APUNTS D'ÀLGEBRA COMPUTACIONAL: (CAPÍTOL 1)

IDEALS, POLINOMIS, FACTORITZACIÓ ÚNICA I VARIETATS AFINS

A. MONTES

Date: 24 d'abril de 2001.

1. Anells, Ideals

Definició 1.1 (Anell). Un **anell** $\mathcal{R}$ és un grup abelià amb una operació $(a,b) \mapsto ab$ anomenada multiplicació i un "element identitat" 1, que, per tot $a, b, c \in \mathcal{R}$ verifica

$$\begin{array}{rcll} a(bc) & = & (ab)c & \text{(associativa)} \\ a(b+c) & = & ab+ac & \\ (b+c)a & = & ba+ca & \text{(distributiva)} \\ 1\,a & = & a\,1 = a & \text{(identitat)} \end{array}$$

Si a més a més cumpleix per tot $a, b \in \mathcal{R}$ és $ab = ba$, direm que $\mathcal{R}$ és un **anell commutatiu**. En aquest curs tots els anells que apareixeran seran commutatius.

Una **unitat** o **element invertible** d'un anell $\mathcal{R}$ és un element u pel qual existeix un element $v \in \mathcal{R}$, tal que $u\,v = 1$.

Exercici 1.2. Proveu que

a) si un element $u \in \mathcal{R}$ té invers, llavors és únic; es denota $v = u^{-1}$, i s'anomena **invers** de u;
b) el conjunt de les unitats de $\mathcal{R}$ és un grup multiplicatiu.

Un **cos** és un anell pel qual $1 \neq 0$, i tot element no nul és invertible. Denotem $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ per designar respectivament l'anell dels enters i els cossos dels racionals, reals i complexos.

Un **subanell** de $\mathcal{R}$ és un subconjunt tancat per suma, resta i multiplicació que conté la identitat de $\mathcal{R}$.

Definició 1.3 (Ideal). Un **ideal** d'un anell commutatiu $\mathcal{R}$ és un subgrup $\mathcal{I}$ tal que per tot $r \in \mathcal{R}$ i $s \in \mathcal{I}$ es verifica $r\,s \in \mathcal{I}$

Direm que

$$\langle S \rangle = \{\sum_1^n r_i\,s_i : \ r_i \in \mathcal{R},\ s_i \in S,\ n \geq 1\}$$

és l'**ideal generat** per un subconjunt $S \subseteq \mathcal{R}$. Si S és un subconjunt finit $S = \{s_1, \ldots, s_n\}$, llavors escriurem $\langle S \rangle = \langle s_1, \ldots, s_n \rangle$. Convindrem que l'ideal generat pel conjunt buit és el l'ideal $\{0\}$.

Exercici 1.4. Proveu que $\langle S \rangle$ és el mínim ideal que conté S.

Si $\mathcal{I} = \langle S \rangle$ direm que S és un **conjunt de generadors** o una **base** de $\mathcal{I}$.

Un **ideal principal** és un ideal que té una base formada per un únic element: $\mathcal{I} = \langle h \rangle$.

Definició 1.5 (Suma i Producte d'Ideals)**.** Donats dos ideals $\mathcal{I}, \mathcal{J}$ d'un anell $\mathcal{R}$, definim les operacions **suma** i **producte** per

$$\begin{aligned}\mathcal{I} + \mathcal{J} &= \{a + b \ : \ a \in \mathcal{I}, b \in \mathcal{J}\} \\ \mathcal{I} \cdot \mathcal{J} &= \left\{\sum_{k=1}^{n} a_k\, b_k : \ n \geq 1, \ a_k \in \mathcal{I}, \ b_k \in \mathcal{J}\right\}\end{aligned}$$

Més en general, si tenim una col·lecció d'ideals $\{\mathcal{I}_i : i \in I\}$, definim la suma de tots ells

$$\sum_{i \in I} \mathcal{I}_i = \left\{\sum_{j=1}^{n} a_j \ : \ n \geq 1, \ a_j \in \mathcal{I}_{i_j}, \ i_j \in I\right\}$$

Exercici 1.6. Proveu les afirmacions següents: La intersecció (finita o infinita) d'ideals és ideal i el producte finit d'ideals és ideal. La suma (finita o infinita) d'ideals és el mínim ideal que els conté a tots ells. La reunió d'ideals és ideal en general?

Proposició 1.7. *Si $\mathcal{I}$ i $\mathcal{J}$ són ideals de $\mathcal{R}$, llavors $\mathcal{I} \cdot \mathcal{J} \subseteq \mathcal{I} \cap \mathcal{J}$.*

Demostració. Si $a \in \mathcal{I} \cdot \mathcal{J}$, llavors $a = \sum_i b_i\, c_i$, on $b_i \in \mathcal{I}$ i $c_i \in \mathcal{J}$. Per ser $\mathcal{I}, \mathcal{J}$ ideals, cada producte $b_i\, c_i$ pertany a $\mathcal{I}$ i a $\mathcal{J}$ i per tant a la intersecció $I \cap \mathcal{J}$. Per tant, $a = \sum_i b_i\, c_i$ també pertany a $I \cap \mathcal{J}$. □

Proposició 1.8. *Si $\mathcal{I} = \langle a_1, \dots, a_n \rangle$, i $\mathcal{J} = \langle b_1, \dots, b_m \rangle$, llavors:*
(i) $\mathcal{I} + \mathcal{J} = \langle a_1, \dots, a_n, b_1, \dots, b_m \rangle$
(ii) $\mathcal{I} \cdot \mathcal{J} = \langle \{a_r\, b_s : \ 1 \leq r \leq n, \ 1 \leq s \leq m\} \rangle$

En canvi ho hi ha una expressió evident de la intersecció en termes dels generadors corresponents.

Exercici 1.9. Proveu la proposició anterior.

Definició 1.10 (Ideal primer)**.** Direm que un **ideal** $\mathcal{I}$ de un anell commutatiu $\mathcal{R}$ és **primer** si $\mathcal{I} \neq \mathcal{R}$ (diem, llavors, que és un **ideal propi**) i si $a, b \in \mathcal{R}$ i $a\, b \in \mathcal{I}$ implica que $a \in \mathcal{I}$ o $b \in \mathcal{I}$.

Exercici 1.11. Proveu que l'ideal $\mathcal{I}$ és primer ssi per qualssevols dos ideals $\mathcal{J}, \mathcal{K}$ tals que $\mathcal{J}\, \mathcal{K} \subseteq \mathcal{I}$ implica que $\mathcal{J} \subseteq \mathcal{I}$ o $\mathcal{K} \subseteq \mathcal{I}$.

Exercici 1.12. Proveu, per inducció sobre n que si $\mathcal{I}$ és primer i conté un producte d'ideals $\mathcal{J}_1\, \mathcal{J}_2 \dots, \mathcal{J}_n \subseteq \mathcal{I}$, llavors conté algún dels $\mathcal{J}_i$.

Definició 1.13 (Ideal maximal)**.** Un **ideal** $\mathcal{P}$ de $\mathcal{R}$ és **maximal** si és un ideal propi no contingut estrictament en cap altre ideal propi.

Donats $a, b \in \mathcal{R}$, diem que b divideix a (notació: $b \mid a$), si existeix $c \in \mathcal{R}$ tal que $a = b\, c$.

Un **divisor de zero** és un element no nul $r \in \mathcal{R}$ tal que per algún $s \in \mathcal{R}$ no nul es verifica $r\, s = 0$.

Definició 1.14 (Domini)**.** Un **domini** és un anell $\mathcal{R}$ sense divisors de zero, o el que és equivalent, si $\{0\}$ és primer.

Exercici 1.15. Proveu que $\mathcal{R}$ és un domini ssi $a\,b = a\,c,\ a \neq 0 \Longrightarrow b = c$.

Exercici 1.16. Donats un anell commutatiu $\mathcal{R}$ i un ideal $\mathcal{I} \subseteq \mathcal{R}$, proveu que si en el grup quocient $\mathcal{R}/\mathcal{I}$ definit per

$$\begin{aligned} [a]_{\mathcal{I}} &= \{b:\ b \in \mathcal{R},\ b - a \in \mathcal{I}\} \\ [a]_{\mathcal{I}} + [b]_{\mathcal{I}} &= [a+b]_{\mathcal{I}} \\ \mathcal{R}/\mathcal{I} &= \{[a]_{\mathcal{I}}:\ a \in \mathcal{R}\} \end{aligned}$$

afegim la multiplicació definida de forma natural per

$$[a]_{\mathcal{I}} \cdot [b]_{\mathcal{I}} = [a\,b]_{\mathcal{I}}$$

és un anell, que anomenem quocient.

Nota: Cal provar que les operacions estan ben definides i que tenen les propietats d'anell commutatiu.

Proposició 1.17. *$\mathcal{P} \subseteq \mathcal{R}$ és un ideal primer ssi $R/\mathcal{P}$ és un domini.*

Proposició 1.18. *$\mathcal{P} \subseteq \mathcal{R}$ és un ideal maximal ssi $\mathcal{R}/\mathcal{P}$ és un cos.*

Corol·lari 1.19. *Tot ideal maximal és primer.*

Exercici 1.20. Proveu les proposicions 1.17 i 1.18 i el corol·lari 1.19

Definició 1.21 (Element primer)**.** Un **element** $a \in \mathcal{R}$ no nul és **primer** si no és una unitat i si a divideix un producte $b\,c$ llavors a divideix a un dels factors b o c.

Exercici 1.22. Proveu que $a \neq 0$ és primer ssi genera un ideal primer.

Definició 1.23 (Element irreductible)**.** Un **element** $a \in \mathcal{R}$ és **irreductible** si no es pot descomposar en producte $b\,c$ d'elements b, c no unitaris.

Proposició 1.24. *Si $\mathcal{R}$ és un domini, tot primer $p \in \mathcal{R}$ és irreductible.*

Demostració. Si p és primer i $p = u\,v$, llavors $p \mid u$ o $p \mid v$. Ara bé,

$$p \mid u \quad \Rightarrow \quad \exists q \in \mathcal{R},\ q\,p = u \Rightarrow pqv = uv = p \Rightarrow qv = 1 \Rightarrow v \text{ és una unitat.}$$

Anlogament $p \mid v \Rightarrow u$ és una unitat. Per tant p és irreductible. □

2. Dominis Euclidians i PID's

Definició 2.1 (PID = Principal Ideal Domain)**.** Un domini tal que tots els seus ideals són principals diem que és un **domini d'ideals principals** o PID.

Definició 2.2 (Domini Euclidià)**.** [1] Un domini $\mathcal{R}$ és Euclidià si existeix una aplicació de $g:\ \mathcal{R} - \{0\} \to \mathbb{N}$, que anomenem norma, amb la propietat següent:

[1]Usualmet se sol afegir la hipòtesi que si $a, b \in \mathcal{R}$ i $a \neq 0$, $b \neq 0$, llavors $g(ab) \geq g(a)$, pero aquí no ens cal

Donats $a, b \in \mathcal{R}$, amb $b \neq 0$, existeix una expressió

$$a = bq + r$$

on, o bé $r = 0$, o be $g(r) < g(b)$.

Proposició 2.3. *Tot domini Euclidià $\mathcal{R}$ és un domini d'ideals principals.*

Demostració. Sigui $\mathcal{I}$ un ideal de $\mathcal{R}$, que podem suposar $\mathcal{I} \neq \{0\}$. Prenem $a \neq 0$ un element de $\mathcal{I}$ tal que $g(a)$ sigui mínim i veiem que $\mathcal{I} = \langle a \rangle$. Sigui $b \in \mathcal{I}$, $b \neq 0$. Per ser Euclidià, $b = aq + r$ i, o bé $r = 0$ o bé $g(r) < g(a)$. El segon és impossible perquè $r = b - aq \in \mathcal{I}$ i per l'elecció de a, $g(a)$ és mínim. Per tant $r = 0$, i $b \in \langle a \rangle$. $\square$

Exercici 2.4. Proveu que l'anell $\mathbb{Z}$ dels enters amb la norma donada pel valor absolut i la divisió ordinària és un domini Euclidià. És única la divisió?

Exercici 2.5. Proveu que l'anell $K[x]$ dels polinomis d'una variable sobre un cos k també és euclidià amb la norma donada pel grau del polinomi i la divisió ordinària. És única la divisió?

Exercici 2.6. En canvi $K[x, y]$ no és Euclidià. Observem que si volguessim emprar la mateixa forma de divisió que a $K[x]$ a l'intentar dividir $a = xy^3$ per $b = x^2y$, sigui quin sigui el quocient, no es possible cancel·lar el terme xy^3, i així el residu tindria grau total més gran que el de b. Proveu que $k[x, y]$ no és un PID ja que l'ideal $\langle x, y \rangle$ no admet un únic generador.

Definició 2.7 (gcd)**.** Donats dos elements a, b d'un domini $\mathcal{R}$, definim un $\gcd(a, b)$ com un element $d \in \mathcal{R}$ tal que

(i) $d \mid a$ i $d \mid b$.
(ii) Si $p \in \mathcal{R}$ és tal que $p \mid a$ i $p \mid b$, llavors $p \mid d$

Observació 2.8. El $\gcd(a, b)$ si existeix és únic tret de multiplicació per una unitat, ja que si n'hi hagués dos d_1, d_2 es tindria $d_1 \mid d_2$ i $d_2 \mid d_1$, i per tant $d_1 = u\, d_2$ on u és una unitat. Quan el $\gcd(a, b)$ és una unitat, ho escriurem $\gcd(a, b) = 1$.

Proposició 2.9 (Identitat de Bézout)**.** *Si $\mathcal{R}$ és un* PID*, cada parell d'elements a, b té un* $\gcd(a, b)$*, i es verifica una identitat de Bézout de la forma*

$$Aa + Bb = \gcd(a, b), \quad amb \quad A, B \in \mathcal{R}$$

Demostració. L'ideal $\langle a, b \rangle$ és principal, per ser $\mathcal{R}$ un PID. Sigui h el seu generador. Veiem que h és el $\gcd(a, b)$. En efecte: Com que $a \in \langle h \rangle$ i $b \in \langle h \rangle$ es cumpleix la condició (i) de gcd. Si $p \mid a$ i $p \mid b$, llavors $a, b \in \langle p \rangle$ i per tant $h \in \langle a, b \rangle \subseteq \langle p \rangle$. Així $p \mid h$. De $\langle h \rangle = \langle a, b \rangle$ en surt la identitat de Bézout. $\square$

Observació 2.10. En un PID no tenim en general un algorisme per determinar el gcd, mentre que un anell Euclidià tenim l'algorisme d'Euclides.

Definició 2.11 (lcm)**.** Donats dos elements a, b d'un domini $\mathcal{R}$, definim un $\mathrm{lcm}(a, b)$ com un element $m \in \mathcal{R}$ tal que

(i) $a \mid m$ i $b \mid m$.
(ii) Si $p \in \mathcal{R}$ és tal que $a \mid p$ i $b \mid p$, llavors $m \mid p$

Observació 2.12. El $\operatorname{lcm}(a,b)$ si existeix també és únic tret de multiplicació per una unitat.

Proposició 2.13. *Si $\mathcal{R}$ és un* PID, *cada parell d'elements a, b té un* $\operatorname{lcm}(a,b)$, *i* $\langle \operatorname{lcm}(a,b) \rangle = \langle a \rangle \cap \langle b \rangle$.

Demostració. Per ser $\mathcal{R}$ un PID, existeix m tal que $\langle m \rangle = \langle a \rangle \cap \langle b \rangle$. Obviament m verifica (i). Sigui ara M tal que $a \mid M$ i $b \mid M$. En conseqüència $M \in \langle a \rangle$ i $M \in \langle b \rangle$, i per tant $M \in \langle a \rangle \cap \langle b \rangle = \langle m \rangle$. Per tant $m \mid M$. □

Definició de polinomis sobre un anell commutatiu $\mathcal{R}$.

Definició 2.14. Donat un anell commutatiu $\mathcal{R}(+,\ \cdot)$, definim el conjunt de polinomis $\mathcal{R}[x_1, \dots, x_n]$ en les variables $x_1, \dots, x_n$ sobre $\mathcal{R}$, com el conjunt de totes les expressions que comportin un nombre d'operacions finit entre elements de $\mathcal{R}$ afegint les variables abstractes $x_1, \dots, x_n$. Per definició, les variables x_i

(i) es comporten com nous elements de $\mathcal{R}$ respecte a les propietats d'anell, poguent-se associar, commutar etc. amb els restants elements.
(ii) x_i i totes les seves potències i els productes amb diferents potències de les altres variables són elements diferents entre sí i diferents de tots els altres.
(iii) els elements x_i no tenen invers.

Per tant $\mathcal{R}[x_1, \dots, x_n]$ és una extensió de $\mathcal{R}$ amb els elements $x_1, \dots, x_n$. Donat un element de $f \in \mathcal{R}[x_1, \dots, x_n]$, aplicant la propietat distributiva commutativa i associativa tantes vegades com calgui, i posant

$$\overbrace{x_i \cdot x_i \cdot x_i}^{n} = x_i^n$$

podem posar-lo sempre en la forma equivalent:

$$f = \sum_{\alpha_1 \dots \alpha_n} a_{\alpha_1 \dots \alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

Proposició 2.15. *Extenent les operacions de $\mathcal{R}$ a $\mathcal{R}[x_1, \dots, x_n]$, tenint en compte la difinició de polinomi, el conjunt de polinomis sobre $\mathcal{R}$ és un anell commutatiu.*

Farem servir la notació següent:

$$\begin{aligned}
\overline{x} &= x_1, \dots, x_n \\
\alpha &= (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n_{\geq 0} \\
c_\alpha &= c_{\alpha_1, \dots, \alpha_n} \in \mathcal{R} \\
x^\alpha &= x_1^{\alpha_1} \dots x_n^{\alpha_n} \\
f &= \sum_\alpha c_\alpha x^\alpha
\end{aligned}$$

Posat f en la forma anterior, cada sumand $a_\alpha x^\alpha$ és un monomi, l'element a_α és el coeficient, i x^α és un producte de potències.

Corol·lari 2.16. *Dos polinomis f, g de $K[\overline{x}]$ són iguals ssi posats en la forma $f = \sum_\alpha a_\alpha x^\alpha$ i $g = \sum_\beta b_\beta x^\beta$ són tals que tenen els mateixos coeficients en correspondència amb els mateixos productes de potències.*

Exemple 2.17. Sigui

$$f = (a + b \cdot x_1) \cdot (x_2 + c \cdot x_3) \cdot x_1 + (a \cdot x_2 + b) \cdot (c \cdot x_1 + x_2 + a)$$

Expandint tenim:

$$ba + bcx_1 + \left(b + a^2\right) x_2 + (a + ac)\, x_1 x_2 + bx_1^2 x_2 + ax_2^2 + acx_1 x_3 + bcx_1^2 x_3$$

que té la forma indicada.

Podriem també considerar f com un element de $(\mathcal{R}[x_1, x_3])[x_2]$, és a dir, com un polinomi en la variable x_2 a coeficients en l'anell $\mathcal{R}[x_1, x_3]$. Per això treiem factor comú les potències de x_2 així:

$$f = \left(ba + bcx_1 + acx_1 x_3 + bcx_1^2 x_3\right) + \left(b + a^2 + (a + ac)x_1 + bx_1^2\right) x_2 + ax_2^2$$

Degut a les propietats d'anell commutatiu, existeix un isomorfisme trivial entre els polinomis de n variables sobre un anell commutatiu, independentment de quines variables es considerin com a tals i quines formant part dels polinomis de l'anell de coeficients. Si representem per $\overline{y}_1, \overline{y}_2$ dos subconjunts de variables formant una partició qualsevol de les variables $\overline{x} = x_1, \dots x_n$, tenim l'isomorfisme

$$(\mathcal{R}[\overline{y}_1])[\overline{y}_2] \approx (\mathcal{R}[\overline{y}_2])[\overline{y}_1] \approx \mathcal{R}[\overline{y}_1, \overline{y}_2] = \mathcal{R}[\overline{x}]$$

que correspón a treure factor comú els diferents productes de potències de $\overline{y}_2$, $\overline{y}_1$ o bé $\overline{x}$.

3. Anells Noetherians

Definició 3.1 (Anell Noetherià)**.** Direm que un anell $\mathcal{R}$ és **Noetherià**, si cada ideal de $\mathcal{R}$ és generat per un nombre finit d'elements.

Observació 3.2. Els PID's són Noetherians, ja que cada ideal està generat per un únic element.

Proposició 3.3 (Condició de cadena ascendent ACC)**.** *Un anell és Noetherià, ssi tota cadena ascendent d'ideals*

$$\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \dots$$

estaciona, és a dir, existeix un N a partir del qual tots els $\mathcal{I}_k$ són iguals.

Demostració. $\Rightarrow$: Si $\mathcal{R}$ és Noetherià i $\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \cdots$ és una cadena ascendent d'ideals, prenem $\mathcal{I} = \cup_{i=1}^{\infty} \mathcal{I}_i$. (**Ex:** Proveu que $\mathcal{I}$ és un ideal.) Per ser $\mathcal{R}$ noetherià, $\mathcal{I}$ admet un conjunt finit de generadors: $\mathcal{I} = \langle a_1, \dots, a_n \rangle$. Per la definició de $\mathcal{I}$, cada a_i pertany a algun $\mathcal{I}_{i_j}$. Sigui N un cota superior dels indexos i_j. Obviament $\mathcal{I} \subseteq \mathcal{I}_N$, i per tant, $\mathcal{I}_N = \mathcal{I}_{N+1} = \cdots = \mathcal{I}$.

$\Leftarrow$: Demostrem ara que si tota cadena ascendent estaciona, un ideal $\mathcal{I}$ qualsevol admet un conjunt finit de generadors. En efecte, sigui $a_1 \in \mathcal{I}$. Si $\mathcal{I} = \mathcal{I}_1 = \langle a_1 \rangle$, ja hem acabat. En cas contrari sigui $a_2 \in \mathcal{I} - \langle a_1 \rangle$. Si $\mathcal{I} = \mathcal{I}_2 = \langle a_1, a_2 \rangle$ hem acabat, altrament prenem $a_3 \in \mathcal{I} - \langle a_1, a_2 \rangle \ldots$ Aquest procediment acaba, ja que anem construint una cadena ascendent $\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \ldots$, que per hipòtesi estaciona. □

Teorema 3.4 (de la Base d'Hilbert)**.** *Si $\mathcal{R}$ és Noetherià, llavors $\mathcal{R}[x]$ també ho és.*

Demostració. Sigui $\mathcal{I}$ un ideal de $\mathcal{R}[x]$ i $n \geq 0$. Notem

$$\mathcal{I}_n := \{a \in \mathcal{R} \;:\; ax^n + \text{termes de grau inferior} \in \mathcal{I}\}.$$

Com que els $\mathcal{I}_n$ formen una cadena ascendent d'ideals de $\mathcal{R}$ (perquè?), estacionen en un cert índex N. Prenem $S_i \subseteq \mathcal{I}_i$ un sistema finit de generadors de $\mathcal{I}_i$ per a cada $0 \leq i \leq N$, i per cada element $a \in S_i$, un polinomi $f_a \in \mathcal{I}$ de la forma $ax^i +$ termes de grau inferior. Anem a demostrar que $\mathcal{I} = \langle f_a \;: a \in S \rangle$, on $S = S_0 \cup \cdots \cup S_N$. Veiem, per inducció sobre el grau i de f, que si $f \in \mathcal{I}$ llavors $f \in \langle f_a \;: a \in S \rangle$. Per $i = 0$ és clar. Si $0 < i \leq N$ escribim $f = bx^i +$ termes de grau inferior, amb $b \in \mathcal{I}_i$. Llavors $b = \sum_{a \in S_i} u_a a$ i per tant $f - \sum_{a \in S_i} u_a f_a \in \langle f_a \;: a \in S \rangle$ per hipòtesi d'inducció (hem cancel·lat el terme de grau i), d'on també $f \in \langle f_a \;: a \in S \rangle$. Si $i > N$ llavors $b = \sum_{a \in S_N} u_a a$ i fem el mateix raonament amb el polinomi $f - \sum_{a \in S_N} u_a x^{i-N} f_a$. □

Corol·lari 3.5. *L'anell dels polinomis $K[\overline{x}] = K[x_1, \ldots, x_n]$ de n variables sobre un cos (o un anell Noetherià) K és Noetherià.*

Demostració. Només cal aplicar inducció al teorema 3.4. □

Exercici 3.6. Demostreu que si $\mathcal{R}[x]$ és Noetherià també ho és $\mathcal{R}$.

Proposició 3.7. *En un anell Noetherià, de tot sistema generador d'un ideal s'en pot extreure un subsistema finit.*

Demostració. Si $S \subseteq \mathcal{R}$ i $\mathcal{I} = \langle S \rangle$, prenem $a_0 \in S$ qualsevol. Si $S \subseteq \langle a_0 \rangle$ ja hem acabat. Si no, prenem $a_1 \in S - \langle a_0 \rangle$. Si $S \subseteq \langle a_0, a_1 \rangle$ ja hem acabat, altrament prenem $a_2 \in S - \langle a_0, a_1 \rangle \ldots$ Aquest procés ha d'acabar doncs altrament construiríem una cadena infinita estrictament ascendent d'ideals:

$$\langle a_0 \rangle \subset \langle a_0, a_1 \rangle \subset \langle a_0, a_1, a_2 \rangle \subset \cdots$$

□

Proposició 3.8. *Si $\mathcal{R}$ és un domini Noetherià, tot element $a \in \mathcal{R}$ descomposa en producte d'irreductibles.*

Demostració. Si a és irreductible ja hem acabat. Si no, sigui $a = a_1 b_1$ amb a_1, b_1 no unitaris. Obviament, pels ideals generats tenim: $\langle a \rangle \subset \langle a_1 \rangle$ i també $\langle a \rangle \subset \langle b_1 \rangle$, on les inclusions són estrictes. Si algún dels factors (a_1 per exemple) no és irreductible, descomposem $a_1 = a_2 c_2$ i així successivament.

Cal que les descomposicions acabin en producte d'irreductibles, altrament obtindriem una cadena estrictament ascendent d'ideals

$$\langle a\rangle \subset \langle a_1\rangle \subset \langle a_2\rangle \subset \ \ldots$$

en contradicció amb el fet que $\mathcal{R}$ és Noetherià. □

4. Dominis factorials (UFD)

Definició 4.1 (UFD = Unique Factorization Domain)**.** Direm que un domini $\mathcal{R}$ és un **domini de factorització única** o **domini factorial**, (UFD), si cada element es descomposa en producte d'elements irreductibles de $\mathcal{R}$ de 'forma única', és a dir si $a = \prod_{i=1}^{r} p_i = \prod_{i=1}^{s} q_i$ on tots els p_i i q_i són irreductibles llavors $r = s$ i cada p_i és de la forma $q_i u$, amb u unitari.

Lema 4.2. *Sigui $\mathcal{R}$ un domini on tot element admet una descomposició en producte d'irreductibles . Llavors són equivalents:*
(i) *$\mathcal{R}$ és un domini de factorització única.*
(ii) *En $\mathcal{R}$, tot element irreductible és primer.*

Demostració. (i) $\Rightarrow$ (ii): Sigui $\mathcal{R}$ un UFD i sigui $q \in \mathcal{R}$ irreductible. Si $q \nmid b$ i $q \nmid c$, llavors (perquè?) q no està ni en la descomposició de b en irreductibles ni en la de c. Per tant, tampoc ho estarà en la de bc, que és el producte de les de b i de c (perquè?). Així, $q \nmid bc$, i q és primer.

(ii) $\Rightarrow$ (i): Suposem que $a \in \mathcal{R}$ té dues descomposicions:

$$a = a_1 a_2 \ldots a_n = b_1 b_2 \ldots b_m,$$

on cada a_i i cada b_j són primers. Com que cada a_i divideix $\prod_j b_j$, ha de dividir a un d'ells, posem b_j. Però com que b_j és irreductible, això implica que a_i i b_j són iguals tret de multiplicació per una unitat. Podem cancel·lar-los i continuar amb els altres factors. Finalment quan haurem cancel·lat tot els a_i s'han d'haver cancel·lat tots els b_j excepte unitats (perquè?). Això demostra la unicitat de la descomposició. □

Corol·lari 4.3. *Un domini Noetherià $\mathcal{R}$ és* UFD *sii en $\mathcal{R}$ tot irreductible és primer.*

Demostració. Per la proposició 3.8. □

Corol·lari 4.4 (PID $\Rightarrow$ UFD)**.** *Tot domini d'ideals principals és factorial.*

Demostració. Tenint en compte el corol·lari 4.3, únicament caldrà provar que en un PID tot irreductible és primer.

Si a és irreductible, $a \mid bc$ i $a \nmid b$ el $\gcd(a,b)$ és 1, ja que essent a irreductible l'únic divisor no unitatari que admet és ell mateix llevat d'inversible. De $a \mid bc$ deduïm $ka = bc$, i utilitzant una identitat de Bézout per $\gcd(a,b)$ $Aa + Bb = 1$. Multiplicant per c resulta:

$$c = Aac + Bbc = Aac + Bka = a(Ac + Bk)$$

i per tant $a \mid c$. □

Proposició 4.5. *En un* UFD *sempre existeix el* gcd *i el* lcm. *A més:*

(i) *si les descomposicions en factors irreductibles (=primers) de a i b són*

$$a = \prod_i p_i^{\alpha_i}, \quad b = \prod_i p_i^{\beta_i},$$

llavors

$$\gcd(a,b) = \prod_i p_i^{\min(\alpha_i,\beta_i)} \quad , \quad \operatorname{lcm}(a,b) = \prod_i p_i^{\max(\alpha_i,\beta_i)}.$$

(ii) $\gcd(a,b)\operatorname{lcm}(a,b) = a\,b$.

(iii) $\langle \operatorname{lcm}(a,b)\rangle = \langle a\rangle \cap \langle b\rangle$.

Exercici 4.6. Proveu la proposició anterior.

Observació 4.7. En un UFD no té perquè existir identitat de Bézout (tal con es pot observar en l'exercici següent); expressat en termes d'ideals, ja no és vàlida la fórmula $\langle a,b\rangle = \langle \gcd(a,b)\rangle$. En canvi si continua essent vàlida l'expressió corresponent pel lcm donada per (iii) de la proposició anterior, i a partir d'ella podem obtenir el gcd per l'apartat (ii).

Exercici 4.8. $k[x,y]$ és un UFD, com veurem al corol·lari 4.14, i si bé $\gcd(x,y) = 1$, en canvi $1 \notin \langle x,y\rangle$. Proveu-ho.

Definició 4.9 (Contingut d'un polinomi)**.** Sigui $p = \sum_{i=0}^{n} a_i x^i$ un polinomi sobre un UFD. Definim el **contingut** de p així:

$$\operatorname{cont}(p) = \gcd(a_0,\ldots,a_n)$$

Amb aquesta definició, treient factor comú $\operatorname{cont}(p)$, resulta

$$p = \operatorname{cont}(p)\,p_1, \quad \text{on} \quad \operatorname{cont}(p_1) = 1.$$

Direm també que p_1 és la **part primitiva** de p:

$$p_1 = \operatorname{primpart}(p).$$

Lema 4.10. *Sigui $\mathcal{R}$ un* UFD *i $f,g \in \mathcal{R}[x]$. Llavors*

$$\operatorname{cont}(f\,g) = \operatorname{cont}(f)\operatorname{cont}(g).$$

Demostració. Si expressem $f = \operatorname{cont}(f)\,f_1$, $g = \operatorname{cont}(g)\,g_1$ amb $\operatorname{cont}(f_1) = 1$ i $\operatorname{cont}(g_1) = 1$, llavors tindrem:

$$fg = \operatorname{cont}(f)\operatorname{cont}(g)\,f_1\,g_1.$$

Hem de provar que $\operatorname{cont}(f_1\,g_1) = 1$. Posant

$$f_1 = \sum_{i=0}^{n} a_i x^i, \quad g_1 = \sum_{j=0}^{m} b_j x^j, \quad f_1\,g_1 = \sum_{k=0}^{n+m} c_k x^k$$

tindrem

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

Només cal provar que si $p \in \mathcal{R}$ és primer, llavors no divideix algun c_k. Com que p no pot dividir tots els a_i ni tots els b_j, siguin i, j els primers indexos tals que $p \nmid a_i$ i $p \nmid b_j$. El coeficient de x^{i+j} és:

$$c_{i+j} = a_0 b_{i+j} + \cdots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \cdots + a_{i+j} b_0$$

Per hipòtesi $p \mid a_s$ per $0 \leq s < i$ i $p \mid b_s$ per $0 \leq s < j$. Per tant, p divideix a tots els termes del segon membre excepte $a_i b_j$. En canvi, no divideix ni a_i ni b_j, i essent primer, tampoc divideix al producte. Per tant $p \nmid c_{i+j}$. □

Lema 4.11 (de Gauss). *Siguin $\mathcal{R}$ un* UFD *i $f \in \mathcal{R}[x]$, amb* $\operatorname{cont}(f) = 1$*. Llavors f és irreductible en $\mathcal{R}[x]$ ssi ho és a l'anell* $\operatorname{Quot}(\mathcal{R})[x]$*, on* $\operatorname{Quot}(\mathcal{R})$ *és el cos de fraccions de $\mathcal{R}$.*

Demostració. $\Rightarrow$: Suposem que $f \in \mathcal{R}[x]$ és reductible a $\operatorname{Quot}(\mathcal{R})[x]$. Anem a provar que també ho és a $\mathcal{R}[x]$.

En efecte, si $f = \tilde{g}\,\tilde{h}$, i $\tilde{g}, \tilde{h} \in \operatorname{Quot}(\mathcal{R})[x]$ de grau positiu en x (en cas contrari serien unitats), llavors, multiplicant per un cert $d \in \mathcal{R}$, obtenim

$$d\,f = g\,h$$

amb $g, h \in \mathcal{R}[x]$ del mateix grau que $\tilde{g}$ i $\tilde{h}$ respectivament. Pel lema 4.10, $d = \operatorname{cont}(g)\operatorname{cont}(h)$. Dividint $d\,f = g\,h$ per d obtenim

$$f = \frac{g\,h}{d} = \left(\frac{g}{\operatorname{cont}(g)}\right)\left(\frac{h}{\operatorname{cont}(h)}\right),$$

on ara els dos factors de la dreta pertanyen a $\mathcal{R}[x]$. Com que s'obtenen respectivament a partir de $\tilde{g}$ i $\tilde{h}$ multiplicant i dividint per elements de $\mathcal{R}$, continuen tenint grau positiu en x i no són unitats de $\mathcal{R}[x]$. Així f és reductible a $\mathcal{R}[x]$.

$\Leftarrow$: Suposem que $f \in \mathcal{R}[x]$ és reductible a $\mathcal{R}[x]$. Anem a provar que també ho és a $\operatorname{Quot}(\mathcal{R})[x]$. En efecte, si $f = g\,h$ en $\mathcal{R}[x]$, on g i h no són unitats de $\mathcal{R}[x]$, aquesta descomposició també és vàlida a $\operatorname{Quot}(\mathcal{R})[x]$. L'únic que hem de veure és que els factors no són unitaris a $\operatorname{Quot}(\mathcal{R})[x]$. De $\operatorname{cont}(f) = 1$, pel lema 4.10, deduïm que $\operatorname{cont}(g)$ i $\operatorname{cont}(h)$ són unitats de $\mathcal{R}$. Com que g i h no són unitats de $\mathcal{R}[x]$, han de tenir grau positiu en x i per tant tampoc són unitats de $\operatorname{Quot}(\mathcal{R})[x]$. □

Exercici 4.12. Proveu que si $\mathcal{R}$ és UFD, llavors tot element de $\mathcal{R}[x]$ admet una descomposció en irreductibles. Qui són els irreductibles de $\mathcal{R}[x]$?

Teorema 4.13. *Si $\mathcal{R}$ és un* UFD*, llavors $\mathcal{R}[x]$ també ho és.*

Demostració. Tenint en compte el lema 4.2 i l'exercici anterior, només cal provar que si $\mathcal{R}$ és UFD llavors tot element irreductible $f \in \mathcal{R}[x]$ és primer.

Distingirem dos casos:

Cas 1: $\deg(f) = 0$. En aquest cas $f \in \mathcal{R}$ i per tant f també és irreductible en $\mathcal{R}$. Pel lema 4.2 f és primer en $\mathcal{R}$. Suposem ara que $f \mid g\,h$ on $g, h \in \mathcal{R}[x]$. Pel lema 4.10 resulta que $f \mid \operatorname{cont}(g)\operatorname{cont}(h)$, per tant $f \mid \operatorname{cont}(g)$ o $f \mid \operatorname{cont}(h)$. Però si $f \mid \operatorname{cont}(g)$ llavors $f \mid g$ i anàlogament per h.

Cas 2: $\deg(f) > 0$. Observem primer que $\mathrm{cont}(f) = 1$, altrament podriem descomposar $f = \mathrm{cont}(f)\, f_1$, amb $\mathrm{cont}(f_1) = 1$. Suposem que $f \mid g\, h$ a $\mathcal{R}[x]$. Pel lema de Gauss 4.11 f és irreductible a $\mathrm{Quot}(\mathcal{R})[x]$, que és un PID. Per tant f és primer en aquest domini i f divideix g o h a $\mathrm{Quot}(\mathcal{R})[x]$. Anem a veure que f també divideix g o h a $\mathcal{R}[x]$. Si $f\tilde{q} = g$ amb $\tilde{q} \in \mathrm{Quot}(\mathcal{R})[x]$, veiem que $\tilde{q}$ pertany de fet a $\mathcal{R}[x]$. Multiplicant per un $d \in \mathcal{R}$ convenient $q := d\tilde{q} \in \mathcal{R}[x]$. Així $fq = dg$, d'on $\mathrm{cont}\,(q) = d\,\mathrm{cont}(g)$. Per tant $d \mid \mathrm{cont}(q)$, i finalment

$$\tilde{q} = \frac{\mathrm{cont}(q)}{d}\,\frac{q}{\mathrm{cont}(q)} \in \mathcal{R}[x].$$

□

Corol·lari 4.14. *Si $\mathcal{R}$ és* UFD, *llavors l'anell de polinomis de n variables $\mathcal{R}[x_1,\ldots,x_n]$ també ho és.*

Demostració. Aplicant inducció al teorema 4.13. □

Exercici 4.15. Utilitzant el lema de Gauss i emprant algorismes (p.e. en Maple) per trobar el gcd en varies variables, proveu de factoritzar el següent polinomi a $\mathbb{Q}[x,y,z]$. La factorització feta val també a $\mathbb{C}[x,y,z]$? (*Indicació: Considereu $f \in \mathbb{Q}[x,y,z] \subseteq \mathbb{Q}(x,y)[z]$ i factoritzeu en el segon anell*)

$$\begin{aligned} f \;:=\; & x^6yz^3 - 2\,x^5y^2z^2 + x^4y^3z - 3\,x^5yz^3 + 6\,x^4y^2z^2 - 3\,x^3y^3z + 2\,x^4yz^3 \\ & -4\,x^3y^2z^2 + 2\,x^2y^3z - y^5x^4z^3 + 2\,y^6x^3z^2 - y^7x^2z + 3\,y^5x^3z^3 \\ & -6\,y^6x^2z^2 + 3\,y^7xz - 2\,y^5x^2z^3 + 4\,y^6xz^2 - 2\,y^7z. \end{aligned}$$

5. Espai afí

Definició 5.1 (Espai afí)**.** Donat un cos K i un enter n, l'espai afí de dimensió n sobre K és

$$K^n = \{\overline{a} = (a_1,\ldots,a_n) : a_1,\ldots,a_n \in K\}.$$

Cada polinomi $f \in K\overline{x}]$ defineix una funció polinòmica

$$\begin{array}{rccc} f: & K^n & \longrightarrow & K \\ & \overline{a} & \mapsto & f(\overline{a}), \end{array}$$

on $f(\overline{a})$ és el resultat de substituir $\overline{x}$ per $\overline{a}$ en l'expressió de f.

Proposició 5.2. *Si K és un cos infinit, i si $f \in K[\overline{x}]$, llavors $f = 0$ a $K[\overline{x}]$ ssi $f : K^n \to K$ és la funció nul·la.*

Demostració.
$\Rightarrow$: Obvi.

$\Leftarrow$: Ho provarem per inducció sobre el nombre de variables n.
Per $n = 1$, sabem que un polinomi de $K[x]$ no nul té un nombre finit de zeros, i per tant, si s'anul·la en infinits punts ha de ser el polinomi nul.
Sigui $f \in K[x_1, \ldots, x_n]$ un polinomi que s'anul·la sobre tot K^n. Podem escriure f en la forma

$$f = \sum_{i=0}^{N} g_i\, x_n^i$$

on cada $g_i \in K[x_1, \ldots, x_{n-1}]$. Anem a provar que cada g_i és el polinomi nul (de $n-1$ variables), el que implica que f és també el polinomi nul. Fixem $(a_1, \ldots, a_{n-1}) \in K^{n-1}$. Per la hipòtesi sobre f, el polinomi

$$f(a_1, \ldots, a_{n-1}, x_n) \in K[x_n]$$

s'anul·la sobre tot K, per tant ha de ser el polinomi nul. Aquest fet implica que cada un dels coeficients de $f(a_1, \ldots, a_{n-1}, x_n)$ és nul, és a dir cada $g_i(a_1, \ldots, a_{n-1}) = 0$. Com que el punt $(a_1, \ldots, a_{n-1}) \in K^{n-1}$ era arbitrari, cada un dels polinomis g_i s'anul·la idènticament sobre K^{n-1}. Per hipòtesi d'inducció g_i és el polinomi nul.

$\square$

Exercici 5.3. Demostreu que el resultat anterior es pot millorar de la manera següent. Sigui $f \in K[\overline{x}]$ i $A_i \subseteq K$ $i = 1, \ldots, n$ tals que $|A_i| > \deg(f, x_i)$, on $\deg(f, x_i)$ indica el grau de f en x_i (mirat com a polinomi en la variable x_i sobre l'anell $K[x_1, \ldots, \widehat{x_i}, \ldots x_n]$). Si f s'anul·la sobre $A_1 \times \cdots \times A_n$ llavors $f = 0$.

Exemple 5.4. En canvi la proposició anterior no és certa en un cos finit. Posem per cas $K = \mathbb{F}_3$, i considerem el polinomi

$$f = x^3 - x = x(x-1)(x-2) \subset \mathbb{F}_3[x].$$

Obviament f no és el polinomi nul, però la funció associada a f sí que és idènticament nul·la, ja que $f(0) = f(1) = f(2) = 0$.

6. Varietats Afins

Definició 6.1 (Varietats afins). Sigui $n \geq 1$, K un cos i B un subconjunt de $K[\overline{x}]$, on $\overline{x} = x_1, \ldots, x_n$. Definim

$$\mathbb{V}(B) := \{\overline{a} \in K^n \ : \ f(\overline{a}) = 0 \text{ per a tot } f \in B\}.$$

Els conjunts de la forma $\mathbb{V}(B)$, on $B \subseteq K[\overline{x}]$, reben el nom de *varietats afins*. Com que només parlarem de varietats afins ens estalviarem aquest adjectiu.

Proposició 6.2. *Si $\mathcal{I} = \langle B \rangle$ llavors $\mathbb{V}(\mathcal{I}) = \mathbb{V}(B)$, per tant, les varietats venen definides per ideals. En particular si $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ llavors $\mathbb{V}(\mathcal{I}) = \mathbb{V}(\{f_1, \ldots, f_m\})$, que per comoditat notarem $\mathbb{V}(f_1, \ldots, f_m)$.*

Demostració. Exercici. □

Pel teorema de la base de Hilbert, tot ideal és finitament generat, per tant les varietats són sempre solucions d'un nombre finit d'equacions polinomials.

Exemple 6.3. Els punts, les varietats lineals (les solucions d'un sistema lineal), les quàdriques i més en general les solucions d'una equació polinomial són varietats. La reunió de la paràbola $y = x^2$ amb la hipèrbola $xy = 1$ és una varietat. L cúbica guerxa definida per $V = \mathbb{V}(x^3 - z, x^2 - y)$ és una varietat de $\mathbb{R}^3$.

Observació 6.4. Dos ideals diferents poden definir la mateixa varietat, per exemple $\langle x \rangle \neq \langle x^2 \rangle$ en canvi $\mathbb{V}(\langle x \rangle) = \mathbb{V}(\langle x^2 \rangle) = \{0\}$.

Proposició 6.5. *Siguin $\mathcal{I}, \mathcal{J}$ ideals de $K[\overline{x}]$. Llavors:*
(i) $\mathbb{V}(\mathcal{I} \cap \mathcal{J}) = \mathbb{V}(\mathcal{I} \cdot \mathcal{J}) = \mathbb{V}(\mathcal{I}) \cup \mathbb{V}(\mathcal{J})$.
(ii) $\mathbb{V}(\mathcal{I} + \mathcal{J}) = \mathbb{V}(\mathcal{I}) \cap \mathbb{V}(\mathcal{J})$.

Demostració. □

$(\text{i})_a$ Provem que $\mathbb{V}(\mathcal{I} \cap \mathcal{J}) = \mathbb{V}(\mathcal{I} \cdot \mathcal{J})$.
- $\subseteq$: Per tot $\overline{a} \in \mathbb{V}(\mathcal{I} \cap \mathcal{J})$ i $f \in \mathcal{I} \cdot \mathcal{J}$ és $f \in \mathcal{I} \cap \mathcal{J}$. Per tant $f(\overline{a}) = 0$ i $\overline{a} \in \mathbb{V}(\mathcal{I} \cdot \mathcal{J})$.
- $\supseteq$: Per tot $\overline{a} \in \mathbb{V}(\mathcal{I} \cdot \mathcal{J})$ i $f \in \mathcal{I} \cap \mathcal{J}$ és $f \in \mathcal{I}$ i $f \in \mathcal{J}$. Per tant $f^2 \in \mathcal{I} \cdot \mathcal{J}$ i $f^2(\overline{a}) = 0$. Per tant $f(\overline{a}) = 0$ i $\overline{a} \in \mathbb{V}(\mathcal{I} \cap \mathcal{J})$.

$(\text{i})_b$ Provem que $\mathbb{V}(\mathcal{I} \cap \mathcal{J}) = \mathbb{V}(\mathcal{I}) \cup \mathbb{V}(\mathcal{J})$.
- $\supseteq$: Per tot $\overline{a} \in \mathbb{V}(\mathcal{I}) \cup \mathbb{V}(\mathcal{J})$ i $f \in \mathcal{I} \cap \mathcal{J}$ és $f \in \mathcal{I}$ i $f \in \mathcal{J}$. Per tant $f(\overline{a}) = 0$ i $\overline{a} \in \mathbb{V}(\mathcal{I} \cap \mathcal{J})$.
- $\subseteq$: Per tot $\overline{a} \in \mathbb{V}(\mathcal{I} \cap \mathcal{J}) = \mathbb{V}(\mathcal{I} \cdot \mathcal{J})$ tal que $\overline{a} \notin \mathbb{V}(\mathcal{I})$ i $f \in \mathcal{J}$, podem trobar un $g \in \mathcal{I}$ tal que $g(\overline{a}) \neq 0$. Tindrem $fg \in \mathcal{I} \cdot \mathcal{J}$ i per tant $f(\overline{a})g(\overline{a}) = 0$. D'aquí resulta $f(\overline{a}) = 0$ i així $\overline{a} \in \mathbb{V}(\mathcal{J})$.

(ii)
- $\subseteq$: Per tot $\overline{a} \in \mathbb{V}(\mathcal{I} + \mathcal{J})$ i $f \in \mathcal{I}$ és $f(\overline{a}) = 0$ i $\overline{a} \in \mathbb{V}(\mathcal{I})$. Anàlogament de $g \in \mathcal{J}$ resultarà $\overline{a} \in \mathbb{V}(\mathcal{J})$. Per tant resulta $\overline{a} \in \mathbb{V}(\mathcal{I}) \cap \mathbb{V}(\mathcal{J})$.
- $\supseteq$: Per tot $\overline{a} \in \mathbb{V}(\mathcal{I}) \cap \mathbb{V}(\mathcal{J})$ i $f \in \mathcal{I} + \mathcal{J}$ existeixen $u \in \mathcal{I}$ i $v \in \mathcal{J}$ tals que $f = u + v$. D'aquí resulta $f(\overline{a}) = u(\overline{a}) + v(\overline{a}) = 0 + 0 = 0$ i $\overline{a} \in \mathbb{V}(\mathcal{I} + \mathcal{J})$.

Corol·lari 6.6. *Siguin $\mathcal{I} = \langle f_1, \dots, f_r \rangle$ i $\mathcal{J} = \langle g_1, \dots, g_s \rangle$. Tindrem $\mathbb{V}(\mathcal{I}) = \mathbb{V}(f_1, \dots, f_s)$ i $\mathbb{V}(\mathcal{J}) = \mathbb{V}(g_1, \dots, g_s)$. Per la proposició 1.8 resulta*
(i) $\mathbb{V}(\mathcal{I}) \cap \mathbb{V}(\mathcal{J}) = \mathbb{V}(\mathcal{I} + \mathcal{J}) = \mathbb{V}(f_1, \dots, f_r, g_1, \dots, g_s)$.
(ii) $\mathbb{V}(\mathcal{I}) \cup \mathbb{V}(\mathcal{J}) = \mathbb{V}(\mathcal{I} \cap \mathcal{J}) = \mathbb{V}(\mathcal{I} \cdot \mathcal{J}) = \mathbb{V}(f_i g_j : 1 \leq i \leq r, 1 \leq j \leq s)$,

Exemple 6.7. Utilitzant el corol·lari anterior tenim
1. $\mathbb{V}(x - x_1, y - y_1) = \mathbb{V}(x - x_1) \cap \mathbb{V}(y - y_1)$ que defineix un punt com intersecció de dues rectes.
2. $\mathbb{V}(x^4 - xz, x^3 - xy) = \mathbb{V}(x(x^3 - z), x(x^2 - y)) = \mathbb{V}(x) \cup \mathbb{V}(x^3 - z, x^2 - y)$ que ens permet descomposar la varietat donada com unió del plà $x = 0$ i la cúbica guerxa.

7. La topologia de Zariski a K^n

Generalitzant la proposició 6.5 resulta el següent:

Corol·lari 7.1.
(i) *Si* $\{\mathcal{I}_j : 1 \leq j \leq N\}$ *és una col·lecció finita d'ideals de* $K[\overline{x}]$*, llavors*

$$\mathbb{V}\left(\bigcap_{j=1}^{N} \mathcal{I}_j\right) = \bigcup_{j=1}^{N} \mathbb{V}(\mathcal{I}_j).$$

(ii) *Si* $\{\mathcal{I}_j \ : \ j \in J\}$ *és una col·lecció d'ideals de* $K[\overline{x}]$*, llavors*

$$\mathbb{V}\left(\sum_{j\in J} \mathcal{I}_j\right) = \bigcap_{j\in J} \mathbb{V}(\mathcal{I}_j)$$

(iii) *Les varietats són tancades per unió finita i intersecció arbitrària.*

Recordem que una topologia sobre K^n es defineix donant els oberts, que han de ser una col·lecció de subconjunts de K^n tancats per intersecció finita, unió arbitrària i que continguin $\emptyset$ i K^n. Alternativament es pot definir a partir dels tancats (complementaris d'oberts).

Podem, doncs, definir una nova topologia a K^n donant una col·lecció de subconjunts de K^n, tancats per unió finita, intersecció arbitrària i que continguin $\emptyset$ i K^n.

Corol·lari 7.2. *Les varietats de* K^n *són els tancats d'una topologia, que anomenarem* topologia de Zariski. *A la clausura topològica (adherència) d'un subconjunt* A *de* K^n *l'anomenarem* clausura de Zariski de A, *i la denotarem per* $\overline{A}$.

Demostració. Per la proposició anterior, només cal veure que $\emptyset$ i K^n són varietats: $\emptyset = \mathbb{V}(1)$ i $K^n = \mathbb{V}(0)$. □

Observem que, per definició, la clausura de Zariski de A és la mínima varietat que conté A.

Exercici 7.3.
1. Si K és $\mathbb{R}$ o $\mathbb{C}$, la topologia usual és més fina que la topologia de Zariski (els oberts de Zariski són també oberts per la topologia usual).

8. Ideals de varietat. Correspondència Varietats - Ideals de varietat

Definició 8.1. Sigui $n \geq 1$, K un cos i A un subconjunt de K^n. Definim

$$\mathbb{I}(A) = \{f \in K[\overline{x}] : f(\overline{a}) = 0 \text{ per tot } \overline{a} \in A\}$$

Si $V \subset K^n$ és una varietat, a $\mathbb{I}(V)$ l'hi direm *l'ideal de varietat de* V.

Exercici 8.2. Demostreu que $\mathbb{I}(A)$ és un ideal de $K[\overline{x}]$.

Proposició 8.3. *Si* $\mathcal{I}$ *és un ideal de* $K[\overline{x}]$ *i* V *és una varietat de* K^n*, llavors*

(i) $\mathcal{I} \subseteq \mathbb{I}(\mathbb{V}(\mathcal{I}))$,
(ii) $V = \mathbb{V}(\mathbb{I}(V))$.

Demostració.
(i) Per tot $f \in \mathcal{I}$ i $\overline{a} \in \mathbb{V}(\mathcal{I})$ és $f(\overline{a}) = 0$, i per tant $f \in \mathbb{I}(\mathbb{V}(\mathcal{I}))$.
(ii) $\subseteq$: Per tot $\overline{a} \in V$ i $f \in \mathbb{I}(V)$ és $f(\overline{a}) = 0$, i per tant $\overline{a} \in \mathbb{V}(\mathbb{I}(V))$.
$\supseteq$: Sigui $\mathcal{I}$ un ideal que defineix V. Per tot $\overline{a} \in \mathbb{V}(\mathbb{I}(\mathbb{V}(\mathcal{I}))$ i $f \in \mathcal{I}$ és $f \in \mathbb{I}(\mathbb{V}(\mathcal{I}))$, i per tant $f(\overline{a}) = 0$. Per tant $\overline{a} \in \mathbb{V}(\mathcal{I}))$.

□

Observació 8.4. En canvi no és cert que si I és un ideal qualsevol, $\mathbb{I}(\mathbb{V}(I))$ sigui igual a I. Com feiem notar a l'observacio 6.4, els ideals $\langle x^2 \rangle$ i $\langle x \rangle$ són diferents però defineixen la mateixa varietat $V = \{0\}$. Dels dos, $\langle x \rangle$ és l'ideal de la varietat V mentre que $\langle x^2 \rangle$ no ho és. No tots els ideals són ideals de varietat. L'apartat (i) de la proposició 8.3 ens diu que l'ideal de varietat és el màxim ideal que la defineix.

A les proposicións següents, considerem $\mathbb{I}$ i $\mathbb{V}$ com aplicacions, més exactament

$$\mathbb{I} : P(K^n) \to P(K[\overline{x}]),$$

$$\mathbb{V} : P(K[\overline{x}]) \to P(K^n),$$

on P indica les parts d'un conjunt.

Proposició 8.5. *Les aplicacions $\mathbb{I}$ i $\mathbb{V}$ són inverses respecte a la inclusió, és a dir, si $A', B' \subset K[x]$ i $A, B \subset K^n$ es verifica:*
(i) $A' \subseteq B' \Rightarrow \mathbb{V}(B') \subseteq \mathbb{V}(A')$
(ii) $A \subseteq B \Rightarrow \mathbb{I}(B) \subseteq \mathbb{I}(A)$

Demostració. □

(i) Per tot $b \in \mathbb{V}(B')$ i $f \in A'$, és $f \in B'$, i per tant $f(b) = 0$. Això implica que $b \in \mathbb{V}(A')$ i per tant $\mathbb{V}(B') \subseteq \mathbb{V}(A')$.
(ii) Per tot $f \in \mathbb{I}(B)$ i $a \in A$, és $a \in B$, i per tant $f(a) = 0$. Això implica que $f \in \mathbb{I}(A)$ i per tant $\mathbb{I}(B) \subseteq \mathbb{I}(A)$.

Exemple 8.6.

1. En particular tenim $\mathbb{V}(f, g) \subseteq \mathbb{V}(f)$. Per exemple,
$$\{(x_1, y_1)\} = \mathbb{V}(x - x_1, y - y_1) \subseteq \mathbb{V}(x - x_1).$$
El punt (x_1, y_1) pertany al plà $x = x_1$.
2. També, $\mathbb{I}(V \cup W) \subseteq \mathbb{I}(V)$. En concret, si $V = \{(x_1, y_1)\}$ i $W = \{(x_2, y_2)\}$, tindrem $\mathbb{I}(V) = \langle x - x_1, y - y_1 \rangle = \langle u, v \rangle$. No tenim encara eines per verificar-ho, però avancem que l'ideal de varietat de $V \cup W$ és:
$$\mathbb{I}(V \cup W) = \langle (x - x_1)(x - x_2), y - y_1 \frac{x - x_2}{x_1 - x_2} - y_2 \frac{x - x_1}{x_2 - x_1} \rangle = \langle f, g \rangle.$$

Comprovem fàcilment que $f = u(x - x_2) \in \mathbb{I}(V)$ i

$$g = v - u\frac{y_1 - y_2}{x_1 - x_2} \in \mathbb{I}(V).$$

Lema 8.7. *Siguin $A \subset K^n$ i $B \subset K[\overline{x}]$. Es té*

(i) $A \subseteq \mathbb{V} \circ \mathbb{I}(A)$
(ii) $B \subseteq \mathbb{I} \circ \mathbb{V}(B)$.
(iii) $\mathbb{I} \circ \mathbb{V} \circ \mathbb{I} = \mathbb{I}$.
(iv) $\mathbb{V} \circ \mathbb{I} \circ \mathbb{V} = \mathbb{V}$.

Demostració.
(i) Per tot $a \in A$ i $f \in \mathbb{I}(A)$ és $f(a) = 0$. Això implica que $a \in \mathbb{V}(\mathbb{I}(A))$.
(ii) Per tot $f \in B$ i $a \in \mathbb{V}(B)$ és $f(a) = 0$. Això implica que $f \in \mathbb{I}(\mathbb{V}(B))$.
(iii) $\subseteq$: Aplicant $\mathbb{I}$ als dos membres de (i) i tenenint en compte que $\mathbb{I}$ és invers respecte a la inclusió (proposició 8.5) resulta la inclusió $\subseteq$.
$\supseteq$: Posant $B = \mathbb{I}(A)$ en (ii) resulta la inclusió $\supseteq$.
(iv) $\subseteq$: Posant $A = \mathbb{V}(B)$ en (i) resulta la inclusió $\subseteq$.
$\supseteq$: Aplicant $\mathbb{V}$ als dos membres de (ii) i tenenint en compte que $\mathbb{V}$ és invers respecte a la inclusió (proposició 8.5) resulta la inclusió $\supseteq$.
$\square$

Corol·lari 8.8.
(i) *Les varietats són la imatge de $\mathbb{V}$ i els ideals de varietat són la imatge de $\mathbb{I}$.*
(ii) *$\mathbb{I}$ i $\mathbb{V}$ són bijeccions, l'una inversa de l'altra, entre varietats de K^n i ideals de varietat de $K[\overline{x}]$. A més, inverteixen la inclusió, tal com veiem a la proposició 8.5*

Però cal recordar que no tots els ideals són ideals de varietat!

Proposició 8.9. *Si $A \subseteq K^n$, la varietat més petita que conté A és $\mathbb{V}(\mathbb{I}(A))$, que no és altre cosa que la clausura de Zarisky de A:*

$$\overline{A} = \mathbb{V}(\mathbb{I}(A))$$

Demostració. Com que $\mathbb{V}(\mathbb{I}(A))$ és varietat, només cal provar que és la mínima que conté A: si $A \subseteq \mathbb{V}(\mathcal{I})$ llavors $\mathbb{I}(A) \supseteq \mathbb{I}(\mathbb{V}(\mathcal{I}))$ d'on $\mathbb{V}(\mathbb{I}(A)) \subseteq \mathbb{V}(\mathbb{I}(\mathbb{V}(\mathcal{I}))) = \mathbb{V}(\mathcal{I})$. $\square$

Resumint, un conjunt $B \subseteq K[\overline{x}]$ determina una varietat $V = \mathbb{V}(B)$. Però aquesta varietat és la mateixa que la associada a l'ideal $\mathcal{I} = \langle B \rangle$. És a dir, $V = \mathbb{V}(\mathcal{I})$. V també està determinada per altres ideals.
Però a una varietat V li correspón un únic ideal de varietat $\mathbb{I}(V)$, que és el màxim ideal que la defineix. Recíprocament, a l'ideal de la varietat $\mathbb{I}(V)$ li correspón la varietat V. Les aplicacions $\mathbb{V}$ i $\mathbb{I}$ són bijeccions inversa la una de l'altre.
D'altra banda, un conjunt de punts $A \subseteq K^n$ li correspón una varietat $\overline{A}$ que és la clausura de Zarisky de A i que és la varietat més petita que conté A.

La clausura $\overline{A}$ s'obté fent $\overline{A} = \mathbb{V}(\mathbb{I}(A))$.
Representem-ho en un esquema:

$$
\begin{tikzcd}
K[\overline{x}] & K^n \\
B \arrow[d, "\cap"'] \arrow[rdd] & \\
I = \langle B \rangle \arrow[rd] \arrow[d, phantom, "\cap"] & \\
\mathbf{I}(V){=}\mathbf{I}(A) \arrow[r, shift right, "\mathbf{V}"'] & V = \mathbf{V}(B) = \mathbf{V}(I) = \mathbf{V}(\mathbf{I}(V)) = \overline{A} \arrow[l, shift right, "\mathbf{I}"'] \\
 & A \arrow[u, "\cup"'] \arrow[ul]
\end{tikzcd}
$$

Correspondència Ideals - Varietats

Exercici 8.10. 1. $\mathbb{I}(V \cap W) = \mathbb{I}\mathbb{V}(\mathbb{I}(V) + \mathbb{I}(W))$.

Proposició 8.11. *Si V, W són varietats de K^n i $\mathcal{I}, \mathcal{J}$ són ideals de $K[\overline{x}]$, llavors:*

(i) $\mathbb{I}(V \cup W) = \mathbb{I}(V) \cap \mathbb{I}(W)$.
(ii) $\mathbb{I}(V \cap W) \supseteq \mathbb{I}(V) + \mathbb{I}(W)$.
(iii) $V = W$ *sii* $\mathbb{I}(V) = \mathbb{I}(W)$; $V \subseteq W$ *sii* $\mathbb{I}(W) \subseteq \mathbb{I}(V)$ *i* $V \subset W$ *sii* $\mathbb{I}(W) \subset \mathbb{I}(V)$.
(iv) $\mathcal{I}$ *i* $\mathcal{J}$ *defineixen la mateixa varietat sii* $\mathbb{I}\mathbb{V}(\mathcal{I}) = \mathbb{I}\mathbb{V}(\mathcal{J})$.

Demostració.

(i) Per tot $f \in \mathbb{I}(V \cup W)$ és $f \in \mathbb{I}(V)$ i $f \in \mathbb{I}(W)$. Per tant $f \in \mathbb{I}(V) \cap \mathbb{I}(W)$. El raonament és invertible.
(ii) Per tot $h \in \mathbb{I}(V) + \mathbb{I}(W)$ existeixen $f \in \mathbb{I}(V)$ i $g \in \mathbb{I}(W)$ tals que $h = f + g$. Per tant $f \in \mathbb{I}(V \cap W)$ i $g \in \mathbb{I}(V \cap W)$, reslutant que també $h = f + g \in \mathbb{I}(V \cap W)$.
En canvi la inclusió en sentit contrari no és certa. Posem un contraexemple: Considerem les varietats de $\mathbb{C}^2$ següents: $V = \mathbb{V}(y)$ i $W = \mathbb{V}(y - x^2)$. Obviament $\mathbb{I}(V) = \langle y \rangle$ i $\mathbb{I}(W) = \langle y - x^2 \rangle$. Tindrem
$$\mathbb{I}(V) + \mathbb{I}(W) = \langle y, x^2 \rangle \subsetneq \langle y, x \rangle = \mathbb{I}(V \cap W).$$

(iii) Siguin $V = \mathbb{V}(\mathcal{I})$ i $W = \mathbb{V}(\mathcal{J})$. Si $V = W$ clarament $\mathbb{I}(\mathbb{V}(\mathcal{I})) = \mathbb{I}(\mathbb{V}(\mathcal{J}))$, i per tant $\mathbb{I}(V) = \mathbb{I}(W)$. Recíprocament, si $\mathbb{I}(V) = \mathbb{I}(W)$ llavors $\mathbb{V}(\mathcal{I}) = \mathbb{V}\mathbb{I}\mathbb{V}(\mathcal{I}) = \mathbb{V}\mathbb{I}\mathbb{V}(\mathcal{J}) = \mathbb{V}(\mathcal{J})$ i per tant $V = W$.
La inclusió estricte i no estricte es demostren de la mateixa manera.
(iv) És immediat, posant $A' = \mathbb{I}(V)$ i $B' = \mathbb{I}(W)$ a la proposició 8.5.

$\square$

9. Quocient d'ideals i diferència de varietats

Definició 9.1. Es defineix el qüocient d'ideals $\mathcal{I} : \mathcal{J}$ com

$$\mathcal{I} : \mathcal{J} = \{ f \in K[\overline{x}] \ : \ \text{ per tot } g \in \mathcal{J}, \text{ és } fg \in \mathcal{I} \} .$$

és a dir, com el conjunt dels polinomis que multiplicats per algún element de $\mathcal{J}$ pertanyen a $\mathcal{I}$.

Exercici 9.2.
1. Demostreu que $\mathcal{I} : \mathcal{J}$ és un ideal.
2. Proveu que $\mathcal{I} \subseteq \mathcal{I} : \mathcal{J}$.
3. Proveu que $\mathcal{I} : \langle 1 \rangle = \mathcal{I}$.
4. Proveu que $\mathcal{I} : \mathcal{I} = \langle 1 \rangle$
5. Proveu que $(\mathcal{I} : \mathcal{J}) \cdot \mathcal{J} \subseteq \mathcal{I}$.
6. Trobeu un contraexemple a $\mathbb{Z}$ que provi que la inclusió 5. és estricte.
7. Proveu que $\langle p_1 q, \dots , p_r q \rangle : \langle q \rangle = \langle p_1, \dots , p_r \rangle$.
8. Proveu que $(\mathcal{I} \cdot \mathcal{J}) : \mathcal{J} \supseteq \mathcal{I}$.
9. És certa la igualtat en la proposició 8?

Proposició 9.3. *Si V i W són varietats de K^n es té:*

$$\mathbb{I}(V - W) = \mathbb{I}(V) : \mathbb{I}(W).$$

Demostració.

$\subseteq$: Per tot $f \in \mathbb{I}(V - W)$ i $g \in \mathbb{I}(W)$ i $\overline{a} \in V$ és $f(\overline{a})g(\overline{a}) = 0$, ja que si $\overline{a} \in V - W$ és $f(\overline{a}) = 0$ i si $\overline{a} \in W$ és $g(\overline{a}) = 0$. Per tant és $fg \in \mathbb{I}(V)$, i així $f \in \mathbb{I}(V) : \mathbb{I}(W)$.

$\supseteq$: Per tot $f \in \mathbb{I}(V) : \mathbb{I}(W)$ i $\overline{a} \in V - W$, prenem $g \in \mathbb{I}(W)$ tal que $g(\overline{a}) \neq 0$. Llavors $fg \in \mathbb{I}(V)$ i per tant s'anul·la en $\overline{a}$, d'on $f(\overline{a}) = 0$, i $f \in V - W$.

□

Exercici 9.4.
1. Demostreu que si K és infinit i $V \neq K^n$ llavors $\mathbb{I}(K^n - V) = \langle 0 \rangle$ i per tant, $\overline{K^n - V} = K^n$.
2. Demostreu que la clausura de Zariski d'un subconjunt infinit de K és tot K. Què passa en el cas finit?
3. Demostreu que (aquí $K = \mathbb{R}$, de fet només cal K infinit), la clausura de Zariski de
$$\left\{ (x, y) \in \mathbb{R}^2 \ : \ y = x^2, \ x > 0 \right\}$$
és
$$\left\{ (x, y) \in \mathbb{R}^2 \ : \ y = x^2 \right\} .$$
Què passa si K és finit?
4. Demostreu que si $\overline{a} = (a_1, \dots , a_n) \in K^n$ llavors
$$\mathbb{I}(\overline{a}) = \langle x_1 - a_1, \dots , x_n - a_n \rangle .$$

5. Demostreu que si K és $\mathbb{R}$ llavors la clausura de Zariski de la gràfica de la funció sinus és K^2. Què passa a $\mathbb{C}$?
6. $***$ Quina és la causura de Zariski de la gràfica de la funció exponencial $y = e^x$ a $\mathbb{R}^2$?
7. Si K és de característica zero (és a dir $\mathbb{Q} \subseteq K$), llavors $\mathbb{I}(\mathbb{Z}^n) = \langle 0 \rangle$ i $\overline{\mathbb{Z}^n} = K^n$ (*Indicació:* proveu-ho per inducció sobre n).
8. $**$ Demostreu que K és finit sii la topologia de Zariski de K^n és la discreta (n fixat).
9. $* * *$ Demostreu que la clausura de Zariski d'un conjunt amb interior no buit de $\mathbb{R}^n$ és tot $\mathbb{R}^n$ (*Indicació:* Useu el desenvolupament d'un polinomi en sèrie de Taylor).

   Val el mateix per $\mathbb{C}$?

Corol·lari 9.5.
(i) *La topologia de Zariski és Noetheriana, és a dir, tota cadena infinita descendent de varietats estaciona.*
(ii) *La topologia de Zariski és compacta*[2].

Demostració. (i) és conseqüència de la bijecció (que inverteix la inclusió) entre varietat i ideals de varietat i la Noetherianitat de l'anell $K[\overline{x}]$ (usem el teorema de la base de Hilbert). (ii) surt de la Noetherianitat: Si $\langle V_j \ : \ j \in I \rangle$ és una col·lecció de varietats amb intersecció buida i tota subcol·lecció finita té intersecció no buida, podrem construir una cadena infinita estrictament descendent de varietats d'aquesta manera: comencem amb V_i quasevol. Prenem $a \in V_i$ i $i' \in I$ tal que $a \notin V_{i'}$. Llavors $V_i \supset V_{i'} \cap V_i$. Com que $V_i \cap V_{i'} \neq \emptyset$ prenem $a' \in V_{i'} \cap V_i$ i $i'' \in I$ tal que $a' \notin V_{i''}$. Per tant $V_i \supset V_{i'} \cap V_i \supset V_{i''} \cap V_{i'} \cap V_i \ \ldots$ i així succesivament. □

10. Descomposició de varietats en irreductibles

Definició 10.1 (Varietat irreductible)**.** Una varietat V es diu irreductible si $V = V_1 \cup V_2$ on V_1 i V_2 són varietats, implica que o bé $V = V_1$ o bé $V = V_2$.

Exercici 10.2.
1. Demostreu que V és irreductible sii $V \subseteq V_1 \cup \cdots \cup V_r$ implica $V \subseteq V_i$ per algun $1 \leq i \leq r$.
2. Demostreu que si V és finit, llavors V és irreductible sii té un sol element.
3. Demostreu que si K és finit, les úniques varietats irreductibles de K^n són els punts.
4. $***$ La topologia de Zariski d'una varietat V és la induïda per la de tot l'espai afí. Demostreu que V és irreductible sii en V (amb la topologia de Zariski) tot obert és dens.
5. Si V és irreductible i consta de més d'un punt llavors la topologia de Zariski de V no és Hausdorff. (*Indicació:* Useu l'exercici anterior).

[2]La topologia de Zariski no és Hausdorff, ens estem referint a que tot recobriment per oberts admet un subrecobriment finit

Proposició 10.3. *V és irreductible sii $\mathbb{I}(V)$ és primer.*

Demostració.

$\Rightarrow$: Si V és irreductible i $fg \in \mathbb{I}(V)$ llavors $V = \mathbb{V}\mathbb{I}(V) \subseteq \mathbb{V}(fg) = \mathbb{V}(f) \cup \mathbb{V}(g)$ implica $V \subseteq \mathbb{V}(f)$ o $V \subseteq \mathbb{V}(g)$, d'on $f \in \mathbb{I}(V)$ o $g \in \mathbb{I}(V)$.

$\Leftarrow$: Recíprocament, si $\mathbb{I}(V)$ és primer i $V \subseteq V_1 \cup V_2$ llavors $\mathbb{I}(V_1 \cup V_2) = \mathbb{I}(V_1) \cap \mathbb{I}(V_2) \subseteq \mathbb{I}(V)$. Tot es redueix a provar que $\mathbb{I}(V_i) \subseteq \mathbb{I}(V)$ per a algun i, ja que llavors $V \subseteq V_i$. Si $\mathbb{I}(V_1) \not\subseteq \mathbb{I}(V)$ llavors prenem $g \in \mathbb{I}(V_1) - \mathbb{I}(V)$. Si $f \in \mathbb{I}(V_2)$, llavors $fg \in \mathbb{I}(V_1) \cap \mathbb{I}(V_2) \subseteq \mathbb{I}(V)$ d'on $f \in \mathbb{I}(V)$ per ser primer. Això demostra $\mathbb{I}(V_2) \subseteq \mathbb{I}(V)$.

□

Exercici 10.4.
1. Demostreu que si V és irreductible i $W \subset V$, llavors $\overline{V - W} = V$. Doneu exemples on es vegi que la hipòtesi V *irreductible* és necessària.
2. Demostreu que si K és infinit, l'espai afí K^n és irreductible.

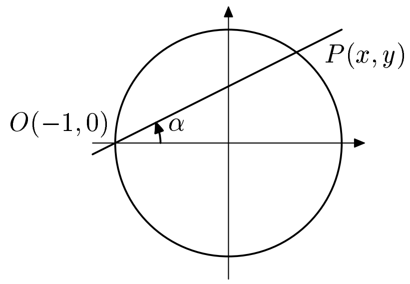
Definició 10.5. Una *parametrització* és una aplicació

$$\begin{array}{cccc} F: & A \subseteq K^r & \longrightarrow & K^n \\ & (t_1, \dots, t_r) & \mapsto & (f_1(t_1, \dots, t_r), \dots, f_n(t_1, \dots, t_r)) \end{array}$$

Entendrem que la *varietat V definida per la parametrització F* és la clausura de Zariski de la imatge F, és a dir $V = \overline{F(A)}$. Dos casos importants són les parametritzacions polinomials i les racionals. Una *parametrització polinomial* és aquella que ve definida component a component per funcions polinomials, és a dir, existeixen $f_1, \dots, f_n \in K[t_1, \dots, t_r]$ tals que $F(\overline{a}) = (f_1(\overline{a}), \dots, f_n(\overline{a}))$. Obsevem que F está definida sobre tot K^r. Una *parametrització racional* és aquella que ve definida component a component per funcions racionals, és a dir, existeixen $f_1, \dots, f_n \in K(t_1, \dots, t_r)$ tals que $F(\overline{a}) = (f_1(\overline{a}), \dots, f_n(\overline{a}))$. Observem que si $f_i = f_i^N / f_i^D$ amb $f_i^N, f_i^D \in K[t_1, \dots, t_r]$, llavors $F: K^r - \mathbb{V}(f_1^D \cdots f_n^D) \to K^n$.

En general $\overline{F(A)}$ no té perque coïncidir amb $F(A)$, com es pot veure als exercicis següents.

Exemple 10.6. Volem parametritzar la circumferència $x^2 + y^2 = 1$. Considerem una recta de pendent m que passa pel punt $O(-1, 0)$ i estudiem el punt $P(x, y)$ de tall amb la circumferència:



Parametrització de la circumferència: $\tan \alpha = m$

Tindrem el sistema

$$\left.\begin{array}{l} y = m(x+1) \\ x^2 + y^2 = 1 \end{array}\right\}$$

D'on resulta:

$$(x+1)(x-1+m^2(x+1)) = 0$$

El punt P correspondrà a les corrdenades:

$$\begin{aligned} x &= \frac{m^2-1}{m^2+1} \\ y &= \frac{2m}{m^2+1} \end{aligned}$$

que és una parametrització racional de la circumferència. Podem observar, que el punt $O(-1,0)$ no queda parametritzat, ja que correspón a $m = \pm\infty$

Exercici 10.7.

1. La cúbica guerxa (a K) és la varietat definida per la parametrització polinomial $F : K \to K^3$, $F(a) = (a, a^2, a^3)$. Trobeu polinomis que defineixin la cúbica guerxa i demostreu que F cobreix tota la cúbica guerxa.
2. Trobeu la varietat definida per la parametrització $F : \mathbb{R} \to \mathbb{R}^2$, $F(a) = (\cos a, \cos 2a)$. F cubreix tota la varietat?
3. $***$ Quina és la varietat engendrada (clausura de Zariski) pel conjunt format per totes les tangents a la cúbica guerxa?

Proposició 10.8. *Si K és infinit, tota varietat definida per una parametrització racional és irreductible.*

Demostració. Suposem que la varietat ve definida per la parametrització donada per les fraccions racionals $(f_1, \ldots, f_n)$, amb $f_i \in K(t_1, \ldots, t_r)$ i denotem $V := \mathbb{V}(f_1^D \cdots f_n^D)$. Com que $\overline{F(K^r - V)} = \mathbb{VI}(F(K^r - V))$, el seu ideal de varietat és $\mathbb{I}\left(\overline{F(K^r - V)}\right) = \mathbb{IVI}(F(K^r - V)) = \mathbb{I}(F(K^r - V))$. Així, cal veure que $\mathbb{I}(F(K^r - V))$ és primer. Si $g_0 = g_1 g_2 \in \mathbb{I}(F(K^r - V))$, llavors la funció definida per la fracció racional $g_0(f_1, \ldots, f_n) \in K(t_1, \ldots, t_r)$ s'anula idènticament sobre $K^r - V$. Si escrivim $g_i(f_1, \ldots, f_n) = g_i^N / g_i^D$, amb $g_i^N, g_i^D \in K[t_1, \ldots, t_r]$ per $i = 1, 2$ llavors $g_0(f_1, \ldots, f_n) = \dfrac{g_1^N g_2^N}{g_1^D g_2^D}$. Així $g_1^N g_2^N \in \mathbb{I}(K^r - V)$. Per ser K infinit i l'exercici 9.4 (perquè $V \neq K^n$?) deduim que $g_1^N g_2^N = 0$ com a polinomi i per tant $g_1^N = 0$ o $g_2^N = 0$. Això implica que $g_1 \in \mathbb{I}(F(K^r - V))$ o $g_2 \in \mathbb{I}(F(K^r - V))$. $\square$

Exercici 10.9. En aquests exercicis K és infinit (Què passa en el cas finit?). Demostreu que:

1. Tota varietat lineal és irreductible.

2. La varietat de K^2 definida per l'equació $y - f(x) = 0$ és irreductible ($f \in K[x]$).
3. Si $\mathcal{I} = \langle yg_1(x) - f_1(x), zg_2(x) - f_2(x) \rangle$, on $f_1, f_2, g_1, g_2 \in K[x]$ i g_1, g_2 són no nuls, llavors $\mathbb{V}(\mathcal{I})$ és irreductible.
4. La hipèrbola d'equació $xy = 1$ és irreductible, tot i que si la dibuixeu a $\mathbb{R}^2$ queda tallada en dos trossos.
5. La Strofoide és la varietat definida per la parametrització $F : \mathbb{R} \to \mathbb{R}^2$, $F(t) = (a \sin t, a \tan t(1 + \sin t)$, on $a \in \mathbb{R}$ fixat. Trobeu l'equació que defineix la Strofoide i proveu que la Strofoide és irreductible (*indicació*: parametritzeu racionalment la Strofoide).

   Més endavant veurem que si K és algebraicament tancat i $f \in K[\overline{x}]$, $\mathbb{V}(f)$ és irreductible sii f és potència d'irreductible. En els exercicis següents veurem que si K no és algebraicament tancat això no té perquè ser cert.
6. Demostreu que $\mathbb{V}(f)$ és irreductible, en canvi f no és potència d'irreductible, on $f = x^3 + xy^2 - x^2y - y^3$. Aquí K és un cos infinit.
7. Demostreu que $\mathbb{V}(f)$ no és irreductible, en canvi f és irreductible, on $f = x^4 - 2x^2y - 2x^2 + 2y^2 + 2y + 1$. Feu-ho a $\mathbb{Q}$ i a $\mathbb{R}$. Què passa a $\mathbb{C}$?.

Proposició 10.10. *Tota varietat descomposa com a unió de varietats irreductibles. Si a més demanem que la descomposició sigui irredundant (és a dir, no n'hi hagi cap continguda en una altra) llavors la descomposició és única.*

Demostració. L'existència de la descomposició és conseqüència de la Noetherianitat. Si V no és irreductible llavors $V = V_1 \cup V_2$, amb $V \supset V_i$ per $i = 1, 2$. Si V_1 i V_2 són irreductibles ja hem acabat, sinó descomposem la que no ho sigui, per exemple $V_2 = V_3 \cup V_4$ amb $V_2 \supset V_i$ per $i = 3, 4$. Si V_3 i V_4 són irreductibles ja hem acabat, sinó descomposem la que no ho sigui ... Aquest procés haurà d'acabar, altrament tindriem una cadena infinita estrictament descendent de varietats. Per tal de veure la unicitat en el cas irredundant, suposem $V_1 \cup \cdots \cup V_k = W_1 \cup \cdots \cup W_r$ cap d'elles irredundant, és a dir $V_i \not\subseteq V_j$ i $W_i \not\subseteq W_j$ per $i \neq j$. Per irreductibilitat, de $V_i \subseteq W_1 \cup \cdots \cup W_r$ deduïm que existeix $f(i) \in \{1, \ldots, r\}$ de manera que $V_i \subseteq W_{f(i)}$. Inversament, veiem que donat $j \in \{1, \ldots, r\}$ existeix $g(j) \in \{1, \ldots, k\}$ de manera que $W_j \subseteq V_{g(j)}$. Així $V_i \subseteq W_{f(i)} \subseteq V_{g \circ f(i)}$, que per irredundància deduïm $i = g \circ f(i)$ i $V_i = W_{f(i)}$. Anàlogament deduïm $\mathrm{Id} = f \circ g$, és a dir f és una bijecció i $V_i = W_{f(i)}$. □

Exercici 10.11. Trobeu la descomposició en varietats irreductibles a $\mathbb{C}$ i a $\mathbb{R}$ de $\mathbb{V}(\mathcal{I})$ on

1. $\mathcal{I} = \left\langle x - 1, x - y^2 \right\rangle$.
2. $(*)$ $\mathcal{I} = \langle x^n - y^m \rangle$
3. $\mathcal{I} = \langle x^2y^2 - 3xy^2 - yx^4 + 3yx^3 - yx + 3y + x^3 - 3x^2,\ -xy^2 + 3yx + y - 3 \rangle$.