# Прости и максимални идеали

Първо ще дефинираме няколко операции между идеали.

## Сечение на идеали

Нека $I, J \blacktriangleleft K$. Тогава

$$I \cap J \blacktriangleleft K \tag{1}$$

## Сума на идеали

Нека $I, J \blacktriangleleft K$. Тогава

$$I + J = \{a + b | a \in I \& b \in J\} \blacktriangleleft K \tag{2}$$

## Произведение на идеали

Нека $I, J \blacktriangleleft K$. Тогава

$$IJ = \{a_1 b_1 + a_2 b_2 + \cdots + a_s b_s | a_i \in I \& b_i \in J \& s \in \mathbb{N}\} \blacktriangleleft K \tag{3}$$

## Прост идеал

**Дефиниция**: Нека $I \blacktriangleleft K$. Ако $a, b \in K$ и от $a.b \in I$ следва, че $a \in I$ или $b \in I$, наричаме $I$ *прост идеал*.

### Пример

Да разгледаме пръстена $\mathbb{Z}$ и идеала породен от цяло число: $I = (u) \quad u \in \mathbb{Z}$.
Ако $a, b$ са произволни цели, то $a.b \in I \iff u/a.b$. Е да, обаче ако $u$ е *просто число*, това е равносилно на $u/a$ или $u/b$. По дефиниция идеала $I = (u)$ е прост.
**Забележка**: Термина *прост идеал* е произлязъл именно от аналогията с простите числа.

## Максимален идеал

**Дефиниция**: Нека $I \blacktriangleleft K$. Ако $\forall J \blacktriangleleft K$ е изпълнено, че от $I \subsetneq J$ следва $J = K$, то $I$ наричаме максимален идеал.

## Теорема за връзката на вида идеал с факторгрупата породена от него

**Дефиниция**: Комутативен пръстен, в който няма делители на нулата се нарича ***област на цялост***.
**Теорема**: Нека $K$ е комутативен пръстен с 1, и нека $I \blacktriangleleft K$. Тогава:

1. $I$ е прост идеал т.с.т.к. $K/I$ е област на цялост.
2. $I$ е максимален идеал т.с.т.к $K/I$ е поле.

скрий

1. $|\Rightarrow|$ Нека $I \blacktriangleleft K$ е прост идеал и да допуснем, че факторгрупата $K/I$ има делител на нулата.
Т.е допускаме, че съществуват ненулеви елементи $a+I$ и $b+I$ от $K/I$, такива че $(a+I)(b+I)=(0+I)$. Но тогава $a.b+I=0+I$, от където получаваме, че $ab \in I$. От простотата на идеала (:) получаваме $a \in I$ или $b \in I$. От тук веднага $a+I=0+I$ или $b+I=0+I$ - противоречие с допуснатото, че са ненулеви елементи. Следователно $K/I$ е област на цялост.
$|\Leftarrow|$ Нека $K/I$ е област на цялост. И нека $a.b \in I$, където $a,b$ са произволни от $K$.
Тогава $a.b+I=0+I=(a+I)(b+I)$. Понеже няма делители на нулата в $K/I$ получаваме, че $a+I=0+I$ или $b+I=0+I$, което е равносилно на $a \in I$ или $b \in I$. Т.е идеала е просто.
2. $|\Rightarrow|$ Нека $I \blacktriangleleft K$ е максимален идеал. Ще докажем, че $K/I$ е комутативен пръстен с 1.
Всъщност, ще покажем как да намираме обратен на произволен елемент от $K/I$. Нека $x+I$ е произволен ненулев от $K/I$. Следователно $x+I \neq 0+I \Rightarrow x \notin I$.
Сега ще разгледаме идеала породен от $x$ : $J=(x)$, и по-подробно сумата $I+J$:
Очевидно $I \subsetneq I+J \blacktriangleleft K$. От максималността на $I$, заключваме, че $I+J=K$. Следователно единичния елемент на $K$ е в $I+J$, т.е $1 \in I+J$, т.е може да се престави като $i+j$, където $i \in I \& j \in J$, и от построяването на $J$ взимаме, че $j=xt$, за някое $t$. Следователно $1=i+xt \iff xt=1-i$. Сега да разпишем $(x+I)(t+I)$:

$$(x+I)(t+I)=xt+I=(1-i)+I=(1+I)-(i+I)=(1+I)-(0+I)=(1-0)+I=1+I \tag{4}$$

което очевидно е единичния елемент в $K/I$. Следователно доказахме, че за произволен елемент $x+I$, обратният му $t+I$, също е от факторгрупата $K/I$. Т.е $K/I$ е комутативен пръстен с 1, т.е поле.
$|\Leftarrow|$ Нека $K/I$ е поле. И нека $I \subsetneq J \blacktriangleleft K$.
Да си вземем произволен елемент $a \in J \setminus I$. $a \notin I$, следователно $a+I \neq 0+I$, следователно си има обратен - нека го кръсим $b+I$. Имаме:

$$(a+I)(b+I)=ab+I=1+I \tag{5}$$

$a.b \in J$, защото $a \in J$.
Сега да поразсъждаваме малко какво значи $a.b+I=1+I$ : ами съществуват елементи $i_1, i_2 \in I$, такива че $ab+i_1=1+i_2$. Е да, но $I \subset J$, следователно $i_1, i_2 \in J$. Това означава, че съседният на $J$ клас, породен от $ab$ , съвпада със съседния клас на $J$ , породен от 1. Т.е $ab+J=1+J$. Но $ab \in J \Rightarrow ab \in J$, т.е $1+J=J$ т.е $1 \in J$. Сега лесно получаваме, че $1x \in J \; \forall x \in K$, следоваателно $J=K$.
Т.е доказахме, че произволен идеал, включващ $I$ и по-голям от него съвпада с $K$. Следователно $I$ е максимален идеал.

# *Взаимно прости идеали*

## Дефиниция *(взаимно прости идеали)*

Нека $K$ е комутативен пръстен с $1$. Нека $I,J \blacktriangleleft K$. Тогава наричаме $I,J$ взаимно прости, ако

$I+J=K$.
**Забележка**: При целите числа имаме $(a,b)=1$, т.г.с.т. $ua+vb=1$ за някои цели $u,v$. Изказано на езика на идеалите: $(a)+(b)=\mathbb{Z}$ (защото сбор на идеали е идеал и очевидно $1$ принадлежи на идеала, следователно съвпада с пръстена).

### Твърдение

Нека $I,J \blacktriangleleft K$. Да се докаже, че

$$IJ \subseteq I\cap J \subseteq I+J \tag{6}$$

скрий

Нека $k\in IJ$. Очевидно $k$ има вида $i_1j_1+i_2j_2+\cdots i_nj_n$. където $i_x\in I\&j_x\in J$. Но $i_xj_x\in I\cap J$ - очевидно, следователно и сбора на всичките също е от сечението. Така получихме $IJ\subseteq I\cap J$.
Нека $k\in I\cap J$. Тогава $k$ със сигурност е от $I$. Следователно може да се представи като $k+0$; понеже $0\in J$ лесно получаваме, че $k=k+0\in I+J$. С това доказахме, че $I\cap J\subseteq I+J$.

### Задачка

Да разгледаме комутативния пръстен с $1$ - $\mathbb{Z}$. Да се намерят идеали $I=(n)$, $J=(k)$ идеали, такива че $IJ\neq I\cap J\neq I+J$.
**Решение**:
Не е трудно да се провери, че:

$$\begin{aligned}(ab)&=IJ\\([a,b])&=I\cap J\\((a,b))&=I+J\end{aligned} \tag{7}$$

като $[a,b]$ е НОК на числата. Сега просто трябва да изберем подходящи числа: ами трябва да не са взаимно прости (чупи се първата част) и трябва да са различни (чупи се втората). Така стигнахме до (примерно) $k=2\&n=4$:

$$\begin{aligned}IJ&=(8)\\I\cap J&=(4)\\I+J&=(2)\end{aligned} \tag{8}$$

## *Китайска теорема за остатъци*

Нека $K$ е комутативен пръстен с $1$. Нека $I_1,I_2,\cdots,I_n \blacktriangleleft K$ са взаимно прости идеали на $K$ : $I_j+I_k=K$. Нека $x_i\in K$ са *произволни* елементи. Ще докажем, че съществува $a\in K$, такова че:

$$\begin{aligned}a&\in x_1+I_1\\a&\in x_2+I_2\\&\vdots\\a&\in x_n+I_n\end{aligned} \tag{9}$$

\iff

$$\begin{aligned}x_1&\in a+I_1\\x_2&\in a+I_2\\&\vdots\\x_n&\in a+I_n\end{aligned}$$

скрий

***Частен случай***: $n=2$.
Нека $1=e_1+e_2$, където $e_1,e_2$, са елементи на $I_1,I_2$.
Нека $a=x_1e_2+x_2e_1$. Тогава:

$$\begin{aligned} a-x_1 &= x_1e_2-x_1+x_2e_1 \\ &= x_1(e_2-1)+x_2e_1 \\ &= (x_2-x_1)e_1 \\ &\in I_1 \end{aligned} \tag{10}$$

Следователно $a\in x_1+I_1$.
Аналогично и $a\in x_2+I_2$. $\square$

За общия случай ще направим конструктувно доказателство - т.е ще покажем как се намира прословутото $a$. За целта първо ще образуваме едни коефициенти - $d_1,d_2,\cdots,d_n$. Ще покажем как се образува само $d_1$, останалите стават аналогично.

$$\begin{matrix} {}_1 & + & I_2 & = & K \\ I_1 & + & I_3 & = & K \\ & & \vdots & & \\ I_1 & + & I_n & = & K \end{matrix} \iff \left\{\left| \begin{matrix} \exists & a_2\in I_1 & \& & b_2\in I_2 & : & 1=a_2+b_2 \\ \exists & a_3\in I_1 & \& & b_3\in I_3 & : & 1=a_3+b_3 \\ & & & \vdots & & \\ \exists & a_n\in I_1 & \& & b_n\in I_n & : & 1=a_n+b_n \end{matrix}\right.\right\}\times \tag{11}$$

Та значи умножаваме получените равенства и получаваме:

$$\begin{aligned} 1 &= (a_2+b_2)(a_3+b_3)\cdots(a_n+b_n) \\ 1 &= A+b_2b_3\cdots b_n \end{aligned} \tag{12}$$

Където $A$ е сумата на всички членове, в които участва поне едно $a_i$. Не е трудно да се провери, че:

- $A\in I_1$ - защото във всяко едно от събираемите в $A$ участва член от $I_1$, следователно и сумата е от $I_1$;
- $b_2b_3\cdots b_n\in\bigcap_{i=2}^n I_i=J_1$ - всяко $b_i$ участва в $I_i$, следователно и произведението им участва във всяко $I_i$, т.е в тяхното сечение.

Всъщност, получихме че $I_1+J_1=K$. Използваме доказаното от частния случай (при $n=2$) за идеалите $I_1,J_1$ и числата $x_1,x_2=1,0$ и кръщаваме резултата $d_1$:

$$\exists d_1: \begin{matrix} d_1 & \in & 1+I_1 \\ d_1 & \in & 0+J_1 \end{matrix} \iff \begin{matrix} d_1-1 & \in & I_1 \\ d_1 & \in & J_1 \end{matrix} \qquad J_1=\bigcap_{i=2}^n I_i \tag{13}$$

Показахме как се построява $d_1$. Сега приемаме, че сме построили $d_2,d_3,\cdots,d_n$ по аналогичен начин, и си **построяваме** $a$ (т.е това което търсим) по следния начин:

$$a=x_1d_1+x_2d_2+\cdots+x_nd_n \tag{14}$$

Сега ще докажем, че изпълнява условията на задачата: Нека $x_i\in I_i$ е произволен елемент. Да си образуваме $a-x_i$ ::

(15)

$$
\begin{aligned}
a - x_i &= x_1 d_1 + x_2 d_2 + \cdots + x_i d_i - x_i + \cdots + x_n d_n \\
&= \underbrace{x_1 d_1}_{\in I_i} + \underbrace{x_2 d_2}_{\in I_i} + \cdots + \underbrace{x_i (d_i - 1)}_{\in I_i} + \cdots + \underbrace{x_n d_n}_{\in I_i} \in I_i
\end{aligned}
$$

Следователно и $a - x_i \in I_i$, т.е $a \in x_i + I_i$. Разсъждението е вярно за произволно $i$, следователно е вярно за всяко. С това теоремата е доказана.

### Оригинален вид

Естествено, горната теорема е перфектна за впечатляване на колежки, но по-опростеният вариант също не е за изпускане.
Това е КТО, както е била известна през трети век на китайците:

Дадени са $n_1, n_2, \cdots, n_k$ естествени числа, всеки две от които са взаимно прости. Тогава, за всеки $a_1, a_2, \cdots, a_k$ цели числа системата:

$$
\begin{aligned}
x &\equiv a_1 \pmod{n_1} \\
x &\equiv a_2 \pmod{n_2} \\
&\cdots \\
x &\equiv a_k \pmod{n_k}
\end{aligned}
\tag{16}
$$

Има решение. Нещо повече, системата има единствено решение $x_0$ в интервала $[0, a_1 a_2 \cdots a_k)$ и всяко друго нейно решение има вида $x_0 + m * a_1 a_2 \cdots a_k$ за някое цяло m.
Ето една задача, чието решение изисква да се използват делимости и КТО.

## *Директна сума на пръстени*

### Дефиниция

Нека $K, M$ са пръстени. Дефинираме операцията $\oplus$:

$$
K \oplus M = \{(a, b) | a \in K \& b \in M\} \tag{17}
$$

Като в това множество дефинираме операции събиране и умножение :

$$
\begin{aligned}
(a, b) + (c, d) &= (a + c, b + d) \\
(a, b). (c, d) &= (a. c, b. d)
\end{aligned}
\tag{18}
$$

### Твърдение

Нека $K$ е комутативен пръстен с 1, и $I_1, I_2, \cdots, I_n$ са негови взаимно прости идеали. Тогава:

$$
K / \bigcap_{s=1}^{n} I_s \cong (K/I_1) \oplus (K/I_2) \oplus \cdots \oplus (K/I_n) \tag{19}
$$

скрий

Ще използваме теоремата за хомоморфизмите при пръстени - именно ще намерим хомоморфизъм и ще докажем, че той има подходящо ядро.
Ще използваме естествения хомоморфизъм разширен над директна сума от идеали - именно:

$$\begin{aligned} \varphi : K &\to (K/I_1) \oplus (K/I_2) \oplus \cdots \oplus (K/I_n) \\ \varphi(a) &= (a + I_1, a + I_2, \cdots, a + I_n) \end{aligned} \tag{20}$$

Сега ще докажем **хомоморфизъм**:

$$\begin{aligned} \varphi(a \overset{+}{\cdot} b) &= ((a \overset{+}{\cdot} b) + I_1, (a \overset{+}{\cdot} b) + I_2, \cdots, (a \overset{+}{\cdot} b) + I_n) \\ &= ((a + I_1) \overset{+}{\cdot} (b + I_1), (a + I_2) \overset{+}{\cdot} (b + I_2), \cdots, (a + I_n) \overset{+}{\cdot} (b + I_n)) \\ &= (a + I_1, a + I_2, \cdots, a + I_n) \overset{+}{\cdot} (b + I_1, b + I_2, \cdots, b + I_n) \\ &= \varphi(a) \overset{+}{\cdot} \varphi(b) \end{aligned} \tag{21}$$

Сега ще докажем, че $\mathrm{Ker}\,\varphi = \bigcap_{s=1}^{n} I_s$.

> Доказателството на посочения факт **силно** се различава от даденото на лекции.
> Посоченото тук **НЕ** използва КТО … и според мен е доста по-лесно.

Нулевият елемент на образа е $\varphi(0) = (0 + I_1, 0 + I_2, \cdots, 0 + I_n) = (I_1, I_2, \cdots, I_n)$. Питаме се, кои елементи отиват в нулевия - т.е кои са тези $a \in K$, за които:

$$\varphi(a) = (a + I_1, a + I_2, \cdots, a + I_n) = (I_1, I_2, \cdots, I_n) \tag{22}$$

Всъщност искаме $a + I_i = I_i \quad \forall i = \overline{1, n}$. Това е равносилно на $a \in I_i \quad \forall i = \overline{1, n}$. Следователно получихме

$$a \in \bigcap_{s=1}^{n} I_s \tag{23}$$

Сега използваме теоремата за хомоморфизмите и сме готови!

page revision: 13, last edited: 26 Jun 2011, 21:08 (741 days ago)