Justificación Algebraica de las Construcciones con Regla y Compás

Luis Crespo[1] Antonio Sángari[2]

[1]Departamento de Matemática
Universidad Nacional de Salta

[2]Departamento de Matemática
Universidad Nacional de Salta

Seminario del Profesorado, 2012

Índice

Repaso de los conceptos visto hasta el momento

Hasta el momento hemos hablado de Extensiones de cuerpos

, la dimensión de estas extensiones, extensiones algebraica y trascendentes, y un Teorema de extensiones de otras extensiones, que nos permitieron dar una solución algebraica a los problemas delianos que fueron la trisección de un ángulo, la duplicación del cubo y a la cuadratura del círculo, todo esto utilizando solamente la regla y el compás.

Comenzaremos,

dando algunas definiciones que nos brindará ayuda para entender las extensiones ciclotómicas, que es adonde se apunta, para poder en última estancia resolver el problema de la posibilidad de la construcción de polígonos regulares con Regla y Compás.
Estas definiciones fueron extraídas de los libros [Hungerford, 1974] y [Stewart, 2004].

Repaso de los conceptos visto hasta el momento

Hasta el momento hemos hablado de Extensiones de cuerpos

, la dimensión de estas extensiones, extensiones algebraica y trascendentes, y un Teorema de extensiones de otras extensiones, que nos permitieron dar una solución algebraica a los problemas delianos que fueron la trisección de un ángulo, la duplicación del cubo y a la cuadratura del círculo, todo esto utilizando solamente la regla y el compás.

Comenzaremos,

dando algunas definiciones que nos brindará ayuda para entender las extensiones ciclotómicas, que es adonde se apunta, para poder en última estancia resolver el problema de la posibilidad de la construcción de polígonos regulares con Regla y Compás.
Estas definiciones fueron extraídas de los libros [Hungerford, 1974] y [Stewart, 2004].

Polinomios de descomposición

Dado un cuerpo K, podemos asociar a cada polinomio $P \in K[x]$

una extensión algebraica que contenga a todas sus raíces y que sea minimal en algún sentido. Este cuerpo será muy importante más adelante, pues nos permitirá extender aplicaciones de un cuerpo K una extensión suya F.

Definición

Sea F/K una extensión, y $P \in K[x]$. Se dice que P se descompone sobre F si P se factoriza como producto de polinomios de primer grado con coeficientes en F.

Polinomios de descomposición

Dado un cuerpo K, podemos asociar a cada polinomio $P \in K[x]$

una extensión algebraica que contenga a todas sus raíces y que sea minimal en algún sentido. Este cuerpo será muy importante más adelante, pues nos permitirá extender aplicaciones de un cuerpo K una extensión suya F.

Definición

Sea F/K una extensión, y $P \in K[x]$. Se dice que P se descompone sobre F si P se factoriza como producto de polinomios de primer grado con coeficientes en F.

Cuerpos de descomposición

Definición

Sea F/K una extensión, y $P \in K[x]$ un polinomio que se descompone sobre F . Se llama cuerpo de descomposición de P en F sobre K al menor subcuerpo de F que contiene a K y sobre el cual P se descompone.

Ejemplos

1. El cuerpo de descomposición de $P = x^2 - 2 \in \mathbb{Q}[x]$ es $\mathbb{Q}(\sqrt{2})$.
2. El cuerpo de descomposición de $P = x^n - 1 \in \mathbb{Q}[x]$ es $\mathbb{Q}(\zeta)$ donde $\zeta = e^{2\pi i/n}$.

Extensiones Normales

Definición

Se dice que una extensión algebraica F/K es normal si todo polinomio irreducible $P \in K[x]$ que tiene una raíz en F se descompone en factores lineales en $F[x]$

Por ejemplo,

.

1. Tenemos que $\mathbb{Q}(i)/\mathbb{Q}$ es una extensión normal, pues $\mathbb{Q}(i)$ es el cuerpo de descomposición sobre $\mathbb{Q}$, del polinomio irreducible $x^2 - 1$.
2. La extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal porque sólo una de las raíces de $x^3 - 2$ esta en $\mathbb{Q}(\sqrt[3]{2})$, las otras son números complejos .
3. La extensión $\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}$ es normal porque $\mathbb{Q}(e^{2\pi i/n})$ es el cuerpo de descomposición de $x^n - 1$ sobre $\mathbb{Q}$.

Extensiones Normales

Definición

Se dice que una extensión algebraica F/K es normal si todo polinomio irreducible $P \in K[x]$ que tiene una raíz en F se descompone en factores lineales en $F[x]$

Por ejemplo,

.

1. Tenemos que $\mathbb{Q}(i)/\mathbb{Q}$ es una extensión normal, pues $\mathbb{Q}(i)$ es el cuerpo de descomposición sobre $\mathbb{Q}$, del polinomio irreducible $x^2 - 1$.
2. La extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal porque sólo una de las raíces de $x^3 - 2$ esta en $\mathbb{Q}(\sqrt[3]{2})$, las otras son números complejos .
3. La extensión $\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}$ es normal porque $\mathbb{Q}(e^{2\pi i/n})$ es el cuerpo de descomposición de $x^n - 1$ sobre $\mathbb{Q}$.

Extensiones de Galois

Sea F un cuerpo. El conjunto de automorfismos de F , denotado $Aut\ F$ posee estructura de grupo con respecto a la operación de composición. En particular, nos interesará un subgrupo de éste. De esta manera, podremos utilizar la teoría de grupos para estudiar la estructura de las extensiones de cuerpos, esto es, funciones biyectivas de F en F que preservan la adición y la multiplicación.

Definición

Sea F/K una extensión de cuerpos. Se llama Grupo de Galois de la extensión $F/K, Gal(F/K)$, al conjunto de los K-automorfismos de F . Es decir son automorfismos de F que dejan fijo al cuerpo K, $Gal(F/K) = \{\sigma \in Aut(F) : \sigma(a) = a \text{ para todo } a \in K\}$

Extensiones de Galois

Sea F un cuerpo. El conjunto de automorfismos de F , denotado *Aut* F posee estructura de grupo con respecto a la operación de composición. En particular, nos interesará un subgrupo de éste. De esta manera, podremos utilizar la teoría de grupos para estudiar la estructura de las extensiones de cuerpos, esto es, funciones biyectivas de F en F que preservan la adición y la multiplicación.

Definición

Sea F/K una extensión de cuerpos. Se llama Grupo de Galois de la extensión $F/K, Gal(F/K)$, al conjunto de los K-automorfismos de F . Es decir son automorfismos de F que dejan fijo al cuerpo K,
$Gal(F/K) =$
$\{\sigma \in Aut(F) : \sigma(a) = a \text{ } para \text{ } todo \text{ } a \in K\}$

Por Ejemplo...

Por ejemplo,

.

$Gal(\mathbb{C}/\mathbb{R}) = \{id, conj\}$, donde $conj(z) = \overline{z}$ es la conjugación compleja. Se tiene $\mathbb{C} = \mathbb{R}(i)$ y como i y $-i$ son las raíces de $x^2 + 1 \in \mathbb{R}[x]$, los únicos posibles automorfismos son $a + ib \to a + ib$ y $a + ib \to a - ib$. El primero es la identidad y el segundo la conjugación. Este último es un $\mathbb{R}$-automorfismo porque deja fijos a los Reales, es biyectivo (es su propia inverso) y satisface las propiedades de homomorfismo ($\overline{z + w} = \overline{z} + \overline{w}, \overline{z.w} = \overline{z}.\overline{w}, \overline{1} = 1$)

Lo que se esta Trabajando

1. Extensiones Separables. {Ciclotómicos : Extensión de Galois de grado $\varphi(n)$, donde φ es la función de Euler.

Bibliografía

Hungerford, T. (1974).
Algebra.
Graduate Texts in Mathematics. Springer-Verlag.

Stewart, I. (2004).
Galois Theory.
Chapman & Hall/CRC Mathematics. Chapman & Hall/CRC.