UNIVERSITAT POLITÈCNICA DE CATALUNYA
FACULTAT DE MATEMÀTIQUES I ESTADÍSTICA

PROBLEMES D'ALGEBRA COMPUTACIONAL

ANTONIO MONTES
Departament de Matemàtica Aplicada II

Gener 1997

Presentació

El recull de problemes que aqui es dona ésta tret essencialment del llibre *Ideals, Varieties and Algorithms* de D. Cox, J. Little, D. O'Shea, Springer (1992). Aquest llibre és la referÈncia bàsica pel curs d'Algebra Computacional de la llicenciatura de Matemàtiques de la FME. Hem considerat que resulta útil disposar de la col.lecció de problemes, separada i traduida, fent alguna adaptació i afegint o suprimint algún problema. Les modificacions són mínimes.

En l'edició d'aquest any hi han novetats.

He incorporat alguns dels darrers examens i un recull de pràctiques interessants. Les pràctiques estan pensades per ser fetes en *Maple*. L'objectiu és aprendre a utilitzar les rutines d'Algebra Computacional que incorpora, veure la seva utilitat i aprendre a reprogramar-les amb l'objectiu de ser capaos de fer modificacions adhoc de l'algorisme de Buchberger.

Finalment he afegit una breu introducció al llenguatge de càlcul simbòlic *Maple*, que és el que es fa servir a les pràctiques de l'assignatura.

1. Geometria, Àlgebra i algorismes

1.1. **Monomis i polinomis multivariats. 1.1.1.** Doneu un polinomi de $\mathbb{F}_2[x,y]$ tal que la funció polinòmica associada de $\mathbb{F}_2^2 \to \mathbb{F}_2$ sigui idÈnticament nul.la. El polinomi no ha de ser nul i preferiblement ha de contenir totes les variables.

1.1.2. La mateixa qüestió del problema anterior, ara per un polinomi de $\mathbb{F}_3[x,y]$, per un polinomi de $\mathbb{F}_2[x_1,\ldots,x_n]$ i per un polinomi de $\mathbb{F}_{p^2}[x]$ amb p primer.

1.1.3. Escriviu

$$f(x,y,z) = 5x^2yz^2 - 3xy^2 + 6xz^3 - 12xy^3z^2 - xyz^5 + 3y^2z^3 - x^2y^3$$

com un polinomi en z a coeficients en $k[x,y]$.

1.1.4. Quants monomis diferents hi amb les variables $x_1, x_2, \ldots, x_n$ de grau total $m = |\alpha|$?

1.1.5. Feu una construcció inductiva, detallada dels polinomis de n variables, introdunt les operacions i provant totes les propietats a partir dels polinomis d'una variable. (Nota: Comenceu provant que $k[x][y] = k[y][x]$ i definint a partir d'aqui $k[x,y]$)

1.1.6. Sigui $f \in C[x_1,\ldots,x_n]$ i sigui M la potència més gran amb que figura qualsevol de les variables a f. Sigui $\mathbb{Z}^n_{M+1}$ el conjunt de punts de $\mathbb{Z}^n$ que té totes les coordenades entre 1 i $M+1$.

$$\mathbb{Z}^n_{M+1} = \{(a_1,\ldots,a_n) : \forall i, \quad a_i \in \mathbb{Z}, \quad 1 \le a_i \le M+1\}$$

Proveu que si la funció associada a f s'anul.la a tots els punts de $\mathbb{Z}^n_{M+1}$, llavors f és el polinomi nul.

1.2. **Varietats. 1.2.1.** **[L]** Feu gràfiques de les següents variatats afins

a) $\mathbf{V}(x^2+y^2-1)$
b) $\mathbf{V}(xy-x^3+1)$
c) $\mathbf{V}(z^2-x^2-y^2)$
d) $\mathbf{V}(z-x^2-y^2)$
e) $\mathbf{V}(y-x^2, z-x^3)$

1.2.2. Estudieu les següents varietats de $\mathbb{R}^2$:

a) $\mathbf{V}(x^2-y^2)$
b) $\mathbf{V}(5x+y-4, x+2y+1)$
c) $\mathbf{V}(y^2-x(x-1)(x-2))$
d) $\mathbf{V}(x^2+y^2-4) \cap \mathbf{V}(xy-1)$

1.2.3. Estudieu les següents varietats de $\mathbb{R}^3$:

a) $\mathbf{V}(x^2+y^2+z^2-1)$
b) $\mathbf{V}(x^2+y^2-1)$
c) $\mathbf{V}(x+2, y-2z)$
d) $\mathbf{V}(xz^2-xy)$
e) $\mathbf{V}(x^4-zx, x^3-yx)$

1.2.4. Sigui $E=\mathbb{R}^3$. Què podeu dir a propòsit de la dimensió de $\mathbf{V}(xz, yz)$?

1.2.5. Sigui A una matriu de $\mathbb{R}^n \to \mathbb{R}^n$. Quina és la dimensió de la varietat lineal $\mathbf{V}(Ax-b)$?

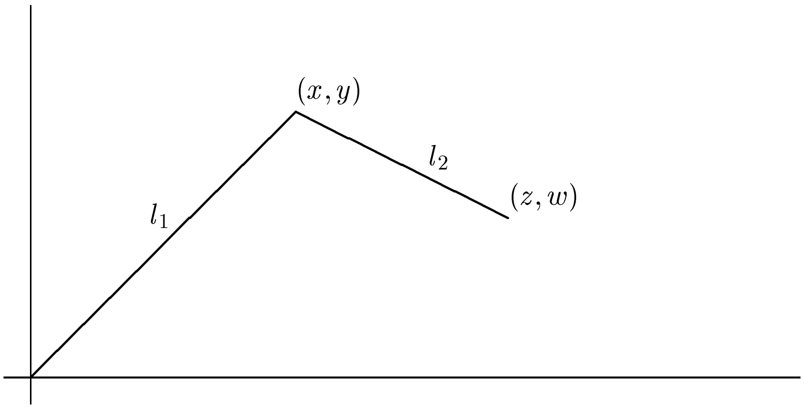
1.2.6. Sigui $f(x,y,z)=x^3+2xyz-z^2$. Volem trobar els extrems de f subjectes a les condicions $g(x,y,z)=x^2+y^2+z^2=1$. El resultat és una varietat algebraica? Què en podeu dir?

1.2.7. Doneu el conjunt de polinomis que determinen la varietat afi de $\mathbb{R}^3$ següent:

$$\mathbf{V}(x^2+y^2+z^2-1) \cup \mathbf{V}(2x+3y-z, x-y+2z-1)$$

i feu una gràfica.

1.2.8. Considereu el següent braç de robot:



L'estat del robot queda determinat donant les quatre coordenades x, y, z, w. Però no són possibles totes les posicions. Determineu la varietat $\mathbf{V}(x,y,z,w)$ de les posicions possibles del robot.

1.2.9. Descomposar com a unió de varietats de $\mathbb{R}^3$ la varietat

$$\mathbf{V}((x-2)(x^2-y), y(x^2-y), (z+1)(x^2-y))$$

1.2.10. Demostreu que tot subconjunt finit de punts de $\mathbb{R}$ és una varietat algebraica.

1.2.11. Proveu que la rosa de quatre pètals que té per equació en polars $r = \sin 2\theta$ és una varietat algebraica de $\mathbb{R}^2$. Sigueu minuciosos en la demostració, i tingueu present que r pot ser negatiu.

1.2.12. Resulta més difícil demostrar que un cert subconjunt *no és* una varietat algebraica. Sigui

$$V = \{(x, x) : \quad x \in \mathbb{R}, \quad x \neq 1\} \subset \mathbb{R}^2$$

Proveu que no és una varietat algebraica.

1.2.13. Sigui $\mathbb{Z}^n \subset \mathbb{C}^n$. Proveu que $\mathbb{Z}^n$ no és una varietat algebraica de $\mathbb{C}^n$.

1.2.14. Considerem ara varietats sobre $\mathbb{Q}$. Les qüestions ara són molt més difícils que sobre $\mathbb{R}$ o $\mathbb{C}$. Per exemple, sigui n un enter positiu i considerem la varietat $F \subset \mathbb{Q}^2$ definida per

$$x^n + y^n = 1$$

Observeu que existeixen algunes solucions obvies per x o y nuls. Una qüestió interessant és saber si existeixen solucions no trivials.

a) Proveu que F_n té dues solucions trivials si n és senar i quatre si n és parell.
b) Proveu que F_n té una solució no trivial per $n \geq 3$ ssi el darrer teorema de Fermat és fals. L'esmentat teorema estableix que per $n \geq 3$ l'equació

$$x^n + y^n = z^n$$

no té solucions enteres on x, y, z siguin tots tres diferents de zero.

El cas general de la conjectura, com sabeu, encara no ha estat provat, si be sabem que és certa per $n \leq 150.000$. Al 1983 G. Faltings va provar que F_n té com a màxim un nombre finit de solucions a $\mathbb{Q}^2$.

1.2.15. Considerem ara un robot a $\mathbb{R}^2$ que consta de tres braos de longituds 3, 2 i 1 respectivament. El bra de longitud 3 pivota sobre l'origen; sobre l'altre extrem d'aquest pivota el bra de longitud de longitud 2, i sobre l'altre extrem del darrer pivota el bra de longitud 1, on est la mà del robot.

a) Quantes variables calen per determinar *l'estat* del robot?
b) Doneu les equacions de la varietat d'estats possibles.
c) Què dirieu a propòsit de la noció intuitiva de dimensió?
d) Anomenant (u, v) les coordenades de la mà del robot, per què es cumpleix que $u^2 + v^2 \leq 36$?
e) Si fixem els dos primers segments en posició alineada, i deixem lliures les altres dues articulacions. Determineu el conjunt de possibles valors de la mà del robot.
f) Mitjanant un gràfic proveu que la mà del robot pot moure's per qualsevol posició del disc de radi 6 centrat a l'origen.

1.2.16.

a) Proveu per inducció que la unió e intersecció d'un nombre finit de varietats afíns és una varietat afí.
b) Doneu un contreexemple per demostrar que la unió infinita de varietats no és sempre una varietat. (Més endavant veurem que la intersecció infinita si dóna lloc a una varietat).
c) Doneu un contreexemple per demostrar que la diferència conjuntista de $V - W$ no és necessàriament una varietat.
d) Siguin $V \subset k^n$ i $W \subset k^m$, varietats afins. Proveu que el següent producte cartesià és una varietat afí:

$$\begin{aligned} V \times W &= \{(x_1, \ldots, x_n, y_1, \ldots, y_m) \in k^{n+m} : \\ &\quad (x_1, \ldots, x_n) \in V, \quad (y_1, \ldots, y_m) \in W\} \end{aligned}$$

1.3. **Parametritzacions. 1.3.1.** Parametritzeu totes les solucions del sistema d'equacions lineals

$$\begin{aligned} x + 2y - 2z + w &= -1 \\ x + y + z - w &= 2 \end{aligned}$$

1.3.2. El conjunt de punts de $\mathbb{R}^2$ parametritzat per les equacions

$$\begin{aligned} x &= \cos(t) \\ y &= \cos(2t) \end{aligned}$$

és una varietat algebraica o un subconjunt d'una varietat algebraica? Preciseu la resposta.

1.3.3. Donada una $f \in k[x]$ trobeu una parametrització de $\mathbf{V}(y - f(x))$

1.3.4. Sigui la següent representació paramètrica

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

a) Trobeu l'equació de la varietat afí que determina.
b) Proveu que parametritza tots els punts de la varietat trobada excepte un punt.

1.3.5. Sigui la hipèrbola $x^2 - y^2 = 1$.

a) Proveu que els punts

$$\begin{aligned} x &= \cosh(t) \\ y &= \sinh(t) \end{aligned}$$

estan sobre la hipèrbola. Quina part de la hipèrbola cobreixen?

b) Proveu que una recta talla a la hipèrbola en 0, 1, o 2 punts, i il.lustreu-ho mitjanamt una gràfica. Considereu separadament els casos $x = a$ i $y = mx + b$.

c) Obteniu una parametrització de la hipèrbola, considerant les rectes no verticals que passen pel punt $(-1, 0)$.

d) La parametrització trobada a c) no està definida per dos valors de t. Relacioneu-ho amb les asímptotes de la hipèrbola.

1.3.6. L'objectiu d'aquest exercici és veure que l'esfera $x^2 + y^2 + z^2 = 1$ de $\mathbb{R}^3$ pot ser parametritzada per

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

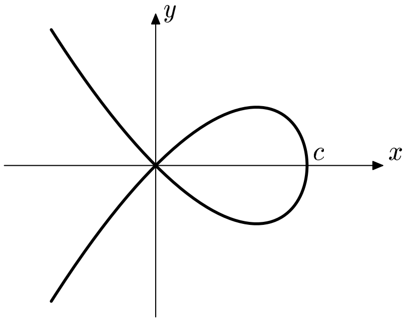
a) Donat una punt $(u, v, 0)$ del plà xy, traceu una línia cap el pol nord $(0, 0, 1)$. Sigui (x, y, z) l'altre punt en que la recta talla a l'esfera. Feu un gràfic per ilustrar-ho, i argumenteu geomètricament que el mapeig (u, v) versus (x, y, z) determina una parametrització de l'esfera a excepció del pol nord.

b) Proveu que la línia que uneix els punts $(0, 0, 1)$ i $(u, v, 0)$ es pot parametritzar per $(tu, tv, 1 - t)$, essent t un paràmetre que varia al llarg de la recta.

c) Substituiu ($x = tu$, $y = tv$, $z = 1 - t$) a l'equació de l'esfera per obtenir la parametrització de l'esfera donada al comenament.

1.3.7. Adapteu l'argumentació del exercici anterior per parametritzar l'esfera n-dimensional $x_1^2 + \cdots + x_n^2 = 1$ de $\mathbb{R}^n$.

1.3.8. Sigui la corba d'equació $y^2 = cx^2 - x^3$, on c és una constant. Heus açi un gràfic de la corba per $c > 0$



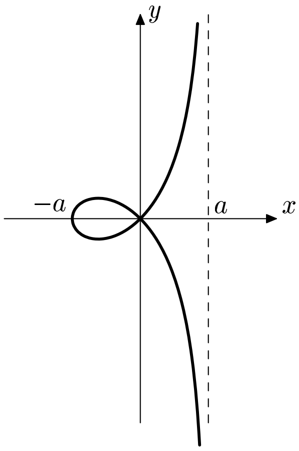
Volem parametritzar-la.

a) Proveu que una recta talla la corba en 0, 1, 2 o 3 punts. Illustreu el resultat sobre el gràfic.
b) Proveu que una recta de pendent m no-vertical que passi per l'origen talla la corba exactament en un punt si $m^2 \neq c$.
c) Considereu ara la recta vertical $x = 1$. Donat un punt $(1, t)$ d'aquesta recta, dibuixeu la recta que el connecta a l'origen. Aquesta recta tallarà a la corba en un punt (x, y). Dibuixeu la construcció, i argumenteu geomètricament per què aquest fet dóna lloc a una parametrització de la corba sencera. Quina és la parametrització que s'obté?

1.3.9. La *strofoide* és una corba que ha estat estudiada per diversos matemàtics, entre els quals destaquen Isaac Barrow (1630-1677), Jean Bernouilli (1667-1748) i Maria Agnesi (1718-1799). Admet una parametrització trigonomètrica, que és la següent:

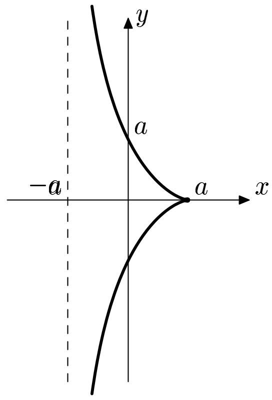
$$\begin{aligned} x &= a\sin(t) \\ y &= a\tan(t)(1+\sin(t)) \end{aligned}$$

on a és una constant. Si variem $-4.2 \leq t \leq 1.0$ obtenim el següent gràfic:

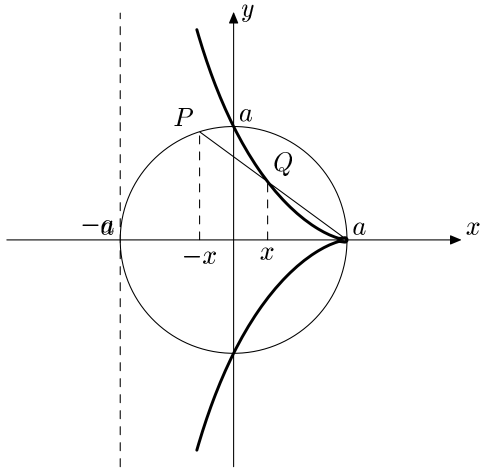


a) Trobeu l'equació en x, y que descriu la strofoide. Aneu amb compte, i comproveu que no és exacte si el resultat obtingut és $(a^2 - x^2)y^2 = x^2(a+x)^2$. Què passa per $x = -a$?
b) Trobeu una parametrització algebraica de la strofoide.

1.3.10. Cap el 180 A.C. Diocles va escriure el llibre *Sobre els miralls*, i en ell va considerar la corba anomenada *cisoide*. La va utilitzar per resoldre el problema de la duplicació del cub. La cisoide té com a equació $y^2(a+x) = (a-x)^3$, on a és una constant. La seva gràfica és la següent:



a) Trobeu una parametrització algebraica de la cisoide.



b) Diocles descriu la cisoide emprant la següent construcció geomètrica. Donat un cercle de radi a (que prendrem centrat a l'origen) prenem x en l'interval $(-a, a]$, i considerem la línia L que uneix al punt $(a, 0)$ al punt del cercle $P = (-x, \sqrt{a^2 - x^2})$. Així queda determinat un punt $Q = (x, y)$ sobre L. Proveu que la cisoide és el lloc geomètric de tots els punts Q.
c) La duplicació del cub és el problema grec classic d'intentar constuir $2^{1/3}$ amb regle i compàs. Sabem que no té solució emprant únicament regle i compàs. Diocles va mostrar que si es permet emprar també

la cisoide, llavors sí que podem constuir $2^{1/3}$. Vegem com funciona. Dibuixeu una línia enllaant $(-a, 0)$ i $(0, a/2)$. Aquesta línia tallarà la cisoide en un punt (x, y). Proveu que

$$2 = \left(\frac{a-x}{y}\right)^3,$$

el que demostra que es pot construir $2^{1/3}$ amb l'ajut de regle compàs i cisoide.

1.3.11. Anem a deduir la següent parametrització de la superfície $x^2 - y^2z^2 + z^3 = 0$:

$$\begin{aligned} x &= t(u^2 - t^2) \\ y &= u \\ z &= u^2 - t^2 \end{aligned}$$

a) Proveu que la corba $x^2 = cz^2 - z^3$ pot ser parametritzada per

$$\begin{aligned} z &= c - t^2 \\ x &= t(c - t^2) \end{aligned}$$

pel mètode del problema 1.3.8.

b) Substituiu c per y^2 en l'apartat anterior i proveu la parametrització desitjada.

c) Expliqueu per què auqesta paramtrització recorre enterament la superfície $\mathbf{V}(x^2 - y^2z^2 + z^3)$.

1.3.12. Sigui la varietat $V = \mathbf{V}(y - x^2, z - x^4) \subset \mathbb{R}^3$

a) Feu una gràfica.

b) Trobeu una paramatrització pel mètode emprat per la cúbica gerxa.

c) Parametritzeu la superfície tangent a V.

1.3.13. Més endavant estudiarem el problema general de trobar una parametrització una superfície. No obstant, quan la superfície és plana, podem fer servir els mètodes de càlcul de l'àlgebra lineal. Sigui, per exemple, el plà de $\mathbb{R}^3$ parametritzat per

$$\begin{aligned} x &= 1 + u - v \\ y &= u + 2v \\ z &= -1 - u + v \end{aligned}$$

Trobeu l'equació del plà. (Nota: Considereu com equació del plà $ax + by + cz = d$. Substitui en la parametrització per obtenir un sistema d'equacions.

Una altra manera d'obtenir-ho fora escriure la parametrització en forma vectorial:

$$(1,0,-1)+u(1,1,-1)+v(-1,2,1)$$

i emprar el producte vectorial.)

1.3.14. Aquest problema tracta de conjunts convexos i serà emprat en el proper per mostrar que una cúbica de Bézier queda a l'interior del seu polígon de control. Un subconjunt $C \subset \mathbb{R}^2$ és *convex* si per cada $P, Q \in C$ el segment que uneix P i Q està íntegrament a l'interior de C.

a) Si $P = \begin{pmatrix} x \\ y \end{pmatrix}$ i $Q = \begin{pmatrix} z \\ w \end{pmatrix}$ estan dins d'un conjunt convex C, proveu que

$$t\begin{pmatrix} x \\ y \end{pmatrix} + (1-t)\begin{pmatrix} z \\ w \end{pmatrix} \in C$$

si $0 \le t \le 1$.

b) Si $P_i = \begin{pmatrix} x_i \\ y_i \end{pmatrix}$ estan dins d'un conjunt convex C per $i \le i \le n$, proveu que

$$\sum_{i=1}^{n} t_i \begin{pmatrix} x_i \\ y_i \end{pmatrix} \in C$$

si $t_1, \dots t_n$ són nombres no-negatius tals que $\sum_{i=1}^{n} t_i = 1$. (Nota: Demostreu-ho per inducció sobre n).

1.3.15. Una cúbica de Bézier ve donada per

$$\begin{aligned} x &= (1-t)^3 x_1 + 3t(1-t)^2 x_2 + 3t^2(1-t)x_3 + t^3 x_4 \\ y &= (1-t)^3 y_1 + 3t(1-t)^2 y_2 + 3t^2(1-t)y_3 + t^3 y_4 \end{aligned}$$

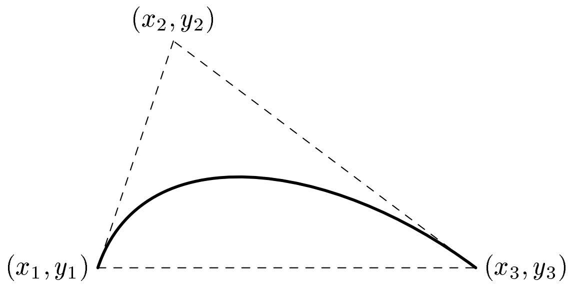
Esciviu les equacions anteriors en forma vectorial i utilitzant el resultat de l'exercici anterior proveu que les cúbiques de Bézier sempre queden a dins del seu polígon de control (Pista: Quant val la suma dels coeficients de l'equació vectorial?).

1.3.16. Un inconvenient de les cúbiques de Bézier és que corbes com hipèrboles o circumferències no poden ser exactament descrites per elles. Ara veurem un mètode per parametritzar seccions còniques. Una secció cònica és una corba en el pla definida per una equació de segon grau de la forma $ax^2 + bxy + cy^2 + dx + ey + f = 0$. Exemples clàssics de còniques són circumferències, el.lipses, paràboles, e hipèrboles. Considerem la corba parametritzada per

$$\begin{aligned} x &= \frac{(1-t)^2 x_1 + 2t(1-t)wx_2 + t^2 x_3}{(1-t)^2 + 2t(1-t)w + t^2} \\ y &= \frac{(1-t)^2 y_1 + 2t(1-t)wy_2 + t^2 y_3}{(1-t)^2 + 2t(1-t)w + t^2} \end{aligned}$$

on $0 \leq t \leq 1$. Les constants $w, x_1, y_1, x_2, y_2, x_3, y_3$ ja venen donades i suposarem també que $w \geq 0$. L'objectiu d'aquest problema ès donar una interpretació geomètrica a les constants $w, x_1, y_1, x_2, y_2, x_3, y_3$.

a) Proveu que la suposició de que $w > 0$ implica que els denominadors de les corbes mai s'anul.len.
b) Avalueu les equacions per $t = 0$ i $t = 1$. Amb això podreu entendre el significat de x_1, y_1, x_3, y_3.
c) Ara avalueu $(x'(0), y'(0))$ i $(x'(1), y'(1))$. Utilitzeu-ho per provar que (x_2, y_2) és la intersecció entre les tangents que formen l'inici i el final de la corba. Expliqueu perqué $(x_1, y_1), (x_2, y_2)$ i (x_3, y_3) són anomenats els punts de control de la corba.
d) Definiu el seu polígon de control (en el nostre cas un triangle), i proveu que la corba definida per les equacions sempre queda dins del seu polígon de control. Pista: Adapta l'argumentació del problema anterior.

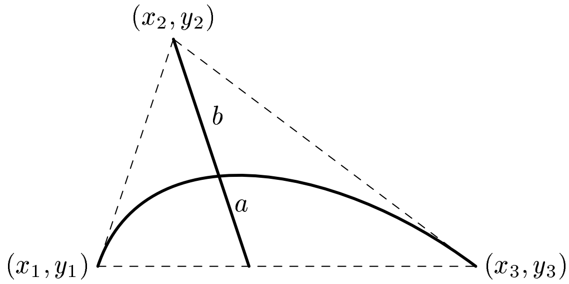


El dibuix intenta explicar el significat de la constant w, anomenada factor aparensa (shape factor). Una pista pot ser la resposta de l'apartat c). Noteu que w apareix en les formules dels vectors tangents quan $t = 0, 1$. Així w controla la velocitat ja que un valor molt gran per w faria que la corba es tanqués a (x_2, y_2). En els dos darrers apartats veurem exactament quin paper juga w.

e) Demostreu que

$$\begin{pmatrix} x\left(\frac{1}{2}\right) \\ y\left(\frac{1}{2}\right) \end{pmatrix} = \frac{1}{1+w}\left(\frac{1}{2}\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} x_3 \\ y_3 \end{pmatrix}\right) + \frac{w}{1+w}\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$$

Feu servir aquesta equació per demostrar que $(x\left(\frac{1}{2}\right), y\left(\frac{1}{2}\right))$ està sobre el segment que connecta (x_2, y_2) al punt mig entre (x_1, y_1) i (x_3, y_3).



f) Noteu que $\left(x\left(\frac{1}{2}\right), y\left(\frac{1}{2}\right)\right)$ parteix el segment en dos troos de longitud a i b tal com indica el dibuix. Demostreu que

$$w = \frac{a}{b}$$

Observeu doncs que w ens indica exactament si la corba talla el segment. Pista: Utilitzeu la fórmula de la distància.

1.3.17. Utilitzeu les equacions del problema anterior per parametritzar l'arc de circumferència $x^2 + y^2 = 1$ des de $(1, 0)$ fins a $(0, 1)$. Pista: Mireu l'apartat f) del problema anterior per demostrar que $w = 1/\sqrt{2}$.

1.4. **Ideals.** **1.4.1.** Les següents equacions descriuen la intersecció entre una circumferència i una hipèrbola.

$$\begin{aligned} x^2 + y^2 - 1 &= 0 \\ xy - 1 &= 0 \end{aligned}$$

a) Alleu la y.
b) Demostreu que el polinomi trobat a l'anterior apartat queda a dins de $< x^2 + y^2 - 1, xy - 1 >$. Pista: Multipliqueu la segona equació per $xy + 1$.

1.4.2. Demostreu les següents igualtats entre ideals en $k[x, y]$:

a) $< x + y, x - y > = < x, y >$.
b) $< x + xy, y + xy, x^2, y^2 > = < x, y >$.
c) $< 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 > = < x^2 - 4, y^2 - 1 >$.

Observeu, doncs, que un mateix ideal pot tenir diferents bases i que les diverses bases poden tenir diferent nombre d'elements.

1.4.3. El mot base s'utilitza en diversos contextes dins les matemàtiques. En aquest problema veurem que una base d'ideal és molt diferent d'una base d'un subespai, que s'estudia a l'algebra lineal.

a) Considereu l'ideal $I = < x > \subset k[x]$. Com ideal de $k[x]$ te una base que consta d'un únic element x. Però pot ser vist com un subespai de $k[x]$ (espai vectorial sobre k). Demostreu que tota base vectorial de I sobre k és infinita. Pista: És suficient trobar una base que sigui infinita. En canvi, acceptant multiplicar x per elements de $k[x]$, en lloc d'elements de k fa que $< x >$ sigui una base finita.

b) A l'àlgebra lineal, una base està formada per un conjunt de generadors i ha de ser linealment independent sobre k. Per un ideal, en canvi, únicament ha de ser un conjunt de generadors, i no s'exigeix independència. La raó d'això és que amb coeficients polinomials no és posible la independència. Per veure això considereu el següent ideal $< x, y > \subset k[x, y]$. Demostreu que hi ha una combinació lineal de y i x amb coeficients polinomics no nuls, de manera que el resultat és igual a zero.

c) Suposem que $f_1, \ldots, f_s$ és la base d'un ideal $I \subset k[x_1, \ldots, x_n]$. Demostreu que si $s \geq 2$ i $f_i \neq 0$ per tot i aleshores, donats i,j, es pot escriure una combinació lineal de f_i i f_j que sigui igual a zero, amb coeficients polinomics no nuls.

d) Una consequència de la falta d'indepèndencia és que quan escrivim un element $f \in < f_1, \ldots, f_s >$ com $f = \sum_{i=1}^{n} h_i f_i$, els coeficients h_i no són únics. Com exemple considereu $f = x^2 + xy + y^2 \in < x, y >$. Expresseu f de dues maneres diferents, com a combinació lineal de x i de y.

e) Una base $f_1, \ldots, f_s$ d'un ideal I s'anomena minimal si cap subconjunt propi de $f_1, \ldots, f_s$ és base de I. Per exemple x, x^2 és una base d'un ideal, però no és minimal ja que amb només x podem generar el mateix ideal. Un ideal pot tenir diverses bases minimals amb diferent nombre d'elements entre elles. Per veure-ho, demostreu que $\{x\}$ i $\{x + x^2, x^2\}$ són bases minimals del mateix ideal de $k[x]$. Compareu la mateixa situació amb l'algebra lineal.

1.4.4. Demostreu que $\mathbf{I}(\mathbf{V}(x^n, y^m)) = < x, y >$ per qualsevol enter positiu n i m.

1.4.5. L'ideal $\mathbf{I}(V)$ d'una varietat te una propietat especial, que no tenen tots els ideals. Definim que un ideal I és *radical*, si quan conté una potència f^m (d'un polinomi f), llavors f també pertany a I. Més concretament, I és radical quan $f \in I$ si i només si $f^m \in I$ per algun enter positiu m.

a) Demostreu que $\mathbf{I}(V)$ és sempre un ideal radical.

b) Demostreu que $< x^2, y^2 >$ no és un ideal radical. Això vol dir que $< x^2, y^2 > \neq \mathbf{I}(V)$ per tota varietat $V \subset K^2$.

1.4.6. Anomenem cúbica guerxa a la varietat $V = \mathbf{V}(y - x^2, z - x^3)$.

a) Utilitzeu la parametrització de la cúbica guerxa per demostrar que $y^2 - xz \in \mathbf{I}(V)$.

b) Expresseu $y^2 - xz$ com a combinació de $y - x^2$ i $z - x^3$.

1.4.7. Demostreu que $\mathbf{I}(V(x - y)) = < x - y >$. El vostre raonament hauria de ser vàlid per qualsevol cos infinit k.

1.4.8. Sigui $V \subset \mathbb{R}^3$ una corba parametritzada per (t, t^3, t^4).

a) Demostreu que V és una varietat afí.
b) Adapteu el mètode emprat en el problema de la cúbica guerxa per determinar $\mathbf{I}(V)$.

1.4.9. Sigui $I \subset \mathbb{F}_2[x,y]$ l'ideal dels polinomis que s'anulen a tot $\mathbb{F}_2^2$. L'objectiu del problema és demostrar que $I = < x^2 - x, y^2 - y >$.

a) Demostreu que $< x^2 - x, y^2 - y > \subset I$.
b) Demostreu que tot $f \in \mathbb{F}_2[x,y]$ pot ser escrit com $f = A(x^2 - x) + B(y^2 - y) + axy + bx + cy + d$ on $A, B \in \mathbb{F}_2[x,y]$ i $a, b, c, d \in \mathbb{F}_2$. Pista: Escriviu f de la forma $\sum_i p_i(x)y^i$ i utilitzeu l'algorisme de la divisió.
c) Demostreu que $axy + bx + cy + d \in I$ si i només si $a = b = c = d = 0$.
d) Utilitzant els apartats b) i c) acabeu de demostrar que $I = < x^2 - x, y^2 - y >$.
e) Expresseu $x^2y + y^2x$ com a combinació de $x^2 - x$ i $y^2 - y$. Pista: Recordeu que $2 = 1 + 1 = 0$ en $\mathbb{F}_2$.

1.4.10. S'ha definit ja $\mathbf{I}(V)$, per a una varietat $V \subset K^n$. Això es pot generalitzar de la següent manera: si S és un conjunt qualsevol tal que $S \subset K^n$ llavors tenim que :

$$\mathbf{I}(S) = \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \ \forall \ (a_1, \ldots, a_n) \in S\}$$

a) Demostreu que $\mathbf{I}(S)$ és un ideal.
b) Sigui $X = \{(a,a) \in \mathbb{R}^2 : a \neq 1\}$. Determineu $\mathbf{I}(\mathbf{X})$.
c) Siguin $\mathbb{Z}^n$ els punts de $\mathbb{C}^n$ amb coordenades enteres. Determineu $\mathbf{I}(\mathbb{Z}^n)$.

1.5. **Polinomis d'una variable. 1.5.1.** Considereu el següent determinant $n \times n$ de Vandermonde determinat per $a_1, \ldots, a_n$ pertanyents a un cos k:

$$det \begin{pmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & \ldots & a_n^{n-1} \end{pmatrix}$$

Demostreu que si les a_i's són diferents entre elles, llavors el determinant és diferent de zero. Pista: Si el determinant és zero, llavors les columnes són linealment dependents. Demostreu que els coeficients d'una combinació lineal determinen un polinomi de grau $\leq n - 1$ amb n arrels.

1.5.2. Demostreu que si h és el GCD de $f, g \in k[x]$, llavors existeixen dos polinomis $A, B \in k[x]$ tal que $Af + Bg = h$.

1.5.3. Donats $f_1, \ldots, f_s \in k[x]$, considereu $h = \mathrm{GCD}(f_2, \ldots, f_s)$. Utilitzeu la igualtat $< h > = < f_2, \ldots, f_s >$ per demostrar que
$< f_1, h > = < f_1, f_2, \ldots, f_s >$.

1.5.4. Suposem que només podeu computar el GCD de dos polinomis simultàniament, (lo qual és cert per la majoria de sistemes de computació algebraica). Doneu el pseudocodi d'un algorisme que calcula el GCD de polinomis $f_1, \dots, f_s \in k[x]$, on $s > 2$. Demostreu que l'algorisme funciona. Pista: Mireu el problema anterior.

1.5.5. Utilitzeu un sistema de computació algebraica per calcular els següents GCD's sobre $\mathbb{Q}$:

a) $\mathrm{GCD}(x^4 + x^2 + 1, x^4 - x^2 - 2x - 1, x^3 - 1)$.
b) $\mathrm{GCD}(x^3 + 2x^2 - x - 2, x^3 - 2x^2 - x + 2, x^3 - x^2 - 4x + 4)$.

1.5.6. Utilitzeu el mètode donat a classe per decidir si:

$$x^4 - 4 \in < x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4, x^3 - 2x^2 - x + 2 >$$

1.5.7. Doneu el pseudocodi d'un algorisme que rebi com a entrada $f, g \in k[x]$ i com a sortida calculi $h, A, B \in k[x]$, on $h = \mathrm{GCD}(f, g)$ i $Af + Bg = h$.

1.5.8. En aquest exercici estudiarem l'anomenat problema de la consistència en el cas d'una variable. Donats $f_1, \dots, f_s \in k[x]$, ens preguntarem si hi ha un algorisme per decidir si $\mathbf{V}(f_1, \dots, f_s)$ és diferent del buit. Veurem que la resposta és positiva quan $k = \mathbb{C}$.

a) Sigui $f \in \mathbb{C}[x]$ un polinomi no nul. Demostreu que $\mathbf{V}(f) = 0$ si i només si f és constant.
b) Si $f_1, \dots, f_s \in \mathbb{C}[x]$ demostreu que $\mathbf{V}(f_1, \dots, f_s) = 0$ si i només si $\mathrm{GCD}(f_1, \dots, f_s) = 1$.
c) Feu un algorisme que determini si $\mathbf{V}(f_1, \dots, f_s)$ és diferent del buit.

Quan $k = \mathbb{R}$, el problema de la consistència és molt més complicat. Requereix donar un algorisme que determini si un polinomi $f \in \mathbb{R}[x]$ té alguna arrel real.

1.5.9. Ara estudiarem el problema del Nullstellensatz en el cas d'una variable. Ens preguntarem per la relació entre $\mathbf{I}(\mathbf{V}(f_1, \dots, f_s))$ i $< f_1, \dots, f_s >$ quan $f_1, \dots, f_s \in \mathbb{C}[x]$. Utilitzant GCDs, ho podrem reduir al cas d'un unic generador. Determinarem explícitament $\mathbf{I}(\mathbf{V}(f))$ quan $f \in \mathbb{C}[x]$ no sigui un polinomi constant. Definim el polinomi: $f_{red} = c(x - a_1) \dots (x - a_l)$. Noteu que f i f_{red} tenen les mateixes arrels, però les seves mutltiplicitats són diferents. Concretament totes les arrels de f_{red} tenen multiplicitat 1. Es comú anomenar f_{red} com redut de f o lliure de quadrats. Per explicar aquest darrer nom, noteu que f_{red} és el factor de f de grau més alt, lliure de quadrats.

a) Demostreu que $\mathbf{V}(f) = \{a_1, \dots, a_l\}$.
b) Demostreu que $\mathbf{I}(\mathbf{V}(f)) =< f_{red} >$.

1.5.10. En aquest problema estudiarem la derivada formal d'un polinomi $f = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \in \mathbb{C}[x]$. La derivada formal es definida normalment com: $f' = na_0^{n-1} + (n-1)a_1x^{n-2} + \cdots + a_{n-1} + 0$. Demostreu les següents regles de derivació:

$$\begin{aligned} (af)' &= af', \quad a \in \mathbb{C} \\ (f+g)' &= f' + g' \\ (fg)' &= f'g + fg' \end{aligned}$$

1.5.11. Ara utilitzarem les propietats de derivació de l'exercici anterior per calcular el $\mathrm{GCD}(f, f')$ quan $f \in \mathbb{C}[x]$.

a) Suposant que $f = (x-a)^r h$ en $\mathbb{C}[x]$ on $h(a) \neq 0$, demostreu que $f' = (x-a)^{r-1}h_1$ on $h_1 \in \mathbb{C}[x]$ no s'anul.la quan $x = a$.

b) Sigui $f = c(x-a_1)^{r_1} \ldots (x-a_l)^{r_l}$ la factorització de f, on $a_1, \ldots, a_l$ són diferents entre ells. Demostreu que $f' = (x-a_1)^{r_1-1} \ldots (x-a_l)^{r_l-1}H$, on $H \in \mathbb{C}[x]$ és un polinomi que no s'anula en $a_1, \ldots, a_l$.

c) Demostreu que $\mathrm{GCD}(f, f') = (x-a_1)^{r_1-1} \ldots (x-a_l)^{r_l-1}$.

1.5.12. Aquest problema tracta del polinomi lliure de quadrats f_{red} de $f \in \mathbb{C}[x]$, definit a l'exercici 5.9.

a) Utilitzeu l'exercici anterior per demostrar que f_{red} s'obté amb la fórmula:

$$f_{red} = \frac{f}{\mathrm{GCD}(f, f')}$$

La virtut d'aquesta fórmula es que ens permet trobar el polinomi lliure de quadrats sense haver de factoritzar f. Això permet donar una descripció algebraica.

b) Utilitzeu un sistema de computació algebraica per trobar el polinomi lliure de quadrats de:

$$x^{11} - x^{10} + 2x^8 - 4x^7 + 3x^5 - 3x^4 + x^3 + 3x^2 - x - 1$$

1.5.13. Utilitzeu l'exercici anterior i el 5.9 per descriure un algorisme que té com entrada els polinomis $f_1, \ldots, f_s \in \mathbb{C}[x]$ i com a sortida una base de $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$. Tal algorisme és molt més difícil de fer quan es tracta de polinomis de més d'una variable.

1.5.14. Trobeu una base per l'ideal $\mathbf{I}(\mathbf{V}(x^5 - 2x^4 + 2x^2 - x, x^5 - x^4 - 2x^3 + 2x^2 + x - 1))$.

2. Bases de Groebner

2.1. **Introducció a les bases de Groebner. 2.1.1.** Determineu si els següents polinomis pertanyen al corresponent ideal $I \subset \mathbb{R}[x]$.

a) $f(x) = x^2 - 3x + 3$. $I = < x - 2 >$.
b) $f(x) = x^5 - 4x + 1$. $I = < x^3 - x^2 + x >$.
c) $f(x) = x^2 - 4x + 4$. $I = < x^3 - 6x^2 + 12x - 8, 2x^3 - 10x^2 + 16x - 8 >$.
d) $f(x) = x^3 - 1$. $I = < x^9 - 1, x^5 + x^3 - x^2 - 1 >$.

2.1.2. Trobeu una parametrització per cada una de les varietats afins definides pels següents sistemes d'equacions:

a) En $\mathbb{R}^3$ o $\mathbb{C}^3$:

$$\begin{aligned} 2x + 3y - z &= 9 \\ x - y &= 1 \\ 3x + 7y - 2z &= 17 \end{aligned}$$

b) En $\mathbb{R}^4$ o $\mathbb{C}^4$:

$$\begin{aligned} x_1 + x_2 - x_3 - x_4 &= 0 \\ x_1 - x_2 + x_3 &= 0 \end{aligned}$$

c) En $\mathbb{R}^3$ o $\mathbb{C}^3$:

$$\begin{aligned} y - x^3 &= 0 \\ z - x^5 &= 0 \end{aligned}$$

2.1.3. Trobeu les equacions implícites per les següents varietats afins parametritzades:

a) En $\mathbb{R}^3$ o $\mathbb{C}^3$:

$$\begin{aligned} x_1 &= t - 5 \\ x_2 &= 2t + 1 \\ x_3 &= -t + 6 \end{aligned}$$

b) En $\mathbb{R}^5$ o $\mathbb{C}^5$:

$$\begin{aligned} x_1 &= 2t - 5u \\ x_2 &= t + 2u \\ x_4 &= -t + u \\ x_5 &= t + 3u \end{aligned}$$

c) En $\mathbb{R}^3$ o $\mathbb{C}^3$:

$$\begin{aligned} x &= t \\ y &= t^4 \\ z &= t^7 \end{aligned}$$

2.1.4. Sigui $x_1, x_2, x_3, \ldots$ una col.lecció infinita de variables independents indexades pels naturals. Un polinomi en les x_i amb coeficients dins un cos k, és una combinació lineal finita de monomis $x_{i_1}^{e_1} \ldots x_{i_n}^{e_n}$. R denotarà el conjunt de tots els polinomis en les x_i. Noteu que podem sumar o multiplicar elements de R de la manera habitual. Així tenim que R és l'anell de polinomis de $k[x_1, x_2, \ldots]$ amb infinites variables.

a) Sigui $I = < x_1, x_2, x_3, \cdots >$ el conjunt de polinomis de la forma $x_{i_1} f_1 + \cdots + x_{i_m} f_m$, on $f_j \in R$. Demostreu que I és un ideal de l'anell R.
b) Demostreu, trobant una contradicció, que I no té un conjunt generador finit. Pista: No és suficient considerar tant sols subconjunts de $\{x_i : i \geq 1\}$.

2.1.5. En aquest problema demostrarem que tota corba polinòmicament parametritzada en k^2, està continguda en una varietat afí.

a) Demostreu que el nombre de monomis diferents $x^e y^f$ de grau $\leq m$ en $k[x, y]$ és igual a $(m+1)(m+2)/2$. (Nota : $\begin{pmatrix} m+2 \\ 2 \end{pmatrix}$ és el coeficient binomial).
b) Demostreu que si $f(t)$ i $g(t)$ són polinomis de grau $\leq n$, aleshores per un m suficientment gran, els monomis :

$$[f(t)]^e [g(t)]^f$$

amb $e + f \leq m$ formen un conjunt linealment dependent en $k[t]$.
c) Deduu de l'apartat b) que si $C : x = f(t), y = g(t)$ és una corba corba parametritzada polinòmicament en k^2, aleshores C està contingut en $\mathbf{V}(F)$ per algun $F \in k[x, y]$.
d) Generalitzeu els apartats b) i c) per demostrar que tota superfície parametritzada per polinomis:

$$x = f(t, u), \ y = g(t, u), \ z = h(t, u)$$

està continguda en una varietat (superfície) algebraica $\mathbf{V}(F)$, on $F \in k[x, y, z]$.

2.2. **Ordres Monomials sobre $k[x_1, \ldots, x_n]$.** Notació:

lex:	lexicogràfic
grevlex:	grau total i després lexicogràfic invers
grlex:	grau total i després lexicogràfic
LM:	Monomi principal
LT:	Terme principal
GCD:	Màxim comú divisor

2.2.1. Reescriviu els següents polinomis, ordenant els termes segons *lex*, *grlex*, i *grevlex*, donant $\mathrm{LM}(f)$, $\mathrm{LT}(f)$, i $\mathrm{multideg}(f)$ en cada cas.

a) $f(x,y,z) = 2x + 3y + z + x^2 - z^2 + x^3$.
b) $f(x,y,z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$.

2.2.2. Cada un dels següents polinomis estan escrits com monomis ordenats segons *lex*, *grlex* o *grevlex*. Determineu quin ordre ha estat utilitzat en cada cas.

a) $f(x,y,z) = 7x^2y^4z - 2xy^6 + x^2y^2$.
b) $f(x,y,z) = xy^3z + xy^2z^2 + x^2z^3$.
c) $f(x,y,z) = x^4y^5z + 2x^3y^2z + 4xy^2z^4$.
d) $f(x,y,z) = x^4y^5z + 2x^3y^2z^2 + 4xy^2z^4$.

2.2.3. Repetiu el primer problema amb les variables ordenades així : $z > y > x$.

2.2.4. Demostreu que *grlex* és un ordre monomial.

2.2.5. Demostreu que *grevlex* és un ordre monomial.

2.2.6. Un altre ordre monomial és el lexicogràfic invers o ordre *invlex* definit de la següent manera: $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, $\alpha >_{invlex} \beta$ si i només si la primera component per la dreta no nula de $\alpha - \beta$ és positiva. Demostreu que *invlex* és equivalent a *lex* amb les variables permutades d'una certa manera. (De quina manera?).

2.2.7. Sigui $>$ un cert ordre monomial.

a) Demostreu que $\alpha \geq 0$ $\forall \alpha \in \mathbb{Z}^n_{\geq 0}$.
b) Demostreu que si x^α divideix a x^β, aleshores $\alpha \leq \beta$. És cert l'invers?
c) Demostreu que si $\alpha \in \mathbb{Z}^n_{\geq 0}$ aleshores α és l'element més petit de $\alpha + \mathbb{Z}^n_{\geq 0}$.

2.2.8. Definiu amb cura, que s'enten per un sistema d'equacions lineals en forma esglaonada, utilitzant l'ordre $x_1 > x_2 > \ldots x_n$.

2.2.9. Sigui $>$ un ordre monomial sobre $k[x_1, \ldots, x_n]$.

a) Sigui $f \in k[x_1, \ldots, x_n]$ i sigui m un monomi. Demostreu que $\mathrm{LT}(m \cdot f) = m \cdot \mathrm{LT}(f)$.
b) Sigui $f, g \in k[x_1, \ldots, x_n]$. És $\mathrm{LT}(f \cdot g)$ necessàriament igual a $\mathrm{LT}(f) \cdot \mathrm{LT}(g)$?.

c) Suposem que $f_i, g_i \in k[x_1, \ldots, x_n]$ i $1 \leq i \leq s$. Llavors $\mathrm{LM}(\sum_{i=1}^{s} f_i g_i)$ és necessàriament igual a $\mathrm{LM}(f_i) \cdot \mathrm{LM}(g_i)$ per a algun i ?.

2.3. **Algorisme de la divisió.** **2.3.1.** Calculeu el residu de la divisió del polinomi f per el conjunt ordenat F. Utilitzeu l'ordre *grlex* i el *lex* en cada cas.

a) $f = x^7y^2 + x^3y^2 - y + 1 \quad F = (xy^2 - x, x - y^3)$.
b) Repetiu-ho permutant els polinomis de F.

2.3.2. Calculeu el residu de la divisió :

a) $f = xy^2z^2 + xy - yz \quad F = (x - y^2, y - z^3, z^2 - 1)$.
b) Repetiu-ho fent permutacions cícliques de F.

2.3.3. Utilitzant un sistema de computació algebraica, comproveu els resultats dels dos problemes anteriors. (Consulteu el manual per saber si el sistema ja té implementat el quocient de polinomis, o si per contra heu d'implementar l'algorisme vosaltres mateixos)

2.3.4. Ara estudiarem la divisió de $f = x^3 - x^2y - x^2z + x$ per $f_1 = x^2y - z$ i $f_2 = xy - 1$

a) Calculeu utilitzant l'ordre *grlex* :

$$r_1 = \text{residu de dividir } f \text{ per } (f_1, f_2)$$

$$r_2 = \text{residu de dividir } f \text{ per } (f_2, f_1)$$

Els resultats haurien de ser diferents. En quin pas de l'algorisme radica la diferència?. (Cal que feu uns quants passos a mà)

b) És $r = r_1 - r_2$ a l'ideal $< f_1, f_2 >$?. Si la resposta és positiva trobeu una expressió explícita de $r = Af_1 + Bf_2$, i si no digueu el perquè.
c) Calculeu el residu de la divisió de r per (f_1, f_2). Perquè podriem haber previst el resultat abans de fer la divisió?
d) Trobeu un altre polinomi $g \in < f_1, f_2 >$ tal que el residu de la divisió de g per (f_1, f_2) sigui diferent de zero. Pista: $(xy + 1) \cdot f_2 = x^2y^2 - 1$, mentre que $y \cdot f_1 = x^2y^2 - yz$.
e) Ens dona l'algorisme de la divisió, una solució per el problema de la pertinena d'ideals, per l'ideal $< f_1, f_2 >$?. Expliqueu la vostra resposta.

2.3.5. Utilitzant l'ordre *grlex*, trobeu un element g de $< f_1, f_2 > = < 2xy^2 - x, 3x^2y - y - 1 > \subset \mathbb{R}[x, y]$ tal que el residu de dividir-l'ho per (f_1, f_2) sigui diferent de zero. Pista: Podeu trobar un tal g on el residu sigui el propi g.

2.3.6. Responeu la pregunta del problema anterior per $< f_1, f_2, f_3 > = < x^4y^2 - z, x^3y^3 - 1, x^2y^4 - 2z > \subset \mathbb{R}[x, y, z]$. Trobeu dos polinomis diferents.

2.3.7. Proveu de construir un patrò general que s'ajusti als tres exercicis anteriors. Quina condició sobre el terme principal del polinomi $g = A_1 f_1 + \cdots + A_s f_s$ garantiria que hi hagués un residu diferent de zero en el quocient per $(f_1, \ldots, f_s)$?. Com afecta la vostra condició al problema de la pertinena a ideals?.

2.3.8. Ja hem vist que tot polinomi $f \in \mathbb{R}[x, y, z]$ pot ser escrit com

$$f = h_1(y - x^2) + h_2(z - x^3) + r$$

on r és un polinomi depenent de x i $\mathbf{V}(y - x^2, z - x^3)$ és la cúbica guerxa de $\mathbb{R}^3$.

a) Doneu una prova d'aquest fet utilitzant l'algorisme de la divisió. Pista: Cal que especifiqueu amb cura l'ordre monomial utilitzat.
b) Utilitzeu la parametrització de la cúbica guerxa per demostrar que $z^2 - x^4 y$ s'anul.la sobre la corba.
c) Trobeu una representació explícita de

$$z^2 - x^4 y = h_1(y - x^2) + h_2(z - x^3)$$

utilitzant l'algorisme de la divisió.

2.3.9. Sigui $V \subset \mathbb{R}^3$ una corba parametritzada per (t, t^m, t^n), $n, m \geq 2$.

a) Demostreu que V és una varietat afí.
b) Determineu $\mathbf{I}(V)$.

2.3.10. Amb aquest exercici volem caracteritzar completament l'expressió

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + r$$

resultat de l'algorisme de la divisió (entre totes les possibles expressions de f d'aquesta forma). Sigui $\mathrm{LM}(f_i) = x^{\alpha(i)}$ i definim

$$\begin{aligned}
\triangle_1 &= \alpha(1) + \mathbb{Z}^n_{\geq 0}, \\
\triangle_2 &= (\alpha(2) + \mathbb{Z}^n_{\geq 0}) - \triangle_1, \\
&\vdots \\
\triangle_s &= (\alpha(s) + \mathbb{Z}^n_{\geq 0}) - \left(\bigcup_{i=1}^{s-1} \triangle_i \right) \\
\bar{\triangle} &= \mathbb{Z}^n_{\geq 0} - \left(\bigcup_{i=1}^{s} \triangle_i \right)
\end{aligned}$$

(Observeu que $\mathbb{Z}^n_{\geq 0}$ és la unió disjunta dels $\triangle_i$ i $\bar{\triangle}$.)

a) Proveu que $\beta \in \triangle_i$ ssi $x^{\alpha(i)}$ divideix a x^β , i cap $x^{\alpha(j)}$ amb $j < i$ divideix x^β.
b) Proveu que $\gamma \in \bar{\triangle}$ ssi cap $x^{\alpha(i)}$ divideix a x^γ.

c) Proveu que a l'expressió $f = a_1f_1 + a_2f_2 + \cdots + a_sf_s + r$ obtinguda per l'algorisme de la divisió, per a tot i, cada monomi x^β de a_i verifica $\beta + \alpha(i) \in \triangle_i$, i cada monomi x^γ de r verifica $\gamma \in \bar{\triangle}$

d) Proveu que existeix una i una sola expressió de la forma $f = a_1f_1 + a_2f_2 + \cdots + a_sf_s + r$ que verifiqui les propietats de l'apartat c).

2.3.11. Demostreu que l'operació de calcular residus en divisions per $F = (f_1, \ldots, f_s)$ és $k-$lineal. O sigui, si el residu de dividir g_i per F és r_i per $i = 1, 2$, aleshores, per tot $c_1, c_2 \in k$, el residu de dividir $c_1g_1 + c_2g_2$ és $c_1r_1 + c_2r_2$. (Feu servir l'exercici anterior.)

2.4. **Ideals de monomis i lema de Dickson.** **2.4.1.** Sigui $I \subset k[x_1, \ldots, x_n]$ un ideal que té la propietat de que per tot $f = \sum_\alpha c_\alpha x^\alpha \in I$, cada monomi x^α de f també pertany a I. Demostreu que I és un ideal de monomis.

2.4.2. Sigui $I = < x^6, x^2y^3, xy^7 > \subset k[x, y]$

a) En el pla-(m, n), dibuixeu el conjunt de vectors (m, n) de monomis x^my^n que siuin elements de I.

b) Si nosaltres apliquem l'algorisme de la divisió a un element $f \in k[x, y]$, utilitzant els generadors de I com a divisors, quins termes poden apareixer en el reste?

2.4.3. Sigui $I = < x^\alpha : \alpha \in A >$ un ideal de monomis, i suposem que tenim una base finita $I = < x^{\beta(1)}, \ldots, x^{\beta(s)} >$. En la demostració del lema de Dickson, vàrem observar que cada $x^{\beta(i)}$ era divisible per $x^{\alpha(i)}$ per algún $\alpha(i) \in A$. Demostreu que $I = < x^{\alpha(1)}, \ldots, x^{\alpha(s)} >$.

2.4.4. Proveu que el lema de Dickson és equivalent a la següent proposició : Donat un subconjunt $A \subset \mathbb{Z}^n_{\geq 0}$, hi ha una col.lecció finita d'elements $\alpha(1), \ldots, \alpha(s) \in A$ tal que per cada $\alpha \in A$, existeix algún i i algún $\gamma \in \mathbb{Z}^n_{\geq 0}$ tal que $\alpha = \alpha(i) + \gamma$.

2.4.5. Una base $\{x^{\alpha(1)}, \ldots, x^{\alpha(s)}\}$ d'un ideal de monomis I, es diu que és *minimal* si cap $x^{\alpha(i)}$ de la base divideix a un altre $x^{\alpha(j)}$ per $i \neq j$.

a) Proveu que tot ideal de monomis té una base minimal.

b) Demostreu que tot ideal de monomis té una *única* base minimal.

2.4.6. Si $I = < x^{\alpha(1)}, \ldots, x^{\alpha(s)} >$ és un ideal de monomis, demostreu que un polinomi f pertany a I si i només si el residu de dividir f per $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ és zero.

2.4.7. Sigui l'anell de polinomis $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$. Definim un ordre monomial $>_{combi}$ en l'anell, que combini ordre *lex* per $x_1, \ldots, x_n$ i ordre *grlex* per $y_1, \ldots, y_m$. Si denotem $x^\alpha y^\beta$ els monomis de $m+n$ variables, on $\alpha \in \mathbb{Z}^n_{\geq 0}$

i $\beta \in \mathbb{Z}^m_{\geq 0}$, definim l'ordre $>_{combi}$ com :

$$x^\alpha y^\beta >_{combi} x^\gamma y^\delta \iff x^\alpha >_{lex} x^\gamma \text{ o be } x^\alpha = x^\gamma \; i \; y^\beta >_{grlex} y^\delta$$

Demostreu que $>_{combi}$ és un ordre monomial. Aquest és un exemple d'ordre producte. Podem crear molts altres ordres monomials seguint aquest mètode.

2.4.8. En aquest problema estudiarem un cas especial d'*ordre amb pes.* Sigui $\mathbf{u} = (u_1, \ldots, u_n)$ un vector de $\mathbb{R}^n$ tal que $u_1, \ldots, u_n$ son positius i linealment independents sobre $\mathbb{Q}$. Direm que $\mathbf{u}$ és un *vector de pes independent.* Per tot $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, definim

$$\alpha >_{\mathbf{u}} \beta \iff \mathbf{u} \cdot \alpha > \mathbf{u} \cdot \beta$$

on el punt representa el producte escalar de vectors. Anomenerem $>_{\mathbf{u}}$ *ordre amb pes* determinat per $\mathbf{u}$.

a) Demostreu que $>_{\mathbf{u}}$ és un ordre monomial. Pista : En quin punt de la demostració, utilitzeu la independència lineal de $u_1, \ldots, u_n$?.
b) Demostreu que $\mathbf{u} = (1, \sqrt{2})$ és un vector de pes independent i que $>_{\mathbf{u}}$ és un ordre amb pes a $\mathbb{Z}^2_{\geq 0}$.
c) Demostreu que $\mathbf{u} = (1, \sqrt{2}, \sqrt{3})$ és un vector de pes independent i que $>_{\mathbf{u}}$ és un ordre de pes a $\mathbb{Z}^3_{\geq 0}$.

2.4.9. Un altre ordre amb pes que té interés es construeix de la següent manera. Sigui $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{Z}^n_{\geq 0}$, i $>_\sigma$ un ordre monomial (com per exemple $>_{lex}$ o $>_{grlex}$) de $\mathbb{Z}^n_{\geq 0}$. Per tot $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, definim $\alpha >_{\mathbf{u},\sigma} \beta$ si i només si

$$\mathbf{u} \cdot \alpha > \mathbf{u} \cdot \beta \text{ o bé } \mathbf{u} \cdot \alpha = \mathbf{u} \cdot \beta \text{ i } \alpha >_\sigma \beta$$

Anomenem $>_{\mathbf{u},\sigma}$ l'ordre amb pes determinat per $\mathbf{u}$ i $>_\sigma$.

a) Demostreu que $>_{\mathbf{u},\sigma}$ és un ordre monomial.
b) Trobeu un $\mathbf{u} \in \mathbb{Z}^n_{\geq 0}$ tal que l'ordre $>_{\mathbf{u},\sigma}$ sigui exactament l'ordre $>_{grevlex}$.
c) En la definició de $>_{\mathbf{u},\sigma}$ l'ordre $>_\sigma$ es fa servir per trencar les classes, ja que sempre apareixen classes en aquest cas. Demostreu que donat un $\mathbf{u} \in \mathbb{Z}^n_{\geq 0}$, hi ha un $\alpha \neq \beta \in \mathbb{Z}^n_{\geq 0}$ tal que $\mathbf{u} \cdot \alpha = \mathbf{u} \cdot \beta$. Pista: Considereu l'equació lineal $u_1 a_1 + \cdots + u_n a_n = 0$ sobre $\mathbb{Q}$. Demostreu que té una solució entera diferent de zero $(a_1, \ldots, a_n)$, i demostreu també que $(a_1, \ldots, a_n) = \alpha - \beta$ per algún $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$.
d) Un exemple útil de pes amb ordre és l'*ordre d'eliminació* introdut per BAYER i STILLMAN (1987). Fixem un enter $1 \leq i \leq n$ i sigui $\mathbf{u} = (1, \ldots, 1, 0, \ldots, 0)$ amb i uns i $n - i$ zeros. S'anomena *i-èsim ordre d'eliminació* $>_i$ a l'ordre amb pes $>_{\mathbf{u},grevlex}$. Proveu que $>_i$ té la següent propietat: Si x^α és un monomi qualsevol en el que apareix alguna de les variables $x_1, \ldots, x_i$, llavors $x^\alpha > x^\beta$ per tot monomi que únicament conté les variables $x_{i+1}, \ldots, x_n$. Els ordres d'eliminació juguen un paper important en la teoria de l'eliminació del proper capítol.

2.5. **El teorema de les bases de Hilbert i de Groebner. 2.5.1.** Sigui $I = < g_1, g_2, g_3 > \subset \mathbb{R}[x, y, z]$ on $g_1 = xy^2 - xz + y, g_2 = xy - z^2$ i $g_3 = x - yz^4$. Utilitzant l'ordre lex, doneu un exemple de $g \in I$ tal que $\mathrm{LT}(g) \notin < \mathrm{LT}(g_1), \mathrm{LT}(g_2), \mathrm{LT}(g_3) >$.

2.5.2. Demostreu que $< \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) >$ és estrictament més petit que $< \mathrm{LT}(I) >$ pels ideals i generadors donats en els exercicis 2.3.5, 2.3.6 i 2.3.7.

2.5.3. Ara generalitzeu els dos exercicis anteriors. Sigui $I = < f_1, \ldots, f_s >$ un ideal tal que $< \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) >$ és estrictament més petit que $< \mathrm{LT}(I) >$.

a) Proveu que hi ha algun $f \in I$ tal que el residu de dividir f per $f_1, \ldots, f_s$ és diferent de zero. Pista: Demostreu primer que $\mathrm{LT}(f) \notin < \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) >$, per algún f.
b) Que diu l'apartat a) sobre el problema de la pertinena a ideals?
c) Quina relacio té l'apartat a) amb la conjectura de l'exercici 2.3.7?

2.5.4. Sigui I un ideal de $k[x_1, \ldots, x_n]$. Demostreu que $G = \{g_1, \ldots, g_t\} \subset I$ és una base de Groebner de I si i només si el terme principal de tot element de I és divisible per algún $\mathrm{LT}(g_i)$.

2.5.5. És $G = \{x^4y^2 - z^5, x^3y^3 - 1, x^2y^4 - 2z\}$ una base de Groebner de l'ideal $< G >$ respecte l'ordre grlex ? Raoneu la resposta.

2.5.6. Repetiu l'exercici 5 per $I = < x - z^2, y - z^3 >$ utilitzant l'ordre lex. Pista: La dificultat està en determinar exactament quins polinomis pertanyen a $< \mathrm{LT}(I) >$.

2.5.7. Sigui $A = (a_{ij})$ una matriu $m \times n$ amb components reals i esglaonada per files, i sigui $J \subset \mathbb{R}[x_1, \ldots, x_n]$ un ideal generat pels polinomis lineals $\sum_{i=1}^{n} a_{ij} x_i$ per $1 \leq j \leq m$. Demostreu que els generadors donats formen una base de Groebner per J, respecte un apropiat ordre lexicogràfic.

2.5.8. Sigui $I \subset k[x_1, \ldots, x_n]$ un *ideal principal* (I es generat per un únic $f \in I$). Demostreu que tot subconjunt finit de I que conté un generador de I és una base de Groebner.

2.5.9. Sigui $f \in k[x_1, \ldots, x_n]$. Si $f \notin < x_1, \ldots, x_n >$, demostreu que $< x_1, \ldots, x_n, f > = k[x_1, \ldots, x_n]$.

2.5.10. Demostreu que si agafem com a hipòtesi que tota cadena ascendent d'ideals de $k[x_1, \ldots, x_n]$ s'estabilitza, llavors el teorema de les bases de Hilbert és una conseqüència. Pista: Argmenteu-ho buscant una contradicció, suposant que hi ha algun ideal $I \subset k[x_1, \ldots, x_n]$ que no té un subconjunt finit de generadors.

2.5.11. Sigui $f_1, f_2, \ldots \in k[x_1, \ldots, x_n]$ una col.lecció infinita de polinomis i sigui $I = < f_1, f_2, \cdots >$ l'ideal generat. Demostreu que hi ha un enter N tal que $I = < f_1, \ldots, f_N >$. Pista: Utilitzeu $f_1, f_2, \ldots$ per crear una cadena ascendent d'ideals.

2.5.12. Donat un conjunt infinit de polinomis $f_1, f_2, \ldots \in k[x_1, \ldots, x_n]$, sigui $\mathbf{V}(f_1, f_2, \ldots) \subset k^n$ les solucions del sistema infinit de equacions $f_1 = f_2 = \cdots = 0$. Demostreu que hi ha algún N tal que $\mathbf{V}(f_1, f_2, \ldots) = \mathbf{V}(f_1, \ldots, f_N)$.

2.5.13. Considereu la varietat $V = \mathbf{V}(x^2 - y, y + x^2 - 4) \subset \mathbb{C}^2$. Noteu que $V = \mathbf{V}(I)$, on $I = < x^2 - y, y + x^2 - 4 >$.

a) Probeu que $I = < x^2 - y, x^2 - 2 >$.
b) Demostreu que $\mathbf{V}(I) = \{(\pm\sqrt{2}, 2)\}$, utilitzant la base de l'apartat anterior.

2.5.14. Quan un ideal té una base on algún dels seus elements pot ser factoritzat, podem utilitzar la factorització com ajuda per entendre la varietat.

a) Demostreu que si $g \in k[x_1, \ldots, x_n]$ factoritza en la forma $g = g_1 g_2$, aleshores per tot f, $\mathbf{V}(f, g) = \mathbf{V}(f, g_1) \cup \mathbf{V}(f, g_2)$.
b) Demostreu que a $\mathbb{R}^3$, $\mathbf{V}(y - x^2, xz - y^4) = \mathbf{V}(y - x^2, xz - x^8)$.
c) Utilitzeu l'apartat a) per descriure la varietat de l'apartat b).

2.6. **Propietats de les bases de Groebner. 2.6.1.** Fixem un ordre monomial, i sigui $I \subset k[x_1, \ldots, x_n]$ un ideal i $f \in k[x_1, \ldots, x_n]$.

a) Demostreu que f es pot posar en la forma $f = g + r$, on $g \in I$ i cap terme de r és divisible per cap element de $\mathrm{LT}(I)$.
b) Donades dues expressions $f = g + r = g' + r'$ com en l'apartat a), probeu que $r = r'$. Així doncs, r està determinada de manera única.

Aquest resultat demostra que una vegada l'ordre monomial està fixat, podem definir un únic "residu de f dividit per I".

2.6.2. Vàrem demostrar que $G = \{x + z, y - z\}$ era una base de Groebner per l'ordre lex. Utilitzarem aquesta base per estudiar la unicitat de l'algorisme de la divisió.

a) Dividiu xy per $x + z, y - z$.
b) Ara utilitzeu ordre invers i dividiu xy per $y - z, x + z$.

Haurieu de trobar els mateixos residus, peró els quocients haurien de ser diferents. Això demostra que la unicitat dels residus és lo millor que podem esperar.

2.6.3. Vàrem demostrar que si $I = < g_1, \ldots, g_t >$ i si $G = \{g_1, \ldots, g_t\}$ és una base de Groebner de I, aleshores $\overline{f}^G = 0$ per tot $f \in I$. Probeu l'invers d'aquesta proposició. O sigui, demostreu que si G és una base per I amb la propietat que $\overline{f}^G = 0$ per tot $f \in I$, aleshores G és una base de Groebner de I.

2.6.4. Siguin G i G' bases de Groebner d'un ideal I respecte el mateix ordre monomial en $k[x_1, \ldots, x_n]$. Demostreu que $\overline{f}^G = \overline{f}^{G'}$ per tot $f \in k[x_1, \ldots, x_n]$. Com a conseqüència el residu de la divisió per una base de Groebner és independent de la base que utilitzem, mentres fem servir un ordre monomial fixat.

2.6.5. Calculeu $S(f,g)$ utilitzant l'ordre lex.

a) $f = 4x^2z - 7y^2, \quad g = xyz^2 + 3xz^4$.
b) $f = x^4y - z^2, \quad g = 3xz^2 - y$.
c) $f = x^7y^2z + 2ixyz, \quad g = 2x^7y^2z + 4$.
d) $f = xy + z^3, \quad g = z^2 - 3z$.

2.6.6. Depén $S(f,g)$ de quin ordre monomial utilitzis?. Doneu algún exemple.

2.6.7. Probeu que $\text{multideg}(S(f,g)) < \gamma$, on $x^\gamma = \text{LCM}(\text{LM}(f), \text{LM}(g))$. Expliqueu perqué aquesta desigualtat és una versió explicativa de que els S-polinomis són dissenyats per produir cancel.lació.

2.6.8. Demostreu que $\{y - x^2, z - x^3\}$ no és una base de Groebner per ordre lex, amb $x > y > z$.

2.6.9. Determineu si els següents conjunts G són bases de Groebner de l'ideal que generen. Podeu utilitzar un sistema de computació algebraica per calcular els S-polinomis i els residus.

a) $G = \{x^2 - y, x^3 - z\}$ amb ordre grlex.
b) $G = \{x^2 - y, x^3 - z\}$ amb ordre invlex.
c) $G = \{xy^2 - xz + y, xy - z^2, x - yz^4\}$ amb ordre lex.

2.6.10. Siguin $f, g \in k[x_1, \ldots, x_n]$ polinomis tals que $\text{LM}(f)$ i $\text{LM}(g)$ són monomis primers entre si, i $\text{LC}(f) = \text{LC}(g) = 1$.

a) Demostreu que $S(f,g) = -(g - \text{LT}(g))f + (f - \text{LT}(f))g$.
b) Deduu que el monomi principal de $S(f,g)$ és un múltiple de $\text{LM}(f)$ o de $\text{LM}(g)$.

2.6.11. Siguin $f, g \in k[x_1, \ldots, x_n]$ i siguin x^α, x^β monomis. Verifiqueu que

$$S(x^\alpha f, x^\beta g) = x^\gamma S(f,g)$$

on

$$x^\gamma = \frac{\text{LCM}(x^\alpha \text{LM}(f), x^\beta \text{LM}(g))}{\text{LCM}(\text{LM}(f), \text{LM}(g))}$$

Assegureu-vos de demostrar que x^γ és un monomi.

2.6.12. Sigui $I \subset k[x_1, \ldots, x_n]$ un ideal, i sigui G una base de Groebner de I.

a) Demostreu que $\overline{f}^G = \overline{g}^G$ si i només si $f - g \in I$.

b) Deduu que
$$\overline{f+g}^G = \overline{f}^G + \overline{g}^G$$

c) Deduu que
$$\overline{fg}^G = \overline{\overline{f}^G \cdot \overline{g}^G}^G$$

2.7. **Algorisme de Buchberger.** **2.7.1.** Trobeu una base de Groebner per cada uns dels següents ideals. Si voleu podeu fer servir un sistema de computació algebraica per calcular els S-polinomis i els residus. Utilitzeu l'ordre lex i grlex en cada cas i compareu els resultats.

a) $I = < x^2y - 1, xy^2 - x >$.

b) $I = < x^2 + y, x^4 + 2x^2y + y^2 + 3 >$. Que us diu el resultat sobre la varietat $\mathbf{V}(I)$.

c) $I = < x - z^4, y - z^5 >$.

2.7.2. Trobeu les bases de Groebner redudes pels ideals de l'exercici anterior respecte els ordres lex i grlex.

2.7.3. Sigui G una base de Groebner per un ideal I amb la propietat que $\mathrm{LC}(g) = 1$ per tot $g \in G$. Probeu que G és una base minimal de Groebner si i només si cap subconjunt propi de G és una base de Groebner de I.

2.7.4. Demostreu que una base de Groebner G de I és minimal si i només si $\mathrm{LC}(g) = 1$ per tot $g \in G$ i $\mathrm{LT}(G)$ és una base minimal de l'ideal de monomis $< \mathrm{LT}(I) >$.

2.7.5. Fixat un ordre monomial, siguin G i $\overline{G}$ bases minimals de Groebner per l'ideal I.

a) Probeu que $\mathrm{LT}(G) = \mathrm{LT}(\overline{G})$.

b) Deduu que G i $\overline{G}$ tenen el mateix nombre d'elements.

2.7.6. Desenvolupeu un algorisme que produeixi una base de Groebner reduda, per un ideal I, donant com entrada una base de Groebner qualsevol de I. Comproveu que l'algorisme funciona.

2.7.7. Considereu l'ideal :

$$I = < 3x - 6y - 2z, 2x - 4y + 4w, x - 2y - z - w > \subset k[x, y, z, w]$$

Utilitzarem l'ordre lex amb $x > y > z > w$.

a) Demostreu que els polinomis lineals determinats per la següent matriu esglaonada per files, donen la base de Groebner minimal $I = < x -$

$2y - z - w, z + 3w >$.

$$\begin{pmatrix} 1 & -2 & -1 & -1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

b) Demostreu que els polinomis lineals de la reducció de la següent matriu esglaonada per files, donen la base de Groebner reduda $I = < x - 2y + 2w, z + 3w >$.

$$\begin{pmatrix} 1 & -2 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

2.7.8. Sigui $A = (a_{ij})$ una matriu $n \times m$ amb components de k i siguin $f_i = a_{i1}x_1 + \dots a_{im}x_m$ els polinomis lineals de $k[x_1, \dots, x_m]$ determinats per les files de A. Considerem l'ideal $I = < f_1, \dots, f_n >$. Utilitzarem l'ordre lex amb $x_1 > x_2 > \dots > x_m$. Ara sigui $B = (b_{ij})$ la matriu esglaonada per files reduda, determinada per A i siguin $g_1, \dots, g_t$ els polinomis lineals determinats per les files no nul.les de B (així doncs $t \leq n$). Probarem que $g_1, \dots, g_t$ formen la base de Groebner reduda de I.

a) Demostreu que $I = < g_1, \dots, g_t >$. Pista: Demostreu que el resultat d'aplicar una operació a les files de A, donen una matriu tal que les seves files generen el mateix ideal.
b) Demostreu que $g_1, \dots, g_t$ formen una base de Groebner per I. Pista: Si el primer 1 de la fila i-èssima de B està a la columna k, podem escriure $g_i = x_k + A$, on A és el polinomi lineal amb cap de les variables corresponents a el primer. Si $g_j = x_l + B$, aleshores necessitareu dividir $S(g_i, g_j) = x_l A - x_k B$ per $g_1, \dots, g_t$. Noteu que utilitzareu només g_i i g_j en la divisió.
c) Expliqueu perqué $g_1, \dots, g_t$ és la base de Groebner reduda .

2.7.9. Demostreu que el resultat d'aplicar l'algorisme d'Euclides en $k[x]$ a qualsevol parell de polinomis f, g, és una base reduda de Groebner per $< f, g >$ (després dividiu per una constant perqué el terme principal sigui igual a 1). Expliqueu com els passos de l'algorisme d'Euclides poden ser vistos com casos especials de les operacions de l'algorisme de Buchberger.

2.8. **Aplicacions de les bases de Groebner.** **2.8.1.** Determineu si $f = xy^3 - z^2 + y^5 - z^3$ pertany a l'ideal $I = < -x^3 + y, x^2y - z >$.

2.8.2. Repetiu l'exercici anterior per $f = x^3z - 2y^2$ i $I = < xz - y, xy + 2z^2, y - z >$.

2.8.3. Trobeu els punts de $\mathbb{C}^3$ que estàn sobre la varietat

$$\mathbf{V}(x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - 3y - z).$$

2.8.4. Repetiu l'exercici anterior per $\mathbf{V}(x^2y - z^3, 2xy - 4z - 1, z - y^2, x^3 - 4zy >$.

2.8.5. Recordem de càlcul que un *punt crític* d'una funció derivable $f(x, y)$ és un punt on les derivades parcials $\frac{\partial f}{\partial x}$ i $\frac{\partial f}{\partial y}$ s'anul.len simultaneament. Quan $f \in \mathbb{R}[x, y]$, els punts crítics es poden trobar aplicant les nostres tècniques al sistema d'equacions polinòmiques

$$\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0.$$

Per veure com funciona això, considereu la funció

$$f(x, y) = (x^2 + y^2 - 4)(x^2 + y^2 - 1) + (x - 3/2)^2 + (y - 3/2)^2.$$

a) Trobeu tots els punts crítics de $f(x, y)$.
b) Classifiqueu-los com a màxims locals, minims locals o punts de sella. Pista: Utilitzeu el hessià.

2.8.6. Sigui la superfície en $\mathbb{R}^3$ formada per les rectes que uneixen parells de punts de les rectes

$$\left\{ \begin{array}{ccc} x & = & t \\ y & = & 0 \\ z & = & 1 \end{array} \right\} \left\{ \begin{array}{ccc} x & = & 0 \\ y & = & 1 \\ z & = & t \end{array} \right\}$$

que tenen el mateix valor del paràmetre t. (Es un exemple de superfície reglada).

a) Demostreu que la superfície S es pot donar de la següent forma paramètrica

$$\begin{array}{ccl} x & = & ut \\ y & = & 1 - u \\ z & = & u + t - ut \end{array}$$

b) Busqueu una equació implícita de la varietat V que conté la superfície S.
c) Demostreu que $V = S$ (o sigui, demostreu que cada punt de la varietat V es pot obtindre substituint alguns valors per t, u en les equacions de l'apartat a). Pista: Proveu de "resoldre" l'equació de V amb una variable com a funció de les altres dues.

2.8.7. Algunes corbes paramètriques i superfícies són varietats algebràiques si be les paremetritzacions donades inclouen funcions com el sinus o el cosinus. En aquest problema veurem que la següent superfície paramètrica

T

$$\begin{aligned} x &= (2+cos(t))cos(u) \\ y &= (2+cos(t))sin(u) \\ z &= sin(t) \end{aligned}$$

està sobre una varietat afí de $\mathbb{R}^3$.

a) Dibuixeu T. Pista: Utilitzeu coordenades cilíndriques.
b) Sigui $a = cos(t), b = sin(t), c = cos(u), d = sin(u)$. Reescriviu les equacions com equacions polinòmiques en a, b, c, d, x, y, z.
c) Els parells a, b i c, d de l'apartat b) no són independents ja que verifiquen les següents identitats polinòmiques.

$$a^2 + b^2 - 1 = 0, \qquad c^2 + d^2 - 1 = 0$$

que provenen de les identitats de la trigonometria elemental. Formeu un sistema de cinc equacions per ajuntar a les equacions esmentades amb les del apartat b), i calculeu una base de Groebner pel corresponent ideal. Utilitzeu l'ordre monomial lex i l'ordre entre variables $a > b > c > d > x > y > z$. El resultat hauria de ser un únic polinomi que depèn únicament de x, y, z. Aquesta és l'equació de la varietat que conté T.

2.8.8. Considereu la corba paramètrica $K \subset \mathbb{R}^3$ donada per

$$\begin{aligned} x &= (2+cos(2s))(cos(3s) \\ y &= (2+cos(2s))(sin(3s) \\ z &= sin(2s). \end{aligned}$$

a) Expresseu les equacions de K com equacions polinòmiques en x, y, z, $a = cos(s), b = sin(s)$.
b) Calculant una base de Groebner per l'ideal generat per les equacions de l'apartat a) i $a^2+b^2-1 = 0$, demostreu que K és (un subconjunt de) una corba afí algebraica. Trobeu equacions implícites per una corba que contingui K.
c) Demostreu que l'equació de la superfície de l'exercici anterior està continguda a l'ideal generat per les equacions de l'apartat b). Que vol dir geomètricament això? (podeu arribar a la mateixa conclusió comparant les parametritzacions de T i K, sense calcular res.

2.8.9. Utilitzeu el mètode dels multiplicadors de Lagrange per trobar els punts de la superfície $x^4 + y^2 + z^2 - 1 = 0$ més aprop a el punt $(1, 1, 1)$ de $\mathbb{R}^3$.

2.9. **Millores de l'algorisme de Buchberger.** **2.9.1.** Siguin $S = (c_1, \dots, c_s)$ i $T = (d_1, \dots, d_s) \in (k[x_1, \dots, x_n])^s$ syzygies de les formes $F = (f_1, \dots, f_s)$.

a) Demostreu que $S + T = (c_1 + d_1, \dots, c_s + d_s)$ és també una syzygia.
b) Demostreu que si $g \in k[x_1, \dots, x_n]$, aleshores $g \cdot S = (gc_1, \dots, gc_s)$ és també una syzygia.

2.9.2. Donada $G = (g_1, \dots, g_s) \in (k[x_1, \dots, x_s])^s$, podem definir una syzygia en G com una s-tupla $S = (h_1, \dots, h_s) \in (k[x_1, \dots, x_s])^s$ tal que $\sum_i h_i g_i = 0$. [Noteu que les syzygies que estudiem són syzygies sobre $\mathrm{LT}(G) = (\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s))$.]

a) Demostreu que si $G = (x^2 - y, xy - z, y^2 - xz)$, aleshores $(z, -y, x)$ defineix una syzygia sobre G.
b) Trobeu una altre syzygia sobre G.
c) Demostreu que si S, T són syzygies sobre G, i $g \in k[x_1, \dots, x_n]$, aleshores $S + T$ i gS són també syzygies sobre G.

2.9.3. Sigui M una matriu de polinomis $n \times (n+1)$ en $k[x_1, \dots, x_n]$. Sigui I l'ideal generat pels determinants de totes les submatrius $n \times n$ de M (tals ideals són exemples d'ideals determinants).

a) Trobeu una matriu 2×3 tal que l'ideal determinant associat a les submatrius 2×2, és l'ideal amb els generadors de l'exercici anterior.
b) Expresseu la syzygia donada a l'apartat a) de l'exercici anterior en termes de la vostra matriu.
c) Doneu un mètode general per produir syzygies sobre els generadors d'un ideal determinant. Pista: Trobeu maneres de produr matrius $(n+1) \times (n+1)$ a partir de M, amb determinants nuls.

2.9.4. Probeu que la syzygia S_{ij}

$$S_{ij} = \frac{x^\gamma}{\mathrm{LT}(f_i)} \mathbf{e}_i - \frac{x^\gamma}{\mathrm{LT}(f_j)} \mathbf{e}_j$$

és homogènia de multigrau γ

2.9.5. Suposem que S_j és una syzygia homogènia de multigrau γ_j en $S(G)$. Demostreu que $S_j \cdot G$ té multigrau $< \gamma_j$. Això implica que $x^{\delta - \gamma_j} S_j \cdot G$ te multigrau $< \delta$.

2.9.6. Sigui G un subconjunt finit de $k[x_1, \dots, x_n]$ i sigui $f \in < G >$. Si $\overline{f}^G = r \neq 0$, aleshores demostreu que $f \to_{G'} 0$, on $G' = G \cup \{r\}$.

2.9.7. Considereu els següents polinomis

$$x^{n+1} - yz^{n-1}w, \quad xy^{n-1} - z^n, \quad x^n z - y^n w,$$

Utilitzeu l'ordre lex amb $x > y > z > w$. Mora [veure LAZARD (1983)] va demostrar que la base de Groebner reduda contenia el polinomi

$$z^{n^2+1} - y^{n^2}w.$$

Proveu que és cert quan n és 3,4 o 5. Són molt grans les bases de Groebner?

2.9.8. En aquest exercici veurem alguns exemples de com l'ordre pot afectar en el càlcul de les bases de Groebner i la complexitat de la resposta.

a) Calculeu una base de Groebner per $I = < x^5 + y^4 + z^3 - 1, x^3 + y^2 + z^2 - 1 >$ utilitzant l'ordre lex i grevelex amb $x > y > z$. Potser no ni haurà gaire diferència en temps de càlcul, però veureu que la base és molt més simple amb grevlex.

b) Calculeu una base de Groebner per $I = < x^5 + y^4 + z^3 - 1, x^3 + y^3 + z^2 - 1 >$ utilitzant l'ordre lex i grevelex amb $x > y > z$. Difereix només d'un exponent respecte l'exemple anterior, però la base de Groebner per l'ordre lex és molt més desagradable (un dels seus polinomis te 282 termes, és de grau 25 i el coeficient més gran és 167383594). Depenent de l'ordinador i l'algorisme que l'implementa, el càlcul per l'ordre lex pot ser inacabable.

c) Sigui $I = < x^4 - yz^2w, xy^2 - z^3, x^3z - y^3w >$ l'ideal generat pels polinomis de l'exercici anterior amb $n = 3$. Utilitzant l'ordre lex i grevlex amb $x > y > z > w$, demostreu que les bases de Groebner resultants són les mateixes. Grevlex no és sempre millor que lex, però en la pràctica, sempre és millor utilitzar grevlex si és possible.

3. Teoria de l'Eliminació

3.1. **Teoria de l'eliminació. 3.1.1.** Sigui $I \subset k[x_1, \ldots, x_n]$ un ideal.

a) Probeu que $I_k = I \bigcap k[x_{k+1}, \ldots, x_n]$ és un ideal de $k[x_{k+1}, \ldots, x_n]$.
b) Probeu que l'ideal $I_{k+1} \subset k[x_{k+2}, \ldots, x_n]$ és l'ideal de la primera eliminació de $I_k \subset k[x_{k+1}, \ldots, x_n]$. Aquesta observació ens permet d'utilitzar el teorema de l'extensió reiteradament per eliminar més d'una variable.

3.1.2. Considereu el sistema d'equacions

$$\begin{aligned} x^2 + 2y^2 &= 3, \\ x^2 + xy + y^2 &= 3. \end{aligned}$$

a) Si I és l'ideal generat per aquestes equacions, trobeu bases de $I \bigcap k[x]$ i $I \bigcap k[y]$.
b) Trobeu totes les solucions de les equacions.
c) Quines d'aquestes són racionals ? (estan a $\mathbb{Q}^2$).
d) Quin és el cos k més petit, tal que totes les solucions queden a k^2?

3.1.3. Determineu totes les solucions $(x, y) \in \mathbb{Q}^2$ del següent sistema d'equacions

$$\begin{aligned} x^2 + 2y^2 &= 2, \\ x^2 + xy + y^2 &= 2. \end{aligned}$$

Determineu també, totes les solucions a $\mathbb{C}^2$

3.1.4. Trobeu bases pels ideals d'eliminació I_1, I_2 de l'ideal I determinat per les equacions :

$$\begin{aligned} x^2 + y^2 + z^2 &= 4, \\ x^2 + 2y^2 &= 5, \\ xz &= 1 \end{aligned}$$

Quantes solucions racionals (en $\mathbb{Q}^3$) hi han?

3.1.5. En aquest exercici, demostrarem una versió més general del teorema d'eliminació. Fixat un enter $1 \leq k \leq n$, direm que un ordre monomial $>$ sobre $k[x_1, \ldots, x_n]$ és de tipus k-eliminació quan tot monomi que conté algún $x_1, \ldots, x_k$ és més gran que tots els monomis de $k[x_{k+1}, \ldots, x_n]$. Probeu la següent generalització del teorema d'eliminació. Si I és un ideal de $k[x_1, \ldots, x_n]$ i G és una base de Groebner de I respecte un ordre monomial de tipus k-eliminació, aleshores $G\bigcap k[x_{k+1},\dots,x_n]$ és una base del k-èssim ideal d'eliminació $I\bigcap k[x_{k+1},\dots,x_n]$.

3.1.6. Per acabar de veure la generalitazció del teorema d'eliminació, es convenient estudiar alguns exemples interessants d'ordres monomials de tipus k-eliminació. Considerem dos ordres.

a) Fixat un enter $1\le k\le n$ es defineix l'ordre $>_k$ com segueix: si $\alpha,\beta\in\mathbb{Z}^n_{\geq 0}$ llavors $\alpha>_k\beta$ si

$$\begin{array}{l} \alpha_1+\cdots+\alpha_k>\beta_1+\cdots+\beta_k \\ \text{o bé}\quad \alpha_1+\cdots+\alpha_k=\beta_1+\cdots+\beta_k,\quad \alpha>_{grevlex}\beta. \end{array}$$

Proveu que $>_k$ és un ordre monomial del tipus k-eliminació (anomenat ordre de k-eliminació de BAYER i STILLMAN).

b) Al capítol anterior vàrem considerar un exemple d'ordre producte que barrejava ordre lex amb grlex amb diferents tipus de variables. Expliqueu com crear ordres producte que donen com a resultat grevlex alhora en $k[x_1,\dots,x_k]$ i en $k[x_{k+1},\dots,x_n]$ i demostreu que aquest ordre és k-eliminació.

c) Si G és una base de Groebner de $I\subset k[x_1,\dots,x_n]$ per algún dels ordres monomials de l'apartat b), expliqueu perqué $G\bigcap k[x_{k+1},\dots,x_n]$ és una base de Groebner respecte grevlex.

3.1.7. Considereu les equacions

$$\begin{aligned} t^2+x^2+y^2+z^2 &= 0,\\ t^2+2x^2-xy-z^2 &= 0,\\ t+y^3-z^3 &= 0. \end{aligned}$$

Volem eliminar t d'aquestes equacions. Sigui $I=<t^2+x^2+y^2+z^2,t^2+2x^2-xy-z^2,t+y^3-z^3>$ l'ideal corresponent.

a) Utilitzeu ordre lex amb $t>x>y>z$, per calcular una base de Groebner de I, i trobeu una base per $I\bigcap k[x,y,z]$. Haurieu de trobar quatre generadors, un dels quals té grau total 12.

b) Utilitzeu grevlex per calcular una base de Groebner de $I\bigcap k[x,y,z]$. Trobareu un conjunt simple de dos generadors.

c) Combineu la solució de l'apartat b) amb el polinomi $t+y^3-z^3$ i demostreu que dona una base de Groebner de I respecte l'ordre d'eliminació $>_1$ del problema anterior. Noteu que aquesta base és molt més simple que la trobada a l'apartat a). Si teniu accés a un sistema de computació algebraica que conegui ordres d'eliminació, comproveu la vostra solució.

3.1.8. Considereu el següent sistem d'equacions :

$$\begin{aligned} x^5 + \frac{1}{x^5} &= y, \\ x + \frac{1}{x} &= z. \end{aligned}$$

Sigui I l'ideal en $\mathbb{C}[x,y,z]$ determinat per les equacions.

a) Trobeu una base de $I_1 \subset \mathbb{C}[y,z]$ i demostreu que $I_2 = \{0\}$.
b) Utilitzeu el teorema d'extensió per probar que cada solució parcial $c \in \mathbf{V}(I_2) = \mathbb{C}$ dona lloc, per extensió a una solució en $\mathbf{V}(I) \subset \mathbb{C}^3$.
c) Quines solucions parcials $(y,z) \in \mathbf{V}(I_1) \subset \mathbb{R}^2$ s'extenen a solucions en $\mathbf{V}(I) \subset \mathbb{R}^3$. Expliqueu perqué això no contradiu el terorema d'extensió.
d) Si considerem z com un "parametre", resoleu el sistema considerant x, y com funcions algebraiques de z per obtindre una "parametrització" de $\mathbf{V}(I)$.

3.2. **La geometria de l'eliminació. 3.2.1.** En aquest problema analitzarem la demostració de la interpretació geomètrica del teorema d'extensió, en el cas especial $I = < f_1, f_2, f_3 >$, on

$$\begin{aligned} f_1 &= yx^3 + x^2, \\ f_2 &= y^3x^2 + y^2, \\ f_3 &= yx^4 + x^2 + y^2. \end{aligned}$$

a) Trobeu una base de Groebner de I i demostreu que $I_1 = < y^2 >$.
b) Demostreu que $\mathbf{V}(I_1) = \mathbf{V}(I_1) \bigcap \mathbf{V}(g_1, g_2, , g_3)$, on g_i és el coeficient principal de x en f_i. Era el cas del teorema d'extensió quan $W = \mathbf{V}(I_1)$.
c) Sigui $\tilde{I} = < f_1, f_2, f_3, g_1, g_2, g_3 >$. Demostreu que $I \neq \tilde{I}$ i que $\mathbf{V}(I) = \mathbf{V}(\tilde{I})$. Comprobeu també que $\mathbf{V}(I_1) = \mathbf{V}(\tilde{I}_1)$.
d) Seguiu el mètode descrit a classe per obtenir una nova base de $\tilde{I}$. Utilitzeu aquesta nova base per demostrar que $\tilde{W} \neq \mathbf{V}(I_1)$.

3.2.2. Siguin $f_i, g_i, h_i \in k[x_1, \ldots, x_n]$ per $1 \leq i \leq s$. Posant $\tilde{f}_i = f_i + h_i g_i$, demostreu que

$$< f_1, \ldots, f_s, g_1, \ldots, g_s > = < \tilde{f}_1, \ldots, \tilde{f}_s, g_1, \ldots, g_s > .$$

Expliqueu en quin punt la demostració del teorema d'extensió utilizava un cas especial d'aquest resultat.

3.2.3. Per veure com el teorema de la clausura pot fallar a $\mathbb{R}$, considereu l'ideal

$$I = < x^2 + y^2 + z^2 + 2, 3x^2 + 4y^2 + 4z^2 + 5 > .$$

Sigui $V = \mathbf{V}(I)$, i sigui π_1 la projecció de (x,y,z) a (y,z).

a) Treballant sobre $\mathbb{C}$, proveu que $\mathbf{V}(I_1) = \pi_1(V)$.

b) Treballant sobre $\mathbb{R}$, proveu que $V = \phi$ i que $\mathbf{V}(I_1)$ és infinit. Així resulta que $\mathbf{V}(I_1)$ pot ser més gran que la varietat més petita que conté $\pi_1(V)$ quan el cos no es algebraicament tancat.

3.3. **El teorema de la implicitació polinòmica.** **3.3.1.** Quan $k = \mathbb{C}$, la conclusió del teorema de la implicitació polinòmica pot ser més forta. Es pot demostrar que hi ha una varietat $W \subset_{\neq} \mathbf{V}(I_m)$ tal que $\mathbf{V}(I_m) - W \subset F(\mathbb{C}^m)$. Proveu-ho utilitzant el teroema de la clausura.

3.3.2. Doneu un exemple per demostrar que l'exercici anterior no funciona sobre $\mathbb{R}$. Pista: t^2 és sempre positiu.

3.3.3. Sigui S la superfície paramètrica definida per

$$\begin{aligned} x &= uv, \\ y &= u^2, \\ z &= v^2. \end{aligned}$$

a) Trobeu la equació de la varietat V més petita que conté S.
b) Utilitzeu el terorema d'extensió sobre $\mathbb{C}$ per probar que $S = V$.
c) Sobre $\mathbb{R}$, demostreu que S sols cubreix la meitat de V. Quina parametrització cubreix l'altra meitat ?.

3.3.4. Sigui S la superfície paramètrica definida per

$$\begin{aligned} x &= uv, \\ y &= uv^2, \\ z &= u^2. \end{aligned}$$

a) Trobeu la equació de la varietat V més petita que conté S.
b) Sobre $\mathbb{C}$, demostreu que V conté punts que no estan sobre S. Determineu exactament quins són aquests punts. Pista: Utilitzeu l'ordre lexicogràfic amb $u > v > x > y > z$.

3.3.5. La superfície d'Enneper està definida paramètricament per

$$\begin{aligned} x &= 3u + 3uv^2 - u^3, \\ y &= 3v + 3u^2v - v^3, \\ z &= 3u^2 - 3v^2. \end{aligned}$$

a) Trobeu la equació de la varietat V més petita que conté la superfície d'Enneper. Serà una equació molt complicada!.

b) Utilitzeu el terorema d'extensió sobre $\mathbb{C}$ per probar que les equacions donades parametritzen tota la superfície V. Pista: Hi ha molts polinomis a la base de Groebner. Procura trobar el que necessites.

3.3.6. La superfície del paraigües de Whitney està definida paramètricament per

$$\begin{aligned} x &= uv, \\ y &= v, \\ z &= u^2. \end{aligned}$$

a) Trobeu l'equació de la varietat més petita que conté el paraigües de Whitney.
b) Demostreu que la parametrització omple la varietat sobre $\mathbb{C}$ peró no sobre $\mathbb{R}$. Sobre $\mathbb{R}$ quins punts són omitits?.
c) Demostreu que els paràmetres u i v no estan sempre determinats únicament per x, y i z. Trobeu els punts on falla la unicitat i relacioneu-ho amb el gràfic de la varietat.

3.3.7. Donada una parametrització racional com en el problema 3, hi ha un cas on l'ideal $I = < g_1x_1 - f_1, \ldots, g_nx_n - f_n >$ obtingut per "neteja de denominadors" dona la resposta correcta. Suposem que $x_i = f_i(t)/g_i(t)$, on t és l'únic paràmetre. Podem asumir que per cada i, $f_i(t)$ i $g_i(t)$ són primers entre si en $k[t]$ (o sigui que no tenen cap arrel comuna). Si $I \subset k[t, x_1, \ldots, x_n]$, proveu que $\mathbf{V}(I_1)$ és la varietat més petita que conté $F(k - W)$, on $g = g_1 \ldots g_n \in k[t]$ i $W = \mathbf{V}(g) \subset k$.

3.3.8. El *folium* de Descartes pot ser paremetritzat per

$$\begin{aligned} x &= \frac{3t}{1+t^3}, \\ y &= \frac{3t^2}{1+t^3}. \end{aligned}$$

a) Trobeu l'equació del *folium*. Pista: Feu servir l'exercici anterior.
b) Sobre $\mathbb{C}$ o $\mathbb{R}$, demostreu que les paremetritzacions cobreixen tota la corba.

3.3.9. En la secció d'ideals, vàrem estudiar les següents equacions paramètriques sobre $\mathbb{R}$:

$$\begin{aligned} x &= \frac{(1-t)^2x_1 + 2t(1-t)wx_2 + t^2x_3}{(1-t)^2 + 2t(1-t)w + t^2} \\ y &= \frac{(1-t)^2y_1 + 2t(1-t)wy_2 + t^2y_3}{(1-t)^2 + 2t(1-t)w + t^2} \end{aligned}$$

on $w, x_1, y_1, x_2, y_2, x_3, y_3$ són constants i $w > 0$. Eliminant t, demostreu que aquestes equacions descriuen un tro de secció cònica. Rercordeu que una secció cònica es descrita per una equació de la forma

$$ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

3.4. **Punts singulars i envolvents.** **3.4.1.** Sigui C la corba de k^2 definida per $x^3 - xy + y^2 = 1$. Noteu que $(1,1) \in C$. Ara considereu la recta parametrizada per

$$\begin{aligned} x &= 1 + ct, \\ y &= 1 + dt. \end{aligned}$$

Calculeu la multiplicitat d'aquesta recta en el punt $(1,1)$. Què diu això sobre la recta tangent?. Ajut: Hi haurà dos casos a considerar.

3.4.2. A la definició de multiplicitat d'una intersecció faltava demostrar que la noció de multiplicitat és independent de com està parametritzada.

a) Demostreu que les parametritzacions

$$x = a + ct, \qquad x = a + c't,$$

$$y = b + dt, \qquad y = b + d't.$$

corresponen a la mateixa recta si i només si hi ha un nombre real $\lambda \neq 0$ tal que $(c,d) = \lambda(c',d')$. Ajut: En la parametrització $x = a + ct, y = b + dt$ d'una recta L, recordeu que L és paral.lela al vector (c,d).

b) Suposem que les dues parametritzacions de l'apartat a) corresponen a la mateixa recta L que intersecta amb $\mathbf{V}(f)$ a (a,b). Proveu que els polinomis $g(t) = f(a + ct, b + dt)$ i $g'(t) = f(a + c't, b + d't)$ tenen la mateixa multiplicitat a $t = 0$. Ajut: Utilitzeu l'apartat a) per relacionar g i g'. Això demostra que la multipicitat de L a (a,b) (on intersecta amb $\mathbf{V}(f)$), està ben definida.

3.4.3. Considereu les rectes

$$\begin{aligned} x &= t, \\ y &= b + t. \end{aligned}$$

Aquestes línies tenen pendent 1 i ordenada a l'origen b. Per quins valors de b s'obté una recta tangent al cercle $x^2 + y^2 = 2$?. Dibuixeu-ho. Ajuda: Considereu $g(t) = t^2 + (b+t)^2 - 2$. Les arrels d'aquesta equació determinen els valors de t on intersecta la recta amb el cercle.

3.4.4. Si $(a, b) \in \mathbf{V}(f)$ i $\nabla f(a, b) \neq (0, 0)$, proveu que la recta tangent de $\mathbf{V}(f)$ a (a, b) queda definida per l'equació

$$\frac{\partial}{\partial x} f(a, b) \cdot (x - a) + \frac{\partial}{\partial y} f(a, b) \cdot (y - b) = 0.$$

3.4.5. Sigui $g \in k[t]$ un polinomi tal que $g(0) = 0$.

a) Proveu que $t = 0$ és una arrel de multiplicitat ≥ 2 de g si i només si $g'(0) = 0$. Ajut: Escriviu $g(t) = th(t)$, i utilitzeu la regla del producte.
b) Generalitzant, proveu que $t = 0$ és una arrel de multiplicitat $\geq k$ si i només si $g'(0) = g''(0) = \cdots = g^{(k-1)}(0) = 0$.

3.4.6. Sigui una recta L parametritzada per $x = a + ct$, $y = b + dt$, on $(a, b) \in \mathbf{V}(f)$. Sigui també $g(t) = f(a + ct, b + dt)$. Proveu que L intersecta $\mathbf{V}(f)$ amb multiplicitat k si i només si $g'(0) = g''(0) = \cdots = g^{(k-1)}(0) = 0$ però $g^k(0) \neq 0$. Ajut: Utilitzeu l'exercici anterior.

3.4.7. En aquest exercici estudiarem com una recta tangent pot intersectar amb una corba de multiplicitat més gran que dos. Sigui C una corba definida per $y = f(x)$, on $f \in k[x]$. C és doncs la gràfica de f.

a) Doneu una demostració algebraica que la recta tangent a C en el punt $(a, f(a))$ queda parametritzada per

$$\begin{aligned} x &= a + t, \\ y &= f(a) + f'(a)t. \end{aligned}$$

Ajut: Considereu $g(t) = f(a) + f'(a)t - f(a + t)$.
b) Demostreu que la recta tangent a $(a, f(a))$ intersecta amb la corba amb multiplicitat ≥ 3 si i només si $f''(a) = 0$. Ajut: Utilitzeu l'exercici anterior.
c) Demostreu que la multiplicitat és exactament 3 si i només si $f''(a) = 0$ peró $f'''(0) \neq 0$.
d) Sobre $\mathbb{R}$, es defineix un punt de inflexió com un punt on a $f''(x)$ canvia de signe. Proveu que si la multiplicitat és 3, aleshores $(a, f(a))$ és un punt de inflexió.

3.4.8. Ara calcularem alguns punts sigulars.

a) Demostreu que $(0, 0)$ és l'únic punt singular de $y^2 = x^3$.
b) En el capítol anterior vàrem estudiar la corba $y^2 = cx^2 - x^3$, on c és una constant. Trobeu tots els punts singulars de la corba.
b) Demostreu que la circumferència $x^2 + y^2 = a^2$ no té punts singulars.

3.4.9. Una utilitat de les multiplicitats és demostrar que una singularitat és "pitjor" que una altra.

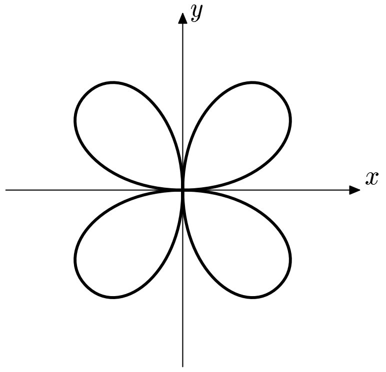
a) Per la corba $y^2 = x^3$, demostreu que la majoria de rectes que passen per l'origen, intersecten amb la corba amb multiplicitat 2.
b) Per $x^4 + 2xy^2 + y^3 = 0$, demostreu que totes les rectes que passen per l'origen, intersecten amb la corba amb multiplicitat ≥ 3.

Això d'alguna manera diu que la singularitat a l'origen és "pitjor" per la segona corba. Utilitzant aquestes idees, un pot definir la noció de multiplicitat d'un punt singular.

3.4.10. Hem demostrat que $(0,0)$ és un punt singular de la corba C definida per $y^2 = x^2(1+x)$. Però en el dibuix de C, sembla observar-se dues rectes tangents que passen per l'origen. Podem utilitzar les multiplicitats per diferenciar-les?.

a) Demostreu que amb dues excepcions, totes les rectes que passen per l'origen intersecten amb C amb multiplicitat 2. Quines són les rectes que tenen multiplicitat 3?.
b) Perquè les rectes tangents haurien de tenir multiplicitat més alta?.

3.4.11. La rosa de quatre pètals es definida en coordenades polars per l'equació $r = sin(2\theta)$. En coordenades cartesianes, la corba està definida per l'equació $(x^2 + y^2)^3 = 4x^2y^2$.



a) Demostreu que la majoria de rectes que passen per l'origen intersecten amb la rosa a l'origen amb multiplicitat 4. Quina interpretació geomètrica té aquest número?.
b) Trobeu les rectes que passen per l'origen i que intersecten amb la rosa amb multiplicitat > 4. Doneu una interpretació geomètrica dels nombres de les multiplicitats.

3.4.12. Considereu una superfície $\mathbf{V}(f) \subset k^3$ definida per $f \in k[x,y,z]$.

a) Definiu que és el que suposa per $(a,b,c) \in \mathbf{V}(f)$ ser un punt singular.
b) Determineu tots els punts singulars de l'esfera $x^2 + y^2 + z^2 = 1$. Té sentit la resposta?.
c) Determineu tots els punts singulars de la superfície $\mathbf{V}(x^2 - y^2z^2 + z^3)$.

3.4.13. Ara estudiarem l'envolvent de la família $F = (x-t)^2 - y + t$.

a) És obvi que l'envolvent és una recta de pendent 1. Utilitzeu el càlcul elemental per demostrar que la recta és $y = x - 1/4$.
b) Utlitzeu la definició d'envolvent per calcular-l'ho.
c) Trobeu una parametrització de l'envolvent tal que per tot t el punt $(f(t), g(t))$ està sobre la paràbola $\mathbf{V}(F_t)$. Noteu que aquesta és la classe de parametrització que vam utilitzar.

3.4.14. Sigui l'envolvent de la família $(x-t)^2 + (y-t^2)^2 = 4$.

a) Dibuixeu les dues circumferències tangets als punts $(x, y) = (0, 17/4)$ i $(\pm 0.936845, 1.63988)$.
b) Pel punt $(0, 4.25) = (0, 17/4)$, trobeu el valor de les t's que donen les dues circumferències tangents.
c) Demostreu que els valors exactes dels punts de l'apartat a) són donats per

$$\left(0, \frac{17}{4}\right) \quad \text{i} \quad \left(\pm\frac{1}{2}\sqrt{15 + 6\sqrt[3]{2} - 12\sqrt[3]{4}},\ \frac{1}{4}(-1 + 6\sqrt[3]{2})\right).$$

Ajut: La majoria de sistemes de computació algebraica tenen comandes per factoritzar polinomis i resoldre equacions cúbiques.

3.4.15. Considereu la família determinada per $F = (x-t)^2 + y^2 - (1/2)t^2$.

a) Calculeu l'envolvent d'aquesta família.
b) Dibuixeu-ho.

3.4.16. Considereu la família de cercles definida per $(x-t)^2 + (y-t^2)^2 = t^2$ en el pla $\mathbb{R}^2$.

a) Calculeu l'equació de l'envolvent d'aquesta família i demostreu que és unió de les dues varietats.
b) Utilitzeu el teorema d'extensió i una base de Groebner per determinar quantes corbes de la família són tangents en un punt qualsevol de l'envolvent. Dibuixeu-ho.

3.4.17. En aquest exercici demostrarem que la nostra definició d'envolvent és massa simple.

a) Donada una família de cercles de radi 1, amb els centres sobre l'eix x, feu un dibuix per demostrar que l'envolvent són les rectes $y = \pm 1$.
b) Utilitzeu la definició per calcular l'envolvent de la família donada per $F = (x-t)^2 + y^2 - 1$.
c) Utilitzeu la definició per trobar l'envolvent quan la família és $F = (x-t^3)^2 + y^2 - 1$. Noteu que una de les corbes de la família és part de la resposta. Això és degut a què t^3 permet a les corbes agrupar-se a prop de $t = 0$, lo qual fora a $\mathbf{V}(F_0)$ a aparèixer en l'envolvent.

3.4.18. Suposem que tenim una família de corbes en $\mathbb{R}^2$ determinades per $F \in \mathbb{R}[x, y, t]$. Algunes de les corbes $\mathbf{V}(F_t)$ tenen punts singulars, i altres no. Podem trobar les corbes que en tenen?

a) Considereu les equacions $F = \frac{\partial}{\partial x}F = \frac{\partial}{\partial y}F = 0$ de $\mathbb{R}^3$ i utilitzant la teoria d'eliminació, describiu un procediment per determinar quines t's corresponents a les corbes, tenen punts singulars.

b) Apliqueu el mètode de l'apartat a) per trobar les corbes de la familia $F = xy - t$ que tenen punts singulars.

3.5. **Factorització única i resultants.** **3.5.1.** Calculeu la resultant de $x^5 - 3x^4 - 2x^3 + 3x^2 + 7x + 6$ i $x^4 + x^2 + 1$. Tenen algún factor comú a $\mathbb{Q}[x]$? Expliqueu el vostre raonament.

3.5.2. Si $f = c(x - a_1)^{r_1} \dots (x - a_l)^{r_l} \in \mathbb{C}[x]$, aleshores

$$\mathrm{GCD}(f, f') = (x - a_1)^{r_1 - 1} \dots (x - a_l)^{r_l - 1}.$$

Sobre un cos k qualsevol, un polinomi $f \in k[x]$ de grau positiu pot no ser producte de factors lineals. Però per la factorització única, sabem que f es pot ser escriure de la forma

$$f = f_1^{r_1} \dots f_l^{r_l},$$

on $f_1, \dots, f_l \in k[x]$ són irreduibles, i cap f_i, és múltiple de cap altra f_j per $i \neq j$. Proveu que si k conté els nombres racionals $\mathbb{Q}$, aleshores

$$\mathrm{GCD}(f, f') = f_1^{r_1 - 1} \dots f_l^{r_l - 1}.$$

Ajut: La demostració utilitza la factorització única. La hipòtesi $\mathbb{Q} \subset k$ és necessària per asegurar que $f' \neq 0$.

3.5.3. Si $f = a_0 x^l + \dots + a_l \in k[x]$, on $a_0 \neq 0$ i $l > 0$, aleshores el discriminant de f és defineix per

$$\mathrm{disc}(f) = \frac{(-1)^{l(l-1)/2}}{a_0} \mathrm{Res}(f, f', x).$$

Proveu que f té un factor múltiple (o sigui que f és divisible per h^2 per algún $h \in k[x]$ de grau positiu) si i només si $\mathrm{disc}(f) = 0$. Ajut: Utilitzeu l'exercici anterior. Sobre $\mathbb{C}$, aquest resultat diu que un polinomi té una arrel de grau múltiple si i només si aquest discriminant és zero.

3.5.4. Utilitzeu l'exercici anterior per determinar si $6x^4 - 23x^3 + 32x^2 - 19x + 4$ té una arrel de grau múltiple en $\mathbb{C}$. Quina és l'arrel múltiple?

3.5.5. Calculeu el discriminant del polinomi quadràtic $f = ax^2 + bx + c$. Expliqueu com es relaciona la vostra resposta amb la fórmula quadràtica, i proveu que f té una arrel múltiple si i només si el discriminant s'anul.la.

3.5.6. Considereu els polinomis $f = 2x^2 + 3x + 1$ i $g = 7x^2 + x + 3$.

a) Utilitzeu l'algorisme d'Euclides per trobar el GCD d'aquests polinomis.

b) Trobeu polinomis $A, B \in \mathbb{Q}[x]$ tals que $Af + Bg = 1$. Ajut: Utilitzeu els càlculs de l'apartat a).
c) En l'equació trobada a l'apartat b), treieu els denominadors. Com es relaciona això amb la resultant?.

3.5.7. Si $f, g \in \mathbb{Z}[x]$, expliqueu perqué $\mathrm{Res}(f, g, x) \in \mathbb{Z}$

3.5.8. Sigui $f = xy - 1$ i $g = x^2 + y^2 - 4$. Considererem f i g com polinomis en x amb coeficients en $k(y)$.

a) Amb els polinomis f, g, construu el sistema d'equacions que descriu $\tilde{A}f + \tilde{B}g = 1$. Ajut: $\tilde{A}$ és constant i $\tilde{B}$ és lineal. D'aquesta manera, harieu de tenir tres equacions amb tres incògnites.
b) Utilitzeu la regla de Cramer per resoldre el sistema d'equacions obtingut a l'apartat a). Ajut: El denominador és la resultant.
c) Quina equació obteniu en eliminar els denominadors de l'apartat b).

3.5.9. Hem definit $\mathrm{Res}(f, g, x)$ quan $f, g \in k[x]$ tenen grau positiu. Ara anem a explorar que passa quan un dels dos o tots dos són constants.

a) En primer lloc suposem que f te grau $l > 0$ i $g = b_0$ és una constant (que pot ser zero). Proveu que la matriu de Sylverter de f i g és la matriu $l \times l$ amb b_0 a la diagonal principal i la resta 0. Concluiu que $\mathrm{Res}(f, b_0, x) = b_0^l$.
b) Proveu que si f i g són com a l'apartat a), les proposicions 6 i 7 del text segueixen essent vàlides.
c) Quant val $\mathrm{Res}(a_0, g, x)$ quan $f = a_0$ i $g = b_0$ són unes constants. En aquest cas es defineix

$$\mathrm{Res}(a_0, b_0) = \begin{cases} 0 & \text{si } a_0 = 0 \text{ ó } b_0 = 0 \\ 1 & \text{si } a_0 \neq 0 \text{ i } b_0 \neq 0 \end{cases}$$

Prenent $f = g = 2$ com elements de $\mathbb{Q}[x]$, proveu que les proposicions 8 i 9 poden fallar per f i g constants.

3.5.10. Proveu que si f té grau l i g té grau m, llavors la resultant té la següent propietat de simetria:

$$\mathrm{Res}(f, g, x) = (-1)^{lm}\mathrm{Res}(g, f, x).$$

3.5.11. Siguin $f = a_0x^l + \cdots + a_l$ i $g = b_0x^m + \cdots + b_m$ polinomis en $k[x]$, i suposem $l \geq m$:

a) Sigui $\tilde{f} = f - (a_0/b_0)x^{l-m}g$ i $\deg(\tilde{f}) \leq l - 1$. Aleshores proveu que si $\deg(\tilde{f}) = l - 1$ llavors

$$\mathrm{Res}(f, g, x) = b_0\mathrm{Res}(\tilde{f}, g, x).$$

b) Sigui $\tilde{f}$ com l'apartat a), però ara permetem la posibilitat de que el grau de $\tilde{f}$ pugui ser estrictament més petit que $l-1$. Proveu que

$$\operatorname{Res}(f,g,x) = b_0^{l-\deg(\tilde{f})}\operatorname{Res}(\tilde{f},g,x).$$

Ajut: L'exponent $l - \deg(\tilde{f})$ us diu quantes vegades s'expandeix per menors.

c) Utilitzeu ara l'algorisme de la divisió per escriure $f = qg + r$ en $k[x]$, on $\deg(r) < \deg(g)$. Utilitzeu l'apartat b) per demostrar que

$$\operatorname{Res}(f,g,x) = b_0^{l-\deg(r)}\operatorname{Res}(r,g,x).$$

3.5.12. En aquest problema, modificarem l'algorisme d'Euclides per donar un algorisme que calcula resultants. L'idea bàsica és la següent: per trobar el GCD de f i g, vam utilitzar l'algorisme de la divisió per escriure $f = qg + r,\ g = q'r + r'$, etc. Les igualtats

$$\operatorname{GCD}(f,g) = \operatorname{GCD}(g,r) = \operatorname{GCD}(r,r') = \dots$$

ens permetien calcular el GCD quan el graus decreixien. Utilitzant l'exercici anterior, podem expresar les dues igualtats en versió "resultant" :

$$\begin{aligned}
\operatorname{Res}(f,g,x) &= (b_0)^{\deg(f)-\deg(r)}\operatorname{Res}(r,g,x)\\
&= (-1)^{\deg(g)\deg(r)}(b_0)^{\deg(f)-\deg(r)}\operatorname{Res}(g,r,x)\\
&= (-1)^{\deg(g)\deg(r)}(b_0)^{\deg(f)-\deg(r)}({b'}_0)^{\deg(g)-\deg(r')}\operatorname{Res}(r',r,x)\\
&= (-1)^{\deg(g)\deg(r)+\deg(r)\deg(r')}(b_0)^{\deg(f)-\deg(r)}({b'}_0)^{\deg(g)-\deg(r')}\\
&\quad\ \operatorname{Res}(r,r',x),
\end{aligned}$$

on b_0 (resp. b'_0) és el coeficient principal de g (respecte r). Continuant el procés, ho podem reduir al cas on el segon polinomi és constant.

Per construr el pseudocodi, necesitarem dues funcions: $r = \operatorname{residu}(f,g)$ i $\operatorname{lead}(f)$, que retorna el coeficient principal de f. Ara ja podem escriure l'algorisme que troba $\operatorname{Res}(f,g,x)$:

ENTRADA: f, g
SORTIDA: res
$h := f$
$s := g$
$res := 1$
MENTRE $\deg(s) > 0$ FER
  $r := \operatorname{residu}(h,s)$
  $res := (-1)^{\deg(r)\deg(s)}\ \operatorname{lead}(s)^{\deg(h)-\deg(r)} res$
  $h := s$
  $s := r$
FMENTRE
SI $h = 0$ o $r = 0$ ALESHORES $res := 0$ SINO

SI $\deg(h) > 0$ ALESHORES $res := s^{\deg(h)} res$

Proveu que aquest algorisme calcula la resultant de f i g.

3.6. **Resultants i el teorema d'extensió. 3.6.1.** A $k[x,y]$, considereu els dos polinomis

$$\begin{aligned} f &= x^2y - 3xy^2 + x^2 - 3xy, \\ g &= x^3y - 4y^2 + y + x^3 - 4y + 1. \end{aligned}$$

a) Calculeu $\mathrm{Res}(f,g,x)$.
b) Calculeu $\mathrm{Res}(f,g,y)$.
c) Que implica el resultat de l'apartat b) sobre f i g?

3.6.2. Siguin $f, g \in \mathbb{C}[x,y]$. Demostrarem que

$\mathbf{V}(f,g)$ és infinit $\Longleftrightarrow$ f i g tenen un factor comú no constant a $\mathbb{C}[x,y]$.

a) Proveu que $\mathbf{V}(f)$ és infinit quan f no és constant.
b) Si f i g tenen un factor comú no constant $h \in \mathbb{C}[x,y]$, aleshores utilitzeu l'apartat a) per demostrar que $\mathbf{V}(f,g)$ és infinit.
c) Demostreu que si f i g no tenen factors comuns no constants, llavors $\mathrm{Res}(f,g,x)$ i $\mathrm{Res}(f,g,y)$ són diferents de zero i arribeu finalment a la conclusió que $\mathbf{V}(f,g)$ és finit.

3.6.3. Si $f, g \in k[x,y]$ vam demostrar que

$$\mathrm{Res}(f,g,x) \ \in I_1 = < f, g > \bigcap k[y].$$

El que és interessant és que la resultant no genera necessàriament I_1.

a) Demostreu que $\mathrm{Res}(f,g,x)$ genera I_1, per $f = xy - 1$ i $g = x^2 + y^2 - 4$.
b) Demostreu que $\mathrm{Res}(f,g,x)$ no genera I_1, per $f = xy - 1$ i $g = yx^2 + y^2 - 4$. Veieu alguna connexió entre l'apartat b) i el teorema d'extensió?

3.6.4. En la demostració del teorema 3, vam avaluar la resultant $h = \mathrm{Res}(f,g,x_1)$ a $y = c$, i conjecturavem que el resultat encara era la resultant. Per veure que això no sempre és cert, posarem alguns exemples.

a) Sigui $f = x^2y + 3x - 1$ i $g = 6x^2 + y^2 - 4$. Calculeu $h = \mathrm{Res}(f,g,x)$ i demostreu que $h(0) = -180$. Però si posem $y = 0$ en f i g, tenim els següents polinomis $3x - 1$ i $6x^2 - 4$. Comprobeu que $\mathrm{Res}(3x-1, 6x^2-4) = -30$. Així, $h(0)$ no és la resultant. Noteu que la igualtat falla: $h(0)$ és un determinant 4×4, mentre que $\mathrm{Res}(3x-1, 6x^2-4)$ és un determinant 3×3.
b) Ara sigui $f = x^2y + 3xy - 1$ i $g = 6x^2 + y^2 - 4$. Calculeu $h = \mathrm{Res}(f,g,x)$ i verifiqueu que $h(0) = 36$. Posant $y = 0$ en f i g s'obtenen els polinomis -1 i $6x^2 - 4$. Proveu que la resultant és 1. Així doncs $h(0)$ té un factor 36 de més.

3.6.5. Sigui $f = x^2y+x-1$ i $g = x^2y+x+y^2-4$. Si $h = \mathrm{Res}(f,g,x) \in \mathbb{C}[y]$, demostreu que $h(0) = 0$. Però si substituim $y = 0$ a f i g, tindrem $x-1$ i $x-4$. Demostreu que aquests polinomis tenen una resultant diferent de zero. D'aquesta manera $h(0)$ no és una resultant.

3.6.6. Sigui $I = < f_1, f_2, f_3 > \subset k[w,x,y,z]$, on

$$\begin{aligned} f_1 &= x^4 - 2xy^2 + zw, \\ f_2 &= wx^2 - w^2z + y, \\ f_3 &= x^3 + 3w. \end{aligned}$$

a) Calculeu les resultants generalitzades de f_1, f_2, f_3 respecte w. Haurieu d'aconseguir dos polinomis $h_{10}, h_{01} \in k[x,y,z]$.
b) Demostreu que $I_1 = I \bigcap k[x,y,z]$ no és generat per les resultants generalitzades. Ajut: Utilitzeu ordre lexicogràfic amb $w > z > y > x$.

3.6.7. Siguin els polinomis $f, g_1, \ldots, g_s \in k[x]$. Proveu que f és un factor comú de $g_1, \ldots, g_s$, si i només si f divideix a $g_1u_1 + \cdots + g_su_s$ en $k[x, u_1, \ldots, u_s]$.

4. El Diccionari Àlgebra-Geometria

4.1. **Hilbert Nullstellensatz. 4.1.1.** Recordeu que $\mathbf{V}(y-x^2, z-x^3)$ és la cúbica gerxa de $\mathbb{R}^3$.

a) Proveu que $\mathbf{V}((y-x^2)^2, (z-x^3)^2)$ és la mateixa varietat.
b) Proveu que tota varietat $\mathbf{V}(I) \subset \mathbb{R}^n$, $I \subset \mathbb{R}[x_1, \ldots, x_n]$, pot definir-se per una única equació (i per tant, per un ideal principal).

4.1.2. Sigui $J = < x^2+y^2-1, y-1 >$. Trobeu $f \in \mathbf{I}(\mathbf{V}(J)$ tal que $f \notin J$.

4.1.3. Amb el canvi de variable

$$\begin{aligned} x_1 &= \tilde{x}_1 \\ x_2 &= \tilde{x}_2 + a_2\tilde{x}_1 \\ &\ldots \\ x_n &= \tilde{x}_n + a_n\tilde{x}_1 \end{aligned}$$

un polinomi $f(x_1, \ldots, x_n)$ de grau total N es transforma en un polinomi de la forma

$$\tilde{f} = c(a_2, \ldots, a_n)\tilde{x}_1^N + \text{termes on } \tilde{x}_i \text{ té grau } < N$$

Volem provar que $c(a_2, \ldots, a_n)$ és un polinomi no nul en $a_2, \ldots, a_n$.

a) Escriviu $f = h_N + h_{N-1} + \cdots + h_0$ on cada h_i, per $0 \geq i \geq N$ és homogeni de grau i (és a dir, cada monomi de h_i té grau total i). Proveu que, després del canvi de coordenades, el coeficient $c(a_2, \ldots, a_N)$ de $\tilde{x}_1^N$ en $\tilde{f}$ és $h_N(1, a_2, \ldots, a_n)$.
b) Sigui $h(x_1, \ldots, x_n)$ un polinomi homogeni. Proveu que h és el polinomi nul a $k[x_1, \ldots, x_n]$ ssi $h(1, x_2, \ldots, x_n)$ és el polinomi nul a $k[x_2, \ldots, x_n]$.
c) Finalment proveu que $c(a_2, \ldots, a_n)$ és un polinomi no nul en $a_2, \ldots, a_n$.

4.1.4. Proveu que un cos algebraicament tancat ha de ser infinit. Ajut: Donats n elements $a_1, \ldots a_n$ d'un cos k podem escriure un polinomi $f \in k[x]$ amb la propietat de que $f(a_i) = 1$ per tot i ?

4.1.5. El propòsit d'aquest exercici és provar que si k és un cos qualsevol que no és algebraicament tancat, llavors tota varietat $V \subset k^n$ pot ser definida per una única equació.

a) Sigui $f = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ un polinomi de grau n i definim la seva homogeneïtzació f^h com $f^h = a_0x^n + a_1x^{n-1}y + \cdots + a_{n-1}xy^{n-1} + a_ny^n$. Proveu que f té alguna arrel a k ssi existeix algún $(a,b) \in k^2$ tal que $(a,b) \neq (0,0)$ i $f^h(a,b) = 0$. Ajut: Proveu que $f^h(a,b) = b^n f^h(a/b, 1)$ per $b \neq 0$.
b) Si k no és algebraicament tancat, proveu que existeix $f \in k[x,y]$ tal que la varietat definida per $f = 0$ consisteix exactament en l'origen

$(0,0) \in k^2$. Ajut: Considereu un polinomi de $k[x]$ que no tingui arrels a k, i la seva homogeneització.

c) Si k no és algebraicament tancat, proveu que existeix per a cada enter $s > 0$ un $f \in k[x_1, \ldots, x_s]$ tal que la única solució de $f = 0$ és l'origen $(0, \ldots, 0) \in k^s$. Ajut: Utilitzeu inducció i l'apartat b). Vegeu també l'exercici 1.

d) Si $W = \mathbf{V}(g_1, \ldots, g_s)$ és una varietat de k^n, on k no és algebraicament tancat, porveu que W pot ser definida per una única equació. Ajut: Considereu el polinomi $f(g_1, \ldots, g_s)$ anterior.

4.1.6. Sigui k un cos arbitrari i S el subconjunt de tots els polinomis de $k[x_1, \ldots, x_n]$ que no tenen zeros a k^n. Si I és un ideal qualsevol de $k[x_1, \ldots, x_n]$ tal que $I \cap S = \phi$, proveu que $\mathbf{V}(I) \neq \phi$. Ajut: Si k no és algebraicament tancat emprar l'exercici anterior.

4.1.7. A l'exercici 1 hem trobat dos ideals de $\mathbb{R}[x, y]$ que donen lloc a la mateixa varietat no nul.la. Proveu que un d'ells conté l'altre. És possible trobar dos ideals a $\mathbb{R}[x, y]$, no continguts un en l'altre, que donin lloc a la mateixa varietat? La mateixa qüestió a $\mathbb{R}[x]$.

4.2. **Ideals radicals i correspondència Ideal-Varietat.** **4.2.1.** Sigui k un cos (no cal que sigui algebraicament tancat). Proveu que $\sqrt{< x^2, y^2 >} =< x, y >$ i, més en general, proveu que per a qualssevulla n, m enters és $\sqrt{< x^n, y^m >} =< x, y >$.

4.2.2. Sigui $I = < f^2, g^3 >$, on f i g són polinomis no constants de $k[x, y]$. Es verifica necessàriament $\sqrt{I} = < f, g >$? Expliqueu-ho.

4.2.3. Proveu que $< x^2 + 1 > \subset \mathbb{R}[x]$ és un ideal radical, però en canvi $\mathbf{V}(x^2 + 1)$ és la varietat buida.

4.2.4. Sigui I un ideal de $k[x_1, \ldots, x_n]$, on k és un cos arbitrari.

a) Proveu que $\sqrt{I}$ és un ideal radical.

b) Proveu que I és radical ssi $I = \sqrt{I}$.

c) Proveu que $\sqrt{\sqrt{I}} = \sqrt{I}$.

4.2.5. Proveu que **I** i **V** són inverses respecte de la inclusió.

4.2.6. Sigui I un ideal de $k[x_1, \ldots, x_n]$.

a) En el cas particular en que $\sqrt{I} = < f_1, f_2 >$, amb $f_i^{m_i} \in I$, proveu que $f^{m_1+m_2-1} \in I$ per tot $f \in \sqrt{I}$.

b) Proveu ara que per tot I, existeix un m_0 tal que $f^{m_0} \in I$ per tot $f \in \sqrt{I}$. Ajut: Escriviu $\sqrt{I} = < f1, \ldots, f_s >$.

4.2.7. Determineu si els següents polinomis pertanyen als corresponents radicals. Si la resposta és afirmativa, quina és la potència mínima del polinomi que pertany a l'ideal?

a) És $x + y \in \sqrt{< x^3, y^3, xy(x+y) >}$?
b) És $x^2 + 3xz \in \sqrt{< x + z, x^2y, x - z^2 >}$?

4.2.8. Proveu que si f_m i f_{m+1} són polinomis homogenis de graus m i $m+1$ respectivament, sense factors comuns [és a dir $\mathrm{GCD}(f_m, f_{m+1}) = 1$], llavors $h = f_m + f_{m+1}$ és irreductible.

4.2.9. Donats $f, g \in k[x_1, \ldots, x_n]$, utilitzeu la factorització única per provar que existeix el $\mathrm{GCD}(f, g)$. Proveu també que $\mathrm{GCD}(f, g)$ és únic a excepció d'una constant multiplicativa de k diferent de zero.

4.2.10. Proveu la següent caracterització teòrica del $\mathrm{GCD}(f, g)$: Donats $f, g, h \in k[x_1, \ldots, x_n]$, llavors $h = \mathrm{GCD}(f, g)$ ssi h és un generador de l'ideal principal més petit que conté $< f, g >$, (és a dir, si $J \subset < h >$, on J és un ideal principal tal que $< f, g > \subset J$.

4.2.11. Trobeu una base de l'ideal

$$\sqrt{< x^5 - 2x^4 + 2x^2 - x, x^5 - x^4 - 2x^3 + 2x^2 + x - 1 >}$$

4.2.12. Sigui el polinomi de $\mathbb{Q}[x, y]$,

$$\begin{aligned} f &= x^5 + 3x^4y + 3x^3y^2 - 2x^4y^2 + x^2y^3 - 6x^3y^3 - 6x^2y^4 \\ &\quad + x^3y^4 - 2xy^5 + 3x^2y^5 + 3xy^6 + y^7. \end{aligned}$$

Calculeu $\sqrt{< f >}$.

4.2.13. Sigui $J = < xy, (x - y)x >$. Describiu $\mathbf{V}(J)$ i proveu que

$$\sqrt{J} = < x > .$$

4.2.14. Proveu que $I = < xy, xz, yz >$ és un ideal radical. Ajut: Si dividim $f \in k[x, y, z]$ per xy, xz, yz, quin aspecte té el residu? Cóm és f^m?

5. Examens

5.1. **Examen** 17-4-96.

• **1.** Quan un ideal té una base on algún dels seus elements pot ser factoritzat, podem utilitzar la factorització com ajuda per entendre la varietat.

a) Demostreu que si $g \in k[x_1, \ldots, x_n]$ factoritza en la forma $g = g_1 g_2$, i $f \in k[x_1, \ldots, x_n]$, per $i = 1 \div s$, llavors
$$\mathbf{V}(f, g) = \mathbf{V}(f, g_1) \cup \mathbf{V}(f, g_2).$$

b) Demostreu que a $\mathbb{R}^3$,
$$\mathbf{V}(y - x^3, x^2 z - y^4) = \mathbf{V}(y - x^3, x^2 z - x^{12}).$$
Nota: Utilitzeu ideals i sigueu rigorosos en la demostració! Si feu servir alguna proposició, enuncieu-la.

c) Utilitzeu a) per descriure la varietat de l'apartat b).

d) Escriviu la fórmula que generalitza a la de l'apartat a) per $\mathbf{V}(f_1, \ldots, f_s)$, i $f_i = g_{i1} \cdots g_{i,j_i}$.

• **2.** Donat un ideal $I \subset k[x_1, \ldots, x_n]$, (on k és un cos), definim el conjunt $C_I \subset k^n$ associat a I de la següent manera:
$$C_I = \{(a_1, \ldots, a_n) \in k^n : \text{ per tot } f \in I \text{ és } f(a_1, \ldots, a_n) = 0\}.$$

a) Demostreu (donant l'enunciat dels teoremes que utilitzeu), que C_I és una varietat algebraica. Per aquest motiu C_I s'anomena varietat de l'ideal I i es denota per $\mathbf{V}(I)$.

b) Donat un subconjunt $S \subset k^n$, com definiries un subconjunt $F_S \subset k[x_1, \ldots, x_n]$ associat a S ? És un ideal? Justifica la resposta.

c) Com podem associar una varietat a S ? Quines relacions i haurà entre S i l'esmentada varietat? Justifiqueu la resposta.

• **3.** Siguin $f_1 = y^3 - x^2 z$ i $f_2 = xz - 1$.

a) Proveu que $\{f_1, f_2\}$ és una base de Gröbner de l'ideal $I = < f_1, f_2 >$ respecte a l'ordre `grevlex` amb $x > y > z$.

b) Doneu la b. de G. reduda, una b. de G minimal però no reduda i una b. de G. que no sigui minimal.

c) Determineu una b. de G. de I en ordre `lex` amb $x > y > z$.

d) Doneu la b. de G. reduda.

e) Dieu si el polinomi $f = x^2 y^3 + y^4 z + x^2 z^2 - x^3 - xyz$ pertany a I.

• **4.** A $\mathbb{F}_2[x, y]$ considerem el conjunt I de polinomis que s'anul.len sobre $\mathbb{F}_2$.

a) Proveu que I és un ideal de $\mathbb{F}_2[x, y]$.

b) Proveu que $F = \{x^2 - x, y^2 - y\}$ és una base de I. És una base de Gröbner per algún ordre?
c) Ara volem fer el mateix a $\mathbb{F}_3[x,y]$. Trobeu una base de l'ideal de polinomis de $\mathbb{F}_3[x,y]$ que s'anul.len a $\mathbb{F}_3$, i proveu que ho és.

5.2. **Examen.** 1-7-96.

• **1.** Donada la corba de $\mathbb{R}^2$

$$(x^2+y^2)^2 - y(3x^2-y^2) = 0$$

a) Escriviu el sistema que determina els seus punts singulars. L'ideal generat per aquest sistema l'anomenarem I. La seva base de Gröbner lex amb $x > y$ és $G = \{x^2 - y^2, xy, y^3\}$. Determineu $\mathbf{V}(I)$ i proveu que l'origen és l'únic punt singular. Determineu $\sqrt{I}$ a $\mathbb{C}[x,y]$ i a $\mathbb{R}[x,y]$.
b) Amb quina multiplicitat mínima tallen a la corba les rectes que passen per $(0,0)$?
c) Determineu les rectes que passen per $(0,0)$ i tallen a la corba amb multiplicitat més gran que la mínima determinada. Les anomenarem tangents efectives. Quina forma té la corba al voltant de l'origen?

• **2.** Sigui $I \subset \mathbb{C}[x,y,z]$ un ideal i G una base de Gröbner respecte a l'ordre lex amb $z > y > x$:

$$\begin{aligned} G \;=\; & < (x-2)(y-1)z^2 - xy,\ (8y^2-8y)z - 4xy^2 + \\ & +4y^3x - 2x^2y - x^3y,\ (x^2-4)z - 2xy, \\ & 8xy + 4x^2y - 4x^2y^2 + 4x^2y^3 - 2x^3y - x^4y > \end{aligned}$$

i $I_1 = I \cap \mathbb{C}[x,y]$.

a) Doneu I_1. Per quins punts de les solucions parcials $\mathbf{V}(I_1)$ el teorema d'extensió no garanteix que hi hagi solució completa a $\mathbf{V}(I)$ sobre $\mathbb{C}$?
b) Estudieu que passa en cada un dels punts determinats a a). Exten la solució? Si per algún d'ells extén, quàntes solucions de $\mathbf{V}(I)$ corresponen a la solució parcial?
c) Pels restants punts de $\mathbf{V}(I_1)$ discutiu també quàntes solucions de $\mathbf{V}(I)$ corresponen a cada punt.
d) Discutiu els apartats b) i c) a $\mathbb{R}[x,y,z]$.
e) Utilitzeu el fet que G és una base de Gröbner lex en algún apartat? En quin i per què?
f) Describiu geomètricament la varietat $\mathbf{V}(I)$ a la llum dels resultats obtinguts i descomposeu-la tant com pogueu.

• **3.** Donats

$$\begin{aligned} f &= xy^3 - 2xy^2 + 3xy - y^2 - 3 + 2y \\ g &= y^3 - 2y^2 + 3y + xy^2 - 2xy + 3x \end{aligned}$$

a) Determineu $\mathrm{Res}(f,g,x)$. Què podeu afirmar sobre els factors comuns de f i g ?
b) Proveu que $\mathrm{Res}(f,g,y)=0$. Què podeu afirmar sobre els factors comuns de f i g a partir de a) i b) ? Determineu-los.
c) Com sabeu $\mathrm{Res}(f,g,x)$ pertany a l'ideal $< f,g > \cap \mathbb{C}[y]$. Determineu la combinació lineal que genera $\mathrm{Res}(f,g,x)$ a partir de f i g.

6. Pràctiques

6.1. **Pràctica: Gràfiques de Varietats.** *Comandes a recordar: Maple* disposa de moltes comandes per fer gràfics en 2D i 3D. En 3D, la funció gràfica més característica és `plot3d`. Però carregant la llibreria `plots`, amb la comanda `with(plots);` tenim accés a moltes altres comandes gràfiques. Destaquem `cylinderplot`, `sphereplot`, `implicitplot3d`. Además, cadascuna d'aquestes funcions, admet diferents representacions dels arguments. Consulteu els ajuts per fer la pràctica.

Objectiu: Visualitzar els gràfics de les següents varietats algebraiques de 3D, a fi d'aprendre a utilitzar les comandes gràfiques de forma interessant.

- **1.** La cúbica guerxa:
$$V_1 = \mathbf{V}(y - x^2, z - x^3)$$
- **2.** El paraboloid
$$V_2 = \mathbf{V}(z - x^2 - y^2)$$
- **3.** El con
$$V_3 = \mathbf{V}(z^2 - x^2 - y^2)$$
- **4.** Una corba amb una linia singular
$$V_4 = \mathbf{V}(x^2 - y^2z^2 + z^3)$$

que es pot parametritzar de la següent manera:
$$\begin{aligned} x &= t(u^2 - t^2) \\ y &= u \\ z &= u^2 - t^2. \end{aligned}$$

Feu la gràfica pels valors dels paràmetres $-1 \leq t \leq 1$ i $-1 \leq u \leq 1$

6.2. **Pràctica: Ordenació de monomis i divisió. Objectiu:** Capturar les rutines d'ordenació monomial i de determinació del terme principal (*lead-term*), de la llibreria `grobner` de Maple, fer adaptacions i programar la divisió de polinomis utilitzant el paquet capturat.

Procediment: Per aquest objectiu utilitzarem Maple per DOS enlloc de per Windows.

En primer lloc executarem `with(grobner)` per carregar la llibreria. Seguidament feu un help de la rutina `leadmon` de la llibreria i familiaritzeu-vos amb ella. Observeu que permet obtenir tant el monomi principal com el coeficient principal. Practiqueu amb exemples comprenent també exemples de $\mathbb{Q}(a, b, \dots)[x, y, \dots]$.

A continuació, des del menú F10 aneu a "interface" i canvieu `verboseproc` al valor 2. Això permetrà que pogueu llistar les rutines de les llibreries de Maple també. Feu `print(leadmon)`. Observareu el llistat de la rutina i veureu que crida a una altra rutina del paquet `grobner`. LListeu-la també i així successivament per totes les rutines pròpies del paquet cridades a partir de `leadmon`. Un cop llistades totes, també des del menú F10 salveu la sessió en un arxiu. Haureu capturat les rutines i estareu en disposició de per la pràctica.

Pràctica:

Un cop capturades les rutines descrites més amunt, estudieu la seva estructura i mireu d'entendre-les. Són fora senzilles. Canvieu de nom les rutines, tant en les capaleres com en les cirdes internes a fi de que no es confonguin amb les de la llibrearia i a fi de modificar-les sense interferir. Doneu un nom curt a cada rutina que correspongui a la seva funció. Així `leadmon` l'anomenareu `leadt`.

• **1.** Modifiqueu la rutina `leadmon` de forma que accepti els noms `lex` ademés de `plex` i `grevlex` ademés de `tdeg`. Afegiu una nova rutina semblant a la que calcula el teme principal en ordre *grevlex* que el calculi en ordre `grlex`. Quines són les funcions essencials de Maple que fan eficient el càlcul del terme principal? Com són aquestes rutines i per què?

• **2.** Utilitzant la rutina `leadt` que heu capturat i transformat, programeu la divisió seguint l'estil de programació de les rutines capturades. La rutina ha de retornar el residu de la divisió i optativament fer accessibles els quocients, de la mateixa manera que `leadmon` fa accessible el coeficient principal.

• **3.** Apliqueu les rutines programades comprovant que cumpleixen totes les propietats de la divisió. Proveu-les també a $\mathbb{Q}(a, b, c)[x, y, z]$. Funciona correctament?

6.3. **Pràctica: Algorisme de Buchberger. Objectiu:** Programar l'algorisme de Buchberger de forma eficient, incorporant els dos criteris per evitar comprobacions, i que hem estudiat. La rutina ha de ser autònoma, és a dir, sense fer servir la llibreria `grobner` de Maple, o apropiant-se de les parts que necessiteu.

• **1.** Heu d'utilitzar i perfeccionar les rutines programades a la pràctica 6.2 i perfeccionar-les.

• **2.** En segon lloc necessitareu programar també de manera eficient la rutina `spol` que podeu comparar amb `spoly`. Abans de passar a preparar l'algorisme de Buchberger, contrasteu que les vostres rutines bàsiques funcionen adequadament i sino trobeu les mancances, comenteu-les i amilloreu-les.

• **3.** Un cop assegurat que disposeu de rutines eficients, passeu a programar l'algorisme de Buchberger directe i feu una rutina que anomenarem `buchber0`, i un algorisme `reduc` per redur una base de Groebner. Com criteri de normalització podeu utilitzar el que donen `primpart` i `content`.

Compareu, calculant algunes bases de Groebner senzilles, que s'obté el resultat adient i compareu també temps. Atenció, la rutina `gbasis` de la llibreria `grobner` porta incorporada la opció `remember`, i això comporta que una vegada ha calculat una base de Groebner concreta, quan se li torna a demanar el mateix càlcul no el repeteix sino que retorna el resultat directament. Per mesurar temps d'aquesta rutina i les que ella crida cal doncs que les mesureu la primera vegada que li feu calcular.

• **4.** Finalment construu la rutina `buchber` incorporant els dos criteris per evitar comprovacions estudiats a classe i feu control de temps. Feu també estadístiques, per alguna base de Grobner de complicació mitjana, del nombre de comprobacions que evita un criteri i l'altre i estimeu el temps que han pogut estalviar.

6.4. **Pràctica: Implicitació racional.** *Comandes a recordar:* Ademés de les comandes característiques de bases de Groebner recordeu: `map, indets, collect, numer, expand`.

Llibreria que s'ha de carregar: `geomplot`. Per carregar-la cal fer `with(share): readshare(geomplot,geomplot): with(geomplot):`

Objectiu: Revisar el problema 1.3.9. de l'impliciatació de la *strofoide* a la llum dels teoremes de la implicitació racional i de l'extensió.

Les equacions paramètriques de la strofoide venen donades per

$$\begin{aligned} x &= a \sin t \\ y &= a \tan t(1 + \sin t) \end{aligned}$$

(1)

• **1.** Utilitzant `plot` en versió paramètrica, representeu el conjunt de punts descrit per la paramatrització donada, per $-\pi \leq t \leq \pi$, i en la finestra `x=-2..2, y=-2..2`. Teniu alguna observació a fer?

• **2.** Elimineu sense precaucions t de la parametrització (1), i obteniu una varietat de $\mathbb{R}^2$ que conté la parametrització

• **3.** Emprant `gmplot` de la llibreria `geomplot`, representeu la varietat obtinguda en 2). Oi que sobra un tro?

• **4.** A fi d'obtenir una parametrització racional, feu el canvi de variable $\tan \frac{t}{2} = u$. Obtindreu una parametrització racional de la strofoide.

• **5.** Poseu $a = 1$. Empreu ara el teorema de l'implicitació racional per obtenir la varietat algebraica més petita que conté la parametrització calculada a 4).

• **6.** Feu novament el gràfic de la varietat obtinguda. És ara correcte?

• **7.** Apliqueu el teorema de l'extensió per saber si la parametrització de 4) omple tota la varietat determinada a 5). Distingiu el cas $\mathbb{C}$ del cas $\mathbb{R}$.

6.5. **Pràctica: Primeres aplicacions de les bases de Gröbner. Comandes:** Cal carregar la llibreria `grobner` fent `with(grobner)`. D'aquesta llibreria us seran útils les comandes `gbasis` i `normalf`. Altres comandes de Maple útils per la pràctica: `map`, `diff`, `solve`, `indets`.

Pràctica:

- **1. Pertinena a un ideal, comparació d'ideals.**
Donats els dos ideals

$$\begin{aligned} F_1 &= [xz - y^2, x^3 - z^2] \\ F_2 &= [-y^2z + x^4, -y^2z^4 + x^2y^4z, y^8z - y^2z^6] \end{aligned}$$

a) Són el mateix ideal?
b) Algún d'ells està inclos en l'altre?

- **2. Solució d'un sistema d'equacions**
Volem trobar els màxims i mínims de la funció $f = x^3+2xyz-z^2$ subjectes a la condició $x^2 + y^2 + z^2 = 1$.
Procedirem de la següent manera:
  - Determineu el sistema d'equacions que s'ha de verificar emprant els multiplicadors de Lagrange.
  - Considereu l'ideal generat per les equacions corresponents i determineu la base de Gröbner en ordre `lex` amb $m > x > y > z$.
  - Encara que no hem vist la raó, observareu que entre els polinomis de la base de Gröbner hi ha un que únicament conté la z, un que conté la y i la z i un que conté la x, y, z o pot ser només la x i la z.
  - Resoleu l'equació en z. Per cada valor de z obteniu els valors de y i x substituint i aillant en les equacions corresponents.
  - Quants punts obtenim? Quant val f en cada un d'aquests punts?

6.6. **Pràctica: Envolvents i punts singulars.** *Comandes útils a recordar:* Ademés de les comandes característiques de bases de Gröbner recordeu: `map, indets, collect, expand, solve, fsolve`.

Llibreries que s'han de carregar: `grobner, geomplot`. Per carregar la segona cal fer

```
with(share): readshare(geomplot,geomplot): with(geomplot):
```

Objectiu: Sigui la següent família de cercles $\mathbf{V}(F_t)$ amb $t \in \mathbb{R}$ donada per

$$F = (x-t)^2 + (y-t^2)^2 - 4$$

Volem determinar l'envolvent C els seus punts singulars, i estudiar quants cercles tangents passen per cada punt de l'envolvent, així com l'ordre amb que tallen les rectes en els punts singulars.

• **1.** Assigneu a `F` la família de corbes.

• **2.** Emprant `gmplot`, representeu uns quants cercles de la família $\mathbf{V}(F_t)$, per $t = i/2$, $i = -6 \div 6$.

• **3.** Assigneu a `F1` la llista de polinomis que defineixen l'envolvent.

• **4.** Determineu la varietat que defineix l'envolvent, calculant la base de Groebner `G1` corresponent.

• **5.** Feu un gràfic amb l'envolvent, i afegiu (en un altre color) els cercles de la família $\mathbf{V}(F_t)$ dibuixats en la pregunta 2. Us esperàveu el gràfic que apareix? Quina sorpresa trobeu?

• **6.** Calculeu, si en té, els punts singulars de l'envolvent.

• **7.** Es pregunta: Per cada punt (x, y) de l'envolvent hi ha algún cercle que és tangent? Per què? Contesteu utilitzant el teorema de l'extensió.

• **8.** A la vista de la base de Gröbner calculada, podem afirmar que per un punt ordinari de C hi ha un únic cercle tangent? Per quins punts passen més d'un cercle tangent? Extreieu de la base de Gröbner les equacions que determinen aquests punts. Quants cercles tangents passen per cada un d'aquests punts especials?

• **9.** Determineu els punts de C per on poden passar més d'un cercle tangent.

• **10.** Determineu els cercles tangents en aquests punts.

• **11.** Feu un gràfic amb l'envolvent i els cercles calculats a 10.

• **12.** Determineu tots els cercles de la família $\mathbf{V}(F_t)$ que passen pels punts singulars. Són tots tangents?

• **13.** Estudieu ara la multiplicitat amb que tallen a l'envolvent les rectes que passen pels punts singulars. Interpreteu les rectes que tallen amb màxima multiplicitat.