

Sissejuhatus algebra struktuuridesse

2023 kevad

Definitsioon

Olgu n mittenegatiivne täisarv. **n -kohaline** (ehk **n -aarne**) **algebraalne tehe** hulgal A on kujutus $A^n \longrightarrow A$, hulgast A^n hulka A .

Arvu n nimetatakse tehte $A^n \longrightarrow A$ **aarsuseks**.

Märkus

Nullaarsed tehted $A^0 = \{\} \longrightarrow A$ hulgal A on 1-1-vastavuses hulga A elementidega. Seega mõtleme unaarsest tehtest, kui hulga A fikseeritud elemendist.*

Algebralised struktuurid

Definitsioon

Hulka Ω koos tükeldusega

$$\Omega = \bigsqcup_{n=0}^{\infty} \Omega_n$$

alamhulkade Ω_n (mis võivad olla ka tühjad) lõikumatuks ühendiks nimetame **tüübiks** ehk **signatuuriks**. Iga $\omega \in \Omega_n$ korral loeme, et tehtmärgi ω aarsus on n .

Definitsioon

Olgu Ω tüüp ja A hulk. Kui iga arvu $n \in \mathbb{N} \cup \{0\}$ korral vastab igale tehtmärgile $\omega \in \Omega_n$ üks konkreetne n -kohaline algebraline tehe $\omega^A : A^n \rightarrow A$, siis ütleme, et paar $(A, \{\omega^A \mid \omega \in \Omega\})$ on Ω -**algebra**.

Homomorfismid

Definitsioon

Olgu A ja B Ω -algebrad. Kujutust $f : A \rightarrow B$ nimetatakse **homomorfismiks**, kui f säilitab kõik nendel struktuuridel defineeritud tehted. See tähendab, et

- 1 $f(\omega^A(a_1, a_2, \dots, a_n)) = \omega^B(f(a_1), f(a_2), \dots, f(a_n))$ iga $n \in \mathbb{N}$, iga $\omega \in \Omega_n$ ja mistahes elementide $a_1, a_2, \dots, a_n \in A$ korral,
- 2 $f(0_\omega^A) = 0_\omega^B$ iga $\omega \in \Omega_0$ korral.

Märkus

Nullaarne juht (2) on homomorfismi definitsioonis eraldiseisev seetõttu, et mugavuse mõttes vaatame nullaarseid tehteid elementidena, mitte kujutustena.

Homomorfismide omadused

Lause

Ω -algebrate homomorfismide korrutis on Ω -algebrate homomorfism.

Definitsioon

Homomorfismi $A \longrightarrow A$, Ω -algebrast A iseendasse, nimetatakse Ω -algebra A **endomorfismiks**.

Kõigi homomorfismide $A \longrightarrow B$ hulka Ω -algebrast A Ω -algebrasse B tähistatakse sümboliga $\text{Hom}(A, B)$. Ω -algebra A kõigi endomorfismide hulka tähistatakse sümboliga $\text{End}(A)$.

Lause

Ω -algebra A endomorfismide hulk $\text{End}(A)$ on monoid kujutuste korrutamise suhtes.

Isomorfismid ja bijektiivsed homomorfismid

Definitsioon

Bijektiivseid Ω -algebrate homomorfisme nimetatakse **isomorfismideks**. Ω -algebraid A ja B nimetatakse **isomorfseteks**, kui leidub isomorfism $f : A \rightarrow B$. Sellisel juhul kirjutatakse $A \cong B$.

Paneme nüüd tähele, et bijektiivse homomorfismi pöördkujutus on samuti homomorfism.

Lause

Isomorfismi pöördkujutus on isomorfism.

See omadus on mõningati algebrale spetsiifiline, kuna näiteks järjestust säilitava bijektsiooni pöördkujutus ei pruugi järjestust säilitada.

Alamalgebrad ja injektiivsed homomorfismid

Definitsioon

Ω -algebra A alamhulka A' nimetatakse **alamalgebraks**, kui A' on kinnine kõigi tehete $\omega^A, \omega \in \Omega$ suhtes. See tähendab, et

- 1 $\omega^A(a_1, a_2, \dots, a_n) \in A'$ iga $n \in \mathbb{N}$, iga $\omega \in \Omega_n$ ja mistahes elementide $a_1, a_2, \dots, a_n \in A'$ korral,
- 2 $0_\omega^A \in A'$ iga $\omega \in \Omega_0$ korral.

Kujutuse $f: A \longrightarrow B$ **kujutiseks** nimetatakse hulka

$$\text{Im } f = \{b \in B \mid (\exists a \in A) f(a) = b\} = \{f(a) \mid a \in A\} \subseteq B.$$

Lause

Kui $f: A \rightarrow B$ on Ω -algebra homomorfism, siis $\text{Im } f$ on Ω -algebra B alamalgebra.

Alamalgebrad ja injektiivsed homomorfismid

Lause

Ω -algebra A alamalgebrat A' saame vaadata Ω -algebrana ahendatud tehete suhtes.

Saame ka minna teistpidi.

Lause

Kui A' on Ω -algebra A alamalgebra, siis alamhulga sisestus $A' \longrightarrow A$ on injektiivne homomorfism.

Algebratele on omapärane omadus, et iga injektiivne homomorfism on isomorfismi täpsuseni alamalgebra sisestus.

Osaliselt järjestatud hulkade jaoks selline väide näiteks ei kehti.

Faktoralgebrad ja sürjektiivsed homomorfismid

Injektiivseid homomorfisme saime kirjeldada kasutades alamalgebraid. Sürjektiivsete homomorfismide kirjeldamiseks saab kasutada *faktoralgebra* mõistet.

Selleks, et faktorhulk A/ρ oleks loomulikul viisil algebra, peame nõudma ekvivalentsiseoselt ρ enamat.

Definitsioon

Ω -algebra A **kongruents** on selline ekvivalentsiseos ρ hulgal A , mis on kooskõlas tehetega. See tähendab, et

$$\begin{aligned} & a_1 \rho b_1 \wedge a_2 \rho b_2 \wedge \dots \wedge a_n \rho b_n \\ \implies & \omega^A(a_1, a_2, \dots, a_n) \rho \omega^A(b_1, b_2, \dots, b_n) \end{aligned}$$

iga $n \in \mathbb{N}$, iga $\omega \in \Omega_n$ ja mistahes elementide $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n \in A$ korral.

Kui ρ on kongruents Ω -algebral A , siis saame hulga A/ρ peal Ω -algebra struktuuri, kui defineerime $\omega \in \Omega_n$ korral

$$\omega^{A/\rho}(\overline{a_1}, \dots, \overline{a_n}) = \overline{\omega^A(a_1, \dots, a_n)}.$$

Ekvivalentsiseose ρ kongruentsiks olemise tingimus ütleb täpselt seda, et ρ definitsioon on korrektne, ehk seda, et definitsiooni parem pool ei sõltu võrduse vasakul poolel olevate ekvivalentsiklasside esindajate valikust.

Faktoralgebra A/ρ ja algebra A on seotud sürjektiivse homomorfismiga

$$\pi: A \longrightarrow A/\rho, \quad a \mapsto \overline{a},$$

mida kutsutakse **loomulikuks projektsiooniks**.

Seega, kongruentsile vastab üks sürjektiivne kujutus. Vaatame nüüd, kuidas saab (mitte ilmtingimata sürjektiivsele) kujutusele saab seada vastavusse kongruentsi.

Faktoralgebrad ja sürjektiivsed homomorfismid

Definitsioon

Ω -algebrate homomorfismi $f: A \longrightarrow A'$ **tuumaks** nimetatakse binaarset seost

$$\text{Ker } f = \{(a, a') \in A \times A \mid f(a) = f(a')\}.$$

Lause

Ω -algebrate homomorfismi $f: A \longrightarrow A'$ tuum on kongruents algebral A .

Teoreem (Homomorfismiteoreem)

Olgu $f: A \rightarrow B$ homomorfism Ω -algebrate vahel. Siis leidub üksühene homomorfism $g: A/\text{Ker } f \rightarrow B$ nii, et $f = g\pi$, kus $\pi: A \rightarrow A/\text{Ker } f$ on loomulik projektsioon.

Rühmade juht

Traditsiooniliselt antakse rühma definitsioon järgmisel kujul.

Definitsioon

Rühm on hulk G koos kahekohalise algebralise tehtega $*$, mis rahuldab järgmisi tingimusi:

- G1.** $(a * b) * c = a * (b * c)$ iga $a, b, c \in G$ korral;
- G2.** leidub element $e \in G$ nii, et $a * e = a = e * a$ iga $a \in G$ korral;
- G3.** iga $a \in G$ korral leidub element $b \in G$ nii, et $a * b = e = b * a$.

Elementi e tingimuses G2 nimetatakse selle rühma

ühikelemendiks. Elementi b tingimuses G3 nimetatakse elemendi a **pöördelemendiks** ja tähistatakse sümboliga a^{-1} .

Rühma ühikelementi tähistatakse tihti ka sümboliga 1. Nii ühikelement kui iga elemendi pöördelement rühmas on üheselt määratud.

Definitsioon

Rühm on hulk G koos kahekohalise algebralise tehtega $*$, mis rahuldab järgmisi tingimusi:

- G1.** $(a * b) * c = a * (b * c)$ iga $a, b, c \in G$ korral;
- G2.** leidub element $e \in G$ nii, et $a * e = a = e * a$ iga $a \in G$ korral;
- G3.** iga $a \in G$ korral leidub element $b \in G$ nii, et $a * b = e = b * a$.

Ühikelement ei esine otseselt sellises rühma definitsioonis konstandina 1 ning samuti pöördelemendi võtmise operatsioon ei eksisteeri sellises rühma definitsioonis eraldi operatsioonina.

See tähendab, et sellise definitsiooni juures ei ole ühik ja elemendi pööramine osa *struktuurist*, vaid on *omadused*.

Rühmade juht

Et rühmad paremini Ω -algebrate kontekstiga ühilduks, peaksime lisama rühma definitsioonile konstandi 1 ning pööramise tehte $()^{-1}$.

Definitsioon

Rühm on hulk G koos konstandiga 1, unaarse tehtega $()^{-1}$ ja kahekohalise tehtega $*$, mis rahuldavad järgmisi tingimusi:

G1. $(a * b) * c = a * (b * c)$ iga $a, b, c \in G$ korral;

G2. $a * 1 = a = 1 * a$ iga $a \in G$ korral;

G3. iga $a \in G$ korral $a * a^{-1} = e = a^{-1} * a$.

Selle definitsiooni vahe eelmisega on see, et Ω -algebrate kontekstis ei pruugi eelmise definitsiooni põhjal rühma alamstruktuur olla rühm.

Lause

Rühma G mittetühi alamhulk H on alamrühm parajasti siis, kui H on kinnine korrutamise ja pöördelendi võtmise suhtes.

Märgime, et tavaliselt kasutame rühma ühiku jaoks tähist 1 siis, kui 1 on signatuuris antud sümbol, ning tähist e , kui rühma ühik on antud omadusega, nagu esimeses definitsioonis.

Rühmade juht

Igale kongruentsile ρ rühmal G saame seada vastavusse ühikelemendi $\bar{1}$ ekvivalentsiklassi. On lihtne veenduda, et $\bar{1}$ on rühma G alamrühm.

Lause

Kui H on rühma G alamrühm, siis hulgad iga $a, b \in G$ korral

- hulgad aH ja bH kas ühtivad või on lõikumatud;*
- $aH = bH$ parajasti siis, kui $a^{-1}b \in H$.*

Lausest näeme, et iga alamrühm tekitab rühmal ekvivalentsiseose. Üldjuhul ei pruugi aga see seos olla kongruents.

Et tekitatud seos oleks kongruents, on piisav ja tarvilik tingimus, et alamrühm oleks **normaalne**, ehk rahuldaks tingimust, et iga $a \in G$ korral $a^{-1}Ha = H$.

Hulkade otsekorrutised

Hulkade X_i , $i \in I$ **otsekorrutis** on hulk

$$\prod_{i \in I} X_i = \left\{ x : I \rightarrow \bigcup_{i \in I} X_i \mid (\forall i \in I) x(i) \in X_i \right\}.$$

Tähistame kujutuse $x : I \rightarrow \bigcup_{i \in I} X_i$ korral $x_i := x(i)$. Sellist kujutust kirjutame üles kujul $x = (x_i)_{i \in I}$ ja kutsume **pereks, mis on indekseeritud hulga I järgi**. Elementi x_i kutsume pere $(x_i)_{i \in I}$ **i -ndaks komponendiks**. Niisiis otsekorrutis koosneb kõigist peredest $(x_i)_{i \in I}$, kus $x_i \in X_i$ iga $i \in I$ korral. Peresid $(x_i)_{i \in I}$ ja $(y_i)_{i \in I}$ loeme **võrdseteks**, kui nende vastavad komponendid on võrdsed, s.t.

$$(x_i)_{i \in I} = (y_i)_{i \in I} \iff (\forall i \in I) x_i = y_i.$$

Algebrate otsekorrutised

Vaatleme nüüd Ω -algebraid X_i , $i \in I$. Defineerime hulkade otsekorrutisel $X := \prod_{i \in I} X_i$ tehted n.ö. komponenthaaval:

$$\omega^X \left((x_i^1)_{i \in I}, (x_i^2)_{i \in I}, \dots, (x_i^n)_{i \in I} \right) := \left(\omega^{X_i}(x_i^1, x_i^2, \dots, x_i^n) \right)_{i \in I},$$

kui $\omega \in \Omega_n$ ($n \in \mathbb{N}$) ja

$$0_\omega^X := \left(0_\omega^{X_i} \right)_{i \in I},$$

kui $\omega \in \Omega_0$. Nii tehes saame Ω -algebra, mida nimetatakse esialgsete algebrate **otsekorrutiseks**.

- VR1.** $(a + b) + c = a + (b + c)$ iga $a, b, c \in V$ korral;
- VR2.** leidub element $0 \in V$ nii, et iga $a \in V$ korral
 $a + 0 = a = 0 + a$;
- VR3.** iga elemendi $a \in V$ korral leidub element $-a \in V$ nii, et
 $a + (-a) = 0 = (-a) + a$;
- VR4.** $a + b = b + a$ iga $a, b \in V$ korral;
- VR5.** $k(a + b) = ka + kb$ iga $a, b \in V$ ja $k \in K$ korral;
- VR6.** $(k + l)a = ka + la$ iga $a \in V$ ja $k, l \in K$ korral;
- VR7.** $(kl)a = k(la)$ iga $a \in V$ ja $k, l \in K$ korral;
- VR8.** $1a = a$ iga $a \in V$ korral.

Vektorruumide alamalgebrad kutsutakse **alamruumideks**.

Lause

Vektorruumi V mittetühi alamhulk V' on alamruum parajasti siis, kui

AR1 *iga $a, b \in V'$ korral $a + b \in V'$ (s.t. V' on kinnine liitmise suhtes);*

AR2 *iga $a \in V'$ ja $k \in K$ korral $ka \in V'$ (s.t. V' on kinnine skalaariga korrutamiste suhtes).*

Definitsioon

Olgu V vektorruum üle korpuse K ja $a_1, \dots, a_s \in V$, kus $s \in \mathbb{N}$.
Mistahes avaldist

$$k_1 a_1 + k_2 a_2 + \dots + k_s a_s, \quad (1)$$

kus $k_1, \dots, k_s \in K$, aga ka selle avaldise poolt määratud V elementi, nimetatakse vektorite $a_1, \dots, a_s$

lineaarkombinatsiooniks. Skalaare $k_1, \dots, k_s$ nimetatakse selle lineaarkombinatsiooni **kordajateks**.

Lineaarne sõltumatus vektorruumis

Definitsioon

Vektorruumi V (mis on antud üle korpuse K) lõplikku vektorite hulka $\{a_1, a_2, \dots, a_s\}$, $s \in \mathbb{N}$, nimetatakse **lineaarselt sõltumatuks**, kui mistahes skalaaride $k_1, k_2, \dots, k_s \in K$ korral võrdusest

$$k_1 a_1 + k_2 a_2 + \dots + k_s a_s = 0$$

järeldub, et

$$k_1 = k_2 = \dots = k_s = 0.$$

Lisaks sellele loeme ka tühja vektorite hulga lineaarselt sõltumatuks. Lõpmatut vektorite hulka nimetatakse **lineaarselt sõltumatuks**, kui tema iga lõplik alamhulk on lineaarselt sõltumatu.

Vektorruumi baas

Definitsioon

Vektorruumi V vektorite hulka B nimetatakse **baasiks**, kui

- 1 hulk B on lineaarselt sõltumatu,
- 2 vektorruumi V iga nullist erinev vektor avaldub hulka B kuuluvate vektorite lineaarkombinatsioonina.

Teoreem

Igas mittetriviaalses vektorruumis leidub baas.

Teoreem

Iga mittetriviaalse vektorruumi V korral (üle korpuse K) leidub selline hulk I , et

$$V \cong \bigoplus_{i \in I} V_i,$$

Rühmade isomorfismiteoreemid

Teoreem (Esimene isomorfismiteoreem)

Olgu G rühm, $H \leq G$ ja $K \trianglelefteq G$. Siis

$$H/(H \cap K) \cong HK/K.$$

Teoreem (Teine isomorfismiteoreem)

Olgu G rühm, $H \trianglelefteq G$, $K \trianglelefteq G$ ja $K \subseteq H$. Siis

$$(G/K)/(H/K) \cong G/H.$$

Teoreem (Kolmas isomorfismiteoreem)

Olgu G rühm, $H \trianglelefteq G$, $\pi : G \rightarrow G/H$ loomulik projektsioon, $N \trianglelefteq G/H$ ja $M = \pi^{-1}(N)$. Siis $M \trianglelefteq G$ ja

$$G/M \cong (G/H)/N.$$

Definitsioon

Substitutsiooni nimetatakse **tsükliks**, kui ta paigutab mingeid elemente tsüklikiliselt ümber ning jätab ülejäänud elemendid paigale. Tsükli σ , mis paigutab ümber elemente $i_1, i_2, \dots, i_k$ nii, et

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1,$$

tähistame lühidalt

$$(i_1, i_2, \dots, i_k).$$

Arvu k nimetame tsükli $(i_1, i_2, \dots, i_k)$ **pikkuseks**.

Definitsioon

Tsükleid $(i_1, i_2, \dots, i_k)$ ja $(j_1, j_2, \dots, j_l)$ nimetatakse **sõltumatuteks**, kui $\{i_1, i_2, \dots, i_k\} \cap \{j_1, j_2, \dots, j_l\} = \emptyset$.

Lause

Iga substituutsiooni saab esitada sõltumatute tsüklite korrutisena.

Näide

Rühmas S_9 saame esitada

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 6 & 9 & 7 & 4 & 2 & 1 & 8 & 3 \end{pmatrix} = (1, 5, 4, 7)(2, 6)(3, 9).$$

Definitsioon

Transpositsioon on tsükkel pikkusega 2.

Lause

Transpositsioon on paaritu substituutsioon.

Lause

Olgu $n \geq 2$. Iga paarissubstitutsioon n elemendist on esitatav paarisarvu transpositsioonide korrutisena. Iga paaritu substitutsioon n elemendist on esitatav paaritu arvu transpositsioonide korrutisena.

Järeldus

Olgu $n \geq 2$. Siis on paaris- ja paarituid substitutsioone n elemendist ühepalju.

Lause

Olgu substitutsioon σ esitatav k transpositsiooni korrutisena. Siis σ on paarissubstitutsioon parajasti siis, kui k on paarisarv.

Järeldus

Substitutsioonid σ ja σ^{-1} on sama paarsusega.

Lause

Tsükli $(i_1, i_2, \dots, i_k)$ paarsus on võrdne arvu $k - 1$ paarsusega.

Lause

Paarissubstitutsioonide hulk A_n on rühma S_n normaaljagaja.

Teoreem

Kui $n \geq 5$, siis A_n on lihtne rühm.

Märkus

Saab näidata, et A_2 ja A_3 on lihtsad rühmad, aga A_4 ei ole.

Definitsioon

Olgu $A_i, i \in I$ hulga I poolt indekseeritud Abeli rühmade pere. Nende Abeli rühmade **väliseks otsesummaks** nimetatakse Abeli rühmade A_i otsekorrutise $\prod_{i \in I} A_i$ alamrühma

$$\bigoplus_{i \in I} A_i = \{(a_i)_{i \in I} \in \prod_{i \in I} A_i \mid \text{card}\{i \in I \mid a_i \neq 0\} < \infty.\}$$

Kui $I = \{1, 2, \dots, n\}$, siis Abeli rühmade $A_1, A_2, \dots, A_n$ välist otsesummat tähistatakse harilikult $A_1 \oplus A_2 \oplus \dots \oplus A_n$.

Definitsioon

Olgu A Abeli rühm ja $A_i, i \in I$ tema alamrühmad. Nende alamrühmade **summaks** nimetatakse alamrühma $\sum_{i \in I} A_i$, mis koosneb kõigist lõplikest summadest, kus liidetavateks on paarikaupa erinevate indeksitega alamrühmade elemendid, s.t.

$$\sum_{i \in I} A_i = \{a \in A \mid a = a_{i_1} + \dots + a_{i_k}, k \in \mathbb{N},$$

$i_1, \dots, i_k \in I$ on paarikaupa erinevad, $a_{i_1} \in A_{i_1}, \dots, a_{i_k} \in A_{i_k}\}$.

Lõpliku indeksite hulga $I = \{i_1, \dots, i_n\}$ korral kirjutatakse $\sum_{i \in I} A_i$ asemel $A_{i_1} + \dots + A_{i_n}$ ja kehtib võrdus

$$A_{i_1} + \dots + A_{i_n} = \{a_1 + \dots + a_n \mid a_1 \in A_{i_1}, \dots, a_n \in A_{i_n}\}.$$

Definitsioon

Abeli rühma A alamrühmade $A_i, i \in I$ summat $\sum_{i \in I} A_i$ nimetatakse **sisemiseks otsesummaks**, kui iga lõpliku alamhulga $\{i_0, i_1, \dots, i_n\} \subseteq I$ korral

$$A_{i_0} \cap (A_{i_1} + \dots + A_{i_n}) = \{0\}.$$

Kui alamrühmade $A_i, i \in I$ summa on sisemine otsesumma, siis kirjutatakse

$$\sum_{i \in I} A_i = \dot{\sum}_{i \in I} A_i.$$

Teoreem

Olgu A Abeli rühm ja $A_i, i \in I$ tema alamrühmad. Kui nende alamrühmade sisemine otsesumma on olemas, siis on sisemine ja väline otsesumma isomorfsed.

Lause

Abeli rühma A alamrühmade B ja C summa $B + C$ on sisemine otsesumma parajasti siis, kui iga $b, b' \in B$ ja $c, c' \in C$ korral

$$b + c = b' + c' \implies b = b' \text{ ja } c = c'$$

Definitsioon

Olgu a Abeli rühma A element ja $n \in \mathbb{N}$. Öeldakse, et elemendi a **järk** on n , kui $na = 0$ ja n on vähim naturaalarv, mille korral selline võrdus kehtib. Kui $na \neq 0$ ühegi naturaalarvu n korral, siis öeldakse, et element a on **lõpmatut järku**. Elemendi a järku tähistatakse sümboliga $\text{ord}(a)$.

Definitsioon

Abeli rühma **perioodiline osa** on tema alamhulk, mis koosneb tema kõigist lõplikku järku elementidest. Abeli rühma nimetatakse **perioodiliseks**, kui kõik tema elemendid on lõplikku järku.

Definitsioon

Kui A on Abeli rühm ja p on algarv, siis hulka

$$A_p = \{a \in A \mid \text{ord}(a) \text{ on } p \text{ aste}\} \subseteq A$$

nimetatakse rühma A **p -komponendiks**. Saab näidata, et A_p on A alamrühm. Kui $A = A_p$, siis öeldakse, et A on **p -rühm**.

Lemma

Iga mittetriviaalne Abeli p -rühm sisaldab elementi, mille järk on p .

Lemma

Kui A on Abeli rühm, $a \in A$ ja $m \in \mathbb{N}$, siis

$$ma = 0 \iff \text{ord}(a) \mid m.$$

Teoreem

Perioodiline Abeli rühm on oma p -komponentide sisemine otsesumma.

Definitsioon

Abeli rühma A nimetatakse **jaguvaks**, kui iga elemendi $a \in A$ ja iga naturaalarvu n korral leidub selline $b \in A$, et $nb = a$. Elementi b nimetatakse elemendi a ja naturaalarvu n **jagatiseks**.

Näide

1. Rühma $(\mathbb{Z}, +)$ ei ole jaguv.
2. Rühm $(\mathbb{Q}, +)$ on jaguv.

Lause

Abeli rühm A on jaguv parajasti siis, kui iga elemendi $a \in A$ ja iga algarvu p korral leidub selline $b \in A$, et $pb = a$.

Me ütleme, et Abeli rühm B on Abeli rühma A **homomorfne kujutis**, kui leidub sürjektiivne homomorfism $f : A \rightarrow B$.

Lause

Jaguva Abeli rühma homomorfne kujutis on jaguv.

Lause

Jaguvate Abeli rühmade otsekorrutis ja väline otsesumma on jaguvad.

Lause

Olgu B Abeli rühm, $A \leq B$ ja olgu $f : A \rightarrow D$ mingi homomorfism, kusjuures D on jaguv Abeli rühm. Siis leidub homomorfism $g : B \rightarrow D$ nii, et $g|_A = f$.

Definitsioon

Öeldakse, et Abeli rühm on **väändeta**, kui kõik tema nullist erinevad elemendid on lõpmatut järku.

Näide

Rühmad $(\mathbb{Z}, +)$ ja $(\mathbb{Q}, +)$ on väändeta.

Lause

Mittetriviaalne väändeta jaguv rühm sisaldab rühmaga $\mathbb{Q}$ isomorfset alamrühma.

Vaatleme hulka

$$Q(b) = \{(xb)/n \mid x \in \mathbb{Z}, n \in \mathbb{N}\} \subseteq B.$$

Defineerime kujutuse $f : \mathbb{Q} \rightarrow B$ võrdusega

$$f\left(\frac{x}{n}\right) := (xb)/n.$$

Definitsioon

Hulka R koos kahe kahekohalise algebralise tehtega $+$ ja $\cdot$ nimetatakse (ühikelemendiga assotsiatiivseks) **ringiks**, kui

- R1.** $(a + b) + c = a + (b + c)$ iga $a, b, c \in R$ korral;
- R2.** leidub element $0 \in R$ nii, et $a + 0 = a = 0 + a$ iga $a \in R$ korral;
- R3.** iga $a \in R$ korral leidub element $-a \in R$ nii, et $a + (-a) = 0 = (-a) + a$;
- R4.** $a + b = b + a$ iga $a, b \in R$ korral;
- R5.** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ iga $a, b, c \in R$ korral;
- R6.** leidub element $1 \in R$ nii, et $a \cdot 1 = a = 1 \cdot a$ iga $a \in R$ korral;
- R7.** $a \cdot (b + c) = a \cdot b + a \cdot c$ iga $a, b, c \in R$ korral;
- R8.** $(a + b) \cdot c = a \cdot c + b \cdot c$ iga $a, b, c \in R$ korral.

Definitsioon

Ringi $(R, +, \cdot)$ nimetatakse

- **jagamisega ringiks**, kui $(R \setminus \{0\}, \cdot)$ on rühm;
- **korpuseks**, kui $(R \setminus \{0\}, \cdot)$ on Abeli rühm.

Märkus

Ringi puhul on võimalik, et $1 = 0$. Sellisel juhul see ring koosnebki ainult ühest elemendist, sest mistahes elemendi a korral $a = a1 = a0 = 0$. Järelikult, kui ringis on vähemalt kaks elementi, siis selles ringis $1 \neq 0$. Muuhulgas korpuses on alati $1 \neq 0$.

Ringide homomorfismid

Lause

Olgu R_1 ja R_2 ringid. Kujutus $f: R_1 \rightarrow R_2$ on ringide homomorfism parajasti siis, kui

- 1 $f(a + b) = f(a) + f(b)$ iga $a, b \in R_1$ korral;
- 2 $f(ab) = f(a)f(b)$ iga $a, b \in R_1$ korral;
- 3 $f(1) = 1$.

Definitsioon

Ringide homomorfismi $f: R_1 \rightarrow R_2$ **tuumaks** nimetatakse hulka

$$\text{Ker}(f) = \{a \in R_1 \mid f(a) = 0\}.$$

Lause

Ringide homomorfism $f: R_1 \rightarrow R_2$ on üksühene parajasti siis, kui $\text{Ker}(f) = \{0\}$.

Ringide ideaalid

Definitsioon

Ringi R mittetühja alamhulka I nimetatakse **parempoolseks (vasakpoolseks) ideaaliks**, kui

- 1 $a + b \in I$ iga $a, b \in I$ korral;
- 2 $ar \in I$ ($ra \in I$) iga $a \in I$ ja $r \in R$ korral.

Parempoolset ideaali, mis on samaaegselt ka vasakpoolne ideaal, nimetatakse **ideaaliks**.

Mistahes ringi R korral on R ise ja $\{0\}$ ideaalid. Neid ideaale nimetatakse **triviaalseteks**.

Lause

Ringide homomorfismi tuum on ideaal.

Ringi peaideaalid

Lemma

Olgu R ring ja $a \in R$. Siis

① hulk

$$aR = \{ar \mid r \in R\}$$

on ringi R parempoolne ideaal,

② hulk

$$Ra = \{ra \mid r \in R\}$$

on ringi R vasakpoolne ideaal,

③ hulk

$$RaR = \left\{ \sum_{i=1}^n x_i a y_i \mid n \in \mathbb{N}, x_i, y_i \in R \right\}$$

on ringi R ideaal.

Ringi peaideaalid

Definitsioon

Ideaale aR , Ra ja RaR nimetatakse vastavalt ringi R elemendi a poolt tekitatud **parempoolseks peaideaaliks**, **vasakpoolseks peaideaaliks** ja **(kahepoolseks) peaideaaliks**.

Lemma

Ringi parempoolsete ideaalide (vasakpoolsete ideaalide, ideaalide) ühisosa on samuti parempoolne ideaal (vasakpoolne ideaal, ideaal).

Lause

Ringis, mis sisaldab vähemalt kahte elementi, ei ole mittetriviaalseid parempoolseid ideaale parajasti siis, kui see ring on jagamisega ring.

Definitsioon

Ringi nimetatakse **lihtsaks**, kui temas ei ole mittetriviaalseid ideaale.

Lause

Olgu D jagamisega ring ja $n \in \mathbb{N}$. Siis ring $\text{Mat}_n(D)$ on lihtne.

Minimaalsed ideaalid

Definitsioon

Ringi R parempoolset ideaali I nimetatakse **minimaalseks parempoolseks ideaaliks**, kui I on minimaalne element ringi R nullist erinevate parempoolsete ideaalide hulgas.

Lause

Olgu D jagamisega ring ja $n \in \mathbb{N}$. Siis ring $\text{Mat}_n(D)$ sisaldab minimaalset parempoolset ideaali.

Teoreem

Ring R on lihtne minimaalset parempoolset ideaali sisaldav ring parajasti siis, kui leidub jagamisega ring D ja naturaalarv n nii, et

$$R \cong \text{Mat}_n(D).$$

Definitsioon

Hulka A koos kujutustega $+: A \times A \rightarrow A$ ja $\cdot: R \times A \rightarrow A$ nimetatakse (vasakpoolseks) **mooduliks** üle ringi R , kui

- M1.** $(a + b) + c = a + (b + c)$ iga $a, b, c \in A$ korral;
- M2.** leidub element $0 \in A$ nii, et iga $a \in A$ korral $a + 0 = a = 0 + a$;
- M3.** iga elemendi $a \in A$ korral leidub element $-a \in A$ nii, et $a + (-a) = 0 = (-a) + a$;
- M4.** $a + b = b + a$ iga $a, b \in A$ korral;
- M5.** $k(a + b) = ka + kb$ iga $a, b \in A$ ja $k \in R$ korral;
- M6.** $(k + l)a = ka + la$ iga $a \in A$ ja $k, l \in R$ korral;
- M7.** $(kl)a = k(la)$ iga $a \in A$ ja $k, l \in R$ korral;
- M8.** $1a = a$ iga $a \in A$ korral.

Täpsed jada

Olgu meil jada vasakpoolsetest R -moodulitest A_α ning nendevahelistest homomorfismidest f_α :

$$\dots \xrightarrow{f_{\alpha-1}} A_\alpha \xrightarrow{f_\alpha} A_{\alpha+1} \xrightarrow{f_{\alpha+1}} \dots \quad (2)$$

Definitsioon

Moodulite jada kujul (2) nimetatakse **täpseks kohal** α , kui

$$\text{Ker}(f_\alpha) = \text{Im}(f_{\alpha-1}).$$

Sellist jada, mis on täpne igal kohal, nimetatakse **täpseks**.

Jada täpsusest kohal α järeldub otseselt, et $f_\alpha f_{\alpha-1} = 0$, ehk täpsel kohal kahe homomorfismi järjestikune rakendamine annab tulemuseks nullhomomorfismi.

Lühikesed täpsed jadad

Lemma

Moodulite jada

- ① $0 \rightarrow A \xrightarrow{f} B$ on täpne parajasti siis kui f on injektiivne;
- ② $A \xrightarrow{f} B \rightarrow 0$ on täpne parajasti siis kui f on sürjektiivne;
- ③ $0 \rightarrow A \xrightarrow{f} B \rightarrow 0$ on täpne parajasti siis kui f on bijektiivne.

Definitsioon

Täpset jada kujul

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

nimetatakse **lühikeseks täpseks jadaks**.

Kui lühikeses täpses jadas samastada A ja sellega isomorfne B alammodul $\operatorname{Im}(f)$, siis võiks tinglikult kirjutada $C \cong B/A$.

Teoreem

Olgu

$$0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} C \longrightarrow 0$$

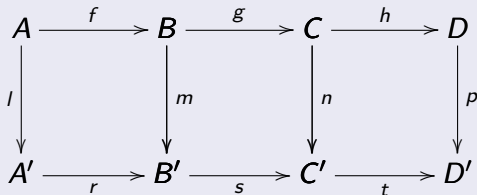
lühike täpne jada. Siis järgmised väited on samaväärsed.

- (i) *Leidub homomorfism $\varphi: B \rightarrow A$ nii, et $\varphi\iota = 1_A$.*
- (ii) *Leidub endomorfism $f: B \rightarrow B$ nii, et $f^2 = f$ ja $\text{Im}(f) = \text{Im}(\iota)$.*
- (iii) *Leidub mooduli B alammodul H nii, et $B = \text{Im } \iota \dot{+} H$.*
- (iv) *Leidub homomorfism $\psi: C \rightarrow B$ nii, et $\pi\psi = 1_C$.*

4-lemma

Teoreem (4-lemma)

Kui kommutatiivse diagrammi



read on täpsed jadad, m ja p on injektiivsed ja l on sürjektiivne, siis n on injektiivne.

Vabad moodulid

Definitsioon

Moodulit nimetatakse **vabaks** kui temas leidub baas, s.t. lineaarselt sõltumatu moodustajate süsteem.

Lause

Vasakpoolne R -moodul F on vaba parajasti siis, kui ta on isomorfne välise otsesummaga sellistest moodulitest A_i , kus $A_i \cong {}_R R$ iga $i \in I$ korral:

$$F \cong \bigoplus_{i \in I} A_i.$$

Lause

Iga moodul on vaba mooduli homomorfne kujutis (faktormoodul).

Projektiivsed moodulid

Definitsioon

Moodulit ${}_R P$ nimetatakse **projektiivseks**, kui iga sürjektiivse moodulite homomorfismi $\pi: {}_R A \rightarrow {}_R B$ ja iga moodulite homomorfismi $f: {}_R P \rightarrow {}_R B$ korral leidub moodulite homomorfism $g: {}_R P \rightarrow {}_R A$ nii, et $f = \pi g$.

Lause

Iga vaba moodul F on projektiivne.

Lause

Kui P ja Q on R -moodulid ja moodul $P \oplus Q$ on projektiivne, siis ka P ja Q on projektiivsed.

Teoreem

Järgmised väited R -mooduli P kohta on samaväärsed.

- 1 Moodul P on projektiivne.
- 2 Iga lühikese täpse jada

$$0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} P \longrightarrow 0$$

korral leidub homomorfism $\psi: P \rightarrow B$ nii, et $\pi\psi = 1_P$.

- 3 Leidub vaba moodul F nii, et $F = A \dot{+} B$, kusjuures üks otseliidetavatest on isomorfne mooduliga P .

Definitsioon

Poolrühmaks nimetatakse hulka S koos sellel defineeritud kahekohalise algebralise tehtega $\cdot$, mis on assotsiatiivne, see tähendab, et mistahes $a, b, c \in S$ korral $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. Harilikult kirjutatakse $a \cdot b$ asemel lihtsalt ab .

Definitsioon

Olgu S ja T poolrühmad. Kujutust $f: S \longrightarrow T$ nimetatakse **poolrühmade homomorfismiks**, kui

$$f(xy) = f(x)f(y)$$

iga $x, y \in S$ korral.

Näide

1. $(\mathbb{N}, +)$ on poolrühm, mis ei ole monoid.
2. $(\mathbb{N}, \cdot)$ on monoid ühikelemendiga 1.
3. Kordarvude hulk on poolrühm korrutamise suhtes.
4. Mittetühja hulga X kõigi teisenduste hulk $\mathcal{T}(X)$ on monoid teisenduste järjestrakendamise suhtes. Selle monoidi ühikelement on hulga X samasusteisendus 1_X .
5. Olgu X suvaline mittetühi hulk. Defineerides

$$xy := x$$

iga $x, y \in X$ korral saame poolrühma, mida nimetatakse vasakpoolsete nullide poolrühmaks.

Lõplikud poolrühmad

Näide

Lõpliku poolrühma korrutamistehe antakse sageli tabeli abil, mida kutsutakse Cayley tabeliks (või lihtsalt korrutamistabeliks). Sellises tabelis on elemendiga a märgistatud rea ja elemendiga b märgistatud veeru lõikekohas korrutis ab . Näiteks võib vaadelda poolrühma

$$S = \{e, a, f, b\},$$

mille Cayley tabel on

	e	a	f	b
e	e	e	e	b
a	e	e	a	b
f	e	e	f	b
b	b	b	b	e

Definitsioon

Alamhulka I poolrühmas S nimetatakse poolrühma S **parempoolseks (vasakpoolseks) ideaaliks**, kui

$$as \in I \ (sa \in I)$$

mistahes $a \in I$, $s \in S$ korral. Poolrühma S **ideaaliks** nimetatakse parempoolset ideaali I , mis on samal ajal ka vasakpoolne ideaal.

Definitsiooni järgi loeme ka poolrühma tühja alamhulga ideaaliks. On selge, et poolrühma ideaal on alampoolrühm. Vastupidine üldjuhul ei kehti.

Definitsioon

Poolrühma S ideaali I nimetatakse **minimaalseks ideaaliks**, kui

- 1 $I \neq \emptyset$
- 2 iga ideaali J korral $J \neq \emptyset$ ja $J \subseteq I \Rightarrow J = I$.

Ideaalid vs. kongruentsid

Ringide puhul olid ideaalid üksüheses vastavuses ringi kongruentsidega. Paraku aga suvalise poolrühma S kõiki kongruentse ainult poolrühma S ideaale vaadates kirjeldada ei õnnestu.

Kuigi igale kongruentsile ei vasta ideaal, saab siiski ideaali põhjal järgmisel viisil kongruentsi defineerida.

Reesi faktorpoolrühm ideaali järgi

Kui I on mittetühi ideaal poolrühmas S , saame defineerida poolrühmal S kongruentsi ρ_I seosega

$$x\rho_I y \iff \begin{cases} x, y \in I & \text{või} \\ x = y. \end{cases}$$

Selle kongruentsi järgi faktorpoolrühma tähistatakse $S/I \stackrel{\text{def}}{=} S/\rho_I$.

Lause

Kui poolrühmas S leidub ühikelement (s.t. element $e \in S$, mille korral $ex = x = xe$ iga $x \in S$ jaoks), on see poolrühmas ainus ühikelement.

Seega saame poolrühma ühikelemendist (kui ta leidub) mõelda, kui fikseeritud elemendist 1.

Definitsioon

Monoidiks nimetatakse poolrühma koos fikseeritud ühikelemendiga 1 (s.t. on antud selline element 1, et iga $1 \in S$ korral $1a = a = a1$).

Monoidide homomorfism vs poolrühmade homomorfism

Kui kui S ja T on monoidid ning $f: S \longrightarrow T$ on poolrühmade homomorfism, ei pruugi see ühikelementi säilitada. Kuna ühikut vaatame osana monoidi struktuurist, peaksime monoidide homomorfismilt nõudma ühiku säilitamist.

Definitsioon

Olgu S ja T monoidid. Kujutust $f: S \longrightarrow T$ nimetatakse **monoidide homomorfismiks**, kui

$$f(1) = 1$$

ning

$$f(xy) = f(x)f(y)$$

iga $x, y \in S$ korral.

Poolrühma monoidiks muutmine ühiku välisel lisamisel

Definitsioon

Olgu S poolrühm, olgu 1 mingi element, mis ei kuulu hulka S ja

$$S^1 = S \cup \{1\}.$$

Defineerime hulgal S^1 korrutamise nii, et poolrühma S elementide omavahelisi korrutisi ei muudeta, $1 \cdot 1 = 1$ ja

$$1s = s1 = s$$

iga $s \in S$ korral. Ilmselt on S^1 monoid ühikelemendiga 1 . Öeldakse, et monoid S^1 on saadud poolrühmast S **ühikelemendi välisel lisamisel**.

Mistahes poolrühma S ja elemendi $a \in S$ korral tähistame

$$Sa = \{sa \mid s \in S\},$$

$$aS = \{as \mid s \in S\},$$

$$SaS = \{sat \mid s, t \in S\}.$$

Siis

$$S^1a = Sa \cup \{a\},$$

$$aS^1 = aS \cup \{a\},$$

$$S^1aS^1 = SaS \cup Sa \cup aS \cup \{a\}.$$

Lemma

Olgu S poolrühm ja $a \in S$. Siis

- ① S^1a on vähim vasakpoolne ideaal, mis sisaldab elementi a ,
- ② aS^1 on vähim parempoolne ideaal, mis sisaldab elementi a ,
- ③ S^1aS^1 on vähim ideaal, mis sisaldab elementi a .

Lemma

Olgu S poolrühm ja $a \in S$. Siis

- ① S^1a on vähim vasakpoolne ideaal, mis sisaldab elementi a ,
- ② aS^1 on vähim parempoolne ideaal, mis sisaldab elementi a ,
- ③ S^1aS^1 on vähim ideaal, mis sisaldab elementi a .

Definitsioon

Öeldakse, et S^1a (aS^1 , S^1aS^1) on poolrühma S elemendi a poolt tekitatud **vasakpoolne peaideaal** (vastavalt **parempoolne peaideaal**, **peaideaal**).

Lihtsad poolrühmad

Definitsioon

Poolrühma S ideaali I nimetatakse **pärisideaaliks**, kui $I \neq S$.

Definitsioon

Mittetühja poolrühma S nimetatakse **lihtsaks**, kui ta ei sisalda mittetühje pärisideaale.

Seega poolrühm on lihtne parajasti siis, kui tal on täpselt kaks ideaali: $\emptyset$ ja S .

Lause

Poolrühm S on lihtne parajasti siis, kui $SaS = S$ iga $a \in S$ korral.

Lihtsad poolrühmad

Definitsioon

Poolrühma S ideaali I nimetatakse **pärisideaaliks**, kui $I \neq S$.

Definitsioon

Mittetühja poolrühma S nimetatakse **lihtsaks**, kui ta ei sisalda mittetühje pärisideaale.

Seega poolrühm on lihtne parajasti siis, kui tal on täpselt kaks ideaali: $\emptyset$ ja S .

Lause

Poolrühm S on lihtne parajasti siis, kui $SaS = S$ iga $a \in S$ korral.

Kui A ja B on poolrühma S alamhulgad, siis kasutatakse tähistust

$$AB = \{ab \mid a \in A, b \in B\}.$$

Muuhulgas $A = B = S$ korral kirjutatakse $SS = S^2$.

Definitsioon

Poolrühma S nimetatakse **faktoriseeruvaks**, kui $S^2 = S$.

Teiste sõnadega: poolrühm on faktoriseeruv, kui selle iga element on esitatav kahe elemendi korrutisena.

Lause

Lihne poolrühm on faktoriseeruv.

Lause

Kui M on minimaalne ideaal poolrühmas S , siis M on ise lihne poolrühm.

Definitsioon

Olgu $\mathcal{J}$, $\mathcal{L}$, $\mathcal{R}$, $\mathcal{H}$ ja $\mathcal{D}$ seosed poolrühmal S , mis on defineeritud järgmiselt:

$$a\mathcal{J}b \iff S^1aS^1 = S^1bS^1$$

$$a\mathcal{R}b \iff aS^1 = bS^1$$

$$a\mathcal{L}b \iff S^1a = S^1b$$

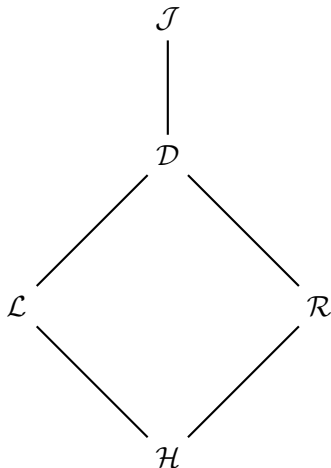
$$\mathcal{H} = \mathcal{L} \cap \mathcal{R}$$

$$\mathcal{D} = \mathcal{L} \circ \mathcal{R}$$

mistahes $a, b \in S$ korral. Seoseid $\mathcal{J}$, $\mathcal{L}$, $\mathcal{R}$, $\mathcal{H}$ ja $\mathcal{D}$ nimetatakse **Greeni seosteks** poolrühmal S .

Seosed $\mathcal{R}$, $\mathcal{L}$ ja $\mathcal{J}$ on ekvivalentsiseosed hulgal S .

Saab näidata, et $\mathcal{H} = \mathcal{L} \wedge \mathcal{R}$ ja $\mathcal{D} = \mathcal{L} \vee \mathcal{R}$, kus alumine ja ülemine raja $\mathcal{R}$ ja $\mathcal{L}$ vahel leitakse hulga S kõigi ekvivalentsiseoste hulgas, mis on järjestatud hulk sisalduvusseose suhtes. Sümbol $\circ$ tähistab binaarsete seoste korrutamist. Saab näidata, et $\mathcal{D} \subseteq \mathcal{J}$. On selge, et $\mathcal{H} \subseteq \mathcal{L} \subseteq \mathcal{D}$ ja $\mathcal{H} \subseteq \mathcal{R} \subseteq \mathcal{D}$.



Näide

Mistahes hulkade A ja X korral on hulk $S = A \times X$ poolrühm korrutamise

$$(a, x)(a', x') := (a, x')$$

suhtes. Vaatleme olukorda, kus $A = \{a, b\}$ ja $X = \{x, y, z\}$. Otsekorrutise $A \times X$ elemendid võib kirjutada üles tabelina

(a, x)	(a, y)	(a, z)
(b, x)	(b, y)	(b, z)

.

On võimalik näidata, et selle tabeli read on poolrühma $A \times X$ $\mathcal{R}$ -klassid ja veerud on $\mathcal{L}$ -klassid. Seega $\mathcal{H}$ -klassid on üheelemendilised ja poolrühmal on üksainus $\mathcal{D}$ -klass, mis koosneb kõigist tema elementidest.

Lause

Seos $\mathcal{R}$ on vasakpoolne kongruents poolrühmal S ja seos $\mathcal{L}$ on parempoolne kongruents poolrühmal S , see tähendab, et iga $a, b, c \in S$ korral

$$a\mathcal{R}b \implies ca\mathcal{R}cb,$$

$$a\mathcal{L}b \implies ac\mathcal{L}bc.$$

Definitsioon

Poolrühma S elementi e nimetatakse **idempotendiks**, kui $e^2 = e$.
Poolrühma S kõigi idempotentide hulka tähistatakse $E(S)$.

Lemma

Kui S on rühm, siis selles leidub täpselt üks idempotent.

Definitsioon

Poolrühma S idempotenti e nimetatakse **primitiivseks**, kui iga $f \in E(S)$ korral:

$$ef = fe = f \Rightarrow e = f.$$

Definitsioon

Lihtsat poolrühma S , mis sisaldab primitiivset idempotenti, nimetatakse **täiesti lihtsaks**.

Lemma

Poolrühma iga minimaalne vasakpoolne (parempoolne) ideaal on selle poolrühma $\mathcal{L}$ -klass ($\mathcal{R}$ -klass).

Lause

Olgu S poolrühm.

- ① Kui L on poolrühma S minimaalne vasakpoolne ideaal, siis $L = Sa$ iga $a \in L$ korral.*
- ② Kui R on poolrühma S minimaalne parempoolne ideaal, siis $R = aS$ iga $a \in R$ korral.*

Lause

Kui S on lihtne poolrühm ja sisaldab minimaalset vasakpoolset ideaali L (minimaalset parempoolset ideaali R), siis S on oma minimaalsete vasakpoolsete (parempoolsete) ideaalide ühend.

Lemma

Olgu S poolrühm, $a, b \in S$ ja $b \mathcal{H} ab$. Tähistame $H := H_b = H_{ab}$. Siis kujutus

$$\lambda_a : H \rightarrow H, \quad x \mapsto ax$$

on bijektiivne.

Lemma

Mittetühi poolrühm S on rühm parajasti siis, kui $aS = S$ ja $Sa = S$ iga $a \in S$ korral.

Lause

Järgmised väited poolrühma S $\mathcal{H}$ -klassi H kohta on samaväärsed.

- ① *Leidub $e^2 = e \in H$.*
- ② *Leiduvad $a, b \in H$ nii, et $ab \in H$.*
- ③ *H on poolrühma S alampoolrühm, mis on rühm.*

Lause

Täiesti lihtsa poolrühma kõik $\mathcal{H}$ -klassid on rühmad.

Lause

Olgu S lihtne poolrühm, mis sisaldab vähemalt ühte minimaalset vasakpoolset ideaali ning vähemalt ühte minimaalset parempoolset ideaali. Siis poolrühma S iga minimaalse vasakpoolse ideaali L ja iga minimaalse parempoolse ideaali R korral kehtivad tingimused:

- ① $LR = S$;
- ② RL on rühm;
- ③ rühma RL ühikelement e on primitiivne idempotent.

Seega S on täiesti lihtne.

Definitsioon

Poolrühma S idempotenti e nimetatakse **primitiivseks**, kui iga $f \in E(S)$ korral:

$$ef = fe = f \Rightarrow e = f.$$

Teoreem

Olgu S lihtne poolrühm. Siis järgmised väited on samaväärsed:

- ① S on täiesti lihtne;*
- ② S on rühmade ühend;*
- ③ S kõik vasakpoolsed ja parempoolsed peaideaalid on minimaalsed;*
- ④ S sisaldab vähemalt ühte minimaalset vasakpoolset ideaali ja vähemalt ühte minimaalset parempoolset ideaali.*

Järeldus

Lõplik poolrühm on täiesti lihtne parajasti siis, kui ta on lihtne.

Definitsioon

Poolrühma S nimetatakse **regulaarseks**, kui

$$(\forall a \in S)(\exists x \in S) a = axa.$$

Kui a ja x on sellised elemendid, et $a = axa$, siis $ax = axax$ ja $xa = xaxa$, mis tähendab, et ax ja xa on idempotendid. Seega regulaarsetes poolrühmades on üldiselt “palju” idempotente.

Näide

1. Kui X on mittetühi hulk, siis tema teisenduste poolrühm $\mathcal{T}(X)$ on regulaarne. Kui $f \in \mathcal{T}(X)$, siis defineerime teisenduse $g \in \mathcal{T}(X)$ nii, et ta viib iga elemendi hulgast $\text{Im}(f)$ mingiks selle elemendi originaaliks f suhtes, ja kõigil teistel X elementidel on g defineeritud suvaliselt. Siis $f = fgf$.
2. Poolrühm $(\text{Mat}_n(K), \cdot)$, kus K on korpus, on regulaarne. Ruutmaatriksi A Moore'i-Penrose'i pöördmaatriks A^+ rahuldab muuhulgas võrdust $AA^+A = A$.

Definitsioon

Poolrühma S elementi a' nimetatakse elemendi a **inversseks elemendiks**, kui $a = aa'a$ ja $a' = a'aa'$.

Lause

Regulaarse poolrühma igal elemendil leidub vähemalt üks inversne element.

Definitsioon

Poolrühma nimetatakse **inversseks**, kui tema igal elemendil leidub täpselt üks inversne element.

Definitsioon

Poolrühma nimetatakse **inversseks**, kui tema igal elemendil leidub täpselt üks inversne element.

Edaspidi tähistame inverse poolrühma elemendi a üheselt määratud inverset elementi sümboliga a' . Definitsioonist järeldub, et $(a')' = a$. Kuna iga idempotent e on iseenda inversne element, siis inversses poolrühmas $e' = e$.

Näide

Iga rühm on inversne poolrühm, kus $a' = a^{-1}$.

Iga inversne poolrühm on regulaarne. Järgmine tulemus ütleb, millised regulaarsed poolrühmad on inverssed.

Teoreem

Regulaarne poolrühm on inversne parajasti siis, kui tema idempotendid kommuteeruvad.

Polügoonid

Polügoonide teema juures eeldame kõikjal, et S on monoid ühikelemendiga 1.

Definitsioon

Hulka A nimetatakse **parempoolseks polügooniks üle monoidi S** ehk **parempoolseks S -polügooniks**, kui on antud kujutus $r: A \times S \rightarrow A$, $(a, s) \mapsto as$, nii, et

① $(as)t = a(st)$,

② $a1 = a$

mistahes $a \in A$ ja $s, t \in S$ korral. Kujutust $r: A \times S \rightarrow A$ nimetatakse ka monoidi S **(parempoolseks) toimeks** hulgal A .

Definitsioon

Alamhulka B nimetatakse polügooni A_S **alampolügooniks**, kui iga $b \in B$ ja $s \in S$ korral $bs \in B$.

Polügoonide näited

Näide

- 1 Olgu $(R, +, \cdot)$ ring. Siis iga parempoolne R -moodul on polügoon üle selle ringi multiplikatiivse monoidi $(R, \cdot)$.
- 2 Olgu S monoid. Siis S on polügoon üle iseenda, kui toime defineerida monoidi S korrutamise abil. Seda polügooni tähistatakse S_S .
- 3 Olgu A mittetühi hulk ja $\mathcal{T}$ selle hulga kõigi teisenduste monoid järjestrakendamise suhtes. Defineerides vasakpoolse toime $\mathcal{T} \times A \longrightarrow A$ võrdusega

$$fa := f(a)$$

$a \in A, f \in \mathcal{T}$, saame vasakpoolse polügooni ${}_{\mathcal{T}}A$.

- 4 Olgu S monoid. Siis S iga parempoolne ideaal on polügooni S_S alampolügoon. Muuhulgas parempoolsed peaideaalid sS , kus $s \in S$, on polügooni S_S alampolügoonid.

Lahutumatud polügoonid

Definitsioon

Polügooni nimetatakse **lahutumatuks**, kui teda ei saa esitada kahe mittetühja lõikumatu alampolügooni ühendina.

Ütleme et polügoon A_S on alamhulga $X \subseteq A$ poolt tekitatud (ehk moodustatud), kui iga element $a \in A$ esitub kujul $a = xs$ mingi $x \in X$ ning $s \in S$ jaoks.

Lause

Olgu A_S ühe elemendi $a \in A$ poolt moodustatud S -polügoon. Siis A_S on lahutumatu.

Näide

Olgu S monoid ning $s \in S$. Siis sS on lahutumatu parempoolne S -polügoon.

Lahutus lahutumatute polügoonide ühendiks

Lemma

Kui C_i , $i \in I$ on parempoolse S -polügooni A_S lahutumatute alampolügoonide pere ning $\bigcap_{i \in I} C_i \neq \emptyset$, on ühend $\bigcup_{i \in I} C_i$ polügooni A_S lahutumatu alampolügoon.

Lause

Iga mittetühi polügoon on esitatav mittetühjade lahutumatute alampolügoonide lõikumatu ühendina.

Kui polügoon A_S avaldub lahutumatute alampolügoonide C_i lõikumatu ühendina

$$A = \bigsqcup_{i \in I} C_i,$$

võime nimetada polügoone C_i polügooni A **lahutumatuteks komponentideks** (või sidususkomponentideks).

Kui polügoon A_S avaldub lahutumatute alampolügoonide C_i lõikumatu ühendina

$$A = \bigsqcup_{i \in I} C_i,$$

võime nimetada polügoone C_i polügooni A **lahutumatuteks komponentideks** (või sidususkomponentideks).

Näide

Kui X on suvaline hulk ja S on monoid, saame hulka $X \times S$ vaadata parempoolse S -polügoonina, defineerides $(x, s) \in X \times S$ ning $t \in S$ jaoks

$$(x, s)t := (x, st).$$

Siis polügooni $X \times S$ lahutumatuteks komponentideks on alampolügoonid $\{(x, s) \mid s \in S\}$, kus $x \in X$, kuna

$$X \times S = \bigsqcup_{x \in X} \{(x, s) \mid s \in S\} = \bigsqcup_{x \in X} \{x\} \times S.$$

Vabad polügoonid

Definitsioon

Polügooni A_S alamhulka X nimetatakse **baasiks**, kui iga $a \in A$ korral leiduvad üheselt määratud $x \in X$ ja $s \in S$ nii, et $a = xs$.

Definitsioon

Polügooni nimetatakse **vabaks**, kui temas leidub baas.

Näide

Kui X on suvaline hulk ja S on monoid, saame hulka $X \times S$ vaadata parempoolse S -polügoonina, defineerides $(x, s) \in X \times S$ ning $t \in S$ jaoks

$$(x, s)t := (x, st).$$

Siis polügoon $X \times S$ on vaba ja selle baasiks on $\{(x, 1) \mid x \in X\}$.

Definitsioon

Polügooni A_S alamhulka X nimetatakse **baasiks**, kui iga $a \in A$ korral leiduvad üheselt määratud $x \in X$ ja $s \in S$ nii, et $a = xs$.

$X \times S$ on parempoolne S -polügoon toimega

$$(x, s)t := (x, st).$$

Siis polügoon $X \times S$ on vaba ja selle baasiks on $\{(x, 1) \mid x \in X\}$.

Lause

Kui A_S on parempoolne S -polügoon ning $X \subseteq A$, siis

① *kujutus*

$$r: X \times S \longrightarrow A, \quad (x, s) \mapsto xs$$

parempoolsete S -polügoonide homomorfism ning

② *kujutus r on bijektiivne (ning seega S -polügoonide isomorfism) parajasti siis, kui X on polügooni A_S baasiks.*

Näide

Kui X on suvaline hulk ja S on monoid, saame hulka $X \times S$ vaadata parempoolse S -polügoonina, defineerides $(x, s) \in X \times S$ ning $t \in S$ jaoks

$$(x, s)t := (x, st).$$

Siis polügoon $X \times S$ on vaba ja selle baasiks on $\{(x, 1) \mid x \in X\}$.

Kujutus

$$r: A \times S \longrightarrow A, \quad (a, s) \mapsto as$$

parempoolsete S -polügoonide homomorfism.

Lause

Iga polügoon on vaba polügooni homomorfne kujutis.

Kui $X \subseteq A$, siis kujutus

$$r: X \times S \longrightarrow A, \quad (x, s) \mapsto xs$$

on bijektiivne (ning seega S -polügoonide isomorfism) parajasti siis, kui X on polügooni A_S baasiks.

Teoreem

Polügooni F_S jaoks on järgmised väited samaväärsed:

- ① *polügoon F_S on vaba,*
- ② *F_S esitub lõikumatu ühendina*

$$F = \bigsqcup_{i \in I} F_i,$$

kus $F_i \cong S_S$ iga $i \in I$ korral.

Projektiivsed polügoonid

Definitsioon

Polügooni P_S nimetatakse **projektiivseks**, kui iga sürjektiivse homomorfismi $\pi : A_S \rightarrow B_S$ ja iga homomorfismi $f : P_S \rightarrow B_S$ korral leidub homomorfism $g : P_S \rightarrow A_S$ nii, et $\pi g = f$, s.t. järgmine diagramm on kommutatiivne:

$$\begin{array}{ccc} & P_S & \\ g \swarrow & & \searrow f \\ A_S & \xrightarrow{\pi} & B_S \end{array}$$

Näide

Tühi polügoon $\emptyset_S$ on projektiivne, sest ainuke homomorfism $\emptyset_S \rightarrow B_S$ on tühi kujutus ja seega ka g ossa sobib tühi kujutus.

Lemma

Kui S on monoid, on kujutus

$$\lambda: S_S \rightarrow \text{End}(S_S, S_S), \quad s \mapsto (t \mapsto st)$$

monoidide isomorfism pöördkujutusega

$$\text{ev}_1: \text{End}(S_S, S_S) \rightarrow S_S, \quad f \mapsto f(1).$$

Lemma

Olgu $r: X \rightarrow Y$ ning $i: Y \rightarrow X$ funktsioonid hulkade X ja Y vahel nii, et $r \circ i = 1_Y$. Siis kehtivad järgmised väited:

- ❶ *kujutus $i: Y \rightarrow X$ on injektiivne,*
- ❷ *$\text{Im}(i) = \text{Im}(i \circ r)$ ning*
- ❸ *kujutus $i \circ r: X \rightarrow X$ on idempotentne (s.t. $(i \circ r) \circ (i \circ r) = i \circ r$).*

Lause

Olgu polügoon P_S oma mittetühjade alampolügoonide P_i , $i \in I$, lõikumatu ühend, s.t. $P_S = \bigsqcup_{i \in I} P_i$. Polügoon P_S on projektiivne parajasti siis, kui iga $i \in I$ korral polügoon P_i on projektiivne.

Lemma

Lahutumatu polügoon P_S on projektiivne parajasti siis, kui leidub idempotent $e \in S$ nii, et $P \cong eS$, kus eS on vaadatud polügooni S_S alampolügoonina.

Teoreem

Polügoon P_S on projektiivne parajasti siis, kui

$$P = \bigsqcup_{i \in I} P_i,$$

kusjuures iga $i \in I$ korral leidub idempotent $e_i \in S$ nii, et $P_i \cong e_i S$.

Lõplikud korpused

Definitsioon

Korpus on kommutatiivne ring, mille nullist erinevad elemendid moodustavad korrutamise suhtes rühma.

Korpuse K ühikelementi tähistame 1 ja nullelementi 0 . Me tähistame ka $K^* := K \setminus \{0\}$ ja ütleme, et $(K^*, \cdot)$ on korpuse K **multiplikatiivne rühm**.

Korpuses K saame $m \in \mathbb{Z}$ ning $a \in K$ korral vaadata elementi kujul

$$ma = \underbrace{a + a + \dots + a}_m, \quad m \text{ liidetavat}$$

Kujutus

$$\mathbb{Z} \longrightarrow K, \quad m \mapsto m1$$

on ringide homomorfism.

Definitsioon

Korpuse L alamringi K nimetatakse **alamkorpuseks**, kui $a^{-1} \in K$ iga $a \in K \setminus \{0\}$ korral.

Olgu p ühikelemendi $1 \in K$ järk aditiivses rühmas $(K, +)$, s.t. vähim selline naturaalarv p , et $p1 = 0$. Siis öeldakse, et korpuse K **karakteristika** on p ja tähistatakse $\text{char}K = p$. Definitsioonist järeldeb, et kui $\text{char}K = p$, siis iga $a \in K$ korral $pa = 0$, sest

$$pa = p(1 \cdot a) = (p1)a = 0a = 0.$$

Lause

Lõpliku korpuse karakteristika on algarv.

Lause

Kui korpuse K karakteristika on p , siis see korpus sisaldab jäägiklassikorpusega $\mathbb{Z}_p$ isomorfset alamkorpust.

Definitsioon

Kui korpus K on korpuse L alamkorpus, siis öeldakse, et korpus L on korpuse K **laiend**.

Lause

Korpuse K iga laiendit L võib vaadelda vektorruumina üle korpuse K . Kui L on lõplik ja $|K| = q$, siis $|L| = q^m$, kus $m \in \mathbb{N}$.

Teoreem

Lõpliku korpuse elementide arv on algarvu aste.

Lemma

Kui korpuse K karakteristika on p , siis iga $a, b \in K$ ja $n \in \mathbb{N}$ korral

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}.$$

Lemma

Kui K on lõplik korpus ning $|K| = q$, siis

- ① *iga $a \in K^*$ korral $a^{q-1} = 1$,*
- ② *iga $a \in K$ korral $a^q = a$.*

Kui $p(x) \in K[x]$ on mingi polünoom üle korpuse K , siis selle polünoomi poolt tekitatud peaideaal

$$p(x)K[x] = \{p(x)h(x) \mid h(x) \in K[x]\}$$

koosneb kõigist polünoomidest ringis $K[x]$, mis jaguvad polünoomiga $p(x)$. Kõrvalklass esindajaga $f(x) \in K[x]$ ideaali $p(x)K[x]$ järgi on hulk

$$[f(x)] = f(x) + p(x)K[x] = \{f(x) + p(x)h(x) \mid h(x) \in K[x]\}.$$

Muuhulgas $[0] = p(x)K[x]$. Saab näidata, et

$$[f(x)] = [g(x)] \iff f(x) - g(x) \in p(x)K[x] \iff p(x) \mid f(x) - g(x).$$

Lause

Olgu K korpus ja $p(x) \in K[x]$ taandumatu polünoom, mille aste $d \geq 2$. Siis faktoring $L = K[x]/p(x)K[x]$ on korpus, mis sisaldab korpusega K isomorfset alamkorpust ning milles polünoomil $p(x)$ on olemas juur. Kui $|K| = p^m$, siis $|L| = p^{md}$.

Lause

Olgu K korpus ja $p(x) \in K[x]$ taandumatu polünoom, mille aste $d \geq 2$. Siis faktoring $L = K[x]/p(x)K[x]$ on korpus, mis sisaldab korpusega K isomorfset alamkorpust ning milles polünoomil $p(x)$ on olemas juur. Kui $|K| = p^m$, siis $|L| = p^{md}$.

Teoreem

Olgu $f(x) \in K[x]$ polünoom kordajatega korpusest K ning olgu $f(x)$ aste $n \geq 1$. Siis leidub korpuse K selline laiend L , milles polünoomil $f(x)$ on n juurt.

Definitsioon

Korpuse K laiendit L nimetatakse polünoomi $f(x) \in K[x]$ **lahutuskorpuseks**, kui $f(x)$ lahutub lineaartegurite korrutiseks üle L ,

$$f(x) = b(x - a_1) \dots (x - a_n),$$

kus $a_1, \dots, a_n, b \in L$, ning korpuse L iga alamkorpuse M korral, mis sisaldab korpust K ja elemente $a_1, \dots, a_n$, kehtib võrdus $M = L$.

Kui K on lõplik, siis ka $f(x)$ lahutuskorpus L on lõplik. Kehtib järgmine teoreem, mida me siinkohal ei tõesta.

Teoreem (tõestuseta)

Polünoomi lahutuskorpus on isomorfismi täpsuseni üheselt määratud.

Teoreem

Iga algarvu p ja naturaalarvu n korral leidub korpus, milles on p^n elementi. See korpus on isomorfismi täpsuseni üheselt määratud.

TÕESTUS.

- Olgu L polünoomi $x^q - x$ lahutuskorpus.
- Olgu $x^q - x = (x - a_1) \dots (x - a_q)$, kus $a_1, \dots, a_q \in L$.
- $x^q - x$ ei oma kordseid juuri, kuna
$$\text{SÜT}((x^q - x), (x^q - x)') = \text{SÜT}((x^q - x), -1) = 1$$
- $K = \{a_1, \dots, a_q\} = \{a \in L \mid a^q = a\} \subseteq L$ on alamkorpus.
- Kuna $\mathbb{Z}_p \subseteq K$, siis $K = L$.
- Ühesus tuleb lahutuskorpuse ühesusest, kuna q elemendilises korpuses L' iga $a \in L'$ korral $a^q = a$.



Võre osaliselt järjestatud hulgana

Definitsioon

Osaliselt järjestatud hulga $(P, \leq)$ elementi c nimetatakse elementide a ja b ülemiseks **tõkkeks**, kui $a \leq c$ ja $b \leq c$. Elementide a ja b **ülemine raja** on nende elementide vähim ülemine tõke. Analoogiliselt saab defineerida alumised tõkked ja alumised rajad. Ülemist raja tähistatakse $a \vee b$ ja alumist raja $a \wedge b$.

Definitsioon

Võre on järjestatud hulk, mille igal kahel elemendil leidub ülemine ja alumine raja.

Võre algebralise struktuurina

Definitsioon

Võre on mittetühi hulk L , millel on defineeritud kaks algebralist tehet $+$ ja $\cdot$ (liitmine ja korrutamine) nii, et mistahes $a, b, c \in L$ korral

$$\begin{array}{ll} (a + b) + c = a + (b + c) & (ab)c = a(bc) \\ a + b = b + a & ab = ba \\ a + a = a & aa = a \\ (a + b)a = a & ab + a = a \end{array}$$

Lause

Olgu $(L, +, \cdot)$ võre algebralise definitsiooni mõttes. Siis mistahes $a, b \in L$ korral

$$a = ab \iff b = a + b.$$

Teoreem

Kui $(L, \leq)$ on võre järjestusteoreetilises mõttes ja defineerime kahekohalised tehted $+$ ja $\cdot$ võrdustega

$$a + b := a \vee b,$$

$$ab := a \wedge b,$$

siis $(L, +, \cdot)$ on võre algebralises mõttes.

Teoreem

Kui $(L, +, \cdot)$ on võre algebralises mõttes ja defineerime seose $\leq$ järgmiselt:

$$a \leq b \iff a = ab,$$

siis $(L, \leq)$ on võre järjestusteoreetilises mõttes. Selles võres

$$a \leq b \implies ac \leq bc \quad \text{ja} \quad a + c \leq b + c \quad (3)$$

mistahes $a, b, c \in L$ korral.

Täielikud võred

Definitsioon

Osaliselt järjestatud hulka L nimetatakse **täielikuks võreks**, kui selle mistahes alamhulgal on olemas nii ülemine kui alumine raja.

Definitsiooni järgi peab leiduma ka tühja alamhulga alumine ja ülemine raja.

Näide

- 1 Kõik lõplikud võred on täielikud.
- 2 Hulga X alamhulkade võre $(\mathcal{P}(X), \cup, \cap)$ on täielik.
- 3 Naturaalarvude hulk $\mathbb{N}$ ja $\mathbb{N}^*$ võtmise suhtes on võre, mis ei ole täielik, sest puudub suurim element.
- 4 Ratsionaalarvude hulk $\mathbb{Q}$ ei ole täielik võre. Kui r on irratsionaalarv, siis hulgal $\{a \in \mathbb{Q} \mid r < a\}$ on lõpmata palju alumisi tõkkeid, aga puudub alumine raja.

Täielikud võred

Lause

Osaliselt järjestatud hulga L korral on järgmised väited samaväärsed.

- ① *L on täielik võre.*
- ② *Hulga L igal alamhulgal on olemas alumine raja.*
- ③ *Hulga L igal mittetühjal alamhulgal on olemas alumine raja ning hulk L sisaldab suurimat elementi.*

Teoreem (Knaster–Tarski teoreem)

Täieliku võre L ja mistahes järjestust säilitava teisenduse $f : L \rightarrow L$ korral leidub element $x_0 \in L$ nii, et $f(x_0) = x_0$.

Modulaarsed võred

Lause

Mistahes võre L ja elementide $a, b, c \in L$ korral

- ① $a + bc \leq (a + b)(a + c);$
- ② *kui $a \leq c$, siis $a + bc \leq (a + b)c$.*

Definitsioon

Võret L nimetatakse **modulaarseks**, kui mistahes $a, b, c \in L$ korral

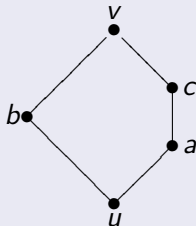
$$a \leq c \implies a + bc = (a + b)c.$$

Näide

Saab näidata, et rühma kõigi normaaljagajate võre tehete $\cdot$ ja $\cap$ suhtes on modulaarne.

Näide

Viieelemendiline võre



ei ole modulaarne. Seda võret tähistatakse sümboliga N_5 .

Lause

Mooduli M_R (R on ring) alammodulite võre $(\text{Sub}(M), +, \cap)$ on modulaarne.

Modulaarsusega samaväärsed tingimused

Teoreem

Võre L jaoks on järgmised väited samaväärsed.

- ① *L on modulaarne.*
- ② *Kui $a, b, c \in L$, $a \geq b$, $a + c = b + c$ ja $ac = bc$, siis $a = b$.*
- ③ *L ei sisalda võrega N_5 isomorfset alamvõret.*

Distributiivsed võred

Definitsioon

Võret L nimetatakse **distributiivseks**, kui mistahes $a, b, c \in L$ korral

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

Lemma

Iga distributiivne võre on modulaarne.

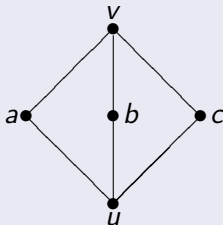
Näide

- 1 Hulga X alamhulkade võre $(\mathcal{P}(X), \cup, \cap)$ on distributiivne.
- 2 Naturaalarvude hulk suurima ühisteguri ja vähima ühiskordse võtmise suhtes on distributiivne võre.
- 3 Ahelad on distributiivsed võred.

Distributiivsed võred

Näide

Võre



ei ole distributiivne. Selle võre tähistuseks on M_3 .

Teoreem (tõestuseta)

Võre L on distributiivne parajasti siis, kui ta ei sisalda võredega N_5 ja M_3 isomorfseid alamvõresid.

Tuletame meelde Ω -algebra definitsiooni.

Definitsioon

Hulka Ω koos tükeldusega

$$\Omega = \bigsqcup_{n=0}^{\infty} \Omega_n$$

alamhulkade Ω_n (mis võivad olla ka tühjad) lõikumatuks ühendiks nimetame **tüübiks** ehk **signatuuriks**. Iga $\omega \in \Omega_n$ korral loeme, et tehtemärgi ω aarsus on n .

Definitsioon

Olgu Ω tüüp ja A hulk. Kui iga arvu $n \in \mathbb{N} \cup \{0\}$ korral vastab igale tehtemärgile $\omega \in \Omega_n$ üks konkreetne n -kohaline algebraline tehe $\omega^A: A^n \rightarrow A$, siis ütleme, et paar $(A, \{\omega^A \mid \omega \in \Omega\})$ on Ω -**algebra**.

Universaalalgebra uurib Ω -algebraid üldkujul.

Nagu me oleme juba näinud, saab Ω -algebrate puhul rääkida homomorfismidest, alamalgebratest, kongruentsidest ja faktoralgebratest. Neid mõisted seob Ω -algebrate homomorfismiteoreem.

Teoreem (Homomorfismiteoreem)

Olgu $f : A \rightarrow B$ homomorfism Ω -algebrate vahel. Siis leidub üksühene homomorfism $g : A / \text{Ker } f \rightarrow B$ nii, et $f = g\pi$, kus $\pi : A \rightarrow A / \text{Ker } f$ on loomulik projektsioon.

Algebras ei uurita tavaliselt ainult hulki koos suvaliste tehetega, vaid nõutakse ka tehetelt teatud võrduste rahuldamist (näiteks $x + y = y + x$ või $xx^{-1} = 1$). Et universaalalgebra kontekstis sellistest võrdustest üldjuhul rääkida, toome sisse *termi* mõiste.

Olgu $\Omega = \bigsqcup_{n=0}^{\infty} \Omega_n$ signatuur ja X hulgaga Ω lõikumatu hulk. Me mõtleme X elementidest kui muutujatest (selles tähenduses nagu muutuja esineb polünoomi definitsioonis), vahel ütleme nende kohta ka “täht”.

Definitsioon

(Ω, X) -**termid** defineeritakse järgmiste kolme tingimuse abil.

- 1 Hulga $\Omega_0 \cup X$ elemendid on 0-astme (Ω, X) -termid.
- 2 Kui $n, m \in \mathbb{N}$, $\omega \in \Omega_n$ ja $t_1, \dots, t_n$ on ülimalt $(m-1)$ -astme (Ω, X) -termid, kusjuures vähemalt üks neist on täpselt $(m-1)$ -astme (Ω, X) -term, siis “sõna” $\omega(t_1, \dots, t_n)$ on m -astme (Ω, X) -term.
- 3 Rohkem (Ω, X) -terme ei ole.

(Ω, X) -termide algebra

Kõikide (Ω, X) -termide hulk $F(X)$ on Ω -algebra, kui defineerida iga $\omega \in \Omega_0$ jaoks

$$\omega^{F(X)} = \omega \in F(X)$$

ning mistahes $\omega \in \Omega_n$, $n \in \mathbb{N}$ ja $t_1, \dots, t_n \in F(X)$ korral võtta

$$\omega^{F(X)}(t_1, \dots, t_n) = \omega(t_1, \dots, t_n) \in F(X).$$

Saadud algebrat **$F(X)$** nimetatakse **termide algebraks** või **absoluutselt vabaks algebraks** baasiga X ja signatuuriga Ω .

Definitsioon

Kui $t = t(x_1, \dots, x_n) \in F(X) = T(\Omega, X)$ ja $\mathbf{A}$ on Ω -algebra, siis n -aarne funktsioon $t^A: A^n \rightarrow A$ defineeritakse järgmiselt:

- 1 kui $t = \omega \in \Omega_0$, siis mistahes $a_1, \dots, a_n \in A$ korral $t^A(a_1, \dots, a_n) = 0_\omega^A$, kus 0_ω^A on nullaarse tehte ω poolt fikseeritud element hulgas A ,
- 2 kui $t = x \in X$, siis $x = x_i$ mingi $i \in \{1, \dots, n\}$ korral, ja mistahes $a_1, \dots, a_n \in A$ jaoks saame võtta funktsiooniks t^A **projektsiooni** i -ndale komponendile, s.t.

$$t^A(a_1, \dots, a_n) = a_i,$$

- 3 kui $t = \omega(t_1, \dots, t_s) \in F(X)$ on m -astme term, s.t. $t_1, \dots, t_s$ on ülimalt $(m-1)$ astme termid ja $\omega \in \Omega_s$, siis mistahes $a_1, \dots, a_n \in A$ korral

$$t^A(a_1, \dots, a_n) = \omega^A(t_1^A(a_1, \dots, a_n), \dots, t_s^A(a_1, \dots, a_n)).$$

Definitsioon

Olgu Ω signatuur ja $u, v \in F(X) = T(\Omega, X)$, kus $X = \{x_1, x_2, \dots\}$ on loenduv hulk. Öeldakse, et Ω -algebral **A** kehtib **samasus** $u = v$, kui termidele u ja v vastavad termfunktsioonid on võrdsed, s.t. $u^A = v^A$.

Formaalselt on samasus termide paar (u, v) , aga sisulise arusaamise lihtsustamiseks kirjutame selle üles kujul $u = v$.

Definitsioon

Ω -algebrate klassi $\mathcal{K}$ nimetatakse **muutkonnaks**, kui leidub selline samasuste hulk S , et klassi $\mathcal{K}$ kuuluvad need ja ainult need algebrad, mis rahuldavad kõiki hulka S kuuluvaid samasusi.

Muutkondadena on kirjeldatavad näiteks ringide klass ning vektorruumide klass, aga mitte korpuste klass.

Miks muutkondadest hoolime?

See, et algebrate klass on muutkond, ehk on esitatav samasuste kaudu, annab meile automaatselt mitmed head omadused. Näiteks, muutkond on kinnine

- 1 alamalgebrate võtmise suhtes,
- 2 faktoralgebrate võtmise suhtes ning
- 3 korrutiste võtmise suhtes.

Tuleb välja, et kehtib ka vastupidine. Iga eelneva kolme operatsiooni suhtes kinnine Ω -algebrate klass on samasuste kaudu kirjeldatav.

Teoreem (Birkhoff)

Mittetriviaalne Ω -algebrate klass on muutkond parajasti siis, kui see on kinnine alamalgebrate, homomorfsete kujutiste ja (mistahes võimsusega) otsekorrutiste võtmise suhtes.

Ω -algebrate ning muutkondade kontekstis saab arendada suurt osa algebrast. Siiski, mõned vaadeldud struktuurid, näiteks täielikud võred, ei ole kenasti kirjeldatavad Ω -algebrate keeles. Üks võimalus on üldistada muutkonna mõiste kategooria mõistele. Idee on järgmine:

- meil on mingi matemaatiliste struktuuride klass (näiteks rühmad või meetrilised ruumid),
- struktuuride klassiga käib kaasa struktuuri säilitava kujutuse mõiste (rühmade homomorfism, kaugust ahendav kujutus).

Tuleb välja, et ainult neid kahte asja teades on võimalik suhteliselt palju teooriat arendada, teadmata midagi konkreetset struktuuride enda kohta .

Kategooria definitsioon

Definitsioon

Kategooria $\mathcal{C}$ koosneb järgmistest komponentidest:

- 1 klass $\mathcal{C}_0$, mille elemente kutsume selle kategooria **objektideks**;
- 2 iga objektipaari (A, B) jaoks on olemas hulk $\mathcal{C}(A, B)$, mille elemente nimetame **morfismideks** objektist A objekti B ;
- 3 iga objektikolmiku (A, B, C) jaoks on olemas kujutus (**komponeerimine** ehk **korrutamine**)

$$\mathcal{C}(A, B) \times \mathcal{C}(B, C) \longrightarrow \mathcal{C}(A, C);$$

paari (f, g) kujutist (morfismide f ja g **kompositsiooni** ehk **korrutist**) tähistame $g \circ f$ või lühidalt gf ;

- 4 iga objekti A jaoks on olemas morfism $1_A \in \mathcal{C}(A, A)$, mida kutsutakse objekti A **ühikmorfismiks**.

Kategooria definitsioon (jätk)

Kategooria andmed peavad lisaks rahuldama järgmisi tingimusi:

Definitsioon

- 1 Kui $(A, B) \neq (A', B')$, siis $\mathcal{C}(A, B) \cap \mathcal{C}(A', B') = \emptyset$.
- 2 **Assotsiatiivsuse aksioom:** mistahes morfismide $f \in \mathcal{C}(A, B)$, $g \in \mathcal{C}(B, C)$, $h \in \mathcal{C}(C, D)$ korral kehtib võrdus

$$h(gf) = (hg)f.$$

- 3 **ühiku aksioom:** mistahes morfismide $f \in \mathcal{C}(A, B)$, $g \in \mathcal{C}(B, C)$ korral kehtivad võrdused $1_B f = f$ ja $g 1_B = g$.

Kui mingi Ω -algebra endomorfismid moodustavad monoidi, siis üldisemalt iga Ω -algebrate klass (näiteks mingi muutkond) moodustab kategooria, mille objektide klassiks on antud algebrate klass ning mille morfismideks on Ω -algebrate homomorfismid.

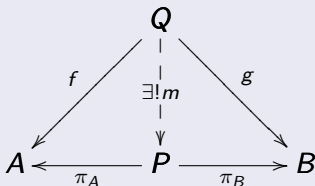
Kategooriate näited

Kui mingite matemaatiliste struktuuride vahel leidub struktuuri säilitava kujutuse mõiste, siis saame neist tavaliselt moodustada kategooria. Vastavat kategooriat tähistatakse tavaliselt kas lühendiga struktuuri nimest või morfismi nimest.

Tähis	objektid	morfismid
Set	hulgad	kujutused
Rel	hulgad	binaarsed seosed hulkade vahel
Mon	monoidid	monoidide homomorfismid
Gr	rühmad	rühmade homomorfismid
Ab	Abeli rühmad	rühmade homomorfismid
Vec_K	vektorruumid üle K	lineaarkujutused
Top	topoloogilised ruumid	pidevad kujutused
Graph	graafid	graafide homomorfismid

Definitsioon

Kategooria $\mathcal{C}$ objektide A, B **korruis** on kolmik (P, π_A, π_B) , kus $P \in \mathcal{C}_0$ ja $\pi_A: P \rightarrow A$, $\pi_B: P \rightarrow B$ on morfismid kategoorias $\mathcal{C}$ (mida nimetatakse **projektsioonideks**), mis rahuldavad tingimust, et kui $Q \in \mathcal{C}_0$ on objekt ja $f: Q \rightarrow A$, $g: Q \rightarrow B$ on morfismid, siis leidub üheselt määratud morfism $m: Q \rightarrow P$ nii, et järgmine diagramm kommuteerub:



Tihti peale kirjutatakse m asemel (f, g) . Üheselt määratud m leidumise omadust kutsutakse tihti korruiste **universaalomaduseks**.

Korrutised hulkade kategoorias

Olgu A ja B objektid kategoorias $\mathbf{Set}$, ehk siis hulgad. Nende objektide korrutis kategoorias $\mathbf{Set}$ on kolmik (P, π_A, π_B) , mida saab illustreerida hulkade ning funktsioonide diagrammiga

$$A \xleftarrow{\pi_A} P \xrightarrow{\pi_B} B.$$

Funktsioonid π_A ning π_B võimaldavad meil igale elemendile $p \in P$ seada vastavusse paari $(a, b) := (\pi_A(p), \pi_B(p)) \in A \times B$. Korrutise universaalomadus väljendab seda, et iga paari $(a, b) \in A \times B$ jaoks leidub unikaalne $p \in P$, mis sellele paarile vastab.

Selle nägemiseks võtame universaalomaduses $Q := \{*\}$ ja esitame suvalise hulga X elemente funktsioonidega $\{*\} \longrightarrow X$.

