Пръстени - определение, свойства

Сайт: learn.fmi.uni-sofia.bg
Курс: Алгебра 2, поток 1, летен семестър 2021/2022
Книга: Пръстени - определение, свойства

Разпечатано от: Мартин Попов
Дата: Saturday, 16 April 2022, 13:46

Съдържание

1. Определение

Определение:
Нека M е непразно множество, в което има две бинарни операции - условно едната наричаме събиране " $+$ ", а другата умножение ".". Казваме, че M е пръстен относно въведените операции, когато са изпълнени свойствата:

- M е Абелева група относно операцията "+", т.е.
  - $(a+b)+c=a+(b+c),\ \forall a,b,c \in M$ - *асоциативност*;
  - $a+b=b+a,\ \forall a,b \in M$ - *комутативност*;
  - съществува нулев елемент, за който $a+0=a,\ \forall a \in M$;
  - за всеки елемент $a \in M$ съществува $b \in M$, за които $a+b=b+a=0$.}
- $(a.b).c=a.(b.c),\ \forall a,b,c \in M$ - *асоциативност*.
- *дистрибутивни закони:*
  - $(a+b).c=a.c+b.c,\ \forall a,b,c \in M$;
  - $a.(b+c)=a.b+a.c,\ \forall a,b,c \in M$.

Определение:
Ако в пръстена M е изпълнен комутативния закон за умножението $ab=ba,\ \forall a,b \in M$, тогава пръстенът се нарича комутативен.

Определение:
Ако в пръстена M има елемент e, за който $ae=ea=a,\ \forall a \in M$, тогава пръстенът се нарича пръстен с единица.

Определение:
Нека M е пръстен с единица e . Казва се че елементът $a \in M$ е обратим, ако съществува такъв елемент $b \in M$ от пръстена, за който е изпълнено $a.b=b.a=e$

Определение:
Комутативен пръстен F с единица $(e \neq 0)$, в който всеки ненулев елемент е обратим се нарича **поле**. (*Забележка: Всяко поле има поне 2 елемента.*)

При определянето на пръстен в дефиницията са използвани основните свойства на числата, известни ни от училище и затова:

Примери за пръстени при числовите множества:

- Всички основни известни числови множества са комутативни пръстени с единица - пръстена на рационалните числа $\mathbb{Q}$, пръстена на реалните числа $\mathbb{R}$ и пръстена на комплексните числа $\mathbb{C}$. В тези числови множества само елемента 0 не е обратим и затова $\mathbb{Q}, \mathbb{R}$ и $\mathbb{C}$ са полета.
- Множеството на целите числа $\mathbb{Z}$ също е комутативен пръстен с единица. Единствените цели числа, на които обратните числа също са цели са $1, -1$, обратните на останалите цели числа са рационални, например $3^{-1}=\frac{1}{3} \notin \mathbb{Z}$. Поради тази причина целите числа $\mathbb{Z}$ образуват пръстен, но не образуват поле.
- Множеството $5\mathbb{Z}$ също е пръстен, но в него *няма* елемент, който да изпълнява условието $ae=ea=a,\ \forall a \in 5\mathbb{Z}$, затова $5\mathbb{Z}$ е пръстен без единица.

1.1. Примери(1) - Zn

Пример:

Нека n е естествено число и със $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ сме означили множеството от класовете остатъци по модул n, където $\overline{k} = \{k + ns \mid s \in \mathbb{Z}\}$. По подобен начин, по който дефинирахме събиране в $\mathbb{Z}_n$, може да се дефинира и умножение в множеството.

$$\overline{a} + \overline{c} = \overline{a+c}, \quad \overline{a}.\overline{c} = \overline{a.c}$$

Знаем, че за класовете остатъци е изпълнено

$$\begin{array}{rcl} a_1 \in \overline{a} & \Leftrightarrow & a_1 = a + ns_1 \quad \Leftrightarrow \quad \overline{a} = \overline{a_1} \\ c_1 \in \overline{c} & \Leftrightarrow & c_1 = c + ns_2 \quad \Leftrightarrow \quad \overline{c} = \overline{c_1} \end{array}$$

откъдето непосредствено получаваме

$$\begin{array}{rcl} a_1 + c_1 = a + c + n(s_1 + s_2) \in \overline{a+c} & \Rightarrow & \overline{a_1 + c_1} = \overline{a+c} \\ a_1.c_1 = a.c + n(c.s_1 + a.s_2 + ns_1s_2) \in \overline{a.c} & \Rightarrow & \overline{a_1.c_1} = \overline{a.c} \end{array}$$

По този начин се вижда, че операциите събиране и умножение в $\mathbb{Z}_n$ са коректно дефинирани. Лесно се установява, че са изпълнени аксиомите от дефиницията на пръстен и това е пример на краен комутативен пръстен с единица $\overline{1}$, който се нарича пръстен от класовете остатъци по модул n.
Например, таблицата за умножение в пръстена $\mathbb{Z}_6$ е следната:

умножение в $\mathbb{Z}_6$:

.	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Пример:
Пръстенът $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ от класовете остатъци по модул 2 е поле, защото има единствен ненулев елемнт $\overline{1}$, който е единицата в пръстена и е обратим. Полето $\mathbb{Z}_2$ е полето, което има най-малко елементи.

1.2. Примери(2)

Пример:
Нека да разгледаме множеството от всички квадратни матрици $M_{n\times n}(\mathbb{R})$. От курса по линейна алгебра, знаем как се събират и умножават матрици и за множеството $M_{n\times n}(\mathbb{R})$ тези две операции са бинарни. Знаем, ча при $n \geq 2$ умножението на матрици е некомутативно. Множеството от квадратните матрици е пример на некомутативен пръстен с единица (E- единичната матрица).

Пример:
Булев пръстен ще получим, ако вземем множеството $M = J_2^n$ от булевите $n-$ мерни вектори, където $J_2 = \{\mathfrak{o}, \mathfrak{1}\}$ и за $a = (a_1, \ldots, a_n) \in M$ и $b = (b_1, \ldots, b_n) \in M$ да разгледаме бинарните операции "изключващо ИЛИ" (сума по модул 2) $a \oplus b = (a_1 \oplus b_1, \ldots, a_n \oplus b_n)$ и конюнкция $a \wedge b = (a_1 \wedge b_1, \ldots, a_n \wedge b_n)$, като и двете операции са асоциативни и комутативни. От свойствата на тези булеви операции се установява, че:

- $(M, \oplus)$ е Абелева група относно дизюнкцията, където неутралния елемент е $\mathfrak{o} = (\mathfrak{o}, \ldots, \mathfrak{o})$ и симетричния на $a = (a_1, \ldots, a_n)$ е допълнението $\overline{a} = (\overline{a}_1, \ldots, \overline{a}_n)$, където $\overline{\mathfrak{o}} = \mathfrak{1}$, $\overline{\mathfrak{1}} = \mathfrak{o}$;
- изпълнен е дистрибутивния закон $a \wedge (b \oplus c) = (a \wedge b) \oplus (a \wedge c)$;
- векторът $\mathfrak{e} = (\mathfrak{1}, \ldots, \mathfrak{1})$ изпълнява условието $a \wedge \mathfrak{e} = a$.

По този начин се установява, че множеството $M = J_2^n$ от булевите $n-$ мерни вектори с операциите "изключващо ИЛИ" $a \oplus b$ (която играе ролята на събирането) и операцията конюнкция $a \wedge b$, която е вместо "." образува комутативен пръстен с единица, който се нарича булев пръстен. Характерно негово свойство, е че за произволен елемент $x \in M$ е изпълнено $x \wedge x = x$.

Пример:

Множеството на полиномите $\mathbb{R}[x]$ на една променлива и множеството на диференцируемите функции в $\mathbb{R}$ са примери на комутативни пръстени с единица..

1.3. Множества, които не са пръстени:

Пример- Множества, които не са пръстени:

- В множеството $\mathbb{N}$ на естествените числа събирането "+" и произведението "." са бинарни операции. Но, въпреки това естествените числа $\mathbb{N}$ не образуват пръстен, защото противоположните числа на естествените числа не са естествени числа.
- Ако V линейно пространство над поле F, тогава V е Абелева група относно събирането. Но няма бинарна операция умножение и затова в общия случай линейното пространство не е пръстен. Умножението $\lambda x \in V$ от определението на линейно пространство, не е бинарна операция, защото двата аргумента на тази операцията $\lambda \in F$ и $x \in V$ принадлежат на различни множества.
- Ако разгледаме геометричните вектори в тримерното пространство $\mathbb{R}^3$ при тях имаме дефинирана сума на вектори, спрямо която тримерните вектори, образуват Абелева група. По геометрия се дефинира и векторно произведение $\vec{a} \times \vec{b}$, което е бинарна операция в множеството на тримерните вектори. За събирането и векторното произведение са в сила дистрибутивните закони. Но векторното произведение не изпълнява асоциативния закон, а вместо това изпълнява тъждеството на Якоби: $(\vec{a} \times \vec{b}) \times \vec{c} + (\vec{b} \times \vec{c}) \times \vec{a} + (\vec{c} \times \vec{a}) \times \vec{b} = \vec{0}$. Така, че тримерните геометрични вектори с операциите сума и векторно произведение не образуват пръстен.

2. Свойства

Свойство 1.

Ако M е пръстен, тогава са изпълнени основните свойства за адитивната група на M:

- нулевият елемент на групата е единствен,
- за всеки елемент от групата има единствен противоположен елемент,
- уравнението $a + x = b$ има единствено решение $x = b + (-a) = b - a$, което се нарича разлика на двата елемента,
- Ако $a \in M$ и n е естествено число се дефинира n-кратно на елеменат като $\underbrace{a + \ldots + a}_{n} = na$. Изпълнени са

$$
\begin{aligned}
&(n+k)a = na + ka; \\
&n(k(a)) = (nk)a \qquad , \ \forall a, b \in M, \ \text{ и } \forall n, k \in \mathbb{N}; \ (\text{групата е абелева}) \\
&n(a+b) = na + nb
\end{aligned}
$$

Свойство 2.

а) За произволен елемент $a \in M$ е изпълнено $0.a = a.0 = 0$;

б) $-(ab) = (-a)b = a(-b), \ \forall a, b \in M$;

в) $a(b-c) = ab - ac, \ \ (a-b)c = ac - bc, \ \ \forall a, b, c \in M$.

Доказателство: а)

$$
\begin{gathered}
0a = (0+0)a = 0a + 0a \\
\Downarrow \\
0a + (-0a) = 0a + 0a + (-0a) \\
\Downarrow \\
0 = 0a
\end{gathered}
$$

Свойството $a.0 = 0$ се получава по аналогичен начин.

б) Като се използва, че в пръстена всеки елемент има единствен противоположен елемент и се приложи дистрибутивността се получава:

$$
\begin{aligned}
ab + (-a)b = (a + (-a))b = 0b = 0 \Rightarrow \quad -(ab) = (-a)b \\
ab + a(-b) = a(b + (-b)) = a0 = 0 \Rightarrow \quad -(ab) = a(-b)
\end{aligned}
$$

в) Нека $x = b - c$, тогава x е решение на уравнението $c + x = b$. Умножаваме от двете страни по a и получаваме $a(c + x) = ac + ax = ab$, следователно $ax = ab - ac$ откъдето виждаме, че $a(b - c) = ab - ac$.

□

2.1. Обобщена асоциативност

Свойство 3. *[обобщена асоциативност]*

Нека $a_1, a_2, \ldots, a_n$ са произволни елементи от пръстена. Ако без да променяме реда на множителите, тогава по какъвто и начин да се разположат скобите в това произведение, винаги се получава еднакъв резултат.

Доказателство:
При доказателството се изпълзва само асоциативността на умножението и затова е същото, както сме го доказали при свойствата на групи. Само за пълнота го прилагам тук.

Нека $a_1, \ldots, a_n \in M$ са произволни елементи от пръстена, и да отбележим с $h(a_1, \ldots, a_n)$ резултатът, който се получава при разполагането на скобите, по такъв начин че първо да се умножат a_1 и a_2, полученото произведение се умножава по a_3, полученото произведение се умножава по следващия елемент и т. н. накрая се умножава по a_n.

$$\begin{array}{rcl} h(a_1, a_2, \ldots, a_{n-1}, a_n) & = & (\ldots((a_1.a_2).a_3).\ldots.a_{n-1}).a_n \\ h(a_1, a_2, \ldots, a_{n-1}, a_n) & = & h(a_1, a_2, \ldots, a_{n-1}).a_n \end{array}.$$

Ще докажем, следното твърдение:

При произволно разполагане на скоби в произведението $a_1.a_2.\ldots.a_n$, винаги ще се получи стойността $h(a_1, \ldots, a_n) = (\ldots((a_1.a_2).a_3).\ldots.a_{n-1}).a_n$.

Прави се с индукция по $n \geq 3$.

В случая $n = 3$ от асоциативния закон имаме $a_1(a_2.a_3) = (a_1.a_2)a_3 = h(a_1, a_2, a_3)$.

Нека $n \geq 3$ и да предположим, че твърдението е изпълнено за всички естествени числа k, за които $3 \leq k \leq n$. Разглеждаме произведение $f(a_1, \ldots, a_{n+1})$, в което скобите са разположени по произволен начин. Нека скобите, съответстващи на последното произведение, което трябва да бъдат между a_s и a_{s+1}:

$$f(a_1, \ldots, a_{n+1}) = l(a_1, \ldots, a_s).r(a_{s+1}, \ldots, a_{n+1})$$

Прилагаме индукционното предположение за стойностите $l(a_1, \ldots, a_s)$, $r(a_{s+1}, \ldots, a_{n+1})$ и $h(a_1, \ldots, a_s).h(a_{s+1}, \ldots, a_n)$ и получаваме

$$\begin{array}{rcl} f(a_1, \ldots, a_{n+1}) & = & l(a_1, \ldots, a_s).r(a_{s+1}, \ldots, a_{n+1}) = \\ & = & h(a_1, \ldots, a_s).h(a_{s+1}, \ldots, a_{n+1}) = \\ & = & h(a_1, \ldots, a_s).(h(a_{s+1}, \ldots, a_n).a_{n+1}) = \\ & = & (h(a_1, \ldots, a_s).h(a_{s+1}, \ldots, a_n)).a_{n+1} = \\ & = & h(a_1, \ldots, a_n).a_{n+1} = \\ & = & h(a_1, \ldots, a_n, a_{n+1}) \end{array}$$

□

2.2. Степен на елемент

Свойство 4: *[степен на елемент от пръстен]*

Нека n е естествено число, елемента $a^n = \underbrace{a.\ldots.a}_{n}$ се нарича $n-$ та степен на $a \in M$. Изпълнени са свойствата:

$$a^{n+k} = a^n.a^k$$
$$(a^n)^k = a^{nk}$$

Доказателство:
В резултат от обобщената асоциативност получаваме, че в произведението $a^n = \underbrace{a.\ldots.a}_{n}$ няма нужда от поставяне на скоби, защото винаги се получават еднакви стойности. Тогава

$$a^n.a^k = \underbrace{a.\ldots.a}_{n}.\underbrace{a.\ldots.a}_{k} = \underbrace{a.\ldots.a}_{n+k} = a^{n+k}$$

$$(a^n)^k = \underbrace{(\underbrace{a.\ldots.a}_{n}).\ldots.(\underbrace{a.\ldots.a}_{n})}_{k} = \underbrace{a.\ldots.a}_{k.n} = a^{n.k}$$

□

2.3. Единичен елемент (св-ва)

Свойство 5:

Ако в пръстена M има единичен елемент e, тогава

- единичният елемент е единствен.
- $(-e)a = a(-e) = -a$, за произволен $a \in M$.

Доказателство:

- Ако допуснем че елементите e_1 и e_2 изпълнявт свойството за дефиниране на единичен елемент, тогава:

$$\begin{array}{l} \triangleright \ \ a = ae_1 = e_1 a \\ \triangleright \ \ a = ae_2 = e_2 a \end{array}, \ \forall a \in M \implies e_1 = e_1 . e_2 = e_2 .$$

Получи се, че $e_1 = e_2$, и затова ако съществува единичен елемент в пръстена M, той е е единствен.

- $0 = 0a = (e + (-e))a = ea + (-e)a = a + (-e)a \implies (-e)a = -a.$

□

2.4. Обратими елементи (св-ва)

Свойство 6.
Нека M е пръстен с единица e . Тогава:

- Ако елементът $a \in M$ е обратим, тогава съществува ***единствен*** елемент $b \in M$, за който $a.b = b.a = e$. *Този елемент b ще наричаме обратен на a и ще го записваме $b = a^{-1}$.*
- Ако $a \in M$ е обратим, тогава обратният елемент $b = a^{-1}$ също е обратим и $(a^{-1})^{-1} = a$.
- Ако a, b са обратими тогава $a.b$ също е обратим и $(a.b)^{-1} = b^{-1}a^{-1}$.

Доказателство:

- Нека елементът $a \in M$ е обратим, и ако за елементите b_1, b_2 са изпълнени равенствата, лесно се получава че тези елементи съвпадат:

$$\begin{array}{l} \triangleright\ ab_1 = b_1a = e \\ \triangleright\ ab_2 = b_2a = e \end{array} \implies b_1 = b_1(ab_2) = (b_1a)b_2 = eb_2 = b_2.$$

- Ако елементът $a \in M$ е обратим, тогава равенството $a.a^{-1} = a^{-1}.a = e$ освен, че ни показва, че a^{-1} е обратен на a, може да се разглежда като сочещо, че a е обратен на a^{-1}, затова може да запишем $(a^{-1})^{-1} = a$.
- Ако a, b са обратими елементи, проверяваме:

$$\left.\begin{array}{l} \checkmark ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = e \\ \checkmark (b^{-1}a^{-1})ab = b^{-1}(a^{-1}a)b = b^{-1}eb = e \end{array}\right\} \implies (a.b)^{-1} = b^{-1}a^{-1}.$$

□

2.5. Мултипликативна група

Твърдение:
Ако M е пръстен с единица, тогава множеството $M^* = \{a \in M \mid \exists\, a^{-1}\}$ от всички обратими елементи в пръстена образува група относно операцията умножение и тази група се нарича *мултипликативна група на пръстена* .

Доказателство:
Доказахме, че ако $a, b \in M^*$ са обратими елементи, тогава $a.b \in M^*$ също е обратим, което означава, че произведението е бинарна операция в M^*. Тази операция е асоциативна, защото произведението в пръстена удовлетварява асоциативния закон. Единичния елемент е обратим и $e^{-1} = e \in M^*$, а също и ако $a \in M^*$ обратим, то $a^{-1} \in M^*$ също. Следователно $(M^*, .)$ е група .

□

Пример:

Съгласно определението, за всяко поле F обратими елементи са всички ненулеви елементи, затова $F^* = F \setminus \{0\}$. Поради тази причина за числовите полета имаме $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

Пример:

а) Единствените цели числа, на които обратните са също цели са $1, -1,$ и затова $\mathbb{Z}^* = \{1, -1\}$.

б) От таблицата за умножение на пръстена $\mathbb{Z}_6$; виждаме, че освен единичния елемент $\bar{1}$ има само още един обратим и това е $\bar{5}$. Получава се $\mathbb{Z}_6^* = \{\bar{1},\ \bar{5}\}$

в) Знаем, че една матрица е обратима, точно когато нейната детерминанта е различна от нула, откъдето получаваме $M_{n\times n}^*(\mathbb{R}) = GL(n, \mathbb{R})$.

2.6. Делители на нулата

Определение:
Ненулевите елементи от пръстен M се наричат делители на нулата, ако е изпълнено, че $ab = 0$, където $a \neq 0,\ b \neq 0.$

Още от училище знаем, че в числовите множества няма такива ненулеви числа, чието произведение е 0 и следователно в тях няма делители на 0.
Пример:
Нека да разгледаме квадратните матрици $A = \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}$ и $B = \begin{pmatrix} 2 & -4 \\ -1 & 2 \end{pmatrix}$ от пръстена $M_{2\times 2}(\mathbb{R})$. Като умножим тези две матрици установяваме, че $A.B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$. Следователно ненулевите матрици A, B са делители на нулата.

Ако разгледаме малко по-внимателно предния пример, установяваме че детерминантите на матриците A, B са равни на 0. За упражнение, докажете, че една ненулева квадратна матрица A е делител на нулата тогава и само тогава, когато $\det(A) = 0.$ (*Упътване: Използва се една от основните теореми за линейни системи от Алгебра 1.)*

Пример:
Ако разгледаме таблицата за умножение в пръстена $\mathbb{Z}_6$ установяваме, че $\overline{2}.\overline{3} = \overline{0};\ \overline{3}.\overline{4} = \overline{0},$ следователно елементите $\overline{2}, \overline{3}, \overline{4}$ са делители на нулата в $\mathbb{Z}_6$.

Свойство:
Нека M е пръстен с единица. Не е възможно един елемент едновременно да бъде обратим и делител на нулата.
Доказателство:
Допускаме противното, т.е. че $a \neq 0$ е едновременно обратим и делител на нулата. Тогава съществуват a^{-1} - обратен на a и елемент $b \neq 0$, за който $ab = 0$ (или $ba = 0.$) Вижда се, че се

$$ab = 0 \Rightarrow a^{-1}ab = a^{-1}0 = 0 \Rightarrow b = 0$$

Откъдето получаваме противоречие, с избора на $b \neq 0.$ Следователно е невъзможно един елемент да е обратим и делител на нулата.

□

Следствие: В полетата няма делители на нулата.

3. Подпръстени

Определение:
Подмножеството $K \subset M$ се нарича подпръстен на пръстена M, ако K е пръстен относно операциите, които получава ("наследява") от M (*записва се* $K < M$).

Определение:
Подмножеството $L \subset F$ се нарича подполе на полето F, ако L има поне два елемента и е поле относно операциите, които получава ("наследява") от F (*записва се* $L < F$).

Примери:

- При числата имаме, че стойността на сумата и произведението на две цели числа не зависи от това дали ги разглеждаме като цели, или като рационални, или като реални или като комплексни числа. Чрез такива разсъждения можем да се убедим, че е налице следната редица от подпръстени $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$.
- Аналогично, полетата $\mathbb{Q}$ и $\mathbb{R}$ са подполета на полето на комплексните числа $\mathbb{C}$.
- Ако M е пръстен, тогава подмножеството $O = \{0\}$ е подпръстен, който е "тривиален" подпръстен. Пръстенът M може да се разглежда и като подпръстен на M, което е и другия "тривиален" подпръстен.

3.1. Твърдение - подпръстен

Твърдение:
Нека M е пръстен и $\emptyset \neq K \subset M$. Тогава е изпълнено:

$$K \text{ е подпръстен на } M \iff \begin{cases} a-b \in K, & \forall a,b \in K \\ ab \in K, & \forall a,b \in K \end{cases}.$$

Доказателство:
$\Rightarrow$) Нека K е подпръстен на M, тогава произведението, наследено от M, е бинарна операция в K и затова $ab \in K,\ \forall a,b \in K$.
K е пръстен, затова в K има нулев елемент и нека това да е елемента $\tilde{0} \in K$, за който $\tilde{0}+a=a,\ \forall a \in K$. Ще докажем, че $\tilde{0}$ е точно нулевият елемент на M:

$$\begin{array}{rcll} \tilde{0}+a & = & a, & \forall a \in K,\ (\text{равенство в } K \subset M) \\ & \Downarrow & & \exists\ (-a) \in M \\ \tilde{0}+a+(-a) & = & a+(-a) & (\text{равенство в пръстена } M) \\ & \Downarrow & & \\ \tilde{0} & = & 0 \in K & (0 \text{ е нулев елемент в } K) \end{array}$$

За всеки елемент $b \in K \subset M$ съществува противоположен елемент в пръстена K и нека да го означим със $\widetilde{-b} \in K$, тогава:

$$\begin{array}{rcll} \widetilde{-b}+b & = & 0, & (\text{равенство в } K \subset M) \\ & \Downarrow & & \exists\ (-b) \in M \\ \widetilde{-b}+b+(-b) & = & 0+(-b) & (\text{равенство в пръстена } M) \\ & \Downarrow & & \\ \widetilde{-b} & = & -b \in K & (-b \text{ е елемент на пръстена } K) \end{array}$$

Получи се, че ако $b \in K$, тогава $-b \in K$, откъдето получаваме $a-b=a+(-b) \in K,\ \forall a,b \in K$.

$\Leftarrow$) Ако за $K \subset M.$ са изпълнени двете условия, тогава от $ab \in K,\ \forall a,b \in K$ следва, че умножението е бинарна операция за $K.$
Ако $a \in K \Rightarrow a-a=0 \in K$ и получаваме, че нулевият елемент на M принадлежи на K, а от $0-a=-a \in K,\ \forall a \in K$ получаваме, че противоположният $-a$ на елемента $a \in K$ също принадлежи на K.
Следователно:

$$a,b \in K \Rightarrow a,-b \in K \Rightarrow a-(-b)=a+b \in K$$

и установяваме, че сумата е бинарна операция в K.
Асоциативните и дистрибутивните закони важат за всички елементи от множеството M, следователно и за елементите на подмножеството K. Получихме, че е изпълнено определението за пръстен и затова K е подпръстен на M.

□

Пример:
Да разгледаме подмножеството от комплексни числа, които имат цяла реална и имагинерна част
$\mathbb{Z}[i]=\{a+bi|a,b \in \mathbb{Z}\} \subset \mathbb{C}$, те се наричат цели Гаусови числа. Проверяваме

$$\left| \begin{array}{l} z_1=a_1+b_1 i \in \mathbb{Z}[i] \\ z_1=a_1+b_1 i \in \mathbb{Z}[i] \end{array} \right. \Rightarrow \begin{cases} z_1-z_2=(a_1-a_2)+(b_1-b_2)i \in \mathbb{Z}[i] \\ z_1 . z_2=(a_1 a_2-b_1 b_2)+(a_1 b_2+a_2 b_1)i \in \mathbb{Z}[i] \end{cases}.$$

Получихме, че $\mathbb{Z}[i]$ е подпръстен на полето на комплексните числа$\mathbb{C}$.

3.2. Твърдение - подполе

Твърдение:
Нека F е поле, $L \subset F$ и $|L| \geq 2$. Тогава е изпълнено:

$$L \text{ е подполе на } F \iff \begin{cases} a-b \in L, & \forall a,b \in L \\ ab \in L, & \forall a,b \in L \\ c^{-1} \in L, & \forall c \in L \text{ и } c \neq 0 \end{cases}.$$

Доказателство:
$\Rightarrow$) Нека L е подполе на F, тогава L е подпръстен на F, следователно са изпълнени първите две условия. Ако $e_1 \in L$ е единичният елемент на полето L, тогава е изпълнено $e_1 a = a, \forall a \in L$. Нека a е ненулев елемнт от L, следователно a е обратим като елемент на F и съществува $a^{-1} \in F$ тогава:

$$\begin{aligned} e_1 a &= a, && \forall a \in L, \ (\text{равенство в } L \subset F) \\ &\Downarrow && \text{ако } 0 \neq a \in L \ (\exists a^{-1} \in F) \\ e_1 a a^{-1} &= a a^{-1} && (\text{равенство в полето } F) \\ &\Downarrow \\ e_1 &= e \in L \end{aligned}$$

Получи се, че точно единичния елемент на полето F е единичен елемент на подполето $e \in L$.
Ако $a \neq 0, a \in L$ е произволен ненулев елемен от $L \subset F$ - полета, да бележим обратния елемнт на a в полето L с $\widetilde{a^{-1}}$, обратния елемнт на a в полето F с a^{-1}.

$$\left.\begin{aligned} (\text{в } F) \quad e &= a.a^{-1} \\ (\text{в } L \subset F) \quad e &= a.\widetilde{a^{-1}} \end{aligned}\right\} \Rightarrow \widetilde{a^{-1}} = \widetilde{a^{-1}}.a.a^{-1} = ea^{-1} = a^{-1} \in L$$

Получи се, че е изпълнено и третото условие $a^{-1} \in L$

$\Leftarrow$) От $\left\{\begin{array}{ll} a-b \in L, & \forall a,b \in L \\ ab \in L, & \forall a,b \in L \end{array}\right\}$ следва, че L е подпръстен на полето F, затова и L е комутативен пръстен. От $|L| \geq 2$ получаваме, че в L има ненулев елемент $a \in L$, следователно и $a^{-1} \in L$. От $a.a^{-1} = e \in L$ следва, че пръстенът L е с единица, в който всеки ненулев елемент е обратим, т.е. L е поле.

□

Пример:
За да приложим твърдението към множеството
$\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} | a,b \in \mathbb{Q}\} \subset \mathbb{R}$, проверяваме за произволни $z_1 = a_1 + b_1\sqrt{5} \in \mathbb{Q}(\sqrt{5})$ и $z_2 = a_2 + b_2\sqrt{5} \in \mathbb{Q}(\sqrt{5})$:
- $z_1 + z_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt{5} \in \mathbb{Q}(\sqrt{5})$;
- $z_1 . z_2 = (a_1 . a_2 + 5b_1 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{5} \in \mathbb{Q}(\sqrt{5})$;
- ако $z_1 \neq 0$, тогава $a_1^2 - 5b_1^2 \neq 0$ и лесно се получава, че $z^{-1} \in \mathbb{Q}(\sqrt{5})$

$$\frac{1}{z_1} = \frac{1}{a_1 + b_1\sqrt{5}} = \frac{a_1 - b_1\sqrt{5}}{a_1^2 - 5b_1^2} = \frac{a_1}{a_1^2 - 5b_1^2} - \frac{b_1}{a_1^2 - 5b_1^2}\sqrt{5} \in \mathbb{Q}(\sqrt{5})$$

По този начин, установихме, че $\mathbb{Q}(\sqrt{5})$ е поле, защото е подполе на $\mathbb{R}$.

3.3. Друг пример

Пример:
Нека да разгледаме подмножеството $L = \{\overline{0}, \overline{3}\} \subset \mathbb{Z}_6$. от класове остатъци по модул 6. Ясно е, че

$$\overline{3} + \overline{3} = \overline{0} \in L, \quad -\overline{3} = \overline{3} \in L, \quad \overline{3}.\overline{3} = \overline{3} \in L,$$

откъдето получаваме, че множеството L е пръстен, който е подпръстен на $\mathbb{Z}_6$.

Подмножеството L не съдържа единичния елемент на пръстена $\mathbb{Z}_6$, но елементът $\overline{3} \in L$ играе ролята на единичен елемент в L, защото $\overline{0}.\overline{3} = \overline{0}$ и $\overline{3}.\overline{3} = \overline{3}$.
Тук се забелязва, че L и $\mathbb{Z}_6$ са пръстени с единица и въпреки че $L \subset \mathbb{Z}_6$, единичните им елементи са различни - за L е $\overline{3}$, а за $\mathbb{Z}_6$ е $\overline{1}$.

Освен това от равенството $\overline{3}.\overline{3} = \overline{3}$ установяваме, че $\overline{3} \in L$ е обратим елемент в L, въпреки че не е обратим елемент в $\mathbb{Z}_6$. По този начин се вижда, че пръстенът L е поле, докато $\mathbb{Z}_6$ не е поле.

Задача за упражнение: Дадено е множеството $T = \{\overline{0}, \overline{2}, \overline{4}\} \subset \mathbb{Z}_6$, състоящо се от класове остатъци по модул 6. Да се докаже, че T е пръстен. Да се установи дали T е поле.

4. Свойства на Zn

Теорема:
Нека $n > 1$ е естествено число и $\overline{a} \in \mathbb{Z}_n$ $\overline{a} \neq \overline{0}$. Тогава е изпълнено:
а) Елементът $\overline{a} \in \mathbb{Z}_n$ е делител на нулата в $\mathbb{Z}_n$ тогава и само тогава, когато за най-големия общ делител е изпълнено $d = (a, n) > 1$.
б) Елементът $\overline{a} \in \mathbb{Z}_n$ е обратим в $\mathbb{Z}_n$ тогава и само тогава, когато a и n са взаимно прости, т.е. $(a, n) = 1$.

Доказателство:
Нека a е естествено число, за което е изпълнено $n \nmid a$, т.е. $1 \leq (a, n) < n$. Изпълнено е:

- Ако $d = (a, n) = 1$: От тъждеството на Безу следва че, съществуват цели числа u, v за които е изпълнено$au + nv = 1$. От него получаваме сравнението $au \equiv 1(\mathtt{mod}\ n.)$ Записваме това сравнение като равенство в пръстена $\mathbb{Z}_n$ от класовете остатъци $\overline{a}.\overline{u} = \overline{1},$ откъдето виждаме, че $\overline{a} \in \mathbb{Z}_n$ е обратим елемент и неговият обратен е $\overline{a}^{-1} = \overline{u}$.
- Ако $d = (a, n) > 1$: нека да означим $a_1 = \frac{a}{d},\ n_1 = \frac{n}{d} < n$. Тогава е изпълнено

$$a.n_1 = (a_1 d)n_1 = a_1 n \implies n|(a.n_1) \implies \overline{a}.\overline{n_1} = \overline{0} \text{ и } \overline{n_1} \neq \overline{0}.$$

Следователно елементът $\overline{a} \in \mathbb{Z}_n$ е делител на нулата.

По този начин установихме, че всеки ненулев елемент в пръстена $\mathbb{Z}_n$ е или делител на 0 или е обратим. Тъй като не е възможно един елемент да е едновременно и обратим и делител на нулата, получаваме търсените еквивалентности от т.а) и т. б).

□

Забележка: От доказателството на теоремата става ясен начинът, по който се намират обратните на обратимите елементи от пръстените $\mathbb{Z}_n$.

Пример:
Да разгледаме пръстена $\mathbb{Z}_{100}$ и да намерим обратния елемент на $\overline{41}$. Прилагаме алгоритъма на Евклид и после се връщаме в обратния ред по получените равенства, за да получим тъждеството на Безу

$$\begin{array}{lll} 100 = 2.41 + 18 & 18 = 100 - 2.41 & 1 = 16(100 - 2.41) - 7.41 = 16.100 - 39.41 \\ 41 = 2.18 + 5 & 5 = 41 - 2.18 & 1 = 2.18 - 7(41 - 2.18) = 16.18 - 7.41 \Uparrow \\ 18 = 3.5 + 3 & 3 = 18 - 3.5 & 1 = 2(18 - 3.5) - 5 = 2.18 - 7.5 \Uparrow \\ 5 = 1.3 + 2 & 2 = 5 - 3 & 1 = 3 - (5 - 3) = 2.3 - 5 \Uparrow \\ 3 = 1.2 + 1 & 1 = 3 - 2 & \Rightarrow \quad 1 = 3 - 2 \Uparrow \end{array}$$

Получи се $1 = 16.100 - 39.41,$ откъдето имаме сравнението

$$-39.41 \equiv 1(\mathtt{mod}\ 100),\ \text{но}\ -39 \equiv 61(\mathtt{mod}\ 100) \implies 61.41 \equiv 1(\mathtt{mod}\ 100)$$

и окончателно получаваме $\overline{41}^{-1} = \overline{61}.$

4.1. Zn поле ли е?

Следствие:
Пръстенът $\mathbb{Z}_n$ е поле, тогава и само тогава когато n е просто число.

Доказателство:
Комбинирайки доказаното от предишната теорема с основното свойство на простите числа се получава:

$$
\begin{gathered}
n \text{ е просто число} \\
\Updownarrow \\
\text{изпълнено е } (a,n)=1, \ \ \forall a \in \mathbb{Z}, \ \ 1 \leq a < n \\
\Updownarrow \\
\text{елементът } \overline{a} \in \mathbb{Z}_n \text{ е обратим}, \ \ \forall a \in \mathbb{Z}, \ \ 1 \leq a < n \\
\Updownarrow \\
\text{всички ненулеви елементи в } \mathbb{Z}_n \text{ са обратими} \\
\Updownarrow \\
\mathbb{Z}_n \text{ е поле}
\end{gathered}
$$

□

4.2. Теорема на Ойлер-Ферма

Непосредствено от теоремата се получава пълно описание на мултипликативната група на $\mathbb{Z}_n$
Следствие: *(Мултипликативна група $\mathbb{Z}_n^*$)*

- $\mathbb{Z}_n^* = \{\, \overline{a} \mid (a,n) = 1\}$;
- $|\mathbb{Z}_n^*| = \varphi(n),$ където $\varphi(n)$ е функцията на Ойлер.

Теорема на Ойлер-Ферма:
Ако a, n са цели числа, които са взаимно прости $(a,n) = 1,$ тогава $a^{\varphi(n)} \equiv 1 \pmod{n}.$

Доказателство:
Към взаимно простите числа a, n прилагаме предната теорема и получаваме, че елемента $\overline{a}$ е обратим в пръстена от класовете остатъци $\mathbb{Z}_n$. Следователно $\overline{a}$ е елемент на мултипликативната група $\mathbb{Z}_n^*$, която има $\varphi(n)$ елемента. Според едно от следствията на Теоремата на Лагранж е знаем, че $\mathtt{ord}(\overline{a}) \mid \varphi(n)$, затова е изпълнено $\overline{a}^{\varphi(n)} = \overline{1}.$ Това равенство записваме като сравнение и получаваме $a^{\varphi(n)} \equiv 1 \pmod{n}.$

□

Следствие:
Ако p е просто число за цялото число a е изпълнено $a^p \equiv a \pmod{p}$

(Получава се от $\varphi(p) = p - 1.$)

4.3. Теорема на Уилсон

Теорема на Уилсън:
Ако p е просто число, тогава е изпълнено $(p-1)! \equiv -1 \pmod{p}$.

Доказателства:
Знаем, че когато p е просто число, тогава пръстенът от класовете остатъци $\mathbb{Z}_p$ е поле. Ако пресметнем на колко е равно произведението на всички ненулеви елементи от полето, ще можем да определим остатъка на $(p-1)!$. Когато $p = 2$ равенството очевидно е изпълнено и затова нека $p > 2$.

За целта, да определим кои обратими елементи $\overline{x} \in \mathbb{Z}_p$, съвпадат със своя обратен:

$$\overline{x} = \overline{x}^{-1} \Leftrightarrow \overline{x}^2 = \overline{1} \Leftrightarrow (\overline{x} - \overline{1})(\overline{x} + \overline{1}) = \overline{0}$$

В полето $\mathbb{Z}_p$ няма делители на нулата, затова последното равенство може да се изпълни, само когато единият от двата множителя е нула. Откъдето получаваме, че $\overline{x} = \overline{1}$ или $\overline{x} = -\overline{1} = \overline{p-1}$.

Получава се, че ако $p > 2$, множеството от елементи $\{\overline{2}, \ldots, \overline{p-2}\}$ може да се разбие на непресичащи се двойки елементи от вида $\{\overline{y}, \overline{y}^{-1}\}$ и поради тази причина за произведението имаме $\overline{2}. \ldots . \overline{p-2} = \overline{1}$. Следователно

$$\overline{1}. \overline{2}. \ldots . \overline{p-2}. \overline{p-1} = \overline{p-1} \Rightarrow (p-1)! \equiv -1 \pmod{p}$$

□