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

Studiju kurss

Algebriskās struktūras

4.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

Lekcijas mērķis:

- apgūt kongruences, blakusklašu un faktorgrupas jēdzienu

Lekcijas kopsavilkums:

- var vispārināt atlikumu operācijas uz patvaļīgu grupu gadījumu un ieviest faktorgrupas jēdzienu.

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

Svarīgākie fakti un metodes: kongruenču ekvivalences īpašība, blakusklašu īpašības, Lagranža teorēma, kongruenču un blakusklašu īpašības normālajām apakšgrupām, blakusklašu operācijas korektums un īpašības

1. Kongruences un blakusklases

1.1. Kongruence

1.1. piemērs. Atcerēsimies kongruences veselo skaitļu teorijā:

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

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

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

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

$$\begin{cases} a \equiv b \ (\text{mod } H) \\ b \equiv c \ (\text{mod } H) \end{cases} \implies \begin{cases} ab^{-1} = h \in H \\ bc^{-1} = h' \in H. \end{cases}$$

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. $a \fallingdotseq b(\bmod H) \iff Ha = Hb$,
   $a \risingdotseq b(\bmod H) \iff aH = bH$.
2. $R_H(a) = Ha$ un $L_H(a) = aH$.

PIERĀDĪJUMS Apskatīsim tikai labējo kongruenci.

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

$\forall\ h' \in H$ izpildās

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

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

$$ab^{-1} = h \in H \implies a \equiv b(\bmod H).$$

2. $a \equiv b(\bmod H) \implies a = hb$ un $b = h^{-1}a$, kur $h \in H \implies$
$b \in Ha \implies R_H(a) \subseteq Ha$.

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

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

1.2. piemērs. Vektoru grupa.

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. $\blacksquare$

2. Normālās apakšgrupas un faktorizācija

2.1. Normālās apakšgrupas

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

$$\begin{cases} a \equiv b (\text{mod m}) \\ a' \equiv b' (\text{mod m}) \end{cases} \implies a + a' \equiv b + b' (\text{mod m}).$$

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

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

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

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

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.

<u>1. $\Longrightarrow$ 2.</u> Apskatīsim elementu $a^{-1}ha$ patvaļīgam $h \in N$:

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

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

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

$h' \in N \implies$

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

3. $\implies$ 1. 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 apakškopas 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. $N \trianglelefteq G$.

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

PIERĀDĪJUMS No iepriekšējām teorēmām seko, ka

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

2.4. teorēma. $N \trianglelefteq G \implies G/N$ 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 $G\big/N$ sauc par *faktorgrupu* G mod N.

2.3. piemērs. Atlikumu klašu grupa.

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

3. 4.mājasdarbs

3.1. 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 2010 un 2011 elementiem. Ir zināms, ka $|G| \leq 2^{22}$. Kāds var būt $|G|$? (*Norādījums: izmantojiet Lagranža teorēmu*)

4.3 Pierādiet, ka $H \trianglelefteq G$, 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 $\forall\ b \in N'$ 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.

3.2. 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*

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

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