Пръстени

Дефиниция (пръстен)

Нека $M \neq \varnothing$ е **непразно** множество и $+$ и $.$ са бинарни операции в M

Казваме, че M е **пръстен**, ако са изпълнени следните свойства:

1. M е абелева група относно събирането (**+**), т.е. за $\forall\, a,b,c \in M$:
   - $a+b=b+a,\ \forall\, a,b \in M$
   - $(a+b)+c=a+(b+c),\ \forall\, a,b,c \in M$
   - $\exists\, 0 \in M : a+0=0+a=a,\ \forall\, a \in M$
   - $\forall\, a \in M,\ \exists b \in M :\ a+b=0$
2. Асоциативност на умножението (**.**): $(ab)c=a(bc),\ \forall a,b,c \in M$
3. Два дистрибутивни закона:
   - $a(b+c)=ab+ac,\ \forall a,b,c \in M$
   - $(a+b)c=ac+bc,\ \forall a,b,c \in M$

Дефиниция (комутативен пръстен)

Нека M е пръстен.
Ако $ab=ba,\ \forall a,b \in M \Longrightarrow$ пръстенът е **комутативен**.

Дефиниция (пръстен с единица)

Нека M е пръстен.
Ако $\exists e \in M :\ ae=ea=a,\ \forall a \in M \Longrightarrow M$ е **пръстен с единица**.

Примери

Пример 1:
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ са *комутативни пръстени с единица*.
Непосредствено се проверява от дефинициите.

Пример 2:
Евклидовото пространство **не** е пръстен.
В този случай *умножение* дори не е бинарна операция, защото както знаем:

вектор.вектор = скалар (греда!)

Пример 3:
$M_{n,n}(\mathbb{R})$ е пръстен с единица.
Също непосредствено се проверява от дефиницията.

Пример 4:
$\mathbb{R}[x]$ – множеството от всички полиноми с реални коефициенти.
$\mathbb{R}[x]$ е също пръстен.

Пример 5:

Всички диференцируеми функции образуват пръстен

Пример 6:
Всички функции, които в дадена точка имат дадена стойност, образуват пръстен.
// $f(e) = 0$ примерно

Пример 7:
Всички булеви функции с операции *събиране по модул две* и *конюнкция* образуват пръстен (булев пръстен)[1]

Пример 8:
$6\mathbb{Z} = \{6n \mid n \in \mathbb{Z}\}$ е пръстен.

$6n.1 = 6n$, но $1 \notin 6\mathbb{Z} \Longrightarrow 6\mathbb{Z}$ е пръстен без единица.

Пример 9:
Нека разгледаме Z_n - класовете остатъци по модул n.

$Z_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$

$\bar{a} + \bar{b} = \bar{r}$, където $a + b \equiv r \pmod{n}$, $r \in \{0, 1, \ldots, n-1\}$

Сега дефинираме следната операция *умножение на класове*:
$\bar{a}.\bar{b} = \bar{t}$ и $a.b \equiv t \pmod{n}$

Непосредствено се проверява, че всички свойства от дефиницията са изпълнени, т.е.
Z_n с операциите *събиране на класове* и *умножение на класове* е пръстен от класовете остатъци по модул n.

Обратими елементи

Дефиниция (обратим елемент в пръстен)

Нека M е пръстен с единица и $a \in M$.
a наричаме **обратим**, ако $\exists b \in M : \ ab = ba = e$.

Следствие (единственост на обратния елемент)
Ако a е обратим, то $\exists! b : \ ab = ba = e$.
Отбелязваме $b = a^{-1}$

Доказателство:
Допускаме, че $\exists\, b_1, b_2$, такива че
$b_1 \mathrm{a} = ab_1 = e$ и $b_2 a = ab_2 = e$.

$b_1 = b_1 e = b_1(ab_2) = (b_1 a)b_2 = eb_2 = b_2 \implies b_1 = b_2 . \square$

Дефиниция (мултипликативна група на пръстен)

Нека M е пръстен с единица.

$M^* = \{a \in M \mid \exists b \in M : \ ab = ba = e\} \subsetneq M$
Т.е. M^* е множеството от всички обратими елементи на M.

//M^* е същинско подмножество на M, тъй като знаем, че нулата си няма обратен елемент, т.е. $0 \notin M^*$.

M^* се нарича **мултипликативна група** на пръстена M.

Сега ще покажем, че M^* е наистина мултипликативна група.

Нека $x, y \in M^*$

$(xy)y^{-1}x^{-1} = e$
$(y^{-1}x^{-1})(xy) = e \Longrightarrow xy \in M^*, \ (xy)^{-1} = y^{-1}x^{-1}$

$(x^{-1})^{-1} = x \in M^* \Longrightarrow x^{-1} \in M^*$

До тук за M^* имаме:

- $x, y \in M^* \Longrightarrow xy \in M^*$
- $(xy)z = x(yz)$ (асоциативността е в сила в M, т.е. и в M^*)
- $\exists 1 \in M^* : \ 1.a = a.1 = a, \ \forall a \in M^*$
- $x \in M^* \Longrightarrow x^{-1} \in M^*$

Така, по дефиния, можем да твърдим, че M^* е група относно умножението.

Примери

$Z^* = \{1, -1\} = C_2$ е мултипликативната група на $\mathbb{Z}$.

$Q^* = \mathbb{Q} \setminus \{0\}$ е мултипликативната група на $\mathbb{Q}$

$R^* = \mathbb{R} \setminus \{0\}$ е мултипликативната група на $\mathbb{R}$

$C^* = \mathbb{C} \setminus \{0\}$ е мултипликативната група на $\mathbb{C}$

$M_{n,n}^*(\mathbb{R}) = GL_n(\mathbb{R})$ е мултипликативната група на $M_{n,n}(\mathbb{R})$ (по дефиниция)

Дефиниция (поле)

Комутативен пръстен с единица,в който всеки ненулев елемент е обратим, наричаме **поле**.

Примери

От дефиницията следва, че $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ са полета.

Дефиниция (подпръстен)

Нека M е пръстен и $\varnothing \neq M' \subset M$ е пръстен относно същите операции.
Казваме, че M' е **подпръстен** на M.

Отбелазваме: $M' \subset M$

Дефиниция (подполе)

Нека F е поле и $\varnothing \neq F' \subset F$ е поле относно същите операции.
Казваме, че F' е **подполе** на F.

Примери

1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
2. $\mathbb{R} \subset \mathbb{R}[x]$
3. $6\mathbb{Z} \subset \mathbb{Z}$

Твърдения

Твърдение 1

Нека M е пръстен и $\varnothing \neq K \subset M$

K е подпръстен

$$\iff \begin{cases} a+b \in K, \ \forall a,b \in K \\ -a \in K, \ \forall a \in K \\ ab \in K, \ \forall a,b \in K \end{cases} \iff \begin{cases} a-b \in K, \ \forall a,b \in K \\ ab \in K, \ \forall a,b \in K \end{cases} \tag{1}$$

Доказателство:
За първата група от свойства твърдението е очевидно - лесно се проверява, че са изпълнени всички свойства за пръстен - комутативността и асоциативността идват от пръстена, обратния елемент идва директно от условието, а нулата се получава като съберем елемент с неговия обратен.
Сега ще докажем, че втората група от условия е равносилна на първата.
$|\Rightarrow|$ очевидно - от $a+b \in K \& -a \in K \Rightarrow a+(-b) \in K$.
$|\Leftarrow|$ Първо ще докажем, че $0 \in K$. Ами $a-a=0 \in K$. Сега заместваме a с 0 и получаваме $0-b \in K \quad \forall b \in K$, следователно $-b \in K \ \forall b \in K$. Следователно $a-(-b)=a+b \in K \ \forall a,b \in K$. Т.е доказахме, че от

$a-b \in K \, \forall a,b \in K \Rightarrow a+b \in K \, \forall a,b \in K \& -a \in K \, \forall a \in K.$

Твърдение 2

Нека F е поле, $\varnothing \neq K \subset F$ и $\exists a \neq 0 \in K$

K е подполе

$$\iff \begin{cases} a-b \in K, \, \forall a,b \in K \\ a^{-1} \in K, \, \forall a \neq 0 \in K \\ ab \in K, \, \forall a,b \in K \end{cases} \tag{2}$$

Доказателство:
$| \Leftarrow |$ Използваме горното твърдение и получаваме, че K е пръстен, в който освен това всеки ненулев елемент си има обратен. По дефиницията за поле следва, че K е поле.

Делители на нулата

Дефиниция (делители на нулата)

Нека M е пръстен и $a \neq 0, \, b \neq 0 \in M$, такива, че $ab = 0$
a и b наричаме **делители на нулата** в пръстена M

Пример

Разглеждаме $M_2(\mathbb{R})$

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R})$$

$$A.A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$\Longrightarrow A$ е делител на нулата.

Твърдение

Ако M е пръстен с единица **не** е възможно един елемент да е едновременно обратим и делител на нулата.

Доказателство:
Допускаме, че е възможно, т.е.
$\exists a \in M$, такъв, че да е едновременно обратим и делител на нулата.

a – обратим $\Longrightarrow \exists\, a^{-1} \in M$
a – делител на нулата $\Longrightarrow \exists\, b \neq 0 \in M :\ ab = 0$

$ab = 0 \iff a^{-1}(ab) = a^{-1}0 \iff b = 0$ – противоречие!

Следователно допускането не е вярно, т.е. не съществува елемент, който да е едновременно обратим и делител на нулата. □

Теорема 1

$\mathbb{Z}_n$ - пръстен от класовете остатъци по модул n и $\bar{a} \neq \bar{0} \in \mathbb{Z}_n$

1. $\bar{a}$ е делител на нулата $\iff (a, n) > 1$
2. $\bar{a}$ е обратим $\iff (a, n) = 1$

Доказателство:
1.
$| \Leftarrow |$
Нека $(a, n) = d > 1$. Тогава съществува разлагане на числата a, n:
$a = a_1 d,\ a_1 \neq 0 \in \mathbb{Z}$
$n = n_1 d,\ n_1 \neq 0 \in \mathbb{Z}\ (\overline{n_1} \neq \bar{0})$
Сега ще покажем, че произведението на a и n_1 е 0, т.е че a е делител на 0.

$$an_1 = (a_1 d)n_1 = a_1(dn_1) = a_1 n = 0 \tag{3}$$

получихме 0 (при сметки в група $\mathbb{Z}_n$), защото n при деление с остатък n връща 0.

$| \Rightarrow |$
Нека a е делител на 0. Тогава съществуват $a, b \in \mathbb{Z}_n$, различни от 0 и $\bar{a}.\bar{b} = 0$. Да допуснем, че $(n, a) = 1$. Следователно $n/a.b \& (n, a) = 1 \Rightarrow n/b$. От тук получаваме, че $\bar{b} = 0$. Противоречие! Следователно $(n, a) > 1$.

2.
$| \Rightarrow |$ Да допуснем, че a е обратим и $(a, n) > 1$. Следователно (от 1) получаваме, че a е делител на 0. Противоречие (не може хем да е обратим, хем да е делител на 0).
$| \Leftarrow |$ Ще използваме теоремата на Безу: Щом $(a, n) = 1$ следователно съществуват цели числа b, c такива че:

$$ab + nc = 1 \tag{4}$$

Да разгледаме това равенство в групата $\mathbb{Z}_n$:

$$\bar{a}\bar{b} + \underbrace{\bar{n}}_{0}\bar{c} = \bar{1} \tag{5}$$

Следователно $\bar{a}\bar{b} = \bar{1}$, т.е намерихме обратния елемент на $\bar{a}$ - именно $\bar{b}$.
Следователно a е обратим.

Теорема 2

$\mathbb{Z}_n$ е поле $\iff$ n е просто.

Доказалтество:
Ами ако допуснем, че съществува поле $\mathbb{Z}_n$, при n не просто, тогава със сигурност съществува поне един делител на n различен от 1 - нека го наречем a. Т.е имаме $(n, a) = a > 1$. От тук a е делител на нулата, следователно не е обратим. Противоречие с факта, че $\mathbb{Z}_n$ е поле (всеки елемент трябва да е обратим).

Теорема на Ойлер-Ферма

Нека $a, n \in \mathbb{N},\ n > 1,\ (a, n) = 1$

$\implies a^{\varphi(n)} \equiv 1 \pmod{n}$

В частност, ако $n = p$ е просто, то $a^{p-1} \equiv 1 \pmod{p}$ (това е теоремата на Ферма).

Доказателство:
Да разгледаме мултипликативната група на $\mathbb{Z}_n$:

$$\mathbb{Z}_n^* = \{a | (a, n) = 1\} \tag{6}$$

Очевидно $|\mathbb{Z}_n^*| = \varphi(n)$ - броя на взаимно простите с n числа, по-малки от n.
От теоремата на Лагранж имаме, че за всеки елемент $\bar{a} \in \mathbb{Z}_n^*$: $|\bar{a}| / \varphi(n)$ - т.е реда на елемента $\bar{a}$ дели реда на групата, който е $\varphi(n)$. Е да, ама както знаем ред на елемента се дефинира като минимален брой пъти, които трябва да умножим елемента със себе си за да получим 1. Следователно:

$$\underbrace{\bar{a}.\bar{a}.\bar{a} \cdots . \bar{a}}_{|a|} = \bar{1} \implies \underbrace{\bar{a}.\bar{a}.\bar{a} \cdots . \bar{a}}_{\varphi(n) = |a|k} = \bar{1} \tag{7}$$

От тук вече очевидно $a^{\varphi(n)} \equiv 1 \pmod{n}$ разбира се за $(a, n) = 1$.

Теорема на Уилсън

Нека $p \in \mathbb{N}$ е просто $\implies (p-1)! \equiv -1 \pmod{p}$.

Доказателство:
Ще използваме полето $\mathbb{Z}_p$ при p просто.
Първо ще докажем, че $\bar{x} \neq \bar{x}^{-1}$ за всяко $\bar{x} \neq \bar{1}, \overline{p-1}$.
Ами да проверим кога $\bar{x}\bar{x} = \bar{1}$. По дефиниция имаме $x.x \equiv 1 \pmod{p}$.
Следователно $p / x^2 - 1 = (x-1)(x+1)$. Тъй като p е просто имаме $p / x - 1$ или

$p/x+1$. Разбира се $x \in \mathbb{Z}_p$ следователно единствените 2 стойности са $x=\bar{1}$ и $x=\overline{p-1}$.

Сега да разгледаме

$$\bar{2}.\bar{3}.\cdots.\overline{p-2} \tag{8}$$

Тъй като обратния на всеки елемент е различен от самия него - т.е е някой от другите, то всички елементи се групират по двойки - всеки със неговия обратен (каква идилия) и в крайна сметка излиза,че цялото произведение е $\bar{1}$. Така получаваме окончателно, че

$$\bar{1}.\bar{2}.\bar{3}.\cdots\overline{p-2}.\overline{p-1}=\bar{1}.\bar{1}.\overline{-1}=\overline{-1} \tag{9}$$

Т.е $(p-1)! \equiv -1 \pmod{p}$.

Footnotes

1. На който му се занимава, да докаже защо аджеба всички тези примери са коректни примери за пръстени

page revision: 7, last edited: 8 May 2012, 01:12 (425 days ago)