Capítulo 4

Números Racionales.

Luego de construir los Números Naturales, se presentaron ciertos problemas como ¿Cuál es el resultado de 3 menos 5?, para poder encontrar una solución se creó a partir de $\mathbb{N}$ el conjunto de los Números Enteros que se representan con el símbolo de $\mathbb{Z}$. Pero la vida cotidiana siguió exigiendo la creación de nuevos conjuntos a partir de los ya conocidos.

Consideremos el conjunto $\mathbb{Z}$ como conjunto base y definamos

$$\mathbb{Z}^* := \mathbb{Z} - \{0\}$$

a partir de este nuevo conjunto construimos el producto cartesiano

$$\mathbb{Z} \times \mathbb{Z}^* = \{(a, b) \mid a \in \mathbb{Z} \ \wedge \ b \in \mathbb{Z}^*\}$$

de donde $\mathbb{Z} \times \mathbb{Z}^*$ se denominan fracciones
Notación: Sea $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ una mejor notación para los elementos de este nuevo conjunto es

$$(a, b) = \frac{a}{b}$$

Más aún el elemento a se denominará como numerador y b el denominador.

Definición 39 *Sean $\frac{a}{b}$ y $\frac{c}{d} \in \mathbb{Z} \times \mathbb{Z}^*$, definiremos la siguiente relación dada por*

$$\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad = bc$$

Propiedad 129 *La relación definida anteriormente $\sim$, es una relación de equivalencia.*

Demostración:

(i) **La relación $\sim$ es refleja:**
Sean $\frac{a}{b} \in \mathbb{Z} \times \mathbb{Z}^*$
Como

$$ab = ab$$

entonces

$$\frac{a}{b} \sim \frac{a}{b}$$

luego la relación es refleja.

(ii) **La relación $\sim$ es simétrica:**

Sean $\frac{a}{b}, \frac{c}{d} \in \mathbb{Z} \times \mathbb{Z}^*$ tales que

$$\begin{aligned} \frac{a}{b} \sim \frac{c}{d} &\Leftrightarrow \\ &\Leftrightarrow \quad cb = ad \\ &\Leftrightarrow \quad \frac{c}{d} \sim \frac{a}{b}. \end{aligned}$$

(iii) **La relación $\sim$ es transitiva:**

Sean $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Z} \times \mathbb{Z}^*$ tales que

$$\frac{a}{b} \sim \frac{c}{d} \ \wedge \ \frac{c}{d} \sim \frac{e}{f}$$

Si

$$\begin{aligned} \frac{a}{b} \sim \frac{c}{d} \ \wedge \ \frac{c}{d} \sim \frac{e}{f} \ \Leftrightarrow \ & ad = cb \ \wedge \ cf = ed \\ & adf = cbf \ \wedge \ cfb = edb. \end{aligned}$$

Por lo tanto $adf = edb$, cancelando obtenemos $af = eb$, luego

$$\frac{a}{b} \sim \frac{e}{f}.$$

Observación: La relación de equivalencia definida anteriormente particiona el conjunto $\mathbb{Z} \times \mathbb{Z}^*$ en las clases de equivalencia, que se denotan por

$$\mathbb{Z} \times \mathbb{Z}^*/_\sim := \text{ conjunto cuociente}$$

Definición 40 *Dado $\mathbb{Z} \times \mathbb{Z}^*$, se define el conjunto cuociente*

$$\mathbb{Z} \times \mathbb{Z}^*/_\sim := \left\{ \left[\frac{a}{b}\right] \mid \frac{a}{b} \in \mathbb{Z} \times \mathbb{Z}^* \right\}$$

donde

$$\left[\frac{a}{b}\right] := \left\{ \frac{c}{d} \in \mathbb{Z} \times \mathbb{Z}^* \mid \frac{c}{d} \sim \frac{a}{b} \right\}.$$

Notación: Para una mayor comodidad, denotamos

$$\mathbb{Z} \times \mathbb{Z}^*/_\sim = \mathbb{Q}$$

y $\mathbb{Q}$ se llama el conjunto de los números racionales.

4.1. Suma y Producto en $\mathbb{Q}$

Propiedad 130 *Sean* $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{c_1}{d_1}, \frac{c_2}{d_2} \in \mathbb{Z} \times \mathbb{Z}^*$, *tales que* $\frac{a_1}{b_1} \sim \frac{a_2}{b_2}$ *y* $\frac{c_1}{d_1} \sim \frac{c_2}{d_2}$ *entonces*

$$\frac{a_1 d_1 + c_1 b_1}{b_1 d_1} \sim \frac{a_2 d_2 + c_2 b_2}{b_2 d_2} \qquad y \qquad \frac{a_1 c_1}{b_1 d_1} \sim \frac{a_2 c_2}{b_2 d_2}$$

Demostración: Sean $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{c_1}{d_1}, \frac{c_2}{d_2} \in \mathbb{Z} \times \mathbb{Z}^*$, tales que

$$\frac{a_1}{b_1} \sim \frac{a_2}{b_2} \qquad \text{y} \qquad \frac{c_1}{d_1} \sim \frac{c_2}{d_2}$$

Luego se tiene que

$$a_1 b_2 = a_2 b_1 \qquad \text{y} \qquad c_1 d_2 = c_2 d_1$$

Ahora formaremos la Suma:

$$\begin{aligned}
(a_1 d_1 + c_1 b_1) b_2 d_2 &= a_1 d_1 b_2 d_2 + c_1 b_1 b_2 d_2 \\
&= (a_1 b_2) d_1 d_2 + (c_1 d_2) b_1 b_2 \\
&= (a_2 b_1) d_1 d_2 + (c_2 d_1) b_1 b_2 \\
&= (a_2 d_2 (b_1 d_1) + c_2 b_2 (d_1 b_1) \\
&= (a_2 d_2 + c_2 b_2) d_1 b_1
\end{aligned}$$

Por lo tanto

$$(a_1 d_1 + c_1 b_1) b_2 d_2 = (a_2 d_2 + c_2 b_2) d_1 b_1$$

de lo cual obtenemos que

$$\frac{a_1 d_1 + c_1 b_1}{b_1 d_1} \sim \frac{a_2 d_2 + c_2 b_2}{b_2 d_2}$$

Ahora veremos la multiplicación

$$\begin{aligned}
(a_1 c_1)(b_2 d_2) &= (a_1 b_2)(c_1 d_2) \\
&= (a_2 b_1)(c_2 d_1) \\
&= a_2 c_2 b_1 d_1.
\end{aligned}$$

De esta manera tenemos que

$$(a_1 c_1)(b_2 d_2) = a_2 c_2 b_1 d_1.$$

es decir,

$$\frac{a_1 c_1}{b_1 d_1} \sim \frac{a_2 c_2}{b_2 d_2}$$

□

El teorema nos permite definir la suma y el producto

Definición 41 *Sean* $\left[\frac{a}{b}\right]$ *y* $\left[\frac{c}{d}\right] \in \mathbb{Q}$
Adición en $\mathbb{Q}$**:** *Se define la adición en* $\mathbb{Q}$ *por*

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] := \left[\frac{ad+bc}{bd}\right].$$

Producto $\mathbb{Q}$**:** *Se define la multiplicación en* $\mathbb{Q}$ *por:*

$$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] := \left[\frac{ac}{bd}\right].$$

4.1.1. Suma de Números Racionales

Propiedad 131 *Los números racionales con la suma forman un grupo abeliano*

$$(\mathbb{Q}, +) \quad \textit{es un grupo abeliano.}$$

Demostración: Sean $\left[\frac{a_1}{b_1}\right], \left[\frac{a_2}{b_2}\right], \left[\frac{a_3}{b_3}\right] \in \mathbb{Q}$.
Asociativa:

$$\left[\frac{a_1}{b_1}\right] + \left(\left[\frac{a_2}{b_2}\right] + \left[\frac{a_3}{b_3}\right]\right) = \left(\left[\frac{a_1}{b_1}\right] + \left[\frac{a_2}{b_2}\right]\right) + \left[\frac{a_3}{b_3}\right].$$

Para ellos

$$\begin{aligned}
\left[\frac{a_1}{b_1}\right] + \left(\left[\frac{a_2}{b_2}\right] + \left[\frac{a_3}{b_3}\right]\right) &= \left[\frac{a_1}{b_1}\right] + \left(\left[\frac{a_2b_3 + a_3b_2}{b_2b_3}\right]\right) \\
&= \left[\frac{a_1}{b_1}\right] + \left[\frac{a_2b_3 + a_3b_2}{b_2b_3}\right] \\
&= \left[\frac{a_1b_2b_3 + a_2b_1b_3 + a_3b_1b_2}{b_1b_2b_3}\right] \\
&= \left[\frac{(a_1b_2 + a_2b_1)b_3 + a_3b_1b_2}{b_1b_2b_3}\right] \\
&= \left[\frac{a_1b_2 + a_2b_1}{b_1b_2}\right] + \left[\frac{a_3}{b_3}\right] \\
&= \left(\left[\frac{a_1b_2 + a_2b_1}{b_1b_2}\right]\right) + \left[\frac{a_3}{b_3}\right] \\
&= \left(\left[\frac{a_1}{b_1}\right] + \left[\frac{a_2}{b_2}\right]\right) + \left[\frac{a_3}{b_3}\right]
\end{aligned}$$

Por lo tanto la operación suma es asociativa.
Neutro Aditivo: Sean $\left[\frac{0}{1}\right] \in \mathbb{Q}$ y cumple con

$$\left[\frac{a_1}{b_1}\right] + \left[\frac{0}{1}\right] = \left[\frac{a_1}{b_1}\right]$$

Lo cual se comprueba del siguiente modo

$$\begin{aligned}\left[\frac{a_1}{b_1}\right]+\left[\frac{0}{1}\right] &= \left[\frac{a_1 1+0b_1}{b_1 1}\right]\\ &= \left[\frac{a_1}{b_1}\right]\end{aligned}$$

luego tenemos que el neutro aditivo existe y es

$$\left[\frac{0}{b}\right]=\left[\frac{0}{1}\right] \quad \text{con } b\in\mathbb{Z}^*$$

Inverso Aditivo: Dado $\left[\frac{a_1}{b_1}\right]$ existe $\left[\frac{-a_1}{b_1}\right]\in\mathbb{Q}$ tal que

$$\left[\frac{a_1}{b_1}\right]+\left[\frac{-a_1}{b_1}\right]=\left[\frac{0}{1}\right]$$

Justifiquemos lo anterior

$$\begin{aligned}\left[\frac{a_1}{b_1}\right]+\left[\frac{-a_1}{b_1}\right] &= \left[\frac{a_1b_1+(-a_1)b_1}{b_1b_1}\right]\\ &= \left[\frac{0}{b_1b_1}\right]=\left[\frac{0}{1}\right]\end{aligned}$$

Lo anterior demuestra que existe el inverso aditivo, de esta manera tenemos que el inverso aditivo de $\left[\frac{a_1}{b_1}\right]$ es $\left[\frac{-a_1}{b_1}\right]$

Conmutatividad: Debemos probar que

$$\left[\frac{a_1}{b_1}\right]+\left[\frac{a_2}{b_2}\right]=\left[\frac{a_2}{b_2}\right]+\left[\frac{a_1}{b_1}\right]$$

Para ello

$$\begin{aligned}\left[\frac{a_1}{b_1}\right]+\left[\frac{a_2}{b_2}\right] &= \left[\frac{a_2b_1+a_1b_2}{b_2b_1}\right]\\ &= \left[\frac{a_2}{b_2}\right]+\left[\frac{a_1}{b_1}\right].\end{aligned}$$

Luego la suma es conmutativa.

Notación: Sean $\left[\frac{a}{b}\right]$ y $\left[\frac{c}{d}\right]\in\mathbb{Q}$, entonces

$$\left[\frac{a}{b}\right]-\left[\frac{c}{d}\right]=\left[\frac{a}{b}\right]+\left[\frac{-c}{d}\right]$$

4.1.2. Multiplicación de Números Racionales

Propiedad 132 *Los números racionales con las propiedades de la multiplicación forman un grupo abeliano.*

$$(\mathbb{Q}^*, \cdot) \quad \textit{es un grupo abeliano,}$$

donde $\mathbb{Q}^* = \mathbb{Q} - \{0\}$.

Demostración: Sean $\left[\frac{a_1}{b_1}\right], \left[\frac{a_2}{b_2}\right], \left[\frac{a_3}{b_3}\right] \in \mathbb{Q}$

Asociativa:

$$\left[\frac{a_1}{b_1}\right] \cdot \left(\left[\frac{a_2}{b_2}\right] \cdot \left[\frac{a_3}{b_3}\right]\right) = \left(\left[\frac{a_1}{b_1}\right] \cdot \left[\frac{a_2}{b_2}\right]\right) \cdot \left[\frac{a_3}{b_3}\right].$$

Para ellos

$$\begin{aligned}
\left[\frac{a_1}{b_1}\right] \cdot \left(\left[\frac{a_2}{b_2}\right] \cdot \left[\frac{a_3}{b_3}\right]\right) &= \left[\frac{a_1}{b_1}\right] \cdot \left(\left[\frac{a_2 a_3}{b_2 b_3}\right]\right) \\
&= \left[\frac{a_1}{b_1}\right] \cdot \left[\frac{a_2 a_3}{b_2 b_3}\right] \\
&= \left[\frac{a_1 a_2 a_3}{b_1 b_2 b_3}\right] \\
&= \left[\frac{a_1 a_2}{b_1 b_2}\right] \cdot \left[\frac{a_3}{b_3}\right] \\
&= \left(\left[\frac{a_1 a_2}{b_1 b_2}\right]\right) \cdot \left[\frac{a_3}{b_3}\right] \\
&= \left(\left[\frac{a_1}{b_1}\right] \cdot \left[\frac{a_2}{b_2}\right]\right) \cdot \left[\frac{a_3}{b_3}\right]
\end{aligned}$$

Luego la multiplicación es asociativa.

Neutro multiplicativo: Existe $\left[\frac{1}{1}\right] \in \mathbb{Q}$ que cumple

$$\left[\frac{a_1}{b_1}\right] \cdot \left[\frac{1}{1}\right] = \left[\frac{a_1}{b_1}\right]$$

Lo cual se comprueba del siguiente modo

$$\begin{aligned}
\left[\frac{a_1}{b_1}\right] \cdot \left[\frac{1}{1}\right] &= \left[\frac{a_1 1}{b_1 1}\right] \\
&= \left[\frac{a_1}{b_1}\right]
\end{aligned}$$

luego tenemos que el neutro aditivo existe y es

$$\left[\frac{a}{a}\right] = \left[\frac{1}{1}\right] \quad \text{con } a \in \mathbb{Z}^*$$

Inverso multiplicativo: Sean $\left[\frac{a_1}{b_1}\right] \in \mathbb{Q}^*$ luego existe $\left[\frac{b_1}{a_1}\right] \in \mathbb{Q}^*$ que cumple

$$\left[\frac{a_1}{b_1}\right] \cdot \left[\frac{b_1}{a_1}\right] = \left[\frac{1}{1}\right]$$

Justifiquemos lo anterior

$$\begin{aligned} \left[\frac{a_1}{b_1}\right] \cdot \left[\frac{b_1}{a_1}\right] &= \left[\frac{a_1 b_1}{a_1 b_1}\right] \\ &= \left[\frac{1}{1}\right] \end{aligned}$$

Lo anterior demuestra que existe el inverso multiplicativo, de esta manera tenemos que el inverso de $\left[\frac{a_1}{b_1}\right]$ es $\left[\frac{b_1}{a_1}\right]$
Conmutatividad: Debemos probar que

$$\left[\frac{a_1}{b_1}\right] \cdot \left[\frac{a_2}{b_2}\right] = \left[\frac{a_2}{b_2}\right] \cdot \left[\frac{a_1}{b_1}\right]$$

Para ello

$$\begin{aligned} \left[\frac{a_1}{b_1}\right] \cdot \left[\frac{a_2}{b_2}\right] &= \left[\frac{a_1 a_2}{b_1 b_2}\right] \\ &= \left[\frac{a_2 a_1}{b_2 b_1}\right] \\ &= \left[\frac{a_2}{b_2}\right] \cdot \left[\frac{a_1}{b_1}\right]. \end{aligned}$$

Luego el producto es conmutativo □
Notación: Sean $\left[\frac{a}{b}\right]$ y $\left[\frac{c}{d}\right] \in \mathbb{Q}^*$, entonces

$$\left[\frac{a}{b}\right] : \left[\frac{c}{d}\right] = \left[\frac{a}{b}\right] \cdot \left[\frac{d}{c}\right].$$

Teorema 133 *El conjunto de los números racionales, con la suma y producto definidos anteriores* $(\mathbb{Q}, +, \cdot)$*, es un cuerpo.*

Demostración: Se ha demostrado anteriormente que $(\mathbb{Q}, +)$ y $(\mathbb{Q}^*, \cdot)$ son grupos abelianos, luego falta ver la distributividad
Distributividad: Sean $\left[\frac{a_1}{b_1}\right], \left[\frac{a_2}{b_2}\right], \left[\frac{a_3}{b_3}\right] \in \mathbb{Q}$, entonces se cumple

$$\left[\frac{a_1}{b_1}\right] \cdot \left(\left[\frac{a_2}{b_2}\right] + \left[\frac{a_3}{b_3}\right]\right) = \left(\left[\frac{a_1}{b_1}\right] \cdot \left[\frac{a_2}{b_2}\right]\right) + \left(\left[\frac{a_1}{b_1}\right] \cdot \left[\frac{a_3}{b_3}\right]\right)$$

Veamos

$$\begin{aligned}
\left[\frac{a_1}{b_1}\right]\cdot\left(\left[\frac{a_2}{b_2}\right]+\left[\frac{a_3}{b_3}\right]\right) &= \left[\frac{a_1}{b_1}\right]\cdot\left(\left[\frac{a_2b_3+a_3b_2}{b_2b_3}\right]\right)\\
&= \left[\frac{a_1}{b_1}\right]\cdot\left[\frac{a_2b_3+a_3b_2}{b_2b_3}\right]\\
&= \left[\frac{a_1a_2b_3+a_1a_3b_2}{b_1b_2b_3}\right]\\
&= \left[\frac{a_1a_2}{b_1b_2}\right]+\left(\left[\frac{a_1a_3}{b_1b_3}\right]\right)\\
&= \left(\left[\frac{a_1}{b_1}\right]\cdot\left[\frac{a_2}{b_2}\right]\right)+\left(\left[\frac{a_1}{b_1}\right]\cdot\left[\frac{a_3}{b_3}\right]\right)
\end{aligned}$$

Observación: Luego de haber definido el conjunto de los números racionales o $\mathbb{Q}$, el no contiene todos los números que necesitamos por ejemplo la ecuación $x^2 = 5$ no tiene solución en $\mathbb{Q}$, es decir, el número que en forma habitual se denotado por $\sqrt{5} \notin \mathbb{Q}$.

Propiedad 134 *Sea $p \in \mathbb{Z}$ un número primo entonces el número $\sqrt{p} \notin \mathbb{Q}$.*

Demostración: Para este caso la demostración la realizaremos por el método del absurdo que consiste en suponer como cierto la negación de la proposición como sigue:

Supongamos que la ecuación $x^2 = \left[\frac{p}{1}\right]$ tiene solución en $\mathbb{Q}$, entonces la solución se puede representar como una fracción

$$\begin{aligned}
\left[\frac{p}{1}\right] &= \left(\left[\frac{a}{b}\right]\right)^2 \quad \text{donde} \quad (a,b)=1\\
\text{Luego, } \frac{p}{1} &\sim \frac{a^2}{b^2}\\
pb^2 &= a^2
\end{aligned}$$

Luego $p|a^2$, es decir $p|a$. Por lo tanto $a = pk$ con $k \in \mathbb{Z}$ reemplazando

$$\begin{aligned}
pb^2 &= p^2k^2\\
b^2 &= pk^2
\end{aligned}$$

Por la justificación similar a la anterior $p|b^2$ es decir $p|b$, lo cual es una contradicción ya que $(a,b) = 1$. Por lo tanto

$$\sqrt{p} \notin \mathbb{Q}$$

□

Notación: A cada número racional

$$\left[\frac{a}{b}\right] = \left\{\frac{x}{y} \;\middle|\; \frac{x}{y} \sim \frac{a}{b}\right\}$$

lo denotaremos simplemente $\frac{a}{b}$.

Debemos tener claridad en la diferencia entre fracción y número racional ya que en este caso nos refiriendo a la clase.

Por ejemplo las fracciones $\frac{5}{15}$, $\frac{1}{3}$ no son iguales, pero como números racional si son iguales las clases, ya que $\frac{5}{15} \sim \frac{1}{3}$.

4.1.3. Expresión decimal en $\mathbb{Q}$.

Dado un número racional $\frac{a}{b}$, luego aplicamos el algoritmo de la división y obtenemos

$$a = bq + r, \quad \text{con } 0 \leq r < b$$

si volvemos aplicar el algoritmo de la división obtenemos

$$\begin{aligned} 10 \cdot r &= bq_1 + r_1, \quad \text{con } 0 \leq r_1 < b \\ 10 \cdot r_1 &= bq_2 + r_2, \quad \text{con } 0 \leq r_2 < b \\ &\vdots \\ 10 \cdot r_t &= bq_{t+1} + r_{t+1}, \quad \text{con } 0 \leq r_{t+1} < b \end{aligned}$$

como los posibles resto r_i son finito, luego en algún momento es 0 o se repite, de lo cual obtenemos que los números racionales se representan por números decimales finito o los números decimales infinitos periódicos, es decir,

$$\frac{a}{b} = q_1, q_2 q_3 \ldots q_t \text{ o bien } \frac{a}{b} = \frac{a}{b} = q_1, q_2 q_3 \ldots \overline{q_s \ldots q_t}$$

Ejemplo de ello tenemos

$$\frac{1}{4} = 0,25 \quad \frac{1}{3} = 0,\overline{3}$$

Existe otros números que no pertenecen a $\mathbb{Q}$, estos son los llamados números decimales infinitos no periódico o irracionales $\mathbb{I}$, ya que no se puede encontrar una representación en números racionales.

Los Números Reales

Con los conjuntos de los números racionales e irracionales que denotamos como $\mathbb{Q}$ e $\mathbb{I}$ respectivamente, podemos construir un nuevo conjunto que se puede crear a partir de estos dos. Estos nuevos elementos los llamaremos números reales y algunos elementos que pertenecen a este conjunto son

$$\pi;\ \sqrt{3};\ 0,1;\ 5,\overline{6}; \cdots$$

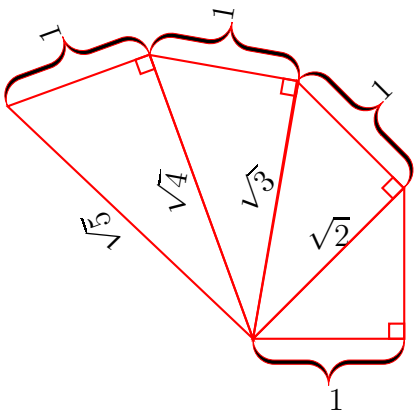
En este conjunto existe un producto y una suma compatible con de $\mathbb{Q}$, que entrega la siguiente propiedad

Teorema 135 $(\mathbb{R}, +, \cdot)$ *es un cuerpo.*

4.2. Extensiones Cuadráticas de los Racionales $\mathbb{Q}[\sqrt{p}]$.

Como justificamos anteriormente los números $\sqrt{2}, \sqrt{3}, \cdots \notin \mathbb{Q}$, pero si a $\mathbb{Q}$ le agregamos estos números lo que tenemos como resultado son cuerpos intermedios llamados extensiones cuadráticas debido a que vienen dados por raíces cuadráticas.

Observación: De los números anterior existe algunos de ellos que pueden ser representados por el llamado espiral pitagórica, que se inicia con un triángulo isosceles, con lados de longitud 1, y el siguiente triángulo rectángulo de altura 1 y base la hipotenusa del anterior, como en la figura.



Definición 42 *Sea $p \in \mathbb{Z}$, tal que $\sqrt{p} \notin \mathbb{Q}$*

Se define $\mathbb{Q}[\sqrt{p}]$ por

$$\mathbb{Q}[\sqrt{p}] := \{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\}$$

Observación: Notemos que dado un número $x \in \mathbb{Q}[\sqrt{p}]$, existe únicos elementos $a, b \in \mathbb{Q}$, tal que $x = a + b\sqrt{p}$.

Si suponemos que existe dos expresiones distintas $a + b\sqrt{p} = c + d\sqrt{p}$, obtenemos una contradicción con que $\sqrt{p} \notin \mathbb{Q}$. Esta observación nos permite definir las siguientes operaciones binarias.

4.2.1. Suma y Producto en $\mathbb{Q}[\sqrt{p}]$.

Sean $a_1 + b_1\sqrt{p}, a_2 + b_2\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$. Se define las siguientes operaciones:

Suma:

$$(a_1 + b_1\sqrt{p}) + (a_2 + b_2\sqrt{p}) := (a_1 + a_2) + (b_1 + b_2)\sqrt{p}$$

Producto:

$$(a_1 + b_1\sqrt{p}) \cdot (a_2 + b_2\sqrt{p}) := (a_1a_2 + pb_1b_2) + (a_1b_2 + a_2b_1)\sqrt{p}$$

Propiedades de la Suma en $\mathbb{Q}[\sqrt{p}]$.

Propiedad 136 *La extensión cuadrática con la operación suma es un grupo abeliano, es decir,*

$$(\mathbb{Q}[\sqrt{p}],+) \quad \textit{es un grupo abeliano}$$

Demostración: Recuerde que $(\mathbb{Q},+)$ es un grupo abeliano.

Sean $a_1+b_1\sqrt{p},\ a_2+b_2\sqrt{p},\ a_3+b_3\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$

Asociativa:

$$(a_1+b_1\sqrt{p})+[(a_2+b_2\sqrt{p})+(a_3+b_3\sqrt{p})] = [(a_1+b_1\sqrt{p})+(a_2+b_2\sqrt{p})]+(a_3+b_3\sqrt{p})$$

Para ello,

$$\begin{aligned}(a_1+b_1\sqrt{p})+[(a_2+b_2\sqrt{p})+(a_3+b_3\sqrt{p})] &= (a_1+b_1\sqrt{p})+[(a_2+a_3)+(b_2+b_3)\sqrt{p}] \\ &= (a_1+a_2+a_3)+(b_1+b_2+b_3)\sqrt{p} \\ &= [(a_1+a_2)+(b_1+b_2)\sqrt{p}]+(a_3+b_3\sqrt{p}). \\ &= [(a_1+b_2)\sqrt{p})+(a_2+b_2\sqrt{p})]+(a_3+b_3\sqrt{p}).\end{aligned}$$

Por lo tanto, la operación suma es asociativa

Neutro Aditivo: Existe $0+0\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$

Que cumple con:

$$\begin{aligned}(a_1+b_1\sqrt{p})+(0+0\sqrt{p}) &= (a_1+0)+(b_1+0)\sqrt{p} \\ &= a_1+b_1\sqrt{p}\end{aligned}$$

luego el neutro aditivo existe y es $0=0+0\sqrt{p}$.

Inverso Aditivo: Sea $a_1+b_1\sqrt{p}$, existe $(-a_1)+(-b_1)\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$ que cumple con

$$(a_1+b_1\sqrt{p})+((-a_1)+(-b_1)\sqrt{p}) = 0+0\sqrt{p}$$

Comprobemos lo anterior

$$\begin{aligned}(a_1+b_1\sqrt{p})+((-a_1)+(-b_1)\sqrt{p}) &= (a_1+(-a_1))+(b_1+(-b_1))\sqrt{p} \\ &= 0+0\sqrt{p}\end{aligned}$$

Lo anterior demuestra que existe el inverso aditivo de $a_1+b_1\sqrt{p}$ es $(-a_1)+(-b_1)\sqrt{p}$.

Conmutatividad: Debemos probar

$$(a_1+b_1\sqrt{p})+(a_2+b_2\sqrt{p}) = (a_2+b_2\sqrt{p})+(a_1+b_1\sqrt{p})$$

Para ello

$$\begin{aligned}(a_1+b_1\sqrt{p})+(a_2+b_2\sqrt{p}) &= (a_1+a_2)+(b_1+b_2)\sqrt{p} \\ &= (a_2+a_1)+(b_2+b_1)\sqrt{p} \\ &= (a_2+b_2\sqrt{p})+(a_1+b_1\sqrt{p}).\end{aligned}$$

□

Propiedad del Producto en $\mathbb{Q}[\sqrt{p}]$.

Propiedad 137 *El conjunto $\mathbb{Q}[\sqrt{p}]$ con la multiplicación forman un grupo abeliano*

$$(\mathbb{Q}^*[\sqrt{p}],\cdot) \quad \textit{es un grupo abeliano}$$

donde $\mathbb{Q}^*[\sqrt{p}]$ es $\mathbb{Q}[\sqrt{p}]-\{0\}$.

Demostración: Sean $a_1+b_1\sqrt{p},\ a_2+b_2\sqrt{p},\ a_3+b_3\sqrt{p}\in\mathbb{Q}[\sqrt{p}]$
Asociativa:

$$(a_1+b_1\sqrt{p})\cdot[(a_2+b_2\sqrt{p})\cdot(a_3+b_3\sqrt{p})]=[(a_1+b_1\sqrt{p})\cdot(a_2+b_2\sqrt{p})]\cdot(a_3+b_3\sqrt{p})$$

Para ello

$$\begin{aligned}
& (a_1+b_1\sqrt{p})\cdot[(a_2+b_2\sqrt{p})\cdot(a_3+b_3\sqrt{p})]\\
= \ & (a_1+b_1\sqrt{p})\cdot[(a_2a_3+pb_2b_3)+(a_3b_2+a_2b_3)\sqrt{p}]\\
= \ & [a_1(a_2a_3+pb_2b_3)+pb_1(a_3b_2+a_2b_3)]+[a_1(a_3b_2+a_2b_3)+(a_2a_3+pb_2b_3)b_1]\sqrt{p}\\
= \ & (a_1a_2a_3+a_1pb_2b_3+a_3b_2b_1p+a_2b_3b_1p)+(a_1a_3b_2+a_1a_2b_3+a_2a_3b_1+pb_1b_2b_3)\sqrt{p}\\
= \ & [(a_1a_2+b_2b_1p)a_3+(a_1b_2+a_2b_1)b_3p]+[(a_1a_2+pb_1b_2)b_3+a_3(a_1b_2+a_2b_1)]\sqrt{p}\\
= \ & [(a_1a_2+b_2b_1p)+(a_1b_2+a_2b_1)\sqrt{p}](a_3+b_3\sqrt{p})\\
= \ & [(a_1+b_1\sqrt{p})\cdot(a_2+b_2\sqrt{p})]\cdot(a_3+b_3\sqrt{p})
\end{aligned}$$

Por lo tanto el producto es asociativo.
Neutro Multiplicativo: Existe $1+0\sqrt{p}\in\mathbb{Q}[\sqrt{p}]$, tal que

$$(a_1+b_1\sqrt{p})\cdot(1+0\sqrt{p})=a_1+b_1\sqrt{p}$$

Lo cual se comprueba del siguiente modo

$$\begin{aligned}
(a_1+b_1\sqrt{p})\cdot(1+0\sqrt{p}) &= (a_11+p0b_1)+(a_10+1b_1)\sqrt{p}\\
&= a_1+b_1\sqrt{p}
\end{aligned}$$

luego tenemos que el neutro multiplicativo existe y es

$$1=1+0\sqrt{p}.$$

Inverso Multiplicativo: Sean $a+b\sqrt{p}\in\mathbb{Q}^*[\sqrt{p}]$, en primer lugar notemos que $a^2-b^2p\neq 0$, propiedad 134, luego existe $\frac{a}{a^2-b^2p}+\frac{-b}{a^2-b^2p}\sqrt{p}\in\mathbb{Q}^*[\sqrt{p}]$ que cumple con

$$(a+b\sqrt{p})\cdot(\frac{a}{a^2-b^2p}+\frac{-b}{a^2-b^2p}\sqrt{p})=1+0\sqrt{p}$$

La prueba de lo anterior esta dada por

$$\begin{aligned}
& (a+b\sqrt{p})\cdot(\frac{a}{a^2-b^2p}+\frac{-b}{a^2-b^2p}\sqrt{p}) \\
= & \left(a\frac{a}{a^2-b^2p}+pb\frac{-b}{a^2-b^2p}\right)+\left(a\frac{-b}{a^2-b^2p}+\frac{a}{a^2-b^2p}b\right)\sqrt{p} \\
= & \frac{a^2-b^2p}{a^2-b^2p}+\frac{-ba+ba}{a^2-b^2p}\sqrt{p} \\
= & 1+0\sqrt{p}
\end{aligned}$$

Por lo tanto el inverso multiplicativo de $a+b\sqrt{p}$ es

$$\frac{a}{a^2-pb^2}+\frac{-b}{a^2-pb^2}\sqrt{p}.$$

Conmutatividad: Debemos probar

$$(a_1+b_1\sqrt{p})\cdot(a_2+b_2\sqrt{p})=(a_2+b_2\sqrt{p})\cdot(a_1+b_1\sqrt{p})$$

Para ello

$$\begin{aligned}
(a_1+b_1\sqrt{p})\cdot(a_2+b_2\sqrt{p}) &= (a_1a_2+pb_1b_2)+(a_1b_2+a_2b_1)\sqrt{p} \\
&= (a_2a_1+pb_2b_1)+(a_2b_1+a_1b_2)\sqrt{p} \\
&= (a_2+b_2\sqrt{p})\cdot(a_1+b_1\sqrt{p}).
\end{aligned}$$

Por lo tanto la multiplicación en $\mathbb{Q}[\sqrt{p}]$ es conmutativa. □

Notación: $a+b\sqrt{p}\in\mathbb{Q}[\sqrt{p}],\ c+d\sqrt{p}\in\mathbb{Q}^*[\sqrt{p}]$ entonces

$$(a+b\sqrt{p}):(c+d\sqrt{p})=(a+b\sqrt{p})\cdot(c+d\sqrt{p})^{-1}$$

Teorema 138 $(\mathbb{Q}[\sqrt{p}],+,\cdot)$ *es un cuerpo.*

Demostración: Se ha demostrado anteriormente que $(\mathbb{Q}[\sqrt{p}],+)$ y $(\mathbb{Q}^*[\sqrt{p}],\cdot)$ son grupos abelianos, luego falta ver la distributividad es decir, debemos demostrar

$a_1+b_1\sqrt{p},a_2+b_2\sqrt{p},a_3+b_3\sqrt{p}\in\mathbb{Q}[\sqrt{p}]$ tenemos

$$(a_1+b_1\sqrt{p})\cdot[(a_2+b_2\sqrt{p})+(a_3+b_3\sqrt{p})]=[(a_1+b_1\sqrt{p})\cdot(a_2+b_2\sqrt{p})+(a_1+b_1\sqrt{p})\cdot(a_3+b_3\sqrt{p})].$$

Veamos

$$(a_1+b_1\sqrt{p})\cdot[(a_2+b_2\sqrt{p})+(a_3+b_3\sqrt{p})] = (a_1+b_1\sqrt{p})\cdot[(a_2+a_3)+(b_2+b_3)\sqrt{p}]$$

lo que es igual a

$$\begin{aligned}
& (a_1(a_2+a_3)+pb_1(b_2+b_3))+(a_1(b_2+b_3)+b_1(a_2+a_3)\sqrt{p} \\
= & (a_1a_2+a_1a_3+pb_1b_2+pb_1b_3)+(a_1b_2+a_1b_3+a_2b_1+a_3b_1)\sqrt{p} \\
= & (a_1a_2+pb_1b_2+a_1a_3+pb_1b_3)+(a_1b_2+a_2b_1+a_1b_3+a_3b_1)\sqrt{p} \\
= & ((a_1a_2+pb_1b_2)+(a_1b_2+a_2b_1)\sqrt{p})+((a_1a_3+pb_1b_3)+(a_1b_3+a_3b_1)\sqrt{p}) \\
= & [(a_1+b_1\sqrt{p})\cdot(a_2+b_2\sqrt{p})]+[(a_1+b_1\sqrt{p})\cdot(a_3+b_3\sqrt{p})].
\end{aligned}$$

Ejemplo 106 *Resolver en* $\mathbb{Q}[\sqrt{5}]$*, la ecuación*

$$(2+3\sqrt{5})x = 3-\sqrt{5}$$

Solución: Como sabemos, el inverso se obtiene del siguiente modo

$$(2+3\sqrt{5})^{-1} = \frac{2}{4-5\cdot 9} - \frac{3}{4-5\cdot 9}\sqrt{5} = -\frac{2}{41} + \frac{3}{41}\sqrt{5}$$

luego se tiene que

$$x = (3-\sqrt{5})(-\frac{2}{41} + \frac{3}{41}\sqrt{5}) = (-3\frac{2}{41} + 5\cdot(-1)\frac{3}{41}) + (3\frac{3}{41} - \frac{2}{41}(-1))\sqrt{5}$$

Por lo tanto,

$$x = -\frac{21}{41} + \frac{11}{41}\sqrt{5}$$

El conjunto solución es

$$S = \left\{-\frac{21}{41} + \frac{11}{41}\sqrt{5}\right\}$$

Ejemplo 107 *Resolver en* $\mathbb{Q}[\sqrt{7}]$*, el sistema ecuaciones*

$$\boxed{\begin{array}{rcl}(2+\sqrt{7})x + y &=& 3+\sqrt{7}\\ (3-\sqrt{7})x + \sqrt{7}y &=& 1\end{array}}$$

Solución: Amplifiquemos la primera ecuación

$$\boxed{\begin{array}{rcll}(2+\sqrt{7})x + y &=& 3+\sqrt{7} & /\cdot -\sqrt{7}\\ (3+\sqrt{7})x + \sqrt{7}y &=& 1 & \end{array}}$$

Obtenemos

$$\boxed{\begin{array}{rcl}(-7-2\sqrt{7})x - \sqrt{7}y &=& -7-3\sqrt{7}\\ (3+\sqrt{7})x + \sqrt{7}y &=& 1\end{array}}$$

Sumando obtenemos

$$\begin{array}{rcl}(-4-\sqrt{7})x &=& -6-3\sqrt{7}\\ x &=& (-6-3\sqrt{7})(-4-\sqrt{7})^{-1}\\ x &=& (-6-3\sqrt{7})(\frac{-4}{9} + \frac{1}{9}\sqrt{7})\\ x &=& \frac{1}{3} + \frac{2}{3}\sqrt{7}\end{array}$$

Reemplazando en la primera ecuación obtenemos

$$\begin{array}{rcl}y &=& 3+\sqrt{7} - (2+\sqrt{7})(\frac{1}{3} + \frac{2}{3}\sqrt{7})\\ y &=& 3+\sqrt{7} - (\frac{16}{3} + \frac{5}{3}\sqrt{7})\\ y &=& -\frac{7}{3} - \frac{2}{3}\sqrt{7}\end{array}$$

Luego, el conjunto solución del sistema es

$$S = \left\{\left(\frac{1}{3} + \frac{2}{3}\sqrt{7}, -\frac{7}{3} - \frac{2}{3}\sqrt{7}\right)\right\}$$

4.2.2. Conjugación de $\mathbb{Q}[p]$.

Definición 43 *Sea $a+b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$.*
Se define el conjugación de $a+b\sqrt{p}$ por $a-b\sqrt{p}$ y se denota de la siguiente forma:

$$\overline{a+b\sqrt{p}} := a-b\sqrt{p}.$$

Observación: La conjugación es una función dada por

$$\begin{array}{rccc} \overline{} & : & \mathbb{Q}[\sqrt{p}\,] & \to & \mathbb{Q}[\sqrt{p}\,] \\ & & a+b\sqrt{p} & \mapsto & \overline{a+b\sqrt{p}} = a-b\sqrt{p}. \end{array}$$

Cumple las siguientes propiedades

Teorema 139 *Sean $a+b\sqrt{p}, c+d\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$*

(i)
$$\overline{(a+b\sqrt{p})+(c+d\sqrt{p})} = \overline{(a+b\sqrt{p})} + \overline{(c+d\sqrt{p})}.$$

(ii)
$$\overline{(a+b\sqrt{p})\cdot(c+d\sqrt{p})} = \overline{(a+b\sqrt{p})} \cdot \overline{(c+d\sqrt{p})}.$$

(iii)
$$\overline{a+b\sqrt{p}} = a+b\sqrt{p} \quad \textit{si y sólo si} \quad b=0.$$

Demostración:

(i) Sean $a+b\sqrt{p}, c+d\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$, luego

$$\begin{aligned} \overline{(a+b\sqrt{p})+(c+d\sqrt{p})} &= \overline{(a+c)+(b+d)\sqrt{p}} \\ &= (a+c)-(b+d)\sqrt{p} \\ &= (a+c)+((-b)+(-d))\sqrt{p} \\ &= (a-b\sqrt{p})+(c-d\sqrt{p}) \\ &= \overline{a+b\sqrt{p}} + \overline{c+d\sqrt{p}}. \end{aligned}$$

(ii) Sean $a+b\sqrt{p}, c+d\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$, tenemos

$$\begin{aligned} \overline{(a+b\sqrt{p})\cdot(c+d\sqrt{p})} &= \overline{(ac+pbd)+(ad+bc)\sqrt{p}} \\ &= ((ac+bd)-(ad+bc)\sqrt{p} \\ &= (ac+(-b)(-d))+(a(-d)+(-b)c)\sqrt{p} \\ &= (a-b\sqrt{p})\cdot(c-d\sqrt{p}) \\ &= \overline{a+b\sqrt{p}} \cdot \overline{c+d\sqrt{p}}. \end{aligned}$$

(iii) Sea $a+b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$, luego

$$\overline{a+b\sqrt{p}} = a-b\sqrt{p}$$

pero a, b son únicos luego

$$a = a \vee b = -b$$

Por lo tanto, $b=0$

4.2.3. La Norma de $\mathbb{Q}[\sqrt{p}]$.

Definición 44 *Sea $a+b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$, se define la norma de $a+b\sqrt{p}$ por a^2-b^2p y se denota por*

$$\| a + b\sqrt{p} \| := a^2 - b^2p.$$

Observación: La norma es una función dada por

$$\begin{array}{rccc} \| \ \| & : & \mathbb{Q}[\sqrt{p}] & \to & \mathbb{Q} \\ & & a + b\sqrt{p} & \mapsto & \| a + b\sqrt{p} \| = a^2 - b^2p. \end{array}$$

Teorema 140 *Sean $a + b\sqrt{p}, c + d\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$*

i)

$$\| \overline{(a + b\sqrt{p})} \| = \| a + b\sqrt{p} \|$$

ii)

$$\| (a + b\sqrt{p}) \| = (a + b\sqrt{p})\overline{(a + b\sqrt{p})}$$

iii)

$$\| (a + b\sqrt{p}) \cdot (c + d\sqrt{p}) \| = \| a + b\sqrt{p} \| \cdot \| c + d\sqrt{p} \|$$

Demostración: Sean $a + b\sqrt{p}, c + d\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$, luego

$$\begin{array}{rcl} \| (a_+b\sqrt{p}) \cdot (c + d\sqrt{p}) \| & = & \| (ac + pbd) + (ad + bd)\sqrt{p} \| \\ & = & (ac + pbd)^2 - (ad + bd)^2p \\ & = & a^2c^2 + 2acpbd + p^2b^2d^2 - (a^2d^2 + 2adcb + c^2b^2)p \\ & = & a^2c^2 + 2acpbd + p^2b^2d^2 - a^2d^2p - 2adcbp - c^2b^2p \\ & = & a^2c^2 + p^2b^2d^2 - a^2d^2p - c^2b^2p \\ & = & (a^2 - pb^2) \cdot (c^2 - pd^2) \\ & = & \| a + b\sqrt{p} \| \cdot \| c + d\sqrt{p} \| \end{array}$$

4.2.4. Anillo de Enteros de $\mathbb{Z}[\sqrt{p}]$.

Definición 45 *Se define $\mathbb{Z}[\sqrt{p}]$ igual a*

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

Observación: Dadas las contenciones anteriores se tiene que

$$\mathbb{Z}[\sqrt{p}] \subseteq \mathbb{Q}[\sqrt{p}]$$

Luego el conjugado y norma están definidas, más aún

$$\begin{array}{rccc} \| \ \| & : & \mathbb{Z}[\sqrt{p}\,] & \to & \mathbb{Z} \\ & & a + b\sqrt{p} & \mapsto & \| a + b\sqrt{p} \| := a^2 - b^2p. \end{array}$$

Teorema 141 $(\mathbb{Z}[\sqrt{p}], +, \cdot)$ *es un anillo conmutativo.*

Definición 46 *Sea $u \in \mathbb{Z}[\sqrt{p}]$, se dice que u es una unidad de $\mathbb{Z}[\sqrt{p}]$, si y sólo si existe un elemento $v \in \mathbb{Z}[\sqrt{p}]$, tal que $uv = 1$.*

Notación: Denotaremos el conjunto unidad de $\mathbb{Z}[\sqrt{p}]$ por $\mathcal{U}(\mathbb{Z}[\sqrt{p}])$

Ejemplo 108 *Determine en cada caso si el elemento es*

1. $3 + 2\sqrt{2}$ *es un unidad* $\mathbb{Z}[\sqrt{2}]$
2. $3 + 2\sqrt{3}$ *es un unidad* $\mathbb{Z}[\sqrt{3}]$

Solución: 1. Supongamos $3 + 2\sqrt{2}$ es un unidad, luego existe $x + y\sqrt{2}$ tal que

$$\begin{aligned}(3 + 2\sqrt{2})(x + y\sqrt{2}) &= 1 + 0\sqrt{2}\\ (3x + 4y) + (3y + 2x)\sqrt{2} &= 1 + 0\sqrt{2}\end{aligned}$$

De lo cual obtenemos, el siguiente sistema

$$\left.\begin{array}{rcl} 3x + 4y &=& 1 \ / \cdot 2 \\ 2x + 3y &=& 0 \ / \cdot -3 \end{array}\right|$$

Sumando las ecuaciones obtenemos $-y = 2$, es decir $y = -2$. reemplazando obtenemos $x = 3$,

$$(3 + 2\sqrt{2})^{-1} = 3 - 2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

luego tenemos $3 + 2\sqrt{2} \in \mathcal{U}(\mathbb{Z}[\sqrt{2}])$.

2. Supongamos ahora que $3 + 2\sqrt{3}$ es un unidad, luego existe $x + y\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ tal que

$$\begin{aligned}(3 + 2\sqrt{3})(x + y\sqrt{3}) &= 1 + 0\sqrt{3}\\ (3x + 6y) + (3y + 2x)\sqrt{3} &= 1 + 0\sqrt{3}\end{aligned}$$

De lo cual obtenemos

$$\left.\begin{array}{rcl} 3x + 6y &=& 1 \\ 2x + 3y &=& 0 \end{array}\right|$$

Pero la primera ecuación nos entrega que $3|1$, lo que es una contradicción. Por tanto tenemos $3 + 2\sqrt{3} \notin \mathcal{U}(\mathbb{Z}[\sqrt{3}])$.

Propiedad 142 *$a + b\sqrt{p} \in \mathcal{U}(\mathbb{Z}[\sqrt{p}])$ si y sólo si $\|a + b\sqrt{p}\| \in \{1. - 1\}$*

Demostración: Supongamos que $a + b\sqrt{p}$ es una unidad, luego existe $x + y\sqrt{p}$ tal que

$$\begin{aligned}(a + b\sqrt{p})(x + y\sqrt{p}) &= 1 + 0\sqrt{p} \ /\| \ \|\\ \|(a + b\sqrt{p})(x + y\sqrt{p})\| &= \|1 + 0\sqrt{p}\|\\ \|a + b\sqrt{p}\|\|x + y\sqrt{p}\| &= 1\end{aligned}$$

Por lo tanto, $\|a + b\sqrt{p})\|$ es unidad en $\mathbb{Z}$, por ende $\|a + b\sqrt{p}\| \in \{1. - 1\}$.

En el otro sentido, supongamos que $\|a + b\sqrt{p}\| = 1$, podemos comprobar que

$$(a + b\sqrt{p})(a - b\sqrt{p}) = (a^2 - bp^2) + (-ab + ab)\sqrt{p} = 1 + 0\sqrt{p}$$

Propiedad 143 $(\mathcal{U}(\mathbb{Z}[\sqrt{p}]), \cdot)$ *es un grupo abeliano.*

Observación: Note que los conjuntos anteriores incluido las operaciones, también es posible construirlos del siguiente modo, en $\mathbb{Z} \times \mathbb{Z}$ o en $\mathbb{Q} \times \mathbb{Q}$, se define las siguientes operaciones

$$\begin{aligned} (a,b) + (c,d) &= (a+c, b+d) \\ (a,b) \cdot (c,d) &= (ac+bdp, ad+bc) \end{aligned}$$

y con ellos tenemos la misma estructura, sin incorporar el símbolo $\sqrt{p}$ explícitamente.