ANILLOS DE ORIGAMI

Ana Gautier Flores

ANILLOS DE ORIGAMI

Ana Gautier Flores

Memoria presentada como parte de los requisitos para la obtención del título de Grado en Matemáticas por la Universidad de Sevilla.

Tutorizada por

Prof. Alberto Castaño Domínguez

Resumen

En este trabajo vamos a estudiar las construcciones de origami, que son conjuntos de puntos del plano complejo que se obtienen de forma análoga a la de los puntos de corte entre dos pliegues en una figura de origami. La idea es partir de un conjunto de direcciones dadas y dos puntos, que suelen ser 0 y 1, e ir intersecando rectas que pasen por tales puntos con los ángulos de esas direcciones para construir puntos nuevos y luego poder usarlos en la obtención de otros posteriores. El objetivo principal de la memoria será probar que este tipo de conjunto de puntos es un anillo en diversas situaciones.

Para ello, vamos estudiar las propiedades y resultados que caracterizan a los puntos que lo forman. Además, distinguiremos diferentes casos según el cardinal del conjunto de direcciones o las propiedades algebraicas de tal conjunto, que nos llevarán a ver qué tipo de estructura algebraica o geométrica caracteriza a la construcción de origami en esos casos. Veremos que los anillos ciclotómicos y de enteros cuadráticos son dos ejemplos de anillos conocidos a los que podemos llegar partiendo de una construcción de origami, y que, además, en algunos casos concretos de direcciones también podremos partir de anillos de enteros cuadráticos y obtener los de origami.

English Abstract

The goal of this memory is to focus on origami constructions, which are sets of points on the complex plane that are obtained in an analogous way to the intersection points between two folds in an origami figure. The idea is to start from a set of given directions and two points, which are usually 0 and 1, and intersect lines that pass through such points with those angles to construct new points and then be able to use them to obtain subsequent ones. The main objective of the work will be to prove that this type of set of points is a ring in different situations.

To do this, we are going to study the properties and results that characterize the points that form it. Furthermore, we will see different cases according to the number of possible directions or its algebraic properties, which will lead us to endow origami rings with an algebraic or geometric structure in those cases. We will see that cyclotomic and quadratic integer rings are two examples of known rings that we can get from an origami construction. In addition, in some specific cases of possible directions we will be able to start from the ring of integers of an imaginary quadratic number field and obtain an origami ring.

Índice general

Introducción

El origami, término que procede de los vocablos japoneses "ori" (pliegue) y "kami" (papel), es un arte que consiste en el plegado de papel para obtener figuras de formas variadas. A pesar de que sus orígenes se remontan a hace más de cinco siglos, a día de hoy sigue aportando resultados tanto artísticos como científicos. Nosotros nos centraremos en estos últimos, estudiando una teoría matemática inspirada en el origami. En ella, podemos hacer una analogía entre los pliegues del papel y las rectas del plano complejo, a la vez que entre los puntos que se crean intersecando dos pliegues y los resultantes de intersecar dos rectas en el plano, respectivamente. La idea matemática se basa entonces en, dado un conjunto de posibles direcciones que nos derminarán rectas del plano y dos puntos de partida (que suelen ser 0 y 1), construir de forma iterativa nuevos puntos mediante las intersecciones de tales rectas, y luego usarlos para obtener otros nuevos. Esos conjuntos de puntos son los que llamamos construcciones de origami, y los que veremos que, en particular, serán anillos bajo ciertas condiciones, de ahí el título de nuestra memoria. Además de ello, nos plantearemos otras cuestiones que no serán meramente algebraicas, sino también geométricas o topológicas sobre tales conjuntos. Cabe destacar que este trabajo es parte de una teoría mas amplia, ejemplos de otras preguntas que caben hacerse son la extensión a dimensiones superiores y la noción de puntos constructibles análoga a las construcciones con regla y compás.

Sea $T := S^1 \subset \mathbb{C}$ la circunferencia unidad. Consideraremos U como un subconjunto de $T/\{\pm 1\}$ de posibles direcciones, que contiene al 1. Si p, q son puntos de $\mathbb{C}$, la recta que pasa por p con dirección $u \in U$ se denota por $L_u(p)$, y $L_v(q)$ denota entonces a aquella que pasa por q con dirección $v \in U$. La intersección de ambas vendrá dada por el punto $I_{u,v}(p, q) := L_u(p) \cap L_v(q)$. Además, diremos que un punto p es un monomio si puede construirse comenzando en 1 mediante intersecciones del tipo $I_{u,v}(\bullet, 0)$ con $u, v \in U$. Abundando en lo anterior, llamamos $M_0 := \{0, 1\}$, y para $j \geq 1$ definimos M_j como el conjunto de todos los puntos intersección de la forma

$I_{u,v}(p,q)$ para $u \neq v$ y $p \neq q$, tal que $u, v \in U$ y $p, q \in M_{j-1}$. Usando esta definición, podemos considerar la construcción de origami $R(U)$ como $R(U) := \bigcup_{j\geq 0} M_j$. Resulta natural preguntarse en qué casos $R(U)$ es anillo, que es el objetivo principal de nuestro trabajo.

La respuesta a lo anterior dependerá de las condiciones sobre el conjunto U, pues, si este es un semigrupo con al menos tres elementos, tendremos que $R(U)$ es un subanillo de $\mathbb{C}$ formado por las combinaciones lineales enteras de monomios. Por otro lado, si U tiene exactamente tres elementos, sin necesidad de ser semigrupo, $R(U)$ será siempre un $\mathbb{Z}$-módulo de la forma $\mathbb{Z} + \mathbb{Z}z$ (con $z := I_{u,v}(0,1)$) ; en particular, será un anillo si z es un entero algebraico de grado 2 sobre $\mathbb{Z}$. De hecho, en estas condiciones, veremos que coincide con el anillo de enteros de una extensión cuadrática. En el caso de que U sea el grupo cíclico generado por una raíz primitiva de la unidad, $R(U)$ coincidirá con subanillos de extensiones ciclotómicas de la forma $\mathbb{Q}(\zeta_n)$, distinguiendo dos situaciones según n sea o no primo. Resultará interesante probar por el camino otras propiedades sobre $R(U)$ que no serán de naturaleza puramente algebraica, como lo será por ejemplo la densidad de $R(U)$ en $\mathbb{C}$ (visto también como el espacio vectorial $\mathbb{R}^2$), cuando U tiene al menos cuatro elementos.

En el Capítulo 1 tendremos varias secciones. En la primera se ven las definiciones principales que usaremos a lo largo del resto de capítulos y algunas propiedades interesantes. En la Sección 1.2 tendremos una primera prueba sobre la estructura de anillo de $R(U)$. A continuación, veremos algunos ejemplos y resultados en los que $R(U)$ constituye un anillo sin ser U un semigrupo en la Sección 1.3. Terminaremos esta primera parte viendo que cuando U determina al menos cuatro direcciones, $R(U)$ es denso en $\mathbb{C}$. En los capítulos 2 y 3 se estudian casos particulares de anillos conocidos que coinciden con $R(U)$ bajo ciertas hipótesis. En particular, en el último de ellos veremos que partiendo de cualquier anillo de enteros cuadráticos somos capaces de conseguir un anillo de origami.

1 Construcciones de origami

Nuestro primer objetivo en este trabajo será, tomando como referencia principal el artículo [3], definir una serie de puntos del plano complejo que asemejaremos a las intersecciones entre pliegues del papel en figuras de origami. A partir de las propiedades que tienen todos ellos, veremos que, bajo ciertas hipótesis, constituyen un subanillo del plano complejo $\mathbb{C}$ en distintas situaciones.

1.1 Definiciones y propiedades básicas

Inicialmente, veamos la notación que usaremos a lo largo de las secciones.

Notación 1.1.1. Identificaremos los pliegues de origami con rectas del plano complejo. Una recta viene dada por un punto p contenido en ella y una dirección, que es un número complejo distinto de 0 que llamamos u. Por lo tanto, la recta que pasa por p con dirección u se expresará:

$$L_u(p) := \{p + ru : r \in \mathbb{R}\}.$$

Sabemos que dos números complejos distintos de cero determinan la misma dirección si son múltiplos reales el uno del otro, por lo que supondremos que los vectores directores son números complejos de valor absoluto 1.

En ese caso, consideramos $T := S^1 \subset \mathbb{C}$, la circunferencia unidad vista como grupo con el producto. A partir de ella, podemos definir el conjunto de direcciones posibles, que denotaremos por U, como un subconjunto de $T/\{\pm 1\}$. De ahora en adelante, usaremos ese conjunto para trabajar con un semigrupo [1] $(U, *)$, donde la

[1] Un semigrupo es un sistema algebraico de la forma $(A, *)$ en la cual A es un conjunto no vacío, y

operación $*$ designa el producto usual.

En las secciones y capítulos siguientes, abusaremos de notación y, siempre que quede claro en el contexto, escribiremos u y v para referirnos a, indistintamente, elementos de $T/\{\pm 1\}$, números complejos no nulos o vectores de $\mathbb{C}$ visto como $\mathbb{R}$-espacio vectorial.

Es posible identificar $T/\{\pm 1\}$ con el grupo cociente $G = \mathbb{R}/(\pi\mathbb{Z})$. De esta forma, podemos asignar a cada $\theta \in G$ el punto $e^{i\theta}$. Siguiendo este razonamiento, el eje horizontal (el 1 en U) será aquel que tiene ángulo 0. No olvidemos que sumar ángulos en sentido geométrico se corresponde con la multiplicación en el semigrupo U.

Además, veremos que hay situaciones que no requieren que U sea un semigrupo, y será interesante estudiar qué ocurre entonces con conjuntos arbitrarios de ángulos.

Seguimos trabajando con U y con puntos del plano complejo $\mathbb{C}$, ya que, a partir de ellos, se puede generar otro conjunto de puntos con ciertas propiedades, que será objeto central de estudio en este trabajo. Para facilitar la comprensión de los resultados que veremos, introducimos primero la siguiente notación:

Notación 1.1.2. Si las direcciones u y v determinan rectas distintas (es decir, $u \neq v$ mód $\{\pm 1\}$), entonces

$$I_{u,v}(p,q) := L_u(p) \cap L_v(q)$$

es el único punto de intersección de ambas rectas o pliegues.

Definición 1.1.3. *Sea $M_0 := \{0,1\}$, para $j \geq 1$ definimos M_j como el conjunto de todos los puntos intersección de la forma $I_{u,v}(p,q)$ para $u \neq v$ y $p \neq q$, tal que $u, v \in U$ y $p, q \in M_{j-1}$. Usando esta definición, podemos considerar la* ***construcción (o conjunto) de origami*** *$R(U)$ como $R(U) := \bigcup_{j\geq 0} M_j$, con el que trabajaremos a lo largo de estas páginas.*

Veamos ahora que podemos hallar una fórmula explícita para $I_{u,v}(p,q)$ y que esta operación tiene diversas propiedades interesantes, tanto geométricas como algebraicas.

Sean u, v direcciones distintas, y consideremos las rectas $L_u(p)$ y $L_v(q)$. La inter-

$*$ es una operación interna definida en A, que debe ser asociativa.

sección de ambas es el punto $I_{u,v}(p,q)$ que es la única solución z tal que

$$z = p + ru = q + sv \quad r, s \in \mathbb{R}.$$

Como $s = v^{-1}(p - q + ru)$ es real, podemos imponer que la parte imaginaria de la expresión derecha se anule para obtener una ecuación que puede resolverse para r:

$$r = \frac{Im((q-p)/v)}{Im(u/v)}.$$

Notación 1.1.4. De ahora en adelante, consideraremos:

$$s_{x,y} = x\bar{y} - \bar{x}y = 2i|y|^2 Im(x/y),$$

para cualesquiera complejos no nulos x, y donde $|y|^2 = y \cdot \bar{y}$. Notamos que $s_{(\bullet,\bullet)}$ es antisimétrica y, vista como forma en dos variables complejas, es $\mathbb{R}$-bilineal.

Usando la notación anterior, podemos reescribir la ecuación para r de la forma:

$$r = \frac{s_{q-p,v}}{s_{u,v}}.$$

Esto proporciona otra forma de expresar también los puntos de intersección:

$$I_{u,v}(p,q) = p + \frac{s_{q-p,v}}{s_{u,v}}u = \frac{s_{u,v}p + s_{q,v}u - s_{p,v}u}{s_{u,v}}.$$

Sustituyendo la definición y operando llegamos a la siguiente fórmula:

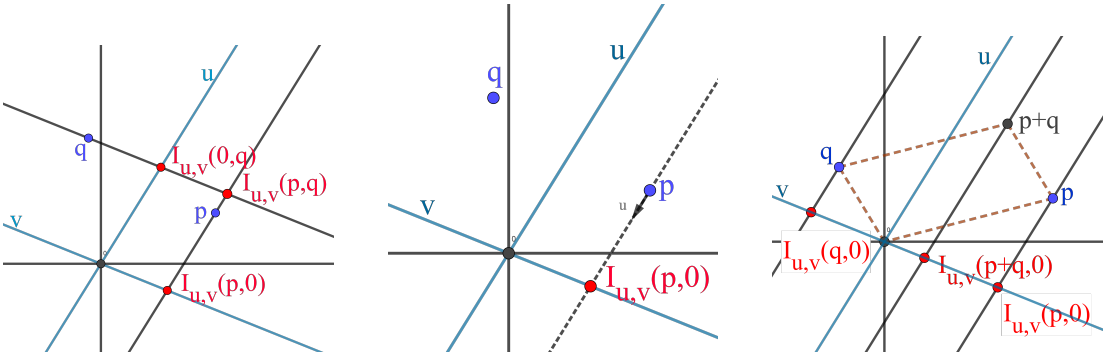
$$I_{u,v}(p,q) = \frac{\bar{p}uv - p\bar{u}v - \bar{q}uv + qu\bar{v}}{s_{u,v}} = \frac{s_{u,p}}{s_{u,v}}v + \frac{s_{v,q}}{s_{v,u}}u. \tag{1.1}$$

Veamos ahora algunas propiedades básicas de (1.1).

Proposición 1.1.5. Sean p, q dos puntos del plano, y u, v dos direcciones. Se tienen las siguientes propiedades:

- **Simetría**: $I_{u,v}(p,q) = I_{v,u}(q,p)$.
- **Reducción**: $I_{u,v}(p,q) = I_{u,v}(p,0) + I_{u,v}(0,q)$.

- **Proyección**: $I_{u,v}(p,0)$ es una proyección del punto p sobre la recta $\{rv : r \in \mathbb{R}\}$ en la dirección u [2].
- **Linealidad**: $I_{u,v}(p+q,0) = I_{u,v}(p,0) + I_{u,v}(q,0)$, y para $r \in \mathbb{R}$, $I_{u,v}(rp,0) = rI_{u,v}(p,0)$.
- **Convexidad**: $I_{u,v}(p,q)$ tiene la forma $Ap+Bq$ donde A y B definen aplicaciones $\mathbb{R}$-lineales del plano complejo que cumplen $A + B = I_2$.
- **Rotación**: Para $w \in \mathbf{T}$, $wI_{u,v}(p,q) = I_{wu,wv}(wp, wq)$.



(a) Reducción. (b) Proyección. (c) Linealidad.

Figura 1.1: Propiedades.

Demostración. Vamos a ir probando todas las propiedades enunciadas, aunque todas ellas son triviales excepto la de convexidad:

- **Simetría**: es evidente por la propia definición.
- **Reducción**: Tenemos

$$\begin{aligned} I_{u,v}(p,0) + I_{u,v}(0,q) &= \frac{u\bar{p}v - \bar{u}pv}{s_{u,v}} + \frac{-v\bar{q}u + \bar{v}qu}{s_{u,v}} \\ &= \frac{u\bar{p}v - \bar{u}pv - v\bar{q}u + \bar{v}qu}{s_{u,v}} = I_{u,v}(p,q). \end{aligned}$$

  Geométricamente, podemos comprobar que esto se tiene gracias a la ley de los paralelogramos, como muestra la figura 1.1a.
- **Proyección**: Esta propiedad se obtiene de forma directa, pues $I_{u,v}(p,0)$ es el único punto que está en la recta $p + \langle u \rangle$ y en la recta $0 + \langle v \rangle$ por definición.

[2] La **proyección** de p sobre una recta L en la dirección u es el punto de la forma $p + ru$ que está en L.

- **Linealidad**: Una parte de esta propiedad y la anterior también se reflejan en la figura 1.1, de hecho, esta es consecuencia de la anterior. Analíticamente, haciendo uso de la expresión (1.1) en cada caso a probar tenemos que:

$$I_{u,v}(p+q,0) = \frac{s_{u,p+q}}{s_{u,v}}v,$$

y para $r \in \mathbb{R}$,

$$I_{u,v}(rp,0) = \frac{s_{u,rp}}{s_{u,v}}v.$$

Y como el operador $s_{(\bullet,\bullet)}$ es $\mathbb{R}$-bilineal, la prueba es directa en ambos casos.

- **Convexidad**: Sean P, Q dos puntos del plano y u, v dos direcciones distintas tal que $u = e^{i\alpha}$ y $v = e^{i\beta}$, con $\alpha \neq \pm\beta \mod 2\pi$.
Construimos ahora las rectas $r := P + < u >$ y $s := Q + < v >$ que, por definición, tendrán distintas pendientes. Llamemos R al punto de corte de ambas, y veamos que puede expresarse como combinación convexa de dos matrices por cada uno de los puntos iniciales.
Como el argumento de la prueba es independiente al sistema de referencia usado, tomaremos el siguiente sistema de referencia para que la prueba sea más sencilla:

$$\mathcal{R} = \{Q, \overrightarrow{QP}, \vec{v}\},$$

el cual se considera bajo ciertas hipótesis:

  - $\overrightarrow{QP} \neq \vec{0}$ (pues $P \neq Q$).
  - $v \notin < \overrightarrow{QP} >$ (de lo contrario existirían infinitos puntos de intersección).

Notemos que al considerar cualquier otro sistema de referencia, estaríamos multiplicando por una matriz invertible y su inversa, a izquierda y derecha de A y B, respectivamente. Por tanto, el hecho de que A y B sumen la identidad no se ve alterado.
Si definimos

$$R := Q + \mu\vec{v}, \tag{1.2}$$

queremos que:

$$R = A\begin{pmatrix} p_1 \\ p_2 \end{pmatrix} + B\begin{pmatrix} q_1 \\ q_2 \end{pmatrix} \text{ tal que } A + B = I_2,$$

donde $(p_1, p_2), (q_1, q_2)$ son las coordenadas de P, Q respectivamente.
Tomemos ahora

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \text{ por determinar y } B = I_2 - A.$$

Entonces, el punto R usando la expresión inicial y esta consideración podría expresarse como sigue:

$$R = I_2 \begin{pmatrix} q_1 \\ q_2 \end{pmatrix} + A \begin{pmatrix} p_1 - q_1 \\ p_2 - q_2 \end{pmatrix} = Q + A \cdot \overrightarrow{QP}.$$

Y teniendo en cuenta que $(\overrightarrow{QP})_{\mathcal{R}} = (1, 0)$, nos queda $A \cdot \overrightarrow{QP} = (a_{11}, a_{21})$. Eso unido a la expresión del punto R en (1.2) nos lleva a buscar los coeficientes de la matriz A de tal forma que:

$$A \cdot \overrightarrow{QP} = \mu\vec{v} = \overrightarrow{(0, \mu)}_{\mathcal{R}},$$

de donde se tiene que:

$$A = \begin{pmatrix} 0 & a_{12} \\ \mu & a_{22} \end{pmatrix} \text{ por lo que } B = \begin{pmatrix} 1 & -a_{12} \\ -\mu & 1 - a_{22} \end{pmatrix}.$$

Es posible concluir entonces la prueba de esta propiedad. Destacamos además que no es necesario que las matrices sean regulares, sino que con tener rango 1 es suficiente. De hecho, en la referencia [3], encontramos un ejemplo de tales matrices usando argumentos trigonométricos en los que se da este hecho. En nuestro caso, tomando $\mu \neq 0$, $a_{22} = 1$ y $a_{12} = 0$ tenemos un ejemplo válido en el que tanto A como B tendrían rango 1 y seguirían cumpliendo la propiedad.

Se denomina convexidad porque como la matriz $B = A - I_2$, podríamos verlo como una analogía de la combinación convexa en espacios vectoriales reales.

- **Rotación:** Al igual que otras anteriores, esta propiedad es evidente. Basta con observar que multiplicar por $w \in T$ es equivalente, geométricamente, a rotar un ángulo igual a su argumento.

Una vez definidos los conjuntos con los que trabajaremos y algunas características de los elementos que lo forman, vamos a ver en la siguiente sección qué estructura tiene $R(U)$ bajo ciertas condiciones sobre U.

1.2 Estructura de anillo de R(U)

En esta sección U será un **semigrupo** de direcciones fijadas y veremos que $R(U)$ forma un subanillo de $\mathbb{C}$, siempre y cuando U contenga al 1 y determine, al menos,

tres direcciones distintas. Es más, es el mínimo número de direcciones a considerar si se pretende tener puntos de corte de la forma $I_{u,v}(0,1)$ en $R(U)$, distintos de los triviales, de lo contrario solo estaría formado por los puntos 0 y 1.

Pasamos entonces al estudio de tal conjunto, para el cual previamente vamos a introducir nuevos conceptos que nos ayudarán en algunas de las pruebas:

Definición 1.2.1. *Un punto p se dice **monomio primitivo** si puede ser construido en un solo paso a partir del 0 y del 1, es decir*

$$p = I_{u,v}(1,0) \quad u, v \in U.$$

*En general, decimos que un punto p en $R(U)$ es un **monomio** (o U-monomio) si puede construirse comenzando en 1 usando solo intersecciones de la forma $I_{u,v}(\bullet, 0)$, es decir, aquellas en las que la segunda recta pasa por el origen.*

Observación 1.2.2. El punto 1 se considera también un monomio, que podríamos llamar monomio trivial.

De la definición anterior se deduce que los monomios pueden formar una sucesión de la forma

$$p_1 = I_{u_1,v_1}(1,0), \quad p_2 = I_{u_2,v_2}(p_1,0), \quad p_3 = I_{u_3,v_3}(p_2,0), \ldots$$

Si $p = p_k = I_{u_k,v_k}(p_{k-1},0)$ es el k-ésimo elemento de una sucesión de monomios, diremos que es un monomio de longitud a lo sumo k.

Relacionando este nuevo concepto con la definición 1.1.3, tenemos que todo monomio construido de esta forma está en M_k.

Pasamos ahora a enunciar algunas propiedades de tales elementos. Cabe destacar que en el siguiente resultado hemos relajado las hipótesis de que U sea grupo para una de las pruebas, mientras que en la referencia [3] son más estrictos con este aspecto.

Lema 1.2.3. El producto de dos monomios es un monomio. Si además U es un grupo, cualquier monomio es producto de monomios primitivos.

Demostración. Dados u y v en U, sea $I_{u,v}(1,0) = \frac{s_{u,1}}{s_{u,v}} v$ usando la expresión (1.1), donde tomaremos $r \in \mathbb{R}$ como $r = \frac{s_{u,1}}{s_{u,v}}$.

Veamos primero que el producto de dos monomios primitivos es un monomio, para lo cual consideramos el producto de dos monomios primitivos con distintas di-

recciones, y desarrollamos la expresión:

$$I_{u,v}(1,0)I_{u',v'}(1,0) = rv\, I_{u',v'}(1,0),$$

teniendo en cuenta las propiedades de rotación por el elemento v y linealidad por ser $r \in \mathbb{R}$, llegamos a:

$$rv\, I_{u',v'}(1,0) = I_{vu',vv'}(rv,0) = I_{vu',vv'}(I_{u,v}(1,0),0).$$

Por tanto, tenemos entonces una expresión que antes definíamos como monomio, hemos probado que el producto de dos monomios primitivos es un monomio. Nótese que las nuevas direcciones siguen estando en U gracias a ser este un semigrupo.

A continuación, vamos a probar la primera tesis del lema. Consideramos para ello las sucesiones que dan lugar a dos monomios con los que trabajaremos:

$$\begin{aligned} P_1 &= I_{u_1,v_1}(1,0) & Q_1 &= I_{u'_1,v'_1}(1,0)\\ P_2 &= I_{u_2,v_2}(P_1,0) & Q_2 &= I_{u'_2,v'_2}(Q_1,0)\\ &\dots & &\dots\\ P_k &= I_{u_k,v_k}(P_{k-1},0). & Q_l &= I_{u'_l,v'_l}(Q_{l-1},0). \end{aligned}$$

Entonces $P_k = I_{u_k,v_k}(P_{k-1},0)$ y $Q_l = I_{u'_l,v'_l}(Q_{l-1},0)$ son dos monomios de longitud a lo sumo k y l, respectivamente. Tendremos en cuenta que cualquier monomio de la forma $I_{u,v}(\bullet,0)$ puede expresarse como $\frac{s_{u,\bullet}}{s_{u,v}}v = rv$, donde $r \in \mathbb{R}$ sería el módulo de tal punto. Como el producto es conmutativo en $\mathbb{C}$, $P_kQ_l = Q_lP_k$. Por tanto, podemos desarrollar la expresión y aplicar a ella propiedades que ya conocemos:

$$\begin{aligned} Q_lP_k &= I_{u'_l,v'_l}(Q_{l-1},0)I_{u_k,v_k}(P_{k-1},0)\\ &= rv'_l I_{u_k,v_k}(P_{k-1},0)\\ &= I_{v'_lu_k,v'_lv_k}(rv'_lP_{k-1},0)\\ &= I_{v'_lu_k,v'_lv_k}(rv'_l I_{u_{k-1},v_{k-1}}(P_{k-2},0),0)\\ &= I_{v'_lu_k,v'_lv_k}(I_{v'_lu_{k-1},v'_lv_{k-1}}(rv'_lP_{k-2},0),0)\\ &= \dots = I_{v'_lu_k,v'_lv_k}(I_{v'_lu_{k-1},v'_lv_{k-1}}(\dots(I_{v'_lu_1,v'_lv_1}(rv'_l,0)\dots,0),0),0). \end{aligned}$$

De esta forma, teniendo en cuenta que $rv'_l = I_{u'_lv'_l}(Q_{l-1},0)$ es un monomio, el producto Q_lP_k también lo será por definición, como queríamos probar. Si en vez de

un par de monomios consideramos el producto de un número mayor de ellos, basta considerar productos de dos sucesivamente usando la asociatividad del producto de $\mathbb{C}$, y así probaríamos que también es un monomio.

Para terminar la demostración nos falta ver que en caso de que U sea grupo, cualquier monomio puede expresarse como una multiplicación de monomios primitivos. Para ello, operamos con un monomio de longitud a lo sumo 2:

$$I_{u_2,v_2}(I_{u_1,v_1}(1,0),0) = I_{u_2,v_2}(rv_1,0) = rI_{u_2,v_2}(v_1,0) = rv_1 I_{v_1^{-1}u_2,v_1^{-1}v_2}(1,0),$$

donde la primera igualdad se tiene por definición del operador intersección, la segunda gracias a la propiedad de linealidad y la última por reducción. Dado que U es un grupo, existe el inverso multiplicativo de v_1. En consecuencia, al ser rv_1 un monomio primitivo e $I_{v_1^{-1}u_2,v_1^{-1}v_2}(1,0)$ otro, tenemos que cualquier monomio puede expresarse como producto de dos monomios primitivos. Si el monomio es de longitud a lo sumo $k \geq 3$, se puede argumentar de manera similar por inducción, usando de nuevo la asociatividad.

Cabe mencionar que en las pruebas basta con considerar que U sea un semigrupo, pues la única propiedad que usamos es que el producto sea cerrado.

Veamos ahora el resultado principal de esta sección:

Teorema 1.2.4. *Si U es un monoide[3] de direcciones que determinan al menos tres pliegues, entonces $R(U)$ es el conjunto de combinaciones lineales enteras de monomios y, por tanto, es un subanillo de $\mathbb{C}$.*

Demostración. Para probar que $R(U)$ es un subanillo necesitaríamos ver que es un grupo tanto con la suma como con el producto. Lo vemos a continuación:

Grupo abeliano con la suma

Primero, veamos que 2 y -1 están en $R(U)$. Como hay al menos tres rectas determinadas a partir de las direcciones en U, existen direcciones u y v de tal forma que son distintas entre ellas y de 1.

Usamos u y v para construir el punto $p_1 = I_{u,v}(0,1)$, que estará fuera del eje horizontal. Podemos considerar entonces $p_2 = I_{u,1}(1,p_1)$ sobre una recta horizontal que pasa por p_1. En esta situación se puede verificar algebraica (y geométricamente)

[3]Un monoide es un semigrupo con elemento neutro.

que

$$2 = I_{1,v}(0, p_2).$$

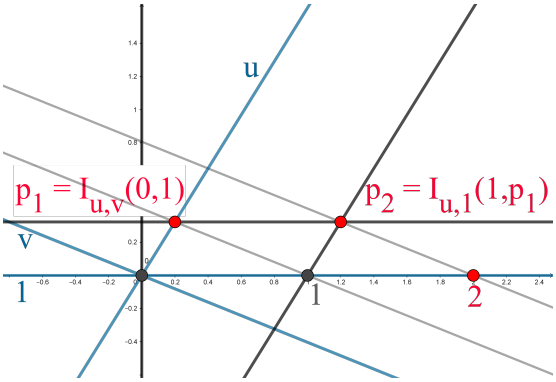


Figura 1.2: Construcción del punto 2.

De forma similar, si $p_3 := I_{v,1}(0, p_1)$ entonces se prueba que

$$-1 = I_{1,u}(0, p_3).$$

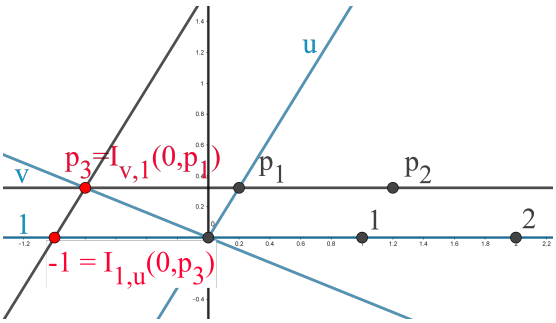


Figura 1.3: Construcción del punto -1.

A continuación, veamos que si p está en $R(U)$, entonces $p + 1$ también. Para ello, aplicamos los pasos que usamos para construir p, pero en vez de empezar con los puntos 0 y 1, lo hacemos con los puntos 1 y 2, y llegamos a $p+1$. Esto es consecuencia de la linealidad y la reducción, pues $I_{u,v}(p+r, q+r) = I_{u,v}(p, q)+I_{u,v}(r, r) = I_{u,v}(p, q)+r$.

Los tres puntos anteriores nos servirán para probar que si p y q están en $R(U)$, entonces también está la suma de ambos. Basta repetir los pasos para construir q, empezando en 0 y 1, pero esta vez empezando en p y $p + 1$, y llegamos a $p + q$.

Finalmente, por linealidad vemos que si p está en $R(U)$, entonces los mismos pasos que usamos para construir p a partir de 0 y 1, nos valen para llegar a $-p$ pero partiendo de 0 y -1.

Con todo ello, concluimos que en este caso $R(U)$ es un grupo con la suma, por ser ésta una operación cerrada para todo punto de $R(U)$. Además, se ha probado que contiene a los opuestos y eso es suficiente, porque como está en $\mathbb{C}$ la asociatividad se tiene por ser también una propiedad de $\mathbb{C}$.

Cabe mencionar que hasta el momento no hemos usado que U sea un semigrupo, y por tanto $R(U)$ siempre es un subgrupo de $\mathbb{C}$ con la suma, independientemente de las direcciones que consideremos, siempre y cuando U contenga al 1.

Grupo con el producto

Para este apartado necesitaremos ver que, dados dos puntos cualesquiera de $R(U)$, el producto es una operación interna. Lo primero que haremos será probar que $R(U)$ es el conjunto de combinaciones lineales enteras de monomios, que denotaremos por S.

Se tiene que S es un grupo con la suma, ya que las combinaciones lineales de un conjunto de generadores son cerradas porque solo sumamos los respectivos coeficientes. Es más, como el producto de monomios es un monomio por el lema 1.2.3, S es un anillo. Veamos ahora que este conjunto coincide con $R(U)$ por doble inclusión.

$\boxed{S \subset R(U)}$ Como $R(U)$ contiene a todos los monomios y es un grupo con la suma, en particular, contiene a S .

$\boxed{R(U) \subset S}$ Para probar esta inclusión usaremos los M_j de la definición 1.1.3 y tendremos en cuenta que si p es un punto de $R(U)$ entonces es de la forma

$$p = I_{u,v}(q, r).$$

Por otro lado, tenemos que el conjunto S puede expresarse como:

$$S = \left\{ \sum \lambda_i m_i \,|\, \lambda_i \in \mathbb{Z}, m_i \text{ monomio} \right\}.$$

Usaremos un argumento de inducción sobre los subíndices j de esos M_j:

Comenzamos por el caso base $j = 0$, que serían los puntos $\{0, 1\}$, que están en S, pues las combinaciones lineales de monomios contienen, en particular, a todo $\mathbb{Z}$.

Tomamos como hipótesis de inducción que si un punto $p \in M_j$, entonces $p \in S$. Veamos entonces lo que ocurre si tomamos un punto $p \in M_{j+1}$, que será de la forma $I_{u,v}(q, r)$ donde $q, r \in M_j$, los cuales están en S por hipótesis.

Gracias a las propiedades del operador I, podemos expresar el punto p como

$$p = I_{u,v}(q, 0) + I_{v,u}(r, 0),$$

donde $q, r \in S$, por lo que se tiene la siguiente equivalencia:

$$p = I_{u,v}\Big(\sum_{i=1}^{r} \alpha_i m_i, 0\Big) + I_{v,u}\Big(\sum_{k=1}^{s} \beta_k m_k, 0\Big),$$

en la cual $\alpha, \beta \in \mathbb{Z}$ y $m_i,\ m_k$ son los monomios que aparecen en la combinación lineal de p, q como elementos de S. Por último, gracias a la linealidad del operador llegamos a:

$$p = \sum_{i=1}^{r} \alpha_i I_{u,v}(m_i, 0) + \sum_{k=1}^{s} \beta_k I_{v,u}(m_k, 0).$$

Podemos concluir entonces que $p \in S$, debido a que cada uno de los sumandos son combinaciones lineales de monomios. Al ser p un punto cualquiera de $R(U)$, se tiene la contención que se quería probar.

Observamos entonces que se da la igualdad entre ambos $R(U)$ y S, por lo que podemos afirmar que en ese caso los puntos son combinaciones lineales de monomios. En consecuencia, el producto de dos puntos cualesquiera de $R(U)$ es cerrado, pues el producto de monomios vimos antes que también era cerrado.

De esta forma, tenemos que, al ser un subgrupo con la suma y cerrado para el producto (teniendo en cuenta que 1 pertenece a $R(U)$ por asunción), $R(U)$ es un subanillo de $\mathbb{C}$.

Hasta aquí ya habríamos probado que si U es un subconjunto cualquiera de $T/\{\pm 1\}$ que contiene a la unidad, $R(U)$ es grupo con la suma. Si además de ello, se tiene que U es un semigrupo, entonces $R(U)$ es un subanillo de $\mathbb{C}$ que coincide con el de combinaciones lineales de monomios. Concluimos que no es necesaria la condición de grupo sobre U como se refleja en el artículo [3], sino que es suficiente imponer que sea un monoide y que tenga al menos tres elementos para que se cumpla el teorema anterior.

De hecho, si U es un grupo, recordamos que entonces se pueden descomponer los monomios como producto de monomios primitivos, con lo cual, los elementos de $R(U)$ son polinomios en varias variables de coeficientes enteros evaluados en los monomios primitivos. Más aún, el cardinal de las variables es el de dichos monomios.

1.3 ¿Qué ocurre si U no es un semigrupo?

Hasta ahora hemos estado considerando un semigrupo de direcciones U, pero cabe plantearnos qué estructura tendría $R(U)$ en el caso de que U **no fuese** siquiera un **semigrupo**. Este enfoque se trabaja en la referencia [5] con algunos ejemplos y resultados de interés.

A continuación, se muestra un conjunto de direcciones U para los cuales $R(U)$ es un anillo incluso cuando U no es semigrupo. Este ejemplo aparece en la referencia [5], aunque se ha completado con información de la referencia [4]:

Ejemplo 1.3.1. Sea $U = \{1, e^{\pi i/4}, i\}$, el cual no es un semigrupo, pues $e^{\frac{\pi i}{4}} i = e^{\frac{3\pi i}{4}} \notin U$. Se tiene que, partiendo de los puntos $\{0, 1\}$, el conjunto $R\left(1, e^{\pi i/4}, i\right)$ coincide con el anillo $\mathbb{Z}[i]$. Es fácil ver que esto ocurre en la figura 1.4, donde, tras varias iteraciones, observamos que los puntos construidos son de la forma $a + bi$ con $a, b \in \mathbb{Z}$. De hecho, veremos en el Capítulo 3 que esta construcción de origami genera los enteros de Gauss, que son un subanillo de $\mathbb{C}$, sin necesidad de que U sea un semigrupo.

Sin embargo, este y otros son algunos casos concretos pero no tenemos un resultado general que nos permita discernir la estructura de $R(U)$. Podríamos suponer que $R(U)$ es siempre un anillo, pero veremos que esto no se da necesariamente incluso si U posee tres direcciones, una de las cuales es 1. Resulta útil recordar para esta sección la fórmula (1.1):

$$I_{u,v}(p, q) = \frac{s_{u,p}}{s_{u,v}} v + \frac{s_{v,q}}{s_{v,u}} u. \tag{1.3}$$

Comenzamos enunciando entonces los resultados de interés introducidos anteriormente:

Teorema 1.3.2. *Sea $U = \{1, u, v\}$ con $u = e^{i\alpha}$ y $v = e^{i\beta}$ dados, donde $0 \neq \alpha \neq \beta \neq 0$* mód π. *Sea*

$$z := I_{u,v}(0, 1) = \frac{s_{v,1}}{s_{v,u}} u = I_{v,u}(1, 0).$$

Entonces se tiene que $R(U) = \mathbb{Z} + \mathbb{Z}z$.

Demostración. Como $1, z$ están en el grupo aditivo $R(U)$, tenemos entonces que $\mathbb{Z} + \mathbb{Z}z \subseteq R(U)$.

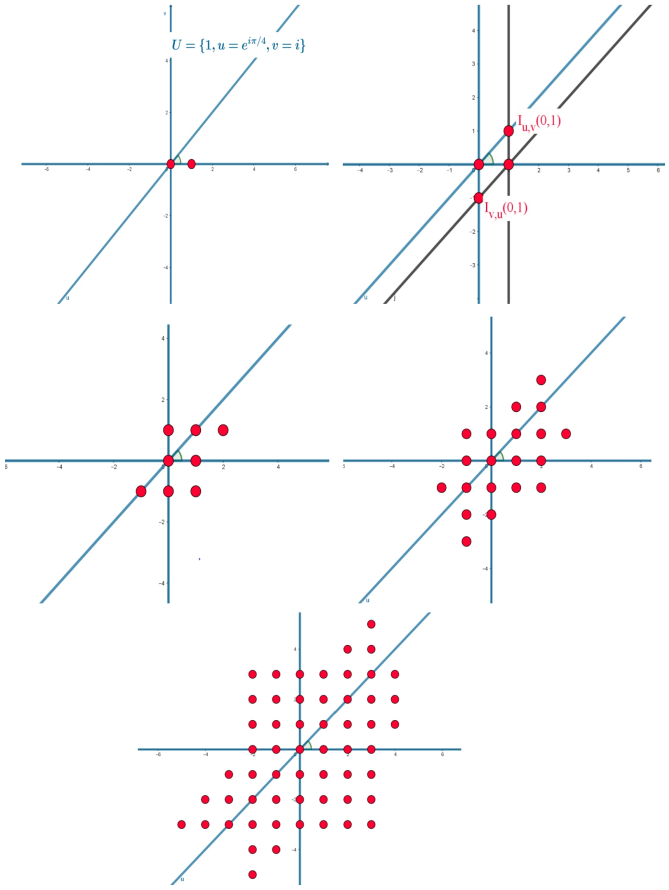


Figura 1.4: Construcción iterativa de M_4.

Probaremos la otra inclusión usando la definición 1.1.3, viendo que $M_j \subseteq \mathbb{Z} + \mathbb{Z}z$ por inducción en j, estrategia que es similar a la que seguimos en la demostración del teorema 1.2.4.

Comenzamos por el caso base $j = 0$, es decir, consideramos M_0, que definimos como $\{0, 1\}$, los cuales son enteros.

Tomamos ahora $s, t \in M_j$, y suponemos que entonces existen $a, b \in \mathbb{Z}$ tal que $s = a + bz$. Dado que $M_{j+1} = \{I_{u,v}(s,t)$ tal que $u, v \in U,\ s, t \in M_j\}$, basta con ver que $M_{j+1} \subseteq \mathbb{Z} + \mathbb{Z}z$ para concluir la prueba. Esto ocurrirá si y solo si

$$I_{u,v}(s,t) \in \mathbb{Z} + \mathbb{Z}z \text{ para cualesquiera } s, t \in M_j.$$

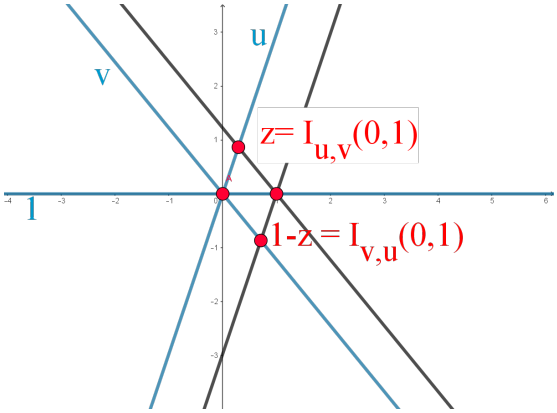


Figura 1.5: Construcción del punto z.

Usando las propiedades de la proposición 1.1.5, tendremos que

$$I_{u,v}(s,t) = I_{u,v}(s,0) + I_{u,v}(0,t) = I_{u,v}(s,0) + I_{v,u}(t,0).$$

Por tanto, si probamos que $I_{x,y}(s,0) \in \mathbb{Z} + \mathbb{Z}z$ para todos los pares $\{x,y\} \subseteq U$, al ser s un punto cualquiera y x, y dos direcciones cualesquiera de U, tendremos que el mismo razonamiento se puede aplicar a $I_{v,u}(t,0)$ tomando $s = t$ y concluiríamos la prueba. Entonces, considerando los posibles pares de elementos de U, bastaría probar que los siguientes seis puntos están en $\mathbb{Z} + \mathbb{Z}z$. Estos son:

$$I_{u,v}(s,0), \quad I_{v,u}(s,0), \quad I_{u,1}(s,0), \quad I_{v,1}(s,0), \quad I_{1,u}(s,0), \quad I_{1,v}(s,0).$$

Vemos entonces cuáles serían esos puntos y que efectivamente están en $\mathbb{Z} + \mathbb{Z}z$, teniendo en cuenta para los razonamientos la expresión de z, las propiedades de la proposición (1.1.5) y la hipótesis de inducción sobre s.

Además, dado que $\frac{s_{v,1}}{s_{v,u}} \in \mathbb{R}$, sabemos que

$$s_{u,z} = u\bar{z} - \bar{u}z = u\bar{u}\left(\frac{s_{v,1}}{s_{v,u}} - \frac{s_{v,1}}{s_{v,u}}\right) = 0, \tag{1.4}$$

y análogamente:

$$s_{v,z} = v\bar{z} - \bar{v}z = \frac{s_{v,1}}{s_{v,u}}(v\bar{u} - \bar{v}u) = s_{v,1}. \tag{1.5}$$

Por tanto:

- $I_{u,v}(s,0) = I_{u,v}(a+bz,0) = aI_{u,v}(1,0) + bI_{u,v}(z,0) = a(1-z) \in \mathbb{Z} + \mathbb{Z}z$, usando (1.4) y que

$$I_{u,v}(1,0) = \frac{s_{u,1}}{s_{u,v}}v = \frac{(u-\bar{u})v}{s_{u,v}} = \frac{(\bar{u}-u)v}{s_{v,u}}$$

coincide con

$$1 - z = 1 - \frac{s_{v,1}}{s_{v,u}}u = \frac{s_{v,u} - s_{v,1}u}{s_{v,u}} = \frac{v\bar{u} - \bar{v}u - vu + \bar{v}u}{s_{v,u}} = \frac{(\bar{u}-u)v}{s_{v,u}}.$$

Geométricamente puede verse en la figura 1.6.

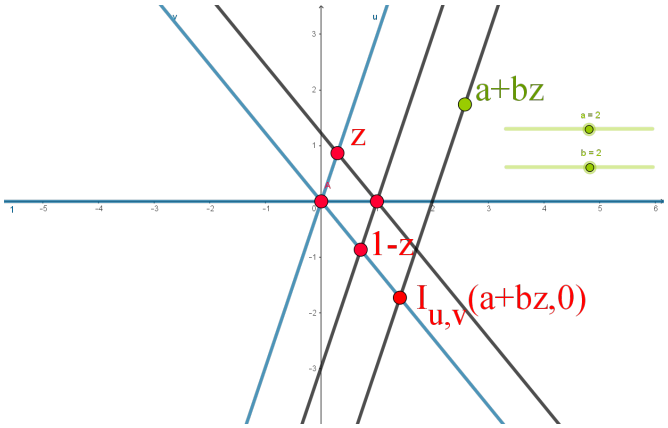


Figura 1.6: Construcción de $I_{u,v}(s,0)$.

- $I_{v,u}(s,0) = aI_{v,u}(1,0) + bI_{v,u}(z,0) = az + bz = (a+b)z \in \mathbb{Z} + \mathbb{Z}z$,
por la definición de z y porque $I_{v,u}(z,0) = I_{u,v}(0,z) = \frac{s_{v,z}}{s_{v,u}}u = \frac{s_{v,1}}{s_{v,u}}u = z$ por (1.5), además de que z está en la recta de dirección u que pasa por 0.
- $I_{u,1}(s,0) = aI_{u,1}(1,0) + bI_{u,1}(z,0) = a$,
ya que $I_{u,1}(1,0) = \frac{s_{u,1}}{s_{u,1}} \cdot 1 = 1$ e $I_{u,1}(z,0) = I_{1,u}(0,z) = \frac{s_{u,z}}{s_{u,1}} \cdot 1 = 0$ por (1.4).
- $I_{v,1}(s,0) = aI_{v,1}(1,0) + bI_{v,1}(z,0) = a + b$,
pues $I_{v,1}(z,0) = I_{1,v}(0,z) = \frac{s_{v,z}}{s_{v,1}} \cdot 1 = \frac{s_{v,1}}{s_{v,1}} = I_{1,v}(0,1) = 1$ por (1.5).
- $I_{1,u}(s,0) = aI_{1,u}(1,0) + bI_{1,u}(z,0) = bz$,
puesto que $I_{1,u}(1,0) = \frac{s_{1,1}}{s_{1,u}}u = 0$ e $I_{1,u}(z,0) = z$, pues z ya se encuentra en la recta de dirección u que pasa por 0. Podemos contemplar también este caso de forma geométrica en la figura 1.7.
- $I_{1,v}(s,0) = aI_{1,v}(1,0) + bI_{1,v}(z,0) = b(1-z)$,
porque $I_{1,v}(1,0) = 0$ e

$$I_{1,v}(z,0) = \frac{s_{1,z}}{s_{1,v}}v = \frac{\bar{z}-z}{\bar{v}-v}v = \frac{\bar{u}-u}{\bar{v}-v}\frac{s_{v,1}}{s_{v,u}}v = \frac{v\bar{u}-vu}{\bar{v}-v}\frac{s_{v,1}}{s_{v,u}} = \frac{uv-\bar{u}v}{v\bar{u}-\bar{v}u},$$

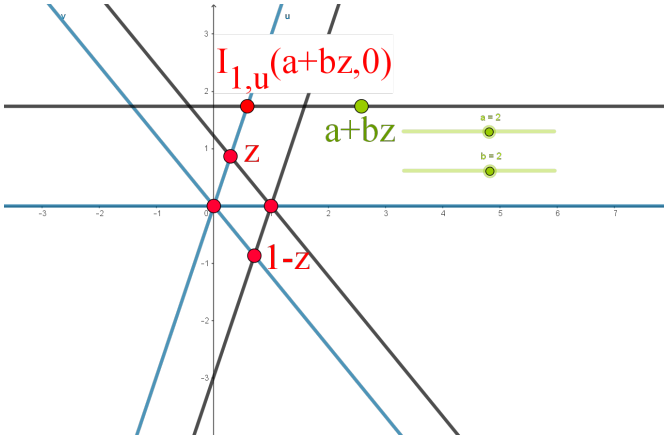


Figura 1.7: Construcción de $I_{1,u}(s,0)$.

y si desarrollamos

$$z-1=\frac{s_{v,1}}{s_{v,u}}u-1=\frac{(v-\bar{v})u-v\bar{u}+\bar{v}u}{s_{v,u}}=\frac{uv-\bar{u}v}{v\bar{u}-\bar{v}u},$$

obtenemos el resultado anterior. Luego $I_{1,v}(z,0)=z-1$.

Al haber visto que los seis puntos posibles están en $\mathbb{Z}+\mathbb{Z}z$, tenemos que entonces $R(U)\subseteq\mathbb{Z}+\mathbb{Z}z$. En conclusión, se da la igualdad entre ambos como queríamos probar.

En el teorema anterior estamos suponiendo que una de las direcciones de U es 1, veamos que esto se puede hacer sin pérdida de generalidad:

Sea $U=\{x,u,v\}$ un conjunto de tres direcciones diferentes y $M_0=\{0,1\}$. Definimos ahora $1':=I_{x,v}(0,1)$, y sabemos que mediante una transformación lineal podemos convertir M_0 en $\{0,1'\}$. Podemos asumir entonces que una de las direcciones equivale a 1, con lo cual, salvo una transformación lineal, hemos probado que $R(U)$ es de la forma $\mathbb{Z}+\mathbb{Z}z$ cuando U tiene exactamente 3 elementos.

El teorema anterior es uno de los principales de la referencia [5], pues demuestra que, dado un conjunto U de exactamente tres direcciones, $R(U)$ tiene siempre una estructura concreta como $\mathbb{Z}$-módulo.

A continuación, avanzamos un poco más y planteamos si es posible ver $R(1,u,v)$ como un anillo. Queremos saber entonces para qué direcciones distintas $u=e^{i\alpha}$, $v=$

$e^{i\beta}$ diferentes de 1 (mód$\{\pm 1\}$) se tendría que el conjunto $R(1,u,v) = \mathbb{Z} + \mathbb{Z}z$ es un anillo.

Partiendo de que la operación suma es cerrada en $R(1,u,v)$, tendremos que comprobar si el producto también lo es para que sea un anillo. Consideramos dos elementos del conjunto, que sabemos que también son elementos de $\mathbb{Z} + \mathbb{Z}z$ y vemos qué ocurre:

$$(a + bz)(c + dz) = ac + (ad + bc)z + bdz^2.$$

Por tanto, tendremos que $\mathbb{Z} + \mathbb{Z}z$ es cerrado bajo el producto si y solo si $z^2 \in \mathbb{Z} + \mathbb{Z}z$. Eso equivale a que existan $a, b \in \mathbb{Z}$ tal que z^2 sea un elemento de la forma $a + bz$, o lo que es lo mismo, que z verifique un polinomio de grado 2 sobre $\mathbb{Z}$. En particular, z tendría que ser un entero algebraico [4] de grado 2 sobre $\mathbb{Z}$.

A partir del razonamiento anterior, comentamos un ejemplo que aparece en la referencia que estamos usando y que, además, volverá a aparecer en un capítulo posterior del estudio. Para ello, recordemos que llamamos α y β a los argumentos de u y v, respectivamente:

Ejemplo 1.3.3. Consideramos $R(1,u,v)$ con $u = i$. Sabemos que $1, i$ son direcciones perpendiculares entre ellas, y sea $z := I_{i,v}(0,1) = ri$ para algún $r \in \mathbb{R}$, obtenido de la forma que se muestra en la imagen 1.8.

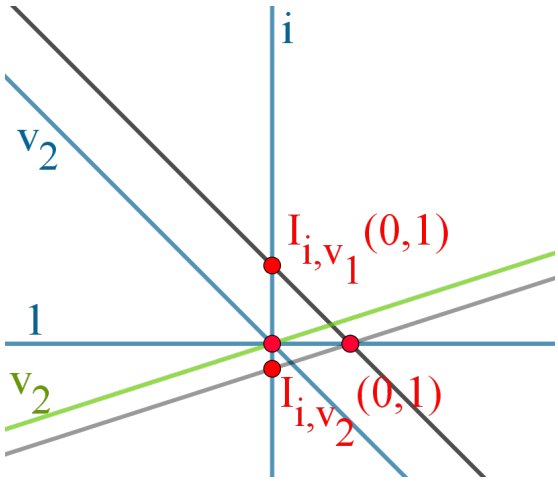


Figura 1.8: Puntos z imaginarios puros para cualquier valor de v.

Es posible llegar a que $r = \tan(\pi - \beta) = -\tan(\beta) \neq 0$ por ser $1, i, v$ direcciones distintas. Lo vemos gráficamente en 1.9.

[4] Un número complejo es un entero algebraico si y solo si es raíz de un polinomio mónico con

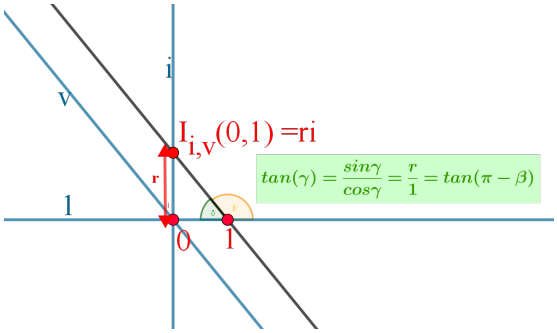


Figura 1.9: Valor de r usando el Teorema de Pitágoras.

En ese caso, para que $\boldsymbol{R}(1, u, v)$ sea anillo, $z^2 = (ri)^2 = -(\tan\beta)^2$ debe ser un entero, es decir, $\tan\beta = \sqrt{d}$ con $d \in \mathbb{Z}_{>0}$. La igualdad anterior es equivalente a que $\beta = \arctan\sqrt{d}$ con d un entero positivo. En tal caso, tendremos ya una expresión para v, que será $v = e^{i\arctan\sqrt{d}}$, y $\boldsymbol{R}(1, i, v) = \mathbb{Z} + \mathbb{Z}(\tan\beta)i = \mathbb{Z} + \mathbb{Z}\sqrt{-d}$.

Continuamos ahora con una condición necesaria para que $\boldsymbol{R}(\boldsymbol{U})$ sea anillo, que se obtiene siguiendo el hilo argumental del principio de esta sección.

Proposición 1.3.4. En las condiciones anteriores, si $\boldsymbol{R}(\boldsymbol{U})$ es anillo, entonces necesariamente debe ocurrir que $\cos^2\alpha \in \mathbb{Q}$.

Demostración. Volvemos a considerar el número complejo $z = I_{u,v}(0, 1)$, que no puede ser real porque por definición va a estar fuera de la recta que une 0 y 1. El polinomio mínimo de z sobre $\mathbb{R}$ será $(x - z)(x - \bar{z}) = x^2 - (z + \bar{z})x + z\bar{z}$. Dado que z es entero sobre $\mathbb{Z}$ de grado 2, el polinomio sobre $\mathbb{Z}$ que verifica z, siendo de grado 2 y mónico, debe coincidir con el mínimo sobre $\mathbb{R}$, que también es de grado dos porque z no es real. De esta forma, tenemos que $\boldsymbol{R}(\boldsymbol{U})$ es un anillo si se cumple:

$$k := z + \bar{z} = 2\boldsymbol{Re}(z) \in \mathbb{Z},$$
$$m := z\bar{z} = |z|^2 = \in \mathbb{Z}.$$

Nos conviene introducir de alguna forma los ángulos α y β en nuestro razonamiento para llegar al objetivo que queremos probar. A tal efecto, consideramos las siguientes igualdades trigonométricas:

$$\frac{\boldsymbol{Im}(z)}{\boldsymbol{Re}(z)} = \tan\alpha \quad \text{y} \quad \frac{\boldsymbol{Im}(z)}{1 - \boldsymbol{Re}(z)} = -\tan\beta,$$

coeficientes en $\mathbb{Z}$.

que pueden observarse con ayuda de la figura 1.10.

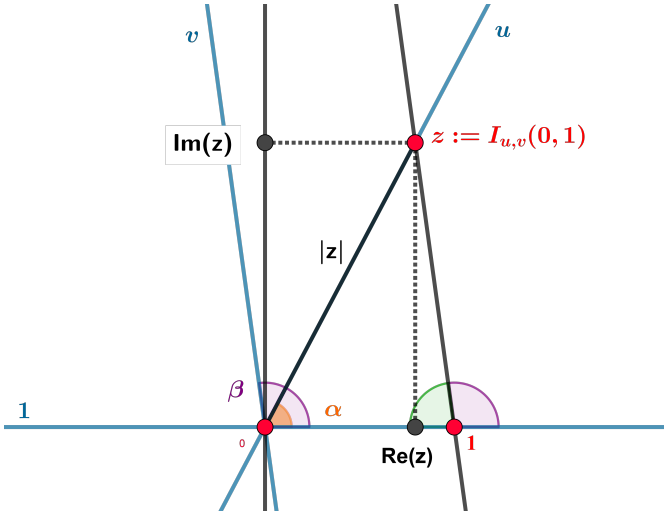


Figura 1.10: Construcción del punto z a partir de α y β.

Despejando $Im(z)$ en cada caso e igualando ambas expresiones llegamos a que:

$$Re(z) = \frac{\cos\alpha \ \sin\beta}{\sin(\beta - \alpha)},$$

y en consecuencia,

$$Im(z) = \frac{\sin\alpha \ \sin\beta}{\sin(\beta - \alpha)}.$$

Teniendo en cuenta todo lo anterior, $R(U)$ será un anillo bajo las siguientes condiciones:

$$k = 2Re(z) = 2\frac{\sin\beta \ \cos\alpha}{\sin(\beta - \alpha)} \in \mathbb{Z},$$
$$m = |z|^2 = \frac{\sin^2\beta}{\sin^2(\beta - \alpha)} \in \mathbb{Z}.$$

Si las relacionamos entre ellas, tenemos que $k/2 = Re(z) = \cos\alpha\sqrt{m}$, o lo que es lo mismo, $\cos\alpha = \frac{k}{2\sqrt{m}}$. En tal situación, debe ocurrir que $\cos^2\alpha = \frac{k^2}{4m}$ sea un número racional.

Por tanto, si $R(U)$ es anillo, $\cos^2\alpha \in \mathbb{Q}$, y por simetría, $\cos^2\beta \in \mathbb{Q}$.

Sin embargo, no es una propiedad suficiente para probar que $R(U)$ es anillo. Un claro contraejemplo es el caso de $R(1, e^{\pi i/3}, e^{5\pi i/6})$, donde $z = \frac{1}{4} + \frac{\sqrt{3}}{4}i$. Observamos que $\cos \pi/3 = \frac{1}{2}$, pero $k = \frac{1}{2} \notin \mathbb{Z}$.

Si endurecemos un poco la condición a que $\cos \alpha \in \mathbb{Q}$, entonces es suficiente para afirmar que, en tal caso, existe un ángulo β tal que el $R(U)$ correspondiente es un anillo. Veamos ese resultado:

Proposición 1.3.5. Para infinitos pares u, v de direcciones el conjunto $R(1, u, v)$ es un anillo.

Demostración. Para probarlo, suponemos que $\cos \alpha = \frac{s}{t}$ y sin pérdida de generalidad $s, t \in \mathbb{Z}$ primos relativos. Sea entonces $Re(z) = s$ y $|z| = t$, con $t > 0$. Es posible expresar z como $z = s + i\sqrt{t^2 - s^2}$, usando la construcción de z de la figura 1.11 y el Teorema de Pitágoras.

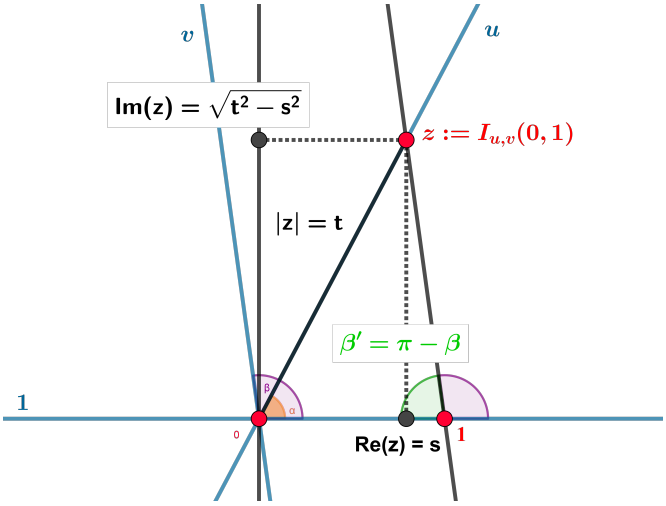


Figura 1.11: Construcción del punto z.

Además, como β y β' son suplementarios, tienen tangentes opuestas. Por lo que si $\tan(\beta') = \frac{\sqrt{t^2-s^2}}{1-s}$, llegamos a que $\beta' = \arctan\left(\frac{\sqrt{t^2-s^2}}{1-s}\right)$, y por tanto, $\beta = -\arctan\left(\frac{\sqrt{t^2-s^2}}{1-s}\right) = \arctan\left(\frac{\sqrt{t^2-s^2}}{s-1}\right)$. Luego para todo α tal que $\cos \alpha \in \mathbb{Q}$ podemos encontrar β tal que $R(1, u = e^{i\alpha}, v = e^{i\beta})$ es un anillo, pues en este contexto, z verifica una ecuación de grado 2 cuyos coeficientes son enteros, por la discusión posterior al teorema 1.3.2. ∎

Nótese que si sólo se cumple la condición de que $\cos \alpha$ sea racional, entonces no tendremos una condición suficiente para que $R(1, u, v)$ sea un anillo, basta volver al

contraejemplo anterior a esta proposición para comprobarlo.

En el caso de que s, t no sean primos relativos, solo obtendríamos un subanillo de $\mathbb{Z} + \mathbb{Z}z$. Presentamos un ejemplo en el que ello ocurre:

Ejemplo 1.3.6. Supongamos que $mcd(s,t) = 2$, lo que nos daría lugar a la situación descrita en la figura 1.12.

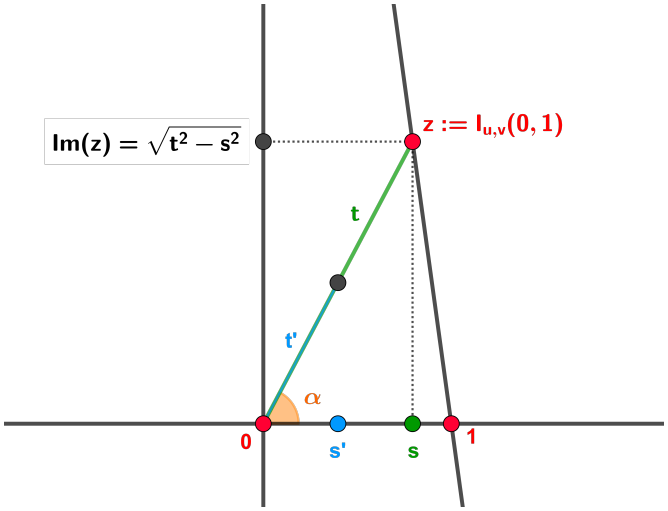


Figura 1.12: Caso de s y t no coprimos.

Es posible tomar entonces $s' = s/2$ y $t' = t/2$ y tendríamos que $\cos\alpha = \frac{s}{t} = \frac{s'}{t'}$. Evidentemente, $z' \in \mathbb{Z} + \mathbb{Z}z$, por tanto, obtenemos un subanillo de $\mathbb{Z} + \mathbb{Z}z$. Es más, cada forma de expresar el cociente $\frac{s}{t}$ nos daría un subanillo también.

Por último, cabe destacar que hasta ahora hemos trabajado con conjuntos U de tres elementos. Resulta interesante preguntarnos qué ocurre si U está formado por cuatro o más direcciones, otro de los enfoques de la referencia [5] que se trata a continuación.

1.4 Densidad con al menos cuatro direcciones

De nuevo, salvo una transformación lineal, podemos suponer que estamos trabajando con un conjunto $R(1, u, v, w)$ con todas sus direcciones diferentes entre ellas. Además, podemos tomar u, v, w tales que $u = e^{i\alpha}$, $v = e^{i\beta}$ y $w = e^{i\gamma}$ con $0 < \alpha < \beta < \gamma < \pi$. Sea

$$p := I_{u,w}(0,1) \quad y \quad r := I_{1,v}(p,0).$$

Observamos que en la recta horizontal que pasa por p, denotada por $L_1(p)$, se tiene que $r < p$ teniendo en cuenta la parte real de cada punto. De ahí deducimos que, al ser $L_w(r)$ y $L_w(p) = L_w(1)$ paralelas, el punto $I_{1,w}(0, r)$ es menor que 1.

De hecho, como $\beta < \gamma$, encontramos que $I_{1,w}(p, 0) < r$ en $L_1(p)$. Esto, unido a lo anterior, nos lleva a que $I_{1,w}(p, 0) < r < p$ en esa recta. Usando que el menor de los tres puntos anteriores está también en la recta $L_w(0)$, y que esta es paralela a $L_w(r)$, llegamos a que $I_{1,w}(0, r) > 0$.

Todos estos puntos y rectas hasta ahora construidos los adjuntamos en el siguiente gráfico:

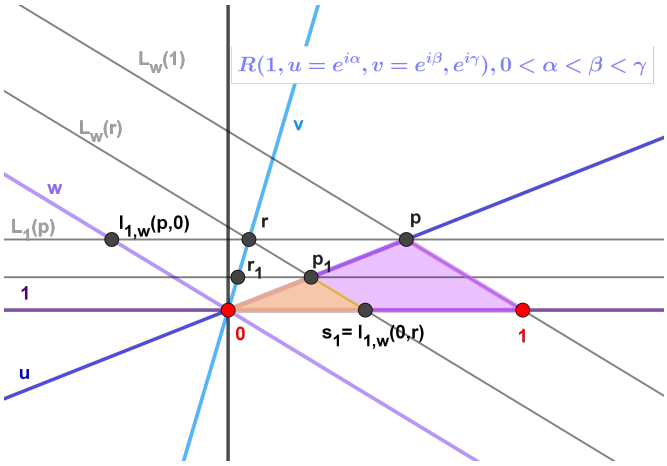


Figura 1.13: Construcción de los puntos principales.

Si nos fijamos en la figura anterior, resulta fácil comprobar que el triángulo $0p1$ es semejante al $0p_1s_1$, donde

$$p_1 := I_{u,w}(0, r) \quad y \quad s_1 := I_{1,w}(0, r).$$

Tal punto s_1 es el que, en párrafos anteriores, vimos que estaba entre 0 y 1, por lo que $p_1 \in (0, p)$ y $s_1 \in (0, 1)$.

Usando el punto p_1, somos capaces de construir otro punto en $L_v(0)$, que será $r_1 := I_{1,v}(p_1, 0)$. Además, $r_1 \in (0, r)$, pues $p_1 \in (0, p)$.

Es entonces cuando, gracias a las direcciones y puntos anteriores, podemos construir también

$$p_2 := I_{u,w}(0, r_1) \quad y \quad s_2 := I_{1,w}(0, r_1),$$

donde $p_2 \in (0, p_1)$, $s_2 \in (0, s_1)$.

Si repetimos de nuevo el proceso, creamos nuevos puntos de forma iterativa. Gracias a ello, somos capaces de formar las sucesiones $\{p_i\}_{i\geq 0}$ y $\{s_i\}_{i\geq 0}$ (además de la $\{r_i\}_{i\geq 0}$ auxiliar) cuyos términos se detallan a continuación:

$$p_i := I_{u,w}(0, r_{i-1}), \quad s_i := I_{1,w}(0, r_{i-1}), \quad r_{i-1} := I_{1,v}(p_{i-1}, 0).$$

Para cada $i = 1, 2, 3 \ldots$, tenemos que los triángulos $0p_is_i$ y $0p1$ son semejantes, y además, se van haciendo cada vez más pequeños en módulo. Los puntos de cada sucesión son diferentes entre ellos porque se encuentran en direcciones distintas del plano, por lo que están bien definidos. Por último, es fácil ver que las tres sucesiones de puntos convergen a 0, aunque realmente las que más nos interesan son las dos primeras. Adjuntamos una figura obtenida a partir de la anterior, con algunas iteraciones más, donde podemos ver gráficamente lo que acabamos de explicar:

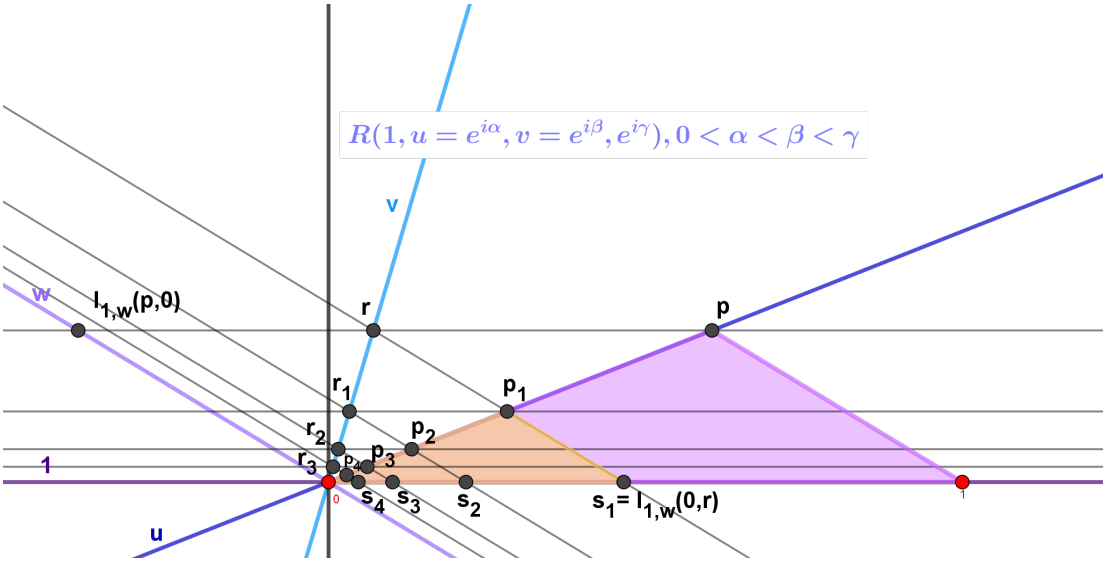


Figura 1.14: Construcción de las sucesiones.

Acabamos de ver entonces que existen dos sucesiones convergentes en dos direcciones linealmente independientes en $R(U)$, lo cual volveremos a usar más adelante.

Veamos ahora que en estas condiciones, tendremos que $R(1, u, v, w)$ es denso en $\mathbb{R}^2$. Para que eso ocurra, necesitamos probar que la clausura topológica de $R(U)$, que podemos denotar por X, coincide con el propio $\mathbb{R}^2$. El siguiente lema de la referencia [6, 8.6, p. 83] nos propicia tal resultado:

Lema 1.4.1. Sea X un subgrupo cerrado de $\mathbb{R}^2$, que no esté contenido en una recta.

Entonces existe una base b, b' de $\mathbb{R}^2$ tal que X coincide con uno de los tres conjuntos siguientes:

1. $\mathbb{R}b + \mathbb{R}b' = \mathbb{R}^2$.
2. $\mathbb{R}b + \mathbb{Z}b'$.
3. $\mathbb{Z}b + \mathbb{Z}b'$.

Teorema 1.4.2. *La clausura topológica de $R(U)$ coincide con $\mathbb{R}^2$. En consecuencia, $R(1, u, v, w)$ es denso en $\mathbb{R}^2$.*

Demostración. Suponiendo que $X = \overline{R(U)}$ cumple las hipótesis del lema anterior, intentaremos ver cuál de las tres opciones de dicho lema se corresponde con tal clausura.

Si X fuese $\mathbb{Z}b + \mathbb{Z}b'$, tendríamos un conjunto de puntos discretos, con lo cual habría entornos de 0 sin otros elementos de X (y de $R(U)$, por tanto). Esto hace que no contemplemos entonces este caso, ya que anteriormente hemos visto que en cualquier entorno de 0 podemos encontrar infinitos elementos de $R(U)$, pues existen dos sucesiones convergentes a tal punto.

Podría darse que X coincidiera con $\mathbb{R}b + \mathbb{Z}b'$, pero solo en el caso de que ambas sucesiones convergiesen a 0 y sus términos fuesen linealmente dependientes, es decir, se encontraran en la misma dirección. Sin embargo, tampoco se da tal situación, dado que antes comentamos que los elementos de cada una estaban en rectas independientes entre ellas.

Finalmente, concluimos que necesariamente X debe ser $\mathbb{R}^2$. Falta entonces ver que estamos en las hipótesis del lema.

Sabemos que, por definición, X es topológicamente cerrado. Además, no está contenido en una recta porque tenemos tres puntos que originan las sucesiones que no son colineales. Finalmente, aunque es conocido que la clausura de un subgrupo de un grupo topológico sigue siendo un grupo, en este caso podemos probarlo de una forma más sencilla:

En $\mathbb{R}^2$, la clausura son los puntos límite de sucesiones cuyos términos pertenecen a ciertos grupos, en este caso, a $R(U)$. Entonces, como es no vacía, tendríamos que ver que la diferencia de esos puntos límite pertenece a la clausura y así tendríamos que X es un grupo con la suma, al igual que $R(U)$. Sean entonces $Y, Z \in X$ los puntos límite de las sucesiones $\{Y_n\}_{n\geq 1}, \{Z_n\}_{n\geq 1}$, respectivamente, cuyos términos están en $R(U)$. Dado que sabemos que restar ambas sucesiones equivale a restar sus términos,

al ser $R(U)$ grupo, tendremos que la sucesión $\{Y_n - Z_n\}_{n\geq 1}$ está en $R(U)$. Esto nos lleva a que entonces, su punto límite, que es $Y - Z$, estará en X.

Concluimos que se cumplen todas las hipótesis, y que, en consecuencia, $R(1, u, v, w)$ es denso en $\mathbb{R}^2$ como queríamos probar. De hecho, el lema anterior nos da la existencia de una base b, b' de $\mathbb{R}^2$, y al ser los vectores $0s_1$ y $0p_1$ independientes, podríamos tomarlos como base para ver un caso particular de los elementos de X si lo deseamos.

Damos por finalizado entonces este primer capítulo introductorio a nuestro objeto de estudio y pasamos entonces a ver algunos casos particulares interesantes en los siguientes.

2 | Anillos ciclotómicos

Ahora vamos a considerar el caso en el que U es, al menos, un **semigrupo** de direcciones de cardinal finito. Concretamente, trabajaremos con el **grupo cíclico** de direcciones generado por $e^{i\pi/n}$, denotado por U_n. Nótese que para este desarrollo nos basaremos en la referencia [3] de nuevo. Además, introducimos un resultado que nos será de ayuda en este capítulo:

Lema 2.0.1. $R(U)$ es el menor subanillo de $\mathbb{C}$ que contiene todos los elementos de la forma

$$\frac{1-a}{1-b}$$

donde a, b son elementos de U^2 no triviales. Además, todos los monomios son invertibles.

Demostración. Consideramos la definición de monomio primitivo y desarrollamos la expresión usando (1.1):

$$\begin{aligned} I_{u,v}(1,0) = \frac{s_{u,1}}{s_{u,v}} v = \frac{u-\bar{u}}{u\bar{v}-\bar{u}v} v = \frac{(u-\bar{u})|v|}{u(\bar{v})^2-\bar{u}|v|} = \frac{u-\bar{u}}{u(\bar{v})^2-\bar{u}} \\ = \frac{u^2-|u|}{u^2(\bar{v})^2-|u|} = \frac{u^2-1}{(u/v)^2-1}. \end{aligned}$$

Dado que u, v son elementos de U, sus cuadrados lo son de U^2. Por tanto, tenemos que los monomios primitivos pueden expresarse como $\frac{1-a}{1-b}$ con $a, b \in U^2$. Es más, dado que en este caso $R(U)$ se construye a partir de los monomios primitivos (como comentamos al final de la Sección 1.2), cualquier anillo que los contenga contendrá a $R(U)$ también. De este modo, $R(U)$ es el anillo más pequeño que contiene a los elementos de esta forma.

Por otro lado, si cambiamos a por b en el cociente anterior obtenemos el inverso de tal elemento. Esto nos lleva a que los monomios primitivos son unidades en $R(U)$.

Además, como cualquier monomio es producto de monomios primitivos por definición y el producto de unidades es una unidad, cualquier monomio es una unidad.

Recordamos ahora que la extensión ciclotómica $\mathbb{Q}(\zeta_n)$ es el menor subcuerpo de $\mathbb{C}$ que contiene la raíz primitiva n-ésima de la unidad $\zeta_n := e^{2\pi i/n}$.

En estos términos, tomamos ahora el grupo U (que es subgrupo de $T/\{\pm 1\}$) como U_n, el generado por $\zeta_{2n} = e^{i\pi/n}$. En consecuencia, U_n^2 tendría como generador $\zeta_n = e^{2\pi i/n}$.

Como ese grupo U_n tendrá al menos tres direcciones, por el teorema 1.2.4, sabemos que $R(U_n)$ en este caso es un anillo de $\mathbb{C}$ y podemos relacionarlo con $\mathbb{Q}(\zeta_n)$ mediante el siguiente resultado.

Proposición 2.0.2. El anillo $R(U_n)$ es un subanillo de $\mathbb{Q}(\zeta_n)$.

Demostración. Como ambos son anillos, solo será necesario probar que los elementos de $R(U_n)$ pueden expresarse como polinomios en ζ_n con coeficientes racionales. En particular, dado que al ser U_n un grupo sabemos que $R(U_n)$ está generado como anillo por los monomios primitivos, basta comprobar que estos están en $\mathbb{Q}(\zeta_n)$.

Usando el lema 2.0.1, y sabiendo que los elementos de U_n^2 están generados por ζ_n como comentábamos anteriormente, tenemos lo que queremos. Esto se debe a que al ser ζ_n una raíz de la unidad, $\frac{1}{1-\zeta_n}$ es un polinomio en ζ_n.

Vamos a ver ahora que además $R(U_n)$ tiene una expresión concreta como subanillo de $\mathbb{Q}(\zeta_n)$, según n sea primo o no.

Para ello, vamos a usar el lema 2.0.1 y consideraremos los monomios primitivos de $R(U_n)$ como cocientes de la forma

$$m_{a,b} := \frac{(1-\zeta_n^a)}{(1-\zeta_n^b)},$$

los cuales además son ejemplos de unidades ciclotómicas de $\mathbb{Q}(\zeta_n)$.

Observación 2.0.3. Recordamos que, dado que tenemos la igualdad:

$$X^n - 1 = \prod_{k=0}^{n-1} (X - \zeta_n^k),$$

es posible llegar a la expresión:

$$n = \prod_{k=1}^{n-1} (1 - \zeta_n^k) \tag{2.1}$$

simplemente dividiendo lo anterior por $X - 1$ y tomando X igual a 1.

Veamos entonces el teorema que nos da las expresiones explícitas antes comentadas.

Teorema 2.0.4. *Sea $n \geq 3$, y sean $U = U_n$ y $\zeta = \zeta_n$. Se tiene:*

1. *El anillo $R(U)$ contiene a ζ.*
2. *Cualquier elemento del anillo $R(U)$ está en el anillo $\mathbb{Z}[\zeta, 1/n]$.*
3. *Si n es primo, entonces $R(U) = \mathbb{Z}[\zeta]$.*
4. *Si n no es primo, entonces $R(U) = \mathbb{Z}[\zeta, 1/n]$.*

Demostración. En primer lugar, vamos a probar que $\mathbb{Z}[\zeta] \subset R(U)$. Como $\mathbb{Z} \subset R(U)$ (pues $0, 1 \in R(U)$ por definición) y además $R(U)$ es un anillo, basta ver que $-\zeta$ o ζ está en $R(U)$. Para ello, usaremos que $-1 \in R(U)$ y que

$$\frac{1-\zeta}{1-\zeta^{-1}} = \frac{1-\zeta}{\frac{\zeta-1}{\zeta}} = -\zeta \quad \in R(U).$$

A continuación, veremos que $R(U) \subset \mathbb{Z}[\zeta, 1/n]$. Si consideramos la expresión (2.1), observamos que se tiene que $1 - \zeta^a$ divide a n si a no es congruente con 0 módulo n. Si tomamos entonces un monomio primitivo de $R(U)$ de la forma $m_{a,b}$ y despejamos el denominador en una expresión como la (2.1), llegamos a que:

$$1 - \zeta^b = \frac{n}{\prod_{k=1,k\neq b}^{n-1}(1-\zeta^k)},$$

y sustituyendo en $m_{a,b}$ tendremos entonces que:

$$m_{a,b} = \frac{1-\zeta^a}{\frac{n}{\prod_{k=1,k\neq b}^{n-1}(1-\zeta^k)}} = \frac{(1-\zeta^a)\prod_{k=1,k\neq b}^{n-1}(1-\zeta^k)}{n}.$$

Es decir, cualquier monomio primitivo de $R(U)$ puede escribirse como un polinomio en ζ con coeficientes enteros dividido por n. En consecuencia, como cualquier elemento de $R(U)$ es un polinomio de coeficientes enteros en los monomios primitivos, tenemos la inclusión buscada.

Para el tercer apartado supondremos que n es primo, y volveremos a considerar el monomio $m_{a,b}$ aprovechando que un b cualquiera es coprimo con n, por ser n primo. Usando la identidad de Bézout, llegaríamos a la ecuación $a = rb - sn$ con $r, s \in \mathbb{Z}$. En ese caso, y aplicando esto al monomio siguiente, tendríamos que:

$$\frac{1-\zeta^a}{1-\zeta^b} = \frac{1-\zeta^{a+sn}}{1-\zeta^b} = \frac{1-\zeta^{rb}}{1-\zeta^b}$$

y como rb es múltiplo de b, sabemos que ese cociente puede expresarse entonces como un polinomio en ζ con coeficientes enteros. De ahí que ya tengamos una de las inclusiones, y la contraria se tendría por el apartado (1) probado anteriormente.

Finalmente, para probar la igualdad de anillos $\boldsymbol{R}(\boldsymbol{U}) = \mathbb{Z}[\zeta, 1/n]$ cuando n no es primo, usaremos la doble inclusión. Por el apartado (2) tenemos una de ellas, y para probar la otra basta con ver que $1/n \in \boldsymbol{R}(\boldsymbol{U})$, pues $1 \in \boldsymbol{R}(\boldsymbol{U})$ por ser anillo y $\zeta \in \boldsymbol{R}(\boldsymbol{U})$ por el apartado (1).

Es suficiente ver que $1/p \in \boldsymbol{R}(\boldsymbol{U})$ para cualquier primo p que divida a n. Además, como n no es primo, o bien es el producto de dos o más primos distintos con exponente 1, o bien es múltiplo de alguna potencia de un primo. Con lo cual podemos dividir la prueba en dos casos, uno en el que p^2 divide a n y otro en el que existe otro primo q tal que pq divide a n.

Para el primer caso, podemos suponer $n = p^2m$. Tenemos entonces que $\zeta_{p^2} = \zeta_n^m$, en particular, cualquier cociente de esta forma $\frac{1-\zeta_{p^2}^a}{1-\zeta_{p^2}^b}$ está en $\boldsymbol{R}(\boldsymbol{U})$, por lo que el producto de ellos también lo estará. Ayudándonos de esas expresiones veamos si podemos obtener $\frac{1}{p}$, que es a lo que queremos llegar.

Usando la expresión (2.1) para $n = p^2$, tenemos que:

$$p^2 = \prod_{k=1}^{p^2-1}(1-\zeta_{p^2}^k),$$

donde hay $\Phi(p^2) = p(p-1)$ términos donde k es coprimo con p, y $p-1$ términos donde k es divisible por p.

Tomamos primero el producto estos últimos términos, es decir,

$$\prod_{k=1}^{p-1}(1-\zeta_{p^2}^{kp}),$$

donde usando que $\zeta_{p^2}^p = e^{\frac{2\pi ip}{p^2}} = \zeta_p$, podemos afirmar que lo anterior es equivalente a

$$\prod_{k=1}^{p-1}(1-\zeta_p^k) = p.$$

Ahora, vemos qué ocurre con los k coprimos con p. Como p^2 se puede descomponer en los términos tal que k es coprimo con p y en los divisibles por p y sabemos que este último producto es p, despejando el producto que nos interesa en este caso llegamos a que

$$\prod_{k=1,p\nmid k}^{p^2-1}(1-\zeta_{p^2}^k) = \frac{p^2}{p} = p.$$

De ambos razonamientos, cabe considerar el desarrollo en monomios primitivos siguiente, que nos llevará a la expresión que buscamos:

$$\prod_{k=1,p\nmid k}^{p^2-1}\frac{1-\zeta_{p^2}^k}{1-\zeta_{p^2}^{pk}} = \prod_{k=1,p\nmid k}^{p^2-1}\frac{1-\zeta_{p^2}^k}{1-\zeta_p^k},$$

podemos ver que hay p bloques de la forma $1, 2, \dots, p-1|p+1, p+2, \dots, 2p-1|\dots$ donde el numerador no se repite y el denominador sí. Por tanto, el denominador estará elevado a p por cada repetición por bloques; y el numerador irá cambiando. Como por lo anterior sabemos que ambos productos dan p, tendremos que:

$$\prod_{k=1,p\nmid k}^{p^2-1}\frac{1-\zeta_{p^2}^k}{1-\zeta_p^k} = \frac{p}{p^p} = \frac{1}{p^{p-1}} \in R(U).$$

Al tener entonces ese elemento y multiplicarlo por p^{p-2}, que es entero, llegaríamos a que $1/p$ está en $R(U)$.

Consideremos ahora el caso en el que n es divisible al menos por dos primos distintos p y q. De nuevo, es suficiente contemplar el caso $n = pq$. Sustituyendo ese n particular en la expresión (2.1) tenemos que:

$$pq = \prod_{k=1}^{pq-1}(1-\zeta_{pq}^k).$$

Observamos que ahora podemos dividir términos del producto en tres tipos: aquellos tal que k es coprimo con p y q, k es divisible por p o k es divisible por q.

Veamos cuánto salen los productos en cada caso. Comenzamos por los términos tales que k es divisible por p. Esos serán los de la forma $p, 2p, \dots, (q-1)p$, donde entonces el producto será

$$\prod_{k=1}^{q-1}(1-\zeta_{pq}^{kp}) = \prod_{j=1}^{q-1}(1-\zeta_q^j) = q.$$

Análogamente, si tenemos en cuenta que los términos tales que k es divisible por q, los posibles índices que encontraremos serán $q, 2q, \dots, (p-1)q$, de donde, al igual que antes:

$$\prod_{k=1}^{p-1}(1-\zeta_{pq}^{kq}) = \prod_{j=1}^{p-1}(1-\zeta_p^j) = p.$$

Llegamos a que en esta situación, pq se factoriza como un producto de términos que es igual a p, y otro que es igual a q, luego el producto de los términos restantes debe ser 1 forzosamente para que se cumpla la igualdad. Esto quiere decir que los términos $(1-\zeta_{pq}^k)$ con k coprimo con p, q son invertibles. En particular, 1 pertenece a los últimos exponentes mencionados y $1-\zeta_{pq}$ es una unidad. Esto quiere decir que el monomio

$$\prod_{j=1}^{p-1}\frac{1-\zeta_{pq}}{1-\zeta_{pq}^{qk}} = \frac{u}{p} \in R(U),$$

usando que el producto de unidades es unidad. Y por tanto, si multiplicamos por el inverso de u, tendremos que $1/p \in R(U)$ como queríamos probar.

En conclusión, hemos visto de ambas formas que $1/p \in R(U)$ y en tal caso tendremos que $\mathbb{Z}[\zeta_n, 1/n] \subset R(U)$, que junto al apartado (2) termina la prueba.

Un caso particular del teorema anterior es el caso de $n = 3$, en el que U_3 es el grupo cíclico generado por $\zeta_{2n} = \zeta_6$. Entonces se tiene que $R(U_3) = \mathbb{Z}[\zeta_3]$, por ser 3 primo, como puede verse geométricamente en la figura 2.1. Un enfoque alternativo de lo que acabamos de comentar se encuentra en el capítulo 3, dado que $\mathbb{Z}[\zeta_3]$ es el anillo de enteros de una extensión cuadrática en el caso de $d \equiv 1 \mod 4$ (concretamente $d = -3$). Por tanto, tendremos que tal anillo coincide con $R(U_3) = R(1, e^{i\theta}, e^{i(\pi-\theta)})$, donde $\theta = arg(1+\sqrt{-3}) = \pi/3$.

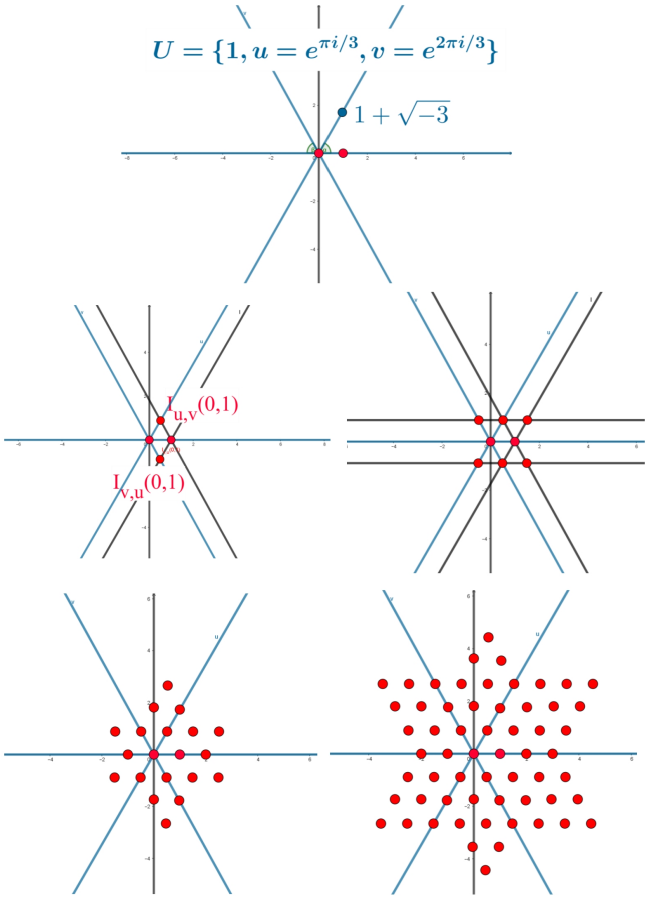


Figura 2.1: Construcción iterativa de puntos de $R(U)$.

3 | Anillos de enteros cuadráticos

Hasta ahora hemos visto propiedades en general y cómo se obtienen a partir de un grupo cíclico finito los anillos de origami relacionados con extensiones ciclotómicas.

En este capítulo, como se plasma en las referencias [4] y [5], vamos a estudiar los anillos de enteros de extensiones cuadráticas. Destaquemos que la referencia [5] nos demuestra que imponiendo propiedades sobre $1, u, v$ podemos obtener un anillo de enteros cuadrático. Sin embargo, el artículo [4] va más allá y prueba que **todo** anillo de enteros cuadrático se puede expresar como $R(1, u, v)$ para ciertos $\{1, u, v\}$ concretos. Usaremos por tanto ese enfoque en nuestro estudio porque cubre todos los anillos de enteros cuadráticos.

En primer lugar, recordamos que toda extensión cuadrática imaginaria se puede escribir de manera única como $\mathbb{Q}(\sqrt{d})$, siendo d un entero negativo libre de cuadrados[1]. Denotamos por $\mathcal{O}(\mathbb{Q}(\sqrt{d}))$ al anillo de enteros algebraicos en $\mathbb{Q}(\sqrt{d})$. Nos interesa tener en cuenta algunos resultados generales sobre tales anillos, que vemos a continuación.

Recordamos que si $\delta = a + b\sqrt{d}$ es un elemento de $\mathbb{Q}(\sqrt{d})$ que no es racional, podemos considerar el polinomio mínimo $x^2 + 2ax + (a^2 - b^2 d)$ de δ sobre $\mathbb{Q}$, del cual δ y $\bar{\delta} = a - b\sqrt{d}$ son raíces. En este apartado, cuando hablemos de conjugación nos referiremos a la aplicación que manda cualquier δ en $\bar{\delta}$.

Lema 3.0.1. En las condiciones anteriores, $\delta = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, con $a, b \in \mathbb{Q}$, es entero sobre $\mathbb{Z}$ si y solo si también lo es $\bar{\delta}$. En ese caso, $2a$ y $a^2 - b^2 d$ son enteros.

Demostración. Tomamos cualquier polinomio $p(x)$ con coeficientes enteros tal que δ sea raíz suya. Como la conjugación en el sentido anterior es un homomorfismo de $\mathbb{Q}$-álgebras, se tiene que $0 = \overline{p(\delta)} = p(\bar{\delta})$.

[1] Un número entero se dice libre de cuadrados si no es divisible por ningún p^2, con p primo.

Luego cualquier polinomio con coeficientes enteros que tenga a δ como raíz, también tendrá a $\bar{\delta}$.

En particular, $s := \delta + \bar{\delta}$ y $p := \delta\bar{\delta}$ también están en $\overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{d})}$, que es como denotamos a la clausura entera de $\mathbb{Z}$ en $\mathbb{Q}(\sqrt{d})$ [2]. De hecho, tenemos que $s = 2a$, $p = a^2 - b^2 d$.

Por otro lado, δ y $\bar{\delta}$ verifican la ecuación $t^2 - st + p = 0$, la cual, a priori, tiene sus coeficientes en $\mathbb{Q}$. Luego $s, p \in \mathbb{Q}$.

Gracias a los dos párrafos anteriores, nos encontramos ante la siguiente situación que concluye la prueba de este lema:

$$s, p \in \mathbb{Q} \cap \overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{d})} = \mathbb{Q} \cap \overline{\mathbb{Z}}^{\mathbb{Q}} = \mathbb{Z}. \tag{3.1}$$

Observación 3.0.2. Nótese que el resultado que nos proporciona la última igualdad de (3.1) podemos encontrarlo en [2, Example 5.0], aunque incluimos la breve prueba a continuación:

Si un número racional $x = r/s$, con r, s coprimos, es entero sobre $\mathbb{Z}$, por definición sabemos que satisface una ecuación de esta forma:

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0,$$

donde los a_i son enteros. Sustituyendo la expresión de x y multiplicando por s^n tenemos equivalentemente

$$r^n + a_1 r^{n-1} s + \ldots + a_n s^n = 0.$$

Por tanto, s divide a r^n, es decir $s = \pm 1$, y $x \in \mathbb{Z}$. En conclusión, los racionales que son enteros sobre $\mathbb{Z}$ son, en concreto, enteros.

Del lema anterior, en particular, se puede deducir que el polinomio mínimo de δ y $\bar{\delta}$ sobre $\mathbb{Q}$ realmente tiene coeficientes enteros, es decir, coincide con el que nos da la relación de dependencia entera.

Las posibilidades para a y b dependen de las congruencias de d módulo 4, como veremos en la siguiente proposición. Aunque este resultado es muy conocido (véase, por ejemplo, [1, Prop.13.1.6]), hemos optado por incluir una prueba para hacer la memoria más autocontenida.

[2] La clausura entera de $\mathbb{Z}$ en $\mathbb{Q}(\sqrt{d})$ es el anillo que contiene los elementos de $\mathbb{Q}(\sqrt{d})$ que son enteros sobre $\mathbb{Z}$.

Proposición 3.0.3. Sea d un entero libre de cuadrados. Entonces el anillo de enteros algebraicos de $\mathbb{Q}(\sqrt{d})$ es:

$$\mathcal{O}(\mathbb{Q}(\sqrt{d})) = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} & d \not\equiv 1 \mod 4 \\ \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} & d \equiv 1 \mod 4. \end{cases}$$

Demostración. Comencemos por ver la contención más sencilla, es decir, veamos que los elementos de $\mathbb{Z}[\sqrt{d}]$ y $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ son enteros algebraicos sobre $\mathbb{Z}$.

Si $z \in \mathbb{Z}[\sqrt{d}]$ es de la forma $p+q\sqrt{d}$ (con $p, q \in \mathbb{Z}$ y $q \neq 0$), su polinomio mínimo es $x^2 - 2px + p^2 - q^2 d$. Observamos que todos los coeficientes son enteros, y por tanto z es un entero algebraico sobre $\mathbb{Z}$.

Si, por el contrario, $z = p + q\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, su polinomio mínimo será $x^2 - (2p+q)x + p^2 + pq - q^2\left(\frac{1-d}{4}\right)$. En este caso, como estamos suponiendo que $d \equiv 1 \mod 4$, z vuelve a ser un entero algebraico. Por tanto, tenemos que $\mathbb{Z}[\sqrt{d}]$ y $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ están en el anillo de enteros algebraicos.

Recíprocamente, supongamos que tenemos un entero algebraico $\delta = a + b\sqrt{d}$, con $a, b \in \mathbb{Q}$. Por el lema 3.0.1, podemos partir de que $2a$ y $a^2 - b^2 d \in \mathbb{Z}$.

Sea entonces $a = \frac{a_1}{a_2}$, con a_1, a_2 enteros. Como $2a = \frac{2a_1}{a_2}$ es entero, suponiendo que el cociente que define a a es irreducible, llegamos a que debe ocurrir que $a_2 \mid 2$ para que se sigan teniendo esas condiciones. De ahí deducimos que, o bien $a_2 = 1$, o bien $a_2 = 2$.

Si $a_2 = 1$, es claro que $a \in \mathbb{Z}$. Nos falta entonces exigir que también se cumpla que $a^2 - b^2 d \in \mathbb{Z}$, lo cual equivale a que $b^2 d \in \mathbb{Z}$. De nuevo, si $b = \frac{b_1}{b_2}$, debe ocurrir que $b^2 d = d\frac{b_1^2}{b_2^2} \in \mathbb{Z}$. Al ser b_1 y b_2 coprimos, necesariamente $b_2 \mid d$, y como d es libre de cuadrados, la única opción es que $b_2 = 1$. Luego $b \in \mathbb{Z}$, es decir, tanto a como b son enteros.

Si contemplamos ahora el caso en el que $a_2 = 2$, entonces $a = \frac{a_1}{2}$. De nuevo, exigimos que $a^2 + b^2 d$ sea entero. Para ello, tomamos $b = \frac{b_1}{b_2}$, y por la expresión anterior nos queda que

$$a^2 - b^2 d = \frac{a_1^2}{4} - \frac{b_1^2 d}{b_2^2} = \frac{a_1^2 b_2^2 - 4b_1^2 d}{4b_2^2} \tag{3.2}$$

que debe ser entero.

Por un lado, el término b_2^2 debe ser divisor de $4b_1^2d$. De donde, al ser b_1 coprimo con b_2, necesariamente b_2^2 divide a $4d$. Y como d es libre de cuadrados, b_2 debe ser 1 o 2. Esto nos lleva a otros dos casos según el valor de b_2:

- Si $b_2 = 1$, de 3.2 tenemos que $\frac{a_1^2-4b_1^2d}{4}$ debe ser entero, y como 4 divide a $4b_1^2d$, entonces solo habría que imponer que a_1^2 fuese múltiplo de 4. Esto equivale a que entonces a_1 debería ser múltiplo de 2. No tiene sentido considerar tal caso, porque a_1 y a_2, son coprimos.
- Si $b_2 = 2$, usando 3.2 llegamos a que $\frac{a_1^2-b_1^2d}{4}$ debe ser entero. Siguiendo el razonamiento anterior, tendría que ocurrir que $a_1^2 - b_1^2d$ fuese múltiplo de 4. Además, tanto a_1 como b_1 son impares (de ser pares estaríamos en casos anteriores). Esto nos lleva a que $a_1^2, b_1^2 \equiv 1 \mod 4$, y en consecuencia, $1 - d$ tendría que ser múltiplo de 4 para terminar con nuestra prueba. De ahí que, necesariamente debamos tomar $d \equiv 1 \mod 4$. En ese caso, $b = b_1/2$. Entonces, dado que a_1 y b_1 deben tener la misma paridad, es equivalente escribir ese anillo como $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Es más, de ser a_1 y b_1 pares, este anillo incluye a $\mathbb{Z}[\sqrt{d}]$.

Concluimos que entonces si $d \equiv 1 \mod 4$, los enteros algebraicos serán de la forma $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$; y por el contrario, si $d \not\equiv 1 \mod 4$, serán elementos de $\mathbb{Z}[\sqrt{d}]$. De esta forma tenemos que los enteros algebraicos están contenidos en $\mathcal{O}(\mathbb{Q}(\sqrt{d}))$, terminando así la demostración.

Una vez recopilada la información anterior, la pregunta que cabe hacerse es qué relación existe entre tales subanillos del plano complejo y los anillos de origami. La respuesta a ello nos la proporciona el resultado principal de este capítulo:

Teorema 3.0.4. *Sea $d < 0$ un entero libre de cuadrados, y sea $\theta = arg(1 + \sqrt{d})$. Entonces, el anillo de enteros cuadrático de $\mathbb{Q}(\sqrt{d})$ coincide con $\boldsymbol{R}(\boldsymbol{U})$, donde*

1. $U = \{1, i, e^{i\theta}\}$ *si* $d \equiv 2\, o\, 3 \mod 4$.
2. $U = \{1, e^{i\theta}, e^{i(\pi-\theta)}\}$ *si* $d \equiv 1 \mod 4$

Demostración. Vamos a dividir la prueba en dos partes, una para cada posible conjunto de direcciones U:

$\boxed{U = \{1, i, e^{i\theta}\}}$

En este caso, dado que $d \equiv 2\, o\, 3 \mod 4$, tenemos que $\mathcal{O}(\mathbb{Q}(\sqrt{d})) = \mathbb{Z}[\sqrt{d}]$ por la proposición 3.0.3.

Veamos en primer lugar que $\boldsymbol{R}(U) \subseteq \mathbb{Z}[\sqrt{d}]$, es decir, que $I_{u,v}(p,q) \in \mathbb{Z}[\sqrt{d}]$ para cualesquiera $u, v \in U$ y $p, q \in \mathbb{Z}[\sqrt{d}]$.

Como hay tres direcciones posibles, tenemos 6 casos a considerar. Sean $p = a + b\sqrt{d}$ y $q = c + e\sqrt{d}$. Nos fijamos en que podemos remitirnos a la prueba del teorema 1.3.2, y tomar $z = I_{i,e^{i\theta}}(0,1) = \frac{s_{v,1}}{s_{v,u}} i = \frac{v-\bar{v}}{\bar{u}v-u\bar{v}} i = \frac{v-\bar{v}}{-iv-i\bar{v}} i = \frac{2i\sin\theta}{-2i\cos\theta} i = -i\tan\theta = -i\sqrt{-d} = -\sqrt{d}$, con $d < 0$ un entero libre de cuadrados. De esta forma, tendríamos que $\boldsymbol{R}(U)$ está en $\mathbb{Z}[\sqrt{d}]$, siendo $U = \{1, i, e^{i\theta}\}$ en nuestro caso. Es más, por el mismo teorema tendríamos que no solo se da tal contención, sino también la igualdad. Además, como en este caso z es un entero de grado 2, tenemos que es un anillo.

Aunque en el párrafo anterior ya podríamos terminar la demostración de este caso, veamos desde el punto de vista de la referencia [4] una prueba de la contención contraria, es decir, que $\mathbb{Z}[\sqrt{d}] \subseteq \boldsymbol{R}(U)$. Para ello, tomamos $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, y veamos que podemos llegar a tal punto comenzando en $\{0, 1\}$ e intersecando las direcciones de $\boldsymbol{U}$. Esta demostración podemos reducirla a probar que, dados dos puntos $\{n + k\sqrt{d}, n + 1 + k\sqrt{d}\}$, podemos construir también

$$n - 1 + k\sqrt{d}, n + (k+1)\sqrt{d}, n + 1 + (k+1)\sqrt{d},$$

$$n + 2 + k\sqrt{d}, n + 1 + (k-1)\sqrt{d}, n + (k-1)\sqrt{d}.$$

En realidad, lo que estamos haciendo es una una inducción doble sobre las componentes reales e imaginarias de un entero arbitrario construido. El objetivo es probar que para cualquier par de puntos consecutivos, podemos construir puntos cuyas coordenadas enteras con respecto a la base $\{1, \sqrt{d}\}$ difieren en una unidad respecto a ellos en todas las direcciones posibles. Notemos que, en tal caso, hablamos de un total de seis puntos alrededor de los que partimos, los cuales se hallan como se explica a continuación:

Comenzamos en los dos puntos de partida y con las direcciones distintas de 1, construimos el siguiente punto usando las fórmulas del teorema 1.3.2 junto con las propiedades del operador I vistas en la proposición 1.1.5. Hacemos el primero de

ellos con más detalle:

$$\begin{aligned} I_{i,e^{i\theta}}(n+k\sqrt{d}, n+1+k\sqrt{d}) &= I_{i,e^{i\theta}}(n, n+1) + k\sqrt{d} \\ &= \frac{s_{i,n}}{s_{i,e^{i\theta}}} e^{i\theta} + \frac{s_{e^{i\theta},n+1}}{s_{e^{i\theta},i}} i + k\sqrt{d} \\ &= \frac{2in}{i(2\cos\theta)} e^{i\theta} + \frac{(2i\sin\theta)(n+1)}{(-i)(2\cos\theta)} i + k\sqrt{d} \\ &= \frac{n(\cos\theta + i\sin\theta) - (n+1)i\sin\theta}{\cos\theta} + k\sqrt{d} \\ &= n - i\tan\theta + k\sqrt{d} = n - \sqrt{d} + k\sqrt{d} \\ &= n + (k-1)\sqrt{d}. \end{aligned}$$

Tomamos este nuevo punto y el anterior y hallamos

$$I_{i,1}(n+1+k\sqrt{d}, n+(k-1)\sqrt{d}) = n+1+(k-1)\sqrt{d},$$

que es otro punto de debajo de los dos iniciales. Por último, ayudándonos del que acabamos de construir, conseguimos

$$I_{1,e^{i\theta}}(n+1+k\sqrt{d}, n+1+(k-1)\sqrt{d}) = n+2+k\sqrt{d}.$$

Para simplificar la notación en la prueba, cuando escribamos los puntos (a, b) nos referiremos a $a + b\sqrt{d}$. Observemos la imagen 3.1 para tener una idea geométrica de cuál sería el razonamiento de la prueba (hasta ahora solo habríamos construido los verdes).

Por otro lado, para los puntos de arriba, empezamos tomando

$$I_{e^{i\theta},i}(n+k\sqrt{d}, n+1+k\sqrt{d}) = n+1+(k+1)\sqrt{d}.$$

A continuación, usando este último, podemos construir

$$I_{i,1}(n+k\sqrt{d}, n+1+(k+1)\sqrt{d}) = n+(k+1)\sqrt{d}.$$

Por último, nos ayudamos de nuevo del anterior y de uno de los iniciales y construimos:

$$I_{1,e^{i\theta}}(n+k\sqrt{d}, n+(k+1)\sqrt{d}) = n-1+k\sqrt{d}.$$

Hemos probado entonces que $\mathbb{Z}[\sqrt{d}] \subseteq R(U)$, completando así la prueba de igualdad entre ambos.

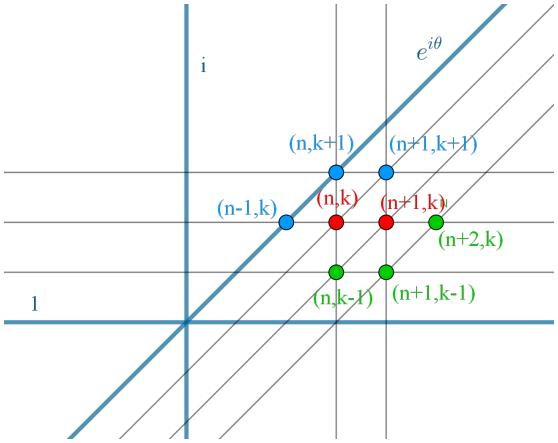


Figura 3.1: Construcción de puntos alrededor de los iniciales.

$$U = \{1, e^{i\theta}, e^{i(\pi-\theta)}\}$$

Para este apartado usaremos la misma estrategia que para el anterior pero con una sutil diferencia dada por la estructura del anillo, ya que al ser $d \equiv 1 \mod 4$, el anillo $\mathcal{O}(\mathbb{Q}(\sqrt{d}))$ se corresponde con $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ por la proposición 3.0.3.

Comenzaremos la prueba viendo que $R(U) \subseteq \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, lo que se traduce en ver que cada punto de la forma $I_{u,v}(p,q)$, con $u, v \in U$ y $p, q \in \mathcal{O}(\mathbb{Q}(\sqrt{d}))$, está en ese anillo de enteros cuadrático.

De nuevo, podemos usar la prueba del teorema 1.3.2, pues en este caso $z = I_{e^{i\theta},e^{i(\pi-\theta)}}(0,1) = \frac{1+\sqrt{d}}{2}$. Para hallar este punto, usamos que $\theta = arg(1+\sqrt{d})$ y que el triángulo formado por $0, 1, z$ es isósceles (porque los argumentos de las dos direcciones son ángulos suplementarios). Por tanto, z es el punto medio del segmento entre 0 y $1+\sqrt{d}$. De esta forma, razonando como en el caso anterior tenemos que no solo $R(U) \subseteq \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, sino que coinciden, siendo además ambos anillos por ser z un entero de grado 2.

Ya tendríamos terminada la prueba, aunque incluimos el enfoque iterativo de la referencia [4] para ver que $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subseteq R(U)$, para lo cual tomamos un elemento $\frac{a+b\sqrt{d}}{2}$ de $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ y, como en la prueba anterior, veremos que se puede obtener mediante intersecciones cuyos puntos de partida son $\{0, 1\}$.

Como antes, podemos reducir este razonamiento a ver que dados los puntos

$$\left\{\frac{n+k\sqrt{d}}{2}, \frac{n+2+k\sqrt{d}}{2}\right\}$$

podemos construir

$$\frac{n+1+(k+1)\sqrt{d}}{2}, \frac{n+3+(k+1)\sqrt{d}}{2}, \frac{n+4+k\sqrt{d}}{2},$$
$$\frac{n+1+(k-1)\sqrt{d}}{2}, \frac{n-1+(k-1)\sqrt{d}}{2}, \frac{n-2+k\sqrt{d}}{2}$$

tal como se ilustra a continuación. Esta vez, cuando escribamos (a, b) nos referiremos a $(a+b\sqrt{d})/2$:

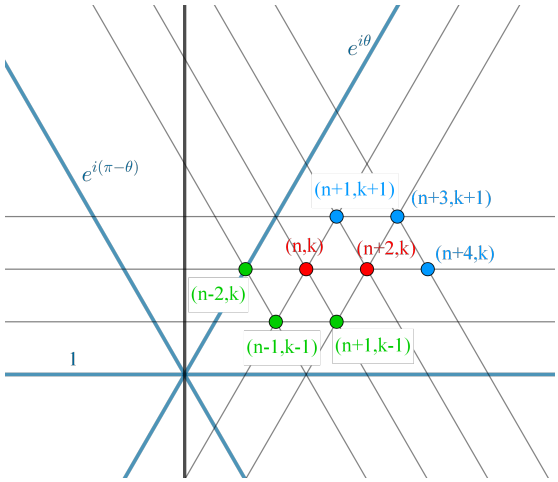


Figura 3.2: Construcción de puntos alrededor de los iniciales.

Notemos que, en realidad, la prueba trata de ver que los seis puntos de alrededor (en el sentido de la prueba anterior) pueden obtenerse.

Comenzamos utilizando los puntos iniciales y las direcciones distintas de 1 para el primer punto:

$$I_{e^{i\theta},e^{i(\pi-\theta)}}\left(\frac{n+k\sqrt{d}}{2}, \frac{n+2+k\sqrt{d}}{2}\right) = \frac{n+1+(k+1)\sqrt{d}}{2}.$$

A partir de este y uno inicial, construimos

$$I_{1,e^{i\theta}}\left(\frac{n+1+(k+1)\sqrt{d}}{2}, \frac{n+2+k\sqrt{d}}{2}\right) = \frac{n+3+(k+1)\sqrt{d}}{2}.$$

Para terminar los puntos de la parte superior, hallamos

$$I_{1,e^{i(\pi-\theta)}}\left(\frac{n+2+k\sqrt{d}}{2},\frac{n+3+(k+1)\sqrt{d}}{2}\right)=\frac{n+4+k\sqrt{d}}{2}.$$

Ahora, todo es simétrico respecto del punto $\frac{n+1+k\sqrt{d}}{2}$, pues, de los puntos iniciales pero con las direcciones intercambiadas llegamos a

$$I_{e^{i(\pi-\theta)},e^{i\theta}}\left(\frac{n+k\sqrt{d}}{2},\frac{n+2+k\sqrt{d}}{2}\right)=\frac{n+1+(k-1)\sqrt{d}}{2}.$$

Usando tal punto junto a uno de los iniciales

$$I_{1,e^{i\theta}}\left(\frac{n+1+(k-1)\sqrt{d}}{2},\frac{n+k\sqrt{d}}{2}\right)=\frac{n-1+(k-1)\sqrt{d}}{2}.$$

Finalmente, desde ese y otro de los de partida obtenemos el punto que nos queda:

$$I_{1,e^{i(\pi-\theta)}}\left(\frac{n+k\sqrt{d}}{2},\frac{n-1+(k-1)\sqrt{d}}{2}\right)=\frac{n-2+k\sqrt{d}}{2}.$$

Con esto finaliza la segunda parte de la prueba y tenemos que entonces para ciertos U, el anillo de enteros cuadrático $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ coincide con $R(U)$, que era el objetivo principal de este capítulo.

Para finalizar, podríamos ir un poco más allá y comentar que el resultado [5, Theorem 8] podría verse como un caso particular de este anterior.

Índice de figuras

Bibliografía

[1] M. Artin, *Algebra*. Englewood Cliffs (New Jersey) : Prentice-Hall, (1991).

[2] M. F. Atiyah e I. G. Macdonald, *Introduction to commutative algebra*. Addison-Wesley Publishing Co. et. al., (1969).

[3] J. Buhler, S. Butler, W. De Launey y R. Graham, "Origami Rings", *Journal of the Australian Mathematical Society*, vol. 92, n.º 3, (2012).

[4] J. Kritschgau y A. Salerno, "Origami constructions of rings of integers of imaginary quadratic fields", *Integers*, vol. 17, (2017).

[5] D. Nedrenco, "On origami rings", *arXiv preprint arXiv:1502.07995*, (2015).

[6] H. Salzmann, T. Grundhöfer, H. Hähl y R. Löwen, *The classical fields*. Cambridge University Press, Cambridge, (2007), Structural features of the real and rational numbers.