Seminario del Profesorado en Matemática

Justificación algebraica de las construcciones con regla y compás

El subtítulo

Luis Fernando Crespo

Date (optional)

Replace this box e. g. by the coat of arms of the university.

Universidad Nacional de Salta
Facultad de Ciencias Exactas

Director
Prof. A. Sángari

Referees
Prof. Dr. aaa bbb
Prof. Dr. xxx yyy

Date of the graduation (optional)
xx.yy.zzzz

A mis queridos .....

Índice general

Resumen

el origen de las inversiones

1 Introducción

Definición 1. Un cuerpo F se dice que es una extensión de cuerpo un K(o simplemente una extensión de K) siempre que K sea un subcuerpo de F. La notación que se usa habitualmente para designar una extensión es F/K o también $F : K$.

Se dice que una extensión F/K es finita si F como K-espacio vectorial es de dimensión finita. A la dimensión de este espacio vectorial se le llama grado de la extensión y se denota $[F : K]$.

Observación 2. Si tomamos a F como un $K-$espacio vectorial, esto nos permite utilizar los conceptos y resultados del álgebra lineal en el estudio de los extensiones de cuerpos.

Ejemplo 3.

1. $[\mathbb{C} : \mathbb{R}] = 2$; ya que cada $\alpha \in \mathbb{C}$ admite una única expresión $\alpha = a + b.i$ con $i^2 = -1$ y $a, b \in \mathbb{R}$, lo cual significa que $\{1, i\}$ constituye una base de $\mathbb{C}$ como $\mathbb{R}-$espacio vectorial.
2. $[\mathbb{C} : \mathbb{R}]$ y $[\mathbb{R} : \mathbb{Q}]$ son extensiones no finitas.
3. $\left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2$,$\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2}, a, b \in \mathbb{Q}\right\}$ $B = \left\{1, \sqrt{2}\right\}$ generan $\mathbb{Q}\sqrt{2}$.

Teorema. *Sea F una extensión de un cuerpo E y E una extensión de un cuerpo K. Entonces $[F : K] = [F : E]\,[E : K]$. Por otra parte $[F : K]$ es finita si y solo si $[F : E]$ y $[E : K]$ son finitas.*

Demostración. Supongamos primero que $K \subset E$ y $E \subset F$ son extensiones finitas. Sean entonces $\{\alpha_1, ..., \alpha_m\}$ una E-base de F, y $\{\beta_1, ..., \beta_n\}$ una K-base de E .

Dado $\gamma \in F$, existen únicos $a_i \in E$ tales que $\gamma = a_1\alpha_1 + ... + a_m\alpha_m$.

A su vez $a_i \in E$, luego existen $b_{ij} \in K$ tales que $a_i = b_{i1}\beta_1 + ... + b_{in}\beta_n$. Por lo tanto

$$\gamma = \sum_{i=1,j=1}^{m.n} b_{ij}\beta_j\alpha_i$$

Entonces $\{\beta_j\alpha_i\}_{i,j=1}^{m.n}$ es un generador de K sobre F.

Es linealmente independiente: Supongamos que $\sum_{i,j} b_{ij}\beta_j\alpha_i = 0$, es decir, $\sum_i a_i\alpha_i = 0$. Como $\{a_i\}_{i=1}^{m}$ es linealmente independiente, entonces $a_i = 0$ para todo $i = 1, ..., m$. Entonces $\{b_{i1}\beta_1 + ... + b_{in}\beta_n\} = 0$. Como $\{\beta_j\}_{j=1}^{n}$ es linealmente independiente , entonces $b_{ij} = 0$ para todo i, j. □

En la situación que $K \subset E \subset F$ del Teorema Elemento 1, E se dice que es un cuerpo intermedio de K en F.

Si F es un cuerpo y $X \subset F$, entonces el **subcuerpo generado** por X es la intersección de todos los subcuerpos de F que contienen a X. Si F es una extensión de cuerpos de K y $X \subset F$ entonces el subcuerpo generado por $K \bigcup X$ se llama el subcuerpo generado por X sobre K y se denota $K(X)$.

Si $X = \{u_1, ..., u_n\}$, entonces el subcuerpo $K(X)$ de F se denota por $K(u_1, ..., u_n)$.El cuerpo $K(u_1, ..., u_n)$ se dice que es una **extensión finitamente generada** de K. Si $X = \{u\}$, entonces $K(u)$ se dice que es una **extensión simple** de K.

Definición 4. Sea F una extensión de cuerpos de K. Un elemento u de F se dice que es **algebraico** sobre K siempre que u sea una raíz de algún polinomio distinto de cero $f \in K[u]$. Si u no es una raíz de cualquier polinomio distinto de cero $f \in K[u]$, u se dice que es **trascendental** sobre K. F se llama **extensión algebraica** de K si cada elemento de F es algebraico sobre K. F se llama **extensión trascendental** si por lo menos un elemento de F es trascendental sobre K.

Ejemplo 5. $\mathbb{C}/\mathbb{R}$ es una extensión simple puesto que $\mathbb{C} = \mathbb{R}(i)$.

Observación 6. Una extensión puede ser simple aunque aparentemente esté generada por un conjunto de varios elementos. Así ejemplo,$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es simple porque como veremos un próximo ejemplo, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

$(\sqrt{2}, \sqrt{3}) \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ por lo tanto $(\sqrt{2}+\sqrt{3}) \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, además $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ por lo que $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Proposición 7. *Toda extensión finita es algebraica.*

Corolario 8. *Sea F/K una extensión y sea $\alpha \in F$ un elemento algebraico sobre K. Entonces la extensión $K(\alpha)/K$ es algebraica.*

Definición 9. Sea F/K una extensión de cuerpos. Entonces el conjunto

$$E = \{u \in F / u\, es\, algebraico\, sobre\, K\}$$

es un subcuerpo de F que contiene a K.(E se llama la **clausura algebraica** de K en F).

1.1. Construcción con regla y compás

Vamos a utilizar las extensiones de cuerpos para resolver dos problemas famosos de la antigüedad:

- ¿Es posible trisecar un ángulo arbitrario solo por construcciones de regla y compás?

- ¿Es posible a través de construcciones de regla y compás duplicar un cubo arbitrario (es decir para construir el lado de un cubo que tiene el doble de la volumen del cubo dado)?

De aquí en más construible sera sinónimo de construible con regla y compás. Dada una linea recta L y un punto un punto P que no este en L, la única linea recta que pasa por P y es paralela a L es construible. Podemos entonces construir dos lineas rectas perpendiculares (ejes). Tomemos una unidad de longitud, y a partir de esta construimos todos los puntos en el plano de coordenadas enteras.

Si F es un subcuerpo del cuerpo $\mathbb{R}$ de los números reales, el plano de F es el subconjunto del plano formado por los puntos de la forma (c, d), con $c \in F$, $d \in F$. Si P ,Q son puntos distintos en el plano de F, la única recta que pasa por P y Q se llama recta en F y el círculo con centro en P y radio el segmento PQ se llama círculo en F. Se verifica que toda linea recta en F tiene una ecuación de la forma $ax + by + c = 0 \ \ (a, b, c) \in F$ y todo círculo en F tiene una ecuación de la forma $x^2 + y^2 + ax + by + c = 0 \ \ (a, b, c) \in F$. Aceptaremos el siguiente resultado:

Lema 10. *Sea F un subcuerpo del cuerpo de los números reales $\mathbb{R}$ y sea L_1, L_2 lineas rectas no paralelas en F y C_1,C_2 círculos distintos en F. Entonces*

1. *$L_1 \cap L_2 = \emptyset$ es un punto en el plano de F.*
2. *$L_1 \cap L_2 = \emptyset$ o consiste en uno o dos puntos en el plano de $F(\sqrt{u})$ para algún $u \in F$, $(u \geq 0)$.*
3. *$C_1 \cap C_2 = \emptyset$ o consiste en uno o dos puntos en el plano de $F(\sqrt{u})$ para algún $u \in F$, $(u \geq 0)$.*

Un número real c se dice construible si el punto $(c, 0)$ puede ser localizado en el plano mediante una sucesión finita de construcciones con regla y compás que comiencen en un punto con coordenadas enteras. Claramente, el número c es construible si y sólo si se puede construir un segmento de longitud $|c|$. Más aún, el punto (c, d) en el plano es construible si y sólo si c y d son construibles. Notemos que los enteros son claramente construibles; además se puede probar los siguientes hechos:

1. Los números racionales son construibles.
2. Si c es construibles, entonces $\sqrt{c}$ también lo es.
3. Si c y d son construibles, entonces $c \pm d$, cd y $c/d \, (d \neq 0)$ son construibles, así los números construibles son un subcuerpo de los números reales.

Proposición 11. *Si un número real c es construible, entonces c es algebraico de grado una potencia de 2 sobre el cuerpo $\mathbb{Q}$ de los racionales.*

Demostración. Como los racionales son construibles, que un número c sea construible significa que el punto $(c, 0)$ puede ser ubicado mediante una sucesión finita de construcciones con regla y compás que comiencen en un punto perteneciente al plano de $\mathbb{Q}$. El primer paso es la construcción de una recta o un círculo, los cuales están determinados por dos puntos (en el caso del círculo el centro y el radio) en el plano de $\mathbb{Q}$. Del mismo modo en las sucesivas etapas construimos una recta o un círculo, a partir de puntos en el plano de $\mathbb{Q}$ o puntos construidos en la etapa anterior. Por el lema 1 el primer punto construido esta en cuerpo $\mathbb{Q}(\sqrt{u})$, con $u \in \mathbb{Q}$ o equivalentemente en el plano de $\mathbb{Q}(v)$ con $v^2 \in \mathbb{Q}$. Esta es una extensión de grado 1 o 2 sobre $\mathbb{Q}$. El próximo punto construido esta en el plano $\mathbb{Q}(v, w) = \mathbb{Q}(v)(w)$ con $w^2 \in \mathbb{Q}(v)$. Luego de numero finitos de pasos tendremos $v_\imath^2 \in \mathbb{Q}(v_1, v_2, ..., v_{\imath-1})$ y $[\mathbb{Q}(v_1, ..., v_{\imath-1}) : \mathbb{Q}(v_1, ..., v_\imath] = 1$ ó 2 $(2 \leq \imath \leq n)$. El punto $(c, 0)$ construido mediante este proceso está en el plano de $F = \mathbb{Q}(v_1, ..., v_n)$. Así $[F : \mathbb{Q}]$ es una potencia de 2 y luego c es algebraico sobre $\mathbb{Q}$. Como $\mathbb{Q} \subset \mathbb{Q}(c) \subset F$ implica que $[\mathbb{Q}(c) : \mathbb{Q}]$ divide a $[F : \mathbb{Q}]$ y por lo tanto el grado de $[\mathbb{Q}(c) : \mathbb{Q}]$ de c sobre $\mathbb{Q}$ es una potencia de 2. □

Corolario 12. *Un ángulo de 60° no puede ser trisecado por construcciones con regla y compás.*

Demostración. Trisecar un ángulo dado θ es equivalente a: dado $\cos\theta$, construir $\cos\theta/3$. En efecto, tener un ángulo θ es equivalente a tener el punto en la circunferencia unidad con ángulo θ, es decir, a tener $(\cos\theta, \sin\theta)$, que es equivalente a tener sólo $\cos\theta$.

Consideremos $\theta = 60°$. Entonces $\cos\theta = 1/2$. Tenemos la identidad :

$$\cos\theta = 4\cos^3\theta/3 - 3\cos\theta/3$$

En este caso si $\beta = \cos 20°$, la fórmula queda

$$4\beta^3 - 3\beta - 1/2 = 0 \Rightarrow 8\beta^3 - 6\beta - 1 = 0 \Rightarrow (2\beta)^3 - 3(2\beta) - 1 = 0$$

Si $\alpha = 2\beta$, nos queda $\alpha^3 - 3\alpha - 1 = 0$. Construir β es equivalente a construir α, pero α es raiz del polinomio $f = x^3 - 3x - 1$ de grado 3 que es irreducible sobre $\mathbb{Q}$. Tenemos entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, luego α no es construible por proposición 11. □

Corolario 13. *Es imposible con regla y compás la construcción para duplicar un cubo de longitud de lado 1 .*

Demostración. Para duplicar el cubo unitario tendríamos que construir $\sqrt[3]{2}$ a partir de $\mathbb{Q}$, pero $\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 3$ que no es potencia de dos, por lo que por proposición 11, no es construible. □

Corolario 14. *Es imposible cuadrar un circulo con construcciones de regla y compás.*

Demostración. Para construir un cuadrado con misma área que un círculo de diámetro 1, tendríamos que construir $\sqrt{\pi}$. Pero si $\sqrt{\pi}$ fuera algebraico, también π sería algebraico. En efecto, si consideramos $\mathbb{Q} \subset \mathbb{Q}(\pi) \subset \mathbb{Q}(\sqrt{\pi})$, entonces la transitividad de grados nos dice $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}(\pi)]\,[\mathbb{Q}(\pi) : \mathbb{Q}]$. Suponiendo el lado izquierdo finito, se tendría $[\mathbb{Q}(\pi) : \mathbb{Q}] < \infty$, absurdo. □

1.2. Teorema Fundamental

Sea F un cuerpo. El conjunto de $Aut\,F$ de los todos los automorfismos $F \to F$ forman un grupo bajo las operaciones de composición de funciones. En general, no es abeliano. Fue un descubrimiento notable de Galois que muchas preguntas acerca de que los cuerpos son, de hecho, equivalentes a las preguntas de teoría de grupos determinados por grupos de automorfismos de cuerpos. Cuando surgen estas preguntas, que implican generalmente no solo a F, sino también a un subcuerpo de F. En otras palabras, nos ocupamos de las extensiones de cuerpo.

Si F es una extensión de un cuerpo$K$, la estructura de F como un K -espacio vectorial tiene mucha significancia. Por lo tanto, parece natural considerar los automorfismos de F que también son K-module maps. Es evidente que el conjunto de todos los automorfismos, es un subgrupo de $Aut\,F$.

Definición 15. Sean E y F extensiones de cuerpos de un cuerpo K. Un función no nula $\sigma : E \to F$ que es tanto un cuerpo y un K-homomorfismo módulo se denomina un K-homomorfismo. Del mismo modo, si un automorfismo de cuerpos $\sigma \in Aut\,F$ es un $K-$homomorfismo, entonces σ se llama un $K-$automorfismo de F. El grupo de todos los $K-$automorfismo de F se llaman el grupo de Galois de F sobre K, y se denota $Aut_K\,F$.

1.3. Extensiones Ciclotómicas

Vamos a examinar los cuerpos de división del polinomio $x^n - 1_K$, con especial atención al caso $K = \mathbb{Q}$. Estos cuerpos de división(descomposición) resultan ser las extensiones abelianas cuyo grupos de Galois son bien conocidos.Un cuerpo F de descomposición(división) sobre un cuerpo K de $x^n - 1_K \in K\,[x]$,(cuando $n \geq 1$) se llama una extensión ciclotómica de orden n. Si la característica de $K = p \neq 0$ y $n = mp^t$ con $(p, m) = 1$, entonces $x^n - 1_K = (x^m - 1)^{p^t}$(EJERCICIO) de modo que una extensión ciclotomica de orden n coincide con una de orden m. Por lo general se supone que la característica de K no divide a n.

La dimensión de una extensión cuerpo ciclotómica de orden n está relacionada con la función de Euler φ de la elemental de números,

2 Título del cap 2

2.1. Revisión

bla bla bla bla bla bla bla bla bla bla bla bla bla PPS bla, see [3, 2].

2.2. Siguiente sección

Agradecimientos

Gracias,Gracias,Gracias

3 Title of the first appendix chapter

3.1. Overview

bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla roughness parameter R_a bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla, see [ISO].

3.2. The next section

Bibliografía

[ISO] ISO 10780:1994, stationary source emissions – measurement of velocity and volume flowrate of gas streams in ducts.

[2] Marquardt, D. W. (1963). An algorithm for least-squares estimation of nonlinear parameters. *SIAM Journal on Applied Mathematics*, 11(2):431 – 441.

[3] Richardson, O. (1921). *The Emission of Electricity from Hot Bodies*. Longmans, Green and co.

Nomenclatura

R_a	arithmetic average roughness
PPS	Polyphenylene sulfide