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

Studiju kurss

Algebriskās struktūras

4.lekcija

Docētājs: Dr. P. Daugulis

2010./2011.studiju gads

Saturs

Lekcijas mērķis:

- apgūt kongruences un blakusklašu pamatīpašības,
- apgūt faktorgrupas jēdzienu,
- apgūt "pirmo izomorfismu teorēmu".

Lekcijas kopsavilkums:

- var vispārināt veselo skaitļu kongruences un atlikumu klašu jēdzienu uz patvaļīgu grupu gadījumu,
- var vispārināt atlikumu operācijas uz patvaļīgu grupu gadījumu un ieviest faktorgrupas jēdzienu,
- grupu homomorfisma attēls ir izomorfs definīcijās apgabala grupas faktorgrupai mod kodols.

Svarīgākie jēdzieni: labējā un kreisā kongruence, labās un kreisās blakusklases, normāla apakšgrupa, faktorgrupa.

Svarīgākie fakti un metodes: kongruenču ekvivalences īpašība, blakusklašu īpašības, Lagranža īpašība, kongruenču un blakusklašu īpašības normālajām apakšgrupām, blakusklašu operācijuas korektums un īpašības, pirmā izomorfismu teorēma.

1. Kongruences un blakusklases

1.1. Kongruence

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

$$a \equiv b(\mathrm{mod}\ m) \iff a - b = mq \in m\mathbb{Z},$$

$$f(X) \equiv g(X)(\mathrm{mod}\ m(X)) \iff f(X) - g(X) = m(X)q(X) \in I.$$

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 ($a \risingdotseq b(\mathrm{mod}\ H)$), ja $ab^{-1} \in H$;

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

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

1.1. 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
$\forall\ a \in G:\ aa^{-1} = e \in H \implies a \equiv a(\mathrm{mod}\ H)$.

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

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 $\Longrightarrow$ $hh' = ab^{-1}bc^{-1} = ac^{-1} \in H$
$\Longrightarrow$ $a \equiv c(\text{mod } H)$. ■

1.2. 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 -

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

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

1.2. 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 $h \in H \Longrightarrow$

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

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

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

1.2. piemērs. Vektoru grupa. Brīvās grupas.

1.3. Lagranža teorēma

1.3. teorēma. *G, $H \leq G$. $\forall\ a \in G\ \exists$ bijektīvas funkcijas*

$$\begin{cases} f_R : H \to Ha \\ f_L : H \to aH. \end{cases}$$

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

Injektivitāte $f_R(h_1) = f_R(h_2) \implies h_1 a = h_2 a \implies h_1 = h_2$. ■

1.2. piezīme. $|G| < \infty \implies \forall Ha$ izpildās $|Ha| = |aH| = |H|$.

1.4. teorēma. (*Lagranža teorēma*) $|G| < \infty$, $H \leq G \implies |H| \mid |G|$.

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

$$|G| = |H|k, \text{ kur } k \text{ ir blakusklašu skaits.} ■$$

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

1.5. teorēma. G ir galīga grupa

1. $ord(a) = n \implies n \mid |G|$.
2. $\forall\, a$ izpildās $a^{|G|} = e$.

PIERĀDĪJUMS

1. $\langle a\rangle \leq G \implies |\langle a\rangle| \mid |G|$.

2. $ord(a) = n \implies |G| = nq \implies$

$$a^{|G|} = a^{nq} = (a^n)^q = e^q = e. \blacksquare$$

1.6. teorēma. $|G| = p$ ir pirmskaitlis $\implies$

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. $g \neq e \implies \langle g \rangle = G$.

3. Seko no teorēmas par cikliskajām grupām. ■

2. Normālās apakšgrupas un faktorizācija

2.1. Normālās apakšgrupas

2.1. piemērs. Atcerēsimies kongruences īpašību veselo skaitļu un polinomu teorijā:

$$\left\{\begin{array}{l} a \equiv b(\text{mod m}) \\ a' \equiv b'(\text{mod m}) \end{array}\right. \implies a + a' \equiv b + b'(\text{mod m}).$$

Šī īpašība ļauj korekti definēt operāciju kongruences klašu kopa un dabiskā projekcija

$$\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$

ir grupu homomorfisms.

Ja grupa nav komutatīva, tad šī īpašība var neizpildīties.

Grupas G apakšgrupu N sauksim par *normālu apakšgrupu (normālu dalītāju, $N \trianglelefteq G$)*, ja $\forall a \in G$:

$$Na = aN.$$

Ja grupai nav netriviālu normālu apakšgrupu, tad to sauc par *vienkāršu grupu*.

2.2. piemērs. $\forall$ G apakšgrupas $\{e\}$ un G ir normālas. Ja G ir komutatīva, tad katra apakšgrupa ir normāla.

2.1. teorēma. $N \trianglelefteq G$.

$$\left\{ \begin{array}{l} a \equiv b (\mathrm{mod}\ N) \\ a' \equiv b' (\mathrm{mod}\ N) \end{array} \right. \quad \Longrightarrow \quad aa' \equiv bb' (\mathrm{mod}\ N).$$

(abām kongruencēm)

PIERĀDĪJUMS No kongruences seko

$$\begin{cases} ab^{-1} = h \in N \\ a'b'^{-1} = h' \in N \end{cases} \Longrightarrow (aa')(bb')^{-1} = aa'b'^{-1}b^{-1} = ah'b^{-1}.$$

$$Na = aN \Longrightarrow \exists\, h'' \in N : \; ah' = h''a \Longrightarrow$$

$$(aa')(bb')^{-1} = ah'b^{-1} = h''ab^{-1} = h''h \in N.$$

Seko, ka $aa' \equiv bb' (\mathrm{mod}\ N)$. ■

2.2. teorēma. Sekojošie apgalvojumi ir ekvivalenti:

1. $N \trianglelefteq G$;
2. $\forall a \in G : a^{-1}Na \subseteq N$;
3. $\forall a \in G : a^{-1}Na = N$.

PIERĀDĪJUMS Pierādīsim apgalvojumu ekvivalenci ar ciklisko metodi.

$\underline{1. \Longrightarrow 2.}$ Apskatīsim elementu $a^{-1}ha$ patvaļīgam $h \in N$:

$$a^{-1}ha = (h^{-1}a)^{-1}a.$$

$$Na = aN \implies \exists\, h' \in N: \ ah' = h^{-1}a \implies$$
$$a^{-1}ha = (h^{-1}a)^{-1}a = (ah')^{-1}a = h'^{-1}a^{-1}a = h'^{-1} \in N.$$

<u>2. $\implies$ 3.</u> Ir jāpierāda, ka $N \subseteq a^{-1}Na$. Dots, ka $h' \in N$, jāpierāda, ka $\forall a \in G: \ a^{-1}h'a \in N$.

$$h' \in N \implies$$
$$h' = a^{-1}ah'a^{-1}a = a^{-1}\underbrace{(ah'a^{-1})}_{\in N}a = a^{-1}h''a \in a^{-1}Na.$$

<u>3. $\implies$ 1.</u> Jāpierāda, ka $\forall\ h \in N\ \exists\ h' \in N: \ ha = ah'$ un $h'' \in N: \ ah = h''a$.

Dots, ka $a^{-1}ha = h' \in N \implies ha = ah'$. Dots, ka $h = a^{-1}h''a \implies ah = h''a$. ■

2.2. Faktorgrupas

$N \trianglelefteq G$. Apzīmēsim labo blakusklašu kopu ar G/N. Tādējādi G/N elementi ir kopas formā Na. Varam mēģināt definēt operāciju labo blakusklašu kopā šādi:

$$(Na)(Nb) = N(ab).$$

Citiem vārdiem sakot, izvēlamies no katras blakusklases vienu pārstāvi, veicam ar tiem operāciju un definējam rezultāta blakusklasi kā blakusklašu operācijas rezultātu.

Katrs no kopas Na elementiem var tikt izvēlēts a vietā kā blakusklases pārstāvis.

Jautājums ir, vai šī operācija ar blakusklasēm ir korekti definēta - nav atkarīga no klases pārstāvju izvēles.

2.3. teorēma. $N \trianglelefteq G$.

$$\begin{cases} Na = Nb \\ Na' = Nb' \end{cases} \implies N(aa') = N(bb').$$

PIERĀDĪJUMS No iepriekšējām teorēmām seko, ka

$$\begin{cases} a \equiv b(\bmod\ N) \\ a' \equiv b'(\bmod\ N) \end{cases} \Longrightarrow aa' \equiv bb'(\bmod\ N) \Longrightarrow Naa' = Nbb'. \blacksquare$$

2.4. teorēma. $N \trianglelefteq G \Longrightarrow G/N$ ir grupa ar definēto operāciju.

PIERĀDĪJUMS Ir jāpārbauda, ka ir spēkā grupas aksiomas.

Asociativitāte $\forall a, b, c \in G$ izpildās

$$\Big((Na)(Nb)\Big)(Nc) = N(ab)Nc = N\Big((ab)c\Big) =$$

$$N\Big(a(bc)\Big) = (Na)N(bc) = (Na)\Big((Nb)(Nc)\Big).$$

Vienības elements $\forall a \in G$ izpildās

$$\begin{cases} (Na)(Ne) = N(ae) = Na \\ (Ne)(Na) = N(ea) = Na. \end{cases}$$

Seko, ka Ne ir vienības elements.

Inversā elementa eksistence $\forall a \in G$ izpildās

$$(Na)(Na^{-1}) = N(aa^{-1}) = Ne \implies (Na)^{-1} = Na^{-1}. \blacksquare$$

Grupu G/N sauc par *faktorgrupu* G mod N.

2.3. piemērs. Atlikumu klašu grupa.

Ja $G = \Sigma_3$ un $|N| = 3$, tad $G/N \simeq \mathbb{Z}/2\mathbb{Z}$.

3. "Pirmā izomorfismu teorēma"

3.1. Palīgrezultāts

3.1. teorēma.

1. $f : G \to H$ ir grupu homomorfisms. Tad
$$Ker(f) \trianglelefteq G.$$
2. $f : G \to H$ ir grupu homomorfisms. Tad
$$f \text{ ir injektīvs} \iff Ker(f) = \{e\}.$$
3. $N \trianglelefteq G$. Tad funkcija
$$\pi : G \to G/N,$$
$$\pi(a) = Na$$
ir sirjektīvs homomorfisms un $Ker(f) = N$,

PIERĀDĪJUMS
1. Agrāk tika pierādīts, ka $Ker(f) \leq G$.

Pierādīsim, ka $Ker(f) \trianglelefteq G$. Pierādīsim, ka $\forall x \in Ker(f)$, $\forall a \in G$ izpildās $a^{-1}xa \in Ker(f)$:

$$f(a^{-1}xa) = f(a^{-1})f(x)f(a) = f(a)^{-1}ef(a) = f(a)^{-1}f(a) = e.$$

2. f ir injektīvs $\Longrightarrow$ $Ker(f) = \{e\}$ pēc injektivitātes definīcijas. Pieņemsim, ka $Ker(f) = \{e\}$. $f(a) = f(a')$ $\Longrightarrow$

$$f(aa'^{-1}) = f(a)f(a'^{-1}) = f(a)f(a')^{-1} = e$$

$\Longrightarrow$ $aa'^{-1} = e$ un $a = a'$.

3. <u>Sirjektivitāte</u> $\forall a \in G : Na = \pi(a)$.

<u>Homomorfisms</u> $\forall a, a' \in G :$

$$\pi(aa') = N(aa') = (Na)(Na').$$

<u>Kodols</u> $\pi(a) = Na = Ne$ $\Longrightarrow$ $a \in N$ $\Longrightarrow$ $Ker(\pi) \subseteq N$.
$h \in N$ $\Longrightarrow$ $\pi(h) = Nh = N = Ne$ $\Longrightarrow$ $Ker(\pi) = N$. ■

3.1. piemērs. Atlikumu grupas.

3.2. Galvenais rezultāts

3.2. teorēma. (*Pirmā izomorfismu teorēma*) Ja $f : G \to H$ ir grupu homomorfisms, tad

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

PIERĀDĪJUMS Apzīmēsim $Ker(f)$ ar N. Definēsim funkciju

$$\varphi : G/N \to Im(f),$$

$$\varphi(Na) = f(a).$$

Pierādīsim, ka φ ir korekti definēts grupu izomorfisms.

Korektums $Na = Na' \implies a = ha' \implies$

$$\varphi(Na) = f(a) = f(ha') = f(h)f(a') = ef(a') = f(a') = \varphi(Na').$$

Homomorfisms

$$\varphi((Na)(Nb)) = \varphi(Nab) = f(ab) = f(a)f(b) = \varphi(Na)\varphi(Nb).$$

Bijektivitāte Sirjektivitāte - $\forall t \in Im(f)$ izpildās

$$t = f(a) = \varphi(Na).$$

Injektivitāte - $\varphi(Na) = \varphi(Na') \implies f(a) = f(a') \implies$

$$f(a)f(a')^{-1} = f(aa'^{-1}) = e$$

un $aa'^{-1} = h \in N \implies a = ha' \implies Na = Na'$. ■

3.1. piezīme. No pirmās izomorfismu teorēmas seko, ka vienkāršās grupas nevar tikt "vienkāršotas" - ja G ir vienkārša grupa, tad neeksistē netriviāli neinjektīvi homomorfismi $f : G \to H$ (kuriem $Ker(f) \neq G$).

Šī novērojuma dēļ ir interesanti pētīt un klasificēt vienkāršās grupas. No 1950.g. līdz 1980.g tika īstenots pētniecības projekts, kura mērķis bija klasificēt galīgās vienkāršās grupas. Tiek uzskatīts, ka ap 1980.g šis mērķis tika sasniegts.

4. 4.mājasdarbs

4.1. Obligātie uzdevumi

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

4.2 Grupa G satur apakšgrupas ar 2009 un 2010 elementiem. Ir zināms, ka $|G| \leq 13^6$. Kāds var būt $|G|$? (*Norādījums: izmantojiet Lagranža teorēmu*)

4.3 Pierādiet, ka $H \trianglelefteq G$ šādos gadījumos:
(a) ja $[G : H] = 2$;
(b) ja $G = GL(n, \mathbb{R})$ un $H = SL(n, \mathbb{R})$;

4.4 Dots, ka $N, N' \trianglelefteq G$ un $N \cap N' = \{e\}$. Pierādīt, ka $\forall a \in N$ un $\forall a \in N'$ izpildās $ab = ba$.

4.5 Pieņemsim, ka G ir visu to reālo matricu kopa, kas ir formā

$$\left[\begin{array}{c|c|c} 1 & x & y \\ \hline 0 & 1 & z \\ \hline 0 & 0 & 1 \end{array}\right]$$

(a) Pierādiet, ka G ir grupa ar matricu reizināšanas operāciju, atrodiet vienības elementu un inversos elementus.
(b) Atrodiet $Z(G)$, pierādiet, ka $Z(G) \simeq (\mathbb{R}, +)$.
(c) Pierādiet, ka $G/Z(G)$ ir izomorfa plaknes vektoru kopai ar saskaitīšanas operāciju.

4.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

4.6 G ir galīga grupa, $H \leq G$. Pierādīt, ka eksistē elementi $a_1, ..., a_n$, $n = |G|/|H|$ tādi, ka $a_1H, ..., a_nH$ ir kreiso blakusklašu kopa un $Ha_1, ..., Ha_n$ ir labo blakusklašu kopa. Citiem vārdiem sakot, eksistē *kopīga H blakusklašu pārstāvju sistēma.*

4.7 G - grupa, $H, K \leq G$. Definēsim (H, K)-*divkāršo blakusklasi*

$$HaK = \{g | g = hak, h \in H, k \in K\}.$$

Pierādīt, ka (H, K)-divkāršās blakusklases veido G sadalījumu.