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

Studiju kurss

Algebriskās struktūras

1.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Algebriskās operācijas

1.1. Pamatdefinīcijas

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*.

Ja ir dota kopa A, tad 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 kopas elementu virknei $(a_1, ..., a_n)$ (*operandiem*) kādu kopas elementu $\mu(a_1, ..., a_n)$ (*operācijas rezultātu*).

Ja $n = 1$, tad operāciju sauc par *unāru*. Ja $n = 2$, tad operāciju sauc par *bināru*, ja $n = 3$, tad par *ternāru*.

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

Bināru operāciju gadījumā ir pieņemts pieraksta $\mu(a_1, a_2)$ vietā lietot atdalošos simbolus - operācijas zīmes, piemēram $a_1 \circ a_2$, $a_1 \star a_2$ vai vispār nelietot 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:

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

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 (universālu algebru, Σ-algebru)*, kopu $\{n_1, ..., n_l\}$ sauc par tās *tipu* un kopu Σ - par *signatūru*.

1.2. Operāciju uzdošanas veidi

Operācijas var uzdot šādos veidos:

- Pārskaitot operācijas rezultātus visām operandu iespējām, ja kopa A ir galīga un satur pietiekoši maz elementu, lai šī procedūra būtu realizējama.

  Šajā gadījumā ir lietderīgi apkopot operācijas pielietošanas rezultātus tabulas (bināru operāciju gadījumā: *Kēli tabulas, reizināšanas tabulas*) veidā, kas bināru operāciju gadījumā atgādina skaitļu reizināšanas tabulu: tabulas rindas un kolonnas tiek indeksētas ar kopas A elementiem, tabulas rūtiņā, kas atbilst elementa a rindai un elementa b kolonnai tiek ierakstīts elements $a * b$.

- Uzdodot operāciju ar tās raksturīgo īpašību vai aprēķināšanas procedūru, kā tas ir, piemēram, aritmētisko operāciju gadījumā.

- Programmēšanā operācija parasti tiek uzdota ar apakšprogrammu.

1.3. Apakšalgebras

Ir dota kopa A, tās apakškopa $S \subseteq A$ un n-āra operācija μ.

Apakškopu S sauc par *slēgtu attiecībā uz* μ, tad un tikai tad, ja katrai n-elementus garai S elementu virknei $(s_1, ..., s_n)$ izpildās nosacījums

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

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

1.2. piemērs. Apakšalgebru piemēri:

- $A = \mathbb{R}$ reālie skaitļi ar operācijām $+, \times$. Racionālie skaitļi - apakšalgebra.
- M - kopa, $A = P(M)$, operācijas - šķēlums, apvienojums, papildinājums, jebkura apakškopa $P(X)$, kur $X \subseteq M$, ir apakšalgebra.

- $A = Fun(\mathbb{R}, \mathbb{R})$ (viena argumenta funkcijas ar definīcijas apgabalu $\mathbb{R}$), operācijas - saskaitīšana, reizināšana, atvasināšana, apakšalgebras - polinomi, racionālas funkcijas, elementārās funkcijas.

Ir dota kopa A, tās apakškopa X un n-āra operācija μ. Definēsim

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

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 operāciju μ un pievienojot kopai X visus iegūtos A elementus.

1.3. piemērs. $(\mathbb{Z}, +\times)$, $S = \{2\}$, $\overline{S} = \mathbb{Z}$.

1.1. teorēma. (*slēguma īpašības*)

1. Ja $X \subseteq Y$, tad $\overline{X} \subseteq \overline{Y}$.
2. $X \subseteq \overline{X}$.
3. $\overline{\overline{X}} = \overline{X}$.
4. $\overline{X} \cup \overline{Y} \subseteq \overline{X \cup Y}$.

PIERĀDĪJUMS Patstāvīgi.

1.4. Veidotājelementi

Ir dota algebra (A, Σ). Tās apakškopu $X \subseteq A$ sauc par *veidotājsistēmu* un tās elementus par *veidotājelementiem* tad un tikai tad, ja $\overline{X} = A$. Citiem vārdiem, jebkuru kopas A elementu var iegūt sākot ar kopas X elementiem un vairākkārtīgi pielietojot algebras Σ operācijas.

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

Apskatīsim algebru $(\mathbb{Z}_n, +)$, redzam, ka kopas $\{1\}$ un $\{1, 2\}$ ir veidotājsistēmas, kopa $\{2\}$ nav veidotājsistēma.

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

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

Apskatīsim algebru $(\mathbb{Z}_n, +)$, redzam, ka kopa $\{1\}$ ir minimāla veidotāsistēma, 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* tad un tikai tad, ja katram indeksam i un katrai sakārtotai kopas A elementu virknei $(a_1, ..., a_{n_i})$ izpildās nosacījums

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

citiem vārdiem:

- funkcija f respektē operāciju tabulas,
- operāciju un funkcijas aprēķināšanu var mainīt vietām.

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

Ja eksistē algebru (A, Σ) un (B, T) izomorfizms $f : A \to B$, tad saka, ka algebras ir izomorfas un pieraksta šo faktu veidā $A \simeq B$.

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 binaru operāciju $*$ sauc par *grupoīdu* (apzīmē ar pierakstu $(A, *)$).

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.

2.1. piezīme. Datorzinātnē un datortehnoloģijās izmanto 3 veidu pierakstus, lai uzdotu binaru operācijas:

- *prefiksa pieraksts*- $\mu(a_1, a_2) = *a_1a_2$,
- *infiksa pieraksts*- $\mu(a_1, a_2) = a_1 * a_2$,
- *postfiksa pieraksts* - $\mu(a_1, a_2) = a_1a_2*$.

2.2. Bināro operāciju speciālgadījumi

Definēsim šādus speciālgadījumus:

- *asociatīva operācija* - visiem a, b, c izpildās
$$(a * b) * c = a * (b * c);$$
- *komutatīva operācija* - visiem a, b izpildās
$$a * b = b * a;$$
- *kreisi distributīva operācija* - visiem a, b, c izpildās
$$a * (b \circ c) = (a * b) \circ (b * c);$$

- *labēji distributīva operācija* - visiem a, b, c izpildās
$$(a \circ b) * c = (a * c) \circ (b * c);$$
- *idempotenta operācija* - visiem 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.

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

PIERĀDĪJUMS Pieņemsim, ka ir dots grupoīds $(A, *)$. Izmantosim matemātisko indukciju ar argumentu n - elementu virknes garumu.

Indukcijas bāze Ja $n = 1$ vai $n = 2$, tad teorēmas apgalvojums ir acīmredzams.

Indukcijas solis Pieņemsim, ka teorēmas apgalvojums ir patiess $\forall k < n$, tas nozīmē, ka 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

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

Apskatot pēdējo pielietoto operāciju, redzam, ka 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*).

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. ■

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

Ja $(A, *)$ ir asociatīvs grupoīds, tad operācijas $*$ pielietošanu virknei $\underbrace{(a, ..., a)}_{n \text{ reizes}}$ sauc par a n-to pakāpi un apzīmē ar pierakstu a^n (*multip-*

likatīvajā pierakstā).

2.2. teorēma. Ja $(A, *)$ ir asociatīvs grupoīds, tad ir spēkā vienādības

1. $a^n * a^m = a^{n+m}$;
2. $(a^n)^m = a^{nm}$.

2.3. piemērs. Skaitļu saskaitīšana un reizināšana, vektoru saskaitīšana, funkciju kompozīcija, vārdu savienošana - asociatīvas operācijas.

Skaitļu dalīšana un atņemšana - neasociatīvas operācijas.

2.3. piezīme. Asociativitātes jēdziena svarīgums ir saistīts ar to, ka funkciju kompozīcija un kopu pamatoperācijas - apvienojums un šķēlums ir asociatīvas operācijas.

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 *kreiso vienības elementu (kreiso vieninieku)*, ja $\forall a \in A$ izpildās vienādība $e * a = a$.

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

Elementu sauc par grupoīda vienības elementu (vieninieku), ja tas ir kreisais un labais vienības elements.

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

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

Ja grupoīdā eksistē vienības elements e, tad elementu a sauc par *invertējamu elementu*, ja tas ir gan labēji, gan kreisi invertējams.

2.3. teorēma.

1. Ja grupoīdā eksistē vienības elements, tad tas ir vienīgais vienības elements šajā grupoīdā;
2. ja asociatīvā grupoīdā ar vienības elementu elementam a eksistē gan kreisais, gan labais inversais elements, tad elementam tie ir vienādi;
3. ja asociatīva grupoīdā ar vienības elementu elementam a eksistē inversais elements, tad tas ir vienīgais a inversais elements;
4. ja asociatīvā grupoīdā ar vienības elementu e elementi a un b ir invertējami, tad elements $a * b$ arī ir invertējams un
$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

5. ja grupoīdā ar vienības elementu e elements a ir invertējams, arī a^{-1} ir invertējams un
$$(a^{-1})^{-1} = a.$$

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: $\forall a \in A$:
$$ae = ea = a,$$
$$ae' = e'a = a.$$
Ņemot $a = e$, iegūsim
$$ee' = e'e = e.$$
Ņemot $a = e'$, iegūsim
$$e'e = ee' = e'.$$

Redzam, ka $e = e'$.

2) Pieņemsim, ka $La = e$ un $aR = e$. Redzam, ka

$$LaR = (La)R = eR = R.$$

No otras puses

$$LaR = L(aR) = Le = L,$$

tātad $L = R$.

3) 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

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

4) Pārbaudīsim, ka $b^{-1}a^{-1}$ ir inversais elements attiecībā uz elementu ab:

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e.$$

5) Pārbaudīsim, ka a ir inversais elements attiecībā uz elementu a^{-1}:

$$a^{-1}a = e.$$

■

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

3.1. Asociatīvie grupoīdi

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

Grupoīdu ar asociatīvu bināru operāciju sauc par *pusgrupu*.

Grupoīdu ar asociatīvu bināru operāciju, kas satur vienības elementu, sauc par *monoīdu*.

Grupoīdu ar asociatīvu bināru operāciju, kas

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

sauc par *grupu*.

3.1. piemērs. Pusgrupas - $(\mathbb{N}, +)$, $(\mathbb{R}, \times)$.

Monoīdi - $(Fun(X, X), \circ)$.

Grupas - $(Bij(X, X), \circ)$, kur $Bij(X, X) \subseteq Fun(X, X)$ ir visu bijektīvu funkciju apakškopa, kuru definīcijas un vērtību apgabals ir kopa X.

3.2. Gredzenu tipa struktūras

Gredzena tipa struktūras:

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

Gredzena tipa struktūras ir skaitļu kopu vispārinājums.

Svarīgs speciālgadījums - lauki.

3.3. Režğu tipa struktūras

Režğu tipa struktūras:

- divas vai vairāk bināras asociatīvas un komutatīvas operācijas,
- ir spēkā distributīvās īpašības,
- katrs elements ir idempotents.

Režgu tipa struktūras vispārina kopu šķēlumu un apvienojumu.

4. 1.mājasdarbs

1. Atrast minimālas veidotājsistēmas šādām algebrām:
   (a) $(\mathbb{Z}/5\mathbb{Z}, +)$
   (b) $(\mathbb{Z}/12\mathbb{Z}, \times)$,
   (c) $(\mathbb{R}[X], \times)$.
2. Atrodiet piemērus šādām operācijām:
   (a) nav ne komutatīva, ne asociatīva,
   (b) nav komutatīva, bet ir asociatīva.
3. 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 invertējamos elementus.