

Увод

Појам скупа. Скуп

Скуп је појам који се не дефинише.

$$A = \{a, b, c\}$$

$$P = \{x: x = 2k, k \in \mathbb{N}\} \text{ - парни бројеви}$$

Празан скуп: \emptyset - скуп без елемената

дефиниција - реченица која се уводи новим појмом (символ).

(Д:) Скуп B је подскуп скупа A .

- Ако је сваки елемент скупа B елемент скупа A .

$$\forall x \in B \Rightarrow x \in A$$

$$\text{Напомена: } (\forall A) \emptyset \subset A$$

- За сваки скуп A важи, празан скуп је подскуп скупа A .

(Д:) Партиципни скуп скупа A

$P(A)$ је скуп свих подскупова скупа A .

Пример: $A = \{a, b, c\}$

$$P(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}$$

(Т:) Ако је $|A| = n$, тада је $|P(A)| = 2^n$

$$\text{доказ: } |P(A)| = 1 + n + \binom{n}{2} + \binom{n}{3} + \dots + \binom{n}{n-1} + 1 =$$

$$= \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \dots + \binom{n}{n} = \sum_{k=0}^n \binom{n}{k} 1^k \cdot 1^{n-k} =$$

$$= (1+1)^n = 2^n$$

Ⓛ: Уређен пар (a, b) је $\{\{a, b\}, \{a\}\}$

* неформална Ⓛ:

Скуп та два елементи код којих се зна редослед.

Прва информација - два елементи

Друга информација - редослед

Ⓛ: Два уређена пара (a, b) и (c, d) , једнака су ако
 $a = c$ и $b = d$.

Ⓛ: $P^n(A) = P(P^{n-1}(A))$, $P^1(A) = P(A)$

Ⓛ: Декартов производ скупова A и B , $A \times B$ је скуп
 $\{(a, b) : a \in A, b \in B\}$

Ⓛ: Уређена n -торка елемената (a_1, a_2, \dots, a_n) је
 $((a_1, a_2, \dots, a_{n-1}), a_n)$, где је (a_1, a_2) уређен пар.

Ⓛ: $A^2 = A \times A$

Ⓛ: $A^n = A \times A^{n-1}$, $A^2 = A \times A$

Пресликавање (функција)

Ⓛ: Пресликавање $f: X \rightarrow Y$ - скупа X у скуп Y је један
подскуп скупа $X \times Y$ са особинама:

1) скуп свих првих компоненти (домен пресликавања) је X ;

2) ако $(x, y) \in f$ и $(x, z) \in f$, тада је $y = z$.

$\{a, b, c\}$

$\{a, a, b, b, b, c\}$ - Игнорише се понављање скупа.

1) Пример:

$f: X \rightarrow Y$

$X = \{1, 2, 3\}$

$f = \{(1, b), (2, c), (3, b)\}$

$Y = \{a, b, c, d\}$

$\{b, c\} = f(X) \subset Y$

$$2) \quad X = \{1, 2, 3\}$$

$$Y = \{a, b, c\}$$

$$f = \{(1, a), (2, b), (3, c)\}$$

$$y = f(x)$$

$$a = f(1)$$

$$b = f(2)$$

$$c = f(3)$$

Ⓙ: Два преликавања f и g , једнака су ако имају исти домен X и $(\forall x \in X) \quad f(x) = g(x)$

Преликавање је скуп!

Ⓐ: Преликавање $f: X \rightarrow Y$ је "1-1" преликавање
 - инјекција - ако се различити оригинали увек преликавају у различите слике

Ⓑ: Преликавање $f: X \rightarrow Y$ је преликавање "НА" скуп Y .
 - сурјекција - ако је $y = f(x)$

Сви елементи X употребљени као слика.

Ⓐ: Преликавање $f: X \rightarrow Y$ које је истовремено "1-1" и "НА" је бијекција или бијубока (двострано једнозначна) кореспонденција.

Ⓐ: Нека је $f: X \rightarrow Y$ и $g: Y \rightarrow Z$. Производ или композиција преликавања f и g је преликавање $h: X \rightarrow Z$ дефинисано са
 $h(x) = (fg)(x) = (f \circ g)(x) = g(f(x)) \quad (x \in X)$

Пример:

$$X = \{1, 2, 3\}$$

$$Y = \{a, b, c\}$$

$$Z = \{\alpha, \beta\}$$

$$f = \{(1, a), (2, b), (3, c)\}$$

$$g = \{(a, \alpha), (b, \beta), (c, \beta)\}$$

$$h = f \circ g = \{(1, a), (2, b), (3, \alpha)\}$$

Ⓙ: Ако је $f: X \rightarrow Y$, $g: Y \rightarrow Z$, $h: Z \rightarrow U$, тада је $(fg)h = f(gh)$ - асоцијативна операција

доказ: $fg: X \rightarrow Z$, $(fg)h: X \rightarrow U$

$gh: Y \rightarrow U$, $f(gh): X \rightarrow U$

$$x \in X : ((fg)h)(x) = (h(fg)(x)) = h(g(f(x)))$$

$$(f(gh))(x) = (gh)(f(x)) = h(g(f(x)))$$

①: Идентичко преликавање скупа X дефинисано је са
 $(\forall x \in X) f(x) = x$.

①: Ако је $f: X \rightarrow Y$ и ако постоји преликавање $f^{-1}: f(X) \rightarrow X$ таква да је $f \circ f^{-1}$ идентичко преликавање скупа $f(X)$, каже се да је f^{-1} инверзно преликавање преликавања f .

Пример:

$$X = \{1, 2, 3\}$$

$$Y = \{a, b, c, d\}$$

$$f = \{(1, b), (2, a), (3, b)\}$$

$$f^{-1} = \{(a, 2), (b, 1), (d, 3)\}$$

①: Ако је f "1-1" преликавање, тада постоји инверзно преликавање и оно је јединствено.

Бинарна релација

①: Бинарна релација R у скупу A јесте једно преликавање
 $R: A^2 \rightarrow \{\text{јесте, није}\}$, тј $R: A^2 \rightarrow \{0, 1\}$

Ако су x и y у релацији R ,
 пише се xRy .

①: Бинарна релација R у скупу A јесте један подскуп скупа A^2 .

①: n -арна релација у скупу A јесте једно преликавање
 $R: A^n \rightarrow \{0, 1\}$, један подскуп скупа A^n .

Пример: скуп N

да ли је $x + 2y + 3z = 8$?

$(1, 2, 1)$ јесте у релацији

$(1, 4, 5)$ није у релацији

①: Бинарна релација R у скупу A је рефлексивна, ако је
 $(\forall x \in A) \quad xRx$.

①: Бинарна релација R у скупу A је симетрична, ако је
 $(\forall x, y \in A) \quad (xRy \Rightarrow yRx)$

①: Бинарна релација R у скупу A је антисиметрична, ако
 $(\forall x, y \in A) \quad (xRy \wedge yRx \Rightarrow x=y)$

①: Бинарна релација R у скупу A је транзитивна, ако
 $(\forall x, y, z \in A) \quad (xRy \wedge yRz \Rightarrow xRz)$.

①: Бинарна релација која је рефлексивна, симетрична и транзитивна
 назива се релација еквиваленције.

Примери: $=$, \parallel , \cong , $\equiv (\text{mod } k)$

Класе еквиваленције

①: Бинарна релација R која је рефлексивна, антисиметрична и
 транзитивна назива се релација парцијалног уређења.

Примери: $1^\circ \leq (\geq)$

$2^\circ \mid$ (деливост) $(y \in \mathbb{N})$: $X \rightarrow Y$: X дели Y

$3^\circ \subset$ (инклузија)

Дефиниције

$(x \in B \Rightarrow x \in A)$ онда је $A \subset B$

$A \subset B \quad (x \in B \Rightarrow x \in A)$

У дефиницији се "акко" замењује са "ако".

Општа алгебра

①: Бинорна операција f у скупу A јесте свако пресликавање.
 $f: A^2 \rightarrow A$

Напомена: каже се још да је бинорна операција f унутрашња операција скупа A , тј да је скуп A затворен у односу на f .

Означава се са $f(x, y) = xfy$.

①: n -арна операција у скупу A је свако пресликавање
 $f: A^n \rightarrow A$

①: Уређен пар (G, \circ) скупа G и бинорне операције \circ у скупу G , назива се групоид.

Пример: $G = \{a, b, c\}$

\circ	a	b	c
a	b	a	a
b	a	c	b
c	c	c	a

← Кејлијева таблица

①: Нека је (G, \circ) групоид и $x, y \in G$. Ако је $x \circ y = y \circ x$, каже се да су елементи x и y пермутабилни.

①: Ако су у групоиду (G, \circ) свака два елемента пермутабилна, каже се да је групоид комутативан.

①: Ако у групоиду (G, \circ) важи:

$(\forall x, y, z) \quad (x \circ (y \circ z)) = ((x \circ y) \circ z)$, каже се да је групоид (G, \circ) асоцијативан групоид или семигрупа.

①: У семигрупи (G, \circ) је:

$$(\forall a \in G) \quad a^n = a \cdot a^{n-1}, \quad a^1 = a, \quad n \in \mathbb{N}$$

①: Нека је (G, \circ) групу. Ако $(\exists e' \in G)(\forall a \in G) e' \cdot a = a$, e' се назива леви неутрални елемент групе (G, \circ) .

Аналогино: десни неутрални елемент e'' $a \cdot e'' = a$

②: Ако у групи постоје e' и e'' , они су једнаки.

Доказ: $e' \cdot e'' = e'' = e'$

③: Нека је (G, \circ) група. Ако $(\exists e \in G)(\forall a \in G) e \cdot a = a \cdot e = a$, e је неутрални елемент групе.

④: Група има највише један неутрални елемент.

Доказ: $e_1 \neq e_2$

$$e_1 \cdot e_2 = e_2 = e_1$$

⑤: Сегрегирани са неутралним елементом, назива се моноид.

⑥: У моноиду (G, \circ) са неутралним елементом e је $(\forall a \in G) a \circ e = a$.

Примери: $(\mathbb{N}, +)$ - комутативна сегрегирани

(\mathbb{N}, \cdot) - комутативни моноид

уопште $\leftarrow (\mathbb{Z}, \circ)$ $a \circ b \stackrel{\text{def}}{=} a + 2b$

древни

Група, није комутативна, није асоцијативна, са десним неутралним елементом 0

⑦: Нека је (G, \circ) група са неутралним елементом e и $a \in G$. Ако $(\exists a' \in G) a' \cdot a = e$, a' се назива леви инверзни елемент елемента a . Аналогино десни инверзни елемент a'' .

⑧: У сегрегирани су a' и a'' једнаки ако постоје.

Доказ: $a' \cdot (a \cdot a'') = a' \cdot e = a' =$

$$= (a' \cdot a) \cdot a'' = e \cdot a'' = a''$$

①: Нека је (G, \circ) групу са нултим елементом e и $a \in G$.
 Ако $(\exists a^{-1} \in G) \ a^{-1} \cdot a = a \cdot a^{-1} = e$, a^{-1} се назива инверзни елемент елемента a .

②: У моноиду сваки елемент a има највише један инверзни елемент.

Доказ: КЊИГА ✓

③: Нека је (G, \circ) моноид са нултим елементом e . Тада је $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$, $a, b \in G$ (ако a^{-1} и b^{-1} постоје)

Доказ: $(a \cdot b)(b^{-1} \cdot a^{-1}) = ((a \cdot b) \cdot b^{-1}) \cdot a^{-1} =$

$$= (a(b \cdot b^{-1})) a^{-1} = (ae) a^{-1} = a \cdot a^{-1} = e$$

Такође

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

④: У моноиду је $a^{-n} \stackrel{\text{def}}{=} (a^{-1})^n$, $n \in \mathbb{N}$
 Степеновање негативним целим бројем (у моноиду)

Напомена: $(a^n)^{-1}$ (може се доказати)

⑤: Групу (G, \circ) у коме су једнакост решење све линеарне једначине облика $a \cdot x = b$ и $y \cdot a = b$, $a, b \in G$, x и y непознате је квазигрупа. Квазигрупа са нултим елементом назива се петља.

Пример: $G = \{a, b, c, d\}$

\cdot	a	b	c	d
a	b	c	d	②
b				
c				
d				

$$\begin{aligned} a \cdot b &= c \\ a \cdot d &= c \\ a \cdot x &= c \end{aligned}$$

⑥: Нека је (G, \circ) групу са следећим својствима:

1) асоцијативност

2) $(\exists e \in G)(\forall x \in G) \ x \cdot e = e \cdot x = x$

3) $(\forall x \in G)(\exists x^{-1} \in G) \ x^{-1} \cdot x = x \cdot x^{-1} = e$

Тада је (G, \circ) група.

⑦: Свака група је квазигрупа.

Пример:

Група (G, \cdot)
 $G = \{a, b, c\}$

Група $(H, *)$
 $H = \{\alpha, \beta, \gamma\}$

\cdot	a	b	c
a	b	c	b
b	a	b	b
c	c	b	a

$*$	α	β	γ
α	β	γ	β
β	α	β	β
γ	γ	β	α

 $f: G \rightarrow H$ (бјекција)

$$f(a) = \alpha$$

$$f(b) = \beta$$

$$f(c) = \gamma$$

$$\gamma = \alpha * \beta = f(a) * f(b)$$

$$= f(c) = f(a \cdot b)$$

ТАБЛА

TABLA

①: Ако су дати групе (G, \cdot) и $(H, *)$ и ако постоји бјекција $f: G \rightarrow H$, тако да $(\forall x, y \in G), (f(x \cdot y)) = f(x) * f(y)$ које се да су та два групе изоморфна, а бјекција f се назива изоморфизам.

②: Ако се у претходној дефиницији изостави захтев да је f бјекција (тј f је произвољно пресликавање), f се назива хомоморфизам.

Групе

①: Група чија је операција комутативна, назива се комутативна или Абелова група.

②: Група (G, \cdot) је коначна или бесконачна према томе какав је $|G|$.

③: Ред коначне групе (G, \cdot) је $|G|$.

④: Свака група је квазигрупа.

Доказ: Нека је (G, \cdot) група.

$$a \cdot x = b, \quad a, b \in G$$

$$a \cdot x = b \quad / \cdot a^{-1}$$

$$\Leftrightarrow a^{-1} \cdot (a \cdot x) = a^{-1} \cdot b$$

$$\Leftrightarrow (a^{-1} \cdot a) \cdot x = a^{-1} \cdot b$$

$$\Leftrightarrow e \cdot x = x = a^{-1} \cdot b \in G$$

$\Rightarrow x$ је једино решење једначине, тј:
 (G, \cdot) је квазигрупа.

Ⓓ: Ако је (G, \cdot) истовремено симигрупа и квазигрупа,
 (G, \cdot) је група.

Доказ: $a \in G$

$$a \cdot x = a$$

Нека је $x = e$ њено јединствено
 решење.

$$b \in G$$

$$y \cdot a = b$$

$$y \cdot a = y \cdot (a \cdot e) = (y \cdot a) \cdot e = \underline{b \cdot e = b}$$

$\Rightarrow e$ је десни неутрални елемент

На исти начин можемо и леви
 неутрални елемент e'

$\Rightarrow e = e'$, тј постоји неутрални елемент e

$$a \in G$$

$$a \cdot x = e$$

Њено јединствено решење десни инверзни елемент
 елемента a . На исти начин леви инверзни, а леви и десни
 су у симигрупи једнаки, тј постоји инверзни елемент елемента

\Rightarrow Сваки елемент има инверзан.

Примери: 1) $(\mathbb{Z}, +)$ Абелова група

$(\mathbb{Q}, +)$ и (\mathbb{Q}, \cdot)
↑
рационални бројеви

$(\mathbb{R}, +)$ и $(\mathbb{R} \setminus \{0\}, \cdot)$ — Абелова група
↑
реални бројеви

$(\mathbb{C}, +)$ и $(\mathbb{C} \setminus \{0\}, \cdot)$
↑
комплексни бројеви

2) $(V, +)$ Абелова група (вектори)

3) $P = \{0, 1, 2, 3\}$

$M = \{1, i, -1, -i\}$

$(P, +_4)$

(M, \cdot)

$$1 = i^0$$

$$i = i^1$$

$$-1 = i^2$$

$$-i = i^3$$

$$i^4 = 1$$

$$i^{k_1} \cdot i^{k_2} = i^{k_1 + k_2} \\ = i^{k_1 + 4k_2}$$

(M, \cdot) јесте
Абелова група.

$$f: P \rightarrow M$$

$$(\forall k \in P) \quad f(k) = i^k$$

f је биекција!

$$f(k_1 +_4 k_2) = i^{k_1 +_4 k_2} = i^{k_1} \cdot i^{k_2} = \underline{f(k_1) \cdot f(k_2)}$$

$\Rightarrow (P, +_4)$ и (M, \cdot) су изоморфни!

$\Rightarrow (P, +_4)$ Абелова група.

4) $P = \{0, 1, 2, \dots, p-1\}, p \in \mathbb{N}$

$(P, +_p)$

Јесте групоид.
 асоцијативност?

$a +_p (b +_p c) = (a +_p b) +_p c ?$

$a +_p (b +_p c) = a +_p (b + c + kp)$

\uparrow
 0 или -1

$a + b + c + kp + lp = a + b + c + mp \equiv a + b + c \pmod{p}$

\uparrow
 0 или -1

\uparrow
 0 или -1 или -2

$(a +_p b) +_p c \equiv a + b + c \pmod{p}$

$\Rightarrow a +_p (b +_p c) \equiv (a +_p b) +_p c \pmod{p}$

између себе конгруентни

\Rightarrow једнакост! (то значи асоцијативност)

Неутрални елемент 0

Инверзни елемент ...

(Аделова група)

5) $P_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

$P_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

$P_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

$P_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

$P_1 = \begin{pmatrix} 2 & 1 & 4 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

$P_1 \circ P_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

$P_2 \circ P_2 = P_0$

$P_3 \circ P_3 = P_0$

\circ	P_0	P_1	P_2	P_3
P_0	P_0	P_1	P_2	P_3
P_1	P_1	P_0	P_3	P_2
P_2	P_2	P_3	P_0	P_1
P_3	P_3	P_2	P_1	P_0

Ово је Абелова група!

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$$

$$P_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$P^{-1} ?$$

$$P \circ P^{-1} = P^{-1} \circ P = P_0$$

$$P = \begin{pmatrix} 4 & 1 & 2 & 3 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$P^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix}$$

6) Скуп свих пермутација скупа $\{1, 2, \dots, n\}$. То је група у односу на операцију \circ .

7) $\{1, 2, \dots, p-1\}$, p је прост број,
 операција \cdot_p (множење по $\text{mod } p$),
 Јесте Абелова група!

$\{1, 2, 3, 4, 5\}$
 множење по
 модулу 6

Подгрупе

Ⓜ: Ако је (G, \circ) група, $H \subseteq G$, $H \neq \emptyset$ и ако је (H, \circ) група, каже се да је (H, \circ) подгрупа групе (G, \circ) .

Пример: $(\mathbb{Z}, +)$ је подгрупа од $(\mathbb{Q}, +)$

①. (H, \cdot) је подгрупа групе (G, \cdot) ако важи

- 1° $\emptyset \neq H \subseteq G$
- 2° $(\forall x, y \in H) \quad x \cdot y \in H$
- 3° $(\forall x \in H) \quad x^{-1} \in H$

Доказ: $H \subseteq G$ због 1°

Асоцијативност се наслеђује из G

Због 2° и 3° $\forall x \in H, \quad x \cdot x^{-1} = e \in H$

Због 3° сваки $x \in H$ има инверзан елемент

73 Т. ✓

①: (Лагранжова теорема) Ако је (H, \cdot) подгрупа реда m коначне групе (G, \cdot) реда n , тада $m | n$.

Алгебраичке структуре
 са две операције

$(S, +, \cdot)$

$+$ и \cdot у бинарне операције у скупу S са следећим особинама:

- 1) $(S, +)$ је Абелова група
- 2) (S, \cdot) је ампгрупа
- 3) $(\forall x, y, z \in S) \quad x \cdot (y + z) = (x \cdot y) + (x \cdot z),$
 $(x + y) \cdot z = (x \cdot z) + (y \cdot z),$

тј важи лева и десна дистрибутивност операције \cdot према $+$, назива се ПРСТЕН.

Напомена 1) приоритет \cdot у односу на $+$:

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

- 2) 0 је нултни елемент за +, а 1 за \cdot ;
 Супротан елемент елементa а у односу на +
 писатемо -a.

$$a + (-a) = a - a.$$

Ⓐ: Прстен чија операција \cdot има нултни елемент,
 назива се прстен са јединицом.

Ⓐ: Прстен чија је операција \cdot комутативна, назива се
комутативан прстен.

Ⓢ: У прстену $(S, +, \cdot)$ је
 $(\forall x \in S) \quad x \cdot 0 = 0 \cdot x = 0$

$$\text{доказ: } x \cdot 0 = x \cdot 0 + 0 = (x \cdot 0) + (x \cdot 0) \\ \Rightarrow x \cdot 0 = 0$$

Ⓢ: У прстену $(\forall x, y \in S) \quad -(x \cdot y) = x \cdot (-y) = (-x) \cdot y$

Пример: 1) $(\mathbb{Z}, +, \cdot)$ комутативан прстен са јединицом

2) $P = \{0, 1, 2, \dots, p-1\}, \quad p \in \mathbb{N}$

$(P, +_p, \cdot_p)$ комутативан прстен са јединицом

3) Скуп свих реалних бројева

комутативан прстен са јединицом
 (у односу на + и \cdot бројева)

Ⓐ: Нека су $(S, +, \cdot)$ и (T, \oplus, \circ) две алгебарске структуре
 са по две бинарне операције и нека је $f: S \rightarrow T$ биекција.
 Ако важи:

$$(\forall x, y \in S) \quad f(x+y) = f(x) \oplus f(y),$$

$$f(x \cdot y) = f(x) \circ f(y)$$

каме се да у $(S, +, \cdot)$ и (T, \oplus, \odot) изоморфне структуре, а функција f назива се изоморфизам обих структура.

Тело и поље

①: Тело је уређена тројка $(S, +, \cdot)$ где је S скуп, а $+$ и \cdot две бинарне операције у овом скупу S , при чему важе:

- 1° $(S, +)$ је Абелова група
- 2° $(S \setminus \{0\}, \cdot)$ је група
- 3° Важе лева и десна дистрибутивност операције \cdot према операцији $+$.

②: Поље је тело чија је операција \cdot комутативна (тј. улов 2° $(S \setminus \{0\}, \cdot)$ је Абелова група)

Примери: 1) Бесконачна поља $(S, +, \cdot)$
 $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$

2) Коначна поља $(S, +, \cdot)$
 ↑
 коначан скуп

$(\mathbb{F}_p, +_p, \cdot_p)$ где је $p = \{0, 1, 2, \dots, p-1\}$ и p представља прост број.

③: Свако коначно тело је поље.

④: Коначно поље од n елемената постоји ако и само ако је $n = p^k$ где је p прост број, а $k \in \mathbb{N}$.

⑤: Сва коначна поља са istim бројем елемената су међусобно изоморфна.

КОНОЧНО

Општа ознака

 $GF(n)$

Пример:

 $GF(3)$
 $n = 3^1$
 $(\{0, 1, 2\}, +_3, \cdot_3)$

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

\cdot_3	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Полноми

Полном P над неким полем $(F, +, \cdot)$ је израз (функција) облика $P(x) = a_0 + a_1x + \dots + a_nx^n$, где $a_i \in F$.

Пример: $P(x) = 1 + 2x + x^2 + x^3$
 $Q(x) = 1 + x^2$

у пољу $GF(3) = (\{0, 1, 2\}, +_3, \cdot_3)$

За свако $x \in \{0, 1, 2\}$ $P(x) = Q(x)$

$$x=0 \quad P(0) = Q(0)$$

$$x=1 \quad P(1) = Q(1)$$

$$x=2 \quad P(2) = Q(2)$$

$$1 + 2 \cdot 2 + 2^2 + 2^3 = 1 + 2^2$$

$$1 + 1 + 1 + 2 = 1 + 1$$

2

2

①: Полном P над полем $(F, +, \cdot)$ је распоред $(a_0, a_1, a_2, \dots, a_n, 0, 0, 0, \dots)$ где за свако i $a_i \in F$ и почев од неког коначног места у распореду сви елементи $a_i = 0$.

Пример:
$$P = (a_0, a_1, a_2, a_3, \dots) = (1, 2, 1, 1, 0, 0, 0, \dots)$$

$$Q = (1, 0, 1, 0, 0, 0, \dots)$$

Ознака: $P = (a_0, a_1, \dots, a_n, 0, 0, \dots) = (a_0, a_1, \dots, a_n) \quad a_i \in F$

① Елементи $a_i \in F$ зову се коэффициенти полинома P .

Коэффициент a_0 зове се свободни члан полинома P .

Степен полинома P је највећи број n за који $a_n \neq 0$.

(Ознака: $\deg P = n$)

Ако је $\deg P = n$, тада се a_n зове главни (водећи, најстарији) коэффициент полинома P .

Ако је главни коэффициент $a_n = 1$, кажемо да је полином нормиран.

Ако је $\deg P = 0$, кажемо да је полином P нултог степена (константа).

$$P = (a_0, 0, 0, \dots) = (a_0) \quad a_0 \in F$$

Ако је $\deg P = 1$ кажемо да је P линеаран полином.

$$P = (a_0, a_1, 0, 0, \dots) = (a_0, a_1)$$

Ако је $\deg P = 2$ кажемо да је P квadratични полином.

$$P = (a_0, a_1, a_2, 0, 0, \dots) = (a_0, a_1, a_2)$$

Полином $(0, 0, 0, \dots)$ зове се нула полином (ознака 0).

Степен нула полинома се не дефинише.

Пример: Навести пример једног полинома степена 4.

$$\deg P = 4$$

а) над пољем $(\mathbb{C}, +, \cdot)$

б) над пољем $\mathbb{GF}(3)$

$$(a_0, a_1, a_2, a_3, a_4, 0, 0, \dots)$$

a) $(3, 0, 1, 2, 5, 0, 0, \dots)$

$$(0, 0, -3i, 0, 4, 0, 0, \dots)$$

d) $(2, 1, 0, 0, 2, 0, 0, \dots)$

①: Полином $P = (a_0, a_1, a_2, \dots)$ једнак је полиному $Q = (b_0, b_1, b_2, \dots)$ ако и само ако

$$a_0 = b_0, \quad a_1 = b_1, \quad \dots, \quad a_i = b_i \quad \text{за свако } i$$

①: Нека су дајти полиноми $P = (a_0, a_1, \dots)$ и $Q = (b_0, b_1, \dots)$ над пољем $(F, +, \cdot)$

$$P + Q \stackrel{\text{деф.}}{=} (a_0 + b_0, a_1 + b_1, \dots, a_i + b_i, \dots)$$

$$P \cdot Q \stackrel{\text{деф.}}{=} (c_0, c_1, c_2, \dots) \quad \text{где} \quad c_k = \sum_{i=0}^k a_i b_{k-i}, \quad k=0, 1, 2, \dots$$

Пример: $P = \begin{matrix} a_0 & a_1 & a_2 \\ (1, 2, 2) \end{matrix} \quad (\deg P = 2)$

$$Q = \begin{matrix} b_0 & b_1 & b_2 & b_3 \\ (2, 0, 1, 1) \end{matrix} \quad (\deg Q = 3)$$

a) у пољу $(\mathbb{R}, +, \cdot)$

$$P + Q = (1+2, 2+0, 2+1, 0+1)$$

$$= (3, 2, 3, 1)$$

d) у пољу $GF(3) = (\{0, 1, 2\}, +, \cdot)$

$$P + Q = (1+_3 2, 2+_3 0, 2+_3 1, 0+_3 1)$$

$$= (0, 2, 0, 1)$$

$$P \cdot Q = \left(\begin{matrix} 2, 4, \boxed{5}, 3, 4, 2 \\ c_0, c_1, c_2, c_3, c_4, c_5 \end{matrix} \right)$$

$$(dg(P \cdot Q) = 5 = dgP + dgQ)$$

$$\boxed{K=2}$$

$$\begin{aligned} c_2 &= \sum_{i=0}^2 a_i \cdot b_{2-i} = a_0 b_2 + a_1 b_1 + a_2 b_0 \\ &= 1 \cdot 1 + 2 \cdot 0 + 2 \cdot 2 \\ &= 5 \end{aligned}$$

$$P \cdot Q = \left(\begin{matrix} 2, 1, \boxed{2}, 0, 1, 2 \\ c_0, c_1, c_2, c_3, c_4, c_5 \end{matrix} \right)$$

$$\begin{aligned} c_2 &= \sum_{i=0}^2 a_i \cdot b_{2-i} = a_0 b_2 + a_1 b_1 + a_2 b_0 \\ &= 1 \cdot 1 + 2 \cdot 0 + 2 \cdot 2 = 2 \end{aligned}$$

Ⓙ. Нека је \mathcal{P} скуп свих полинома над пољем F . Тада је $(\mathcal{P}, +, \cdot)$ комутативни прстен са јединицом.

Ⓒ. Прстен $(\mathcal{P}, +, \cdot)$ зове се прстен полинома над пољем F .

$$\text{Ⓙ. } dg(P \cdot Q) = dgP + dgQ$$

Означе: Полином $(0, 1, 0, 0, \dots) = (0, 1)$ означимо са 1 .
 Полином нултог степена $(a_0, 0, 0, \dots) = (a_0)$
 означимо са a_0 . ($a_0 \in F$)

①. 1) $S^k = \underbrace{S \cdot S \cdot \dots \cdot S}_{k\text{-пута}} = \underbrace{(0, 0, \dots, 0, 1, 0, 0, \dots)}_k$

2) $(c, 0, 0, \dots) \cdot S^k = c \cdot S^k = \underbrace{(0, 0, \dots, 0, c, 0, 0, \dots)}_k$

3) $(c, 0, 0, \dots) \cdot (a_0, a_1, a_2, \dots, a_n) = c(a_0, a_1, \dots, a_n) = (ca_0, ca_1, \dots, ca_n)$

4) Сваки полином $P = (a_0, a_1, \dots, a_n)$ може се представити у облику $P = (a_0, a_1, \dots, a_n) = a_0 + a_1 \cdot S + a_2 S^2 + \dots + a_n S^n$

④ Нека је дат полином $P = a_0 + a_1 S + \dots + a_n S^n$ над пољем F . Вредност полинома P у некој тачки $x_0 \in F$ дефинише се на следећи начин: $P(x_0) = a_0 + a_1 x_0 + \dots + a_n x_0^n$.

Преобраћање $F \rightarrow F$ дефинисано са: $(\forall x \in F) x \mapsto P(x)$ тј. $x \mapsto a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$, зове се полиномска функција придружена полиному P .

Пример: $P = (1, 2, 1, 1)$ $P(x) = 1 + 2 \cdot x + 1 \cdot x^2 + 1 \cdot x^3$
 $Q = (1, 0, 1)$ $Q(x) = 1 + 0 \cdot x + 1 \cdot x^2$
 полином полиномске функције

Важно: $P = Q \Rightarrow$ полиномска функција је придружена полиному P
 $P =$ полиномска функција је придружена полиному Q

\Leftarrow
 у пољу $GF(3)$ $(\forall x) P(x) = Q(x)$

Дељење полинома

полином U : полином $V = Q$ остатак R
 $(V \neq 0)$ \downarrow
 количник

$$dgU \geq dgV \quad (dgQ = dgU - dgV) \quad (dgR < dgV)$$

$(\mathbb{Z}, +, \cdot)$ прстен

$(\mathbb{P}, +, \cdot)$ прстен

Ⓙ Нека су датии полиноми U и V над пољем F и $V \neq 0$ и $dgU \geq dgV$. Тада постоје јединствени полиноми Q и R , такви да важи $U = V \cdot Q + R$, где је (степен полинома Q) $dgQ = dgU - dgV$ и $dgR < dgV$.

Ⓘ: Полином Q из претходне теореме зове се количник, а полином R зове се остатак. при дељењу полинома U полиномом V .

Ⓛ: Ако је $R = 0$ кажемо да је полином U дељив полиномом V .
 (означа $U|V$)

Пример: $P = (1, 1, 0, 0, 2) = 1 + 1 \cdot S + 0 \cdot S^2 + 0 \cdot S^3 + 2 \cdot S^4$
 $Q = (0, 1, 1) = 0 + 1 \cdot S + 1 \cdot S^2$

а) у пољу $(\mathbb{R}, +, \cdot)$

д) у пољу \mathbb{F}_3

a) $P : Q$

$$\begin{array}{r} (2s^4 + s + 1) : (s^2 + s) = 2s^2 - 2s + 2 \\ \underline{- 2s^4 + 2s^3} \\ - 2s^3 + s + 1 \\ \underline{+ 2s^3 + 2s^2} \\ 2s^2 + s + 1 \\ \underline{- 2s^2 + 2s} \\ -s + 1 \text{ ————— остаток} \end{array}$$

$$P = Q \cdot (2s^2 - 2s + 2) + (-s + 1)$$

d) $(2s^4 + s + 1) : (s^2 + s) = \underbrace{2s^2 + s + 2}_{\text{коэффициент}}$

$$\begin{array}{r} \underline{- 2s^4 + 2s^3} \\ 1s^3 + s + 1 \\ \underline{- s^3 + s^2} \\ 2s^2 + s + 1 \\ \underline{- 2s^2 + 2s} \\ (2s + 1) \rightarrow \text{остаток} \end{array}$$

Ⓙ. Сваки полином P дељив је произвољном константом $c \in F$,
 $c \neq 0$

Пример: $P = (2, 1, 1, 0, 0, \dots) = 2 + s + s^2$
 $c = 2$

a) у пољу $(R, +, \cdot)$

$$P = 2 \cdot \underbrace{\left(1 + \frac{1}{2}s + \frac{1}{2}s^2\right)}_{\text{коэффициент}}$$

b) у пољу $GF(3)$

$$P = 2 \cdot (1 + 2s + 2s^2)$$

$$\boxed{2} \cdot x = 1$$

$$2^{-1} = 2$$

означава елемент