Refinamientos de un teorema de Kronecker

R. Toledano
FIQ-UNL-IMAL

7 de mayo de 2010

Raíces de la unidad

Un número complejo α se dice que es una raíz de la unidad si α satisface una ecuación de la forma

$$\alpha^n = 1 \quad \text{para algún } n \in \mathbb{N}.$$

Raíces de la unidad

Un número complejo α se dice que es una raíz de la unidad si α satisface una ecuación de la forma

$$\alpha^n = 1 \quad \texttt{para algún } n \in \mathbb{N}.$$

En otras palabras, decimos que α es una raíz de la unidad si existen k y $n \in \mathbb{N}$ tales que $\alpha = e^{2\pi ik/n}$.

Un teorema de Kronecker

En 1857 Kronecker demuestra el siguiente resultado:

Un teorema de Kronecker

`En 1857 Kronecker demuestra el siguiente resultado:`

Una raíz $\alpha \neq 0$ de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ es una raíz de la unidad si toda raíz β de $f(x)$ satisface $|\beta| \leq 1$.

Refinamientos del teorema de Kronecker

En 1964 Schinzel y Zassenhaus demuestran el siguiente resultado:

Refinamientos del teorema de Kronecker

`En 1964 Schinzel y Zassenhaus demuestran el siguiente resultado:`

Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n.

Refinamientos del teorema de Kronecker

`En 1964 Schinzel y Zassenhaus demuestran el siguiente resultado:`

Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n.
Entonces α es una raíz de la unidad si toda raíz β de $f(x)$ satisface

$$|\beta| \leq 1 + \frac{c}{2^n},$$

donde c es una constante absoluta.

Refinamientos del teorema de Kronecker

Algunos años después, se obtuvieron las siguientes mejoras:

Refinamientos del teorema de Kronecker

Algunos años después, se obtuvieron las siguientes mejoras:

(Blansky-Montgomery, 1971.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n.

Refinamientos del teorema de Kronecker

`Algunos años después, se obtuvieron las siguientes mejoras:`

(Blansky-Montgomery, 1971.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n.
Entonces α es una raíz de la unidad si toda raíz β de $f(x)$ satisface

$$|\beta| \leq 1 + \frac{1}{30n^2 \log(6n)}.$$

Refinamientos del teorema de Kronecker

Algunos años después, se obtuvieron las siguientes mejoras:

(Blansky-Montgomery, 1971.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n.
Entonces α es una raíz de la unidad si toda raíz β de $f(x)$ satisface

$$|\beta| \leq 1 + \frac{1}{30n^2 \log(6n)} .$$

(Dobrowolski, 1978.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n.

Refinamientos del teorema de Kronecker

`Algunos años después, se obtuvieron las siguientes mejoras:`

(Blansky-Montgomery, 1971.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n.
Entonces α es una raíz de la unidad si toda raíz β de $f(x)$ satisface

$$|\beta| \leq 1 + \frac{1}{30n^2 \log(6n)}\,.$$

(Dobrowolski, 1978.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n.
Entonces para cada $\epsilon > 0$ existe n_ϵ tal que para todo $n \geq n_\epsilon$ se tiene que α es una raíz de la unidad si toda raíz β de $f(x)$ satisface

$$|\beta| \leq 1 + \frac{1-\epsilon}{n}\left(\frac{\log\log n}{\log n}\right)^3\,.$$

Refinamientos del teorema de Kronecker

(Voutier, 1996.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n.

Refinamientos del teorema de Kronecker

(Voutier, 1996.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n.
Entonces α es una raíz de la unidad si toda raíz β de $f(x)$ satisface

$$|\beta| \leq 1 + \frac{1}{2n} \left(\frac{\log \log n}{\log n} \right)^3 .$$

Refinamientos del teorema de Kronecker

(Voutier, 1996.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n.
Entonces α es una raíz de la unidad si toda raíz β de $f(x)$ satisface

$$|\beta| \leq 1 + \frac{1}{2n} \left(\frac{\log \log n}{\log n} \right)^3 .$$

`Para ciertas clases de polinomios hay resultados mejores:`

Refinamientos del teorema de Kronecker

(Voutier, 1996.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n.
Entonces α es una raíz de la unidad si toda raíz β de $f(x)$ satisface

$$|\beta| \leq 1 + \frac{1}{2n} \left(\frac{\log \log n}{\log n} \right)^3 .$$

`Para ciertas clases de polinomios hay resultados mejores:`
(Smyth, 1971.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico, irreducible y no recíproco $f(x) \in \mathbb{Z}[x]$ de grado n.

Refinamientos del teorema de Kronecker

(Voutier, 1996.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n.
Entonces α es una raíz de la unidad si toda raíz β de $f(x)$ satisface

$$|\beta| \leq 1 + \frac{1}{2n} \left(\frac{\log \log n}{\log n} \right)^3 .$$

`Para ciertas clases de polinomios hay resultados mejores:`
(Smyth, 1971.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico, irreducible y no recíproco $f(x) \in \mathbb{Z}[x]$ de grado n.
Entonces α es una raíz de la unidad si toda raíz β de $f(x)$ satisface

$$|\beta| \leq 1 + \frac{\log \theta}{n} ,$$

donde θ es la única raíz real de $x^3 - x - 1$.

Refinamientos del teorema de Kronecker

(Schinzel, 1973.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n tal que todas sus raíces son reales.

Refinamientos del teorema de Kronecker

(Schinzel, 1973.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n tal que todas sus raíces son reales.
Entonces α es una raíz de la unidad si toda raíz β de $f(x)$ satisface

$$|\beta| < 1 + \frac{\log \frac{1+\sqrt{5}}{2}}{n}.$$

Refinamientos del teorema de Kronecker

(Schinzel, 1973.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n tal que todas sus raíces son reales.
Entonces α es una raíz de la unidad si toda raíz β de $f(x)$ satisface

$$|\beta| < 1 + \frac{\log \frac{1+\sqrt{5}}{2}}{n}.$$

(Borwein-Dobrowolski-Mossinghoff, 2007.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n tal que todos sus coeficientes son impares.

Refinamientos del teorema de Kronecker

(Schinzel, 1973.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n tal que todas sus raíces son reales.
Entonces α es una raíz de la unidad si toda raíz β de $f(x)$ satisface

$$|\beta| < 1 + \frac{\log \frac{1+\sqrt{5}}{2}}{n} .$$

(Borwein-Dobrowolski-Mossinghoff, 2007.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n tal que todos sus coeficientes son impares.
Entonces α es una raíz de la unidad si toda raíz β de $f(x)$ satisface

$$|\beta| \leq 1 + \frac{\log 3}{2n+2} .$$

Refinamientos del teorema de Kronecker

Se conjetura la validez del siguiente resultado:

Refinamientos del teorema de Kronecker

Se conjetura la validez del siguiente resultado:
(Conjetura de Schinzel-Zassenhaus, 1964.) Sea $\alpha \neq 0$ una raíz de un polinomio mónico e irreducible $f(x) \in \mathbb{Z}[x]$ de grado n. Entonces α es una raíz de la unidad si toda raíz β de $f(x)$ satisface

$$|\beta| \leq 1 + \frac{c}{n},$$

donde c es una constante absoluta.

Un problema

Sea $A \subset \mathbb{C}$ un anillo. Sea $f(x) \in A[x]$ un polinomio mónico y de grado n. Sean $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ las raíces de $f(x)$ y supongamos que $\alpha \neq 0$.

Un problema

Sea $A \subset \mathbb{C}$ un anillo. Sea $f(x) \in A[x]$ un polinomio mónico y de grado n. Sean $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ las raíces de $f(x)$ y supongamos que $\alpha \neq 0$.

Hallar condiciones sobre A para asegurar la existencia de una función real $\phi(x) = \phi_A(x)$ que tenga la siguiente propiedad:

α es una raíz de la unidad si

$$|\alpha_i| \leq \phi(n)\,,$$

para todo $i = 1, \ldots, n$.

Ideales en un anillo conmutativo

Sea A un anillo conmutativo. Un ideal $\mathfrak{I}$ de A es un subanillo de A que tiene la siguiente propiedad de *absorción*: para todo $x \in A$ y para todo $y \in \mathfrak{I}$ se tiene que $xy \in \mathfrak{I}$.

Ideales en un anillo conmutativo

Sea A un anillo conmutativo. Un ideal $\mathfrak{I}$ de A es un subanillo de A que tiene la siguiente propiedad de *absorción*: para todo $x \in A$ y para todo $y \in \mathfrak{I}$ se tiene que $xy \in \mathfrak{I}$.

Por ejemplo $\{0\}$ y A son ideales (triviales) de A. Todo ideal de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ con $n \in \mathbb{N}$.

Ideales en un anillo conmutativo

Sea A un anillo conmutativo. Un ideal $\mathfrak{I}$ de A es un subanillo de A que tiene la siguiente propiedad de *absorción*: para todo $x \in A$ y para todo $y \in \mathfrak{I}$ se tiene que $xy \in \mathfrak{I}$.

Por ejemplo $\{0\}$ y A son ideales (triviales) de A. Todo ideal de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ con $n \in \mathbb{N}$.

Hay dos clases importantes de ideales: Un ideal $\mathfrak{I} \neq A$ se dice que es *primo* si cada vez que $xy \in \mathfrak{I}$ entonces $x \in \mathfrak{I}$ o $y \in \mathfrak{I}$.

Ideales en un anillo conmutativo

Sea A un anillo conmutativo. Un ideal $\mathfrak{I}$ de A es un subanillo de A que tiene la siguiente propiedad de *absorción*: para todo $x \in A$ y para todo $y \in \mathfrak{I}$ se tiene que $xy \in \mathfrak{I}$.

Por ejemplo $\{0\}$ y A son ideales (triviales) de A. Todo ideal de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ con $n \in \mathbb{N}$.

Hay dos clases importantes de ideales: Un ideal $\mathfrak{I} \neq A$ se dice que es *primo* si cada vez que $xy \in \mathfrak{I}$ entonces $x \in \mathfrak{I}$ o $y \in \mathfrak{I}$.

Un ideal $\mathfrak{M} \neq A$ se dice que es *maximal* si no hay otro ideal $\mathfrak{I} \neq A$ que lo contenga.

Ideales en un anillo conmutativo

Sea A un anillo conmutativo. Un ideal $\mathfrak{I}$ de A es un subanillo de A que tiene la siguiente propiedad de *absorción*: para todo $x \in A$ y para todo $y \in \mathfrak{I}$ se tiene que $xy \in \mathfrak{I}$.

Por ejemplo $\{0\}$ y A son ideales (triviales) de A. Todo ideal de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ con $n \in \mathbb{N}$.

Hay dos clases importantes de ideales: Un ideal $\mathfrak{I} \neq A$ se dice que es *primo* si cada vez que $xy \in \mathfrak{I}$ entonces $x \in \mathfrak{I}$ o $y \in \mathfrak{I}$.

Un ideal $\mathfrak{M} \neq A$ se dice que es *maximal* si no hay otro ideal $\mathfrak{J} \neq A$ que lo contenga.

Todo ideal maximal es primo.

Ideales en un anillo conmutativo

Sea A un anillo conmutativo. Un ideal $\mathfrak{I}$ de A es un subanillo de A que tiene la siguiente propiedad de *absorción*: para todo $x \in A$ y para todo $y \in \mathfrak{I}$ se tiene que $xy \in \mathfrak{I}$.

Por ejemplo $\{0\}$ y A son ideales (triviales) de A. Todo ideal de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ con $n \in \mathbb{N}$.

Hay dos clases importantes de ideales: Un ideal $\mathfrak{I} \neq A$ se dice que es *primo* si cada vez que $xy \in \mathfrak{I}$ entonces $x \in \mathfrak{I}$ o $y \in \mathfrak{I}$.

Un ideal $\mathfrak{M} \neq A$ se dice que es *maximal* si no hay otro ideal $\mathfrak{J} \neq A$ que lo contenga.

Todo ideal maximal es primo.

La recíproca no es cierta en general. La recíproca vale en los *dominios de Dedekind*, como por ejemplo, $\mathbb{Z}$.

Cuerpos numéricos

Si un cuerpo L contiene a otro cuerpo K se tiene que L es un K-espacio vectorial.

Cuerpos numéricos

Si un cuerpo L contiene a otro cuerpo K se tiene que L es un K-espacio vectorial.

Si $\dim_K(L) = n < \infty$ entonces se dice que L es una *extensión finita de K de grado n*.

Cuerpos numéricos

Si un cuerpo L contiene a otro cuerpo K se tiene que L es un K-espacio vectorial.

Si $\dim_K(L) = n < \infty$ entonces se dice que L es una *extensión finita de* K *de grado* n.

Un *cuerpo numérico* K es una extensión finita del cuerpo de los números racionales.

Cuerpos numéricos

Si un cuerpo L contiene a otro cuerpo K se tiene que L es un K-espacio vectorial.

Si $\dim_K(L) = n < \infty$ entonces se dice que L es una *extensión finita de K de grado n*.

Un *cuerpo numérico* K es una extensión finita del cuerpo de los números racionales.

Por ejemplo, $K = \mathbb{Q}(\sqrt{5}) := \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$ es un cuerpo numérico y es de grado 2 pues $\{1, \sqrt{5}\}$ es una base de K sobre $\mathbb{Q}$.

Cuerpos numéricos

Si un cuerpo L contiene a otro cuerpo K se tiene que L es un K-espacio vectorial.

Si $\dim_K(L) = n < \infty$ entonces se dice que L es una *extensión finita de K de grado n*.

Un *cuerpo numérico* K es una extensión finita del cuerpo de los números racionales.

Por ejemplo, $K = \mathbb{Q}(\sqrt{5}) := \{a + b\sqrt{5} \,:\, a, b \in \mathbb{Q}\}$ es un cuerpo numérico y es de grado 2 pues $\{1, \sqrt{5}\}$ es una base de K sobre $\mathbb{Q}$.

En realidad, todo cuerpo numérico K es de la forma $\mathbb{Q}(\alpha) := \{\sum_{j=0}^{n-1} a_j\alpha^j \,:\, a_j \in \mathbb{Q}\}$ donde α es una raíz de un polinomio mónico e irreducible de grado n con coeficientes enteros.

Anillo de enteros

En todo cuerpo numérico K se tiene el *anillo de enteros* $\mathcal{O}_K$ que se define como $\overline{\mathbb{Z}} \cap K$ donde $\overline{\mathbb{Z}}$ es el conjunto de todos los enteros algebraicos.

Anillo de enteros

En todo cuerpo numérico K se tiene el *anillo de enteros* $\mathcal{O}_K$ que se define como $\overline{\mathbb{Z}} \cap K$ donde $\overline{\mathbb{Z}}$ es el conjunto de todos los enteros algebraicos.

En $\mathcal{O}_K$ todo ideal primo es maximal ($\mathcal{O}_K$ es, en realidad, un dominio de Dedekind).

Anillo de enteros

En todo cuerpo numérico K se tiene el *anillo de enteros* $\mathcal{O}_K$ que se define como $\overline{\mathbb{Z}} \cap K$ donde $\overline{\mathbb{Z}}$ es el conjunto de todos los enteros algebraicos.

En $\mathcal{O}_K$ todo ideal primo es maximal ($\mathcal{O}_K$ es, en realidad, un dominio de Dedekind).

$\mathcal{O}_K$ es finitamente generado sobre $\mathbb{Z}$: existen $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ tales que

$$\mathcal{O}_K = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$$

y, además, $\{\alpha_1, \ldots, \alpha_n\}$ es una base de K sobre $\mathbb{Q}$.

Anillo de enteros

En todo cuerpo numérico K se tiene el *anillo de enteros* $\mathcal{O}_K$ que se define como $\overline{\mathbb{Z}} \cap K$ donde $\overline{\mathbb{Z}}$ es el conjunto de todos los enteros algebraicos.

En $\mathcal{O}_K$ todo ideal primo es maximal ($\mathcal{O}_K$ es, en realidad, un dominio de Dedekind).

$\mathcal{O}_K$ es finitamente generado sobre $\mathbb{Z}$: existen $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ tales que

$$\mathcal{O}_K = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$$

y, además, $\{\alpha_1, \ldots, \alpha_n\}$ es una base de K sobre $\mathbb{Q}$.

En $\mathcal{O}_K$ vale la factorización única a nivel de ideales: para cada ideal no trivial $\mathfrak{I}$ de $\mathcal{O}_K$ existen únicos ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ y únicos enteros positivos $e_1, \ldots, e_s$ tales que

$$\mathfrak{I} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$$

Situación importante

$$\begin{array}{ccc} K & p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_s^{e_s} \\ \Big| & \Big| \\ \mathbb{Q} & p \text{ primo} \end{array}$$

donde $e(\mathfrak{p}_i|p) = e_i$ se denomina *índice de ramificación* de $\mathfrak{p}_i$ sobre p.

Situación importante

$$\begin{array}{ll} K & p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_s^{e_s} \\ \Big| & \Big| \\ \mathbb{Q} & p \text{ primo} \end{array}$$

donde $e(\mathfrak{p}_i|p) = e_i$ se denomina *índice de ramificación* de $\mathfrak{p}_i$ sobre p.

Si algún $e(\mathfrak{p}_i|p) > 1$ se dice que p *ramifica* en K.

Situación importante

$$\begin{array}{cl} K & p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_s^{e_s} \\ | & | \\ \mathbb{Q} & p \text{ primo} \end{array}$$

donde $e(\mathfrak{p}_i|p) = e_i$ se denomina *índice de ramificación* de $\mathfrak{p}_i$ sobre p.

Si algún $e(\mathfrak{p}_i|p) > 1$ se dice que p *ramifica* en K.

En caso contrario, es decir $e(\mathfrak{p}_i|p) = 1$ para $i = 1, \ldots, s$, se dice que p *no ramifica* en K.

Situación importante

$$\begin{array}{ccl} K & p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_s^{e_s} \\ \Big| & \Big| \\ \mathbb{Q} & p \text{ primo} \end{array}$$

donde $e(\mathfrak{p}_i|p) = e_i$ se denomina *índice de ramificación* de $\mathfrak{p}_i$ sobre p.

Si algún $e(\mathfrak{p}_i|p) > 1$ se dice que p *ramifica* en K.

En caso contrario, es decir $e(\mathfrak{p}_i|p) = 1$ para $i = 1, \ldots, s$, se dice que p *no ramifica* en K.

En cualquier caso, se dice que $\mathfrak{p}_i$ está *sobre* p.

Situación importante

$$\begin{array}{ll} K & p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_s^{e_s} \\ \Big| & \Big| \\ \mathbb{Q} & p \text{ primo} \end{array}$$

donde $e(\mathfrak{p}_i|p) = e_i$ se denomina *índice de ramificación* de $\mathfrak{p}_i$ sobre p.

Si algún $e(\mathfrak{p}_i|p) > 1$ se dice que p *ramifica* en K.

En caso contrario, es decir $e(\mathfrak{p}_i|p) = 1$ para $i = 1, \ldots, s$, se dice que p *no ramifica* en K.

En cualquier caso, se dice que $\mathfrak{p}_i$ está *sobre* p.

Solamente una cantidad finita de primos p ramifican en K.

Discriminante de K

Cada cuerpo numérico K tiene asociado un número entero d_K que se denomina *discriminante* de K que tiene, en particular, la siguiente propiedad:

Discriminante de K

Cada cuerpo numérico K tiene asociado un número entero d_K que se denomina *discriminante* de K que tiene, en particular, la siguiente propiedad:

Un número primo p ramifica en K sí y sólo sí $p | d_K$

Extensiones de Galois

Cada cuerpo numérico K tiene asociado un grupo denominado *grupo de automorfismos de* K *sobre* $\mathbb{Q}$.

Extensiones de Galois

Cada cuerpo numérico K tiene asociado un grupo denominado *grupo de automorfismos de K sobre $\mathbb{Q}$*.

A tal grupo se lo denota por $\mathrm{Aut}_{\mathbb{Q}}(K)$ y sus elementos son isomorfismos de cuerpos $\sigma\colon K \to K$ tales que $\sigma(x) = x$ para todo $x \in \mathbb{Q}$.

Extensiones de Galois

Cada cuerpo numérico K tiene asociado un grupo denominado *grupo de automorfismos de* K *sobre* $\mathbb{Q}$.

A tal grupo se lo denota por $\mathrm{Aut}_{\mathbb{Q}}(K)$ y sus elementos son isomorfismos de cuerpos $\sigma\colon K \to K$ tales que $\sigma(x) = x$ para todo $x \in \mathbb{Q}$.

Siempre se tiene que $|\mathrm{Aut}_{\mathbb{Q}}(K)| \leq n$, donde n es el grado de K sobre $\mathbb{Q}$.

Extensiones de Galois

Cada cuerpo numérico K tiene asociado un grupo denominado *grupo de automorfismos de* K *sobre* $\mathbb{Q}$.

A tal grupo se lo denota por $\mathrm{Aut}_{\mathbb{Q}}(K)$ y sus elementos son isomorfismos de cuerpos $\sigma\colon K \to K$ tales que $\sigma(x) = x$ para todo $x \in \mathbb{Q}$.

Siempre se tiene que $|\mathrm{Aut}_{\mathbb{Q}}(K)| \leq n$, donde n es el grado de K sobre $\mathbb{Q}$.

Cuando $|\mathrm{Aut}_{\mathbb{Q}}(K)| = n$, se dice que K es una *extensión de Galois* de $\mathbb{Q}$ y se escribe $\mathrm{Gal}(K/\mathbb{Q})$ en lugar de $\mathrm{Aut}_{\mathbb{Q}}(K)$.

Extensiones de Galois

Cada cuerpo numérico K tiene asociado un grupo denominado *grupo de automorfismos de K sobre $\mathbb{Q}$*.

A tal grupo se lo denota por $\mathrm{Aut}_{\mathbb{Q}}(K)$ y sus elementos son isomorfismos de cuerpos $\sigma\colon K \to K$ tales que $\sigma(x) = x$ para todo $x \in \mathbb{Q}$.

Siempre se tiene que $|\mathrm{Aut}_{\mathbb{Q}}(K)| \leq n$, donde n es el grado de K sobre $\mathbb{Q}$.

Cuando $|\mathrm{Aut}_{\mathbb{Q}}(K)| = n$, se dice que K es una *extensión de Galois* de $\mathbb{Q}$ y se escribe $\mathrm{Gal}(K/\mathbb{Q})$ en lugar de $\mathrm{Aut}_{\mathbb{Q}}(K)$.

A $\mathrm{Gal}(K/\mathbb{Q})$ se lo denomina el *grupo de Galois de la extensión K de $\mathbb{Q}$*.

El automorfismo de Frobenius

Si un ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ está sobre un número primo p, entonces el cuerpo $\mathcal{O}_K/\mathfrak{p}$ es una extensión finita del cuerpo $\mathbb{Z}/p\mathbb{Z}$ de grado $t_{\mathfrak{p}}$.

El automorfismo de Frobenius

Si un ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ está sobre un número primo p, entonces el cuerpo $\mathcal{O}_K/\mathfrak{p}$ es una extensión finita del cuerpo $\mathbb{Z}/p\mathbb{Z}$ de grado $t_{\mathfrak{p}}$.

Al número $t_{\mathfrak{p}}$ se lo denomina *grado residual de* $\mathfrak{p}$ *sobre* p y usualmente se lo denota por $f(\mathfrak{p}|p)$.

El automorfismo de Frobenius

Si un ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ está sobre un número primo p, entonces el cuerpo $\mathcal{O}_K/\mathfrak{p}$ es una extensión finita del cuerpo $\mathbb{Z}/p\mathbb{Z}$ de grado $t_\mathfrak{p}$.

Al número $t_\mathfrak{p}$ se lo denomina *grado residual de* $\mathfrak{p}$ *sobre* p y usualmente se lo denota por $f(\mathfrak{p}|p)$.

Cuando la extensión K de $\mathbb{Q}$ es de Galois, todos los grados residuales $f(\mathfrak{p}_i|p)$ son iguales. Denotamos por t a este valor común.

El automorfismo de Frobenius

Si un ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ está sobre un número primo p, entonces el cuerpo $\mathcal{O}_K/\mathfrak{p}$ es una extensión finita del cuerpo $\mathbb{Z}/p\mathbb{Z}$ de grado $t_\mathfrak{p}$.

Al número $t_\mathfrak{p}$ se lo denomina *grado residual de* $\mathfrak{p}$ *sobre* p y usualmente se lo denota por $f(\mathfrak{p}|p)$.

Cuando la extensión K de $\mathbb{Q}$ es de Galois, todos los grados residuales $f(\mathfrak{p}_i|p)$ son iguales. Denotamos por t a este valor común.

Además, para cada $\mathfrak{p}$ arriba de p existe un elemento $\sigma_\mathfrak{p} \in \mathrm{Gal}(K/\mathbb{Q})$ que tiene la siguiente propiedad:

$$\sigma_\mathfrak{p}(x) \equiv x^p \mod \mathfrak{p} \quad \text{para todo } x \in \mathcal{O}_K$$

El automorfismo de Frobenius

A este elemento $\sigma_{\mathfrak{p}}$ se lo denomina *automorfismo de Frobenius de* $\mathfrak{p}$ sobre p.

El automorfismo de Frobenius

A este elemento $\sigma_{\mathfrak{p}}$ se lo denomina *automorfismo de Frobenius de* $\mathfrak{p}$ sobre p.

Para todo $\mathfrak{p}$ que está sobre p, el automorfismo de Frobenius $\sigma_{\mathfrak{p}}$ satisface $\sigma_{\mathfrak{p}}^{f(\mathfrak{p}|p)} = id$.

El automorfismo de Frobenius

A este elemento $\sigma_{\mathfrak{p}}$ se lo denomina *automorfismo de Frobenius de* $\mathfrak{p}$ sobre p.

Para todo $\mathfrak{p}$ que está sobre p, el automorfismo de Frobenius $\sigma_{\mathfrak{p}}$ satisface $\sigma_{\mathfrak{p}}^{f(\mathfrak{p}|p)} = id$.

Por lo tanto, si $K/\mathbb{Q}$ es de Galois y $\mathfrak{p}$ que está sobre p, el automorfismo de Frobenius $\sigma_{\mathfrak{p}}$ satisface $\sigma_{\mathfrak{p}}^{t} = id$, donde $t = f(\mathfrak{p}|p)$ para todo $\mathfrak{p}$ sobre p.

De vuelta a las raíces de la unidad

Podemos ahora enunciar el siguiente teorema:

De vuelta a las raíces de la unidad

Podemos ahora enunciar el siguiente teorema:

Sea K una extensión finita y de Galois de $\mathbb{Q}$. Sea $h \in \mathcal{O}_K[x]$ un polinomio mónico de grado n tal que $h(0) \neq 0$ y cuyas raíces son $\alpha = \alpha_1, \ldots, \alpha_n$.

De vuelta a las raíces de la unidad

Podemos ahora enunciar el siguiente teorema:

Sea K una extensión finita y de Galois de $\mathbb{Q}$. Sea $h \in \mathcal{O}_K[x]$ un polinomio mónico de grado n tal que $h(0) \neq 0$ y cuyas raíces son $\alpha = \alpha_1, \ldots, \alpha_n$.

Sea $\delta = \inf\{|\omega| : 0 \neq \omega \in \mathcal{O}_K\}$. Luego $\delta > 0$. Sea p un número primo tal que p es coprimo con d_K y $p \geq 2n\,\mathrm{e}\,\delta^{-1}$.

De vuelta a las raíces de la unidad

Podemos ahora enunciar el siguiente teorema:

Sea K una extensión finita y de Galois de $\mathbb{Q}$. Sea $h \in \mathcal{O}_K[x]$ un polinomio mónico de grado n tal que $h(0) \neq 0$ y cuyas raíces son $\alpha = \alpha_1, \ldots, \alpha_n$.

Sea $\delta = \inf\{|\omega| : 0 \neq \omega \in \mathcal{O}_K\}$. Luego $\delta > 0$. Sea p un número primo tal que p es coprimo con d_K y $p \geq 2n\,\mathrm{e}\,\delta^{-1}$.

Entonces α es una raíz de la unidad si

$$|\alpha_i| \leq 1 + \frac{1}{p^t n} \quad \text{para } i = 1, \ldots, n$$

donde $t = f(\mathfrak{p}|p)$ para cualquier $\mathfrak{p}$ que está sobre p.

De vuelta a las raíces de la unidad: Idea principal

Consideramos las sumas $S_k = \sum_{i=1}^{n} \alpha_i^k$ para todo entero no negativo k.

De vuelta a las raíces de la unidad: Idea principal

Consideramos las sumas $S_k = \sum_{i=1}^{n} \alpha_i^k$ para todo entero no negativo k.

Si para algún entero $m \geq 2$ se tiene que

De vuelta a las raíces de la unidad: Idea principal

Consideramos las sumas $S_k = \sum_{i=1}^{n} \alpha_i^k$ para todo entero no negativo k.

Si para algún entero $m \geq 2$ se tiene que

$S_k = S_{km}$ para $1 \leq k \leq n$, entonces se tiene que

De vuelta a las raíces de la unidad: Idea principal

Consideramos las sumas $S_k = \sum_{i=1}^{n} \alpha_i^k$ para todo entero no negativo k.

Si para algún entero $m \geq 2$ se tiene que

$S_k = S_{km}$ para $1 \leq k \leq n$, entonces se tiene que

$\prod_{i=1}^{n}(x - \alpha_i) = \prod_{i=1}^{n}(x - \alpha_i^m)$.

De vuelta a las raíces de la unidad: Idea principal

Consideramos las sumas $S_k = \sum_{i=1}^{n} \alpha_i^k$ para todo entero no negativo k.

Si para algún entero $m \geq 2$ se tiene que

$S_k = S_{km}$ para $1 \leq k \leq n$, entonces se tiene que

$\prod_{i=1}^{n}(x - \alpha_i) = \prod_{i=1}^{n}(x - \alpha_i^m)$.

Esto implica que para cada $1 \leq i \leq n$ existe $1 \leq j \leq n$ tal que $\alpha_i = \alpha_j^m$.

De vuelta a las raíces de la unidad: Idea principal

Por la teoría de Galois, existe $\sigma \in \mathsf{Gal}(K/\mathbb{Q})$ tal que $\sigma(\alpha_j) = \alpha_i$.

De vuelta a las raíces de la unidad: Idea principal

Por la teoría de Galois, existe $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ tal que $\sigma(\alpha_j) = \alpha_i$.

Entonces $\sigma(\alpha_i) = \sigma(\alpha_j^m) = (\sigma(\alpha_j))^m = \alpha_i^m$. Luego

De vuelta a las raíces de la unidad: Idea principal

Por la teoría de Galois, existe $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ tal que $\sigma(\alpha_j) = \alpha_i$.

Entonces $\sigma(\alpha_i) = \sigma(\alpha_j^m) = (\sigma(\alpha_j))^m = \alpha_i^m$. Luego

$\sigma^2(\alpha_i) = \sigma(\alpha_i^m) = \alpha_i^{m^2}$.

De vuelta a las raíces de la unidad: Idea principal

Por la teoría de Galois, existe $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ tal que $\sigma(\alpha_j) = \alpha_i$.

Entonces $\sigma(\alpha_i) = \sigma(\alpha_j^m) = (\sigma(\alpha_j))^m = \alpha_i^m$. Luego

$\sigma^2(\alpha_i) = \sigma(\alpha_i^m) = \alpha_i^{m^2}$.

Como $\mathrm{Gal}(K/\mathbb{Q})$ es un grupo de orden n, entonces $\sigma^n = id$. Luego

De vuelta a las raíces de la unidad: Idea principal

Por la teoría de Galois, existe $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ tal que $\sigma(\alpha_j) = \alpha_i$.

Entonces $\sigma(\alpha_i) = \sigma(\alpha_j^m) = (\sigma(\alpha_j))^m = \alpha_i^m$. Luego

$\sigma^2(\alpha_i) = \sigma(\alpha_i^m) = \alpha_i^{m^2}$.

Como $\mathrm{Gal}(K/\mathbb{Q})$ es un grupo de orden n, entonces $\sigma^n = id$. Luego

$\alpha_i = \sigma^n(\alpha_i) = \alpha_i^{m^n}$. Es decir $\alpha_i^{m^n - 1} = 1$ y, por lo tanto, α_i es una raíz de la unidad.

De vuelta a las raíces de la unidad

Consideremos las sumas $S_k = \sum_{i=1}^{n} \alpha_i^k$ para todo entero no negativo k.

De vuelta a las raíces de la unidad

Consideremos las sumas $S_k = \sum_{i=1}^{n} \alpha_i^k$ para todo entero no negativo k.

Se demuestra que cada $S_k \in \mathcal{O}_K$ y que $S_k^p \equiv S_{kp} \mod p\mathcal{O}_K$.

De vuelta a las raíces de la unidad

Consideremos las sumas $S_k = \sum_{i=1}^{n} \alpha_i^k$ para todo entero no negativo k.

Se demuestra que cada $S_k \in \mathcal{O}_K$ y que $S_k^p \equiv S_{kp} \mod p\mathcal{O}_K$.

Por inducción se tiene que $S_k^{p^j} \equiv S_{kp^j} \mod p\mathcal{O}_K$.

De vuelta a las raíces de la unidad

Consideremos las sumas $S_k = \sum_{i=1}^{n} \alpha_i^k$ para todo entero no negativo k.

Se demuestra que cada $S_k \in \mathcal{O}_K$ y que $S_k^p \equiv S_{kp} \mod p\mathcal{O}_K$.

Por inducción se tiene que $S_k^{p^j} \equiv S_{kp^j} \mod p\mathcal{O}_K$.

Como p no divide a d_K entonces p no ramifica en K. Es decir

$$p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_s = \bigcap_{i=1}^{s} \mathfrak{p}_i$$

De vuelta a las raíces de la unidad

Consideremos las sumas $S_k = \sum_{i=1}^{n} \alpha_i^k$ para todo entero no negativo k.

Se demuestra que cada $S_k \in \mathcal{O}_K$ y que $S_k^p \equiv S_{kp} \mod p\mathcal{O}_K$.

Por inducción se tiene que $S_k^{p^j} \equiv S_{kp^j} \mod p\mathcal{O}_K$.

Como p no divide a d_K entonces p no ramifica en K. Es decir

$$p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_s = \bigcap_{i=1}^{s} \mathfrak{p}_i$$

Luego $S_k^{p^j} \equiv S_{kp^j} \mod \mathfrak{p}$ donde $\mathfrak{p}$ es cualquiera de los ideales en la factorización de $p\mathcal{O}_K$

De vuelta a las raíces de la unidad

Aplicando el automorfismo de Frobenius se tiene que

$$\sigma_{\mathfrak{p}}(S_k) \equiv S_k^p \equiv S_{kp} \mod \mathfrak{p}$$

De vuelta a las raíces de la unidad

Aplicando el automorfismo de Frobenius se tiene que

$$\sigma_{\mathfrak{p}}(S_k) \equiv S_k^p \equiv S_{kp} \mod \mathfrak{p}$$

con lo cual $S_k \equiv \sigma_{\mathfrak{p}}^t(S_k) \equiv S_{kp^t} \mod \mathfrak{p}$.

De vuelta a las raíces de la unidad

Aplicando el automorfismo de Frobenius se tiene que

$$\sigma_{\mathfrak{p}}(S_k) \equiv S_k^p \equiv S_{kp} \mod \mathfrak{p}$$

con lo cual $S_k \equiv \sigma_{\mathfrak{p}}^t(S_k) \equiv S_{kp^t} \mod \mathfrak{p}$.

Entonces $S_k \equiv S_{kp^t} \mod p\mathcal{O}_K$.

De vuelta a las raíces de la unidad

Aplicando el automorfismo de Frobenius se tiene que

$$\sigma_{\mathfrak{p}}(S_k) \equiv S_k^p \equiv S_{kp} \mod \mathfrak{p}$$

con lo cual $S_k \equiv \sigma_{\mathfrak{p}}^t(S_k) \equiv S_{kp^t} \mod \mathfrak{p}$.

Entonces $S_k \equiv S_{kp^t} \mod p\mathcal{O}_K$.

Esto quiere decir que si $S_k \neq S_{kp^t}$ entonces existe $0 \neq \omega \in \mathcal{O}_K$ tal que

$$S_{kp^t} - S_k = p\omega$$

De vuelta a las raíces de la unidad

Recordemos que para cada $1 \leq i \leq n$ asumimos que

$$|\alpha_i| \leq 1 + \frac{1}{p^t n}$$

De vuelta a las raíces de la unidad

Recordemos que para cada $1 \leq i \leq n$ asumimos que

$$|\alpha_i| \leq 1 + \frac{1}{p^t n}$$

Luego, para $1 \leq k \leq n$ se tiene que

$$|S_{kp^t}| \leq \sum_{i=1}^{n} |\alpha_i|^{kp^t} \leq n \left(1 + \frac{1}{p^t n}\right)^{kp^t} < n\,\mathrm{e}$$

De vuelta a las raíces de la unidad

Recordemos que para cada $1 \leq i \leq n$ asumimos que

$$|\alpha_i| \leq 1 + \frac{1}{p^t n}$$

Luego, para $1 \leq k \leq n$ se tiene que

$$|S_{kp^t}| \leq \sum_{i=1}^{n} |\alpha_i|^{kp^t} \leq n \left(1 + \frac{1}{p^t n}\right)^{kp^t} < n\,\mathrm{e}$$

De manera similar se tiene que $|S_k| < n\,\mathrm{e}$ para $1 \leq k \leq n$.

De vuelta a las raíces de la unidad

Recordemos que para cada $1 \leq i \leq n$ asumimos que

$$|\alpha_i| \leq 1 + \frac{1}{p^t n}$$

Luego, para $1 \leq k \leq n$ se tiene que

$$|S_{kp^t}| \leq \sum_{i=1}^{n} |\alpha_i|^{kp^t} \leq n \left(1 + \frac{1}{p^t n}\right)^{kp^t} < n\,\mathrm{e}$$

De manera similar se tiene que $|S_k| < n\,\mathrm{e}$ para $1 \leq k \leq n$.

Entonces

$$|S_{kp^t} - S_k| < 2n\,\mathrm{e} \leq p\delta \leq p|\omega| \quad \text{para } 1 \leq k \leq n$$

De vuelta a las raíces de la unidad

Como $S_k \neq S_{kp^t}$ implica que $S_{kp^t} - S_k = p\omega$, la desigualdad previa nos dice que

De vuelta a las raíces de la unidad

Como $S_k \neq S_{kp^t}$ implica que $S_{kp^t} - S_k = p\omega$, la desigualdad previa nos dice que

$S_k = S_{kp^t}$ para $1 \leq k \leq n$,

De vuelta a las raíces de la unidad

Como $S_k \neq S_{kp^t}$ implica que $S_{kp^t} - S_k = p\omega$, la desigualdad previa nos dice que

$S_k = S_{kp^t}$ para $1 \leq k \leq n$,

que es lo que se necesitaba para demostrar que $\alpha = \alpha_1, \ldots, \alpha_n$ son raíces de la unidad.

MUCHAS GRACIAS POR LA ATENCIÓN!!!