ЛЕКЦИЯ 26

ИДЕАЛИ В ПРЪСТЕН. ФАКТОРПРЪСТЕНИ. ХОМОМОРФИЗМИ НА ПРЪСТЕНИ. ТЕОРЕМА ЗА ЕПИМОРФИЗМИТЕ НА ПРЪСТЕНИ.

Определение. *Нека K е прѣстен и $I \subseteq K$, $I \neq \emptyset$. Казваме, че I е идеал на K и пишем $I \lhd K$, ако са изпѣлнени следните условия:*

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

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

Ако прѣстенѣт е комутативен, достатѣчно е 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 $x_0 \in [a, b]$. Лесно се проверява, че I е идеал.

3) Очевидно е, че всеки идеал е подпръстен. Обратното не е вярно. Така например в пръстена на квадратните матрици от даден ред, диагоналните матрици образуват подпръстен, който не е идеал. Защо? Кон-

стантите в пръстена на полиномите също образуват подпръстен, който не е идеал.

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

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

Задача. *Да се докаже, че всяка подгрупа на адитивната група на $\mathbb{Z}$ е идеал в $\mathbb{Z}$.*

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

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

Съгласно Лекция 22, Твърдение 6 имаме

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

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, съгласно (*) имаме $a - a' = i \in I$ и $b - b' = j \in I$.

Като умножим равенствата $a = a' + i$ и $b = b' + j$, получаваме

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

От (*) следва че $ab+I = a'b'+I$. С това коректността на произведението на съседни класове е доказано. И така в множеството на адитивните съседните класове $K/I = \{a + I \mid a \in K\}$ имаме две операции:

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

и дефинираното от нас произведение

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

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

Доказателство:

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. Да припомним, че I е нулевият елемент на K/I и противоположният елемент на $a + I$ е $(-a) + I$. Остава да проверим, че умножението е асоциативно и, че са верни двата дистрибутивни закона. 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:

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

и

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

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.

Пръстен от остатъците по модул n

С $n\mathbb{Z}$ означаваме множеството на целите числа, които се делят на n. Да си припомним, че $n\mathbb{Z} \lhd \mathbb{Z}$.

Разглеждаме факторпръстена на пръстена $\mathbb{Z}$ по идеала $n\mathbb{Z}$. Този факторпръстен се нарича пръстен на остатъците по модул n и се бележи с $\mathbb{Z}_n$. Съгласно (*)

$$k + n\mathbb{Z} = l + n\mathbb{Z} \Leftrightarrow k - l \in n\mathbb{Z}, \qquad (\#)$$

т. е. съседните класове $k + n\mathbb{Z}$ и $l + n\mathbb{Z}$ са равни тогава и само тогава, когато k и l при делене на n дават един и същ остатък.

Нека $m \in \mathbb{Z}$ и $m = nq + r$, $0 \leq r < n$. Понеже $m - r \in n\mathbb{Z}$, от $(\#)$ става ясно, че $m + n\mathbb{Z} = r + n\mathbb{Z}$, т. е. всеки съседен клас на $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ съвпада с един от съседните класове

$$n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}. \qquad (\#\#)$$

От $(\#)$ следва, че съседните класове от $(\#\#)$ са ралични. Следователно

$$\mathbb{Z}_n = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}.$$

От последното равенство получаваме, че $|\mathbb{Z}_n| = n$.

Пример. *Разглеждаме факторпръстена* $\mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z}$, *имаме* $\mathbb{Z} = \{3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$. *За краткост полагаме:* $3\mathbb{Z} = \overline{0}$, $1 + 3\mathbb{Z} = \overline{1}$, $2 + 3\mathbb{Z} = \overline{2}$. *В този факторпръстен имаме*

$$\begin{aligned}
&\overline{1} + \overline{1} = (1 + 3\mathbb{Z}) + (1 + 3\mathbb{Z}) = 2 + 3\mathbb{Z} = \overline{2} \\
&\overline{2} + \overline{2} = (2 + 3\mathbb{Z}) + (2 + 3\mathbb{Z}) = 4 + 3\mathbb{Z} = 1 + 3\mathbb{Z} = \overline{1} \\
&\overline{1} + \overline{2} = (1 + 3\mathbb{Z}) + (2 + 3\mathbb{Z}) = 3 + 3\mathbb{Z} = 3\mathbb{Z} = \overline{0} \\
&\overline{1} * \overline{1} = (1 + 3\mathbb{Z})(1 + 3\mathbb{Z}) = 1 + 3\mathbb{Z} = \overline{1} \\
&\overline{2} * \overline{2} = (2 + 3\mathbb{Z})(2 + 3\mathbb{Z}) = 4 + 3\mathbb{Z} = 1 + 3\mathbb{Z} = \overline{1}
\end{aligned}$$

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 $\mathbb{Z}_3$ *има единица и, че всеки ненулев елемент е обратим. Следователно* $\mathbb{Z}_3$ *е поле с три елемента. Факторпръстенът* $\mathbb{Z}_4$ *не е поле, защото в него има делители на нулата* ($\overline{2} * \overline{2} = \overline{0}$). *По нататък ще видим, че* $\mathbb{Z}_n$ *е поле тогава и само тогава, когато* n *е просто.*

Хомоморфизми на пръстени

Определение. *Нека K и K' са пръстени. Казваме, че изображението*

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

е хомоморфизъм на K в K', ако φ изобразява произведение в произведение и сумата в сума в смисъл, че

$$\text{ако } x \xrightarrow{\varphi} x' \quad \text{и} \quad y \xrightarrow{\varphi} y',$$

тогава

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

т. е., ако φ е хомоморфизъм на адитивната група на K в адитивната група K', 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'.

Твърдение 1. *Нека K и K' са пръстени и $K \xrightarrow{\varphi} K'$ е хомоморфизъм на тези пръстени. Тогава $\operatorname{Im}(\varphi)$ е подпръстен на K'.*

Доказателство:

Нека $a', b' \in \operatorname{Im}(\varphi)$. 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 $a'b' \in \operatorname{Im}(\varphi)$. Съгласно Свойство 3 от лекция 23, $\operatorname{Im}(\varphi)$ е подгрупа на адитивната група на K'. Поради това $a'+b' \in K'$ и $-a' \in K'$.

Определение. *Нека $K \xrightarrow{\varphi} K'$ е хомоморфизъм на K в K'. Ядро на този хомоморфизъм наричаме*

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

където $0'$ е нулевият елемент на K'.

Твърдение 2. $\operatorname{Ker}(\varphi)$ *е идеал на пръстена K.*

Доказателство:

Тъй като φ е хомоморфизъм на адитивната група на K в адитивната група на K' и $\operatorname{Ker}(\varphi)$ е ядро на този хомоморфизъм, съгласно Свойство 4 от лекция 23, $\operatorname{Ker}(\varphi)$ е подгрупа на адитивната група на K. Остава да проверим второто изискване за идеал:

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

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

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

с което Твърдение 2 е доказано.

Теорема 1. *Нека K е пръстен и $I \lhd K$. Тогава изображението $a \xrightarrow{\pi} a + I$, $\forall a \in K$ е епиморфизъм на K върху факторпръстена K/I. При това $\mathrm{Ker}\,(\pi) \equiv I$. Този епиморфизъм се нарича естествен епиморфизъм на K върху факторпръстена K/I.*

Доказателство:

Съгласно Лекция 24, Теорема 2, π е епиморфизъм на адитивната група на K върху адитивната група на K/I и $\mathrm{Ker}\,(\pi)$ съвпада с I. Остава да проверим, че π изобразява произведението в произведение.

Нека a, $b \in K$. Тогава

$$\begin{aligned} a &\xrightarrow{\pi} a + I, \\ b &\xrightarrow{\pi} b + I, \\ ab &\xrightarrow{\pi} ab + I, \end{aligned}$$

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 2. (за епиморфизмите на пръстените) *Нека $K \xrightarrow{\varphi} K'$ е епиморфизъм на пръстена K върху пръстена K'. Нека $I = \mathrm{Ker}\,(\varphi)$. Разглеждаме изображението*

$$K/I \xrightarrow{\psi} K',$$

което се дефинира по следния начин:

$$a + I \xrightarrow{\psi} a', \text{ ако } a \xrightarrow{\varphi} a'.$$

Тогава ψ е изоморфизъм между факторпръстена K/I и K'.

Доказателство:

Съгласно Лекция 25, 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

$$a \xrightarrow{\varphi} a' \text{ и } b \xrightarrow{\varphi} b',$$

тогава

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

Трябва да докажем, че $(a+I)(b+I) \xrightarrow{\psi} a'b'$. Тъй като

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

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