1 Definició i operacions

Sigui K un cos commutatiu. Un *polinomi amb coeficients a* K és una successió $\{a_n\}$ d'elements de K que és nul·la d'un lloc en endavant: $\{a_n\} = \{a_0, a_1, a_2, \ldots\}$. Si $a_m \neq 0$ i $a_i = 0$ per $i > m$ diem que m és el *grau* del polinomi, i escrivim $m = \mathrm{gr}\{a_n\}$ (observem que el polinomi $\{0, 0, \ldots\}$ no té grau). Els termes a_i de la successió són els *coeficients* del polinomi; a_m és el *coeficient principal* o de major grau i a_0 el *terme independent*.

Anomenem $K[x]$ el conjunt de polinomis amb coeficients a K. Definim a $K[x]$ unes operacions *suma* i *producte* de la següent manera:

$$\{a_0, a_1, a_2, \ldots\} + \{b_0, b_1, b_2, \ldots\} = \{a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots\}$$

$$\{a_0, a_1, a_2, \ldots\} \cdot \{b_0, b_1, b_2, \ldots\} = \{a_0b_0, a_0b_1 + a_1b_0, \ldots, \textstyle\sum_{i+j=m} a_ib_j, \ldots\}$$

Aquestes operacions doten a $K[x]$ d'estructura d'anell commutatiu i unitari. L'element neutre de la suma és el $\{0, 0, \ldots\}$, i el del producte el $\{1, 0, \ldots\}$.

Definim també una operació externa, el *producte per escalars* de K: si $a \in K$ llavors

$$a \cdot \{a_0, a_1, a_2, \ldots\} = \{aa_0, aa_1, aa_2, \ldots\}$$

i aquesta operació verifica les quatre propietats que fan que, amb ella i la suma, $K[x]$ sigui un K-espai vectorial: per a tots $a, b \in K$, $\{a_n\}, \{b_n\} \in K[x]$, $(a + b)\{a_n\} = a\{a_n\} + b\{a_n\}$, $a(\{a_n\} + \{b_n\}) = a\{a_n\} + a\{b_n\}$, $a(b\{a_n\}) = (ab)\{a_n\}$, $1\{a_n\} = \{a_n\}$. Si en lloc de partir d'un cos K haguéssim partit d'un anell communitatiu i unitari A, tindríem que $A[x]$, amb aquestes operacions, és un A-mòdul.

Aquestes operacions ens permeten descomposar el polinomi $\{a_n\} = \{a_0, a_1, a_2, \ldots\}$ com

$$\{a_n\} = \{a_0, 0, \ldots\} + a_1\{0, 1, 0 \ldots\} + \cdots + a_n\{0, \ldots, 0, 1, 0, \ldots\} + \cdots$$

Ara bé, observem que $\{a_0, 0 \ldots\} + \{b_0, 0, \ldots\} = \{a_0 + b_0, 0, \ldots\}$ i també $\{a_0, 0 \ldots\} \cdot \{b_0, 0, \ldots\} = \{a_0b_0, 0, \ldots\}$, això és, els polinomis de grau 0 amb les operacions definides es comporten exactament igual que els elements de K, i podem definir l'homomorfisme injectiu $\phi : K \longrightarrow K[x]$ com $\phi(a) = \{a, 0, \ldots\}$. A la pràctica escriurem $a_0 = \{a_0, 0, \ldots\}$, pensant que K està immers en $K[x]$ de forma natural.

Si escrivim $x = \{0, 1, 0 \ldots\}$, llavors $x^2 = \{0, 0, 1, 0 \ldots\}$, i en general $x^n = \{\overbrace{0, \ldots, 0}^{n}, 1, 0, \ldots\}$, de forma que, amb aquestes notacions, la descomposició anterior s'escriu com

$$\{a_n\} = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots ,$$

on aquesta suma és finita, i d'ara endavant escriurem $a(x)$ en lloc de $\{a_n\}$ per referir-nos a aquest polinomi.

El grau d'un polinomi verifica dues propietats immediates de provar però importants:

- $\mathrm{gr}(p(x)+q(x)) \leq \max\{\mathrm{gr}(p(x)), \mathrm{gr}(q(x))\}$, amb igualtat quan $\mathrm{gr}(p(x)) \neq \mathrm{gr}(q(x))$ o bé quan $\mathrm{gr}(p(x)) = \mathrm{gr}(q(x))$ i els coeficients principals no són oposats,
- $\mathrm{gr}(p(x)q(x)) = \mathrm{gr}(p(x)) + \mathrm{gr}(q(x))$,

d'on es dedueixen altres propietats:

- *Llei de simplificació:* $a(x)p(x) = a(x)q(x) \ \Rightarrow\ p(x) = q(x)$ per a tot $a(x) \neq 0$. En efecte, aplicant la fórmula del grau del producte tenim que $\mathrm{gr}(a(x)) + \mathrm{gr}(p(x)) = \mathrm{gr}(a(x)) + \mathrm{gr}(q(x)) \Rightarrow \mathrm{gr}(p(x)) = \mathrm{gr}(q(x))$, i comparant els coeficients de $a(x)p(x)$ i $a(x)q(x)$ començant pel de major grau i descendint, tot aplicant la llei de simplificació a K, arribem a veure que tots coincideixen.
- *Absència de divisors de* 0 *no trivials:* si $p(x)q(x) = 0 \Rightarrow p(x) = 0$ o $q(x) = 0$, perquè si no fos així el seu producte tindria un grau ≥ 0 i per tant no seria el polinomi nul.
- *Els únics elements inversibles de* $K[x]$ *són els de grau* 0, ja que si $p(x)q(x) = 1 \Rightarrow \mathrm{gr}(p(x)) + \mathrm{gr}(q(x)) = 0$, i per tant tots dos tenen grau 0 (són elements de K).

2 Fórmula de Newton

Si $n, k \in \mathbb{N}$ amb $n \geq k$, el nombre combinatori $\binom{n}{k}$ es defineix com

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

i representa el nombre de subconjunts de k elements d'un conjunt de n (equivalentment, el nombre de formes diferents de triar k objectes d'un total de n). En efecte, si fem una tria ordenada de k elements d'un total de n, tenim n possibilitats per triar-ne el primer. Un cop triat, tenim $n-1$ per triar el segon, etc. En total tenim $n(n-1)\cdots(n-k+1) = n!/(n-k)!$ possibilitats per triar-ne els k. Com és una tria ordenada i en un subconjunt no importa l'ordre, de cada reordenació dels k elements en resulta el mateix subconjunt. Com hi ha $k!$ reordenacions possibles, dividint per aquest nombre obtenim el total de subconjunts, això és, $\frac{n!}{k!(n-k)!} = \binom{n}{k}$.

La fórmula de Newton, també coneguda com binomi de Newton o teorema del binomi, empra aquests nombres per calcular la potència d'un binomi:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

La demostració més senzilla usa un argument combinatori: el membre esquerre es un producte de n binomis $(x+y)$, i en desenvolupar-lo resultarà una suma de monomis de la forma $x^k y^{n-k}$. El monomi $x^k y^{n-k}$ apareixerà tants cops com formes diferents tinguem per a triar k lletres x del producte dels n binomis, és a dir, $\binom{n}{k}$, i això demostra la igualtat.

Leibniz generalitzà aquest resultat a un polinomi arbitrari (teorema multinomial):

$$(x_1 + \cdots + x_m)^n = \sum_{k_1+\cdots+k_m=n} \binom{n}{k_1\ k_2\ \cdots\ k_m} x_1^{k_1} \cdots x_m^{k_m},$$

on $\binom{n}{k_1\ k_2\ \cdots\ k_m} = \frac{n!}{k_1! \cdots k_m!}$, i el raonament és idèntic al de la fórmula de Newton.

3 Divisibilitat a $K[x]$

La teoria de la divisibilitat a $K[x]$ es basa en el següent resultat:

Teorema de la divisió entera. *Donats* $a(x), b(x) \in K[x]$, $b(x) \neq 0$, *existeixen* $q(x), r(x) \in K[x]$ *únics tals que* $a(x) = b(x)q(x) + r(x)$, *amb* $r(x) = 0$ *o* $\mathrm{gr}(r(x)) < \mathrm{gr}(b(x))$. $q(x)$ *i* $r(x)$ *s'anomenen respectivament el* quocient *i la* resta *de la divisió entera de* $a(x)$ *per* $b(x)$.

Demostració: Sigui $\mathrm{gr}(a(x)) = n$, $\mathrm{gr}(b(x)) = m$, això és, $a(x) = a_0 + a_1 x + \cdots + a_n x^n$ amb $a_n \neq 0$, i $b(x) = b_0 + b_1 x + \cdots + b_m x^m$ amb $b_m \neq 0$. Si $n < m$ tenim $q(x) = 0$ i $r(x) = a(x)$, i hem acabat. En cas contrari podem escriure

$$a(x) - b(x)\left(\frac{a_n}{b_m}\, x^{n-m}\right) = r_1(x)$$

amb $r_1(x) = 0$ o $\mathrm{gr}(r_1(x)) < n$. Si $r_1(x) = 0$ o bé $\mathrm{gr}(r_1(x)) < m$ posem $q(x) = \frac{a_n}{b_m}\, x^{n-m}$, $r(x) = r_1(x)$, i hem acabat. En cas contrari escrivim $r_1(x) = c_0 + c_1 x + \cdots + c_{n_1} x^{n_1}$ on $m \leq n_1 < n$, i posem

$$r_1(x) - b(x)\left(\frac{c_{n_1}}{b_m}\, x^{n_1-m}\right) = r_2(x) \ \Rightarrow\ a(x) = b(x)\left(\frac{a_n}{b_m}\, x^{n-m} + \frac{c_{n_1}}{b_m}\, x^{n_1-m}\right) + r_2(x)$$

amb $r_2(x) = 0$ o $\mathrm{gr}(r_2(x)) < n_1$. Si $r_2(x) = 0$ o bé $\mathrm{gr}(r_2(x)) < m$, hem acabat. En cas contrari tornem a repetir el procés, i com els graus dels $r_i(x)$ va disminuint arribarà un moment que el procés acabarà i haurem obtingut un $q(x)$ i un $r(x) = r_k(x)$.

Per veure la unicitat d'aquesta expressió suposem que $a(x) = b(x)q(x)+r(x) = b(x)q'(x)+r'(x)$, i escrivim $b(x)(q(x) - q'(x)) = r'(x) - r(x)$. Si fos $r'(x) - r(x) \neq 0$, tindríem $\mathrm{gr}(r'(x)-r(x)) < m$ mentre que $\mathrm{gr}(b(x)(q(x)-q'(x))) \geq m$, contradicció. Així, $r'(x) = r(x)$ i, per tant, també $q'(x) = q(x)$ en ser $b(x) \neq 0$. $\square$

Si la resta de la divisió entera de $a(x)$ per $b(x)$ és 0 diem que $b(x)$ *divideix* o és un *divisor* de $a(x)$, i escrivim $b(x)|a(x)$, o bé que $a(x)$ és un *múltiple* de $b(x)$. Notem per $(b(x))$ el conjunt de múltiples de $b(x)$.

Un *ideal* de $K[x]$ és un subconjunt no buit $I \subset K[x]$ que verifica: si $p(x), q(x) \in I$ i $s(x) \in K[x]$ llavors $p(x) + q(x) \in I$ i $p(x)s(x) \in I$. Per exemple, el conjunt $(b(x))$ és un ideal.

Proposició. *Tots els ideals $I \subset K[x]$ són de la forma $I = (b(x))$ per algun $b(x) \in K[x]$.*

Demostració: Si $I = \{0\}$ llavors $I = (0)$ i hem acabat. En cas contrari prenem $b(x) \in I$ de grau mínim. Per definició d'ideal tenim que $(b(x)) \subset I$. Per veure la inclusió en l'altre sentit, sigui $a(x) \in I$ i, pel teorema de la divisió entera, $a(x) = b(x)q(x) + r(x)$ amb $\mathrm{gr}(r(x)) < \mathrm{gr}(b(x))$ o $r(x) = 0$. Però $r(x) = a(x) - b(x)q(x) \in I$, i com $b(x)$ l'hem triat de grau mínim, ha de ser $r(x) = 0$ i per tant $a(x) \in (b(x)) \Rightarrow I \subset (b(x))$. $\square$

4 Mínim comú múltiple i màxim comú divisor a $K[x]$

Donats els polinomis $a_1(x), \ldots, a_n(x)$, la intersecció d'ideals $(a_1(x)) \cap \cdots \cap (a_n(x))$ és el conjunt de múltiples comuns a tots ells, i és clarament un ideal. Per la proposició anterior, $(a_1(x)) \cap \cdots \cap (a_n(x)) = (m(x))$ per un cert $m(x)$, que anomenem *mínim comú múltiple* de $a_1(x), \ldots, a_n(x)$, i escrivim $m(x) = \mathrm{mcm}(a_1(x), \ldots, a_n(x))$. En efecte, qualsevol altre $m'(x)$ múltiple comú dels $a_i(x)$ pertany a la intersecció, i per tant a $(m(x))$, de forma que $m(x)|m'(x)$.

La unió $(a_1(x)) \cup \cdots \cup (a_n(x))$ en general no és un ideal. El mínim ideal que conté aquesta unió ha de contenir totes les sumes de múltiples dels $a_i(x)$, això és, $\{a_1(x)c_1(x) + \cdots + a_n(x)c_n(x) \mid c_i(x) \in K[x]\}$, i aquest conjunt ja és un ideal de $K[x]$, que designarem per $(a_1(x), \ldots, a_n(x))$, i serà igual a $(d(x))$ per un cert $d(x) \in K[x]$. L'anomenem *màxim comú divisor* de $a_1(x), \ldots, a_n(x)$, perquè al ser $a_i(x) \in (d(x)) \Rightarrow d(x)|a_i(x)$ i si $d'(x)$ és un altre divisor comú a ells tindrem $(a_i(x)) \subset (d'(x)) \Rightarrow (d(x)) \subset (d'(x)) \Rightarrow d'(x)|d(x)$.

Observem que per a tot $k \in K$, $k \cdot m(x)$ i $k \cdot d(x)$ també són, respectivament, un mcm i un mcd de $a_1(x), \ldots, a_n(x)$, i que en la construcció del mcd hem obtingut la

Identitat de Bézout. *Si* $d(x) = \mathrm{mcd}(a_1(x), \ldots, a_n(x))$, *llavors existeixen* $c_1(x), \ldots, c_n(x) \in K[x]$ *tals que* $d(x) = a_1(x)c_1(x) + \cdots + a_n(x)c_n(x)$. □

A la pràctica, per calcular el mcd de dos polinomis emprem el següent resultat:

Proposició. *Si* $a(x), b(x) \in K[x]$ *i* $a(x) = b(x)q(x) + r(x)$ *és la divisió entera de* $a(x)$ *per* $b(x)$ *llavors* $\mathrm{mcd}(a(x), b(x)) = \mathrm{mcd}(b(x), r(x))$.

Demostració: És immediata a partir del fet que $(a(x), b(x)) = (b(x), r(x))$, perquè un element $a(x)c_1(x) + b(x)c_2(x) \in (a(x), b(x))$ es pot escriure com $b(x)(q(x)c_1(x) + c_2(x)) + r(x)c_1(x) \in (b(x), r(x))$, i recíprocament, $b(x)p_1(x) + r(x)p_2(x) \in (b(x), r(x))$ pot escriure's com $a(x)p_2(x) + b(x)(p_1(x) - q(x)p_2(x)) \in (a(x), b(x))$. □

L'*algorisme d'Euclides* a $K[x]$ consisteix a aplicar reiteradament aquesta proposició:

$$\mathrm{mcd}(a(x), b(x)) = \mathrm{mcd}(b(x), r(x)) = \mathrm{mcd}(r(x), r_1(x)) = \mathrm{mcd}(r_1(x), r_2(x)) = \cdots$$

on els $r_i(x)$ són les restes successives de la divisió entera de $r_{i-2}(x)$ per $r_{i-1}(x)$. Aquest procés és finit perquè els $r_i(x)$ van baixant de grau fins que s'arriba a $\mathrm{mcd}(r_{k-1}(x), r_k(x)) = \mathrm{mcd}(r_k(x), 0)$ i per tant $\mathrm{mcd}(a(x), b(x)) = r_k(x)$.

Per calcular el mcd de més de dos polinomis usem l'expressió $\mathrm{mcd}(a_1(x), \ldots, a_n(x)) = \mathrm{mcd}(\mathrm{mcd}(a_1(x), \ldots, a_{n-1}(x)), a_n(x))$ iterativament. Un cop desenvolupat l'algorisme d'Euclides, fent una substitució cap enrere obtenim la identitat de Bézout. En efecte, $r_k(x) = r_{k-2}(x) - r_{k-1}(x)q_k(x)$, però $r_{k-1}(x)$ també pot escriure's com una suma de múltiples de $r_{k-2}(x)$ i $r_{k-3}(x)$, i així successivament fins arribar a escriure'l com $a(x)c_1(x) + b(x)c_2(x)$.

Teorema d'Euclides. *Si* $a(x)|b(x)c(x)$ *i* $\mathrm{mcd}(a(x), b(x)) = 1$ *llavors* $a(x)|c(x)$.

Demostració: La identitat de Bézout ens permet escriure $a(x)r(x) + b(x)s(x) = 1$. Multiplicant per $c(x)$ tenim $a(x)c(x)r(x) + b(x)c(x)s(x) = c(x)$, i com $a(x)$ divideix els dos sumands, també divideix $c(x)$. □

Proposició. *Si* $m(x) = \mathrm{mcm}(a(x), b(x))$ *i* $d(x) = \mathrm{mcd}(a(x), b(x))$ *llavors* $m(x)d(x) = k\, a(x)b(x)$ *amb* $k \in K$.

Demostració: Posem $a(x) = d(x)a'(x)$, $b(x) = d(x)b'(x)$ i anem a veure que $d(x)a'(x)b'(x)$ és un mcm de $a(x), b(x)$. Que és múltiple comú és evident, i si $n(x)$ n'és un altre escrivim $n(x) = a(x)r(s) = b(x)s(x) \Rightarrow n(x) = a'(x)r(x) = b'(x)s(x)$. Així $a'(x)|b'(x)s(x)$ i $\mathrm{mcd}(a'(x), b'(x)) = 1$. Pel teorema d'Euclides, $a'(x)|s(x) \Rightarrow s(x) = a'(x)t(x)$ i per tant $n(x) = b(x)s(x) = d(x)b'(x)a'(x)t(x)$ és múltiple de $d(x)a'(x)b'(x)$. □

5 Polinomis irreductibles

Un polinomi $p(x)$ de grau no nul es diu *irreductible* o *primer* quan els seus únics divisors són k i $k \cdot p(x)$ per a tot $k \in K$. El teorema fonamental de l'àlgebra, que no demostrarem, afirma que els polinomis irreductibles de $\mathbb{C}[x]$ són els de grau 1:

Teorema fonamental de l'àlgebra. *Tot polinomi $p(x) \in \mathbb{C}[x]$, $\mathrm{gr}(p(x)) > 0$, té un zero.*

Tots dos enunciats són equivalents, perquè si $p(x)$ té grau > 1 i z és un zero de $p(x)$ llavors $(x-z)|p(x)$, i recíprocament, si $p(x)$ té un divisor irreductible $\alpha + \beta x$, tindrà el zero $-\alpha/\beta$.

Si ara $p(x) \in \mathbb{R}[x]$, amb $\mathrm{gr}(p(x)) = n > 1$, podem considerar-lo a $\mathbb{C}[x]$, i en virtud del teorema anterior tindrà n arrels repartides entre $\mathbb{R}$ i $\mathbb{C}$. Si $\alpha \in \mathbb{R}$ i $p(\alpha) = 0$ llavors $(x-\alpha)|p(x)$. Si $z \in \mathbb{C}$ i $p(z) = 0$, també $\bar{z}$ és una arrel de $p(x)$, perquè $p(\bar{z}) = \overline{p(z)} = \bar{0} = 0$, i aleshores $(x-z)(x-\bar{z})|p(x)$, però $(x-z)(x-\bar{z}) = x^2 - 2\mathrm{Re}(z)x + |z|^2 \in \mathbb{R}[x]$ i és clarament irreductible, perquè si no ho fos tindria un factor lineal i, en conseqüència, una arrel real. Per tant,

Teorema. *Els polinomis irreductibles de $\mathbb{R}[x]$ són de grau ≤ 2. Concretament, els irreductibles de grau 2 són de la forma $x^2 + bx + c$ amb $\Delta = b^2 - 4c < 0$.* □

Veiem ara, per a $K[x]$, el resultat equivalent al teorema fonamental de l'aritmètica a $\mathbb{Z}$:

Teorema. *Tot polinomi $a(x)$ de grau no nul és producte de polinomis irreductibles. A més, aquesta factorització és única llevat de l'ordre i de factors del cos K.*

DEMOSTRACIÓ: Si $a(x)$ és primer, hem acabat. Del contrari, sigui $p_1(x)$ un divisor de grau mínim de $a(x)$. Llavors $p_1(x)$ és primer, perquè si tingués un divisor no trivial seria de grau inferior a $p_1(x)$, i com també dividiria a $a(x)$ estaria en contradicció amb la tria que hem fet de grau mínim. Posem $a(x) = p_1(x)a_1(x)$. Si $a_1(x)$ és primer, hem acabat. Si no, sigui $p_2(x)$ un divisor de grau mínim de $a_1(x)$, que serà primer, i per tant $p(x) = p_1(x)p_2(x)a_2(x)$. Iterant el procés, que és finit en anar baixant de grau els $a_i(x)$, arribarem a $a_n(x) = p_n(x)$ primer, i per tant $p(x) = p_1(x) \cdots p_n(x)$.
Per veure ara la unicitat, suposem que $p_1(x) \cdots p_n(x) = q_1(x) \cdots q_m(x)$ són dues descomposicions de $a(x)$. Com els $p_i(x)$, $q_j(x)$ són primers, $\mathrm{mcd}(p_i(x), q_j(x)) = 1$ o bé coincideixen llevat d'un factor de K. Llavors $p_1(x)|q_1(x) \cdots q_m(x)$, i pot passar que $p_1(x) = k \cdot q_1(x)$ o bé $\mathrm{mcd}(p_1(x), q_1(x)) = 1$ i llavors, pel teorema d'Euclides, $p_1(x)|q_2(x) \cdots q_m(x)$. En tal cas repetim el raonament, i $p_1(x) = k \cdot q_2(x)$ o bé són coprimers i $p_1(x)|q_3(x) \cdots q_m(x)$. Iterant el procés acabem obtenint que $p_1(x)$ coincideix amb algun $q_j(x)$ llevat d'un factor $k \in K$ o bé $p_1(x)|q_{m-1}(x)q_m(x)$, i en aquest cas $p_1(x) = k \cdot q_{m-1}(x)$ o $p_1(x) = k \cdot q_m(x)$.
Per tant $q_1(x)$ coincideix, llevat d'un factor de K, amb un $q_j(x)$, que reordenant els $q_j(x)$ po-

dem suposar que és $q_1(x)$. Així, aplicant la llei de simplificació tenim que $p_2(x)\cdots p_n(x) = k\cdot q_2(x)\cdots q_m(x)$. Repetint el mateix argument per a $q_2(x)$ obtenim que coincideix amb un dels $q_j(x)$ llevat d'un factor de K, i així successivament. Si fos $n<m$ o $n>m$ arribaríem a les situacions $1 = k\cdot q_{n+1}(x)\cdots q_m(x)$, o $p_{m+1}(x)\cdots p_n(x) = k$ que són impossibles. Per tant $n = m$ i les dues descomposicions són úniques llevat de l'ordre i de factors de K. $\square$

6 Fraccions algebraiques

Considerem ara $p(x), q(x)$ amb $q(x)\neq 0$ i formem les parelles $(p(x), q(x)) \in K[x]\times K[x]^*$. Anomenem *fracció algebraica* a tota parella d'aquest tipus. En aquest conjunt definim la relació $(p(x), q(x)) \sim (p'(x), q'(x)) \Leftrightarrow p(x)q'(x) = q(x)p'(x)$, i és immediat comprovar que és d'equivalència. Formem llavors el conjunt de classes d'equivalència $(K[x]\times K[x]^*)/\sim$, que anomenarem $K(x)$. A cadascuna d'aquestes classes, fent un abús de llenguatge, la seguirem anomenant "fracció algebraica" (encara que en alguns textos s'anomenen *raons algebraiques*), i les escriurem com un quocient $p(x)/q(x)$, de forma que si $(p(x), q(x)) \sim (p'(x), q'(x))$ escriurem $p(x)/q(x) = p'(x)/q'(x)$. Anomenem *numerador* i *denominador* de la fracció als polinomis $p(x)$ i $q(x)$, respectivament.

Donada la fracció $p(x)/q(x)$, sempre procurarem triar un representant el més senzill possible. Diem que $(p(x), q(x))$ és una fracció *irreductible* si $\mathrm{mcd}(p(x), q(x)) = 1$. Així, si $d(x)$ és un divisor comú de $p(x)$ i $q(x)$, escrivim $p(x) = d(x)p'(x)$, $q(x) = d(x)q'(x)$ i llavors $p(x)/q(x) = p'(x)/q'(x)$. En particular, si $d(x) = \mathrm{mcd}(p(x), q(x))$, el representant $(p'(x), q'(x))$ és irreductible.

Definim ara unes operacions *suma* i *producte* a $K(x)$:

$$\frac{p(x)}{q(x)} + \frac{r(x)}{s(x)} = \frac{p(x)s(x) + q(x)r(x)}{q(x)s(x)} \quad , \quad \frac{p(x)}{q(x)}\cdot\frac{r(x)}{s(x)} = \frac{p(x)r(x)}{q(x)s(x)}.$$

És fàcil veure que aquesta definició és consistent, això és, que no depèn dels representants escollits per a cada fracció. La suma verifica les propietats associativa i commutativa, l'element neutre és el $0/1$ i l'oposat de $p(x)/q(x)$ és $-p(x)/q(x)$. El producte també és associatiu i commutatiu i té la propietat distributiva amb la suma; l'element neutre és el $1/1$ i si $p(x)/q(x)\neq 0/1$ el seu invers és $q(x)/p(x)$. Amb tot això tenim que $(K(x), +, \cdot)$ és un cos, i $K[x]\subset K(x)$ de forma natural, identificant $p(x)$ amb $p(x)/1$.

Considerem ara el cos $\mathbb{R}(x)$ de les fraccions algebraiques a coeficients reals, i veiem un parell de resultats que ens permetran expressar una fracció com a suma de fraccions més senzilles. L'anomenarem *descomposició en fraccions simples*. Observem primer que si $\mathrm{gr}(p(x)) \geq \mathrm{gr}(q(x))$ podem fer la divisió entera i $p(x) = q(x)c(x) + r(x)$ i llavors $p(x)/q(x) =$

$c(x) + r(x)/q(x)$ amb $\mathrm{gr}(r(x)) < \mathrm{gr}(q(x))$. A $c(x)$ se l'anomena la *part entera* de la fracció $p(x)/q(x)$.

Proposició. *Sigui $p(x)/q(x) \in \mathbb{R}(x)$ amb $\mathrm{gr}(p(x)) < \mathrm{gr}(q(x))$ i sigui $\alpha \in \mathbb{R}$ una arrel de $q(x)$ de multiplicitat m, això és, $q(x) = (x-\alpha)^m q'(x)$ amb $q'(\alpha) \neq 0$. Llavors $p(x)/q(x)$ s'expressa de forma única com*

$$\frac{p(x)}{q(x)} = \frac{a}{(x-\alpha)^m} + \frac{b(x)}{(x-\alpha)^{m-1}q'(x)}$$

on $a \in \mathbb{R}$ i $\mathrm{gr}(b(x)) < \mathrm{gr}((x-\alpha)^{m-1}q'(x))$.

Demostració: L'expressió de l'enunciat és equivalent a $p(x) = a \cdot q'(x) + b(x)(x-\alpha)$. Si donem a x el valor α obtenim $a = p(\alpha)/q'(\alpha)$, i escollint aquest valor per a obtenim

$$b(x) = \frac{p(x) - \frac{p(\alpha)}{q'(\alpha)}\, q'(x)}{x-\alpha}$$

que verifica la condició de l'enunciat. Amb això provem l'existència i, per construcció, la unicitat de l'expressió, i tenim un mètode per calcular a i $b(x)$. □

Proposició. *Sigui $p(x)/q(x) \in \mathbb{R}(x)$ amb $\mathrm{gr}(p(x)) < \mathrm{gr}(q(x))$ i $q(x) = (x^2+tx+s)^m q'(x)$, on x^2+tx+s és irreductible a $\mathbb{R}[x]$ i no divideix a $q'(x)$. Llavors $p(x)/q(x)$ s'expressa de forma única com*

$$\frac{p(x)}{q(x)} = \frac{ax+b}{(x^2+tx+s)^m} + \frac{c(x)}{(x^2+tx+s)^{m-1}q'(x)}$$

on $a, b \in \mathbb{R}$ i $\mathrm{gr}(c(x)) < \mathrm{gr}((x^2+tx+s)^{m-1}q'(x))$.

Demostració: L'expressió de l'enunciat equival a $p(x) = (ax+b)q'(x) + c(x)(x^2+tx+s)$. Si ω i $\bar{\omega}$ són els zeros complexos de x^2+tx+s llavors $p(\omega) = (a\omega+b)q'(\omega)$ i $p(\bar{\omega}) = (a\bar{\omega}+b)q'(\bar{\omega})$ on $q'(\omega) \neq 0$ i $q'(\bar{\omega}) \neq 0$ per hipòtesi. Posant llavors $\alpha = p(\omega)/q'(\omega)$ i $\bar{\alpha} = p(\bar{\omega})/q'(\bar{\omega})$, el sistema format per les equacions $a\omega + b = \alpha$ i $a\bar{\omega} + b = \bar{\alpha}$ té solucions reals

$$a = \frac{\alpha - \bar{\alpha}}{\omega - \bar{\omega}} = \frac{\mathrm{Im}(\alpha)}{\mathrm{Im}(\omega)} \quad , \quad b = \frac{\bar{\alpha}\omega - \alpha\bar{\omega}}{\omega - \bar{\omega}} = \frac{\mathrm{Im}(\bar{\alpha}\omega)}{\mathrm{Im}(\omega)}.$$

Prenent llavors aquests valors per a, b posem

$$c(x) = \frac{p(x) - (ax+b)q'(x)}{x^2+tx+s}$$

que verifica les condicions de l'enunciat. □

Sabent que els polinomis irreductibles de $\mathbb{R}[x]$ són, com a molt, de grau 2, la reiteració d'aquests dos resultats ens dóna una descomposició de qualsevol $p(x)/q(x) \in \mathbb{R}(x)$ com suma de fraccions simples: si factoritzem $q(x)$,

$$q(x) = (x-\alpha_1)^{m_1} \cdots (x-\alpha_r)^{m_r}(x^2+t_1x+s_1)^{n_1} \cdots (x^2+t_kx+s_k)^{n_k}$$

llavors $p(x)/q(x)$ admet la descomposició única

$$\begin{aligned}\frac{p(x)}{q(x)} &= p_1(x) + \frac{a_1^1}{x-\alpha_1} + \cdots + \frac{a_1^{m_1}}{(x-\alpha_1)^{m_1}} + \cdots + \frac{a_r^1}{x-\alpha_r} + \cdots + \frac{a_r^{m_r}}{(x-\alpha_r)^{m_r}} + \\ &+ \frac{b_1^1x+c_1^1}{x^2+t_1x+s_1} + \cdots + \frac{b_1^{n_1}x+c_1^{n_1}}{(x^2+t_1x+s_1)^{n_1}} + \cdots + \frac{b_k^1x+c_k^1}{x^2+t_kx+s_k} + \cdots + \frac{b_k^{n_k}x+c_k^{n_k}}{(x^2+t_kx+s_k)^{n_k}},\end{aligned}$$

que és especialment útil per al càlcul de primitives de funcions racionals.