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

Studiju kurss

Algebriskās struktūras

2.lekcija

Docētājs: Dr. P. Daugulis

2010./2011.studiju gads

Saturs

Lekcijas mērķis:

- apgūt grupu teorijas pamatjēdzienus.

Lekcijas kopsavilkums:

- grupas gadījumā var konkretizēt un attīstīt agrāk apskatītos vispārīgās algebras jēdzienus.
- bieži izmantotās matemātiskās struktūrās var saskatīt grupas.

Svarīgākie jēdzieni: grupa, komutatīva grupa, grupas elementa kārta, apakškopas slēgums grupā, grupas grafs, ģeometrisko pārveidojumu grupa, permutāciju grupa, matricu aditīvās un multiplikatīvās grupas, cikliskā grupa, brīvā grupa, apakšgrupa, cikliskā apakšgrupa, centrs, komutatoru apakšgrupa.

Svarīgākie fakti un metodes: grupas pamatīpašības, apakšgrupu tranzitivitāte, apakšgrupu šķēluma ir apakšgrupa, apakšgrupu apvienojuma īpašība.

1. Grupu teorijas pamati

1.1. Ievads

1.1.1. Motivācija

Risinot matemātikas uzdevumus, bieži parādās invertējami pārveidojumi, piemēram,

- invertējamas aritmētiskas operācijas tādas kā saskaitīšana,
- lineāru vienādojumu sistēmu elementārie pārveidojumi,
- ğeometriskie pārveidojumi,
- simetrijas pārveidojumi,
- bijektīvas funkcijas u.c.

ar dabiski definētu bināru operāciju (ğeometrisko pārveidojumu vai funkciju kompozīcija u.c.).

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

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

Vēsturiski grupas jēdziens sākotnēji tika izdalīts veicot pētījumus

- veselo skaitļu teorijā (L.Eilers, K.Gauss, grupas $(\mathbb{Z}/m\mathbb{Z}, +)$),
- algebrisko vienādojumu teorijā (N.Ābels, E.Galuā, permutāciju grupas) un
- ģeometrijā (F.Kleins, ģeometrisko pārveidojumu grupas).

1.1.2. Definīcijas

Grupa ir kopa G ar šādu algebrisku struktūru:

- dota asociatīva bināra operācija:

$$(a, b) \mapsto ab,$$

- $\exists$ vienības elements e, kas $\forall\ g \in G$ apmierina nosacījumu

$$ge = eg = g,$$

- $\forall\ g \in G\ \exists$ inversais elements g^{-1}:

$$gg^{-1} = g^{-1}g = e.$$

Grupu G sauc par *komutatīvu grupu* vai *Ābela grupu*, ja operācija ir komutatīva: $\forall\ a, b \in G$ izpildās vienādība

$$ab = ba.$$

Vispārīgos gadījumos grupu teorijā parasti izmanto multiplikatīvo pierakstu. Tādējādi par grupas operāciju var domāt kā par nekomutatīvu reizināšanu.

Ja grupa ir acīmredzami komutatīva (piemēram, $(\mathbb{Z}, +)$), tad biežāk tiek izmantots aditīvais pieraksts. Izņēmums - skaitļu reizināšana.

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

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

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

$A \in G$, $B \in G$, $x \in G$. Definēsim

$$AB = \{g \in G | g = ab,\ \text{kur } a \in A, b \in B\},$$
$$Ax = \{g | g = ax,\ \text{kur } a \in A\},$$
$$xA = \{g | g = xa,\ \text{kur } a \in A\},$$
$$A^{-1} = \{g \in G | g = a^{-1},\ \text{kur } a \in A\}.$$

1.1.3. Veidotājsistēmas

Grupas gadījumā var konkretizēt apakškopas slēguma operāciju, veidotājsistēmas jēdzienu. Grupu teorijā X slēgumu apzīmē kā $\langle X \rangle$.

$\langle X \rangle$ elementi ir *vārdi* formā

$$x_1^{\epsilon_1} \ldots x_n^{\epsilon_n}, \text{ kur } x_i \in X, \epsilon_i \in \mathbb{Z}.$$

1.1. piemērs. $(\mathbb{Z}, +)$, $X = \{1\}$, $\langle X \rangle = \mathbb{Z}$.
$Y = \{2\}$, $\langle Y \rangle = 2\mathbb{Z}$.

$G = (\mathbb{Z}, +), X = \{a, b\}$. $\langle X \rangle = \langle LKD(a, b) \rangle$.

1.2. piemērs. G ir veidotājsistēma attiecībā uz G.
$(\mathbb{Z}, +)$. $\{1, -1\}$ nav minimāla veidotājsistēma, bet $\{1\}$ ir minimāla veidotājsistēma.

1.1.4. Grupas grafs

Ja ir dota grupas veidotājsistēma, tad grupas struktūru var vizualizēt ar *Kēli grafa (grupas grafa)* palīdzību:

- virsotnes - grupas elementi,
- orientētas šķautnes ar indeksiem (krāsām) - reizināšana ar veidotājsistēmas elementiem.

1.3. piemērs. $(\mathbb{Z}, +)$, $(\mathbb{Z}/m\mathbb{Z}, +)$.

1.1.5. Pamatīpašības

1.1. teorēma. Jebkurā grupā izpildās šādas vienādības:

1. $(ab)^{-1} = b^{-1}a^{-1}$.
2. $ac = bc \implies a = b$.
3. $ca = cb \implies a = b$.
4. $(a^{-1})^{-1} = a$.

5. Vienādojumi $ax = b$ un $xa = b$ ir viennozīmīgi atrisināmi attiecībā uz $x \ \forall \ a, b$.
6. Vienības elements ir noteikts viennozīmīgi.
7. Katram elementam inversais elements ir noteikts viennozīmīgi.

PIERĀDĪJUMS 1. Redzam, ka

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

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

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

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

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

4. $aa^{-1} = a^{-1}a = e \implies a = (a^{-1})^{-1}$.

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

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

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

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

6., 7. seko no iepriekšējas lekcijas teorēmas. ■

1.2. Klasiskie piemēri

Grupas ir visuresošas - tā ir visizplatītākā un visvairāk pētītā algebriskā struktūra.

1.2.1. Pārveidojumu, permutāciju grupas

Kopas X permutāciju (bijektīvu funkciju $X \to X$) kopa ar funkciju kompozīcijas operāciju - $(\Sigma_X, \circ)$. Ja $X = \{1, 2, ..., n\}$, tad apzīmēsim Σ_X ar Σ_n.

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

Ģeometrisku figūru pārveidojumu (paššaglabājošu rotāciju, u.c.) kopas ar pārveidojumu kompozīcijas operāciju.

- vienības elements - vienības pārveidojums, visi punkti fiksēti,
- elementa inversais elements - inversais (pretējais) pārveidojums.

Bieži ğeometrisko figūru pārveidojumu grupas var interpretēt kā permutāciju grupas, jo pietiek apskatīt dažu izdalītu figūru punktu vai apakškopu pārveidojumus, piemēram, virsotnes, šķautņu viduspunktus, šķautnes u.c.

1.4. piemērs. Taisne ar centru, taisnstūris, trijstūri (neregulārs, vienādsānu, regulārs). Rubika kuba grupa.

1.2.2. Skaitļu aditīvās grupas

$(\mathbb{Z},+)$, $(\mathbb{Z}/m\mathbb{Z},+)$. Citas skaitļu kopas ar saskaitīšanas operāciju. Tiek izmantots aditīvais pieraksts.

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

1.2.3. Skaitļu multiplikatīvās grupas

$(\mathbb{R}\backslash\{0\},\times)$, $(\mathcal{U}_m,\times)$. Citas skaitļu kopas formā $k\backslash\{0\}$, kur k - lauks, ar reizināšanas operāciju. Tiek izmantots multiplikatīvais pieraksts.

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

1.5. piemērs. *Riņķa grupa* $U = \{z \in \mathbb{C} | |z| = 1\}$ ar reizināšanas operāciju.

1.2.4. Vektoru grupas

Vektori ar vektoru saskaitīšanas operāciju. Lineāras telpas elementi ar saskaitīšanas operāciju. Tiek izmantots aditīvais pieraksts.

- vienības elements - nulles vektors vai elements $\overrightarrow{0}$,
- elementa $\overrightarrow{a}$ inversais elements - $-\overrightarrow{a}$.

1.2.5. Matricu aditīvās grupas

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

- vienības elements - nulles matrica $\mathbf{O}$,
- elementa $\mathbf{M}$ inversais elements - $-\mathbf{M}$.

1.2.6. Matricu multiplikatīvās grupas

Invertējamas $n \times n$-matricas ar elementiem laukā k ar matricu reizināšanas operāciju - $GL(n, k)$ (*vispārējā lineārā grupa, general linear group*). Tiek izmantos multiplikatīvais pieraksts.

Matrica $\mathbf{A} \in \mathcal{M}at(n, n, k)$ ir invertējama $\iff \det(\mathbf{A}) \neq 0$.

- $\det(\mathbf{A}) \neq 0$, $\det(\mathbf{B}) \neq 0 \implies \det(\mathbf{AB}) = \det(\mathbf{A})\det(\mathbf{B}) \neq 0$.
- vienības elements - vienības matrica $\mathbf{E}_n$,
- elementa $\mathbf{A}$ inversais elements - inversā matrica $\mathbf{A}^{-1}$.

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 aksiomu izpildi:

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

1.2.7. Cikliskās grupas

Grupu G sauc par *ciklisku grupu*, ja $\exists\ g \in G$ (*grupas ğenerators*): $\forall a \in G\ \exists n \in \mathbb{Z}:\ a = g^n$. Šādā gadījumā $G = \langle g \rangle$.

1.6. piemērs. $(\mathbb{Z}, +)$, $(\mathbb{Z}_m, +)$, $G = \langle 1 \rangle$.
$(\mathcal{U}_p, \times)$, $\mathcal{U}_p = \langle g \rangle$, kur g - primitīvā sakne.

1.2.8. Brīvās grupas

Dota kopa X. Definēsim grupu, kuras elementus interpretēsim kā X elementu formālo pakāpju reizinājumus.

Definēsim X^{-1}, kuras elementi ir X elementu formālie inversie elementi: $\forall x \in X\ \exists\ x^{-1} \in X^{-1}$.

Definēsim (papildus) vienības elementa simbolu $e \notin X \cup X^{-1}$.

Apskatīsim visas iespējamās virknes alfabētā $X \cup X^{-1} \cup \{e\}$ un vienkāršosim jeb *reducēsim* tās saskaņā ar šādiem likumiem:

- simbolu e vienmēr var izdzēst (kā "vienības elementu"),
- simbolu pārus xx^{-1} un $x^{-1}x$, $\forall\, x \in X$, var pārvērst par e,
- $x^u x^v$ var pārvērst par x^{u+v}.

Pārveidojot visas virknes saskaņā ar šiem likumiem, iegūsim *reducētos vārdus* formā

$$x_1^{k_1} x_2^{k_2} ... x_n^{k_n},$$

kur $k_i \in \mathbb{Z}$, $x_i \in X \cup X^{-1}$, $x_i \neq x_{i+1}$. Definēsim e arī kā reducētu vārdu.

Definēsim kopu $\mathbb{F}\langle X \rangle$, kuras elementi ir visi reducētie vārdi.

1.7. piemērs. $X = \{a, b, c\}$. Reducēts vārdi - $abcb^{-1}a^2$. Nereducēts vārds - $ab^2b^{-2}c$.

Par divu vārdu $a_1 ... a_m$ un $b_1 ... b_l$ savienojumu sauksim vārdu

$$a_1 ... a_m b_1 ... a_l.$$

Ja ir dots divu vārdu savienojums, tad dabiski ir vēlēties to reducēt. Pieņemsim, ka ir doti vārdi $x = x_1^{k_1} ... x_m^{k_m}$ un $y = y_1^{r_1} ... y_l^{r_l}$. Apzīmēsim to savienojuma redukciju ar $red(x, y)$.

Definēsim bināru operāciju kopā $\mathbb{F}\langle X \rangle$:

$$xy = red(x, y).$$

1.2. teorēma. $\mathbb{F}\langle X \rangle$ ar definēto operāciju ir grupa.

PIERĀDĪJUMS
Vienības elements e ir vienības elements.

Inversais elements $(x_1^{k_1} ... x_m^{k_m})^{-1} = x_m^{-k_m} x_{m-1}^{-k_{m-1}} ... x_1^{-k_m}$.

Asociativitāte Patstāvīgs darbs. ■

$\mathbb{F}\langle X \rangle$ sauc par *brīvo grupu ar ģenerējošo kopu* X.

Ja $|X| = n$, tad $\mathbb{F}\langle X \rangle$ apzīmē ar $\mathbb{F}_n$.

1.1. piezīme. Brīvās grupas Kēli grafs ir koks - nav ciklu.

1.2.9. Klasiskie pielietojumi

Grupu teoriju izmanto

- gredzenu un lauku teorijā (gredzenā ir uzdota komutatīvas grupas struktūra, raksturo skaitļu, atlikumu un no tiem atvasinātu gredzenu struktūru),
- kriptogrāfijā (izmanto gredzenus),
- Eiklīda ģeometrijā (kā simetrijas mēru, ģeometrisko transformāciju grupas),
- topoloģisko telpu teorijā (homotopiju grupas, homoloģiju/kohomoloģiju grupas, raksturo "mezglotu" telpu struktūru)
- diferenciālvienādojumu teorijā (diferenciālo operāciju simetriju grupas u.c.),
- fizikā (daudz pielietojumu, dažādu struktūru simetriju grupas),
- ķīmijā (kristālu, molekulu, ķīmisko reakciju grafu simetriju grupas u.c.)
- mūzikā (kvintu cikliskā grupa, dažādu muzikālu struktūru simetriju grupas).

1.3. Apakšgrupas

1.3.1. Definīcija

G- grupa, $H \subseteq G$. H sauc par *apakšgrupu* ($H \leq G$), ja

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

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

1.8. piemērs. $\forall$ G $\exists$ divas *neīstas apakšgrupas:* $\{e\}$ un G.

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

1.3. teorēma. $H \leq G \iff \begin{cases} H^2 = H \\ H^{-1} = H. \end{cases}$

PIERĀDĪJUMS

$\underline{\Longrightarrow}$

$$H \leq G \implies \left(h \in H \iff h^{-1} \in H\right) \implies \boxed{H = H^{-1}}.$$

$$H \leq G \implies \left(\begin{cases} h \in H \\ h' \in H \end{cases} \implies hh' \in H\right) \implies \boxed{H^2 \subseteq H}.$$

$$\begin{cases} H^2 \subseteq H \\ H = H^{-1} \end{cases} \implies e \in H \implies \boxed{H = He \subseteq H^2}$$
$$\implies H^2 = H.$$

$\underline{\Leftarrow}$

$$\begin{cases} H^2 = H \\ H = H^{-1} \end{cases} \implies \begin{cases} h, h' \in H \implies hh' \in H \\ h \in H \implies h^{-1} \in H \\ e \in H \end{cases} \qquad \blacksquare$$

1.3.2. Operācijas ar apakšgrupām

Iekļaušana

1.4. teorēma. (*tranzitivitāte*) $K \leq H$ un $H \leq G \implies K \leq G$.

Šķēlums

1.5. teorēma. G - grupa. $H_1 \leq G$, $H_2 \leq G \implies H_1 \cap H_2 \leq G$ (apakšgrupu šķēlums ir apakšgrupa)

PIERĀDĪJUMS
Neitrālais elements $e \in H_i \implies e \in H_1 \cap H_2$.

$h \in H_1 \cap H_2 \implies h \in H_i,\ h^{-1} \in H_i \implies h^{-1} \in H_1 \cap H_2$.

$h, h' \in H_i \implies hh' \in H_i \implies hh' \in H_1 \cap H_2$.

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

Apvienojums

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

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

(apakšgrupu apvienojums ir apakšgrupa $\iff$ viena no tām ir apakškopa otrā).

PIERĀDĪJUMS $\Leftarrow$ acīmredzami, jo tad $H_1 \cup H_2 = H_i$.

$\implies$ Pieņemsim pretējo -

$$\begin{cases} H_1 \not\subseteq H_2 \\ H_2 \not\subseteq H_1 \end{cases} \implies \begin{cases} H_1 \backslash H_2 \neq \emptyset \\ H_2 \backslash H_1 \neq \emptyset. \end{cases} \implies \begin{cases} \exists a \in H_1 \backslash H_2 \\ \exists b \in H_2 \backslash H_1. \end{cases}$$

Apskatīsim elementu ab. $H_1 \cup H_2 \leq G \implies ab \in H_1$ vai $ab \in H_2$.

Pieņemsim, ka $ab \in H_1$, tas ir, $ab = h_1 \in H_1 \implies b = a^{-1}h_1$ $\implies b \in H_1$ - pretruna.

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

1.3.3. Klasiskas apakšgrupas

Cikliskās apakšgrupas

$\forall\, a \in G$ apakšgrupu $\langle a \rangle = \{g | g = a^n\}$ sauc par *ciklisku apakšgrupu ar ğeneratoru* a.

Centrs

Definēsim *centru* $\mathcal{Z}(G) = \{g | gx = xg, \forall\, x \in G\}$. Var pierādīt, ka $\mathcal{Z}(G) \leq G$.

Komutatoru apakšgrupa

Kā "mērīt" novirzi no komutativitātes?

- Elementi ab un ba var būt dažādi.
- Var pieņemt par nekomutativitātes mēru elementu

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

to sauc par a un b *komutatoru*. Citiem vārdiem sakot, $[a, b]$ ir "koriğējošais reizinātājs", lai mainītu vietām a un b:

$$ab = [a, b]ba.$$

- Apzīmēsim visu komutatoru kopu ar C.
- Definēsim *komutatoru apakšgrupu* $G' = \langle C \rangle$.

1.10. piemērs. G - komutatīva grupa $\implies G' = \{e\}$, $\mathcal{Z}(G) = G$.

2. 2.mājasdarbs

2.1. Obligātie uzdevumi

2.1 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.

2.2 Grupā G $\forall$ $g \in G$ izpildās nosacījums $g^2 = e$. Pierādīt, ka G ir komutatīva grupa.

2.3 G ir taisnstūra (ne kvadrāta) rotāciju grupai.

(a) Aizpildīt G operācijas tabulu.
(b) Atrast vismaz vienu G minimālu veidotājsistēmu $\mathcal{V}$.
(c) Uzzīmēt G Kēli grafu attiecībā uz $\mathcal{V}$.

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

2.5 G - grupa. Pierādīt, ka $\mathcal{Z}(G) \leq G$.

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

2.6 G - galīga grupa, $S \subseteq G$. Izpildās šāda īpašība: $a, b \in S \implies ab \in S$. Pierādīt, ka $S \leq G$.

2.7 Atrast minimālas veidotājsistēmas grupām $(\Sigma_n, \circ)$, $\forall\, n$.