Vamos ver mais tarde técnicas para calcular o grau $[L : K]$ em certos casos importantes. Para já começamos com um resultado geral, que tem um papel nesta teoria análogo ao do Teorema de Lagrange na teoria dos grupos (finitos).

Teorema. [Teorema da Torre]
Sejam $M \supseteq L \supseteq K$ extensões sucessivas de um corpo K. Então

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

`[Note que o produto à direita é simplesmente uma multiplicação de cardinais; no caso de algum dos graus ser infinito, a fórmula significa que` $[M : K] = \infty$ `se e só se` $[M : L] = \infty$ `ou` $[L : K] = \infty$`]`

Demonstração. Seja $\{a_i\}_{i\in I}$ uma base do espaço vectorial L sobre K e seja $\{b_j\}_{j\in J}$ uma base do espaço vectorial M sobre L. Bastará provar que $\{a_i b_j\}_{i\in I, j\in J}$ é uma base do espaço vectorial M sobre K.

É claro que cada elemento $a_i b_j$ pertence a M, pois $a_i \in L \subseteq M$ e $b_j \in M$. Provemos que se trata de um conjunto de vectores linearmente independente sobre K:

Se

$$\sum_{i\in I, j\in J} \kappa_{ij} a_i b_j = 0,$$

com $\kappa_{ij} \in K$, isto significa que $\sum_{j\in J}\Big(\sum_{i\in I} \kappa_{ij} a_i\Big) b_j = 0$. Como cada $\sum_{i\in I} \kappa_{ij} a_i$ pertence a L e os b_j são linearmente independentes sobre L, então $\sum_{i\in I} \kappa_{ij} a_i = 0$ para qualquer $j \in J$. Mas os a_i são linearmente independentes sobre K e, portanto, $\kappa_{i,j} = 0$ para qualquer $i \in I$ e $j \in J$.

Finalmente, vejamos que se trata de um conjunto de geradores de M sobre K:

Seja $c \in M$. Então podemos escrever $c = \sum_{j\in J} l_j b_j$, onde $l_j \in L$, porque $\{b_j\}_{j\in J}$ é uma base de M sobre L. Mas, por sua vez, cada l_j é uma combinação linear $l_j = \sum_{i\in I} \kappa_{ij} a_i$, porque $\{a_i\}_{i\in I}$ é uma base de L sobre K. Consequentemente, $c = \sum_{i,j} \kappa_{ij} a_i b_j$. ∎

Note que $[L : K] = 1$ se e só se $L = K$. De facto, se $[L : K] = 1$, seja $\{a\}$ uma base do espaço L sobre K; como $1 \in L$, podemos escrever $1 = \kappa a$ para algum $\kappa \in K$, o que mostra que $a = \kappa^{-1} \in K$ e, consequentemente, que $L \subseteq K$. O recíproco é óbvio.

Seja L uma extensão de K. Se $S \subseteq L$ é um subconjunto, designamos por $K(S)$ a extensão de K *gerada* por S, ou seja, o *menor* subcorpo de L que contém $K \cup S$. É claro que $K(S)$ é uma extensão de K contida em L. Se $S = \{\theta_1, \ldots, \theta_n\}$ ou $S = \{\theta\}$, escrevemos simplesmente $K(\theta_1, \ldots, \theta_n)$ ou $K(\theta)$ em vez de $K(S)$. Neste último caso, $K(\theta)$ diz-se uma *extensão simples* de K.

Exemplos: (1) $\mathbb{R}(i) = \mathbb{C}$: Por definição, $\mathbb{R}(i)$ é o menor subcorpo de $\mathbb{C}$ que contém $\mathbb{R} \cup \{i\}$, em particular, $\mathbb{R}(i) \subseteq \mathbb{C}$. Como $\mathbb{R}(i)$ é um corpo terá que conter necessariamente todos os elementos da forma $a + ib$, com $a, b \in \mathbb{R}$. Portanto $\mathbb{C} \subseteq \mathbb{R}(i)$.

Se $z \in \mathbb{C}$ então z escreve-se na forma $a + ib$ com a e b únicos, o que implica que $\{1, i\}$ é uma base de $\mathbb{C}$ sobre $\mathbb{R}$. Logo $[\mathbb{C} : \mathbb{R}] = 2$. Como 2 é primo, segue do Teorema da Torre que se K é tal que $\mathbb{R} \subseteq K \subseteq \mathbb{C}$ então ou $[K : \mathbb{R}] = 1$ ou $[\mathbb{C} : K] = 1$, ou seja, $K = \mathbb{R}$ ou $K = \mathbb{C}$.

(2) $\mathbb{Q}(i) = \{a + ib : a, b \in \mathbb{Q}\} \subset \mathbb{C}$: Como $\mathbb{Q}(i)$ é um corpo, por definição, terá que conter necessariamente todos os elementos da forma $a + ib$, com $a, b \in \mathbb{Q}$. Quanto à inclusão recíproca, bastará assegurarmos que $\{a + ib : a, b \in \mathbb{Q}\}$ é um subcorpo de $\mathbb{C}$. Sejam $a + ib, c + id$ com $a, b, c, d \in \mathbb{Q}$. Não é difícil mostrar que $(a+ib)-(c+id)$ ainda pertence a $\{a+ib : a, b \in \mathbb{Q}\}$. Suponhamos que $c+id \neq 0$ (isto é, $c \neq 0$ ou $d \neq 0$). Então $c - id \neq 0$, pelo que

$$(a + ib)(c + id)^{-1} = \frac{a + ib}{c + id} = \frac{a + ib}{c + id}\,\frac{c - id}{c - id} = \frac{ac - bd}{c^2 + d^2} + i\frac{bc - ad}{c^2 + d^2}$$

ainda pertence a $\{a + ib : a, b \in \mathbb{Q}\}$.

É claro que, tal como no exemplo anterior, $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, sendo $\{1, i\}$ a base de $\mathbb{Q}(i)$ sobre $\mathbb{Q}$.

(3) Do mesmo modo que no exemplo anterior, pode provar-se que

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

e $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Neste caso a base é $\{1, \sqrt{2}\}$.

(4) Note que para o elemento $\sqrt[3]{2}$ ainda se tem $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\} \subseteq \mathbb{Q}(\sqrt[3]{2})$, mas desta vez não temos igualdade (o elemento $\sqrt[3]{4} = (\sqrt[3]{2})^2$ pertence a $\mathbb{Q}(\sqrt[3]{2})$ mas não pertence a $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\}$). Neste caso,

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$$

e $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

ELEMENTOS ALGÉBRICOS E TRANSCENDENTES

Seja L uma extensão de K e seja $\theta \in L$. Dizemos que θ é *algébrico sobre* K se existe um polinómio não-nulo $p(\boldsymbol{x}) \in K[x]$ tal que $p(\theta) = 0$. Caso contrário, dizemos que θ é *transcendente sobre* K.

Exemplos: (1) Se $\theta \in K$ então θ é raiz de $\boldsymbol{x} - \theta \in K[x]$ e portanto θ é algébrico sobre K.

(2) $\sqrt{2}$ e i são algébricos sobre $\mathbb{Q}$: $\sqrt{2}$ é raiz de $\boldsymbol{x}^2 - 2 \in \mathbb{Q}[x]$ e i é raiz de $\boldsymbol{x}^2 + 1 \in \mathbb{Q}[x]$.

(3) É um facto bem conhecido que os números reais π e e são ambos transcendentes sobre $\mathbb{Q}$, isto é, não existe nenhum polinómio $p(\boldsymbol{x}) \in \mathbb{Q}[x]$ que tenha π ou e por raiz. As demonstrações destes factos envolvem análise infinitesimal e devem-se originalmente a Lindemann (1882) e a Hermite (1873), respectivamente.

Mas é claro que π e e já são algébricos sobre $\mathbb{R}$.

EXTENSÕES ALGÉBRICAS E TRANSCENDENTES

Uma extensão L de K diz-se uma *extensão algébrica de* K se todos os elementos de L são algébricos sobre K. Caso contrário, dizemos que L é uma *extensão transcendente de* K.

Proposição. *Seja L uma extensão finita de K. Então L é algébrica sobre K.*

Demonstração. Suponhamos que $[L : K] = n \in \mathbb{N}$. Para cada $\theta \in L$, $\{1, \theta, \theta^2, \ldots, \theta^n\}$ é um conjunto linearmente dependente de L sobre K (pois tem $n+1$ vectores). Isso significa que existem $a_0, a_1, a_2, \ldots, a_n \in K$, não todos nulos, tais que

$$a_0 + a_1\theta + a_2\theta^2 + \cdots + a_n\theta^n = 0.$$

Então o polinómio

$$p(\boldsymbol{x}) = a_0 + a_1\boldsymbol{x} + a_2\boldsymbol{x}^2 + \cdots a_n\boldsymbol{x}^n \in K[x]$$

tem a raiz θ, o que mostra que θ é algébrico sobre K. ∎

Portanto, uma extensão transcendente é necessariamente de dimensão infinita.