CURS 7

Elemente ireductibile şi elemente prime

Noţiunea de număr prim se poate defini prin oricare dintre proprietăţile: Fie $p \in \mathbb{Z}^*$, $p \neq \pm 1$.

i) p nu are divizori diferiţi de ± 1 şi $\pm p$.

ii) $a, b \in \mathbb{Z}$; $p \mid ab \Rightarrow p \mid a$ sau $p \mid b$.

Vom vedea că într-un domeniu de integritate $(R, +, \cdot)$ oarecare proprietăţile i) şi ii) ne vor conduce la două noţiuni diferite.

În cele ce urmează considerăm $(R, +, \cdot)$ domeniu de integritate.

Definiţia 1. Un element $p \in R^*$ se numeşte **element ireductibil** dacă verifică condiţiile:

1) p nu este inversabil.

2) p nu are divizori proprii, adică

$$x \in R,\ x \mid p \Rightarrow x \text{ inversabil sau } x \sim p.$$

Un element neinversabil din R^* care nu este ireductibil se numeşte **element reductibil**.

Observaţiile 2. a) Un element $p \in R^*$ este ireductibil dacă şi numai dacă verifică condiţia 1) din definiţia de mai sus şi oricare dintre condiţiile:

$2'$) $p = xy \Rightarrow x$ inversabil sau y inversabil.

$2''$) $p = xy \Rightarrow x \sim p$ sau $y \sim p$.

$2'''$) $[p]$ este element minimal în $(R/\sim \setminus \{[1]\}, \leq)$.

b) Dacă $p \in R$ este ireductibil, atunci orice element din R asociat cu p este ireductibil.

c) Un element nenul şi neinversabil al lui R este reductibil dacă şi numai dacă poate fi scris ca produsul a două elemente neinversabile (adică admite o descompunere netrivială în factori).

Exemplele 3. a) Elementele ireductibile p din $(\mathbb{Z}, +, \cdot)$ sunt numerele prime şi opusele lor.

b) Un polinom nenul şi neinversabil $f \in R[X]$ cu coeficienţi într-un domeniu de integritate R este reductibil dacă admite o descompunere netrivială în factori, altfel f este ireductibil. Astfel, polinomul $f = 2X + 2 \in \mathbb{Z}[X]$ este reductibil deoarece 2 şi $X + 1$ din descompunerea $f = 2(X + 1)$ sunt ambele elemente neinversabile. Dar vom vedea că polinomul $2X + 2$ din $\mathbb{R}[X]$ este ireductibil.

Exerciţiul 1. Fie K un corp comutativ şi $f \in K[X]$. Să se arate că:

a) dacă $\operatorname{grad} f = 1$ atunci f este ireductibil;

b) dacă $\operatorname{grad} f \in \{2, 3\}$ atunci f este ireductibil dacă şi numai dacă f nu are nici o rădăcină în K;

c) polinoamele ireductibile din $K[X]$ de grad 4 (sau mai mare) nu pot fi, în general, caracterizate ca la b).

Soluţie: Reamintim că polinoamele inversabile din $K[X]$ sunt polinoamele constante nenule, adică polinoamele de grad 0 şi că

$$\operatorname{grad}(gh) = \operatorname{grad} g + \operatorname{grad} h,\ \forall g, h \in K[X]. \tag{1}$$

a) Dacă $\operatorname{grad} f = 1$ atunci f este nenul şi neinversabil, iar dacă $f = gh$, atunci din (1) rezultă $\operatorname{grad} f = 0$ sau $\operatorname{grad} g = 0$, adică f inversabil sau g inversabil. Deci f este ireductibil.

b) Fie $f \in K[X]$ cu $\operatorname{grad} f \in \{2, 3\}$. Evident, f este nenul şi neinversabil. Arătăm că f este reductibil dacă şi numai dacă f are cel puţin o rădăcină în K. Într-adevăr, folosind (1) se deduce

că o descompunere $f = gh$ a lui f este netrivială dacă şi numai dacă $\operatorname{grad} f = 1$ sau $\operatorname{grad} g = 1$, adică sau f sau g are forma $aX + b$, cu $a \neq 0$, ceea ce înseamnă că f are pe $-a^{-1}b \in K$ rădăcină.
c) Polinomul $(X^2 + 1)^2 \in \mathbb{R}[X]$ este reductibil, dar nu are rădăcini reale.

Exerciţiul 2. Să se arate că:
a) Un polinom $f \in \mathbb{C}[X]$ cu coeficienţi complecşi este ireductibil dacă şi numai dacă $\operatorname{grad} f = 1$.
b) Un polinom $f \in \mathbb{R}[X]$ cu coeficienţi reali este ireductibil dacă şi numai dacă $\operatorname{grad} f = 1$ sau f are gradul 2 şi f nu are rădăcini reale.

Soluţie: a) Aceasta rezultă din exerciţiul anterior şi din **Teorema fundamentală a algebrei (d'Alembert-Gauss)**: *Orice polinom de grad mai mare sau egal cu 1 din $\mathbb{C}[X]$ are cel puţin o rădăcină complexă.*
b) Din exerciţiul anterior rezultă că polinoamele de grad 1 şi cele de grad 2 fără rădăcini reale sunt ireductibile în $\mathbb{R}[X]$. Reciproc, arătăm că toate polinoamele de grad cel puţin 1 din $\mathbb{R}[X]$ (adică nenule şi neinversabile) care nu sunt de forma menţionată sunt reductibile. Pentru polinoamele de gradul 2, acest fapt e evident. Eventual, reamintim că dacă a este coeficientul dominant al lui f şi $x_1, x_2 \in \mathbb{R}$ sunt rădăcinile lui f, atunci $f = a(X - x_1)(X - x_2)$.

Rămâne de demonstrat că că dacă $f \in \mathbb{R}[X]$ şi $\operatorname{grad} f \geq 3$ atunci f este reductibil în $\mathbb{R}[X]$. Din $f \in \mathbb{R}[X] \subseteq \mathbb{C}[X]$ rezultă că f are o rădăcină complexă z. Dacă $z \in \mathbb{R}$ atunci $X - z$ divide pe f. Dacă $z \in \mathbb{C} \setminus \mathbb{R}$ atunci şi conjugatul $\overline{z}$ al lui z este rădăcină a lui f. Cum $z \neq \overline{z}$, polinoamele $X - z$ şi $X - \overline{z}$ sunt relativ prime, deci $(X - z)(X - \overline{z}) \in \mathbb{R}[X]$ divide pe f.

Observaţiile 4. i) Polinomul $f = aX^2 + bX + c$ din $\mathbb{R}[X]$ $(a, b, c \in \mathbb{R},\ a \neq 0)$ nu are rădăcini reale dacă şi numai dacă $\Delta = b^2 - 4ac < 0$.
ii) Polinoamele de la b) sunt polinoamele ale căror funcţii polinomiale pot fi recunoscute ca fiind numitorii fracţiilor care apar în sumele prin care exprimăm funcţiile raţionale reale pentru a le putea integra. Acolo se foloseşte, pe lângă forma polinoamelor ireductibile din $\mathbb{R}[X]$ şi existenţa unei desompuneri în factori ireductibili pentru orice polinom din $\mathbb{R}[X]$ de grad cel puţin 1, fapt ce va rezulta din cursurile viitoare.

Exerciţiul 3. Fie $d \in \mathbb{Z} \setminus \{1\}$ un întreg liber de pătrate şi $\delta : \mathbb{Z}[\sqrt{d}] \to \mathbb{N}$, $\delta(z) = |z \cdot \overline{z}|$ funcţia normă. Să se arate că pentru orice $z_1, z_2, z \in \mathbb{Z}[\sqrt{d}]$ sunt adevărate afirmaţiile:
i) dacă $z_1 | z_2$, atunci $\delta(z_1) | \delta(z_2)$;
ii) $z_1 \sim z_2$ dacă şi numai dacă $\delta(z_1) = \delta(z_2)$ şi $z_1 | z_2$;
iii) $\delta(z_1) = \delta(z_2)$ nu implică, în general, $z_1 \sim z_2$;
iv) dacă $\delta(z)$ e număr prim, atunci z este element ireductibil în $\mathbb{Z}[\sqrt{d}]$.

Soluţie: Se foloseşte exerciţiul 2 din cursul 4.
i) Dacă $z_2 = z_1 z$ în $\mathbb{Z}[\sqrt{d}]$ atunci $\delta(z_2) = \delta(z_1)\delta(z)$ în $\mathbb{N}$, prin urmare $\delta(z_1) | \delta(z_2)$.
ii) Din i) şi din antisimetria $|$ în $\mathbb{N}$ rezultă că $z_1 \sim z_2$ dacă şi numai dacă $\delta(z_1) = \delta(z_2)$ (şi, evident, şi $z_1 | z_2$). Reciproc, dacă $z_2 = z_1 z$ $(z \in \mathbb{Z}[\sqrt{d}])$ atunci $\delta(z_2) = \delta(z_1)\delta(z)$. Din $\delta(z_1) = \delta(z_2)$ rezultă că $z_1 = z_2 = 0$ sau $\delta(z) = 1$, adică z e inversabil, prin urmare $z_1 \sim z_2$.
iii) În $\mathbb{Z}[i]$, $\delta(1 + 2i) = \delta(1 - 2i) = 5$, dar $\dfrac{1 + 2i}{1 - 2i} = -\dfrac{3}{5} + \dfrac{4}{5}\, i \notin \mathbb{Z}[i]$.
iv) $\delta(z)$ număr prim, deci diferit de 0 şi 1, implică z nenul şi neinversabil, iar dacă $z = z_1 z_2$ în $\mathbb{Z}[\sqrt{d}]$ atunci $\delta(z) = \delta(z_1)\delta(z_2)$ în $\mathbb{N}$ cu $\delta(z)$ număr prim, prin urmare sau $\delta(z_1) = 1$ sau $\delta(z_2) = 1$.

Observaţia 5. Punctul iii) arată că afirmaţia i) nu e întotdeauna o echivalenţă, iar, după cum va rezulta din punctul 1) b) al exerciţiului următor, nici afirmaţia iv) de mai sus nu este o echivalenţă.

Exerciţiul 4. 1) Să se arate că în $(\mathbb{Z}[i], +, \cdot)$ au loc următoarele:

a) 2, 5 şi 17 nu sunt elemente ireductibile;

b) 3 şi 7 sunt elemente ireductibile;

c) $1+i$ şi $1+2i$ sunt elemente ireductibile.

2) Să se scrie 4 şi $18+36i$ ca produs de elemente ireductibile din $\mathbb{Z}[i]$.

Soluţie: 1) a) Cum $\delta(1+i) = \delta(1-i) = 2 \neq 1$, numărul $2 = (1+i)(1-i)$ este un produs de elementele neinversabile, prin urmare 2 este reductibil în $\mathbb{Z}[i]$. Similar, $5 = (1+2i)(1-2i)$ şi $17 = (1+4i)(1-4i)$ sunt produse de elemente neinversabile.
b) Cum $\delta(3) = 9$ avem 3 neinversabil, iar dacă $z_k = a_k + b_k i \in \mathbb{Z}[i]$, $k = 1, 2$ şi $3 = z_1 z_2$ atunci $9 = \delta(z_1)\delta(z_2)$. Cum $\delta(z_k) = a_k^2 + b_k^2 \in \mathbb{N}$ $(k = 1, 2)$, această egalitate are loc doar în următoarele cazuri:

- $\delta(z_1) = 1$ şi $\delta(z_2) = 9$, caz în care z_1 este inversabil;
- $\delta(z_1) = \delta(z_2) = 3$, caz care nu convine deoarece nu există $a_k, b_k \in \mathbb{Z}$ astfel încât $a_k^2 + b_k^2 = 3$ (dacă $a_k = 0$ atunci $b_k^2 = 3$ şi $b_k \notin \mathbb{Z}$, dacă $|a_k| = 1$ atunci $b_k^2 = 2$ şi, din nou, $b_k \notin \mathbb{Z}$, iar dacă $|a_k| \geq 2$ atunci $b_k^2 < 0$, prin urmare numărul b_k nu e nici măcar real).
- $\delta(z_1) = 9$ şi $\delta(z_2) = 1$, caz în care z_2 este inversabil.

Aşadar, $3 = z_1 z_2$ implică z_1 inversabil sau z_2 inversabil, prin urmare 3 este ireductibil în $\mathbb{Z}[i]$. Analog se arată că 7 este element ireductibil în $\mathbb{Z}[i]$ (recomand ca temă refacerea raţionamentului în acest caz).
c) Numerele $\delta(1+i) = 2$, $\delta(1+2i) = 5$ sunt prime şi se aplică punctul iv) al exerciţiului anterior.
2) $4 = (1+i)^2(1-i)^2 = -(1+i)^4$, $18+36i = 18(1+2i) = (-i)3^2(1+i)^2(1+2i)$ (atragem atenţia că -1 şi $-i$ sunt elemente inversabile în $\mathbb{Z}[i]$, deci prezenţa lor lângă un element ireductibil şi, implicit, în produs, nu ,,afectează" ireductibilitatea factorilor descompunerii).

Definiţia 6. Un element $p \in R^*$ se numeşte **element prim** dacă verifică condiţiile:

$\alpha)$ p este neinversabil.

$\beta)$ $x, y \in R;\ p \mid xy \Rightarrow p \mid x$ sau $p \mid y$.

Observaţiile 7. a) Dacă $p \in R$ este prim, atunci orice element din R asociat cu p este prim.
b) Dacă $p \in R$ este prim şi p divide produsul $x_1 \dots x_n$ de elemente din R, atunci p divide unul dintre factorii $x_1, \dots, x_n$.

Exemplul 8. Elementele prime din $(\mathbb{Z}, +, \cdot)$ sunt numerele (naturale) prime şi opusele lor.

Exerciţiul 5. Să se arate că în $(\mathbb{Z}[i\sqrt{5}], +, \cdot)$ au loc următoarele:

a) $2,\ 3,\ 1+i\sqrt{5},\ 1-i\sqrt{5}$ sunt elemente ireductibile în $\mathbb{Z}[i\sqrt{5}]$;

b) 3 este element ireductibil, dar nu este element prim;

c) 6 şi $2(1+i\sqrt{5})$ nu au un c.m.m.d.c.;

d) 3 şi $1+i\sqrt{5}$ au un c.m.m.d.c.

e) $i\sqrt{5}$ este element prim.

Soluţie: a) Cum $\delta(3) = 9$, 3 nu e inversabil, iar dacă $z_k = a_k + b_k i \in \mathbb{Z}[i\sqrt{5}]$, $k = 1, 2$ şi $3 = z_1 z_2$ atunci $9 = \delta(z_1)\delta(z_2)$. Cum $\delta(z_k) = a_k^2 + 5b_k^2 \in \mathbb{N}$ $(k = 1, 2)$, această egalitate are loc doar în următoarele cazuri:

- $\delta(z_1) = 1$ şi $\delta(z_2) = 9$, caz în care z_1 este inversabil;

- $\delta(z_1) = 9$ şi $\delta(z_2) = 1$, caz în care z_2 este inversabil;
- $\delta(z_1) = \delta(z_2) = 3$, caz care nu convine deoarece nu există $a_k, b_k \in \mathbb{Z}$ astfel încât $a_k^2 + 5b_k^2 = 3$ (dacă $b_k = 0$ atunci $a_k^2 = 3$ şi $a_k \notin \mathbb{Z}$, dacă $|b_k| \geq 1$ atunci $5b_k^2 \geq 5$ şi $a_k \notin \mathbb{R}$).

Aşadar, $3 = z_1 z_2$ implică z_1 inversabil sau z_2 inversabil, prin urmare 3 este ireductibil în $\mathbb{Z}[i\sqrt{5}]$.

Nici $1+i\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$ nu este element inversabil deoarece $\delta(1+i\sqrt{5}) = 6$, iar dacă $1+i\sqrt{5} = z_1 z_2$ cu $z_k = a_k + b_k i \in \mathbb{Z}[i\sqrt{5}]$, $k = 1, 2$, atunci $6 = \delta(z_1)\delta(z_2)$. Cum $\delta(z_k) = a_k^2 + 5b_k^2 \in \mathbb{N}$ $(k = 1, 2)$, această egalitate are loc doar în următoarele cazuri:

- $\delta(z_1) = 1$ şi $\delta(z_2) = 6$, caz în care z_1 este inversabil;
- $\delta(z_1) = 6$ şi $\delta(z_2) = 1$, caz în care z_2 este inversabil;
- $\delta(z_1) = 2,\ \delta(z_2) = 3$, caz care am văzut mai sus că nu convine;
- $\delta(z_1) = 3,\ \delta(z_2) = 2$, caz care am văzut mai sus că nu convine.

Aşadar, $1 + i\sqrt{5} = z_1 z_2$ implică sau z_1 sau z_2 inversabil, deci $1 + i\sqrt{5}$ este ireductibil în $\mathbb{Z}[i\sqrt{5}]$.

Pentru celelalte elemente, ireductibilitatea se demonstrează similar şi o lăsăm temă.

b) Din a) rezultă că 3 este ireductibil în $\mathbb{Z}\left[i\sqrt{5}\right]$. Dar 3 divide pe $6 = \left(1 + i\sqrt{5}\right)\left(1 - i\sqrt{5}\right)$ şi nu divide nici pe $1 + i\sqrt{5}$, nici pe $1 - i\sqrt{5}$ pentru că

$$\delta(3) = 9 \nmid 6 = \delta(1 \pm i\sqrt{5}).$$

Rezultă că 3 nu este element prim în $\mathbb{Z}[i\sqrt{5}]$.

c) Presupunem prin reducere la absurd că $d = a + bi$ $(a, b \in \mathbb{Z})$ ar fi un c.m.m.d.c. al lui 6 şi $2\left(1 + i\sqrt{5}\right)$. Rezultă că $d \,|\, 6$ şi $d \,|\, 2\left(1 + i\sqrt{5}\right)$, ceea ce implică

$$\delta(d) \mid (\delta(6), \delta(2(1 + i\sqrt{5}))) = (36, 4 \cdot 6) = 12.$$

Dar 2 şi $1 + i\sqrt{5}$ sunt divizori comuni pentru 6 şi $2\left(1 + i\sqrt{5}\right)$, prin urmare, ei sunt divizori ai lui d. Ar rezulta că, în $\mathbb{N}$, c.m.m.d.c. $[\delta(2), \delta(1 + i\sqrt{5})]$ divide pe $\delta(d)$, adică

$$[4, 6] = [\delta(2), \delta(1 + i\sqrt{5})] \mid \delta(d),$$

de unde am deduce şi că $12|\delta(d)$. Rezultă că $\delta(d) = 12$ şi de aici deducem că există o scriere

$$12 = a^2 + 5b^2 \text{ cu } a, b \in \mathbb{Z},$$

ceea ce nu este posibil (dacă $|b| \leq 1$ atunci $a \in \mathbb{R} \setminus \mathbb{Q}$, iar dacă $|b| \geq 2$ atunci $a \in \mathbb{C} \setminus \mathbb{Q}$). Am obţinut o contradicţie, şi, astfel, rezultă că nu există un c.m.m.d.c. pentru 6 şi $2\left(1 + i\sqrt{5}\right)$.

d) Cum 3 este element ireductibil, singurii săi divizori sunt (abstracţie făcând de o asociere în divizibilitate) 1 şi 3. Mai mult 3 nu divide pe $1 + i\sqrt{5}$, deci singurul divizor comun pentru 3 şi $1 + i\sqrt{5}$ este 1, care este şi cel mai mare divizor comun al lor.

e) Evident, $i\sqrt{5}$ este nenul şi neinversabil. Fie $z_1, z_2 \in \mathbb{Z}[i\sqrt{5}]$ $(z_k = a_k + b_k i \in \mathbb{Z}[i\sqrt{5}],\ a_k, b_k \in \mathbb{Z},$ $k = 1, 2)$ astfel încât $i\sqrt{5} \mid z_1 z_2$. Cum $5 = \delta(i\sqrt{5}) \mid \delta(z_1)\delta(z_2)$ în $\mathbb{N}$, $5 \mid \delta(z_1)$ sau $5 \mid \delta(z_2)$. Aşadar,

$$\exists k \in \{1, 2\} :\ 5 \mid (a_k^2 + 5b_k^2) \ \ (\text{în } \mathbb{N}).$$

Rezultă că $5 \mid a_k^2$ şi, implicit, $5 \mid a_k$ (atât în $\mathbb{Z}$ cât şi în $\mathbb{Z}[i\sqrt{5}]$). Cum $-(i\sqrt{5})^2 = 5$, se deduce că $i\sqrt{5} \mid a_k$ în $\mathbb{Z}[i\sqrt{5}]$. Evident, $i\sqrt{5} \mid b_k i\sqrt{5}$ (în $\mathbb{Z}[i\sqrt{5}]$). În consecinţă,

$$\exists k \in \{1, 2\} :\ i\sqrt{5} \mid z_k = a_k + b_k i\sqrt{5},$$

ceea ce completează demonstraţia faptului că $i\sqrt{5}$ este prim în $\mathbb{Z}[i\sqrt{5}]$.

Teorema 9. Fie R un domeniu de integritate. Au loc următoarele:
1) Orice element prim din R este ireductibil.
2) Dacă orice două elemente din R au un c.m.m.d.c., atunci orice element ireductibil din R este prim.

Demonstraţie. 1) Presupunem că $p \in R$ este prim şi $p = xy$. Rezultă că $p \mid xy$ şi $x \mid p$, $y \mid p$. Din faptul că p este prim şi $p \mid xy$ rezultă $p \mid x$ sau $p \mid y$. Prin urmare $x \mid p$ şi $p \mid x$ sau $y \mid p$ şi $p \mid y$, adică $p \sim x$ sau $p \sim y$. Deci p este ireductibil.
2) Fie $p \in R$ un element ireductibil şi $x, y \in R$. Dacă $p \mid xy$ şi p nu divide pe x, atunci $(xy, p) = p$ şi $(x, p) = 1$. Deci

$$(y, p) = (y(x, p), p) = ((yx, yp), p) = (yx, (yp, p)) = (yx, p) = p,$$

adică $(y, p) = p$, de unde rezultă $p \mid y$. Prin urmare p este prim. □

Am văzut în cursul anterior că dacă R este un domeniu cu ideale principale, atunci pentru orice $a, b \in R$ există un c.m.m.d.c. şi că

$$d = (a, b) \Leftrightarrow dR = aR + bR.$$

Astfel, din teorema anterioară rezultă:

Corolarul 10. Într-un domeniu cu ideale principale un element este ireductibil dacă şi numai dacă este prim.

Cum $\mathbb{Z}$ este un domeniu cu ideale principale, corolarul anterior dă încă o motivaţie pentru faptul că în $\mathbb{Z}$ elementele ireductibil şi elementele prime coincid. Însă, în general, reciproca afirmaţiei 1) din teorema de mai sus nu este adevărată.

Exemplul 11. Exerciţiul 5 ne-a arătat că 3 este ireductibil în domeniul de integritate $\mathbb{Z}[i\sqrt{5}]$, dar nu este prim. Din punctul 2) al teoremei 9 urmează că există numere în $\mathbb{Z}[i\sqrt{5}]^*$ care nu au un c.m.m.d.c., iar punctul c) al exerciţiului 5 furnizează un exemplu în acest sens.

Observaţia 12. Din exemplul de mai sus deducem că $\mathbb{Z}[i\sqrt{5}]$ nu este un domeniu cu ideale principale. Unul dintre motivele pentru care în exerciţiile referitoare la $\mathbb{C}[X]$, $\mathbb{R}[X]$, $\mathbb{Z}[i]$ nu am vorbit şi despre elemente prime este acela că aceste domenii de integritate sunt domenii cu ideale principale (şi chiar ceva mai mult, după cum vom vedea în lecţiile viitoare), deci în acestea elementele ireductibile coincid cu elementele prime.