Domenii Euclidiene

In algebra abstracta, un domeniu euclidian (de asemenea numit inel euclidian) este un tip de inel in care are loc teorema impartirii cu rest.

Definitie

Un domeniu euclidian este un tip particular de domeniu de integritate D, in care putem defini o functie v care duce elementele nenule ale lui D in multimea numerelor naturale nenule, astfel incit urmatoarea proprietate (numita teorema impartirii cu rest) are loc:

- Daca a si b sunt elemente ale lui D si b este nenul, atunci exista q si r in D, astfel incit $a = bq + r$ si fie $r = 0$, fie $v(r) < v(b)$.

Functia v se numeste norma.

In toate cartile de algebra in care se studiaza domeniile euclidiene, intilnim inca o proprietate in definitia unui domeniu euclidian, si anume:

- Pentru orice elemente nenule a,b din D, avem $v(a) \leq v(ab)$.

Aceasta proprietate se poate insa demonstra intr-un domeniu euclidian, de aceea nu o vom include in definitia data.

Intr-adevar, daca (D,v) este un domeniu euclidian, conform definitiei data anterior, atunci putem defini functia w, definite pe multimea elementelor nenule ale lui D, astfel:

$w(a) = \min\{ v(ax) : x \text{ parcurge elementele nenule ale lui } D\}$.

Atunci (D,w) este un domeniu euclidian conform definitiei de mai sus si, in plus, satisface conditia : $w(a) \leq w(ab)$ pentru toate elementele nenule a si b din D.

Pentru a verifica faptul ca w este o norma, presupunem ca b nu divide pe a si intre expresiile de forma $a = bq + r$, o alegm pe cea pentru care v(r) este minim. Daca $w(r) \geq w(b)$, atunci exista un c, pentru care $v(r) \geq v(bc)$. Putem scrie $a = bcQ + R$ cu $v(R) < v(bc) \leq v(r)$, care contrazice minimalitatea lui v(r).

Exemple de domenii euclidiene:

- Inelul intregilor Z este euclidian, in raport cu functia modul.
- Inelul intregilor lui Gauss Z[i] este euclidian, in raport cu urmatoarea functie norma: $v(a+bi) = a^2+b^2$.
- Inelul intregilor lui Eisenstein $Z[\omega]$ (unde ω este radacina cubica a lui 1) este inel euclidian. Definim $v(a+b\omega) = a^2-ab+b^2$.
- Inelul polinoamelor K[X] peste un corp comutativ K este euclidian. Pentru orice polinom nenul f, definim v(f) ca fiind gradul lui f.

- Inelul seriilor formale K[[X]] peste un corp comutativ K este euclidian. Pentru orice serie formala nenula f, definim v(f) ca fiind gradul celei mai mici puteri a lui X, care apare in scrierea lui f.
- Orice corp comutativ este euclidian. Definim v(x) = 1 pentru orice x nenul.

Exemplele de iele de polinoame si de serii de puteri intr-o variabila sunt un motiv pentru a considera functia norma v nedefinita in 0.

Proprietati

Urmatoarele proprietati ale domeniilor euclidiene nu necesita $v(a) \leq v(ab)$:

- Algoritmul lui Euclid are loc (de aici provine si numele de domeniu euclidian).
- Orice domeniu euclidian este un domeniu cu ideale principale.

  Intr-adevar, daca I este un ideal nenul al domeniului Euclidian D si a este astfel incit v(a) este minim pentru toate elementele nenule ale lui I, atunci I = aD.

- Idealele principale generate de elemente a caror norma are valoarea minima coincide cu intregul inelul. Cu alte cuvinte, aceste elemente sunt inversabile (numite si unitati). (Daca are loc inegalitatea $v(a) \leq v(ab)$ atunci toate elementele invesabile au norma minima.)

- Orice element nenul si neinversabil este produs de elemente ireductibile. Aceasta rezulta din rezultatul corespunzator pentru domenii cu ideale principale (sau domenii noetheriene).

Reciproc, nu orice DIP este euclidian, desi exemple nu sunt usor de gasit. Pentru d = -19, -43, -67, -163, inelele $Q(\sqrt{d})$ sunt DIP, dar nu sunt euclidiene, dar in cazurile d = -1, -2, -3, -7, -11 sunt euclidiene.

Domenii cu ideale principale

Definitie

Un domeniu cu ideale principale, notat si DIP este un domeniu de integritate in care orice ideal este principal, adica este generat de un singur element.

Domeniile cu ideale principale sunt obiecte matematice care se comporta in mare masura ca intregii, relative la divizibilitate: orice element dintr-un DIP are o descompunere unica in elemente prime (astfel, are loc o teorema analoaga teoremei fundamentale a aritmeticii); orice doua elemente dintr-un DIP au un cel mai mare divisor comun.

Un domeniu cu ideale principale este un tip particular de domeniu de integritate.

Exemple

- K:orice corp comutativ,
- Z: inelul intregilor,
- K[X]: inelul polinoamelor intr-o variabila cu coeficienti intr-un corp comutativ K.
- Z[i]: inelul intregilor lui Gauss
- Z[ω] (unde este o radacina cubica a unitatii): inelul intregilor lui Eisenstein.

Exemple de domenii de integritate care nu sunt DIP::

- Z[X]: inelul polinoamelor cu coeficienti intregi.

Nu este principal, deoarece idealul generat de 2 si de X este un exemplu de ideal care nu este generat de un singur polinom.

- K[X,Y]: Idealul (X,Y) nu este principal.

Domeniile cu ideale principale sunt importante datorita teoremei de structura a modulelor finit generate peste domenii cu ideale principale:

Daca R este un domeniu cu ideale principale si M este un R-modul finit generat, atunci o multime de generatori minimala pentru M are proprietati similare unei baze pentru un spatiu vectorial finit generat (peste un corp comutativ).

Sa remarcam insa ca pentru module, pot exista elementele nenule r si m din R si respectiv M, astfel incit $r.m = 0$.

Daca M este un modul liber peste un domeniu cu ideale principale R, atunci orice submodul al lui M este liber. Aceasta nu are loc pentru orice tip de module. De exemplu submodulul (2, X) al lui Z[X] nu este liber peste Z[X].

Proprietati

Intr-un domeniu cu ideale principale, orice doua elemente a,b au un cel mai mare divizor comun , care poate fi obtinut ca generator al idealului (a,b).

Toate domeniile euclidiene sunt DIP, dar reciproca nu este adevarata. Un exemplu de DIP, care nu este domeniu euclidian este $Z[(1+\sqrt{-19})/2]$.

Orice DIP este DFU. Reciproca nu este adevarata, deoarece pentru orice corp K, K[X,Y] este DFU, dar nu este DIP (pentru a arata aceasta, consideram idealul (X,Y). Acesta nu

este intreg inelul, deoarece nu contine polinoame de grad 0 si si nu este generat de un singur element.)

Alte proprietati:

1. Orice domeniu cu ideale principale este noetherian.

2. In toate inelele, idealele maximale sunt prime. Reciproca nu este adevarata. Insa, intr-un DIP, orice ideal prim nenul este maximal.

3. Toate DIP sunt domenii de integritate inchise.

Cele trei afirmatii anterioare definesc un domeniu dedekindian, si deci orice DIP este un domeniu dedekindian.

Pe de alta parte, orice DFU, care este un domeniu dedekindian este de asemenea DIP.

In concluzie, un clasa tuturor DFU, care sunt dedekindiene coincide cu clasa tuturor DIP.

Domenii factoriale

Intuitiv, un domeniu cu factorizare unica (DFU) este un domeniu de integritate in care orice element, cu anumite exceptii, poate fi scris in mod unic ca produs de elemente prime, similar cu teorema fundamentala a aritmeticii pentru numere intregi. Inelele DFU sunt uneori numite inele factoriale, conform terminologiei lui Bourbaki.

Un domeniu factorial este un tip particular de domeniu de integritate.

Definitie

Un domeniu cu factorizare unica este un domeniu de integritate R, in care orice element nenul si neinversabil x poate fi scris ca produs de elemente ireductibile ale lui R:

$x = p_1 p_2 ... p_n$

si aceasa reprezentare este unica in urmatorul sens: daca $q_1,...,q_m$ sunt elemente ireductibile ale lui R, astfel incit

$x = q_1 q_2 ... q_m$,

atunci m = n si exista o bijectie $\varphi : \{1,...,n\} \rightarrow \{1,...,m\}$ astfel incit p_i este asociat cu $q_{\varphi(i)}$ pentru i = 1, ..., n.

Unicitatea este uneori greu de verificat, de aceea urmatoarea definitie echivalenta este utila: un domeniu cu factorizare unica este un domeniu de integritate in care orice element nenul si neinversabil poate fi scris ca produs de elemente prime.

Exemple

Majoritatea inelelor din matematica elementara sunt DFU.

• Toate domeniile cu ideale principale, deci si domeniile euclidiene sunt DFU. In particular, inlul intregilor (vexi teorema fundamentala a aritmeticii), inelul intregilor lui Gauss, inelul intregilor lui Eisenstein sunt DFU.

• Orice corp comutativ este in mod trivial un DFU, deoarece orice element nenul este inversabil.

• Daca R este DFU, atunci si inelul polinoamelor R[x] cu coeficienti in R este DFU. In particular, inelul polinoamelor cu coeficienti intr-un corp comutativ este DFU.

Alte exemple de DFU:

• Inelul seriilor formale de puteri $K[[X_1,...,X_n]]$ peste un corp comutativ K.

• Prin inductie, se arata ca inelele polinomiale $Z[X_1, ..., X_n]$, $K[X_1, ..., X_n]$ (unde K este un corp comutativ) sunt DFU. (Orice inel polynomial cu mai mult de o variabila este un exemplu de DFU, care nu este un domeniu cu ideale principale.)

Contraexemple:

• Inelul $Z[\sqrt{-5}]$ a tuturor numerelor complexe de forma $a+ib\sqrt{5}$, unde a si b sunt numere intregi. Atunci 6 se descompune in factori astfel $2\cdot 3$, dar si $(1+i\sqrt{5})(1-i\sqrt{5})$. Acestea sunt descompuneri diferite, deoarece singurele elemente inversabile ale inelului sunt 1 si - 1; astfel, elementele 2, 3, $1+i\sqrt{5}$, $1-i\sqrt{5}$ nu sunt asociate. In plus, toti cei patru factori sunt ireductibili.

• Majoritatea inelelor factorale unui inel polynomial nu sunt DFU. Iata un exemplu:

Fie R un inel comutativ. Atunci R[X,Y,Z,W] / (XY - ZW) nu este DFU. Demonstratia consta in doua parti.

I) Mai intii aratam ca $X_1=X+(XY-ZW)$, $Y_1=Y+(XY-ZW)$, $Z_1=Z+(XY-ZW)$ si $W_1=W+(XY-ZW)$ sunt toate ireductibile. Presupunem prin reducere la absurd ca X1 se descompune in doua elemente nenule neinversabile. Deoarece X_1 are gradul 1, un factor $\alpha X_1 + \beta Y_1 + \gamma Z_1 + \delta W_1$ are gradul 1 si celalalt factor r are gradul 0. Obtinem $X_1 = r\alpha X_1 + r\beta Y_1 + r\gamma Z_1 + r\delta W_1$. In R[X,Y,Z,W], elementul $(r\alpha -1)X + r\beta Y + r\gamma Z + r\delta W$ de grad 1 trebuie sa fie un element al idealului (XY-ZW), dar elementele nenule ale acestui ideal au

gradul mai mare sau egal cu 2. In consecinta, $(r\alpha-1)X + r\beta Y + r\gamma Z + r\delta W$ trebuie sa fie 0 in R[X,Y,Z,W]. De aici rezulta ca $r\alpha = 1$, deci r este inversabil, contradictie. Similar, se arata ca Y_1, Z_1 si W_1 sunt ireductibile.

II) Elementul $X_1 Y_1$ coincide cu elementul $Z_1 W_1$ deoarece avem $X_1 Y_1 - Z_1 W_1 = 0$. aceasta inseamna ca $X_1 Y_1$ si $Z_1 W_1$ sunt doua descompuneri diferite ale aceluiasi element in elemente ireducibile, deci R[X,Y,Z,W] / (XY-ZW) nu este DFU^{-}.

Proprietati

Anumite concepte pentru numere intregi pot fi generalizate pentru DFU:

- Intr-un DFU, orice element ireductibil este prim. (In orice domeniu de integritate, orice element prim este ireductibil, dar reciproca nu este mereu adevarata.) Remarcam doar ca orice domeniu noetherian este DFU daca si numai daca orice element ireductibil este prim.

- Orice doua (sau un numar finit de elemente) ale unui DFU au un cel mai mare divizor comun si un cel mai mic multiplu comun. Cel mai mare divizor comun a doua elemente a si b este un element d care divide atit pe a, cit si pe b si astfel incit orice alt divizor comun al lui a si b divide pe d. Toti cei mai mari divizori comuni ai lui a si b sunt asociati. All greatest common divisors of a and b are associated.

- Orice DFU este un domeniu de integritate inchis. Cu alte cuvinte, daca R este DFU cu corpul de fractii K si daca un element k al lui K este redacina unui polinom monic cu coeficienti in R, atunci k este element al lui R.

Conditii echivalente pentru un inel, pentru a fi DFU.

- Un domeniu de integritate este DFU daca si numai daca are loc conditia lanturilor ascendente pentru ideale principale si orice doua elemente au un cel mai mic multiplu comun.

- Daca R este un domeniu de integritate, atunci R este DFU daca si numai daca orice ideal prim nenulal lui R are un element nenul prim. (Kaplansky)

Module

Conceptul de modul peste un inel este o generalizare a notiunii de spatiu liniar, unde corpul comutativ al scalarilor se inlocuieste cu un inel.
Astfel un modul (ca si un spatiu liniar) este in primul rind un grup aditiv abelian; se defineste apoi un produs intre elementele inelului si elementele modulului si au loc anumite proprietati.

Modulele sunt strins legate de teoria reprezentarilor de grupuri. Ele constituie notiuni centrale ale algebrei comutative si algebrei omologice, fiind folosite intens in geometria algebrica si topologia algebrica.

Motivatia

Intr-un spatiu vectorial, multimea scalarilor formeaza un corp comutativ si actioneaza pe vectori prin inmultirea cu scalari.
Intr-un modul, scalarii sunt elementele unui inel, de aceea conceptul de modul reprezinta o generalizare substantiala a conceptului de spatiu liniar. In algebra comutativa, este important ca atit idealele, cit si inelele factor sa fie module, asa incit multe proprietati ale idealelor sau ale inelelor factor pot fi tratate prin intermediul notiunii de modul.
In algebra necomutativa, anumite conditii referitoare la inele pot fi exprimate fie cu ajutorul idealelor stingi sau modulelor stingi.
O mare parte a teoriei modulelor consta in extinderea cit mai mult posibil a unor proprietati ale spatiilor liniare in contextual modulelor peste un anumit tip de inele, de exemplu DIP.
Totusi, modulele sunt mai complicate decit spatiile liniare. Nu toate modulele au baza, si chiar atunci cind au baza, nu au neaparat acelasi numar de elemente in baza, spre deosebire de spatiile liniare, pentru care toate bazele unui spatiu liniar au acelasi cardinal.

Definitie

Un R-modul sting peste un inel R consta dintr-un grup abelian (M, +) si o operatie externa $R \times M \rightarrow M$ (numita inmultire cu scalari si notata de obicei prin juxtapunere, adica rx pentru r din R si x din M) astfel incit
Pentru orice r, s din R, x, y din M, avem

1. $r(x+y) = rx+ry$
2. $(r+s)x = rx+sx$
3. $(rs)x = r(sx)$
4. $1x = x$

Daca notam actiunea scalara astfel: $fr(x) = rx$ si cu f funtia care asociaza fiecarui r pe fr, atunci prima axioma afirma ca fr este un morfism de grupuri al lui M, iar celelalte trei axiome afirma ca f este un morfism de inele de la inelul R la inelul endomorfismelor End(M). Astfel un modul este actiunea unui inel pe un grup abelian.
Un R-modul la dreapta M se defineste similar, doar ca inelul actioneaza la dreapta, adica. Avem o inmultire cu scalari de forma $M \times R \rightarrow M$, iar axiomele de mai sus sunt scrise cu scalari r si s la dreapta lui x si y.
Atunci cind inelele nu sunt unitare, se omite conditia 4 din definitia unui R-modul. De aceea, structurile mai sus definite se numesc R-module la stinga unitare. In cele ce urmeaza, vom considera doar inele si module unitare.

Un bimodul este un modul atit la stinga, cit si la dreapta, astfel incit cele doua inmultiri sunt compatibile. Daca R este comutativ, atunci R-modulele la stinga coincide cu R-modulele la dreapta si le numim simplu R-module.

Exemple

- Daca K este un corp comutativ, atuci conceptele de K-spatiu vectorial si K-modul coincid.
- Conceptul de Z-modul coincide cu notiunea de grup abelian. Cu alte cuvinte, orice grup abelian este un modul peste inelul intregilor Z. Pentru $n > 0$, avem $nx = x + x + ... + x$ (de n ori), $0x = 0$ si $(-n)x = -(nx)$. Astfel de module nu au baza (grupurile care contin elemente de torsiune nu au baza). (Totusi, un corp comutativ finit, cosiderat ca modul peste el insusi , are baza).
- Daca R este un inel arbitrar si n este un numar natural, atunci produsul cartezian $R \times R \times \ldots \times R$ (de n ori) este atit modul la stinga cit si la dreapta peste R, daca definim operatiile pe componente. Pentru $n = 1$, R este un R-modul, unde inmultirea cu scalari este chiar inmultirea din inel. Pentru $n = 0$ obtinem R-modulul trivial $\{0\}$. Modulele de acest tip sunt libere si numarul n este rangul modulului liber.
- Daca S este o multime nevida, M este un R-modul la stinga si MS este multimea tuturor functiilor $f : S \to M$, atunci adunarea si inmultirea cu scalari din MS definite prin $(f + g)(s) = f(s) + g(s)$ si $(rf)(s) = rf(s)$ dau o structura de R-modul sting lui MS. Cazul R-modulelor drepte este analog. In particular, daca R este comutativ atunci multimea morfismelor de R-module $h : M \to N$ este un R-modul.
- Multimea matricelor patratice de tip $n \times n$ cu elemente reale formeaza un inel R, iar spatiul euclidian R^n este un R-modul la stinga peste R daca definim operatia externa ca fiind inmultirea matricelor.
- Daca R este un inel arbitrar si I este un ideal sting al lui R, atunci I este un modul la stinga peste R. Analog, idealele drepte sunt module la dreapta.
- Daca R este un inel, definim inelul op R care are aceeasi multime support si aceeasi adunare, dar inmultirea este definite astfel: daca $ab = c$ in R, atunci $ba = c$ in op R. Orice R-modul la stinga M poate fi vazut ca un modul drept peste op R, si orice modul la dreapta peste R poate fi considerat un modul la stinga peste op R.

Submodule si homomorfisme

Fie M un R-modul sting si N un subgroup al lui M. Spunem ca N este un submodul (sau un R-submodul)daca, pentru orice n din N si orice r din R, produsul rn este in N (sau nr pentru un modul drept).
Multimea submodulelor unui modul dat M, impreuna cu cele doua operatii binare + and $\cap$, formeaza o lattice modulara, adica: date submodulele U, N_1, N_2 ale lui M, astfel incit $N_1 \leq N_2$, atunci: $(N_1 + U) \cap N_2 = N_1 + (U \cap N_2)$.

Daca M si N sunt R-module stingi, atunci functia $f : M \to N$ este un morfism de R-module daca, pentru orice m, n din M si r, s din R, avem

$$f(rm + sn) = rf(m) + sf(n).$$

Un morfism bijectiv de module se numeste izomorfism de module si cele doua module se numesc izomorfe. Nu vom face distinctie intre module izomorfe, pentru ca ele se comporta la fel in studiul proprietatilor algebrice.

Nucleul unui morfism de module $f : M \to N$ este un submodul al lui M, ce contine toate elementele a caror imagine prin f este 0.
Teoremele de izomorfism de la grupuri sau de la spatii liniare sunt valabile si pentru R-module.
R-modulele stingi, impreuna cu morfismele lor de module formeaza o categorie, notata R-Mod si care este o categorie abeliana.

Tipuri de module

Finit generat. Un modul M este finit generat daca exista un numar finit de elemente x1,...,xn in M, astfel incit orice element al lui M este o combinatie liniara a acelor elemente, cu coeficienti din inelul scalarilor R.

Modul ciclic. Un modul se numeste modul ciclic daca este generat de un singur element.

Liber. Un modul liber este un modul care are o baza, sau echivalent, care este izomorf cu o suma directa de copii ale inelului de scalari R. Aceste module sunt foarte similare spatiilor liniare.

Proiectiv. Modulele proiective sunt sumanti directi ai unor module libere.

Injectiv. Module injective sunt definite ca fiind dualele modulelor proiective.

Simplu. Un modul simplu S este un modul nenul si ale carui unice submodule sunt {0} si S. Modulele simple sunt uneori numite ireductibile.

Indecomposabil. Un modul indecompozabil este un modul nenul care nu poate fi scris ca o suma directa de submodule nenule. Orice modul simplu este indecompozabil..

Fidel. Un modul fidel M este unul pentru care actiunea fiecarui $r \neq 0$ din R pe M este netriviala (adica $rx \neq 0$ pentru un x din M). Echivalent, anihilatorul lui M este idealul nul.

Noetherian. Un modul noetherian este un modul, pentru care orice submodul este finit generat. Echivalent, orice lant crescator de submodule devine stationar dupa un numar finit de pasi.

Artinian. Un modul artinian este un modul in careorice lant descrescator de submodule devine stationar dupa un numar finit de pasi.