Cuprins

Capitolul 1

Teoreme de geometrie demonstrate pe calculator

EOMETRIA este una din cele mai vechi ramuri ale matematicii. Simbioza ei cu aritmetica datează încă din antichitate. Legăturile strânse şi fecunde cu algebra sunt mai noi, şi au la origine coordonatizarea descoperită de Descartes.

În acest capitol va fi vorba de legături descoperite mai recent, denumite astăzi geometrie algebrică. Vom face o introducere în geometria algebrică computaţională, care se bazează esenţial pe teoria bazelor Gröbner . Contextul general va fi în acelaşi timp algebric şi geometric. Din punct de vedere algebric, obiectele de studiu vor fi idealele inelelor de polinoame cu mai multe variabile, iar din punct de vedere geometric, varietăţile afine sau proiective.

1.1 Concepte de bază

În ACEASTĂ SECŢIUNE reamintim câteva concepte de bază ale algebrei polinoamelor cu mai multe variabile, precum şi a noţiunilor geometrice aferente acestora, a varietăţilor algebrice.

1.1.1 Polinoame cu mai multe variabile

Polinoamele sunt expresii algebrice construite din variabile şi numere (coeficienţi) cu ajutorul operaţiilor de adunare, scădere şi înmulţire.

Prin urmare aceste trei operaţii se pot efectua neîngrădit şi între polinoame. Pentru a putea încerca împărţirea (cu rest) a polinoamelor este convenabil ca între coeficienţii acestora să dispunem şi de împărţire neîngrădită, în termeni

tehnici mulţimea coeficienţilor este bine să formeze un corp de numere. Corpurile de numere cele mai familiare sunt:

- corpul numerelor raţionale $\mathbf{Q}$
- corpul numerelor reale $\mathbf{R}$
- corpul numerelor complexe $\mathbf{C}$
- corpri de numere algebrice, ex. $\mathbf{Q}(\sqrt{2})$
- corpuri finite, ex. $\mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_5$.

Aceste corpuri de numere le vom avea în vedere şi în realizarea computaţională a polinoamelor. Ocazional, vor mai apare şi corpuri de fracţii raţionale, dar ele vor avea o prezentare satisfăcătoare în locul respectiv.

În cele ce urmează cititorul este invitat să gândească în primul rând corpul numerelor complexe drept corp al coeficienţilor.

Definiţie 1.1.1. Un *monom* în variabilele $x_1, x_2, \ldots, x_n$ este un produs de forma

$$x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \cdots \cdot x_n^{\alpha_n},$$

unde exponenţii sunt întregi nenegativi. Suma acestora $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$ se numeşte *gradul total* al monomului.

Dăm acum o definiţie formală pentru noţiunea de polinom.

Definiţie 1.1.2. Un *polinom* f în variabilele $x_1, x_2, \ldots, x_n$ cu coeficienţi în corpul k este o combinaţie liniară finită de monoame, cu coeficienţi din k, adică

$$f = \sum_\alpha a_\alpha x^\alpha, \qquad a_\alpha \in k,$$

unde $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Mulţimea acestor polinoame se notează cu $k[x] = k[x_1, x_2, \ldots, x_n]$.

Următoarea definiţie practic fixează o terminologie.

Definiţie 1.1.3. Fie $f = \sum_\alpha a_\alpha x^\alpha$ un polinom în $k[x]$.

- Numărul $a_\alpha \in k$ se numeşte *coeficientul* lui x^α.
- Dacă $a_\alpha \neq 0$, $a_\alpha x^\alpha$ se numeşte *termen* al polinomului.
- *Gradul* polinomului, notat $\deg(f)$ este $\max_\alpha\{|\alpha|;\ \alpha \neq 0\}$.

Definiţie 1.1.4. Se numeşte *spaţiu afin* n-dimensional peste corpul k

$$k^n = \{(a_1, a_2, \ldots, a_n); \quad a_i \in k, i = 1, 2, \ldots, n\}.$$

Cu ajutorul unui polinom de n variabile putem defini o funcţie pe spaţiul afin n-dimensional, folosind "formula" polinomului pentru calculul valorii funcţiei. Mai exact polinomul $f = \sum_\alpha a_\alpha x^\alpha$ din $k[x_1, x_2, \ldots, x_n]$ defineşte o funcţie

$$f : k^n \to k,$$

prin asocierea lui $(a_1, a_2, \ldots, a_n)$ cu $f(a_1, a_2, \ldots, a_n)$, valoare a polinomului ce se obţine prin înlocuirea lui x_1 cu a_1, a lui x_2 cu a_2, etc.

Se pune imediat întrebarea, în ce măsură polinomul şi funcţia polinomială asociată se determină reciproc? Întrucât diferenţei polinoamelor corespunde diferenţa funcţiilor, şi polinomul nul (cu toţi coeficienţii nuli) defineşte evident funcţia identic nulă, întrebarea de mai sus se reformulează astfel: există oare polinoame nenule, care să definească funcţia polinomială identic nulă?

Răspunsul la această întrebare este negativ – cum ne aşteptăm de altfel – doar în cazul corpurilor infinite. Dacă un corp k este finit, şi spre exemplu are n elemente, $c_1, c_2, \ldots, c_n$, atunci polinomul $f(x) = (x-c_1)\cdot(x-c_2)\cdot\cdots\cdot(x-c_n)$ are gradul n, deci este nenul în $k[x]$, şi evident defineşte funcţia polinomială nulă pe k.

Are loc deci următoarea propoziţie.

Propoziţie 1.1.5. *Fie k un corp infinit şi $f \in k[x_1, x_2, \ldots, x_n]$ un polinom. Atunci $f = 0$ în $k[x_1, x_2, \ldots, x_n]$ dacă şi numai dacă $f : k^n \to k$, este funcţia identic nulă.*

Demonstraţie. Dacă polinomul este nul, funcţia polinomială este evident nulă. Invers, raţionamentul este o inducţie după numărul variabilelor n. Pentru $n = 1$ fie polinomul de grad m,

$$f = c_m x^m + c_{m-1} x^{m-1} + \cdots + c_1 x + c_0.$$

Corpul k fiind infinit, putem considera $m + 1$ valori, $a_0, a_1, \ldots, a_m$, disticte două câte două. Presupunând, că funcţia polinomială este nulă, egalităţile $f(a_0) = 0, f(a_1) = 0, \ldots, f(a_m) = 0$ formează un sistem de ecuaţii omogen, necunoscutele fiind cei m coeficienţi ai polinomului. Determinantul acestui sistem este

$$\begin{vmatrix} a_0^m & a_0^{m-1} & \ldots & a_0 & 1 \\ a_1^m & a_1^{m-1} & \ldots & a_1 & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_m^m & a_m^{m-1} & \ldots & a_m & 1 \end{vmatrix} = \prod_{i<j} (a_i - a_j) \neq 0,$$

un determinant de tip Vandermonde, diferit de 0. Prin urmare singura soluţie a sistemului este cel nul, deci toţi coeficienţii polinomului, în concluzie şi polinomul, este 0.

Pasul inductiv este simplu, şi este lăsat pe seama cititorului. □

1.1.2 Varietăţi afine

Trecând la punctul de vedere geometric, trebuie să începem cu o definiţie fundamentală.

Definiţie 1.1.6. Fie $f_1, f_2, \ldots, f_m$ polinoame în variabilele $x_1, x_2, \ldots, x_n$ cu coeficienţi în corpul k. Se numeşte *varietate afină* definită de aceste polinoame, mulţimea zerourilor comune ale lor, adică mulţimea notată $V(f_1, f_2, \ldots, f_m)$ dată prin

$$\{(a_1, a_2, \ldots, a_n) : \quad f_i(a_1, a_2, \ldots, a_n) = 0, \quad \text{pentru orice } i = 1, 2, \ldots, m\}.$$

Pentru a accentua caracterul geometric al acestei noţiuni să considerăm nişte exemple, pentru care putem face şi reprezentări grafice. Va trebui deci să considerăm corpul $k = \mathbf{R}$ al scalarilor reali.

Iată mai întâi câteva exemple de varietăţi plane.

Exemplu 1.1.7.

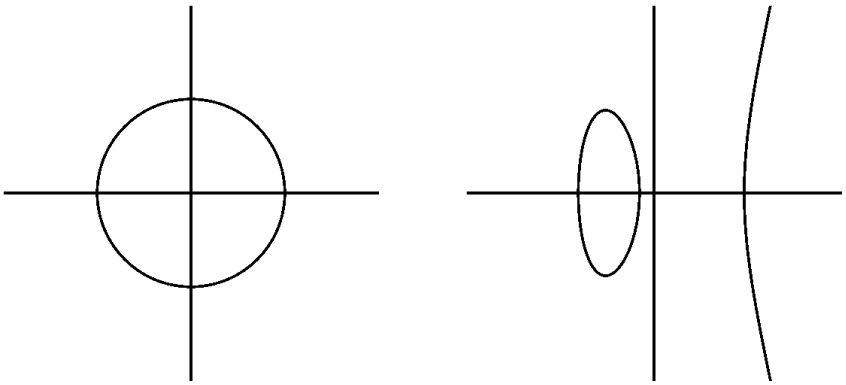

Figura 1.1: $V(xy \cdot (x2 + y2 - 25))$ şi $V(xy(x3 - 20x - 15 - y2))$

Iată şi programul *Singular* cu care am obţinut reprezentarea grafică din figura alăturată 1.1.2. În exemplele care urmează se schimbă doar rândul în care se defineşte idealul I generat de polinomul corespunzător exemplului.

```
LIB "surf.lib";
ring R=0,(x,y),dp;
ideal I=xy*(x2+y2-25);
plot(I);
```

În exemplul de mai sus, factorul xy are un dublu rol. El reprezintă pe de o parte componente ale varietăţii algebrice, dar are şi rolul unui "truc", prin care am inclus axele de coordonate în varietatea algebrică reprezentată.

Iată acum câteva exemple de varietăţi în spaţiu. Acestea pot fi puncte, curbe, sau suprafeţe, respectiv reuniuni ale acestora. În general zerourile unui polinom cu trei variabile reale este o suprafaţă. Programul *surf* apelat din *Singular* este capabil să reprezinte graficul acestor suprafeţe chiar din ecuaţia lor implicită.

Exemplu 1.1.8.

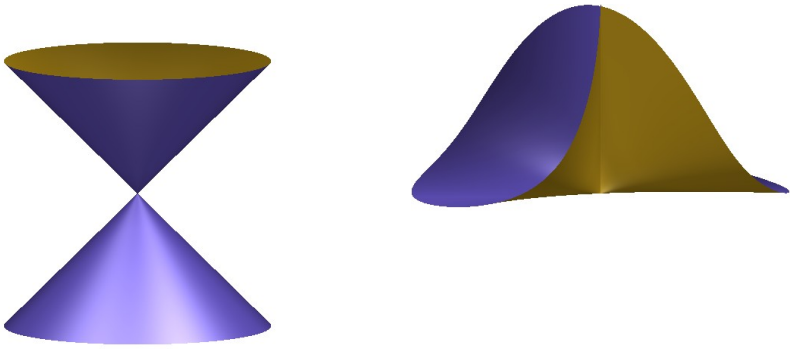

Figura 1.2: $V(x2 - y2 + z2)$ şi $V(x2y - z2)$, "Withney umbrella."

Exemplele care urmează prezintă singularităţi izolate ale unor suprafeţe.

Exemplu 1.1.9.

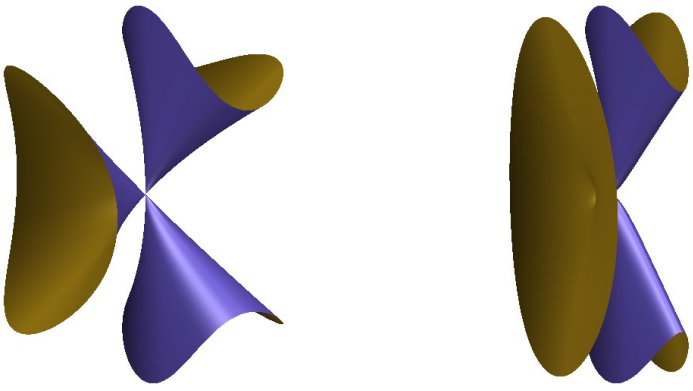

Figura 1.3: $V(z3 - zx2 + y2)$ şi $V(z4 - zx2 + y2)$

În final câteva suprafeţe de interes special. Mai întâi o suprafaţă cuartică (ecuaţie de grad 4), având numărul maxim de singularităţi.

Apoi o serie de suprafeţe de interes pentru clasificarea singularităţiilor suprafeţelor complexe (aici varianta lor în spaţiul real). Prima este o singularitate de tip A_3. Ecuaţia implicită a unei singularităţi de tipul A_k este $A_k = V(x^{k+1} - y2 - z2), k >= 1$. Aici $k = 3$.

Exemplu 1.1.10. O cuartică

$C = V(x4 + y4 + z4 + 1 - x2 - y2 - z2 - y2z2 - z2x2 - x2y2)$,

respectiv singularitatea de tipul

$A_k = V(x^{k+1} - y2 - z2), k >= 1$.

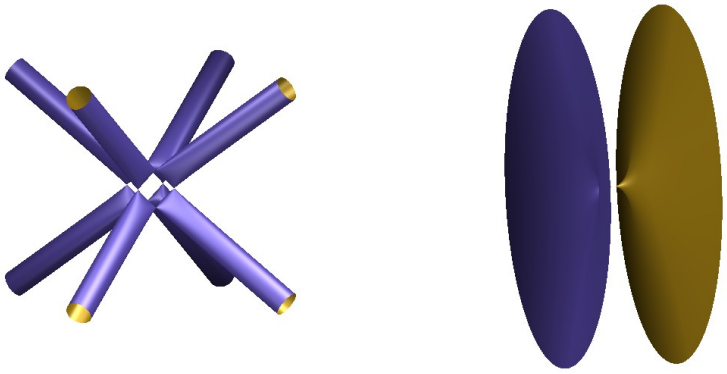

Figura 1.4: O cuartică şi $A_3 = V(x^3 - y2 - z2)$.

Exemplu 1.1.11. Iată şi celelalte singularităţi de tip ADE.

$D_k = V(x(x^{k-2} + y2) + z2)$.

$E_6 = V(x4 + y3 + z2)$.

$E_7 = V(y(x3 + y2) + z2)$.

$E_8 = V(x5 + y3 + z2)$.

Figura 1.5: $D_5 = V(x(x^3 + y2) + z2)$ şi $E_6 = V(x4 + y3 + z2)$.

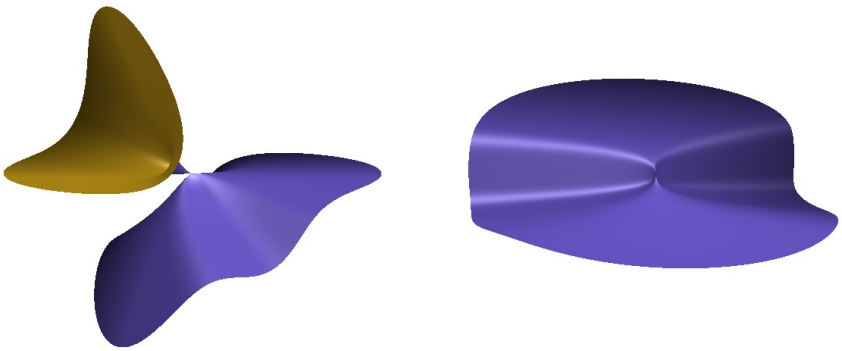

Figura 1.6: $E_7 = V(y(x3 + y2) + z2)$ şi $E_8 = V(x5 + y3 + z2)$.

Revenind la aspecte teoretice, să ne aducem aminte de întrebările pe care le punem în legătură cu problema rezolvării unui sistem de ecuaţii liniare: Are sistemul soluţii sau nu (sunt ecuaţiile sistemului compatibile)? Dacă are, atunci are o singură soluţie, sau mai multe (sistemul este determinat, sau nedeterminat)?

Pentru un sistem de ecuaţii polinomiale neliniar, – deci în legătură cu o varietate algebrică, – întrebările se formulează similar:

- Sunt ecuaţiile compatibile sau nu?
- Dacă sistemul este compatibil, are un număr finit de soluţii sau nu?
- Dacă numărul soluţiilor nu este finit, care este dimensiunea geometrică a mulţimii soluţiilor (numărul parametrilor liberi independenţi)?

Pentru a contura răspunsuri la aceste întrebări, mai avem nevoie de un concept de bază, cel introdus în secţiunea următoare.

Mai înainte însă, să vedem ce operaţii putem face cu varietăţile algebrice? Mai concret, este reuniunea, respectiv intersecţia a două varietăţi algebrice tot o varietate algebrică? Răspunsul este dat în următoarea propoziţie.

Propoziţie 1.1.12. *Fie V şi W varietăţi afine în k^n. Atunci $V \cup W$ şi $V \cap W$ sunt varietăţi afine.*

Demonstraţie. Demonstraţia acestor proprietăţi este una constructivă. Putem da explicit sistemul de ecuaţii polinomiale, ale căror soluţii sunt reuniunea, respectiv intersecţia celor două varietăţi. Fie $V = V(f_1, f_2, \ldots, f_k)$ şi $W = V(g_1, g_2, \ldots, g_l)$. Atunci:

$$\begin{aligned} V \cup W &= V(f_i g_j;\ i = 1, \ldots, k, j = 1, \ldots, l) \\ V \cap W &= V(f_1, f_2, \ldots, f_k, g_1, g_2, \ldots, g_l). \end{aligned}$$

Este clar că $V, W \subseteq V(f_i g_j)$, deci $V \cup W \subseteq V(f_i g_j)$. Invers, fie $(a_1, a_2, \ldots, a_n) \in V(f_i g_j)$ pentru orice i, j. Dacă acest punct este în V, atunci $V(f_i g_j) \subseteq V \cup W$. Dacă însă acest punct nu se află în V, atunci pentru măcar un indice i_0 avem $f_{i_0}(a_1, a_2, \ldots, a_n) \neq 0$. Însă $f_{i_0} g_j(a_1, a_2, \ldots, a_n) = 0$ pentru orice j, deci $g_j(a_1, a_2, \ldots, a_n) = 0$ pentru orice j, ceea ce arată că $(a_1, a_2, \ldots, a_n) \in W$. Prin urmare $V(f_i g_j;\ i = 1, \ldots, k, j = 1, \ldots, l) \subseteq V \cup W$.

Cealaltă egalitate este imediată.

□

1.1.3 Ideale

Vom introduce în această secţiune, corespondentul algebric al conceptului geometric de varietate afină. Acesta este conceptul de ideal.

Să începem cu definiţia conceptului abstract de inel.

Definiţie 1.1.13. O mulţime A înzestrată cu o operaţie de adunare notată $'+'$, şi o operaţie de înmulţire compatibilă cu aceasta (distributivă faţă de aceasta) notată $'\cdot'$, pentru care $(A, +)$ este grup comutativ, şi $(A, \cdot)$ este semigrup, se numeşte *inel*.

Inelul este *comutativ* dacă înmulţirea este comutativă, şi este *unitar*, dacă înmulţirea are element unitate.

În cele ce urmează prin inel vom înţelege un inel comutativ şi unitar, fără a mai preciza explicit aceste proprietăţi.

Observaţia fundamentală pentru contextul nostru este formulată în următoarea propoziţie:

Propoziţie 1.1.14. *Fie k un corp comutativ. Atunci $k[x_1, x_2, \ldots, x_n]$ este un inel comutativ.*

Demonstraţie. Verificarea proprietăţilor care definesc structura de inel este imediată şi este lăsată pe seama cititorului. □

Să remarcăm faptul că singura diferenţă în definiţia unui inel faţă de definiţia unui corp este că aici nu mai pretindem existenţa unui invers pentru fiecare element nenul. Altfel spus, un corp este un inel în care fiecare element nenul este inversabil. Rezultă de aici că problemele legate de divizibilate îşi găsesc ca mediu general şi abstract de studiu, structura de inel.

O primă clasificare a elementelor unui inel este dată prin intermediul conceptelor următoare:

Definiţie 1.1.15. Fie A un inel comutativ şi unitar. Un element $f \in A$, $f \neq 0$ se numeşte *divizor al lui 0* dacă există $g \in A$, $g \neq 0$ astfel încât $f \cdot g = 0$.

Un element $f \in A$, $f \neq 0$ se numeşte *inversabil* sau *unitate* dacă există $g \in A$, $g \neq 0$ astfel încât $f \cdot g = 1$.

Un element nenul, care nu este divizor al lui zero se numeşte *regulat*. Un inel în care nu există divizori ai lui zero se numeşte *domeniu de integritate*.

Evident, elementele inversabile sunt şi regulate. De asemenea este uşor de văzut că într-un inel finit orice element regulat f, este inversabil. Pentru aceasta este suficient să considerăm aplicaţia $\varphi : A \to A$ dată de $\varphi(g) = fg$. Din $fg = fh$ rezultă $f(g-h) = 0$ deci $g - h = 0$, sau $g = h$. Aşadar φ este injectivă, deci şi surjectivă, de unde rezultă că există $b \in A$ astfel ca $f(b) = ab = 1$, ceea ce înseamnă că a este inversabi.

Definim acum conceptul de ideal.

Definiţie 1.1.16. O submulţime nevidă $I \subseteq A$ al inelului A se numeşte *ideal* dacă are proprietăţile

(1) Dacă $f, g \in I$ atunci $f - g \in I$.

(2) Dacă $f \in I$ şi $h \in A$, atunci $hf \in I$.

O primă observaţie imediată este faptul că în definiţie în locul condiţiei $f - g \in I$, se poate lua echivalent condiţia $f + g \in I$. De asemenea, se vede că elementul 0 face parte din orice ideal.

O dată cu definirea unui concept se pune automat problema caracterizării obiectelor pe care aceast concept le descrie. Altfel spus, este natural să dăm exemple caracteristice de ideale. Să menţionăm totuşi, că această abordare, deşi tipică pentru orice prezentare, ascunde ideile care au dus la cristalizarea treptată a conceptului respectiv, şi nici măcar nu se referă în mod necesar la contextul original care a generat această cristalizare. În cazul de faţă pentru conceptul de ideal rolul determinant a avut efortul de a demonstra marea teoremă a lui Fermat, însă detaliile acestei istorii ne-ar duce prea departe de ideile pe care le urmărim aici.

Revenind la exemple carecteristice de ideale, dăm următoarea propoziţie.

Propoziţie 1.1.17. *Fie A un inel şi $f_1, f_2, \ldots, f_m \in A$. Atunci mulţimea*

$$< f_1, f_2, \ldots, f_m >= \{g_1 f_1 + g_2 f_2 + \cdots + g_m f_m | \, g_i \in A, i = 1, \ldots, m\}$$

este ideal în inelul A.

Acest ideal se numeşte *idealul generat* de elementele $f_1, f_2, \ldots, f_m$. De asemenea dacă $I =< f_1, f_2, \ldots, f_m >$, atunci spunem că elementele $f_1, f_2, \ldots, f_m$ formează o *bază* pentru I. În acest caz idealul I se numeşte *finit generat*.

Evident un ideal finit generat are mai multe baze. Dintre bazele unui ideal aşa numitele baze Gröbner au proprietăţi speciale, despre care va fi vorba în secţiunile care urmează.

Definiţie 1.1.18. Un ideal de forma $I =< f >$ se numeşte *ideal principal*. Un inel în care orice ideal este principal se numeşte *inel principal*.

Exemple de inele principale sunt date în următoarea propoziţie:

Propoziţie 1.1.19. *Inelul* $\mathbf{Z}$ *al întregilor şi inelul polinoamelor de o nedeterminată cu coeficienţi într-un corp sunt inele principale.*

Demonstraţie. Fie I un ideal în $\mathbf{Z}$. Dacă $I = \{0\}$, atunci $I = 0 \cdot \mathbf{Z} =< 0 >$ şi suntem gata. Dacă $I \neq \{0\}$, atunci I conţine atât numere pozitive cât şi negative, deoarece odată cu un număr din I şi opusul acestuia (multiplul cu -1) este în I. Fie n cel mai mic număr întreg strict pozitiv din I. Atunci este clar că $n \cdot \mathbf{Z} \subseteq I$. Invers, fie $x \in I$ arbitrar. Pe baza teoremei fundamentale a aritmeticii, există un cât q şi un rest r unic astfel ca

$$x = n \cdot q + r, \qquad 0 \leq r < n.$$

Din egalitatea $r = x - n \cdot q$ se citeşte că $r \in I$, ceea ce nu e posibil – conform alegerii lui n – decât dacă $r = 0$. Astfel $x \in n \cdot \mathbf{Z}$, deci $I \subseteq n \cdot \mathbf{Z}$. Rezultă deci că $I = n \cdot \mathbf{Z}$.

Pentru inelul polinoamelor cu coeficienţi într-un corp demonstraţia este identică în esenţă. Diferenţa constă în faptul că se compară gradele polinoamelor, şi se foloseşte teorema împărţirii întregi a polinoamelor, care asigură – ca şi în cazul numerelor întregi – existenţa şi unicitatea câtului şi restului împărţirii. □

Această propoziţie este importantă mai ales prin consecinţa ei dată în propoziţia 1.1.23 de la pagina 27. Pentru pregătirea enunţului acesteia trebuie să definim conceptul abstract de cel mai mare divizor comun.

Definiţie 1.1.20. Fie A un domeniu de integritate, şi $a, b \in A$. Spunem că elementul a îl *divide* pe b, sau că a este un *divizor* al lui b, (notat $a|b$), dacă există un element $c \in A$ astfel ca $a \cdot c = b$.

Spunem că elementele a şi b sunt *asociate în divizibilitate* dacă se divid reciproc, adică $a|b$ şi $b|a$.

Relaţia de divizibilitate este evident reflexivă şi tranzitivă. De asemenea, se vede imediat, că elementele a şi b sunt asociate dacă şi numai dacă $a = bu$, unde u este un element inversabil. Într-adevăr, dacă u este inversabil atunci există v astfel ca $uv = 1$, deci $av = b$, prin urmare a şi b se divid reciproc. Invers, dacă a şi b se divid reciproc, adică $a = bu$ şi $av = b$, atunci $a = avu$, deci $a - avu = 0$, adică $a(1 - vu) = 0$, de unde rezultă că $1 - vu = 0$, sau $uv = 1$, deci u este inversabil.

Definiţie 1.1.21. Fie A un domeniu de integritate, şi $a, b \in A$. Un element $d \in A$ se numeşte *cel mai mare divizor comun* al elementelor a şi b, şi se notează $d = (a, b)$, dacă

(i) $d|a$ şi $d|b$, adică d este divizor comun, şi

(ii) dacă $d'|a$ şi $d'|b$, atunci $d'|d$, adică d este cel mai mare divizor, în sensul relaţiei de divizibilitate.

Să observăm, că cel mai mare divizor comun a două elemente nu este unic. Mai precis, dacă d_1 şi d_2 este fiecare cel mai mare divizor comun al elementelor a şi b, atunci d_1 şi d_2 sunt elemente asociate, deoarece din definiţia celui mai mare divizor comun 1.1.21(ii) rezultă imediat, că d_1 şi d_2 se divid reciproc. Expresia $d = (a, b)$ conţine aşadar un uşor abuz de notaţie.

În inele principale cel mai mare divizor comun a două elemente are o caracterizare aparte, exprimată cu ajutorul idealelor. Vom da această caracterizare în inelul întregilor.

Să facem mai întâi o observaţie.

Observaţie 1.1.22. Într-un domeniu de integritate

$$< d >=< d' >,$$

dacă şi numai dacă elementele d şi d' sunt asociate.

Demonstraţie. Într-adevăr, din $< d >=< d' >$, sau $d \cdot A = d' \cdot A$ rezultă că $d = d \cdot 1 \in d' \cdot A$ şi $d' = d' \cdot 1 \in d \cdot A$, adică $d = d'u$ şi $d' = dv$, deci elementele d şi d' se divid reciproc. Invers, dacă $d|d'$, sau $du = d'$ atunci $d' \cdot A \subseteq d \cdot A$, deci $< d' > \subseteq < d >$. Similar, dacă $d'|d$ atunci $< d > \subseteq < d' >$. Aşadar dacă d şi d' sunt asociate, atunci $< d >=< d' >$. □

Iată şi caracterizarea celui mai mare divizor comun în domenii de integritate (aici $\mathbf{Z}$).

Propoziţie 1.1.23. *Fie $a, b, d \in \mathbf{Z}$ trei numere întregi. Numărul d este cel mai mare divizor comun al numerelor a şi b, $d = (a, b)$, dacă şi numai dacă*

$$d \cdot \mathbf{Z} = a \cdot \mathbf{Z} + b \cdot \mathbf{Z}.$$

În altă exprimare, dacă $d = (a, b)$, atunci există două numere întregi $x, y \in \mathbf{Z}$ astfel ca $d = ax + by$, şi invers, dacă $d = ax + by$, şi d este un divizor comun al lui a şi b, atunci el este un cel mai mare divizor, $d = (a, b)$.

În particular, numerele a şi b sunt relativ prime exact atunci când 1 are o reprezentare de forma $1 = ax + by$, unde x, y sunt numere întregi potrivite.