Inele euclidiene

Prof Șerban Simona Marinela

Definitie: Un inel integru A impreuna cu o functie f: A-{0}$\rightarrow$N se numeste **inel euclidian** daca are urmatoarele doua proprietati:

1. Oricare ar fi elementele nenule a,b$\in$A , astfel incit a sa divida pe b , rezulta f(a)$\leq$ f(b).
2. Pentru oricare a,b $\in$A , b$\neq$0 exista q,r$\in$A , a.i. a=bq+r, unde r=0 sau f(r)<f(b).

Proprietatea 2 se numeste **teorema impartirii cu rest** in inelul euclidian.

Exemple:

1) Inelul (Z,+,$\bullet$) este euclidian. Intr-adevar , in acest inel are loc teorema impartirii cu rest pentru numere intregi , si anume:
   $\forall$ a,b$\in$Z , b$\neq$0 , $\exists$ q,r$\in$Z a.i. a=bq+r . unde 0$\leq$ r ,| b| .
   Mai mult q si r sunt unice.
   Considerind functia f: Z-{0}$\rightarrow$N, f(n)=| n |, rezulta clar ca inelul Z impreuna cu f este euclidian (satisface conditiile 1 si 2). Mentionam ca teorema impartirii cu rest la numere intregi o vom demonstra in paragraful 1 al capitolului III.
2) Orice corp este inel euclidian. Intr-adevar, daca K este un corp, consideram functia f : K-{0}$\rightarrow$N definita prin f(a)=1, $\forall$a$\in$K ,a$\neq$0 . Aceasta functie satisface 1 si 2.
3) Inelul K[x] al polinoamelor cu coeficienti intr-un corp K pentru care functia f :K[x] -{0}$\rightarrow$N, definita prin f(g)=grad(g), $\forall$ g$\in$K[x] , g$\neq$0 , este un inel euclidian.
   Intr-adevar, daca g,h $\in$K[x], g$\neq$0 si g/h, atunci h=gg', cu g'$\in$K[x], deci grad(g) $\leq$ grad(h), adica f(g)$\leq$ f(h). Deci conditia 1 este indeplinita.
   Sa verificam proprietatea 2. Fie f,g$\in$K[x] cu g$\neq$0. Daca grad(g)=0, atunci f=g(g f), deoarece g$\neq$0 din K, deci inversabil si afirmatia este dovedita, adica este verificata proprietatea 2. Daca grad(g)>0, atunci vom face o inductie dupa gradul lui f. Daca grad(f)<grad(g), in particular, pentru grad(f)=0, din relatia f=g$\bullet$0+f, rezulta 2.
   Presupunem ca 2 afost verificata pentru toate polinoamele f, cu grad(f)<n. Fie atunci f un polinom de grad n, $f = a_0x^n + a_1x^{n-1}+...+a_n$, $a_0 \neq 0$ si g un polinom de gradul m, $g = b_0x^m + b_1x^{m-1}+...+b_m$, $b_0 \neq 0$. Putem presupune ca m$\leq$ n , conform celor demonstrate mai sus. Atunci, polinomul $f_1 = f - a_0b_0^{-1}x^{n-m}g$ are gradul cel mult n-1, deoarece termenii de gradul cel mai mare se reduc , deci grad(f1)<grad(f). Din ipoteza inductiva rezulta, atunci ca exista q,r$\in$K[x] a.i. f1=gq+r, unde r=0 sau grad(r)<grad(g). Atunci avem: $f = g(a_0b^{-1}{}_0x^{n-m} + q) + r$ *si polinoamele* $a_0b_0^{-1}x^{n-m} + q$ *si* r satisfac proprietatea 2. Polinoamele q si r $\in$K[x] , numite **citul** si **restul** , astfel incit f=qg+r, r=0 sau grad(r)<grad(g); In cazul inelului K[x] sunt chiar unice (ca si la Z , de altfel). Dar unicitatea acestora nu este necesara in formula de impartire cu rest , in cazul inelului euclidian.
4) Inelul intregilor lui Gauss este euclidian, in care functia din definitie este norma N. Definim pe Z[i] functia f :Z[i] $\rightarrow$N, f(m+ni)=m +n (f(m+ni) este patratul modulului numarului complex m+ni). Numarului complex z=a+bi, a,b$\in$R, i se asociaza in plan punctul M de coordonate (a,b). Numerele complexe din multimea Z[i] sunt reprezentate in plan prin puncte ale caror coordonate sunt numere intregi.
   Reprezentindu-le , obtinem o retea in plan ca in figura 1. Consideram z,z'$\in$Z[i] , z'$\neq$0 si fie M punctul din plan asociat numarului comlex z/z' . In retea exista un patrat ABCD in care se afla punctul M. Fie A virful cel mai apropiat de M. Daca A(a,b) , atunci a,b$\in$Z si A este asociat numarului complex q=a+ib.

Pe de alta parte , cum latura patratului ABCD este unitate si cum A a fost ales cel mai apropiat de M , obtinem ca distanta MA este mai mica decit jumatate din diagonala patratului. Deci MA≤ $\sqrt{2}$ /2<1, dar MA este egal cu modulul numarului complex z/z'-q. Deci avem: | z/z'-q|≤ 1.
Avem, atunci, |z-qz'|<|z'| si , notind r=z-qz', avem | r |<| z'| sau | r |<| z'| si , deci, f(r)<f(z'). In concluzie, avem z=qz'+r, cu f(r)<f(z') si, deci, Z[i] este inel euclidian. Din aceasta demonstratie rezulta ca restul si citul impartirii nu sunt unic determinate.

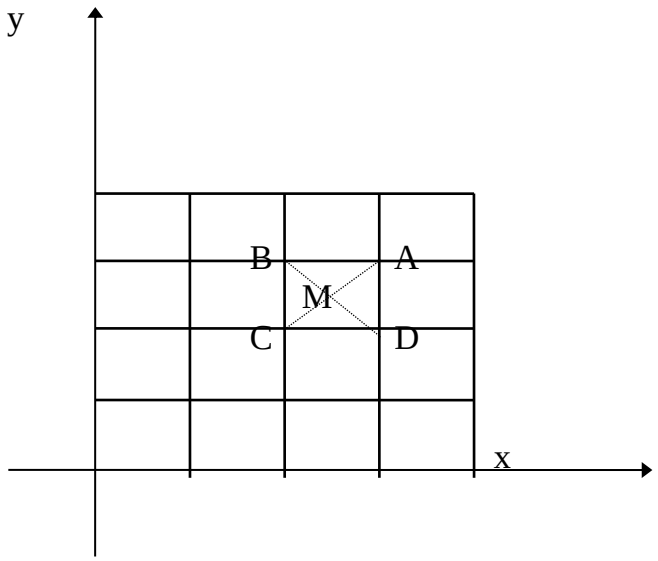
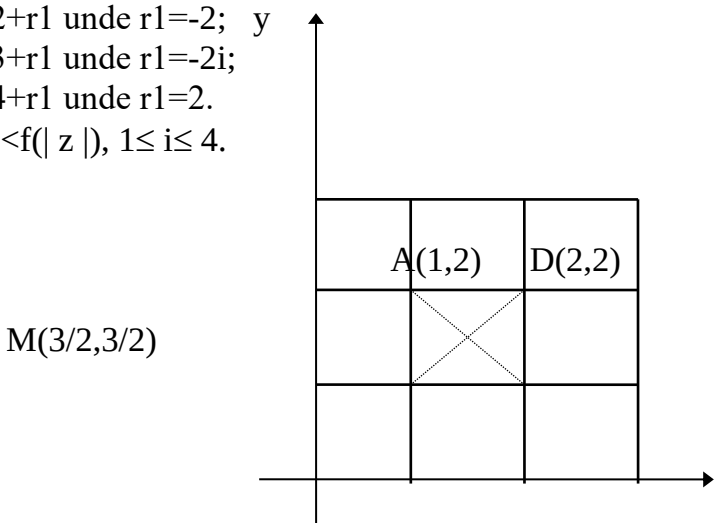


Fig.1.

Intr-adevar, daca M este centrul patratului ABCD, atunci putem alege citul q al impartirii in egelitatea de mai sus , numarul complex q=a+ib, cu a,b∈Z pentru care (a,b) sa fie coordonatele oricaruia din virfurile patratului ABCD.

Sa exemplificam pe un caz numeric ; consideram in Z[i] numerele z=6i si z'=2+2i, pentru care z/z'=6i/(2+2i)=3/2+3i/2.
In figura 2 , punctul M , care este reprezentarea geometrica a numarului comlex z/z'=3/2+3i/2, cade in centrul patrtului ABCD.
Deci putem alege citurile q1=1+i sau q2=2+i sau q3=2+2i sau q4=1+2i.
Avem egalitatile: z=z'q1+r1 unde r1=2i;
z=z'q2+r1 unde r1=-2;
z=z'q3+r1 unde r1=-2i;
z=z'q4+r1 unde r1=2.
In cele 4 cazuri , avem f(ri)<f(| z |), 1≤ i≤ 4.



Propozitia 3.1. Intr-un inel euclidian orice 2 elemente au un cmmdc si un cmmmc .

Demonstratie:

Fie A un inel euclidian si a,b doua elemente din A. Daca unul dintre acestea este nul, atunci celalalt este cmmdc al lor. Putem presupune a,b≠0. In acest caz , pentru a demonstra

propozitia , vom aplica succesiv teorema impartirii cu rest, ceea ce constituie **algoritmul lui Euclid**.

Aplicam teorema impartirii cu rest elementelor a si b si obtinem :

1. $a=bq1+r$, unde $r1=0$ sau $f(r1)<f(b)$;

Daca $r1\neq0$ exista elementele $q2,r2\in A$ a.i.

2. $b=r1q2+r2$, cu $r2=0$ sau $f(r2)<f(r1)$.

Daca $r2\neq0$, aplicam teorema impartirii cu rest elementelor r1 si r2 . Exista elementele $q3,r2\in A$ a.i.:

3. $r1=r2q3+r3$, cu $r3=0$ sau $f(r3)<f(r2)$

Repetind acest procedeu , obtinem elementele q4,q5,…,qn,… si r4,r5,…,rn,…, astfel incit:

4. $r2=r3q4+r4$, cu $r4=0$ sau $f(r4)<f(r3)$;

……..

$r_{n-2}=r_{n-1}q_n+r_n$ cu $r_n=0$ sau $f(r_n)<f(r_{n-1})$;

$r_{n-2}=r_{n-1}q_n+r_{n+1}$ cu $r_{n+1}=0$ sau $f(r_n)<f(r_{n+1})$.

Deoarece sirul $f(r1)>f(r2)>\ldots>f(r_n)>f(r_{n+1})>\ldots$ este un sir descrescator de numere naturale, dupa un numar finit de pasi obtinem neaparat un rest nul , adica exista un numar natural/n a.i. $r_n\neq0$ si $r_{n+1}\neq0$.

Vom arata ca r_n este cmmdc al lui a si b. Cum $r_{n-1}=r_nq_{n+1}\Rightarrow r_n/r_{n-1}$.

Deoarece $r_{n-2}=r_{n-1}q_n+r_n\Rightarrow r_n/r_{n-2}$.In continuare , folosind egelitatea $r_{n-3}=r_{n-2}q_{n-1}+r_{n-1}$ si tinind cont ca r_n/r_{n-1} si r_n/r_{n-2}, rezulta r_n/r_{n-3}.Din aproape in aproape tinind cont de egalitatea 4 , rezulta ca r_n divide elementele r_{n-1}, r_{n-2}, …, r_2,…. Din egalitatea 3 rezulta ca r_n/r_1 si din egalitatea 2 rezulta r_n/a. Deci rn este un divizor comun al elementelor a si b. Din 1 obtinem $r1=a-bq1$ si deci d'/r1. Din 2 obtinem $r2=b-r1q2$. Cum d'/r1 si d'/b $\Rightarrow$ d'/r2 . Din egalitatea 3 obtinem $r3=r1-r2q3$ si deci d'/r3. Acum folosim egalitatea 4 . Din aproape in aproape rezulta ca d' divide elementele r4,r5,…, r_{n-1},r_n. Asadar r_n (ultimul rest nenul) este cmmdc al elementelor a si b. Sirul de egalitati 1,2,3,4,…, $n\neq0$ poarta numele de **algoritmul lui Euclid**. Acest sir de egalitati ne permite sa determinam pentru un inel euclidian un cmmdc a doua elemente. De asemene, cmmdc este unic determinat , abstractie facind de o asociere in divizibilitate , asa cum se demonstreaza prin propozitia 3.1. din acest capitol.

Din propozitia 3.5 , cap.I , rezulta ca orice doua elemente au cmmdc.

Din propozitia precedenta, rezulta:

Corolarul 3.2. Intr-un inel euclidian orice element ireductibil este prim.

Exemplu: In inelul Z[i] , fie a=16+6i si b=7+3i .

Sa calculam cmmdc al lor.

16+6i=(7+3i)(2-i)+(-1+7i), f(-1+7i)<f(7+3i), 50<28.

7+3i=(-1+7i)(1-i)+(1-5i), f(1-5i)<f(-1+7i), 26<50;

-1+7i=(1-5i)(-1+0i)+2I, f(2i)<f(1-5i), 4<26.

1-5i=(-2-i)2I+(-1-i), 2I=(-1-i)(-1-i), f(-1-i)<f(2i), 2<4.

Cmmdc al numerelor 16+6i si 7+3i este -1+i.