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

Studiju kurss

Algebriskās struktūras

2.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Grupu teorijas pamati

1.1. Pamatfakti un piemēri

1.1.1. Motivācija

Risinot matemātikas uzdevumus, bieži parādās invertējami pārveidojumi (ģeometriskie pārveidojumi, simetrijas pārveidojumi, bijektīvas funkcijas u.c.) ar dabiski definētu operāciju (ģeometrisko pārveidojumu vai funkciju kompozīcija).

Nereti šie pārveidojumi saglabā kādus invariantus (ģeometrisko figūru rotācijas, kas saglabā figūras).

Parasti eksistē arī vienības elements (pārveidojums, kas neko nemaina, rotācija par 0, vienības funkcija).

Sākotnējās pārveidojumu kopas dabiski ir slēgt attiecībā uz operāciju un pievienot inversos elementus - tiek iegūta kopa, kas ir slēgta attiecībā un operāciju un invertēšanu. Šādas slēgtas kopas - *grupas*, ir ērtāk pētīt.

Matemātiska objekta pārveidojumu grupu, kas saglabā noteiktus invariantus, var uzskatīt par *simetrijas mēru*.

1.1.2. Definīcijas

Grupa ir kopa G ar šādu struktūru:

- kopā G ir uzdota asociatīva bināra operācija,
- attiecībā uz doto bināro operāciju eksistē vienības elements e, kas katram $g \in G$ apmierina nosacījumu
$$ge = eg = g,$$
- katram kopas $g \in G$ eksistē inversais elements g^{-1}, kas apmierina nosacījumu
$$gg^{-1} = g^{-1}g = e.$$

1.1. piezīme. Grupu var definēt arī kā algebrisku struktūru ar 3 operācijām:

- bināra asociatīva operācija,
- unāra operācija - inversā elementa atrašana,
- 0-āra operācija - vienības elementa definēšana.

Grupu G sauc par *komutatīvu grupu* vai *Ābela grupu*, ja visiem $a, b \in G$ izpildās vienādība

$$ab = ba.$$

Vispārīgos gadījumos grupu teorijā parasti izmanto multiplikatīvo pierakstu. Ja grupa ir komutatīva (piemēram, $\mathbb{Z}$), tad tiek izmantots aditīvais pieraksts.

Ja $|G| < \infty$, tad G sauc par *galīgu grupu*, pretējā gadījumā grupa ir *bezgalīga*.

Ja eksistē $n \in \mathbb{N}$ tāds, ka $g^n = e$, tad g sauc par *elementu ar galīgu kārtu*, pretējā gadījumā - par *elementu ar bezgalīgu kārtu*.

Ja g ir elements ar galīgu kārtu, tad mazāko $k \in \mathbb{N}$, kuram $g^k = e$, sauc par g *kārtu*.

1.1.3. Piemēri

1.1. piemērs. Jebkuras kopas X bijektīvo funkciju sevī (permutāciju) kopa ar funkciju kompozīcijas operāciju - $Bij(X, X)$. Ja $X_n = \{1, 2, ..., n\}$, tad apzīmēsim $Bij(X_n, X_n)$ ar Σ_n.

- vienības elements - vienības permutācija, visi X elementi fiksēti,
- elementa inversais elements - inversā permutācija.

Ģeometrisku figūru pārveidojumu (paššaglabājošu rotāciju, u.c.) kopas ar pārveidojumu kompozīcijas operāciju - taisne ar centru, taisnstūris, trijstūri (neregulārs, vienādsānu, regulārs).

- vienības elements - vienības pārveidojums, visi figūras punkti fiksēti,

- elementa inversais elements - inversais (pretējais) pārveidojums.

Veselo skaitļu kopa $\mathbb{Z}$ ar saskaitīšanas operāciju - $(\mathbb{Z}, +)$. Atlikumu kopa mod m ar atlikumu saskaitīšanas operāciju - $(\mathbb{Z}/m\mathbb{Z}, +)$. Citas skaitļu kopas ar saskaitīšanas operāciju.

- vienības elements - 0,
- elementa a inversais elements - $-a$.

Nenulles reālo skaitļu kopa $\mathbb{R}\backslash\{0\}$ ar reizināšanas operāciju - $(\mathbb{R}\backslash\{0\}, \times)$. Invertējamu atlikumu kopa mod m ar atlikumu reizināšanas operāciju - $(U_m, \times)$. Citas skaitļu kopas ar reizināšanas operāciju.

- vienības elements - 1,
- elementa a inversais elements - a^{-1}.

Vektori ar vektoru saskaitīšanas operāciju. Lineāras telpas elementi ar saskaitīšanas operāciju.

- vienības elements - nulles vektors vai elements $\overrightarrow{0}$,

- elementa $\overrightarrow{a}$ inversais elements - $-\overrightarrow{a}$.

$n \times m$-matricas ar elementiem gredzenā R ar matricu saskaitīšanas operāciju - $\mathcal{M}at(n, m, R)$.

- vienības elements - nulles matrica O,
- elementa M inversais elements - $-M$.

Invertējamas $n \times n$-matricas (kvadrātveida matricas) ar koeficientiem laukā k ar matricu reizināšanas operāciju - $GL(n, k)$ (*vispārējā lineārā grupa, general linear group*). Matrica $A \in \mathcal{M}at(n, n, k)$ ir invertējama tad un tikai tad, ja $\det(A) \neq 0$.

- vienības elements - vienības matrica E_n,
- elementa A inversais elements - inversā matrica A^{-1}.

Invertējamas $n \times n$-matricas ar koeficientiem laukā k, kuru determinants ir vienāds ar 1, ar matricu reizināšanas operāciju - $SL(n, k)$ (*speciālā lineārā grupa, special linear group*). Determinanta multiplikatīvā īpašība nodrošina grupas aksiomas:

- $\det(A) = det(B) = 1 \implies det(AB) = 1.$
- $\det(A) = 1 \implies \det(A^{-1}) = 1.$
- $\det(E_n) = 1.$

Grupu G sauc par ciklisku grupu, ja eksistē $g \in G$ tāds, ka $\forall a \in G$ $\exists n \in \mathbb{Z}$ izpildās nosacījums $a = g^n$.

1.1.4. Pamatīpašības

1.1. teorēma. Jebkurā grupā izpildās šādi nosacījumi:

1. $(ab)^{-1} = b^{-1}a^{-1}$.
2. Ja $ac = bc$, tad $a = b$.
3. Ja $ca = cb$, tad $a = b$.
4. $(a^{-1})^{-1} = a$.
5. Vienādojumi $ax = b$ un $xa = b$ ir viennozīmīgi atrisināms attiecībā uz x visiem a un b.

6. Vienības elements ir noteikts viennozīmīgi.
7. Katram elementam inversais elements ir noteikts viennozīmigi.

PIERĀDĪJUMS 1. Redzam, ka

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

2. Reizināsim vienādības $ac = bc$ abas puses ar c^{-1} no labās puses:

$$\begin{aligned}(ac)c^{-1} = (bc)c^{-1} &\Longrightarrow \\ a(cc^{-1}) = b(cc^{-1}) &\Longrightarrow \\ a = b&.\end{aligned}$$

3. Reizināsim vienādības $ca = cb$ abas puses ar c^{-1} no kreisās puses:

$$\begin{aligned}c^{-1}(ca) = c^{-1}(cb) &\Longrightarrow \\ (c^{-1}c)a = (c^{-1}c)b &\Longrightarrow \\ a = b&.\end{aligned}$$

4. $aa^{-1} = a^{-1}a = e$, tātad a ir inversais elements attiecībā uz a^{-1}.

5. Reizināsim vienādības $ax = b$ abas puses ar a^{-1} no kreisās puses:

$$
\begin{aligned}
a^{-1}(ax) = a^{-1}b &\Longrightarrow \\
(a^{-1}a)x = a^{-1}b &\Longrightarrow \\
x = a^{-1}b&.
\end{aligned}
$$

Reizināsim vienādības $xa = b$ abas puses ar a^{-1} no labās puses:

$$
\begin{aligned}
(xa)a^{-1} = ba^{-1} &\Longrightarrow \\
x(aa^{-1}) = ba^{-1} &\Longrightarrow \\
x = ba^{-1}&.
\end{aligned}
$$

6., 7. seko no iepriekšējas teorēmas. ■

1.2. Apakšgrupas

Ja G ir grupa, tad tās apakškopu H sauc par *apakšgrupu*($H \leq G$), ja

- ja $h_1, h_2 \in H$, tad $h_1 h_2 \in H$ (H ir slēgta attiecībā uz bināro operāciju),
- ja $h \in H$, tad $h^{-1} \in H$ (H ir slēgta attiecībā uz inverso elementu aprēķināšanu),
- $e \in H$.

Par apakšgrupu ir jādomā kā par "mazāku" grupu, kas atrodas "lielākā" grupā G.

1.2. piemērs. Katrai grupai G eksistē divas neīstas apakšgrupas: $\{e\}$ un G.

$$2\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}.$$

1.2. teorēma. (*apakšgrupu tranzitivitātes īpašība*) Ja $K \leq H$ un $H \leq G$, tad $K \leq G$.

1.3. teorēma. G - grupa. Ja $H_1 \leq G$, $H_2 \leq G$, tad

$$H_1 \cap H_2 \leq G$$

(apakšgrupu šķēlums ir apakšgrupa).

PIERĀDĪJUMS Pirmkārt, $e \in H_i$, tātad $e \in H_1 \cap H_2$.

Pieņemsim, ka $h \in H_1 \cap H_2$. Tad $h \in H_i$ un $h^{-1} \in H_i$, tātad $h^{-1} \in H_1 \cap H_2$.

Pieņemsim, ka $h, h' \in H_1$ un $h, h' \in H_2$. Tad $hh' \in H_i$ un tādējādi $hh' \in H_1 \cap H_2$.

1.3. piemērs. $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z} \leq \mathbb{Z}$.

1.4. teorēma. G - grupa, $H_1 \leq G$, $H_2 \leq G$.

$$H_1 \cup H_2 \leq G \iff H_1 \leq H_2 \text{ vai } H_2 \leq H_1$$

(Apakšgrupu apvienojums ir apakšgrupa tad un tikai tad, ja viena no tām ir apakšgrupa otrā).

PIERĀDĪJUMS Pieņemsim pretējo - $H_1 \not\subseteq H_2$ un $H_2 \not\subseteq H_1$. Tātad $\exists a \in H_2 \backslash H_1$ un $\exists b \in H_1 \backslash H_2$.

Apskatīsim elementu ab. Ja $H_1 \cup H_2 \leq G$, tad $ab \in H_1$ vai $ab \in H_2$.

Pieņemsim, ka $ab \in H_1$, tas ir, $ab = h_1 \in H_1$. Tad

$$a = h_1 b^{-1}.$$

Labajā pusē ir elements no kopas H_1, kreisajā - elements no kopas $H_2 \backslash H_1$ - pretruna.

Gadījums, kad $ab \in H_2$ tiek analizēts līdzīgi. Tiek iegūta pretruna.
■

1.3. Grupu morfismi un izomorfisms

Dotas grupas G_1 un G_2. Funkciju $f : G_1 \to G_2$ sauc par *grupu homomorfismu*, ja $\forall g, g' \in G_i$ izpildās

$$f(gg') = f(g)f(g').$$

Par grupu homomorfisma $f : G_1 \to G_2$ *attēlu* $Im(f)$ sauc atbilstošās funkcijas attēlu:

$$Im(f) = \bigcup_{a \in G_1} f(a).$$

Par grupu homomorfisma $f : G_1 \to G_2$ *kodolu* $Ker(f)$ sauc maksimālo G_1 apakškopu, kuras katra elementa attēls ir vienības elements:

$$Ker(f) = \bigcup_{a \in G_1, f(a) = e_{G_2}} a = \{a \in G_1 | f(a) = e_{G_2}\}.$$

Grupu homomorfismu sauc par *grupu izomorfismu*, jas tas ir bijektīvs. Grupu $(G_1, *)$ un $(G_2, \circ)$ izomorfismu apzīmēsim ar pierakstiem $G_1 \simeq G_2$ vai $(G_1, *) \simeq (G_2, \circ)$.

Izomorfismi saglabā operācijas struktūru (reizināšanas tabulu).

1.4. piemērs. $\forall G$ vienības funkcija ir izomorfisms. $\forall G_1, G_2$ funkcija $f : G_1 \to G_2$, $f(g) = e_{G_2}$ ir grupu homomorfisms.

1.5. teorēma.

1. Grupu izomorfisma inversā funkcija ir grupu izomorfisms.
2. Ja $f : G_1 \to G_2$ ir grupu homomorfisms, tad $f(e_{G_1}) = e_{G_2}$.
3. Ja $f : G_1 \to G_2$ ir grupu homomorfisms, tad $f(a^{-1}) = f(a)^{-1}$.
4. Grupu homomorfisma attēls un kodols ir apakšgrupas.

PIERĀDĪJUMS

1. Pieņemsim, ka $f : G_1 \to G_2$ ir bijektīvs grupu homomorfisms ar inverso funkciju $f^{-1} : G_2 \to G_1$.

Pieņemsim, ka $f(a) = b$, $f(a') = b'$ (seko, ka $f^{-1}(b) = a$ un $f^{-1}(b') = a'$).

Redzam, ka

$$f^{-1}(bb') = f^{-1}(f(a)f(a')) = f^{-1}(f(aa')) =$$
$$(f^{-1} \circ f)(aa') = id_{G_1}(aa') = aa' = f^{-1}(b)f^{-1}(b')$$

2. Tā kā $e_{G_1}e_{G_1} = e_{G_1}$, tad

$$f(e_{G_1}e_{G_1}) = f(e_{G_1})f(e_{G_1}) = f(e_{G_1}).$$

Reizinot abas puses ar $f(e_{G_1})^{-1}$, iegūsim, ka $f(e_{G_1}) = e_{G_2}$.

3. Tā kā $aa^{-1} = e_{G_1}$, tad

$$f(aa^{-1}) = f(a)\underbrace{f(a^{-1})}_{=f(a)^{-1}} = f(e_{G_1}) = e_{G_2}.$$

■

4. Ja $b = f(a)$ un $b' = f(a')$, tad

$$bb' = f(a)f(a') = f(aa'),$$

$$b^{-1} = f(a^{-1}).$$

Seko, ka $Im(f) \leq G_2$.

Ja $f(a) = f(a') = e_{G_2}$, tad

$$f(aa') = e_{G_2}e_{G_2} = e_{G_2},$$

$$f(a^{-1}) = f(a)^{-1} = e_{G_2}^{-1} = e_{G_2}.$$

Seko, ka $Ker(f) \leq G_1$. ■

2. 2.mājasdarbs

1. X - kopa, $P(X)$ - X apakškopu kopa. Pierādīt, ka $(P(X), \Delta)$ ir komutatīva grupa (Δ - kopu simetriskās starpības operācija). Atrast vienības elementu un katra elementa inverso elementu.
2. Atrast Kēli tabulu kvadrāta rotāciju grupai.
3. Definēsim grupas elementu a, b komutatoru $[a, b]$ ar vienādību

$$[a, b] = aba^{-1}b^{-1}.$$

   Pierādīt, ka

   (a) $[a, b]^{-1} = [b, a]$,

   (b) $[ab, c] = a[b, c]a^{-1}[a, c]$.

4. G - grupa, $t \in G$ - fiksēts elements. Definēsim kopā G jaunu bināru operāciju $\bullet$:

$$a \bullet b = atb.$$

   Pierādīt, ka $(G, \bullet)$ ir grupa un $(G, \bullet) \simeq G$.