# Algebră III
# Tutoriatul 1

Benea Lorena Cezara
Ștefu Cristi-Ionuț

22 Octombrie 2021

## 1 Inele pătratice

### 1.1 Inelul $\mathbb{Z}[\sqrt{d}]$

Fixăm un întreg $d \neq \{0, 1\}$ care nu este pătrat perfect. Atunci

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}$$

### 1.2 Inelul $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$

Fixăm un întreg $d \neq \{0, 1\}$ care nu este pătrat perfect și $d = 4k + 1, k \in \mathbb{Z}$. Atunci

$$\mathbb{Z}\Big[\frac{1+\sqrt{d}}{2}\Big] = \Big\{a + b\frac{1+\sqrt{d}}{2}\Big| a, b \in \mathbb{Z}\Big\}$$

sau

$$\mathbb{Z}\Big[\frac{1+\sqrt{d}}{2}\Big] = \Big\{\frac{a+b\sqrt{d}}{2}\Big| a, b \in \mathbb{Z}, a \equiv_2 b\Big\}$$

## 2 Divizibilitate

Fie $A$ un domeniu și $a, b \in A$. Zicem că $a$ *divide* $b$ (notat $a|b$) sau $b$ *se divide cu* $a$ (notat $b \vdots a$) dacă există un $c \in A$ astfel încât $b = ac$.

### 2.1 Proprietățile divizibilității

Fie $A$ un domeniu și $a, b, c \in A$. Atunci:
1. $1|u|a|a|0 \ \ \forall u \in U(A)$
2. $a|b$ și $b|c \implies a|c$
3. $a|b$ și $a|c \implies a|b\alpha + c\beta \ \ \forall \alpha, \beta \in A$
4. $a|b \implies ac|bc$
5. $a|b$ și $b|a \iff \exists\ u \in U(A)$ astfel încât $a = bu$

**Observații**
1. Am notat cu $U(A)$ mulțimea elementelor inversabile ale lui $A$.

$$U(A) = \{u \in A | \exists\ v \in A \text{ a. î. } uv = 1\}$$

2. Când $a|b$ și $b|a$ spunem că $a$ și $b$ sunt *asociați* (elemente asociate în divizibilitate) și notăm $a \sim b$

## 3 Funcția normă

### 3.1 Norma pentru $\mathbb{Z}[\sqrt{d}]$

$$N : \mathbb{Z}[\sqrt{d}] \to \mathbb{N}, N(a + b\sqrt{d}) = |a^2 - b^2 d|$$

### 3.2 Norma pentru $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{\frac{a+b\sqrt{d}}{2}\middle| a,b \in \mathbb{Z}, a \equiv_2 b\right\}$

$$N : \mathbb{Z}\Big[\frac{1+\sqrt{d}}{2}\Big] \to \mathbb{N}, N\Big(\frac{a+b\sqrt{d}}{2}\Big) = \Big|\frac{a^2-b^2d}{4}\Big|$$

### 3.3 Norma pentru $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a + b\frac{1+\sqrt{d}}{2}\middle| a,b \in \mathbb{Z}\right\}$

$$N : \mathbb{Z}\Big[\frac{1+\sqrt{d}}{2}\Big] \to \mathbb{N}, N\Big(a+b\frac{1+\sqrt{d}}{2}\Big) = \Big|a^2+ab+b^2\frac{1-d}{4}\Big|$$

### 3.4 Proprietățile funcției normă

Fie $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{N}$ funcția normă. Atunci:
1. $N(zw) = N(z)N(w)\ \forall\ \ z,w \in \mathbb{Z}[\sqrt{d}]$
2. $z|w$ în $\mathbb{Z}[\sqrt{d}] \implies N(z)|N(w)$
3. $U(\mathbb{Z}[\sqrt{d}]) = \{z \in \mathbb{Z}[\sqrt{d}]|N(z) = 1\}$
4. Dacă $z|w$ în $\mathbb{Z}[\sqrt{d}]$ și $N(z) = N(w)$ atunci $z \sim w$

**Observație**. Se poate scrie un rezultat analog și pentru $N : \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \to \mathbb{N}$.

## 4 Exerciții

1. Calculați normele pentru fiecare dintre elementele de mai jos în inelele specificate:
a) $16 + i$ în $\mathbb{Z}[i]$
b) $10 + 2\sqrt{3}$ în $\mathbb{Z}[\sqrt{3}]$
c) $\frac{1+\sqrt{13}}{2}$ în $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$
d) $3 + \sqrt{5}$ în $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$
2. Verificați dacă $2 + 5i$ divide numerele $7 + 3i, 7 - 3i, 7 + i$ în $\mathbb{Z}[i]$.
3. Determinați divizorii lui $17 + 9i$ în $\mathbb{Z}[i]$.
4. Verificați dacă $2 + \sqrt{3}$ divide toate numerele în $\mathbb{Z}[\sqrt{3}]$.
5. Determinați câte un element inversabil diferit de $\pm1$ în inelele: $\mathbb{Z}[\sqrt{3}], \mathbb{Z}[\sqrt{5}], \mathbb{Z}[\sqrt{7}], \mathbb{Z}[\sqrt{11}]$.
6. Arătați că:
a) $2 - i$ divide $a + bi$ în $\mathbb{Z}[i] \iff 5$ divide $a + 2b$ în $\mathbb{Z}$
b) $2 + 3i$ divide $a + bi$ în $\mathbb{Z}[i] \iff 13$ divide $a + 8b$ în $\mathbb{Z}$

# Algebră III
# Tutoriatul 2

Benea Lorena Cezara
Ștefu Cristi-Ionuț

29 Octombrie 2021

## 1 Elemente ireductibile și elemente prime

Fie $A$ un domeniu și fie $\pi \in A$ un element nenul și neinversabil. Atunci:
a) $\pi$ este element **ireductibil** (sau **atom**) dacă nu se poate scrie ca un produs de două elemente neinversabile (echivalent: $\pi = ab \implies a \in U(A)$ sau $b \in U(A)$)
b) $\pi$ este element **prim** dacă $\pi | ab \implies \pi | a$ sau $\pi | b$.

## 2 Algoritm de verificare a primalității unui element în $\mathbb{Z}[\sqrt{d}]$

Fie $\pi = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.
**Dacă** $N(\pi)$ este număr prim **atunci**:

$\pi$ este element prim

**altfel**:

**dacă** $(a, b) = 1$ **atunci**:

$\pi$ NU este element prim

**altfel:**

**dacă** $N(\pi) = p^2,\ p$ este prim **atunci**:

**dacă** $\sqrt{\hat{d}} \notin \mathbb{Z}_p$ **atunci**:

$\pi$ este element prim

**altfel**:

$\pi$ NU este element prim

**altfel**:

$\pi$ NU este element prim

## 3 Observații importante

1. Un element prim este întotdeauna ireductibil, dar un element ireductibil poate fi și prim și neprim.
2. Pentru a verfica condiția $\sqrt{\hat{d}} \notin \mathbb{Z}_p$ din algoritmul de mai sus trebuie să verificăm dacă $\exists\ x \in \mathbb{Z}_p$ cu $x^2 = \hat{d}$. În acest caz, $\sqrt{\hat{d}} \in \mathbb{Z}_p$, iar dacă nu există $\sqrt{\hat{d}} \notin \mathbb{Z}_p$.
3. Pentru inelul $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ condiția $\sqrt{\hat{d}} \notin \mathbb{Z}_p$ se înlocuiește cu verificarea următoare: ecuația

$x^2 - x + \widehat{\frac{1-d}{4}} = \hat{0}$ are sau nu soluții. Cu această înlocuire, algoritmul funcționează și pentru $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

# 4 Exerciții

1. Arătați că în inelul $\mathbb{Z}[\sqrt{6}]$ elementele $1 - \sqrt{6}$ și $35 + 14\sqrt{6}$ sunt prime.
2. Arătați că în inelul $\mathbb{Z}[\sqrt{6}]$ elementul $70 + 20\sqrt{6}$ este reductibil.
3. Investigați dacă numărul 29 este prim în inelul $\mathbb{Z}[\sqrt{61}]$.
4. Arătați că în inelul $\mathbb{Z}\left[\frac{1+\sqrt{-15}}{2}\right]$:
a) 2 este atom neprim
b) $2 + \sqrt{-15}$ este element prim.
5. Verificați dacă în inelul $\mathbb{Z}[\sqrt{10}]$ numerele $2, 3, 7, 21 - 7\sqrt{10}, 3 - 2\sqrt{10}$ sunt elemente ireductibile sau prime.

Algebră III
Tutoriatul 3

Benea Lorena Cezara
Ștefu Cristi-Ionuț

5 Noiembrie 2021

# 1 Inele atomice

**Definiție** Fie $A$ un domeniu. Spunem că $A$ este inel atomic dacă orice element din $A$ care este nenul și neinversabil este produs de atomi.
**Teoremă** Inelele pătratice (i.e. $\mathbb{Z}[\sqrt{d}]$ și $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$) sunt inele atomice.

# 2 Condiție a lanțurilor de divizori (CLD)

**Definiție** Fie $A$ un domeniu. Spunem că $A$ verifică CLD dacă:

$$\forall\ b_1, b_2, \cdots, b_n \in\ A \text{ cu } b_1 \vdots\, b_2 \vdots \cdots b_n \implies \exists\ N \text{ a.î. } b_N \sim b_{N+1} \sim \cdots$$

**Teoremă** Orice inel pătratic verifică CLD.
**Teoremă** Dacă domeniul $A$ verifică CLD, atunci $A$ este atomic.

# 3 Inele factoriale

**Definiție** Un domeniu $A$ se numește inel factorial dacă $A$ este inel atomic și orice element din A care este nenul și neinversabil are o factorizare atomică unică până la ordine și asociați.
**Lemă** Un inel atomic cu toți atomii primi este inel factorial.

## 3.1 Teorema de caracterizare a inelelor factoriale

Pentru un domeniu $A$, următoarele afirmații sunt echivalente:
a) $A$ este inel factorial
b) Orice element din $A$ nenul și neinversabil este produs de elemente prime
c) $A$ este inel atomic cu toți atomii primi.
d) $A$ verifică CLD.

**Teoremă** $\mathbb{Z}[\sqrt{d}]$ inel factorial $\iff$ $\forall\, p \in \mathbb{Z}$ prim $\implies$ $p$ prim în $\mathbb{Z}[\sqrt{d}]$ sau $\exists\, z_0 \in \mathbb{Z}[\sqrt{d}]$ cu $N(z_0) = p$
**Observație** Dacă punem $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ în loc de $\mathbb{Z}[\sqrt{d}]$, teorema are loc.

## 3.2 Exemple uzuale de inele factoriale

$$\mathbb{Z}[i], \mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{-2}], \mathbb{Z}[\sqrt{3}], \mathbb{Z}[\sqrt{6}], \mathbb{Z}[\sqrt{7}], \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right], \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$$

## 3.3 Exemple uzuale de inele nefactoriale

$$\mathbb{Z}[\sqrt{-3}], \mathbb{Z}[\sqrt{-4}], \mathbb{Z}[\sqrt{-5}], \mathbb{Z}[\sqrt{-6}], \mathbb{Z}[\sqrt{-7}]$$

# 4 Exerciții

1. Sunt $6 = \sqrt{6}^2 = 2 \cdot 3$ factorizări atomice ale lui 6 în inelul $\mathbb{Z}[\sqrt{6}]$?
2. Găsiți o factorizare atomică a lui $335 - 117\sqrt{2}$ în inelul $\mathbb{Z}[\sqrt{2}]$.
3. Găsiți o factorizare atomică a lui 91 în inelul $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.
4. Arătați că inelul $\mathbb{Z}[\sqrt{26}]$ este nefactorial.
5. Arătați că inelul $\mathbb{Z}[\sqrt{82}]$ este nefactorial.
6. Arătați că în inelul $\mathbb{Z}[\sqrt{-7}]$ următoarele produse sunt factorizări atomice:

a) $2^5 = (5 + \sqrt{-7})(5 - \sqrt{-7})$
b) $2^6 = (1 + 3\sqrt{-7})(1 - 3\sqrt{-7})$
c) $2^7 = (11 + \sqrt{-7})(11 - \sqrt{-7})$

# Algebră III
# Tutoriatul 4

Benea Lorena Cezara
Ștefu Cristi-Ionuț

12 Noiembrie 2021

## 1 Cel mai mare divizor comun

**Definiție** Fie $A$ un domeniu. Fie $a, b, d \in A$. Spunem că $d$ este cel mai mare divizor comun al perechii $a, b$ și notăm $d = (a, b)$ dacă următoarele condiții sunt îndeplinite simultan:
a) $d|a, d|b$
b) dacă $f \in A, f|a, f|b$ rezultă că $f|d$

## 2 Cel mai mic multiplu comun

**Definiție** Fie $A$ un domeniu. Fie $a, b, m \in A$. Spunem că $m$ este cel mai mic multiplu comun al perechii $a, b$ și notăm $m = [a, b]$ dacă următoarele condiții sunt îndeplinite simultan:
a) $a|m, b|m$
b) dacă $g \in A, a|g, b|g$ rezultă că $m|g$

## 3 Câteva teoreme, propoziții și observații

**Propoziție** Dacă există $(a, b)$ este unic până la o asociere.
**Propoziție** Dacă există $[a, b]$ este unic până la o asociere.
**Teoremă** Într-un inel factorial $A$ oricare două elemente $a, b \in A$ au $(a, b)$ și $[a, b]$.
**Teoremă** Fie $A$ un domeniu și $a, b, c \in A \setminus \{0\}$. Atunci:
a) $(a, b) = d \iff (ac, bc) = dc$
b) $(a, b) = d \implies (\underbrace{\frac{a}{d}}_{\in A}, \underbrace{\frac{b}{d}}_{\in A}) = 1$ (relativ prime sau coprime)
c) $(a, b) = 1, (a, c) = 1 \implies (a, bc) = 1$
d) $a|bc, (a, b) = 1 \implies a|c$
e) $(a, b) = 1, a|c, b|c \implies ab|c$
**Observație** $(a, b)[a, b] = ab$

## 4 Exerciții

1. Fie $a = 779 - 247i$ și $b = 817 + 19i$. Calculați $(a, b)$ și $[a, b]$ în $\mathbb{Z}[i]$.
2. Arătați că în inelul $\mathbb{Z}[\sqrt{-17}]$:
a) $2 + \sqrt{-17}$ și 7 sunt coprime
b) $6 + 3\sqrt{-17}$ și 21 nu au un cel mai mare divizor comun
3. Arătați că în inelul $\mathbb{Z}[\sqrt{-5}]$ numerele $3 + 2\sqrt{-5}$ și $3 - 2\sqrt{-5}$ au un cel mai mic multiplu comun.
4. Calculați $(7 + \sqrt{-2}, 11 - 4\sqrt{-2})$ în $\mathbb{Z}[\sqrt{-2}]$.
5. Calculați $(-1 + 7i, 2 + 11i)$ în $\mathbb{Z}[i]$.

# ALGEBRĂ III

Tutoriatul 5

Bemea Lorena - Cezara

Ștefu Cristi - Ionuț

19 Noiembrie 2021

**DEFINIȚIE**

Un domeniu A se numește inel principal dacă toate idealele sale sunt principale.

$I \subseteq A$ se cheamă ideal dacă $\begin{cases} 0 \in I & \text{și} \\ I - I \subseteq I \\ A \cdot I \subseteq I \end{cases}$

$x \in A$, $Ax = \{ \lambda x \mid \lambda \in A \} = \langle x \rangle$ idealul principal generat de $x$.

**TEOREMĂ**

Orice inel principal este factorial.

**TEOREMĂ**

Fie A un inel factorial.

Atunci A principal $\Leftrightarrow$ $\forall$ 2 elemente prime $p, q \in A$ neasociate sunt comaximale.

**TEOREMĂ**

$\mathbb{Z}[\sqrt{d}]$ este inel factorial $\Leftrightarrow$ este inel principal.

**DEFINIȚIE**

A domeniu, $\alpha, \beta \in A$. Zicem că ele sunt comaximale dacă $\langle a, b \rangle = A$ echiv. $1 = \alpha \cdot \alpha' + \beta \cdot \beta'$.

## EXERCIȚII

1. Arătați că idealul $\langle 2, \sqrt{6} \rangle$ din $\mathbb{Z}[\sqrt{6}]$ este principal.

2. Arătați că idealul $\langle 2, \sqrt{-6} \rangle$ din $\mathbb{Z}[\sqrt{-6}]$ nu este principal.

3. Arătați că numerele $2-\sqrt{7}$ și $3+4\sqrt{7}$ sunt comaximale în $\mathbb{Z}[\sqrt{7}]$.

4. Fie numerele

   $a = 18 + 36\sqrt{-2}$ și $b = 8 + 3\sqrt{-2}$.

   Găsiți $q \in \mathbb{Z}[\sqrt{-2}]$ cu $N(a-bq) < N(b)$.

# Algebră III
# Tutoriatul 6

Benea Lorena Cezara
Ștefu Cristi-Ionuț

24 Noiembrie 2021

## 1 Inel euclidian

**Definiție** Un domeniu $A$ se numește $\varphi-$ inel euclidian dacă $\exists$ o funcție $\varphi : A \setminus \{0\} \to \mathbb{N}$ cu proprietatea $\forall\ a, b \in A, b \neq 0\ \exists\ q, r \in A$ astfel încât $a = bq + r$, unde $r = 0$ sau $r \neq 0$ (în acest caz $\varphi(r) < \varphi(b)$).

## 2 Câteva teoreme și observații

**Observație** În cazul inelelor pătratice ($\mathbb{Z}[\sqrt{d}], \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$) un candidat "natural" pentru $\varphi$ este norma $N$.
**Teoremă** $\mathbb{Z}[\sqrt{d}]$ norm-euclidian $\Longleftrightarrow \forall\ \alpha \in \mathbb{Q}[\sqrt{d}]\ \exists\ q \in \mathbb{Z}[\sqrt{d}]$ cu $N(\alpha - q) < 1$.
**Teoremă** Pentru $d < 0,\ \mathbb{Z}[\sqrt{d}]$ este norm-euclidian $\Longleftrightarrow d = -1$ sau $d = -2$. ($\mathbb{Z}[i],\ \mathbb{Z}[\sqrt{-2}]$)
**Teoremă** Pentru $d < 0, d \equiv_4 1,\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ este norm-euclidian $\Longleftrightarrow d = -3, -7$ sau $-11$.
**Teormă (Chatland-Davenport 1950)**

- $\mathbb{Z}[\sqrt{d}]$ cu $d > 0$ este norm-euclidian $\Longleftrightarrow d \in \{2, 3, 6, 7, 11, 19\}$.
- $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ cu $d > 0$ este norm-euclidian $\Longleftrightarrow d \in \{5, 13, 17, 21, 29, 33, 37, 41, 57, 73\}$.

## 3 Algoritmul lui Euclid

**Input:** $(A, \varphi)$ inel euclidian. $a_0, b_0 \in A$.
**Output:** $d = (a_0, b_0)$

```
a := a_0; b := b_0; d := a;
while b ≠ 0 :
{
    r = a − bq cu r = 0 sau φ(r) < φ(b)
    a := b; b := r;
}
d := a;
```

## 4 Exerciții

1. Fie $a_0 = 43 - 81i,\ b_0 = 33 - 19i$. Calculați $(a_0, b_0)$ în $\mathbb{Z}[i]$ folosind algoritmul lui Euclid. La fiecare parcurgere a buclei "while" scrieți elementele $a, b, r$ sub formă de combinații liniare de $a_0$ și $b_0$.
2. Fie $A$ un domeniu și $a, a', b, b', c \in A$ cu proprietatea $aa' + bb' = 1$. Rezolvați ecuația $ax + by = c$.
3. Rezolvați ecuația $(43 - 81i)x + (33 - 19i)y = 27 - 5i$ în $\mathbb{Z}[i]$.
4. Calculați $(11 + 15\sqrt{2},\ 3 + 13\sqrt{2})$ în $\mathbb{Z}[\sqrt{2}]$ folosind algoritmul lui Euclid.
5. În $\mathbb{Z}[\sqrt{2}]$, rezolvați ecuația $(11 + 15\sqrt{2})x + (3 + 13\sqrt{2})y = 5 - 3\sqrt{2}$.
6. Completați tabelul următor cu (nouă) numere din $\mathbb{Z}[\sqrt{-2}]$ astfel încât produsele pe orizontală/ verticală să fie numerele indicate

| | $29 - 5\sqrt{-2}$ | $6 + 15\sqrt{-2}$ | $-4 + 17\sqrt{-2}$ |
|---|---|---|---|
| $-9 + 9\sqrt{-2}$ | | | |
| $47 + 23\sqrt{-2}$ | | | |
| $18$ | | | |

# Algebră III
# Tutoriatul 7

Benea Lorena Cezara
Ștefu Cristi-Ionuț

8 Decembrie 2021

## 1 Definiții

**1.1** Fie $A$ un domeniu și $p \in A$ nenul și neinversabil. $p$ se zice **element prim** dacă:
$ab \in pA \implies a \in pA$ sau $b \in pA$
$a, b \in A$
**1.2** Fie $A$ un inel și $P$ un ideal $\neq A$. $P$ se zice **ideal prim** dacă:
$ab \in P \implies a \in P$ sau $b \in P$
$a, b \in A$
**1.3** Fie $S$ un inel și $M$ un ideal al lui $A$. Idealul $M$ se zice **ideal maximal** dacă $M \neq A$ și $\nexists$ ideal $M \subset I \subset A$.

## 2 Câteva teoreme, observații și corolare

**Observație** Pentru $A$ domeniu, $p \in A \setminus \{0\}$, avem: $p$ element prim $\iff pA$ ideal prim.
**Teoremă (Lema lui Krull)** În orice inel există cel puțin un ideal maximal.
**Teoremă** Fie $A$ un ideal și $M$ un ideal propriu al lui $A$. Atunci:
i) $M$ ideal prim $\iff A/M$ domeniu.
ii) $M$ ideal maximal $\iff A/M$ corp.
**Corolar 1** Orice ideal maiximal este prim.
**Corolar 2** $\{0\}$ maximal $\iff A$ corp.
$\{0\}$ ideal prim (în $A$) $\iff A$ domeniu.
**Teoremă** Dacă $A$ este un inel principal care nu e corp $\implies$ idealele prime ale lui $A$ sunt:
- $\{0\}$ − nemaximal.
- $pA$, $p$ element prim $\leftarrow$ maximale.

**Teoremă** Idealele prime nenule din $\mathbb{Z}[\sqrt{d}]$ sunt:
- $< p >$ unde $p \in \mathbb{N}$ prim cu $p \nmid x^2 - d \ \forall\ x \in \mathbb{Z}$

sau
- $< p, a - \sqrt{d} >$ unde $p \in \mathbb{N}$ prim cu $p \mid a^2 - d$.

(Sunt de fapt ideale maximale)

## 3 Exerciții

1. Verificați dacă următoarele ideale din $\mathbb{Z}[\sqrt{79}]$ sunt prime:

$$< 11 >,\ < 13 >,\ < 3 + \sqrt{79} >,\ < 6 + \sqrt{79} >,\ < 80 + 9\sqrt{79} > .$$

2. Verificați dacă următoarele ideale din $\mathbb{Z}[\sqrt{79}]$ sunt prime:

$$< 13, 1 + \sqrt{79} >,\ < 7, 3 + \sqrt{79} >,\ < 3, 17 + 2\sqrt{79} >,\ < 7, 1 + \sqrt{79} > .$$

3. Arătați că în $\mathbb{Z}[\sqrt{-6}]$ avem egalitățile:

$$< 5, 2+\sqrt{-6} >= \{5x + 2y + y\sqrt{-6} \mid x, y \in \mathbb{Z}\}$$

și

$$< 11, 4-\sqrt{-6} >= \{11x + 7y + y\sqrt{-6} \mid x, y \in \mathbb{Z}\}$$

4. Arătați că în $\mathbb{Z}[\sqrt{-6}]$ idealul $< 7+\sqrt{-6} >$ este intersecția idealelor prime $< 5, 2+\sqrt{-6} >$ și $< 11, 4-\sqrt{-6} >$.

5. Verificați dacă $\{21x + (11-\sqrt{2})y \mid x, y \in \mathbb{Z}\}$ este ideal în $\mathbb{Z}[\sqrt{2}]$.

# Algebră III
# Tutoriatul 8

Benea Lorena Cezara
Ștefu Cristi-Ionuț

10 Decembrie 2021

## 1 Definiție

$f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$, $A$ factorial.
• Numim conținutul lui $f$ (notat $Cont(f)$)

$$Cont(f) = (a_0, a_1, \ldots, a_n)$$

•$f$ primitiv dacă $Cont(f) = 1$. $\Longleftrightarrow \nexists\ p \in A$ cu $p \mid f$ element prim.

## 2 Teoreme, corolare, propoziții

**Teoremă (Gauss)** $A$ inel factorial $\implies A[x]$ factorial.
**Lemă** Dacă $A$ domeniu și $p \in A$ element prim, atunci $p$ prim și în $A[x]$.
**Teoremă (Lema lui Gauss)** Fie $A$ inel factorial și $f, g \in A[x] \setminus \{0\}$. Atunci:
1) $f \cdot g$ primitiv $\Longleftrightarrow f$ și $g$ sunt primitive.
2) $Cont(f \cdot g) \sim Cont(f) \cdot Cont(g)$
**Propoziție** Fie $A$ inel factorial cu $c.f.(A) = K$ unde $c.f.$ = corpul de fracții și fie $f \in A[x]$ reductibil în $K[x]$. Atunci $f = g \cdot h$ cu $g, h \in A[x]$ de grad $\geq 1$.
**Corolar** Fie $A$ inel factorial și $f \in A[x] \setminus \{0\}$. Atunci $f$ primitiv (în $A[x]$) și ireductibil în $K[x] \Longleftrightarrow f$ element prim în $A[x]$.
**Teoremă (Criteriul lui Eisenstein)**
Fie $A$ inel factorial, $K = c.f.(A)$ și $f = a_nx^n + a_{n-1}x^{x-1} + \cdots + a_1x + a_0 \in A[x]$.
Presupunem că $\exists\ p \in A$ element prim cu:
1)$p \nmid a_n$
2)$p \mid a_{n-1}, a_{n-2}, \ldots, a_1, a_0$
3)$p^2 \nmid a_0$
Atunci $f$ este ireductibil în $K[x]$. ($f$ se zice $p$-Eisenstein)
**Teoremă (Criteriul reducerii)**
Fie $A$ inel factorial, $K = c.f.(A)$, $p \in A$ element prim, $f = a_nx^n + \cdots + a_1x + a_0 \in A[x]$. Notăm $\hat{b} \in A/pA$ pentru $b \in A$. Dacă $\hat{a}_nx^n + \cdots + \hat{a}_1x + \hat{a}_0 \in (A/pA)[x]$ are $\hat{a}_n \neq \hat{0}$ și este ireductibil în $A/pA[x]$ atunci $f$ este ireductibil în $K[x]$.

## 3 Exerciții

1. Calculați conținutul polinomului $(3+i)X^3 + (7+i)X - 10 \in \mathbb{Z}[i][X]$.
2. Arătați că $33X^6 + 84X^5 - 273X^3 + 147X^2 + 168$ ireductibil în $\mathbb{Q}[X]$.
3. Arătați că $3X^5 + 2X^4 - 5X^3 - 4X^2 + 7$ este ireductibil în $\mathbb{Q}[X]$ reducându-l mod 2.
4. Fie polinomul

$$w = 3X^7 + 1067X^6 + 1261X^5 + 1358X^4 + 1455X^3 + 1649X^2 + 1843X + 2037$$

a) Arătați că $w$ este ireductibil în $\mathbb{Q}[X]$ folosind Criteriul lui Eisenstein.
b) Arătați că $w$ este ireductibil în $\mathbb{Q}[X]$ reducându-l mod 2.
5. Factorizați polinoamele $(3+i)X^4 - (3+i)$ și $(5-i)X^6 - (5-i)$ în $\mathbb{Z}[i][X]$ și calculați cmmdc al lor.

# Tutoriat (A+T)

**Def**: $R$ - inel unitar, commutativ, $(M,+)$ grup abelian. Spunem că $(M,+)$ este $R$-modul însoțit de o operație externă $\cdot : R \times M \to M$ $((r,m) \mapsto r \cdot m)$ dacă:

1) $(a+b)\cdot m = a\cdot m + b\cdot m$, $\forall a,b \in R, m \in M$
2) $a(m+m') = a\cdot m + a\cdot m'$, $\forall a \in R, m, m' \in M$
3) $\underbrace{(ab)}_{\in R}\cdot \underbrace{m}_{\in M} = \underbrace{a}_{\in R}\cdot \underbrace{(\underbrace{b}_{\in R}\cdot \underbrace{m}_{\in M})}_{\in M} \in M$, $\forall a,b \in R, m \in M$
4) $\underbrace{1}_{\in R}\cdot m = m$, $\forall m \in M$

**Ex 1** $(M,+)$ grup abelian are o struct. de $\mathbb{Z}_n$ modul $\Leftrightarrow$

$\Leftrightarrow n\cdot x = 0$ $\forall x \in M$, $n \in \mathbb{Z}$ $(n\cdot x = \underbrace{x + \ldots + x}_{n \text{ ori}})$

"$\Rightarrow$" $\cdot : \mathbb{Z}_n \times M \to M$ $\qquad (0_{\mathbb{Z}_n} \cdot x = 0_M \ \forall x \in M)$

$$\underbrace{\hat{n}}_{\in \mathbb{Z}_n} \cdot x = \hat{0} \cdot x = 0_M \qquad \hat{n} = \hat{0}$$

$$\hat{n} \cdot x = 0 =$$

$$\hat{0} = \hat{n} = \underbrace{\hat{1} + \hat{1} + \dots + \hat{1}}_{n \text{ ori}}$$

$$\hat{n} \cdot x = (\underbrace{\hat{1} + \hat{1} + \dots + \hat{1}}_{n \text{ ori}}) \cdot x \overset{1)}{=} \underbrace{\hat{1} \cdot x + \hat{1} \cdot x + \dots + \hat{1} \cdot x}_{n \text{ ori}} = \underbrace{x + x + \dots + x}_{n \text{ ori}} = nx$$

"$\Leftarrow$" $nx = 0 \quad \forall x \in M, n \in \mathbb{Z}$

vrem ca $(M, +)$ $\mathbb{Z}_n$ modul

$(M,+)$ grup abelian $\Rightarrow$ $(M,+)$ $\mathbb{Z}$ modul. $\qquad \cdot : \mathbb{Z} \times M \to M$

$$\underbrace{k}_{\in \mathbb{Z}} \cdot \underbrace{m}_{\in M} = \begin{cases} \underbrace{m + \dots + m}_{k \text{ ori}}, & k > 0 \\ 0, & k = 0 \\ -[(-k) \cdot m], & k < 0 \end{cases} \qquad k \cdot m \in M \quad (M\ \mathbb{Z} \text{ modul})$$

$$\parallel$$

$$-(\underbrace{m + \dots + m}_{})$$

$$-(\underbrace{m+\dots+m}_{-k\text{ ori},\ >0})$$

Vrem să def. $* : \mathbb{Z}_n \times M \longrightarrow M$

bine definită

$\underset{\in \mathbb{Z}_n}{\hat{k}} * \underset{\in M}{m} =: k \cdot m \in M$

Dacă avem $\hat{k} = \hat{l} \overset{?}{\Rightarrow} \hat{k} * m = \hat{l} * m$

$\hat{k} = \hat{l} \Leftrightarrow \widehat{k-l} = \hat{0}$ (în $\mathbb{Z}_n$) $\Leftrightarrow \exists p$ a.î. $k-l = \underbrace{n \cdot p}_{0}$ (dn ip.)

$\Rightarrow k-l=0 \Rightarrow k=l \Rightarrow k \cdot m = l \cdot m \Rightarrow \hat{k} * m = \hat{l} * m$

Contraexemplu fct. care nu e bine def.

$\varphi : \mathbb{Z}_7 \to \mathbb{Z}$

$\varphi(\hat{x}) = x$

$\varphi(\hat{0}) = 0$

$\varphi(\hat{7}) = 7$ $\Big]$ $\not\Leftrightarrow$

$\varphi(\hat{0})$

$(M, +, *)$ $\mathbb{Z}_n$ modul:

1) $\widehat{(a+b)} * m \overset{\text{def. } *}{=} (a+b) \cdot m \overset{\mathbb{Z}\text{ modul}}{=} a \cdot m + b \cdot m \overset{\text{def. } *}{=} \hat{a} * m + \hat{b} * m$ ✓

2) $\hat{a} * (m+m') = a \cdot (m+m') = a \cdot m + a m' = \hat{a} * m + \hat{a} * m'$ ✓

3) $\widehat{(ab)} * m = (ab) \cdot m = a \cdot (b \cdot m) = a \cdot (\hat{b} * m) = \hat{a} * (\hat{b} * m)$ ✓

4) $\hat{1} * m = 1 \cdot m = m$ ✓

$\Rightarrow (M, +, \cdot)$ $\mathbb{Z}_n$ modul

**Def**: $M, M'$ $R$-module, $f: M \to M'$ sn. morfism de module dacă:

1) $f$ morfism de grupuri $f(x+y) = f(x) + f(y)$

2) $f(\underbrace{a}_{\in R} \cdot \underbrace{x}_{\in M}) = \underbrace{a}_{\in R} \cdot \underbrace{f(x)}_{\in M'}$

$\boxed{Ex\ 2}$ $(M, +)$ grup abelian, $\mathbb{Z}[i]$ modul $\Leftrightarrow \exists\, \varphi: M \to M$ morf. de grupuri cu $\varphi^2 = -id_M$

"$\Rightarrow$" $M$ $\mathbb{Z}[i]$ modul

$\cdot : \mathbb{Z}[i] \times M \to M$

$z = a + bi \in \mathbb{Z}[i]$ $(a, b \in \mathbb{Z})$

$$\underbrace{a}_{\in\mathbb{Z}[i]}+\underbrace{bi}_{\in\mathbb{Z}[i]}\,)\cdot \underbrace{x}_{\in M} = a\cdot x + \underbrace{(bi)\cdot x}_{} \overset{def_{4)}}{=} a\cdot x + b\cdot(i\cdot x)$$

$$\cdot\ a\cdot x = (\underbrace{1+1+\dots+1}_{a})\cdot x = \underbrace{(1\cdot x)+\dots+(1\cdot x)}_{a} = \underbrace{x+\dots+x}_{a}$$

$$\cdot\ b\cdot(i\cdot x) = \underbrace{(i\cdot x)+\dots+(i\cdot x)}_{b \text{ ori}}$$

Definim $\varphi : M \to M$ ai $\varphi(x) = i\cdot x$

$\cdot$ $\varphi$ morf de grupuri ( $\varphi(x+y) = i\cdot(x+y) = i\cdot x + i\cdot y$ ) $\checkmark$

$\cdot\ \varphi(\underbrace{a}_{\in\mathbb{Z}[i]}\cdot x) = i\cdot(a\cdot x) = a\cdot(i\cdot x)$ $\checkmark$

$\Rightarrow$ $\varphi$ morf. de module

$$(\varphi\circ\varphi)(x) = \varphi(\varphi(x)) = \varphi(i\cdot x) = i\cdot(i\cdot x) = \underbrace{(i\cdot i)}_{=i^2=-1}\cdot x = -1\cdot x = -x \quad \forall x\in M$$

$$\Rightarrow \varphi^2 = -id_M$$

"$\Leftarrow$" Fie $\varphi : M \to M$ morfism de module a.î. $\varphi^2 = -id_M$

$(M,+)$ grup abelian $\Rightarrow$ $\mathbb{Z}$ modul

$\cdot : \mathbb{Z} \times M \to M$ (produsul de scalari)

$\Rightarrow \exists\ k \cdot y$, $k \in \mathbb{Z}$, $y \in M$

Extindem "$\cdot$" pt. $\mathbb{Z}[i]$ la un produs $* : \mathbb{Z}[i] \times M \to M$

$z = a + bi$

$$z * m = (a+bi) * m \overset{def.}{=} a \cdot m + b \cdot \varphi(m)$$

$(M, +, *)$ $\mathbb{Z}[i]$ modul:

1) $$[\underbrace{(a+bi)+(c+di)}_{=(a+c)+(b+d)i}] * m \overset{def.}{=} (a+c)\cdot m + (b+d)\cdot\varphi(m)$$

$$= \underbrace{a \cdot m + b \cdot \varphi(m)}_{=(a+bi)*m} + \underbrace{c \cdot m + d \cdot \varphi(m)}_{(c+di)*m}$$

$$= (a+bi) * m + (c+di) * m$$

2) $\underbrace{(a+bi)*(\underbrace{m+m'}_{p})}$ $\overset{?}{=}$ $(a+bi)*m + (a+bi)*m'$

$= (a+bi)*p = a\cdot p + b\cdot\varphi(p) = a\cdot(m+m') + b\cdot \underbrace{\varphi(m+m')}_{=\varphi(m)+\varphi(m')}$

$= a\cdot m + a\cdot m' + b\cdot\varphi(m) + b\cdot\varphi(m')$

$= [a\cdot m + b\cdot\varphi(m)] + [a\cdot m' + b\cdot\varphi(m')]$

$= (a+bi)*m + (a+bi)*m'$ ✓

3) $(ab)*m = a*(b*m)$ , $a = a_1+a_2 i$ , $b = b_1+b_2 i$ $a_1, a_2, b_1, b_2 \in \mathbb{Z}$.

$[(a_1+a_2 i)(b_1+b_2 i)]*m = (\underbrace{a_1b_1 - a_2b_2} + \underbrace{(a_1b_2+a_2b_1)}i)*m$

$= (a_1b_1 - a_2b_2)\cdot m + (a_1b_2+a_2b_1)\cdot\varphi(m)$

$= (a_1b_1)m - (a_2b_2)\cdot m + (a_1b_2)\varphi(m) + (a_2b_1)\varphi(m)$

$\overset{?}{=} (a_1+a_2 i)*[(b_1+b_2 i)*m]$

$= \ldots$

4) $1*m = (\underbrace{1+0\cdot i}_{\in\mathbb{Z}[i]})*m = 1\cdot m + \underbrace{0\cdot\varphi(m)}_{0} = 1\cdot m = m$.

# Algebră III
# Tutoriatul 10

Benea Lorena Cezara
Ștefu Cristi-Ionuț

7 Ianuarie 2022

## 1 Exerciții

1. Verificați dacă $4 + 10\sqrt{38}$ se divide cu $6 - \sqrt{38}$ în inelul $\mathbb{Z}[\sqrt{38}]$.
2. Găsiți o factorizare atomică a lui $5 + 3\sqrt{-5}$ în inelul $\mathbb{Z}[\sqrt{-5}]$ argumentând că factorii sunt într-adevăr atomi (nu uitați că un atom $x$ are factorizarea $x = x$).
3. Verificați dacă numărul 29 este prim în inelul $\mathbb{Z}[\sqrt{61}]$.
4. Găsiți factorizarea atomică a lui $8 + 12i$ în inelul $\mathbb{Z}[i]$ argumentând că factorii sunt într-adevăr elemente prime.
5. Fie numerele

$$a = 18 + 36\sqrt{-2} \text{ și } b = 8 + 3\sqrt{-2}.$$

Găsiți $q \in \mathbb{Z}[\sqrt{-2}]$ cu $N(a - bq) < N(b)$.

6. Fie polinomul

$$f = 9 + 4X + 3X^2 + 5X^3 + 4X^4 + 3X^5.$$

Modificați cel mult doi coeficienți ai lui $f$ pentru a obține un polinom ireductibil peste $\mathbb{Q}$ de gradul 5 (justificați ireductibilitatea).

7. Calculați

$$\text{cmmdc } (15 + 38i, 9 + 4i)$$

în inelul $\mathbb{Z}[i]$.