UNIVERSIDAD NACIONAL

DE LA MATANZA

Licenciatura en Matemática Aplicada

El cuerpo $\mathrm{Q}(\alpha)$ *como extensión de* Q

Fayolle Ana Laura

Tutora: *Lic. Mariana Valeria Pérez*

Diciembre 2011

El cuerpo $\mathbb{Q}(\alpha)$ *como extensión de* $\mathbb{Q}$

Fayolle Ana Laura

Introducción

Sabemos que el problema de encontrar soluciones racionales de una ecuación $f(t)=0$ con f un polinomio con coeficientes racionales se resuelve completamente: el criterio de Gauss nos proporciona el conjunto de posibles raíces. También el problema de factorizar en $\mathbb{Q}(t)$ tiene una respuesta definitiva: el algoritmo de factorización de Kronecker[I], aunque no la mejor, es una herramienta para tal tarea.

Incluso conocemos diferentes métodos que permiten localizar de forma aproximada las raíces reales del polinomio f, si es que las tiene. Tales como el método de la bisección, de la secante, el método de Newton-Raphson, entre otros.

[I] En el anexo puede encontrar los pasos en los que consiste tal algoritmo.

Este trabajo pretende abordar el tema de raíces de polinomios, pero desde una perspectiva totalmente diferente.

Por el *teorema fundamental del álgebra*[II] sabemos que todo polinomio con coeficientes racionales, posee al menos una raíz (real o compleja). Eso no lo discutimos.

Ahora, sea $f \in \mathbb{Q}(t)$ irreducible en $\mathbb{Q}$ ¿existe un cuerpo que incluya a $\mathbb{Q}$ y contenga una de sus raíces? La respuesta resultaría trivial si no aclaramos que deseamos que ese cuerpo sea el menor cuerpo que la contenga; pues de no hacer esta aclaración, la respuesta sería *sí* : el cuerpo de los reales, o,"como mucho", el de los complejos.

Así, el trabajo consiste en el análisis de los cuerpos que surgen al tratar ecuaciones del tipo $f(t)=0$, con f un polinomio con coeficientes racionales e irreducible en $\mathbb{Q}$.

Los cuatro capítulos del trabajo responden a la complejidad y generalidad de los casos y conceptos analizados en cada uno de ellos.

En el primer capítulo veremos que el cuerpo buscado surge a partir de una raíz conocida del polinomio (sea ésta real o compleja). Es decir, conociendo un elemento que anula al polinomio, construimos a partir de éste al menor conjunto incluido en $\mathbb{R}$ (o, si el elemento es complejo, incluido en $\mathbb{C}$), que contenga a $\mathbb{Q}$ y resulte cuerpo.

El segundo capítulo propone determinar este cuerpo en casos en que se desconocen las raíces del polinomio. El "quid" del capítulo radica en un método que sólo precisa la confirmación de la existencia de raíces, prescindiendo del reconocimiento preciso de las mismas. La aplicación del mismo supone el manejo de la noción de clases de congruencia módulo un polinomio.

[II] Este teorema es debido a Gauss (1777-1855) quién dio de él cinco demostraciones distintas. Actualmente, existen decenas de demostraciones, algunas usan Análisis Complejo, otras Teoría de Cuerpos o Topología, todas fuera del alcance de estas notas. En el anexo puede encontrar en qué consiste este reconocido teorema.

En el tercer capítulo se hace una comparación de las construcciones hechas en el primero y segundo capítulo. La comparación se erige, y por eso se hace posible, en los morfismos de anillos.

Por último, se concluye con el concepto de *cuerpo de descomposición*. Este último capítulo pretende dar un cierre al recorrido hecho en los capítulos anteriores. Humildemente se presentarán casos que ejemplifiquen lo planteado y que den una idea de lo que este concepto encierra. Pero cabe aceptar que es en sí mismo, un tema tan amplio y profundo, que sobrepasa los límites de este trabajo.

Se notará que cada capítulo finaliza con un teorema y su correspondiente demostración. Es una forma de "coronar" lo expuesto en cada uno de ellos y darle mayor rigor científico.

Al final del trabajo se da una aplicación directa de este tipo de extensión de cuerpos. Ésta consiste en racionalizar[III] expresiones "no del todo usuales".

[III] Veremos más adelante lo que realmente significa *racionalizar* una expresión.

Capítulo 1: *El cuerpo* $\mathbb{Q}(\alpha)$

Sea $f(t)$ un polinomio con coeficientes en un cuerpo E e irreducible en dicho cuerpo.

Sea α un elemento tal que $f(\alpha)=0$.

Nos proponemos definir, primero, al menor conjunto *K* que contenga al elemento α tal que $E \subset K$.

Luego, nuestro objetivo es poder demostrar cuál es la estructura del conjunto *K*.

Para ello trabajaremos con un caso concreto.

Consideremos el polinomio $f(t)=t^3-3 \in \mathbb{Q}[t]$.

Sabemos por el teorema de Gauss que no posee raíces racionales. Por ser un polinomio de grado 3, se desprende entonces, que es irreducible en $\mathbb{Q}$ [IV].

Una raíz del polinomio es $\alpha=\sqrt[3]{3}$, es decir, es el elemento que anula al polinomio, o sea $f(\alpha)=0$.

Es evidente para el lector que $\sqrt[3]{3} \notin \mathbb{Q}$ pues si lo fuera

$\sqrt[3]{3}=\frac{a}{b},\ a,b \in \mathbb{Z} \Rightarrow 3=\frac{a^3}{b^3} \Rightarrow 3b^3=a^3$ absurdo (por el teorema fundamental de la aritmética[V]).

Entonces nuestra pregunta es: ¿Existe un conjunto K tal que $\sqrt[3]{3} \in K$ de manera que $\mathbb{Q} \subset K \subset \mathbb{R}$? ¿Cuál es la estructura de *K*?

[IV] $f \in \mathbb{Q}[t]$ de grado 2 ó 3 es reducible si y sólo si tiene una raíz en $\mathbb{Q}$ (pues por cuestiones de grado, si es reducible tiene que tener al menos un factor de grado 1).

[V] El Teorema Fundamental de la Aritmética aparece en el libro IX de Los Elementos de Euclides, texto del siglo IV antes de nuestra era considerado por muchos como el primer libro de Matemáticas modernas de la historia. El enunciado de tal teorema se encuentra en el anexo.

Para poder responder, es conveniente hacer el siguiente recorrido:

a) Definir al conjunto K como $\mathbb{Q}(\alpha)$.

b) Comprobar que $\mathbb{Q}(\alpha)$ posee estructura de anillo conmutativo bajo la suma y multiplicación.

c) Comprobar que $\mathbb{Q}(\alpha)$ posee estructura de $\mathbb{Q}$-*espacio vectorial* y determinar cuál es su base.

d) Demostrar que todo elemento no nulo de $\mathbb{Q}(\alpha)$ posee inverso. Es decir, ver que $\mathbb{Q}(\alpha)$ posee estructura de cuerpo.

a) Definir al conjunto $\mathbb{Q}(\alpha)$.

Teniendo en claro que $\alpha = \sqrt[3]{3}$, las siguientes igualdades resultan ciertas:

$$\alpha^3 = 3$$

$$\alpha^4 = 3\alpha$$

$$\alpha^5 = 3\alpha^2$$

$$\alpha^6 = 9$$

Así, se puede verificar los resultados de los siguientes cálculos:

$$* \; 2 + 3\alpha^2 + \frac{5}{2}\alpha^4 - 7\alpha^{10} = 2 - \frac{363}{2}\alpha + 3\alpha^2$$

$$* \; -400\alpha^{80} - 5\alpha^2 + 2\alpha^3 - \frac{5}{2}\alpha^4 - 4\alpha^5 = 6 - \frac{15}{2}\alpha - \left(400.3^{26} - 17\right)\alpha^2$$

$$* \; -\alpha^4 + 7 - 4\alpha^{41} - \alpha^{130} + 5\alpha^{51} = \left(7 + 5.3^{17}\right) + \left(-3 - 3^{43}\right)\alpha + \left(-4.3^{13}\right)\alpha^2$$

Estos resultados sugieren que cualquier expresión que involucre sumas y productos de números racionales y del elemento α puede expresarse mediante un elemento del siguiente conjunto:

$$\mathbb{Q}(\alpha) = \left\{ a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q} \right\}$$

Queda claro que $\mathbb{Q} \subset \mathbb{Q}(\alpha)$.

b) Comprobar que $\mathbb{Q}(\alpha)$ posee estructura de anillo conmutativo bajo la suma y multiplicación.

Definimos la suma y producto entre elementos de $\mathbb{Q}(\alpha)$ de la siguiente manera:

suma:

$$\left(a + b\alpha + c\alpha^2\right) + \left(d + e\alpha + f\alpha^2\right) := (a + d) + (b + e)\alpha + (c + f)\alpha^2$$

producto:

$$\left(a + b\alpha + c\alpha^2\right).\left(d + e\alpha + f\alpha^2\right) := (ad + 3bf + 3ce) + (ae + bd + 3cf)\alpha + (af + be + cd)\alpha^2$$

Es sencillo ver que $(\mathbb{Q}(\alpha), +)$ posee estructura de grupo abeliano pues se verifican:

- ✓ La ley de cierre
- ✓ La conmutatividad
- ✓ La asociatividad
- ✓ La existencia de elemento neutro, es decir $e = 0 + 0\alpha + 0\alpha^2$ donde $e \in \mathbb{Q}(\alpha)$
- ✓ La existencia del elemento inverso:

$$\left(a + b\alpha + c\alpha^2\right) + \left(-a + (-b)\alpha + (-c)\alpha^2\right) = 0 + 0\alpha + 0\alpha^2$$

Así verificamos fácilmente que $(\mathbb{Q}(\alpha), +, .)$ es anillo conmutativo, pues:

- ✓ $(\mathbb{Q}(\alpha), +)$ es grupo abeliano

- ✓ La multiplicación es cerrada en $\mathbb{Q}(\alpha)$
- ✓ La multiplicación cumple la propiedad asociativa
- ✓ La multiplicación cumple la propiedad conmutativa
- ✓ Se cumple la distributividad (tanto por izquierda como por derecha) del producto respecto a la suma.

c) Comprobar que $\mathbb{Q}(\alpha)$ posee estructura de $\mathbb{Q}$-*espacio vectorial* y determinar cuál es su base.

La manera en que sumamos elementos de $\mathbb{Q}(\alpha)$ (sumamos los coeficientes de potencias iguales de α) nos hace pensar a $\mathbb{Q}(\alpha)$ como un $\mathbb{Q}$-*espacio vectorial:*

Sean $A, B, C \in \mathbb{Q}(\alpha)$ y $\lambda, \mu \in \mathbb{Q}$

- ✓ $A + B \in \mathbb{Q}(\alpha)$
- ✓ $(A+B)+C = A+(B+C)$
- ✓ $A+B = B+A$
- ✓ $A+0 = A$
- ✓ $A+(-A) = 0$
- ✓ $\lambda . A \in \mathbb{Q}(\alpha)$
- ✓ $\lambda.(\mu A) = (\lambda.\mu)A$
- ✓ $\lambda.(A+B) = \lambda A + \lambda B$
- ✓ $(\lambda+\mu).A = \lambda A + \mu A$

Ahora falta ver que $\{1;\alpha;\alpha^2\}$ es base[VI] de $\mathbb{Q}(\alpha)$ como $\mathbb{Q}$-*espacio vectorial*.

Para ello primero nos apoyaremos en que $f(t)$ es el polinomio de menor grado con coeficientes en $\mathbb{Q}$ que anula a α. Pero esto también debemos demostrarlo:

Sabemos que $f(t)=t^3-3\in\mathbb{Q}[t]$ es irreducible en $\mathbb{Q}$. Veamos que:

Si $g\in\mathbb{Q}[t]$ es un polinomio no nulo que anula a α $\Rightarrow g$ es múltiplo de *f*.

En efecto, supongamos que $g(\alpha)=0$ y $gr\left(g(t)\right)>3$.

Si dividimos al polinomio $g\in\mathbb{Q}[t]$ por $f(t)=t^3-3$ queda

$g(t)=f(t).q(t)+r(t)$ donde $r(t)=0$ *ó* $gr\left(r(t)\right)<3$.

Así, podemos escribir a $r(t)=a+bt+ct^2$ con $a,b,c\in\mathbb{Q}$.

Ahora bien, si evaluamos *g(t)* en α:

$$\underbrace{g(\alpha)}_{=0}=\underbrace{f(\alpha)}_{=0}.q(\alpha)+r(\alpha)\ \Rightarrow r(\alpha)=0\ \Rightarrow a+b\alpha+c\alpha^2=0 \text{ con } a,b,c\in\mathbb{Q}.$$

Entonces *r(t)* resultaría un polinomio de grado igual o menor que 2 que también anula a α (a parte de *f(t)*).

Pero veamos que si el grado de *r(t)* es 1, entonces tenemos que $r(t)=a+bt$ con $a,b\in\mathbb{Q}$, $b\neq 0$.

Por lo que, $r(\alpha)=0\Rightarrow a+b\alpha=0\ \Rightarrow \alpha=-\dfrac{b}{a}\Rightarrow\ \alpha^3=\left(-\dfrac{b}{a}\right)^3\ \Rightarrow 3=-\dfrac{b^3}{a^3}$

VI Condiciones para que un conjunto ordenado B sea base de un espacio vectorial V:
*todos los elementos de B pertenecen al espacio vectorial V.
*los elementos de B forman un sistema linealmente independiente.
*todo elemento de V se puede escribir como combinación lineal de los elementos de la base B

$\Rightarrow\ 3a^3 = -b^3$ y llegamos así a una contradicción, que proviene de suponer que el grado de *r(t)* es 1 (por el teorema fundamental de la aritmética).

De forma similar comprobamos que *r(t)* no puede ser de grado 2.

En efecto, si escribimos: $r(t) = a + bt + ct^2$ con $a, b, c \in \mathbb{Q},\ c \neq 0$ y tal que $r(\alpha) = 0$

como α es simultáneamente raíz de *f(t)* y de *r(t)*, éstos deben poseer un factor en común

$$\Rightarrow \left(f(t); g(t) \right) = d(t) \neq 1 \quad con \quad d(t) \in \mathbb{Q}[t],\ gr\left(d(t)\right) > 0$$ [VII]

$$\Rightarrow d(t) / f(t) \Rightarrow f(t) = d(t).q(t),\ \ con\ q(t) \in \mathbb{Q}[t]$$

Pero *f* es un polinomio irreducible en $\mathbb{Q}[t] \ \Rightarrow\ q(t) = q \in \mathbb{Q}$

Pero como *f* es mónico $\Rightarrow$ *q*=1 $\Rightarrow \left(f(t); r(t) \right) = f(t)$. Pero $\underbrace{f(t)}_{gr\,3} / \underbrace{r(t)}_{gr\,2}$ llegando a una contradicción.

Por lo tanto no existe un polinomio de grado 2 con coeficientes en $\mathbb{Q}$ que anule a α.

El absurdo proviene de suponer que existe un polinomio *g* de grado mayor que 3 que anule a α.

$\therefore\ f(t)$ es el polinomio de menor grado con coeficientes en $\mathbb{Q}$ que anula a α.

Con lo cual, podemos asegurar que cualquier polinomio de la forma:

$r(t) = a + b\alpha + c\alpha^2\ \ con\ a, b, c \in \mathbb{Q}$ tal que $r(\alpha) = 0$ es el polinomio nulo.

Finalmente podemos asegurar que si $a = b = c = 0 \Rightarrow \left\{1;\ \alpha;\ \alpha^2\right\}$ es un sistema linealmente independiente de $\mathbb{Q}(\alpha)$ como $\mathbb{Q}$-*espacio vectorial.*

[VII] Denotamos con $\left(f(t); g(t) \right)$ al divisor común mayor de ambos polinomios.

Así todo elemento $A \in \mathbb{Q}(\alpha)$ lo podemos escribir como $A = a + b\alpha + c\alpha^2$ con $a, b, c \in \mathbb{Q}$ y así resulta una $\mathbb{Q}$-combinación lineal de los elementos $1, \alpha, \alpha^2$, por lo que $\{1;\ \alpha;\ \alpha^2\}$ genera cualquier elemento de $\mathbb{Q}(\alpha)$.

$\therefore$ $\mathrm{B} = \{1;\ \alpha;\ \alpha^2\}$ es una base de $\mathbb{Q}(\alpha)$ y su dimensión es el grado del polinomio $f(t) = t^3 - 3$, es decir $dim_{\mathbb{Q}}\mathbb{Q}(\alpha) = gr(f(t)) = 3$ [VIII].

d) Demostrar que todo elemento no nulo de $\mathbb{Q}(\alpha)$ posee inverso. Es decir, ver que $\mathbb{Q}(\alpha)$ posee estructura de cuerpo.

Dado $a + b\alpha + c\alpha^2 \in \mathbb{Q}(\alpha)$ no nulo, formalmente el inverso multiplicativo tiene la forma $\dfrac{1}{a + b\alpha + c\alpha^2}$ pues $(a + b\alpha + c\alpha^2) \cdot \dfrac{1}{a + b\alpha + c\alpha^2} = 1$.

Pero expresar a tal inverso de esa forma no soluciona el problema. Pues debemos demostrar que $\dfrac{1}{a + b\alpha + c\alpha^2} \in \mathbb{Q}(\alpha)$, es decir, que se puede expresar como combinación lineal de los elementos de $\mathrm{B} = \{1;\ \alpha;\ \alpha^2\}$.

Entonces buscamos un elemento $d + e\alpha + f\alpha^2 \in \mathbb{Q}(\alpha)$ tal que

$$(a + b\alpha + c\alpha^2) \cdot (d + e\alpha + f\alpha^2) = 1$$

Para ello volveremos a una idea básica que se utiliza al trabajar en $\mathbb{Z}$: el algoritmo de Euclides y la identidad de Bézout[IX]. Ésta proporciona un modo de encontrar inversos modulares; aquí la utilizaremos para encontrar el inverso de un elemento de $\mathbb{Q}(\alpha)$.

[VIII] Denotamos $dim_{\mathbb{Q}}\mathbb{Q}(\alpha)$ a la dimensión de $\mathbb{Q}(\alpha)$ como $\mathbb{Q}$-espacio vectorial.

Asociado al elemento $a+b\alpha+c\alpha^2$ tenemos el polinomio $g(t)=a+bt+ct^2 \in \mathbb{Q}[t]$ cuyos coeficientes son las coordenadas del vector $a+b\alpha+c\alpha^2$ con respecto a la base $\mathrm{B}=\{1;\ \alpha;\ \alpha^2\}$.

Como $a+b\alpha+c\alpha^2 \neq 0$ (es decir, es un vector no nulo) $\Rightarrow$ alguna coordenada es no nula, por lo tanto, *g* es un polinomio no nulo y así, $gr(g(t)) \leq 2$.

Por otro lado, el polinomio $f(t)=t^3-3$ es el polinomio irreducible con coeficientes en $\mathbb{Q}$ de grado mínimo que anula a α. Y como $g(t)=a+bt+ct^2$ es tal que $g(\alpha)\neq 0$, entonces α no es raíz de *g(t)* y por consiguiente $(f(t);g(t))=1$

Es decir, los polinomios *f* y *g* son coprimos en $\mathbb{Q}[t]$, de lo que se desprende, debido a la identidad de Bézout, que existen polinomios *r* y *s* en $\mathbb{Q}[t]$ tales que

$$f(t).r(t)+g(t).s(t)=1$$

Evaluando esta identidad en α, resulta que

$$\underbrace{f(\alpha)}_{=0}.r(\alpha)+g(\alpha).s(\alpha)=1 \Rightarrow g(\alpha).s(\alpha)=1 \Rightarrow \left(a+b\alpha+c\alpha^2\right).s(\alpha)=1$$

Así, encontramos una combinación lineal con coeficientes en $\mathbb{Q}$ de potencias de α que proporciona un inverso multiplicativo de $a+b\alpha+c\alpha^2$.

Pero falta un detalle: $s(\alpha)$ se obtiene evaluando el polinomio *s(t)* en α; para ser un elemento de $\mathbb{Q}(\alpha)$, es decir, expresarse en la base $\mathrm{B}=\{1;\ \alpha;\ \alpha^2\}$, el polinomio *s(t)* debe tener grado a lo sumo 2.

Pero…¿por qué estamos tan seguros que el grado de *s(t)* es menor o igual que 2?

Haremos uso del algoritmo de la división.

Supongamos que $gr(s(t)) \geq 3$ es tal que $\left(a+b\alpha+c\alpha^2\right)\cdot s(t)=1$

[IX] En el anexo puede encontrar en qué consiste la Identidad de Bézout.

Dividamos *s(t)* por *f(t)*: $s(t) = f(t).q(t) + s'(t)$ donde $0 < gr(s'(t)) < 3$

$\Rightarrow s(\alpha) = \underbrace{f(\alpha)}_{=0}.q(\alpha) + s'(\alpha) \Rightarrow s(\alpha) = s'(\alpha)$

En conclusión, si *s(t)* es un polinomio de grado mayor o igual que 3 que cumple que $(a + b\alpha + c\alpha^2) \cdot s(\alpha) = 1$, podemos conseguir otro polinomio $s'(t) \in \mathbb{Q}[t]$ con $gr(s'(t)) \leq 2$ tal que $(a + b\alpha + c\alpha^2) \cdot s'(\alpha) = 1 \Rightarrow s(\alpha) \in \mathbb{Q}(\alpha)$

Así hemos demostrado que $\mathbb{Q}(\alpha)$ es un cuerpo que contiene a $\mathbb{Q}$ y, lo más importante, que es un cuerpo donde el polinomio irreducible $f(t) = t^3 - 3 \in \mathbb{Q}[t]$ tiene una raíz.

Aquí concluye el recorrido propuesto en este capítulo.

Pero con el objetivo de darle mayor rigor al trabajo previo, expondremos una serie de definiciones que lo engloban y, a la vez, lo extienden.

Definiciones

En lo que sigue *E* y *K* son cuerpos arbitrarios tales que *K* contiene a *E*.

Definición 1.1. Si K es un cuerpo que contiene a un subcuerpo E, decimos que K es una ***extensión del cuerpo*** E, y se simboliza K/E.

Si K/E es cualquier extensión de cuerpos, luego la multiplicación definida en K convierte a K en un *espacio vectorial* sobre E. Así K es un *E-espacio vectorial.*

El grado de la extensión es la dimensión[X] de K como *E-espacio vectorial*, y lo denotaremos $[K : E]$.

Definición 1.2. Un elemento $\alpha \in K$ es ***algebraico*** sobre E si existe un polinomio $f \in E[t]$ tal que $f(\alpha) = 0$.

Además, si el polinomio f es irreducible sobre E decimos que f es el ***polinomio minimal*** de α sobre E.

Definición 1.3. Se define a $E(\alpha)$ como el conjunto de las combinaciones lineales con coeficientes en E de las potencias de α:

$$E(\alpha) = \left\{ a_0 + a_1\alpha + \ldots + a_n\alpha^n : a_i \in E, n \in N \right\}$$

Esta escritura pone en evidencia que $E(\alpha)$ posee una estructura de *E-espacio vectorial*.

[X] La dimensión de un espacio vectorial se define como el cardinal de una base vectorial para dicho espacio.

Teorema de la extensión $E(\alpha)$ del cuerpo *E*

Sea α algebraico sobre E y sea n el grado del polinomio minimal $f \in E[t]$ de α sobre E. Entonces $E(\alpha)$ es un cuerpo y el grado de la extensión $[E(\alpha):E]$ es igual a n.

La demostración de este teorema sigue pasos similares a los que hemos recorrido en el caso de $f(t) = t^3 - 3 \in Q[t]$ analizado en el presente capítulo. La intención no es ser reiterativos, pero es de suma importancia demostrarlo para dar cuenta del alcance del mismo.

Demostración.

Sea $m(t) = t^n + b_{n-1}t^{n-1} + ... + b_0 \in E[t]$ el minimal de α sobre *E*.

Podemos ver que $E(\alpha)$ es un *E*-espacio vectorial de dimensión *n* y que una base del mismo es el conjunto $B = \{1; \alpha; ...; \alpha^{n-1}\}$. Pues, tomando un elemento $A \in E(\alpha)$ tal que

$$A = a_0.1 + a_1.\alpha + ... + a_{n-1}.\alpha^{n-1} = 0 \Rightarrow a_0 = ... = a_{n-1} = 0$$

Consideremos el polinomio *f* asociado al elemento *A*, $f(t) = a_0 + a_1.t + ... + a_{n-1}.t^{n-1}$ perteneciente a $E[t]$ que anule a α.

Como *m(t)* es el polinomio minimal de α sobre *E*, entones $\underbrace{m(t)}_{gr\ n} / \underbrace{f(t)}_{gr\ n-1}$, o sea, $f(t) = 0$, con lo que resulta $a_0 = ... = a_{n-1} = 0$. Por lo tanto $\{1; \alpha; ...; \alpha^{n-1}\}$ es un sistema linealmente independiente.

En consecuencia, todo elemento $A \in E(\alpha)$ puede expresarse como

$A = a_0.1 + a_1.\alpha + ... + a_{n-1}.\alpha^{n-1}$ con $a_i \in E \Rightarrow \{1; \alpha; ...; \alpha^{n-1}\}$ genera a $E(\alpha)$ con lo cual

$\mathrm{B} = \{1; \alpha; ...; \alpha^{n-1}\}$ es base.

Por las características de los elementos de $E(\alpha)$, es evidente que $E(\alpha)$ es cerrado bajo la suma.

No tan evidente es confirmar que $E(\alpha)$ es cerrado bajo el producto.

Como α es raíz de *m(t)*, tenemos $\alpha^n = -b_0 - b_1\alpha - ... - b_{n-1}\alpha^{n-1}$, es decir, todas las potencias de α se expresan como combinación lineal de los elementos de la base B. Por lo tanto $E(\alpha)$ es cerrado bajo el producto.

Se puede ver entonces que $(E(\alpha);+;.)$ es un anillo que contiene a *E*.

Resta ver que todo elemento no nulo de $E(\alpha)$ posee inverso multiplicativo en $E(\alpha)$.

Dado $A = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} \in E(\alpha)$ no nulo, buscamos un elemento $B \in E(\alpha)$ tal que $A.B = 1$.

Asociado a $A \in E(\alpha)$ tenemos el polinomio $f(t) = a_0 + a_1 t + ... + a_{n-1}t^{n-1} \in E(\alpha)$ donde los coeficientes son las coordenadas del elemento A con respecto a la base B.

Como $A \neq 0$, alguna de las coordenadas del vector es no nula, con lo que *f(t)* es no nulo y $gr(f(t)) \leq n-1$.

Por otro lado *m(t)* es el polinomio minimal de α, es decir, irreducible con coeficientes en *E*.

Como $(f(t); m(t)) = 1$ *en* $E[t]$, por la Identidad de Bézout, sabemos que existen polinomios $r, s \in E[t] / \quad f(t).r(t) + m(t).s(t) = 1$

$$\Rightarrow f(\alpha).r(\alpha) + \underbrace{m(\alpha)}_{=0}.s(\alpha) = 1 \Rightarrow f(\alpha).r(\alpha) = A.r(\alpha) = 1$$

Falta ver que $r(\alpha) \in E(\alpha)$. Para ello debemos ver que $r(t) \in E[t],\ gr(r(t)) \leq n-1$, pero podemos asegurar que existe un polinomio $r(t) \in E[t],\ gr(r(t)) \leq n-1$ tal que $A.r(t) = 1$, así el inverso de A pertenece a $E(\alpha)$.

$\therefore E(\alpha)$ es un cuerpo que contiene a *E*, y es un cuerpo donde el polinomio minimal *m(t)* tiene una raíz.

Capítulo 2: *El cuerpo* $\mathbb{Q}[t]/\langle f(t)\rangle$

Sea $f(t)$ un polinomio con coeficientes en un cuerpo E e irreducible en dicho cuerpo.

Se desconoce al elemento α tal que $f(\alpha)=0$.

Ahora nuestro propósito es "construir" este elemento para poder determinar cuál es el menor conjunto *K* al que pertenece y que a la vez, contenga al cuerpo *E*.

De forma análoga al trabajo hecho en el primer capítulo, se desea determinar la estructura de tal conjunto.

Si bien el objetivo es dar una respuesta válida para cualquier caso, partiremos y trabajaremos con un polinomio en particular a modo de ejemplo para poder después extender las conclusiones. De esta manera se pretende simplificar y darle mayor claridad al problema en cuestión.

Consideremos entonces $f(t)=t^3-3t+1\in\mathbb{Q}[t]$.

Por el teorema de Gauss se deduce que es irreducible en $\mathbb{Q}$ pues no posee raíces racionales.

$f(1)=-1\neq 0$ y $f(-1)=3\neq 0$.

Nuestro objetivo es entonces determinar si existe un conjunto *K* que contenga a $\mathbb{Q}$ y donde f tenga una raíz.

Si bien el planteo es similar al del capítulo 1, la gran diferencia radica en que desconocemos al elemento α tal que $f(\alpha)=0$.

Simplemente nos "conformaremos"[XI] con asegurar la existencia de una raíz real del polinomio *f*. Para ello apelaremos a ciertas nociones de análisis[XII].

Evaluando a la función en $x = 1$ y $x = 2$, y Teorema de Bolzano[XIII] de por medio:

$$\left.\begin{array}{l} f(1) = -1 \\ f(2) = 3 \end{array}\right\} \Rightarrow \exists\ \alpha \in [1;2]/\ f(\alpha) = 0$$

Podemos asegurar que α es la única raíz en el intervalo [1; 2]. Pues analizando el crecimiento de la función mediante su derivada:

$$f'(t) = 3.(t-1).(t+1)$$

	$(-\infty;-1)$	-1	$(-1;1)$	1	$(1;+\infty)$
f'	+		-		+
f	↗		↘		↗

Así α resulta ser algebraico sobre $\mathbb{Q}$ pues $f(\alpha) = 0$.

Es evidente que el elemento α no es racional pues f no posee raíces racionales.

El polinomio *f* es irreducible sobre $\mathbb{Q}$ y anula a α, por lo tanto $f[t] \in \mathbb{Q}[t]$ es el polinomio minimal de α sobre $\mathbb{Q}$.

Así, por el teorema de *La extensión* $E(\alpha)$ *del cuerpo E,* $\mathbb{Q}(\alpha)$ es un cuerpo que extiende a $\mathbb{Q}$ y $[\mathbb{Q}(\alpha):\mathbb{Q}] = gr(f(t)) = 3$, donde claramente $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{R}$.

La construcción de $\mathbb{Q}(\alpha)$ aunque no la hicimos explícita, al ser α algebraico sobre $\mathbb{Q}$, está dada por:

[XI] No es necesario aproximar la raíz pues para el objetivo perseguido alcanza con confirmar su existencia.
[XII] Veremos al polinomio *f(t)* como una función *f:* $\mathbb{R} \to \mathbb{R}$.
[XIII] El *teorema de Bolzano* afirma que si una función es continua en un intervalo cerrado $[a;b]$ y en los extremos del mismo ésta toma valores con signos opuestos, entonces existe al menos una raíz de la función en el interior del intervalo.

$$\mathbb{Q}(\alpha) = \left\{ a_0 + a_1\alpha + a_2\alpha^2 : a_0, a_1, a_2 \in \mathbb{Q} \right\}$$

donde el grado del polinomio minimal de α sobre $\mathbb{Q}$ es 3.

Sabemos que $\alpha \in [1;\ 2]$ y por el método de la Bisección podríamos dar una estimación de la misma. También sabemos que α no es racional. Pero, ¿quién es α ?

Método de Kronecker

Apelaremos a un método que permite "fabricar" raíces de un polinomio $f \in K[t]$ con K cuerpo cuando f es irreducible sobre K., denominado Método de Kronecker.

Este método consiste en tomar congruencias módulo el polinomio f [XIV] y obtener el cuerpo $E = K[t]/\langle f(t) \rangle$ como el conjunto de clases de equivalencia. Esta construcción proporciona una raíz α de f en E, a saber $\alpha := [t]_f$.

Este cuerpo no contiene a K, pero sí una *"copia"* de K.

Sea el isomorfismo de cuerpos $\begin{array}{l} K \xrightarrow{\pi} E \\ a \longrightarrow [a]_f \end{array}$. $\mathrm{Im}\,\pi \subseteq E$ y resulta un subcuerpo isomorfo a K (la copia de K contenida en E).

Así E es una extensión de K, donde $[E:K] = gr(f(t))$ y f tiene una raíz en E.

Apliquémoslo al caso en cuestión.

Tenemos $f(t) = t^3 - 3t + 1 \in \mathbb{Q}[t]$ irreducible en $\mathbb{Q}$.

Sean $a(t)$ y $b(t)$ dos polinomios pertenecientes a $\mathbb{Q}[t]$, sabemos que:

[XIV] La extensión de la noción de clases de congruencia de números a polinomios figura en el anexo.

$$a(t) \equiv b(t)_{\text{mód}\,(f(t))} \Leftrightarrow f(t)/a(t)-b(t)$$

obteniendo el conjunto de clases de equivalencia de polinomios en $\mathbb{Q}[t]$ módulo el polinomio *f(t)* : $\mathbb{Q}[t]/\langle f(t)\rangle$.

Veamos que si *f(t)* es irreducible en $\mathbb{Q}[t]$, entonces $\mathbb{Q}[t]/\langle f(t)\rangle$ resulta un cuerpo.

Sea $[a(t)] \neq 0$ queremos ver que posee inverso multiplicativo en $\mathbb{Q}[t]/\langle f(t)\rangle$.

Si $[a(t)]$ es un polinomio en $\mathbb{Q}[t]$ con $gr(a(t)) < gr(f(t))$, sabemos que $(a(t); f(t)) = d(t)$ donde $gr(d(t)) > 0$.

Entonces $d(t)/f(t)$, con lo que $f(t) = d(t).q(t)$, $q(t) \in \mathbb{Q}[t]$. Pero como *f* es irreducible y mónico, sigue que $q(t) = 1$, resultando $f(t) = d(t)$. Por lo tanto $(a(t); f(t)) = 1$ *ó* $f(t)$.

Pero al ser $[a(t)] \neq [0]$, $f(t)$ no divide a $a(t)$, entonces $(a(t); f(t)) = 1$.

Esto nos permite asegurar que existen $r, s \in \mathbb{Q}[t]/\ a(t).r(t) + f(t).s(t) = 1$. Y pensados según la congruencia módulo *f(t)*, queda: $[1] = [a(t)][r(t)]$

$\therefore$ $[a(t)]$ es unidad en $\mathbb{Q}[t]/\langle f(t)\rangle$.

Entonces podemos afirmar que todo polinomio no nulo de grado menor al grado de *f(t)* es coprimo con *f(t)*. Y así toda clase de congruencia distinta de 0 en $\mathbb{Q}[t]/\langle f(t)\rangle$ posee inverso.

Entonces, definimos a los elementos de $\mathbb{Q}[t]/\langle f(t)\rangle = \left\{ [g(t)]_{f(t)} : g \in \mathbb{Q}[t] \right\}$

Sea $g(t) \in \mathbb{Q}[t]$ y dividiendo por $f(t) = t^3 - 3t + 1$, tenemos

$g(t) = f(t).q(t) + r(t)$ donde $gr(r(t)) < 3$ y *r* es único, por lo tanto $[g(t)]_{f(t)} = [r(t)]_{f(t)}$.

Como *r* es único, toda clase de congruencia módulo *f(t)* está representada por un único polinomio *r(t)* de grado menor a 3.

$$\mathbb{Q}[t]/\left\langle t^3-3t+1\right\rangle=\left\{\left[a+bt+ct^2\right]: a,b,c\in\mathbb{Q}\right\}$$

Entonces confirmamos que $\left(\mathbb{Q}[t]/\left\langle t^3-3t+1\right\rangle;+;\cdot\right)$ posee estructura de cuerpo.

En el que las operaciones de suma y multiplicación se definen del modo siguiente

$$\begin{cases}[r_1]+[r_2]=[r_1+r_2]\\ \\ [r_1]\cdot[r_2]=[r_1\cdot r_2]\end{cases}$$

Vemos también que $\mathbb{Q}[t]/\left\langle t^3-3t+1\right\rangle$ es un $\mathbb{Q}$*-espacio vectorial.*

En donde para todo $\lambda\in\mathbb{Q}$ se verifica que $\lambda\cdot\left[a+bt+ct^2\right]=\left[\lambda a+\lambda bt+\lambda ct^2\right]$

La dimensión de $\mathbb{Q}[t]/\left\langle t^3-3t+1\right\rangle$ como $\mathbb{Q}$-espacio vectorial es 3 y la base es

$B=\left\{[1]\,;\,[t];\,[t]^2\right\}$ pues para que conformen un sistema linealmente independiente deberíamos verificar que si $\alpha[1]+\beta[t]+\gamma[t]^2=0$, entonces $\alpha=\beta=\gamma=0$.

Veamos que $\alpha[1]+\beta[t]+\gamma[t]^2=\left[\alpha 1+\beta t+\gamma t^2\right]=0$

$$\Rightarrow \alpha+\beta t+\gamma t^2\equiv 0_{\text{mód }(t^3-3t+1)}\Rightarrow \alpha+\beta t+\gamma t^2=\left(t^3-3t+1\right).q(t)$$

$$\Rightarrow \underbrace{\left(t^3-3t+1\right)}_{gr\,3}/\underbrace{\left(\alpha+\beta t+\gamma t^2\right)}_{gr\,2}\Rightarrow \alpha+\beta t+\gamma t^2=0\Rightarrow \alpha=\beta=\gamma=0$$

Por lo tanto $[1];[t];[t]^2$ generan a todo elemento perteneciente a $\mathbb{Q}[t]/\left\langle t^3-3t+1\right\rangle$.

Sea $\left[a+bt+ct^2\right]\in\mathbb{Q}[t]/\left\langle t^3-3t+1\right\rangle\Rightarrow\left[a+bt+ct^2\right]=[a]+[b][t]+[c]\left[t^2\right]=a+b[t]+c[t]^2$

Usaremos las operaciones algebraicas en $\mathbb{Q}[t]/\langle t^3-3t+1\rangle$ para simplificar la descripción de los elementos de $\mathbb{Q}[t]/\langle t^3-3t+1\rangle$.

Sea $g(t)=a+bt+ct^2$, con $a,b,c\in\mathbb{Q}$, definimos a la clase de *g(t)* del siguiente modo:

$[g(t)]=[a+bt+ct^2]=[a]+[b][t]+[c][t]^2$ por la definición de suma y producto de las clases de congruencia.

Sea $\pi:\mathbb{Q}\longrightarrow\mathbb{Q}[t]/\langle t^3-3t+1\rangle$ morfismo de cuerpos, donde $a\longrightarrow[a]$

Vemos que:

$$*\begin{cases}\pi(a+b)=\pi(a)+\pi(b)\\ \pi(a.b)=\pi(a).\pi(b)\\ \pi(1)=1\end{cases}$$

* π es inyectiva

Supongamos que $\pi(a_1)=\pi(a_2)\Rightarrow[a_1]=[a_2]\Rightarrow a_1\equiv a_2 \ \ _{mód\ (t^3-3t+1)}\Rightarrow a_1-a_2\equiv 0_{mód\ (t^3-3t+1)}$

$$\Rightarrow\underbrace{(t^3-3t+1)}_{gr\,3}/\underbrace{(a_1-a_2)}_{gr\,0}\Rightarrow a_1-a_2=0\Rightarrow a_1=a_2$$

* π es sobreyectiva

$\operatorname{Im}\pi\subseteq\mathbb{Q}[t]/\langle t^3-3t+1\rangle$ y resulta ser un cuerpo isomorfo a $\mathbb{Q}$.

$\pi:\mathbb{Q}\longrightarrow\operatorname{Im}\pi\subseteq\mathbb{Q}[t]/\langle t^3-3t+1\rangle$ es un morfismo de cuerpos biyectivo

Por lo tanto $\mathbb{Q}\cong\operatorname{Im}\pi$.

Entonces identificamos $\mathbb{Q}$ con su imagen en $\mathbb{Q}[t]/\langle t^3-3t+1\rangle$ mediante el morfismo π y $a\in\mathbb{Q}$ lo identificamos con $[a]_{f(t)}$.

Bajo esta identificación, un elemento de $\mathbb{Q}[t]/\langle t^3-3t+1\rangle$ es

$$[g(t)] = [a + bt + ct^2] = [a] + [b][t] + [c][t^2] = a + b[t] + c[t]^2 \quad \text{con} \quad a,b,c \in \mathbb{Q}$$

Ahora bien, definiendo $\alpha := [t]_{f(t)}$, vemos que $[g(t)] = g([t]) = g(\alpha)$ la clase de congruencia de un polinomio *g(t),* es *g(t)* evaluado en α .

Tomamos el cuerpo $\mathbb{Q}[t]/\langle t^3 - 3t + 1\rangle$ y lo identificamos con $\{a + b\alpha + c\alpha^2 : a;b,c \in \mathbb{Q}\}$ que resulta cuerpo pues $f(t) = t^3 - 3t + 1$ es irreducible sobre $\mathbb{Q}$.

Entonces $\mathbb{Q}[t]/\langle t^3 - 3t + 1\rangle$ es una extensión de $\mathbb{Q}$ cuyo grado es $3 = gr(t^3 - 3t + 1)$ y $\alpha = [t]_{f(t)}$ es raíz en $\mathbb{Q}[t]/\langle t^3 - 3t + 1\rangle$ del polinomio $f(t) = t^3 - 3t + 1$ en $\mathbb{Q}[t]$.

$$0 = [f(t)] = f([t]) = f(\alpha)$$

El método de Kronecker nos permite obtener una raíz del polinomio sin saber el valor de la misma.

Teorema del polinomio minimal

Sean E y K cuerpos tales que $K \subset E$ *y* $\alpha \in E$.

Sea $\varphi_\alpha : K[t] \to E$ *el morfismo de anillos "evaluación en* α *" definido por*

$\varphi_\alpha\left(p(t)\right) = p(\alpha)$.

Supongamos que φ_α *no es inyectivo, o sea que existe* $p(t) \in K[t],\ gr\left(p(t)\right) = d \geq 1$ *tal que*

$\varphi_\alpha\left(p(t)\right) = p(\alpha) = 0$.

Entonces

(i) existe un polinomio mónico m(t) de grado mínimo d >0 en $K[t]$ *tal que*

$\varphi_\alpha\left(m(t)\right) = m(\alpha) = 0$ *(anula a* α *).*

(ii) m(t) es irreducible en K[t].

(iii) $Nu\ \varphi_\alpha = \left\langle m(t) \right\rangle$ [XV]

Si $\alpha \in E$ algebraico sobre *K*, entonces el único polinomio mónico *m(t)* con $m(\alpha) = 0$ se denomina polinomio minimal de α sobre *K*.

Demostración.

$Nu\ \varphi_\alpha = \left\{p(t) \in K[t] : \varphi_\alpha\left(p(t)\right) = 0\right\} = \left\{p(t) \in K[t] : p(\alpha) = 0\right\}$

[XV] Denotamos $Nu\ \varphi_\alpha$ al núcleo del morfismo. El *núcleo* o *kernel de un morfismo* de un anillo *R* en un anillo *R'* es el conjunto de todos los elementos de *R* que van a dar a la identidad 0' de *R'* bajo φ_α .

Si $Nu\,\varphi_\alpha$ contiene un polinomio no nulo, entonces $Nu\,\varphi_\alpha$ contiene un polinomio *m(t)* de grado mínimo *d* >0, por el principio de buena ordenación en el *gr*.

Si $m(t) \in Nu\,\varphi_\alpha$, cualquier asociado a *m(t)* (cualquier polinomio que resulte un múltiplo de *m(t)*) pertenece a $Nu\,\varphi_\alpha$. Entonces podemos asumir que *m(t)* es un polinomio mónico de grado mínimo en $Nu\,\varphi_\alpha$.

Probemos primero *(iii)*

Es evidente que $\langle m(t)\rangle \subseteq Nu\,\varphi_\alpha$

Veamos que $Nu\varphi_\alpha \subseteq \langle m(t)\rangle$.

Supongamos que $f(t)$ es un polinomio perteneciente a $Nu\varphi_\alpha$. Si dividimos *f(t)* por *m(t)*:

$f(t) = m(t).q(t) + r(t)$ con $0 \le gr(r(t)) < gr(m(t))$. Aplicando φ_α a esta ecuación, queda:

$\underset{=0}{f(\alpha)} = \underset{=0}{m(\alpha)}.q(\alpha) + r(\alpha)$, por lo tanto $r(\alpha) = 0$.

Si $r(t) \neq 0$, se tiene que *r(t)* es un polinomio de grado menor que *m(t)* que anula a α, lo que contradice la minimalidad de *m(t)*. Entonces $r(t) = 0$, y así $f(t) = m(t)q(t)$.

$\therefore Nu\,\varphi_\alpha = \langle m(t)\rangle$

Para comprobar *(i)* veremos que *m(t)* es único.

Supongamos que *q(t)* es también un polinomio de grado mínimo en $Nu\,\varphi_\alpha$, entonces, como *m(t)* debe dividir a *q(t)*, éstos deben ser asociados, y como son mónicos resulta $m(t) = q(t)$.

(ii) Por último veamos que *m(t)* es irreducible en $K[t]$.

Sabemos que *m(t)* es el polinomio mónico de grado mínimo en $Nu\,\varphi_\alpha$.

Supongamos que *m(t)* es reducible, así resultaría:

$$m(t) = f(t).g(t) \quad \text{con} \quad \begin{array}{l} 1 \leq gr\left(f(t)\right) < gr\left(m(t)\right) \\ 1 \leq gr\left(g(t)\right) < gr\left(m(t)\right) \end{array}$$

Luego, aplicando φ_α a la factorización de *m(t)* se obtiene:

$m(\alpha) = f(\alpha).q(\alpha)$. Como ésta es una ecuación en *E*, un cuerpo, no tiene divisores de cero, por lo tanto $f(\alpha) = 0 \text{ ó } g(\alpha) = 0$.

Entonces $f(t) \in Nu\varphi_\alpha \text{ ó } g(t) \in Nu\varphi_\alpha$ y $\begin{array}{l} gr\left(f(t)\right) < gr\left(m(t)\right) \\ gr\left(g(t)\right) < gr\left(m(t)\right) \end{array}$. Lo que es un absurdo, pues *m(t)* es el polinomio de grado mínimo que anula a α

$\therefore m(t)$ es el polinomio irreducible en *K[t]*.

Capítulo 3: *Comparación entre* $\mathbb{Q}(\alpha)$ *y* $\mathbb{Q}[t]/\langle f(t)\rangle$

Hasta aquí hemos visto cómo extender un cuerpo conociendo una de sus raíces, y también, cómo hacerlo en el caso de desconocerla.

Surge entonces una ambigüedad entre las dos posibles construcciones de $\mathbb{Q}(\alpha)$: conociendo una de las raíces de un polinomio, se puede extender el cuerpo en el que está definido de forma directa (tal como se explica en el primer capítulo), pero también se lo puede extender aplicando el método de Kronecker, puesto que el mismo se puede aplicar a cualquier polinomio irreducible en un cuerpo dado.

¿Cuál es la relación, entonces, entre estas dos posibles construcciones?

El problema es de definición.

Pero veremos que no hay en realidad problema, pues son isomorfos.

Demostrémoslo con un caso concreto. Retomemos el polinomio trabajado en el primer capítulo: $f(t) = t^3 - 3 \in \mathbb{Q}[t]$

Por un lado $\sqrt[3]{3} \in \mathbb{Q}\left(\sqrt[3]{3}\right)$ es raíz de *f* donde $\mathbb{Q}\left(\sqrt[3]{3}\right) = \left\{ a + b\sqrt[3]{3} + c\left(\sqrt[3]{3}\right)^2 : a;b,c \in \mathbb{Q} \right\}$ cuerpo.

Por el otro, por Kronecker $[t]_{f(t)}$ es raíz de *f* y $[t]_{f(t)} \in \mathbb{Q}[t]/\left\langle t^3 - 3\right\rangle = \left\{ [g(t)]_{f(t)} : g \in \mathbb{Q}[t] \right\}$ cuerpo.

Tenemos dos cuerpo distintos sobre los cuales *f* tiene una raíz.

Resultan ser isomorfos.

Consideremos la función $\psi : \mathbb{Q}[t]/\langle t^3-3\rangle \longrightarrow \mathbb{Q}\left(\sqrt[3]{3}\right)$ donde $\psi([g(t)]) = g\left(\sqrt[3]{3}\right)$

*Veamos que está bien definida

Sea $[g(t)] \in \mathbb{Q}[t]/\langle t^3-3\rangle \Rightarrow g(t) \in \mathbb{Q}[t]$ y $g(t) \equiv p(t)_{\text{mód } (t^3-3)}$

$\Rightarrow t^3-3 / g(t)-p(t) \Rightarrow g(t)-p(t) = q(t).(t^3-3) \Rightarrow g(t) = q(t).(t^3-3)+p(t)$ donde el $gr(p(t)) < 3$, o sea $p(t) = a+bt+ct^2$ con $a,b,c \in \mathbb{Q}$

$\Rightarrow g\left(\sqrt[3]{3}\right) = p\left(\sqrt[3]{3}\right) = \underbrace{a+b\sqrt[3]{3}+c\sqrt[3]{9}}_{\in Q\left(\sqrt[3]{3}\right)}$ con $a,b,c \in \mathbb{Q}$.

Sea $[g_1(t)] = [g_2(t)]$ en $\mathbb{Q}[t]/\langle t^3-3\rangle \Rightarrow \psi([g_1(t)]) = \psi([g_2(t)])$

Como $[g_1(t)] = [g_2(t)] \Rightarrow g_1(t)-g_2(t) \equiv 0_{\text{mód } (t^3-3)} \Rightarrow t^3-3 / g_1(t)-g_2(t)$

$\Rightarrow g_1(t)-g_2(t) = (t^3-3).q(t)$ con $q(t) \in \mathbb{Q}[t]$

$\Rightarrow g_1\left(\sqrt[3]{3}\right) = g_2\left(\sqrt[3]{3}\right) \Rightarrow \psi([g_1(t)]) = \psi([g_2(t)])$

* Veamos que ψ es morfismo de cuerpos

- $\psi([1]) = 1$
- $\psi([g_1]+[g_2]) = \psi([g_1+g_2]) = (g_1+g_2)_{\left(\sqrt[3]{3}\right)} = g_{1\left(\sqrt[3]{3}\right)} + g_{2\left(\sqrt[3]{3}\right)} = \psi([g_1])+\psi([g_2])$
- $\psi([g_1]\cdot[g_2]) = \psi([g_1\cdot g_2]) = (g_1\cdot g_2)_{\left(\sqrt[3]{3}\right)} = g_{1\left(\sqrt[3]{3}\right)} \cdot g_{2\left(\sqrt[3]{3}\right)} = \psi([g_1])\cdot\psi([g_2])$

* Veamos que ψ es inyectiva

Debemos ver que si $\psi([g_1]) = \psi([g_2])$, entonces $g_1(t) = g_2(t)$.

Sabemos que $\psi([g_1]) = \psi([g_2])$ implica que $g_1\left(\sqrt[3]{3}\right) = g_2\left(\sqrt[3]{3}\right)$

Dividimos g_1 por $t^3 - 3 \Rightarrow g_1(t) = (t^3 - 3).q_1(t) + r_1(t) \qquad 0 \leq gr\left(r_1(t)\right) < 3$

Dividimos g_2 por $t^3 - 3 \Rightarrow g_2(t) = (t^3 - 3).q_2(t) + r_2(t) \qquad 0 \leq gr\left(r_2(t)\right) < 3$

Así, queda $g_1\left(\sqrt[3]{3}\right) = r_1\left(\sqrt[3]{3}\right) = a_1\left(\sqrt[3]{3}\right)^2 + a_2\sqrt[3]{3} + a_3$ y

$$g_2\left(\sqrt[3]{3}\right) = r_2\left(\sqrt[3]{3}\right) = b_1\left(\sqrt[3]{3}\right)^2 + b_2\sqrt[3]{3} + b_3$$

Sabemos que $\left\{1; \sqrt[3]{3}; \left(\sqrt[3]{3}\right)^2\right\}$ es base de $\mathbb{Q}\left(\sqrt[3]{3}\right)$ como $\mathbb{Q}$-*espacio vectorial*, y como

$g_1\left(\sqrt[3]{3}\right) = g_2\left(\sqrt[3]{3}\right)$, tenemos : $(a_1 - b_1)\left(\sqrt[3]{3}\right)^2 + (a_2 - b_2)\sqrt[3]{3} + (a_3 - b_3) = 0$

Por lo tanto: $\begin{cases} a_1 = b_1 \\ a_2 = b_2 \\ a_3 = b_3 \end{cases}$

Así, $\begin{matrix} g_1(t) = (t^3 - 3)\, q_1(t) + r(t) \\ g_2(t) = (t^3 - 3)\, q_2(t) + r(t) \end{matrix}$ con lo cual $[g_1(t)] = [r(t)] = [g_2(t)]$

Entonces ψ es monomorfismo

*Veamos que ψ es epimorfismo

Sea $a = a_1 + a_a\sqrt[3]{3} + a_3\left(\sqrt[3]{3}\right)^2 \in \mathbb{Q}\left(\sqrt[3]{3}3\right)$ con $a_1, a_2, a_3 \in \mathbb{Q}$, sabemos que existe un polinomio en $\mathbb{Q}[t]$ asociado a dicho elemento, tal que $a = \psi\left(\left[a_1 + a_2 t + a_3 t^2\right]\right)$

$\therefore\ \mathbb{Q}[t]/\left\langle t^3 - 3\right\rangle \cong \mathbb{Q}\left(\sqrt[3]{3}\right)$, es decir, ambas construcciones son isomorfas.

Teorema del isomorfismo

Sean E y K cuerpos tales que $K \subset E$ *y* $\alpha \neq 0$. $\alpha \in E$ *es algebraico sobre K.*

Sea m(t) el polinomio minimal de α *sobre K de grado n.*

Consideremos al cuerpo $K(\alpha)$ *que contiene a K definido por*

$$K(\alpha) = \left\{ a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} : a_1 \in K \right\}$$

Sea $\varphi_\alpha : K[t] \to K(\alpha)$ *el morfismo de anillos sobreyectivo "evaluación en* α *" definido por*

$\varphi_\alpha\left(p(t)\right) = p(\alpha)$

Entonces φ_α *induce un isomorfismo (de cuerpos)* $\overline{\varphi_\alpha} : K[t]/\langle m(t)\rangle \longrightarrow K(\alpha)$.

Con lo que resulta $K[t]/\langle m(t)\rangle \cong K(\alpha)$.

Demostración.

El morfismo $\varphi_\alpha : K[t] \to K(\alpha)$ en el que $\varphi_\alpha\left(p(t)\right) = p(\alpha)$ está bien definido pues

$p(t) = m(t).q(t) + r(t)$ con $gr\left(r(t)\right) < gr\left(m(t)\right)$, y evaluado en α :

$p(\alpha) = r(\alpha) = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \in K(\alpha)$

$$\begin{array}{ccc} K[t] & \xrightarrow{\varphi_\alpha} & K(\alpha) \\ \downarrow{\scriptstyle \pi_\alpha} & \square & \\ K[t]/\langle m(t)\rangle & & \end{array} \qquad \overline{\varphi_\alpha}\left([p(t)]\right) = \varphi_\alpha\left(p(t)\right) = p(\alpha)$$

* Buena definición de $\overline{\varphi_\alpha}$.

Si $[p(t)] = [g(t)]$ en $K[t]/\langle m(t)\rangle$ debemos comprobar que $\overline{\varphi_\alpha}\left([p(t)]\right) = \overline{\varphi_\alpha}\left([g(t)]\right)$

($\overline{\varphi_\alpha}$ en una clase de equivalencia no depende del representante elegido)

Como $[p(t)]=[g(t)] \Rightarrow p(t)-g(t) \equiv 0_{\text{mód } (m(t))}$, sigue que $p(t)=g(t)+m(t).s(t)$ para algún $s(t) \in K[t]$.

Evaluando en α : $p(\alpha)=g(\alpha)+\underbrace{m(\alpha)}_{=0}.s(\alpha)$, o sea $p(\alpha)=g(\alpha)$. Por lo tanto

$\overline{\varphi_\alpha}([p(t)])=\overline{\varphi_\alpha}([g(t)])$

* $\overline{\varphi_\alpha}$ es morfismo de anillos

$\overline{\varphi_\alpha}([p(t)]+[g(t)])=\overline{\varphi_\alpha}([p(t)+g(t)])=\varphi_\alpha(p(t)+g(t))=\varphi_\alpha(p(t))+\varphi_\alpha(g(t))=$

$=\overline{\varphi_\alpha}([p(t)])+\overline{\varphi_\alpha}([g(t)])$

$\overline{\varphi_\alpha}([p(t)]\cdot[g(t)])=\overline{\varphi_\alpha}([p(t)\cdot g(t)])=\varphi_\alpha(p(t)\cdot g(t))=\varphi_\alpha(p(t))\cdot\varphi_\alpha(g(t))=$

$=\overline{\varphi_\alpha}([p(t)])\cdot\overline{\varphi_\alpha}([g(t)])$

$\overline{\varphi_\alpha}([1])=\varphi_\alpha(1)=1$

* $\overline{\varphi_\alpha}$ es inyectiva

Sea $[f(t)] \in Nu\,\overline{\varphi_\alpha}$ debemos ver que $\overline{\varphi_\alpha}([f(t)])=0$, es decir, que $f(\alpha)=0$.

Si $f(t) \in Nu\varphi_\alpha=\langle m(t)\rangle$, entonces $f(t)=m(t).q(t)$ para algún $q(t) \in K[t]$. Por lo tanto $[f(t)]=[0]$, y así $f(\alpha)=0$.

* $\overline{\varphi_\alpha}$ es sobreyectiva

Sea $a \in K(\alpha)$, se puede expresar de la forma $a=a_0+a_1\alpha+...+a_{n-1}\alpha^{n-1}$ con $a_i \in K$.

Consideremos $f(t) = a_0 + a_1 t + ... + a_{n-1} t^{n-1}$ con $a_i \in K$.

Así, $\varphi_\alpha\left(f(t)\right) = a$ y $\varphi_\alpha\left(f(t)\right) = \overline{\varphi_\alpha}\left(\left[f(t)\right]\right)$.

Con lo que podemos asegurar que existe $\left[f(t)\right] \in K[t]/\left\langle m(t)\right\rangle$ tal que $\overline{\varphi_\alpha}\left(\left[f(t)\right]\right) = a$ -

Capítulo 4: *Cuerpo de descomposición*

Hasta aquí hemos resuelto el problema de determinar el menor cuerpo que contenga una raíz de un polinomio irreducible.

Sea $f(t) \in \mathbb{Q}[t]$ irreducible en $\mathbb{Q}$, somos capaces de construir la menor extensión de $\mathbb{Q}$ en la que *f(t)* posea una raíz (siendo la raíz, conocida o desconocida). Es decir, hallamos una extensión del cuerpo $\mathbb{Q}$ donde *f(t)* posee un factor lineal.

El objetivo de este capítulo es avanzar aún un poco más. Ahora queremos encontrar una extensión finita[XVI] *E* de $\mathbb{Q}$ que contenga todas las raíces de *f;* a esta extensión se la denomina *cuerpo de descomposición*. En otras palabras, buscamos el cuerpo en donde *f* se descomponga como producto de polinomios de grado 1.

Una solución trivial es tomar al cuerpo de los números complejos como cuerpo de descomposición de cualquier polinomio irreducible en $\mathbb{Q}$.

Pero el cuerpo de descomposición entraña una idea de minimalidad: entre todos los cuerpos que contienen las raíces de $f(t) \in \mathbb{Q}[t]$, el cuerpo de descomposición *E* es la menor extensión de $\mathbb{Q}$. (Lo de menor puede ser entendido en el sentido de que si *F* es cualquier otro cuerpo que contiene a todas las raíces de *f*, entonces $E \subset F$).

Entonces, definimos formalmente: *la extensión de cuerpo K de F se denomina cuerpo de descomposición del polinomio* $f(t) \in F[t]$ *si f(x) se descompone completamente en factores*

[XVI] Extensión finita: Diremos que una extensión de cuerpos k $\subset$ K es finitamente generada si existe un subconjunto finito S $\subset$ K tal que K = k(S)

lineales en $K[t]$ *y f(t) no se descompone completamente en factores lineales en ningún otro subcuerpo propio*[XVII] *de K conteniendo a F.*

De este modo, nos encontramos en la siguiente situación: dado un polinomio $f(t) \in \mathbb{Q}[t]$, para encontrar el cuerpo de descomposición *E*, tenemos que encontrar las raíces de *f*, o sea, factorizar el polinomio. Como sabemos, podemos tener una lista de 800 casos de factoreo, y siempre puede aparecer un nuevo polinomio sobre el cual ninguno de los 800 casos puede aplicarse, no podemos decir nada, ni siquiera encontrar una raíz.

Sin embargo, a pesar de estas limitaciones, debemos recordar que disponemos de una idea matemática muy importante (un resultado de Kronecker) que nos permite "fabricar" raíces de un polinomio $f(t) \in \mathbb{Q}[t]$ cuando este es irreducible sobre $\mathbb{Q}$: tomamos congruencias módulo *f* y obtenemos el cuerpo $E := \mathbb{Q}[t] / \langle f(t) \rangle$ como el conjunto de las clases de equivalencia. Esta construcción nos proporciona una raíz α de *f* en *E*, a saber, $\alpha := [t]_{f(t)}$. Además, si bien este cuerpo *E* no contiene a $\mathbb{Q}$, sí contiene una "copia" de $\mathbb{Q}$. En términos más formales, por medio del siguiente morfismo de cuerpos

$$\begin{aligned} \mathbb{Q} &\longrightarrow \mathbb{Q}[t] / \langle f(t) \rangle \\ a &\longrightarrow [a]_{f(t)} \end{aligned}$$

la imagen de $\mathbb{Q}$ está contenida en *E* y resulta un subcuerpo isomorfo a $\mathbb{Q}$. Así *E* es una extensión de $\mathbb{Q}$ de grado igual al grado de *f* y en $\mathbb{Q}[t]$ tenemos que *f* se factoriza en la forma

$f(t) = (t - \alpha) g(t)$ con $g \in \mathbb{Q}[t]$ de grado *n-1*.

¿Qué ocurre con las restantes raíces de *f*, o sea las del polinomio *g*?

[XVII] Subcuerpo propio. Si *F* y *K* son dos cuerpos bajo las mismas operaciones, y $K \subset F$, decimos que *K* es un subcuerpo propio de *F* si $K \neq F$.

Queda expuesto que tenemos una forma de encarar la tarea. Si podemos calcular fácilmente las raíces del polinomio, no hay casi nada que hacer, el cuerpo de descomposición se obtiene de la forma $E = \mathbb{Q}(\alpha_1,...,\alpha_s)$ donde α_i representa las raíces de *f*. La tarea es luego, calcular el grado de la extensión de $E/\mathbb{Q}$. En cambio, si no podemos calcular ninguna raíz en forma, digamos, sencilla, debemos descomponer *f* en factores irreducibles sobre $\mathbb{Q}$ y aplicar el resultado de Kronecker a cada uno de los factores[XVIII].

Ejemplos de cuerpos de descomposición

Con intenciones de aclarar lo expuesto daremos distintos ejemplos:

(1) El polinomio $t^2 - 5t + 6$ se factoriza en $\mathbb{Q}[t]$ como $(t-2)(t-3)$, por lo tanto la extensión finita de $\mathbb{Q}$ que buscamos es el mismo cuerpo $\mathbb{Q}$.

Por otro lado, es claro que las raíces pertenecen, por ejemplo, a $\mathbb{Q}(\sqrt{2})$ ó a $\mathbb{Q}(\sqrt[3]{2})$, extensiones de $\mathbb{Q}$ de grado 2 y 3 respectivamente. Pero el cuerpo de descomposición es aquel en el que el polinomio se puede descomponer en factores lineales, y que no pueda hacerlo en ningún otro subcuerpo propio.

En conclusión, $\mathbb{Q}$ es el cuerpo de descomposición de *f(t)*.

(2) El cuerpo de descomposición de $f(t) = t^2 - 2$ sobre $\mathbb{Q}$ es simplemente $\mathbb{Q}(\sqrt{2})$, puesto que sus dos raíces son $\pm\sqrt{2}$ y $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

[XVIII] Y si no es posible, con nuestras herramientas, descomponer *f* en irreducibles en Q[t], bueno, pasaríamos a otro problema que escapa a esta investigación.

(3) El cuerpo de descomposición de $f(t) = (t^2 - 2)(t^2 - 3)$ es el cuerpo $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ [XIX] generado sobre $\mathbb{Q}$ por $\sqrt{2}$ y $\sqrt{3}$, ya que las raíces del polinomio son $\pm\sqrt{2}, \pm\sqrt{3}$.

Esta extensión es de grado 4 sobre $\mathbb{Q}$, el siguiente diagrama ilustra los subcuerpos que lo generan:

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

(4) El cuerpo de descomposición de $f(t) = t^3 - 2$ sobre $\mathbb{Q}$ no es $\mathbb{Q}(\sqrt[3]{2})$ pues, además de poseer a $\sqrt[3]{2}$ como raíz, posee otras dos raíces, a saber $\sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right)$ y $\sqrt[3]{2}\left(\frac{-1-i\sqrt{3}}{2}\right)$ que no pertenecen obviamente a $\mathbb{Q}(\sqrt[3]{2})$ debido a que los elementos de esta extensión son de la forma $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ con a, b, c racionales, es decir, sólo contiene números reales, y las últimas dos raíces no lo son.

Entonces el cuerpo de descomposición K de $f(t) = t^3 - 2$ se obtiene añadiendo las tres raíces al cuerpo $\mathbb{Q}$. Pero notemos que al agregar las primeras dos raíces obtenemos una ex-

[XIX] Denotamos $F(\alpha, \beta)$ al cuerpo generado sobre F por α y β: es el cuerpo generado por β sobre el cuerpo $F(\alpha)$ generado por α.

tensión K, que también contiene al cociente entre ellas[XX], es decir, contiene a $\left(\frac{-1-i\sqrt{3}}{2}\right)$.

Por consiguiente, contiene a $\sqrt{-3}$.

De otra manera, cualquier cuerpo que contenga a $\sqrt[3]{2}$ y $\sqrt{-3}$ contiene a las tres raíces del polinomio *f(t)*. Por lo tanto el cuerpo de descomposición de *f(t)* sobre $\mathbb{Q}$ es

$K = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{-3}\right)$, de dimensión 6.[XXI]

(5) Tomemos $t^4 + 4 \in \mathbb{Q}[t]$ que no tiene raíces racionales. Sin embargo, se factoriza sobre $\mathbb{Q}$ de la forma:

$$t^4 + 4 = t^4 + 4t^2 + 4 - 4t^2 = \left(t^2 + 2\right)^2 - 4t^2 = \left(t^2 + 2t + 2\right)\left(t^2 - 2t + 2\right)$$

Las raíces del primer factor son $-1 \pm i$ y las del segundo $1 \pm i$ así que el cuerpo de descomposición de este polinomio es $\mathbb{Q}(i)$, una extensión de $\mathbb{Q}$ de grado 2, donde sus elementos tienen la forma: $a + bi$; con a, b racionales.

Esto nos hace tomar cuenta que el grado de descomposición de un polinomio puede tener grado más bajo del imaginado.

[XX] Si α_1, α_2 son algebraicos sobre un cuerpo *K*, entonces el cociente entre α_1 *y* α_2 también es algebraico sobre *K*.

[XXI] El cálculo de la dimensión de extensiones de cuerpos generados por una cantidad finita de elementos algebraicos (*extensiones finitas*), excede de los objetivos de este trabajo.

Teorema del cuerpo de descomposición

Para cualquier cuerpo F, si $f(t) \in F[t]$*, existe una extensión K de F que es el cuerpo de descomposición para f(x).*

Demostración.

Demostraremos este teorema por inducción sobre *d*, el grado del polinomio *f(x)*.

Si $gr\left(f(t)\right) = 1$ el resultado es trivial.

Sea $gr\left(f(t)\right) = d,\ d > 1$.

En *F[t]*, supongamos que $f(t) = p_1(t) \cdot \ldots \cdot p_s(t)$ es el producto de polinomios irreducibles. Si el $gr\left(p_i(t)\right) = 1$ para todo $i = 1, \ldots, s$, luego el cuerpo *K* buscado es el mismo *F*.

Por lo contrario, reenumerando si es necesario, supongamos que $gr\left(p_1(t)\right) > 1$. Sea $L = F[y] / \langle p_1(t) \rangle$ y sea $\alpha := [y]_{p_1(y)}$. Luego *L* es un cuerpo que contiene a *F* (donde identificamos a *F* con las clases de congruencia de polinomios constantes en *L*), y α es una raíz de $p_1(t)$ en *L*. Entonces en *L[t]*, $p_1(t)$ se factorea como $p_1(t) = (t - \alpha) q_1(t)$. Así, en *L[t]*:

$f(t) = (t - \alpha) q_1(t) p_2(t) \cdot \ldots \cdot p_s(t)$

Llamando $g(t) = q_1(t) p_2(t) \cdot \ldots \cdot p_s(t)$ en *L[t]*, es evidente que $gr\left(g(t)\right) = gr\left(f(t)\right) - 1$.

Por inducción, existe un cuerpo *K* que contiene a *L* tal que en *K[t]*, el polinomio *g(t)* se descomponga como el producto de factores lineales. Pero también lo hace $f(t) = (t - \alpha) g(t)$.

Por lo tanto *K* contiene a *F*.

Así queda demostrado que todo polinomio en un cuerpo determinado posee una única extensión del cuerpo que es su cuerpo de descomposición.

Aplicación: *Racionalización*

Nos proponemos racionalizar la siguiente expresión:

$$\frac{3\sqrt[3]{3}}{1+2\sqrt[3]{3}-3\sqrt[3]{9}}$$

Por racionalizar se entiende transformar la expresión dada por una equivalente sin radicales en el denominador.

Estamos acostumbrados a racionalizar expresiones que involucren raíces cuadradas apelando a la noción de conjugado: si $\sqrt{d}$ no es "exacta" entonces se define el conjugado de $a+b\sqrt{d}$ como $a-b\sqrt{d}$. Aprendemos que el *conjugado* es la cantidad por la que hay que multiplicar y dividir para eliminar raíces cuadradas del denominador[XXII].

Pero veremos que la idea de conjugado no es tan clara como parece. Por ejemplo, si consideramos la expresión $\frac{3}{7-\sqrt{5}}$, verificamos que multiplicando y dividiendo por $-7-\sqrt{5}$ también se elimina la raíz del denominador. Es más, cualquier múltiplo racional tanto de $7+\sqrt{5}$ o de $-7-\sqrt{5}$ elimina $\sqrt{5}$ del denominador.

Esto nos lleva a cuestionar aquella idea que tenemos de *"el conjugado"*, pues si está vinculada a la eliminación de raíces en el denominador, entonces hay más conjugados de los que conocíamos: también se le puede cambiar el signo al término que no involucra la raíz cuadrada.

[XXII] Muchos textos de enseñanza media, tomando como punto de partida que $a^2-b^2=(a-b)(a+b)$ dan la siguiente definición: el conjugado de la expresión $a+b$ es $a-b$.

Ahora bien, es evidente que el método de multiplicar y dividir por el conjugado no proporciona una solución en el caso expuesto inicialmente.

En primer lugar, escribiendo $\alpha := \sqrt[3]{3}$ simplificamos la expresión:

$$\frac{3\sqrt[3]{3}}{1+2\sqrt[3]{3}-3\sqrt[3]{9}} = \frac{3\alpha}{1+2\alpha-3\alpha^2}$$

Vemos que α es raíz del polinomio $f(t) = t^3 - 3$ irreducible en $\mathbb{Q}[t]$. Entonces, por el teorema de la extensión $E(\alpha)$ de cualquier cuerpo E[XXIII], sabemos que $\mathbb{Q}(\alpha)$ resulta cuerpo y su grado es 3.

Con lo que podemos reducir el problema de racionalizar la expresión, al de encontrar un elemento de $\mathbb{Q}(\alpha)$, digamos $a + b\alpha + c\alpha^2$, de modo que

$$\left(1+2\alpha-3\alpha^2\right)\left(a+b\alpha+c\alpha^2\right) \qquad (1)$$

resulte racional. En otras palabras, queremos eliminar α.

Antes de continuar, deberíamos saber si el problema planteado inicialmente tiene sentido. Es decir, si el denominador $1+2\sqrt[3]{3}-3\sqrt[3]{9}$ es distinto de cero.

Como $\{1, \alpha, \alpha^2\}$ es base de $\mathbb{Q}(\alpha)$ como $\mathbb{Q}$-espacio vectorial, es evidente que $1+2\sqrt[3]{3}-3\sqrt[3]{9} = 1+2\alpha-3\alpha^2 \neq 0$ pues 1,2, -3 son distintos de cero.

Por lo tanto sabemos que el elemento $1+2\sqrt[3]{3}-3\sqrt[3]{9}$ es una unidad en $\mathbb{Q}(\alpha)$. Determinemos entonces su inverso, es decir, busquemos las coordenadas (en términos de *a, b, c*) en la base $\{1, \alpha, \alpha^2\}$ del elemento que se obtiene en (1).

[XXIII] Demostrado en el Capítulo 1 del presente trabajo.

$$\left(1+2\alpha-3\alpha^2\right)\left(a+b\alpha+c\alpha^2\right)=1$$

Aplicando la propiedad distributiva y reemplazando $\alpha^3=3$ y $\alpha^4=3\alpha$, queda

$$\left(a-9b+6c\right)+\left(2a+b-9c\right)\alpha+\left(-3a+2b+c\right)\alpha^2=1$$

obteniendo un sistema de ecuaciones lineales

$$\begin{cases} a-9b+6c=1 \\ 2a+b-9c=0 \\ -3a+2b+c=0 \end{cases}$$

Luego, por Gauss-Jordan

$$\begin{pmatrix} 1 & -9 & 6 & 1 \\ 2 & 1 & -9 & 0 \\ -3 & 2 & 1 & 0 \end{pmatrix} \square \begin{pmatrix} 1 & -9 & 6 & 1 \\ 0 & -19 & 21 & 2 \\ 0 & -25 & 19 & 3 \end{pmatrix} \square \begin{pmatrix} 1 & -9 & 6 & 1 \\ 0 & -19 & 21 & 2 \\ 0 & 0 & 164 & -7 \end{pmatrix}$$

llegamos a que:

$$a=-\frac{19}{164};\quad b=-\frac{25}{164};\quad c=-\frac{7}{164}$$

Con lo que $\left(1+2\alpha-3\alpha^2\right)\left(-\frac{19}{164}-\frac{25}{164}\alpha-\frac{7}{164}\alpha^2\right)=1$

Así

$$\frac{3\sqrt[3]{3}}{1+2\sqrt[3]{3}-3\sqrt[9]{9}}=\frac{3\alpha}{1+2\alpha-3\alpha^2}=\frac{3\alpha}{1+2\alpha-3\alpha^2}\cdot\frac{-\frac{1}{164}\left(19+25\alpha+7\alpha^2\right)}{-\frac{1}{164}\left(19+25\alpha+7\alpha^2\right)}=-\frac{1}{164}\left(57\alpha+75\alpha^2+21\alpha^3\right)$$

$$-\frac{1}{164}\left(57\alpha+75\alpha^2+63\right)=-\frac{63}{164}-\frac{57}{164}\alpha-\frac{63}{164}\alpha^2=-\frac{63}{164}-\frac{57}{164}\sqrt[3]{3}-\frac{63}{164}\sqrt[3]{9}$$

Podemos observar entonces que racionalizar, en realidad, consistió, por un lado, en mostrar que $1+2\alpha-3\alpha^2$ es un elemento no nulo de $\mathbb{Q}(\alpha)$ y, luego, en mostrar que dicho elemento es una unidad en $\mathbb{Q}(\alpha)$. Y esto último lo logramos, encontrando la expresión en coordenadas del inverso multiplicativo.

En suma, la racionalización no tiene demasiado valor despojado de las observaciones que hemos realizado. Podemos ser más directos: redujimos la cuestión a un problema de álgebra lineal. Y esto es lo relevante, es necesario tener presente que cualquier argumento con respecto a los elementos de $\mathbb{Q}(\alpha)$ involucra la estructura de $\mathbb{Q}$-espacio vectorial. Y a la vez, se pone en discusión la idea que tenemos con respecto a la noción de conjugado. Si aceptamos que el conjugado de una expresión es otra que multiplicando nos permite eliminar la raíz del denominador, entonces en este caso el conjugado de $1+2\alpha-3\alpha^2$ calculado más arriba no requirió cambiar ningún signo.

Conclusión

Claramente el objetivo del trabajo ha sido cumplido de forma satisfactoria.

Somos capaces entonces de, teniendo un cuerpo F cualquiera y un polinomio $p(t)$ perteneciente a $F[t]$ irreducible en dicho cuerpo, encontrar un cuerpo "más grande" que contenga a F en el cual la ecuación $p(t)=0$ tenga solución.

Hemos tratado dos tipos de casos: polinomios cuyas raíces podíamos determinar; y polinomios cuyas raíces nos eran desconocidas.

Se ha dejado en claro que el hecho de conocer, o no, al elemento que anula al polinomio, genera grandes diferencias en el proceso de construcción del cuerpo buscado.

Para el primer caso, la construcción del cuerpo es más concreta, más "palpable". Es sencillo determinar la estructura de los elementos del nuevo cuerpo, pues se apoya en el conocimiento de la raíz del polinomio. En cambio, la segunda construcción es más teórica. Para ella se supone el manejo de varios conceptos del álgebra. Justamente, la construcción de la raíz es básicamente algebraica, y por ende, también la del cuerpo.

De todas maneras hemos encontrado la forma de demostrar que estas construcciones, al parecer, diferentes, terminan siendo similares. En esto tuvo un papel principal el *Teorema del Isomorfismo,* pues permitió confirmar que ambas construcciones son isomorfas.

El cuarto capítulo lo tomamos como una especie de "yapa". Ya hemos dejado expuesto que el concepto de cuerpo de descomposición sobrepasa los límites de este trabajo, pero nos parecía de suma importancia dejar en claro simplemente su definición y algunos ejemplos senci-

llos. La intención es que su lectura confiera una humilde base para poder abordar uno de los diamantes más brillantes de la historia de la matemática: el *Gran Teorema de Galois*.

Para finalizar, nos pareció que el tema de racionalizar expresiones, aportó una mirada más concreta del tema, en la que la aplicación de lo trabajado nos ha proveído de una solución muy sencilla a un problema que a simple vista parecía ser complejo.

Bibliografía

- Dummit, David S.; Foote, Richard M. *ABSTRACT ALGEBRA.* Third Edition. United States of America. John Wiley & Sons Inc. 2004.

- Lidl, Rudolf; Niederreiter, Harald. *FINITE FIEDS – Encyclopedia of Mathematics and its applications, Volume 20*. Second Edition. United States of America. Edited by G, -C. Rota. 1997.

- Childs, Lindsay N. *A CONCRETE INTRODUCTION TO HIGHER ALGEBRA.* Third Edition. New York. Editorial Board. 2009.

- Gentile, Enzo R. *NOTAS DE ÁLGEBRA I.* Primera Edición. Buenos Aires. Eudeba. 1984.

- Krick, Teresa. *POLINOMIOS Y RAÍCES* [En línea]. Departamento de Matemática. Facultad de Ciencias Exactas y Naturales. UBA. <http://mate.dm.uba.ar/~krick/polrai.pdf > [Consulta: Octubre 2011]

- Rowland, Todd; Weisstein, Eric W. *EXTENSION FIELD*. *MathWorld*--A Wolfram Web Resource.< http://mathworld.wolfram.com/ExtensionField.html> [Consulta: Octubre 2011]

Índice

Introducción 1

Capítulo 1: El cuerpo $\mathbb{Q}(\alpha)$ 4

Definición del conjunto $\mathbb{Q}(\alpha)$ 5

$(\mathbb{Q}(\alpha);+;\cdot)$ anillo conmutativo 6

$\mathbb{Q}(\alpha)$ como $\mathbb{Q}$-espacio vectorial 7

$\mathbb{Q}(\alpha)$ cuerpo 10

Definiciones 12

Teorema de la extensión $E(\alpha)$ del cuerpo E 14

Capítulo 2: El cuerpo $\mathbb{Q}[t]/\langle f(t)\rangle$ 17

Método de Kronecker 19

Teorema del polinomio minimal 24

Capítulo 3: Comparación entre $\mathbb{Q}(\alpha)$ y $\mathbb{Q}[t]/\langle f(t)\rangle$ 27

Teorema del isomorfismo 30

Capítulo 4: Cuerpo de descomposición 33

Ejemplos de cuerpos de descomposición 35

Teorema del cuerpo de descomposición 38

Aplicación: Racionalización 39

Concusión 43

Bibliografía 45

Anexo