Capítulo 2

Cuerpos y sus extensiones

2.1. Definición de cuerpo

A lo largo de todo el curso trabajaremos primordialmente con raíces de polinomios, y en la próxima sección probaremos que las operaciones elementales (suma, resta, multiplicación y división) preservan el conjunto formado por ellas. Por ejemplo, podremos deducir que $(1+\sqrt{7})/(1-\sqrt[3]{5})$ es raíz de cierto polinomio en $\mathbb{Q}[x]$ porque 1, $\sqrt{7}$ y $\sqrt[3]{5}$ son raíces de polinomios en $\mathbb{Q}[x]$. Con esto en mente, procedemos como es habitual en Matemáticas, creando una estructura algebraica general que permita abstraer las propiedades esenciales.

Definición: Un *cuerpo*, K, es un anillo tal que $K-\{0\}$ es un grupo abeliano con respecto a la multiplicación.

En pocas palabras, un cuerpo es un conjunto donde podemos sumar, restar, multiplicar y dividir con las propieddes habituales. La exclusión del cero en la definición se debe simplemente a que como todo el mundo sabe, no se puede dividir por cero (bueno, todos menos K. Marx que en "El capital" I §9, después de enunciar una ley económica paradójica, escribe: "Para resolver esta contradicción aparente se requieren aún muchos eslabones intermedios, tal como en el plano del álgebra elemental se necesitan muchos términos medios para comprender que 0/0 puede representar una magnitud real").

Ejemplo. $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos.

Ejemplo. $K=\{a+b\sqrt{2}\ :\ a,b\in\mathbb{Q}\}$ es un cuerpo.
Lo único que no es del todo evidente es la existencia del inverso multiplicativo. Sólo hay que racionalizar:

$$\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}\in K.$$

Ejemplo. Dado un dominio de integridad, $\mathcal{D}$, (esto es, un anillo conmutativo con unidad tal que $ab=0\Rightarrow a=0$ ó $b=0$), el *cuerpo de fracciones* de $\mathcal{D}$ es el conjunto de expresiones de la forma r/s con $r,s\in\mathcal{D}$, $s\neq 0$, bajo la relación de equivalencia $r/s\sim t/u\Leftrightarrow ru=ts$. Con las operaciones naturales, el cuerpo de fracciones hace honor a su nombre y realmente tiene estructura de cuerpo.

Nótese que $\mathcal{D}$ se puede identificar con los elementos de la forma $r/1$. Intuitivamente, el cuerpo de fracciones de $\mathcal{D}$ es el cuerpo que resulta si permitimos dividir en $\mathcal{D}$. Por ejemplo, el cuerpo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$.

Si $\mathcal{D}$ no fuera dominio de integridad, por mucho que nos empeñásemos en dividir, no podríamos llegar a nada con sentido. Por ejemplo, si queremos inventar un "algo" en un cuerpo que extienda a $\mathbb{Z}_6$, tal que $2/3 = algo$, multiplicando por 9 tenemos $0 = 3{\cdot}$algo, con lo que "algo" no tendría inverso (en ese caso $0 = 3$). Las dificultades las dan los divisiores de cero, si no fuera por ellos, como en el cuento de Aladino, tendríamos un flamante cuerpo a partir de un anillo .

Si K es un cuerpo, $K[x]$ es un dominio de integridad y se puede definir su cuerpo de fracciones que se denota con $K(x)$.

$$K(x) = \Big\{ \frac{P}{Q} \ : \ P, Q \in K[x], \ Q \neq 0 \Big\}.$$

Como en el caso de $K[x]$, se suele abusar ligeramente de la notación permitiendo escribir $K(\alpha)$ con α en algún cuerpo que contiene a K, para representar

$$K(\alpha) = \Big\{ \frac{P(\alpha)}{Q(\alpha)} \ : \ P, Q \in K[x], \ Q(\alpha) \neq 0 \Big\}.$$

Desde otro punto de vista, $K(\alpha)$ es el resultado de añadir α a K y hacer todas las posibles sumas, restas, multiplicaciones y divisiones. Con este lenguaje el cuerpo del penúltimo ejemplo es $\mathbb{Q}(\sqrt{2})$. En general, razonando de la misma forma:

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \ : \ a, b \in \mathbb{Q}\}.$$

La notación admite una generalización obvia. Se indica con $K(x_1, x_2, \dots \ x_n)$ el cuerpo de fracciones de $K[x_1, x_2, \dots \ x_n]$, y si $\alpha_1, \alpha_2, \dots \ \alpha_n$ están en un cuerpo que contiene a K entonces se escribe $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ para representar:

$$\Big\{ \frac{P(\alpha_1, \alpha_2, \dots, \alpha_n)}{Q(\alpha_1, \alpha_2, \dots, \alpha_n)} \ : \ P, Q \in K[x_1, x_2, \dots, x_n], \ Q(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0 \Big\}.$$

Es fácil ver que $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ es el cuerpo "más pequeño" que contiene a K y a $\alpha_1, \alpha_2, \dots \ \alpha_n$. También es posible razonar definiendo inductivamente este cuerpo como $K(\alpha_1, \alpha_2, \dots, \alpha_n) = \big(K(\alpha_1, \alpha_2, \dots, \alpha_{n-1})\big)(\alpha_n)$.

Ejemplo. Si p es primo $\mathbb{Z}_p$ es un cuerpo.

Esto no es más que un caso particular de la Proposición 1.2.3 porque $\mathbb{Z}_p$ es por definición $\mathbb{Z}/p\mathbb{Z}$.

Observación: Cuando consideramos $\mathbb{Z}_p$ como cuerpo en vez de como anillo, la notación habitual, que utilizaremos a partir de ahora, es $\mathbb{F}_p$.

Estirando este ejemplo, podemos transformar la Proposición 1.2.3 en conjunción con la 1.3.2 en una fábrica de cuerpos muy retorcidos. Antes de ello, una observación.

Teorema 2.1.1 *Si K es un cuerpo, $K[x]$ es un dominio euclídeo.*

Demostración: La misma que en $\mathbb{Q}$. Basta tomar $N(P) = \partial P$. □

Ejemplo. Dado un cuerpo K y $P \in K[x] - \{0\}$ irreducible, $K[x]/(P)$ es un cuerpo.

Por la Proposición 1.3.2, (P) es maximal y basta aplicar la Proposición 1.2.3. De hecho la irreducibilidad de P es condición necesaria y suficiente para que el cociente sea cuerpo.

Los cocientes de anillos de polinomios serán especialmente importantes este curso, pero nada impediría crear cuerpos tomando cociente en otros anillos. Sólo para practicar veamos un ejemplo desarrollado en este sentido.

Ejemplo. Si $A \subset \mathbb{C}$ es el anillo $A = \left\{n+m\sqrt{-2} \ : \ n, m \in \mathbb{Z}\right\}$, entonces $A/\langle 1+\sqrt{-2}\rangle$ es un cuerpo de tres elementos.

Nótese primero que $\overline{n + m\sqrt{-2}} = \overline{n - m} + \overline{m(1 + \sqrt{-2})} = \overline{n - m}$, y por tanto basta considerar clases cuyos representantes sean números enteros. Por otra parte, $\overline{n} = \overline{n} + \overline{(1 - \sqrt{-2})(1 + \sqrt{-2})} = \overline{n - 3}$. Así pues $A/\langle 1+\sqrt{-2}\rangle = \left\{\overline{0}, \overline{1}, \overline{2}\right\}$ (es fácil comprobar que estas tres clases son distintas). Con ello demostramos que $A/\langle 1 + \sqrt{-2}\rangle$ es idéntico a $\mathbb{F}_3$ salvo cambiar nombres (isomorfo). En general, si un primo p es suma de un cuadrado y el doble de un cuadrado, digamos $p = n^2 + 2m^2$, se puede demostrar que $A/\langle n+m\sqrt{-2}\rangle$ es isomorfo a $\mathbb{F}_p$.

Nota: Las defininiciones de epimorfismo, monomorfismo e isomorfismo se pueden aplicar igualmente a cuerpos, porque un cuerpo es en particular un anillo con unidad.

Aunque la Proposiciones 1.2.3 y 1.3.2 nos juren por los axiomas de las Matemáticas que si P es irreducible $K[x]/\langle P\rangle$ es un cuerpo, no parece nada claro cómo hacer divisiones allí, concretamente cómo hallar el inverso. Para solucionar este problema basta recordar cómo se procede en $\mathbb{F}_p$. Si queremos hallar el inverso de $\overline{a}$, resolvemos la ecuación en enteros $1 = ax + py$, lo cual se podía hacer empleando el algoritmo de Euclides, y reduciendo módulo p se sigue $\overline{1} = \overline{a} \cdot \overline{x}$, esto es, $\overline{a}^{-1} = \overline{x}$. En $K[x]/\langle P\rangle$ todo funciona exactamente igual cambiando el primo p por el polinomio irreducible P.

Como eso del algoritmo de Euclides y la identidad de Bezout se pierde en los añejos abismos de Conjuntos y Números, no está de más ver un par de ejemplos que clarifiquen la situación.

Ejemplo. Hallar el inverso de $\overline{8}$ en $\mathbb{F}_{29}$.

Según lo indicado antes, debemos hallar una solución $n, m \in \mathbb{Z}$ de $1 = 29n + 8m$ y, al reducir módulo 29, se tiene que $\overline{m}$ es la clase que buscamos. Para hallar una solución $n, m \in \mathbb{Z}$ se aplica primero el algoritmo de Euclides a 29 y 8. Como son coprimos (condición necesaria y suficiente para que exista el inverso), al final se obtendrá un uno, que podemos despejar de abajo a arriba hasta conseguir la solución deseada:

$$\begin{array}{rcl} 29 = 8 \cdot 3 + 5 & & (4^{\text{a}} \text{ ecuación}) \ 1 = 3 - 2 \cdot 1 \\ 8 = 5 \cdot 1 + 3 & & (3^{\text{a}} \text{ ecuación}) \ 1 = 3 - (5 - 3 \cdot 1) \cdot 1 = 5 \cdot (-1) + 3 \cdot 2 \\ 5 = 3 \cdot 1 + 2 & \Rightarrow & (2^{\text{a}} \text{ ecuación}) \ 1 = 5 \cdot (-1) + (8 - 5 \cdot 1) \cdot 2 = 8 \cdot 2 + 5 \cdot (-3) \\ 3 = 2 \cdot 1 + 1 & & (1^{\text{a}} \text{ ecuación}) \ 1 = 8 \cdot 2 - (29 - 8 \cdot 3) \cdot 3 = 29 \cdot (-3) + 8 \cdot 11. \end{array}$$

Así pues podemos tomar $n = -3$ y $m = 11$ y se concluye que $\overline{11}$ es el inverso de $\overline{8}$. Para los incrédulos: $11 \cdot 8 = 88 = 1 + 3 \cdot 29$.

Ejemplo. Sean $P = x^4 + x^3 + x^2 + x + 1$ y $Q = x^2 + x + 1$. Calcular el inverso de $\overline{Q}$ en $\mathbb{Q}[x]/\langle P \rangle$.

Obsérvese que P es irreducible por ser el polinomio ciclotómico para $p = 5$. Buscamos una solución de $1 = AP + BQ$ para ciertos $A, B \in \mathbb{Q}[x]$, de donde $\overline{1} = \overline{BQ}$, y $\overline{B}$ será el inverso de $\overline{Q}$. Calculamos A y B procediendo como en el ejemplo anterior:

$$\begin{array}{l} P = Q \cdot x^2 + (x+1) \\ Q = (x+1) \cdot x + 1 \end{array} \Rightarrow \begin{array}{l} (2^{\text{a}} \text{ ecuación}) \ 1 = Q - x(x+1) \\ (1^{\text{a}} \text{ ecuación}) \ 1 = Q - x(P - x^2 Q) = -xP + (x^3+1)Q. \end{array}$$

Por tanto el inverso de $\overline{Q}$ es $\overline{x^3 + 1}$.

Los $\mathbb{F}_p$ no son los únicos cuerpos finitos.

Ejemplo. $K = \mathbb{F}_2[x]/\langle x^2 + x + 1 \rangle$ es un cuerpo de cuatro elementos y el inverso de $\overline{x}$ es $\overline{x + a}$.

Como $x^2 + x + 1$ es irreducible en $\mathbb{F}_2[x]$ (es de segundo grado y no tiene raíces en $\mathbb{F}_2$), K es un cuerpo. Ahora, hallando el resto al dividir por $x^2 + x + 1$, cualquier polinomio $P \in \mathbb{F}_2[x]$ es equivalente a otro de la forma $ax + b$ con $a, b \in \mathbb{F}_2$. Esto da cuatro posibilidades (no equivalentes), obteniéndose $K = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$. En $\mathbb{F}_2[x]$ se cumple $x(x+1) = 1 + (x^2 + x + 1)$, por tanto $\overline{x}$ y $\overline{x+1}$ son inversos uno del otro.

Nota: Tras este ejemplo cabría preguntarse qué cardinal puede tener un cuerpo finito. Resolveremos este problema más adelante en el curso cuando clasifiquemos todos los cuerpos finitos. Por ahora, como intriga de serial, avanzaremos que la lista de posibles cardinales comienza con 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17,.... La solución, en el tercer capítulo.

Ligado a los cuerpos finitos, pero no específico de ellos, está el concepto de característica, que desempeña un curioso papel en algunas propiedades de los cuerpos necesarias para poder aplicar la teoría de Galois.

Definición: Diremos que un cuerpo K (o un anillo) tiene *característica* n si n es el menor número natural tal que $1 + 1 + \overset{n \text{ veces}}{\ldots} + 1 = 0$. Si esta suma fuera siempre distinta de cero se dice que el cuerpo tiene *característica cero*. La notación habitual es $\text{char}(K) = n$.

Ejemplo. $\mathbb{C}$, $\mathbb{R}$ y $\mathbb{Q}$ tienen característica cero.

Ejemplo. $\mathbb{F}_5$ y $\mathbb{F}_5(x)$ tienen característica 5. (El primer cuerpo es finito y el segundo no lo es).

Ejemplo. Si K es un subcuerpo de $\mathbb{C}$, $\text{char}(K) = n$.

2.2. Extensiones de cuerpos

Habitualmente, para resolver una ecuación algebraica no basta con hacer sumas, restas, multiplicaciones y divisiones de los coeficientes, sino que tenemos que añadir algo que extienda el cuerpo generado por los coeficientes (por ejemplo $\sqrt{b^2-4ac}$ en el caso de la ecuación de segundo grado). Así como en Álgebra I estuvimos todo el rato mirando dentro de los grupos estudiando subgrupos y más subgrupos, en Álgebra II seremos más místicos y universalistas buscando experiencias fuera de los cuerpos.

Definición (provisional): Decimos que el cuerpo L es una *extensión* de K, si K es un subcuerpo de L, es decir, $K \subset L$ y las operaciones $+$ y $\times$ en K coinciden con las de L.

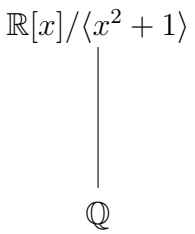
La notación que se usa habitualmente para designar una extensión es L/K o también $L : K$ (aquí preferiremos la primera).

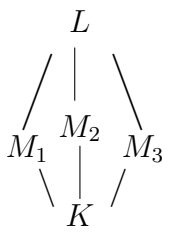
Aunque la definición anterior es satisfactoria en casi todos los casos que aparecerán en el curso, conviene al menos mencionar otra definición un poco más general y más conveniente desde el punto de vista abstracto.

Definición (generalizada): Decimos que el cuerpo L es una *extensión* de K, si existe un monomorfismo $f : K \longrightarrow L$.

Observación: Como recordamos en el primer capítulo, un monomorfismo es una función inyectiva compatible con las operaciones. Para comparar ambas definiciones consideremos $\mathbb{C}$ y $\mathbb{R}/\langle x^2+1\rangle$, que más adelante veremos que son cuerpos isomorfos, es decir, son el mismo cuerpo cambiando los nombres de los elementos. Con la primera definición $\mathbb{C}$ es una extensión de $\mathbb{Q}$, pero en rigor $\mathbb{Q}$ no está incluido en $\mathbb{R}[x]/\langle x^2+1\rangle$ porque este segundo cuerpo es un conjunto de clases de polinomios. Todo vuelve a funcionar si consideramos la composición $\mathbb{Q} \hookrightarrow \mathbb{C} \longleftrightarrow \mathbb{R}[x]/\langle x^2+1\rangle$ que es inyectiva y se ajusta a la segunda definición. A primera vista estas sutilezas y excesos de rigor parecen pamplinas matemáticas, sin embargo aparecerán de forma natural al estudiar cuerpos de descomposición.

Las extensiones de cuerpos muchas veces se indican con diagramas similares a los empleados por ejemplo en los retículos de subgrupos, situándose a mayor altura los cuerpos que "extienden" y conectándolos con líneas a los que son "extendidos". Por ejemplo, la extensión que acabamos de mencionar está representada en el diagrama de la izquierda, mientras que el de la derecha significa que L/M_1, L/M_2, L/M_3, M_1/K, M_2/K y M_3/K son extensiones de cuerpos. En particular, L/K también lo será.





Señalaremos tres tipos destacados de extensiones de cuerpos. En este curso trataremos fundamentalmente las del segundo con $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ y α_i raíces de polinomios en $K[x]$. Un sorprendente resultado del próximo capítulo (el teorema del elemento primitivo) asegurará que casi todas las extensiones de esta forma que podemos imaginar a este nivel, son también del primer tipo.

Definición: Se dice que una extensión, L/K, es:

1) *simple*, si $L = K(\alpha)$ con $\alpha \in L$.

2) *algebraica*, si todo $\alpha \in L$ es *algebraico* sobre K, es decir, existe un polinomio $P \in K[x]$ tal que $P(\alpha) = 0$.

3) *trascendente*, si no es algebraica. En particular existirá algún $\alpha \in L$ que es *trascendente*, es decir, que no es no algebraico.

Ejemplo. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ y $\mathbb{Q}(x)/\mathbb{Q}(x^2)$ son simples y algebraicas.

La segunda es simple porque $\mathbb{Q}(x) = \mathbb{Q}(x^2, x) = \big(\mathbb{Q}(x^2)\big)(x)$. Los elementos $\mathbb{Q}\big(\sqrt{2}\big)$ son de la forma $a+b\sqrt{2}$ con $a, b \in \mathbb{Q}$ y satisfacen la ecuación algebraica $(x-a)^2-2b^2 = 0$, por tanto la primera extensión es algebraica. Para la segunda el argumento es similar si tomamos la precaución de no confundir x con la variable del polinomio que elijamos. Los elementos de $\mathbb{Q}(x)/\mathbb{Q}(x^2)$ son de la forma $f + xg$ con $f, g \in \mathbb{Q}(x^2)$ y por tanto resuelven la ecuación $(X - f)^2 - x^2g^2 = 0$. Nótese que $(X - f)^2 - x^2g^2 \in \mathbb{Q}(x^2)[X]$.

Ejemplo. $\mathbb{Q}(x)/\mathbb{Q}$ y $\mathbb{R}(x, y)/\mathbb{R}(x)$ son simples y trascendentes.

Ejemplo. $\mathbb{C}(x, y)/\mathbb{Q}$ no es simple y es trascendente.

Ejemplo. (Lindemann 1882) $\mathbb{Q}(\pi)/\mathbb{Q}$ es trascendente.

Éste es un resultado muy difícil que probaremos en la última sección del presente capítulo, junto con que $\mathbb{Q}(e)/\mathbb{Q}$ es trascendente.

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

El siguiente resultado es prácticamente trivial, pero ocupa un papel destacado porque permite ligar la teoría de cuerpos, que todavía no nos sabemos, con el álgebra lineal de la que conocemos todo.

Proposición 2.2.1 *Si L/K es una extensión de K, entonces L es un espacio vectorial sobre K.*

Este resultado no sería tan relevante y pasaría de proposición a observación pedante, si no tuvieramos maneras de hacer cálculos con dimensiones y bases, y de usar verdaderamente el álgebra lineal. De ello trata una ristra de proposiciones que se enunciarán enseguida. Antes, un par de sencillas pero cruciales definiciones para poder hablar más con menos palabras.

Definición: A la dimensión de L como espacio vectorial sobre K se le llama *grado* de L/K y se escribe $[L : K]$. Si el grado es finito se dice que la extensión es *finita*, en caso contrario se dice que es *infinita*.

Definición: Si α es algebraico sobre K, se dice que $P \in K[x]$ es el *polinomio mínimo* de α si P es mónico, α es un cero de P y no hay otro polinomio de grado menor con estas características.

Nota: Recuérdese que un polinomio es *mónico* si su coeficiente de mayor grado es 1.

Observación: No es difícil demostrar que el polinomio mínimo, P, de α es único y además cumple (ejercicio)

$$1)\ P \text{ es irreducible} \qquad 2)\ Q \in K[x],\ Q(\alpha) = 0 \ \Rightarrow\ P|Q.$$

Evidentemente, el polinomio mínimo depende del cuerpo sobre el que trabajemos. Muchas veces, si no se indica otra cosa, se sobreentiende que $K = \mathbb{Q}$.

Ejemplo. El polinomio mínimo de $\sqrt[4]{3}$ sobre $\mathbb{Q}$ es $x^4 - 3$ y sobre $\mathbb{Q}(\sqrt{3})$ es $x^2 - \sqrt{3}$.

Ahora ya pasamos a la prometida ristra de proposiciones:

Proposición 2.2.2 *Si L/K y M/L son extensiones de cuerpos*

$$[M : K] = [M : L][L : K].$$

De hecho, si L/K y M/L son finitas y $\{x_1, x_2, \ldots, x_r\}$, $\{y_1, y_2, \ldots, y_s\}$ son sus bases, entonces $\{x_1y_1, x_1y_2, \ldots, x_ry_s\}$ es una base de M/K.

Demostración: Nos restringiremos al caso en que las extensiones son finitas (el otro queda como ejercicio). La proposición se reduce a probar que $B = \{x_1y_1, x_1y_2, \ldots, x_ry_s\}$ es una base de M/K.

1) *B es un sistema de generadores*: Si $z \in M$ entonces como M es un espacio vectorial sobre L con base $\{y_1, y_2, \ldots, y_s\}$

$$z = \lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_s y_s \qquad \text{con } \lambda_i \in L.$$

Pero, de la misma forma, como $\lambda_i \in L$

$$\lambda_i = \mu_{i1} x_1 + \mu_{i2} x_2 + \cdots + \mu_{ir} x_r \qquad \text{con } \mu_{ir} \in K.$$

Sustituyendo estas igualdades en las anteriores se obtiene que z es una combinación lineal de elementos de B con coeficientes en K.

2) *B es linealmente independiente*: Supongamos que tenemos una combinación lineal nula

$$\sum_{i=1}^{r} \sum_{j=1}^{s} \lambda_{ij} x_i y_j = 0 \qquad \text{con } \lambda_{ij} \in K,$$

entonces

$$\sum_{j=1}^{s}\Big(\sum_{i=1}^{r}\lambda_{ij}x_i\Big)y_j=0\ \Rightarrow\ \sum_{i=1}^{r}\lambda_{ij}x_i=0\qquad 1\le j\le s,$$

porque los términos entre paréntesis pertenecen a L y los y_j son una base de M/L. Como, por otra parte, los x_i son una base de L/K, de la última igualdad se concluye finalmente $\lambda_{ij}=0$. □

Proposición 2.2.3 *Toda extensión finita es algebraica.*

Demostración: Sean L/K y $\alpha\in L$, entonces como L/K es finita hay alguna combinación lineal no trivial nula entre los elementos 1, α, α^2, α^3, ...; esto es, existen $\lambda_i\in K$, $0\le i\le n$, no todos nulos tales que $\lambda_n\alpha^n+\lambda_{n-1}\alpha^{n-1}+\cdots+\lambda_1\alpha+\lambda_0=0$, por tanto α es algebraico. □

Proposición 2.2.4 *$K(\alpha)/K$ es finita si y sólo si α es algebraico sobre K. Además en ese caso $[K(\alpha):K]=n$ donde n es el grado del polinomio mínimo de α, de hecho*

$$K(\alpha)=\big\{\lambda_0+\lambda_1\alpha+\lambda_2\alpha^2+\cdots+\lambda_{n-1}\alpha^{n-1}\ \ \textit{con}\ \lambda_i\in K\big\}.$$

Demostración: Sea $\mathcal{A}$ el conjunto que aparece al final del enunciado, esto es,

$$\mathcal{A}=\big\{\lambda_0+\lambda_1\alpha+\lambda_2\alpha^2+\cdots+\lambda_{n-1}\alpha^{n-1}\ \ \text{con}\ \lambda_i\in K\big\}.$$

Suponiendo conocido que $K(\alpha)=\mathcal{A}$, para comprobar que $[K(\alpha):K]=n$, basta ver que no existe ninguna combinación lineal no trivial nula en $\mathcal{A}$. Si $\lambda_0+\lambda_1\alpha+\cdots+\lambda_k\alpha^k$ con $k\le n$, entonces α sería raíz de un polinomio de grado menor que n, lo cual es una contradicción.

Falta por tanto comprobar $K(\alpha)=\mathcal{A}$. Obviamente $\alpha\in\mathcal{A}$ y $\mathcal{A}\subset K(\alpha)$, si demostramos que $\mathcal{A}$ es un cuerpo se tiene $K(\alpha)=\mathcal{A}$ (porque $K(\alpha)$ es el menor cuerpo que contiene a α). Está claro que $\mathcal{A}$ es cerrado por sumas y restas, basta ver que también es cerrado por divisiones (la multiplicación se reduce a dos divisiones: $a\cdot b=a\big/1/b$). Si $a,b\in\mathcal{A}$ entonces $a/b=Q_1(\alpha)/Q_2(\alpha)$ donde Q_1 y $Q_2\neq 0$ son polinomios de grado menor que n. Sea P el polinomio mínimo de α, como $\partial Q_2<\partial P=n$, Q_2 y P son primos entre sí, aplicando el algoritmo de Euclides podemos encontrar $A,B\in K[x]$ tales que

$$1=AP+BQ_2.$$

Multiplicando por Q_1, dividiendo por Q_2 y sustituyendo α, se tiene

$$\frac{Q_1(\alpha)}{Q_2(\alpha)}=Q_1(\alpha)B(\alpha).$$

Por otra parte, al dividir Q_1B entre P se consigue $Q_1B=PC+R$ con $\partial R<\partial P=n$, lo que empleado en la igualdad anterior prueba el resultado. □

Las extensiones algebraicas simples, también se pueden ver como cocientes por ideales, y esto no es rizar el rizo, sino que tendrá gran utilidad en el próximo capítulo para probar elegante y simplemente algunos resultados básicos de la teoría de Galois.

Proposición 2.2.5 *Sea L/K y sea P el polinomio mínimo de $\alpha \in L$ sobre K, entonces*

$$\psi : K(\alpha) \longrightarrow K[x]/\langle P\rangle$$

con $\psi(\alpha) = \overline{x} = x + \langle P\rangle$, define un isomorfismo de cuerpos.

Demostración: Por la proposición anterior se tiene que $\alpha_1, \alpha_2 \in K(\alpha) \Rightarrow \alpha_1 = Q_1(\alpha)$, $\alpha_2 = Q_2(\alpha)$ y $\alpha_1\alpha_2 = Q_3(\alpha)$ con $\partial Q_i < \partial P$.

Es obvio que

$$\psi(\alpha_1 + \alpha_2) = \psi\big(Q_1(\alpha) + Q_2(\alpha)\big) = \overline{Q_1(x)} + \overline{Q_2(x)} = \psi(\alpha_1) + \psi(\alpha_2).$$

Nótese que $Q_1Q_2 - Q_3$ se anula en α, por tanto es divisible por P y su clase en $K[x]/\langle P\rangle$ es la clase de cero. Por tanto

$$\psi(\alpha_1)\psi(\alpha_2) - \psi(\alpha_1\alpha_2) = \overline{Q_1(x)Q_2(x)} - \overline{Q_3(x)} = \overline{0}.$$

Como ψ aplica α en $\overline{x}$, que genera $K[x]/\langle P\rangle$, es un epimorfismo. Además $\psi(\alpha_1) - \psi(\alpha_2) = 0 \Rightarrow Q_1 - Q_2 \in (P) \Rightarrow P | Q_1 - Q_2$ y como $\partial Q_i < \partial P$, $Q_1 = Q_2$ y ψ también es un monomorfismo. □

Ejemplo. $\mathbb{C}$ es isomorfo a $\mathbb{R}[x]/\langle x^2 + 1\rangle$.

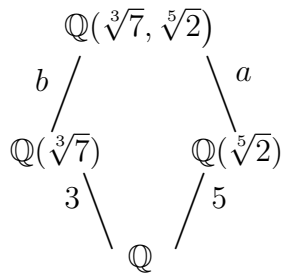
Esta aplicación directa de la Proposición 2.2.5 permite pensar en los números complejos sin introducir cosas tan poco justificables como la raíz cuadrada de -1. A cambio hay que dar un gran salto en la abstracción.

Ejemplo. La Proposición 2.2.4 asegura que $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4$ y además

$$\mathbb{Q}(\sqrt[4]{3}) = \big\{a + b\sqrt[4]{3} + c\sqrt[4]{9} + d\sqrt[4]{27} \ : \ a, b, c, d \in \mathbb{Q}\big\}.$$

Nótese que no es en absoluto trivial probar que el segundo miembro es un cuerpo sin usar esta igualdad. El mismo resultado se podría haber deducido de la Proposición 2.2.2 considerando las extensiones $\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}(\sqrt{3})$ y $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$.

Ejemplo. Calcular el grado del polinomio mínimo de $\sqrt[3]{7}$ en $\mathbb{Q}(\sqrt[5]{2})$.



Por la Proposición 2.2.4, el problema se reduce a calcular $a = [\mathbb{Q}(\sqrt[3]{7}, \sqrt[5]{2}) : \mathbb{Q}(\sqrt[5]{2})]$.

Designemos por n el grado de $\mathbb{Q}(\sqrt[3]{7}, \sqrt[5]{2})/\mathbb{Q}$, entonces por la Proposición 2.2.2 se cumple $n = 5a$ y $n = 3b$ donde b es, como indica el esquema, el grado de $\mathbb{Q}(\sqrt[3]{7}, \sqrt[5]{2})/\mathbb{Q}(\sqrt[3]{7})$. Esto implica que 3 divide a a y 5 divide a b. Por otra parte, $P = x^3 - 7$ es un polinomio en $\mathbb{Q}(\sqrt[5]{2})[x]$ (y también en $\mathbb{Q}[x]$) tal que $\sqrt[3]{7}$ es uno de sus ceros, así pues el grado del polinomio mínimo es menor o igual que 3, es decir, $a \leq 3$. Como ya hemos probado que 3 divide a a, se tiene que $a = 3$. De hecho, este mismo argumento concluye que $b = 5$ y que $n = 15$.

Ejemplo. Si $\alpha \in \mathbb{C}$ es una raíz del polinomio irreducible $P = x^3 + 3x + 3$, expresar $1/(\alpha+1)$ como una combinación lineal racional de 1, α y α^2; es decir, hallar $a, b, c \in \mathbb{Q}$ tales que $1/(\alpha+1) = a + b\alpha + c\alpha^2$.

Nótese que la Proposición 2.2.4 asegura que esto es posible. Tomemos $Q = x + 1$, como P es irreducible el máximo común divisor de P y Q es 1, existen $A, B \in \mathbb{Q}[x]$ tales que

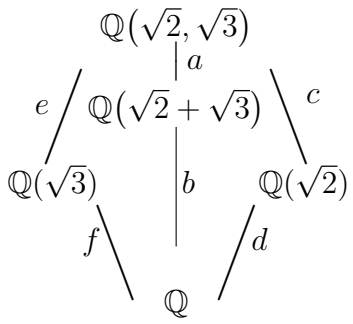
$$1 = AP + BQ.$$

En nuestro caso es fácil ver que puede tomarse $A = -1$ y $B = x^2 - x + 4$. Dividiendo por Q y sustituyendo α, se tiene finalmente

$$\frac{1}{\alpha+1} = 4 - \alpha + \alpha^2.$$

Ejemplo. Comparar los cuerpos $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ y $\mathbb{Q}$.

Se tiene un esquema como el adjunto, donde las letras cursivas representan los grados, que hallaremos a continuación.



Los polinomios mínimos sobre $\mathbb{Q}$ de $\sqrt{2}$ y $\sqrt{3}$ son $x^2 - 2$ y $x^2 - 3$ respectivamente, y $x^2 - 2$ es también el polinomio mínimo de $\sqrt{2}$ en la extensión $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{3})$, ya que si factorizase en $\mathbb{Q}(\sqrt{3})$ se tendría $\sqrt{2} = r + s\sqrt{3}$ con $r, s \in \mathbb{Q}$ y esto no es posible (basta elevar al cuadrado). Estas consideraciones permiten concluir que $d = f = e = 2$. La Proposición 2.2.2 asegura $ab = cd = ef = 4$, por tanto $c = 2$ y las únicas posibilidades para a y b son $b = 4/a$ con $a = 1, 2, 4$. Nótese que $a = 4$ es imposible porque $\sqrt{2}+\sqrt{3} \notin \mathbb{Q}$ (de nuevo basta elevar al cuadrado). Para ver que $a = 1$ y $b = 4$, considérense los polinomios $\left(x - (\sqrt{2}+\sqrt{3})\right)^2 - 3$ y $x^2 - 2$. Ambos están en $\mathbb{Q}(\sqrt{2}+\sqrt{3})[x]$ y ambos son distintos y tienen a $x = \sqrt{2}$ como raíz, por tanto su máximo común divisor en $\mathbb{Q}(\sqrt{2}+\sqrt{3})[x]$ es $x - \sqrt{2}$, por tanto $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ y $\sqrt{3} = (\sqrt{2}+\sqrt{3}) - \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Esto permite concluir $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \supset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ y como $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ es trivial, se tiene que ambos cuerpos son iguales o equivalentemente, $a = 1$ y por tanto $b = 4$.

Parece una casualidad o un milagro forzado que en el ejemplo anterior se hayan podido reducir dos generadores a uno, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$, pero como antes hemos insinuado, hay un sorprendente resultado del próximo capítulo que afirma que esto es moneda común. En particular se deducirá que es imposible encontrar extensiones finitas de cuerpos normales y corrientes ($\mathbb{Q}$, $\mathbb{F}_p$, subcuerpos de $\mathbb{C}\ldots$) que no sean simples.

Ejemplo. Hallar el polinomio mínimo de $\sqrt{2}+\sqrt{3}$ sobre $\mathbb{Q}$.

Por el ejemplo anterior $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$, así que el polinomio mínimo, P, debe tener grado 4. Digamos que es $P = x^4 + ax^3 + bx^2 + cx + d$, entonces

$$(\sqrt{2}+\sqrt{3})^4 + a(\sqrt{2}+\sqrt{3})^3 + b(\sqrt{2}+\sqrt{3})^2 + c(\sqrt{2}+\sqrt{3}) + d = 0.$$

Operando obtenemos una expresión de la forma $A + B\sqrt{2} + C\sqrt{3} + D\sqrt{6} = 0$. Como $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ es una base de $\mathbb{Q}\big(\sqrt{2},\sqrt{3}\big) = \mathbb{Q}\big(\sqrt{2}+\sqrt{3}\big)$ (por la Proposición 2.2.2), entonces los coeficientes A, B, C y D (que dependen de a, b, c y d) deben ser nulos. Esto nos lleva al sistema de ecuaciones

$$\begin{array}{ll} A = 49 + 5b + d = 0 & C = 9a + c = 0 \\ B = 11a + c = 0 & D = 20 + 2b = 0 \end{array}$$

cuya solución es $a = c = 0$, $b = -10$, $d = 1$; por tanto $P = x^4 - 10x^2 + 1$.

Otra manera más sencilla de proceder en este caso es considerar el polinomio $Q = (x - \sqrt{2})^2 - 3$. Obviamente $\sqrt{2} + \sqrt{3}$ es una raíz de Q, pero $Q = x^2 - 2\sqrt{2}\,x - 1 \notin \mathbb{Q}[x]$. Para eliminar los radicales podemos "multiplicar por el conjugado", así $P = (x^2 - 2\sqrt{2}\,x - 1)(x^2 + 2\sqrt{2}\,x - 1)$ es un polinomio en $\mathbb{Q}[x]$ que tiene a $\sqrt{2} + \sqrt{3}$ como raíz, además $\partial P = [\mathbb{Q}\big(\sqrt{2}+\sqrt{3}\big) : \mathbb{Q}] = 4$ implica que es el polinomio mínimo.

Ejemplo. Dada la extensión $L/\mathbb{F}_2$ con $L = \mathbb{F}_2[x]/\langle x^3 + x + 1\rangle$, calcular su grado y el polinomio mínimo de $\alpha = \overline{x^4 + x^2 + 1}$.

En $\mathbb{F}_2[x]$, $x^4+x^2+1 = x+1+(x^3+x+1)x$, por tanto $\alpha = \overline{x+1}$. En general, dividiendo por x^3+x+1, todos los elementos de L se escriben de manera única como combinaciones lineales de $\{\overline{1}, \overline{x}, \overline{x^2}\}$, por consiguiente $[L : \mathbb{F}_2] = 3$. El grado del polinomio mínimo de α debe ser 3 ya que α no está en $\mathbb{F}_2$ (o en su imagen por el monomorfismo $\mathbb{F}_2 \longrightarrow L$, si uno es un purista), y basta entonces hallar un polinomio mónico cúbico que tenga a α como raíz. Sabemos que $\overline{x^3 + x + 1} = 0$. De aquí $(\alpha - 1)^3 + (\alpha - 1) + 1 = 0$ y operando el primer miembro es $\alpha^3 + \alpha^2 + 1$. Así pues, el polinomio mínimo es $P = X^3 + X^2 + 1$.

2.3. Tres problemas clásicos

Esta sección es una de las más bellas del curso. Veremos que el mundo artificial que hemos poblado en las secciones anteriores con estructuras algebraicas tales como cuerpos, espacios vectoriales, anillos y cocientes, no pertenece a la estratosfera de la abstracción matemática, sino que desciende suavemente hasta la base de nuestra historia para dar respuesta a tres cuestiones geométricas con enunciado elemental que no supieron resolver los antiguos griegos.

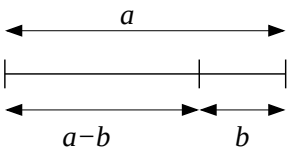
Las cuestiones a las que nos referimos tratan acerca de construcciones con regla y compás, donde la utilidad de estos instrumentos queda limitada de manera que la regla solamente se puede usar para trazar una recta que pasa por dos puntos conocidos, y el compás sólo se puede emplear para trazar una circunferencia de la que se conocen centro y radio.

Una vez fijada una unidad de medida, digamos determinada por $(0, 0)$ y $(1, 0)$, como las rectas tienen ecuaciones de primer grado y las circunferencias de segundo grado, todos los puntos que se pueden construir como intersecciones sucesivas de ellas tienen coordenadas que están en sucesivas extensiones cuadráticas (esto es, de segundo grado). Por tanto, si $(x, y) \in \mathbb{R}^2$ es un punto construible con regla y compás entonces existe una cadena de cuerpos

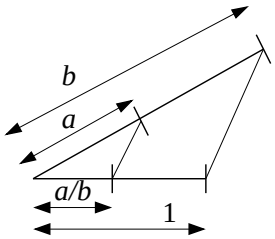
$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_n = L$$

con $[L_{k+1} : L_k] = 2$ y $x, y \in L \subset \mathbb{R}$.

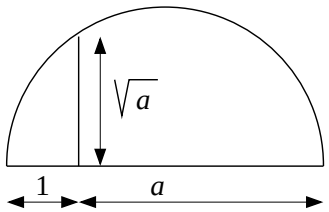
Con la ayuda de algunas construcciones geométricas sencillas conocidas desde la antigüedad es posible comprobar que la suma, resta, multiplicación, división y raíz cuadrada de longitudes construibles con regla y compás, también es construible con regla y compás. Todo lo necesario está contenido en los siguientes diagramas:



1. Construcción de $a - b$



2. Construcción de a/b



3. Construcción de $\sqrt{a}$.

De todo esto se deduce que cualquier elemento de un cuerpo real, L, para el que exista una cadena de subcuerpos como la anterior, puede ser obtenido como coordenada de un punto construible con regla y compás, es decir, se tiene la siguiente caracterización que tomaremos como definición:

Definición: Un punto $(x, y) \in \mathbb{R}^2$ es *construible* con regla y compás si y sólo si x e y pertenecen a un cuerpo $L \subset \mathbb{R}$ tal que existe una cadena de subcuerpos

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_n = L$$

donde todas las extensiones son de grado dos. En breve, diremos que un número real es construible si aparece como coordenada de un punto contruible.

Una consecuencia inmediata de la definición en virtud de la Proposición 2.2.2, es:

Lema 2.3.1 *Si $u \in \mathbb{R}$ es construible, $[\mathbb{Q}(u) : \mathbb{Q}]$ es una potencia de dos.*

Observación: El recíproco de este lema no es cierto sin hipótesis adicionales. Para probar la existencia de contraejemplos se debe utilizar la teoría de Galois en toda su fuerza, así que pospondremos esta cuestión.

Ahora pasaremos a enunciar las tres cuestiones clásicas que se plantearon los antiguos griegos.

⁎1 Dada la arista de un cubo, construir con regla y compás la arista de un cubo de volumen doble.
⁎2 Dado un ángulo, hallar un método para trisecarlo con regla y compás.
⁎3 Dado un círculo, construir con regla y compás un cuadrado de igual área.

Si existiera una construcción que resolviera el primer problema para el cubo de arista 1, entonces se podría construir $\sqrt[3]{2}$. El segundo problema se debe entender como que dado un punto podemos construir otro que subtiende un ángulo (con el eje OX)

que sea la tercera parte. En particular, como $(\cos 60°, \operatorname{sen} 60°) = (1/2, \sqrt{3}/2)$ es construible, el método permitiría construir $(\cos 20°, \operatorname{sen} 20°)$. Por último, una construcción que resolviera el tercer problema para el caso del círculo de radio 1, permitiría construir $\sqrt{\pi}$.

Tras estas observaciones, las dos proposiciones siguientes muestran que no hay ninguna construcción con regla y compás en los términos requeridos que permita resolver estos problemas. La sencillez de la primera proposición contrasta con los siglos que transcurrieron hasta probar la imposibilidad de ⋇1 y ⋇2, lo que debe hacernos meditar sobre la importancia de crear el lenguaje adecuado para resolver un problema matemático. La segunda proposición es bastante más compleja y su prueba opcional en este curso.

Proposición 2.3.2 $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\cos 20°) : \mathbb{Q}] = 3$*, por tanto* ⋇1 *y* ⋇2 *no tienen solución con regla y compás.*

Demostración: La igualdad $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ es trivial porque $x^3 - 2$ es el polinomio mínimo de $\sqrt[3]{2}$. Lás fórmulas de adición de la fórmulas trigonométricas implican:

$$\begin{aligned} \cos(3\alpha) = \cos(2\alpha + \alpha) &= \cos(2\alpha)\cos\alpha - \operatorname{sen}(2\alpha)\operatorname{sen}\alpha \\ &= (\cos^2\alpha - \operatorname{sen}^2\alpha)\cos\alpha - (2\operatorname{sen}\alpha\cos\alpha)\operatorname{sen}\alpha \\ &= 4\cos^3\alpha - 3\cos\alpha \end{aligned}$$

Sustituyendo $\alpha = 20°$, se tiene que $\cos 20°$ es una raíz del polinomio $P = x^3 - 3x/4 - 1/8$. Aplicando el criterio de Eisenstein a $8P\big((x+1)/2\big)$ se deduce que P es irreducible, por tanto es el polinomio mínimo de $\cos 20°$ y $[\mathbb{Q}(\cos 20°) : \mathbb{Q}] = 3$. □

Proposición 2.3.3 (Lindemann) π *es trascendente sobre* $\mathbb{Q}$*, en particular* ⋇3 *no tiene solución con regla y compás.*

Para los que quieran leer la letra pequeña, o para los que no quieran leerla pero tengan interés en saber la idea bajo la demostración, una pequeña explicación previa en miniatura:

El resultado de Lindemann se basa en un trabajo anterior de Hermite en el que probaba que e es un número trascendente. Ambas demostraciones son parecidas gracias a la misteriosa relación $e^{i\pi} = -1$. Lo que hizo Hermite es encontrar fracciones m_j/N que aproximan excepcionalmente bien a e^j, de forma que cuando $N \to \infty$ (con N en cierta subsucesiónde $\mathbb{N}$) el error tiende a cero más rápido que $1/N$. Con ello, fijados $a_n, a_{n-1}, \ldots, a_1 \in \mathbb{Z}$ y definiendo

$$A_N = a_n e^n + a_{n-1}e^{n-1} + \cdots + a_2 e^2 + a_1 e^1 - a_n\frac{A_n}{N} - a_{n-1}\frac{A_{n-1}}{N} - \cdots - a_2\frac{A_2}{N} - a_1\frac{A_1}{N},$$

se tiene $\lim_{N\to\infty} NA_N = 0$. Si e fuera un cero del polinomio $P = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Entonces NA_N conformaría una sucesión de enteros que tiende a cero, y las únicas sucesiones con estas características son las que a partir de un término son idénticamente nulas. Recapitulando, la estrategia para demostrar la trascendencia de e consiste en encontrar una aproximación racional muy buena de sus potencias, y probar

que no ocurre el milagro de que el error es idénticamente nulo para una combinación lineal de ellas.

Para la demostración "de verdad", si $P \in \mathbb{Z}[x]$ con $\partial P \geq 1$, fatoriza en $\mathbb{C}[x]$ como $P = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)$, definimos

$$E_P = e^{\alpha_1} + e^{\alpha_2} + \cdots + e^{\alpha_k}.$$

El resultado fundamental será el que enunciamos a continuación:

Teorema 2.3.4 *Sean $P_1, P_2, \ldots, P_n \in \mathbb{Z}[x]$ tales que $P_j(0) \neq 0$, $1 \leq j \leq n$. Dados $a_n, a_{n-1}, \ldots, a_1 \in \mathbb{Z}$ no simultáneamente nulos, se tiene $a_n E_{P_n} + a_{n-1} E_{P_{n-1}} + \cdots + a_1 E_{P_1} \notin \mathbb{Z} - \{0\}$.*

Demostración: Digamos que P_j factoriza en $\mathbb{C}[x]$ como $P_j = c_j(x-\alpha_{j1})(x-\alpha_{j2})\cdots(x-\alpha_{jk_j})$. Sea $P = \prod_j \prod_l (c_j(x-\alpha_{jl})) \in \mathbb{Z}[x]$ y consideremos las cantidades mágicas (esencialmente introducidas por Hermite)

$$A = \sum_j a_j \sum_l e^{\alpha_{jl}} \int_{\alpha_{jl}}^{\infty} \frac{x^{p-1}e^{-x}}{(p-1)!}\big(P(x)\big)^p dx \qquad \text{y} \qquad B = \int_0^{\infty} \frac{x^{p-1}e^{-x}}{(p-1)!}\big(P(x)\big)^p dx$$

con p un número primo que elegiremos más adelante. Aunque parezca increíble, A y B son enteros y A/B aproxima excepcionalmente bien a la expresión del enunciado.

La igualdad

$$\int_0^{\infty} \frac{x^{p-1}e^{-x}}{(p-1)!} x^k dx = \frac{(p+k-1)!}{(p-1)!}$$

prueba inmediatamente que $B \in \mathbb{Z}$, y si elegimos $p \not| P_j(0)$, se tiene $p \not| B$ porque P tiene un término independiente no nulo. Un argumento similar en A, tras el cambio de variable $u = x - \alpha_{jl}$ en la integral, permite deducir que la suma en l es un polinomio simétrico de coeficientes enteros en $c_j\alpha_{j1}, c_j\alpha_{j2}, \ldots$, esto es, en las raíces del polinomio mónico $c_j^{k_j-1}P_j(x/c_j) \in \mathbb{Z}[x]$. Según el Teorema 1.1.2 se tiene que la suma en l es un polinomio entero evaluado en los coeficientes de este polinomio, y por tanto $A \in \mathbb{Z}$. Además como $P(u+\alpha_{jl})$ no tiene término independiente, $p|A$.

Por otra parte, si llamamos E a la expresión del enunciado, se tiene para ciertas constantes K_1 y K_2

$$|BE - A| = \Big|\sum_j a_j \sum_l e^{\alpha_{jl}} \int_0^{\alpha_{jl}} \frac{x^{p-1}e^{-x}}{(p-1)!}\big(P(x)\big)^p dx\Big| \leq \frac{K_1 \cdot K_2^p}{(p-1)!},$$

donde se ha usado que un polinomio en un intervalo finito está acotado. Tomando p suficientemente grande se consigue que el segundo miembro sea menor que 1. Si E fuera un entero no nulo, podríamos suponer también $p \not| E$ y esto lleva a una contradicción, porque $BE - A$ sería un entero no divisible por p y de valor absoluto menor que 1. □

Corolario 2.3.5 (Hermite 1873) *e es trascendente sobre $\mathbb{Q}$.*

Demostración: Tómese $P_1 = x - 1$, $P_2 = x - 2$,..., $P_m = x - m$ en el teorema anterior. □

Demostración de la Proposición 2.2.3: Si π fuera algebraico, $i\pi$ también lo sería (donde $i = \sqrt{-1}$). En ese caso existe un polinomio irreducible en $\mathbb{Z}[x]$ cuyas raíces son $\alpha_1 = i\pi$, α_2, ... Digamos que c es su coeficiente de mayor grado. La fórmula de Euler implica $e^{\alpha_1} = -1$ con lo cual $\prod_k \left(1 + e^{\alpha_k}\right) = 0$. Y operando en esta igualdad se obtiene

$$1 + \sum_{j_1} e^{\alpha_{j_1}} + \sum_{j_1<j_2} e^{\alpha_{j_1}+\alpha_{j_2}} + \sum_{j_1<j_2<j_3} e^{\alpha_{j_1}+\alpha_{j_2}+\alpha_{j_3}} + \cdots = 0$$

Si consideramos $\prod_m (c(x - e_m))$ donde e_m denota cada exponente no nulo que aparece en la fórmula anterior, entonces $P \in \mathbb{Z}[x]$ (basta aplicar el Teorema 1.1.2 como en el teorema). La igualdad se podría escribir entonces como $1 + r + E_P = 0$ donde r es el número de posibles exponentes nulos, y esto implica $E_P \in \mathbb{Z}^-$ en contradicción con el Teorema 2.3.4. □

Ejercicios del Capítulo 2

LEYENDA: ♡ fácil, ♢ difícil, ♢♢ muy difícil, ∘ opcional.

Sección 2.1

♡**1.** Demostrar que $\mathbb{Z}/6\mathbb{Z}$ no es un cuerpo. Hallar las unidades.

2. Hallar el máximo común divisor de $P = x^4 + 6x^3 + 13x^2 + 12x + 3$ y $Q = x^4 + 5x^3 + 9x^2 + 8x + 2$, y escribirlo en la forma $AP + BQ$.

3. Demostrar que si la característica de un cuerpo no es cero, entonces es un número primo.

4. Demostrar que un dominio de integridad finito es un cuerpo.

5. Sea F un cuerpo y $f(x) \in F[x]$ un polinomio. Se dice que $a \in F$ es un cero de $f(x)$ si $f(a) = 0$. Demostrar que a es un cero de $f(x)$ si y sólo si $x - a$ divide a $f(x)$. *Indicación*: Estudiar el resto al dividir $f(x)$ por $x - a$.

6. El polinomio $f = x^3 - 3x + 1$ es irreducible en $\mathbb{Q}[x]$. Sea $\beta = \overline{x^4 - 3x^2 + 2x + 3} \in \mathbb{Q}[x]/\langle f \rangle$. Hallar β^{-1} y β^2 expresándolos como combinación lineal de $\{1, \overline{x}, \overline{x}^2\}$.

7. Probar que si P es un polinomio no nulo sobre un cuerpo, su número de raíces es menor que el grado. Dar un contraejemplo si el cuerpo se reemplaza por un anillo.

8. Si K es un cuerpo y R es un anillo, probar que cualquier homomorfismo no nulo $f : K \longrightarrow R$ es necesariamente un monomorfismo.

9. Dado un cuerpo L, sea K la intersección de todos sus subcuerpos (K recibe el nombre de *subcuerpo primo* de L). Demostrar que la característica de L es positiva si y sólo si K es isomorfo a $\mathbb{F}_p$, y es cero si y sólo si K es isomorfo a $\mathbb{Q}$.

10. Sea $f : L \to M$ un homomorfismo no trivial de cuerpos. Probar que la característica de L es igual a la de M, y que si K es el subcuerpo primo de L entonces $f(s) = s$ para todo $s \in K$.

11. Encontrar todos los automorfismos de $\mathbb{Q}(\sqrt[3]{5})$. *Indicación*: Hallar la imagen de 5 y emplear $(\sqrt[3]{5})^3 = 5$ para determinar la de $\sqrt[3]{5}$.

12. Calcular todos los automorfismos de $\mathbb{Q}(\sqrt{7})$.

13. Demostrar que $\mathbb{Q}(\sqrt{2})$ no es isomorfo a $\mathbb{Q}(\sqrt{5})$.

14. Demostrar que en $\mathbb{Z}$ y en $K[x]$ (K un cuerpo) hay infinitos irreducibles no asociados.

15. Se dice que un cuerpo K es algebraicamente cerrado si todo polinomio $P \in K[x]$ con $\partial P \geq 2$ se descompone en factores lineales. Probar que ningún cuerpo finito es algebraicamente cerrado

16. Establecer las relaciones de inclusión que hay entre los cuerpos $\mathbb{Q}(i, \sqrt{3})$, $\mathbb{Q}(\sqrt{-3})$ y $\mathbb{Q}(i + \sqrt{3})$.

17. Demostrar que $\mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$ es un cuerpo y calcular su cardinal. Dar la tabla de su producto.

18. Construir un cuerpo con 25 elementos y otro con 27. *Indicación*: No es necesario escribir la tabla de las operaciones en estos cuerpos.

19. Probar que sólo hay un cuerpo de cuatro elementos salvo isomorfismos.

20. Probar que no hay dominios de integridad de seis elementos (por lo tanto no hay cuerpos de seis elementos).

21. Probar que para todo primo p, en $\mathbb{F}_p[x]$ se cumple

$$x^{p-1} - 1 = (x - 1)(x - 2) \cdots (x - (p - 1)).$$

22. Si K tiene característica p, probar que $\phi : K \longrightarrow K$ dado por $\phi(k) = k^p$ es un homomorfismo.

23. Sea $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ en $K[x]$ con $a_0, a_n \neq 0$. f es irreducible si y sólo si $a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$ es irreducible.

♢**24.** Sea A un dominio de integridad y supongamos que existe un cuerpo $K \subset A$ tal que A es un espacio vectorial de dimensión finita sobre K. Demostrar que A es también un cuerpo.

♢**25.** Demostrar que si un primo p es de la forma $p = n^2 + 2m^2$ con $n, m \in \mathbb{Z}$, entonces $\mathbb{Z}[\sqrt{-2}]/(n + m\sqrt{-2})$ es isomorfo a $\mathbb{F}_p$.

Sección 2.2

26. Hallar el grado de las siguientes extensiones y decir de qué tipo son:

i) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ ii) $\mathbb{Q}(e^{2\pi i/5})/\mathbb{Q}$ iii) $\mathbb{R}(\sqrt{3})/\mathbb{R}$ iv) $\mathbb{R}(\sqrt[4]{-3})/\mathbb{R}$
v) $\mathbb{F}_7(t)/\mathbb{F}_7(t^2)$ vi) $\mathbb{F}_7(t)/\mathbb{F}_7$ vii) $\mathbb{Q}(\sqrt{5}, \sqrt[6]{5})/\mathbb{Q}$ viii) $\mathbb{Q}(\sqrt{5}, \sqrt[6]{5})/\mathbb{Q}(\sqrt{5})$

27. Probar que $\mathbb{Q}(\sqrt{7}, \sqrt[3]{7}, \ldots, \sqrt[n]{7}, \ldots)$ no es una extensión finita de $\mathbb{Q}$.

♡**28.** Probar que $A/\mathbb{Q}$ es una extensión infinita, donde $A \subset \mathbb{C}$ son los números algebraicos sobre $\mathbb{Q}$.

29. Demostrar que una extensión de grado primo es simple.

30. Si L/K es finita y P es un polinomio irreducible en $K[x]$, demostrar que si P tiene alguna raíz en L, entonces ∂P divide a $[L : K]$.

31. Si L/K es finita y $K \subset M \subset L$, probar que para cualquier $\alpha \in L$ se cumple $[M(\alpha) : M] \leq [K(\alpha) : K]$.

32. Sea $K(\alpha,\beta)$ una extensión algebraica de K, $n_\alpha = [K(\alpha):K]$, $n_\beta = [K(\beta):K]$ y $n = [K(\alpha,\beta):K]$.

i) Demostrar que $\text{mcm}(n_\alpha, n_\beta)|n$ y $n \leq n_\alpha \cdot n_\beta$. ¿Qué se puede decir si n_α y n_β son coprimos?

ii) Mostrar un ejemplo con $n_\alpha \neq n_\beta$ en el que se cumpla $n < n_\alpha \cdot n_\beta$.

33. Probar que L/K y M/L algebraicas, implica M/K algebraica.

34. Sea $a < 0$ un número real algebraico sobre $\mathbb{Q}$, y sea $p(x) \in \mathbb{Q}[x]$ el polinomio mínimo de a sobre $\mathbb{Q}$. Demostrar que $\sqrt{a}$ es también algebraico sobre $\mathbb{Q}$, y determinar su polinomio mínimo sobre $\mathbb{Q}$.

♡**35.** Sea F un cuerpo y sea $f(x) \in F[x]$ un polinomio no nulo. Probar que si a está en alguna extensión de F, y $f(a)$ es algebraico sobre F, entonces a es algebraico sobre F.

♡**36.** Sea β un cero de $f(x) = x^5 + 2x + 6$. Probar que ninguno de los números $\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}$ pertenece a $\mathbb{Q}(\beta)$.

♡**37.** Si α es trascendente sobre K, ¿cuál es el grado de $K(\alpha)/K$?

38. Probar que un polinomio mónico P (no constante) es el polinomio mínimo de α sobre $K[x]$ si y sólo si es irreducible y cualquier $Q \in K[x]$ con $Q(\alpha) = 0$ es divisible por P.

39. Hallar $[\mathbb{Q}(\sqrt[7]{2}, \sqrt[5]{3}) : \mathbb{Q}]$.

40. Si $[K(\alpha):K] = n$ y $P \in K[x]$ es el polinomio mínimo de α, indicar alguna base de $K[x]/\langle P\rangle$ sobre K.

41. Sean α y β en L/K tales que $[K(\alpha):K] = m$ y $[K(\beta):K] = n$. Demostrar que el grado del polinomio mínimo de β en $K(\alpha)$ es n si y sólo si el grado del polinomio mínimo de α en $K(\beta)$ es m.

42. Calcular el polinomio mínimo de $\sqrt{3} + \sqrt{5}$ en $\mathbb{Q}(\sqrt{15})$.

43. Sea α una raíz de $P = x^3 - x - 2 \in \mathbb{Q}[x]$. Escribir $(\alpha+1)/(\alpha-1)$ como una combinación lineal de 1, α y α^2.

44. Si $K(\alpha)/K$ es una extensión de grado tres, calcular $[K(\alpha^2):K]$. Suponiendo que el polinomio mínimo de α es $x^3 + x - 1$, hallar el polinomio mínimo de α^2.

♢**45.** Calcular el polinomio mínimo de $\sqrt[3]{9} + \sqrt[3]{3} - 1$.

46. Probar que $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

47. Calcular el grado del polinomio mínimo de $\cos(2\pi/p)$ sobre $\mathbb{Q}$ donde p es un primo. *Indicación*: Compárese la extensión correspondiente con $\mathbb{Q}\big(e^{2\pi i/p}\big)/\mathbb{Q}$.

48. Si n y m son enteros positivos libres de cuadrados (no divisibles por cuadrados distintos de 1^2), comparar los cuerpos $\mathbb{Q}(\sqrt{n}, \sqrt{m})$, $\mathbb{Q}(\sqrt{n} + \sqrt{m})$ y $\mathbb{Q}(\sqrt{nm})$.

49. Hallar el grado de la extensión $\mathbb{Q}\big(\sqrt{1+\sqrt{3}}\big)/\mathbb{Q}$.

50. Probar que $\mathbb{Q}(\alpha)/\mathbb{Q}$ es trascendente si y sólo si $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}$ lo es.

51. Sea $A \subset \mathbb{C}$ el cuerpo formado por todos los números algebraicos sobre $\mathbb{Q}$. Demostrar que todo polinomio no constante de $A[x]$ se descompone en factores lineales en este anillo.

52. Si α es trascendente sobre K, hallar $[K(\alpha) : K\big(\alpha^3/(\alpha+1)\big)]$.

♢**53.** Probar que $\mathbb{R}$ no es una extensión simple de $\mathbb{Q}$.

♢**54.** Sea α raíz de un polinomio irreducible $P = x^n - a_{n-1}x^{n-1} + \cdots + (-1)^{n-1}a_1x + (-1)^n a_0$ de grado n primo. Probar que si $\beta = Q(\alpha) \notin \mathbb{Q}$, entonces el polinomio mínimo sobre $\mathbb{Q}$ de β viene dado por el determinante

$$\det(xI - Q(A)) \qquad \text{donde} \qquad A = \begin{pmatrix} 0 & -1 & 0 & 0 & \dots & 0 \\ 0 & 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & 0 & -1 & \dots & 0 \\ \dots & & \dots & & \dots & \\ 0 & 0 & 0 & 0 & \dots & -1 \\ a_0 & a_1 & a_2 & a_3 & \dots & a_{n-1} \end{pmatrix}$$

Sección 2.3

55. Decir cuáles de las siguientes longitudes son construibles con regla y compás

$$\sqrt{\sqrt{2}+\sqrt{3}}, \qquad \sqrt[3]{7+5\sqrt{2}}, \qquad \sqrt{1+\sqrt{\sqrt{2}+\sqrt[3]{3}}}, \qquad e^{i\pi/8} + e^{-i\pi/8}.$$

56. Diseñar un método sencillo para construir la longitud $\sqrt{1+\sqrt{3}}/\sqrt{2}$ con regla y compás.

57. Probar que la distancia al origen de un punto construible, es construible.

58. Demostrar que los polígonos regulares inscritos en el círculo unidad de 7, 11, 13 y 19 lados no son construibles con regla y compás. *Indicación*: Considérese la extensión $\mathbb{Q}\big(e^{2\pi i/p}\big)/\mathbb{Q}$ con p primo.

59. ¿Algún cubo es duplicable? ¿Algún ángulo es trisecable?

60. ¿Es el pentágono regular construible con regla y compás? *Indicación*: Hallar $\cos(2\pi/5) + \cos(4\pi/5)$ y $\cos(2\pi/5) \cdot \cos(4\pi/5)$.

♢**61.** Crear un método para construir el pentágono regular.

62. Usando los principios de lo que más tarde sería la teoría de Galois, Gauss demostró (a los 19 años) que el valor de $\cos(2\pi/17)$ es

$$-\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34-2\sqrt{17}} + \frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}$$

Explicar por qué de esta fórmula se deduce que el polígono regular de 17 lados se puede construir con regla y compás. (Nota: Esta construcción geométrica es una de las pocas

que había escapado al ingenio de los antiguos geómetras griegos. Según se dice, Gauss mandó que fuera inscrita en su tumba).

63. Demostrar que si los polígonos regulares de n y m lados son construibles con regla y compás, también lo es el de $\mathrm{mcm}(n, m)$ lados. Concluir del ejercicio anterior que el polígono regular de 204 lados es construible con regla y compás.

64. Sea α la única raíz real positiva de $P = x^4 - 10x^3 + 26x^2 + 16x - 14$. Sabiendo que no existe $\mathbb{Q} \subsetneq M \subsetneq \mathbb{Q}(\alpha)$ tal que $M/\mathbb{Q}$ sea de grado 2, probar que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ pero α no es construible.

65. ¿Se puede triplicar el cubo?

66. ¿Se puede trisecar el ángulo de $\pi/2^n$ radianes?

67. Decir si las siguientes extensiones son algebraicas o trascendentes.

$$\mathbb{Q}(\pi, \sqrt{3})/\mathbb{Q}(\sqrt{3}), \qquad \mathbb{Q}(\sqrt{\pi})/\mathbb{Q}(\pi), \qquad \mathbb{Q}(e)/\mathbb{Q}(e^5 - e^3 + 7e^2 + 100e - 1).$$

68. Demostrar que si α y β son trascendentes sobre $\mathbb{Q}$, entonces $\alpha + \beta$ ó $\alpha \cdot \beta$ son trascendentes sobre $\mathbb{Q}$. Dar un contraejemplo a la implicación: α, β trascendentes $\Rightarrow$ $\alpha + \beta$ trascendente.

69. Responder a la siguiente crítica: El argumento para probar que el ángulo de $60°$ no se puede trisecar no es concluyente, porque sólo se demuestra que $(\cos 20°, \sin 20°)$ no es construible, y quizá haya algún otro punto distinto del origen) en la recta $u = x \tan 20°$ que sí sea construible, lo que permitiría la trisección.

70. Supongamos que disponemos de una regla curva cuyo borde tiene la forma de la gráfica de $y = x^3$ para $x \geq 0$. Esta regla está sin graduar (aunque tiene marcado el cero) y sólo puede ser usada para trazar la curva que une dos puntos construibles, uno de ellos situado en el origen de la regla. Demostrar que con regla, compás y regla curva se puede duplicar el cubo. ¿Se puede cuadrar el círculo? ¿Y trisecar el ángulo?

$\diamondsuit$**71.** Sea $P(x) = x^n(1-x)^n/n!$. Probar que si π^2 fuera una fracción con numerador a, entonces $E_n = a^n\pi \int_0^1 P(x) \operatorname{sen}(\pi x)\, dx$ sería un entero no nulo para todo n. Demostrar que $\lim E_n = 0$, llegando a una contradicción con que $\pi^2 \in \mathbb{Q}$.

Apéndice del Capítulo 2

Conoce a tus héroes

(Más información en: `http://turnbull.mcs.st-and.ac.uk/history/`)

Apellido: Gauss
Nombre: (Johann) Carl Friedrich
Nacimiento: 1777 Brunswick
Defunción: 1855 Göttigen

Casi siempre se incluye a C.F. Gauss en la subjetiva e hipotética tríada de los mejores matemáticos de todos los tiempos. No mostró interés en publicar rápidamente sus resultados, prefiriendo pulirlos al máximo de acuerdo con su lema *Pauca sed matura* (pocos pero maduros). En relación con el contenido de este curso, probó el teorema fundamental del álgebra, dio un criterio para la constructibilidad del polígono de n lados (para lo que tuvo que crear la teoría de Galois en un caso particular antes de que naciera Galois), se adelantó a la teoría de ideales de Kummer estudiando la teoría de formas cuadráticas (lo que le llevó a la clasificación de los grupos abelianos finitos antes de que fueran siquiera definidos). En el lado negativo, el trabajo sobre la imposibilidad de resolver la quíntica con radicales que le envió Abel en situación desesperada, apareció sin abrir siquiera a la muerte de Gauss.

Bla, bla, bla

- *Que este tema [los números complejos] haya estado rodeado hasta ahora de una misteriosa oscuridad debe ser atribuido en gran medida a una notación mal adaptada. Si por ejemplo, $+1$ y -1 y la raíz cuadrada de -1 hubieran sido llamadas unidades directa, inversa y lateral, en vez de positiva, negativa e imaginaria (o imposible), tal oscuridad podría haber desaparecido.* C.F. Gauss.

- *Cuéntase que uno de los antiguos poetas trágicos hacía aparecer en escena a Minos en el momento en que construía la tumba de Glauco, y al observar que sólo medía cien pies por cada lado, dijo: "Es un espacio muy pequeño para sepulcro de un rey. Duplicadla conservando su forma cúbica, duplicando el lado." Es evidente que se equivocaba, porque duplicando los lados de una figura plana se cuadruplica, mientras que una sólida se octuplica. Entonces se propuso a los geómetras la cuestión de duplicar una figura sólida dada conservando su forma, y este problema se llamó duplicación del cubo. [...] Se cuenta también que, más tarde, los de Delos; obligados por el oráculo a duplicar el altar, tropezaron con la misma dificultad, y entonces se enviaron embajadores a los geómetras que, con Platón, frecuentaban la Academia para que resolvieran la cuestión.* Eratóstenes, 276 a.C. - 194 a.C. (Véase [Ve]).

- *Ningún hombre de ciencia está obligado a resolver toda clase de dificultades que le planteen, sino sólo aquellas que son deducidas falsamente de los principios de la ciencia: no es de nuestra incumbencia refutar aquellas que no surgen de esa forma: así como el deber del geómetra es refutar la cuadratura del círculo por medio de segmentos, pero no es su trabajo refutar la prueba de Antifonte.* Aristóteles, "Física", Libro I.

¿Qué hay que saberse?

Todo lo que no esté en letra pequeña. Especialmente hay que saber calcular polinomios mínimos y grados de extensiones en casos como los descritos en este capítulo.

(PQR) Preguntón, quejoso y respondón

Q- El cálculo del grado en extensiones con radicales parece innecesariamente complicado. Está claro que si añadimos a $\mathbb{Q}$ una raíz cuadrada, la extensión será de grado 2; si añadimos otra distinta será de grado 4; con otra cúbica se tendría grado 12; etc.

R- Sin embargo $\left[\mathbb{Q}\left(\sqrt{2},(\sqrt{8}+1)^{-1}\right):\mathbb{Q}\right]=2$.

Q- Evidentemente porque $\sqrt{8}=2\sqrt{2}$ y entonces es la misma raíz.

R- Entonces, por ejemplo $\left[\mathbb{Q}\left(\sqrt{17+12\sqrt{2}}\right):\mathbb{Q}\right]=4$ y $\left[\mathbb{Q}\left(\sqrt{11+6\sqrt{2}}+\sqrt{11-6\sqrt{2}}\right):\mathbb{Q}\right]=16$, deben ser ciertas.

Q- Creo que sí. Bueno, en el segundo caso no lo veo bien porque quizá $11+6\sqrt{2}$ y $11-6\sqrt{2}$ tengan algo que ver por ser conjugados.

R- Pues los grados son 2 y 1 porque $17+12\sqrt{2}=(3+2\sqrt{2})^2$ y $\sqrt{11+6\sqrt{2}}+\sqrt{11-6\sqrt{2}}=6$.

Q- Pero eso es trampa, porque se puede simplificar.

R- En realidad, el cálculo de polinomios mínimos es una manera de comprobar si se puede simplificar y por tanto detecta las trampas. Los grados suelen coincidir con el productos de los índices de los radicales, pero no siempre, no podemos hacer un teorema de ello.

P- El cálculo de polinomios mínimos lleva al estudio de la irreducibilidad en ciertas extensiones, ¿cómo podemos llevarla a cabo? Parece muy difícil.

R- Y lo es. Ni siquiera en $\mathbb{Q}[x]$ hay un criterio sencillo e infalible.

Q- No me creo que las demostraciones de imposibilidad de los tres problemas clásicos, lo sean realmente. En realidad lo que hemos hecho es dar una definición de construible en términos de la teoría de cuerpos que ningún antiguo griego entendería ni podría considerar nunca como la auténtica definición.

R- Podríamos dar una definición inductiva como en [St] que no apela a la teoría de cuerpos y después deducir la nuestra. Lo fundamental es fijar en términos precisos qué es construir con regla y compás, porque en otro caso podríamos encontrar soluciones que ya los antiguos griegos consideraban ilícitas.

P- ¿Qué tipo de construcciones?

R- Por ejemplo algunas en las que se permite que la regla rote por un punto al tiempo que mide. Por dar una idea, el haz de rectas $y=-mx+1$ corta a la circunferencia unidad en un punto con $x=2m/(m^2+1)$ y al eje OX en $x=1/m$. Que la diferencia entre estas longitudes sea constante da lugar a una ecuación cúbica. Los antiguos griegos crearon algunas curvas mecánicas a través de estas construcciones ilícitas.