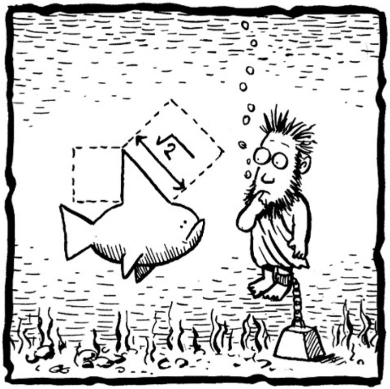
Construcciones con regla y compás: sobre la irresolubilidad de los tres problemas Griegos

Valente Santiago Vargas
Departamento de Matemáticas, Facultad de Ciencias UNAM

22 de Marzo de 2018


√2

Pero, ¿que son los números construibles ?
Para contestar esto consideremos los siguientes ingredientes:

(1) Dos puntos $\{P_1, P_2\}$. La longitud entre tales puntos lo llamaremos 1,

(2) Una regla sin marcas y un compás.

LAS REGLAS DEL JUEGO.

Definición un poco informal

Un punto Q es **construible** si Q es construido por intersecciones sucesivas de las siguientes:

(a) Líneas a tráves de puntos construidos previamente.

(b) Círculos con centro un punto construido previamente y cuyo radio tiene como extremo final otro punto construido previamente.

Las construcciones con regla y compás llevaron a los Griegos a tres problemas famosos que no pudieron resolver.

Las construcciones con regla y compás llevaron a los Griegos a tres problemas famosos que no pudieron resolver.

(1) Dado un cubo de cierto tamaño, ¿es posible construir otro cubo con el doble del volumen?

Las construcciones con regla y compás llevaron a los Griegos a tres problemas famosos que no pudieron resolver.

(1) Dado un cubo de cierto tamaño, ¿es posible construir otro cubo con el doble del volumen?

(2) ¿Es posible trisecar un ángulo?

Las construcciones con regla y compás llevaron a los Griegos a tres problemas famosos que no pudieron resolver.

(1) Dado un cubo de cierto tamaño, ¿es posible construir otro cubo con el doble del volumen?
(2) ¿Es posible trisecar un ángulo?
(3) ¿Es posible cuadrar el círculo?

Veremos que la respuesta es negativa a las tres preguntas. Para esto, necesitamos formular de forma precisa a los puntos construibles.

Definición formal

Sea $S = \{P_1, P_2\}$ un conjunto con dos puntos en el plano cartesiano $\mathbb{R}^2$. Definimos conjuntos $S_m \subseteq \mathbb{R}^2$ de forma inductiva.

(a) $S_1 := S$

(b) $S_{n+1} = S_n \bigcup X_n \bigcup Y_n \bigcup Z_n$ donde

(1) X_n son los puntos que son intersección de lineas que conectan distintos puntos de S_n (construcción hecha con regla).

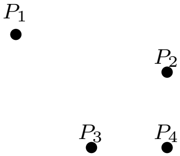


Figura: P es un punto de X_n

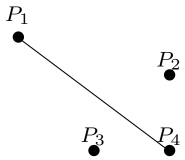


Figura: P es un punto de X_n

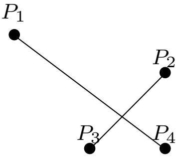


Figura: P es un punto de X_n

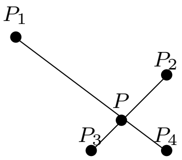


Figura: P es un punto de X_n

(2) Y_n son los puntos que son intersección de lineas que conectan distintos puntos de S_n con círculos que tienen centro en los puntos de S_n y cuyo radio tiene como extremo final a uno de los puntos de S_n (construcción hecha con regla y compás).

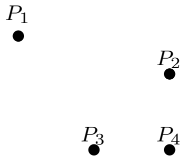
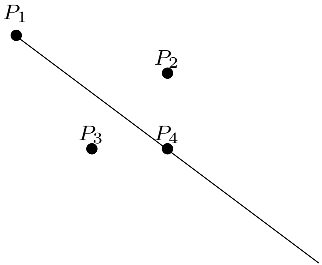
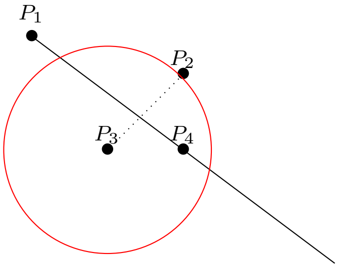


Figura: Q y R son puntos de Y_n

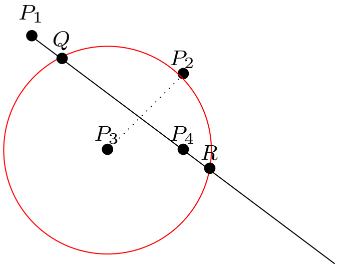
(2) Y_n son los puntos que son intersección de lineas que conectan distintos puntos de S_n con círculos que tienen centro en los puntos de S_n y cuyo radio tiene como extremo final a uno de los puntos de S_n (construcción hecha con regla y compás).



(2) Y_n son los puntos que son intersección de lineas que conectan distintos puntos de S_n con círculos que tienen centro en los puntos de S_n y cuyo radio tiene como extremo final a uno de los puntos de S_n (construcción hecha con regla y compás).



(2) Y_n son los puntos que son intersección de lineas que conectan distintos puntos de S_n con círculos que tienen centro en los puntos de S_n y cuyo radio tiene como extremo final a uno de los puntos de S_n (construcción hecha con regla y compás).



Definición

(3) Z_n son los puntos que son intersección de círculos construidos como en Y_n. Es decir, Z_n son los puntos que son intersección de círculos que tienen centros en S_n y cuyos radios tienen como extremos finales a puntos de S_n (construcción con compás).

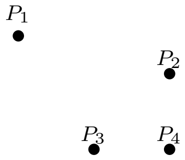
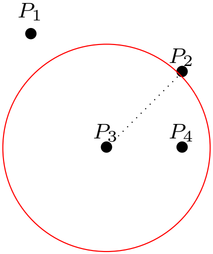


Figura: A y B son puntos de Z_n

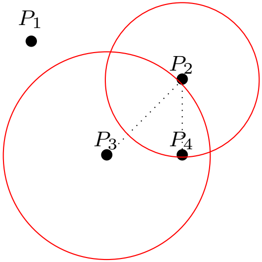
Definición

(3) Z_n son los puntos que son intersección de círculos construidos como en Y_n. Es decir, Z_n son los puntos que son intersección de círculos que tienen centros en S_n y cuyos radios tienen como extremos finales a puntos de S_n (construcción con compás).



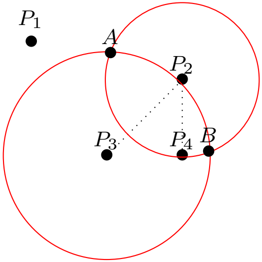
Definición

(3) Z_n son los puntos que son intersección de círculos construidos como en Y_n. Es decir, Z_n son los puntos que son intersección de círculos que tienen centros en S_n y cuyos radios tienen como extremos finales a puntos de S_n (construcción con compás).



Definición

(3) Z_n son los puntos que son intersección de círculos construidos como en Y_n. Es decir, Z_n son los puntos que son intersección de círculos que tienen centros en S_n y cuyos radios tienen como extremos finales a puntos de S_n (construcción con compás).



Números construibles

Sea $C(P_1, P_2) := \bigcup_{i=1}^{\infty} S_i$, se dice que un punto P es **construible con regla y compás** a través de los puntos P_1, P_2 si $P \in C(P_1, P_2)$.

Sean P y Q dos puntos en el plano y sea l la recta que determinan. Al segmento de recta que une a P y Q lo denotaremos por PQ y a la longitud del segmento PQ lo denotaremos por $\overline{PQ}$.

Sean P y Q dos puntos distintos y consideremos la linea recta l que determinan. Con regla y compás se pueden construir una infinidad de puntos en la recta l tal que si dos puntos son consecutivos entonces la distancia entre ellos es la longitud $\overline{PQ}$.

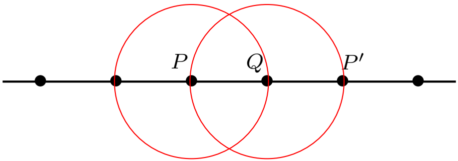


Figura: Construcción 1

Dado $S = \{P_1, P_2\}$ dos puntos en el plano, podemos suponer que en el plano cartesiano se tiene que $P_1 = (0,0)$ y $P_2 = (1,0)$.

Corolario

Con regla y compás se puede construir cualquier punto $P = (n, 0)$ con $n \in \mathbb{Z}$.

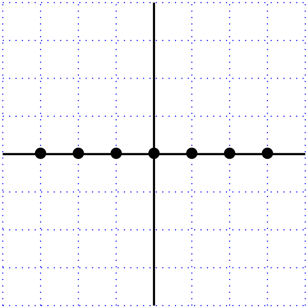


Figura: Construcción de $\mathbb{Z} \times \{0\}$

Perpendiculares 1

Sean P y Q puntos y l la recta que determinan. Sea R un punto que no está sobre la recta l. Entonces con regla y compás se puede construir una perpendicular a l que pasa por R.

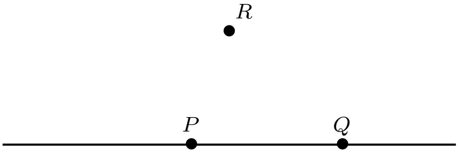


Figura: Construcción 2

Perpendiculares 1

Sean P y Q puntos y l la recta que determinan. Sea R un punto que no está sobre la recta l. Entonces con regla y compás se puede construir una perpendicular a l que pasa por R.

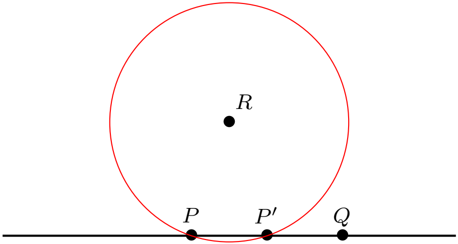
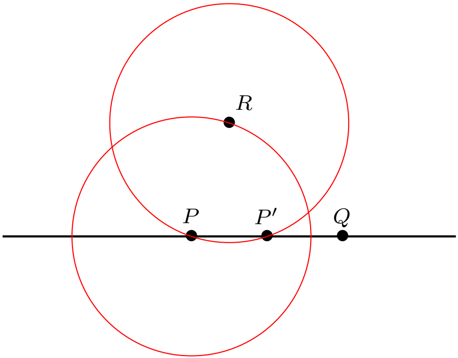


Figura: Construcción 2

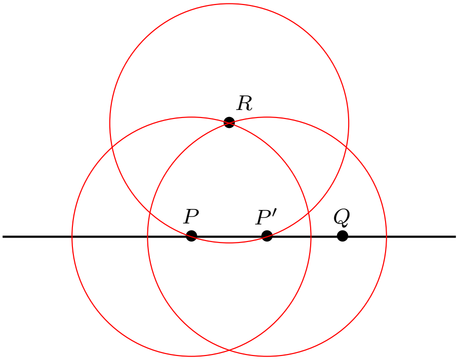
Perpendiculares 1

Sean P y Q puntos y l la recta que determinan. Sea R un punto que no está sobre la recta l. Entonces con regla y compás se puede construir una perpendicular a l que pasa por R.



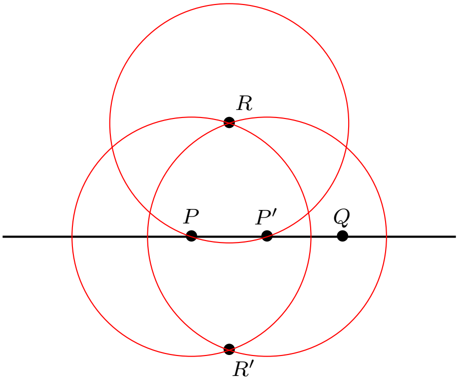
Perpendiculares

Sean P y Q puntos y l la recta que determinan. Sea R un punto que no está sobre la recta l. Entonces con regla y compás se puede construir una perpendicular a l que pasa por R.



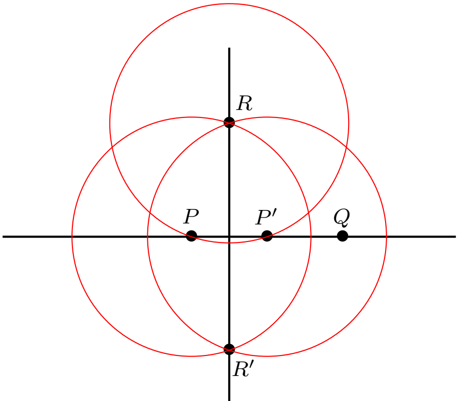
Perpendiculares 1

Sean P y Q puntos y l la recta que determinan. Sea R un punto que no está sobre la recta l. Entonces con regla y compás se puede construir una perpendicular a l que pasa por R.



Perpendiculares 1

Sean P y Q puntos y l la recta que determinan. Sea R un punto que no está sobre la recta l. Entonces con regla y compás se puede construir una perpendicular a l que pasa por R.



Perpendiculares 2

Sean P y Q puntos y l la recta que determinan. Sea R un punto que está sobre la recta l. Entonces con regla y compás se puede construir una perpendicular a l que pasa por R.

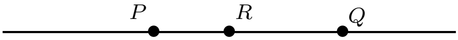


Figura: Construcción 3

Perpendiculares 2

Sean P y Q puntos y l la recta que determinan. Sea R un punto que está sobre la recta l. Entonces con regla y compás se puede construir una perpendicular a l que pasa por R.

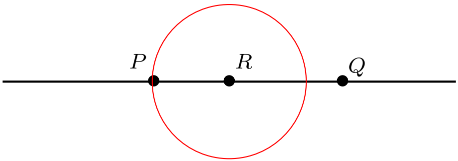


Figura: Construcción 3

Perpendiculares 2

Sean P y Q puntos y l la recta que determinan. Sea R un punto que está sobre la recta l. Entonces con regla y compás se puede construir una perpendicular a l que pasa por R.

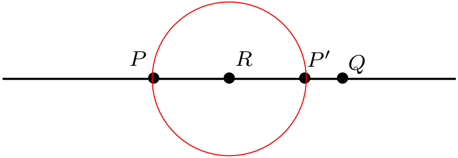


Figura: Construcción 3

Perpendiculares 2

Sean P y Q puntos y l la recta que determinan. Sea R un punto que está sobre la recta l. Entonces con regla y compás se puede construir una perpendicular a l que pasa por R.

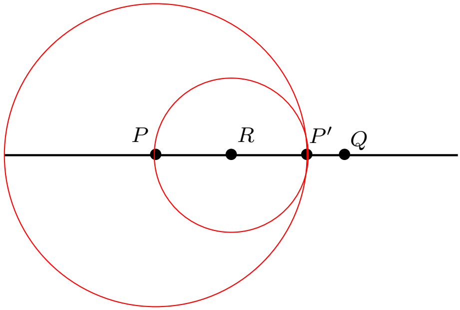


Figura: Construcción 3

Perpendiculares 2

Sean P y Q puntos y l la recta que determinan. Sea R un punto que está sobre la recta l. Entonces con regla y compás se puede construir una perpendicular a l que pasa por R.

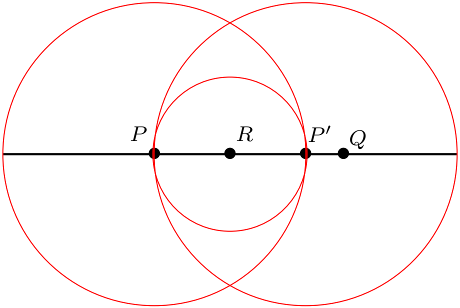


Figura: Construcción 3

Perpendiculares 2

Sean P y Q puntos y l la recta que determinan. Sea R un punto que está sobre la recta l. Entonces con regla y compás se puede construir una perpendicular a l que pasa por R.

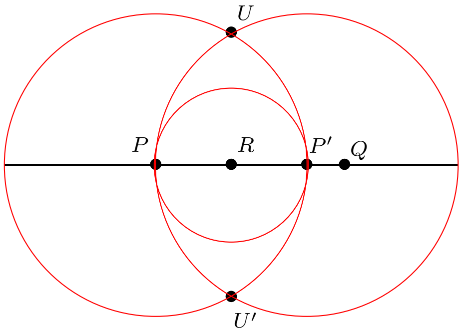
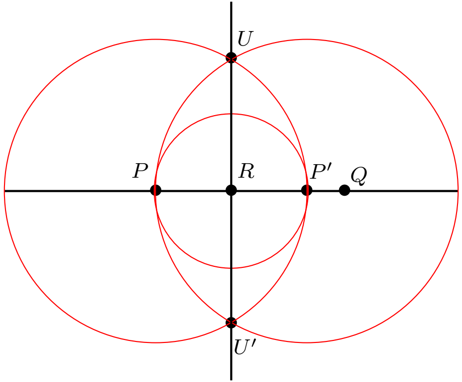


Figura: Construcción 2

Perpendiculares 2

Sean P y Q puntos y l la recta que determinan. Sea R un punto que está sobre la recta l. Entonces con regla y compás se puede construir una perpendicular a l que pasa por R.



Paralelas

Sean P y Q puntos y l la recta que determinan. Sea R un punto que no está sobre la recta l. Entonces con regla y compás se puede construir una paralela a l que pasa por R.

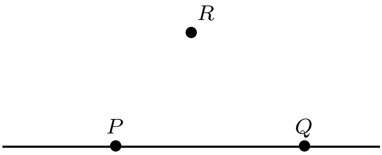
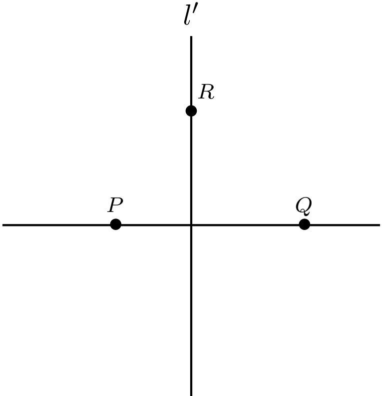


Figura: Construcción 4

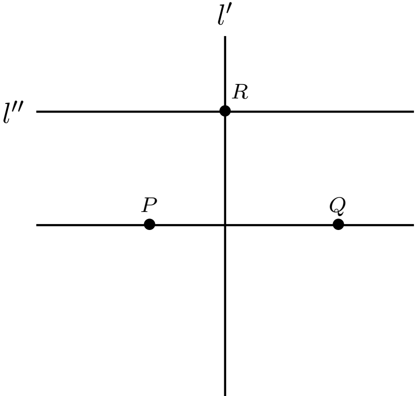
Paralelas

Sean P y Q puntos y l la recta que determinan. Sea R un punto que no está sobre la recta l. Entonces con regla y compás se puede construir una paralela a l que pasa por R.



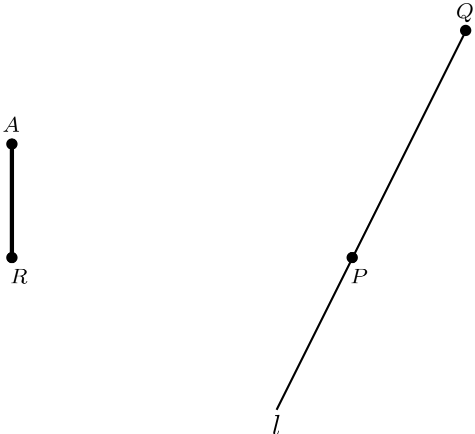
Paralelas

Sean P y Q puntos y l la recta que determinan. Sea R un punto que no está sobre la recta l. Entonces con regla y compás se puede construir una paralela a l que pasa por R.



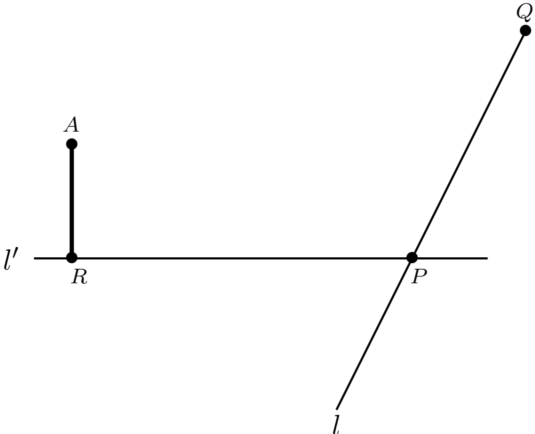
Traslación de distancias

Dado dos puntos R y A un punto P sobre una recta l. Se puede construir un punto B sobre l tal que $\overline{PB} = \overline{RA}$.



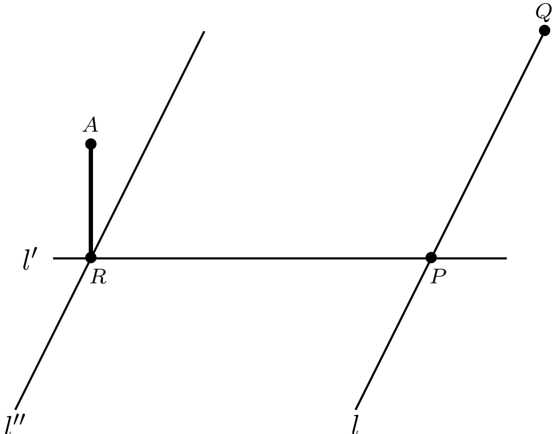
Traslación de distancias

Dado dos puntos R y A un punto P sobre una recta l. Se puede construir un punto B sobre l tal que $\overline{PB} = \overline{RA}$.



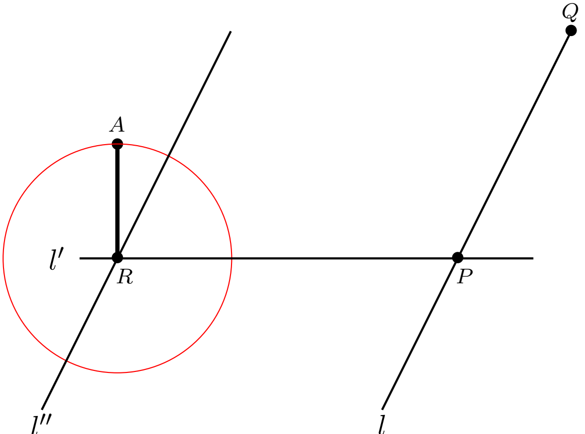
Traslación de distancias

Dado dos puntos R y A un punto P sobre una recta l. Se puede construir un punto B sobre l tal que $\overline{PB} = \overline{RA}$.



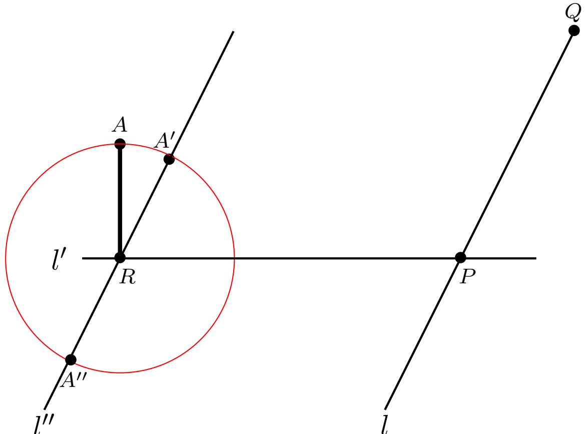
Traslación de distancias

Dado dos puntos R y A un punto P sobre una recta l. Se puede construir un punto B sobre l tal que $\overline{PB} = \overline{RA}$.



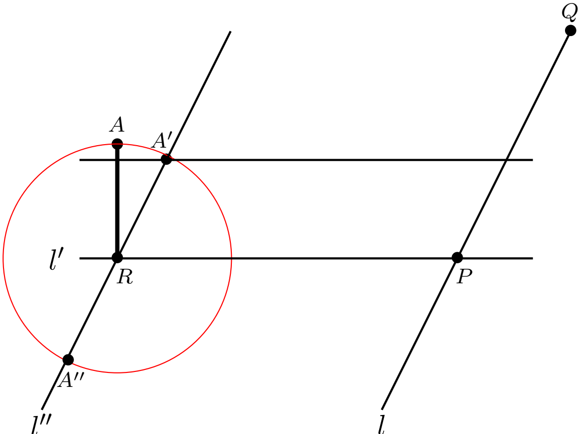
Traslación de distancias

Dado dos puntos R y A un punto P sobre una recta l. Se puede construir un punto B sobre l tal que $\overline{PB} = \overline{RA}$.



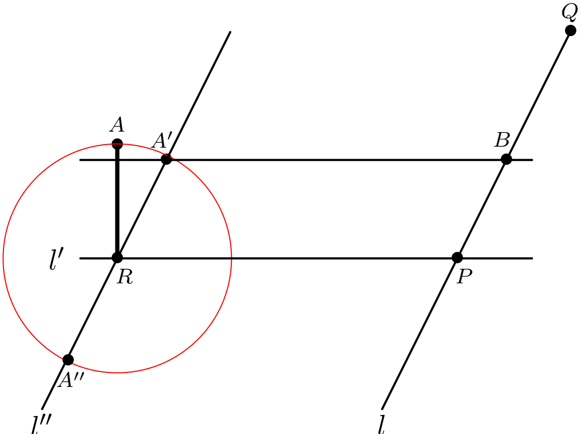
Traslación de distancias

Dado dos puntos R y A un punto P sobre una recta l. Se puede construir un punto B sobre l tal que $\overline{PB} = \overline{RA}$.



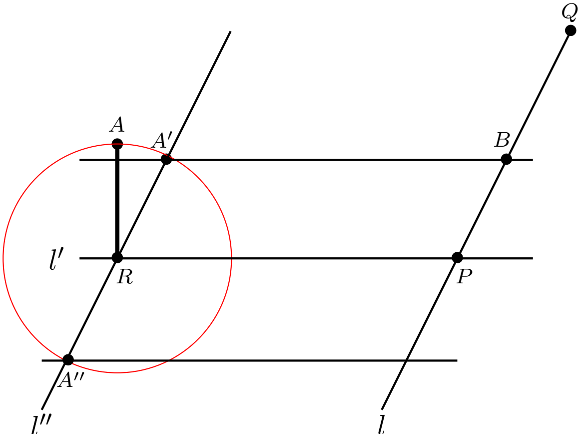
Traslación de distancias

Dado dos puntos R y A un punto P sobre una recta l. Se puede construir un punto B sobre l tal que $\overline{PB} = \overline{RA}$.



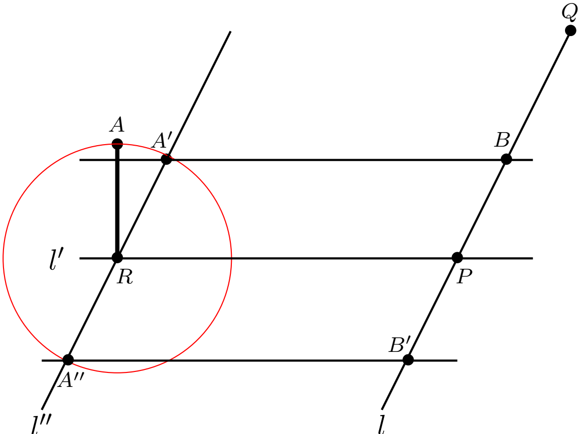
Traslación de distancias

Dado dos puntos R y A un punto P sobre una recta l. Se puede construir un punto B sobre l tal que $\overline{PB} = \overline{RA}$.



Traslación de distancias

Dado dos puntos R y A un punto P sobre una recta l. Se puede construir un punto B sobre l tal que $\overline{PB} = \overline{RA}$.



Construcción de cuadrados

Dado dos puntos P y Q sobre una recta l. Se puede construir un punto cuadrado cuyos lados tengan longitud $\overline{PQ}$.

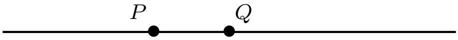


Figura: Cuadrado

Construcción de cuadrados

Dado dos puntos P y Q sobre una recta l. Se puede construir un punto cuadrado cuyos lados tengan longitud $\overline{PQ}$.

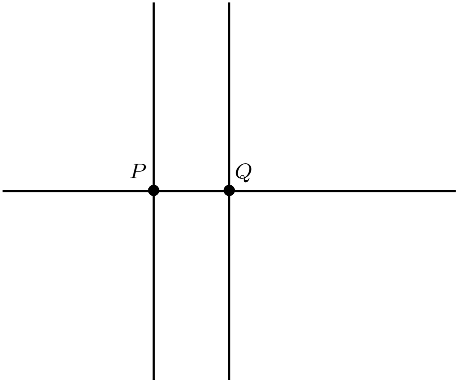


Figura: Cuadrado

Construcción de cuadrados

Dado dos puntos P y Q sobre una recta l. Se puede construir un punto cuadrado cuyos lados tengan longitud $\overline{PQ}$.

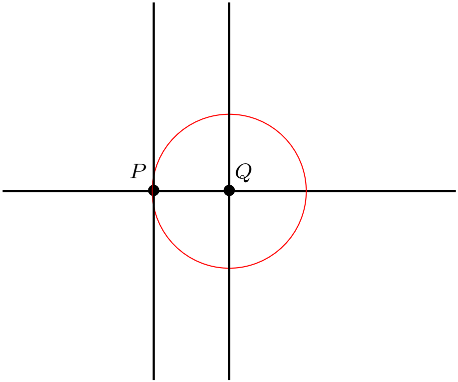


Figura: Cuadrado

Construcción de cuadrados

Dado dos puntos P y Q sobre una recta l. Se puede construir un punto cuadrado cuyos lados tengan longitud $\overline{PQ}$.

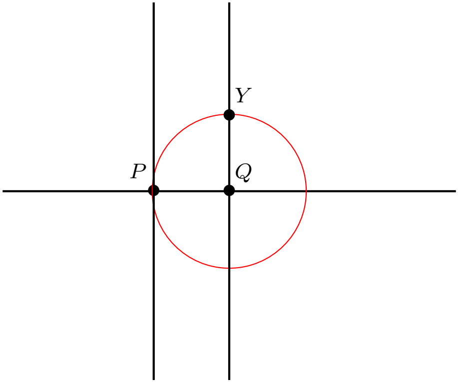


Figura: Cuadrado

Construcción de cuadrados

Dado dos puntos P y Q sobre una recta l. Se puede construir un punto cuadrado cuyos lados tengan longitud $\overline{PQ}$.

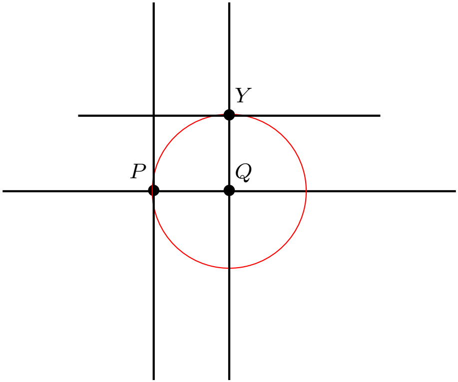


Figura: Cuadrado

Construcción de cuadrados

Dado dos puntos P y Q sobre una recta l. Se puede construir un punto cuadrado cuyos lados tengan longitud $\overline{PQ}$.

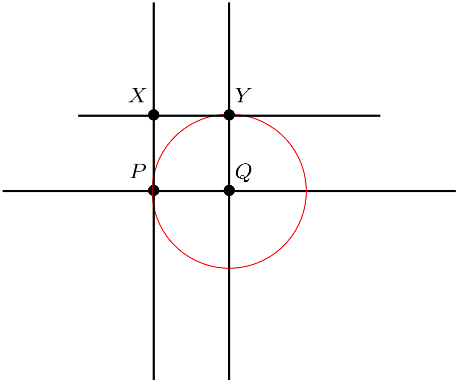


Figura: Cuadrado

Lema

Con regla y compás se puede obtener el reticulado $\mathbb{Z} \times \mathbb{Z}$ del plano.

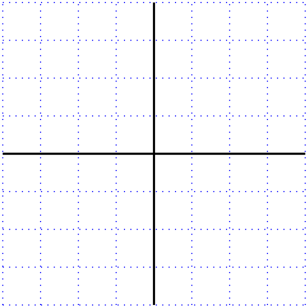


Figura: Reticulado $\mathbb{Z} \times \mathbb{Z}$.

Definición de número construible

Tomando, como medida unitaria la distancia entre $P_1 = (0,0)$ y $P_2 = (1,0)$. Un número real r es **construible** si $|r|$ es la distancia entre dos puntos construibles.

Definición de número construible

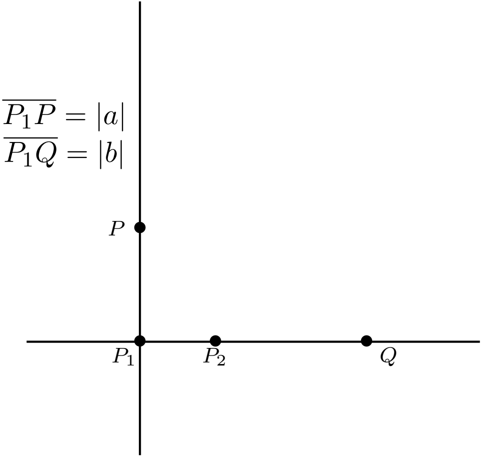
Tomando, como medida unitaria la distancia entre $P_1 = (0,0)$ y $P_2 = (1,0)$. Un número real r es **construible** si $|r|$ es la distancia entre dos puntos construibles.

Corolario

Los números enteros $\mathbb{Z}$ son construibles.

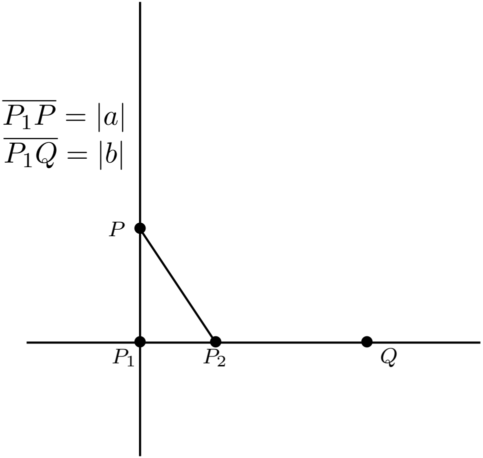
Proposición

Si a y b son construibles, entonces ab es construible.



Proposición

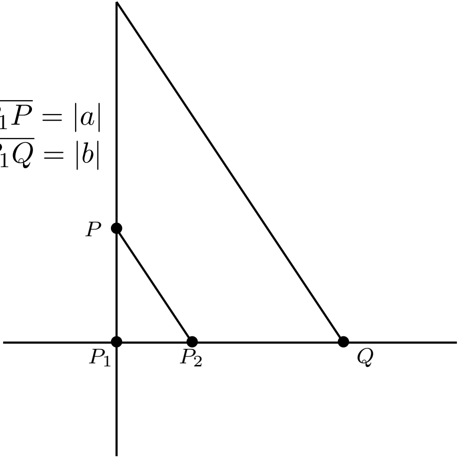
Si a y b son construibles, entonces ab es construible.



Proposición

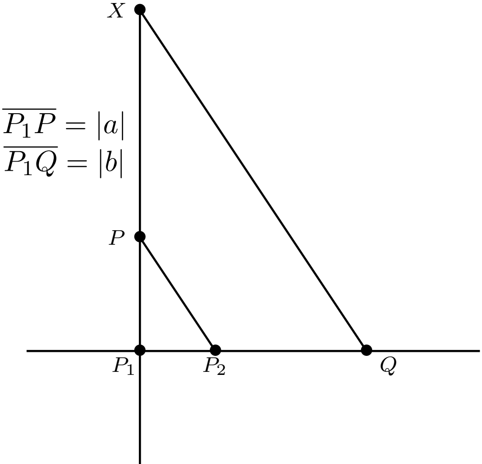
Si a y b son construibles, entonces ab es construible.

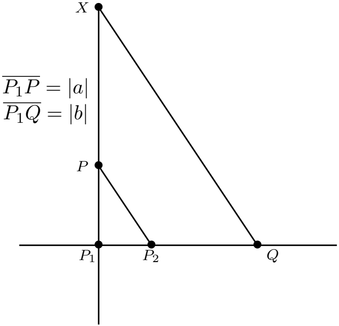
$$\overline{P_1P} = |a|$$
$$\overline{P_1Q} = |b|$$



Proposición

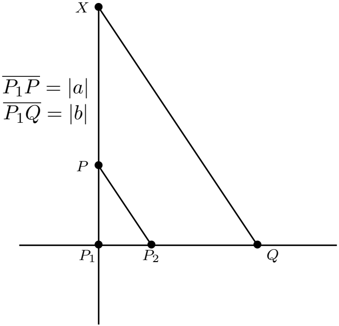
Si a y b son construibles, entonces ab es construible.





Tenemos $\overline{P_1P} = |a|$ y $\overline{P_1Q} = |b|$ y podemos suponer que $Q \neq (1, 0)$.

$$\frac{\overline{P_1X}}{\overline{P_1P}} = \frac{\overline{P_1Q}}{\overline{P_1P_2}}$$



Tenemos $\overline{P_1P} = |a|$ y $\overline{P_1Q} = |b|$ y podemos suponer que $Q \neq (1,0)$.

$$\frac{\overline{P_1X}}{\overline{P_1P}} = \frac{\overline{P_1Q}}{\overline{P_1P_2}} \Longrightarrow \frac{\overline{P_1X}}{|a|} = |b|$$

Proposición

Si a y b son construibles con $b \neq 0$, entonces ab^{-1} es construible.

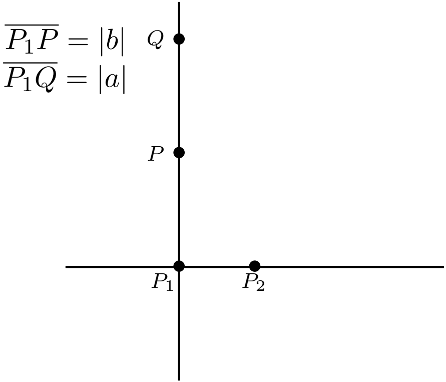


Figura: división

Proposición

Si a y b son construibles con $b \neq 0$, entonces ab^{-1} es construible.

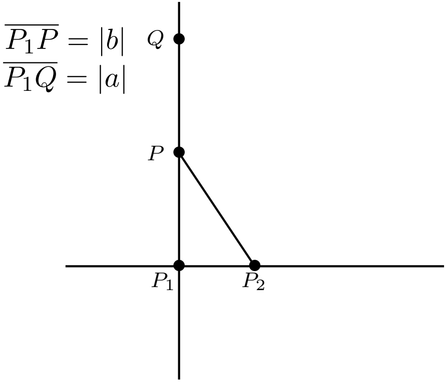


Figura: división

Proposición

Si a y b son construibles con $b \neq 0$, entonces ab^{-1} es construible.

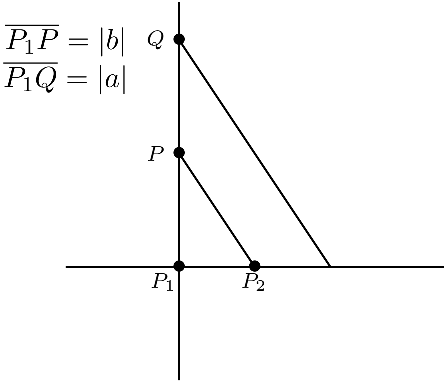


Figura: división

Proposición

Si a y b son construibles con $b \neq 0$, entonces ab^{-1} es construible.

$\overline{P_1P} = |b|$
$\overline{P_1Q} = |a|$

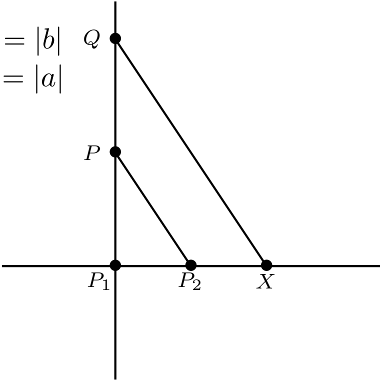
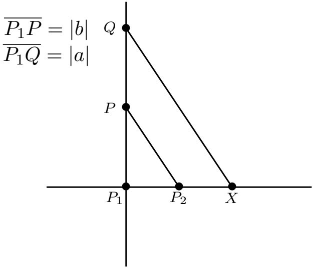


Figura: división



Tenemos $\overline{P_1P} = |b|$ y $\overline{P_1Q} = |a|$ y supongamos $P \neq Q$.

$$\frac{\overline{P_1Q}}{\overline{P_1P}} = \frac{\overline{P_1X}}{\overline{P_1P_2}}.$$

Es decir, $\frac{|a|}{|b|} = \overline{P_1X}$ y entonces ab^{-1} es construible.

Proposición

Si a y b son construibles, entonces $a+b$ y $a-b$ son construibles

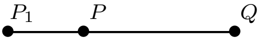


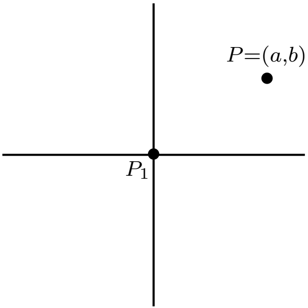
Figura: diferencia de construibles

Supongamos $a, b \geq 0$ y $a \geq b$. Tenemos que $\overline{P_1P} = b$ y $\overline{P_1Q} = a$. Entonces $\overline{PQ} = a - b$ y por lo tanto $a - b$ es construible.

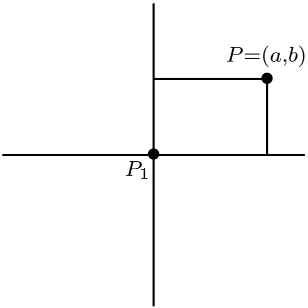
Corolario

Los número racionales $\mathbb{Q}$ son construibles.

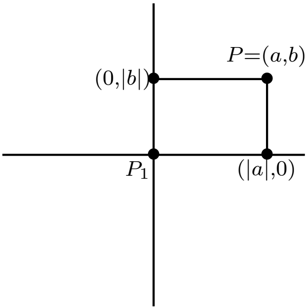
Sea $P = (a, b) \in \mathbb{R}^2$, tenemos que P es un punto construible si y sólo si a y b son número reales construibles.



Sea $P = (a, b) \in \mathbb{R}^2$, tenemos que P es un punto construible si y sólo si a y b son número reales construibles.



Sea $P = (a, b) \in \mathbb{R}^2$, tenemos que P es un punto construible si y sólo si a y b son número reales construibles.



Corolario

Los puntos $P = (a, b)$ con coordenadas racionales son construibles con regla y compás.

Corolario

Los puntos $P = (a, b)$ con coordenadas racionales son construibles con regla y compás.

Corolario

Los numeros construibles son densos en $\mathbb{R}^2$.

Pregunta

¿ Hay números construibles que no son números racionales?

Pregunta

¿ Hay números construibles que no son números racionales?

Respuesta

Si, por ejemplo $\sqrt{2}$ es construible.

Proposición

Si $r \geq 0$ es construible, entonces $\sqrt{r}$ es construible

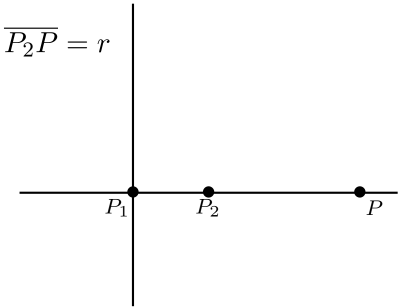


Figura: raíz cuadrada

Proposición

Si $r \geq 0$ es construible, entonces $\sqrt{r}$ es construible

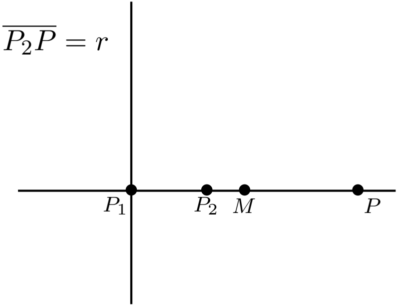


Figura: raíz cuadrada

Proposición

Si $r \geq 0$ es construible, entonces $\sqrt{r}$ es construible.

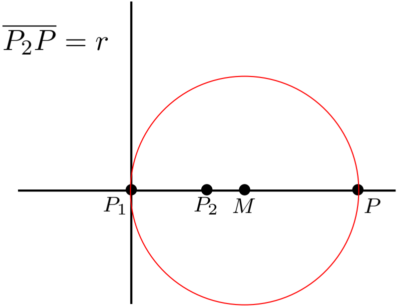


Figura: raíz cuadrada

Proposición

Si $r \geq 0$ es construible, entonces $\sqrt{r}$ es construible.

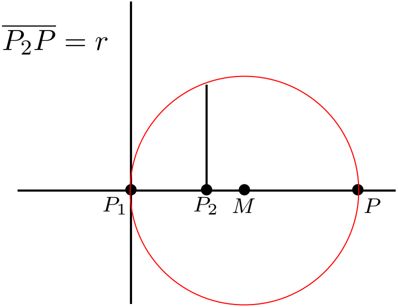


Figura: raíz cuadrada

Proposición

Si $r \geq 0$ es construible, entonces $\sqrt{r}$ es construible.

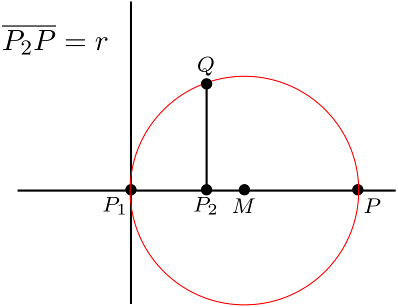


Figura: raíz cuadrada

Proposición

Si $r \geq 0$ es construible, entonces $\sqrt{r}$ es construible.

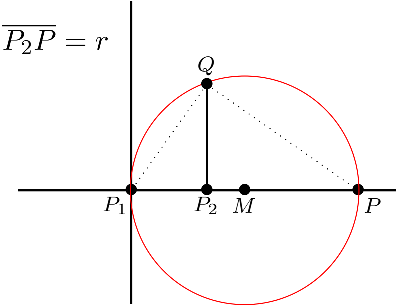
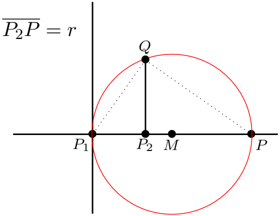
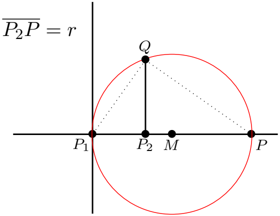


Figura: raíz cuadrada

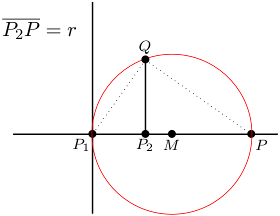


Se tiene que $\triangle P_1P_2Q \simeq \triangle QP_2P$.



Se tiene que $\triangle P_1P_2Q \simeq \triangle QP_2P$.Luego

$$\frac{\overline{P_1P_2}}{\overline{QP_2}} = \frac{\overline{P_2Q}}{\overline{P_2P}}.$$



Se tiene que $\triangle P_1P_2Q \simeq \triangle QP_2P$.Luego

$$\frac{\overline{P_1P_2}}{\overline{QP_2}} = \frac{\overline{P_2Q}}{\overline{P_2P}}.$$

Por lo tanto,

$$\frac{1}{\overline{P_2Q}} = \frac{\overline{P_2Q}}{r}$$

De donde tenemos que $r = (\overline{P_2Q})^2$

El siguiente número es construible.

El siguiente número es construible.

$$\alpha = \frac{-1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}$$

Pregunta

¿ Todos los números reales son cosntruibles con regla y compás?

Para dar respuesta a esta necesitaremos un poco de teoría de campos

Recordemos que un campo es un conjunto no vacío K junto con dos operaciones $+$ y $\bullet$ (suma y producto) que satisfacen:

(a) $(a+b)+c = a+(b+c)\ \forall a,b,c \in K$.

(b) Existe un elemento 0 tal que $a+0 = a = 0+a\ \forall a \in K$

(c) Para todo $a \in K$, existe un elemento $-a \in K$ tal que $a+(-a) = 0$

(d) $a+b = b+a\ \forall a,b \in K$.

(e) $a(bc) = (ab)c\ \forall a,b,c \in K$.

(f) Existe un elemento 1 tal que $a1 = a = 1a\ \forall a \in K$.

(g) Para todo elemento $0 \neq a \in K$, existe un elemento a^{-1} tal que $aa^{-1} = 1$.

(h) $ab = ba\ \forall a,b \in K$.

(i) $a(b+c) = ab+ac\ \forall a,b,c \in K$.

Ejemplos

1. $\mathbb{Q}$
2. $\mathbb{R}$
3. $\mathbb{C}$
4. $\mathbb{Z}_p$
5. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

Subcampo

Sea K un campo y $F \subseteq K$. Se dice que F es un subcampo de K si F es un campo cuando restringuimos las operaciones de K a F.

Subcampo

Sea K un campo y $F \subseteq K$. Se dice que F es un subcampo de K si F es un campo cuando restringuimos las operaciones de K a F.

Ejemplos

1. $\mathbb{Q}$ es un subcampo de $\mathbb{R}$
2. $\mathbb{R}$ es un subcampo de $\mathbb{C}$, etc.

Subcampo

Sea K un campo y $F \subseteq K$. Se dice que F es un subcampo de K si F es un campo cuando restringuimos las operaciones de K a F.

Ejemplos

1. $\mathbb{Q}$ es un subcampo de $\mathbb{R}$
2. $\mathbb{R}$ es un subcampo de $\mathbb{C}$, etc.

El ejemplo importante de está plática

Denotemos por C al conjunto de los números construibles. Por todo lo hecho anterior, tenemos que C es un subcampo y además

$$\mathbb{Q} \subsetneq C \subseteq \mathbb{R}.$$

Notemos que en lo anterior $\mathbb{Q} \subsetneq C$ pues $\sqrt{2}$ es construible pero no es racional.

Notemos que en lo anterior $\mathbb{Q} \subsetneq C$ pues $\sqrt{2}$ es construible pero no es racional.

Pregunta

¿La contención $C \subseteq \mathbb{R}$ es propia?

Notemos que en lo anterior $\mathbb{Q} \subsetneq C$ pues $\sqrt{2}$ es construible pero no es racional.

Pregunta

¿La contención $C \subseteq \mathbb{R}$ es propia?

Para dar una respuesta, necesitaremos la teoría de campos.

Si F es un subcampo de K, se puede ver que K es un F-espacio vectorial.

En efecto,

1. La suma en K es la suma de K vista como campo.
2. Dados $v \in K$ y un $\lambda \in F$, se define el producto λv como el producto de los elementos de λ y v dentro de K. Esto es, se multiplican los elementos λ y v utilizando el producto del campo K pues $F \subseteq K$.

Ejemplos

1. $\mathbb{R}$ es un $\mathbb{Q}$-espacio vectorial.
2. $\mathbb{C}$ es un $\mathbb{R}$-espacio vectorial
3. $\mathbb{Q}(\sqrt{2})$ es un $\mathbb{Q}$-espacio vectorial.

Ejemplos

1. $\mathbb{R}$ es un $\mathbb{Q}$-espacio vectorial.
2. $\mathbb{C}$ es un $\mathbb{R}$-espacio vectorial
3. $\mathbb{Q}(\sqrt{2})$ es un $\mathbb{Q}$-espacio vectorial.

Nuestro ejemplo

El conjunto de números construibles C es un $\mathbb{Q}$-espacio vectorial.

Grado de extensión

Sea $F \subseteq K$ un subcampo de K. Se define el **grado de extensión** del campo K respecto a F como la dimensión de K visto como F-espacio vectorial y se denota por $[K : E]$. Esto, es

$$[K : F] = \dim_F(K).$$

Ejemplos

1. $[\mathbb{C} : \mathbb{R}] = 2$ pues $\beta = \{1, i\}$ es una $\mathbb{R}$-base.
2. $[\mathbb{R} : \mathbb{Q}] = \infty$
3. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ pues $\beta = \{1, \sqrt{2}\}$ es una $\mathbb{Q}$-base.

Sea $F \subseteq K$ un subcampo de K, en este caso se dice que K es una extensión de campos de F y lo denotaremos por K/F. Se dice que K es una extensión finita de F si $[K : F] < \infty$.

Sea $F \subseteq K$ un subcampo de K, en este caso se dice que K es una extensión de campos de F y lo denotaremos por K/F. Se dice que K es una extensión finita de F si $[K : F] < \infty$.

Fórmula del grado

Sean $E \subseteq F \subseteq K$ campos. Entonces K/E es finita si y sólo si K/F y F/E son extensiones finitas y es este caso

$$[K : E] = [K : F][F : E].$$

Dado un subcampo F de $\mathbb{R}$, se ve fácilmente que $\mathbb{Q} \subseteq F$.

Definición

Sea F un subcampo de $\mathbb{R}$.

(a) El F-**plano** es $F \times F = \{(a, b) \mid a, b \in F\}$. A un punto $P = (a, b) \in F \times F$, se le llama un F-**punto**.

(b) Una F-**linea** es una linea en $\mathbb{R}^2$ determinada por dos F-puntos.

(c) Una F-circunferencia es una circunferencia en $\mathbb{R}^2$ con centro un F-punto P que pasa a tráves de otro F punto Q.

Lema

Sea F un subcampo de $\mathbb{R}$.

(a) Si l es una F-linea entonces su ecuación está dada por ecuación: $ax + by + c = 0$ donde $a, b, c \in F$.

(b) Si C es una F-circunferencia su ecuación tiene la forma $x^2 + y^2 + ax + by + c = 0$ con $a, b, c \in F$.

Lema

Sea F un subcampo de $\mathbb{R}$.

(a) Si l es una F-linea entonces su ecuación está dada por ecuación: $ax + by + c = 0$ donde $a, b, c \in F$.

(b) Si C es una F-circunferencia su ecuación tiene la forma $x^2 + y^2 + ax + by + c = 0$ con $a, b, c \in F$.

Idea de la dem de (a):
Sean $P = (a, b)$ y $Q = (c, d)$ dos F-puntos distintos, tal que $a \neq c$. Entonces la F-linea que determinan tiene por ecuación $y - b = \frac{d-b}{c-a}(x - a)$. Luego, como F es un subcampo de $\mathbb{R}$, tenemos que después de simplificar, tenemos la ecuación con las caaracterísticas deseadas.

Proposición

Sea F un subcampo de $\mathbb{R}$.

(a) Sean l y l' dos F-lineas distintas. Si $l \cap l' \neq \emptyset$ entonces $l \cap l'$ consiste de un F-punto.

(b) Sean l una F-linea y C una F-circunferencia. Si $l \cap C \neq \emptyset$ entonces $l \cap C$, consiste de a más dos puntos en el $F(\sqrt{D})$-plano para algún $D > 0$ y $D \in F$.

(c) Sean C y C' dos F-circunferencias. Si $C \cap C' \neq \emptyset$, entonces $C \cap C'$ consiste en a lo más dos puntos en el $F(\sqrt{D})$-plano para algún $D \in F$ con $D > 0$.

$$\text{Con } F(\sqrt{D}) = F \text{ si } \sqrt{D} \in F \text{ y}$$

$$F(\sqrt{D}) := \{a + b\sqrt{D} \mid a, b \in F\}.$$

Idea de la prueba

Básicamente es por que se tienen que resolver ecuaciones a lo más cuadráticas.

Teorema

Sea a un número real construible. Entonces existe una cadena de subcampos de $\mathbb{R}$

$$\mathbb{Q} = F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_n = K$$

tal que

(a) K es un subcampo de $\mathbb{R}$ tal que $a \in K$.

(b) Para $i = 0, \ldots, n-1$ se tiene que

$$F_{i+1} = F_i(\sqrt{d_i})$$

con $d_i \in F_i$ y $d_i > 0$ y tal que $\sqrt{d_i} \notin F_i$.

Y además

$$[K : \mathbb{Q}] = 2^n$$

Campo generado por un elemento

Sea $\alpha \in \mathbb{R}$ un número real, denotamos por $\mathbb{Q}(\alpha)$ al menor subcampo de $\mathbb{R}$ que contiene a $\mathbb{Q}$ y α.

Ejemplos

Sea $\alpha \in \mathbb{R}$ con $\alpha > 0$ tal que $\sqrt{\alpha} \notin \mathbb{Q}$. Entonces

$$\mathbb{Q}(\alpha) = \{a + b\sqrt{\alpha} \mid a, b \in \mathbb{Q}\}.$$

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}.$$

Definición

Sea $\alpha \in \mathbb{R}$, se dice que α es **algebraico** sobre $\mathbb{Q}$ si existe un polinomio no nulo $p(x) \in \mathbb{Q}[x]$ tal que $p(\alpha) = 0$.
En caso contrario se dice que α es trascendente.

Sea $\alpha \in \mathbb{R}$ y consideremos el subcampo $\mathbb{Q}(\alpha)$. Como $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$, tiene sentido preguntarse cual es la dimensión de $\mathbb{Q}(\alpha)$ como $\mathbb{Q}$ espacio vectorial.

Teorema

Sea $\alpha \in \mathbb{R}$ algebraico sobre $\mathbb{Q}$ y sea $p(x) \in \mathbb{Q}[x]$ irreducible tal que $p(\alpha) = 0$. Entonces

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \text{grad}(p(x)).$$

Proposición

Sea F un subcampo de $\mathbb{R}$. Si $[F : \mathbb{Q}] = n < \infty$, entonces todo elemento de F es algebraico sobre $\mathbb{Q}$.

Proposición

Sea F un subcampo de $\mathbb{R}$. Si $[F:\mathbb{Q}] = n < \infty$, entonces todo elemento de F es algebraico sobre $\mathbb{Q}$.

Idea de la prueba. Dado $\alpha \in F$, consideramos el conjunto

$$\{1, \alpha, \alpha^2, \ldots, \alpha^n\}.$$

El cual es linealmente dependiente. Luego existen escalares no todos nulos tal que $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$.

Teorema

Si $\alpha \in \mathbb{R}$ es construible, entonces α es <u>*algebraico*</u> y $\underline{[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k}$ para algún $k \geq 0$.

Definición de ángulo construible

Sea θ un ángulo. Se dice que θ es construible con regla y compás si se pueden construir dos rectas tal que uno de los ángulos entre las dos rectas es θ (los ángulos son medidos en el sentido contrario a las manecillas del reloj).

El ángulo de 60 es construible.

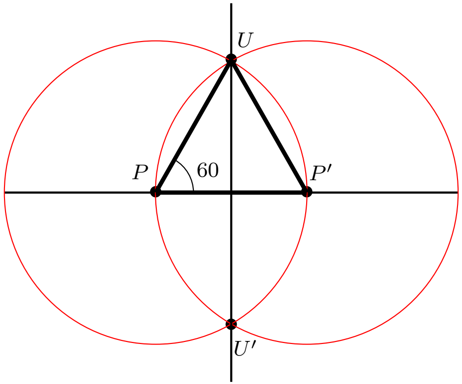


Figura: ángulo de 60

El ángulo θ es construible con regla y compás si y solo si el punto $P = (\cos(\theta), \operatorname{sen}(\theta))$ es un punto construible si y sólo si $\cos(\theta)$ y $\operatorname{sen}(\theta)$ son número reales construibles.

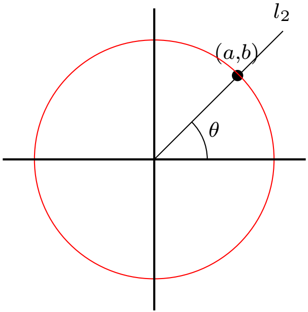


Figura: ángulo construible

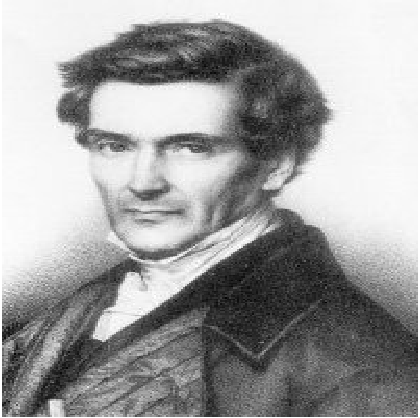
Problema 1

Uno de los problemas de los Griegos es si dado un ángulo construible θ se puede construir $\frac{\theta}{3}$.

Problema 1

Uno de los problemas de los Griegos es si dado un ángulo construible θ se puede construir $\frac{\theta}{3}$.

Para dar una respuesta negativa, basta ver que existe un ángulo construible θ tal que $\frac{\theta}{3}$ no es construible. Para eso, tenemos el siguiente resultado.



Pierre Wantzel, matemático Fránces

Proposición (P.Wantzel, 1837)

Es imposible trisecar el ángulo de 60 grados por regla y compás.

Proposición (P.Wantzel, 1837)

Es imposible trisecar el ángulo de 60 grados por regla y compás.

Basta ver que algunos de $\cos(20)$ y $\operatorname{sen}(20)$ no es const.

Proposición (P.Wantzel, 1837)

Es imposible trisecar el ángulo de 60 grados por regla y compás.

Basta ver que algunos de cos(20) y sen(20) no es const. Veamos que $\alpha = \cos(20)$ no es construible.
Tenemos la fórmula del triple de un ángulo

$$\cos(3\theta) = 4(\cos(\theta))^3 - 3\cos(\theta).$$

Proposición (P.Wantzel, 1837)

Es imposible trisecar el ángulo de 60 grados por regla y compás.

Basta ver que algunos de $\cos(20)$ y $\mathrm{sen}(20)$ no es const. Veamos que $\alpha = \cos(20)$ no es construible.
Tenemos la fórmula del triple de un ángulo

$$\cos(3\theta) = 4(\cos(\theta))^3 - 3\cos(\theta).$$

$$\frac{1}{2} = \cos(60) = 4\alpha^3 - 3\alpha.$$

Proposición (P.Wantzel, 1837)

Es imposible trisecar el ángulo de 60 grados por regla y compás.

Basta ver que algunos de cos(20) y sen(20) no es const. Veamos que $\alpha = \cos(20)$ no es construible.
Tenemos la fórmula del triple de un ángulo

$$\cos(3\theta) = 4(\cos(\theta))^3 - 3\cos(\theta).$$

$$\frac{1}{2} = \cos(60) = 4\alpha^3 - 3\alpha.$$

Tenemos $8\alpha^3 - 6\alpha - 1 = 0$. Es decir, tenemos que α es raíz del polinomio $f(x) = 8x^3 - 6x - 1$.

Proposición (P.Wantzel, 1837)

Es imposible trisecar el ángulo de 60 grados por regla y compás.

Basta ver que algunos de cos(20) y sen(20) no es const. Veamos que $\alpha = \cos(20)$ no es construible.
Tenemos la fórmula del triple de un ángulo

$$\cos(3\theta) = 4(\cos(\theta))^3 - 3\cos(\theta).$$

$$\frac{1}{2} = \cos(60) = 4\alpha^3 - 3\alpha.$$

Tenemos $8\alpha^3 - 6\alpha - 1 = 0$. Es decir, tenemos que α es raíz del polinomio $f(x) = 8x^3 - 6x - 1$.

$$f(x) \text{ irreducible} \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3.$$

Proposición (P.Wantzel, 1837)

Es imposible trisecar el ángulo de 60 grados por regla y compás.

Basta ver que algunos de cos(20) y sen(20) no es const. Veamos que $\alpha = \cos(20)$ no es construible.
Tenemos la fórmula del triple de un ángulo

$$\cos(3\theta) = 4(\cos(\theta))^3 - 3\cos(\theta).$$

$$\frac{1}{2} = \cos(60) = 4\alpha^3 - 3\alpha.$$

Tenemos $8\alpha^3 - 6\alpha - 1 = 0$. Es decir, tenemos que α es raíz del polinomio $f(x) = 8x^3 - 6x - 1$.

$$f(x) \text{ irreducible} \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3.$$

$$\alpha \text{ construible} \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k,$$

Proposición (P.Wantzel, 1837)

Es imposible trisecar el ángulo de 60 grados por regla y compás.

Basta ver que algunos de cos(20) y sen(20) no es const.Veamos que $\alpha = \cos(20)$ no es construible.
Tenemos la fórmula del triple de un ángulo

$$\cos(3\theta) = 4(\cos(\theta))^3 - 3\cos(\theta).$$

$$\frac{1}{2} = \cos(60) = 4\alpha^3 - 3\alpha.$$

Tenemos $8\alpha^3 - 6\alpha - 1 = 0$. Es decir, tenemos que α es raíz del polinomio $f(x) = 8x^3 - 6x - 1$.

$$f(x) \text{ irreducible} \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3.$$

$$\alpha \text{ construible} \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k, !!!!!!!!!!$$

Proposición (P. Wantzel, 1837)

El número $\sqrt[3]{2}$ no es construible y por lo tanto no se puede duplicar el cubo de volumen 1.

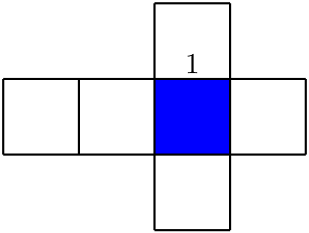


Figura: duplicación del cubo

Proposición (P. Wantzel, 1837)

El número $\sqrt[3]{2}$ no es construible y por lo tanto no se puede duplicar el cubo de volumen 1.

Proposición (P. Wantzel, 1837)

El número $\sqrt[3]{2}$ no es construible y por lo tanto no se puede duplicar el cubo de volumen 1.

Por un lado, $\alpha = \sqrt[3]{2}$ es ráiz del polinomio $x^3 - 2$.

Proposición (P. Wantzel, 1837)

El número $\sqrt[3]{2}$ no es construible y por lo tanto no se puede duplicar el cubo de volumen 1.

Por un lado, $\alpha = \sqrt[3]{2}$ es ráiz del polinomio $x^3 - 2$.

$$f(x) = x^3 - 2 \text{ irreducible } \Rightarrow \ [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

Proposición (P. Wantzel, 1837)

El número $\sqrt[3]{2}$ no es construible y por lo tanto no se puede duplicar el cubo de volumen 1.

Por un lado, $\alpha = \sqrt[3]{2}$ es ráiz del polinomio $x^3 - 2$.

$$f(x) = x^3 - 2 \text{ irreducible } \Rightarrow \; [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

$$\alpha = \sqrt[3]{2} \text{ construible } \Rightarrow [\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q})] = 2^k,$$

Proposición (P. Wantzel, 1837)

El número $\sqrt[3]{2}$ no es construible y por lo tanto no se puede duplicar el cubo de volumen 1.

Por un lado, $\alpha = \sqrt[3]{2}$ es ráiz del polinomio $x^3 - 2$.

$$f(x) = x^3 - 2 \text{ irreducible} \Rightarrow \ [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

$$\alpha = \sqrt[3]{2} \text{ construible} \Rightarrow [\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q})] = 2^k, !!!!!!!!!!.$$

Cuadratura del círculo

Gado un círculo de área A se quiere construir un cuadrado con área A.

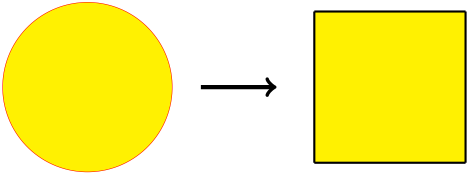


Figura: cuadratura del círculo

Podemos suponer que el radio del círculo es 1 y entonces el círculo tiene area π. Luego, queremos encontrar un cuadrado cuyos lados son de longitud $\sqrt{\pi}$. Es decir, queremos saber si $\sqrt{\pi}$ es un número construible.

Carl Louis Ferdinand von Lindemann, matemático Alemán

Teorema (Lindemann, 1882)

El número π es trascendente.

Teorema (Lindemann, 1882)

El número π es trascendente.

Lindemann

El número $\alpha = \sqrt{\pi}$ no es construible y por lo tanto no se puede cuadrar el círculo de área π.

$$\pi \text{ construible} \Rightarrow \pi \text{ es algebraico,}$$

Teorema (Lindemann, 1882)

El número π es trascendente.

Lindemann

El número $\alpha = \sqrt{\pi}$ no es construible y por lo tanto no se puede cuadrar el círculo de área π.

$$\pi \text{ construible } \Rightarrow \pi \text{ es algebraico}, !!!!!!!!!$$

Corolario

Los números construibles son un subcampo propio de los reales.

Carl Friedrich Gauss, matemático Alemán

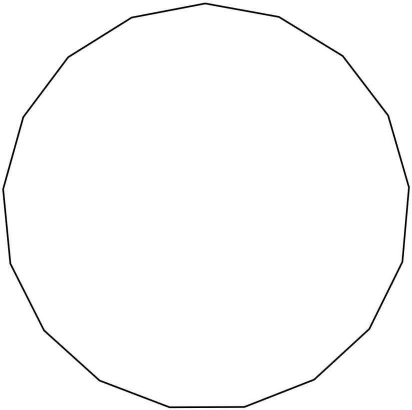
Gauss a los 18 años (el 30 de marzo de 1796, a un mes de cumplir 19 años) descubrió la fórmula

$$\cos\left(\frac{2\pi}{17}\right) = \frac{-1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}$$

Gauss a los 18 años (el 30 de marzo de 1796, a un mes de cumplir 19 años) descubrió la fórmula

$$\begin{aligned}\cos\left(\frac{2\pi}{17}\right) &= \frac{-1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} \\ &\quad + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}\end{aligned}$$

Gauss descubrio la fórmula resolviendo varios sistemas de ecuaciones que involucran ecuaciones cuadráticas.



Como consecuencia de la fórmula anterior, Gauss probó que el Heptadecágono regular es construible con regla y compás.

El problema había permanecido habierto desde los Griegos

El problema había permanecido habierto desde los Griegos

Gracias a este resultado Gauss se decidió por estudiar matemáticas.

De hecho, Gauss le expresó a Bolyai el deseo de decorar su lápida con un heptadecágono. Esto no se pudo hacer, pero en un lado de la base el monumento a Gauss en Brunswick había un diseño. En la parte trasera del monumento había una estrella de 17 puntas, por que el encargado de esculpir el diseño Howaldt se percató de la dificultad de llevar a cabo este deseo sin que la figura fuera confundida con un círculo.

¿Cúales son todos los poligonos regulares construibles con regla y compás

¿Cúales son todos los poligonos regulares construibles con regla y compás

Gauss (Disquisitiones arithmeticae)

Gauss demostró en 1801 que si n es de la forma $n = 2^k p_1 p_2 \dots p_k$ con p_i primos de Fermat, entonces el polígono regular de n-lados es construible con regla y compás

¿Cúales son todos los poligonos regulares construibles con regla y compás

Gauss (Disquisitiones arithmeticae)

Gauss demostró en 1801 que si n es de la forma $n = 2^k p_1 p_2 \dots p_k$ con p_i primos de Fermat, entonces el polígono regular de n-lados es construible con regla y compás

P. Wantzel

Si el polígono regular de n-lados es construible con regla y compás, entonces n es de la forma $n = 2^k p_1 p_2 \dots p_k$ con p_i primos de Fermat.

Recordemos que un número primo de Fermat es un número primo de la forma

$$2^{2^n} + 1.$$

Los únicos numeros primos de Fermat conocidos son: 3, 5, 17, 257, 65537.

GRACIAS