Тв 13 $\mathbb{Z}$ всеки идеал е главен

R - пр.

$I \triangleleft R$ (идеал), ако:

- $\forall i_1, i_2 \quad i_1 - i_2 \in I \quad ((I,+) \triangleleft \underbrace{(R,+)}_{\text{адитивна п.гр на } R})$
- $\forall i \in I, \forall r \in R \quad ir, ri \in I$ (ляв, десен, двустранен)

(R - ком. пр. $ir = ri$)

$X \subseteq R$; $(X) = \bigcap\limits_{\substack{X \subseteq I \triangleleft R \\ \text{идеал}}} I$ - идеал породен от X (най-малкия идеал, който съдържа X)

$|X| = 1$ $(X = \{x\})$ $(X) = (x)$ - главен идеал породен от x

$(x) = \{r_1 x r_2 \mid r_1, r_2 \in R\} \cup \{x^n \mid n \in \mathbb{N} \cup \{0\}\}$

$0 \in R$

R - ком. пр. с 1 $\qquad (x) = \{rx \mid r \in R\}$

Д-во на ТС. Нека $I \lhd \mathbb{Z}$

- $I = \{0\} = (0)$
- $I \neq \{0\}$; $(a \in I \Rightarrow -a \in I) \Rightarrow I \cap \mathbb{N} \neq \emptyset$

Зад. $(1) = R$; $r \in R^{*} \Rightarrow (r) = R$

x - min естествено в I (min в $I \cap \mathbb{N} \subseteq \mathbb{N}$)

$(x) \subseteq I$

? $\supseteq$; $a \in I \qquad \left.\begin{array}{l} a = xq + r, \ 0 \leq r < x \\ x \text{ - min} \end{array}\right\} \ r = 0 \Rightarrow a = \underset{(x)}{\underset{\uparrow}{xq}}$

$\Rightarrow I \subseteq (x)$

Операции с идеали

$I, J \lhd R$ – пр.

- $I \cap J \lhd R$
- $I + J = \{ i + j \mid i \in I, j \in J \} \lhd R$ сума $\mid I, J \subseteq I + J$
- $I \cup J \ntriangleleft R$; $(I \cup J) = I + J$
- $IJ = \{ \sum_{k=1}^{n} i_k j_k \mid n \in \mathbb{N} \cup \{0\} ; \overbrace{i_k \in I, j_k \in J}^{k=1,\dots,n} \} \lhd R$

  $IJ = (\{ ij \mid i \in I, j \in J \})^{0}$

Т.С. $I, J \lhd R$; $I = (m)$, $J = (n)$. Тогава

1) $I \cap J = (k)$; 2) $I + J = (l)$; 3) $IJ = (s)$

$s = mn$; $\boxed{K = \underset{\text{НОК}}{[m,n]}, \quad \ell = \underset{\text{НОД}}{(m,n)}}$ ~~опр.~~

<u>Опр.</u> $m,n \in \mathbb{Z}$, НОД $(m,n) = d$ е:

- $d \mid m$ и $d \mid n$
- Ако $d' \mid m$, $d' \mid n$, то $d' \mid d$

<u>Заб.</u> Приложимо е във всички случаи: ако $d \mid a$ и $d \mid b$, то $d \mid (a,b)$

<u>Опр.</u> $m,n \in \mathbb{Z}$; НОК $[m,n] = K$ е:

- $m \mid K$ и $n \mid K$
- Ако $m \mid K'$ и $n \mid K'$, то $K \mid K'$

<u>Заб.</u> Ако $t \mid a$ и $t \mid b$, то $t \mid [a,b]$

Д-во на Т. 1) $I \cap J = (k)$; $k \overset{?}{=} [m,n]$

- $z \in I \cap J \iff z \in I,\ z \in J \iff m/z$ и n/z

  $z \in (k) \iff k/z$

  $k \in (k)$

- $\underline{k \in}(k) = \underline{I \cap J} \Rightarrow m/k$ и n/k
- Ако m/k' и $n/k' \Rightarrow \underline{k' \in} I \cap J = \underline{(k)} \Rightarrow k/k'$

2) $I + J = (l)$; $l \overset{?}{=} (m,n)$

- $l \in (l) = I + J \Rightarrow \exists u,v : u\underline{m} + v\underline{n} = l \xrightarrow[l'/n]{l'/m} l'/l$
- $I \subseteq (l),\ J \subseteq (l) \Rightarrow l/m$ и $l/n \to l$ е ОД

Заб. $\Rightarrow$ НОД и НОК $\exists$ (според горните деф.)

Заб. $(m) \subseteq (n) \iff n \mid m$

$(m) = (n) \iff m = cn,\ c \in \mathbb{Z}^* = \{\pm 1\}$

Сл. (Безу) $\forall m,n\ \exists u,v: um + vn = (m,n)$

Друго д-во за $\exists$ на НОД и НОК

Тв. Ако $a \mid b$, то $\exists (a,b)$ и $(a,b) = a$ (от опр.)

Заб. Ако d е НОД на a и b, то и $-d$ е НОД (и няма други НОД). Аналогично за НОК

Тв. $\underline{a} = \underline{b}q + \underline{r}$ (без условие за $\underline{r}$). Тогава

$(a,b)\ \exists \iff \exists\ (b,r)$ и в този случай са $=$

Д-во $(\Rightarrow)$ $d = (a,b)$

$- \ d \mid a, b \Rightarrow d \mid r = a - bq$ и $d \mid b \Rightarrow d \mid b, r$

$- \ d' \mid b, r \Rightarrow d' \mid a = bq + r \Rightarrow d' \mid a, b \Rightarrow d' \mid (a,b) = d$

$\Rightarrow (b,r) = d$

$(\Leftarrow)$ Аналог. $\underline{r} = a + (-q)\underline{b}$

Зад. $(a,b) \triangleleft \mathbb{Z}$ (идеалът породен от a и b)

$$(a,b) = \{ua + vb \mid u, v \in \mathbb{Z}\} = (a) + (b) = (\underbrace{(a,b)}_{\text{НОД}})$$

(a,b) – мин ел.

Алгоритъм на Евклид

$$a = b q_1 + r_1 \,, \quad 0 \lneq r_1 < |b| \qquad \mathcal{J}(a,b) = (b, r_1)$$

$$b = r_1 q_2 + r_2 \,, \quad 0 \lneq r_2 < r_1 \qquad \mathcal{J}(b, r_1) = (r_1, r_2)$$

$$r_1 = r_2 q_3 + r_3 \,, \quad 0 \lneq r_3 < r_2 \qquad \mathcal{J}(r_1, r_2) = (r_2, r_3)$$

$$\dots\dots\dots$$

$$r_k = r_{k+1} q_{k+2} + r_{k+2} \,, \quad 0 \lneq r_{k+2} < r_{k+1} \qquad \mathcal{J}(r_k, r_{k+1}) = (r_{k+1}, r_{k+2})$$

$$r_{k+1} = r_{k+2} q_{k+3} \qquad \mathcal{J}(r_{k+1}, r_{k+2}) = r_{k+2}$$

$$\mathcal{J}(a,b) = r_{k+2}$$

<u>Сл.</u> (Безу) $\exists u, v: au + bv = (a,b)$

<u>Д-во</u> по инд. $\exists u_i, v_i : r_i = a u_i + b v_i$

$$\left.\begin{aligned} r_1 &= 1.a + (-q_1) b \\ r_2 &= b - r_1 q_2 = (-q_2) a + (1 + q_1 q_2) b \end{aligned}\right\} \text{база}$$

$r_i = r_{i-2} - r_{i-1} q_i$ – за инд. стъпка

$$\underset{(a,b)}{\underset{\shortparallel}{r_{k+2}}} = \underbrace{u_{k+2}}_{u} a + \underbrace{v_{k+2}}_{v} b$$

<u>Сл.</u> $(ca, cb) = c(a,b)$, $c > 0$

<u>Д-во</u> АЕ за $\underline{ca}$ и $\underline{cb}$ е АЕ за $\underline{a}$ и $\underline{b}$ „умножен" с $\underline{c}$

Сл. $\left((a,b)\dfrac{a}{(a,b)}, (a,b)\dfrac{b}{(a,b)} \right) = (a,b) \cdot \left(\dfrac{a}{(a,b)}, \dfrac{b}{(a,b)} \right)$

$(a,b)=$

$$\Rightarrow \boxed{\left(\frac{a}{(a,b)}, \frac{b}{(a,b)} \right) = 1}$$

Зад. $ua + vb = 1 \Rightarrow (a,b) = 1$

Опр. a, b – взаимнопрости, ако $(a,b) = 1$

Опр. p – просто, ако $p \mid ab \Rightarrow p \mid a$ или $p \mid b$

p – неразложимо, ако от $p = ab \Rightarrow |a| = 1$ или $|b| = 1$
$(\Leftrightarrow |b| = p)$ $(\Leftrightarrow |a| = p)$

(единствените делители на p са ± 1 и $\pm p$)

Тв. p – просто $\Leftrightarrow$ p – неразложимо т.е. (p) е прост (опр.)

<u>Зад</u> (идеал) 1) p-прост $\Leftrightarrow$ $\left(ab \in (p) \Rightarrow a \in (p)\right.$ или $\left.b \in (p)\right)$

2) p-неразл. $\Leftrightarrow$ $\left((p) \subset (a) \underset{\subset R}{\Leftrightarrow} (a) = R\right.$ или $\left.(a) = (p) \right)$

т.е. (p) е „максимален" идеал (опр.)

3) $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \ldots \underset{(a)}{\ldots} \subseteq R$ — кон. вериги с L, всяка

$(a_2|a_1)$ $(a_3|a_2)$ — $\forall$ идеал е главен

$(a) = \bigcup\limits_{i=1}^{\infty} (a_i) \lhd R$

$\exists i : a \in (a_i) \Rightarrow (a) = (a_i)$

<u>Те.</u> $a | bc$, $(a,b) = 1 \Rightarrow a | c$

<u>Д-во</u> Безу $\Rightarrow ua + vb = 1 \rightarrow uac + vbc = c \Rightarrow a | c$

Тб. $a \mid bc \Rightarrow \frac{a}{(a,b)} \mid c$

Д-во $\exists k: bc = ak \Rightarrow \frac{b}{(a,b)} c = \frac{a}{(a,b)} k$

$$\left.\begin{array}{l} \Rightarrow \frac{a}{(a,b)} \mid \frac{b}{(a,b)} c \\ \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1 \end{array}\right\} \Rightarrow \frac{a}{(a,b)} \mid c$$

Тб. $[a,b] = \frac{ab}{(a,b)}$ $(a>0, b>0 \Rightarrow (a,b)>0, [a,b]>0)$

Д-во Пусть $t: a \mid t, b \mid t$ (t - ОК)

$a \mid t \Rightarrow \exists k: t = ak \Rightarrow b \mid ak \Rightarrow \frac{b}{(a,b)} \mid k$

$\Rightarrow k = \frac{b}{(a,b)} l \Rightarrow t = \frac{ab}{(a,b)} l$ (Видно из l, что t со ОК) т.е. $\{ОД\} = \left\{ \frac{ab}{(a,b)} t \mid t \in \mathbb{Z} \right\}$

$\Rightarrow \frac{ab}{(a,b)}$ – ~~НОД~~ НОК