CURS 5

Divizibilitatea în domenii de integritate

În continuare considerăm $(R, +, \cdot)$ un domeniu de integritate.

Definiţia 1. Relaţia $\mid$ definită pe R astfel

$$a \mid b \Leftrightarrow \exists\, x \in R,\ b = ax$$

se numeşte **relaţia de divizibilitate** în R, iar dacă $a \mid b$ se spune că a **divide pe** b sau că b **se divide prin** a sau că a **este un divizor al lui** b sau că b **este un multiplu al lui** a.

Teorema 2. (Proprietăţi ale relaţiei de divizibilitate)
Fie $a, a', b, b', c \in R$. Sunt adevărate afirmaţiile:
(i) $1 \mid a$, $a \mid a$, $a \mid 0$;
(ii) $0 \mid a$ dacă şi numai dacă $a = 0$;
(iii) dacă $a \mid b$ şi $b \mid c$, atunci $a \mid c$;
(iv) dacă $a \mid b$ şi $a' \mid b'$, atunci $aa' \mid bb'$;
(v) dacă $a \mid b$, atunci $a \mid bc$;
(vi) pentru $c \neq 0$, $a \mid b$ dacă şi numai dacă $ac \mid bc$;
(vii) dacă $a \mid b$ şi $a \mid c$, atunci $a \mid b + c$;
(viii) dacă $a \mid b + c$ şi $a \mid b$, atunci $a \mid c$.

Demonstraţie. (i) Din $a = 1a$ rezultă $1 \mid a$ şi $a \mid a$, iar din $a \cdot 0 = 0$ rezultă $a \mid 0$.
(ii) este o consecinţă a faptului că $0 \cdot x = 0$ pentru orice $x \in R$.
(iii) Dacă $a \mid b$ şi $b \mid c$ atunci există $x, y \in A$ astfel încât $b = ax$ şi $c = by$ ceea ce implică $c = a(xy)$, adică $a \mid c$.
(iv), (v) sunt imediate.
(vi) $a \mid b$ şi $c \mid c$ implică $ac \mid bc$. Reciproc, din $ac \mid bc$ rezultă că există $x \in R$ pentru care $bc = (ac)x = a(cx) = a(xc) = (ax)c$. Cum $c \neq 0$, putem simplifica cu c şi avem $b = ax$, adică $a \mid b$.
(vii), (viii) sunt consecinţe imediate ale distributivităţii lui $\cdot$ faţă de $+$. □

Observaţia 3. Relaţia de divizibilitate este o relaţie de preordine — fiind reflexivă (vezi (i)) şi tranzitivă (vezi (iii)) — care nu este, în general, relaţie de ordine. Un exemplu în acest sens este şi domeniul de integritate $(\mathbb{Z}, +, \cdot)$, unde am văzut că $2 \mid -2,\ -2 \mid 2$ şi $2 \neq -2$.

Definiţia 4. Relaţia $\sim$ definită pe R astfel

$$a \sim b \Leftrightarrow a \mid b \text{ şi } b \mid a$$

se numeşte **relaţia de asociere în divizibilitate**, iar dacă $a \sim b$ se spune că a şi b **sunt asociate în divizibilitate**.

Teorema 5. (Proprietăţi ale relaţiei de asociere în divizibilitate)
Fie $a, a', b, b', c \in R$. Sunt adevărate afirmaţiile:
(i) $a \sim a$;
(ii) dacă $a \sim b$ atunci $b \sim a$;
(iii) dacă $a \sim b$ şi $b \sim c$, atunci $a \sim c$;

(iv) $a \sim 0$ dacă şi numai dacă $a = 0$;
(v) dacă $a \sim b$ şi $a' \sim b'$, atunci $aa' \sim bb'$;
(vi) $a \sim 1 \Leftrightarrow a \mid 1 \Leftrightarrow a$ este element inversabil în R;
(vii) $a \sim b$ dacă şi numai dacă există $u \in R$ inversabil astfel încât $b = au$.

Demonstraţie. (i)–(v) rezultă imediat din definiţia asocierii în divizibilitate şi teorema 2.
(vi) Cum 1 divide orice element, $a \sim 1$ este echivalent cu $a \mid 1$, adică există $x \in R$ pentru care $1 = ax$. Evident, aceasta înseamnă că a este inversabil şi $a^{-1} = x$.
(vii) Dacă $a = 0$ atunci $b = 0$ şi proprietatea e evidentă, deci putem considera $a, b \in R^*$.

Atunci $a \sim b$, adică $a \mid b$ şi $b \mid a$, implică existenţa $u, v \in R$ astfel încât $b = au$ şi $a = bv$. Rezultă $a = auv$, de unde $uv = 1$, deci b este de forma $b = au$ cu u inversabil. Reciproc, $a \mid au (= b)$, iar dacă u este inversabil, atunci $a = (au)u^{-1} = bu^{-1}$ implică $b \mid a$. Deci $a \sim b$. □

Corolarul 6. Relaţia de asociere în divizibilitate este o relaţie de echivalenţă. Dacă $a \in R$ atunci clasa de echivalenţă a lui a în raport cu $\sim$ este

$$[a] = aU(R) = \{ax \mid x \in U(R)\}.$$

Observaţiile 7. i) În orice domeniu de integritate R, clasa $[0]$ are un singur element, pe 0.
ii) Pentru orice $a \in R$ elementele inversabile şi elementele asociate cu a sunt divizori ai lui a. Un divizor al lui a diferit de aceştia se numeşte **divizor propriu**.
iii) Relaţia de divizibilitate este relaţie de ordine pe R dacă şi numai dacă relaţia de asociere în divizibilitate coincide cu relaţia de egalitate pe R, ceea ce are loc dacă şi numai dacă singurul element inversabil din R este 1.

Teorema 8. Fie R un domeniu de integritate. Mulţimea cât $R/\sim = \{[a] \mid a \in R\}$ este o mulţime ordonată în raport cu relaţia $\leq$ definită astfel:

$$[a] \leq [b] \Leftrightarrow a \mid b.$$

Demonstraţie. Începem prin a demonstra că definiţia relaţiei $\leq$ este independentă de alegerea reprezentanţilor a şi b. Într-adevăr, dacă $a' \in [a]$ şi $b' \in [b]$ (adică $a \sim a'$ şi $b \sim b'$), atunci avem şi $a' \mid b'$ deoarece $a' \mid a,\ a \mid b$ şi $b \mid b'$ şi $\mid$ este tranzitivă.

Din reflexivitatea şi tranzitivitatea divizibilităţii rezultă imediat reflexivitatea şi tranzitivitatea relaţiei $\leq$, iar dacă $[a] \leq [b]$ şi $[b] \leq [a]$ atunci $a \mid b$ şi $b \mid a$. Aşadar, $a \sim b$, adică $[a] = [b]$. Deci $\leq$ este şi antisimetrică. □

Observaţia 9. Din teorema 5 rezultă că $[1] = U(R)$, iar din teorema 2 rezultă că $[1]$ este cel mai mic element în mulţimea ordonată $(R/\sim, \leq)$.

Exemplele 10. a) În domeniul de integritate $(\mathbb{Z}, +, \cdot)$ avem $[1] = U(\mathbb{Z}) = \{-1, 1\}$. Prin urmare

$$m \sim n \Leftrightarrow m \in \{-n, n\}$$

şi $[n] = \{-n, n\}$ pentru orice $n \in \mathbb{Z}^*$, iar în $(\mathbb{Z}/\sim, \leq)$, $[0] = \{0\}$ este cel mai mare mare element, iar dacă $m, n \in \mathbb{Z}^*$, atunci

$$\{-m, m\} \leq \{-n, n\} \Leftrightarrow m \mid n.$$

Fiecare clasă din $\mathbb{Z}/\sim$ conţine un singur număr natural, de aceea studiul divizibilităţii în $\mathbb{Z}$ se reduce la studiul divizibilităţii în $\mathbb{N}$.

b) Dacă K este un corp comutativ (de exemplu K poate fi $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ (cu p număr prim)) atunci K este un domeniu de integritate cu $U(K) = K^*$. Deci în K avem $a \sim b$ pentru orice $a, b \in K^*$ şi, astfel, $K/\sim$ are doar două elemente: $\{0\}$ (care este $[0]$ şi este cel mai mare) şi K^* (care este $[1]$ şi este cel mai mic).
c) Dacă R este domeniu de integritate, atunci $U(R[X]) = U(R)$ şi, astfel, pentru $f, g \in R[X]$ avem

$$f \sim g \;\Leftrightarrow\; \exists\, a \in R^* \text{ inversabil în } (R, \cdot) \text{ astfel încât } f = ag.$$

În particular, dacă $f, g \in \mathbb{Z}[X]^*$, atunci

$$f \sim g \;\Leftrightarrow\; f = \pm g,$$

iar dacă K este un corp comutativ atunci în domeniul de integritate $K[X]$ avem

$$f \sim g \;\Leftrightarrow\; \exists\, a \in K^* :\; f = ag.$$

Rezultă că fiecare clasă din $(K[X] \setminus \{0\})/\sim$ conţine un singur polinom cu coeficientul termenului de grad maxim egal cu 1.
d) Am văzut în cursul anterior că $U(\mathbb{Z}[i]) = \{-1, 1, -i, i\}$, prin urmare, dacă $z_1, z_2 \in \mathbb{Z}[i]$ atunci

$$z_1 \sim z_2 \;\Leftrightarrow\; z_2 \in \{-z_1, z_1, -iz_1, iz_2\}.$$

e) Cum $U(\mathbb{Z}[i\sqrt{5}]) = \{-1, 1\}$, $z_1 \sim z_2$ în $\mathbb{Z}[i\sqrt{5}]$ dacă şi numai dacă $z_2 \in \{-z_1, z_1\}$.

Teorema 11. Fie R este domeniu de integritate şi $a, b \in R$. Atunci:
i) $a \mid b \;\Leftrightarrow\; bR \subseteq aR \;\Leftrightarrow\; (b) \subseteq (a)$;
ii) $a \sim b \;\Leftrightarrow\; aR = bR \;\Leftrightarrow\; (a) = (b)$.

Demonstraţie. i) $a \mid b \Rightarrow \exists x \in R : b = ax \Rightarrow \forall r \in R, br = (ax)r = a(xr) \in aR$.
Reciproc, $b \in bR \subseteq aR \Rightarrow \exists x \in R : b = ax \Rightarrow a \mid b$.
ii) $a \sim b \Leftrightarrow a \mid b$ şi $b \mid a \Leftrightarrow bR \subseteq aR$ şi $aR \subseteq bR \Leftrightarrow aR = bR$. □

Din teorema anterioară rezultă imediat:

Corolarul 12. Pentru orice elemente $a, b \in R$ ale unui domeniu de integritate R avem:
$[a] \leq [b] \;\Leftrightarrow\; bR \subseteq aR$;
$[a] = [b] \;\Leftrightarrow\; aR = bR$.

Cel mai mare divizor comun şi cel mai mic multiplu comun

Considerăm $(R, +, \cdot)$ un domeniu de integritate.

Definiţia 13. Fie $a_1, \ldots, a_n \in R$ şi $d \in R$. Vom spune că d este **un cel mai mare divizor comun** (c.m.m.d.c) al elementelor $a_1, \ldots, a_n \in R$ dacă în mulţimea ordonată $(R/\sim, \leq)$

$$\exists \inf([a_1], \ldots, [a_n]) \in R/\sim \text{ şi } [d] = \inf([a_1], \ldots, [a_n]).$$

Dacă $a, b \in R$ şi $\inf([a], [b]) = [1]$ adică 1 este un c.m.m.d.c. al elementelor a şi b atunci a şi b se numesc **relativ prime**.

Identificăm fiecare clasă din $R/\sim$ cu câte un reprezentant al ei şi atunci faptul că d este un c.m.m.d.c. al elementelor $a_1, \ldots, a_n$ se notează, aşa cum suntem obişnuiţi pentru numere întregi, cu $d = (a_1, \ldots, a_n)$.

Observaţiile 14. a) Dacă $d = (a_1, \ldots, a_n)$, atunci

$$d' = (a_1, \ldots, a_n) \Leftrightarrow d' \sim d.$$

Prin urmare c.m.m.d.c. dacă există, este determinat până la o asociere în divizibilitate. Dacă în $\mathbb{Z}$ alegeam din fiecare clasă de asociere în divizibilitate a c.m.m.d.c. reprezentantul natural, în continuare nu vom mai proceda la fel, motiv pentru care folosim articolul nehotărât ,,un" atunci când ne referim la c.m.m.d.c.
b) Cum $[a] \leq [b]$ în $R/\sim$ înseamnă $a|b$ în R, definiţia c.m.m.d.c. se traduce în limbajul relaţiei de divizibilitate în forma următoare:

$$d = (a_1, \ldots, a_n) \Leftrightarrow \begin{cases} & d \mid a_1, \ \ldots, \ d \mid a_n \\ d' \in R, & d' \mid a_1, \ldots, d' \mid a_n \Rightarrow d' \mid d \end{cases},$$

formă în care recunoaştem definiţia c.m.m.d.c. în $\mathbb{Z}$.
c) Pentru $a, b \in R$, $a \mid b$ dacă şi numai dacă $(a, b) = a$.
d) Dacă orice două elemente din R au un c.m.m.d.c., atunci pentru orice $a_1, a_2, a_3 \in R$ există un c.m.m.d.c. (a_1, a_2, a_3) şi $((a_1, a_2), a_3) = (a_1, a_2, a_3) = (a_1, (a_2, a_3))$.
e) Dacă orice două elemente din R au un c.m.m.d.c., atunci pentru orice $n \in \mathbb{N}^*$ şi orice elemente $a_1, \ldots, a_n \in R$ există $(a_1, \ldots, a_n)$.

Teorema 15. Dacă orice două elemente din R au un c.m.m.d.c. şi $a, b, c \in R$, atunci:
(1) $(a, b)c = (ac, bc)$;
(2) $(a, b) = 1$ şi $(a, c) = 1 \Rightarrow (a, bc) = 1$;
(3) $a \mid bc$ şi $(a, b) = 1 \Rightarrow a \mid c$.

Demonstraţie. (1) Din $(a, b) \mid a$ şi $(a, b) \mid b$ rezultă $(a, b)c \mid ac$ şi $(a, b)c \mid bc$. Prin urmare, $(a, b)c \mid (ac, bc)$, adică există $x \in R$ astfel încât

$$(ac, bc) = (a, b)cx. \qquad (*)$$

Rezultă $(a, b)cx \mid ac$ şi $(a, b)cx \mid bc$ ceea ce implică $(a, b)x \mid a$ şi $(a, b)x \mid b$, de unde deducem că $(a, b)x \mid (a, b)$. Prin urmare, x este inversabil ceea ce împreună cu $(*)$ ne demonstrează pe (1).
(2) Folosind egalitatea $a = (a, ac)$, observaţia 14.d), relaţia (1) şi ipoteza avem

$$(a, bc) = ((a, ac), bc) = (a, (ac, bc)) = (a, (a, b)c) = (a, c) = 1.$$

(3) Folosind ipoteza şi relaţia (1) avem

$$(a, c) = (a, (a, b)c) = (a, (ac, bc)) = ((a, ac), bc) = (a, bc) = a,$$

adică $(a, c) = a$, ceea ce implică $a \mid c$. □

Corolarul 16. Dacă $d = (a, b)$ şi $a = da'$, $b = db'$, atunci $(a', b') = 1$.

Într-adevăr, din (1) rezultă $d = (da', db') = d(a', b')$ ceea ce implică $(a', b') = 1$.

Definiţia 17. Fie $a_1, \ldots, a_n \in R$ şi $m \in R$. Vom spune că m este **un cel mai mic multiplu comun** (c.m.m.m.c.) al elementelor $a_1, \ldots, a_n$ dacă în mulţimea ordonată $(R/\sim, \leq)$

$$\exists \sup([a_1], \ldots, [a_n]) \in R/\sim \text{ şi } [m] = \sup([a_1], \ldots, [a_n]).$$

Identificăm fiecare clasă din $R/\sim$ cu câte un reprezentant al ei, atunci faptul că m este un c.m.m.m.c. al elementelor $a_1, \ldots, a_n$ se notează cu $m = [a_1, \ldots, a_n]$.

Observaţiile 18. a) Dacă $m = [a_1, \ldots, a_n]$, atunci

$$m' = [a_1, \ldots, a_n] \Leftrightarrow m' \sim m.$$

Prin urmare c.m.m.m.c., dacă există, este determinat până la o asociere în divizibilitate, motiv pentru care şi aici folosim articolul nehotărât ,,un" atunci când ne referim la c.m.m.m.c.
b) ,,Traducerea" în limbajul relaţiei de divizibilitate a definiţiei c.m.m.m.c. este:

$$m = [a_1, \ldots, a_n] \Leftrightarrow \begin{cases} & a_1 \mid m, \ \ldots, \ a_n \mid m \\ m' \in R, & a_1 \mid m', \ldots, a_n \mid m' \Rightarrow m \mid m'. \end{cases}$$

c) Pentru $a, b \in R$, $a \mid b$ dacă şi numai dacă $[a, b] = b$.
d) Dacă orice două elemente din R au un c.m.m.m.c., atunci pentru orice $a_1, a_2, a_3 \in R$ există un c.m.m.m.c. $[a_1, a_2, a_3]$ şi $[[a_1, a_2], a_3] = [a_1, a_2, a_3] = [a_1, [a_2, a_3]]$.
e) Dacă orice două elemente din R au un c.m.m.m.c., atunci pentru orice $n \in \mathbb{N}^*$ şi orice elemente $a_1, \ldots, a_n \in R$ există $[a_1, \ldots, a_n]$.

Teorema 19. Dacă pentru orice $a, b \in R$ există (a, b), atunci există şi un c.m.m.m.c. pentru a şi b şi putem alege din clasa sa un element $[a, b]$ astfel încât $ab = (a, b)[a, b]$.

Demonstraţie. Fie $d = (a, b)$ şi $a = da'$, $b = db'$. Luând $m = da'b'$ avem

$$ab' = m = ba'$$

de unde rezultă $a \mid m$ şi $b \mid m$. Dacă $m' \in R$ este un alt multiplu comun a lui a şi b, adică $m' = ax$ şi $m' = by$ cu $x, y \in R$, atunci $m' = da'x$ şi $m' = db'y$. Astfel,

$$m'b' = mx \text{ şi } m'a' = my,$$

adică m este un divizor comun al elementelor $m'a'$ şi $m'b'$. Atunci m divide şi pe

$$(m'a', m'b') = m'(a', b') = m'$$

adică $m \mid m'$. Astfel am arătat că $m = [a, b]$.

Din $m = ab' = a'b$ rezultă $md = ab$, adică tocmai egalitatea din enunţ. □

Teorema 20. Dacă R este un domeniu cu ideale principale, atunci:

1) Pentru orice $a, b \in R$ există c.m.m.d.c. şi c.m.m.m.c.
2) $d = (a, b) \Leftrightarrow dR = aR + bR$.
3) $m = [a, b] \Leftrightarrow mR = aR \cap bR$.

Demonstraţia 1. Fie $a, b \in R$. Cum R este un domeniu cu ideale principale şi $aR = (a)$ şi $bR = (b)$ sunt ideale ale lui R, rezultă că $aR + bR$ şi $aR \cap bR$ sunt, de asemenea, ideale (a se vedea propoziţia 7 din cursul 4). Aceste ideale vor fi principale, prin urmare există $d, m \in R$ astfel încât

$$dR = aR + bR \text{ şi } mR = aR \cap bR. \qquad (**)$$

Vom arăta că din prima egalitate din $(**)$ rezultă că $d = (a, b)$.

Din $a = a \cdot 1 + b \cdot 0 \in aR + bR$ şi $b = a \cdot 0 + b \cdot 1 \in aR + bR$ rezultă că există $x, y \in R$ astfel încât $dx = a$ şi $dy = b$, prin urmare $d \mid a$ şi $d \mid b$.

Dacă $d' \in R$ este alt divizor comun pentru a şi b, atunci există $x', y' \in R$ astfel încât $a = d'x'$ şi $b = d'y'$. Cum $d \in dR = aR + bR$, deducem că există $u, v \in R$ pentru care $d = au + bv$ şi astfel,

$$d = au + bv = d'x'u + d'y'v = d'(x'u + y'v),$$

deci $d' \mid d$.

1) Din cele de mai sus rezultă că orice două elemente din R au un c.m.m.d.c., deci, conform teoremei anterioare, au şi un c.m.m.m.c.

2) „$\Leftarrow$" Demonstraţia a fost făcută mai sus.

„$\Rightarrow$" Fie $d = (a, b)$. Din $d \mid a$ şi $d \mid b$ rezultă $aR \subseteq dR$ şi $bR \subseteq dR$, prin urmare

$$aR + bR \subseteq dR + dR \subseteq dR.$$

Rămâne de arătat că $dR \subseteq aR + bR$. Cum $aR + bR$ este ideal în R şi R este un domeniu cu ideale principale, există $d' \in R$ astfel ca $aR + bR = (d') = d'R$. Aşa cum am văzut mai sus (imediat dupa $(**)$), de aici rezultă că d' este un divizor comun pentru a şi b. Deducem că $d' \mid d$ şi astfel, $dR \subseteq d'R = aR + bR$.

3) „$\Leftarrow$" $mR \subseteq aR$ şi $mR \subseteq bR$ implică $a \mid m$ şi $b \mid m$. Orice multiplu comun $m' \in R$ al lui a şi b va aparţine atât lui aR cât şi lui bR, prin urmare $m' \in aR \cap bR = mR$ de unde rezultă $m \mid m'$.

„$\Rightarrow$" Din $a \mid m$ şi $b \mid m$ rezultă $mR \subseteq aR$ şi $mR \subseteq bR$, aşadar, $mR \subseteq aR \cap bR$. Dar $aR \cap bR$ este ideal în domeniul cu ideale principale R, prin urmare există m' pentru care $aR \cap bR = (m') = m'R$. Atunci m' este un multiplu comun pentru a şi b, deci $m \mid m'$ şi, astfel, $mR \supseteq m'R = aR \cap bR$. □

Demonstraţia 2. Pentru un domeniu cu ideale principale R mulţimea idealelor lui R coincide cu mulţimea $\mathcal{I}_p$ a idealelor principale ale lui R. Întrucât idealele unui inel formează o latice în raport cu incluziunea, $(\mathcal{I}_p, \subseteq)$ este latice. În această latice avem

$$\sup_{\mathcal{I}_p}(aR, bR) = aR + bR \text{ şi } \inf_{\mathcal{I}_p}(aR, bR) = aR \cap bR.$$

Fie funcţia

$$\varphi : R/\sim \to \mathcal{I}_p,\ \varphi([a]) = aR.$$

Corolarul 12 ne asigură că φ este bine definită şi că este un antiizomorfism de ordine între $(R/\sim, \leq)$ şi $(\mathcal{I}_p, \subseteq)$. Rezultă că şi $(R/\sim, \leq)$ este latice. Conform definiţiilor 13 şi 17 afirmaţia 1) este adevărată şi folosind antiizomorfismul φ avem:

$$d = (a, b) \Leftrightarrow [d] = \inf_{R/\sim}([a], [b]) \Leftrightarrow \varphi([d]) = \sup_{\mathcal{I}_p}(\varphi([a]), \varphi([b])) \Leftrightarrow dR = aR + bR,$$

$$m = [a, b] \Leftrightarrow [m] = \sup_{R/\sim}([a], [b]) \Leftrightarrow \varphi([m]) = \inf_{\mathcal{I}_p}(\varphi([a]), \varphi([b])) \Leftrightarrow mR = aR \cap bR,$$

ceea ce demonstrează pe 2) şi, respectiv, pe 3). □

Corolarul 21. Dacă R este un domeniu cu ideale principale şi $a, b, d \in R$, atunci

a) $d = (a, b) \Rightarrow \exists\ u, v \in R;\ d = au + bv$;

b) $(a, b) = 1 \Leftrightarrow \exists\ u, v \in R;\ au + bv = 1$.

Implicaţia $\Rightarrow$ de la b) se obţine exact ca pentru numere întregi (vezi Cursul 2).

Observaţia 22. Cum $\mathbb{Z}$ este un domeniu cu ideale principale, reprezentarea Bézout a c.m.m.d.c. a două numere întregi este un caz particular al corolarului anterior.