Идеали в комутативен пръстен

K - комутативен пр. с 1

$I, J \triangleleft K$

$I + J = \{a + b \mid a \in I, b \in J\} \triangleleft K$

$\ast\ IJ = \{a_1 b_1 + a_2 b_2 + \dots + a_s b_s \mid s \geq 1,\ a_i \in I, b_i \in J\}$

$IJ \subset I \cap J \subset \begin{matrix} I \\ J \end{matrix} \subseteq I + J$

$\emptyset \neq I \subset K$, $I \triangleleft K$ идеал, когато

$a - b \in I$, $\forall a, b \in I$

$ra \in I$, $\forall a \in I$

$ar \in I$, $\forall r \in K$

$a, b \in \mathbb{Z}$ взаимно прости

$\text{НОД}(a, b) = 1$

$1 = a \cdot u + b \cdot v$

$n = a \cdot un + b vn$, $n \in \mathbb{Z}$

$\boxed{\mathbb{Z} = (a) + (b)}$

$(a) = \{ak \mid k \in \mathbb{Z}\}$

Опр. $I, J \triangleleft K$ - комут. с 1

I, J взаимно прости идеали, когато $\boxed{I + J = K}$

Св-во $I, J \triangleleft K$ комут. с 1

I, J взаимно прости $\Rightarrow IJ = I \cap J$

Д-во $I + J = K \Rightarrow 1 = e_1 + e_2 \quad e_1 \in I, e_2 \in J$

$x \in I \cap J \Rightarrow x = x.1 = x(e_1 + e_2) = xe_1 + xe_2 \in IJ$

$I \cap J \subset IJ$, но $IJ \subset I \cap J \Rightarrow I \cap J = IJ$.

Обща формулировка кит. Th за ост.

Нека K е комутат. пръстен с 1

$I_1, \dots, I_s \triangleleft K$, два по два взаимно прости

$I_l + I_p = K$ за $l \neq p$

Ако $a_1, \dots, a_s$ са произв. $\in K$

Съществува $x \in K$!

$$\left|\begin{array}{l} x \in a_1 + I_1 \\ x \in a_2 + I_2 \\ \vdots \\ x \in a_s + I_s \end{array}\right. \iff \left|\begin{array}{l} a_1 \in x + I_1 \\ a_2 \in x + I_2 \\ \vdots \\ a_s \in x + I_s \end{array}\right.$$

$$\left|\begin{array}{l} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{array}\right.$$

Кит. Th за остатъците

класическа формул.

Нека $m_1, m_2, \dots, m_k$ които са две по две взаимно прости $(m_s, m_t) = 1$

$a_1, \dots, a_k$ произволни

Тогава $\exists\, x$ такова че

$$\left|\begin{array}{l} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{array}\right.$$

Д-во $s=2$

$I_1+I_2=K \Rightarrow \exists\ e_1\in I_1,\ e_2\in I_2$ и $\boxed{1=e_1+e_2}$

взимаме $x=a_1e_2+a_2e_1$

$x-a_1 \overset{?}{\in} I_1$

$x-a_2\in I_2$

$e_2-1=-e_1$

$x-a_1=\underbrace{a_1e_2-a_1}+a_2e_1 = a_1(e_2-1)+a_2e_1=$

$=a_1(-e_1)+a_2e_1\in I_1$

$x-a_1\in I_1 \Rightarrow x\in a_1+I_1$ или $a_1\in x+I_1$

$x-a_2=a_1e_2+\underline{a_2e_1-a_2}=a_1e_2+a_2\underbrace{(e_1-1)}_{-e_2}=\underbrace{a_1e_2+a_2(-e_2)}_{\in I_2}$

$\Rightarrow x-a_2\in I_2 \Rightarrow x\in a_2+I_2$

$I_1, \dots, I_s$ взаимно прости $\quad I_p + I_l = K \quad p \neq l$

$$\left.\begin{array}{lll} I_1 + I_2 = K \Rightarrow & 1 = u_2 + v_2 & \underline{u_2 \in I_1}, v_2 \in I_2 \\ I_1 + I_3 = K \Rightarrow & 1 = u_3 + v_3 & \underline{u_3 \in I_1}, v_3 \in I_3 \\ \vdots & & \\ I_1 + I_s = K \Rightarrow & 1 = u_s + v_s & \underline{u_s \in I_1}, v_s \in I_s \end{array}\right\} \quad 1 = (u_2 + v_2) \cdots (u_s + v_s)$$

разкриване

всяко събираемо което има поне едно u

$v_2 \dots u_i \dots v_s \in I_1$

$$1 = \underbrace{(\quad\quad)}_{\in I_1}^{z_1} + \underbrace{v_2 v_3 \dots v_s}_{= t_1} = z_1 + t_1 \qquad \begin{array}{l} z_1 \in I_1 \\ t_1 \in I_2 \cap I_3 \cap \dots \cap I_s \end{array}$$

$1 = z_1 + t_1, \quad z_1 \in I_1, \quad t_1 \in I_2 \cap I_3 \cap \dots \cap I_s$

$1 = z_2 + t_2 \quad z_2 \in I_2, \quad t_2 \in I_1 \cap I_3 \cap \dots \cap I_s$

$\vdots$

$1 = z_s + t_s, \quad z_s \in I_s, \quad t_s \in I_1 \cap I_2 \dots \cap I_{s-1}$

$I_1 + (I_2 \cap \dots \cap I_s) = K$

$\vdots$

$I_s + (I_1 \cap \dots I_{s-1}) = K$

$1 = z_1 + t_1$, $z_1 \in \mathcal{I}_1$, $t_1 \in \mathcal{I}_2 \cap \dots \cap \mathcal{I}_s$

$\vdots$

$1 = z_s + t_s$, $z_s \in \mathcal{I}_s$, $t_s \in \mathcal{I}_1 \cap \dots \cap \mathcal{I}_{s-1}$

Дадени са $a_1, \dots, a_s$

$$\boxed{x = a_1 t_1 + \dots + a_s t_s}$$

$1 = z_j + t_j$

$t_j - 1 = -z_j \in \mathcal{I}_j$

$$x - a_j = a_1 t_1 + \dots + a_j t_j + \dots + a_s t_s - a_j =$$
$$= \underbrace{a_1 t_1}_{\in \mathcal{I}_j} + \dots + a_j \underbrace{(t_j - 1)}_{\in \mathcal{I}_j} + \dots + \underbrace{a_s t_s}_{\in \mathcal{I}_j}$$

$x - a_j \in \mathcal{I}_j \Rightarrow x \in a_j + \mathcal{I}_j$ или $a_j \in x + \mathcal{I}_j$

$j = 1, \dots, s$

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

$(3, 35) = 1 = 36 \boxed{-35} = 3 \cdot 12 - 1 \cdot 35$

$(5, 21) = 1 = -4 \cdot 5 + \boxed{21} = -20 + 21$

$(7, 15) = 1 = -14 + \boxed{15} = -2 \cdot 7 + 15$

$3 \cdot 5 \cdot 7 = 105$

$-35 \equiv 70 \pmod{105}$

Отв. $x \equiv \underbrace{2 \cdot 70} + \underbrace{3 \cdot 21} + \underbrace{2 \cdot 15} \equiv 23 \ (105)$

233-210

$$\begin{cases} x \equiv a_1 \pmod 7 \\ x \equiv a_2 \pmod 8 \\ x \equiv a_3 \pmod 9 \end{cases}$$

$(7, 8 \cdot 9) = 1 = 31 \cdot 7 \boxed{-3 \cdot 72}$

$(8, 63) = 1 = 64 \boxed{-63}$

$(9, 56) = 1 = 25 \cdot 9 \boxed{-4 \cdot 56}$

$7 \cdot 8 \cdot 9 = \underline{\underline{504}}$

$-3 \cdot 72 = -216 \equiv 288 \ (504)$

$-63 \equiv 441 \ (504)$

$-4 \cdot 56 \equiv 280 \ (504)$

$x = 288 a_1 + 441 a_2 + 280 a_3$

Сл. K - комутат. пръстен с 1

$I_1, \dots, I_s \lhd K$, $I_\ell + I_p = K$, $\forall \ell \neq p$

$$\boxed{K/(I_1 \cap \dots \cap I_s) \cong K/I_1 \times K/I_2 \times \dots \times K/I_s}$$

Д-во $\eta_j : K \to K/I_j$ естествен хомоморфизъм

$\eta : K \to K/I_1 \times K/I_2 \times \dots \times K/I_s$

$\underset{x}{\eta(\overset{\Uparrow}{a})} \to (a+I_1, a+I_2, \dots, a+I_s) =$

$= (\eta_1(a), \eta_2(a), \dots, \eta_s(a))$

$\to \eta$ е хомоморф.

$\ker \eta := \{a \mid \eta_j(a) = I_j, j = 1 \dots s\} =$

$= \bigcap_{j=1}^{s} I_j$

$\to$ от Кит. Th $(a_1 + I_1, \dots, a_s + I_s) = (x + I_1, \dots, x + I_s)$

$\operatorname{Im} \eta = K/I_1 \times K/I_2 \times \dots \times K/I_s$ от Th хомом.

K, M пръстени

$K \times M = \{(a, b) \mid a \in K, b \in M\}$

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

$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)$

$\tilde{K} = \{(a, 0) \mid a \in K\}$

$\tilde{M} = \{(0, b) \mid b \in M\}$

$\tilde{K}, \tilde{M} \lhd K \times M$

$K \times M = \tilde{K} \oplus \tilde{M}$

$0 = (0_K, 0_M)$

$1 = (e_K, e_M)$

Сл. 1 $n = p_1^{k_1} \cdots p_s^{k_s}$ $p_1, \dots, p_s$ – различни пр.

$(p_i^{k_i}, p_j^{k_j}) = 1$ $i \neq j$

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \dots \times \mathbb{Z}_{p_s^{k_s}}$$

$$\varphi(n) = \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \cdots \varphi(p_s^{k_s})$$

Ако $(k, s) = 1$ $\mathbb{Z}_{ks} \cong \mathbb{Z}_k \oplus \mathbb{Z}_s$