Alg S2
pag 1.

Algebră Seminar 2.

$U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$

$U(\mathbb{Z}) = \{\pm 1\}$

$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$

$U(\mathbb{Z}[\sqrt{2}]) = \{\pm (1+\sqrt{2})^m \mid m \in \mathbb{Z}\}$

Notez cu $u = 1+\sqrt{2}$ e un element inversabil $|1+\sqrt{2}| = 1$.

$R = \mathbb{Z}[\sqrt{2}]$

Iau $W = \{a + b\sqrt{2} \in U(R) \mid a, b \in \mathbb{N}\}$

Mă uit la $x \cdot u^{-m}$, $x \in W$ $(u^{-1} \in R \Rightarrow u^{-m} \in R)$

Notez $x \cdot u^{-m} = c + d\sqrt{2} > 0$ (o alegere)

1. $cd > 0 \Rightarrow c, d > 0 \Rightarrow x \cdot u^{-m} \in W$

$x \in W \Rightarrow \exists\, m \in \mathbb{N}$ a.î. $x \in [u^m, u^{m+1})$

$x \cdot u^{-m} \in W \Rightarrow x \cdot u^{-m} \geq 1+\sqrt{2} = u \overset{\cdot u^m}{\Rightarrow} x \geq u^{m+1}$ ↯

2. $cd < 0 \Rightarrow \underbrace{x \cdot u^{-m}}_{\in U(R)} = c + d\sqrt{2} = \dfrac{c^2 - 2d^2}{c - d\sqrt{2}}$

Obs $x \cdot u^{-m}$ este el. inversabil $\Rightarrow |x \cdot u^{-m}| = 1$

$\exists\, y \in R$ a.î. $(x \cdot u^{-m}) \cdot y = 1 \Rightarrow |(x \cdot u^{-m}) \cdot y| = |\underbrace{x \cdot u^{-m}}_{\in \mathbb{N}}| \cdot \underbrace{|y|}_{\in \mathbb{N}} = 1 \Rightarrow |u^{-m} \cdot x| = 1$

$|x \cdot u^{-m}| = 1 \Rightarrow |c + d\sqrt{2}| = 1 \Rightarrow |(c + d\sqrt{2})(c - d\sqrt{2})| = 1 \Rightarrow |c^2 - d^2 2| = 1 \Rightarrow c^2 - d^2 2 = \pm 1$ (*)

$x \cdot u^{-m} = \dfrac{c^2 - 2d^2}{c - d\sqrt{2}} \overset{(*)}{=} \dfrac{1}{|c| + |d|\sqrt{2}} \leq \dfrac{1}{u} \Rightarrow x \cdot u^{-m} \leq \dfrac{1}{u} \Rightarrow x \leq u^{m-1}$ ↯

3. $c \cdot d = 0$. $c \neq 0$ $d = 0 \Rightarrow$

$\Rightarrow \underbrace{x \cdot u^{-m}}_{\in U(R)} = c \Rightarrow x \cdot u^{-m} = 1 \Rightarrow x = u^m \Rightarrow$ orice element inversabil este o putere de $1+\sqrt{2}$

$U(\mathbb{Z}[\sqrt{2}]) = \{\pm (1+\sqrt{2})^m \mid m \in \mathbb{Z}\}$

$U(\mathbb{Z}[\sqrt{3}]) = ?$

$\sqrt{3} = \boxed{1} + (\sqrt{3} - 1)$

$\dfrac{1}{\sqrt{3}-1} = \dfrac{\sqrt{3}+1}{2} = 1 + \left(\dfrac{\sqrt{3}+1}{2} - 1\right) = \boxed{1} + \dfrac{\sqrt{3}-1}{2}$

$\dfrac{2}{\sqrt{3}-1} = \dfrac{2(\sqrt{3}+1)}{2} = \sqrt{3}+1 = 2 + (\sqrt{3}+1-2) = \boxed{2} + (\sqrt{3}-1)$ STOP

mă opresc dacă o parte fracțională se repetă.

$\sqrt{3} = (1; \overline{1; \cancel{2}})$ primul întreg se pune normal, iar ce urmează devine perioadă

ultimul din perioadă se taie

$1 + \dfrac{1}{1} = 2 \rightsquigarrow 2 + 1 \cdot \sqrt{3}$

$2+\sqrt{3}$ unitate fundamentală.

$U(\mathbb{Z}[\sqrt{3}]) = \{\pm (2+\sqrt{3})^m \mid m \in \mathbb{Z}\}$

$(1; 1, 2, 3, \cancel{4})$ → Metoda fracțiilor continue.

$$1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3}}}$$

Ex2) $U(\mathbb{Z}[\sqrt{29}]) = ?$

$$\sqrt{29} = 5 + (\sqrt{29} - 5)$$

$$\frac{1}{\sqrt{29}-5} = \frac{\sqrt{29}+5}{4} = 2 + \left(\frac{\sqrt{29}+5}{4} - 2\right) = 2 + \left(\frac{\sqrt{29}-3}{4}\right)$$

$$\frac{4}{\sqrt{29}-3} = \frac{4(\sqrt{29}+3)}{20} = \frac{\sqrt{29}+3}{5} = 1 + \left(\frac{\sqrt{29}+3}{5} - 1\right) = 1 + \left(\frac{\sqrt{29}-2}{5}\right)$$

$$\frac{5}{\sqrt{29}-2} = \frac{5(\sqrt{29}+2)}{25} = \frac{\sqrt{29}+2}{5} = 1 + \left(\frac{\sqrt{29}+2}{5} - 1\right) = 1 + \left(\frac{\sqrt{29}-3}{5}\right)$$

$$\frac{5}{\sqrt{29}-3} = \frac{5(\sqrt{29}+3)}{20} = \frac{\sqrt{29}+3}{4} = 2 + \left(\frac{\sqrt{29}+3}{4} - 2\right) = 2 + \left(\frac{\sqrt{29}-5}{4}\right)$$

$$\frac{4}{\sqrt{29}-5} = \frac{4(\sqrt{29}+5)}{4} = \sqrt{29}+5 = 10 + (\sqrt{29}-5) \to \text{STOP}.$$

$$\sqrt{29} = (5; \underbrace{2, 1, 1, 2, 1\cancel{0}}_{\text{perioada}})$$

$$5 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}} = 5 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{2}{3}}} = 5 + \cfrac{1}{2 + \cfrac{3}{5}} = 5 + \frac{5}{13} =$$

$$= \frac{70}{13} \rightsquigarrow 70 + 13\cdot\sqrt{29}$$

$$U(\mathbb{Z}[\sqrt{29}]) = \{\pm (70 + 13\cdot\sqrt{29})^n \mid n \in \mathbb{Z}\} \qquad 70^2 + 29\cdot 13^2 = \pm 1$$

$169 \cdot 29$: 1521, 338, 4901

A determina elementele inversabile din $\mathbb{Z}[\sqrt{29}]$ e tot una cu a găsi soluțiile ecuației $x^2 - 29y^2 = \pm 1$.

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

A determina elem. inversabile din $\mathbb{Z}[\sqrt{d}] \Leftrightarrow$ a găsi soluțiile ec. $x^2 - dy^2 = \pm 1$.

C. Idealele lui C?

R = un corp comutativ

Fie I un ideal. $\{0\} \neq I \subseteq R$. *

Fie $0 \neq x \in I \Rightarrow x \in R \underset{R\ corp}{\Rightarrow} x^{-1} \in R \Rightarrow \underbrace{x^{-1}}_{\in R} \cdot \underbrace{x}_{\in I} \in I \Rightarrow 1 \in I \Rightarrow \forall r \in R\ \ r = r \cdot 1 \in I$

$\Rightarrow R \subseteq I \overset{*}{\Rightarrow} R = I$.

Morala: Singurele ideale într-un corp comutativ sunt $\{0\}, R$.

$\boxed{1 \in I \Rightarrow I = R}$

Idealele din $(\mathbb{Z}, +, \cdot)$

Orice subgrup al lui $(\mathbb{Z}, +, \cdot)$ e de forma $m\mathbb{Z}$, $m \in \mathbb{N}$ și acestea sunt chiar idealele lui $(\mathbb{Z}, +, \cdot)$

Fie $a, b \in m\mathbb{Z} \Rightarrow \begin{array}{l} a = ma_1 \\ b = mb_1 \end{array}$ $\begin{array}{l} b_1, a_1 \in \mathbb{Z} \\ m \in \mathbb{N} \end{array} \Rightarrow$

$\Rightarrow a - b = ma_1 - mb_1 = m(\underbrace{a_1 - b_1}_{\in \mathbb{Z}}) \in m\mathbb{Z}$,

Fie $\left.\begin{array}{l} a \in m\mathbb{Z} \\ r \in \mathbb{Z} \end{array}\right\} \Rightarrow a = ma_1$

$ra = a \cdot r = (m \cdot a_1) \cdot r = m(a_1 \cdot r) \in m\mathbb{Z}$

$(\mathbb{Z}, +, \cdot)$ inel comutativ

$\Rightarrow m\mathbb{Z}$ sunt ideale ale lui $(\mathbb{Z}, +, \cdot)$

Idealele lui $(\mathbb{Z}_m, +, \cdot)$

Subgrupurile lui $(\mathbb{Z}_m, +, \cdot)$ sunt de forma $d\mathbb{Z}_m$ cu d/m și acestea sunt chiar idealele lui $(\mathbb{Z}_m, +, \cdot)$

Fie $\bar{a}, \bar{b} \in d\mathbb{Z}_m$ $\quad \bar{a} = d \cdot \bar{a_1}$ $\quad \bar{b} = d \cdot \bar{b_1}$

$\bar{a} - \bar{b} = d \cdot \bar{a_1} - d \cdot \bar{b_1} = d(\bar{a_1} - \bar{b_1}) = d(\underbrace{\overline{a_1 - b_1}}_{\in \mathbb{Z}_m}) \in d\mathbb{Z}_m$ (1)

Fie $\bar{r} \in \mathbb{Z}_m \Rightarrow a \cdot r = r \cdot a \in d\mathbb{Z}_m$ $\quad \bar{a} = d \cdot \bar{a_1}$ $\quad (\mathbb{Z}_m, +, \cdot)$ comutativ (3)

$\bar{r} \cdot (d \cdot \bar{a_1}) = d \cdot \bar{r} \cdot \bar{a_1} = d(\underbrace{\overline{r \cdot a_1}}_{\in \mathbb{Z}_m}) \in d\mathbb{Z}_m$ (2)

Din (1) și (2) $\overset{(3)}{\Rightarrow}$ $d\mathbb{Z}_m$ este ideal al lui $(\mathbb{Z}_m, +, \cdot)$

Alg S2
pag 4

Problema:

1) Fie $I = 20\mathbb{Z}$ $J = 36\mathbb{Z}$. Găsiți $I \cap J$, $I + J$, $I \cdot J$.

Propoziție: I, J, ideale în R, R = inel.

1) $I \cap J$ este ideal în R

2) $I + J = \{ i + j \mid i \in I, j \in J \}$ ideal în R

3) $I \cdot J = \{ \sum_{i=1}^{m} x_i \cdot y_i \mid x_i \in I, y_i \in J \quad m \in \mathbb{N} \} = (xy \mid x \in I, y \in J)$

$I = a\mathbb{Z}$ $J = b\mathbb{Z}$

$a\mathbb{Z} \cap b\mathbb{Z} = \underbrace{[a,b]\mathbb{Z}}_{\text{cmmmc}(a,b)\mathbb{Z}}$ $\qquad a\mathbb{Z} \cdot b\mathbb{Z} = ab\mathbb{Z}$

$a\mathbb{Z} + b\mathbb{Z} = \underbrace{(a,b)\mathbb{Z}}_{\text{cmmdc}(a,b)\mathbb{Z}}$

$I \cap J = [20, 36]\mathbb{Z} = 180\mathbb{Z}$

$I + J = (20, 36)\mathbb{Z} = 4\mathbb{Z}$

$I \cdot J = 20 \cdot 36\mathbb{Z} = 720\mathbb{Z}$

Elemente speciale în inele

1) inversabile ✓ $\qquad U(R)$

2) divizorii lui 0 ✓ $\qquad D(R)$

(x se numește divizor al lui 0 dacă $\exists y \neq 0, y \in R$ a.î. $x \cdot y = 0$)

3) idempotenți $\qquad Idem(R)$

$x \in R$ s.n. idempotent dacă $x^2 = x$

4) nilpotenți $\qquad N(R)$

$x \in R$ s.n. nilpotent dacă $\exists m \in \mathbb{N}^*$ a.î. $x^m = 0$

a) Dacă $R = (\mathbb{Z}, +, \cdot)$

$U(\mathbb{Z}) = \{\pm 1\}$ $\quad Idem(\mathbb{Z}) = \{0, 1\}$ $\quad x^2 = x$ în $\mathbb{Z} \Rightarrow x(x-1) = 0 \Rightarrow$ I $x = 0$, II $x = 1$

$D(\mathbb{Z}) = \{0\}$ $\quad N(\mathbb{Z}) = \{0\}$

b) $R = (\mathbb{Z}_6, +, \cdot)$

$U(\mathbb{Z}_6) = \{\hat{1}, \hat{5}\}$ $\quad Idem(\mathbb{Z}_6) = \{\hat{0}, \hat{1}, \hat{3}, \hat{4}\}$

$D(\mathbb{Z}_6) = \{\hat{0}, \hat{2}, \hat{3}, \hat{4}\}$ $\quad N(\mathbb{Z}_6) = \{\hat{0}\}$

$D(\mathbb{Z}_m) = \mathbb{Z}_m - U(\mathbb{Z}_m)$

$N(\mathbb{Z}_m) = ?$ $\quad m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ $\quad p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} \mid \hat{x}^k \Rightarrow p_i \mid x^k, i \in \overline{1,t} \Rightarrow$

$\hat{x} \in N(\mathbb{Z}_m) \Leftrightarrow \exists k \in \mathbb{N}^*$ a.î. $\hat{x}^k = \hat{0} \Leftrightarrow m \mid \hat{x}^k \Rightarrow$

$\Rightarrow p_1 p_2 \cdots p_t \mid x \Rightarrow x \in \underbrace{p_1 \cdots p_t}_{d} \mathbb{Z}_m$

Alg S2
pag5

$x \in d\mathbb{Z}_m \Rightarrow x = p_1 \cdots p_t \cdot m, \quad m \in \mathbb{Z}_m$

$\Rightarrow ?\ \exists N$ a.î. $(\overline{x^N}) = \overline{0} \Rightarrow m \mid (x^N) \Rightarrow m \mid (p_1 p_2 \cdots p_t m)^N =$

$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} \mid (p_1 p_2 \cdots p_t)^N$

$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} \mid p_1^N p_2^N \cdots p_t^N$

$N \geq \max(\alpha_1, \alpha_2, \ldots, \alpha_t)$

$\mathcal{N}(\mathbb{Z}_m) = d\mathbb{Z}_m, \quad d = p_1 \cdots p_t \quad m = p_1^{\alpha_1} \cdots p_t^{\alpha_t}.$