Álgebra Moderna 2: Teoría de Campos

Rafael Dubois
Universidad del Valle de Guatemala
dub19093@uvg.edu.gt

28 de noviembre de 2021

1. Campos de extensión

Un conjunto no vacío F es un campo si en él se definen dos operaciones binarias (a menudo llamadas suma $(+)$ la primera, y producto $(\cdot)$ la segunda), las cuales cumplen con que $(F,+)$ y $(F-\{0\},\cdot)$ son grupos abelianos, y el producto se distribuye sobre la suma.

Extensión y subcampos

Si F es un campo y K también es un campo tal que $F \subseteq K$, se dice que F es subcampo de K y que K es una extensión de F.

Grado de una extensión

El grado $[K:F]$ de una extensión K de un campo F es la dimensión de K como espacio vectorial sobre F. Cuando K es una extensión finita de F, se tiene $[K:F] \in \mathbb{Z}^+$.

Teorema 5A:

Si L es una extensión finita del campo K, y K es una extensión finita del campo F, entonces L es una extensión finita de F y $[L:F] = [L:K][K:F]$.

Corolario 1 del teorema 5A:

Si L es una extensión finita del campo F y K es un subcampo de L que contiene a F (es decir, $F \subseteq K \subseteq L$), entonces $[K:F] \mid [L:F]$.

Corolario 2 del teorema 5A:

Si F es un campo, K es una extensión finita de F y $[K:F]$ es un número primo, entonces no existe ningún campo L tal que $F \subset L \subset K$.

Elementos algebraicos

Si F es un campo y K es una extensión de F, entonces $a \in K$ es algebraico sobre F si existe $f(x) \in F[x]$ un polinomio no constante tal que $f(a) = 0$. Es decir, a es una raíz de f.

En este documento, los códigos de color van de la siguiente manera: Negro, Títulos; Azul, Lemas; Rojo, Teoremas; Violeta, Definiciones; Morado, Propiedades; Aqua, Otros subtítulos.

Valor de un elemento en un polinomio

Si F es un campo, K es una extensión de F, $f(x) \in F[x]$ y $a \in K$, entonces $f(a)$ es el valor de f en a, y si $f(a) = 0$ se dice que a satisface a f.

Colecciones de subcampos con elementos específicos

Sea F un campo, K una extensión de F, $a \in K$ y $M = \{L : L \text{ es subcampo de } K, a \in L \text{ y } F \subseteq L\}$. Entonces $M \neq \emptyset$, y si $F(a) = \bigcap_{L \in M} L$, se tiene $F(a) \in M$.

El subcampo más pequeño que contiene a un elemento

En el orden parcial de la contención, $F(a)$ es el subcampo más pequeño de K tal que $a \in F(a)$ y $F \subseteq F(a)$. Es decir, $F(a)$ es la extensión más pequeña de F que contiene a a.

Subcampo por adjunción

Si F es un campo, K una extensión de F y $a \in K$, entonces $F(a)$ es el subcampo de K obtenido por adjunción de a a F.

El subcampo por adjunción es de funciones racionales

Si F es un campo, K una extensión de F y $a \in K$, entonces $F(a) = \left\{ \dfrac{p(a)}{q(a)} : p(x), q(x) \in F[x], q(x) \neq 0 \right\}$.

Teorema 5B:

Si F es un campo y K es una extensión de F, entonces $a \in K$ es algebraico sobre F si y solo si $F(a)$ es una extensión finita de F.

Grado de un elemento algebraico

Si F es un campo, K es una extensión de F y $a \in K$, entonces a es algebraico de grado n sobre F si el grado mínimo de un polinomio en $F[x]$ satisfecho por a es n.

Teorema 5C:

Para F un campo y K una extensión de F, $a \in K$ es un elemento algebraico de grado n sobre F si y solo si $[F(a) : F] = n$.

Teorema 5D:

Si F es un campo, K es una extensión de F y $a, b \in K$ son algebraicos sobre F, entonces todos los elementos $a \pm b$, ab y a/b (si $b \neq 0$) son algebraicos sobre F. Es decir, el conjunto de elementos algebraicos de K sobre F forma un subcampo de K.

Corolario del teorema 5D:

Si F es un campo, K es una extensión de F y $a, b \in K$ son algebraicos de grados m y n sobre F, entonces todos los elementos $a \pm b$, ab y a/b (si $b \neq 0$) son algebraicos de grados a lo más mn sobre F.

Notación para subcampos por adjunción doble

Si F es un campo, K es una extensión de F y $a, b \in K$, entonces $[F(a)](b) = F(a, b)$.

Simetría de la doble adjunción

Si F es un campo, K es una extensión de F y $a, b \in K$, entonces $F(a, b) = F(b, a)$.

Notación para subcampos por adjunción múltiple

Si F es un campo, K es una extensión de F y $a_1, ldots, a_n \in K$, entonces $F(a_1, \ldots, a_n)$ es el subcampo más pequeño de K que contiene a F y a $a_1, ldots, a_n$.

Extensión algebraica

Si F es un campo y K es una extensión de F cuyos elementos son todos algebraicos sobre F, entonces K es llamada una extensión algebraica.

Un ejemplo general de extensiones algebraicas

Si F es un campo, K es una extensión de F y $a \in K$, entonces $F(a)$ es una extensión algebraica.

Teorema 5E:

Si L es una extensión algebraica de un campo K, el cual es extensión algebraica de un campo F, entonces L es extensión algebraica de F.

Números complejos algebraicos

Un elemento del conjunto de los números complejos $\mathbb{C}$ es algebraico si este es algebraico sobre $\mathbb{Q}$.

Números complejos trascendentes

Un elemento del conjunto de los números complejos $\mathbb{C}$ es trascendente si este no es algebraico.

2. La trascendencia de e

Teorema 5F

El número e, el cual es el resultado de evaluar en $x = 1$ la función $f : \mathbb{R} \to \mathbb{R}$ con la propiedad de que para todo $x \in \mathbb{R}$ se cumple $f'(x) = f(x)$ y $f(0) = 1$, es un número trascendente.

3. Raíces de polinomios

Raíz de un polinomio

Si F es un campo con $p(x) \in F[x]$, y K es una extensión de F, entonces $a \in K$ es una raíz de $p(x)$ si $p(a) = 0$.

Lema 5.1 (Teorema del residuo):

Si F es un campo con $p(x) \in F[x]$, y K es una extensión de F, entonces para todo $k \in K$ se tiene que $p(x) = (x-k)q(x) + p(k)$, donde $q(x) \in K[x]$ y $\text{gr}(q) = \text{gr}(p) - 1$.

Corolario del lema 5.1:

Si F es un campo, K es una extensión de F y $a \in K$ es una raíz de $p(x) \in F[x]$, entonces $x - a \mid p(x)$.

Raíz de multiplicidad m

Si F es un campo con $p(x) \in F[x]$, y K es una extensión de F, entonces $a \in K$ es una raíz de multiplicidad $m \in \mathbb{Z}^+$ para $p(x)$ si $(x-a)^m \mid p(x)$ pero $(x-a)^{m+1} \nmid p(x)$.

Lema 5.2:

Un polinomio de grado n sobre un campo tiene a lo más n raíces en cualquier extensión del campo, contando m raíces para una raíz de multiplicidad m.

Teorema 5G:

Si F es un campo con $p(x) \in F[x]$ irreducible sobre F con $\text{gr}(p) \geq 1$, entonces existe una extensión E de F tal que $[E : F] = \text{gr}(p)$, y E contiene una raíz de $p(x)$.

Corolario del teorema 5G:

Si F es un campo con $f(x) \in F[x]$, entonces existe una extensión finita E de F tal que esta contiene una raíz de $f(x)$ y $[E : F] \leq \text{gr}(f)$.

Campo de descomposición

Si F es un campo con $f(x) \in F[x]$, una extensión finita E de F es un campo de descomposición de $f(x)$ sobre F si $f(x)$ puede descomponerse o factorizarse como el producto de polinomios lineales sobre E, pero en ningún subcampo propio de E.

Teorema 5H (Existencia de los campos de descomposición):

Si F es un campo con $f(x) \in F[x]$ tal que $\text{gr}(f) \geq 1$, entonces existe E extensión finita de F con $[E : F] \leq \text{gr}(f)!$ tal que E contiene $\text{gr}(f)$ raíces de $f(x)$. Es decir, E contiene un juego completo de raíces de $f(x)$. Cuando $[E : F]$ es mínimo, esto implica que los campos de descomposición existen.

Comentarios del teorema 5H:

Más adelante, en la introducción a la teoría de Galois, se verá que existe un campo F con $f(x) \in F[x]$ tal que el campo de descomposición E para $f(x)$ sobre F cumple $[E : F] = \text{gr}(f)!$. ¿Serán únicos los campos de descomposición?

Lema 5.3:

Si F y F' son campos y $\tau : F \to F'$ con $\tau(\alpha) = \alpha'$ es un isomorfismo, entonces $\tau^* : F[x] \to F'[t]$ con $\tau^*\left(\sum_{i=0}^{n} \alpha_i x^i\right) = \sum_{i=0}^{n} \tau(\alpha_i) t^i$ es, también, un isomorfismo.

Comentarios del lema 5.3:

Si F y F' son campos y $\tau : F \to F'$ es un isomorfismo, el lema 5.3 asegura que la factorización de $f(x) \in F[x]$ coincide exactamente con la de $\tau^*(f(x)) = f'(t) \in F'[t]$, y viceversa.

Irreducibilidad bajo isomorfismo

Si F y F' son campos y $\tau : F \to F'$ es un isomorfismo, entonces $f(x) \in F[x]$ es irreducible sobre F si y solo si $\tau^*(f(x)) \in F'[t]$ es irreducible sobre F'.

Lema 5.4:

Si F y F' son campos, $\tau : F \to F'$ es un isomorfismo y $f(x) \in F[x]$, entonces existe un isomorfismo $\tau^{**} : F[x]/(f(x)) \to F'[t]/(\tau(f(x)))$ tal que si $\alpha \in F$ entonces $\tau^{**}(\alpha) = \tau(\alpha)$, donde $\alpha \approx \alpha + (f(x))$.

Teorema 5I:

Si F es un campo, $p(x) \in F[x]$ es irreducible sobre F, v es una raíz de $p(x)$, F' es un campo y $\tau : F \to F'$ es un isomorfismo, entonces existe un isomorfismo $\sigma : F(v) \to F'(w)$, donde w es una raíz de $\tau^*(p(x))$, y este isomorfismo σ puede elegirse de manera que $\sigma(v) = w$ y $\sigma(\alpha) = \tau(\alpha)$ para todo $\alpha \in F$. Es decir, σ deja fijos, salvo el isomorfismo τ, a los elementos de F.

Corolario del teorema 5I:

Si F es un campo, $p(x) \in F[x]$ es irreducible sobre F, con a y b raíces de $p(x)$, entonces existe un isomorfismo $\sigma : F(a) \to F(b)$ tal que $\sigma(a) = b$ y $\sigma(\alpha) = \alpha$ para todo $\alpha \in F$.

Teorema 5J (Unicidad de los campos de descomposición):

Si F y F' son campos isomorfos bajo $\tau : F \to F'$ y se tiene $f(x) \in F[x]$, entonces el campo de descomposición E de $f(x)$ sobre F es isomorfo al campo de descomposición E' de $\tau^*\big(f(x)\big)$ sobre F', y ese isomorfismo mapea a todo $\alpha \in F$ en $\tau(\alpha) \in F'$.

Nota del teorema 5J

En particular, si $F = F'$ y τ es el isomorfismo identidad de F, el teorema 5J asegura que si E y E' son dos campos de descomposición de $f(x) \in F[x]$ sobre F, entonces $E \approx E'$ con un isomorfismo que deja fijos a los elementos de F.

4. Construcción con regla y compás

Un número $\alpha \in \mathbb{R}$ es construíble si es posible crear un segmento de largo α solamente haciendo uso de recta y compás.

Cerraduras de los números construíbles

Si α y β son construíbles, entonces $\alpha \pm \beta$, $\alpha\beta$, α/β y $\sqrt{\alpha}$ son contruíbles.

Plano de un subcampo de $\mathbb{R}$

Si F es un subcampo de $\mathbb{R}$, se dice que $F \times F$ es el plano de F.

Ecuación de una recta por dos puntos

Si F es un subcampo de $\mathbb{R}$, entonces la ecuación de la recta en $\mathbb{R} \times \mathbb{R}$ que pasa por (a_0, b_0) y (a_1, b_1) en $F \times F$ es $\alpha x + \beta y + \gamma = 0$, con los parámetros $\alpha, \beta, \gamma \in F$ dados por

$$\alpha = \frac{b_1 - b_0}{a_1 - a_0}, \qquad \beta = -1, \qquad \gamma = b_1 - a_1 \frac{b_1 - b_0}{a_1 - a_0}.$$

Ecuación de una circunferencia

Si F es un subcampo de $\mathbb{R}$, entonces la ecuación de la circunferencia en $\mathbb{R} \times \mathbb{R}$ con centro en (h, k) en $F \times F$ y radio $r \in F$ es $x^2 + y^2 + \alpha x + \beta y + \gamma = 0$, con los parámetros $\alpha, \beta, \gamma \in F$ dados por

$$\alpha = -2h, \qquad \beta = -2k, \qquad \gamma = h^2 + k^2 - r^2.$$

Intersección de dos rectas en F

El punto de intersección de dos rectas distintas no paralelas formadas (cada una) por puntos del plano de $F \subseteq \mathbb{R}$, es a su vez un punto en el plano de F.

Intersección de una recta y una circunferencia en F

Si F es un subcampo de $\mathbb{R}$, entonces el o los puntos de intersección entre una recta que pasa por puntos del plano de F y una circunferencia con centro en el plano de F y radio en F, está o están (si existen) en el plano de F o en el plano de $F(\sqrt{\delta})$, donde $\delta \in F^+$.

Intersección de dos circunferencias en F

Si F es un subcampo de $\mathbb{R}$, entonces el o los puntos de intersección entre dos circunferencias con centros en el plano de F y radios en F, está o están (si existen) en el plano de F o en el plano de $F(\sqrt{\delta})$, donde $\delta \in F^+$.

Teorema 5α:

Un número $\alpha \in \mathbb{R}$ es construíble si y solo si existe una cantidad finita de números $\lambda_1, \ldots, \lambda_n \in \mathbb{R}^+$ tales que $\lambda_1^2 \in \mathbb{Q}$ y $\lambda_i^2 \in \mathbb{Q}(\lambda_1, \ldots, \lambda_{i-1})$ para $i \in \{1, 2, \ldots, n\}$, para los cuales $\alpha \in \mathbb{Q}(\lambda_1, \ldots, \lambda_n)$.

Corolario 1 del teorema 5α:

Un número $\alpha \in \mathbb{R}$ es construíble si y solo si existe una cantidad finita de números $\lambda_1, \ldots, \lambda_n \in \mathbb{R}^+$ tales que $[\mathbb{Q}(\lambda_1) : \mathbb{Q}] \leq 2$ y $[\mathbb{Q}(\lambda_1, \ldots, \lambda_i) : \mathbb{Q}(\lambda_1, \ldots, \lambda_{i-1})] \leq 2$ para $i \in \{1, 2, \ldots, n\}$.

Corolario 2 del teorema 5α:

Si un número $\alpha \in \mathbb{R}$ es construíble, entonces α pertenece a una extensión finita de $\mathbb{Q}$ cuyo grado sobre $\mathbb{Q}$ es una potencia de 2.

Corolario 3 del teorema 5α:

Si $\alpha \in \mathbb{R}$ satisface un polinomio irreducible de grado k sobre $\mathbb{Q}$, donde k no es una potencia de 2, entonces α no es construíble.

Teorema 5β (sobre raíces racionales):

Si $f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ con a_n y a_0 distintos de 0 es tal que $f(p/q) = 0$ para algún $p/q \in \mathbb{Q}$ (con p y q primos relativos), entonces $p \mid a_0$ y $q \mid a_n$.

Aplicaciones

Estos resultados pueden ser utilizados para demostrar que es imposible trisectar un ángulo de 60 grados, que es imposible construir un cubo cuyo volumen duplica al de otro cubo, es imposible construir un heptágono regular, entre otros.

5. Más sobre raíces

Derivada de un polinomio

Si D es un dominio entero y $f(x) = \sum_{k=0}^{n} a_k x^k \in D[x]$, entonces su derivada es $f'(x) = \sum_{k=1}^{n} k a_k x^{k-1}$.

Característica de un dominio entero

La característica de un dominio entero es el menor entero no negativo que anula a todos sus elementos.

Característica cero

Un dominio entero D es de característica 0 si la relación $ma = 0$ para $a \neq 0$ en D y $m \in \mathbb{Z}$ solo puede ocurrir si $m = 0$.

Característica finita

Un dominio entero D es de característica finita si existe $p \in \mathbb{Z}^+$ tal que $pa = 0$ para todo $a \in D$. En este caso, p debe ser un número primo.

Propiedades de anillos de polinomios de distintas característica

Si F es un campo de característica p (no cero), la derivada del polinomio x^p en $F[x]$ es $px^{p-1} = 0$. Es decir, en un campo de característica finita no necesariamente un polinomio de derivada nula es un polinomio constante. Sin embargo, si $f(x) \in F[x]$ es un polinomio tal que $f(x^p)$ tiene derivada nula en $F[x]$, este sí debe ser constante. Por su parte, si F es un campo de característica cero y $f(x) \in F[x]$ tiene derivada nula, entonces el polinomio $f(x)$ debe ser constante.

Lema 5.5:

Si D es un dominio entero con $f(x), g(x) \in D[x]$ y $\alpha \in D$, entonces:

- $[f(x) + g(x)]' = f'(x) + g'(x)$;
- $[\alpha f(x)]' = \alpha f'(x)$;
- $[f(x)g(x)]' = f'(x)g(x) + f(x)g'(x)$.

Preservación de factores en extensión

Si F es un campo, K es una extensión de F, y $f(x), g(x) \in F[x]$ tienen un factor común no constante en $K[x]$, entonces tienen también un factor común no constante en $F[x]$.

Lema 5.6:

Si F es un campo, $f(x) \in F[x]$ tiene una raíz múltiple (con multiplicidad) si y solo si $f(x)$ y $f'(x)$ tienen un factor común no constante.

Corolario 1 del lema 5.6:

Si F es un campo y $f(x) \in F[x]$ es irreducible sobre F, entonces:

- Si la característica de F es cero, entonces $f(x)$ no tiene raíces múltiples.
- Si la característica de F es distinta de cero, entonces $f(x)$ tiene una raíz múltiple solo si es de la forma $f(x) = g(x^p)$. Esto también nos dice que si la derivada de $f(x)$ es nula se tiene que $f(x)$ tiene raíces múltiples, y viceversa.

Corolario 2 del lema 5.6 (útil en campos finitos):

Si F es un campo de característica $p \neq 0$, entonces $x^{p^n} - x \in F[x]$ con $n \geq 1$ tiene raíces distintas.

Comentarios sobre los corolarios al lema 5.6

- El corolario 1 del lema 5.6 no excluye la posibilidad de que, si la característica de F es distinta de cero, un polinomio irreducible tenga raíces múltiples. Por ejemplo, sea F_0 un campo de característica 2 y sea $F = F_0(x)$. Considérese el polinomio $t^2 - x \in F[t]$ y nótese que es irreducible sobre F, pues de lo contrario $[p(x)]^2 = x[q(x)]^2$, lo cual implica que un polinomio de grado par es igual a uno de grado impar. Por otro lado, la derivada de $t^2 - x$ en $F[t]$ es $2t$, que como la característica es 2, es nulo. Por corolario 1, $t^2 - x$ tiene raíces múltiples.
- Las implicaciones de distinguir entre campos de característica 0 y de característica positiva son importantes: permiten la posibilidad de polinomios irreducibles con raíces múltiples en el caso de los campos de característica positiva, lo cual es imposible en los campos de característica 0. En esta presentación, se asumirá que todos los campos son de característica 0.

Extensiones simples

Una extensión K de F es simple si $K = F(\alpha)$ para algún $\alpha \in K$.

Elementos y extensiones separables, y campos perfectos

Si F es un campo y K es una extensión de F, entonces $a \in K$ es separable sobre F si satisface a un polinomio en $F[x]$ sin raíces múltiples. Se dice que K es separable sobre F si todos sus elementos son separables sobre F. Un campo F es perfecto si todas sus extensiones finitas son separables sobre F.

Las extensiones finitas separables son simples

Si F es un campo y K es una extensión finita y separable de F, entonces también es simple. El teorema a continuación muestra que todas las extensiones finitas de los campos de característica cero son simples. Además, las extensiones finitas y separables de los campos de característica positiva son simples.

Teorema 5K:

Si F es un campo de característica cero con a y b son algebraicos sobre F. Entonces, existe $c \in F(a, b)$ tal que $F(a, b) = F(c)$.

Corolario del teorema 5K:

Toda extensión finita de un campo de característica cero es simple.

6. Elementos de la teoría de Galois

Automorfismos de campos

Si K es un campo, un automorfismo de K es un isomorfismo $\sigma : K \to K$.

Teorema 5L:

Si K es un campo y $\sigma_1, \ldots, \sigma_n$ son automorfismos distintos de K, entonces es imposible encontrar elementos no todos nulos $a_1, \ldots, a_n \in K$ tales que $\sum_{i=1}^{n} a_i \sigma_i(k) = 0$ para todo $k \in K$.

Campos fijados

Si K es un campo y G es un grupo de automorfismos de K, entonces el campo fijado por G (el cual es subconjunto de K) se define como $\{k \in K \mid \forall \sigma \in G, \sigma(k) = k\}$.

Nota sobre la definición de campos fijados

Esta definición hace sentido si en vez del grupo G se usa cualquier subconjunto de $\mathbb{A}(K)$, el cual es el conjunto de todos los automorfismos en K. De hecho, es posible demostrar que si $B \subseteq \mathbb{A}(K)$ entonces el conjunto fijado por B es igual al conjunto fijado por (B).

Lema 5.7:

Si K es un campo y $G \subseteq \mathbb{A}(K)$, entonces el subconjunto de K fijado por G es un subcampo de K.

Grupo de automorfismos relativo

Sea F un campo y K una extensión de F. Entonces, el grupo de automorfismos de K relativo a F se denota por $G(K, F)$, y está definido por $G(K, F) = \{\sigma \in \mathbb{A}(K) \mid \forall \alpha \in F, \sigma(\alpha) = \alpha\}$.

Lema 5.8:

Si F un campo y K es una extensión de F, entonces $G(K, F)$ es un subgrupo de $\mathbb{A}(K)$.

Nota sobre los últimos resultados

Si K es un campo de característica cero, entonces es un campo infinito. Puesto que $\mathbb{Q}$ es el campo infinito más pequeño, todo campo infinito contiene una copia isomórfica de $\mathbb{Q}$. Entonces, todo campo fijado por cualquier grupo de automorfismos de K contiene a $\mathbb{Q}$, y por lo tanto todo número racional es invariante en la acción de cualquier automorfismo de un campo de característica cero. Por otra parte, en general, $G(K, F)$ no siempre es cíclico ni abeliano.

Algunos ejemplos de grupos de automorfismos

Los complejos relativo a los reales

Considérese $G(\mathbb{C}, \mathbb{R})$. Si $\sigma : \mathbb{C} \to \mathbb{C}$ es un automorfismo que deja fijo a $\mathbb{R}$, entonces $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$, lo cual implica que $\sigma(i)$ puede tomar el valor de i o $-i$. Si $\sigma_1(i) = i$, entonces en general $\sigma_1(a+bi) = \sigma_1(a) + \sigma_1(b)\sigma_1(i) = a + bi$. Es decir, σ_1 es la identidad. Si $\sigma_2(i) = -i$, entonces en general $\sigma_2(a+bi) = \sigma_2(a) + \sigma_2(b)\sigma_2(i) = a - bi$. Es decir, σ_2 es la conjugación. Entonces, $G(\mathbb{C}, \mathbb{R}) = \{I_{\mathbb{C}}, \overline{\cdots}\}$. Como los únicos elementos que quedan fijos bajo todo elemento de $G(\mathbb{C}, \mathbb{R})$ son los reales, entonces el campo fijado por $G(\mathbb{C}, \mathbb{R})$ es $\mathbb{R}$ mismo.

Los racionales adjuntos a $\sqrt[3]{2}$ relativo a los racionales

Considérese $G(\mathbb{Q}(\sqrt[3]{2}),\mathbb{Q})$. Si $\sigma:\mathbb{Q}(\sqrt[3]{2})\to\mathbb{Q}(\sqrt[3]{2})$ es un automorfismo que deja fijo a $\mathbb{Q}$, entonces $\sigma(\sqrt[3]{2})^3=\sigma(2)=2$. Hay tres números complejos que cumplen esto, de los cuales solo $\sqrt[3]{2}\in\mathbb{Q}(\sqrt[3]{2})$. Por lo tanto, solo existe la posibilidad de $\sigma(\sqrt[3]{2})=\sqrt[3]{2}$. Entonces en general,

$$\sigma(a+b\sqrt[3]{2}+c\sqrt[3]{2}^2)=\sigma(a)+\sigma(b)\sigma(\sqrt[3]{2})+\sigma(c)\sigma(\sqrt[3]{2})^2=a+b\sqrt[3]{2}+c\sqrt[3]{2}^2.$$

Esto es, σ fija a todo elemento de $\mathbb{Q}(\sqrt[3]{2})$, y por lo tanto es el automorfismo identidad, y es el único. Es decir, $G(\mathbb{Q}(\sqrt[3]{2}),\mathbb{Q})=\{I_{\mathbb{Q}(\sqrt[3]{2})}\}$. Además, el campo fijado por $G(\mathbb{Q}(\sqrt[3]{2}),\mathbb{Q})$ es $\mathbb{Q}(\sqrt[3]{2})$ en su totalidad.

Los racionales adjuntos a $e^{2\pi i/5}$ relativo a los racionales

Sea $\omega=e^{2\pi i/5}$, y considérese $G(\mathbb{Q}(\omega),\mathbb{Q})$. Dado que es una raíz quinta de la unidad, es claro que $\omega^5=1$ y satisface al polinomio $x^4+x^3+x^2+x+1\in\mathbb{Q}[x]$. Es claro que este es irreducible sobre $\mathbb{Q}$, y por lo tanto $[\mathbb{Q}(\omega):\mathbb{Q}]=4$ y todo elemento en $\mathbb{Q}(\omega)$ es de la forma $\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3$, con $\alpha_0,\alpha_1,\alpha_2,\alpha_3\in\mathbb{Q}$. Ahora bien, si $\sigma:\mathbb{Q}(\omega)\to\mathbb{Q}(\omega)$ es un automorfismo que deja fijo a $\mathbb{Q}$, entonces $\sigma(\omega)^5=\sigma(1)=1$. Pero nótese que $\sigma(\omega)\neq 1$, puesto que σ es sobreyectivo y $\sigma(1)=1$. Entonces podemos hacer $\sigma_k(\omega)=\omega^k$ para $k\in\{1,2,3,4\}$. Es claro que σ_1 es el automorfismo identidad, y no es difícil demostrar que $\sigma_2^2=\sigma_4$, $\sigma_2^3=\sigma_3$, y $\sigma_2^4=\sigma_1$. Entonces, $G(\mathbb{Q}(\omega),\mathbb{Q})=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$ es un grupo cíclico de orden 4. Además, tampoco es difícil demostrar que el campo fijado en este caso es $\mathbb{Q}$ mismo. Por su parte, también es fácil ver que $\sigma_4^2=\sigma_1$, y entonces $\{\sigma_1,\sigma_4\}$ es un subgrupo cíclico de orden 2 de $G(\mathbb{Q}(\omega),\mathbb{Q})$. Por su parte, este tiene como campo fijado a todos los elementos de la forma $\alpha_0+\alpha_2(\omega^2+\omega^3)$, el cual es el campo $\mathbb{Q}(\omega^2+\omega^3)$, y cumple $[\mathbb{Q}(\omega^2+\omega^3):\mathbb{Q}]=2$.

Teorema 5M:

Si F es un campo y K es una extensión finita de F, entonces $o\big(G(K,F)\big)\leq[K:F]$.

Permutaciones en las funciones racionales de varias variables

Si F es un campo, $\sigma\in S_n$ y $r(x_1,\ldots,x_n)\in F(x_1,\ldots,x_n)$, entonces abreviando la notación es posible ver a σ actuando sobre $F(x_1,\ldots,x_n)$:

$$\sigma\big(r(x_1,\ldots,x_n)\big)=r(x_{\sigma(1)},\ldots,x_{\sigma(n)}).$$

De esta forma, σ es un automorfismo de $F(x_1,\ldots,x_n)$.

Campo de las funciones racionales simétricas

Si F es un campo, el campo de las funciones racionales simétricas S sobre F es el subcampo de $F(x_1,\ldots,x_n)$ fijado por S_n. Es decir, $r(x_1,\ldots,x_n)\in S$ si y solo si $r(x_1,\ldots,x_n)=r(x_{\sigma(1)},\ldots,x_{\sigma(n)})$ para todo $\sigma\in S_n$.

Funciones simétricas elementales

Las funciones simétricas elementales de $x_1,\ldots,x_n$ son:

$$a_1(x_1,\ldots,x_n)=\sum_{i=1}^{n}x_i;\qquad a_2(x_1,\ldots,x_n)=\sum_{i<j}^{n}x_ix_j;\qquad\cdots;\qquad a_n(x_1,\ldots,x_n)=\prod_{i=1}^{n}x_i.$$

En efecto, estos polinomios pertenecen al campo de las funciones racionales simétricas.

Polinomios simétricos de dos variables

Si $n = 2$, entonces $a_1 = x_1 + x_2$ y $a_2 = x_1x_2$. Nótese que x_1 y x_2 son las raíces de $t^2 - a_1t + a_2$.

Polinomios simétricos de tres variables

Si $n = 3$, entonces $a_1 = x_1 + x_2 + x_3$, $a_2 = x_1x_2 + x_3x_1$ y $a_3 = x_1x_2x_3$. Nótese que x_1, x_2 y x_3 son las raíces de $t^3 - a_1t^2 + a_2t - a_3$.

Polinomios simétricos de cuatro variables

Si $n = 3$, entonces $a_1 = x_1 + x_2 + x_3 + x_4$, $a_2 = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1$, $a_3 = x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_1 + x_4x_1x_2$. Nótese que x_1, x_2, x_3 y x_4 son las raíces de $t^4 - a_1t^3 + a_2t^2 - a_3t + a_4$.

Polinomios simétricos de n variables

En general, $x_1, \ldots, x_n$ son las raíces de $\sum_{i=0}^{n}(-1)^i a_i t^{n-i}$ con $a_0 = 1$.

Teorema 5N:

Si F es un campo y $n \in \mathbb{Z}^+$, entonces:

- $[F(x_1, \ldots, x_n) : S] = n!$;
- $G\big(F(x_1, \ldots, x_n), S\big) = S_n$;
- (Teorema de polinomios simétricos): Si $a_1, \ldots, a_n$ son las funciones simétricas elementales en las variables $x_1, \ldots, x_n$, entonces $S = F(a_1, \ldots, a_n)$. Esto es, toda función racional simétrica de n variables es una función racional evaluada en las n funciones simétricas elementales. O, puede enunciarse de manera que todo polinomio simétrico en n variables es un polinomio evaluado en las n funciones simétricas elementales;
- $F(x_1, \ldots, x_n)$ es el campo de descomposición sobre $S = F(a_1, \ldots, a_n)$ del polinomio definido por $\sum_{i=0}^{n}(-1)^i a_i t^{n-i} \in F(a_1, \ldots, a_n)[t]$ con $a_0 = 1$.

Comentarios sobre el teorema 5N

En los comentarios al teorema 5H se mencionó que dado un $n \in \mathbb{Z}^+$ es posible contruir un campo y un polinomio de grado n sobre dicho campo, cuyo campo de descomposición es de grado máximo $(n!)$. El teorema 5N explícitamente provee un ejemplo, dado un campo F.

Extensión normal

Si F es un campo, se dice que K es una extensión normal de F si esta es una extensión finita de F y además F es el campo fijado por $G(K, F)$.

Ejemplos de extensiones normales

De los ejemplos vistos respecto a grupos de automorfismos, es claro que $\mathbb{C}$ es extensión normal de $\mathbb{R}$; $\mathbb{Q}(\sqrt[3]{2})$ no es extensión normal de $\mathbb{Q}$; y $\mathbb{Q}(e^{2\pi i/5})$ es extensión normal de $\mathbb{Q}$.

Propiedad de extensiones normales

Si F es un campo, K es una extensión normal de F y $k \in K \sim F$, entonces k no queda invariante por algún automorfismo elemento de $G(K, F)$.

Teorema 5O:

Sea F un campo de característica cero, K una extensión normal de F, sea H un subgrupo de $G(K,F)$ y sea K_H el subcampo de K fijado por H. Entonces:

- $[K : K_H] = o(H)$;
- $H = G(K, K_H)$.

En particular, cuando $H = G(K,F)$, se tiene que $[K : F] = o\big(G(K,F)\big)$.

Lema 5.9:

Si F es un campo, K es el campo de descomposición sobre F de un polinomio $f(x) \in F[x]$, si $p(x) \in F[x]$ es irreducible y es factor de $f(x)$, y si $\alpha_1, \ldots, \alpha_r$ son las raíces de $p(x)$, entonces para cada α_i existe $\sigma_i \in G(K,F)$ tal que $\sigma_i(\alpha_1) = \alpha_i$.

Teorema 5P:

Si F es un campo de característica cero, entonces K es una extensión normal de F si y solo si K es el campo de descomposición de un polinomio sobre F.

Grupo de Galois de un polinomio

Si F es un campo y K es el campo de descomposición de $f(x) \in F[x]$ sobre F, el grupo de Galois de $f(x)$ sobre F es $G(K,F)$.

Nota sobre los grupos de Galois

El grupo de Galois de $f(x)$ sobre F puede considerarse como un grupo de permutaciones de las raíces de $f(x)$. Si α es una raíz de $f(x)$ y $\sigma \in G(K,F)$, entonces $\sigma(\alpha)$ es también una raíz de $f(x)$.

Teorema 5Q (Teorema fundamental de la teoría de Galois):

Si F es un campo, K es el campo de descomposición de $f(x) \in F[x]$ sobre F, y $G(K,F)$ es el grupo de Galois de $f(x)$ sobre F. Entonces, para todo T subcampo de K y para todo H subgrupo de $G(K,F)$ existe una correspondencia biyectiva entre la colección de subcampos de K que contienen a F y los subgrupos de $G(K,F)$, tal que:

- $T = K_{G(K,T)}$;
- $H = G(K, K_H)$;
- $[K : T] = o\big(G(K,T)\big)$ y $[T : F] = i_{G(K,F)}\big(G(K,T)\big)$;
- T es una extensión normal de F si y solo si $G(K,T)$ es un subgrupo normal de $G(K,F)$;
- Si T es una extensión normal de F, entonces $G(T,F) \approx G(K,F)/G(K,T)$.

7. Solubilidad por radicales

Si F es un campo, entonces $p(x) \in F[x]$ es soluble por radicales si existe una colección finita de campos

$$F_1 = F(\omega_1), F_2 = F_1(\omega_2), \ldots, F_k = F_{k-1}(\omega_k) = F(\omega_1, \ldots, \omega_k),$$

tales que $\omega_1^{r_1} \in F, \omega_2^{r_2} \in F_1, \ldots, \omega_k^{r_k} \in F_{k-1}$, para $r_1, r_2, \ldots, r_k \in \mathbb{Z}^+$, y además F_k contiene al campo de descomposición de $p(x)$ sobre F.

Normalidad de F_k

Si F es un campo con $p(x) \in F[x]$ soluble por radicales, entonces F_k es una extensión normal de F.

Polinomio general

Si F es un campo, entonces $p(x) = \sum_{i=0}^{n} a_i x^{n-i} \in F[x]$ con $a_0 = 1$ es el polinomio general de grado n sobre F, y $p(x)$ es un polinomio particular de $F(a_1, \ldots, a_n)$.

Grupos solubles

Un grupo G es soluble si existe una cadena finita de subgrupos tales que

$$(e) = N_k \subseteq N_{k-1} \subseteq \cdots \subseteq N_2 \subseteq N_1 \subseteq N_0 = G,$$

donde N_k es subgrupo normal de N_{k-1} y además N_{k-1}/N_k es abeliano, para cada k.

Ejemplos de grupos solubles

- Todo grupo abeliano es soluble, con $N_0 = G$ y $N_1 = (e)$.
- S_3 es soluble.
- S_4 es soluble.
- S_n con $n \geq 5$ no es soluble.

Subgrupo conmutador

Dado un grupo G con $g_1, g_2 \in G$, el conmutador de g_1 y g_2 es $g_1^{-1} g_2^{-1} g_1 g_2$, y el subgrupo conmutador de G, denotado G', es el subgrupo de G generado por todos los conmutadores de G. Este es un subgrupo normal de G, y además G/G' es un grupo abeliano. Además, G' es el subgrupo normal de G más pequeño cuyo cociente es abeliano. Es decir, si M es normal en G y G/M es abeliano, $G' \subseteq M$.

Segundo subgrupo conmutador

Si G es un grupo, G'' es el subgrupo conmutador de G'. Resulta que G'' es un subgrupo normal de G' y de G. Además, G'/G'' es abeliano.

n-avo subgrupo conmutador

Si G es un grupo, $G^{(n)}$ es el subgrupo conmutador de $G^{(n-1)}$. Resulta que $G^{(n)}$ es un subgrupo normal de $G^{(k)}$ para todo $1 \leq k \leq n-1$, y de G. Además, $G^{(n-1)}/G^{(n)}$ es abeliano.

Lema 5.10:

Un grupo G es soluble si y solo si existe $k \in \mathbb{N}$ tal que $G^{(k)} = (e)$.

Corolario del lema 5.10:

Toda imagen homomórfica de un grupo soluble es un grupo soluble.

Lema $5.\alpha$:

Si G es un grupo y N es un subgrupo normal de G, entonces N' es un subgrupo normal de G.

Lema 5.11:

Si $n \geq 5$ y $k \in \mathbb{Z}^+$, entonces $S_n^{(k)}$ contiene a todos los 3-ciclos de S_n.

Teorema 5R:

Si $n \geq 5$, entonces S_n no es soluble.

Lema 5.12:

Sea F un campo de característica cero que contiene a las n-ésimas raíces de la unidad, sea $a \in F$ no nulo, y sea K el campo de descomposición de $x^n - a \in F[x]$ sobre F. Entonces,

- $K = F(u)$, donde u es cualquier raíz de $x^n - a$;
- El grupo de Galois de $x^n - a$ sobre F es abeliano.

Nota del lema 5.12

Este lema nos dice que si F contiene a todas las n-ésimas raíces de la unidad, entonces al adjuntar una raíz u de $x^n - a$ se obtiene el campo de descomposición sobre F del polinomio $x^n - a$, es decir, $F(u)$ es una extensión normal de F.

Teorema 5S:

Si F es un campo de característica cero que contiene a todas las n-ésimas raíces de la unidad y $p(x) \in F[x]$ es un polinomio soluble por radicales, entonces el grupo de Galois de $p(x)$ sobre F es un grupo soluble.

Teorema 5γ:

Si el grupo de Galois de un polinomio es soluble, entonces el polinomio es soluble por radicales.

Teorema 5δ:

Dado un campo F cualquiera, entonces $p(x) \in F[x]$ es un polinomio soluble por radicales si y solo si el grupo de Galois de $p(x)$ sobre F es un grupo soluble.

Teorema 5T (Teorema de Abel):

El polinomio general de grado $n \geq 5$ no es soluble por radicales.

Los grupos de Galois sobre $\mathbb{Q}$

Teorema 5U (Infinitos ejemplos de alcanzar la cota superior):

Si $q(x) \in \mathbb{Q}[x]$ es irreducible, $p = \text{gr}(q)$ es un número primo, y $q(x)$ posee exactamente dos raíces no reales en $\mathbb{C}$, entonces el grupo de Galois de $q(x)$ sobre $\mathbb{Q}$ es S_p. Además, si K es el campo de descomposición de $q(x)$ sobre $\mathbb{Q}$, entonces $[K : \mathbb{Q}] = o\big(G(K, \mathbb{Q})\big) = o(S_p) = p!$.

Ejemplo 1: $x^3 - 2$

El polinomio $x^3 - 2 \in \mathbb{Q}$ es irreducible, y posee exactamente una raíz real y dos raíces complejas no reales. Entonces el grupo de Galois de $x^3 - 2$ es S_3, y por lo tanto $[E : \mathbb{Q}] = o(S_3) = 3! = 6$ (donde E es el campo de descomposición de $x^3 - 2$ sobre $\mathbb{Q}$). Se sabía con anterioridad que el campo de descomposición de $x^3 - 2$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\omega)$, donde $\omega^3 = 1$ y $\omega \neq 1$. En efecto, es fácil comprobar que se cumple $[\mathbb{Q}(\omega) : \mathbb{Q}] = 6 = 3! = o(S_3)$.

Ejemplo 2: $2x^5 - 10x + 5$

El polinomio $2x^5 - 10x + 5 \in \mathbb{Q}[x]$ es irreducible, y posee exactamente tres raíces reales y dos raíces complejas no reales. El grupo de Galois del polinomio es entonces S_5, y entonces $q(x)$ no es soluble por radicales., y por lo tanto $[E : \mathbb{Q}] = o(S_5) = 5! = 120$ (donde E es el campo de descomposición de $2x^5 - 10x + 5$ sobre $\mathbb{Q}$). Además, por el teorema de Abel, $2x^5 - 10x + 5$ no es soluble por radicales.