

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

Studiju kurss

Algebriskās struktūras

4.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

1. Kongruences un blakusklasses	5
1.1. Kongruence	5
1.2. Blakusklasses	7
1.3. Lagranža teorēma	9
2. Normālās apakšgrupas un faktorizācija	12
2.1. Normālās apakšgrupas	12
2.2. Faktorgrupas	16
3. "Pirmā izomorfismu teorēma"	19
3.1. Palīgrezultāts	19
3.2. Galvenais rezultāts	21
4. 4.mājasdarbs	23
4.1. Obligātie uzdevumi	23
4.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi	24

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 blakusklauses, normāla apakšgrupa, faktorgrupa.

Svarīgākie fakti un metodes: kongruenču ekvivalences īpašība, blakusklašu īpašības, Lagranža īpašība, kongruenču un blakusklašu

īpašības normālajām apakšgrupām, blakusklašu operācijas korektums un īpašības, pirmā izomorfismu teorēma.

1. Kongruences un blakusklasses

1.1. Kongruence

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

$$a \equiv b \pmod{m} \iff a - b = mq \in m\mathbb{Z},$$

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

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* ($a \doteq b \pmod{H}$), ja $ab^{-1} \in H$;

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

Izmantosim apzīmējumu $a \equiv b \pmod{H}$, 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

$$\forall a \in G : aa^{-1} = e \in H \implies a \equiv a \pmod{H}.$$

Simetrija

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

Tranzitivitāte

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

H ir apakšgrupa $\implies hh' = ab^{-1}bc^{-1} = ac^{-1} \in H$
 $\implies a \equiv c \pmod{H}$. ■

1.2. Blakusklasses

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

Divas blakusklasses (kā ekvivalences klases) vai nu pilnīgi sakrīt, vai arī tām nav kopīgu elementu.

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

$$R_H(a) = \{b \in G \mid a \equiv b \pmod{H}\}$$

$$L_H(a) = \{b \in G \mid a \equiv b \pmod{H}\}.$$

1.2. teorēma.

- $a \equiv b \pmod{H} \iff Ha = Hb,$
 $a \equiv b \pmod{H} \iff aH = bH.$
- $R_H(a) = Ha$ un $L_H(a) = aH.$

PIERĀDĪJUMS Apskatīsim tikai labējo kongruenci.

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

$\forall h' \in H$ izpildās

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

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

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

$$2. a \equiv b \pmod{H} \implies a = hb \text{ un } b = h^{-1}a, \text{ kur } h \in H \implies$$

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

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

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

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

PIERĀDĪJUMS Apskatīsim tikai f_R .

Definēsim $f_R : H \rightarrow Ha$ ar nosacījumu

$$f_R(h) = ha.$$

Pierādīsim, ka f_R ir bijektīva funkcija.

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

Injektivitāte $f_R(h_1) = f_R(h_2) \implies h_1a = h_2a \implies h_1 = h_2$. ■

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

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

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

1.5. teorēma. G ir galīga grupa

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

PIERĀDĪJUMS

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

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

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

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:

$$\begin{cases} a \equiv b \pmod{m} \\ a' \equiv b' \pmod{m} \end{cases} \implies a + a' \equiv b + b' \pmod{m}.$$

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

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

ir grupu homomorfisms.

Ja grupa nav komutatīva, tad šī īpašība var neizpildīties.

Grupas G apakšgrupu N saucim 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. $N \trianglelefteq G$.

$$\begin{cases} a \equiv b \pmod{N} \\ a' \equiv b' \pmod{N} \end{cases} \implies aa' \equiv bb' \pmod{N}.$$

(abām kongruencēm)

PIERĀDĪJUMS No kongruences seko

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

$$Na = aN \implies \exists h'' \in N : ah' = h''a \implies \\ (aa')(bb')^{-1} = ah'b^{-1} = h''ab^{-1} = h''h \in N.$$

Seko, ka $aa' \equiv bb' \pmod{N}$. ■

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.

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

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

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

2. \implies 3. 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 kopas formā Na . Varam mēģināt definēt operāciju labo blakusklašu kopā šādi:

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

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

Katrs no kopas Na elementiem var tikt izvēlēts a vietā kā blakusklauses 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

$$\begin{cases} a \equiv b \pmod{N} \\ a' \equiv b' \pmod{N} \end{cases} \implies aa' \equiv bb' \pmod{N} \implies Naa' = Nbb'. \blacksquare$$

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

$$\begin{aligned} ((Na)(Nb))(Na) &= N(ab)Nc = N((ab)c) = \\ &= N(a(bc)) = (Na)N(bc) = (Na)((Nb)(Nc)). \end{aligned}$$

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

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

Grupā G/N sauc par *faktorgrupu* $G \bmod N$.

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. $f : G \rightarrow H$ ir grupu homomorfisms. Tad

$$\text{Ker}(f) \trianglelefteq G.$$

2. $f : G \rightarrow H$ ir grupu homomorfisms. Tad

$$f \text{ ir injektīvs} \iff \text{Ker}(f) = \{e\}.$$

3. $N \trianglelefteq G$. Tad funkcija

$$\begin{aligned} \pi : G &\rightarrow G/N, \\ \pi(a) &= Na \end{aligned}$$

ir surjektīvs homomorfisms un $\text{Ker}(\pi) = N$,

PIERĀDĪJUMS

1. Agrāk tika pierādīts, ka $\text{Ker}(f) \leq G$.

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

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

2. f ir injektīvs $\implies \text{Ker}(f) = \{e\}$ pēc injektivitātes definīcijas.

Pieņemsim, ka $\text{Ker}(f) = \{e\}$. $f(a) = f(a') \implies$

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

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

3. Sirjektivitāte $\forall a \in G : Na = \pi(a)$.

Homomorfisms $\forall a, a' \in G :$

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

Kodols $\pi(a) = Na = Ne \implies a \in N \implies \text{Ker}(\pi) \subseteq N$.

$h \in N \implies \pi(h) = Nh = N = Ne \implies \text{Ker}(\pi) = N$. ■

3.1. piemērs. Atlikumu grupas.

3.2. Galvenais rezultāts

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

$$\text{Im}(f) \simeq G/\text{Ker}(f).$$

PIERĀDĪJUMS Apzīmēsim $\text{Ker}(f)$ ar N . Definēsim funkciju

$$\begin{aligned}\varphi : G/N &\rightarrow \text{Im}(f), \\ \varphi(Na) &= f(a).\end{aligned}$$

Pierādīsim, ka φ ir korekti definēts grupu izomorfisms.

$$\begin{aligned}\text{Korektums } Na = Na' &\implies a = ha' \implies \\ \varphi(Na) = f(a) &= f(ha') = f(h)f(a') = ef(a') = f(a') = \varphi(Na').\end{aligned}$$

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 $f : G \rightarrow H$ (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 blakusklares 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:
- ja $[G : H] = 2$;
 - 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

$$\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}$$

- (a) Pierādiet, ka G ir grupa ar matricu reizināšanas operāciju, atrodi 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, \dots, a_n , $n = |G|/|H|$ tādi, ka a_1H, \dots, a_nH ir kreiso blakusklašu kopa un Ha_1, \dots, 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) -divkārsšo blakusklassi

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

Pierādīt, ka (H, K) -divkārsšās blakusklasses veido G sadalījumu.