CURS 4

Pregătirea instrumentelor de lucru

Domenii de integritate, elemente inversabile

O mulţime R împreună cu două operaţii binare $+$ şi $\cdot$ este un **inel comutativ** dacă $(R, +)$ este grup abelian, $(R, \cdot)$ este monoid comutativ şi $\cdot$ este distributivă faţă $+$. Un inel comutativ nenul $(R, +, \cdot)$ este un **domeniu de integritate** dacă nu are divizori ai lui zero.

Observaţia 1. E important în cele ce urmează fapul că în monoidul multiplicativ $(R, \cdot)$ al unui domeniu de integritate $(R, +, \cdot)$ putem simplifica cu orice element nenul, adică pentru $a, x, y \in R$, cu $a \neq 0$,

$$ax = ay \Rightarrow x = y.$$

Un **element** $a \in R$ al unui inel comutativ R este **inversabil** dacă există $x^{-1} \in R$ astfel ca $xx^{-1} = 1$. Un inel comutativ nenul în care toate elementele nenule sunt inversabile se numeşte **corp comutativ**. Evident, *orice corp comutativ este un domeniu de integritate.*

În continuare, notăm cu $U(R)$ **mulţimea elementelor inversabile ale inelului** R.

Observaţia 2. Mulţimea $U(R) = \{x \in R \mid \exists x^{-1} \in R : xx^{-1} = 1\}$ este parte stabilă în $(R, \cdot)$ şi, împreună cu operaţia indusă de $\cdot$, este un grup (comutativ).

Exemplele 3. a) Inelul numerelor întregi $(\mathbb{Z}, +, \cdot)$ este un domeniu de integritate care nu este corp. Elementele sale inversabile sunt -1 şi 1.
b) Mulţimile $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ formează corpuri comutative împreună cu operaţiile uzuale. Dacă K este corp comutativ (în particular, dacă K este unul dintre corpurile anterior menţionate), atunci $U(K) = K \setminus \{0\} = K^*$.
c) Fie R este un inel comutativ şi

$$R[X] = \{f = a_0 + a_1X + \cdots + a_nX^n \mid a_0, a_1, \ldots, a_n \in R,\ n \in \mathbb{N}\}$$

mulţimea polinoamelor în nedeterminata X cu coeficienţi în inelul R. Adunarea şi înmulţirea polinoamelor fac din $(R[X], +, \cdot)$ un inel comutativ cu unitate în care se regăsesc şi elementele lui R şi $U(R) \subseteq U(R[X])$. Dacă R este domeniu de integritate, atunci $R[X]$ este un domeniu de integritate şi $U(R[X]) = U(R)$. În particular, dacă K este corp comutativ, atunci $U(K[X]) = K^*$.
d) Fie $d \in \mathbb{Z} \setminus \{1\}$ este un intreg liber de patrate. Atunci $\mathbb{Z}[\sqrt{d}\,] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ este un domeniu de integritate în raport cu operaţiile uzuale de adunare şi înmulţire.

Dacă $d < 0$ considerăm $\sqrt{d} = i\sqrt{|d|}$ şi $\mathbb{Z}[\sqrt{d}\,] = \mathbb{Z}[i\sqrt{|d|}\,] = \{a + bi\sqrt{|d|} \mid a, b \in \mathbb{Z}\}$. În particular, $\mathbb{Z}[-1] = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ este **inelul întregilor lui Gauss**. Precizăm că $U(\mathbb{Z}[i] = \{-1, 1, i, -i\}$, iar dacă $d \geq 2$ atunci $U(\mathbb{Z}[\sqrt{d}\,]) = \{-1, 1\}$. În schimb, $\mathbb{Z}[\sqrt{2}]$ are o infinitate de elemete inversabile.

De mare utilitate în continuare ne va fi funcţia $\delta : \mathbb{Z}[\sqrt{d}\,] \to \mathbb{N}$, $\delta(z) = |z \cdot \overline{z}|$ (unde $\overline{z} = a - b\sqrt{d}$ este **conjugatul lui** z). Această funcţie, numită **normă**, are următoarele proprietăţi:

i) $\delta(z_1z_2) = \delta(z_1)\delta(z_2),\ \forall z_1, z_2 \in \mathbb{Z}[\sqrt{d}\,]$;
ii) $\delta(z) = 0\ (z \in \mathbb{Z}[\sqrt{d}\,]) \Leftrightarrow z = 0$;
iii) $z \in \mathbb{Z}[\sqrt{d}\,]$ e inversabil în $\mathbb{Z}[\sqrt{d}\,] \Leftrightarrow \delta(z) = 1$;

e) Dacă $d \in \mathbb{Z} \setminus \{1\}$ este un intreg liber de patrate, atunci $\mathbb{Q}(\sqrt{d}\,) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ este un corp comutativ în raport cu operaţiile uzuale de adunare şi înmulţire. Proprietăţile i) şi ii) din exemplul anterior sunt satisfăcute şi de funcţia $\delta_0 : \mathbb{Q}(\sqrt{d}\,) \to \mathbb{Q},\ \delta_0(z) = |z \cdot \overline{z}|$.
f) Fie $n \in \mathbb{N},\ n \geq 2$. Dacă $b \in \mathbb{Z}$, notăm $\widehat{b} = b + n\mathbb{Z} = \{b + nk \mid k \in \mathbb{Z}\}$. Din teorema împărţirii cu rest rezultă că pentru orice $b \in \mathbb{Z}$ există un singur $i \in \{0, 1, \ldots, n-1\}$ (restul împărţirii lui b la n) astfel ca $\widehat{b} = \widehat{i}$. Clasele $\widehat{0}, \widehat{1}, \ldots, \widehat{n-1}$ formează o partiţie a lui $\mathbb{Z}$ care corespunde relaţiei de echivalenţă

$$a \equiv b (\bmod n) \Leftrightarrow n \mid b - a$$

numită **congruenţă modulo** n. Dacă notăm $\mathbb{Z}_n = \{\widehat{0}, \widehat{1}, \ldots, \widehat{n-1}\}$, atunci operaţiile

$$\widehat{a} + \widehat{b} = \widehat{a+b},\ \widehat{a} \cdot \widehat{b} = \widehat{a \cdot b}$$

sunt bine definite pe $\mathbb{Z}_n$ şi $(\mathbb{Z}_n, +, \cdot)$ este un inel comutativ, numit **inelul claselor de resturi modulo** n.

Existenţa divizorilor lui zero în $(\mathbb{Z}_n, +, \cdot)$ depinde de n. De exemplu, în $\mathbb{Z}_4$, $\widehat{2}$ este divizor al lui zero deoarece $\widehat{2} \cdot \widehat{2} = \widehat{4} = \widehat{0}$, chiar dacă $\widehat{2} \neq \widehat{0}$. Dar $(\mathbb{Z}_2, +, \cdot)$ este corp, deoarece $\mathbb{Z}_2 \setminus \{\widehat{0}\} = \{\widehat{1}\}$, iar $\widehat{1}$ este element inversabil în $\mathbb{Z}_2$.

Mai exact, dacă $\widehat{a} \in \mathbb{Z}_n$ atunci $\widehat{a}$ nu este divizor al lui zero în $(\mathbb{Z}_n, +, \cdot)$ dacă şi numai dacă $\widehat{a}$ este inversabil în $(\mathbb{Z}_n, +, \cdot)$, iar aceasta se întâmplă dacă şi numai dacă numerele întregi a şi n sunt relativ prime. În consecinţă, $\mathbb{Z}_n$ este domeniu de integritate dacă şi numai dacă $\mathbb{Z}_n$ este corp comutativ, iar aceasta se întâmplă dacă şi numai dacă n este număr prim.

Un instrument necesar în cele ce vor urma este gradul unui polinom. Fie R este un inel comutativ. Orice polinom nenul f din $R[X]$ admite o scriere unică de forma

$$f = a_0 + a_1X + \cdots + a_nX^n,\ a_0, a_1, \ldots, a_n \in R,\ a_n \neq 0.$$

În acest caz, **gradul lui** f este numărul $n \in \mathbb{N}$ (scriem $\operatorname{grad} f = n$). Prin definiţie, **gradul polinomului nul** 0 este $-\infty$. Remarcăm că polinoamele de grad 0 sunt elementele nenule din R. Extinzând natural adunarea şi relaţia de ordine din $\mathbb{N}$ la $\mathbb{N} \cup \{-\infty\}$, se constată că gradul unui polinom defineşte o funcţie $\operatorname{grad} : R[X] \to \mathbb{N} \cup \{-\infty\}$ care are următoarele proprietăţi:
1) $\operatorname{grad}(f + g) \leq \max\{\operatorname{grad} f, \operatorname{grad} g\},\ \forall f, g \in R[X]$.
2) $\operatorname{grad}(fg) \leq \operatorname{grad} f + \operatorname{grad} g,\ \forall f, g \in R[X]$.
3) Dacă R este un domeniu de integritate, atunci

$$\operatorname{grad}(fg) = \operatorname{grad} f + \operatorname{grad} g,\ \forall f, g \in R[X].$$

Ideale, ideale principale

Fie $(R, +, \cdot)$ un inel comutativ şi $I \subseteq R$. Spunem că I este **ideal al lui** R dacă sunt îndeplinite condiţiile:

1) $I \neq \emptyset$
2) dacă $x, y \in I$, atunci $x + y \in I$;
3) dacă $a \in R$ şi $x \in I$, atunci $xa \in I$.

Observaţiile 4. a) În definitia idealului unui inel, în general, condiţia 2) apare ca
2') dacă $x, y \in I$, atunci $x - y \in I$.

pentru că primele două condiţii asigură faptul că I este un subgrup al lui $(R,+)$. Cum toate inelele noastre au unitate, pentru orice $x \in I$, avem $-x = x \cdot (-1) \in I$, fapt care asigură echivalenţa condiţiilor 1), 2'), 3) cu 1), 2), 3).
b) Orice ideal al lui R este şi subinel al lui R.

Propoziţia 5. Dacă R este un inel comutativ, atunci afirmaţiile de mai jos sunt adevărate:
i) $0 = \{0\}$ şi R sunt ideale.
ii) Dacă I este un ideal care conţine un element inversabil, atunci $I = R$.
iii) Dacă I şi J sunt ideale, atunci $I \cap J$ este un ideal.
iv) Dacă I şi J sunt ideale, atunci $I + J = \{x + y \mid x \in I,\ y \in J\}$ este un ideal.
v) Dacă $I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots$, $n \in \mathbb{N}^*$, este un şir crescător de ideale, atunci $\bigcup_{n\in\mathbb{N}^*} I_n$ e ideal.
vi) Dacă $a_1, \dots, a_n \in R$, atunci

$$(a_1, \dots, a_n) \stackrel{\text{not}}{=} \{a_1x_1 + \dots + a_nx_n \mid x_1, \dots, x_n \in R\}$$

este cel mai mic ideal (în raport cu incluziunea) care conţine elementele $a_1, \dots, a_n$.

Idealul $(a_1, \dots, a_n)$ se numeşte **idealul generat de** $a_1, \dots, a_n$. În particular, dacă $a \in R$ atunci idealul $(a) = \{ax \mid x \in R\} \stackrel{not}{=} aR$ se numeşte **idealul principal generat** de a şi

$$(a_1, \dots, a_n) = a_1R + \dots + a_nR.$$

Definiţiile 6. Fie R un inel comutativ. Un **ideal** I al lui se numeşte **principal** dacă există $a \in R$ astfel încât $I = aR$. Dacă R este domeniu de integritate şi toate idealele lui R sunt principale, spunem că R este un **domeniu cu ideale principale**.

Exemplul 7. Inelul numerelor întregi $(\mathbb{Z}, +, \cdot)$ este un domeniu cu ideale principale. Avem

$$(0) = \{0\} \text{ şi } (n) = (-n) = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\},\ \forall n \in \mathbb{Z}^*,$$

iar mulţimea idealelor lui Z este $\{n\mathbb{Z} \mid n \in \mathbb{N}\}$.