„Нещо" – ЛП, група, пръстен, поле ; М – „нещо"

– подмножество $N \subset M$

– $X \subseteq M$

$= \ell(X)$ (ЛП) $\quad \ell(X) = \bigcap_{X \subseteq U < M} M$

$= (X)$ – група

$(X) = \bigcap_{X \subseteq H < M}$

$= N < M$ (пръстен) ; $X \subseteq M$

$N[X] = \bigcap_{N < K < M \atop X \subseteq K}$

$= N < M$ (подполе); $X \subseteq M$

$$N(X) = \bigcap_{N < K < M,\ X \subseteq K} K$$

Опр. R – поле; $I \lhd R$ – идеал кольца R, если:

– $\forall i_1, i_2 \in I \quad \underline{i_1 - i_2 \in I}$ $\quad ((I,+) < (R,+))$

– $\forall i \in I \ \forall r \in R \quad ir, ri \in I$ (лев., прав., двусторонний)

Зам. 1) G – гр.

$H < G \Leftrightarrow H \subseteq G$ и $h_1, h_2, e, h^{-1} \in H$

$\Leftrightarrow H \subseteq G$ и $h_1, h_2, h^{-1} \in H$

$\Leftrightarrow H \subseteq G$ и $h_1 h_2^{-1} \in H$

можно записывать

Зам. аддитивно

$h_1 + h_2, 0, -h$

$h_1 + h_2, -h$

$h_1 - h_2$

2) $K \subset R$ (подкольцо)

$\Leftrightarrow K \subseteq R$ и $k_1 - k_2, k_1 k_2 \in K$

3) $K \subset F$ (подполе)

$\Leftrightarrow K \subseteq F$ и $k_1 - k_2, \underbrace{k_1 k_2, k^{-1} (k \neq 0)}_{k_1 k_2^{-1} (k_2 \neq 0)} \in K$

Зад. Идеал е и подпръстен

R - пръстен; $X \subseteq R$

$$(X) = \bigcap_{X \subseteq I \lhd R} I$$

Ако $X = \{x\}$, пишем (x) - главен идеал

Зад. 1) ЛП $\quad \mathcal{L}(X) = \left\{ \sum_{i=1}^{n} \lambda_i x_i \;\middle|\; n \in \mathbb{N} \cup \{0\};\ \lambda_i \in F;\ x_i \in X \right\}$

2) група $\quad (X) = \left\{ x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \;\middle|\; n \in \mathbb{N} \cup \{0\};\ \varepsilon_i = \pm 1;\ x_i \in X \right\}$

3) пръстен $\quad K[X] = \left\{ f(x_1, \dots, x_n) \;\middle|\; n \in \mathbb{N} \cup \{0\};\ f \in K[y_1, \dots, y_m];\ x_i \in X \right\}$

полиноми над $y_1, \dots, y_m$ с коеф. от K

Пр. $\mathbb{Z}[\sqrt{2}] = \{ f(\sqrt{2}) \mid f \in \mathbb{Z}[X] \} = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Z} \}$

4) поле

$$K(X) = \left\{ \frac{f(x_1, \dots, x_n)}{g(x_1, \dots, x_n)} \;\middle|\; n \in \mathbb{N} \cup \{0\};\ f, g \in K[y_1, \dots, y_m];\ x_i \in X;\ g(x_1, \dots, x_n) \neq 0 \right\}$$

Пр. $\mathbb{Q}(\sqrt{2}) = \left\{ \frac{f(\sqrt{2})}{g(\sqrt{2})} \;\middle|\; f, g \in \mathbb{Q}[x],\ g(\sqrt{2}) \neq 0 \right\} =$ „$\mathbb{Q}[\sqrt{2}]$"

полиноми над x с коеф. от $\mathbb{Q}$

$$= \left\{ \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \;\middle|\; a, b, c, d \in \mathbb{Q},\ c + d\sqrt{2} \neq 0 \right\} = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$$

$\mathbb{R}(i) = \mathbb{R}[i] = \mathbb{C} \quad \sim \quad \mathbb{Q}(\sqrt{2})$

Опр. G - группа; $H \trianglelefteq G$ — нормальная подгруппа, если

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

(ghg^{-1} - сопряжение h с g)

Теория чисел
(живем в $\mathbb{Z}$)

Зам. в $F[x]$ (F - поле) теория со всего другая

Факт: Всякое подмножество $\mathbb{N}$ имеет наименьший эл.

Опр. Говорим, что $a \mid b$ (a „делит" b), если

$\exists c : b = ac$

Св-ва: 1) $a \mid a$

2) $a \mid b,\ b \neq 0 \Rightarrow |a| \leq |b|$

$(b = ac \to |b| = |a|\,|c| \geq |a|)$ ($\neq 0 \to \neq 1$)

3) $a \mid b$ и $b \mid a \Rightarrow |a| = |b| \Rightarrow b = \pm a$ $(b = \varepsilon a,\ \varepsilon \in \mathbb{Z}^*)$ ($\mathbb{Z}^* = \{\pm 1\}$)

4) $a \mid b$ и $b \mid c \Rightarrow a \mid c$

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

6) $a \mid b,\ a \mid c \Rightarrow a \mid b + c$

$(\exists c_1, c_2 : b = c_1 a,\ c = c_2 a \to b + c = c_1 a + c_2 a = a(c_1 + c_2))$

7) $a \mid b_i \Rightarrow a \mid \sum b_i c_i$

8) $a \mid b \Leftrightarrow (b) \subseteq (a)$

Зам. R – ком.; $X \subseteq R$ $\quad (X) = \left\{ \sum_{i=1}^{n} r_i' x_i r_i'' \mid n \in \mathbb{N} \cup \{0\} \mid r_i', r_i'' \in R, x_i \in X \right\}$

R – ком. с 1

$X = \{x\}$ $\quad (x) = \{ r_1 x r_2 \mid r_1, r_2 \in R \}$

R – ком. ор. с 1 $\quad (x) = \{ rx \mid r \in R \}$

9) $(a) = (b) \Leftrightarrow b = \varepsilon a$, $\varepsilon \in \mathbb{Z}^*$

Теор. о ген. с остатком

$\forall a, b \ (b \neq 0) \quad \exists! \, q, r : \begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$

(q – частное; r – остаток)

Д-во $M = \{a - bq \mid q \in \mathbb{Z}\}$

$M \cap \mathbb{N}_0 \neq \emptyset$; r – min эл. на $M \cap \mathbb{N}_0$ ($\mathbb{N}_0 = \mathbb{N} \cup \{0\}$)

$\Rightarrow \exists q \in \mathbb{Z}: r = a - bq$, т.е. $a = bq + r$ $\rightarrow r \geq 0$

Ако $r \geq |b| \Rightarrow r - |b| = a - (q \pm 1)b \in M \overset{\in \mathbb{N}_0}{\Rightarrow} \in M \cap \mathbb{N}_0$

$r - |b| < r$ ↯

$\Rightarrow r < |b|$

Т. Ако $I \lhd \mathbb{Z}$, то I е главен идеал, т.е. $\exists a \in \mathbb{Z}: I = (a)$

Д-во Нека $I \lhd \mathbb{Z}$

- $I = \{0\} = (0)$
- $I \neq \{0\}$

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

Пусть a — наим. эл. $I \cap \mathbb{N}$

Докажем, что $(a) \subseteq I$ $(a \in I)$

Дано $i \in I$, тогда $\exists q, r: i = aq + r$ и $0 \leq r < |a| = a$

$r = \underline{i} - \underline{a}q \in I$ $(i, a \in I) \Rightarrow r = 0 \Rightarrow i = aq \in (a)$

$\Rightarrow I \subseteq (a) \Rightarrow I = (a)$

<u>Зам.</u> При обращении с коэф. от кольц → аналогично

Операции с идеалами

1) $I_j \lhd R$, $j \in J \Rightarrow \bigcap\limits_{j \in J} I_j \lhd R$

Зам. $\ell(X \cup Y) = \ell(X) + \ell(Y)$

2) $I + J = \{ i + j \mid i \in I, j \in J \} \lhd R$ ($I, J \lhd R$) – сумма

3) $IJ = \left(\{ ij \mid i \in I, j \in J \} \right) = \left\{ \sum\limits_{k=1}^{n} i_k j_k \;\middle|\; n \in \mathbb{N} \cup \{0\},\ i_k \in I,\ j_k \in J \right\}$

$\subseteq I \cap J$

(R – ком. с 1)

Зам. $I \cap J \subseteq I, J$

$I, J \subseteq I + J$; $IJ \subseteq I \cap J$

R – ~~ком~~ с 1 & $IJ \subseteq I, J$

Опр. (НОД) $d = (a, b)$, если:

- $d \mid a$ и $d \mid b$
- Если $d' \mid a$ и $d' \mid b$, то $d' \mid d$

Опр. (НОК) $m = [a, b]$, если:

- $a \mid m$ и $b \mid m$
- Если $a \mid m'$ и $b \mid m'$, то $m \mid m'$

} условия вычисления через делимость

Те 1) $(a) \cap (b) = ([a, b])$

2) $(a) + (b) = ((a, b))$

3) $(a)(b) = (ab)$ (ясно)

} $\Rightarrow$ существование НОД, НОК

Зад. НОД и НОК са определени с точност до ± 1

Д-во 1) $\exists m : (a) \cap (b) = (m)$

- $m \in (m) \Rightarrow m \in (a)$ и $m \in (b) \Rightarrow a \mid m$ и $b \mid m$
- Ако $a \mid m'$ и $b \mid m' \Rightarrow m' \in (a)$ и $m' \in (b) \Rightarrow m' \in (a) \cap (b) = (m)$
  $\Rightarrow m \mid m'$

$\Rightarrow \exists m = [a, b]$

2) $\exists d : (a) + (b) = (d)$

- $(a) \subseteq (d)$ и $(b) \subseteq (d) \Rightarrow d \mid a$ и $d \mid b$
- $d \in (d) = (a) + (b) \Rightarrow \exists u, v : d = au + bv$
  Ако $d' \mid a$ и $d' \mid b \Rightarrow d' \mid d$

$\Rightarrow \exists\, d = (a,b)$

Сл. (Безу) $\forall a,b \; \exists u,v : \; ua + vb = (a,b)$

Алгоритъм на Евклид за намиране на НОД и НОК

Тв. $a \mid b \Rightarrow \exists (a,b) = a$

Тв $a = bq + r$ (δ за отрицателни r). Тогава $(a,b) \exists \Leftrightarrow \exists (b,r)$ и в този случай $(a,b) = (b,r)$

Д-во: ($\Rightarrow$) Нека $d = (a,b)$. Щом $d \mid a, d \mid b \Rightarrow d \mid r = a - bq \overset{d \mid b}{\Rightarrow} d \mid r, b$

– Ако $d' \mid b$ и $d' \mid r \Rightarrow d' \mid a = bq + r \overset{d' \mid b}{\Rightarrow} d' \mid (a,b) = d$

($\Leftarrow$) Аналог $\Rightarrow (b,r) = d$

Алгоритм Евклида (АЕ)

$a = bq_1 + r_1, \quad 0 \leq r_1 < |b|$

$b = r_1 q_2 + r_2, \quad 0 \leq r_2 < |r_1| = r_1$

$r_1 = r_2 q_3 + r_3, \quad 0 \leq r_3 < |r_2| = r_2$

$\dots$

$r_k = r_{k+1} q_{k+2} + r_{k+2}, \quad 0 < r_{k+2} < r_{k+1}$

$r_{k+1} = r_{k+2} q_{k+3}$

Процесс сходится.

$\exists(a,b) = (b, r_1)$

$\exists(b, r_1) = (r_1, r_2)$

$\exists(r_1, r_2) = (r_2, r_3)$

$\dots$

$\exists(r_k, r_{k+1}) = (r_{k+1}, r_{k+2})$

$\exists(r_{k+1}, r_{k+2}) = r_{k+2}$

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

Ст. (Безу) $\exists u, v : au + bv = (a, b)$

Д-во инд. пол. $\forall i = 1, 2, \dots k+2 \quad \exists u_i, v_i :$

$$r_i = u_i a + v_i b$$

База: $r_1 = 1 \cdot a + (-q_1) b$

$$r_2 = b - r_1 q_2 = (-q_2) a + (1 + q_1 q_2) b$$

инд. связка: $r_i = r_{i-2} - r_{i-1} q_i$

$i = k+2 \to r_{k+2} = \underbrace{u_{k+2}}_{u} a + b \underbrace{v_{k+2}}_{v} = ua + bv$