Introduccion a la teoría de números algebraicos
Alejandro Aguilar Zavoznik
Mario Pineda Ruelas

Resumen.

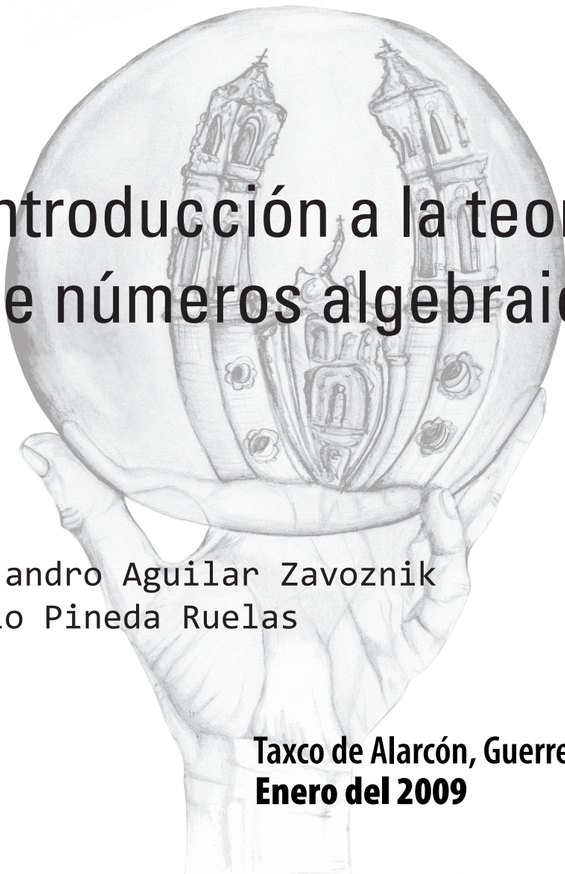
En este taller estudiaremos por medio de ejemplos, la necesidad de la factorización única. Los ejemplos que trataremos se encuentran en cierta clase de anillos que provienen de manera natural de extensiones cuadráticas del campo Q. El lenguaje apropiado para el estudio de este tipo de problemas es el de la arimtmética de los enteros módulo n, grupos, anillos y campos y por lo tanto es recomendable que los participantes hayan cursado al menos un semestre de éstos temas. Comenzaremos con algunos casos clásicos y conforme avance el curso iremos complicando los ejemplos y desarrollando la teoría.

Universidad Autónoma Metropolitana - Iztapalapa

2° Coloquio del Departamento de Matemáticas

UNIVERSIDAD AUTÓNOMA METROPOLITANA
Casa abierta al tiempo

División de Ciencias Básicas e Ingenieria



Introducción a la teoría de números algebraicos

Alejandro Aguilar Zavoznik
Mario Pineda Ruelas

Taxco de Alarcón, Guerrero
Enero del 2009

Introducción a la Teoría de Números Algebraicos

Alejandro Aguilar Zavoznik
Departamento de Matemáticas,
Universidad Autónoma Metropolitana-Iztapalapa,
alexaguilarz@hotmail.com

Mario Pineda Ruelas
Departamento de Matemáticas,
Universidad Autónoma Metropolitana-Iztapalapa,
mpr@xanum.uam.mx

Taxco de Alarcón, Gro., México 2009

Contenido

Introducción

Un curso introductorio a la teoría de números algebraicos es un reto si presuponemos una audiencia que no conocemos sólo por el posible interés en el tema. De cualquier forma, aceptamos el reto y con nuestra propuesta haremos lo que esté a nuestro alcance para inducir a nuestro joven público para que se interese en esta maravillosa disciplina de las mateáticas: la teoría de números algebraicos.

Estas notas están divididas en cuatro lecturas. La primera contiene parte de los antecedentes que consideramos necesarios para poder iniciar el estudio del tema. La segunda y tercera consisten en una variedad de ejemplos en los cuales se podrá vislumbrar una teoría dirigida justamente a uno de los grandes problemas que trata la teoría de números: la factorización. La cuarta lectura es prácticamente una conferencia de la teoría general, la cual, es una invitación a interesarse por el tema.

Esperamos que nuestra audiencia disfrute los temas de estudio que proponemos.

Alejandro Aguilar Zavoznik
Mario Pineda Ruelas,
Departamento de Matemáticas,
Universidad Autónoma Metropolitana-Iztapalapa,
México 2008.

Capítulo 1

El anillo de los enteros

1.1. $\mathbb{Z}$

Una de las estructuras aritméticas más importantes en toda la matemática es el anillo de los enteros $\mathbb{Z}$. Podemos partir de la propiedad más bella (tal vez por su simplicidad) que gozan los enteros:

Teorema 1.1.1 (Algoritmo de la división)**.** *Sean $a, b, \in \mathbb{Z}$ con $a \neq 0$. Existen enteros q y r únicos tal que $b = aq + r$ donde $0 \leq r < |a|$.*

PROOF. Prueba rápida: el conjunto

$$S = \{b - am \geq 0 \quad \text{para ciertos valores} \, m \in \mathbb{Z}\}$$

es no vacío. Por el principio del buen orden (pbo), S contiene un elemento r que satisface $r \leq n$ para todo $n \in S$. Por tanto, $0 \leq r = b - aq$ para algún $q \in \mathbb{Z}$. Puesto que $a \neq 0$, tenemos $a \geq 1$ ó $a \leq -1$. Si $a \geq 1$ entonces

$$b - a(q + 1) = b - aq - a < b - aq = r,$$

así que

$$r - a = b - a(q + 1) < 0,$$

y $r < a$. El caso $a \leq -1$ se sigue al considerar que $b - a(q - 1) < 0$. Por lo tanto, $r < |a|$. La unicidad de q y r se deja como ejercicio para el lector. □

Notemos que si en el enunciado del algoritmo de la división no pedimos que el residuo r sea positivo, entonces r y q no necesariamente son únicos:

$$2 = 11 \cdot 0 + 2 = 11 \cdot 1 + (-9).$$

Problema: Redactar y demostrar una versión general del algoritmo de la división en $\mathbb{Z}$.

Corolario 1.1.2. *$\mathbb{Z}$ es un anillo de ideales principales.*

PROOF. Sea I un ideal en $\mathbb{Z}$ y supongamos que $I \neq \{0\}$. Denotamos por n al menor entero positivo contenido en I. Es claro que $n\mathbb{Z} = \{nz : \, z \in \mathbb{Z}\} \subseteq I$. Si $i \in I$, entonces por el algoritmo de la división

$$i = nq + r, \qquad 0 \leq r \leq n.$$

Observamos que $i - nq = r \in I$. Si $r \neq 0$, entonces n no es el menor entero positivo en I. Así que $r = 0$ y $I \subseteq n\mathbb{Z}$. □

Sean $a, b \in \mathbb{Z}$ con $a \neq 0$. Denotamos por $\mathrm{mcd}(a, b)$ al mayor divisor en común de a, b. Observamos que $\mathrm{mcd}(a, b) \geq 1$. Algunas de las propiedades más importantes del mcd son:

i) $\mathrm{mcd}(a, b)$ es la mínima $\mathbb{Z}$-combinación lineal positiva de a y b.
ii) Si $\mathrm{mcd}(a, b) = g$, entonces $\mathrm{mcd}\left(\frac{a}{g}, \frac{b}{g}\right) = 1$. Lo anterior significa que g contiene en su factorización a todos los divisores que comparten a y b.
iii) Si $a \mid bc$ y $\mathrm{mcd}(a, b) = 1$, entonces $a \mid c$.
iv) Si $a \in \mathbb{Z}$ y p es un primo (ver definición 1.1.3, entonces $\mathrm{mcd}(a, p) = 1$ ó $|p|$.

Cualquier entero $a \neq 0, \pm 1$ tiene al menos cuatro divisores: $\pm 1, \pm a$. Si un entero a tiene al menos un divisor $b \neq \pm a, \pm 1$, entonces $a = bd$ y $d \neq \pm a \pm 1$.

Definición 1.1.3. *Sea $p \in \mathbb{Z}$ con $|p| > 1$. Diremos que p es un número primo si $p = bd$, entonces $b = \pm 1$ ó $d = \pm 1$.*

Los primeros números primos positivos son: $2, 3, 5, 7, 11, ...$, pero también los inversos aditivos de éstos $-2, -3, -5, -11, \ldots$ son números primos. Así que es claro que p es primo si y sólo si $-p$ es primo. Observemos que si $a \in \mathbb{Z}$ y p es cualquier primo, entonces $\mathrm{mcd}(a, p) = 1$ ó p. También es fácil notar que si p, q son primos y $p \mid q$, entonces $|p| = |q|$.

Teorema 1.1.4. [Euclides] *p es primo si y sólo si siempre que $p \mid ab$, entonces $p \mid a$ ó $p \mid b$.*

PROOF. Supongamos que p es primo y $p \mid ab$. Si $p \nmid a$, entonces $\mathrm{mcd}(a, p) = 1$. Así que que $p \mid b$. Inversamente, sea $p = ab$ una factorización de p. En particular $p \mid ab$ y por lo tanto $p \mid a$ ó $p \mid b$. Si $p \mid a$ se tiene que $a = pt$, para algún $t \in \mathbb{N}$. Así que $p = ab = ptb$. De lo anterior se sigue que $b = 1$ y $a = p$ y por lo tanto p es primo. □

El teorema anterior nos autoriza a cambiar la definición de número primo.

Definición 1.1.5. *Diremos que $p \in \mathbb{Z}$ es primo si $|p| > 1$ y siempre que $p \mid ab$, entonces $p \mid a$ ó $p \mid b$. Diremos que un entero π con $|\pi| > 1$ es irreducible si $\pi = ab$, entonces $|a| = 1$ ó $|b| = 1$*

Obviamente primo e irreducible significan exactamente lo mismo en el anillo $\mathbb{Z}$. Existirán estructuras en las que primo e irreducible no coincidan? esta será la guía con la que trabajaremos.

Teorema 1.1.6. *Cualquier entero $m > 1$ admite al menos un divisor primo.*

PROOF. Fácil ejercicio para el lector. Se sugiere usar inducción sobre m. □

Seguramente la propiedad más importante de $\mathbb{Z}$ se refiere a la factorización única de sus elementos.

Corolario 1.1.7. [Teorema Fundamental de la Aritmética] *Todo entero* $\neq 0, \pm 1$ *se puede expresar en forma única (salvo el orden) como un producto finito de números primos.*

PROOF. Es consecuencia directa del Teorema 1.1.4. □

Corolario 1.1.8. *Si* $n > 2$*, entonces existe un primo* p *tal que* $n < p < n!$.

PROOF. El número $z = n! - 1 > 1$ tiene un divisor primo $p \leq z$. Si $p \leq n$, entonces $p \mid n!$ y por lo tanto $p \mid 1$ lo cual es absurdo. Así que $n < p \leq n! - 1 < n!$. □

Corolario 1.1.9. [Teorema de Euclides] *Existen suficientes primos para factorizar cualquier entero* $\neq 0, \pm 1$*, es decir, existe una infinidad de números primos.*

PROOF. Consideremos n suficientemente grande en el corolario anterior. □

Nota: Si $ab = c^n$ y $\mathrm{mcd}(a, b) = 1$, entonces para ciertos enteros c_1, c_2 se tiene que $a = c_1^n$ y $b = c_2^n$. Veamos una aplicación de esta inofensiva propiedad.

Teorema 1.1.10. *La ecuación* $x^2 - y^3 = 1$ *tiene una única solución en los enteros positivos:* $x = 3,\ y = 2$.

PROOF. Tenemos que si x es par, entonces $mcd(x - 1, x + 1) = 1$ y además:

$$(x - 1)(x + 1) = y^3.$$

Por tanto

$$x - 1 = a^3 \quad \text{y} \quad x + 1 = b^3.$$

De lo anterior se sigue que $b^3 - a^3 = (b-a)(b^2+ab+a^2) = 2$ y así $b^2+ab+a^2 \mid 2$, lo cual es imposible. Por lo tanto, si existiera solución $x = 2t + 1$ y $y = 2q$ con $t, q \geq 1$. Es claro que $t = 1$ implica $x = 3$ y $y = 2$. Si $t > 1$, tendríamos $t(t+1) = 2q^3$, lo cual es imposible porque ningún número triangular es un cubo. □

En una carta fechada en 1844 y dirigida a la revista Journal Crelle, el matemático belga E. Charles Catalan conjeturó que si

$$x^n - y^m = 1,$$

entonces $n = 2,\ m = 3,\ x = 3,\ y = 2$. Esta conjetura un poco olvidada, tal vez por el atractivo que tenía la conjetura de Fermat, se sabe que ha sido resuelta por el matemático rumano Preda Mihailescu (2002). El Teorema 1.1.10 es una versión elemental de la conjetura de Catalan.

Regresando a nuestra discusión, el Corolario 1.1.2 nos brinda de manera explícita la forma de cualquier ideal en el anillo $\mathbb{Z}$. Podemos desarrollar teoría general al respecto, adoptando la definición de primo e irreducible que dimos en $\mathbb{Z}$.

1.1.1. Un poco de teoría general

El objetivo de esta breve sección es ubicar parte de nuestro trabajo en un contexto general, que algunas veces es difícil aterrizarlo en anillos específicos. Esto se debe a dificultades ariméticas que no se pueden hacer explícitas. Por ejemplo, si A es un anillo quiénes son sus unidades? significan lo mismo primo e irreducible en cualquier anillo? más aún quiénes son los elementos irreducibles? Estas preguntas serán la guia de nuestras exposisiones.

Teorema 1.1.11. *En cualquier anillo conmutativo unitario, los ideales primos principales están generados por elementos primos.*

PROOF. Sea $P =< \pi >$ un ideal primo principal y supongamos que $\pi \mid ab$. Entonces $ab \in P$ y por lo tanto $a \in P$ ó $b \in P$. Así que $a = \pi q$ ó $b = \pi t$. Esto significa que $\pi \mid a$ ó $\pi \mid b$. Por lo tanto π es primo. □

Teorema 1.1.12. *En cualquier dominio entero unitario A, los ideales máximos principales están generados por elementos irreducibles.*

PROOF. Sea $M =< \pi >$ y $\pi = ab$. Debemos mostrar que $a \in U(A)$ ó $b \in U(A)$. Claramente $< \pi > \subseteq < a > \subseteq A$. Como $< \pi >$ es máximo se tiene $< \pi >=< a >$ ó $< a >= A$. Si $< \pi >=< a >$ se tiene que $a = \pi t$, para algún $t \in A$ y de la igualdad $\pi = ab = \pi tb$ se sigue que $1 = tb$, de donde $b \in U(A)$. Si $< a >= A =< 1 >$, entonces claramente $a \in U(A)$. □

Teorema 1.1.13. *Si A es un DIP, entonces cualquier sucesión ascendente de ideales es finita.*

PROOF. Sea $I_1 \subset I_2 \subset \cdots \subset I_n \subset I_{n+1} \cdots$ cualquier sucesión ascendente de ideales de A y $I = \bigcup_{j=1}^{\infty} I_j$. Claramente I es un ideal de A. Por otro lado $I =< a >$ para algún $a \in A$. Puesto que para algún m se tiene $a \in I_m$, se sigue que $I \subseteq I_m \subseteq I$. Lo anterior significa que $I \in \{I_j\}_{j=1}^{\infty}$. Ahora sea $n \geq m$. Entonces $I = I_m \subseteq I_n \subseteq I$, así $I_n = I_m$ y la sucesión es finita. □

Cualquier anillo que satisface el teorema anterior (no necesariamente DIP) lo llamaremos anillo noetheriano. En nuestro caso, cualquier DIP es noetheriano.

Teorema 1.1.14. *Sea $< a >$ ideal de un anillo A que es un DIP. Entonces existe $< m >$ ideal máximo tal que $< a > \subseteq < m >$.*

PROOF. Sea $X_a = \{I \subset A : I$ es un ideal de A tal que $< a > \subseteq I\}$. Definimos en X_a la siguiente relación: $I \sim J$ si y sólo si $I \subseteq J$. Es claro que X_a es un conjunto parcialmente ordenado con $\sim$. Sea $\mathcal{C}$ cualquier cadena en X_a. Vamos a demostrar que $\mathcal{C}$ tiene un elemento máximo. Sea $M = \bigcup_{I \in \mathcal{C}} I$. Es claro que:

i) M es un ideal de A.
ii) $M \neq A$, pues de lo contrario $1 \in I_j$ para algún j. Por lo tanto $M \in X_a$.
iii) $I_j \subseteq M$.

Lo anterior demuestra que cualquier cadena $\mathcal{C}$ tiene una cota superior en X_a. Entonces por el Lema de Zorn tenemos que X_a tiene al menos un elemento (un ideal que contiene a $< a >$) máximo M. Falta ver que M es un ideal máximo de A. Supongamos que $M \subset I \subset A$. Si $I \not\subset A$, entonces $I \in X_a$ y $M \subset I$. Por tanto M no es un elemento máximo de X_a, así tenemoss $I = A$. □

Nota: En dónde usamos que A es un DIP?

En cualquier anillo conmutativo con unidad A, los elementos que tienen inverso multiplicativo forman un grupo multiplicativo el cual denotamos por $U(A)$. El lector puede verificar fácilmente que: $a = bu$ para algún $u \in U(A)$ si y sólo si $a \mid b$ y $b \mid a$. Cuando esto sucede diremos que a y b son asociados y escribiremos $a \sim b$. Observemos que $< a >=< b >$ si y sólo si $a \sim b$. El conjunto de asociados al elemento a queda descrito por $\{au : u \in U(A)\}$.

Corolario 1.1.15. *Sea A un DIP. Entonces los ideales primos $\neq 0$ son máximos.*

PROOF. Sea $< q >$ un ideal primo con $q \neq 0$ y $< \pi >$ algún ideal máximo tal que $< q > \subseteq < \pi >$. Vamos a mostrar que $< q >=< \pi >$. Sabemos que q es primo y π es irreducible. Puesto que $q \in < q > \subseteq < \pi >$, tenemos $q = \pi t$ para algún $t \in A$. En particular $q \mid \pi t$ y $q \mid \pi$ ó $q \mid t$. Si $q \mid t$, entonces $t = qr$ y de la igualdad $q = \pi t = \pi qr$ tenemos que $\pi \in U(A)$, lo cual no es posible. Así $q \mid \pi$ y $\pi = qu$ para algún $u \in U(A)$. Por lo tanto $< \pi >=< q >$. □

Corolario 1.1.16. *En un DIP primo e irreducible son lo mismo.*

PROOF. Fácil ejercicio para el lector. □

Nota: Qué podemos decir si un elemento irreducible es asociado a un elemento primo?

Antes de continuar precisemos el concepto de factorización única: Diremos que el anillo A tiene la propiedad de la factorización única si cualquier elemento $a \in A \setminus U(A)$, con $a \neq 0$ se puede expresar en forma *única* como producto finito de irreducibles. Aquí la unicidad significa lo siguiente: Si

$$a = \pi_1 \pi_2 \cdots \pi_r = q_1 q_2 \cdots q_k,$$

con π_j, q_s irreducibles, entonces $r = k$ y cada π_j es asociado de algún q_l. Por ejemplo, en $\mathbb{Z}$ tenemos que $2 \cdot 3 = (-2) \cdot (-3)$ son la misma factorización, ya que 2 y -2 son asociados y 3 y -3 tamién lo son.

En seguida tenemos la versión de la factorización única en cualquier DIP.

Teorema 1.1.17 (Teorema Fundamental de la Aritmética en un DIP)**.** *Sea A un DIP. Cualquier elemento $a \in A \setminus \{0\}$ es una unidad o se puede escribir como producto finito de irreducibles y unidades.*

PROOF. Sea $a \in A \setminus \{0\}$ y supongamos que $a \notin U(A)$. Así que $< a > \subset A$. Si a es irreducible la afirmación se cumple pues $a = a \cdot 1$. Así que podemos suponer que a no es irreducible. Sea $M =< \pi_1 >$ algún ideal máximo de A tal que $< a > \subseteq < \pi_1 >$. Puesto que $a \in < a > \subseteq < \pi_1 >$ se tiene que $a = \pi_1 t_1$, para algún $t_1 \in A$. Claramente $t_1 \notin U(A)$ pues de lo contrario $a \sim \pi$ y a sería irreducible. Sea $< \pi_2 >$ algún ideal máximo de A tal que $< t_1 > \subseteq < \pi_2 >$. Entonces $t_1 = \pi_2 t_2$ para algún $t_2 \in A$. De la anterior igualdad se sigue que $< t_1 > \subseteq < t_2 >$. Así $a = \pi_1 \pi_2 t_2$. Continuando con este proceso obtenemos una cadena de ideales

$$< t_1 > \subseteq < t_2 > \subseteq < t_3 > \subseteq ....$$

la cual debe terminar porque A es noetheriano. Así que el proceso es finito y se sigue el resultado. □

Corolario 1.1.18. *Sea A un DIP. La factorización que asegura el teorema anterior es única salvo orden y unidades.*

PROOF. Ejercicio para el lector □

Para verificar si cierto anillo tiene la propiedad de ser de factorización única existen varios caminos. Por ejemplo se puede intentar mostrar que es euclidiano, o que es un DIP, etc. El siguiente resultado nos proporciona una alternativa.

Teorema 1.1.19. *Sea A un anillo en donde es posible la factorización finita en irreducibles. Entonces en A la factorización es única si y sólo si primo e irreducible coinciden.*

PROOF. Sólo demostraremos una implicación. Supongamos que cualquier irreducible es primo y sea

$$\alpha = u_1 \pi_1 \cdots \pi_k = u_2 q_1 \cdots q_s,$$

con π_i, q_j irreducibles en A y u_1, u_2 son unidades. Si $k = 0$, entonces $s = 0$ y α es unidad. Si $k = 1$, entonces tenemos $u_1 \pi_1 = u_2 q_1 \cdots q_s$. Supongamos que $s > 1$. Entonces $\pi_1 \mid u_2$ o $\pi_1 \mid q_j$ para algún j. La primera afirmación no es posible, así que $q_j = u_1' \pi_1$, para algún $u_1' \in U(A)$. No perdemos generalidad si suponemos que $j = 1$ y así tenemos

$$u_1 \pi_1 = u_2 u_1' \pi_1 q_2 \cdots q_s.$$

Por lo tanto $u_1 = u_2 u_1' q_2 \cdots q_s$ y $q_2, ..., q_s \in U(A)$ lo cual es absurdo pues los q_j son irreducibles. Así que $s = 1$ y π_1 es asociado de q_1. Supongamos que si

$$\alpha = u_1 \pi_1 \cdots \pi_k = u_2 q_1 \cdots q_s,$$

entonces $k = s$ y cada π_i es asociado de algún q_j. Consideremos

$$u_1 \pi_1 \cdots \pi_k \pi_{k+1} = u_2 q_1 \cdots q_s,$$

con $u_1, u_2 \in U(A)$. Entonces π_{k+1} es asociado de algún q_j el cual podemos suponer que es q_1. Así $q_1 = u_1' \pi_{k+1}$. Por lo tanto

$$u_1 \pi_1 \cdots \pi_k \pi_{k+1} = u_2 u_1' \pi_{k+1}' \cdots q_s.$$

Cancelando π_{k+1} en ambos lados obtenemos

$$u_1\pi_1\cdots\pi_k\pi_k = u_2u_1'q_2'\cdots q_s.$$

Por lo tanto $k = s-1$ y así $k+1 = s$. □

Problema: Sea A un anillo en donde es posible la factorización finita en irreducibles. Demuestra que si en A la factorización es única, entonces los elementos primos e irreducible coinciden.

1.1.2. El anillo de los enteros gaussianos

Consideremos la extensión de campos $\mathbb{Q}(i)/\mathbb{Q}$. Definimos en anillo de los enteros gaussianos como:

$$\mathbb{Z}[i] = \{\alpha \in \mathbb{Q}(i) : f(\alpha) = 0 \text{ para algún } f(x) \in \mathbb{Z}[x] \text{ mónico}\}.$$

Aunque esta definición no describe explícitamente a los elementos de $\mathbb{Z}[i]$, se puede probar relativamente fácil que

$$\mathbb{Z}[i] = \{a+bi : a.b \in \mathbb{Z}\} = \mathbb{Z} + i\mathbb{Z}.$$

Más adelante veremos con detalle cómo describir estos anillos que provienen de manera natural de extensiones cuadráticas del campo $\mathbb{Q}$.

La función norma $N : \mathbb{Z}[i] \to \mathbb{N}_0$ definida como $N(a+bi) = a^2+b^2$ tiene las siguientes propiedades:

i) $N(a+bi) \geq 0$ y $N(a+bi) = 0$ si y sólo si $a = b = 0$.
ii) $N((a+bi)(c+di)) = N(a+bi)N(c+di)$.
iii) $a+bi$ tienen inverso multiplicativo en $\mathbb{Z}[i]$ si y sólo si $N(a+bi) = 1$. Concretamente $U(\mathbb{Z}[i]) = \{1,-1,i,-i\}$.
iv) Si $a+bi \mid c+di$, entonces $N(a+bi) \mid N(c+di)$.

Seguramente, la riqueza del anillo $\mathbb{Z}[i]$ proviene de la posibilidad de dividir, tal como sucede en $\mathbb{Z}$.

Teorema 1.1.20 (Algoritmo de la división en $\mathbb{Z}[\beth]$)**.** *Si $z_1, z_2 \in \mathbb{Z}[i]$ con $z_2 \neq 0$, entonces existen $k,\ \delta \in \mathbb{Z}[i]$ tales que*

$$z_1 = z_2k + \delta \ \text{ y } \ 0 \leq N(\delta) < N(z_2).$$

PROOF. Prueba rápida: Escribimos $\dfrac{z_1}{z_2} = A + Bi$ con $A, B \in \mathbb{Q}$ y elegimos los enteros x, y con la siguiente propiedad:

$$|A-x| \leq \frac{1}{2} \qquad \text{y} \qquad |B-y| \leq \frac{1}{2}.$$

Los enteros gaussianos $k = x+yi$ y $\delta = z_1 - z_2(x+yi)$ satisfacen la afirmación del teorema. □

Ahora tenemos una clasificación de los irreducibles (o primos) en el anillo $\mathbb{Z}[i]$

Teorema 1.1.21. *Los primos en $\mathbb{Z}[i]$ son :*

i) $1+i$ *y sus asociados.*
ii) *Los factores* $a+bi$ *de primos racionales de la forma* $4n+1$ *y sus asociados.*
iii) *Los primos racionales de la forma* $4n+3$ *y sus asociados.*

Observe el lector que la afirmación ii) nos indica que los primos racionales de la forma $4n+1$ ahora ya se pueden factorizar (!!!). Para una prueba del Teorema 1.1.21 se sugiere revisar [**35**].

Problema: Escribir los detalles de la demostración del Algoritmo de la división en $\mathbb{Z}[i]$.

Problema: Traducir la aritmética de los enteros gaussianos al lenguaje de anillos.

Veamos un ejemplo de cómo usar a los enteros gaussianos para resolver una ecuación diofantina.

Teorema 1.1.22. *La ecuación* $x^2 - y^3 = -1$ *tiene como única solución entera* $y = 1$ *y* $x = 0$.

PROOF. Tenemos la factorización:

$$y^3 = (x+i)(x-i)$$

Así que esto sugiere usar el anillo de los enteros gaussianos $\mathbb{Z}[i]$. El lector interesado puede seguir los siguientes pasos para concluir la demostración:

i) Se demuestra que $\mathrm{mcd}(x+i, x-i) = 1$.
ii) Se concluye que $x+i = (a+bi)^3$ y $x-i = (a-bi)^3$! salvo unidades.

y el resto debe ser rutina. □

Problema: Considerar el anillo $\mathbb{Z}[2i] = \{a+2bi : a, b \in \mathbb{Z}\}$. Encuentra $U(\mathbb{Z}[2i])$. Demuestra que 2 y $2i$ son irreducibles. son primos en $\mathbb{Z}[2i]$? Es $\mathbb{Z}[2i]$ un anillo de factorización única aún cuando $\mathbb{Z}[2i] \subset \mathbb{Z}[i]$?

1.1.3. La ecuación de Bachet (1624) $x^2 - y^3 = -19$.

En este ejemplo veremos cómo un anillo que no tiene la propiedad de ser de factorización única, está sumergido en un anillo que si es un DFU. Consideremos la ecuación diofantina $x^2 - y^3 = -19$. Primero veremos un *critero* que nos indique si nuestra ecuación es o no soluble en los enteros x, y. La igualdad

$$x^2 + 19 = (x + \sqrt{-19})(x - \sqrt{-19}) = y^3,$$

nos sugiere trabajar en el anillo

$$\mathbb{Z}[\sqrt{-19}] = \{a + b\sqrt{-19} : \ a, b \in \mathbb{Z}\}.$$

En este caso, la función norma está definida como $N(a+b\sqrt{-19}) = a^2+19b^2$. Es fácil mostrar que el elemento $a+b\sqrt{-19}$ tiene inverso multiplicativo en el anillo $\mathbb{Z}[\sqrt{-19}]$ si y sólo si $a^2 + 19b^2 = 1$. Primeras consideraciones:

i) Si $19 \mid y$, entonces $19 \mid y^3$ y por tanto $19 \mid x$. Así $x^2 - y^3 = 19^2 q = -19$ lo cual es imposible en $\mathbb{Z}$. Similarmente $2 \nmid y$. En conclusión $19 \nmid y$ y $2 \nmid y$. Así $1 = ry^3 + s2 \cdot 19$ en $\mathbb{Z}$.

ii) $U(\mathbb{Z}[\sqrt{-19}]) = \{1, -1\}$.

iii) Sea $\mu \in \mathbb{Z}[\sqrt{-19}]$ Tal que $\mu \mid x + \sqrt{-19}$ y $\mu \mid x - \sqrt{-19})$. Entonces $\mu \mid 2\sqrt{-19}$ y por tanto $\mu \mid 2 \cdot 19$. Pero $\mu \mid y^3$, así que $\mu \mid ry^3 + s2 \cdot 19 = 1$. Así $\mu = \pm 1$ y por lo tanto $\mathrm{mcd}(x + \sqrt{-19}, x - \sqrt{-19}) = 1$. Notemos que cualquier unidad en $\mathbb{Z}[\sqrt{-19}]$ es un cubo.

iv) $x + \sqrt{-19} = (a + b\sqrt{-19})^3 = (a^3 - 3 \cdot 19ab^2) + (3a^2b - 19b^3)\sqrt{-19}$.

v) El sistema:

$$x = a^3 - 3 \cdot 19ab^2$$
$$1 = 3a^2b - 19b^3,$$

no es soluble en $\mathbb{Z}$.

vi) De lo anterior concluimos que la ecuación $x^2 - y^3 = -19$ no es soluble en $\mathbb{Z}$.

A primera vista todas las operaciones que efectuamos son correctas. Pero

$$18^2 - 7^3 = -19$$

qué hicimos mal ? Observemos la siguiente factorización

$$35 = 5 \cdot 7 = (4 + \sqrt{-19})(4 - \sqrt{-19})$$

Por qué son diferentes? o son la misma? Por simplicidad recordemos nuestras definiciones:

Definición 1.1.23. *π es primo si $\pi \mid \alpha\beta$, entonces $\pi \mid \alpha$ ó $\pi \mid \beta$.*

Definición 1.1.24. *π es irreducible si $\pi = \alpha\beta$, entonces α ó β es unidad.*

En general, no es dificil mostrar que cualquier elemento primo es irreducible (inténtelo). En nuestro caso $5, 7, 4+\sqrt{-19}, 4-\sqrt{-19}$ son irreducibles en $\mathbb{Z}[\sqrt{-19}]$ no asociados dos a dos. ! Y no son primos. Por ejemplo: 5 es irreducible: Si $5 = \alpha\beta$, entonces

$$25 = N(\alpha)N(\beta)$$

y por tanto

$$N(\alpha) = 5 = N(\beta) \quad \text{ó}$$
$$N(\alpha) = 25 \quad \text{y} \quad N(\beta) = 1.$$

El primer caso no es posible y así β es unidad. Por qué 5 no es primo en $\mathbb{Z}[\sqrt{-19}]$? Primero notemos que

$$5 \mid (4+\sqrt{-19})(4-\sqrt{-19}).$$

Si $5 \mid 4+\sqrt{-19}$, entonces

$$4+\sqrt{-19} = 5(a+b\sqrt{-19}) = 5a+5b\sqrt{-19}.$$

En particular $5 \mid 4$ en $\mathbb{Z}$, lo cual es imposible. Similarmente $5 \nmid 4-\sqrt{-19}$ y por tanto 5 no es primo.

Más adelante veremos que el anillo $\mathbb{Z}[\sqrt{-19}]$ está contenido en otro anillo que es de factorización única, aún cuando $\mathbb{Z}[\sqrt{-19}]$ no lo es. Cómo explicamos este fenómeno?

Teorema 1.1.25. *Las soluciones enteras de la ecuación de Bachet $x^2 - y^3 = -19$ son: $x = \pm 18$ y $y = 7$.*

PROOF. Seguir las mismas ideas y trabajar en el anillo de enteros de la extensión $\mathbb{Q}(\sqrt{-19})/\mathbb{Q}$. Se sugiere estudiar la ecuación:

$$x+\sqrt{-19} = \Big(\frac{a+b\sqrt{-19}}{2}\Big)^3.$$

□

1.1.4. El problema de las unidades y la factorización

En esencia, las ideas que hemos utilizados son las mismas. Ahora consideremos la ecuación $x^2 - 18 = y^3$. En este caso tenemos

$$x^2 - 18 = (x-\sqrt{18})(x+\sqrt{18}) = (x-3\sqrt{2})(x+3\sqrt{2}) = y^3,$$

y por lo tanto, parece conveniente trabajar en el anillo

$$\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} : \ a, b \in \mathbb{Z}\}.$$

Se sabe que el anillo $\mathbb{Z}[\sqrt{2}]$ es euclidiano y en consecuencia, es un anillo de factorización única en donde elemento primo e irreducible coinciden. Un ejercicio fácil para el lector consiste en mostrar que $\sqrt{2}$ y 3 son elementos primos en $\mathbb{Z}[\sqrt{2}]$. Ahora notemos que si $x = 2t$ y $y = 2q$, entonces $x^2 \equiv 0 \pmod 4$ y

$$x^2 \equiv 4t^2 \equiv 8q^3 + 18 \equiv 2 \equiv 0 \pmod 4,$$

lo cual no es posible. Obviamente, no puede suceder que x, y tengan paridad diferente. Por lo tanto, si x, y es cualquier solución, necesariamente x, y deben ser impares. Supongamos que el lector ya ha verificado que 3 es primo en $\mathbb{Z}[\sqrt{2}]$.

Ahora mostraremos que la ecuación $x^2 - 18 = y^3$ no es soluble. Primero veremos que los factores $x - 3\sqrt{2}$ y $x + 3\sqrt{2}$ son primos relativos en el anillo $\mathbb{Z}[\sqrt{2}]$.

Sea $\alpha = \mathrm{mcd}(x - 3\sqrt{2}, x + 3\sqrt{2})$ y π algún divisor primo de α. Entonces $\pi \mid 6\sqrt{2}$ y puesto que $2 = (\sqrt{2})^2$ tenemos $\pi \mid 3 \cdot (\sqrt{2})^3$. Si $\pi \mid \sqrt{2}$, tenemos que $\pi = u\sqrt{2}$ para alguna unidad $u \in \mathbb{Z}[\sqrt{2}]$. Como $\pi \mid x + 3\sqrt{2}$, tenemos $\sqrt{2} \mid x + 3\sqrt{2}$. Por lo tanto $2 \mid x$ y x es par, lo cual no es posible.

Por otro lado, si $\pi \mid 3$, entonces $\pi = 3u$ para alguna unidad $u \in \mathbb{Z}[\sqrt{2}]$. Por lo anterior tenemos que $3 \mid x + 3\sqrt{2}$ y así $3 \mid y$ y $3 \mid x$. Sea $y = 3a$ y $x = 3b$. Entonces de la igualdad $x^2 - 18 = y^3$ obtenemos $b^2 \equiv 3a^3 + 2 \equiv 2 \pmod 3$. Puesto que x es impar, necesariamente b debe ser impar. Si $b = 3k + r$ y k es par, entonces $b = 3k + 1$ y por lo tanto $b^2 \equiv 1 \pmod 3$, lo cual no es posible. Análogamente si k es impar obtenemos un absurdo. Por lo anterior, $\pi \nmid 3$. En conclusión, α no tiene divisores primos y así α debe ser una unidad. Hemos mostrado que $\mathrm{mcd}(x + 3\sqrt{2}, x - 3\sqrt{2}) = 1$. Por lo tanto cada factor de $y^3 = (x + 3\sqrt{2})(x - 3\sqrt{2})$ debe ser un cubo. Supongamos que $x + 3\sqrt{2} = (a + b\sqrt{2})^3$. Entonces

$$x + 3\sqrt{2} = a^3 + 3a^2b\sqrt{2} + 6ab^2 + 2b^3\sqrt{2} = (a^3 + 6ab^2) + (3a^2b + 2b^3)\sqrt{2}.$$

De la igualdad anterior surge el sistema

$$\begin{aligned} a^3 + 6ab^2 &= x \\ 3a^2b + 2b^3 &= 3. \end{aligned}$$

La segunda ecuación la podemos escribir como

$$b(3a^2 + 2b^2) = 3,$$

la cual obviamente no tiene solución en los enteros a, b. Si trabajamos con la igualdad $x - 3\sqrt{2} = (a + b\sqrt{2})^3$, llegamos a la misma conclusión. Con lo anterior concluimos que $x^2 - 18 = y^3$ no tiene soluciones enteras x, y.

Algo hicimos mal: $19^2 - 18 = 7^3$.

Problema: Descubra el error en la argumentación anterior.

1.1.5. El anillo $\mathbb{Z}[\sqrt{10}]$

En esta sección estudiaremos con detalle la aritmética del anillo

$$\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} : a, b \in \mathbb{Z}\}.$$

Veremos, entre otras cosas, que no es un anillo de factorización única, encontraremos el grupo de unidades y daremos ejemplos de cómo se comportan distintas factorizaciones de un mismo número. Comenzaremos definiendo la norma de un elemento. Consideremos la función

$$N : \mathbb{Z}[\sqrt{10}] \to \mathbb{Z}$$

definida como $N(a + b\sqrt{10}) = a^2 - 10b^2$. Observemos que

$$N(a + b\sqrt{10}) = (a + b\sqrt{10})(a - b\sqrt{10}).$$

Teorema 1.1.26. *La función N es multiplicativa.*

PROOF.

$$\begin{aligned} N(a + b\sqrt{10})N(c + d\sqrt{10}) &= (a^2 - 10b^2)(c^2 - 10b^2) \\ &= a^2c^2 - 10a^2d^2 - 10b^2c^2 + 100b^2d^2 \\ &= (ac + 10bd)^2 - 10(ad + bc)^2 \\ &= N((a + b\sqrt{10})(c + d\sqrt{10})), \end{aligned}$$

□

Lema 1.1.27. *$a + b\sqrt{10} \in \mathbb{Z}[\sqrt{10}]$ es una unidad si y sólo si $|N(a + b\sqrt{10})| = 1$.*

PROOF. Si α es una unidad, entonces α^{-1} es un elemento del anillo. Como la norma es multiplicativa, entonces:

$$N(\alpha)N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = N(1) = 1,$$

y debido a que el codominio de la norma es $\mathbb{Z}$, entonces las únicas posibilidades son

$$N(\alpha) = N(\alpha^{-1}) = 1 \qquad \text{ó} \qquad N(\alpha) = N(\alpha^{-1}) = -1,$$

en cualquier caso, se cumple la afirmación. Inversamente, si $N(a + b\sqrt{10}) = 1$, entonces

$$(a + b\sqrt{10})(a - b\sqrt{10}) = 1,$$

y por lo tanto, $a + b\sqrt{10}$ es una unidad, pues $a - b\sqrt{10}$ es su inverso multiplicativo. Si $N(a + b\sqrt{10}) = -1$, entonces $(a + b\sqrt{10})(a - b\sqrt{10}) = -1$ y $-a + b\sqrt{10}$ es el inverso multiplicativo de $a + b\sqrt{10}$. □

Como caso particular del célebre Teorema de las Unidades de Dirichlet sabemos que el anillo $\mathbb{Z}[\sqrt{10}]$ contiene una unidad especial $\epsilon > 1$ que satisface: si $\mu \in U(\mathbb{Z}[\sqrt{10}])$, entonces existe $n \in \mathbb{Z}$ tal que $\mu = \pm\epsilon^n$. Esta unidad se conoce como la *unidad fundamental* del anillo. Vamos a demostrar que $\epsilon = 3 + \sqrt{10}$.

Proposición 1.1.28. *Si $\mu \in U(\mathbb{Z}[\sqrt{10}])$, entonces $\mu = \pm(3 + \sqrt{10})^m$, para algún $m \in \mathbb{Z}$.*

PROOF. Primero vamos a mostrar que no existen unidades μ tal que $1 < \mu < 3 + \sqrt{10}$. Supongamos que efectivamente, existe al menos una unidad μ tal que

$$1 < \mu < 3 + \sqrt{10}.$$

Si escribimos $\mu = a + b\sqrt{10}$, entonces podemos suponer sin pérdida de generalidad que $a, b \in \mathbb{N}$ (por qué?). Observemos que $1 = |(a + b\sqrt{10})(a - b\sqrt{10})|$. Si escribimos $\bar{\mu} = a - b\sqrt{10}$, entonces es claro que:

i) $\bar{\mu} \in \mathbb{Z}[\sqrt{10}]$.
ii) $|\mu\mu^{-1}| = |\mu\bar{\mu}| = 1$.
iii) $\mu + \bar{\mu} = 2a \in 2\mathbb{Z}$.

Puesto que $1 < \mu < 3 + \sqrt{10}$, invirtiendo se tiene

$$\sqrt{10} - 3 = \frac{1}{3 + \sqrt{10}} < \bar{\mu} < 1,$$

y por lo tanto

$$\sqrt{10} - 2 < \mu + \bar{\mu} < 4 + \sqrt{10},$$

o equivalentemente

$$\frac{\sqrt{10}}{2} - 1 < \frac{\mu + \bar{\mu}}{2} < 2 + \frac{\sqrt{10}}{2}.$$

Con ayuda de una calculadora obervamos que

$$\frac{\sqrt{10}}{2} - 1 > .5811 \qquad \text{y} \qquad \frac{\sqrt{10}}{2} + 2 < 4.$$

Por lo tanto, necesariamente $a = 1, 2$ ó 3. En cada caso producimos las ecuaciones

$$1 - 10b^2 = \pm 1, \quad 4 - 10b^2 = \pm 1, \quad 9 - 10b^2 = \pm 1,$$

las cuales no son solubles en el entero b. Lo anterior significa que la unidad $3+\sqrt{10}$ es la menor unidad positiva en el anillo $\mathbb{Z}[\sqrt{10}]$.

Ahora fijemos una unidad positiva de $\mathbb{Z}[\sqrt{10}]$, digamos u'. Como

$$\lim_{n \to -\infty} (3 + \sqrt{10})^n = 0 \quad \text{y} \quad \lim_{n \to +\infty} (3 + \sqrt{10})^n = \infty,$$

y para todo $n \in \mathbb{Z}$ se tiene que $(3 + \sqrt{10})^n < (3 + \sqrt{10})^{n+1}$ entonces existe un único $m \in \mathbb{Z}$ tal que

$$(3 + \sqrt{10})^m \leq u' < (3 + \sqrt{10})^{m+1}.$$

Multiplicando por $(3 + \sqrt{10})^{-m}$ obtenemos

$$1 \leq u'(3 + \sqrt{10})^{-m} < 3 + \sqrt{10},$$

pero no hay ninguna unidad entre 1 y $3 + \sqrt{10}$ así que $1 = u'(3 + \sqrt{10})^{-m}$, y por lo tanto $u' = (3 + \sqrt{10})^m$.

Ahora, si u' es negativo, multipliquemos por -1, y debe de cumplirse que $-u' = (3 + \sqrt{10})^m$ para algún $m \in \mathbb{Z}$; por lo tanto, $u' = -(3 + \sqrt{10})^m$. $\square$

Problema: Encuentre un isomorfismo entre los grupos $U(\mathbb{Z}[\sqrt{10}])$ y $\mathbb{Z}_2 \times \mathbb{Z}$.

Problema: Sea $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : \ a, b \in \mathbb{Z}\}$. Demuestre que la unidad fundamental en éste anillo es $1 + \sqrt{2}$.

Proposición 1.1.29. *Si $\alpha, \beta \in \mathbb{Z}[\sqrt{10}]$ son asociados, entonces $|N(\alpha)| = |N(\beta)|$.*

PROOF. Fácil ejercicio para el lector. □

Problema: Encuentre dos números en $\mathbb{Z}[i]$ con la misma norma y no asociados.

Problema: Encuentre dos números en $\mathbb{Z}[\sqrt{10}]$ con la misma norma y no asociados.

Problema: Demuestre que 2 y $\sqrt{10}$ no son asociados en el anillo $\mathbb{Z}[\sqrt{10}]$.

Problema: Sea A un dominio entero con 1. Demuestre que cualquier elemento primo es irreducible.

En general se tiene que:

Proposición 1.1.30. *Un dominio entero es de factorización única si y sólo si todos los números irreducibles son primos.*

PROOF. Ver la demostración del Teorema 1.1.19. □

En conclusión, basta con encontrar un número irreducible que no sea primo para que un dominio entero no sea de factorización única. En $\mathbb{Z}[\sqrt{10}]$ el número 2 es irreducible, sin embargo $2 \cdot 5 = 10 = \sqrt{10}\sqrt{10}$, así que $2 \mid 10$, pero $2 \nmid \sqrt{10}$. Esto último lo podemos demostrar usando el siguiente lema.

Lema 1.1.31. *Si $\alpha, \beta \in \mathbb{Z}[\sqrt{10}]$ y $\alpha \mid \beta$, entonces $N(\alpha) \mid N(\beta)$.*

PROOF. Fácil ejercicio para el lector. □

Regresemos a nuestra discusión de primo e irreducible. Por ejemplo, en el anillo $\mathbb{Z}[\sqrt{10}]$ tenemos que 7 es un elemento primo, y dos distintas factorizaciones de 70 son:

$$\begin{aligned} 70 &= 2 \cdot 5 \cdot 7 \\ &= \sqrt{10} \cdot \sqrt{10} \cdot 7 \end{aligned}$$

en donde $2, 5, \sqrt{10}$ son irreducibles, pero no son primos, por lo que en algunas factorizaciones sí aparecen y en otras no; sin embargo 7 sí es un elemento primo, y como tal, aparece en las dos factorizaciones de 70. Será posible factorizar (aunque sea teóricamente) cualquier elemento de $\mathbb{Z}[\sqrt{10}]$?

Teorema 1.1.32. *Si $\alpha \in \mathbb{Z}[\sqrt{10}]$, con $\alpha \neq 0$ y no unidad, entonces α se puede escribir como producto finito de irreducibles.*

PROOF. Prueba rápida: Consideremos el conjunto

$$A = \{x \in \mathbb{Z}[\sqrt{10}] \setminus \{0\} : x \text{ no es unidad y } x \text{ no es producto de irreducibles}\}$$

y suponga que $B = \{|N(x)| : x \in A\} \neq \emptyset$. La conclusión es casi inmediata. □

Problema: Escriba los detalles de la demostración del Teorema 1.1.32.

Problema: Con respecto a las dos factorizaciones *diferentes* del número 70 piense usted por qué siempre aparece el 7? Intente formular una conjetura al respecto.

Aparentemente tenemos algo muy bueno (aunque hasta el momento es teórico): la certeza de poder factorizar como producto finito de irreducibles. Ahora surgen otras dudas: sabemos identificar a un elemento irreducible? sabemos distinguir un irreducible de un primo? En general y afortunadamente, la respuesta no es muy alentadora y para muestra basta un botón: El caso del anillo $\mathbb{Z}$, en donde existen muchos misterios por resolver. Por ejemplo, hasta la fecha, absolutamente nadie tiene un algoritmo eficáz para factorizar enteros y más aún, no se tiene un método o prueba (test) que identifique a los primos de $\mathbb{Z}$.

En $\mathbb{Z}[\sqrt{10}]$ el problema de la no factorización única no se hereda al semigrupo de los ideales $\neq 0$ del anillo.

Teorema 1.1.33. *En $\mathbb{Z}[\sqrt{10}]$ todo ideal distinto de $\langle 0\rangle$ y de $\langle 1\rangle$ se factoriza de forma única como producto de ideales primos.*

PROOF. Usualmente se demuestra que el número de clase es finito. Luego la conclusión es fácil. Posponemos la demostración para más adelante. □

Diremos que un ideal I divide al ideal J si existe un tercer ideal K tal que $J = IK$ (es la misma definición de divisibilidad en un anillo). Tenemos la siguiente equivalencia importante: I divide a J si y sólo si I contiene a J, esto es:

$$I \mid J \qquad \text{si y sólo si} \qquad I \supseteq J.$$

En $\mathbb{Z}$, todos los ideales son principales y gracias a esto se cumple

$$\langle a\rangle\langle b\rangle = \langle ab\rangle,$$

así que $a \mid b$ si y sólo si $\langle a\rangle \mid \langle b\rangle$ o equivalentemente

$$a \mid b \qquad \text{si y sólo si} \qquad \langle a\rangle \supseteq \langle b\rangle.$$

Por ejemplo $6 \mid 18$ pues $\langle 6\rangle \supseteq \langle 18\rangle$ y $\langle 6\rangle\langle 3\rangle = \langle 18\rangle$. Ahora daremos algunos ejemplos para ver como podemos utilizar la factorización única en ideales para factorizar a los elementos del anillo. Regresemos a 70 en el anillo $\mathbb{Z}[\sqrt{10}]$.

Sabemos que 70 tiene dos factorizaciones como elemento, pero el ideal principal $\langle 70\rangle$ solamente tiene una factorización en ideales primos:

$$\langle 70\rangle = \langle 2, \sqrt{10}\rangle^2\langle 5, \sqrt{10}\rangle^2\langle 7\rangle.$$

Es importante observar que $\langle 2, \sqrt{10}\rangle$ y $\langle 5, \sqrt{10}\rangle$ se describen usando dos generadores; de hecho, esto es necesario pues estos dos ideales no son principales. Sin embargo

$$\langle 2, \sqrt{10}\rangle^2 = \langle 2\rangle, \quad \langle 5, \sqrt{10}\rangle^2 = \langle 5\rangle, \quad \langle 2, \sqrt{10}\rangle\langle 5, \sqrt{10}\rangle = \langle \sqrt{10}\rangle,$$

así que de aquí se obtienen las dos posibles factorizaciones de 70, la primera

$$\langle 70\rangle = \langle 2, \sqrt{10}\rangle^2\langle 5, \sqrt{10}\rangle^2\langle 7\rangle = \langle 2\rangle\langle 5\rangle\langle 7\rangle$$

y la segunda factorización se obtiene agrupando los ideales no principales de otra forma:

$$\langle 70\rangle = \langle 2, \sqrt{10}\rangle\langle 5, \sqrt{10}\rangle\langle 2, \sqrt{10}\rangle\langle 5, \sqrt{10}\rangle\langle 7\rangle = \langle \sqrt{10}\rangle\langle \sqrt{10}\rangle\langle 7\rangle.$$

El anillo $\mathbb{Z}[\sqrt{10}]$ tiene algunas propiedades que será muy útiles a la hora de agrupar ideales como en el ejemplo anterior.

Proposición 1.1.34. *Sea $\pi \in \mathbb{Z}[\sqrt{10}]$*

i) *π es primo si y sólo si el ideal principal $\langle \pi\rangle$ es primo.*
ii) *π es irreducible, pero no primo, si y sólo si $\langle \pi\rangle = P_1P_2$ donde P_1, P_2 son dos ideales primos tales que ninguno de los dos es principal.*

El inciso i) es válido en cualquier dominio entero, sin embargo, el inciso ii) depende del anillo en el que estamos factorizando. Como consecuencia de lo anterior, para poder clasificar los elementos primos e irreducibles de $\mathbb{Z}[\sqrt{10}]$ basta con encontrar todos los ideales de $\mathbb{Z}[\sqrt{10}]$ y decidir si son o no principales. Por ejemplo

$$I_1 = \langle 2, \sqrt{10}\rangle,\ I_2 = \langle 3, 1+\sqrt{10}\rangle\ , I_3 = \langle 13, 1+2\sqrt{10}\rangle,\ I_4 = \langle 37, 18+5\sqrt{10}\rangle$$

son cuatro ideales primos que no son principales (por qué?) y observamos que el producto

$$I_1I_2I_3I_4 = \langle 2+17\sqrt{10}\rangle$$

es principal. Así que, para encontrar todas las factorizaciones de $2+17\sqrt{10}$ tendremos que encontrar todas las posibles agrupaciones de parejas de estos ideales.

En total son:

$$\begin{aligned} I_1I_2 &= \langle 4+\sqrt{10}\rangle \\ I_1I_3 &= \langle 8+3\sqrt{10}\rangle \\ I_1I_4 &= \langle 42-13\sqrt{10}\rangle \\ I_2I_3 &= \langle 7+\sqrt{10}\rangle \\ I_2I_4 &= \langle 19-5\sqrt{10}\rangle \\ I_3I_4 &= \langle 29+6\sqrt{10}\rangle \\ I_1I_2I_3I_4 &= \langle 4+\sqrt{10}\rangle\langle 29+6\sqrt{10}\rangle \\ I_1I_2I_3I_4 &= \langle 8+3\sqrt{10}\rangle\langle 19-5\sqrt{10}\rangle \\ I_1I_2I_3I_4 &= \langle 42-13\sqrt{10}\rangle\langle 7+\sqrt{10}\rangle \end{aligned}$$

Ahora observemos los siguientes productos:

$$\begin{aligned} \langle 4+\sqrt{10}\rangle\langle 29+6\sqrt{10}\rangle &= \langle 176+53\sqrt{10}\rangle \\ \langle 8+3\sqrt{10}\rangle\langle 19-5\sqrt{10}\rangle &= \langle 2+17\sqrt{10}\rangle \\ \langle 42-13\sqrt{10}\rangle\langle 7+\sqrt{10}\rangle &= \langle 164-49\sqrt{10}\rangle, \end{aligned}$$

y notemos que por ejemplo

$$(164-49\sqrt{10})(3+\sqrt{10})^2 = (2+17\sqrt{10})(3+\sqrt{10}) = 176+53\sqrt{10},$$

y por tanto $164-49\sqrt{10} \sim 176+53\sqrt{10}$. Así que, para encontrar todas las factorizaciones en irreducibles de $2+17\sqrt{10}$ tomamos las tres factorizaciones de ideales anteriores y multiplicamos por la unidad correspondiente. Esto no es un ajuste artificial pues en cualquier anillo conmutativo si u es una unidad y $\langle\alpha\rangle$ es un ideal principal, entonces $\langle\alpha\rangle = \langle u\alpha\rangle$; así que lo que pasa es que tenemos los ideales que necesitamos, pero no están representados con los generadores adecuados. Si al ideal $\langle 29+6\sqrt{10}\rangle$ lo hubiéramos expresado como

$$\langle 29+6\sqrt{10}\rangle = \left\langle \frac{1}{3+\sqrt{10}}(29+6\sqrt{10}) \right\rangle = \langle -27+11\sqrt{10}\rangle,$$

tendríamos

$$\langle 2+17\sqrt{10}\rangle = \langle 4+\sqrt{10}\rangle\langle -27+11\sqrt{10}\rangle,$$

donde ahora sí $2+17\sqrt{10} = (4+\sqrt{10})(-27+11\sqrt{10})$. De la misma forma, si en lugar de $\langle 7+\sqrt{10}\rangle$ tomamos

$$\langle 7+\sqrt{10}\rangle = \langle (7+\sqrt{10})(3+\sqrt{10})\rangle = \langle 31+10\sqrt{10}\rangle$$

encontramos que

$$\langle 2+17\sqrt{10}\rangle = \langle 42-13\sqrt{10}\rangle\langle 31+10\sqrt{10}\rangle.$$

Así que, como estas son las únicas tres posibles agrupaciones de dos en dos de los ideales I_1, I_2, I_3, I_4, entonces las únicas tres factorizaciones de $2+17\sqrt{10}$ son:

$$\begin{aligned} 2+17\sqrt{10} &= (4+\sqrt{10})(-27+11\sqrt{10}) \\ &= (8+3\sqrt{10})(19-5\sqrt{10}) \\ &= (42-13\sqrt{10})(31+10\sqrt{10}). \end{aligned}$$

Cualquier otra factorización que encontremos será equivalente a alguna de estas tres. Por ejemplo, si tomamos la unidad $u = 721 - 228\sqrt{10}$, la primera factorización también la podríamos escribir como:

$$\begin{aligned} 2+17\sqrt{10} &= (4+\sqrt{10})(-27+11\sqrt{10}) \\ &= (4+\sqrt{10})u\frac{1}{u}(-27+11\sqrt{10}) \\ &= (4+\sqrt{10})(721-228\sqrt{10})\frac{-27+11\sqrt{10}}{721-228\sqrt{10}} \\ &= (604-191\sqrt{10})(5613+1775\sqrt{10}). \end{aligned}$$

De esta forma hemos obtenido otra factorización de $2+\sqrt{17}$, pero esencialmente $(4+\sqrt{10})(-27+11\sqrt{10})$ y $(604-191\sqrt{10})(5613+1775\sqrt{10})$ son la misma factorización pues $4+\sqrt{10}$ y $604-191\sqrt{10}$ son asociados y $-27+11\sqrt{10}$ y $5613+1775\sqrt{10}$ también lo son.

Finalizaremos el estudio del anillo $\mathbb{Z}[\sqrt{10}]$ enunciando algunos resultados (sin demostrasión) que nos permitirán saber cuáles son los ideales primos del anillo y para distinguir si son o no principales.

Proposición 1.1.35. *Dado un ideal primo P de $\mathbb{Z}[\sqrt{10}]$, existe $p \in \mathbb{Z}$ primo tal que $P \mid \langle p \rangle$.*

El resultado anterior nos dice que basta con estudiar cómo se factorizan los ideales de la forma $\langle p \rangle$ para todos los primos p de $\mathbb{Z}$ con el objeto de encontrar todos los ideales primos de $\mathbb{Z}[\sqrt{10}]$; que es lo que tenemos gracias a la siguiente proposición.

Proposición 1.1.36. *El ideal $\langle p \rangle$ se factoriza como producto de ideales primos de acuerdo a las siguientes condiciones:*

i) *Si $p = 2$ ó $p = 5$, $\langle p \rangle = \langle p, \sqrt{10} \rangle^2$.*
ii) *Si $p \equiv 1, 3, 9, 13, 27, 31, 37, 39 \pmod{40}$ la ecuación $a^2 \equiv 10 \pmod{p}$ tiene solución, y dado un valor de a, $\langle p \rangle = \langle p, a+\sqrt{10} \rangle \langle p, a-\sqrt{10} \rangle$.*
iii) *Si $p \equiv 7, 11, 17, 19, 21, 23, 29, 33 \pmod{40}$, entonces $\langle p \rangle$ es un ideal primo.*

Notemos que cualquier otra posibilidad módulo 40 nos da un múltiplo de 2 o un múltiplo de 5, que no pueden ser números primos, por lo que estos dieciocho casos cubren a todos los primos de $\mathbb{Z}$ módulo 40. Por ejemplo, 53 es un primo congruente

con 13 módulo 40, así que cumple la condición del caso ii). Una solución de $a^2 \equiv 10 \pmod{53}$ es 13. Por lo tanto

$$\langle 53\rangle = \langle 53, 13+\sqrt{10}\rangle\langle 53, 13-\sqrt{10}\rangle.$$

Por otro lado, $97 \equiv 17 \pmod{40}$, así que el ideal $\langle 97\rangle$ es un ideal primo de $\mathbb{Z}[\sqrt{10}]$.

Finalmente, para poder clasificar a los primos y los irreducibles de $\mathbb{Z}[\sqrt{10}]$ tenemos que saber cuando un ideal primo es principal y cuando no lo es. En el caso del inciso iii) es claro que los ideales primos $\langle p\rangle$ son principales, y en el inciso i) el proceso es finito, por lo que podemos verificar que ninguno de los dos ideales es principal. Así que el principal problema son los ideales del inciso ii).

Proposición 1.1.37. *Sea P un ideal primo. P es principal si y sólo si se cumple alguna de las siguientes condiciones:*

i) $P = \langle p\rangle$ *con* $p \equiv 7, 11, 17, 19, 21, 23, 29, 33 \pmod{40}$.
ii) $P = \langle p, a \pm \sqrt{10}\rangle$ *con* $p \equiv 1, 9, 31, 39 \pmod{40}$.

P no es principal si y sólo si se cumple alguna de las siguientes condiciones:

iii) $P = \langle 2, \sqrt{10}\rangle$.
iv) $P = \langle 5, \sqrt{10}\rangle$.
v) $P = \langle p, a \pm \sqrt{10}\rangle$ *con* $p \equiv 3, 13, 27, 37 \pmod{40}$

Con esto ya sabemos cuándo un ideal es principal y cuándo no lo es, lo que nos ayuda a encontrar todos los primos y los irreducibles de $\mathbb{Z}[\sqrt{10}]$, pues sabemos que si P es un ideal primo principal, entonces cualquier generador de P es un elemento primo, y si P_1, P_2 son dos ideales primos no principales, el producto de ellos va a ser un ideal principal generado por un irreducible que no es primo. Por ejemplo $\langle 53, 13+\sqrt{10}\rangle$ y $\langle 53, 13-\sqrt{10}\rangle$ son ideales primos que no son principales, pues $53 \equiv 13 \pmod{40}$, por lo que $\langle 53\rangle$, que es el producto de éstos, es un ideal principal que es producto de dos ideales primos no principales, lo que nos indica que en $\mathbb{Z}[\sqrt{10}]$ el número 53 es irreducible, pero no es un número primo. De hecho, esto mismo sucede con cualquier primo p de $\mathbb{Z}$ congruente con 3, 13, 27 ó 37 módulo 40.

Finalmente tenemos el siguiente criterio, que es consecuencia de todo lo anterior:

Teorema 1.1.38. *Sean $\pi = a+b\sqrt{10}$ un elemento de $\mathbb{Z}[\sqrt{10}]$ y $N(\pi) = a^2-10b^2$. π es un elemento primo si y sólo si se cumple una de las dos condiciones siguientes:*

i) $|N(\pi)| = p$, *con p un primo de $\mathbb{Z}$,* $p \equiv 1, 9, 31, 39 \pmod{40}$.
ii) $|N(\pi)| = p^2$ *con p un primo de $\mathbb{Z}$,* $p \equiv 7, 11, 17, 19, 21, 23, 29, 33 \pmod{40}$.

y π es un irreducible si y sólo si cumple alguna de las siguientes condiciones:

i) π *es primo.*
ii) $|N(\pi)| = pq$ *con* p *y* q *dos primo de* $\mathbb{Z}$ *(que pueden ser iguales o distintos),* $p \equiv 2, 3, 5, 13, 27, 37 \pmod{40}$.

Capítulo 2

Ejemplos y resultados generales

En este capítulo daremos algunos resultados básicos de la teoría de números algebraicos de una forma más general que la que usamos en el capítulo anterior.

2.1. Campos de números y anillos de enteros

Definición 2.1.1. *Un número complejo z es un entero algebraico si z es raíz de un polinomio mónico con coeficientes enteros $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$.*

Definición 2.1.2. *Decimos que K es un campo de números si $K/\mathbb{Q}$ es una extensión de campos finita.*

El anillo de enteros de un campo de números K es el conjunto

$$\mathcal{O}_K = \{x \in K : x \text{ es un entero algebraico}\}.$$

La primera pregunta que surge es, si tenemos un campo de números, cuál es su anillo de enteros? Una forma de responder esta pregunta es dando una base entera de K.

Definición 2.1.3. *Una base entera de un campo de números K es una base de K como $\mathbb{Q}$-espacio vectorial, $\alpha_1, \ldots, \alpha_n$ tal que $\alpha_i \in \mathcal{O}_K$ para $1 \leq i \leq n$ y además es una base de $\mathcal{O}_K$ como $\mathbb{Z}$-módulo, es decir,*

$$\mathcal{O}_K = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \cdots \alpha_n\mathbb{Z}.$$

Un concepto que nos permite saber si una base genera al anillo de enteros como $\mathbb{Z}$-módulo es el discriminante, para esto, tenemos que definir la traza de un elemento de K.

Definición 2.1.4. *Sean $K/\mathbb{Q}$ una extensión de grado n, $\alpha \in K$ un elemento y $\sigma_1, \sigma_2, \ldots, \sigma_n$ los n monomorfismos $\sigma_i : K \to \mathbb{C}$ (se puede demostrar que existen exactamente n). Definimos la traza de α como*

$$t(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_n(\alpha).$$

La norma de α se define

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

Por ejemplo, en el campo $K = \mathbb{Q}(\sqrt{10})$ los dos monomorfismos de K a $\mathbb{C}$ son la identidad, que llamaremos σ_1 y la conjugación, que es la función

$$\sigma_2(a + b\sqrt{10}) = a - b\sqrt{10}.$$

Así que la traza de un elemento arbitrario $\alpha = a + b\sqrt{10}$ es

$$t(a+b\sqrt{10}) = \sigma_1(a+b\sqrt{10}) + \sigma_2(a+b\sqrt{10}) = (a+b\sqrt{10}) + (a-b\sqrt{10}) = 2a,$$

y su norma es

$$N(a+b\sqrt{10}) = \sigma_1(a+b\sqrt{10})\sigma_2(a+b\sqrt{10}) = (a+b\sqrt{10})(a-b\sqrt{10}) = a^2-10b^2.$$

Proposición 2.1.5. *Sea K un campo de números tal que $[K : Q] = n$. Si $\alpha, \beta \in K$ y $c \in \mathbb{Q}$, entonces:*

i) $N(\alpha\beta) = N(\alpha)N(\beta)$.
ii) $N(c) = c^n$.
iii) $t(\alpha + \beta) = t(\alpha) + t(\beta)$.
iv) $t(c) = nc$.

PROOF. La demostración se deja de ejercicio (Sugerencia: Usar al hecho de que los σ_i son homomorfismos del campo K). □

Una propiedad importante de los enteros algebraicos es que:

Proposición 2.1.6. *Si $\alpha \in K$ es un entero algebraico, entonces $t(\alpha)$ y $N(\alpha)$ están en $\mathbb{Z}$.*

PROOF. Sea $p(x) = x^n + a_{n-1}^{n-1} + \cdots + a_1x + a_0$ el polinomio irreducible de α. Usando teoría de Galois se puede ver que $t(\alpha) = a_{n-1}$ y $N(\alpha) = a_0$, y como el polinomio irreducible de un entero algebraico está en $\mathbb{Z}[x]$, entonces el resultado es cierto. □

Definición 2.1.7. *Sea $\alpha_1, \ldots, \alpha_n$ una base entera del campo K. Sea M la matriz (a_{ij}) donde $a_{ij} = t(\alpha_i\alpha_j)$. El discriminante del campo K se define como $\delta_K = det(M)$.*

El discriminante de un campo es un concepto muy importante pues nos ayuda a identificar cuando un conjunto de elementos de $\mathcal{O}_K$ es una base entera y además nos da información sobre la factorización de algunos ideales de $\mathcal{O}_K$. Sin embargo, en este texto no veremos como se utiliza.

Existen algoritmos para encontrar una base entera y el discriminante de cualquier campo de números, sin embargo, un problema interesante es encontrar una base entera explícita para alguna familia de campos. A continuación daremos algunos ejemplos.

2.2. Campos cuadráticos

Un campo cuadrático es un campo de números K tal que $[K : \mathbb{Q}] = 2$. Se puede ver que cualquier campo cuadrático es de la forma $K = \mathbb{Q}(\sqrt{d})$ con d un entero libre de cuadrados, así que los elementos de K son de la forma $a + b\sqrt{d}$ con $a, b \in \mathbb{Q}$. Si d es positivo, diremos que K es un campo cuadrático real ya que $K \subseteq \mathbb{R}$, y en caso de ser negativo lo llamaremos campo cuadrático imaginario, debido a que una parte del campo no cae en $\mathbb{R}$. Los dos monomorfismos que van de K a los

números complejos son la identidad σ_1 y la conjugación $\sigma_2(a+b\sqrt{d}) = a - b\sqrt{d}$, así que

$$t(a+b\sqrt{d}) = 2a, \quad N(a+b\sqrt{d}) = a^2 - db^2.$$

Lema 2.2.1. *Sea $K = \mathbb{Q}(\sqrt{d})$ y $\alpha = a + b\sqrt{d} \in K$ con $a, b \in \mathbb{Q}$. Entonces, $\alpha \in \mathcal{O}_K$ si y sólo si $2a, 2b \in \mathbb{Z}$ y $(2a)^2 - (2b)^2 d \equiv 0 \pmod 4$.*

PROOF. Supongamos que $\alpha \in \mathcal{O}_K$. Sabemos que $t(\alpha), N(\alpha) \in \mathbb{Z}$, esto es $2a \in \mathbb{Z}$ y $a^2 - b^2 d \in \mathbb{Z}$. Así, $(2a)^2 - (2b)^2 d \in 4\mathbb{Z}$, esto es $(2a)^2 \equiv (2b)^2 d \pmod 4$. Ya que $2a \in \mathbb{Z}$, entonces $(2b)^2 d \in \mathbb{Z}$ y $(2b)^2 d \equiv 0, 1 \pmod 4$. Tenemos dos opciones, si $(2a)^2 \equiv 0 \pmod 4$, entonces, como d es libre de cuadrados, $4b^2 \equiv 0 \pmod 4$ y $b \in \mathbb{Z}$. Si $(2a)^2 \equiv 1 \pmod 4$, entonces $d \equiv 1 \pmod 4$ y $(2b)^2 \equiv 1 \pmod 4$, y por lo tanto $2b$ es un entero impar.

Inversamente, si $2a, 2b \in \mathbb{Z}$ y $(2a)^2 - (2b)^2 d \equiv 0 \pmod 4$, entonces $a^2 - b^2 d \in \mathbb{Z}$. Por lo tanto $p(x) = x^2 - 2ax + (a^2 - b^2 d) \in \mathbb{Z}[x]$ es un polinomio mónico con coeficientes enteros tal que $p(a + b\sqrt{d}) = 0$ y $\alpha \in \mathcal{O}_K$. □

Corolario 2.2.2. *Tómese la extensión $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ con d libre de cuadrados. Si $d \equiv 2, 3 \pmod 4$ entonces una base entera de $\mathcal{O}_K$ es $\{1, \sqrt{d}\}$ y si $d \equiv 1 \pmod 4$ entonces $\left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$ es una base entera de $\mathcal{O}_K$.*

PROOF. Sea $\alpha = a + b\sqrt{d} \in \mathcal{O}_K$. Si $d \equiv 2 \equiv -2 \pmod 4$, entonces

$$0 \equiv (2a)^2 - (2b)^2 d \equiv (2a)^2 + 2(2b)^2 \pmod 4,$$

y si $d \equiv 3 \equiv -1 \pmod 4$, entonces

$$0 \equiv (2a)^2 - (2b)^2 d \equiv (2a)^2 + (2b)^2 \pmod 4.$$

En cualquiera de los dos casos, $2a$ y $2b$ tienen que ser enteros pares, y por lo tanto $a, b \in \mathbb{Z}$, esto quiere decir que a y b son enteros. Por lo tanto, usando el lema anterior, tenemos que α es un entero algebraico si y sólo si $a, b \in \mathbb{Z}$, y una base entera es $\{1, \sqrt{d}\}$.

Ahora supongamos que $d \equiv 1 \pmod 4$. Tenemos que $(2a)^2 - (2b)^2 d \equiv (2a)^2 - (2b)^2 \equiv 0 \pmod 4$. Entonces $(2a)^2 \equiv (2b)^2 \pmod 4$ y $2a \equiv 2b \pmod 2$.

Podemos escribir

$$\begin{aligned}\alpha = a + b\sqrt{d} &= \frac{2(a+b\sqrt{d})}{2} = \frac{2a-2b}{2} + \frac{2b+2b\sqrt{d}}{2} \\ &= \frac{2a-2b}{2} + 2b\frac{1+\sqrt{d}}{2},\end{aligned}$$

y ya que $\frac{2a-2b}{2}, 2b \in \mathbb{Z}$, entonces se cumple que $\mathcal{O}_K \subseteq \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$. Para la otra contención es suficiente mostrar que $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$. Puesto que $\frac{1-d}{4} \in \mathbb{Z}$, se tiene que $f(x) = x^2 + x + \frac{1-d}{4} \in \mathbb{Z}[x]$ es irreducible por el criterio de Eisenstein.

Además $f\left(\frac{1+\sqrt{d}}{2}\right) = 0$ y por lo tanto $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$. Esto quiere decir que una base entera de $\mathcal{O}_K$ es $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$. □

Usando el resultado del corolario anterior, calcularemos el discriminante de $K = \mathbb{Q}(\sqrt{d})$.

Corolario 2.2.3. *Sea δ_K el discriminante de $K = \mathbb{Q}(\sqrt{d})$ con d un entero libre de cuadrados. Si $d \equiv 2, 3 \pmod 4$, entonces $\delta_K = 4d$. Si $d \equiv 1 \pmod 4$, entonces $\delta_K = d$.*

PROOF. Si $d \equiv 2, 3 \pmod 4$ sabemos que $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Sean $\alpha_1 = 1$ y $\alpha_2 = \sqrt{d}$. Entonces, como $\{\alpha_1, \alpha_2\}$ es una base entera de $\mathcal{O}_K$, se tiene que

$$\delta_K = \det(t(\alpha_i\alpha_j)) = \det\begin{pmatrix} t(1) & t(\sqrt{d}) \\ t(\sqrt{d}) & t(d) \end{pmatrix} = \det\begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

Si $d \equiv 1 \pmod 4$ entonces $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$. Sean $\alpha = 1$ y $\alpha_2 = \frac{1+\sqrt{d}}{2}$. Entonces

$$\begin{aligned}\delta_K &= \det(t(\alpha_i\alpha_j)) \\ &= \det\begin{pmatrix} t(1) & t\left(\frac{1+\sqrt{d}}{2}\right) \\ t\left(\frac{1+\sqrt{d}}{2}\right) & t\left(\left(\frac{1+\sqrt{d}}{2}\right)^2\right) \end{pmatrix} \det\begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = d.\end{aligned}$$

□

2.3. Otros ejemplos de bases enteras

Existen otros ejemplos en los que se tiene explícitamente una base entera de una familia de campos de números.

Proposición 2.3.1. *Sean $\xi = e^{(2\pi i/n)}$ una raíz n-ésima primitiva de la unidad y $K = \mathbb{Q}(\xi)$. K es una extensión finita sobre $\mathbb{Q}$ de grado $\phi(n)$ (donde ϕ es la función ϕ de Euler) y*

$$\{1, \xi, \xi^2, \ldots, \xi^{\phi(n)-2}, \xi^{\phi(n)-1}\}$$

es una base entera de K.

Por ejemplo, $\xi = e^{(2\pi i/5)}$ es una raíz quinta primitiva de la unida, y $K(\xi)$ es una extensión de $\mathbb{Q}$ de grado 4, por lo que es un campo de números. Una base entera de K es

$$\{1, \xi, \xi^2, \xi^3\} = \{1, e^{(2\pi i/5)}, e^{(4\pi i/5)}, e^{(6\pi i/5)}\}.$$

El elemento ξ^4 también es un elemento de K, pero no está en la base entera. De hecho, no es necesario agregarlo pues $1 + \xi + \xi^2 + \xi^3 + \xi^4 = 0$, y por lo tanto

$$\xi^4 = -1 - \xi - \xi^2 - \xi^3,$$

así que se puede escribir como combinación lineal de los elementos de la base entera usando coeficientes enteros.

Si ξ es una raíz n-ésima primitiva de la unidad, la intersección de $\mathbb{Q}(\xi)$ con $\mathbb{R}$ es una extensión de grado $\phi(n)/2$, tomando en cuenta que $\phi(n)$ es par si $n \geq 3$. Sea $\varepsilon = \xi + \dfrac{1}{\xi}$, una base entera de $\mathbb{Q}(\xi) \cap \mathbb{R}$ es

$$\{1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{(\phi(n)-1)/2}\}.$$

Cuando existe α tal que la base entera de un campo de números es de la forma $\{1, \alpha, \ldots, \alpha^k\}$ se dice que ésta es una base entera de potencias, y el anillo de enteros es igual a $\mathbb{Z}[\alpha]$, es decir, los polinomios con coeficientes enteros evaluados en α. Todos los ejemplos que hemos dado son campos de números que tienen una base entera de potencias, sin embargo, éstas no son tan frecuentes, de hecho, se sabe que hay una infinidad de campos que no tienen una base entera de potencias. Algunos de estos se dan en los campos cúbicos.

Proposición 2.3.2. *Sean $d = ab^2$ un entero libre de cubos, con a, b libres de cuadrados, y $K = \mathbb{Q}(\sqrt[3]{d})$. Una base entera de K es:*

i) *Si $d \equiv 1 \pmod 9$,*

$$\left\{ \sqrt[3]{ab^2}, \sqrt[3]{a^2b}, \frac{1 + \sqrt[3]{ab^2} + \sqrt[3]{a^2b^4}}{3} \right\}$$

es una base entera de K.

ii) *Si $d \equiv 8 \pmod 9$, entonces*

$$\left\{ \sqrt[3]{ab^2}, \sqrt[3]{a^2b}, \frac{1 - \sqrt[3]{ab^2} + \sqrt[3]{a^2b^4}}{3} \right\}$$

es una base entera de K.

iii) *Si $d \not\equiv 1, 8 \pmod 9$, entonces*

$$\left\{1, \sqrt[3]{ab^2}, \sqrt[3]{a^2b}\right\}$$

es una base entera de K.

Por ejemplo, $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$ es una base entera del anillo de enteros de la extensión $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$.

2.4. Factorización en un campo de números

Ya vimos en el caso de $\mathbb{Z}[\sqrt{10}]$ que para encontrar los ideales primos basta con factorizar los ideales de la forma $\langle p \rangle$ para todos los primos p de $\mathbb{Z}$. Lo mismo sucede en todos los anillos de enteros. El siguiente resultado nos ayuda a resolver este problema de una forma mucho más general.

Teorema 2.4.1. [Teorema de Kummer] *Sean $K = \mathbb{Q}(\alpha)$ un campo de números de grado n con*

$$\mathcal{O}_K = \mathbb{Z}[\alpha] = \mathbb{Z} + \alpha\mathbb{Z} + \alpha^2\mathbb{Z} + \cdots + \alpha^{n-1}\mathbb{Z},$$

p un primo en $\mathbb{Z}$ y $f(x)$ el irreducible de α en $\mathbb{Q}$ y $\overline{f}(x)$ el polinomio f considerado en $\mathbb{Z}/p\mathbb{Z}$ usando el mapeo natural. $f(x)$ se puede factorizar como

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

donde $\overline{g_1}(x), \ldots, \overline{g_r}(x)$ son polinomios mónicos irreducibles distintos en $\mathbb{Z}/p\mathbb{Z}[x]$ y $e_1, \ldots, e_e$ son enteros. Para cada i tomemos un polinomio $g_i(x)$ en $\mathbb{Z}[x]$ tal que el mapeo natural manda $g_i(x)$ a $\overline{g_i}(x)$, y definamos

$$P_i = \langle p, g_i(\alpha) \rangle.$$

Todos los P_i son ideales primos con norma $N(P_i) = p^{gr(g_i)}$, y además podemos factorizar al ideal $\langle p \rangle$ como

$$\langle p \rangle = P_1^{e_1} \cdot P_2^{e_1} \cdots P_r^{e_r}.$$

En los campos cuadráticos, podemos aplicar el resultado anterior y obtener:

Proposición 2.4.2. *Sea $p \in \mathbb{Z}$ un primo impar y δ_K el discriminante de $K = \mathbb{Q}(\sqrt{d})$.*

i) *Si $p \nmid \delta_K$ y la congruencia $x^2 \equiv d \pmod{p}$ tiene solución en $\mathbb{Z}$, entonces $\langle p \rangle = P_1 P_2$ donde P_1, P_2 son dos ideales primos distintos.*
ii) *Si $p \nmid \delta_K$ y la congruencia $x^2 \equiv d \pmod{p}$ no tiene solución en $\mathbb{Z}$, entonces $\langle p \rangle$ es un ideal primo.*
iii) *Si $p \mid \delta_K$ entonces $\langle p \rangle = P^2$, para un ideal primo P.*

Proposición 2.4.3. *Sea $p = 2$ y δ_K el discriminante de K.*

i) *Si $2 \nmid \delta_K$ y $d \equiv 1 \pmod{8}$, entonces $\langle 2 \rangle = P_1 P_2$ donde P_1, P_2 son dos ideales primos distintos.*
ii) *Si $2 \nmid \delta_K$ y $d \equiv 5 \pmod{8}$, entonces $\langle 2 \rangle$ es primo.*
iii) *Si $2 \mid \delta_K$, esto es, $d \equiv 2, 3 \pmod{4}$, entonces $\langle 2 \rangle = P^2$ donde P es un ideal primo.*

Para demostrar estos dos resultados, podemos usar el hecho de que la base de un campo cuadrático es de la forma $1, \alpha$, y por lo tanto, cumple la hipótesis del Teorema de Kummer.

Podemos dar los generadores de los ideales primos que nos indican las dos proposiciones anteriores. Por ejemplo, si $d \equiv 1 \pmod{8}$,

$$\langle 2 \rangle = \left\langle 2, \frac{1 + \sqrt{d}}{2} \right\rangle \left\langle 2, \frac{1 - \sqrt{d}}{2} \right\rangle,$$

y si $d \equiv 2 \pmod{4}$ $\langle 2 \rangle = \langle 2, \sqrt{d} \rangle^2$; y finalmente, si $d \equiv 3 \pmod{4}$ entonces

$$\langle 2 \rangle = \langle 2, 1 + \sqrt{2} \rangle^2.$$

En el caso de los primos impares, si existe $a \in \mathbb{Z}$ tal que $a^2 \equiv d \pmod{p}$, entonces

$$\langle p \rangle = \langle p, a + \sqrt{d} \rangle \langle p, a - \sqrt{d} \rangle.$$

Y si $p \mid \delta_K$ entonces $p \mid d$ y

$$\langle p \rangle = \langle p, \sqrt{d} \rangle^2.$$

Por ejemplo, el anillo de enteros de $K = \mathbb{Q}(\sqrt{10})$ es $\mathbb{Z}[\sqrt{10}]$. En $\mathcal{O}_K$,

$$\langle 2 \rangle = \langle 2, \sqrt{10} \rangle^2, \quad \langle 5 \rangle = \langle 5, \sqrt{10} \rangle^2.$$

Si $p = 3$, $1^2 \equiv 10 \pmod{3}$, entonces

$$\langle 3 \rangle = \langle 3, 1 + \sqrt{10} \rangle \langle 3, 1 - \sqrt{10} \rangle.$$

Finalmente, $x^2 \equiv 10 \pmod{7}$ no tiene solución, entonces $\langle 7 \rangle$ es un ideal primo.

Ahora consideremos el campo $K = \mathbb{Q}(\xi)$, donde $\xi = e^{2\pi i/5}$. Ya mencionamos que una base entera de K es $1, \xi, \xi^2, \xi^3$, por lo que podemos utilizar el Teorema de Kummer. El polinomio irreducible de ξ es

$$f(x) = x^4 + x^3 + x^2 + x + 1.$$

Así, si queremos encontrar la factorización de $\langle 2 \rangle$, debemos de factorizar $f(x)$ en $\mathbb{Z}/2\mathbb{Z}[x]$. En este caso, el polinomio sigue siendo irreducible, por lo tanto $\langle 2 \rangle$ es un ideal primo. Lo mismo sucede con $\langle 3 \rangle$. Por otro lado, en $\mathbb{Z}/5\mathbb{Z}[x]$, el polinomio se factoriza como:

$$x^4 + x^3 + x^2 + x + 1 = (4 + x)^4.$$

El teorema nos dice que, en este caso,

$$\langle 5 \rangle = \langle 5, 4 + \xi \rangle^4.$$

Por otro lado, en $\mathbb{Z}/11\mathbb{Z}[x]$ tenemos

$$x^4 + x^3 + x^2 + x + 1 = (2 + x)(6 + x)(7 + x)(8 + x),$$

entonces

$$\langle 11 \rangle = \langle 11, 2 + \xi \rangle \langle 11, 6 + \xi \rangle \langle 11, 7 + \xi \rangle \langle 11, 8 + \xi \rangle.$$

En $\mathbb{Z}/19\mathbb{Z}[x]$

$$x^4 + x^3 + x^2 + x + 1 = (1 + 5x + x^2)(1 + 5x + x^2),$$

por lo que

$$\langle 19 \rangle = \langle 1 + 5\xi + \xi^2 \rangle \langle 1 + 15\xi + \xi^2 \rangle.$$

Ahora hagamos algunos ejemplos en el anillo de enteros de $\mathbb{Q}(\sqrt[3]{5})$, que como ya dijimos, una base entera de este campo es $1, \sqrt[3]{5}, \sqrt[3]{25}$, y cumple las condiciones del Teorema de Kummer. El polinomio irreducible de $\sqrt[3]{5}$ es $x^3 - 5$, así que tenemos que factorizar este polinomio en algunos campos finitos para poder factorizar los primos de $\mathbb{Z}$. Por ejemplo, módulo 2

$$x^3 - 5 = (1 + x)(1 + x + x^2)$$

y por lo tanto

$$\langle 2 \rangle = \langle 2, 1 + \sqrt[3]{5} \rangle \langle 2, 1 + \sqrt[3]{5} + \sqrt[3]{25} \rangle.$$

En $\mathbb{Z}/3\mathbb{Z}$, $x^3 - 5 = (1 + x)^3$, por lo que

$$\langle 3\rangle = \langle 3, 1 + \sqrt[3]{5}\rangle^3.$$

Módulo 7, el polinomio $x^3 - 5$ es irreducible, entonces $\langle 7\rangle$ es un ideal primo. En $\mathbb{Z}/13\mathbb{Z}[x]$ el polinomio se factoriza

$$x^3 - 5 = (2 + x)(5 + x)(6 + x),$$

así que

$$\langle 13\rangle = \langle 13, 2 + \sqrt[3]{5}\rangle\langle 13, 5 + \sqrt[3]{5}\rangle\langle 13, 6 + \sqrt[3]{5}\rangle.$$

2.5. Grupo de unidades en anillos de enteros de campos cuadráticos

En esta sección vamos a estudiar el grupo de unidades del anillo de enteros de un campo cuadrático. Sea $K = \mathbb{Q}(\sqrt{d})$. El primer caso que estudiaremos será cuando d es negativo. En este caso el grupo de unidades es un grupo finito. Posteriormente veremos lo que sucede en el caso d positivo. No podremos decir exactamente cuáles son las unidades, sin embargo, veremos que todas dependen de una de ellas.

Tenemos que empezar por dar un criterio para identificar unidades en un anillo de enteros.

Proposición 2.5.1. *Sea $K = \mathbb{Q}(\sqrt{d})$ y $\alpha \in \mathcal{O}_K$. Entonces α es una unidad si y sólo si $|N(\alpha)| = 1$.*

PROOF. La demostració es igual que la que dimos en $\mathbb{Z}[\sqrt{10}]$, por lo que se deja como ejercicio. □

Ya que tenemos un criterio para saber si un entero algebraico es unidad, procederemos a encontrar el grupo de unidades de los anillos de enteros que nos interesan. Empezaremos con el caso $d < 0$ y libre de cuadrados. Denotemos al grupo de unidades de $\mathcal{O}_K = \mathbb{Q}(\sqrt{d})$ como U_d.

Proposición 2.5.2. *Sea $d < 0$ un entero racional libre de cuadrados. Entonces*

i) $U_{-1} = \{\pm 1, \pm i\}$.

ii) $U_{-3} = \{\pm 1, \pm\omega, \pm\omega^2\}$ *donde* $\omega = \dfrac{-1 + \sqrt{-3}}{2}$.

iii) $U_d = \{\pm 1\}$ *para* $d = -2$ *ó* $d < -1$.

PROOF. En el caso $d \equiv 2, 3 \pmod 4$ sabemos que $\mathcal{O}_K = \mathbb{Z} + \sqrt{d}\mathbb{Z}$, por lo que cualquier unidad α se puede escribir como $\alpha = a + b\sqrt{d}$ con $a, b \in \mathbb{Z}$. Si $d = -1$, sabemos que el valor absoluto de la norma de α es igual a 1 si y sólo si $a^2 + b^2 = 1$. Las soluciones enteras de esta ecuación son $a = \pm 1, b = 0$ y $a = 0, b = \pm 1$. Por lo tanto,

$$U_{-1} = \{\pm 1, \pm i\}.$$

Si $d < -1$, tenemos que $a^2 + |d|b^2 = 1$. Así que necesariamente $b = 0$. Por lo tanto, las únicas soluciones son $a = \pm 1, b = 0$. Esto nos da el inciso iii) cuando $d \equiv 2, 3 \pmod 4$.

Si $d \equiv 1 \pmod 4$, $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Entonces las unidades las podemos escribir como

$$\alpha = \frac{a + \sqrt{d}b}{2}$$

con $a, b \in \mathbb{Z}$ y $a \equiv b \pmod 2$. Ahora, $|N(\alpha)| = 1$ si y sólo si $a^2 + |d|b^2 = 4$.

Si $d = -3$ tenemos que resolver la ecuación, $a^2 + 3b^2 = 4$. Las únicas soluciones enteras son $a = \pm 2, b = 0$ y $a = \pm 1, b = \pm 1$. Si $a = \pm 2, b = 0$ entonces ± 1 son unidades. Si $a = -1$ y $b = 1$, entonces

$$\omega = \frac{-1 + \sqrt{-3}}{2}$$

es unidad y por lo tanto $\pm\omega$, $\pm\omega^2 \in U_{-3}$.

Si $d < -3$ tenemos la igualdad $a^2 + |d|b^2 = 4$. Como $|d| > 4$, necesariamente $b = 0$. Por lo tanto $a = \pm 2$, lo que nos da el resultado iii) con $d \equiv 1 \pmod 4$. □

Notamos que en los tres casos, el grupo de unidades es cíclico. Ahora encontraremos el grupo de unidades de un anillo de enteros de un campo cuadrático real. Estos dependen de una unidad a la que llamaremos *unidad fundamental*.

Proposición 2.5.3. *Sea $K = \mathbb{Q}(\sqrt{d})$ con $d > 0$ y libre de cuadrados. Existe una unidad $u > 1$ (unidad fundamental) tal que cada unidad de $\mathcal{O}_K$ es de la forma $\pm u^n$ con $n \in \mathbb{Z}$.*

PROOF. Esta demostración se deja como ejercicio. Se deben de seguir los siguientes pasos.

i) Vamos a dar por hecho que la Ecuación de Pell, $x^2 - dy^2 = 1$, tiene al menos una solución en $\mathbb{Z}$ con $x \geq 1$ y $y \geq 1$ (ver [**35**], pag. 88).
ii) Usando estos valores, podemos garantizar que existe una unidad $M = x + y\sqrt{d}$ que es mayor que 1.
iii) Demostrar que en el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ hay un número finito de elementos α tales que $-M \leq \alpha \leq M$.
iv) Sea $\mu = a + b\sqrt{d}$ ó $\mu = \frac{a + b\sqrt{d}}{2}$ una unidad. Pruebe que $a - b\sqrt{d}$, $-a + b\sqrt{d}$ y $-a - b\sqrt{d}$ también son unidades (en el segundo caso, dividiendo entre 2). Además, pruebe que exactamente una de éstas es mayor que 1.
v) Usando la información anterior, podemos asegurar que hay un número finito de unidades μ tales que $1 < \mu \leq M$.
vi) Sea ϵ la menor de las unidades que se encuentran en este intervalo (Por qué existe una mínima?).

vii) Use el procedimiento que se uso en $\mathbb{Z}[\sqrt{10}]$ para demostrar que, en el anillo de enteros de $\mathbb{Q}(\sqrt{d})$, cualquier unidad es de la forma $\pm\epsilon^n$. ϵ es la unidad fundamental.

□

K	Unidad fundamental de $\mathcal{O}_K$
$\mathbb{Q}(\sqrt{2})$	$1+\sqrt{2}$
$\mathbb{Q}(\sqrt{3})$	$2+\sqrt{3}$
$\mathbb{Q}(\sqrt{7})$	$8+3\sqrt{7}$
$\mathbb{Q}(\sqrt{11})$	$10+3\sqrt{11}$
$\mathbb{Q}(\sqrt{15})$	$4+\sqrt{15}$
$\mathbb{Q}(\sqrt{22})$	$197+42\sqrt{22}$
$\mathbb{Q}(\sqrt{31})$	$1520+273\sqrt{31}$
$\mathbb{Q}(\sqrt{94})$	$2143295+221064\sqrt{94}$
$\mathbb{Q}(\sqrt{165})$	$\frac{13+\sqrt{165}}{2}$

Bibliografía

[1] Adams W. W., and Goldstein L. J., *Introduction to Number Theory*. Prentice-Hall 1976.

[2] Andrews G. E., *Number Theory*. Dover 1994.

[3] Ellison W.J., Ellison J.P. *et al*. The diophantine equation $y^2 + k = x^3$. J. Number Theory **4** (1972), 107-117.

[4] Enzenberger H. M., *El diablo de los Números*. Siruela 1998.

[5] Finkelstein R., London H., *On Mordell's equation $y^2 - k = x^3$: an interesting case of Sierpinski*. J. Number Theory **2**, 310-321 (1970).

[6] Flannery D., *The square root of 2: a dialogue concerning a number and a sequence*. Copernicus-Springer-Verlag, 2006.

[7] Gallian J. A. and Winters S., *Modular Arithmetic in the Marketplace*. American Mathematical Montly, **95** No. 6, 548-551 (1988).

[8] Gardner M., *On Expressing Integers as the Sums of Cubes and Other Unsolved Number-Theory Problems*. Scientific American, **229**, 118-121 (1973).

[9] Gauss K. F., *Disquisitiones Arithmeticae*. Traducción del latín al español por Hugo Barrantes Campos, Michael Josephy y Ángel Ruiz Zúñiga. Colección *Enrique Pérez Arbelaéz*, **10**, Academia Colombiana de Ciencias Exactas, Físicas y Naturales, Bogotá, 1995.

[10] Granville A. *It is easy to determine whether a given integer is prime*. American Mathemathical Montly, **42**, 3-38 (2005).

[11] Guy Richard K. *Unsolved Problems in Number Theory*. Problem Books in Mathematics. Springer, New York 2004.

[12] Hardy G.H., Wright E.M. *An introduction to the theory of numbers*. Oxford University Press, Oxford 1979.

[13] Hoffman P., *Archimedes' revenge*. Norton, New York, 1988.

[14] Ireland K., M. Rosen., *A classical introduction to modern number theory*. GTM **84** Springer Verlag 1982.

[15] Ivorra Castillo C., *Teoría de Números*. Publicación electrónica http://www.uv.es/ivorra/.

[16] Jones J.P., *et al*. *Diophantine representation of the set of prime numbers*. American Mathematical Montly, **83**, No. 6, 449-464 (1976).

[17] LeVeque William J., *Fundamentals of Number Theory*. Dover 1996.

[18] Nair M.A., *A note on the equation $x^2 - y^3 = k$*. Quart. J. Math. Oxford (2) **29**, 483-487 (1978).

[19] Nahin P.J., *An imaginary tale: The story of $\sqrt{-1}$*. Princeton University Press, Princeton, NJ, 1998.

[20] Narkiewicz, W., *Elementary and analitic theory of algebraic numbers*. Third edition. Springer-Verlag 2004.
[21] Niven I., Zuckerman S., Montgomery H.L., *An Introduction to the Theory of Numbers*. 5th ed., John Wiley, New York, 1991.
[22] Ore O., *Number Theory and its history*. Reimpresión de la versión original de 1948. Dover 1988, New York.
[23] Pineda-Ruelas M, Villa-Salvador G. Teoría Clásica de Números (en revisión).
[24] Pomerance C., *Very Short Primality Proofs*. Mathematics of Computation **48**, no. 177, 315-322 (1987).
[25] Proyecto GIMPS (Great Internet Mersenne Prime Search). http://www.mersenne.org/prime.htm
[26] Quine, W.J., Fermat's Last Theorem in combinatorial form. American Mathematical Montly, **95**, No. 7, 305-319 (1988).
[27] Ribenboim P., *Algebraic Numbers*, Wiley, New York 1972
[28] Ribenboim P., *El famoso polinomio generador de primos de Euler y el número de clase de los cuerpos cuadráticos imaginarios*. Revista Colombiana de Matemáticas, vol. **21**, 263-284 (1987).
[29] Ribenboim P., *Números primos: mistérios e recordes*. Coleção Matemática Universitaria, Rio de Janeiro: IMPA 2001.
[30] Ribenboim P., *The new book of prime number records*. Springer Verlag, New York (1996).
[31] Ribenboim P., *Classical Theory of Algebraic Numbers*. Universitext, Springer, New York (2001).
[32] Rivest R., Shamir A., Adleman L., *A method for obtain digital signatures and public-key cryptosystems*. Comm. of the ACM, **21**, 120-126 (1978).
[33] Rosen K.H., *Elementary Number Theory and its Applications*. Third ed., Addison Wesley, Paris 1993.
[34] Shanks D., *Solved and Unsolved Problems in Number Theory*. Chelsea, New York, 2002.
[35] Sierpiński W., *Elementary theory of numbers*. North-Holland, Amsterdan 1988.
[36] Silverman J. H., *A friendly Introduction to number theory*. Prentice-Hall, 3 edition, New Jersey 2005.
[37] Schroeder M.R., *Number Theory in Science and Communication: With applications in cryptography, physics, digital information, computing, and self-similarity*. Springer Series in Information Sciences, 7. Fourth edition. Springer Verlag, Berlin 2006.
[38] Stewart I., *De aquí al infinito; Las matemáticas de hoy*. Crítica, Barcelona 2004.
[39] Stewart I., Tall D., *Algebraic Number Theory and Fermat Last Theorem*. A K Peters, third edition, 2002.
[40] Stillwell J., *Elements of Number Theory*, Undergraduate Texts in Mathematics, Springer Verlag, New York 2003.
[41] Sylvester J.J., *El estudio que no sabe nada de la observación*. Colección Sigma. El Mundo de las Matemáticas, Vol. 5 Grijabo, España 1968.

[42] The Prime Pages. http://primes.utm.edu/
[43] Thompson J., *A method for finding primes*. American Mathematical Monthly, **60**, No. 3, 175 (1953).
[44] Uspensky J.V., *A method for finding units in cubic orders of a negative discriminat*, Trans. Amer. Math. Soc., **33**, 1-22 (1931).
[45] Uspensky J.V., *Teoría de ecuaciones*. Limusa, 2002.
[46] Vardi I., Archimedes' Cattle Problem. American Mathematical Montly, **105**, No. 4, 305-319 (1998).
[47] Wagon S., *The evidence: primality testing*. Math. Intellingencer **8**, no.3, 58-61 (1986).
[48] Weil A., *Two lectures on number theory, past and present*, Enseignement Math. **20**, 87-110 (1974).
[49] Weil A., *Number theory: An approach through history from Hummurapi to Legendre*, Birkhäuser, Boston, 1984.
[50] Weyl H., *El modo matemático de pensar*. Colección Sigma. El Mundo de las Matemáticas, Vol. 5 Grijabo, España 1968.
[51] Williams H.C., Holte R., *Computation of the solutions of* $x^3+dy^3=1$. Math. Comp. **31** no. 139, 778-785 (1977).
[52] Williams Kenneth S., *Note on Non-Euclidean Principal Ideal Domains*. Mathematics Magazine, **48**, No. 3, 176-177 (1975).