Tema 5.- Números algebraicos. Cuerpos de números. Grado.

5.1 Cuerpo de fracciones de un dominio.

Tratamos de generalizar la construcción de $\mathbb{Q}$, a partir de $\mathbb{Z}$.

Sea A un dominio de integridad. En $A \times (A \setminus \{0\})$ definimos la siguiente relación,

$$(a, b) \sim (a', b') \Leftrightarrow ab' - a'b = 0.$$

Utilizando la propiedad cancelativa en A, se prueba que la relación anterior es de equivalencia. A la clase de (a, b) la representamos por $\frac{a}{b}$, y al conjunto cociente $A \times (A \setminus \{0\})/\sim$ lo representamos por $Q(A)$.

Se definen en $Q(A)$ una suma y un producto de la siguiente manera:

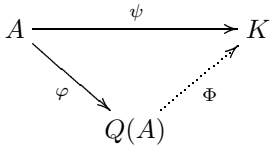
$$\begin{cases} \dfrac{a}{b} + \dfrac{a'}{b'} = \dfrac{ab' + a'b}{bb'} \\ \dfrac{a}{b} \cdot \dfrac{a'}{b'} = \dfrac{aa'}{bb'} \end{cases}$$

La comprobación de que están bien definidas es mecánica. También es muy fácil comprobar que $(Q(A), +, \cdot)$ es un cuerpo, con $\frac{0}{1}$, y $\frac{1}{1}$ como elemento nulo y unidad, respectivamente. Así mismo, se verifica que $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$, y $(\frac{a}{b})^{-1} = \frac{b}{a}$. En realidad todo el formalismo de los quebrados en $\mathbb{Q}$ es igualmente válido en $Q(A)$. A $Q(A)$ lo llamaremos *cuerpo de fracciones* de A, porque sus elementos son fracciones de elementos de A.

Proposición 5.1.1.– Sea A un dominio de integridad y $Q(A)$ su cuerpo de fracciones. Se verifica:

1. La aplicación $\varphi : A \to Q(A)$ definida por $\varphi(a) = \frac{a}{1}$ es un homomorfismo inyectivo de anillos.

2. (*Propiedad universal de* $Q(A)$) Si K es un cuerpo cualquiera, todo homomorfismo inyectivo de anillos $\psi : A \to K$ factoriza por φ, es decir, existe un único homomorfismo de anillos $\Phi : Q(A) \to K$ que hace conmutativo el siguiente diagrama:



   Es decir, $\Phi\varphi = \psi$.

3. Si L es un cuerpo que verifica la propiedad anterior de $Q(A)$, entonces L es isomorfo a $Q(A)$.

Se tiene, por tanto, que $Q(A)$ es el menor cuerpo que contiene a un dominio isomorfo a A, salvo isomorfismo. Dicho de otro modo, todo cuerpo que contiene a un dominio isomorfo a A, contiene también a un cuerpo isomorfo a $Q(A)$.

DEMOSTRACIÓN: El primer apartado es trivial. Para el segundo, definimos Φ mediante la expresión $\Phi(\frac{a}{b}) = \psi(a)\psi(b)^{-1}$. Hay que verificar que Φ está bien definida:

$$\frac{a}{b} = \frac{a'}{b'} \Rightarrow ab' = a'b \Rightarrow \psi(a)\psi(b') = \psi(a')\psi(b) \Rightarrow \psi(a)\psi(b)^{-1} = \psi(a')\psi(b')^{-1},$$

y que es un homomorfismo de anillos:

$$\begin{aligned}\Phi(\frac{a}{b} + \frac{a'}{b'}) &= \Phi(\frac{ab' + a'b}{bb'}) = \psi(ab' + a'b)\psi(bb')^{-1} = \\ &= \psi(a)\psi(b)^{-1} + \psi(a')\psi(b')^{-1} = \Phi(\frac{a}{b}) + \Phi(\frac{a'}{b'}),\end{aligned}$$

y análogamente conserva el producto y el elemento unidad. Se comprueba fácilmente que Φ hace conmutativo el diagrama, y de hecho es la única definición posible para que esto se cumpla, puesto que:

$$\Phi(\frac{a}{b}) = \Phi(\frac{a}{1} \cdot \frac{1}{b})) = \Phi(\frac{a}{1}) \cdot \Phi(\frac{1}{b}) = \Phi\varphi(a)\Phi\varphi(b)^{-1} = \psi(a)\psi(b)^{-1}.$$

Para la unicidad procedemos igual que hicimos en el tema 12, en la propiedad universal de los grupos libres. Sea L un cuerpo verificando la propiedad universal, con $\varphi' : A \to L$. Tomando $K = Q(A)$, existe $\phi' : L \to Q(A)$ tal que $\varphi = \phi'\varphi'$. Aplicando 2) a $K = L$ y φ', se tiene que $\varphi' = \Phi\varphi$. De ambas, se tiene $\varphi = \Phi'\Phi\varphi$. Pero aplicando 2) a $K = Q(A)$ y φ, se tiene que $\Phi'\Phi$ y la identidad hacen conmutativo el correspondiente diagrama; por la unicidad se tiene que $\Phi'\Phi = \mathrm{id}$. Análogamente se tiene que $\Phi\Phi' = \mathrm{id}$, luego Φ es el isomorfismo buscado. □

Ejemplo 5.1.2.–

1. Si A es un cuerpo, por la propiedad universal, se tiene que $Q(A) = A$.
2. Si $A = \mathbb{Z}$, la construcción hecha de $Q(A)$ conduce a $\mathbb{Q}$.
3. El cuerpo de fracciones de $\mathbb{Z}[i]$ es $\mathbb{Q}[i] = \{u+vi \in \mathbb{C}, \forall u, v \in \mathbb{Q}\}$. Identificar $\frac{a+bi}{c+di} \in Q(\mathbb{Z}[i])$ con $\frac{(a+bi)(c-di)}{c^2+d^2} = u + vi \in \mathbb{Q}[i]$, con $u = \frac{ac+bd}{c^+d^2} \in \mathbb{Q}$ y $v = \frac{bc-ad}{c^+d^2} \in \mathbb{Q}$.
4. Análogamente el cuerpo de fracciones de $\mathbb{Z}[\sqrt{m}]$, con m entero libre de cuadrados, es $\mathbb{Q}[\sqrt{m}] = \{u + v\sqrt{m} \in \mathbb{C}, \forall u, v \in \mathbb{Q}\}$.
5. El cuerpo de fracciones del anillo de polinomios $k[X]$ con coeficientes en un cuerpo k, es $k(X)$, conjunto de cocientes de polinomios en la variable X.

5.2 Característica de un cuerpo.

Sea K un cuerpo. Todo homomorfismo de anillos φ de $\mathbb{Z}$ en K, lleva el elemento unidad de $\mathbb{Z}$ en el elemento unidad de K. Como vimos en el ejemplo 10.2.3.5, esto define unívocamente a φ. Por tanto existe un único homomorfismo de anillos φ de $\mathbb{Z}$ en K.

Caso inyectivo Si el homomorfismo φ de $\mathbb{Z}$ en K es inyectivo, en la sección anterior hemos visto que entonces K contiene a $\mathbb{Q}$. En ese caso diremos que K es un cuerpo de *característica cero*. Los cuerpos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son de característica cero, puesto que contienen a $\mathbb{Z}$. Además todo subcuerpo K de $\mathbb{C}$ es de característica cero. En otro caso el homomorfismo $\varphi : \mathbb{Z} \to K$ no inyectivo se extiende a $\mathbb{C}$, contradicción. Por tanto, todo subcuerpo de $\mathbb{C}$ contiene a $\mathbb{Q}$.

Caso no inyectivo En ese caso, $\ker(\varphi)$ es un ideal $\mathbb{Z}p$, con $p > 0$. Por el primer teorema de isomorfía $\mathbb{Z}/\mathbb{Z}p$ es isomorfo a un subanillo de K, luego no tiene divisores de cero. Así $\mathbb{Z}/\mathbb{Z}p$ es un dominio de integridad, o equivalentemente un cuerpo, y además, p es un número primo. Diremos entonces que K es un cuerpo de *característica p*. En ese caso se verifica que $px = 0$, para cada $x \in K$.

Todos los cuerpos finitos son de característica positiva. Además si K es finito de característica $p > 0$, es un espacio vectorial de dimensión finita n sobre $\mathbb{Z}/\mathbb{Z}p$, por tanto, su cardinal es p^n.

5.3 Números algebraicos y trascendentes.

Definición 5.3.1.– Un número complejo α se dice *algebraico* (sobre $\mathbb{Q}$), si existe un polinomio $f(X) \in \mathbb{Q}[X]$ no nulo, con $f(\alpha) = 0$. Se dirá que α es *trascendente*, si no es algebraico.

En la definición anterior podemos suponer que $f(X) \in \mathbb{Q}[X]$ es mónico, es decir, de coeficiente líder igual a 1.

Ejemplo 5.3.2.–

1. Todos los números racionales son algebraicos.
2. Para cada $d \in \mathbb{Z}$ libre de cuadrados, $\sqrt{d}$ es algebraico.
3. Liouville (1844) fue el primero en encontrar un número trascendente:

$$\xi = \sum_{n=1}^{\infty} 10^{-n!} = 0.11000100000000000000000001...$$

4. Hermite (1873) probó que el número e es trascendente.
5. Lindemann demostró la trascendencia de π en 1882.
6. Cantor en 1874 probó la existencia de infinidad de números trascendentes, sin construirlos.

Proposición 5.3.3.– Sea $\alpha \in \mathbb{C}$, definimos $\mathbb{Q}[\alpha] = \mathrm{im}(\varphi)$, con $\varphi : \mathbb{Q}[X] \to \mathbb{C}$ definido por $\varphi(X) = \alpha$. Se verifica:

1. $\mathbb{Q}[\alpha]$ es la intersección de todos los subanillos de $\mathbb{C}$ que contienen a $\mathbb{Q}$ y a α.

2. α es trascendente si y sólo si φ es inyectivo.

3. α es algebraico si y sólo si $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha]$ es finita. A esta dimensión se le llama *grado de* α (sobre $\mathbb{Q}$).

DEMOSTRACIÓN: Las dos primeras afirmaciones son triviales. Para cada entero $n > 0$, sea $\mathbb{Q}[\alpha]_n$ el conjunto de polinomios en α, de grado menor o igual a n, con coeficientes racionales. Supongamos que $\alpha \in \mathbb{C}$ es algebraico, entonces existe un $f(X) \in \mathbb{Q}[X]$ mónico de grado $n > 0$, tal que $f(\alpha) = 0$; lo que implica que $\alpha^n \in \mathbb{Q}[\alpha]_{n-1}$. Por recurrencia, se tiene que $\mathbb{Q}[\alpha] \subset \mathbb{Q}[\alpha]_{n-1}$. De aquí que $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha] \leq n$.

Recíprocamente, sea $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha] = n$, entonces $\{1, \alpha, \ldots, \alpha^n\}$ son linealmente dependientes. Por tanto existen $a_i \in \mathbb{Q}$, $i = 0, \ldots, n$, no todos nulos, tales que $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$. Se tiene así que α es algebraico. □

Proposición 5.3.4.– Sea $\alpha \in \mathbb{C}$ algebraico de grado n.

1. Existe un único polinomio $f(X) \in \mathbb{Q}[X]$ mónico de grado n tal que $f(\alpha) = 0$.

2. Si $g(X) \in \mathbb{Q}[X]$ es otro polinomio tal que $g(\alpha) = 0$, entonces $f|g$.

3. f es irreducible en $\mathbb{Q}[X]$.

A $f(X)$ se le llama *polinomio mínimo de* α (sobre $\mathbb{Q}$).

DEMOSTRACIÓN: Si $\alpha \in \mathbb{C}$ algebraico, el homomorfismo $\varphi : \mathbb{Q}[X] \to \mathbb{Q}[\alpha]$ de la proposición anterior no es inyectivo. Como $\mathbb{Q}[X]$ es un dominio de ideales principales, existe un $f(X) \in \mathbb{Q}[X]$ mónico tal que $\ker(\varphi) = (f)$. Sea $\mathrm{gr}(f) = m$, entonces $\mathbb{Q}[\alpha] \subset \mathbb{Q}[\alpha]_{m-1}$. Por tanto $n = \dim_{\mathbb{Q}} \mathbb{Q}[\alpha] \leq \dim_{\mathbb{Q}} \mathbb{Q}[\alpha]_{m-1} \leq m$. Recíprocamente $\{1, \alpha, \ldots, \alpha^{m-1}\}$ son linealmente independientes. En efecto, si $a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1} = 0$, entonces $a_0 + a_1X + \ldots + a_{m-1}X^{m-1} \in \ker(\varphi)$; pero este polinomio es de menor grado que f, luego debe ser idénticamente nulo.

El segundo apartado es trivial.

Por último, si $f = f_1 f_2$ en $\mathbb{Q}[X]$, se tiene que $0 = f(\alpha) = f_1(\alpha)f_2(\alpha)$, y de aquí se deduce que algún f_i está en el $\ker(\varphi)$, luego es asociado a f. □

Corolario 5.3.5.– $\alpha \in \mathbb{C}$ es algebraico si y sólo si $\mathbb{Q}[\alpha]$ es un cuerpo. En ese caso, su cuerpo de fracciones $\mathbb{Q}(\alpha)$ coincide con él.

DEMOSTRACIÓN: Si $\alpha \in \mathbb{C}$ es algebraico y $g(\alpha) \in \mathbb{Q}[\alpha] \setminus \{0\}$, entonces $g(X) \notin \ker(\varphi)$. Por ser f irreducible y $g \notin (f)$, se tiene que $1 = \mathrm{m.c.d.}(f, g)$. Por la identidad de Bézout, existen $a, b \in \mathbb{Q}[X]$ con $1 = af + bg$. Aplicando φ a lo anterior, queda $1 = b(\alpha)g(\alpha)$. Así $b(\alpha) = g(\alpha)^{-1}$.

Recíprocamente, si $\alpha^{-1} = g(\alpha) \in \mathbb{Q}[\alpha]$, se tiene que $\alpha g(\alpha) - 1 = 0$. Luego α es algebraico. □

5.4 Clausura algebraica.

Definición 5.4.1.– Se llama *clausura algebraica de* $\mathbb{Q}$ al conjunto $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha\text{es algebraico}\}$.

Proposición 5.4.2.– $\overline{\mathbb{Q}} \subset \mathbb{C}$ es un cuerpo.

DEMOSTRACIÓN: A la vista del corolario anterior basta probar que $\overline{\mathbb{Q}}$ es un anillo. Para ello, sean $\alpha, \beta \in \overline{\mathbb{Q}}$. Ya vimos que $\mathbb{Q}[\alpha]$ tiene una base de la forma $\{1, \alpha, \ldots, \alpha^m\}$, para cierto m, y $\mathbb{Q}[\beta]$ tiene una base de la forma $\{1, \beta, \ldots, \beta^n\}$, para cierto n. Sea V el subespacio vectorial de $\mathbb{C}$ generado por $\{\alpha^i\beta^j, \forall i, j, 0 \leq i \leq m, 0 \leq j \leq n\}$. Se prueba fácilmente que $\mathbb{Q}[\alpha - \beta]$ y $\mathbb{Q}[\alpha\beta]$ están contenidos en V, luego son de dimensión finita, y por 5.3.3 $\alpha - \beta$ y $\alpha\beta$ están en $\overline{\mathbb{Q}}$. □

Corolario 5.4.3.– Si K es un subanillo de $\mathbb{C}$ que contiene a $\mathbb{Q}$, y $\dim_{\mathbb{Q}} K$ finita, entonces K es un cuerpo y $K \subset \overline{\mathbb{Q}}$.

DEMOSTRACIÓN: Sea $\alpha \in K$ no nulo, entonces $\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset K$. Luego $\alpha \in \overline{\mathbb{Q}}$, y $\alpha^{-1} \in \mathbb{Q}[\alpha] \subset K$. □

Proposición 5.4.4.– $\overline{\mathbb{Q}}$ es numerable. En consecuencia hay una infinidad no numerable de números trascendentes.

DEMOSTRACIÓN: Se comprueba que $\overline{\mathbb{Q}}$ es una unión numerable de conjuntos finitos. En efecto, $\mathbb{Q}$ es numerable, y el conjunto de polinomios de grado n en $\mathbb{Q}[X]$ es $\mathbb{Q}^{n+1}$ que es también numerable; el conjunto de soluciones de cada polinomio es finito. □

5.5 Cuerpos de números.

Sea $K \subset \mathbb{C}$ un subcuerpo, ya vimos en la sección 5.2 que $K \supset \mathbb{Q}$. Pondremos $[K : Q]$ para indicar la $\dim_Q K$, y a este valor lo llamaremos *grado de K sobre* $\mathbb{Q}$. En general, si $K \subset L \subset \mathbb{C}$ con K subcuerpo y L subanillo, entonces se dice *grado de L sobre K* a $[L : K] = \dim_K L$.

Proposición 5.5.1.– *Fórmula del grado.* Sea $k \subset K \subset L \subset \mathbb{C}$, siendo k, K subcuerpos y L subanillo. Entonces $[L : k] < +\infty$ si y sólo si $[L : K] < +\infty$ y $[K : k] < +\infty$. En ese caso $[L : k] = [L : K][K : k]$.

DEMOSTRACIÓN: Si $\{x_i\}_{i \in I}$ es una base de L sobre K, y $\{y_j\}_{j \in J}$ es una base de K sobre k, entonces $\{x_i y_j\}_{i \in I, j \in J}$ es una base de L sobre k. □

Definición 5.5.2.– Un *cuerpo de números* K es un subcuerpo de $\mathbb{C}$ de grado finito sobre $\mathbb{Q}$.

Nota 5.5.3.–

1. Un ejemplo de cuerpo de números es $\mathbb{Q}[\alpha]$, con α algebraico. Aunque en la proposición siguiente daremos otros ejemplos, un teorema de Noether nos dirá más adelante que éste es el único ejemplo de cuerpos de números.

2. En el corolario 5.4.3 hemos visto que los cuerpos de números están contenidos en $\overline{\mathbb{Q}}$.

3. Por el mismo resultado citado basta exigirle a K que sea subanillo, en vez de subcuerpo, para ser cuerpo de números.

Definición 5.5.4.– Sean $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, definimos $\mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ como la imagen de $\varphi : \mathbb{Q}[X_1, \ldots, X_n] \to \mathbb{C}$, con $\varphi(X_i) = \alpha_i$, para cada $i = 1, \ldots, n$.

Proposición 5.5.5.– K es un cuerpo de números si y sólo si existen $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ algebraicos tales que $K = \mathbb{Q}[\alpha_1, \ldots, \alpha_n]$. En ese caso, $\mathbb{Q}[\alpha_1, \ldots, \alpha_n] = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

Demostración: Si $K \subset \mathbb{C}$ es un cuerpo de números, por la proposición anterior, basta tomar una base de K como $\mathbb{Q}$-espacio vectorial. Recíprocamente, sean $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$. Hay que demostrar que $[\mathbb{Q}[\alpha_1, \ldots, \alpha_n] : \mathbb{Q}] < +\infty$. Lo haremos por inducción sobre n. Si $n = 1$ ya está visto. Supongamos que $[\mathbb{Q}[\alpha_1, \ldots, \alpha_{n-1}] : \mathbb{Q}] < +\infty$. En ese caso $\mathbb{Q}[\alpha_1, \ldots, \alpha_{n-1}] = \mathbb{Q}(\alpha_1, \ldots, \alpha_{n-1}) = L$. Por la fórmula del grado, basta ver que

$$[\mathbb{Q}[\alpha_1, \ldots, \alpha_n] : \mathbb{Q}[\alpha_1, \ldots, \alpha_{n-1}]] < +\infty.$$

Pero $\mathbb{Q}[\alpha_1, \ldots, \alpha_n] = L[\alpha_n]$, y como α_n es algebraico, un razonamiento análogo al de 5.3.3.3 prueba que $[L[\alpha_n] : L] < +\infty$. □