (K \cap \mathbb{A}) = Q \cap K$ ya que $Q \subset \mathbb{A}$. Finalmente, para demostrar (3)⇒(4), observamos que $Q \cap \mathcal{O}_K$ contiene a P y es obviamente un ideal de $\mathcal{O}_K$; como P es primo, es maximal y tenemos que $Q \cap \mathcal{O}_K = P$ ó $\mathcal{O}_K$. Si $Q \cap \mathcal{O}_K = \mathcal{O}_K$, entonces $1 \in Q$, que es un contradicción ya que Q es primo. □

Cuando los condiciones (1) a (5) se cumplen, decimos que Q **está sobre** P, o P **está bajo** Q.

Teorema 2.15. *Cada primo Q de $\mathcal{O}_L$ está sobre un único primo P de $\mathcal{O}_K$; cada primo P de $\mathcal{O}_K$ está bajo al menos un primo Q de $\mathcal{O}_L$.*

Demostración. Para la primera parte, es suficiente demostrar que $Q \cap \mathcal{O}_K$ es primo en $\mathcal{O}_K$. $Q \cap \mathcal{O}_K$ es obviamente un ideal en $\mathcal{O}_K$ ya que Q es ideal en $\mathcal{O}_L$. Si $ab \in Q \cap \mathcal{O}_K$ con $a, b \in \mathcal{O}_K$ entonces uno de los elementos a, b (digamos a) está en Q, pero como $a \in \mathcal{O}_K$, $a \in Q \cap \mathcal{O}_K$. Como $1 \notin Q$ tenemos que $1 \notin Q \cap \mathcal{O}_K$, entonces $Q \cap \mathcal{O}_K$ es maximal, si no es (0). Como Q es maximal, $Q \neq (0)$. Por la condicion (5) es suficiente demostrar que $K \cap Q \neq (0)$. Sea $\alpha \in Q - (0)$; entonces $N(\alpha) \in \mathbb{Z}$, $N(\alpha) \neq 0$, y como $\mathbb{Z} \subset Q$, $N(\alpha) \in Q$. Como $\mathbb{Z} \subset K$, $N(\alpha) \in K \cap Q$.

Para la segunda parte, los primos sobre P son los divisores primos de $P\mathcal{O}_L$; entonces tenemos que demostrar que $P\mathcal{O}_L \neq \mathcal{O}_L$, para que tenga al menos un divisor primo. Es suficiente demostrar que $1 \notin P\mathcal{O}_L$. Usando el lema 2.5 existe $\gamma \in K - \mathcal{O}_K$ tal que $\gamma P \subset \mathcal{O}_K$. Entonces $\gamma P\mathcal{O}_L \subset \mathcal{O}_K\mathcal{O}_L = \mathcal{O}_L$. Si $1 \in P\mathcal{O}_L$, entonces $\gamma \in \mathcal{O}_L$, pero entonces $\gamma \in \mathcal{O}_K$, una contradicción. □

Los primos sobre un primo dado P son aquellos que están en la descomposición en primos de $P\mathcal{O}_L$. Las potencias en que ocurren son llamadas **índices de ramificación**. Esto es, si Q^e es la potencia exacta de Q que divide a $P\mathcal{O}_L$, entonces e es el índice de ramificación de Q sobre P, denotado por $e(Q|P)$.

Hay otro número importante asociado con un par de primos P y Q, con Q sobre P. Sabemos que los anillos $\mathcal{O}_K/P$ y $\mathcal{O}_L/Q$ son campos ya que P y Q son maximales. Podemos ver $\mathcal{O}_K/P$ como subcampo de $\mathcal{O}_L/Q$: la inclusión $\mathcal{O}_K \subset \mathcal{O}_L$ induce un morfismo de anillos $\mathcal{O}_K \to \mathcal{O}_L/Q$ con núcleo $\mathcal{O}_K \cap Q = P$. Entonces tenemos un encaje $\mathcal{O}_K/P \to \mathcal{O}_L/Q$. Estos son llamados los **campos residuales** asociados con P y Q. Sabemos que son campos finitos gracias a la proposición 2.1. Por lo cual $\mathcal{O}_L/Q$ es una extensión finita de $\mathcal{O}_K/P$; sea f el grado de esta extensión. Entonces f se llama el **grado de inercia** de Q sobre P y lo denotamos por $f(Q|P)$.

Lema 2.16. *Sean A y B dos ideales en un dominio de Dedekind R, con $B \subset A$ y $A \neq R$. Entonces existe $\gamma \in K$ tal que $\gamma B \subset R$, $\gamma B \not\subseteq A$.*

Demostración. Por el teorema 2.3 existe un ideal C no cero tal que BC es principal, digamos que $BC = (\alpha)$. Entonces $BC \not\subseteq \alpha A$; fijamos $\beta \in C$ tal que

$\beta B \not\subseteq \alpha A$ y sea $\gamma = \frac{\beta}{\alpha}$. □

Teorema 2.17. *Sea n el grado de L sobre K y sean $Q_1, \ldots, Q_r$ los primos de $\mathcal{O}_L$ sobre el ideal primo P de $\mathcal{O}_K$. Sean $e_1, \ldots, e_r$ y $f_1, \ldots, f_r$ los índices de ramificación y los grados de inercia, respectivamente. Entonces:*

$$\sum_{i=1}^{r} e_i f_i = n.$$

Vamos a demostrar este teorema simultaneamente con otro. Para un $\mathcal{O}_K$-ideal I escribimos

$$\|I\| \text{ para denotar } |\mathcal{O}_K/I|.$$

Teorema 2.18. *Sean $\mathcal{O}_K$,$\mathcal{O}_L$,K y L como antes y $n = [L : K]$.*
(a) Para ideales I y J en $\mathcal{O}_K$,

$$\|IJ\| = \|I\|\|J\|.$$

(b) Sea I un ideal en $\mathcal{O}_K$. Para el $\mathcal{O}_L$-ideal $I\mathcal{O}_L$,

$$\|I\mathcal{O}_L\| = \|I\|^n.$$

(c) Sea $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$. Para el ideal principal (α).

$$\|(\alpha)\| = |N^K(\alpha)|.$$

Demostración. Demostración de teorema 2.18 (a)

Primero lo hacemos cuando I y J son coprimos y después demostraremos que $\|P^m\| = \|P\|^m$ para todo primo P. Entonces esto va a implicar que

$$\|P_1^{m_1} \ldots P_r^{m_r}\| = \|P_1\|^{m_1} \ldots \|P_r\|^{m_r};$$

factorizando I y J en primos y aplicando la formula de arriba obtenemos 2.18 (a).

Supongamos, pues, que I y J son coprimos. Entonces $I + J = \mathcal{O}_K$ e $I \cap J = IJ$. Por el teorema Chino hay un isomorfismo

$$\mathcal{O}_K/IJ \to \mathcal{O}_K/I \times \mathcal{O}_K/J,$$

lo que implica

$$\|IJ\| = \|I\|\|J\|.$$

Ahora consideramos $\|P^m\|$, P un ideal primo. Tenemos una cadena descendente de ideales $\mathcal{O}_K \supset P \supset P^2 \supset \cdots \supset P^m$. Entonces sería suficiente demostrar que, para cada k,

$$\|P\| = |P^k/P^{k+1}|$$

donde los P^k son considerados como grupos aditivos. Afirmamos que hay un isomorfismo de grupos

$$\mathcal{O}_K/P \to P^k/P^{k+1}.$$

Primero, fijando $\alpha \in P^k - P^{k+1}$, tenemos el isomorfismo canónico

$$\mathcal{O}_K/P \to \alpha\mathcal{O}_K/\alpha P.$$

Ahora, la inclusión $\alpha\mathcal{O}_K \subset P^k$ induce el morfismo

$$\alpha\mathcal{O}_K \to P^k/P^{k+1}$$

con núcleo $(\alpha\mathcal{O}_K) \cap P^{k+1}$ e imagen $((\alpha\mathcal{O}_K) + P^{k+1})/P^{k+1}$. Para demostrar lo que queremos (por el primer teorema de isomorfismo) hay que demostrar que $(\alpha\mathcal{O}_K) \cap P^{k+1} = \alpha P$ y $(\alpha\mathcal{O}_K) + P^{k+1} = P^k$. Para esto usamos el mcd y mcm. Tenemos que $\alpha P \subset \alpha\mathcal{O}_K$ y $\alpha P \subset P^{k+1}$ entonces $\alpha P \subset \alpha\mathcal{O}_K \cap P^{k+1}$, si la contención es propia, $P \subset \frac{1}{\alpha}J$ propiamente donde $J = \alpha\mathcal{O}_K \cap P^{k+1}$. Pero P es maximal, entonces $\frac{1}{\alpha}J = \mathcal{O}_K$, i.e $J = (\alpha)$, pero esto es una contradicción ya que $\alpha \notin P^{k+1}$. Obviamente el $mcd(\alpha\mathcal{O}_K, P^{k+1})$ es un potencia de P, notamos que $P^k | P^{k+1}$ y como $\alpha \in P^k$, $P^k | \alpha\mathcal{O}_K$. Si $mcd(\alpha\mathcal{O}_K, P^{k+1}) = P^{k+1}$ entonces $(\alpha\mathcal{O}_K) \subset P^{k+1}$ entonces $\alpha \in P^{k+1}$ una contradicción. □

Demostración. Caso especial del teorema 2.17:

El caso cuando $K = \mathbb{Q}$. Entonces $P = p\mathbb{Z}$ para algún primo $p \in \mathbb{Z}$. Tenemos

$$p\mathbb{Z}\mathcal{O}_L = p\mathcal{O}_L = \prod_{i=1}^{r} Q_i^{e_i},$$

entonces

$$\|p\mathcal{O}_L\| = \prod_{i=1}^{r} \|Q_i\|^{e_i} = \prod_{i=1}^{r} (p^{f_i})^{e_i}.$$

Ya que $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ que tiene p elementos y el grado de la extensión es f_i.

También sabemos que $\|p\mathcal{O}_L\| = p^n$, ya que la extensión es de grado n. Por lo tanto tenemos el caso especial. □

Demostración. del teorema 2.18 (b):

Usando la parte (a), es suficiente demostrar el caso cuando I es un primo P; el caso general se sigue factorizando I en primos.

Notamos que $\mathcal{O}_L/P\mathcal{O}_L$ es un anillo que contiene $\mathcal{O}_K/P$ ya que $\mathcal{O}_K \subset \mathcal{O}_L$. Entonces existe un morfismo $\mathcal{O}_K \to \mathcal{O}_L/P\mathcal{O}_L$ con núcleo $\mathcal{O}_K \cap P\mathcal{O}_L$, pero $\mathcal{O}_K \cap P\mathcal{O}_L = P$ ya que $P \subset \mathcal{O}_K$ y $P \subset P\mathcal{O}_L$ y por el teorema 2.14 para cualquier primo Q que divida a $P\mathcal{O}_L$, $P\mathcal{O}_L \subset Q$, entonces $\mathcal{O}_K \cap P\mathcal{O}_L \subset \mathcal{O}_K \cap Q = P$ finalmente, $\mathcal{O}_K \cap P\mathcal{O}_L = P$. Afirmamos que la dimensión de $\mathcal{O}_L/P\mathcal{O}_L$ sobre $\mathcal{O}_K/P$ es n.

Primero demostramos que a los más es n. Es suficiente demostrar que cualquier $n+1$ elementos son linealmente dependientes. Fijamos $\alpha_1, \ldots, \alpha_{n+1} \in \mathcal{O}_L$ y demostramos que los elementos correspondientes en $\mathcal{O}_L/P\mathcal{O}_L$ son linealmente dependientes sobre $\mathcal{O}_K/P$. Sabemos que $\alpha_1, \ldots, \alpha_{n+1}$ son linealmente dependientes sobre K (extensión de grado n), entonces son linealmente dependientes sobre $\mathcal{O}_K$. Entonces tenemos $\beta_1\alpha_1 + \cdots + \beta_{n+1}\alpha_{n+1} = 0$ para algunos $\beta_1, \ldots, \beta_{n+1} \in \mathcal{O}_K$, no todos 0. Si existe i tal que $\beta_i \notin P$ ya terminamos, en caso contrario aplicamos el lema 2.16 con $A = P$ y $B = (\beta_1, \ldots, \beta_{n+1})$. Entonces $\gamma\beta_i$ cumplen.

Para tener igualdad, sea $P \cap \mathbb{Z} = p\mathbb{Z}$ y consideramos todos los primos P_i de $\mathcal{O}_K$ que están sobre $p\mathbb{Z}$. Sabemos que $\mathcal{O}_L/P_i\mathcal{O}_L$ es espacio vectorial sobre $\mathcal{O}_K/P_i$ de dimensioón $n_i \leq n$; demostramos que son iguales para cada i, en particular cuando $P_i = P$. Sea $e_i = e(P_i|p)$ y $f_i = f(P_i|p)$. Entonces $\sum e_i f_i = m$, donde m es el grado de K sobre $\mathbb{Q}$ por el caso especial. Tenemos $p\mathcal{O}_K = \prod P_i^{e_i}$, entonces $p\mathcal{O}_L = \prod (P_i\mathcal{O}_L)^{e_i}$. Usando (a), obtenemos

$$\|p\mathcal{O}_L\| = \prod \|P_i\mathcal{O}_L\|^{e_i} = \prod \|P_i\|^{n_i e_i} = \prod (p^{f_i})^{n_i e_i}.$$

Sabemos también por el caso especial que $\|p\mathcal{O}_L\| = p^{rnn}$, entonces $mn = \sum f_i n_i e_i$. Como todo $n_i \leq n$ y $\sum e_i f_i = m$, se sigue que $n_i = n$ para todo i. □

Demostración. Caso general del teorema 2.17

Tenemos $P\mathcal{O}_L = \prod Q_i^{e_i}$, entonces

$$\|P\mathcal{O}_L\| = \prod \|Q_i\|^{e_i} = \prod \|P\|^{f_i e_i}$$

por (a) y la definición de f_i. Por (b) sabemos que $\|P\mathcal{O}_L\| = \|P\|^n$. Entonces $n = \sum e_i f_i$. □

Demostración. Parte (c)

Extendemos K a un extensión normal M de $\mathbb{Q}$ y sea $\mathcal{O}_M = \mathbb{A} \cap M$. Para cada encaje σ de K en $\mathbb{C}$, tenemos

$$\|\sigma(\alpha)\mathcal{O}_M\| = \|\alpha\mathcal{O}_M\|;$$

ya que extendemos σ a un automorfismo de M y observamos que $\sigma(\mathcal{O}_M) = \mathcal{O}_M$. Sea $N = N^K(\alpha)$. Entonces por (a) tenemos

$$\|N\mathcal{O}_M\| = \prod_\sigma \|\sigma(\alpha)\mathcal{O}_M\| = \|\alpha\mathcal{O}_M\|^n.$$

Como $\|N\mathcal{O}_T\| = |N|^{nm}$, donde $m = [M : K]$ y por (b) $\|\alpha\mathcal{O}_T\| = \|\alpha\mathcal{O}_K\|^m$, obetenemos $\|\alpha\mathcal{O}_K\| = |N|$. □

Capítulo 3

Clases de ideales

Teorema 3.1. *Sean K un campo numérico y $\mathbb{A} \cap K = \mathcal{O}_K$. Entonces existe un número real positivo λ (que depende de K) tal que cada ideal no cero I de $\mathcal{O}_K$ contiene un elemento no cero α con*

$$|N^K(\alpha)| \leq \lambda \|I\|.$$

Demostración. Fijamos una base entera $\alpha_1, \ldots, \alpha_n$ para $\mathcal{O}_K$ y sean $\sigma_1, \ldots, \sigma_n$ los encajes de K en $\mathbb{C}$. Afirmamos que podemos tomar λ como

$$\prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i \alpha_j|.$$

Para cualquier ideal I, sea m el único natural tal que

$$m^n \leq \|I\| < (m+1)^n$$

y consideramos los $(m+1)^n$ elementos de $\mathcal{O}_K$

$$\sum_{j=1}^{n} m_j \alpha_j, m_j \in \mathbb{Z}, 0 \leq m_j \leq m.$$

Dos de estos deben ser congruentes *mod* I ya que hay más de $\|I\|$ de ellos; tomando la diferencia de estos dos elementos, obtenemos un elemento no cero de I que tiene la forma

$$\alpha = \sum_{j=1}^{n} m_j \alpha_j, m_j \in \mathbb{Z}, |m_j| \leq m.$$

Finalmente, tenemos

$$|N^K(\alpha)| = \prod_{i=1}^{n} |\sigma_i \alpha| \leq \prod_{i=1}^{n} \sum_{j=1}^{n} |m_j||\sigma_i \alpha_j| \leq m^n \lambda \leq \|I\|\lambda.$$

□

Corolario 3.2. *Cada clase de ideales de $\mathcal{O}_K$ contiene un ideal J con $\|J\| \leq \lambda$, λ como en el teorema 3.1.*

Demostración. Dada un clase de ideales C, consideramos la clase inversa C^{-1} y fijamos cualquier ideal $I \in C^{-1}$. Obtenemos $\alpha \in I$ como en el teorema 3.1. I contiene el ideal principal (α), i.e. $I|(\alpha)$, entonces $(\alpha) = IJ$ para algún ideal $J \in C$. Finalmente usando teorema 2.18 tenemos que

$$\|I\|\|J\| = \|(\alpha)\| = |N^K(\alpha)| \leq \|I\|\lambda.$$

□

Corolario 3.3. *Hay un número fininto de clases de ideales.*

Demostración. Solamente hay un número finito de ideales J que satisfacen $\|J\| \leq \lambda$ porque la disigualdad restringe a un número finito de posibles divisores primos de J y sus potencias. (Si $J = \prod P_i^{n_i}$, entonces $\|J\| = \prod \|P_i\|^{n_i}$.)

□

Lema 3.4. *Un ideal I no cero de $\mathcal{O}_K$ es principal, sii existe un elemento $\alpha \in I$, no cero tal que $|N(\alpha)| = |\mathcal{O}_K/I| = \|I\|$.*

Demostración. Sea $\alpha \in I$, no cero. Entonces $\alpha\mathcal{O}_K \subset I$ y existe un ideal no cero J tal que $IJ = (\alpha)$. Ahora $|\mathcal{O}_K/I| = |\mathcal{O}_K/(\alpha)|$ es equivalente a $|\mathcal{O}_K/J| = 1$, lo cual pasa sii $J = \mathcal{O}_K$. □

Teorema 3.5. *Sean K un campo numérico y I un ideal en $\mathcal{O}_K$. Entonces existe un natural k tal que I^k es principal.*

Demostración. Directamente de que las clases forman un grupo finito. □

Proposición 3.6. *Dado un anillo numérico $\mathcal{O}_K$, siempre existe una extension finita L de K donde todos los ideales de $\mathcal{O}_K$ son principales.*

Demostración. Es suficiente demostrar que subiendo un ideal principal llegamos a un ideal principal, que si dos ideales están relacionados en $\mathcal{O}_K$, están relacionados en $\mathcal{O}_L$, y que para un ideal I en $\mathcal{O}_K$ existe una extensión finita $K \subset L$ tal que $I\mathcal{O}_L$ es principal. Si $\alpha I = \beta J$ entonces subiendolos $\alpha I\mathcal{O}_L = \beta J\mathcal{O}_L$. Si I es principal, digamos $I = (\alpha)$ entonces $I\mathcal{O}_L = (\alpha)\mathcal{O}_L$ el cual es principal. Sea $m \in \mathbb{N}$ tal que $I^m = \alpha\mathcal{O}_K$. Afirmamos que $K(\alpha^{\frac{1}{m}})$ funciona. $(I\mathcal{O}_L)^m = I^m\mathcal{O}_L = \alpha\mathcal{O}_K\mathcal{O}_L = \alpha\mathcal{O}_L = (\alpha^{\frac{1}{m}}\mathcal{O}_L)^m$ y tenemos la última parte. □

Proposición 3.7. *Sea (a,b) un ideal en $\mathcal{O}_K$, entonces (a,b) es principal sii existen $x, y \in \mathcal{O}_K$, tales que $\frac{a}{b} = \frac{x}{y}$ y $(x,y) = \mathcal{O}_K$.*

Demostración. Sea $(a,b) = (d)$ y $a = dx$, $b = dy$ y supongamos que $(x,y) \neq \mathcal{O}_K$. Entonces hay un primo P que divide a (x,y), i.e $P|(x)$ y $P|(y)$. Entonces $(d)P|(dx)$ y $(d)P|(dy)$, lo cual implica que $(d)P|(a) + (b) = (a,b) = (d)$ entonces $P|(1)$ lo cual es una contradicción, ya que P era primo.

Si para el ideal (a,b) existen $x, y \in \mathcal{O}_K$ tales que $\frac{a}{b} = \frac{x}{y}$ y $(x,y) = \mathcal{O}_K$ entonces excribimos $1 = xr_1 + yr_2$ y afirmamos que $(a,b) = (ar_1 + br_2)$. Sabemos que $bx = ay$ y $a = axr_1 + ayr_2$ entonces $a = axr_1 + bxr_2 = x(ar_1 + br_2)$ y $b = bxr_1 + byr_2$ entonces $b = ayr_1 + byr_2 = y(ar_1 + br_2)$ entonces $a, b \in (ar_1 + br_2)$ y trivialmente $(ar_1 + br_2) \subset (a,b)$. □

Definición 3.1. *Decimos que un polinomio $f(x) \in \overline{\mathbb{Q}}[x]$ está definido sobre K sii todos los coeficientes de $f(x)$ están en K.*

Definición 3.2. *Sea $f(x) \in \mathbb{A}[x]$ y sea K un campo numérico sobre el cual $f(x)$ está definido. Sea $\mathcal{O}_K$ el anillo de enteros de K. Definimos el* ***contenido*** *de $f(x)$ en K como el ideal generado en $\mathcal{O}_K$ por los coeficientes de $f(x)$. Decimos que $f(x)$ es* ***primitivo*** *en K si el contenido de $f(x)$ es $\mathcal{O}_K$.*

El contenido de un polinomio obviamente depende de K, puesto que es un ideal del anillo de enteros de K; sin embargo, la propiedad de ser primitivo no depende de K:

Lema 3.8. *Sea $f(x) \in \mathbb{A}[x]$ y sean K y K' dos campos numéricos sobre los cuales $f(x)$ está definido. Entonces $f(x)$ es primitivo en K sii es primitivo en K'.*

Demostración. Fijando en el compositum de K y K', es suficiente demostrarlo cuando $K \subset K'$.

Si $f(x)$ no es primitivo en K, entonces hay un ideal primo P de $\mathcal{O}_K$ tal que cada coeficiente de $f(x)$ está en P; para ver esto, sea I el contenido de $f(x)$ y lo factorizamos en primos

$$I = P_1 \dots P_n.$$

Entonces cualquier P_i contiene a I. Sea Q un primo de $\mathcal{O}_{K'}$ que está sobre P. Entonces cada coeficiente de $f(x)$, cuando $f(x)$ es considerado como polinomio en $\mathcal{O}_{K'}[x]$, está en Q, entonces el contenido de $f(x)$ en K' no es $\mathcal{O}_{K'}$, ya que Q lo divide.

Si $f(x)$ no es primitivo en K', entonces hay un ideal primo Q de $\mathcal{O}_{K'}$ tal que cada coeficiente de $f(x)$ está en Q. Sea $P = Q \cap K$. Como $f(x)$ está definido sobre K, los coeficientes de $f(x)$ están en P, entonces $f(x)$ no es primitivo. □

Por el lema 3.8 simplemente decimos que $f(x)$ es primitivo para decir que está en $\mathbb{A}[x]$ y es primitivo en cualquier campo numérico K en el cual está definido.

Teorema 3.9. ***Lema de Gauss***
El producto de dos polinomios primitivos es primitivo.

Demostración. Sean $f(x), g(x) \in \mathbb{A}[x]$ dos polinomios primitivos y sea K cualquier campo numérico sobre el cual están definidos. Escribimos

$$f(x) = \sum a_i x^i; g(x) = \sum b_j x^j; f(x)g(x) = \sum c_k x^k.$$

Supongamos que todos los c_k están en un primo P de $\mathcal{O}_K$. Como $f(x)$ es primitivo, hay un índice i tal que $a_i \notin P$; y un j con $b_j \notin P$. Sea i_o el primer índice tal que $a_{i_o} \notin P$ y sea j_o el primer índice tal que $b_{j_o} \notin P$. Consideramos $c_{i_o+j_o}$. Tenemos que $c_{i_o+j_o}$ es:

$$a_o b_{i_o+j_o} + \cdots + a_{i_o-1} b_{j_o+1} + a_{i_o} b_{j_o} + a_{i_o+1} b_{j_o-1} + \cdots + a_{i_o+j_o} b_o.$$

Todos los términos en el lado derecho, excepto por $a_{i_o} b_{j_o}$, están en P, igual que $c_{i_o+j_o}$. Esta contradicción demuestra que $f(x)g(x)$ es primitivo también. □

Teorema 3.10. *Sea $f(x) \in \overline{\mathbb{Q}}[x]$ un polinomio no cero y sea K un campo numérico sobre el cual $f(x)$ está definido. Entonces existe una extensión finita L de K tal que*

$$f(x) = c_f f^*(x)$$

donde c_f es una constante de L y $f^*(x)$ es un polinomio primitivo con coeficientes en L. Más aún, c_f y $f^*(x)$ son únicos salvo unidades de $\mathcal{O}_L$.

Demostración. Escribimos $f(x)$ como:

$$f(x) = \frac{a_n}{b_n} x^n + \cdots + \frac{a_o}{b_o}$$

con cada $a_i, b_i \in \mathcal{O}_K$. Para cada i, tomamos una extensión finita K_i de K si es necesario, para que el ideal (a_i, b_i) sea principal, generado por un entero algebraico c_i. Entonces existen enteros algebraicos r_i, s_i tales que $a_i = c_i r_i$,

$b_i = c_i s_i$, con $(r_i, s_i) = \mathcal{O}_{K_i}$. Haciendo esto para cada i y tomando el compositum de todo K_i, obtenemos una extensión finita K' de K, donde podemos escribir

$$f(x) = \frac{r_n}{s_n}x^n + \cdots + \frac{r_o}{s_o},$$

con $r_i, s_i \in \mathcal{O}_{K_i}$ y $(r_i, s_i) = \mathcal{O}_{K_i}$ para cada i.

Sea $c = \frac{1}{s_o s_1 \ldots s_n}$. Entonces existe un polinomio $g(x) \in \mathcal{O}_{K'}[x]$ tal que $f(x) = cg(x)$.

El contenido de $g(x)$ es un ideal de $\mathcal{O}_{K'}$; entonces existe un extensión finita L de K' (entonces L es una extensión finita de K), donde el contenido de $g(x)$ es principal, generado por algún entero algebraico c'. Ahora sea $f^*(x) = \frac{1}{c'}g(x)$. f^* es primitivo, con coeficientes en $\mathcal{O}_L$. Ahora tenemos

$$f(x) = cg(x) = (cc')f^*(x).$$

Si definimos $c_f = cc'$ ya tenemos existencia.

Aquí notamos que si $f(x) \in \mathbb{A}[x]$, entonces $c = 1$ y en consecuencia $c_f \in \mathbb{A}$.

Para demostrar unicidad salvo unidades en $\mathcal{O}_L$, es suficiente demostrar que $f^*(x)$ es único salvo unidades en $\mathcal{O}_L$. Entonces supongamos que $f^*(x) = cg^*(x)$, donde $c \in L$ y $g^*(x) \in \mathcal{O}_L[x]$ es primitivo. Escribimos $c = \frac{u}{v}$ con $u, v \in \mathcal{O}_L$; tomando una extensión finita de L si es necesario, supongamos que u, v son coprimos. Entonces $ug^*(x) = vf^*(x)$; si u no es unidad, entonces existe un idea primo P que contiene a u, entonces contiene todos los coeficientes de $ug^*(x)$; pero como u, v son coprimos y cada coeficiente de $vf^*(x)$ está en P (ya que los contenidos son iguales), se sigue que cada coeficiente de $f^*(x)$ está en P, entonces $f^*(x)$ no es primitivo, una contradicción. Una argumento simétrico demuestra que v es unidad en la extensión. Entonces c es unidad en $\mathbb{A}$. Pero $\frac{1}{c}$ está en L, entonces $\frac{1}{c}$ está en $\mathcal{O}_L$, entonces es unidad en $\mathcal{O}_L$ □

Teorema 3.11. *Sea K un campo numérico y sean $f(x), g(x) \in \mathcal{O}_K[x]$. Entonces el contenido de $f(x)g(x)$ en K es el producto de los contenidos de $f(x)$ en K y $g(x)$ en K.*

Demostración. Por el teorema 3.10, hay una extensión K' de K donde podemos escribir $f(x) = c_f f^*(x)$ y $g(x) = c_g g^*(x)$, con $f^*(x)$ y $g^*(x)$ primitivos. Su productos es $c_f c_g f^*(x) g^*(x)$ y por el lema de Gauss, $f^*(x)g^*(x)$ es primitivo; entonces el contenido de $f(x)g(x)$ en K' es el ideal $(c_f c_g)$. Como (c_f) es el contenido de $f(x)$ y (c_g), $(c_f, c_g \in \mathbb{A})$ es el contenido de $g(x)$ en K', tenemos en K', que el contenido del producto es el producto de los contenidos. Ahora intersectando los ideales con $\mathcal{O}_K$ nos da el resultado en K. □

Teorema 3.12. *Sea K un campo numérico y sea $f(x) \in \mathcal{O}_K[x]$. Si es posible factorizar $f(x)$ en un producto de polinomios con coeficientes en K, entonces existe una extensión finita L de K tal que $f(x)$ se puede factorizar en un producto de polinomios del mismo grado como en la factorizacion original, con coeficientes en $\mathcal{O}_L$.*

Demostración. Escribimos $f(x)=g(x)h(x)$, con $g(x), h(x) \in K[x]$. Por teorema el 3.10, existe una extensión finita L de K donde podemos escribir

$$f(x) = c_f f^*(x) = c_g g^*(x) c_h h^*(x),$$

con $c_f, c_g, c_h \in L$, $f^*(x), g^*(x), h^*(x) \in \mathcal{O}_L[x]$ primitivos. Por la lema de Gauss, $g^*(x)h^*(x)$ es primitivo también. Por unicidad de la descomposición en primos , tenemos

$$c_f = u c_g c_h; f^*(x) = v g^*(x) h^*(x)$$

donde u, y v son unidades en $\mathcal{O}_L$. En particular, $c_g c_h \in \mathcal{O}_L$. Entonces $f(x)$ está escrito como producto de dos polinomios con coeficientes enteros algebraicos, a saber $c_g c_h g^*(x)$ y $h^*(x)$, que son de los mismos grados que $g(x)$ y $h(x)$respectivamente. □

Corolario 3.13. *Cada polinomio no constante $f(x) \in \mathbb{A}[x]$ se puede factorizar en un producto de factores lineales(no necesariamente mónicos), cada uno con coeficientes enteros algebraicos.*

Demostración. Sea $f(x) \in \mathbb{A}[x]$. Sea K el campo de descomposición de $f(x)$. Entonces en K, $f(x)$ se puede escribir como producto de términos lineales, cada uno con coeficientes en K. Como $f(x)$ tiene coeficientes enteros algebraicos, aplicamos el teorema 3.12 a esta descomposición, para obtener una extensión finita L de K donde es posible escribir a $f(x)$ como producto de polinomios de grado 1, cada uno con coeficientes enteros algebraicos. □

Corolario 3.14. *Cada polinomio $f(x) \in \mathbb{Z}[x]$ se puede factorizar en un producto de factores lineales (no necesariamente mónicos), cada uno con coeficientes enteros algebraicos.*

Demostración. Directamente del corolario 3.13. □

Lema 3.15. *Sea $Ax^2 + Bx + C$ con $A, B, C \in \mathbb{Z}$ y si factorizamos esto en su campo de descomposición en $A(x - r_1)(x - r_2)$ con r_1, r_2 las raíces, $r_1 = \frac{-B+\sqrt{B^2-4AC}}{2A}$ y $r_1 = \frac{-B-\sqrt{B^2-4AC}}{2A}$. Si tenemos $(B^2 - 4AC, 2A)$ principal y quitamos los denominadores, los polinomios que queden son primitivos y el constante es unidad.*

Demostración. Directamente del corolario 3.14, el teorema 3.10 y la proposición 3.7 ya que $(A, B, C) = 1$. □

Teorema 3.16. *Sea $f(x) \in \mathbb{A}[x]$ un polinomio primitivo. Si*

$$f(x) = g_1(x) \dots g_n(x) = h_1(x) \dots h_n(x),$$

donde cada $g_i(x), h_j(x) \in \mathbb{A}[x]$ es un polinomio de grado 1, entonces, salvo un reordenamiento de los $h_j(x)$, existen unidades $u_1, \dots, u_n \in \mathbb{A}$ tales que $\prod u_i = 1$ y $u_i h_i(x) = g_i(x)$. En particular, cada u_i es unidad de $\mathcal{O}_K$ para cualquier campo numérico K que lo contiene.

Demostración. Sea K un campo numérico sobre el cual cada $g_i(x)$ y cada $h_j(x)$ está definido.

Como el producto de los contenidos de los $g_i(x)$ es igual al contenido de $f(x)$, se sigue que cada $g_i(x)$ es primitivo. El mismo argumento funciona para cada $h_j(x)$.

Sean $r_1, \ldots, r_n \in \overline{\mathbb{Q}}$ los raíces de $f(x)$, contando multiplicidad, tomados en un orden fijo y supongamos que los $g_i(x)$ y $h_j(x)$ son ordenados de tal forma que r_i es la única raíz de $g_i(x)$ y de $h_i(x)$ para cada i, $1 \leq i \leq n$.

Fijamos un índice i. Escribimos $g_i(x) = ax + b$, $h_i(x) = cx + d$, con $a, b, c, d \in \mathcal{O}_K$, $ac \neq 0$. Como cada uno es primitivo, se sigue que los ideales (a, b) y (c, d) son el ideal trivial $\mathcal{O}_K$.

Como r_i es raíz de ambos $g_i(x)$ y $h_i(x)$, se sigue que existe un elemento $u_i \in K$ tal que $g_i(x) = u_i h_i(x)$. Tomando una extensión de K si es necesario, podemos escribir $u_i = \frac{v_i}{w_i}$, con v_i y w_i enteros algebraicos y (v_i, w_i) el ideal trivial. Entonces, $w_i g_i(x) = v_i h_i(x)$, entonces $w_i(a, b) = v_i(c, d)$. Como ambos (a, b) y (c, d) son el ideal trivial y (w_i) y (v_i) son coprimos, por factorizacion única los dos son el ideal trivial, entonces w_i, v_i son enteros algebraicos, entonces también lo es u_i.

Una substitución y cancelación demuestra que $\prod u_i = 1$. □

Teorema 3.17. *Sea $f(x) \in \mathbb{A}[x]$ un polinomio primitivo y sea*

$$f(x) = h_1(x) \ldots h_n(x)$$

una factorización lineal de $f(x)$, tal que cada factor tiene coeficientes enteros algebraicos. Entonces para cada factorización

$$c_f f(x) = g_1(x) \ldots g_n(x),$$

donde cada $g_i(x)$ es un polinomio lineal con coeficientes enteros algebraicos, salvo un reordenamiento de los $h_j(x)$, existen enteros algebraicos $c_1, \ldots, c_n$ tales que:

$$g_i(x) = c_i h_i(x),$$

y

$$(c_f) = (\prod c_i).$$

Demostración. Supongamos que tenemos

$$c_f f(x) = g_1(x) \dots g_n(x).$$

Ponemos en correspondencia cada $g_i(x)$ con un $h_i(x)$ (después de reordenar los $h_i(x)$ si es necesario) tal que $g_i(x)$ y $h_i(x)$ tienen la misma raíz, como en el teorema 3.16 . Hay un entero algebraico c_i, tal que $g_i(x) = c_i h_i(x)$. Entonces

$$c_f f(x) = g_1(x) \dots g_n(x) = (\prod_{i=1}^{n} c_i) h_1(x) \dots h_n(x)$$

y como los h_i son primitivos, el contenido del lado derecho es generado por $\prod c_i$. Entonces, c_f y $\prod c_i$ son asociados. □

Capítulo 4

Un algoritmo

El problema, que me planteó Arturo Magidin es:

Problema:
Dado un polinomio $f(x) \in \mathbb{Z}[x]$ tal que $f(x) = Ax^2+Bx+C$, $(A, B, C) = 1$, $A > 1$, da un algoritmo para factorizar $f(x)$ en un producto de dos polinomios lineales con coeficientes enteros algebraicos.

Notamos que tal factorización existe gracias al corolario 3.14.
Tenemos:

$$Ax^2 + Bx + C = (\alpha_1 x + \beta_1)(\alpha_2 x + \beta_2)$$

y esto implica que:

$$A = \alpha_1\alpha_2,\ B = \alpha_1\beta_2 + \alpha_2\beta_1,\ C = \beta_1\beta_2$$

Tenemos los casos especiales:

Caso 1: $B = 0$
Tenemos $Ax^2 + C = 0$, entonces $\alpha_1 = \alpha_2 = \sqrt{A}$, y $\beta_1 = \sqrt{-C}$ y $\beta_2 = -\sqrt{-C}$.

Caso 2: $C = 0$

Tenemos $(x)(Ax+B)=0$, entonces $\alpha_1=1$, $\alpha_2=A$, $\beta_1=0$ y $\beta_2=B$

Caso 3: $C=\pm 1$

Sin perdida de generalidad, supongamos que $C=1$. Entonces tenemos $Ax^2+Bx+1=0$, haciendo un cambio de variable, $y=\frac{1}{x}$, llegamos a $\frac{A}{y^2}+\frac{B}{y}+1=0$ ó $A+By+y^2=0$, el cual es un polinomio mónico con raíces en $\mathbb{A}$, i.e. sus raíces son números enteros algebraicos. Sean r_1, r_2 las raíces de $A+By+y^2$. Ahora $A+By+y^2=\frac{1}{x^2}+\frac{B}{x}+A=(\frac{1}{x}-r_1)(\frac{1}{x}-r_2)$, entonces $1+Bx+Ax^2=(1-r_1x)(1-r_2x)$.

Caso 4: $C|B$

Tenemos $f(x)=Ax^2+Bx+C=Ax^2+kCx+C$ para algún $k\in\mathbb{Z}$ tal que $B=kC$. Afirmamos que si r es raíz de $f(x)$, entonces $\frac{\sqrt{C}}{r}$ es un entero algebraico. Esto es porque si suponemos que $\frac{\sqrt{C}}{r}$ es raíz de x^2+Dx+E, entonces tenemos $\frac{C}{r^2}+D\frac{\sqrt{C}}{r}+E=0$, i.e. $C+D\sqrt{C}r+Er^2=0$. Entonces como tenemos que $r^2+k\frac{C}{A}r+\frac{C}{A}=0=r^2+\frac{D\sqrt{C}}{E}r+\frac{C}{E}$, llegamos a que:

$$E=A \text{ y } D=k\sqrt{C}$$

i.e. que $\frac{\sqrt{C}}{r}$ es raíz de $x^2+k\sqrt{C}x+A$. Sabemos que si $Z\in\mathbb{Z}$ y $\sqrt{Z}\in\mathbb{Q}$ entonces $\sqrt{Z}\in\mathbb{Z}$. Si $\sqrt{C}\in\mathbb{Q}$, entonces $\sqrt{C}\in\mathbb{Z}$ y en consecuencia $\frac{\sqrt{C}}{r}\in\mathbb{A}$. Por lo tanto supongamos que $\sqrt{C}\notin\mathbb{Q}$. Ahora multiplicamos $x^2+k\sqrt{C}x+A$ por un polinomio mónico x^2+Fx+G con coeficientes en $\mathbb{Q}(\sqrt{C})$ y supongamos que los coeficientes están en $\mathbb{Z}$, i.e que

$$F+k\sqrt{C}=Z_1$$

$$A+G+kF\sqrt{C}=Z_2$$

$$AF+kG\sqrt{C}=Z_3$$

$$AG=Z_4$$

donde $Z_i \in \mathbb{Z}$. Ahora $Z_3 = AF + kG\sqrt{C} = AF + k\sqrt{C}\frac{Z_4}{A}$ entonces $\sqrt{C}(\frac{Z_4}{A^2} - 1) = \frac{Z_3}{Ak} - \frac{Z_1}{k}$. Si $(\frac{Z_4}{A^2} - 1) \neq 0$ tenemos que $\sqrt{C} \in \mathbb{Q}$ que es una contradicción. Entonces $Z_4 = A^2$ y $G = A$. Ahora como $F = Z_1 - k\sqrt{C}$ tenemos $Z_2 = 2A + k\sqrt{C}(Z_1 - k\sqrt{C})$ y un argumento similar demuestra que $Z_1 = 0$. Obtenemos $F = -k\sqrt{C}$. Por lo que $x^2 + Fx + G = x^2 - k\sqrt{C}x + A$. Multiplicando llegamos a que $\frac{\sqrt{C}}{r}$ es raíz de $x^4 + (2A - k^2C)x^2 + A^2$, es decir, $\frac{\sqrt{C}}{r}$ es un entero algebraico. Como:

$$Ax^2 + Bx + C = (\alpha_1 x + \beta_1)(\alpha_2 x + \beta_2)$$

tenemos $r_1 = \frac{-\beta_1}{\alpha_1}$ y $r_2 = \frac{-\beta_2}{\alpha_2}$, i.e. que $\alpha_1 = \frac{-\beta_1}{r_1}$ y $\alpha_2 = \frac{-\beta_2}{r_2}$. Sean $\beta_1 = -\sqrt{C} = \beta_2$ y $\alpha_1 = \frac{-\sqrt{C}}{r} = \alpha_2$ y todos son enteros algebraicos. Entonces $Ax^2 + Bx + C = (\frac{-\sqrt{C}}{r_1}x - \sqrt{C})(\frac{-\sqrt{C}}{r_2}x - \sqrt{C})$.

Ejemplo:

Lo que sigue es un ejemplo donde llegamos a factorizar el polinomio en un paso (ver algoritmo) gracias a que $I = (-11 + \sqrt{21}, 10)$ es principal.

Consideramos el polinomio $f(x) = 5x^2 + 11x + 5$.

$$f(x) = 5\left[x - \frac{-11 + \sqrt{21}}{10}\right]\left[x - \frac{-11 - \sqrt{21}}{10}\right]$$

Ahora $(-11 + \sqrt{21}, 10) = (-1 + \sqrt{21})$. De hecho

$$(-1 + \sqrt{21})\left(\frac{1}{2} + \frac{\sqrt{21}}{2}\right) = 10$$

$$(-1 + \sqrt{21})\left(\frac{1}{2} - \frac{\sqrt{21}}{2}\right) = -11 + \sqrt{21}$$

y

$$-1 + \sqrt{21} = 1 \cdot (-11 + \sqrt{21}) + 1 \cdot 10$$

Además $(-11-\sqrt{21},10)=(-1-\sqrt{21})$ con

$$(-1-\sqrt{21})\left(\frac{1}{2}-\frac{\sqrt{21}}{2}\right)=10$$

$$(1+\sqrt{21})\left(-\frac{1}{2}-\frac{\sqrt{21}}{2}\right)=-11-\sqrt{21}$$

$$-1-\sqrt{21}=1\cdot(-11-\sqrt{21})+1\cdot 10$$

la factorización es:

$$\left[x\left(\frac{1}{2}+\frac{\sqrt{21}}{2}\right)-\left(\frac{1}{2}-\frac{\sqrt{21}}{2}\right)\right]\cdot \left[x\left(-\frac{1}{2}+\frac{\sqrt{21}}{2}\right)-\left(-\frac{1}{2}-\frac{\sqrt{21}}{2}\right)\right]$$

esto gracias el lema 3.15.

Siguen algunos lemas que usamos para justificar el algoritmo:

Lema 4.1. *Sea $K=\mathbb{Q}(\sqrt{m})$, donde m es un entero libre de cuadrados y sea $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ su anillo numérico con base entera $\{1,\frac{1+\sqrt{m}}{t}\}$ (sea $\alpha=\frac{1+\sqrt{m}}{t}$) donde $t=1$ o 2. Sea $I=(x,y)$ un ideal en $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$, escribimos $x,x\alpha,y,y\alpha$ como combinación lineal de la base entera $\{1,\frac{1+\sqrt{m}}{t}\}$ y escribimos la matriz corespondiente M. Reducimos M a su forma **hermitiana** H. Si hacemos las mismas operaciones a la matriz identidad que hicimos para obtener H de M llegamos a una matriz U tal que $H=MU$. Esto actua como cambio de base (ver demostración de lema 4.3) y nos da (ver lema 4.2) $\|I\|$.*

Demostración. Esto es posible gracias el teorema 2.6, pagina 179 de **Algorithmic Algebraic Number Theory** [P-Z]. □

Ahora vemos un ejemplo que ilustra el cambio de base descrito arriba.

Ejemplo:

Consideramos $\mathcal{O}_{\mathbb{Q}(\sqrt{-31})}$ que tiene base entera $\{1, \frac{1+\sqrt{-31}}{2}\}$. Sea $\alpha = \frac{1+\sqrt{-31}}{2}$. Sea $I = (10, -3+\sqrt{-31})$, queremos calcular una base entera de I.

Multiplicamos 10 y $-3+\sqrt{-31}$ por la base de $\mathcal{O}_{\mathbb{Q}(\sqrt{-31})}$ y escribimos los resultados como combinación lineal de la base de $\mathcal{O}_{\mathbb{Q}(\sqrt{-31})}$:

$$10 \cdot 1 = 10 \cdot 1 + 0 \cdot \alpha$$

$$10 \cdot \alpha = 0 \times 1 + 10 \cdot \alpha$$

$$(-3+\sqrt{-31}) \cdot 1 = -4 \cdot 1 + 2 \cdot \alpha$$

$$(-3+\sqrt{-31}) \cdot \alpha = -16 \cdot 1 - 2 \cdot \alpha$$

Tomando los coeficientes llegamos a la matriz:

$$M = \begin{pmatrix} 10 & 0 & -4 & -16 \\ 0 & 10 & 2 & -2 \end{pmatrix}$$

A M la reducimos a su forma hermitiana:

$$H = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 4 & 10 & 0 & 0 \end{pmatrix}$$

Entonces una base entera de I es $\{2+4\alpha, -10\alpha\}$. Esto además nos da $\|I\| = 20$, ya que el determinante de:

$$\begin{pmatrix} 2 & 0 \\ 4 & 10 \end{pmatrix}$$

es 20.

Si a la matriz identidad (4×4) hacemos las mismas operaciónes que le hicimos a M para obtener a H, llegamos a la matriz invertible:

$$U = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & -1 & 1 \\ 2 & 0 & 5 & -4 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

tal que $H = MU$. Esta es una matriz de cambio de base en el sentido de que nos da una base entera de I. Por ejemplo para escibir $2 + 4\alpha$, que tiene coeficientes $(1, 0, 0, 0) = v$ en términos del base de $\mathcal{O}_{\mathbb{Q}(\sqrt{-31})}$ multiplicamos Uv y obtenemos el vector $w = (1, 0, 2, 0)$. Para ver esto en detalle, ver página 398 [P-Z].

Lema 4.2. *Si $I = \{\alpha_1, \ldots, \alpha_r\}$ es un ideal de $\mathcal{O}_K$ y después llegamos a*

$$H = \begin{pmatrix} a & 0 & 0 & 0 & \ldots \\ b & c & 0 & 0 & \ldots \end{pmatrix}$$

la matriz hermitiana corespondiente, entonces $\|I\| = ac$.

Demostración. Dos elementos $x, y \in \mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ estan relacionados sii $x - y \in I$, esto es si $x = d + e(\frac{1+\sqrt{m}}{t})$ e $y = d' + e'(\frac{1+\sqrt{m}}{t})$ estan relacionados sii $a|(d-d')$ y $c|(e - e') - \frac{b(d-d')}{a}$. □

Lema 4.3. *$x \in \mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ está en I sii $x = d + e(\frac{1+\sqrt{m}}{t})$ $d, e \in \mathbb{Z}$, $a|d$ y $c|(e - \frac{db}{a})$.*

Demostración. Una base entera para I es $\{a + b\frac{1+\sqrt{m}}{t}, c\frac{1+\sqrt{m}}{t}\}$ donde $t = 1$ ó 2. Sea $x \in \mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ tal que $x = d + e(\frac{1+\sqrt{m}}{t})$ con $d, e \in \mathbb{Z}$. $x \in I$ sii existen enteros z_1, z_2 tales que $x = z_1 a + (z_1 b + z_2 c)(\frac{1+\sqrt{m}}{t})$, esto implica que $z_1 a = d$ y que $z_1 b + z_2 c = e$, i.e que $a|d$ y $c|(e - \frac{db}{a})$. □

Lema 4.4. *Para m negativo es posible ver si un ideal I de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ es principal.*

Demostración. Gracias al lema 3.4 y al lema 4.2. Si $x \in \mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ con $x = d + e(\frac{1+\sqrt{m}}{t})$ entonces $N(x) = (d^2 + \frac{e^2}{2})^2 - \frac{me^2}{4}$ cuando $t = 2$ y $N(x) = (d+e)^2 - me^2$ cuando $t = 1$. Esto pone restriciones si uno esta en I, por ejemplo si $t = 1$ y $x \in I$ tenemos $N(x) = (d+e)^2 - me^2 = ac$. Esto implica que $d^2 \leq ac$ y que $e^2 \leq \frac{ac}{1-m}$ entonces el número de elementos que pueden satisfacer las desigualdes es finito y también tienen que satisfacer las condiciones del párrafo anterior. □

Algoritmo (con $B^2 - 4AC < 0$)

1) Tomamos $f(x) = Ax^2 + Bx + C \in \mathbb{Z}[x]$.

2) Calculamos quién es m, (debe ser libre de cuadrados), esto es, escribimos $\sqrt{B^2 - 4AC} = s\sqrt{m}$.

3) Fijamos una base entera para $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$. Tomamos $\{1, \alpha\}$ donde $\alpha = \frac{1+\sqrt{m}}{t}$. Esto gracias al corolario 1.4.

4) Determinamos si el ideal $(2A, -B + \delta) = I$ es principal (donde $\delta = s\sqrt{m} = \sqrt{B^2 - 4AC}$, y m es libre de cuadrados), esto es posible gracias al lema 4.4. Si I es principal, vas a 6 con $k = 1$. Si I no es principal vas a 5.

5) I^k es principal para alguna $k \in \mathbb{N}$, gracias al teorema 3.5.

6) Sea $k \in \mathbb{N}$ tal que $I^k = \lambda^k \mathcal{O}_K$. Extendemos a $K(\lambda, \overline{\lambda})$, donde $\overline{\lambda}^k$ es el conjugado de λ^k.

7) Factorizamos $f(x)$ en producto de dos polinomios lineales con coeficientes enteros algebraicos, $f(x) = \frac{\lambda\overline{\lambda}}{4A}\left(\frac{2A}{\lambda}x - \frac{(B+\delta)}{\lambda}\right)\left(\frac{2A}{\overline{\lambda}}x - \frac{(B-\delta)}{\overline{\lambda}}\right)$ donde $\frac{\lambda\overline{\lambda}}{4A}$ es unidad en $\mathcal{O}_{\mathbb{Q}(\lambda)}$ gracias al lema 3.15.

Ejemplo:

Consideramos el polinomio $5x^2+3x+2$. Las raíces son $\frac{-3\pm\sqrt{-31}}{10}$. Como $-31 \equiv 1 \ (mod\ 4)$ sabemos que el anillo numérico $\mathcal{O}_{\mathbb{Q}(\sqrt{-31})}$ tiene base entera $\{1, \frac{1+\sqrt{-31}}{2}\}$. Sea $I = (10, -3+\sqrt{-31})$, queremos ver si I es principal. Calculamos la matriz M:

$$M = \begin{pmatrix} 10 & 0 & -4 & -16 \\ 0 & 10 & 2 & -2 \end{pmatrix}$$

y reduciendolo a su forma hermitiana tenemos:

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 4 & 10 & 0 & 0 \end{pmatrix}$$

entonces una base entera para I es $\{2+4(\frac{1+\sqrt{-31}}{2}), 10(\frac{1+\sqrt{-31}}{2})\}$ y $\|I\| = 20$. Hay que buscar si existe un elemento en I con norma 20. Esto es si existe $x = d + e\alpha$ donde $\alpha = \frac{1+\sqrt{-31}}{2}$. Entonces $|d| \leq 4$ y $|e| \leq 1$ y también necesitamos que $2|d$ y que $10|(e-d2)$ lo cual no hay aparte del nulo. Entonces I no es principal.

Ahora $I^2 = (100, -30+10\sqrt{-31}, -22-6\sqrt{-31})$ entonces tenemos:

$$\begin{pmatrix} 100 & 0 & -40 & -160 & -16 & 96 \\ 0 & 100 & 20 & -20 & -12 & -28 \end{pmatrix}$$

y reduciendolo a su forma heritiana tenemos:

$$\begin{pmatrix} 4 & 0 & 0 & 0 & 0 & 0 \\ 28 & 100 & 0 & 0 & 0 & 0 \end{pmatrix}$$

entonce una base entera de I^2 es $\{4+28(\frac{1+\sqrt{-31}}{2}), 100(\frac{1+\sqrt{-31}}{2})\}$ y $\|I\| = 400$. Y resulta que I^2 no es principal.

Finalmente $I^3 = (2+4\alpha, 10\alpha)(4+28\alpha, 100\alpha)$ donde $\alpha = \frac{1+\sqrt{-31}}{2}$. Entonces la matriz reducida es:

$$\begin{pmatrix} 8 & 0 & 0 & 0 \\ 656 & 1000 & 0 & 0 \end{pmatrix}$$

entonces I^3 tiene base entera $\{8+656\alpha, 1000\alpha\}$ y $\|I\| = 8000$. Debemos buscar todos los elementos $a+b\alpha$ tales que $N(a+b\alpha) = 8000$ y luego ver si estos pertenecen a I^3. Como $N(a+b\alpha) = (a+\frac{b}{2})^2 + \frac{31}{4}b^2$ llegamos (después de algunos cálculos) a que $I^3 = (-24+32\alpha)$.

Si definemos $\beta^3 = -24+32\alpha$ y γ^3 igual a la conjugado de β^3 entonces:

$$5x^2+3x+2 =$$

$$\frac{5\beta\gamma}{100}\left(\frac{10}{\beta}x - \left(\frac{-3+\sqrt{-31}}{\beta}\right)\right)\left(\frac{10}{\gamma}x - \left(\frac{-3-\sqrt{-31}}{\gamma}\right)\right)$$

En todo lo que sigue $B^2-4AC > 0$. Esta parte también es más informal en el sentido que citamos muchos teoremas sin demostrarlos. Para el lector interesado citamos donde puede encontrarlos en [P-Z].

Cuando $B^2-4AC > 0$ el algoritmo usado arriba es casi igual, la gran diferencia es en el paso para determinar si el ideal dado es principal; este caso es mucho más complicado.

Teorema 4.5. *Dado un anillo numérico $\mathcal{O}_\mathcal{K}$, existe solemente un número finito de elementos no asociados de norma acotada.*

Demostración. Dado $c \in \mathbb{N}$, definimos $I = c\mathcal{O}_\mathcal{K}$. Sabemos que $\|I\| = c^n$ donde $[K : \mathbb{Q}] = n$. Tomamos $\alpha, \beta \in \mathcal{O}_\mathcal{K}$ tales que $\alpha \equiv \beta \ (\ mod I\ )$ y $|N(\alpha)| = |N(\beta)| = c$. Esto implica que $\alpha - \beta = \gamma c$ para alguna $\gamma \in \mathcal{O}_\mathcal{K}$. Esto es, $\alpha = \beta + c\gamma$. Dividiendo por β obtenemos $\frac{\alpha}{\beta} = 1 \pm \frac{N(\beta)}{\beta}\gamma$ en K. Como $\gamma \in \mathcal{O}_\mathcal{K}$ y $\frac{N(\beta)}{\beta} \in \mathcal{O}_\mathcal{K}$ tenemos que $\frac{\alpha}{\beta} \in \mathcal{O}_\mathcal{K}$. Un arguemto similar demuestra que $\frac{\beta}{\alpha} \in \mathcal{O}_\mathcal{K}$. Entonces α, β son asociados. □

En la página 334 de [P-Z] hay un teorema de Dirichlet que para nuestro caso dice:

Teorema 4.6. *El grupo de unidades, $\mathcal{U}(\mathcal{O}_\mathcal{K})$, de $\mathcal{O}_\mathcal{K}$ es $\mathbb{Z}_2 \times \{\langle\eta\rangle\}$ donde $\langle\eta\rangle$ es isomorfo a $\mathbb{Z}$ y η es el generador. A η se le llama una* ***unidad fundamental.***

Demostración. Página 334 de [P-Z] □

Teorema 4.7. *Dado $a \in \mathbb{N}$ existen solemente un número finito de elementos no-asociados $\alpha \in \mathcal{O}_K$ tales que $N(\alpha) = a$; estos puden ser calculados efectivamente.*

Demostración. La primera parte es gracias a teorema 4.5. La segunda parte está en la página 409 de [P-Z]. □

Para calcular algunas cotas en el teorema 4.7 es necesario calcular la base dual de $\{1, \alpha\}$ donde $\alpha = \frac{1+\sqrt{m}}{t}$. (Ver pagina 336-337 de [P-Z]). Entonces la base dual de $\{1, \alpha\}$ es la solución $\{\delta, \mu\}$ al sistema de ecuaciones:

1) $T(1\delta) = 1$
2) $T(1\mu) = 0$
3) $T(\alpha\delta) = 0$
4) $T(\alpha\mu) = 1$.

La base dual es $\left\{\frac{1}{2} - \frac{1}{2\sqrt{m}}, \frac{t}{2\sqrt{m}}\right\}$.

Entonces si un ideal I es principal, existe $x = x_1 + x_2\alpha \in I$, con $x_1 = T(x\delta)$ y $x_2 = T(x\mu)$, que satisfacen las siguentes cotas:

1) $|x_1| \leq S_1|\delta| + S_2|\overline{\delta}| = T_1$
2) $|x_2| \leq S_1|\mu| + S_2|\overline{\mu}| = T_2$

donde $\overline{\delta}$, $\overline{\mu}$ son los conjugados de δ, μ respectivamente y

1') $S_1 = exp\left(\frac{1}{2}|log|\eta|| + \frac{log||I||}{2}\right)$

2') $S_2 = exp\left(\frac{1}{2}|log|\overline{\eta}|| + \frac{log||I||}{2}\right)$

con $\overline{\eta}$ el conjugado de η.

Teorema 4.8. *Para calcular la unidad fundamental es suficiente encontrar el natural mínimo y tal que:*

1) si $m \equiv 2$ o $3 \pmod 4$, $\pm 1 + my^2$ es un cuadrado.
2) si $m \equiv 1 \pmod 4$, $\pm 4 + my^2$ es un cuadrado.

Demostración. La primer parte de Capítulo 5 de [P-Z]. Buscamos un elemento de la forma $x + y\sqrt{m}$ con norma ± 1 entonces tenemos:

1) si $m \equiv 2$ o $3 \pmod 4$ tenemos $x^2 - my^2 = \pm 1$

2) si $m \equiv 1 \ (mod 4)$ tenemos $x^2 - my^2 = \pm 4$ □

Recapitulando:

1) $\mathbb{Q}(\sqrt{m})$ tiene base $\{1, \alpha\}$ donde $\alpha = \frac{1+\sqrt{m}}{t}$.

2) $\{1, \alpha\}$ tiene base dual $\{\frac{1}{2} - \frac{1}{2\sqrt{m}}, \frac{t}{2\sqrt{m}}\}$.

3) Calculamos la unidad fundamental η

4) Calculamos S_1, S_2 como arriba

5) Calculamos cotas para solución de $x = x_1 + x_2\alpha$

$|x_1| \leq T_1$

$|x_2| \leq T_2$

si no hay ningún elemento que satisface las cotas, el ideal no es principal.

Entonces para el caso cuando $m > 0$ usamos el mismo algoritmo que en el caso $m < 0$, excepto para ver si el ideal es principal.

Ejemplo:

Consideramos el polinomio $f(x) = 11x^2 + 6x - 3$ que tiene raices $r = \frac{-3\pm\sqrt{42}}{11}$. Como $42 \equiv 2 \ (mod\ 4)$ tenemos una base entera $\{1, \sqrt{42}\}$ con base dual $\{\frac{1}{2}, \frac{\sqrt{42}}{84}\}$ (ésta se calcula como antes pero obtenemos una base dual diferente pues comenzamos con otra base entera). Calculamos la unidad fundamental (usdando **Maple**) $\eta = 13 + 2\sqrt{42}$. Tenemos $I = (11, -3 + \sqrt{42})$. Entonces calculamos su matriz corespondiente:

$$\begin{pmatrix} 11 & 0 & -3 & 42 \\ 0 & 11 & 1 & -3 \end{pmatrix}$$

que tiene forma hermitiana:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 7 & 11 & 0 & 0 \end{pmatrix}$$

lo cual nos dice que $\|I\| = 11$.

Ahora calculamos S_1, S_2:

$$S_1 = exp\left(\frac{1}{2}|log|13 + 2\sqrt{42}|| + \frac{log 11}{2}\right) \leq 17$$

$$S_2 = exp\left(\frac{1}{2}|log|13 - 2\sqrt{42}|| + \frac{log11}{2}\right) \leq 1$$

y con esto calculamos T_1, T_2

$$T_1 = \frac{1}{2}(17+1) = 9$$

$$T_2 = \frac{\sqrt{42}}{84}(18) \leq 2.$$

Entonces tenemos que $|x_1| \leq 9$ y $|x_2| \leq 2$.
Con estas restricciones no hay soluciones a $x_1^2 - 42x_2^2 = 11$, lo cual implica que I no es principal.

Como $I = (11, -3+\sqrt{42}) = (1+7\sqrt{42}, 11\sqrt{42})$ tenemos $I^2 = (2059 + 14\sqrt{42}, 3234 + 11\sqrt{42}, 5082)$. Su matriz correspondiente es:

$$\begin{pmatrix} 2059 & 588 & 3234 & 462 & 5082 & 0 \\ 14 & 2059 & 11 & 3234 & 0 & 5082 \end{pmatrix}$$

que tiene forma hermitiana:

$$\begin{pmatrix} 1 & 0 & 0 & \cdots \\ 7 & 121 & 0 & \cdots \end{pmatrix}$$

I^2 tiene base entera $\{1 + 7\sqrt{42}, 121\sqrt{42}\}$. Calculamos otra vez las cotas y encontramos que los posibles candidatos son:

$$11, 17 - 2\sqrt{42} \text{ y } 17 + 2\sqrt{42}$$

de los cual solamente $17 - 2\sqrt{42}$ pertenece a I^2. Por lo tanto

$$I^2 = (17 - 2\sqrt{42}).$$

Extendemos $\mathbb{Q}(\sqrt{42})$ a $\mathbb{Q}(\sqrt{42}, \sqrt{17-2\sqrt{42}}, \sqrt{17+2\sqrt{42}})$ en donde:

$$11x^2+6x-3=11\left(x-\frac{-3+\sqrt{42}}{11}\right)\left(x-\frac{-3-\sqrt{42}}{11}\right)$$

lo cual es:

$$11\left(x-\frac{\frac{-3+\sqrt{42}}{\sqrt{17-2\sqrt{42}}}}{\frac{11}{\sqrt{17-2\sqrt{42}}}}\right)\left(x-\frac{\frac{-3-\sqrt{42}}{\sqrt{17+2\sqrt{42}}}}{\frac{11}{\sqrt{17+2\sqrt{42}}}}\right)$$

y finalmente tenemos:

$$\left(\frac{\sqrt{17-2\sqrt{42}}\sqrt{17+2\sqrt{42}}}{11}\right)\cdot$$

$$\left(\frac{11}{\sqrt{17-2\sqrt{42}}}x-\frac{-3+\sqrt{42}}{\sqrt{17-2\sqrt{42}}}\right)\left(\frac{11}{\sqrt{17+2\sqrt{42}}}x-\frac{-3-\sqrt{42}}{\sqrt{17+2\sqrt{42}}}\right).$$

Entonces

$$11x^2+6x-3=$$

$$\left(\frac{11}{\sqrt{17-2\sqrt{42}}}x-\frac{-3+\sqrt{42}}{\sqrt{17-2\sqrt{42}}}\right)\left(\frac{11}{\sqrt{17+2\sqrt{42}}}x-\frac{-3-\sqrt{42}}{\sqrt{17+2\sqrt{42}}}\right)$$

Bibliografía

[M-M] A. Magidin y D. McKinnon. *Gauss's Lemma for number fields.* En proceso de arbitraje. 2003.

[Mar] D. Marcus. *Number Fields.* Springer-Verlag, 1974.

[P-Z] M. Posht y H. Zassenhaus. *Algorithmic Algebraic Number Theory.* Cambridge University Press. 1989.

[Fra] J. Fraleigh. *A first course in abstract algebra.* Addison-Weasly. 1989.