# LA FUNCION $\phi$ DE EULER EN $\mathbb{Z}[\sqrt{2}]$

Tesis

entregada a la

Universidad de Chile

en cumplimiento parcial de los requisitos

para optar al grado de

Magister en Ciencias Matemáticas con mención en Algebra

FACULTAD DE CIENCIAS

por

RENE ROMO CASTRO

Agosto, 1987



Patrocinante: Dr. Ricardo Baeza R.

Facultad de Ciencias

Universidad de Chile

# I N F O R M E  D E  A P R O B A C I O N

## T E S I S  D E  M A G I S T E R

Se informa a la Escuela de Postgrado de la Facultad de Ciencias que la Tesis de Magister presentada por el Candidato

RENE ROMO CASTRO

ha sido aprobada por la Comisión Informante de Tesis como requisito de tesis para el grado de Magister en Ciencias Matemáticas con mención en Algebra

Patrocinante de Tesis

Dr. Ricardo Baeza R. Ricardo Baeza

Comisión Informante de Tesis

Dr. Oscar Barriga B.

# I N D I C E

Pág.

# I N T R O D U C C I O N

En The American Mathematical Monthly (1983, pág. 518-528) aparece un artículo de James Cross titulado The Euler $\phi$-function in the Gaussian Integers. En ese trabajo se define y estudia la función $\phi$ de Euler en $\mathbb{Z}[\sqrt{-1}]$ determinando la estructura de los grupos de unidades de los anillos cuocientes de $\mathbb{Z}[\sqrt{-1}]$ módulo potencias de primos de este anillo principal y obtiene como resultado adicional todos los enteros gaussianos que tienen raíces primitivas.

En este trabajo definimos y estudiamos la función $\phi$ de Euler en $\mathbb{Z}[\sqrt{2}]$, el anillo de enteros del cuerpo cuadrático real $\mathbb{Q}(\sqrt{2})$ y determinamos todos los enteros de este anillo que tienen raíces primitivas siguiendo un programa análogo al de Gross en su trabajo, salvo en la Sección 9, en donde determinamos los enteros de $\mathbb{Z}[\sqrt{2}]$ que tienen raíces primitivas siguiendo las ideas en [5].

En las Secciones 4, 6 y 7 determinamos las estructuras de los grupos de unidades del anillo $\dfrac{\mathbb{Z}[\sqrt{2}]}{\beta^n\,\mathbb{Z}[\sqrt{2}]}$, donde $\beta$ es uno cualquiera de los tres tipos de primos en $\mathbb{Z}[\sqrt{2}]$. Empleamos estos resultados en la

Sección 9 para determinar los enteros en $\mathbb{Z}[\sqrt{2}]$ que tienen raíces primitivas.

Podemos generalizar el Teorema 3 de la Sección 4. En efecto, es posible determinar la estructura de los grupos de unidades $\left(\mathcal{O}_K/\mathfrak{q}^n\right)^*$ donde $\mathfrak{q}$ es un ideal primo de $K = \mathbb{Q}(\sqrt{d})$ tal que $\mathfrak{q}\mathfrak{q}' = (q)$, $q$ primo racional que se factoriza en $\mathcal{O}_K$. De hecho se demuestra que $\left(\mathcal{O}_K/\mathfrak{q}^n\right)^* \simeq \left(\frac{\mathbb{Z}}{q^n\mathbb{Z}}\right)^*$. Podemos también determinar la estructura de los grupos de unidades $\left(\mathcal{O}_K/\mathfrak{p}^n\right)^*$ donde $\mathfrak{p} = (p)$, $p$ primo racional inerte en $\mathcal{O}_K$. Esta estructura se determina solo para $d \equiv 2$ ó $3(4)$, donde $d$ es tal que $K = \mathbb{Q}(\sqrt{d})$. El resultado obtenido es el siguiente:

$$\left(\mathcal{O}_K/\mathfrak{p}^n\right)^* = C_{p^{n-1}} \times C_{p^{n-1}} \times C_{p^2-1} .$$

Para primos racionales que son cuadrados de ideales primos no hay resultados salvo para $d = -1$ y $d = 2$.

Para $d = -1$, Cross demuestra en [4] que

$$\left(\frac{\mathbb{Z}[\sqrt{-1}]}{\alpha^n\mathbb{Z}[\sqrt{-1}]}\right)^* \simeq \begin{cases} C_{2^{m-1}} \times C_{2^{m-2}} \times C_4 , & \text{si } n = 2m \\ C_{2^{m-1}} \times C_{2^{m-1}} \times C_4 , & \text{si } n = 2m+1 . \end{cases}$$

donde $\alpha = 1 + i$, $2 = \alpha\alpha' = -i\alpha^2$, de modo que $(2) = (\alpha)^2$.

Para $d = 2$ , demostramos en la Sección 7 de este trabajo que

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n \mathbb{Z}[\sqrt{2}]}\right)^* \simeq \begin{cases} C_{2^m} \times C_{2^{m-2}} \times C_2 , & \text{si } n = 2m \\ \\ C_{2^m} \times C_{2^{m-1}} \times C_2 , & \text{si } n = 2m + 1 . \end{cases}$$

Aquí $\alpha = \sqrt{2}$ , de manera que $(2) = (\alpha)^2$ . $(\alpha)$ indica el ideal en $\mathbb{Z}[\sqrt{2}]$ generado por $\alpha$ .

# C A P I T U L O 1

## LA FUNCION $\phi$ DE EULER EN $\mathbb{Z}[\sqrt{2}]$

### 1. Nociones Preliminares.

Comenzamos esta Sección revisando la función $\phi$ de Euler en $\mathbb{Z}$, la definimos en $\mathbb{Z}[\sqrt{2}]$ y discutimos algunos problemas cuyas respuestas son bien conocidas en $\mathbb{Z}$ y que intentamos resolver en $\mathbb{Z}[\sqrt{2}]$.

Sea $n$ un entero $\neq 0$ y $\mathbb{Z}/n\mathbb{Z}$ el anillo cuociente de $\mathbb{Z}$ módulo $n$. Si $n > 0$, entonces

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$$

donde los paréntesis cuadrados indican clases de equivalencias, módulo $n$. Ya que $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/-n\mathbb{Z}$ nos restringimos solo a enteros positivos. Las unidades de este anillo forman un grupo multiplicativo que se denota por $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ y el valor de la función $\phi$ de Euler en $n$ se define como el orden de este grupo. Es claro que $[k]$ en $\mathbb{Z}/n\mathbb{Z}$ es una unidad sí y sólo si $(k,n) = 1$, es decir, sí y sólo si $k$ y $n$ son relativa -

mente primos. Así, para $n > 1$, $\phi(n)$ es el número de enteros positivos menores que $n$ y relativamente primos con $n$. Si $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ es cíclico y $[k]$ un generador de este grupo, entonces $k$ se llama una raíz primitiva módulo $n$.

Si denotamos por $C_n$ el grupo aditivo (cíclico) de $\mathbb{Z}/n\mathbb{Z}$, entonces para $m > 1$ la estructura de $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$ está dada por (ver [5]):

i) $\left(\mathbb{Z}/2\mathbb{Z}\right)^* \simeq C_1$

ii) $\left(\mathbb{Z}/4\mathbb{Z}\right)^* \simeq C_2$

iii) $\left(\mathbb{Z}/2^n\mathbb{Z}\right)^* \simeq C_2 \times C_{2^{n-2}}$, $n > 2$

iv) $\left(\mathbb{Z}/p^n\mathbb{Z}\right)^* \simeq C_{p^n - p^{n-1}}$, $p$ primo impar

v) $\left(\mathbb{Z}/mn\mathbb{Z}\right)^* \simeq \left(\mathbb{Z}/m\mathbb{Z}\right)^* \times \left(\mathbb{Z}/n\mathbb{Z}\right)^*$, $(m,n) = 1$.

La estructura de $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$ para $m$ arbitrario se obtiene por su factorización en primos.

De los isomorfismos en (i), (ii) y (iv) y de nuestra definición de raíces primitivas se deduce de inmediato que hay raíces primitivas módulo 2, 4 y $p^n$. Sin embargo, no hay raíces primitivas módulo 8 pués

$$\left(\mathbb{Z}/8\mathbb{Z}\right)^* = \{[1], [3], [5], [7]\} \simeq C_2 \times C_2$$

y este grupo tiene solo elementos de orden 2 ó 1. Un resultado muy conocido (ver por ejemplo [5]) establece que $n$ tiene raíces primitivas sí y sólo si $n = 2, 4, p^n$ ó $2p^n$, donde $p$ es un primo impar y $n \geq 1$.

La definición de la función $\phi$ de Euler puede extenderse de manera natural a $\mathbb{Z}[\sqrt{2}]$ . Sea $\beta \neq 0$ en $\mathbb{Z}[\sqrt{2}]$ y $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta\,\mathbb{Z}[\sqrt{2}]}\right)^*$ el grupo de unidades del anillo $\frac{\mathbb{Z}[\sqrt{2}]}{\beta\,\mathbb{Z}[\sqrt{2}]}$ . Entonces la función $\phi$ de Euler sobre $\mathbb{Z}[\sqrt{2}]$ se define por

$$\phi(\beta) = \#\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta\,\mathbb{Z}[\sqrt{2}]}\right)^* , \qquad \forall\ \beta \neq 0 \text{ en } \mathbb{Z}[\sqrt{2}]$$

Con mayor generalidad, para todo cuerpo de números $K/\mathbb{Q}$ con anillo de enteros $\mathcal{O}_K$ se define la función $\phi_K$ sobre el conjunto de ideales $\mathfrak{A} \neq (0)$ de $\mathcal{O}_K$ por

$$\phi_K(\mathfrak{A}) = \#\left(\mathcal{O}_K/\mathfrak{A}\right)^*$$

Nosotros en este trabajo nos limitamos a considerar solamente el caso $K = \mathbb{Q}(\sqrt{2})$ ; $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ .

Por el Teorema Chino del Resto aplicado a $\mathbb{Z}[\sqrt{2}]$ se tiene:

$$\frac{\mathbb{Z}[\sqrt{2}]}{(\gamma_1, \ldots, \gamma_m)} \simeq \frac{\mathbb{Z}[\sqrt{2}]}{(\gamma_1)} \times \ldots\ldots \times \frac{\mathbb{Z}[\sqrt{2}]}{(\gamma_m)}$$

donde $\gamma_1, \ldots, \gamma_m$ son enteros relativamente primos. En particular, si $\beta = \beta_1^{n_1} \ldots \beta_r^{n_r}$ , $n_i \geq 1$ es la factorización de $\beta$ en primos de $\mathbb{Z}[\sqrt{2}]$ :

$$\frac{\mathbb{Z}[\sqrt{2}]}{\beta\,\mathbb{Z}[\sqrt{2}]} \simeq \frac{\mathbb{Z}[\sqrt{2}]}{\beta_1^{n_1}\,\mathbb{Z}[\sqrt{2}]} \times \ldots\ldots \times \frac{\mathbb{Z}[\sqrt{2}]}{\beta_r^{n_r}\,\mathbb{Z}[\sqrt{2}]}$$

Este isomorfismo de anillos induce un isomorfismo de grupos de unidades

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta\ \mathbb{Z}[\sqrt{2}]}\right)^* \simeq \left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta_1^{n_1}\ \mathbb{Z}[\sqrt{2}]}\right)^* \times \cdots\cdots \times \left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta_r^{n_r}\ \mathbb{Z}[\sqrt{2}]}\right)^*$$

En particular

$$\phi(\beta) = \phi\left(\beta_1^{n_1}\right) \cdots\cdots \phi\left(\beta_r^{n_r}\right) .$$

Vemos que para conocer nuestra función $\phi$ sobre $\mathbb{Z}[\sqrt{2}]$, necesitamos conocer la estructura del grupo de unidades $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta^n\ \mathbb{Z}[\sqrt{2}]}\right)^*$, donde $\beta$ es primo en $\mathbb{Z}[\sqrt{2}]$.

Si $p$ es un primo racional impar, entonces $\left(\mathbb{Z}/p^n\mathbb{Z}\right)^*$ es cíclico. ¿Ocurre lo mismo con $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\mathbb{Z}[\sqrt{2}]}\right)^*$? Con mayor generalidad, ¿para qué enteros $\gamma$ en $\mathbb{Z}[\sqrt{2}]$ es $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\gamma\ \mathbb{Z}[\sqrt{2}]}\right)^*$ cíclico? La respuesta a la primera pregunta es no. Esto se muestra determinando los órdenes de los elementos de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{3^2\ \mathbb{Z}[\sqrt{2}]}\right)^*$. Como lo veremos en el Ejemplo 4, un sistema completo de representantes incongruentes módulo 9 está dado por el conjunto $a + b\sqrt{2}$, donde $a$ y $b$ recorren independientemente los enteros entre 0 y 9 y al menos uno de ellos es relativamente primo con 3. Los 72 elementos de este grupo y sus órdenes están dados en el ordenamiento rectangular de la Tabla 1.

| | $[\sqrt{2}]$ | $[2\sqrt{2}]$ | | $[4\sqrt{2}]$ | $[5\sqrt{2}]$ | | $[7\sqrt{2}]$ | $[8\sqrt{2}]$ |
|---|---|---|---|---|---|---|---|---|
| | 12 | 4 | | 12 | 12 | | 4 | 12 |
| [1] | $[1+\sqrt{2}]$ | $[1+2\sqrt{2}]$ | $[1+3\sqrt{2}]$ | $[1+4\sqrt{2}]$ | $[1+5\sqrt{2}]$ | $[1+6\sqrt{2}]$ | $[1+7\sqrt{2}]$ | $[1+8\sqrt{2}]$ |
| 1 | 24 | 24 | 3 | 24 | 24 | 3 | 24 | 24 |
| [2] | $[2+\sqrt{2}]$ | $[2+2\sqrt{2}]$ | $[2+3\sqrt{2}]$ | $[2+4\sqrt{2}]$ | $[2+5\sqrt{2}]$ | $[2+6\sqrt{2}]$ | $[2+7\sqrt{2}]$ | $[2+8\sqrt{2}]$ |
| 6 | 24 | 24 | 6 | 8 | 8 | 6 | 24 | 24 |
| | $[3+\sqrt{2}]$ | $[3+2\sqrt{2}]$ | | $[3+4\sqrt{2}]$ | $[3+5\sqrt{2}]$ | | $[3+7\sqrt{2}]$ | $[3+8\sqrt{2}]$ |
| | 12 | 12 | | 12 | 12 | | 12 | 12 |
| [4] | $[4+\sqrt{2}]$ | $[4+2\sqrt{2}]$ | $[4+3\sqrt{2}]$ | $[4+4\sqrt{2}]$ | $[4+5\sqrt{2}]$ | $[4+6\sqrt{2}]$ | $[4+7\sqrt{2}]$ | $[4+8\sqrt{2}]$ |
| 3 | 24 | 24 | 3 | 24 | 24 | 3 | 24 | 24 |
| [5] | $[5+\sqrt{2}]$ | $[5+2\sqrt{2}]$ | $[5+3\sqrt{2}]$ | $[5+4\sqrt{2}]$ | $[5+5\sqrt{2}]$ | $[5+6\sqrt{2}]$ | $[5+7\sqrt{2}]$ | $[5+8\sqrt{2}]$ |
| 6 | 24 | 24 | 6 | 24 | 24 | 6 | 24 | 24 |
| | $[6+\sqrt{2}]$ | $[6+2\sqrt{2}]$ | | $[6+4\sqrt{2}]$ | $[6+5\sqrt{2}]$ | | $[6+7\sqrt{2}]$ | $[6+8\sqrt{2}]$ |
| | 12 | 12 | | 12 | 12 | | 12 | 12 |
| [7] | $[7+\sqrt{2}]$ | $[7+2\sqrt{2}]$ | $[7+3\sqrt{2}]$ | $[7+4\sqrt{2}]$ | $[7+5\sqrt{2}]$ | $[7+6\sqrt{2}]$ | $[7+7\sqrt{2}]$ | $[7+8\sqrt{2}]$ |
| 3 | 24 | 24 | 3 | 8 | 8 | 3 | 24 | 24 |
| [8] | $[8+\sqrt{2}]$ | $[8+2\sqrt{2}]$ | $[8+3\sqrt{2}]$ | $[8+4\sqrt{2}]$ | $[8+5\sqrt{2}]$ | $[8+6\sqrt{2}]$ | $[8+7\sqrt{2}]$ | $[8+8\sqrt{2}]$ |
| 2 | 24 | 24 | 6 | 24 | 24 | 6 | 24 | 24 |

En esta tabla, los paréntesis cuadrados indican clases de equivalencia, los números sin paréntesis indican ordenes. Por ejemplo, el orden de $[4 + 7\sqrt{2}]$ es 24, el orden de $[5]$ es 6, el orden de $[1 + 3\sqrt{2}]$ es 3. Estos ordenes fueron determinados por cálculos directos. Por ejemplo:

| | ORDEN |
|---|---|
| $(1 + \sqrt{2}) \equiv 1 + \sqrt{2}$ (9) | 24 |
| $(1 + \sqrt{2})^2 \equiv 3 + 2\sqrt{2}$ (9) | 12 |
| $(1 + \sqrt{2})^3 \equiv 7 + 5\sqrt{2}$ (9) | 8 |
| $(1 + \sqrt{2})^4 \equiv 8 + 3\sqrt{2}$ (9) | 6 |
| $(1 + \sqrt{2})^5 \equiv 5 + 2\sqrt{2}$ (9) | 24 |
| $(1 + \sqrt{2})^6 \equiv 7\sqrt{2}$ (9) | 4 |
| $(1 + \sqrt{2})^7 \equiv 7\sqrt{2}(1 + \sqrt{2}) \equiv 5 + 7\sqrt{2}$ (9) | 24 |
| $(1 + \sqrt{2})^8 \equiv 7\sqrt{2}(1 + \sqrt{2})^2 \equiv 1 + 3\sqrt{2}$ (9) | 3 |
| $(1 + \sqrt{2})^9 \equiv 7\sqrt{2}(1 + \sqrt{2})^3 \equiv 7 + 4\sqrt{2}$ (9) | 8 |
| $(1 + \sqrt{2})^{10} \equiv 7\sqrt{2}(1 + \sqrt{2})^4 \equiv 6 + 2\sqrt{2}$ (9) | 12 |
| $(1 + \sqrt{2})^{11} \equiv 7\sqrt{2}(1 + \sqrt{2})^5 \equiv 1 + 8\sqrt{2}$ (9) | 24 |
| $(1 + \sqrt{2})^{12} \equiv (7\sqrt{2})(7\sqrt{2}) \equiv -1$ (9) | 2 |
| $(1 + \sqrt{2})^{13} \equiv -(1 + \sqrt{2}) \equiv 8 + 8\sqrt{2}$ (9) | 24 |
| $(1 + \sqrt{2})^{14} \equiv -(1 + \sqrt{2})^2 \equiv 6 + 7\sqrt{2}$ (9) | 12 |
| $(1 + \sqrt{2})^{15} \equiv -(1 + \sqrt{2})^3 \equiv 2 + 4\sqrt{2}$ (9) | 8 |

| | ORDEN |
|---|---|
| $(1+\sqrt{2})^{16} \equiv -(1+\sqrt{2})^{4} \equiv 1 + 6\sqrt{2}$ (9) | 8 |
| $(1+\sqrt{2})^{17} \equiv -(1+\sqrt{2})^{5} \equiv 4 + 7\sqrt{2}$ (9) | 24 |
| $(1+\sqrt{2})^{18} \equiv -(1+\sqrt{2})^{6} \equiv 2\sqrt{2}$ (9) | 4 |
| $(1+\sqrt{2})^{19} \equiv -(1+\sqrt{2})^{7} \equiv 4\sqrt{2}$ (9) | 24 |
| $(1+\sqrt{2})^{20} \equiv -(1+\sqrt{2})^{8} \equiv 8 + 6\sqrt{2}$ (9) | 6 |
| $(1+\sqrt{2})^{21} \equiv -(1+\sqrt{2})^{9} \equiv 2 + 5\sqrt{2}$ (9) | 8 |
| $(1+\sqrt{2})^{22} \equiv -(1+\sqrt{2})^{10} \equiv 3 + 7\sqrt{2}$ (9) | 12 |
| $(1+\sqrt{2})^{23} \equiv -(1+\sqrt{2})^{11} \equiv 8 + \sqrt{2}$ (9) | 24 |
| $(1+\sqrt{2})^{24} \equiv -(1+\sqrt{2})^{12} \equiv 1$ (9) | 1 |

Sea $x = [1 + \sqrt{2}]$ y $G = \langle x \rangle$ el grupo cíclico de orden 24 generado por $x$. El conjunto de generadores de $G$ consiste de los elementos $x^s$, donde $(s,24) = 1$, es decir, los generadores de $G$ son $x$, $x^5$, $x^7$, $x^{11}$, $x^{13}$, $x^{17}$, $x^{19}$ y $x^{23}$. Así, $[1 + \sqrt{2}]$, $[1 + \sqrt{2}]^2 = [5 + 2\sqrt{2}]$, ... $[1 + \sqrt{2}]^{23} = [8 + \sqrt{2}]$ son elementos de orden 24. Sea $y \in G$, entonces $y = x^r$ e $y$ genera un subgrupo de orden $\frac{24}{(r,24)}$. En particular, $y = x^2$ genera un subgrupo de orden 12. Los generadores de $G_1 = \langle y \rangle = \langle x^2 \rangle$ son elementos de la forma $y^t$, con $(t,12) = 1$ es decir son $y$, $y^5$, $y^7$ e $y^{11}$ ó $x^2$, $x^{10}$, $x^{14}$ y $x^{22}$. Estos son los elementos de orden 12 en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{9\,\mathbb{Z}[\sqrt{2}]}\right)^*$. $[1 + \sqrt{2}]^3 = [7 + 5\sqrt{2}]$ genera un subgrupo de orden $8 = \frac{24}{(3,24)}$. Los otros generadores de este subgrupo son $[1 + \sqrt{2}]^3$,

$[1 + \sqrt{2}]^9$ , $[1 + \sqrt{2}]^{15}$ y $[1 + \sqrt{2}]^{21}$ . De esta manera se continúa con los elementos que restan.

Ya que el máximo orden observado en la Tabla es 24, resulta que hay primos impares para los cuales la respuesta a nuestra pregunta es no. Probaremos en el Ejemplo 7 que

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{9\,\mathbb{Z}[\sqrt{2}]}\right)^* \simeq C_3 \times C_3 \times C_8 \quad .$$

Vamos ahora a determinar la estructura de los grupos $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$ , donde $\beta$ es un primo en $\mathbb{Z}[\sqrt{2}]$ . Para ello:

i) Identificamos los primos en $\mathbb{Z}[\sqrt{2}]$ . Hay sólo tres tipos de ellos. (Ver, por ejemplo, [3], pág. 358).

ii) Describimos los elementos de los anillos cuocientes de $\mathbb{Z}[\sqrt{2}]$ , módulo potencias de primos y los elementos de los grupos de unidades de tales anillos.

iii) Estudiamos la estructura de estos grupos mediante ejemplos que permitan formular conjeturas sobre los factores directos de estos grupos que son grupos abelianos finitos. Finalmente,

iv) Demostramos estas conjeturas.

2. Primos en $\mathbb{Z}[\sqrt{2}]$ . (Ver [3], pág. 358).

Sean $\alpha$ y $\beta$ en $\mathbb{Z}[\sqrt{2}]$ . $\beta$ divide a $\alpha$ lo que anotamos $\beta|\alpha$ , si $\alpha = \beta\gamma$ , para algún $\gamma \in \mathbb{Z}[\sqrt{2}]$ . $\mu$ es una unidad si $\mu|1$ , es decir $1 = \mu\eta$ , para algún $\eta \in \mathbb{Z}[\sqrt{2}]$ . En particular $1$ y $-1$ son unidades de $\mathbb{Z}[\sqrt{2}]$ . Los números $\mu\beta$ se dicen asociados de $\beta$ . Un número $\pi$ en $\mathbb{Z}[\sqrt{2}]$ se dice primo si es divisible solo por unidades y sus asociados. Si $\mu_1$, $\mu_2$ , $\mu_2 \neq 0$ son unidades entonces $\mu_1\mu_2$ y $\frac{\mu_1}{\mu_2}$ son unidades. Para $\beta = a + b\sqrt{2}$ definimos el conjugado de $\beta$ por $\beta' = a - b\sqrt{2}$ . La norma $N$ de $\beta$ se define por

$$N\beta = \beta\beta' = a^2 - 2b^2 .$$

La norma de $\beta$ es un entero racional. La norma de un producto es el producto de las normas. $\mu$ es una unidad si y sólo si $N\mu = \pm 1$ .

Todo primo $\pi$ en $\mathbb{Z}[\sqrt{2}]$ es un divisor de exactamente un primo racional $p$ [1]. Sea $p = \pi\lambda$ , donde $\lambda \in \mathbb{Z}[\sqrt{2}]$ . Entonces $N\pi = p^2$ ó $N\pi = p$ . Si $N\pi = p^2$ , $p$ es un asociado de $\pi$ y por tanto es primo en $\mathbb{Z}[\sqrt{2}]$ . Supongamos que $N\pi = a^2 - 2b^2 = p$ , $\pi = a + b\sqrt{2}$ . Si $p \equiv \pm 3 \pmod 8$ , la ecuación $a^2 - 2b^2 = p$ es imposible en $\mathbb{Z}$ . (Pués si $a^2 - 2b^2 = p$ es soluble en $\mathbb{Z}$ , entonces $a^2 - 2b^2 \equiv \pm 3 \pmod 8$. Pero $a^2 - 2b^2 \equiv 0 , \pm 1 , \pm 2 , 4 \pmod 8$ . Luego los primos racionales de la forma $8k \pm 3$ son primos en $\mathbb{Z}[\sqrt{2}]$ .

Si $p \equiv \pm 1 \pmod 8$ , entonces 2 es resto cuadrático módulo $p$ , es decir, $p|x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ , para algún entero racional $x$ .

Si $p$ es primo en $\mathbb{Z}[\sqrt{2}]$, $p|x+\sqrt{2}$ ó $p|x-\sqrt{2}$. Esto es imposible. Luego $p$ no es primo en $\mathbb{Z}[\sqrt{2}]$, pero si lo son $\pi$ y $\lambda = \pi'$. Finalmente

$$2 = (\sqrt{2})^2$$

y $\sqrt{2}$ es primo en $\mathbb{Z}[\sqrt{2}]$. Así, los primos en $\mathbb{Z}[\sqrt{2}]$ son

1. $\sqrt{2}$
2. Los primos racionales de la forma $8k \pm 3$
3. Los factores $a + b\sqrt{2}$ de los primos racionales de la forma $8k \pm 1$ y los asociados de todos estos números.

La factorización en primos de $\mathbb{Z}[\sqrt{2}]$ es única, salvo el orden de los factores y multiplicación por unidades. Ver [3], pág. 212.

Ejemplo 1. En $\mathbb{Z}[\sqrt{2}]$, $-7 = (1+2\sqrt{2})(1-2\sqrt{2})$. Si $1+2\sqrt{2} = \beta\gamma$ en $\mathbb{Z}[\sqrt{2}]$, entonces $N(1+2\sqrt{2}) = -7 = N\beta N\gamma$ en $\mathbb{Z}$. Luego $N\beta = \pm 1$ ó $N\gamma = \pm 1$, es decir, al menos uno de los factores es una unidad. Por tanto $1+2\sqrt{2}$ es primo en $\mathbb{Z}[\sqrt{2}]$. En forma análoga se prueba que $1-2\sqrt{2}$ es primo.

Ejemplo 2. Sea $p = 3$. Si $3 = \beta\gamma$ en $\mathbb{Z}[\sqrt{2}]$, $9 = N\beta N\gamma$ en $\mathbb{Z}$. Entonces $N\beta = 3 = N\gamma$ o la norma de uno de los factores es 1. Ya que $a^2 - 2b^2 = 3$ es imposible en $\mathbb{Z}$, se tiene que $\beta$ ó $\gamma$ es una unidad. Luego 3 es primo en $\mathbb{Z}[\sqrt{2}]$.

3. Las clases de equivalencia en $\dfrac{\mathbb{Z}[\sqrt{2}]}{\beta^n\,\mathbb{Z}[\sqrt{2}]}$ y en $\left(\dfrac{\mathbb{Z}[\sqrt{2}]}{\beta^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$, donde $\beta$ es primo en $\mathbb{Z}[\sqrt{2}]$ .

Ahora que hemos encontrado los primos en $\mathbb{Z}[\sqrt{2}]$ los elevamos a potencia entera positiva y buscamos representantes para las clases de equivalencia de los anillos cuocientes y grupos de unidades correspondientes. Los Teoremas 1 y 2 que enunciamos a continuación resuelven este problema. En lo que sigue adoptamos la siguiente notación: $p > 0$ y $q$ indican primos racionales tales que $p \equiv \pm 3 \pmod 8$ y $q \equiv \pm 1 \pmod 8$ . $\pi$ indica un factor primo de $q$ y haremos $\alpha = \sqrt{2}$ . Nos restringimos a primos $p$ positivos pues $(-p)^n = (-1)^n p^n$ y en consecuencia $\dfrac{\mathbb{Z}[\sqrt{2}]}{(-p)^n\,\mathbb{Z}[\sqrt{2}]} = \dfrac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}$ .

Teorema 1. Las clases de equivalencia de $\mathbb{Z}[\sqrt{2}]$ módulo una potencia de un primo están dadas por

1. $$\frac{\mathbb{Z}[\sqrt{2}]}{\pi^n\,\mathbb{Z}[\sqrt{2}]} = \left\{[a] \mid 0 \le a < |q|^n\right\}$$

2. $$\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]} = \left\{[a + b\sqrt{2}] \mid 0 \le a < p^n \ , \ \ 0 \le b < p^n\right\}$$

3. $$\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m}\,\mathbb{Z}[\sqrt{2}]} = \left\{[a + b\sqrt{2}] \mid 0 \le a < 2^m \ , \ \ 0 \le b < 2^m\right\}$$

4. $$\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m+1}\,\mathbb{Z}[\sqrt{2}]} = \left\{[a + b\sqrt{2}] \mid 0 \le a < 2^{m+1} \ ; \ \ 0 \le b < 2^m\right\}$$

En el enunciado de este Teorema, así como en los Ejemplos que consideremos a continuación entendemos que los conjuntos de representantes dados son completos y sin repetición.

Demostración: Observemos primero que $\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m}\,\mathbb{Z}[\sqrt{2}]} = \frac{\mathbb{Z}[\sqrt{2}]}{2^m\,\mathbb{Z}[\sqrt{2}]}$ y $\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m+1}\,\mathbb{Z}[\sqrt{2}]} = \frac{\mathbb{Z}[\sqrt{2}]}{2^m\alpha\,\mathbb{Z}[\sqrt{2}]}$ ya que $\alpha^{2m} = 2^m$. Si $a + b\sqrt{2} \equiv c + d\sqrt{2}\ (\alpha^{2m})$, entonces $2^m$ divide a $a - c + (b - d)\sqrt{2}$, es decir $2^m$ divide a $a - c$ y a $b - d$. Pero $a, c < 2^m$, $b, d < 2^m$. Luego $a = c$ y $b = d$. Esto significa que las clases en (3) son todas distintas. Un argumento similar se usa para probar que las clases en (2) no se repiten. Las clases en (1) son todas distintas pues si $[a] = [b]$ en $\frac{\mathbb{Z}[\sqrt{2}]}{\pi^n\,\mathbb{Z}[\sqrt{2}]}$, entonces $\pi^n \mid a - b$. Sea $a - b = \pi^n\gamma$, para algún $\gamma$ en $\mathbb{Z}[\sqrt{2}]$. Conjugando se tiene $a - b = (\pi')^n\gamma'$ de manera que $(\pi')^n \mid a - b$. Como $\pi$ y $\pi'$ son primos no asociados se tiene que $(\pi\pi')^n = q^n \mid a - b$. Así, $a = b$ y las clases en (1) son todas distintas. Finalmente, si $a + b\sqrt{2} \equiv c + d\sqrt{2}\ (\alpha^{2m+1})$, entonces $2^m\alpha \mid a - c + (b - d)\sqrt{2}$ y $2^m \mid b - d$. Como $b - d < 2^m$, se tiene $b = d$. Ahora $2^m\alpha \mid a - c$, es decir,

$$\frac{a - c}{2^m\alpha} = \frac{(a - c)\alpha}{2^{m+1}} \in \mathbb{Z}[\sqrt{2}]\ .$$

Luego $2^{m+1} \mid a - c$. Como $a - c < 2^{m+1}$, se tiene $a = c$. Hemos probado que las clases en (1) son todas distintas.

Probamos ahora que los sistemas dados por los conjuntos del Teorema son completos. Sea $\beta = x + y\sqrt{2}$ en $\mathbb{Z}[\sqrt{2}]$. Dividiendo $x$ e $y$ por $2^m$ se obtiene

$$x - a = 2^m k \qquad y \qquad x - b = 2^m k'$$

donde $k$ y $k'$ son enteros y $a,b$ son enteros no negativos ambos menores que $2^m$. Esto significa que $\beta \equiv a + b\sqrt{2}\ (2^m)$ y en consecuencia $\beta$ pertenece a una de las clases en (3). Como un argumento similar se prueba que $\beta$ pertenece a una de las clases en (2). Reduciendo $x$ e $y$ por múltiplos de $2^{m+1}$ se tiene $\beta \equiv a + b\sqrt{2}\ (2^{m+1})$, donde $a$ y $b$ son enteros no negativos ambos menores que $2^{m+1}$. Si $b < 2^m$, $\beta$ pertenece a una de las clases en $\dfrac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m+1}\,\mathbb{Z}[\sqrt{2}]}$. Si $b \geq 2^m$, se suma y resta $2^m\alpha$ obteniendo

$$a + b\sqrt{2} = a + (b - 2^m)\sqrt{2} + 2^m\alpha$$

Entonces

$$\beta \equiv a + (b - 2^m)\sqrt{2}(\alpha^{2m+1})$$

donde $0 \leq b - 2^m < 2^m$ (pues $2^m \leq b < 2^{m+1} = 2^m + 2^m$). Así, $\beta$ pertenece a una de las clases en (4). Demostramos ahora que $\sqrt{2}$ pertenece a una de las clases en (1). Sea $\pi^n = a - b\sqrt{2}$, entonces $b\sqrt{2} \equiv a(\pi^n)$. Se tiene que $(b,q) = 1$, pues si $q|b$, entonces $\pi|b$ y $\pi|a$. También $\pi'|a$, de manera que $q = \pi\pi'|a$. Por tanto, $q|\pi^n$ que es imposible. Así, $(b,q) = 1$ y la congruencia $bz \equiv 1(|q|^n)$ es soluble en $\mathbb{Z}$. De la congruencia $b\sqrt{2} \equiv a(\pi^n)$ se deduce $bz\sqrt{2} \equiv az(\pi^n)$, esto es,

$\sqrt{2} \equiv az(\pi^n)$ . Dividiendo az por $|q|^n$ se obtiene $\sqrt{2}$ en una de las clases de $\frac{\mathbb{Z}[\sqrt{2}]}{\pi^n \mathbb{Z}[\sqrt{2}]}$ . Ya que x,y y $\sqrt{2}$ están en una de estas cla - ses, entonces $\beta = x + y\sqrt{2}$ también está.

Este Teorema implica que $\frac{\mathbb{Z}[\sqrt{2}]}{\pi^n \mathbb{Z}[\sqrt{2}]}$ tiene $|q|^n$ elementos

$\frac{\mathbb{Z}[\sqrt{2}]}{p^n \mathbb{Z}[\sqrt{2}]}$ tiene $p^{2n}$ elementos y $\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n \mathbb{Z}[\sqrt{2}]}$ tiene $2^n$ elementos.

Estos hechos son casos especiales del siguiente resultado general: el número de elementos en $\frac{\mathbb{Z}[\sqrt{2}]}{\beta \mathbb{Z}[\sqrt{2}]}$ es $|N\beta|$ . Ver [1], Cap. IX.

Determinamos ahora las unidades de los anillos cuyos elementos se han especificado en el Teorema anterior.

Teorema 2. $[a]$ en $\frac{\mathbb{Z}[\sqrt{2}]}{\pi^n \mathbb{Z}[\sqrt{2}]}$ es una unidad sí y sólo si $(a,q) = 1$ .

$[a + b\sqrt{2}]$ en $\frac{\mathbb{Z}[\sqrt{2}]}{p^n \mathbb{Z}[\sqrt{2}]}$ es una unidad sí y sólo si $(a,p) = 1$ ó

$(b,p) = 1$ . $[a + b\sqrt{2}]$ en $\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n \mathbb{Z}[\sqrt{2}]}$ es una unidad sí y sólo si

$2 \nmid a$ .

Demostración: Sean $\beta$ y $\gamma$ en $\mathbb{Z}[\sqrt{2}]$ . Entonces $[\beta]$ es una unidad en $\frac{\mathbb{Z}[\sqrt{2}]}{\gamma \mathbb{Z}[\sqrt{2}]}$ sí y sólo si $[\beta][\delta] = [1]$ en $\frac{\mathbb{Z}[\sqrt{2}]}{\gamma \mathbb{Z}[\sqrt{2}]}$ , para algún $\delta$ en $\mathbb{Z}[\sqrt{2}]$ . Entonces $[\beta]$ es unidad sí y sólo si $\beta\delta \equiv 1(\gamma)$ , esto es, sí y sólo si $\beta\delta + \gamma\eta = 1$ , para algún $\eta \in \mathbb{Z}[\sqrt{2}]$ . Así, $[\beta]$ es una

unidad en $\frac{\mathbb{Z}[\sqrt{2}]}{\gamma\,\mathbb{Z}[\sqrt{2}]} \iff \beta$ y $\gamma$ son relativamente primos. Se deduce que

$[a]$ es una unidad en $\frac{\mathbb{Z}[\sqrt{2}]}{\pi^n\,\mathbb{Z}[\sqrt{2}]} \iff (a,\pi^n) = 1 \iff (a,\pi) = 1 \iff q \nmid a$ .

$[a + b\sqrt{2}]$ es una unidad en $\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]} \iff (a + b\sqrt{2}, p^n) = 1 \iff$

$\iff p \nmid a + b\sqrt{2} \iff p \nmid a$ ó $p \nmid b$ . Finalmente, $[a + b\sqrt{2}]$ es una unidad

en $\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n\,\mathbb{Z}[\sqrt{2}]} \iff (a + b\sqrt{2}, \alpha^n) = 1 \iff \sqrt{2} \nmid a + b\sqrt{2}$ . Pero

$$\sqrt{2} \mid a + b\sqrt{2} \iff \frac{a + b\sqrt{2}}{\sqrt{2}} = \frac{2b + a\sqrt{2}}{2} \in \mathbb{Z}[\sqrt{2}] \iff 2 \mid a \ .$$

Es decir, $\sqrt{2} \nmid a + b\sqrt{2} \iff 2 \nmid a$ .

Ejemplo 3. Sea $\pi = 1 + 2\sqrt{2}$ . $\pi$ es primo en $\mathbb{Z}[\sqrt{2}]$ pues $\pi\pi' = -7$ . Por los Teoremas 1 y 2 se tiene que

$$\frac{\mathbb{Z}[\sqrt{2}]}{\pi^2\,\mathbb{Z}[\sqrt{2}]} = \{[0], [1], \ldots, [48]\}$$

y $[a]$ en $\frac{\mathbb{Z}[\sqrt{2}]}{\pi^2\,\mathbb{Z}[\sqrt{2}]}$ es una unidad sí y sólo si 7 no divide a **a** . ¿A qué clase módulo $\pi^2$ pertenece $\sqrt{2}$ ? $\pi^2 = 9 + 4\sqrt{2}$ , de modo que $4\sqrt{2} \equiv -9 (\pi^2)$ . Multiplicando esta congruencia por 12 se obtiene $49\sqrt{2} - \sqrt{2} \equiv -108 (\pi^2)$ . Ya que $\pi^2$ es un divisor de 49, esta congruencia se reduce a $\sqrt{2} \equiv 10 (\pi^2)$ . Podemos verificar directamente este resultado: $\frac{10 - \sqrt{2}}{\pi^2} = \frac{10 - \sqrt{2}}{9 + 4\sqrt{2}} = 2 - \sqrt{2}$ , de manera que $\pi^2$ es un divisor de $10 - \sqrt{2}$ en $\mathbb{Z}[\sqrt{2}]$ . En consecuencia $\sqrt{2} \equiv 10 (\pi^2)$ y $\sqrt{2}$ pertenece a $[10]$.

En este Ejemplo se comprueba que $\left(\frac{\mathbb{Z}[\sqrt{2}]}{(1+2\sqrt{2})^2\,\mathbb{Z}[\sqrt{2}]}\right)^* \simeq$ $\simeq \left(\mathbb{Z}/49\,\mathbb{Z}\right)^*$. Ya que $\left(\mathbb{Z}/49\,\mathbb{Z}\right)^*$ es cíclico, $\pi^2 = 9 + 4\sqrt{2}$ tiene raíces primitivas. De hecho, 3 es una raíz primitiva módulo $\pi^2$.

Ejemplo 4. Por los Teorema 1 y 2

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{3^2\,\mathbb{Z}[\sqrt{2}]}\right)^* = \left(\frac{\mathbb{Z}[\sqrt{2}]}{9\,\mathbb{Z}[\sqrt{2}]}\right)^* = \left\{[a+b\sqrt{2}] \mid 0 \le a,b < 9\ ,\ (3,a) = 1 \text{ ó } (3,b) = 1\right\}$$

Observemos que $\left(\mathbb{Z}/9\,\mathbb{Z}\right)^*$ está incluído isomorficamente en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{9\,\mathbb{Z}[\sqrt{2}]}\right)^*$, pues $\left(\mathbb{Z}/9\,\mathbb{Z}\right)^* = \left\{[1], [2], [4], [5], [7], [8]\right\}$ puede identificarse mediante la aplicación inclusión con $\left\{[1], [2], [4], [5], [7], [8]\right\}$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{9\,\mathbb{Z}[\sqrt{2}]}\right)^*$.

Ejemplo 5. En virtud de los Teoremas 1 y 2

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^5\,\mathbb{Z}[\sqrt{2}]}\right)^* = \left(\frac{\mathbb{Z}[\sqrt{2}]}{4\alpha\,\mathbb{Z}[\sqrt{2}]}\right)^*$$

$$= \left\{[1], [3], [5], [7], [1+\sqrt{2}], [3+\sqrt{2}], [5+\sqrt{2}], [7+\sqrt{2}], [1+2\sqrt{2}], [3+2\sqrt{2}], [5+2\sqrt{2}], [7+2\sqrt{2}], [3+3\sqrt{2}], [5+3\sqrt{2}], [7+3\sqrt{2}]\right\}$$

Observemos que $\left(\mathbb{Z}/8\mathbb{Z}\right)^* = \left\{[1], [3], [5], [7]\right\}$ está incluído isomórficamente en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^5\,\mathbb{Z}[\sqrt{2}]}\right)^*$. Como $\left(\mathbb{Z}/8\,\mathbb{Z}\right)^*$ no es cíclico y ya que todo subgrupo de un grupo cíclico es cíclico, $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^5\,\mathbb{Z}[\sqrt{2}]}\right)^*$ no es cíclico.

En consecuencia $\alpha^5 = 4\sqrt{2}$ no tiene raíces primitivas.

Adelantémonos a los resultados determinando la estructura de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^5\,\mathbb{Z}[\sqrt{2}]}\right)^*$. Sea $H$ el subgrupo generado por $[1+\sqrt{2}]$, $K$ y $J$ los subgrupos generados por $[5]$ y $[-1]$. Entonces

$$H = \left\{[1], [1+\sqrt{2}], [3+2\sqrt{2}], [7+\sqrt{2}]\right\}$$

$$K = \left\{[1], [5]\right\} \quad \text{y} \quad J = \left\{[1], [-1]\right\}$$

Ahora

$$K \times J = \left\{[1], [5], [-1], [-5]\right\} = \left\{[1], [5], [7], [3]\right\}$$

Como $[-1]$ no está en $K$, $K \cap J = \{[1]\}$ y ya que tanto $K \times J$ como $H$ tienen orden 4, se tiene que el orden de $H \times (K \times J)$ es $16 = \phi(\alpha^5)$. Luego

$$\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^5\,\mathbb{Z}[\sqrt{2}]} = H \times K \times J \simeq C_4 \times C_2 \times C_2$$

Usando los Teoremas 1 y 2 podemos contar los elementos de los grupos de unidades. Obtenemos los siguientes resultados

i) $\phi(\pi^n) = \phi(q^n) = q^n - q^{n-1} = q^{n-1}(q-1)$

ii) $\phi(p^n) = p^{2n} - p^{2n-2} = p^{2n-2}(p^2-1)$

iii) $\phi(\alpha^n) = 2^n - 2^{n-1} = 2^{n-1}$.

A modo de ejemplo probemos (ii). Ya que el número de clases en $\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}$ es $Np^n = p^{2n}$, el orden $\phi(p^n)$ del grupo de unidades de este anillo se

se obtiene restando de $p^{2n}$ el número de clases $[a + b\sqrt{2}]$ en $\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}$ para las cuales $p$ es un divisor de $a$ y $b$. Hay entre 0 y $p^n$, $p^{n-1}$ enteros $a$ que son múltiplos de $p$ y $p^{n-1}$ enteros $b$ que son múltiplos de $p$. Es decir, hay $p^{2n-2}$ clases en $\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}$ en las que $p$ es un divisor de $a$ y $b$. Por lo tanto

$$\phi(p^n) = p^{2n} - p^{2n-2} = p^{2n-2}(p^2 - 1)$$

En forma análoga se obtienen los otros resultados. Estos pueden verificarse en los Ejemplos 3, 4 y 5.

Prosiguiendo con nuestro programa, vamos a determinar las estructuras de los grupos de unidades que hemos estado estudiando.

4. La estructura de $\left(\frac{\mathbb{Z}[\sqrt{-2}]}{\pi^n\,\mathbb{Z}[\sqrt{-2}]}\right)^*$.

Vimos en el Ejemplo 3 que $\left(\frac{\mathbb{Z}[\sqrt{-2}]}{\pi^2\,\mathbb{Z}[\sqrt{-2}]}\right)^*$ es cíclico. Esto corresponde exactamente a la situación general.

Teorema 3. $\left(\frac{\mathbb{Z}[\sqrt{-2}]}{\pi^n\,\mathbb{Z}[\sqrt{-2}]}\right)^* \simeq C_{|q|^n-|q|^{n-1}}$

Demostración: Por el Teorema 2

$$\left(\frac{\mathbb{Z}[\sqrt{-2}]}{\pi^n\,\mathbb{Z}[\sqrt{-2}]}\right)^* = \left\{[a] \mid 0 \leq a < |q|^n\,,\quad q \nmid a\right\}.$$

La aplicación $[a] \in \left(\mathbb{Z}/_{|q|^n\,\mathbb{Z}}\right)^* \longrightarrow [a] \in \left(\frac{\mathbb{Z}[\sqrt{-2}]}{\pi^n\,\mathbb{Z}[\sqrt{-2}]}\right)^*$ es un isomorfismo de $\left(\mathbb{Z}/_{|q|^n\,\mathbb{Z}}\right)^*$ sobre $\left(\frac{\mathbb{Z}[\sqrt{-2}]}{\pi^n\,\mathbb{Z}[\sqrt{-2}]}\right)^*$. En efecto, las proposiciones $(a,|q|^n) = 1 \Rightarrow q \nmid a$ y $|q|^n \mid a - b \Rightarrow \pi^n \mid a - b$ implican que $[a] \to [a]$ está bien definida. Además, $\pi^n \mid a - b \Rightarrow q^n \mid a - b$ significa que la aplicación es inyectiva.

Por otra parte $\left(\mathbb{Z}/_{|q|^n\,\mathbb{Z}}\right)^*$ y $\left(\frac{\mathbb{Z}[\sqrt{-2}]}{\pi^n\,\mathbb{Z}[\sqrt{-2}]}\right)^*$ tienen el mismo orden $\phi(\pi^n) = |q|^n - |q|^{n-1}$, de modo que la aplicación es sobreyectiva.

5. Algunas ideas preliminares referentes a $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n\ \mathbb{Z}[\sqrt{2}]}\right)^*$ y a $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\ \mathbb{Z}[\sqrt{2}]}\right)^*$.

En la Sección anterior tratamos de primos en $\mathbb{Z}[\sqrt{2}]$ que son factores de primos racionales. Los grupos de unidades que corresponden a los otros dos tipos de primos son en general no cíclicos según lo visto en la Introducción y en el Ejemplo 5. Demostramos en el Ejemplo 5 que $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^5\ \mathbb{Z}[\sqrt{2}]}\right)^* = H \times K \times J$. Veamos si podemos obtener una estructura similar cuando $\alpha$ se eleva a una potencia par.

Ejemplo 6. Por los Teoremas 1 y 2

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^6\ \mathbb{Z}[\sqrt{2}]}\right)^* = \left(\frac{\mathbb{Z}[\sqrt{2}]}{8\ \mathbb{Z}[\sqrt{2}]}\right)^* = \left\{[a + b\sqrt{2}] \mid 0 \leq a,b < 8\ ,\ 2 \nmid a\right\}$$

Sean como antes $H,K$ y $J$ subgrupos de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{8\ \mathbb{Z}[\sqrt{2}]}\right)^*$ generados por $[1 + \sqrt{2}]$, $[5]$ y $[-1]$ respectivamente. Entonces

$$H = \{[1], [1 + \sqrt{2}], [3 + 2\sqrt{2}], [7 + 5\sqrt{2}], [1 + 4\sqrt{2}], [1 + 5\sqrt{2}]$$
$$[3 + 6\sqrt{2}], [7 + \sqrt{2}]\}$$

$$K = \{[1], [5]\} \qquad y \qquad J = \{[1], [-1]\}\ .$$

Se tiene que $K \times J = \{[1], [3], [5], [7]\}$, de modo que $H \cap (K \times J) = \{[1]\}$. Luego el orden de $H \times K \times J$ es $32 = \phi(\alpha^6)$.

Luego $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^6\ \mathbb{Z}[\sqrt{2}]}\right)^* = H \times K \times J$.

Los Ejemplos 5 y 6 permiten conjeturar que $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n\,\mathbb{Z}[\sqrt{2}]}\right)^* = H \times K \times J$ donde H,K y J son los subgrupos generados por $[1+\sqrt{2}]$, $[5]$ y $[-1]$ respectivamente. Esta conjetura funciona para $\alpha^7$ y $\alpha^8$, pero consideremos otra referente a $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$. Esta conjetura involucra el subgrupo generado por $[1+p\sqrt{2}]$. Estudiaremos este subgrupo y el subgrupo H simultáneamente.

Ahora $\phi(3^2) = 72$, $\phi(3^3) = 648$, $\phi(5^2) = 600$. Es claro que las ideas que se refieren a la estructura de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$ no pueden obtenerse dando tablas de multiplicación. Sin embargo, mediante cálculos directos, pueden encontrarse los órdenes de los elementos de algunos de estos grupos y esperar observar algo significativo. Los resultados de este cálculo se resumen a continuación donde hemos calculado los máximos ordenes observados y el orden de $[1+p\sqrt{2}]$

| GRUPO | ORDEN | MAX. ORDEN DE UN ELEMENTO | ORDEN DE $[1 + p\sqrt{2}]$ |
|---|---|---|---|
| $\left(\mathbb{Z}[\sqrt{2}]/3^2\,\mathbb{Z}[\sqrt{2}]\right)^*$ | $72 = 3^2(3^2 - 1)$ | $24 = 3(3^2 - 1)$ | 3 |
| $\left(\mathbb{Z}[\sqrt{2}]/3^3\,\mathbb{Z}[\sqrt{2}]\right)^*$ | $648 = 3^4(3^2 - 1)$ | $72 = 3^2(3^2 - 1)$ | 9 |
| $\left(\mathbb{Z}[\sqrt{2}]/5^2\,\mathbb{Z}[\sqrt{2}]\right)^*$ | $600 = 5^2(5^2 - 1)$ | $120 = 5(5^2 - 1)$ | 5 |
| $\left(\mathbb{Z}[\sqrt{2}]/5^3\,\mathbb{Z}[\sqrt{2}]\right)^*$ | $15.000 = 5^4(5^2 - 1)$ | $600 = 5^2(5^2 - 1)$ | 25 |
| $\left(\mathbb{Z}[\sqrt{2}]/11^2\,\mathbb{Z}[\sqrt{2}]\right)^*$ | $11^2(11^2 - 1)$ | $1.320 = 11(11^2 - 1)$ | 11 |

Vemos en cada caso que el mayor orden observado es $p^{n-1}(p^2 - 1)$ y el producto de este número con $p^{n-1}$ es $\Phi(p^n) = p^{2n-2}(p^2 - 1)$. Podemos conjeturar que $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^* = L \times K$ donde $L$ es cíclico de orden $p^{n-1}(p^2 - 1)$ y $K$ tiene orden $p^{n-1}$. Esto implicaría que $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^* = H \times K \times R$, donde $H$ tiene orden $p^{n-1}$ y $R$ tiene orden $p^2 - 1$. Observamos también que el orden de $[1 + p\sqrt{2}]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$ parece ser $p^{n-1}$, si $n > 1$.

Ejemplo 7. Con referencia a la Tabla 1 sean $H,K$ y $R$ los subgrupos de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{9\,\mathbb{Z}[\sqrt{2}]}\right)^*$ generados por $[1 + 3\sqrt{2}]$, $[4]$ y $[7 + 5\sqrt{2}]$. Entonces

$$H = \{[1], [1 + 3\sqrt{2}], [1 + 6\sqrt{2}]\}$$

$$K = \{[1], [4], [7]\}$$

y $$R = \{[1], [7 + 5\sqrt{2}], [7\sqrt{2}], [7 + 4\sqrt{2}], [8], [2 + 4\sqrt{2}],$$

$$[2\sqrt{2}], [2 + 5\sqrt{2}]\} .$$

Ya que $H \cap K = \{[1]\}$ , $H \times K$ tiene orden 9 y como 8 es relativamente primo con 9, $(H \cap K) \cap R = \{[1]\}$ . ($G$ grupo finito, $G_1 \leq G$ , $G_2 \leq G$ . $(|G_1|, |G_2|) = 1 \Rightarrow G_1 \cap G_2 = \{1\}$ . En efecto, $g \in G_1 \cap G_2 \Rightarrow |g| \mid |G_1|$ , $|g| \mid |G_2| \Rightarrow |g| \mid (|G_1|, |G_2|) = 1 \Rightarrow g = 1$) . Se tiene así que $H \times K \times R$ tiene $72 = \phi(3^2)$ elementos. Por lo tanto

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{9\,\mathbb{Z}[\sqrt{2}]}\right)^* = H \times K \times R$$

En resumen, los Ejemplos 5, 6 y 7 y la Tabla de órdenes nos permiten afirmar que

i) $$\left(\frac{\mathbb{Z}[\sqrt{2}]}{a^n\,\mathbb{Z}[\sqrt{2}]}\right)^* = H \times K \times J$$ , donde $H, K$ y $J$ son generados por

$[1 + \sqrt{2}]$ , $[5]$ y $[-1]$ respectivamente.

ii) $$\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^* = H \times K \times R$$ , donde $H$ es generado por $[1 + p\sqrt{2}]$ ,

$K$ tiene orden $p^{n-1}$ , $(n > 1)$ y $R$ tiene orden $p^2 - 1$ .

Probaremos ahora estas afirmaciones estudiando los subgrupos indicados por $H$ en (i) y (ii). Para ello necesitamos los siguientes dos Lemas cuyas demostraciones son básicamente las del Lema 3 y Corolarios 1 y

2 en [6] p. 42, 43.

Lema 1. Sea $\ell$ entero positivo y $\beta \equiv \gamma(p^{\ell})$ , entonces

$$\beta^p \equiv \gamma^p(p^{\ell+1}) .$$

Demostración: Podemos escribir $\beta = \gamma + p^{\ell}\delta$ , $\delta \in \mathbb{Z}[\sqrt{2}]$ . Por el Teorema del Binomio, $\beta^p = \gamma^p + p^{\ell+1}\gamma^{p-1}\delta + A$ , donde $A$ es un entero de $\mathbb{Z}[\sqrt{2}]$ divisible por $p^{\ell+2}$ . El segundo término es claramente divisible por $p^{\ell+1}$ . Así, $\beta^p \equiv \gamma^p(p^{\ell+1})$ .

Lema 2. Sea $k$ entero no negativo. Entonces

$$(1 + p\sqrt{2})^{p^k} = 1 + p^{k+1}\sqrt{2} + p^{k+2}\gamma , \qquad \gamma \in \mathbb{Z}[\sqrt{2}] .$$

Demostración: Probaremos por inducción sobre $k$ que

$$(1 + p\beta)^{p^k} \equiv 1 + p^{k+1}\beta(p^{k+2}) , \qquad \forall\, k \geq 0 .$$

Para $k = 0$ , la congruencia es inmediata. Supongamos que para cierto $k > 0$ , $(1 + p\beta)^{p^k} \equiv 1 + p^{k+1}\beta(p^{k+2})$ . Probaremos que ésta es verdadera para $k + 1$ . Por el Lema 1 tenemos que

$$(1 + p\beta)^{p^{k+1}} \equiv (1 + p^{k+1}\beta)^p(p^{k+3}) .$$

Por el Teorema del Binomio, $(1 + p^{k+1}\beta)^p = 1 + p^{k+2}\beta + B$ , donde $B$ es una suma de $p - 1$ términos. Ya que $p$ es primo, $\binom{p}{j}$ , $0 < j < p$ , es dividible por $p$ . Así, todos los términos de $B$ , con la posible excepción del último, $p^{(k+1)p}\beta^p$ , son divisibles por $p^{k+3}$ , puesto que

$1 + 2(k + 1) \geq k + 3$ si $k > 0$ . Además, $1 + j(k + 1) \geq k + 3$ , pues $j \geq 2$ . Ya que $p \geq 3$ , $p(k + 1) \geq 3$ . Así, $p^{k+3}$ divide a $B$ y

$$(1 + p^{k+1}\beta)^p \equiv 1 + p^{k+2}\beta(p^{k+3}) .$$

Hemos demostrado que $(1 + p\beta)^{p^k} \equiv 1 + p^{k+1}\beta(p^{k+2})$ , $\forall\, k \geq 0$ .

Haciendo $\beta = \sqrt{2}$ , se obtiene la fórmula del Lema.

Corolario. Sea $n$ entero mayor que 1. Sea $\rho = 1 + p\sqrt{2}$ . Entonces el orden de $[\rho]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es $p^{n-1}$ .

Demostración: Haciendo $k = n - 1$ en la fórmula del Lema 2 se tiene

$$\rho^{p^{n-1}} = 1 + p^n\sqrt{2} + p^{n+1}\gamma \quad , \text{ para algún } \gamma \text{ en } \mathbb{Z}[\sqrt{2}]$$

$$\equiv 1(p^n) ,$$

por consiguiente, el orden de $[\rho]$ es un divisor de $p^{n-1}$ . Es suficiente probar que

$$\rho^{p^{n-2}} \not\equiv 1(p^n) .$$

Haciendo $k = n - 2$ , tenemos

$$\rho^{p^{n-2}} = 1 + p^{n-1}\sqrt{2} + p^n\gamma \quad , \qquad \gamma \in \mathbb{Z}[\sqrt{2}]$$

$$\equiv 1 + p^{n-1}\sqrt{2}\ (p^n) .$$

Por lo tanto el orden de $[1 + p\sqrt{2}]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es $p^{n-1}$ .

Estudiamos ahora el orden de $[1 + \sqrt{2}]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m}\,\mathbb{Z}[\sqrt{2}]}\right)^*$ y en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m+1}\,\mathbb{Z}[\sqrt{2}]}\right)^*$ . La siguiente tabla nos permite formular una conjetura al respecto:

| GRUPO | ORDEN | ORDEN DE $[1 + \sqrt{2}]$ |
|---|---|---|
| $\left(\mathbb{Z}[\sqrt{2}]/\alpha^4\,\mathbb{Z}[\sqrt{2}]\right)^*$ | $8 = 2^3$ | $4 = 2^2$ |
| $\left(\mathbb{Z}[\sqrt{2}]/\alpha^5\,\mathbb{Z}[\sqrt{2}]\right)^*$ | $16 = 2^4$ | $4 = 2^2$ |
| $\left(\mathbb{Z}[\sqrt{2}]/\alpha^6\,\mathbb{Z}[\sqrt{2}]\right)^*$ | $32 = 2^5$ | $8 = 2^3$ |
| $\left(\mathbb{Z}[\sqrt{2}]/\alpha^7\,\mathbb{Z}[\sqrt{2}]\right)^*$ | $64 = 2^6$ | $8 = 2^3$ |
| $\left(\mathbb{Z}[\sqrt{2}]/\alpha^8\,\mathbb{Z}[\sqrt{2}]\right)^*$ | $128 = 2^7$ | $16 = 2^4$ |
| $\left(\mathbb{Z}[\sqrt{2}]/\alpha^9\,\mathbb{Z}[\sqrt{2}]\right)^*$ | $256 = 2^8$ | $16 = 2^4$ |

Al parecer el orden de $[1 + \sqrt{2}]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m}\,\mathbb{Z}[\sqrt{2}]}\right)^*$ y en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m+1}\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es $2^m$ . De hecho este es el caso si $m > 1$ . Nuestra conjetura no se cumple para $m = 1$ . Se verifica que el orden de $[1 + \sqrt{2}]$

en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^2\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es 2. Sin embargo, el orden de $[1+\sqrt{2}]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^3\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es 4.

Lema 3. Sea $m$ un entero mayor que 1 y $\delta = 1+\sqrt{2}$. Entonces el orden de $[\delta]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m}\,\mathbb{Z}[\sqrt{2}]}\right)^*$ y en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m+1}\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es $2^m$.

Demostración: Observemos primero que

$$\beta \equiv \gamma(2^m\alpha) \Rightarrow \beta^2 \equiv \gamma^2(2^{m+1}\alpha) \qquad (*)$$

En efecto, de $\beta \equiv \gamma(2^m\alpha)$ se obtiene $\beta - \gamma = 2^m\alpha\eta$ y $\beta + \gamma \equiv 2\gamma(2^m\alpha)$. Así

$$\beta^2 - \gamma^2 = (\beta-\gamma)(\beta+\gamma) = 2^{m+1}\alpha\mu \text{ , con } \mu \in \mathbb{Z}[\sqrt{2}] .$$

Usemos inducción para demostrar que

$$\delta^{2^m} \equiv 1(2^m\alpha) , \qquad \forall\, m > 1 .$$

Para $m = 2$, $(1+\sqrt{2})^4 = 17 + 12\sqrt{2}$

$$\equiv 1 + 4\sqrt{2}\ (8)$$

$$\equiv 1\ (4\alpha)$$

Sea $m > 2$ y supongamos que $\delta^{2^m} \equiv 1(2^m\alpha)$. Por (*) se tiene $\delta^{2^{m+1}} \equiv 1(2^{m+1}\alpha)$. Luego

$$\delta^{2^m} \equiv 1(2^m\alpha) , \qquad \forall\, m > 1$$

y el orden de $[\delta]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m+1}\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es un divisor de $2^m$ . Para demostrar que el orden de $[\delta]$ es $2^m$ es suficiente probar que

$$\delta^{2^{m-1}} \equiv 1 + 2^{m-1}\sqrt{2}(2^m\alpha) , \qquad \forall\, m > 1 .$$

Si $m = 3$ , $\quad \delta^4 = 17 + 12\sqrt{2}$

$$\equiv 1 + 12\sqrt{2}\ (16) .$$

Como $8\alpha$ divide a 16, se obtiene

$$\delta^4 \equiv 1 + 4\sqrt{2}\ (8\alpha)$$

Para $m > 3$ , supongamos que $\delta^{2^{m-1}} \equiv 1 + 2^{m-1}\sqrt{2}\ (2^m\alpha)$ . Entonces por (*) se tiene

$$\delta^{2^m} \equiv (1 + 2^{m-1}\sqrt{2})^2(2^{m+1}\alpha)$$

$$\equiv 1 + 2^m\sqrt{2} + 2^{2m-1}(2^{m+1}\alpha)$$

Pero $2^{m+1}\alpha$ divide a $2^{2m-1}$ , pues para $m \geq 3$ :

$$\frac{2^{2m-1}}{2^{m+1}\,\alpha} = \frac{2^{2m-1}\alpha}{2^{m+2}} = 2^{m-3}\alpha \in \mathbb{Z}[\sqrt{2}]$$

Luego

$$\delta^{2^m} \equiv 1 + 2^m\sqrt{2}\ (2^{m+1}\alpha) .$$

Para $m = 2$ ,

$$\delta^2 = (1 + \sqrt{2})^2 = 3 + 2\sqrt{2} \not\equiv 1(4\alpha)$$

Hemos probado así que

$$\delta^{2^{m-1}} \not\equiv 1(2^m\alpha) \quad , \qquad \forall\, m > 1$$

Por tanto, el orden de $[\delta]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m+1}\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es $2^m$ .

El resultado anterior implica que

$$\delta^{2^m} \equiv 1(2^m) \quad \text{y} \quad \delta^{2^{m-1}} \not\equiv 1(2^m) \quad , \qquad \forall\, m > 1 \ ,$$

de modo que el orden de $[\delta]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m}\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es también $2^m$ .

De acuerdo con nuestras conjeturas intentamos usar los subgrupos generados por $[1 + p\sqrt{2}]$ y $[1 + \sqrt{2}]$ e indicados por $H$ como factores de ciertos productos directos. Para este propósito será necesario el siguiente Lema que se refiere a la forma de los elementos de $H$ .

Lema 4. Sean $m$ y $n$ enteros positivos mayores que 1.
Sean $\rho = 1 + p\sqrt{2}$ y $\delta = 1 + \sqrt{2}$ . Ningún elemento, excepto $[1]$, del subgrupo de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$ generado por $[\rho]$ y ningún elemento, excepto $[1]$, del subgrupo de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m}\,\mathbb{Z}[\sqrt{2}]}\right)^*$ o de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m+1}\,\mathbb{Z}[\sqrt{2}]}\right)^*$ generado por $[\delta]$ puede representarse por una clase de la forma $[c]$ ó $[c\sqrt{2}]$ , donde $c$ es un entero racional.

Demostración: Un número $c \in \mathbb{R}$ se llama especial si $c \in \mathbb{Z}$ ó $c = c_1\sqrt{2}$, donde $c_1 \in \mathbb{Z}$. Probaremos que para todo $b$, $0 < b < p^{n-1}$, $\rho^b$ no es congruente módulo $p^n$ a un número especial. Sea

$$B = \{b \mid 0 < b < p^{n-1}, \ \rho^b \equiv c(p^n)\} .$$

$p^{n-2} \notin B$, pues si $p^{n-2} \in B$, entonces $\rho^{p^{n-2}} \equiv s(p^n)$, donde $s$ es algún número especial. Por otra parte, haciendo $k = n - 2$ en la fórmula del Lema 2 se tiene $\rho^{p^{n-2}} \equiv 1 + p^{n-1}\sqrt{2}\ (p^n)$. Se deduce que $1 - s + p^{n-1}\sqrt{2} \equiv 0(p^n)$.

Si $s \in \mathbb{Z}$, entonces $p^n \mid p^{n-1}$. Si $s = s_1\sqrt{2}$, entonces $p^n \mid 1$. En ambos casos hay contradicciones que provienen de suponer que $p^{n-2} \in B$. Por tanto $p^{n-2} \notin B$. Para completar la demostración supongamos que $B$ es no vacío y sea $L$ el menor elemento de $B$. Sean $d$ y $r$ en $\mathbb{Z}$ tales que

$$p^{n-1} = Ld + r , \quad \text{con} \quad 0 \leq r < L$$

Si $r = 0$, $p^{n-1} = Ld$ y $L = p^t$, para algún $t$ que satisface $0 < t < n - 2$. (Hemos demostrado que $t \neq n - 2$). Entonces

$$\rho^{p^{n-2}} = \rho^{L \cdot p^{n-2-t}}$$

Como $L \in B$, $\rho^L \equiv$ # especial $(p^n)$ y en consecuencia

$$\rho^{p^{n-2}} = \rho^{L \cdot p^{n-2-t}} \equiv \text{\# especial } (p^n) ,$$

lo que es imposible, pues $p^{n-2} \notin B$. Por tanto $r \neq 0$.

Ya que el orden de $[\rho]$ es $p^{n-1}$ ,

(1) $\quad [1] = [\rho^{Ld}][\rho^r] = [s][\rho^r]$ en $\left(\dfrac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$

donde $s$ es un número especial. Sea $s = x$ ó $s = x\sqrt{2}$ , con $x$ entero racional. Ya que $[s]$ es un elemento de $\left(\dfrac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$ entonces $p$ no divide a $x$ , (pues $[a + b\sqrt{2}] \in \dfrac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}$ es unidad $\Leftrightarrow p \nmid a$ ó $p \nmid b$) . Sea $y \in \mathbb{Z}$ tal que $[xy] = [1]$ en $\left(\mathbb{Z}/_{p^n\,\mathbb{Z}}\right)^*$ , entonces $p^n$ divide a $xy - 1$ en $\mathbb{Z}$ y también en $\mathbb{Z}[\sqrt{2}]$ . Por tanto $[xy] = [1]$ en $\left(\dfrac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$ . Multiplicando (1) por $[y]$ se obtiene

(2) $\quad [y] = [ys][\rho^r]$ en $\left(\dfrac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$

Si $s = x$ , entonces $[y] = [\rho^r]$.

Si $s = x\sqrt{2}$ , entonces $[y] = [\sqrt{2}][\rho^r]$ (3)

Pero $[\sqrt{2}]$ es un elemento de $\left(\dfrac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$ y $[\sqrt{2}]^{-1} = [u\sqrt{2}]$ , $u \in \mathbb{Z}$ , es una clase especial. Pues, si $[a + b\sqrt{2}] \in \dfrac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}$ es tal que $[a + b\sqrt{2}][\sqrt{2}] = [1]$ , entonces $2b - 1 + a\sqrt{2} \equiv 0(p^n)$ , es decir, $p^n \mid 2b - 1$ y $p^n \mid a$ . Se deduce que $a = 0$ y $2b \equiv 1(p^n)$ . Esta última congruencia tiene solución $b \equiv u$ en $\mathbb{Z}$ pues $p$ no divide a 2 . Multiplicando (3) por $[\sqrt{2}]^{-1}$ se obtiene $[yu\sqrt{2}] = [\rho^r]$ . En ambos casos, $\rho^r$ es congruente módulo $p^n$ a un número especial, es decir,

$r \in B$ , lo que contradice nuestra elección de $L$ . Esta contradicción proviene de suponer que $B$ es no vacío. Hemos demostrado así la primera parte del Lema. Para la demostración de la segunda parte se considera nuevamente

$$B = \{b \mid 0 < b < 2^m \quad , \quad \delta^b \equiv c(2^m)\} \neq \phi \ .$$

Como antes se deduce que $2^{m-1} \notin B$ . Sea $L$ el elemento mínimo de $B$ y $d,r$ enteros racionales tales que

$$2^m = Ld + r \quad , \quad 0 \leq r < L \ .$$

Entonces $r \neq 0$ .

Ya que el orden de $[\delta]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m}\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es $2^m$ ,

$$[1] = [\delta^{Ld}][\delta^r] = [s][\delta^r] \quad \text{en} \quad \left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m}\,\mathbb{Z}[\sqrt{2}]}\right)^* \ ,$$

para algún $s$ especial. Sea $s = x$ ó $s = x\sqrt{2}$ , $x$ entero.

Puesto que $[s]$ es un elemento del grupo de unidades, entonces por el Teorema 2, $s = x\sqrt{2}$ es imposible. Si $s = x$ , entonces $x$ es impar. Sea $y \in \mathbb{Z}$ tal que $[yx] = [1]$ en $\left(\mathbb{Z}/_{2^m\,\mathbb{Z}}\right)^*$ . Entonces $2^m$ divide a $xy - 1$ en $\mathbb{Z}$ y en $\mathbb{Z}[\sqrt{2}]$ . Por tanto, $[xy] = [1]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{2^m\,\mathbb{Z}[\sqrt{2}]}\right)^*$ . Multiplicando (4) por $[y]$ se tiene

$$[y] = [ys][\delta^r] = [\delta^r] \quad \text{en} \quad \left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m}\,\mathbb{Z}[\sqrt{2}]}\right)^* \ .$$

Luego $r \in B$ , lo que contradice nuestra elección de $L$ . Hemos demostrado así que ningún elemento, salvo $[1]$, del subgrupo de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m}\,\mathbb{Z}[\sqrt{2}]}\right)^*$ generado por $[\delta]$ es una clase especial. Observemos por último que $\forall\, b$ , $0 < b < 2^m$ , $\delta^b \not\equiv s(2^m)$ implica $\delta^b \not\equiv s(2^m\alpha)$ . Con esto se completa la demostración del Lema.

6. Estructura de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$ .

Conjeturamos en la Sección precedente que $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^* = H \times K \times R$ , donde $H$ es generado por $[1 + p\sqrt{2}]$ , $K$ tiene orden $p^{n-1}$ y $R$ es de orden $p^2 - 1$ . Hemos establecido las propiedades que nos interesan en $H$ . Estudiaremos ahora el subgrupo $K$ .

Vimos en el Ejemplo 4 que $\left(\mathbb{Z}/9\,\mathbb{Z}\right)^*$ está contenido en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{9\,\mathbb{Z}[\sqrt{2}]}\right)^*$ mediante un isomorfismo obvio. Esto es un caso particular del siguiente resultado general: la aplicación

$$[a] \in \left(\mathbb{Z}/p^n\,\mathbb{Z}\right)^* \longrightarrow [a] \in \left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$$

es un isomorfismo. Sabemos que $\left(\mathbb{Z}/p^n\,\mathbb{Z}\right)^*$ es cíclico de orden $p^{n-1}(p - 1)$ . Entonces existe $[a]$ en $\left(\mathbb{Z}/p^n\,\mathbb{Z}\right)^*$ de orden $p^{n-1}$ . El isomorfismo implica luego que $[a]$ tiene orden $p^{n-1}$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$. Sea $K$ el subgrupo generado por $[a]$ . Cada elemento de $K$ se representa por una clase especial. Así, $H \cap K = \{[1]\}$ y $H \times K$ es de orden $p^{2n-2}$ .

Estudiamos ahora el subgrupo $R$ . Como $p$ es primo en $\mathbb{Z}[\sqrt{2}]$ , $\frac{\mathbb{Z}[\sqrt{2}]}{p\,\mathbb{Z}[\sqrt{2}]}$ es un cuerpo y $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es cíclico de orden $p^2 - 1$ ,

ya que es el grupo multiplicativo de un cuerpo finito. Sea $[\beta]$ un generador de este grupo. Entonces $\beta^{p^2-1} \equiv 1(p)$ y $\beta^{p^2-1} = 1 + \gamma p$, cierto $\gamma \in \mathbb{Z}[\sqrt{2}]$. Por la demostración del Lema 2, $(1 + \gamma p)^{p^{n-1}} = 1 + \eta p^n$, con $\eta \in \mathbb{Z}[\sqrt{2}]$. Por tanto $\left(\beta^{p^{n-1}}\right)^{p^2-1} \equiv 1(p^n)$, es decir, el orden de $[\beta^{p^{n-1}}]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es un divisor de $p^2 - 1$. Sea $t$ el orden de $[\beta^{p^{n-1}}]$. Entonces $\beta^{tp^{n-1}} \equiv 1(p^n)$ y en consecuencia $\beta^{tp^{n-1}} \equiv 1(p)$. Ya que el orden de $[\beta]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es $p^2 - 1$, se deduce que $p^2 - 1$ divide a $tp^{n-1}$. Como $p^2 - 1$ y $p^{n-1}$ son relativamente primos, sigue que $p^2 - 1$ es un divisor de $t$. Luego $t = p^2 - 1$ y el orden de $[\beta^{p^{n-1}}]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es $p^2 - 1$. Sea $R$ el subgrupo de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$ generado por $[\beta^{p^{n-1}}]$. Ya que todo elemento de $H \times K$ tiene orden una potencia de $p$, $(H \times K) \cap R = \{[1]\}$ y el orden de $H \times K \times R$ es $p^{2n-2}(p^2 - 1) = \phi(p^n)$. Así, la afirmación $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^* = H \times K \times R$ está demostrada. En resumen:

Teorema 4.

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^* \simeq C_{p^{n-1}} \times C_{p^{n-1}} \times C_{p^2-1}$$

La demostración de este Teorema es válida sólo para $n > 1$, pero el Teorema también se cumple para $n = 1$. En este caso $C_{p^{n-1}}$ es trivial y $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p\,\mathbb{Z}[\sqrt{2}]}\right)^* \simeq C_{p^2-1}$.

Observación. En el Ejemplo 7, los subgrupos K y R pueden obtenerse sin referencia a la Tabla 1. Examinamos primero los seis elementos de $\left(\mathbb{Z}/9\,\mathbb{Z}\right)^*$, encontrando que $[4]$ tiene orden 3 y hacemos K el subgrupo generado por $[4]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{9\,\mathbb{Z}[\sqrt{2}]}\right)^*$. Luego escribimos los ocho elementos de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{3\,\mathbb{Z}[\sqrt{2}]}\right)^*$ y vemos que $[1+\sqrt{2}]$ es un generador. Consideramos R como el subgrupo generado por $[(1+\sqrt{2})^3] = [7+5\sqrt{2}]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{9\,\mathbb{Z}[\sqrt{2}]}\right)^*$.

7. Estructura de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n\ \mathbb{Z}[\sqrt{2}]}\right)^*$ .

Comprobamos en la Sección 5 que $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n\ \mathbb{Z}[\sqrt{2}]}\right)^* = H \times K \times J$ , donde H, K y J son los subgrupos generados por $[1+\sqrt{2}]$, $[5]$ y $[-1]$ respectivamente. Sin embargo, el Lema 3 se cumple para $m > 1$ , de manera que para $n < 4$ determinamos directamente la estructura de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n\ \mathbb{Z}[\sqrt{2}]}\right)^*$ . Más aún, en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^4\ \mathbb{Z}[\sqrt{2}]}\right)^* = \left(\frac{\mathbb{Z}[\sqrt{2}]}{4\ \mathbb{Z}[\sqrt{2}]}\right)^*$ el subgrupo generado por $[5]$ es trivial. Por tanto damos la estructura de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n\ \mathbb{Z}[\sqrt{2}]}\right)^*$ en dos Teoremas; el primero aplicable a $n = 1, 2, 3$ y $4$ y el segundo, a $n \geq 5$ .

Teorema 5.

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha\ \mathbb{Z}[\sqrt{2}]}\right)^* \simeq C_1 \quad ; \quad \left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^2\ \mathbb{Z}[\sqrt{2}]}\right)^* \simeq C_2$$

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^3\ \mathbb{Z}[\sqrt{2}]}\right)^* \simeq C_4 \quad ; \quad \left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^4\ \mathbb{Z}[\sqrt{2}]}\right)^* \simeq C_2 \times C_4 \ .$$

Demostración: Por el Teorema 2,

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha\ \mathbb{Z}[\sqrt{2}]}\right)^* = \{[1]\}$$

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^2\ \mathbb{Z}[\sqrt{2}]}\right)^* = \{[1],\ [1+\sqrt{2}]\}$$

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^3\,\mathbb{Z}[\sqrt{2}]}\right)^* = \{[1],\ [3],\ [1+\sqrt{2}],\ [3+\sqrt{2}]\}$$

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^4\,\mathbb{Z}[\sqrt{2}]}\right)^* = \{[1],\ [3],\ [1+\sqrt{2}],\ [3+\sqrt{2}],\ [1+2\sqrt{3}],\ [3+2\sqrt{2}],\ [1+3\sqrt{2}],\ [3+3\sqrt{2}]\}\ .$$

Podemos verificar que $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^3\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es el grupo cíclico de orden cuatro generado por $[1+\sqrt{2}]$ . Por otra parte, $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^4\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es el producto directo de los subgrupos cíclicos

$$H = \{[1],\ [1+\sqrt{2}],\ [3+2\sqrt{2}],\ [3+\sqrt{2}]\}$$

y $$D = \{[1],\ [1+2\sqrt{2}]\}\ .$$

Supongamos ahora que $n \geq 5$ y probamos la afirmación (i) de la Sección 5. Hemos estudiado el subgrupo $H$ en lo que se refiere a su orden y a la forma de sus elementos. Las propiedades de $K$ que nos interesan están dadas en el siguiente Lema:

Lema 5. Sea $n \geq 5$ . El orden de $[5]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es $2^{m-2}$ ó $2^{m-1}$ si $n = 2m$ ó $n = 2m+1$ . El elemento $[-1]$ de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$ no está en $K$ .

Demostración: Se demuestra usando inducción que para $\ell \geq 3$

$$5^{2^{\ell-3}} \equiv 1 + 2^{\ell-1}(2^{\ell})$$

y $$5^{2^{\ell-2}} \equiv 1(2^{\ell}) \qquad (*)$$

Cuando $n = 2m$ ó $n = 2m + 1$, hagamos $\ell = m$ ó $\ell = m + 1$ en (*). Se obtienen

$$5^{2^{m-2}} \equiv 1(2^{m}) \quad \text{y} \quad 5^{2^{m-1}} \equiv 1(2^{m+1}),$$

es decir, $[5]$ tiene orden $2^{m-2}$ en $\left(\mathbb{Z}/2^{m}\,\mathbb{Z}\right)^{*}$ y orden $2^{m-1}$ en $\left(\mathbb{Z}/2^{m+1}\,\mathbb{Z}\right)^{*}$. Ya que las aplicaciones

$$[a] \in \left(\mathbb{Z}/2^{m}\,\mathbb{Z}\right)^{*} \longrightarrow [a] \in \left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m}\,\mathbb{Z}[\sqrt{2}]}\right)^{*}$$

y

$$[a] \in \left(\mathbb{Z}/2^{m+1}\,\mathbb{Z}\right)^{*} \longrightarrow [a] \in \left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m+1}\,\mathbb{Z}[\sqrt{2}]}\right)^{*}$$

son isomorfismos, se deduce que $K$ tiene orden $2^{m-2}$ en $\dfrac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m}\,\mathbb{Z}[\sqrt{2}]}$ y orden $2^{m-1}$ en $\left(\dfrac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m+1}\,\mathbb{Z}[\sqrt{2}]}\right)^{*}$. Para probar que $[-1]$ no está en $K$ observemos que $-1 \equiv 5^{t}(2^{\ell})$, $\forall\, \ell \geq 3$, $0 < t < 2^{\ell-2}$ implica $2 \equiv 0(4)$ lo que es imposible.

Puesto que $[-1]$ no está en $K$, $K \cap J = \{[1]\}$ y ya que cada elemento de $K \times J$ es una clase de la forma $[c]$ con $c \in \mathbb{Z}$, $H \cap (K \times J) = \{[1]\}$. El orden de $H \times K \times J$ es por tanto

$$2^{m} \cdot 2^{m-2} \cdot 2 = 2^{2m-1} = 2^{n-1} = \phi(\alpha^{n}), \quad \text{si} \quad n = 2m$$

$$2^{m} \cdot 2^{m-1} \cdot 2 = 2^{2m} = 2^{n-1} = \phi(\alpha^{n}), \quad \text{si} \quad n = 2m + 1$$

Por tanto $\left(\frac{\mathbb{Z}[\sqrt{-2}]}{\alpha^n\,\mathbb{Z}[\sqrt{-2}]}\right)^* = H \times K \times J$ . Hemos probado el siguiente Teorema

Teorema 6. Si $n \geq 5$ , entonces

$$\left(\frac{\mathbb{Z}[\sqrt{-2}]}{\alpha^n\,\mathbb{Z}[\sqrt{-2}]}\right)^* \simeq \begin{cases} C_{2^m} \times C_{2^{m-2}} \times C_2 \,, & \text{si } n = 2m \\ C_{2^m} \times C_{2^{m-1}} \times C_2 \,, & \text{si } n = 2m+1 \,. \end{cases}$$

8. $\phi$ es multiplicativa.

Probaremos aquí que $\phi(\beta_1\beta_2) = \phi(\beta_1)\phi(\beta_2)$ , para todo $\beta_1,\beta_2 \in \mathbb{Z}[\sqrt{2}]$ tales que $(\beta_1,\beta_2) = 1$ . La herramienta fundamental a emplear será el Teorema Chino del Resto. Adoptaremos en esta Sección la siguiente notación:

i) $\beta\,\mathbb{Z}[\sqrt{2}] = (\beta)$ ;

ii) $[\eta] = \eta + (\beta)$ .

Teorema 8. Sean $\beta_1$ y $\beta_2$ en $\mathbb{Z}[\sqrt{2}]$ tales que $(\beta_1,\beta_2) = 1$ . Entonces

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{(\beta_1\beta_2)}\right)^* \simeq \left(\frac{\mathbb{Z}[\sqrt{2}]}{(\beta_1)}\right)^* \times \frac{\mathbb{Z}[\sqrt{2}]}{(\beta_2)}$$

Demostración: Sea $f : \mathbb{Z}[\sqrt{2}] \longrightarrow \frac{\mathbb{Z}[\sqrt{2}]}{(\beta_1)} \times \frac{\mathbb{Z}[\sqrt{2}]}{(\beta_2)}$ ;

$\eta \to (f_1(\eta), f_2(\eta))$ la aplicación de $\mathbb{Z}[\sqrt{2}]$ en el producto de anillos inducida por los homomorfismos canónicos $f_i : \mathbb{Z}[\sqrt{2}] \longrightarrow \frac{\mathbb{Z}[\sqrt{2}]}{(\beta_i)}$ con $f_i(\eta) = \eta + (\beta_i)$ , $i = 1,2$ . $f$ es un homomorfismo sobreyectivo de núcleo $(\beta_1) \cap (\beta_2)$ . En efecto

$$\eta \in \operatorname{Ker} f \iff f(\eta) = (\eta + (\beta_1),\ \eta + (\beta_2)) = ((\beta_1),(\beta_2))$$

$$\iff \eta + (\beta_i) = (\beta_i) \ , \quad i = 1,2$$

$$\iff \eta \in (\beta_i) \qquad , \quad i = 1,2$$

$$\iff \eta \in (\beta_1) \cap (\beta_2)$$

Observemos también que $(\beta_1,\beta_2) = 1$ implica $(\beta_1) \cap (\beta_2) = (\beta_1)(\beta_2)$ .

Para verificar la sobreyectividad sea $(\eta_1 + (\beta_1), \eta_2 + (\beta_2))$ en $\frac{\mathbb{Z}[\sqrt{-2}]}{(\beta_1)} \times \frac{\mathbb{Z}[\sqrt{-2}]}{(\beta_2)}$ . Entonces $\eta_1,\eta_2 \in \mathbb{Z}[\sqrt{-2}]$ y por el Teorema Chino del Resto existe $\eta \in \mathbb{Z}[\sqrt{-2}]$ tal que $\eta \equiv \eta_i(\beta_i)$ , $i = 1,2$ , es decir, $\eta + (\beta_i) \equiv \eta_i + (\beta_i)$ , $i = 1,2$ . Entonces $f_i(\eta) = \eta_i + (\beta_i)$ y $f(\eta) = (\eta_1 + (\beta_1), \eta_2 + (\beta_2))$ . Se deduce que

$$\bar{f} : \frac{\mathbb{Z}[\sqrt{-2}]}{(\beta_1\beta_2)} \longrightarrow \frac{\mathbb{Z}[\sqrt{-2}]}{(\beta_1)} \times \frac{\mathbb{Z}[\sqrt{-2}]}{(\beta_2)} \quad ,$$

$\bar{f}(\eta + (\beta_1\beta_2)) = (f_1(\eta), f_2(\eta))$ es un isomorfismo de anillos. Este isomorfismo induce un isomorfismo entre los grupos de unidades, pues $(\eta,\beta_1\beta_2) = 1$ implica $(\eta,\beta_1) = 1$ y $(\eta,\beta_2) = 1$ . Luego

$$\left(\frac{\mathbb{Z}[\sqrt{-2}]}{(\beta_1\beta_2)}\right)^* \simeq \left(\frac{\mathbb{Z}[\sqrt{-2}]}{(\beta_1)}\right)^* \times \left(\frac{\mathbb{Z}[\sqrt{-2}]}{(\beta_2)}\right)^* .$$

Del Teorema anterior se deduce que

$$\phi(\beta_1\beta_2) = \phi(\beta_1)\phi(\beta_2) , \quad \forall\, \beta_1,\beta_2 \in \mathbb{Z}[\sqrt{-2}] \text{ con } (\beta_1,\beta_2) = 1 .$$

Por inducción se demuestra que si $\beta_1, \ldots, \beta_r$ en $\mathbb{Z}[\sqrt{-2}]$ son tales que $(\beta_i,\beta_j) = 1$ , $\forall\, i \neq j$ ,

$$\phi(\beta_1 \ldots \beta_r) = \phi(\beta_1) \ldots \phi(\beta_r)$$

En particular, si $\beta = \beta_1^{n_1} \ldots \beta_r^{n_r}$ , donde $\beta_1, \ldots, \beta_r$ son primos en $\mathbb{Z}[\sqrt{-2}]$ y $n_1, \ldots, n_r$ enteros $\geq 1$ , entonces

$$\phi(\beta) = \phi(\beta_1^{n_1}) \ldots\ldots \phi(\beta_r^{n_r})$$

El siguiente ejemplo ilustra los principales resultados de este trabajo.

Ejemplo 8. Sea $\gamma = 144 + 162\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ . La norma de $\gamma$ es

$$N\gamma = -31.752 = -2^3\ 7^2 \cdot 3^4 .$$

Ya que $\alpha^2 = 2$ y $-7 = (1 + 2\sqrt{2})(1 - 2\sqrt{2})$

$$N\gamma = -\alpha^6 \cdot (1 + 2\sqrt{2})^2 (1 - 2\sqrt{2})^2\ 3^4$$

$$= 3^2 \cdot (1 + 2\sqrt{2})^2 \alpha^3 [\,3^2 (1 + 2\sqrt{2})^2 (\alpha^3)]' = \gamma\gamma' .$$

Luego, la descomposición de $\gamma$ en factores primos de $\mathbb{Z}[\sqrt{2}]$ es

$$\gamma = 3^2\alpha^3(1 + 2\sqrt{2})^2 .$$

Sería interesante describir los elementos del anillo $\dfrac{\mathbb{Z}[\sqrt{2}]}{\gamma\ \mathbb{Z}[\sqrt{2}]}$ . Para ello sea $\{\gamma, \gamma\sqrt{2}\}$ una base entera del ideal $(\gamma)$ . Entonces

$$(\gamma) = (\gamma, \gamma\sqrt{2}) = (144 + 162\sqrt{2},\ 324 + 144\sqrt{2})$$

$$= (1764,\ -80 + 18\sqrt{2}) .$$

Así,

$$\frac{\mathbb{Z}[\sqrt{2}]}{\gamma\ \mathbb{Z}[\sqrt{2}]} = \{[\,a + b\sqrt{2}] \mid 0 \leq a < 1764\ ,\quad 0 \leq b < 18]\}$$

Observemos que las clases en $\dfrac{\mathbb{Z}[\sqrt{2}]}{\gamma\ \mathbb{Z}[\sqrt{2}]}$ son todas distintas y que cualquier entero de $\mathbb{Z}[\sqrt{2}]$ pertenece a una de esta clases. El número de ellas es $1764 \times 18 = 31752 = |N\gamma|$ . Ya que $\gamma = 3^2\alpha^3\pi^2$ , donde $3, \alpha$ y $\pi = 1 + 2\sqrt{2}$ son primos en $\mathbb{Z}[\sqrt{2}]$ , la estructura del anillo

$\dfrac{\mathbb{Z}[\sqrt{-2}]}{\gamma\ \mathbb{Z}[\sqrt{-2}]}$ está dada por

$$\frac{\mathbb{Z}[\sqrt{-2}]}{\gamma\ \mathbb{Z}[\sqrt{-2}]} \simeq \frac{\mathbb{Z}[\sqrt{-2}]}{3^2\ \mathbb{Z}[\sqrt{-2}]} \times \frac{\mathbb{Z}[\sqrt{-2}]}{\alpha^3\ \mathbb{Z}[\sqrt{-2}]} \times \frac{\mathbb{Z}[\sqrt{-2}]}{\pi^2\ \mathbb{Z}[\sqrt{-2}]} .$$

El orden del grupo de unidades de este anillo diferencia, módulo $\gamma$ es

$$\phi(\gamma) = \phi(3^2)\phi(\alpha^2)\phi(\pi^2) = 72 \cdot 4 \cdot 42 = 12096 .$$

Sin embargo, una información más importante de este grupo abeliano de 12096 elementos está dada por su estructura

$$\left(\frac{\mathbb{Z}[\sqrt{-2}]}{\gamma\ \mathbb{Z}[\sqrt{-2}]}\right)^* \simeq \left(\frac{\mathbb{Z}[\sqrt{-2}]}{3^2\ \mathbb{Z}[\sqrt{-2}]}\right)^* \times \left(\frac{\mathbb{Z}[\sqrt{-2}]}{\alpha^3\ \mathbb{Z}[\sqrt{-2}]}\right)^* \times \left(\frac{\mathbb{Z}[\sqrt{-2}]}{\pi^2\ \mathbb{Z}[\sqrt{-2}]}\right)^* .$$

9. Raíces Primitivas.

Definición: Sean $\rho$ y $\beta$ enteros relativamente primos en $\mathbb{Z}[\sqrt{2}]$. $\rho$ se llama una raíz primitiva módulo $\beta$ si $\rho^{\phi(\beta)} \equiv 1(\beta)$ y no se cumple $\rho^r \equiv 1(\beta)$ para $1 \leq r < \phi(\beta)$. Podemos reformular esta definición como sigue: Sea $[\rho]$ un elemento de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta\,\mathbb{Z}[\sqrt{2}]}\right)^*$. $\rho$ es una raíz primitiva módulo $\beta$ si el orden de $[\rho]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es el orden $\phi(\beta)$ del grupo $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta\,\mathbb{Z}[\sqrt{2}]}\right)^*$. Esto significa que $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es cíclico con generador $[\rho]$.

Ejemplo 9. Sea $\beta = 2$. Entonces $\left(\frac{\mathbb{Z}[\sqrt{2}]}{2\,\mathbb{Z}[\sqrt{2}]}\right)^* = \left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^2\,\mathbb{Z}[\sqrt{2}]}\right)^*$. Por el Teorema 5 tenemos que $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^2\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es un grupo cíclico de orden $\phi(\alpha^2) = 2$ con generador $[1 + \sqrt{2}]$. Existen por tanto raíces primitivas módulo 2. Ella es $1 + \sqrt{2}$. Sin embargo no hay raíces primitivas módulo 4 pues por el Teorema 5,

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{4\,\mathbb{Z}[\sqrt{2}]}\right)^* = \left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^4\,\mathbb{Z}[\sqrt{2}]}\right)^* \simeq C_2 \times C_4 .$$

y esto no es un grupo cíclico.

El Teorema 4 implica que $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es cíclico solo si $n = 1$. Hay por tanto raíces primitivas módulo $p$, para todo primo racional

$p \equiv \pm 3(8)$ . En particular 3 tiene raíces primitivas. Para calcular estas raíces primitivas recordemos que

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{3\,\mathbb{Z}[\sqrt{2}]}\right)^* = \{[1], [2], [\sqrt{2}], [1+\sqrt{2}], [2+\sqrt{2}], [2\sqrt{2}], [1+2\sqrt{2}], [2+2\sqrt{2}]\} \simeq C_8$$

Un generador de este grupo es $[1+\sqrt{2}]$ . Los otros generadores son $[1+\sqrt{2}]^3 = [1+2\sqrt{2}]$ ; $[1+\sqrt{2}]^5 = [2+2\sqrt{2}]$ y $[1+\sqrt{2}]^7 = [2+\sqrt{2}]$ . Así, las raíces primitivas (incongruentes) módulo 3 son $1+\sqrt{2}$ ; $1+2\sqrt{2}$ , $2+2\sqrt{2}$ y $2+\sqrt{2}$ . ¿Hay raíces primitivas módulo 6? Ya que $6 = 3\alpha^2$ , los Teoremas 4, 5 y el Teorema Chino de los Restos implican que

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{6\,\mathbb{Z}[\sqrt{2}]}\right)^* \simeq \left(\frac{\mathbb{Z}[\sqrt{2}]}{3\,\mathbb{Z}[\sqrt{2}]}\right)^* \times \left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^2\,\mathbb{Z}[\sqrt{2}]}\right)^* \simeq C_2 \times C_8$$

Sabemos que el producto de dos grupos cíclicos es cíclico sí y sólo si sus ordenes son relativamente primos. Ahora $\left(\frac{\mathbb{Z}[\sqrt{2}]}{3\,\mathbb{Z}[\sqrt{2}]}\right)^*$ y $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^2\,\mathbb{Z}[\sqrt{2}]}\right)^*$ son grupos cíclicos ambos de orden par. Luego $\left(\frac{\mathbb{Z}[\sqrt{2}]}{6\,\mathbb{Z}[\sqrt{2}]}\right)^*$ no es cíclico y 6 no tiene raíces primitivas.

Sea $\beta = 8 + 5\sqrt{2}$ . Entonces $\beta = \sqrt{2}(5+4\sqrt{2}) = \alpha\pi$ , donde $\alpha = \sqrt{2}$ y $\pi = 5+4\sqrt{2}$ , $\pi\pi' = -7 \equiv 1(8)$ son primos en $\mathbb{Z}[\sqrt{2}]$ . Hay raíces primitivas módulo $\beta$ pues

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta\,\mathbb{Z}[\sqrt{2}]}\right)^* \simeq \left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha\,\mathbb{Z}[\sqrt{2}]}\right)^* \times \left(\frac{\mathbb{Z}[\sqrt{2}]}{\pi\,\mathbb{Z}[\sqrt{2}]}\right)^* \simeq \left(\frac{\mathbb{Z}[\sqrt{2}]}{\pi\,\mathbb{Z}[\sqrt{2}]}\right)^* \simeq C_6$$

es un grupo cíclico de orden $\phi(\beta) = 6$ . Para calcular las raíces primitivas módulo $\beta$ sea $\{\beta, \beta\sqrt{2}\}$ una base entera del ideal $(\beta)$ . Entonces

$$(\beta) = (\beta, \beta\sqrt{2}) = (8 + 5\sqrt{2},\ 10 + 8\sqrt{2}) = (14,\ -4 + \sqrt{2})$$

y

$$\frac{\mathbb{Z}[\sqrt{2}]}{\beta\ \mathbb{Z}[\sqrt{2}]} = \{[a + b\sqrt{2}] \mid 0 \leq a < 14\ ,\ \ 0 \leq b < 1\}$$

$$= \{[0], [1], [2], \ldots\ldots [12], [13]\}$$

Las raíces primitivas módulo $\beta = 8 + 5\sqrt{2}$ se encuentran entre los representantes de las clases anteriores que son relativamente primos con $\beta$ y tales que $\rho^{\phi(\beta)} \equiv 1(\beta)$ , $\rho^{r} \not\equiv 1(\beta)$ para $1 \leq r < \phi(\beta)$ . Ahora, $[3]$ es un elemento del grupo $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta\ \mathbb{Z}[\sqrt{2}]}\right)^{*}$ pues 3 es primo en $\mathbb{Z}[\sqrt{2}]$ que no divide a $\beta = 8 + 5\sqrt{3}$ . Las potencias de 3 módulo $|N\beta| = 14$ son

$$3\ ,\ \ 3^2 \equiv 9\ ,\ \ 3^3 \equiv 13\ ,\ \ 3^4 \equiv 11\ ,\ \ 3^5 \equiv 5\ ,\ \ 3^6 \equiv 1$$

ya que $\beta$ divide a 14, $[3]$ tiene orden $\phi(\beta) = 6$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta\ \mathbb{Z}[\sqrt{2}]}\right)^{*}$ .

Así,

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta\ \mathbb{Z}[\sqrt{2}]}\right)^{*} = \langle [3] \rangle = \langle [5] \rangle\ ,\qquad [5] = [3^5]$$

$$= \{[1],\ [3],\ [5],\ [9],\ [11],\ [13]\}$$

y las raíces primitivas módulo $\beta = 8 + 5\sqrt{2}$ son 3 y 5 .

El Ejemplo 9 muestra que no todo entero en $\mathbb{Z}[\sqrt{2}]$ tiene raíces primitivas. El siguiente Teorema determina todos los enteros que las tienen:

Teorema 8. El entero $\beta$ tiene raíces primitivas sí y solo si $\beta = \alpha$, $\alpha^2$, $\alpha^3$, $p$, $\pi^n$, $\alpha p$ y $\alpha\pi^n$, $n \geq 1$.

Demostración: Si $\beta$ es uno cualquiera de los enteros anteriores, entonces por los Teoremas 3, 4, 5 y el Teorema Chino de los Restos en $\mathbb{Z}[\sqrt{2}]$ se tiene que $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es cíclico. Luego los enteros anteriores tienen raíces primitivas. Supongamos ahora que existen raíces primitivas módulo un entero $\beta$ de $\mathbb{Z}[\sqrt{2}]$. Sea

$$\beta = \alpha^a \prod_1^r p_i^{m_i} \prod_1^s \pi_j^{n_j}, \quad p_i \equiv \pm 3(8), \quad \pi_j\pi_j' = q_j \equiv \pm 1(8)$$

la factorización de $\beta$ en primos de $\mathbb{Z}[\sqrt{2}]$. Entonces

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta\,\mathbb{Z}[\sqrt{2}]}\right)^* \simeq \left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^a\,\mathbb{Z}[\sqrt{2}]}\right)^* \times \prod_1^r \left(\frac{\mathbb{Z}[\sqrt{2}]}{p_i^{m_i}\,\mathbb{Z}[\sqrt{2}]}\right)^* \times \prod_1^s \left(\frac{\mathbb{Z}[\sqrt{2}]}{\pi_j^{m_j}\,\mathbb{Z}[\sqrt{2}]}\right)^*$$

es cíclico. Se deduce que $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^a\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es cíclico y por el Teorema 5, $a \leq 3$. Se tiene también que los $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p_i^{m_i}\,\mathbb{Z}[\sqrt{2}]}\right)^*$ son cíclicos y por el Teorema 4, $m_i = 1$, $\forall\, i$. Se deduce $r = 1$, pues si $r \geq 2$, entonces $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p_1\,\mathbb{Z}[\sqrt{2}]}\right)^* \times \left(\frac{\mathbb{Z}[\sqrt{2}]}{p_2\,\mathbb{Z}[\sqrt{2}]}\right)^*$ es cíclico, ya que es un subgrupo del grupo cíclico $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta\,\mathbb{Z}[\sqrt{2}]}\right)^*$. Luego sus ordenes son relativamente primos. Pero $\phi(p_1) = p_1^2 - 1$, $\phi(p_2) = p_2^2 - 1$ son ambos pares y el máximo común

divisor de sus ordenes es divisible por 2. Contradicción. Luego $r = 1$ .

Por el Teorema 3, los $\left(\frac{\mathbb{Z}[\sqrt{-2}]}{\pi_j^{n_j}\,\mathbb{Z}[\sqrt{-2}]}\right)^* \simeq \left(\frac{\mathbb{Z}}{q_j^{n_j}\,\mathbb{Z}}\right)^*$ son cíclicos. Se demues-

tra, como en el caso anterior, que $s = 1$ . Hasta aquí hemos probado que

$\beta$ tiene raíces primitivas sólo si $\beta = \alpha^a\, p\, \Pi^n$ , $a \leq 3$ , ya que

$\left(\frac{\mathbb{Z}[\sqrt{-2}]}{\alpha^a p\,\mathbb{Z}[\sqrt{-2}]}\right)^* \simeq \left(\frac{\mathbb{Z}[\sqrt{-2}]}{\alpha^a\,\mathbb{Z}[\sqrt{-2}]}\right)^* \times \left(\frac{\mathbb{Z}[\sqrt{-2}]}{p\,\mathbb{Z}[\sqrt{-2}]}\right)^*$ es cíclico sólo si $a = 1$

y

$$\left(\frac{\mathbb{Z}[\sqrt{-2}]}{\alpha^a\,\Pi^n\,\mathbb{Z}[\sqrt{-2}]}\right)^* \simeq \left(\frac{\mathbb{Z}[\sqrt{-2}]}{\alpha^a\,\mathbb{Z}[\sqrt{-2}]}\right)^* \times \left(\frac{\mathbb{Z}[\sqrt{-2}]}{\pi^n\,\mathbb{Z}[\sqrt{-2}]}\right)^*$$

es cíclico sólo si $a = 1$ , se concluye que $\beta$ tiene racíces primitivas

sólo si $\beta = \alpha$ , $\alpha^2$ , $\alpha^3$ , $p$ , $\pi^n$ , $\alpha p$ y $\alpha\pi^n$ .

## REFERENCIAS


[1] Hancock, H., Foundations of the Theory of Algebraic Numbers. New York, Dover Publications, Inc. (1964), Cap. IX

[2] Hecke, E., Lectures on the Theory of Algebraic Numbers. New York, Springer Verlag GTM (1977), Cap. V. Sección 24

[3] Hardy, Wright., An Introduction to the Theory of Numbers. Oxford at the Claredon Press (1954), Cap. XIV-XV

[4] Cross, J., The Euler $\varphi$ function in the Gaussian Integers. American Mathematical Monthly Vol. 8, N° 8 (1983), pág. 518-528

[5] Baeza, R., Notas del Curso Teoría de Números, 2° Semestre (1983) Facultad de Ciencias, Universidad de Chile

[6] Ireland-Rosen., A classical Introduction to Modern Number Theory. Springer Verlag, N. York (1982), pág. 42, 43.