CURS 8

Domenii factoriale

Teorema următoare determină clasa mulţimilor ordonate în care se poate aplica demonstraţia prin inducţie. Acest rezultat se va dovedi de mare utilitate în acest curs.

Teorema 1. Pentru o mulţime ordonată $(A, \leq)$ sunt echivalente următoarele condiţii:
1) **Condiţia minimalităţii**: fiecare submulţime nevidă $B \subseteq A$ are cel puţin un element minimal.
2) **Condiţia inductivităţii**: orice submulţime $B \subseteq A$ care are proprietăţile:
α) B conţine toate elementele minimale ale lui A,
β) $a \in A$ şi $\{x \in A \mid x < a\} \subseteq B \Rightarrow a \in B$,
coincide cu A.
3) **Condiţia lanţurilor descrescătoare**: orice şir strict descrescător de elemente din A,

$$a_1 > a_2 > \cdots > a_n > \dots ,$$

este finit. Cu alte cuvinte, orice şir monoton descrescător din A e staţionar, adică pentru orice şir

$$a_1 \geq a_2 \geq \cdots \geq a_n \geq \dots$$

din A există un indice m astfel încât $a_m = a_{m+1} = \dots$

Demonstraţie. (facultativă)
1) $\Rightarrow$ 2). Presupunem, prin reducere la absurd, că există $B \subseteq A$ care verifică α) şi β), dar $B \neq A$. Conform 1), $A \setminus B$ are cel puţin un element minimal a. Evident $a \notin B$, iar din α) deducem că a nu este element minimal al lui A. Prin urmare, dacă $x \in A$ astfel încât $x < a$, din minimalitatea lui a în $A \setminus B$, rezultă că $x \notin A \setminus B$, adică $x \in B$. Aşadar,

$$a \in A \text{ şi } \{x \in A \mid x < a\} \subseteq B,$$

iar cum B verifică pe β) deducem că $a \in B$, ceea ce contrazice alegerea lui a.

2) $\Rightarrow$ 3). Fie B mulţimea elementelor $b \in A$ care verifică proprietatea: orice şir strict descrescător de elemente din A care începe cu b este finit. Toate elementele minimale în A verifică această proprietate, deci aparţin lui B. Dacă $a \in A$ şi orice şir strict descrescător care începe cu orice $x \in A$, $x < a$ este finit, atunci şi orice şir strict descrescător care începe cu a este finit, adică $a \in B$. Deci B verifică pe α) şi β), ceea ce implică $B = A$.

3) $\Rightarrow$ 1). Arătăm că negaţia lui 1) implică negaţia lui 3). Din negaţia lui 1) rezultă că există o submulţime nevidă $B \subseteq A$ care nu are nici un element minimal. Folosind axioma alegerii, putem alege câte un element din fiecare submulţime nevidă a lui B. Construim un şir strict descrescător infinit de elemente din B după cum urmează. Notăm cu a_1 elementul ales din B. Întrucât a_1 nu este minimal în B rezultă că $B_1 = \{a \in B \mid a < a_1\} \subseteq B$ este nevidă. Notăm cu a_2 elementul ales din B_1. Odată ales elementul $a_n \in B$, cum a_n nu e minimal în B rezultă că $B_n = \{a \in B \mid a < a_n\} \subseteq B$ este nevidă. Notăm cu a_{n+1} elementul ales din B_n. În acest fel rezultă şirul infinit

$$a_1 > a_2 > \cdots > a_n > \dots ,$$

şi astfel am demonstrat negaţia lui 3). □

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

Definiţia 2. Fie $a \in R$, $x_i \in R$, $(i = 1, \ldots, k)$, $y_j \in R$ $(j = 1, \ldots, n)$ şi

$$a = x_1 \cdots x_k = y_1 \cdots y_n$$

două descompuneri ale lui a în factori. Spunem că cele două **descompuneri** sunt **asociate** dacă $k = n$ şi, după o eventuală renumerotare a factorilor celei de-a doua descompuneri, $x_i \sim y_i$ pentru toţi $i = 1, \ldots, n$.

Exemplul 3. Dacă $1 = u_1 \ldots u_k$ în R, atunci descompunerea $a = x_1 \cdots x_k$ este asociată cu descompunerea $a = (u_1 x_1) \cdots (u_k x_k)$.

Definiţia 4. Un domeniu de integritate $(R, +, \cdot)$ se numeşte **domeniu factorial** sau **domeniu cu factorizare unică (în factori ireductibili)** dacă orice $a \in R^*$ neinversabil se descompune în produs de elemente ireductibile şi orice două descompuneri ale lui a în produse de elemente ireductibile sunt asociate, adică a are o descompunere unică (abstracţie făcând de o asociere) în produs de elemente ireductibile.

Exemplul 5. Din teorema fundamentală a aritmeticii rezultă că $(\mathbb{Z}, +, \cdot)$ este un domeniu factorial.

Existenţa descompunerii oricărui element nenul neinversabil în factori ireductibili, neinsoţită neapătrat de unicitate, defineşte o clasă de domenii de integritate care include clasa domeniilor factoriale fără a coincide coincide cu aceasta.

Definiţia 6. Un domeniu de integritate R se numeşte **domeniu** (sau **inel**) **semifactorial** dacă orice $a \in R^*$ neinversabil poate fi scris ca produs de elemente ireductibile.

Exerciţiul 1. Fie R un domeniu de integritate. Dacă există o funcţie $\varphi : R^* \to \mathbb{N}$ cu proprietatea

$$a, b \in R^*,\ b \mid a,\ a \nmid b \Rightarrow \varphi(b) < \varphi(a), \qquad (*)$$

atunci R este un domeniu semifactorial.

Soluţie: Presupunem, prin reducere la absurd, că R nu este inel semifactorial. Atunci mulţimea

$$M = \{a \in R^* \mid a \text{ e neinversabil şi nu e produs de elemente ireductibile}\}$$

e nevidă şi $\varphi(M) = \{\varphi(a) \mid a \in M\}$ este o submulţime nevidă a lui $\mathbb{N}$, prin urmare are cel mai mic element. Fie $b \in M$ cu $\varphi(b) = \min \varphi(M)$. Cum M nu conţine elementele ireductibile (acestea fiind produse de elemente ireductibile cu un factor), b nu este ireductibil, nici inversabil, deci există $b', b'' \in R^*$, ambele neinversabile, astfel încât $b = b'b''$. Atunci $b \nmid b'$ şi $b \nmid b''$ şi din $(*)$ rezultă $\varphi(b') < \varphi(b)$ şi $\varphi(b'') < \varphi(b)$. Având în vedere cum a fost ales b, e necesar ca b' şi b'' să admită câte o descompunere în factori ireductibili. Dar atunci şi $b = b'b''$ poate fi scris ca produs de elemente ireductibile, ceea ce contrazice faptul că $b \in M$. Deci $M = \emptyset$ şi demonstraţia este completă.

Exerciţiul 2. Fie K un corp comutativ. Să se arate că domeniul de integritate $K[X]$ este semifactorial.

Soluţie: Pentru $f, g, h \in K[X]$, cu $f = gh$, din $\operatorname{grad} f = \operatorname{grad} g + \operatorname{grad} h$ se deduce că

$$\operatorname{grad} f = \operatorname{grad} g \Leftrightarrow \operatorname{grad} h = 0 \Leftrightarrow h \in U(K[X]) \Leftrightarrow f \sim g.$$

Proprietatea lui $K[X]$ de a fi semifactorial rezultă acum aplicând exerciţiul anterior funcţiei $\varphi = \text{grad} : K[X] \setminus \{0\} \to \mathbb{N}$.

Exerciţiul 3. i) Să se arate că orice număr prim este element ireductibil în $\mathbb{Z}[X]$.
ii) Să se arate că domeniul de integritate $\mathbb{Z}[X]$ este semifactorial.

Soluţie: i) Fie $p \in \mathbb{N}$ un număr prim. Dacă $f, g \in \mathbb{Z}[X]$ şi $p = fg$ din $0 = \text{grad}\, p = \text{grad}\, f + \text{grad}\, g$ se deduce că $f, g \in \mathbb{Z}$, prin urmare $f = \pm 1$ sau $g = \pm 1$. Deci p nu are divizori proprii în $\mathbb{Z}[X]$.
ii) Demonstrăm că orice polinom $f \in \mathbb{Z}[X] \setminus \{-1, 0, 1\}$ poate fi scris ca un produs de polinoame ireductibile. Procedăm prin inducţie după gradul lui f. Dacă $\text{grad}\, f = 0$ atunci $f \in \mathbb{Z}$ este neinversabil şi atunci f este un produs de numere prime. Concluzia rezultă din i). Considerăm $\text{grad}\, f \geq 1$ şi presupunem afirmaţia adevărată pentru polinoamele de grad mai mic decât $\text{grad}\, f$. Fia $a \in \mathbb{Z}$ c.m.m.d.c. al coeficienţilor lui f. Cum $\text{grad}\, f \geq 1$, f poate fi scris $f = ag$ cu $g \in \mathbb{Z}[X]$ cu $\text{grad}\, g = \text{grad}\, f \geq 1$ şi c.m.m.d.c. al coeficienţilor lui g egal cu 1. Pe a îl putem scrie ca produs de numere prime (care sunt elemente ireductibile în $\mathbb{Z}[X]$). Dacă g este ireductibil, problema este rezolvată. În caz contrar, g poate fi descompus ca produs de 2 polinoame neinversabile g' şi g''. Cum polinomul g are c.m.m.d.c. al coeficienţilor săi egal cu 1, avem $g', g'' \notin \mathbb{Z}$, prin urmare $\text{grad}\, g' < \text{grad}\, f$ şi $\text{grad}\, g'' < \text{grad}\, f$. Se aplică ipoteza inducţiei şi se obţine o descompunere a lui f în factori ireductibili.

Observaţia 7. De notat că rezolvarea exerciţiului 3 nu se poate face ca şi cea a exerciţiului 2 deoarece funcţia $\varphi = \text{grad} : \mathbb{Z}[X] \setminus \{0\} \to \mathbb{N}$ nu satisface condiţia $(*)$. De exemplu, în inelul $\mathbb{Z}[X]$, $X \mid 2X$ fără a fi asociate şi, totuşi, $\text{grad}\, X = 1 = \text{grad}\, 2X$.

Exerciţiul 4. Fie $d \in \mathbb{Z} \setminus \{1\}$ un întreg liber de pătrate. Să se arate că în $\mathbb{Z}[\sqrt{d}]$ este un domeniu semifactorial.

Soluţie: Fie $\delta : \mathbb{Z}[\sqrt{d}] \to \mathbb{N}$, $\delta(z) = |z \cdot \overline{z}|$. Din exerciţiul 2 din cursul 4 b) ii) şi iii) rezultă că pentru orice $z \in \mathbb{Z}[\sqrt{d}]$ nenul şi neinversabil $\delta(z) \in \mathbb{N}$, $\delta(z) \geq 2$. Concluzia se obţine acum folosind punctul b) i) din acelaşi exerciţiu (2 din cursul 4) pentru a arăta că δ verifică condiţia $(*)$ din exerciţiul 1. Într-adevăr, dacă $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$, $z_1 \mid z_2$ şi $z_2 \nmid z_1$ atunci există $z \in \mathbb{Z}[\sqrt{d}]$ nenul şi neinversabil astfel încât $z_2 = z_1 z$. atunci $\delta(z_2) = \delta(z_1)\delta(z)$ şi cum $\delta(z) \geq 2$, rezultă $\delta(z_1) < \delta(z_2)$.

Exerciţiul 5. Să se arate că: a) $\mathbb{Z}[i\sqrt{5}]$; b) $\mathbb{Z}[i\sqrt{6}]$; c) $\mathbb{Z}[i\sqrt{17}]$; d) $\mathbb{Z}[i\sqrt{29}]$ sunt inele semifactoriale care nu sunt domenii factoriale.

Soluţie: Faptul că domeniile din enunţ sunt semifactoriale rezultă din exerciţiul anterior.
a) O justificare pentru faptul că domeniul $\mathbb{Z}[i\sqrt{5}]$ nu e factorial rezultă considerând descompunerile

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

ale lui 6. Am văzut în cursul anterior că 2, 3, $1 + i\sqrt{5}$ şi $1 - i\sqrt{5}$ sunt elemente ireductibile în $\mathbb{Z}[i\sqrt{5}]$, dar cele două descompuneri ale lui 6 în produs de elemente ireductibile nu sunt asociate deoarece elementele asociate au aceeaşi normă iar $\delta(1 - i\sqrt{5}) = \delta(1 + i\sqrt{5}) = 6$ e diferit şi de $\delta(2) = 4$ şi de $\delta(1) = 9$.
b) $6 = 2 \cdot 3 = i\sqrt{6}(-i\sqrt{6})$ sunt două descompuneri ale lui 6 în produs de elemente ireductibile care nu sunt asociate.
c) $18 = 2 \cdot 3 \cdot 3 = (1 + i\sqrt{17})(1 - i\sqrt{17})$ sunt două descompuneri ale lui 18 în produs de elemente ireductibile care nu sunt asociate.
d) $30 = 2 \cdot 3 \cdot 5 = (1 + i\sqrt{29})(1 - i\sqrt{29})$ sunt două descompuneri ale lui 30 în produs de elemente ireductibile care nu sunt asociate.

Teorema 8. Dacă R este un domeniu factorial, atunci:
1) Mulţimea ordonată $(R^*/\sim, \leq)$ verifică condiţia minimalităţii, adică orice submulţime nevidă a lui $R^*/\sim$ are un element minimal.
2) Orice pereche de elemente din R are un c.m.m.d.c.

Demonstraţie. 1) Conform teoremei 1, pentru a demonstra condiţia 1) este suficient să arătăm că orice şir strict descrescător de clase de asociere în divizibilitate din $R/\sim \setminus\{[0]\}$

$$[x_1] > [x_2] > [x_3] > \dots \tag{1}$$

este finit.

Pentru $a \in R$, vom nota cu $l(a)$ numărul factorilor dintr-o descompunere a lui a în produs de factori ireductibili dacă a nu este inversabil şi $l(a) = 0$ dacă a este inversabil. Evident, dacă $a = a_1a_2$, atunci $l(a) = l(a_1) + l(a_2)$.

Cum $[x_i] > [x_{i+1}]$ dacă şi numai dacă $x_{i+1} \mid x_i$ şi $x_i \nmid x_{i+1}$, rezultă că $l(x_{i+1}) < l(x_i)$ şi, astfel, din (1) rezultă că

$$l(x_1) > l(x_2) > l(x_3) > \dots \tag{2}$$

este un şir strict descrescător de numere naturale. Prin urmare, (2) este un şir finit, de unde rezultă că (1) este un şir finit. Deci este verificată condiţia 1).
2) Fie $a_1, a_2 \in R$. Dacă $a_1 = 0$ atunci există un c.m.m.d.c. pentru a_1 şi a_2 şi $(a_1, a_2) = a_2$. La fel şi dacă $a_2 = 0$. Considerăm $a_1, a_2 \in R^*$ şi $p_1, \dots, p_n$ elemente ireductibile din R astfel încât oricare două dintre ele nu sunt asociate în divizibilitate şi

$$a_1 = up_1^{k_1} \dots p_n^{k_n} \text{ şi } a_2 = u'p_1^{l_1} \dots p_n^{l_n}$$

unde $u, u' \in R$ sunt elemente inversabile şi $k_i, l_i \in \mathbb{N}$, $i = 1, \dots, n$. Orice divizor x al lui a_1 se poate scrie sub forma $x = u''p_1^{s_1} \dots p_n^{s_n}$, unde $u'' \in R$ este inversabil, $0 \leq s_i \leq k_i$ $(i = 1, \dots, n)$ şi o afirmaţie analoagă are loc pentru divizorii lui a_2. Deci $d = p_1^{m_1} \dots p_n^{m_n}$, unde $m_i = \min\{k_i, l_i\}$ $(i = 1, \dots, n)$ este un c.m.m.d.c. al lui a_1 şi a_2. Prin urmare, este verificată şi condiţia 2). □

Teorema 9. Un domeniu de integritate R este factorial dacă şi numai dacă verifică condiţiile:
1) Mulţimea ordonată $(R^*/\sim, \leq)$ verifică condiţia minimalităţii.
2′) Orice element ireductibil din R este prim.

Demonstraţie. Dacă R este un domeniu factorial, atunci din teorema anterioră şi din teorema 9 din cursul 7 rezultă că R verifică pe 1) şi 2′).

Reciproc, presupunem că R verifică pe 1) şi 2′) şi vom arăta că orice element $a \in R^*$ neinversabil are o descompunere unică, abstracţie făcând de o asociere, în produs de elemente ireductibile. Întâi să observăm că dacă a are această proprietate, atunci orice element asociat cu a are această proprietate. Această constatare ne permite, pe baza condiţiei 1) şi a teoremei 1, să dăm o demonstraţie inductivă în raport cu relaţia $\leq$ din $R^*/\sim \setminus\{[1]\}$. Afirmaţia are loc pentru elementele ireductibile din R, adică pentru elementele minimale din $R^*/\sim \setminus\{[1]\}$. Presupunem că $[a]$ nu este element minimal în $R^*/\sim \setminus\{[1]\}$ şi că afirmaţia are loc pentru toţi divizorii proprii ai lui a. Rezultă că $a = a_1a_2$ unde a_1, a_2 sunt divizori proprii ai lui a. Conform ipotezei inducţiei $a_1 = p_1 \dots p_k$ şi $a_2 = p_{k+1} \dots p_n$, unde p_i $(i = 1, \dots, n)$ sunt elemente ireductibile. De aici rezultă

$$a = p_1 \dots p_k p_{k+1} \dots p_n \tag{3}$$

adică a are o descompunere în produs de elemente ireductibile. Fie

$$a = q_1 \dots q_s \tag{4}$$

o altă descompunere a lui a în produs de elemente ireductibile. Din $2')$ rezultă că elementul q_1 este prim şi din $q_1 \mid p_1 \cdots p_n$ rezultă că q_1 divide cel puţin unul dintre elementele $p_1, \dots, p_n$. Cum R este comutativ, putem considera, fără a restrânge generalitatea, că $q_1 \mid p_1$. Din p_1 ireductibil urmează că p_1 şi q_1 sunt asociate adică există $u \in R$ inversabil astfel ca $p_1 = uq_1$. Prin urmare

$$uq_1p_2 \dots p_n = q_1q_2 \dots q_s.$$

Prin simplificare cu q_1 se obţine că $(up_2)p_3 \dots p_n = q_2q_3 \dots q_s$ sunt descompuneri în factori ireductibili ale unui divizor propriu al lui a şi, conform ipotezei inducţiei, acestea sunt asociate. Rezultă că descompunerile (3) şi (4) ale lui a sunt asociate. □

Folosind teorema 9 din cursul 7 se constată imediat că:

Corolarul 10. Un domeniu de integritate R este factorial dacă şi numai dacă verifică condiţiile:
1) Mulţimea ordonată $(R^*/\sim, \leq)$ verifică condiţia minimalităţii, adică orice submulţime nevidă a lui $R^*/\sim$ are un element minimal.
2) Orice pereche de elemente din R are un c.m.m.d.c.

Observaţiile 11. a) Faptul că domeniul de integritate $(\mathbb{Z}[i\sqrt{5}], +, \cdot)$ nu este factorial rezultă imediat din teorema 9 şi exemplul 11 din cursul 7.
b) Condiţia 1) din teoremele 8 şi 9 este echivalentă cu afirmaţia: *pentru orice şir* $x_1, x_2, \dots, x_n, \dots$ *de elemente din* R *cu proprietatea* $x_{i+1} \mid x_i$ *pentru orice* $i \in \mathbb{N}^*$, *există* $k \in \mathbb{N}^*$ *astfel încât* $x_i \sim x_k$ *pentru toţi* $i \geq k$.

Teorema 12. Orice domeniu cu ideale principale este factorial.

Demonstraţie. Presupunem că R este un domeniu cu ideale principale. Din corolarul 10 din cursul 7 rezultă că orice element ireductibil din R este prim. Conform teoremei 9, pentru a arăta că R este factorial este suficient să arătăm că mulţimea $(R^*/\sim, \leq)$ verifică condiţia minimalităţii. Cum pentru orice $a, b \in R$ avem

$$[a] \leq [b] \;\Leftrightarrow\; bR \subseteq aR$$

această condiţie este echivalentă cu afirmaţia: pentru orice şir crescător de ideale

$$a_0R \subseteq a_1R \subseteq \dots \subseteq a_nR \subseteq \dots \tag{5}$$

există un indice m astfel încât $a_nR = a_mR$ pentru orice $n \geq m$. Din (5) rezultă că $U = \bigcup_{n=0}^{\infty} a_nR$ este ideal (vezi Propoziţia 7 v) din cursul 4). Domeniul R fiind cu ideale principale urmează că există $b \in R$ astfel încât $\bigcup_{n=0}^{\infty} a_nR = U = bR$. Deducem de aici existenţa unui $m \in \mathbb{N}$ astfel încât $b \in a_mR$, ceea ce implică $U = bR \subseteq a_mR$. Incluziunea inversă fiind evidentă, urmează $U = a_mR$ şi atunci $a_nR = U = a_mR$, pentru orice $n \geq m$. □

Observaţiile 13. a) În lecţiile următoare vom identifica o subclasă a clasei domeniilor cu ideale principale (din care fac parte şi $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{R}[X]$ şi $\mathbb{C}[X]$) care ne va ajuta să îmbogăţim considerabil lista de exemple de domenii cu ideale principale şi implicit de exemple de domenii factoriale.
b) Există domenii factoriale care nu sunt domenii cu ideale principale. Vom vedea în lecţiile viitoare dedicate divizibilităţii polinoamelor că $\mathbb{Z}[X]$ este un astfel de inel.