DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra
Bakalaura studiju programma "Matemātika"

Studiju kurss

Algebriskās struktūras

1.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

1. Algebriskās operācijas **5**

1.1. Operācijas un algebras 5

1.2. Apakšalgebras 8

1.3. Slēgums 9

1.4. Veidotājelementi 10

1.5. Algebru morfismi un izomorfisms 12

2. Binārās operācijas **13**

2.1. Ievads 13

2.2. Bināro operāciju speciālgadījumi 14

2.3. Grupoīdu elementi ar speciālām īpašībām 19

2.4. Multiplikatīvais un aditīvais pieraksts 21

3. Svarīgāko algebrisko struktūru pārskats **22**

3.1. Asociatīvie grupoīdi 23

3.2. Gredzeni 24

3.3. Moduļi 24

3.4. Režğu tipa struktūras 25

4. 1.mājasdarbs **26**

4.1. Obligātie uzdevumi 26

4.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi 27

Lekcijas mērķis:

- apgūt algebrisko struktūru teorijas pamatjēdzienus.

Lekcijas kopsavilkums:

- vispārinot dažādas matemātiskas aktivitātes var definēt vairāku tipu algebriskas struktūras.

Svarīgākie jēdzieni: n-āra operācija, algebriska struktūra, slēgta kopa, apakšalgebra, slēgums, veidotājsistēma, morfisms, izomorfisms, bināra operācija, asociatīva operācija, komutatīva operācija, vienības elements, invertējams elements, multiplikatīvais pieraksts, aditīvais pieraksts, pusgrupa, monoīds, grupa, gredzens, lauks, modulis, režğis.

Svarīgākie fakti un metodes: slēguma īpašības, asociatīvas operācijas pielietošanas neatkarība no kārtības, vienības elementu un invertējamu elementu īpašības.

1. Algebriskās operācijas

1.1. Operācijas un algebras

Bieži vien kopās, ar kurām nākas sastapties pielietojumos, ir uzdoti pārveidojumi, kas diviem vai vairākiem kopas elementiem piekārto kādu šīs kopas elementu.

1.1. piemērs.

- Kopu operācijas,
- funkciju kompozīcija,
- aritmētiskās operācijas.

Ir lietderīgi pētīt šādus pārveidojumus abstraktā veidā (neatkarīgi no kopu un pārveidojumu dabas), ar to nodarbojas matemātikas nozare - *algebra*.

1.1. piezīme. Termins "algebra" tiek lietots vismaz trijās nozīmēs:

- visa algebrisko struktūru teorija,
- kopa ar operācijām,
- noteikta veida struktūra.

Operācija

A - kopa. Funkciju

$$\mu : A^n \to A,$$
$$(a_1, ..., a_n) \mapsto \mu(a_1, ..., a_n)$$

sauc par n-āru operāciju, kas uzdota kopā A, $n \geq 1$.

Citiem vārdiem - n-āra operācija piekārto n elementus garai sakārtotai A elementu virknei $(a_1, ..., a_n)$ (*operandiem*) kādu kopas elementu $\mu(a_1, ..., a_n)$ (*operācijas rezultātu*).

Speciālgadījumi:

- $n = 1$ - *unāra operācija*,

- $n = 2$ - *bināru operācija,*
- $n = 3$ - *ternāra operācija.*

Par 0-*āru operāciju (konstanti)* kopā A sauc funkciju $\nu : \{\emptyset\} \to A$. Var domāt, ka 0-āra operācija definē vienu A elementu.

Ja ir dota kopa A un tās operāciju kopa $\Sigma = \{\mu_1, ..., \mu_l\}$, kur

$$\mu_i : A^{n_i} \to A,$$

tad pāri (A, Σ) sauc par *algebrisku struktūru* vai *algebru (Σ-algebru)*, kopu $\{n_1, ..., n_l\}$ sauc par tās *tipu* un kopu Σ - par *signatūru.*

Operācijas var uzdot šādos veidos:

- pārskaitot operācijas rezultātus visām operandu iespējām, ja kopa A ir galīga un pietiekoši maza (*Kēli tabulas, operāciju tabulas*),
- uzdodot operāciju ar tās raksturīgo īpašību vai aprēķināšanas procedūru, kā tas ir, piemēram, aritmētisko operāciju gadījumā.

1.2. Apakšalgebras

Dota kopa A, $S \subseteq A$ un n-āra operācija μ.

S sauc par *slēgtu attiecībā uz* μ $\iff$ $\forall$ elementu virknei $(s_1, ..., s_n) \in S^n$ izpildās

$$\mu(s_1, ..., s_n) \in S.$$

Ja ir dota algebra (A, Σ), tad apakškopu S, kas ir slēgta attiecībā uz visām operācijām sauc par Σ-*apakšalgebru* vai vienkārši *apakšalgebru* ($S \leq A$).

1.2. piemērs. Apakšalgebru piemēri:

- $A = \mathbb{R}$ reālie skaitļi ar operācijām $+, \times$. Racionālie skaitļi - apakšalgebra.
- $A = Fun(\mathbb{R}, \mathbb{R})$ (viena reāla argumenta funkcijas), operācijas - saskaitīšana, reizināšana, atvasināšana, apakšalgebras - polinomi, racionālas funkcijas, elementārās funkcijas.

1.3. Slēgums

Ir dota algebra (A, Σ) un tās apakškopa X.

Definēsim

$$\Sigma(X) = X \cup \bigcup_{(a_1,...,a_n)\in X^n, \mu\in\Sigma} \mu(a_1, ..., a_n).$$

Citiem vārdiem sakot, pievienojam kopai X visus iespējamos operāciju rezultātus.

Definēsim arī

$$\Sigma^k(X) = \Sigma(\Sigma^{k-1}(X)),$$
$$\Sigma^0(X) = X.$$

Par apakškopas X *slēgumu attiecībā uz* μ sauc kopas A apakškopu

$$\overline{X} = X \cup \Sigma(X) \cup \Sigma^2(X) \cup ... = \bigcup_{i\geq 0} \Sigma^i(X).$$

Citiem vārdiem sakot, $\overline{X}$ iegūst, vairākkārt pielietojot X elementiem operācijas un pievienojot kopai X visus iegūtos A elementus.

1.3. piemērs. $(\mathbb{Z}, +, \times)$, $S = \{1\}$, $\overline{S} = \mathbb{N}$.

1.1. teorēma. (*slēguma īpašības*)

1. $X \subseteq Y \implies \overline{X} \subseteq \overline{Y}$.
2. $X \subseteq \overline{X}$.
3. $\overline{\overline{X}} = \overline{X}$.
4. $\overline{X} \cup \overline{Y} \subseteq \overline{X \cup Y}$.
5. $\overline{X}$ ir slēgta kopa.

PIERĀDĪJUMS Patstāvīgi.

1.4. Veidotājelementi

Dota algebras (A, Σ) apakškopa $X \subseteq A$. Ja $\overline{X} = A$, tad A sauc par *veidotājsistēmu* un tās elementus par *veidotājelementiem.*

Citiem vārdiem, jebkuru A elementu var iegūt sākot ar kopas X elementiem un vairākkārtīgi pielietojot operācijas.

1.4. piemērs. $(\mathbb{Z}, +)$. $\{1, -1\}$ un $\{1, -1, 2, 3, 4\}$ ir veidotājsistēmas, $\{1\}$, $\mathbb{N}$ nav veidotājsistēmas.

$(\mathbb{Z}_m, +)$. $\{1\}$ un $\{1, 2\}$ ir veidotājsistēmas, $\{2\}$ nav veidotājsistēma vispārīgā gadījumā.

Veidotājsistēmu sauc par *minimālu veidotājsistēmu*, ja nekāda tās īsta apakškopa nav veidotājsistēma.

1.5. piemērs. $(\mathbb{Z}, +)$. $\{1, -1\}$ ir minimāla veidotājsistēma, bet $\{1, -1, 2, 3, 4\}$ nav minimāla veidotājsistēma.

$(\mathbb{Z}_n, +)$. $\{1\}$ ir minimāla veidotājsistēma, bet $\{1, 2\}$ nav minimāla.

1.5. Algebru morfismi un izomorfisms

Kad divas algebras var uzskatīt par vienādām vai līdzīgām (ignorējot kopu un operāciju dabu)?

Ja ir dotas 2 algebras (A, Σ) un (B, T) ar vienādiem tipiem

$$\Sigma = \{\sigma_1, ..., \sigma_l\}, T = \{\tau_1, ..., \tau_l\}$$

tad funkciju $f : A \to B$ sauc par *algebru morfismu*, ja $\forall$ i un $\forall$ A elementu virknei $(a_1, ..., a_{n_i})$ izpildās

$$f(\sigma_i(a_1, ..., a_{n_i})) = \tau_i(f(a_1), ..., f(a_{n_i})).$$

Citiem vārdiem, operāciju un funkcijas aprēķināšanu var mainīt vietām.

Morfismu sauc par *izomorfismu*, ja tas ir bijektīvs.

Ja $\exists$ algebru (A, Σ) un (B, T) izomorfisms $f : A \to B$, tad saka, ka algebras ir izomorfas ($A \simeq B$).

1.6. piemērs. $(\mathbb{Z}, +) \simeq (A, \times)$, kur $A = \{1, a, a^{-1}, a^2, a^{-2}, ...\}$ un $a > 0$, $a \neq 1$.

2. Binārās operācijas

2.1. Ievads

Kopu A ar vienu bināru operāciju $*$ sauc par *grupoīdu* $(A, *)$.

Pieraksta $\mu(a_1, a_2)$ vietā parasti lieto atdalošos simbolus - operācijas zīmes, piemēram $a_1 \circ a_2$, $a_1 \star a_2$ vai vispār nelieto atdalošos simbolus, piemēram, $\mu(a_1, a_2) = a_1 a_2$.

Ja operācijas tiek pielietota vairākas reizes, tad pielietošanas kārtību var viennozīmīgi noteikt izmantojot iekavas un pēctecīgi pielietojot operāciju sākot ar iekšējām iekavām, piemēram:

$$\mu(\mu(x, y), \mu(z, \mu(t, u))) = (x * y) * (z * (t * u)).$$

2.1. piemērs. Bināras operācijas:

- skaitļu aritmētiskās operācijas,
- kopu operācijas,
- virkņu *savienošana* (alfabēts Σ, virkņu kopa Σ^*, ja $u = u_1 ... u_m$ un $v = v_1 ... v_k$, tad *savienojums* $uv = u_1 ... u_m v_1 ... v_k$.)
- vektoru operācijas,
- ģeometrisku pārveidojumu kompozīcija.

2.2. Bināro operāciju speciālgadījumi

Bināro operāciju speciālgadījumi:

- *asociatīva operācija* - $\forall\ a, b, c$ izpildās

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

- *komutatīva operācija* - $\forall\ a, b$ izpildās

$$a * b = b * a;$$

- *idempotenta operācija* - $\forall\ a$ izpildās

$$a * a = a.$$

2.2. piemērs. Asociatīvu, komutatīvu un distributīvu operāciju piemēri - skaitļu saskaitīšana, reizināšana, kopu apvienojums un šķēlums.

Idempotentas operācijas piemērs - kopu šķēlums un kopu apvienojums.

2.3. piemērs. Asociatīvas operācijas neatkarība no iekavām.
$a((bc)d) = (a(bc))d = (((ab)c)d)$.
$(ab)(cd) = (((ab)c)d)$.

2.1. teorēma. Ja bināra operācija ir asociatīva, tad šīs operācijas pielietošanas rezultāts sakārtotai n elementu virknei nav atkarīgs no operācijas pielietošanas kārtības.

PIERĀDĪJUMS (Patstāvīgi) $(A, *)$ - asociatīvs grupoīds.

Pierādījuma ideja - parādīt, ka katru operācijas pielietošanas rezultātu sakārtotai virknei var pārveidot kanoniskā formā izmantojot asociativitāti.

Izmantosim matemātisko indukciju ar argumentu n - elementu virknes garumu.

Indukcijas bāze Ja $n = 1$ vai $n = 2$, tad teorēmas apgalvojums ir acīmredzams - ir ne vairāk kā viena operācija.

Indukcijas solis Pieņemsim, ka teorēmas apgalvojums ir patiess $\forall k < n$: operācijas pielietojums sakārtotai elementu virknei, kuras garums nepārsniedz $n-1$, nav atkarīgs no pielietošanas kārtības (iekavu salikšanas kārtības), apzīmēsim tā rezultātu virknei $(a_1, ..., a_k)$ ar

$$(a_1 * a_2 * ... * a_k).$$

Pierādīsim, ka no pieņēmuma seko, ka operācijas pielietojums sakārtotai elementu virknei, kuras garums ir vienāds ar n, nav atkarīgs no pielietošanas kārtības.

Atdalīsim pēdējo pielietoto operāciju. Operāciju pielietošanas rezultāts ir formā

$$(a_1 * ... * a_i) * (a_{i+1} * ... * a_n),\ \text{kur } i < n.$$

Pietiek pierādīt, ka $\forall i < n$ ir spēkā sakarība

$$(a_1 * ... * a_i) * (a_{i+1} * ... * a_n) = ((...(a_1 * a_2) * ...a_n)$$

(izteiksmi labajā pusē sauc par *kreisi normētu*).

Saskaņā ar indukcijas pieņēmumu, operācijas pielietojums sakārtotai elementu virknei, kuras garums nepārsniedz $n-1$, ir vienāds ar kreisi normēto.

Ja $i = n-1$, tad

$$(a_1 * ... * a_{n-1}) * a_n = \underbrace{(...(a_1 * ...) * a_{n-1})}_{\text{kreisi normēts}} * a_n = \underbrace{((...(a_1 * a_2) * ...a_n)}_{\text{kreisi normēts}}.$$

Ja $i < n-1$, tad saskaņā ar asociativitātes definīciju un indukcijas pieņēmumu

$$(a_1 * ... * a_i) * (a_{i+1} * ... * a_n) = (a_1 * ... * a_i) * \underbrace{(...(a_{i+1} * ...) * a_n)}_{\text{kreisi normēts}} =$$

$$((a_1 * ... * a_i) * (a_{i+1} * ... * a_{n-1})) * a_n = \underbrace{(...(a_1 * ...) * a_{n-1})}_{\text{kreisi normēts}} * a_n =$$

$$\underbrace{(...(a_1 * ...) * a_n)}_{\text{kreisi normēts}},$$

kas bija jāpierāda. ■

2.1. piezīme. Viens no teorēmas pielietojumiem ir tāds, ka pieraksta ekonomijas dēļ asociatīvas operācijas gadījumā nav vajadzības rakstīt iekavas, ja tam nav īpašas nepieciešamības.

2.3. Grupoīdu elementi ar speciālām īpašībām

Grupoīda $(A, *)$ elementu a sauc par *idempotentu*, ja izpildās vienādība $a * a = a$.

Elementu e sauc par grupoīda *vienības elementu (neitrālo elementu, vieninieku)*, ja $\forall\ a \in A$ izpildās vienādība

$$e * a = a * e = a.$$

Ja grupoīdā $\exists$ vienības elements e, tad elementu a sauc par *invertējamu elementu*, ja $\exists\ b \in A$ tāds, ka $a * b = b * a = e$.

2.2. teorēma.

1. Ja grupoīdā eksistē vienības elements, tad tas ir vienīgais vienības elements šajā grupoīdā;
2. ja asociatīva grupoīdā ar vienības elementu elementam a eksistē inversais elements, tad tas ir vienīgais a inversais elements;

PIERĀDĪJUMS. (Sākot ar šo teorēmu pieraksta ekonomijas dēļ nerakstīsim operācijas atdalošo simbolu, ja tas nerada pārpratumus).

1. Pieņemsim pretējo: grupoīdā A ir divi elementi e un e' , kas apmierina vienības elementa īpašību: $\forall a \in A$:

$$ae = ea = a,$$

$$ae' = e'a = a.$$

$a = e \implies ee' = e'e = e.$
$a = e' \implies e'e = ee' = e' \implies e = e'.$

2. Pieņemsim, ka elementam a asociatīvā grupoīdā ar vienības elementu e ir divi inversie elementi b un b'. Saskaņā ar inversā elementa definīciju

$$ab = ba = ab' = b'a = e.$$

Reizinot vienādības $ab = e$ abas puses ar b' no kreisās puses un izmantojot asociativitāti iegūstam

$$b'(ab) = b'e = b = b'.\blacksquare$$

2.4. Multiplikatīvais un aditīvais pieraksts

Strādājot ar binārajām operācijām visbiežāk tiek izmantots viens no diviem pieraksta veidiem -

- *multiplikatīvais pieraksts*,
- *aditīvais pieraksts.*

Multiplikatīvajā pierakstā

- bināro operāciju visbiežāk apzīmē ar $\cdot$, $*$ vai kādu līdzīgu simbolu vai arī vispār neraksta atdalošo simbolu,
- vienības elementu apzīmē e ar vai 1,
- elementa a inverso elementu apzīmē ar a^{-1}.

Aditīvo pierakstu izmanto, ja binārā operācija ir acīmredzami komutatīva (var mainīt vietām operandus), piemēram, skaitļu vai vektoru saskaitīšana, šajā gadījumā ir pieņemts apzīmēt

- bināro operāciju ar simbolu $+$ vai kādu tam līdzīgu simbolu, piemēram, $\bigoplus$,

- vienības elementu (ja tas eksistē) - ar 0,
- elementa a inverso elementu - ar $-a$,
- elementa a pakāpi a^n - ar $na = \underbrace{a + a + ... + a}_{n \text{ reizes}}$.

3. Svarīgāko algebrisko struktūru pārskats

Biežāk pētītās algebriskās struktūras ir radušās skaitļošanas un cita veida matemātisko aktivitāšu vispārināšanas rezultātā:

- *asociatīvie grupoīdi (pusgrupas, monoīdi, grupas)* - funkciju kopu un kompozīcijas operācijas vispārināšana,
- *gredzeni* - skaitļu kopu un aritmētisko operāciju vispārināšana,
- *moduļi* - lineāro telpu un lineāro operāciju vispārināšana,
- *režģi* - kopu un kopu operāciju vispārināšana.

3.1. Asociatīvie grupoīdi

Algebras ar vienu asociatīvu bināru operāciju ir saistītas ar funkciju kompozīcijas vispārināšanu.

Pusgrupa - grupoīds ar asociatīvu bināru operāciju.

Monoīds - grupoīds ar asociatīvu bināru operāciju, kas satur vienības elementu.

Grupa - grupoīds ar asociatīvu bināru operāciju, kas

- satur vienības elementu,
- kurā katrs elements ir invertējams.

3.1. piemērs. Pusgrupas - $(\mathbb{N}, +)$, $(\mathbb{R}, \times)$.
Monoīdi - $(Fun(X, X), \circ)$.
Grupas - $(\mathbb{Z}, +)$, $(\mathcal{U}_m, \times)$, $(\Sigma_n, \circ)$.

3.2. Gredzeni

Gredzena struktūra:

- divas bināras asociatīvas operācijas "reizināšana" un "saskaitīšana",
- "saskaitīšana" ir komutatīva,
- ir spēkā distributīvā īpašība.

Gredzeni ir skaitļu kopu vispārinājumi.

Svarīgs speciālgadījums - lauki.

3.3. Moduļi

R - gredzens. *R-modulis* $(M, +, \cdot)$:

- $(M, +)$ - komutatīva grupa,
- $\cdot : R \times M \longrightarrow M$ (*R darbība*) apmierina aksiomas:
  1. $r(m + m') = rm + rm'$,

2. $(r + r')m = rm + r'm$,
3. $(rr')m = r(r'm)$,
4. $1 \cdot m = m$.

Moduļi vispārina lineārās telpas, kurās R ir lauks un R darbība ir reizināšana ar lauka elementu.

3.4. Režğu tipa struktūras

Režğis - $(L, \bigvee, \bigwedge)$, kas apmierina šādas aksiomas:

- $\bigvee$ un $\bigwedge$ ir komutatīvas, asociatīvas un idempotentas,
- $a \bigvee (a \bigwedge b) = a$, $a \bigwedge (a \bigvee b) = a$ (absorpcijas likumi).

Režgu tipa struktūras

- vispārina kopu šķēlumu un apvienojumu,
- vispārina matemātiskās loģikas operācijas (konjunkciju un disjunkciju),

4. 1.mājasdarbs

4.1. Obligātie uzdevumi

1.1 Atrast minimālas veidotājsistēmas šādām algebrām:

(a) $(\mathbb{Z}/5\mathbb{Z}, +)$

(b) $(\mathbb{Z}/12\mathbb{Z}, \times)$,

1.2 Definēsim *Pauli matricas:*

$p_1 = \left[\begin{array}{c|c} 0 & 1 \\ \hline 1 & 0 \end{array}\right]$, $p_2 = \left[\begin{array}{c|c} 0 & -i \\ \hline i & 0 \end{array}\right]$, $p_3 = \left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & -1 \end{array}\right]$, kur $i^2 = -1$.

Atrast kopas $\{p_1, p_2, p_3\}$ slēgumu attiecībā uz matricu reizināšanas operāciju.

1.3 Atrodiet piemērus šādām operācijām:

(a) nav ne komutatīva, ne asociatīva,

(b) nav komutatīva, bet ir asociatīva,

(c) kopa bezgalīga, operācija ir asociatīva, eksistē vienības elements, neviens cits elements nav invertējams.

1.4 Apskatīsim grupoīdu $(\mathbb{Z}, \diamond)$, kur $\mathbb{Z}$ ir veselo skaitļu kopa un operācija $\diamond$ ir definēta ar formulu

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

Pierādīt, ka $(\mathbb{Z}, \diamond)$ ir komutatīvs monoīds. Kāds elements ir vienības elements? Atrast visus idempotentos un invertējamos elementus.

1.5 Noteikt, vai dotās funkcijas ir algebrisko struktūru morfismi.

(a) $A = (\mathbb{Z}, +)$, $f : A \to A$, $f(x) = x + 1$.

(b) $A = (\mathbb{R}[X], +, \cdot)$, $B = (\mathbb{R}, +, \cdot)$, $f : A \to B$, $f(p) = p(0)$.

4.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

1.6 Pierādīt teorēmu par slēguma īpašībām.

1.7 Pierādīt, ka katrā galīgā pusgrupā eksistē idempotents elements.