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

Studiju kurss

Algebriskās struktūras

3.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

Lekcijas mērķis:

- apgūt grupu homomorfismu pamatjēdzienus.

Lekcijas kopsavilkums:

- var definēt un pētīt funkcijas, kas saglabā operācijas - grupu homomorfismus,

Svarīgākie jēdzieni: grupu homomorfisms, izomorfisms, homomorfisma attēls un kodols, labējā un kreisā kongruence, labās un kreisās blakusklases.

Svarīgākie fakti un metodes: homomorfismu īpašības, Kēli teorēma, ciklisko grupu īpašības, ciklisko grupu klasifikācija, kongruenču ekvivalences īpašība, blakusklašu īpašības.

1. Grupu morfismi un izomorfisms

1.1. Ievads

G_1, G_2 - grupas. 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:

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

Bijektīvu grupu homomorfismu sauc par *grupu izomorfismu*. Grupu G_1 un G_2 izomorfismu apzīmēsim ar pierakstu $G_1 \simeq G_2$.

Izomorfismu $G \to G$ sauc par G *automorfismu.*

Izomorfismi saglabā operācijas struktūru (operācijas tabulu), tikai pārapzīmē elementus un operāciju.

1.1. piemērs. $\forall$ G vienības funkcija id_G ir izomorfisms.

$\forall$ G_1, G_2 konstantā funkcija $f : G_1 \to G_2$, $f(g) = e_{G_2}$ ir grupu homomorfisms.

$\forall$ $H \leq G$ ir definēts *iekļaušanas homomorfisms* $\iota_H : H \to G$.

$\forall$ $a \in G$ ir definēts *konjugācijas homomorfisms* $G \to G$, $g \mapsto aga^{-1}$.

1.1. teorēma. $f : G \longrightarrow H$ ir grupu homomorfisms.

1. f ir izomorfisms $\implies$ f^{-1} ir izomorfisms.
2. $f(e_G) = e_H$.
3. $f(a^{-1}) = f(a)^{-1}$.
4. $Im(f) \leq H$, $Ker(f) \leq G$.
5. $|G| < \infty \implies |Im(f)| < \infty$.

6. G - komutatīva grupa $\Longrightarrow$ $Im(f)$ - komutatīva grupa.

PIERĀDĪJUMS

1. f ir bijektīvs homomorfisms ar inverso funkciju $f^{-1}: H \to G$.

Pieņemsim, ka $\begin{cases} f(a) = b \\ f(a') = b' \end{cases}$ (seko, ka $\begin{cases} f^{-1}(b) = a \\ f^{-1}(b') = a'. \end{cases}$)

$$\boxed{f^{-1}(bb')} = f^{-1}(f(a)f(a')) = f^{-1}(f(aa')) =$$

$$(f^{-1} \circ f)(aa') = \mathrm{id}_G(aa') = aa' = \boxed{f^{-1}(b)f^{-1}(b')}.$$

2. $e_G e_G = e_G \Longrightarrow f(e_G e_G) = f(e_G)f(e_G) = f(e_G) \Longrightarrow$
$f(e_G)f(e_G)f(e_G)^{-1} = f(e_G)f(e_G)^{-1} \Longrightarrow f(e_G) = e_H.$

3. $aa^{-1} = e_G \Longrightarrow$

$$f(aa^{-1}) = f(a)\underbrace{f(a^{-1})}_{=f(a)^{-1}} = f(e_G) = e_H.$$

4. $\begin{cases} b = f(a) \\ b' = f(a') \end{cases} \Longrightarrow \begin{cases} bb' = f(a)f(a') = f(aa') \in Im(f) \\ b^{-1} = f(a^{-1}) \in Im(f) \end{cases}$

$e_H = f(e_G) \in Im(f) \Longrightarrow Im(f) \leq H.$

$f(a) = f(a') = e_H \Longrightarrow \begin{cases} f(aa') = f(a)f(a') = e_H e_H = e_H \\ f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H \end{cases}$

$e_G \in Ker(f) \Longrightarrow Ker(f) \leq G.$

5. $|Im(f)| \leq |G| < \infty.$

6. $\forall\, b, b' \in Im(f)\ \exists\, a, a' \in G : \begin{cases} b = f(a) \\ b' = f(a') \end{cases} \Longrightarrow$

$$\boxed{bb'} = f(a)f(a') = f(aa') = f(a'a) = f(a')f(a) = \boxed{b'b}. \blacksquare$$

1.2. piemērs. $(\mathbb{Z}, +) \simeq (G, \times)$, kur $G = \langle a \rangle = \{1, a, a^{-1}, a^2, a^{-2}, ...\}$, $a > 1$.

1.2. Svarīgākie homomorfismi un izomorfismi

1.2.1. Klasiskie piemēri

<u>Aditīvās un multiplikatīvās skaitļu grupas</u>

$\forall\ m \in \mathbb{Z}$ ir definēts homomorfisms "redukcija mod m"

$$\pi_m : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_m, +).$$

$\forall\ a \in \mathbb{R}($ vai $\mathbb{C})\backslash\{0\}$ ir definēts *eksponencēšanas homomorfisms*

$$\exp_a : (\mathbb{R}, +) \longrightarrow (\mathbb{R}\backslash\{0\}, \times),$$
$$x \mapsto a^x.$$

Moduļa homomorfisms

$$(\mathbb{C}\backslash\{0\}, \times) \longrightarrow (\mathbb{R}\backslash\{0\}, \times),$$
$$z \mapsto |z|.$$

Matricu multiplikatīvās grupas

$\forall\ n \in \mathbb{Z}, \forall$ laukam k ir definēts *determinanta homomorfisms*

$$\det : (GL(n,k), \times) \longrightarrow (k \backslash \{0\}, \times),$$
$$\mathbf{A} \mapsto \det(\mathbf{A}).$$

Permutāciju grupas

$\forall\ \Sigma_n$ ir definēts *paritātes (zīmes) homomorfisms*

$$\epsilon : (\Sigma_n, \circ) \longrightarrow (\{1, -1\}, \times),$$
$$\sigma \mapsto \epsilon(\sigma) = (-1)^{n-m},$$

kur m ir σ ciklu skaits.

1.2.2. Kēli teorēma

1.2. teorēma. $f : G \to H$- injektīvs homomorfisms $\Longrightarrow\ G \simeq Im(f)$.

PIERĀDĪJUMS f ir grupu homomorfisms, kas sirjektīvi attēlo G uz $Im(f)$. f ir injektīva funkcija $\Longrightarrow$ $f : G \to Im(f) \leq H$ ir bijektīva funkcija.■

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

PIERĀDĪJUMS G - grupa. Apskatīsim $Bij(G, G)$ - kopas G permutāciju kopu.

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

Pierādīsim, ka katram $g \in G$ funkcija

$$f_g : G \to G,$$

$$f_g(a) = ga,$$

ir kopas G permutācija:

- $\forall b \in G : \ b = g(g^{-1}b) = f_g(g^{-1}b) \Longrightarrow f_g$ ir sirjektīva funkcija;

- $ga_1 = ga_2 \implies g^{-1}ga_1 = g^{-1}ga_2 \implies a_1 = a_2 \implies f_g$ 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

$$\varphi(g_1g_2)(a) = f_{g_1g_2}(a) = g_1g_2a = g_1(g_2a) = f_{g_1}(f_{g_2}(a)) = (f_{g_1} \circ f_{g_2})(a) = (\varphi(g_1) \circ \varphi(g_2))(a).$$

Injektivitāte $\varphi(g_1) = \varphi(g_2) \implies \forall a \in G$ izpildās

$$\varphi(g_1)(a) = g_1a = \varphi(g_2)(a) = g_2a \implies g_1 = g_2.\blacksquare$$

1.1. piezīme. Kēli teorēma $\implies \Big(|G| < \infty \implies G \simeq H \leq \Sigma_{|G|}\Big)$.

1.2.3. Ciklisko grupu izomorfisma tipu klasifikācija

$\forall\ g \in G$ ar $\langle g \rangle$ apzīmēsim apakšgrupu, kuru ģenerē g:

$$\langle g \rangle = \{a \in G | a = g^n\}.$$

$g \in G$ kārtu apzīmēsim ar $ord(g)$.

1.4. teorēma. G ir grupa, $g \in G$. Ir spēkā šādi apgalvojumi:

1. $\Big(\exists\ n, m \in \mathbb{Z}, n \neq m:\ g^n = g^m\Big) \implies \Big(ord(g) < \infty\Big)$;
2. $\Big(ord(g) = k\Big) \implies \Big(g^l = e \iff l \equiv 0(\text{mod } k)\Big)$;
3. $\Big(ord(g) = k\Big) \implies \Big(g^{l_1} = g^{l_2} \iff l_1 \equiv l_2(\text{mod k})\Big)$;

PIERĀDĪJUMS

1. $g^n = g^m \implies g^{n-m} = g^{m-m} = e \implies ord(g) \leq |n - m|$.

2. $l \equiv 0(\text{mod } k) \implies k|l \implies l = qk \implies$

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

Pieņemsim, ka $g^l = e \Longrightarrow l = qk + r$, kur $0 \le r < k$. Redzam, ka

$$g^l = g^{qk+r} = g^{qk} g^r = (g^k)^q g^r = g^r = e \Longrightarrow r = 0.$$

3. Izmantojam dalīšanu ar atlikumu līdzīgi kā iepriekšējā punktā.

■

1.5. teorēma.

1. $ord(g) = k \Longrightarrow \langle g \rangle = \{e = g^0, g, g^2, ..., g^{k-1}\}$.
2. $ord(g) = \infty \Longrightarrow \langle g \rangle = \{e = g^0, g^{\pm 1}, g^{\pm 2}, ..., \}$.

1.6. teorēma. $G = \langle g \rangle$ ir bezgalīga cikliska grupa $\Longrightarrow G \simeq \mathbb{Z}$.

PIERĀDĪJUMS Definēsim funkciju

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

Pierādīsim, ka f ir bijektīvs grupu homomorfisms.

Sirjektivitāte
G ir cikliska grupa $\Longrightarrow$ $\forall a \in G \; \exists m \in \mathbb{Z}:$

$$a = g^m = f(m).$$

Injektivitāte
$f(n_1) = f(n_2)$ $\Longrightarrow$ $g^{n_1} = g^{n_2}$. 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 $ord(g) < \infty$ un tādējādi g nevar būt visas bezgalīgās grupas ģenerators.

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

1.7. teorēma. $\left\{ \begin{array}{l} G = \langle g \rangle \\ |G| = m \end{array} \right. \Longrightarrow G \simeq \mathbb{Z}_m.$

PIERĀDĪJUMS Definēsim funkciju

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

Pierādīsim, ka f ir bijektīvs grupu homomorfisms.

Sirjektivitāte
$G = \langle g \rangle \implies \forall a \in G \; \exists \, l \in \mathbb{Z}:$

$$a = g^l = f(l).$$

Injektivitāte
$f(n_1) = f(n_2) \implies g^{n_1} = g^{n_2} \implies$

$$g^{n_1} g^{-n_2} = g^{n_1 - n_2} = g^{n_2} g^{-n_2} = e \implies n_1 \equiv n_2 (\text{mod m}).$$

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

1.3. piemērs. $(\langle -1 \rangle, \cdot) \simeq (\mathbb{Z}/2\mathbb{Z}, +)$, $(\langle i \rangle, \cdot) \simeq (\mathbb{Z}/4\mathbb{Z}, +)$.

2. Kongruences un blakusklases

2.1. Kongruence

2.1. 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 multiplikatīvo pierakstu:

- aditīvajam pierakstam $a - b$ var atbilst divi multiplikatīvie pieraksti: ab^{-1} un $b^{-1}a$,
- var secināt, ka būs divi kongruences jēdzieni.

G - grupa, $H \leq G$. G elementi a un b ir

- *labēji kongruenti* mod H ($a \fallingdotseq b (\text{mod } H)$), ja $ab^{-1} \in H$;

- *kreisi kongruenti* mod H ($a \fallingdotseq b(\text{mod } H)$), ja $b^{-1}a \in H$.

Izmantosim apzīmējumu $a \equiv b(\text{mod } H)$, ja nav svarīgi, kāda no kongruencēm ir domāta.

2.1. teorēma. $\forall\ H \leq G$ abas kongruences ir ekvivalences attiecības.

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

Refleksivitāte
$\forall\ a \in G: \ aa^{-1} = e \in H \implies a \equiv a(\text{mod } H)$.

Simetrija
$a \equiv b(\text{mod } H) \implies ab^{-1} \in H$. H ir apakšgrupa $\implies$
$(ab^{-1})^{-1} = ba^{-1} \in H \implies b \equiv a(\text{mod } H)$.

Tranzitivitāte

$$\begin{cases} a \equiv b \pmod{H} \\ b \equiv c \pmod{H} \end{cases} \Longrightarrow \begin{cases} ab^{-1} = h \in H \\ bc^{-1} = h' \in H. \end{cases}$$

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

$\Longrightarrow$ $a \equiv c (\mathrm{mod}\ H)$. ■

2.2. Blakusklases

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

Divas blakusklases (kā ekvivalences klases) 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 -

$$R_H(a) = \{b \in G | a \risingdotseq b (\mathrm{mod}\ H)\}$$

$$L_H(a) = \{b \in G | a \fallingdotseq b (\mathrm{mod}\ H)\}.$$

2.2. teorēma.

1. $a \risingdotseq b (\mathrm{mod}\ H) \iff Ha = Hb,$

   $a \fallingdotseq b (\mathrm{mod}\ H) \iff aH = bH.$

2. $R_H(a) = Ha$ un $L_H(a) = aH.$

PIERĀDĪJUMS Apskatīsim tikai labējo kongruenci.

1. $a \equiv b (\mathrm{mod}\ H) \Longrightarrow \begin{cases} a = hb \\ b = h^{-1}a \end{cases}$ kur $h \in H.$

$\forall\ h' \in H$ izpildās

$$\begin{cases} h'a = h'hb \\ h'b = h'h^{-1}a \end{cases} \Longrightarrow \begin{cases} Ha \subseteq Hb \\ Hb \subseteq Ha \end{cases} \Longrightarrow Ha = Hb.$$

$$Ha = Hb \Longrightarrow \exists\ h \in H:\ a = hb \Longrightarrow$$

$$ab^{-1} = h \in H \Longrightarrow a \equiv b (\mathrm{mod}\ H).$$

2. $a \equiv b (\mathrm{mod}\ H) \Longrightarrow a = hb$ un $b = h^{-1}a$, kur $h \in H \Longrightarrow$

$b \in Ha \implies R_H(a) \subseteq Ha.$

$b \in Ha \implies b = h'a \implies ab^{-1} = h'^{-1} \in H,\ a \equiv b (\mathrm{mod}\ H) \implies Ha \subseteq R_H(a).$ ■

2.1. piezīme. Elements a ir blakusklašu aH un Ha *pārstāvis.* Vienai blakusklasei var būt vairāki pārstāvji.

2.2. piemērs. Vektoru grupa.

3. 3.mājasdarbs

3.1. Obligātie uzdevumi

3.1 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 $(G, \bullet) \simeq G$.

3.2 G ir komutatīva grupa, T - to G elementu apakškopa, kuriem ir galīgas kārtas. Pierādīt, ka $T \leq G$ (*torsionapakšgrupa*).

3.3 Atrast visas cikliskās apakšgrupas grupā $(\mathbb{Z}/12\mathbb{Z}, +)$.

3.4 Aprakstiet labās blakusklases grupai $G = \Sigma_3$ attiecībā uz apakšgrupu $H = \{e, (123), (132)\}$.

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

3.5 Pierādiet, ka $(\mathbb{Z}[X], +) \simeq (\mathbb{Q}^+, \times)$, kur $\mathbb{Q}^+$ ir pozitīvo racionālo skaitļu kopa.