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

Studiju kurss

Algebriskās struktūras

3.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Daži svarīgi izomorfismi

1.1. Kēli teorēma

1.1. teorēma. Ja $f : G \to H$ ir injektīvs grupu homomorfisms, tad

$$G \simeq Im(f).$$

PIERĀDĪJUMS f ir grupu homomorfisms, kas sirjektīvi attēlo G uz $Im(f)$. Tā kā f ir injektīva funkcija, tad tā ir bijektīva funkcija no G uz $Im(f) \leq H$.

1.2. teorēma. (*Kēli (Cayley) teorēma*) Katra grupa ir izomorfa kādai permutāciju grupai.

PIERĀDĪJUMS Pieņemsim, ka ir dota grupa G. Apskatīsim

$$Bij(G, G)$$

- kopas G permutāciju kopu.

Atradīsim injektīvu grupu homomorfismu $f : G \to Bij(G, G)$. Saskaņā ar iepriekšējo teorēmu tas nozīmēs, ka $G \simeq Im(f)$.

Pierādīsim, ka katram $g \in G$ funkcija

$$f_g : G \to G,$$
$$f_g(a) = ga$$

ir kopas G permutācija:

- $\forall b \in G$ izpildās $b = g(g^{-1}b) = f_g(g^{-1}b)$, tāpēc f_g ir sirjektīva funkcija;
- ja $ga_1 = ga_2$, tad $g^{-1}ga_1 = g^{-1}ga_2$ un tāpēc $a_1 = a_2$, seko, ka f_g ir injektīva funkcija.

Definēsim funkciju

$$\varphi : G \to Bij(G, G),$$
$$\varphi(g) = f_g.$$

Pierādīsim, ka φ ir injektīvs grupu homomorfisms.

Homomorfisms Redzam, ka

$$\varphi(g_1 g_2)(a) = f_{g_1 g_2}(a) = g_1 g_2 a = f_{g_1}(f_{g_2}(a)) = (f_{g_1} \circ f_{g_2})(a) = (\varphi(g_1) \circ \varphi(g_2)(a).$$

Injektivitāte Ja $\varphi(g_1) = \varphi(g_2)$, tad $\forall a \in G$ izpildās

$$\varphi(g_1)(a) = g_1 a = \varphi(g_2)(a) = g_2 a.$$

Tas nozīmē, ka $g_1 = g_2$ ■

1.1. piezīme. No Kēli teorēmas seko, ka ja G ir galīga grupa, tad $G \simeq H \leq \Sigma_n$.

1.2. Ciklisko grupu izomorfisma tipu klasifikācija

Ja grupa G ir cikliska grupa ar ģeneratoru g, tad apzīmēsim to ar $G = \langle g \rangle$.

Katram $g \in G$ ar $\langle g \rangle$ apzīmēsim arī apakšgrupu, kuru ģenerē g: $\{a \in G | a = g^n\}$.

1.3. teorēma. Ja G ir grupa un $g \in G$, tad ir spēkā šādi apgalvojumi:

1. ja eksistē dažādi $n, m \in \mathbb{Z}$, kuriem
$$g^n = g^m,$$
tad g ir galīgas kārtas elements;
2. ja g ir galīgas kārtas elements ar kārtu k, tad
$$g^l = e \iff l \equiv 0(\text{mod k});$$
3. ja g ir galīgas kārtas elements ar kārtu k, tad
$$g^{l_1} = g^{l_2} \iff l_1 \equiv l_2(\text{mod k});$$

4. ja g ir galīgas kārtas elements ar kārtu k un $m|k$, tad elementam g^m kārta ir vienāda ar $\frac{k}{m}$;
5. ja g ir bezgalīgas kārtas elements, tad visi elementi g^n ir dažādi.

PIERĀDĪJUMS

1. Ja $g^n = g^m$, tad $g^{n-m} = g^{m-m} = e$ un g kārta nav lielāka kā $n - m$.

2. Ja $l|k$, tad $l = qk$ un

$$g^l = g^{qk} = (g^k)^q = e^q = e.$$

Pieņemsim, ka $g^l = e$. Izdalīsim l ar k:

$$l = qk + r,$$

kur $0 \leq r < k$. Redzam, ka

$$g^l = g^{qk+r} = g^{qk}g^r = (g^k)^q g^r = g^r = e,$$

tāpēc $r = 0$.

3. Izmantojam dalīšanu ar atlikumu līdzīgi kā iepriekšējā punktā.

4. Pieņemsm, ka $k = qm$. Redzam, ka

$$(g^m)^q = g^{qm} = g^k = e.$$

Ja $(g^m)^l = e$, tad $ml \equiv 0(\text{mod k})$. Ja $0 \neq l < q$, tad $0 \neq ml < k$ - pretruna.

5. Seko no 1.

■

1.4. teorēma.

1. Ja g ir galīgas kārtas elements ar kārtu k, tad

$$\langle g \rangle = \{e = g^0, g, g^2, ..., g^{k-1}\}.$$

2. Ja g ir bezgalīgas kārtas elements, tad

$$\langle g \rangle = \{e = g^0, g^{\pm 1}, g^{\pm 2}, ..., \}.$$

1.1. piemērs. Fermā un Eilera teorēmas var interpretēt grupu teorijas terminos - kopā U_m multiplikatīvas grupas elementu kārtas dala $\varphi(m)$.

1.5. teorēma. Ja $G = \langle g \rangle$ ir bezgalīga cikliska grupa, tad

$$G \simeq \mathbb{Z}.$$

PIERĀDĪJUMS Definēsim funkciju

$$f : \mathbb{Z} \to G,$$
$$f(n) = g^n.$$

Pierādīsim, ka f ir bijektīvs grupu homomorfisms.

Sirjektivitāte Tā kā G ir cikliska grupa, tad $\forall a \in G \; \exists m \in \mathbb{Z}$ tāds, ka $a = g^m$.

Injektivitāte Ja $f(n_1) = f(n_2)$, tad $g^{n_1} = g^{n_2}$. Pieņemsim, ka $n_1 > n_2$, tad

$$g^{n_1} g^{-n_2} = g^{n_1 - n_2} = g^{n_2} g^{-n_2} = e.$$

Seko, ka g nevar būt visas bezgalīgās grupas ģenerators.

Homomorfisms $f(n_1 + n_2) = g^{n_1+n_2} = g^{n_1} g^{n_2} = f(n_1) f(n_1)$ ■

1.6. teorēma. Ja $G = \langle g \rangle$ ir galīga cikliska grupa ar k elementiem, tad

$$G \simeq \mathbb{Z}/k\mathbb{Z}.$$

PIERĀDĪJUMS Definēsim funkciju

$$f : \mathbb{Z}/k\mathbb{Z} \to G,$$
$$f(n) = g^n.$$

Pierādīsim, ka f ir bijektīvs grupu homomorfisms.

Sirjektivitāte Tā kā G ir cikliska grupa, tad $\forall a \in G\ \exists m \in \mathbb{Z}$ tāds, ka $a = g^m$.

Injektivitāte Ja $f(n_1) = f(n_2)$, tad $g^{n_1} = g^{n_2}$. Seko, ka

$$g^{n_1} g^{-n_2} = g^{n_1 - n_2} = g^{n_2} g^{-n_2} = e$$

Seko, ka $n_1 \equiv n_2 (\text{mod k})$, tātad $n_1 = n_2$.

Homomorfisms $f(n_1 + n_2) = g^{n_1 + n_2} = g^{n_1} g^{n_2} = f(n_1) f(n_1)$ ■

2. Grupu veidotājsistēmas

2.1. Veidotājsistēmas

Grupās var definēt apakškopas slēgumu - visus iespējamos reizinājumus, kas satur apakškopas elementus un to inversos elementus.

Ja $S \subseteq G$, tad slēgumu $\overline{S}$ grupu teorijā pieņemts apzīmēt ar $\langle S \rangle$.

Var domāt, ka $\langle S \rangle$ elementi ir *vārdi* formā

$$s_1^{\epsilon_1} s_2^{\epsilon_2} ... s_n^{\epsilon_n},$$

kur $s_i \in S$ un $\epsilon_i \in \mathbb{Z}$.

2.1. piemērs. Ja $G = (\mathbb{Z}, +)$ un $S = \{a, b\}$, tad $\langle S \rangle = \langle LKD(a, b) \rangle$.

2.1. teorēma. Ja $\emptyset \neq S \subseteq G$, tad

1. $S \subseteq \langle S \rangle \leq G$,
2. ja $S \subseteq H$, tad $\langle S \rangle \leq H$,
3. $$\langle S \rangle = \bigcap_{S \subseteq H} H.$$

PIERĀDĪJUMS

1. Seko no $\langle S \rangle$ definīcijas.

2. Ja $H \supseteq S$, tad H satur visus S elementus, to inversos un visus iespējamos reizinājumus, tāpēc $\langle S \rangle \leq H$.

3. No iepriekšējā apgalvojums seko, ka
$$\langle S \rangle \leq \bigcap_{S \subseteq H} H.$$

Tā kā $\langle S \rangle$ ir apakšgrupa, kas satur S, tad

$$\bigcap_{S \subseteq H} H = \langle S \rangle \cap \bigcap_{S \subseteq H \neq \langle S \rangle} H \leq \langle S \rangle.$$

■

2.2. Grupu grafi

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

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

Grupas grafā ir spēkā šādas interpretācijas:

- pāreja no orientēta maršruta pirmās virsotnes uz pēdējo - pirmajai virsotnei atbilstošā elementa reizināšana ar maršrutam atbilstošo vārdu vai elementu,

- maršturu pēctecīga apiešana - atbilstošo elementu reizināšana,
- noslēgts orientēts maršruts - identitāte $g_1^{\epsilon_1} g_2^{\epsilon_2} .. g_n^{\epsilon_n} = e$,
- grafa stingrā (abpusējā) sakarība - vienādojuma $ax = b$ atrisināmība.

2.2. piemērs. Cikliskās grupas, trijstūri, četrstūri.

3. Kongruences un blakusklases

3.1. Kongruence

3.1. piemērs. Atcerēsimies kongruences veselo skaitļu un polinomu teorijā:

$$a \equiv b(\text{mod m}) \iff a - b = mq \in m\mathbb{Z},$$
$$f(X) \equiv g(X)(\text{mod m(X)}) \iff f(X) - g(X) = m(X)q(X) \in I.$$

Šie jēdzieni attiecas uz komutatīvām grupām un ir doti aditīvajā pierakstā. Vispārināsim šos jēdzienus uz vispārīgu (ne obligāti komutatīvu) grupu gadījumu izmantojot vispārīgāko multiplikatīvo pierakstu.

Dota grupa G un tās apakšgrupa $H \leq G$. Teiksim, ka G elementi a un b ir *labēji kongruenti* mod H (apzīmēsim ar $a \equiv b(\text{mod } H)$), ja

$$ab^{-1} \in H.$$

Teiksim, ka G elementi a un b ir *kreisi kongruenti* mod H, ja

$$b^{-1}a \in H.$$

Izmantosim apzīmējumus $a \equiv b(\text{mod } H)$ (ja nav svarīgi kāda no kongruencēm ir domāta) vai $a \dot{=} b(\text{mod } H)$ (labējai) un $a \dot{=} b(\text{mod } H)$ (kreisajai).

3.1. teorēma. Katrai $H \leq G$ abas kongruences ir ekvivalences attiecības.

PIERĀDĪJUMS Jāpierāda, ka kongruence ir refleksīva, simetriska un tranzitīva. Apskatīsim tikai labējo kongruence, kreisā tiek pierādīta līdzīgi.

Refleksivitāte Katram $a \in G$ izpildās $aa^{-1} = e \in H$, tāpēc

$$a \equiv a(\text{mod } H).$$

Simetrija Ja $a \equiv b(\text{mod } H)$, tad $ab^{-1} \in H$. Tā kā H ir apakšgrupa, tad $(ab^{-1})^{-1} = ba^{-1} \in H$ un $b \equiv a(\text{mod } H)$.

Tranzitivitāte Ja $a \equiv b(\text{mod } H)$ un $b \equiv c(\text{mod } H)$, tad

$$ab^{-1} = h \in H$$

un

$$bc^{-1} = h' \in H.$$

Tā kā H ir apakšgrupa, tad

$$hh' = ab^{-1}bc^{-1} = ac^{-1} \in H$$

un $a \equiv c(\text{mod } H)$. ■

3.2. Blakusklases

Katrai $H \leq G$ ir definēti divi sadalījumi ekvivalences klasēs - *labās* un *kreisās blakusklases (cosets)* mod H.

Divas blakusklases vai nu pilnīgi sakrīt, vai arī tām nav kopīgu elementu.

Elementa $a \in G$ labējā (kreisā) blakusklase mod H ir to G elementu apakškopa, kas ir labēji (kreisi) kongruenti ar a mod H -

$$R_H(a) = \{b \in G | a \dot{=} b (\text{mod } H)\}$$

$$L_H(a) = \{b \in G | a \dot{=} b (\text{mod } H)\}$$

Ja $S \subseteq G$ un $g \in G$, tad definēsim

$$gS = \{a \in G | a = gs, \text{ kur} s \in S\}$$

un

$$Sg = \{a \in G | a = sg, \text{ kur} s \in S\}.$$

3.2. teorēma.

1. $a \dot{=} b(\text{mod } H) \iff Ha = Hb,$
   $a \dot{=} b(\text{mod } H) \iff aH = bH.$
2. $R_H(a) = Ha$ un $L_H(a) = aH.$

PIERĀDĪJUMS Apskatīsim tikai labējo kongruenci.

1. Ja $a \equiv b(\text{mod } H)$, tad $a = hb$, kur $h \in H$. Katram h' izpildās

$$h'a = h'hb$$

un

$$h'b = h'h^{-1}a$$

. Seko, ka

$$Ha = Hb.$$

Ja $Ha = Hb$, tad eksistē h, h' tādi, ka

$$ha = h'b.$$

Seko, ka

$$ab^{-1} = h'h^{-1} \in H$$

un tādējādi $a \equiv b(\text{mod } H)$.

2. Ja $a \equiv b(\text{mod } H)$, tad $a = hb$ un $b = h^{-1}a$, kur $h \in H$. Seko, ka $b \in Ha$ un tādējādi $R_H(a) \subseteq Ha$.

Ja $b \in Ha$, tad $b = h'a$. Seko, ka $ab^{-1} = h'^{-1} \in H$, $a \equiv b(\text{mod } H)$ un tādējādi $Ha \subseteq R_H(a)$. ■

3.3. Lagranža teorēma

Blakusklases veido G sadalījumu, tāpēc

$$G = \bigcup_{a \in G} Ha = \bigcup_{a \in G} aH.$$

3.3. teorēma. Dota grupa G un apakšgrupa $H \leq G$. Katram $a \in G$ eksistē bijektīvas funkcijas $f_R : H \to Ha$ un $f_R : H \to aH$.

PIERĀDĪJUMS Apskatīsim tikai f_R.

Definēsim $f_R : H \to Ha$ ar nosacījumu

$$f_R(h) = ha.$$

Pierādīsim, ka f_R ir bijektīva funkcija.

Sirjektivitāte Katram $ha \in Ha$ izpildās $ha = f_R(h)$.

Injektivitāte Ja $f_R(h_1) = f_R(h_2)$, tad $h_1a = h_2a$ un $h_1 = h_2$. ■

3.1. piezīme. No teorēmas seko, ka ja G ir galīga grupa, tad visām blakusklasēm elementu skaits ir vienāds ar $|H|$.

3.4. teorēma. (*Lagranža teorēma*) Ja G ir galīga grupa un $H \leq H$, tad

$$|H| \mid |G|.$$

PIERĀDĪJUMS Tā kā visām labajām blakusklasēm mod H elementu skaits ir vienāds un blakusklases veido G sadalījumu, tad

$$|G| = |H|k,$$

kur k ir blakusklašu skaits. ■

Galīgā grupā G blakusklašu skaitu sauc par H *indeksu* un apzīmē ar $[G : H]$.

3.5. teorēma. G ir galīga grupa

1. Ja $a \in G$ kārta ir vienāda ar n, tad $n \mid |G|$.
2. Katram $a \in$ izpildās $a^{|G|} = e$.

PIERĀDĪJUMS

1. $\langle a \rangle \leq G$, tāpēc $|\langle a \rangle| \mid |G|$.

2. Ja g kārta ir n, tad pēc iepriekšējā apgalvojuma $|G| = nq$ un
$$a^{|G|} = a^{nq} = (a^n)^q = e^q = e.$$

■

3.6. teorēma. Ja $|G| = p$ ir pirmskaitlis, tad

1. G nav netriviālu apakšgrupu,
2. G ir cikliska grupa,
3. $G \simeq \mathbb{Z}/p\mathbb{Z}$.

PIERĀDĪJUMS

1. Seko no Lagranža teorēmas.

2. Ja $g \neq e$, tad $\langle g \rangle = G$.

3. Seko no teorēmas par cikliskajām grupām. ■

4. 3.mājasdarbs

1. Dots,ka G ir komutatīva grupa, T - to G elementu apakškopa, kuriem ir galīgas kārtas. Pierādīt, ka T ir apakšgrupa (*torsion-apakšgrupa*).
2. Atrast visas cikliskās apakšgrupas grupā $(\mathbb{Z}/12\mathbb{Z}, +)$.
3. Atrast minimālu veidotājsistēmu kvadrāta rotāciju grupai un uzzīmēt atbilstošo grupas grafu.
4. Aprakstiet labās blakusklases grupai $G = \Sigma_3$ attiecībā uz apakšgrupu $H = \{e, (123), (132)\}$.
5. Grupa G satur apakšgrupas ar 208 un 2008 elementiem. Ir zināms, ka $|G| \leq 100000$. Kāds var būt $|G|$? (*Norādījums: izmantojiet Lagranža teorēmu*)