Идеали в пръстен. Факторпръстени. Хомоморфизми на пръстени. Теорема за епиморфизмите на пръстени.

Определение:

Нека K е пръстен и $I \subseteq K$ *,* $I \neq \varnothing$*. Казваме, че I е идеал на K и пишем* $I \lhd K$ *, ако са изпълнени следните условия:*

1) I е подгрупа в адитивната група на K, т.е. от a, $b \in I \Rightarrow a + b \in I$ *и* $-a \in I$*;*

2) за $\forall\, i \in I$ *и* $\forall\, a \in K$ *имаме:* $ai \in I$ *и* $ia \in I$*.*

Ако пръстенът е комутативен е достатъчно да проверим само едното от: $ai \in I$, $ia \in I$.

Примери:

1) несобствените подпръстени на даден пръстен, т.е. нулевият подпръстен и самият пръстен, са очевидно идеали, които се наричат несобствени идеали. Идеалът $I=\{0\}$ се нарича нулев идеал.

2) Нека $C[a, b]$ е множеството на непрекъснатите функции дефинирани в [a ,b] с обичайните две операции, с които $C[a, b]$ е пръстен.

Разглеждаме $I=\{ f(x) \in [a, b] \mid f(x_0)=0 \}$ за някое фиксирано x_0. Лесно се проверява, че I е идеал.

3) очевидно е, че всеки идеал е подпръстен. Обратното не е вярно тъй като диагоналните матрици от даден ред очевидно образуват подпръстен, който не е идеал. Защо?

4) В пръстена на целите числа **Z**, множеството от числата, които се делят на дадено фиксирано число *n* е идеал, който се означава с ***n*Z.**

5) Във всяко поле единствените идеали са тривиалните т.е. полетата нямат собствени идеали. Наистина нека *F* е поле и *F'* е идеал на *F*. Да допуснем, че $I \neq \{0\}$. Нека $a \in I$ и $a \neq 0$. Понеже *F* е поле, то $\exists\ a^{-1}$. Тогава $aa^{-1} \in I \Rightarrow e \in I$ (единицата). Ако *b* е произволен елемент на *F,* тогава $b = b.e$, но $e \in I \Rightarrow b \in I$ и тъй като *b* е произволен $\Rightarrow F \equiv I$. От тези разсъждения става ясно, че ако един идеал съдържа единицата на даден пръстен то този идеал съвпада с пръстена.

Факторпръстени

Нека *K* е пръстен и $I \lhd K$. Тъй като адитивната група на *K* е комутативна, идеалът *I* ще бъде нормална подгрупа на адитивната група на *K*. Да разгледаме факторгрупата на адитивната група на *K* по идеала *I.*

$K/I = \{a + I \mid a \in K\}$ – факторгрупа. Както знаем тези съседни класове се събират по следния начин

$$(a + I)+(b + I)=(a + b)+ I$$

Също от по-рано знаем

$$a + I=b + I \Leftrightarrow a - b \in I. \qquad (*)$$

Дефинираме произведение на съседни класове в K/I по следния начин:

$$(a + I)(b + I) = ab +I$$

При този начин на дефиниране на произведение на адитивни съседни класове трябва да се провери, че тази операция е дефинирана коректно. По-точно трябва да проверим, че ако

$$a' + I = a + I \ \text{ и } \ b' + I = b + I.$$

Тогава: $a'b' + I \equiv ab + I$. Наистина от $a' + I = a + I$ имаме $a - a' \in I$. Следователно $a - a' = i \in I$ т.е. $a = a' + i$

от $b' + I = b + I$ имаме $b - b' \in I$. Следователно $b - b' = j \in I$ т.е. $b = b' + j$.

Поради това

$$ab - a'b' = aj + ib + ij \in I ,$$

което означава, че $ab + I = a'b' + I$. С това коректността на произведението на съседни класове е доказано.
И така в множеството на съседните класове $K/I = \{ a + I \mid a \in K \}$ имаме две операции:

$$(a + I) + (b + I) = (a + b) + I \text{ (наследна от групите)}$$

и дефинираното от нас произведение

$$(a + I)(b + I) = ab + I$$

<u>Твърдение:</u> *Относно тези операции* K/I *е пръстен, който се нарича факторпръстен на пръстена K по идеала I.*

<u>Доказателство:</u>
Тъй като адитивната група на *K* е комутативна, факторгрупата K/I на тази адитивна група също ще е комутативна. Това означава, че K/I относно "+" удовлетворява първите четири аксиоми за пръстен. Остава да проверим, че умножението асоциативно и, че е верен дистрибутивният закон.
Имаме

$$[(a + I)(b + I)](c + I) = (ab + I)(c + I) = (ab)c + I$$

и

$$(a + I)[(b + I)(c + I)] = (a + I)(bc + I) = a(bc) + I$$

Понеже умножението в *K* е асоциативно от тези равенства следва

$$[(a + I)(b + I)](c + I) = (a + I)[(b + I)(c + I)],$$

с което доказахме, че умножението във факторгрупата също е асоциативно.
За да докажем дистрибутивния закон разглеждаме равенствата:

$$[(a + I) + (b + I)](c + I) = [(a +b) + I](c +I) = (a + b)c + I$$

$$(a + I)(c + I) + (b + I)(c + I) = (ac +I) + (bc + I) = (ac +bc) + I$$

Понеже в пръстена *K* имаме $(a + b)c = ac + bc$ от тези равенства получаваме, че дистрибутивният закон е верен и в факторпръстена. По същия начин се проверява и другия дистрибутивен закон (когато множителят е от ляво). И така доказахме, че факторпръстенът е пръстен.

<u>Пръстен по остатъците по модул *n*</u>

Разглеждаме факторпръстена на пръстена Z по идеала nZ.
Този факторпръстен се нарича пръстен на остатъците по модул *n* и се бележи с Z_n. Съгласно (*)

$$k + \boldsymbol{nZ} = l + \boldsymbol{nZ} \Leftrightarrow k - l \in \boldsymbol{nZ}$$

т.е. съседните класове $k + nZ$ и $j + nZ$ са равни тогава и само тогава, когато *k* и *l* при делене на *n* да дават един и същ остатък.

Имаме:

остатъци	0	1	2	……..	*n* - 1
съседни класове	***nZ***	***1+nZ***	***2+nZ***		***(n -1) + nZ***

Всяко цяло число ще попадне точно в един от съседните класове взависимост от това какъв е остатъкът му при делене с *n* следователно ***nZ, 1+nZ, … , (n – 1)+ nZ*** са всичките съседни класове на факторпръстена nZ. Освен това всеки два от тези съседни класове са различни. Поради това броят на съседните класове е равен точно на *n*, с което доказахме, че $|Z_n| = n$.

<u>Пример:</u>
Разглеждаме факторпръстена $Z_3 = {}^{Z}\!/_{3Z}$ имаме $\boldsymbol{Z_3}$ ***= {3Z, 1+3Z, 2+3Z}.*** За краткост полагаме: *3Z=*$\overline{0}$, *1+3Z=*$\overline{1}$, *2+3Z=*$\overline{2}$. В този факторпръстен имаме

$$\overline{1} + \overline{1} = \boldsymbol{(1 + 3Z) + (1 + 3Z) = 2 + 3Z} = \overline{2}$$
$$\overline{2} + \overline{2} = \boldsymbol{(2 + 3Z) + (2 + 3Z) = 4 + 3Z = 1 + 3Z} = \overline{1}$$
$$\overline{1} * \overline{1} = \boldsymbol{(1 + 3Z)(1 + 3Z) = 1 + 3Z} = \overline{1}$$
$$\overline{2} * \overline{2} = \boldsymbol{(2 + 3Z)(2 + 3Z) = 4 + 3Z = 1 + 3Z} = \overline{1}$$

По подробно операциите в този пръстен са дадени от таблиците:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

От таблицата става ясно, че в $\boldsymbol{Z_3}$ има единица и, че всеки ненулев елемент е обратим $\Rightarrow \boldsymbol{Z_3}$ е поле с три елемента. Факторпръстенът $\boldsymbol{Z_4}$ не е поле, защото в него има делители на нулата ($\overline{2} * \overline{2} = \overline{0}$). По натътък ще видим, че Z_n е поле тогава и само тогава, когато *n* е просто.

<u>Хомоморфизми на пръстени</u>

<u>Определение:</u> *Нека K и K' са пртени. Кзваме, че изображението*

$$K \xrightarrow{\varphi} K'$$

е хомоморфизъм на K в K', ако от

$$x \xrightarrow{\varphi} x' \quad и \quad y \xrightarrow{\varphi} y'$$

тогава

$$x+y \xrightarrow{\varphi} x'+y' \text{ и } xy \xrightarrow{\varphi} x'y'$$

т.е., ако φ е хомоморфизъм ба адитивната група, който има допълнителното свойство, че изобразява произведението в произведение.
Ако φ е "върху", казваме, че φ е епиморфизъм на K върху K'.
Ако φ е 1-1 изображение, казваме, че φ е изоморфизъм между K и K'.

<u>Твъдение 1:</u> *Нека K и K' са пръстени и $K \xrightarrow{\varphi} K'$ е хомоморфизъм на тези пръстени. Тогава $Im(\varphi)$ е подпръстен на K'.*

<u>Доказателство</u>:
Тъй като φ е хомоморфизъм на адитивните групи, образът е подпръстен на адитивната група на K'. С това изяснихме, че е изпълнено първото изискване за подпръстен. Нека $a', b' \in Im(\varphi)$. Тогава $\exists a,\ b \in K$ такива, че $a \xrightarrow{\varphi} a'$ и $b \xrightarrow{\varphi} b'$. Понеже φ е хомоморфизъм $ab \xrightarrow{\varphi} a'b'$, *което означава, че $a'b' \in Im(\varphi)$.*□

<u>Определение:</u> *Нека $K \xrightarrow{\varphi} K'$ е хомоморфизъм на K в K'. Ядрото на този хомоморфизъм наричаме*

$$Ker(\varphi)=\{\, a \in K \mid a \xrightarrow{\varphi} 0' \,\},$$

Където $0'$ е нулевият елемент на K'

<u>Твърдение 2:</u> *Ядрото на φ е идеал на пръстена K.*

<u>Доказателство</u>:
Тъй като $Ker(\varphi)$ съвпада с ядрото на хомоморфизма адитивните групи на пръстените, съгласно това, което знаем от групите имаме, че $Ker(\varphi)$ е подгрупа на адитивната група на *K*. Остава да проверим второто изискване за идеал:

Нека $i \in Ker(\varphi)$ и $a \in K$. Тогава $i \xrightarrow{\varphi} 0'$. Ако $a \xrightarrow{\varphi} a'$, имаме

$$ai \xrightarrow{\varphi} a'0' = 0' \Rightarrow ai \in Ker(\varphi),$$

$$ia \xrightarrow{\varphi} 0'a' = 0' \Rightarrow ia \in Ker(\varphi),$$

с което Тв2 е доказано.□

<u>Теорема 2:</u> *Нека K е пръстен и $I \triangleleft K$. Тогава изображението $a \xrightarrow{\pi} a+I, \forall a \in K$ е епиморфизъм на K върху факторпръстена K/I. При това $Ker(\pi) \equiv I$. Този епиморфизъм се нарича естествен епиморфизъм на K върху факторпръстена K/I.*

__Доказателство__:

От групите знаем, че π е епиморфизъм на адитивната група на K върху адитивната група на K/I. Също при групите изяснихме, че $Ker(\pi)$ съвпада с I. Остава да проверим, че π изобразява призведението в произведение.

Нека $a, b \in K$. Тогава

$$a \xrightarrow{\pi} a + I,$$

$$b \xrightarrow{\pi} b + I,$$

$$ab \xrightarrow{\pi} ab + I .$$

Понеже $ab+ I=(a+ I)(b+ I)$ имаме, че

$$ab \xrightarrow{\pi} (a + I)(b + I)$$

т.е. наистина π изобразява произведението в произведение.□

__**Теорема (за епиморфизмите на пръстените):**__ *Нека* $K \xrightarrow{\varphi} K'$ *е епиморфизъм на пръстена K върху пръстена K'. Нека I= Ker(*φ*). Разглеждаме изображението*

$$a + I \xrightarrow{\psi} a',$$

където $a \xrightarrow{\varphi} a'$. *Тогава* ψ *е изоморфизъм между факторпръстена* K/I *и* K'.

__Доказателство__:

При групите вече изяснихме, че ψ е изоморфизъм на адитивната група на K/I и адитивната група на K' (теоремата за епиморфизма на групи). Остава да проверим, че ψ изобразява произведението в произведение. Нека $a+I$ и $b+I$ са два произволни съседни класа от факторпръстена K/I.

Ако

$$a \xrightarrow{\varphi} a' \quad и \quad b \xrightarrow{\varphi} b'$$

тогава

$$ab \xrightarrow{\varphi} a'b'.$$

Следователно $ab + I \xrightarrow{\psi} a'b'$. Понеже $ab+I=(a+I)(b+I)$ имаме, че $(a+I)(b+I) \xrightarrow{\psi} a'b'$. Тъй като $a'=\psi\ (a+I)$ и $b'=\psi\ (b+I)$ получаваме

$$(a+I)(b+I) \xrightarrow{\psi} \psi\,(a+I)\,\psi\,(b+I).$$ □