$X \subseteq V$ - ЛП

$$\ell(X) = \left\{ \sum_{i=1}^{n} \lambda_i x_i \,\middle|\, n \in \mathbb{N} \cup \{\overset{\theta}{\uparrow}\!\!0\},\ \lambda_i \in F,\ x_i \in X \right\}$$

$$= \bigcap_{X \subseteq U < V} U$$

A - тип α ; α = група, пръстен, поле ; $X \subseteq A$

$$\langle X \rangle := \bigcap_{X \subseteq \underbrace{B < A}_{B \text{ е под}\alpha \text{ на } A}} B$$

g^n, $n.g$ – обозначения $g \in$ група ($\cdot$ или $+$); пръстен

Пр. $2\mathbb{Z} = \{2z \mid z \in \mathbb{Z}\}$; операции?

– операциите в $\mathbb{Z}$

$$(2z_1) + (2z_2) = 2(z_1 + z_2)$$

$$(2z_1) \cdot (2z_2) = 2(2z_1 z_2)$$

подпръстен

пръстен; комутативен без делители 0

няма 1

– чрез биекция

$$f : \mathbb{Z} \longrightarrow 2\mathbb{Z}$$

$$z \longmapsto 2z$$

$$(2z_1) + (2z_2) := 2(z_1 + z_2)$$

$$(2z_1)(2z_2) := 2(z_1 z_2)$$

$$a + b = f\left(f^{-1}(a) + f^{-1}(b)\right); \quad f(ab) = f\left(f^{-1}(a) \cdot f^{-1}(b)\right)$$

$a, b \in 2\mathbb{Z}$

$\Big(\Rightarrow f^{-1}(a+b) = f^{-1}(a) + f^{-1}(b)$; $f^{-1}(ab) = f^{-1}(a) \cdot f^{-1}(b)$;

$a = f(x), b = f(y) \to f(x) + f(y) = f(x+y)$; $f(x) \cdot f(y) = f(xy)$

f, f^{-1} – са хомоморфизми ~~биекц~~ изоморфизъм

Разбира се, че $2\mathbb{Z}$ е пръстен с тези операции;

с единица — $2 = 2.1 = f(1) \Big)$

Зад. A, B – α

$A \times B = \{(a, b) \mid a \in A, b \in B\}$ } пак α

$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$

e_A, e_B – неутрални ~~ед.~~ ел. на A и B

$\{(e_A, b) \mid b \in B\} \subset A \times B$ подгр.; изоморфно на B

$1_A, 1_B$ – ед. на A и B (пръстени)

$(1_A, 1_B)$ – ед. на $A \times B$

$\mathbb{Z} \times 2\mathbb{Z}$ – пр.; без 1 ($2\mathbb{Z}$ с опер. на $\mathbb{Z}$)

$\mathbb{Z} \times \{0\} = \{(z, 0) \mid z \in \mathbb{Z}\} \subseteq \mathbb{Z} \times 2\mathbb{Z}$

изоморфно на $\mathbb{Z}$ → пръстен с 1

$$g^n = \begin{cases} \underbrace{g \cdots g}_{n}, & n > 0 \\ 1, & n = 0 \\ \underbrace{g^{-1} \cdots g^{-1}}_{-n}, & n < 0 \end{cases} \qquad n.g = \begin{cases} \underbrace{g + \cdots + g}_{n}, & n > 0 \\ 0, & n = 0 \\ \underbrace{(-g) + \cdots + (-g)}_{-n}, & n < 0 \end{cases}$$

$(g^m)^n = g^{mn}$; $g^m . g^n = g^{m+n}$; $m.(n.g) = (mn).g$, $mg + ng = (m+n)g$

!!! Това са означения

G - група ; $X \subseteq G$

$$\langle X \rangle = \{ x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \mid n \in \mathbb{N} \cup \{\overset{e}{0}\};\ x_i \in X,\ \overbrace{\varepsilon_i = \pm 1}^{\varepsilon_i \in \mathbb{Z}} \}$$ | Защо?

$\langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \}$ — циклична подгрупа породена от g

$\langle X \rangle$ — думите в азбуката $X \cup X^{-1}$

$X^{-1} = \{x^{-1} \mid x \in X\}$; празна дума $\leftrightarrow$ ед. ел.

R - пръстен ; $X \subseteq R$

$$\langle X \rangle = \{ \underbrace{\prod_{j=1}^{p} x_{i_j} + \ldots + \prod_{e=1}^{q} x_{k_e}}_{n} \mid n \in \mathbb{N} \cup \{0\},\ x_{\_} \in X;\ p, q \ldots \in \mathbb{N} \}$$

<u>Опр.</u> 1) $H \lhd G$ (H е <u>нормална</u> подгрупа на G), ако група

$H < G$ и $\forall h \in H, \forall g \in G \quad ghg^{-1} \in H$

2) $I \lhd R$ (I е идеал на пръстена R), ако

— $\forall i_1, i_2 \in I \Rightarrow i_1 - i_2 \in I$ $(\Leftrightarrow (I,+) < (R,+); \lhd)$

— $\forall i \in I, \forall r \in R$

$= ir \in I$ - десен идеал

$= ri \in I$ - лев идеал

$= ir, ri \in I$ - (двостран) идеал

Релација на еквивалентност

- $R \subset A \times B$ - релација; $aRb \Leftrightarrow (a,b) \in R$
- $R \subset A \times A$ - релација на еквивалентност, ако

$= \forall a \in A \ (a,a) \in R \ (aRa)$ рефлексивност

$= aRb \Rightarrow bRa$ симетричност

$= aRb, bRc \Rightarrow aRc$ транзитивност

Пр. 1/ $\leq$ удовл. (и)

2/ $=$ ОК

3/ $<$ удовл. 3

4/ A – т. в равн.; $A \times A$ – множ. от наредени дв.

$\vec{BC} \sim \vec{DE} \overset{def}{\iff} BC \parallel DE$; $BC = DE$; C и E са в една

„еквивалентни" полуравнина относно BD или

$D, E \in BD$ и BC и DE са еднопосочни

- $\vec{BC} \sim \vec{BC}$

- $\vec{BC} \sim \vec{DE} \Rightarrow \vec{DE} \sim \vec{BC}$

- $\vec{BC} \sim \vec{DE}$ и $\vec{DE} \sim \vec{FG} \Rightarrow \vec{BC} \sim \vec{FG}$

$\Rightarrow \sim$ е релация на еквивалентност (РЕ)

Тв. $\sim$ е РЕС в A. Тогава A се разбива на непресичащи се класове на еквивалентност

$[a] = \{b \in A \mid a \sim b\}$ (клас на екв. на $a \in A$)

Доб. $[a] = [b]$ или $[a] \cap [b] = \emptyset$

$x \in [a] \cap [b] \to a \sim x, \underbrace{b \sim x}_{x \sim b} \} a \sim b$

$\forall y \in [a] \to a \sim y \xrightarrow[b \sim a]{a \sim b} b \sim y \Rightarrow [a] \subseteq [b]$

Аналог. $[b] \subseteq [a]$

$\Big\} =$

рефл. $\Rightarrow \forall a \in [a]$

Зад. ∀ РЕ ⟺ разбиване на множеството на непресичащи се подмножества

$$X = \bigcup_{i\in I} X_i \,, \quad \forall i \neq j \quad X_i \cap X_j = \emptyset$$

Деф. $\sim$: $a \sim b \iff \exists\, i \in I : a, b \in X_i$

$$a \in X_i \iff [a] = X_i$$

Зад. $[a] = [b] \iff a \sim b$

Делимост на числата (разгл. мн. $\mathbb{Z}$)

Опр. $a \mid b$ (a „дели" b), ако $\exists c : b = ac$

Св-ва

1) a / a

2) $a / b, \; b \neq 0 \Rightarrow |a| \leq |b| \quad (b = ac, \; c \neq 0 \rightarrow |c| \geq 1)$

3) a / b и $b / a \Rightarrow |a| = |b| \quad (b = \pm a)$

4) $a / b, \; b / c \Rightarrow a / c$

$\left(\exists d : \underline{b = da} \, ; \; \exists e : \underline{c = be} \rightarrow c = d\underline{a} \cdot e = a(de) \right)$

Забл. за $\mathbb{N}$ 1, 3, 4 – дефинират релация на наредба (частична)

5) $a / b \Rightarrow a / bc$

6) $a / b, \; a / c \Rightarrow a / b + c$

7) $a / b_1, \ldots, a / b_n \Rightarrow \forall c_1 \ldots c_n \quad a / b_1 c_1 + \ldots + b_n c_n$

Т-ма (Теорема за деление с частно и остатък)

$\forall a, b \neq 0 \ \exists!\, q, r : a = bq + r$ и $0 \leq r < |b|$

(q - частно ; r - остатък)

вярно за $\mathbb{N} \cup \{0\}$

Факт: $\forall$ $\neq \emptyset$ подмножество на $\mathbb{N}$ има най-малък елемент

Д-во $M = \{a - bq \mid q \in \mathbb{Z}\}$; $M_0 = M \cap (\mathbb{N} \cup \{0\})$; $M_0 \neq \emptyset$

r - min ел. на M_0 $\Rightarrow \exists q \in \mathbb{Z} : r = a - bq$, т.е. $a = bq + r$

$r \geq 0$ - ясно ; Ако $r \geq |b|$ $\quad r_1 = \overbrace{a - bq}^{r} - |b| \in M$, $r_1 \geq 0 \to r_1 \in M_0$

$r_1 < r$ $(r - r_1 = |b| > 0)$ $\uparrow\downarrow$ $\Rightarrow$ $r < |b|$

$\Rightarrow q$ и r $\exists$

Единственост: нека $a = bq_1 + r_1 = bq_2 + r_2$ и $0 \le r_1, r_2 < |b|$

$b(q_1 - q_2) = r_2 - r_1$

Ако $q_1 \neq q_2$, то $|r_2 - r_1| \geq b$. Но $|r_2 - r_1| < |b|$ $\uparrow\downarrow$

$\Rightarrow q_1 = q_2 \Rightarrow r_1 = r_2$

Опр. R - пръстен, $X \subseteq R$

$$(X) = \bigcap_{X \subseteq I \triangleleft R} I$$ идеал на R породен от X

Св. $(X) = \{\sum_{i=1}^{n} r_i' x_i r_i'' \mid n \in \mathbb{N} \cup \{0\};\ r_i', r_i'' \in R,\ x_i \in X\}$

Опр. $X = \{a\}$, тогава $(X) = (a)$ - главен идеал породен от a; Ако R - комутативен с 1 $(a) = \{ar \mid r \in R\}$