DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra

Studiju kurss

Veselo skaitļu teorija

6.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

Lekcijas mērķis:

- apgūt svarīgu algebrisko struktūru: grupu un gredzenu pamatjēdzienus,
- atpazīt grupu un gredzenu struktūras atlikumu kopās.

Lekcijas kopsavilkums:

- var definēt divas svarīgas algebriskas struktūras: grupas un gredzenus, apskatīt to vienkāršākās īpašības,
- atlikumu operācijas dot iespēju definēt grupu un gredzenu struktūras.

Svarīgākie jēdzieni: grupa, grupu homomorfisms un izomorfisms, multiplikatīvais un aditīvais pieraksts, apakšgrupa, cikliska apakšgrupa, blakusklase, faktorgrupa, tiešā summa, gredzens, gredzenu homomorfisms, lauks.

Svarīgākie fakti un metodes: atlikumu aditīvās un multiplikatīvās grupas eksistence, atlikumu gredzena eksistence.

1. Atlikumu gredzeni un algebriskās struktūras

1.1. Grupas

Par *grupu* sauc kopu G, kurā ir uzdota viena binära (divu argumentu) operācija

$$G \times G \to G,$$
$$(x, y) \mapsto xy$$

kas apmierina šādas īpašības:

- operācija ir asociatīva: $(xy)z = x(yz)\ \forall\ x, y, z$,
- $\exists$ neitrālais (vienības) elements e: $xe = ex = x\ \forall\ x \in G$,
- $\forall\ x \in G\ \exists\ y = x^{-1} \in G$ (x inversais elements): $xy = yx = e$.

Grupas operāciju apzīmē ar kādu atdalošo simbolu $(\cdot, *, +)$.

G_1, G_2 - grupas. Funkciju $f : G_1 \to G_2$ sauc par *grupu homomorfismu*, ja tā saglabā grupas operāciju (komutē ar grupas operāciju):

$$f(x *_{G_1} y) = f(x) *_{G_2} f(y).$$

Bijektīvu grupu homomorfismu sauc par *grupu izomorfismu.* Ja $\exists$ grupu izomorfisms $f : G \to H$, tad G un H sauc par *izomorfām grupām*, apzīmē $G \simeq H$.

Izomorfas grupas var uzskatīt par neatšķiramām no struktūras viedokļa. Grupu izomorfisma attiecība ir ekvivalence.

Ja operācija ir komutatīva, tad grupu sauc par *komutatīvu (Ābela) grupu.* Mēs šajā kursā sākot ar šo vietu strādāsim ar komutatīvajām grupām.

Komutatīvām grupām parasti lieto *aditīvo pierakstu* -

- par atdalošo simbolu izmanto + vai līdzīgu simbolu,
- neitrālo elementu apzīmē ar 0,

- inverso elementu $-x$.

1.1. piemērs. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ar saskaitīšanas operāciju ir komutatīvas grupas. $(m\mathbb{Z}, +)$ ir komutatīva grupa. Vektoru kopa ar vektoru saskaitīšanas operāciju ir grupa.

Grupas apakškopu H sauksim par G *apakšgrupu* $(H \leq G)$, ja

1. $h \in H$ un $h' \in H \implies h + h' \in H$;
2. $h \in H \implies -h \in H$;
3. $e \in H$.

Fiksēsim $g \in G$. Kopu $\{0, \pm a, \pm 2a, \pm 3a, ...\}$ sauc par *ciklisku apakšgrupu ar ģeneratoru* g, apzīmē ar $\langle a \rangle$.

Grupas faktorstruktūras - *faktorgrupas*. Katrai apakšgrupa $H \leq G$ definē *blakusklases* - kopas

$$g + H = \{g + h | h \in H\}.$$

Tādējādi tiek definēts kopas G sadalījums.

Var definēt operāciju blakusklašu kopā G/H līdzīgi tam kā tika definētas operācija atlikumu klasēs.

G - komutatīva grupa, $H \leq G$, $K \leq G$. Saka, ka G ir savu apakšgrupu H un K *tiešā summa* ($G = H \oplus K$), ja $\forall g \in G$ ir vienno zīmīgi izsakāms formā

$$g = h + k, \text{ kur } h \in H, k \in K.$$

1.2. piemērs. Telpas vektoru telpa $\mathbb{R}^3 = \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$. $\forall$ vektors viennozīmīgi izsakās kā bāzes vektoru lineāra kombinācija vai kā tādu vektoru summa, kas pieder koordinātu taisnēm.

1.1. teorēma.

1. $\forall\, m \in \mathbb{Z}$ $(\mathbb{Z}_m, +)$ ir komutatīva grupa (*atlikumu aditīvā grupa*).
2. Redukcija $\pi_m : \mathbb{Z} \to \mathbb{Z}_m$ ir grupu homomorfisms.

PIERĀDĪJUMS
1. Atlikumu klašu saskaitīšana ir asociatīva un komutatīva.
$\forall\, x \in \mathbb{Z}_m : x + (-x) \equiv 0 (\mathrm{mod}\ m)$.
$0 \in \mathbb{Z}_m$ ir neitrālais elements.

2. $\pi_m(a+b) = \pi_m(a) + \pi_b(b)$. ■

1.2. teorēma. $\forall\, m \in \mathbb{Z}$ $(\mathcal{U}_m, \cdot)$ ir komutatīva grupa (*atlikumu multiplikatīvā grupa*).

PIERĀDĪJUMS
Korektums
$u, u' \in \mathcal{U}_m \implies (uu')^{-1} = u^{-1}u'^{-1} \implies uu' \in \mathcal{U}_m$.

Asociativitāte un komutativitāte
Atlikumu reizināšana ir asociatīva un komutatīva.

Neitrālais elements
$1 \in \mathbb{Z}_m$ ir neitrālais elements.

Invertējamība
$\forall\ u \in \mathcal{U}_m\ \exists\ u^{-1} \in \mathcal{U}_m.$
$\forall\ x \in \mathbb{Z}_m : x + (-x) \equiv 0 (\text{mod } m).$ ■

1.2. Gredzeni

Par *gredzenu* sauc kopu R, kurā ir uzdotas divas bināras operācijas

$$(x, y) \mapsto x + y, (x, y) \mapsto xy,$$

kas apmierina šādas īpašības:

- $(R, +)$ ir komutatīva grupa (asociativitāte, neitrālais elements 0, inversais elements, komutativitāte),
- operācija $\cdot$ ir asociatīva,
- ir spēkā kreisā un labā distributīvās īpašības: $a(b + c) = ab + ac, (a + b)c = ac + bc$.

Gredzenu sauc par komutatīvu, ja operācija $\cdot$ ir komutatīva.

Gredzenu sauc par *gredzenu ar vieninieku*, ja eksistē netrālais elements 1 attiecībā uz reizināšanas operāciju: $x \cdot 1 = 1 \cdot x = x$.

Gedzena elementu sauksim par *(multiplikatīvi) invertējamu*, ja tam eksistē labais un kreisais inversais elements attiecībā uz reizināšanu.

Komutatīvu gredzenu sauc par *lauku*, ja visi nenulles elementi ir invertējami.

1.1. piezīme. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ar saskaitīšanas un reizināšanas operācijām ir komutatīvi gredzeni ar vieninieku. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ir lauki.

1.3. teorēma.
$\forall\, m \in \mathbb{Z}, m \geq 2$ $(\mathbb{Z}_m, +, \cdot)$ ir komutatīvs gredzens ar vieninieku.

PIERĀDĪJUMS
Atlikumu klašu saskaitīšana un reizināšana ir asociatīva un komutatīva.

Ir spēkā distributīvā īpašība. $1 \in \mathbb{Z}_m$ ir neitrālais elements attiecībā uz saskaitīšanu. ■

1.2. piezīme. $\mathbb{Z}_m$ ir lauks $\iff$ $m \in \mathbb{P}$, apzīmē kā $\mathbb{F}_p$ vai $GF(p)$.

2. 6.mājasdarbs

2.1. Obligātie uzdevumi

6.1 Atrast visas apakšgrupas atlikumu aditīvajai grupai $(\mathbb{Z}_6, +)$.

6.2 Gredzena elementu a sauc par *idempotentu*, ja $a^2 = a$. Gredzena elementu a sauc par *nilponentu*, ja $a^k = 0$ kādam $k \in \mathbb{N}$. Atrast visus idempotentos un nilpotentos elementus gredzenā $\mathbb{Z}_{12}$.

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

6.3 $G = (\mathbb{Z}, +)$. Vai eksistē tādas apakšgrupas $A \neq \{0\}$ un $B \neq \{0\}$, ka $G = A \oplus B$?

6.4 Doti m, $a \in \mathbb{Z}_m$. Ar ko ir vienāda a kārta? (Par komutatīvas grupas G elementa g *kārtu* sauc mazāko $n \in \mathbb{N} \cup \{0\}) : n \cdot a = 0$).