Линеарна алгебра 1

прво предавање

Институт за математику и информатику
Природно-математички факултет
Универзитет у Крагујевцу

Бинарне операције, основне структуре и морфизми

Нека је A непразан скуп и f пресликавање скупа $A \times A$ у скуп A.

Дефиниција

Пресликавање $f : A \times A \to A$ се зове бинарна операција на скупу A.

Бинарне операције, основне структуре и морфизми

Нека је A непразан скуп и f пресликавање скупа $A \times A$ у скуп A.

Дефиниција

Пресликавање $f : A \times A \to A$ се зове бинарна операција на скупу A.

Надаље ћемо са $*$, или на неки други начин, на пример са $\circ$, $\oplus$, $\odot$, $\square$, $+$, ... означавати бинарну операцију у смислу претходне дефиниције. Тада кажемо да је скуп A снабдевен операцијом $*$. Ту чињеницу ћемо симболизовати са $(A, *)$.

Бинарне операције, основне структуре и морфизми

Нека је A непразан скуп и f пресликавање скупа $A \times A$ у скуп A.

Дефиниција

Пресликавање $f : A \times A \to A$ се зове бинарна операција на скупу A.

Надаље ћемо са $*$, или на неки други начин, на пример са $\circ$, $\oplus$, $\odot$, $\square$, $+$, ... означавати бинарну операцију у смислу претходне дефиниције. Тада кажемо да је скуп A снабдевен операцијом $*$. Ту чињеницу ћемо симболизовати са $(A, *)$.

Наравно, могуће је у истом скупу дефинисати више операција, на пример, у скупу $\mathbb{R}$ операције $+$ и $\cdot$. Тада бисмо имали означавање $(\mathbb{R}, +, \cdot)$.

Бинарне операције, основне структуре и морфизми

Нека је A непразан скуп и f пресликавање скупа $A \times A$ у скуп A.

Дефиниција

Пресликавање $f : A \times A \to A$ се зове бинарна операција на скупу A.

Надаље ћемо са $*$, или на неки други начин, на пример са $\circ$, $\oplus$, $\odot$, $\square$, $+$, ... означавати бинарну операцију у смислу претходне дефиниције. Тада кажемо да је скуп A снабдевен операцијом $*$. Ту чињеницу ћемо симболизовати са $(A, *)$.

Наравно, могуће је у истом скупу дефинисати више операција, на пример, у скупу $\mathbb{R}$ операције $+$ и $\cdot$. Тада бисмо имали означавање $(\mathbb{R}, +, \cdot)$.

За $(A, *)$ кажемо да је алгебарска структура.

Нека је бинарна операција $*$ дефинисана у непразном скупу A.

Дефиниција

Кажемо да је бинарна операција $*$ асоцијативна ако за свако $a, b, c \in A$ важи

$$a * (b * c) = (a * b) * c.$$

Нека је бинарна операција $*$ дефинисана у непразном скупу A.

Дефиниција

Кажемо да је бинарна операција $*$ асоцијативна ако за свако $a, b, c \in A$ важи

$$a * (b * c) = (a * b) * c.$$

Дакле, ако је операција $*$ асоцијативна, могуће је писати

$$a * (b * c) = (a * b) * c = a * b * c.$$

Нека је бинарна операција $*$ дефинисана у непразном скупу A.

Дефиниција

Кажемо да је бинарна операција $*$ асоцијативна ако за свако $a, b, c \in A$ важи

$$a * (b * c) = (a * b) * c.$$

Дакле, ако је операција $*$ асоцијативна, могуће је писати

$$a * (b * c) = (a * b) * c = a * b * c.$$

Дефиниција

Бинарна операција $*$ је комутативна, ако за свако $a, b \in A$ важи једнакост

$$a * b = b * a.$$

Дефиниција

Ако у $(A, *)$ *постоји елемент* e*, такав да је за свако* $a \in A$

$$a * e = e * a = a,$$

кажемо да је $e \in A$ *неутрални или јединични елемент за операцију* $*$.

Дефиниција

Ако у $(A, *)$ постоји елемент e, такав да је за свако $a \in A$

$$a * e = e * a = a,$$

кажемо да је $e \in A$ неутрални или јединични елемент за операцију $*$.

Теорема

Ако у $(A, *)$ постоји неутрални елемент, онда је он јединствен.

Дефиниција

Ако у $(A, *)$ постоји елемент e, такав да је за свако $a \in A$

$$a * e = e * a = a,$$

кажемо да је $e \in A$ неутрални или јединични елемент за операцију $*$.

Теорема

Ако у $(A, *)$ постоји неутрални елемент, онда је он јединствен.

Доказ. Претпоставимо супротно,

Дефиниција

Ако у $(A, *)$ постоји елемент e, такав да је за свако $a \in A$

$$a * e = e * a = a,$$

кажемо да је $e \in A$ неутрални или јединични елемент за операцију $*$.

Теорема

Ако у $(A, *)$ постоји неутрални елемент, онда је он јединствен.

Доказ. Претпоставимо супротно, тј. да у скупу A постоје два елемента e и f $(e \neq f)$, таква да је за свако $a \in A$ $a * e = e * a = a$ и $a * f = f * a = a$.

Дефиниција

Ако у $(A, *)$ постоји елемент e, такав да је за свако $a \in A$

$$a * e = e * a = a,$$

кажемо да је $e \in A$ неутрални или јединични елемент за операцију $*$.

Теорема

Ако у $(A, *)$ постоји неутрални елемент, онда је он јединствен.

Доказ. Претпоставимо супротно, тј. да у скупу A постоје два елемента e и f $(e \neq f)$, таква да је за свако $a \in A$
$a * e = e * a = a$ и $a * f = f * a = a$.
Како је a произвољан елемент из A, ставимо $a = f$ у првој једнакости и $a = e$ у другој.

Тада добијамо $f * e = e * f = f$ и $e * f = f * e = e$, одакле следује

Тада добијамо $f * e = e * f = f$ и $e * f = f * e = e$, одакле следује $e = f$,

Тада добијамо $f * e = e * f = f$ и $e * f = f * e = e$, одакле следује $e = f$, што је у контрадикцији са претпоставком $e \neq f$. $\square$

Тада добијамо $f * e = e * f = f$ и $e * f = f * e = e$, одакле следује $e = f$, што је у контрадикцији са претпоставком $e \neq f$. $\square$

Дефиниција

Ако у $(A, *)$ постоји неутрални елемент e и ако за $a \in A$ постоји елемент $a^{-1} \in A$, такав да је

$$a^{-1} * a = a * a^{-1} = e,$$

кажемо да је a^{-1} инверзни елемент за $a \in A$, у односу на операцију $*$.

Тада добијамо $f * e = e * f = f$ и $e * f = f * e = e$, одакле следује $e = f$, што је у контрадикцији са претпоставком $e \neq f$. $\square$

Дефиниција

Ако у $(A, *)$ постоји неутрални елемент e и ако за $a \in A$ постоји елемент $a^{-1} \in A$, такав да је

$$a^{-1} * a = a * a^{-1} = e,$$

кажемо да је a^{-1} инверзни елемент за $a \in A$, у односу на операцију $*$.

Наравно, ако, у смислу претходне дефиниције постоји $a^{-1} \in A$, тада је $a \in A$ инверзни елемент за a^{-1}. Важи, дакле, $(a^{-1})^{-1} = a$. Уместо ознаке a^{-1} за инверзни елемент користимо и ознаку a'.

Теорема

Нека у $(A, *)$ постоји неутрални елемент e и нека је $*$ асоцијативна операција. Ако за елемент $a \in A$ постоји инверзни елемент $a^{-1} \in A$, тада је он јединствен.

Теорема

Нека у $(A, *)$ постоји неутрални елемент e и нека је $*$ асоцијативна операција. Ако за елемент $a \in A$ постоји инверзни елемент $a^{-1} \in A$, тада је он јединствен.

Доказ. Претпоставимо супротно, тј. нека за $a \in A$ постоје два међу собом различита инверзна елемента a_1^{-1} и a_2^{-1}. Тада важи

$$a_1^{-1} = a_1^{-1} * e = a_1^{-1} * (a * a_2^{-1}) = (a_1^{-1} * a) * a_2^{-1} = e * a_2^{-1} = a_2^{-1},$$

што је у супротности са учињеном претпоставком. □

Теорема

Нека у $(A, *)$ постоји неутрални елемент e и нека је $*$ асоцијативна операција. Ако за елемент $a \in A$ постоји инверзни елемент $a^{-1} \in A$, тада је он јединствен.

Доказ. Претпоставимо супротно, тј. нека за $a \in A$ постоје два међу собом различита инверзна елемента a_1^{-1} и a_2^{-1}. Тада важи

$$a_1^{-1} = a_1^{-1} * e = a_1^{-1} * (a * a_2^{-1}) = (a_1^{-1} * a) * a_2^{-1} = e * a_2^{-1} = a_2^{-1},$$

што је у супротности са учињеном претпоставком. □

Нека је $*$ једна бинарна операција дефинисана у непразном скупу G.

Дефиниција

За алгебарску структуру $(G, *)$ кажемо да је групоид.

Дефиниција

Ако је операција $*$ асоцијативна, за структуру $(G, *)$ кажемо да је асоцијативни групоид или полугрупа (или семигрупа).

Дефиниција

Ако је операција $*$ асоцијативна, за структуру $(G, *)$ кажемо да је асоцијативни групоид или полугрупа (или семигрупа).

Пример

Како је операција сабирања у скупу природних бројева $\mathbb{N}$ асоцијативна, структура $(\mathbb{N}, +)$ је асоцијативни групоид.

Дефиниција

Ако је операција $*$ асоцијативна, за структуру $(G, *)$ кажемо да је асоцијативни групоид или полугрупа (или семигрупа).

Пример

Како је операција сабирања у скупу природних бројева $\mathbb{N}$ асоцијативна, структура $(\mathbb{N}, +)$ је асоцијативни групоид.

Дефиниција

Ако у групоиду $(G, *)$ постоји неутрални елемент, тада кажемо да је групоид $(G, *)$ са јединицом.

Дефиниција

Ако је операција $*$ асоцијативна, за структуру $(G, *)$ кажемо да је асоцијативни групоид или полугрупа (или семигрупа).

Пример

Како је операција сабирања у скупу природних бројева $\mathbb{N}$ асоцијативна, структура $(\mathbb{N}, +)$ је асоцијативни групоид.

Дефиниција

Ако у групоиду $(G, *)$ постоји неутрални елемент, тада кажемо да је групоид $(G, *)$ са јединицом.

Пример

Структуре $(\mathbb{N}_0, +)$ и $(\mathbb{N}, \cdot)$ су групоиди са јединицом. Неутрални елементи у овим структурама су 0 и 1, респективно.

Дефиниција

Нека је бинарна операција $*$, дефинисана у скупу G. За групоид $(G, *)$ кажемо да је група ако су испуњени следећи услови:

(Г1) *Операција $*$ је асоцијативна;*

(Г2) *У скупу G постоји неутрални елемент за операцију $*$;*

(Г3) *За сваки елемент из G постоји у G њему инверзни елемент у односу на операцију $*$.*

Дефиниција

Нека је бинарна операција $*$, дефинисана у скупу G. За групоид $(G, *)$ кажемо да је група ако су испуњени следећи услови:

(Г1) *Операција $*$ је асоцијативна;*

(Г2) *У скупу G постоји неутрални елемент за операцију $*$;*

(Г3) *За сваки елемент из G постоји у G њему инверзни елемент у односу на операцију $*$.*

Дефиниција

За групу $(G, *)$ кажемо да је комутативна или Абелова, ако операција $*$ има особину комутативности.

Дефиниција

Нека је бинарна операција $*$, дефинисана у скупу G. За групоид $(G, *)$ кажемо да је група ако су испуњени следећи услови:

(Г1) *Операција $*$ је асоцијативна;*

(Г2) *У скупу G постоји неутрални елемент за операцију $*$;*

(Г3) *За сваки елемент из G постоји у G њему инверзни елемент у односу на операцију $*$.*

Дефиниција

За групу $(G, *)$ кажемо да је комутативна или Абелова, ако операција $*$ има особину комутативности.

Ако скуп G садржи коначан број елемената, на пример n, за групу $(G, *)$ кажемо да је коначног реда n.

Дефиниција

Нека су $(G_1, *)$ *и* $(G_2, \circ)$ *групе и нека је* f *пресликавање скупа* G_1 *у скуп* G_2 *такво да је, за свако* $a, b \in G_1$,

$$f(a * b) = f(a) \circ f(b).$$

За пресликавање f *кажемо да је хомоморфизам групе* $(G_1, *)$ *у групу* $(G_2, \circ)$.

Дефиниција

Нека су $(G_1, *)$ *и* $(G_2, \circ)$ *групе и нека је* f *пресликавање скупа* G_1 *у скуп* G_2 *такво да је, за свако* $a, b \in G_1$,

$$f(a * b) = f(a) \circ f(b).$$

За пресликавање f *кажемо да је хомоморфизам групе* $(G_1, *)$ *у групу* $(G_2, \circ)$. *Ако је* f *пресликавање „на", за групу* $(G_2, \circ)$ *кажемо да је хомоморфна слика групе* $(G_1, *)$.

Дефиниција

Ако су $(G_1, *)$ *и* $(G_2, \circ)$ *групе истога реда и ако је* f *бијективно пресликавање скупа* G_1 *на скуп* G_2 *такво да је, за свако* $a, b \in G_1$,

$$f(a * b) = f(a) \circ f(b),$$

кажемо да је пресликавање f *изоморфизам групе* $(G_1, *)$ *на групу* $(G_2, \circ)$.

Дефиниција

Ако су $(G_1, *)$ *и* $(G_2, \circ)$ *групе истога реда и ако је* f *бијективно пресликавање скупа* G_1 *на скуп* G_2 *такво да је, за свако* $a, b \in G_1$,

$$f(a * b) = f(a) \circ f(b),$$

кажемо да је пресликавање f *изоморфизам групе* $(G_1, *)$ *на групу* $(G_2, \circ)$.

Пример

Функција $f(x) = \log x$ *је један изоморфизам групе* $(\mathbb{R}^+, \cdot)$ *на групу* $(\mathbb{R}, +)$.

Теорема

Ако је пресликавање f изоморфизам групе $(G_1, *)$ на групу $(G_2, \circ)$, тада је инверзно пресликавање f^{-1} изоморфизам групе $(G_2, \circ)$ на групу $(G_1, *)$.

Теорема

Ако је пресликавање f изоморфизам групе $(G_1, *)$ на групу $(G_2, \circ)$, тада је инверзно пресликавање f^{-1} изоморфизам групе $(G_2, \circ)$ на групу $(G_1, *)$.

Доказ. Нека су x и y било који елементи из G_2. Тада су $f^{-1}(x)$ и $f^{-1}(y)$ њима одговарајући елементи из G_1.

Теорема

Ако је пресликавање f изоморфизам групе $(G_1, *)$ на групу $(G_2, \circ)$, тада је инверзно пресликавање f^{-1} изоморфизам групе $(G_2, \circ)$ на групу $(G_1, *)$.

Доказ. Нека су x и y било који елементи из G_2. Тада су $f^{-1}(x)$ и $f^{-1}(y)$ њима одговарајући елементи из G_1.Како је f изоморфизам групе $(G_1, *)$ на групу $(G_2, \circ)$, важи једнакост

$$f(f^{-1}(x) * f^{-1}(y)) = f(f^{-1}(x)) \circ f(f^{-1}(y)) = x \circ y,$$

одакле непосредно следује

Теорема

Ако је пресликавање f изоморфизам групе $(G_1, *)$ на групу $(G_2, \circ)$, тада је инверзно пресликавање f^{-1} изоморфизам групе $(G_2, \circ)$ на групу $(G_1, *)$.

Доказ. Нека су x и y било који елементи из G_2. Тада су $f^{-1}(x)$ и $f^{-1}(y)$ њима одговарајући елементи из G_1.Како је f изоморфизам групе $(G_1, *)$ на групу $(G_2, \circ)$, важи једнакост

$$f(f^{-1}(x) * f^{-1}(y)) = f(f^{-1}(x)) \circ f(f^{-1}(y)) = x \circ y,$$

одакле непосредно следује

$$f^{-1}(x \circ y) = f^{-1}(f(f^{-1}(x) * f^{-1}(y))) = f^{-1}(x) * f^{-1}(y).$$

Теорема

Ако је пресликавање f изоморфизам групе $(G_1, *)$ на групу $(G_2, \circ)$, тада је инверзно пресликавање f^{-1} изоморфизам групе $(G_2, \circ)$ на групу $(G_1, *)$.

Доказ. Нека су x и y било који елементи из G_2. Тада су $f^{-1}(x)$ и $f^{-1}(y)$ њима одговарајући елементи из G_1.Како је f изоморфизам групе $(G_1, *)$ на групу $(G_2, \circ)$, важи једнакост

$$f(f^{-1}(x) * f^{-1}(y)) = f(f^{-1}(x)) \circ f(f^{-1}(y)) = x \circ y,$$

одакле непосредно следује

$$f^{-1}(x \circ y) = f^{-1}(f(f^{-1}(x) * f^{-1}(y))) = f^{-1}(x) * f^{-1}(y).$$

Према томе, пресликавање f^{-1} је изоморфизам групе $(G_2, \circ)$ на групу $(G_1, *)$. $\square$

Дакле, ако постоји изоморфизам групе $(G_1, *)$ на групу $(G_2, \circ)$, постоји и изоморфизам групе $(G_2, \circ)$ на групу $(G_1, *)$. Због тога, за такве групе кажемо да су изоморфне, тј. кажемо да је свака од њих изоморфна оној другој, у ознаци $(G_1, *) \cong (G_2, \circ)$.

Дакле, ако постоји изоморфизам групе $(G_1, *)$ на групу $(G_2, \circ)$, постоји и изоморфизам групе $(G_2, \circ)$ на групу $(G_1, *)$. Због тога, за такве групе кажемо да су изоморфне, тј. кажемо да је свака од њих изоморфна оној другој, у ознаци $(G_1, *) \cong (G_2, \circ)$.

Дефиниција

Ако је пресликавање f изоморфизам групе $(G, *)$ на саму себе, за пресликавање f кажемо да је аутоморфизам групе $(G, *)$.

Алгебарске структуре са две операције

Нека је S непразан скуп и нека су у њему дефинисане две бинарне операције $*$ и $\circ$.

Алгебарске структуре са две операције

Нека је S непразан скуп и нека су у њему дефинисане две бинарне операције $*$ и $\circ$. Самим тим, $(S, *)$ и $(S, \circ)$ су извесне алгебарске структуре.

Алгебарске структуре са две операције

Нека је S непразан скуп и нека су у њему дефинисане две бинарне операције $*$ и $\circ$. Самим тим, $(S, *)$ и $(S, \circ)$ су извесне алгебарске структуре. Међутим, могуће је посматрати нову структуру коју чини скуп S снабдевен обема операцијама.

Алгебарске структуре са две операције

Нека је S непразан скуп и нека су у њему дефинисане две бинарне операције $*$ и $\circ$. Самим тим, $(S, *)$ и $(S, \circ)$ су извесне алгебарске структуре. Међутим, могуће је посматрати нову структуру коју чини скуп S снабдевен обема операцијама.

Пре него што изучимо неке од ових структура, дефинисаћемо особину дистрибутивност једне операције у односу на другу операцију.

Дефиниција

Кажемо да је бинарна операција $*$ дистрибутивна у односу на бинарну операцију $\circ$ ако за свако $a, b, c \in S$ важе једнакости

$$a * (b \circ c) = (a * b) \circ (a * c), \quad (a \circ b) * c = (a * c) \circ (b * c).$$

Наравно, ако за свако $a, b, c \in S$ важе једнакости

$$a \circ (b * c) = (a \circ b) * (a \circ c),$$

$$(a * b) \circ c = (a \circ c) * (b \circ c),$$

кажемо да је бинарна операција $\circ$ дистрибутивна у односу на операцију $*$.

Наравно, ако за свако $a, b, c \in S$ важе једнакости

$$a \circ (b * c) = (a \circ b) * (a \circ c),$$

$$(a * b) \circ c = (a \circ c) * (b \circ c),$$

кажемо да је бинарна операција $\circ$ дистрибутивна у односу на операцију $*$.

Пример

Множење реалних бројева је дистрибутивна операција у односу на сабирање реалних бројева. Обрнуто, сабирање није дистрибутивна операција у односу на множење реалних бројева.

Дефиниција

Нека су у скупу S дефинисане две бинарне операције $*$ и $\circ$. Ако су испуњени следећи услови:

(P1) $(S, *)$ *је комутативна група;*

(P2) *Операција $\circ$ је асоцијативна;*

(P3) *Операција $\circ$ је дистрибутивна у односу на операцију $*$,*

кажемо да скуп S чини прстен у односу на операције $*$ и $\circ$, означавајући га са $(S, *, \circ)$.

Дефиниција

Нека су у скупу S дефинисане две бинарне операције $*$ и $\circ$. Ако су испуњени следећи услови:

(P1) $(S, *)$ *је комутативна група;*

(P2) *Операција $\circ$ је асоцијативна;*

(P3) *Операција $\circ$ је дистрибутивна у односу на операцију $*$,*

кажемо да скуп S чини прстен у односу на операције $*$ и $\circ$, означавајући га са $(S, *, \circ)$.

Пример

$(\mathbb{Z}, +, \cdot)$ *је прстен. Заиста, овде је $(Z, +)$ Абелова група, операција $\cdot$ је асоцијативна и, најзад, операција $\cdot$ је дистрибутивна у односу на операцију сабирања $+$.*

Управо, због прстена целих бројева $(\mathbb{Z}, +, \cdot)$ уобичајено је да се неутрални елемент за операцију $*$ означава са 0, а инверзни елемент елемента a са $-a$.

Управо, због прстена целих бројева $(\mathbb{Z}, +, \cdot)$ уобичајено је да се неутрални елемент за операцију $*$ означава са 0, а инверзни елемент елемента a са $-a$.

Теорема

У прстену $(S, *, \circ)$ важи:

(1) $0 \circ a = a \circ 0 = 0$;

(2) $a \circ (-b) = -(a \circ b) = (-a) \circ b$;

(3) $(-a) \circ (-b) = a \circ b$.

Доказ.

(1) Коришћењем претходних особина лако налазимо да је

$$\begin{aligned}
0 =& (-(a \circ 0)) * (a \circ 0) \\
=& (-(a \circ 0)) * (a \circ (0 * 0)) \\
=& (-(a \circ 0)) * ((a \circ 0) * (a \circ 0)) \\
=& ((-(a \circ 0)) * (a \circ 0)) * (a \circ 0) \\
=& 0 * (a \circ 0) = a \circ 0.
\end{aligned}$$

Доказ.

(1) Коришћењем претходних особина лако налазимо да је

$$\begin{aligned} 0 =& (-(a \circ 0)) * (a \circ 0) \\ =& (-(a \circ 0)) * (a \circ (0 * 0)) \\ =& (-(a \circ 0)) * ((a \circ 0) * (a \circ 0)) \\ =& ((-(a \circ 0)) * (a \circ 0)) * (a \circ 0) \\ =& 0 * (a \circ 0) = a \circ 0. \end{aligned}$$

Слично, $0 \circ a = 0$.

(2) Једноставно налазимо да је

$$\begin{aligned}(-a)\circ b =& 0 * ((-a)\circ b)\\ =& ((-(a\circ b))*(a\circ b))*((-a)\circ b)\\ =& (-(a\circ b))*((a\circ b)*((-a)\circ b))\\ =& (-(a\circ b))*((a*(-a))\circ b)\\ =& (-(a\circ b))*(0\circ b)\\ =& (-(a\circ b))*0\\ =& -(a\circ b).\end{aligned}$$

(2) Једноставно налазимо да је

$$\begin{aligned}(-a)\circ b =& 0 * ((-a)\circ b)\\ =& ((-(a\circ b)) * (a\circ b)) * ((-a)\circ b)\\ =& (-(a\circ b)) * ((a\circ b) * ((-a)\circ b))\\ =& (-(a\circ b)) * ((a * (-a))\circ b)\\ =& (-(a\circ b)) * (0\circ b)\\ =& (-(a\circ b)) * 0\\ =& -(a\circ b).\end{aligned}$$

Слично, $a\circ(-b) = -(a\circ b)$.

(2) Једноставно налазимо да је

$$\begin{aligned}(-a)\circ b =& 0 * ((-a)\circ b)\\ =& ((-(a\circ b)) * (a\circ b)) * ((-a)\circ b)\\ =& (-(a\circ b)) * ((a\circ b) * ((-a)\circ b))\\ =& (-(a\circ b)) * ((a * (-a))\circ b)\\ =& (-(a\circ b)) * (0\circ b)\\ =& (-(a\circ b)) * 0\\ =& -(a\circ b).\end{aligned}$$

Слично, $a\circ(-b) = -(a\circ b)$.

(3) Важи да је $(-a)\circ(-b) = -(a\circ(-b)) = -(-(a\circ b)) = a\circ b$. $\square$

Дефиниција

Прстен $(S, *, \circ)$ је комутативан ако је операција $\circ$ комутативна.

Дефиниција

Прстен $(S, *, \circ)$ је комутативан ако је операција $\circ$ комутативна.

Дефиниција

Прстен $(S, *, \circ)$ је прстен са јединицом ако постоји елемент $1 \in S$ такав да важи $1 \circ x = x \circ 1 = x$.

Дефиниција

Прстен $(S, *, \circ)$ је комутативан ако је операција $\circ$ комутативна.

Дефиниција

Прстен $(S, *, \circ)$ је прстен са јединицом ако постоји елемент $1 \in S$ такав да важи $1 \circ x = x \circ 1 = x$.

Елемент $1 \in S$ се зове јединица прстена.

Дефиниција

Прстен $(S, *, \circ)$ је комутативан ако је операција $\circ$ комутативна.

Дефиниција

Прстен $(S, *, \circ)$ је прстен са јединицом ако постоји елемент $1 \in S$ такав да важи $1 \circ x = x \circ 1 = x$.

Елемент $1 \in S$ се зове јединица прстена.

Дефиниција

Комутативан прстен са јединицом $(S, *, \circ)$ је интегрални домен ако нема делитеље нуле, тј.

$$(\forall a, b \in S)(a \circ b = 0 \Leftrightarrow a = 0 \vee b = 0).$$

Пример

$(\mathbb{Z}, +, \cdot)$ и $(\mathbb{Q}, +, \cdot)$ су интегрални домени, док $(\mathbb{Z}_4, +_4, \cdot_4)$ је комутативан прстен са јединицом, али није интегрални домен (нпр. $2 \cdot_4 2 = 0$)

Пример

$(\mathbb{Z}, +, \cdot)$ и $(\mathbb{Q}, +, \cdot)$ су интегрални домени, док $(\mathbb{Z}_4, +_4, \cdot_4)$ је комутативан прстен са јединицом, али није интегрални домен (нпр. $2 \cdot_4 2 = 0$)

Дефиниција

Нека је $(S, +, \cdot, 0, 1)$ прстен са јединицом. Уколико постоји $n \geq 2$, такво да је $\underbrace{1 + \cdots + 1}_{n} = 0$ онда кажемо да је прстен P коначне карактеристике и најмање такво n зовемо карактеристика прстена S.

Пример

$(\mathbb{Z}, +, \cdot)$ и $(\mathbb{Q}, +, \cdot)$ су интегрални домени, док $(\mathbb{Z}_4, +_4, \cdot_4)$ је комутативан прстен са јединицом, али није интегрални домен (нпр. $2 \cdot_4 2 = 0$)

Дефиниција

Нека је $(S, +, \cdot, 0, 1)$ прстен са јединицом. Уколико постоји $n \geq 2$, такво да је $\underbrace{1 + \cdots + 1}_{n} = 0$ онда кажемо да је прстен P коначне карактеристике и најмање такво n зовемо карактеристика прстена S.

Дефиниција

Нека је $(S, +, \cdot, 0, 1)$ прстен са јединицом. Уколико је $\underbrace{1 + \cdots + 1}_{n} \neq 0$, за све $n \geqslant 2$, онда кажемо да је прстен карактеристике нула (или бесконачне карактеристике).

Карактеристику прстена S ћемо означавати са $\mathrm{char}(S)$.

Карактеристику прстена S ћемо означавати са $\mathrm{char}(S)$.

Дефиниција

Ако је $(S \setminus \{0\}, \circ)$ група, за прстен $(S, *, \circ)$ кажемо да је тело.

Карактеристику прстена S ћемо означавати са $\mathrm{char}(S)$.

Дефиниција

Ако је $(S \setminus \{0\}, \circ)$ група, за прстен $(S, *, \circ)$ кажемо да је тело.

Дефиниција

Ако је $(F \setminus \{0\}, \circ)$ Абелова група, за прстен $(F, *, \circ)$ кажемо да је поље.

Карактеристику прстена S ћемо означавати са $\mathrm{char}(S)$.

Дефиниција

Ако је $(S \setminus \{0\}, \circ)$ група, за прстен $(S, *, \circ)$ кажемо да је тело.

Дефиниција

Ако је $(F \setminus \{0\}, \circ)$ Абелова група, за прстен $(F, *, \circ)$ кажемо да је поље.

Неутрални елемент у односу на операцију $\circ$ најчешће означавамо са 1, а инверзни елемент елемента a са a^{-1}.

Карактеристику прстена S ћемо означавати са $\mathrm{char}(S)$.

Дефиниција

Ако је $(S \setminus \{0\}, \circ)$ група, за прстен $(S, *, \circ)$ кажемо да је тело.

Дефиниција

Ако је $(F \setminus \{0\}, \circ)$ Абелова група, за прстен $(F, *, \circ)$ кажемо да је поље.

Неутрални елемент у односу на операцију $\circ$ најчешће означавамо са 1, а инверзни елемент елемента a са a^{-1}.

Пример

$(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ и $(\mathbb{C}, +, \cdot)$ су поља, док $(\mathbb{Z}, +, \cdot)$ није поље. $(\mathbb{Z}_n, +_n, \cdot_n)$ је поље ако и само ако је n прост број.

Теорема

Свако поље је интегрални домен.

Теорема

Свако поље је интегрални домен.

Доказ. Нека је $(F, +, \cdot)$ поље. Покажимо да у пољу F нема делитеља нуле.

Теорема

Свако поље је интегрални домен.

Доказ. Нека је $(F, +, \cdot)$ поље. Покажимо да у пољу F нема делитеља нуле. За произвољно $a, b \in F$ из $a \cdot b = 0$ и $a \neq 0$ следи

Теорема

Свако поље је интегрални домен.

Доказ. Нека је $(F, +, \cdot)$ поље. Покажимо да у пољу F нема делитеља нуле. За произвољно $a, b \in F$ из $a \cdot b = 0$ и $a \neq 0$ следи да постоји $a^{-1} \in F$

Теорема

Свако поље је интегрални домен.

Доказ. Нека је $(F, +, \cdot)$ поље. Покажимо да у пољу F нема делитеља нуле. За произвољно $a, b \in F$ из $a \cdot b = 0$ и $a \neq 0$ следи да постоји $a^{-1} \in F$ и стога

$$b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0.$$

Теорема

Свако поље је интегрални домен.

Доказ. Нека је $(F, +, \cdot)$ поље. Покажимо да у пољу F нема делитеља нуле. За произвољно $a, b \in F$ из $a \cdot b = 0$ и $a \neq 0$ следи да постоји $a^{-1} \in F$ и стога

$$b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0.$$

Дакле, из $a \cdot b = 0$ следи $a = 0$ или $b = 0$.

Теорема

Свако поље је интегрални домен.

Доказ. Нека је $(F, +, \cdot)$ поље. Покажимо да у пољу F нема делитеља нуле. За произвољно $a, b \in F$ из $a \cdot b = 0$ и $a \neq 0$ следи да постоји $a^{-1} \in F$ и стога

$$b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0.$$

Дакле, из $a \cdot b = 0$ следи $a = 0$ или $b = 0$.
Стога, $(F, +, \cdot)$ је и интегрални домен. $\square$

Теорема

Ако поље $(F, +, \cdot)$ има коначну карактеристику онда она мора бити прост број.

Теорема

Ако поље $(F, +, \cdot)$ има коначну карактеристику онда она мора бити прост број.

Доказ. Нека је карактеристика поља $(F, +, \cdot)$ број $p \neq 0$.

Теорема

Ако поље $(F, +, \cdot)$ има коначну карактеристику онда она мора бити прост број.

Доказ. Нека је карактеристика поља $(F, +, \cdot)$ број $p \neq 0$. Ако је $p = m \cdot k$, $1 < m < p$, $1 < k < p$ сложен број тада

Теорема

Ако поље $(F, +, \cdot)$ има коначну карактеристику онда она мора бити прост број.

Доказ. Нека је карактеристика поља $(F, +, \cdot)$ број $p \neq 0$. Ако је $p = m \cdot k$, $1 < m < p$, $1 < k < p$ сложен број тада из

$$0 = \underbrace{1 + \cdots + 1}_{p} = (\underbrace{1 + \cdots + 1}_{m}) \cdot (\underbrace{1 + \cdots + 1}_{k})$$

следи

Теорема

Ако поље $(F, +, \cdot)$ има коначну карактеристику онда она мора бити прост број.

Доказ. Нека је карактеристика поља $(F, +, \cdot)$ број $p \neq 0$. Ако је $p = m \cdot k$, $1 < m < p$, $1 < k < p$ сложен број тада из

$$0 = \underbrace{1 + \cdots + 1}_{p} = (\underbrace{1 + \cdots + 1}_{m}) \cdot (\underbrace{1 + \cdots + 1}_{k})$$

следи $\underbrace{1 + \cdots + 1}_{m} = 0$ или

Теорема

Ако поље $(F, +, \cdot)$ има коначну карактеристику онда она мора бити прост број.

Доказ. Нека је карактеристика поља $(F, +, \cdot)$ број $p \neq 0$. Ако је $p = m \cdot k$, $1 < m < p$, $1 < k < p$ сложен број тада из

$$0 = \underbrace{1 + \cdots + 1}_{p} = (\underbrace{1 + \cdots + 1}_{m}) \cdot (\underbrace{1 + \cdots + 1}_{k})$$

следи $\underbrace{1 + \cdots + 1}_{m} = 0$ или $\underbrace{1 + \cdots + 1}_{k} = 0$

Теорема

Ако поље $(F, +, \cdot)$ има коначну карактеристику онда она мора бити прост број.

Доказ. Нека је карактеристика поља $(F, +, \cdot)$ број $p \neq 0$. Ако је $p = m \cdot k$, $1 < m < p$, $1 < k < p$ сложен број тада из

$$0 = \underbrace{1 + \cdots + 1}_{p} = (\underbrace{1 + \cdots + 1}_{m}) \cdot (\underbrace{1 + \cdots + 1}_{k})$$

следи $\underbrace{1 + \cdots + 1}_{m} = 0$ или $\underbrace{1 + \cdots + 1}_{k} = 0$ па је $\mathrm{char}(F) \leqslant m < p$ или $\mathrm{char}(F) \leqslant k < p$,

Теорема

Ако поље $(F, +, \cdot)$ има коначну карактеристику онда она мора бити прост број.

Доказ. Нека је карактеристика поља $(F, +, \cdot)$ број $p \neq 0$. Ако је $p = m \cdot k$, $1 < m < p$, $1 < k < p$ сложен број тада из

$$0 = \underbrace{1 + \cdots + 1}_{p} = (\underbrace{1 + \cdots + 1}_{m}) \cdot (\underbrace{1 + \cdots + 1}_{k})$$

следи $\underbrace{1 + \cdots + 1}_{m} = 0$ или $\underbrace{1 + \cdots + 1}_{k} = 0$ па је $\mathrm{char}(F) \leqslant m < p$ или $\mathrm{char}(F) \leqslant k < p$, што је супротно претпоставци $\mathrm{char}(F) = p$.

Теорема

Ако поље $(F, +, \cdot)$ има коначну карактеристику онда она мора бити прост број.

Доказ. Нека је карактеристика поља $(F, +, \cdot)$ број $p \neq 0$. Ако је $p = m \cdot k$, $1 < m < p$, $1 < k < p$ сложен број тада из

$$0 = \underbrace{1 + \cdots + 1}_{p} = (\underbrace{1 + \cdots + 1}_{m}) \cdot (\underbrace{1 + \cdots + 1}_{k})$$

следи $\underbrace{1 + \cdots + 1}_{m} = 0$ или $\underbrace{1 + \cdots + 1}_{k} = 0$ па је $\mathrm{char}(F) \leqslant m < p$ или $\mathrm{char}(F) \leqslant k < p$, што је супротно претпоставци $\mathrm{char}(F) = p$. Дакле, p је прост број. □