2 paskaita

Grupių pavyzdžiai:

1 pvz. Nagrinėsime ~~A~~ ~~aibę~~ ~~ir~~ visų $n \times n$ matricų su nenuliniu determinantu aibę. Ją pažymėsime $GL_n(\mathbb{R})$.

Iš tiesinės algebros kurso žinome, kad jei $\det A \neq 0$, $\det B \neq 0 \Rightarrow \det AB \neq 0$. Taigi, jei $A, B \in GL_n(\mathbb{R}) \Rightarrow AB \in GL_n(\mathbb{R})$. Toliau, turime $(AB)C = A(BC)$ ir egzistuoja toks išskirtinis elementas E, kad $AE = EA = A$. Be to, kiekviena tokia matrica turi atvirkštinę A^{-1}, kuriai teisingos lygybės

$$AA^{-1} = A^{-1}A = E.$$

Aibė $GL_n(\mathbb{R})$, nagrinėjama kartu su binariąja operacija (kompozicijos dėsniu) $A * B = AB$ yra vadinama pilnąja tiesine n-tojo laipsnio grupe virš $\mathbb{R}$.

Jei nagrinėsime visų $n \times n$ matricų aibę (ją žymėsime $(M_n(\mathbb{R}), \cdot, E)$), matysime, kad tai monoidas. Tada $GL_n(\mathbb{R}) \subset M_n(\mathbb{R})$ ir $GL_n(\mathbb{R})$ yra to monoido pomonoidis (dalinis monoidas). Kartu matome, kad aibėje $GL_n(\mathbb{R})$ apibrėžta turtingesnė algebrinė struktūra – ~~grupė~~ tai yra grupė.

Grupė, kurioje $\cdot$ operacija komutatyvi yra vadinama Abelio grupe. Matome, kad $GL_n(\mathbb{R})$ nėra Abelio grupė.

Tegul G – grupė.

<u>Apibrėžimas</u>. Poaibis $H \subset G$ yra vadinamas grupės G pogrupiu, jeigu $e \in H$, $h_1, h_2 \Rightarrow h_1 \cdot h_2 \in H$ ir $h \in H \Rightarrow h^{-1} \in H$. Pogrupis $H \subset G$ vadinamas tikriniu, jeigu $H \neq \{e\}$ ir $H \neq G$.

2 pvz. Pilnojoje tiesinėje grupėje $GL_n(\mathbb{R})$ nagrinėsime poaibį $SL_n(\mathbb{R})$, kurį sudaro $n \times n$ matricos, kurių determinantas lygus 1.

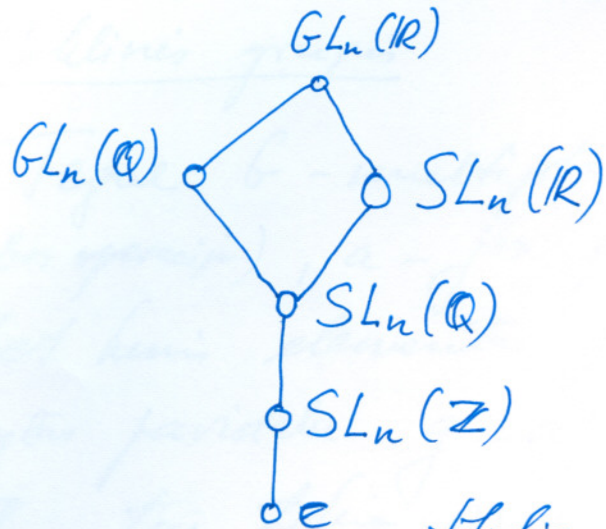
$$SL_n(\mathbb{R}) = \{ A \in GL_n(\mathbb{R}) \mid \det A = 1 \}$$

Aišku, kad $E \in SL_n(\mathbb{R})$. Iš determinantų teorijos žinome, kad

$$\det A = 1,\ \det B = 1 \Rightarrow \det AB = 1$$
$$\det A^{-1} = (\det A)^{-1} = 1$$

Todėl $SL_n(\mathbb{R})$ – grupės $GL_n(\mathbb{R})$ pogrupis. Jis vadinamas specialiąja tiesine laipsnio n grupe virš $\mathbb{R}$. Ją dar vadina unimoduliarine grupe (nors pastarajai kartais priskiriamos matricos, kurių determinantas lygus ± 1.

Tiesinių grupių virš skirtingų skaičių aibių (kūnų) tarpusavio ryšius galima pavaizduoti tokia schema:



, tiksliau, E - vienetinė matrica

3 pvz. Jei anksčiau nagrinėtuose pavyzdžiuose tarsime, kad $n=1$, gausime <u>multiplikacines</u> grupes

$$\mathbb{R}^* = \mathbb{R}\setminus\{0\} = GL_1(\mathbb{R}), \quad \mathbb{Q}^* = \mathbb{Q}\setminus\{0\} = GL_1(\mathbb{Q}),$$

t.y. nenulinių realiųjų ar racionaliųjų skaičių aibes su grupine sandaugos operacija. Tos grupės yra begalinės. Jei dabar imsime $GL_1(\mathbb{Z})$, tai, kadangi aibėje $\mathbb{Z}$ tik du elementai turi atvirkštinius, t.y. 1 ir -1, tai $GL_1(\mathbb{Z}) = \{\pm 1\}$. Be to $SL_1(\mathbb{R}) = SL_1(\mathbb{Q}) = SL_1(\mathbb{Z}) = 1$. Taigi, tos grupės yra trivialios (susideda iš vieno elemento).

Tačiau kai $n=2$, grupė $SL_2(\mathbb{Z})$ jau yra begalinė. Jai priklauso visos matricos

$$\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ m & 1 \end{bmatrix} \quad \begin{bmatrix} m & m-1 \\ 1 & 1 \end{bmatrix}, \quad m \in \mathbb{Z}$$

Paminėsime dar begalines <u>adicines</u> grupes:

$(\mathbb{R}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{Z}, +, 0)$.

Cikliniės grupės

Tegul G – multiplikacinė grupė (t.y. su daugybos operacija), a – jos fiksuotas elementas. Jei bet kuris elementas $g \in G$ gali būti užrašytas pavidalu $g = a^n$ prie tam tikro $n \in \mathbb{Z}$, tai tokia grupė žymima $\langle a \rangle$, t.y. $G = \langle a \rangle$ ir vadinama ciklinė grupe. Sakoma, kad a yra jos sudaromoji, arba kad grupę G generuoja jos elementas a. Analogiškai ciklinė grupė apibrėžiama adiciniu atveju:

$$\langle a \rangle = \{ na \mid n \in \mathbb{Z} \}$$

Iš apibrėžimo neseka, kad visi a^n – skirtingi. Toliau sutarsime žymėti $(a^{-1})^k = a^{-k}$ ir įrodysime tokį teiginį.

Teorema. Kokie bebūtų $m, n \in \mathbb{Z}$,

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}$$

Įrodymas. Indukcija pagal m arba pagal n.

Paprasčiausias ciklinės grupės pavyzdys – tai adicinė sveikųjų skaičių grupė $(\mathbb{Z}, +, 0)$, generuota elemento 1 arba -1. Galima įrodyti, kad matrica $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ generuoja grupėje $SL_2(\mathbb{Z})$ begalinį ciklinį pogrupį.

Apibrėžimas. Grupės elementų skaičius (aibės galia) yra vadinamas grupės eile.

1.4. Žiedai.

Apibrėžimas. Tegul K – netuščia aibė, kurioje įvestos dvi binariosios algebrinės operacijos $+$ (sudėtis) ir $\cdot$ – daugyba, tenkinančios šias sąlygas:

K1) $(K, +)$ – Abelio grupė

K2) $(K, \cdot)$ – pusgrupė

K3) sudėtis ir daugyba susieto distributyvumo dėsniu

$$(a+b)c = ac+bc \quad , \quad c(a+b) = ca+cb$$

visiems $a, b, c \in K$.

Tokiu atveju algebra $(K, +, \cdot)$ vadinama *žiedu*.

Algebrinė struktūra $(K, +)$ vadinama žiedo *adicine grupe*, o $(K, \cdot)$ – jo *multiplikacine pusgrupe*. Jei $(K, \cdot)$ – monoidas, tai sakome, kad $(K, +, \cdot)$ – *žiedas su vienetu*.

Žiedo vienetinį elementą priimta žymėti tiesiog 1. Gali būti toks žiedo apibrėžimas, kuriame K2 nėra, t.y., daugybos operacija apibrėžta, bet nėra asociatyvi. Tokiu atveju kalbama apie *neasociatyvųjį žiedą*. Toliau čia mes nagrinėsime tik asociatyviuosius žiedus.

Žiedo K ~~požiedis~~ poaibis vadinamas <u>požiedžiu</u>, jeigu

$$x, y \in L \Rightarrow x-y \in L,\ xy \in L,\ \text{t.y.},$$

jei L - adicinės grupės pogrupis ir multiplikacinės ~~pusgrupės~~ popusgrupis.

Žiedas vadinamas <u>komutatyviuoju</u>, jeigu $xy=yx \quad \forall x,y \in K$. (Tačiau komutatyvieji žiedai nevadinami Abelio žiedais).

<u>Žiedų pavyzdžiai:</u>

1 pvz. $(\mathbb{Z}, +, \cdot)$ - sveikųjų skaičių žiedas su įprastinėmis sudėties ir daugybos operacijomis. Aibė sveikųjų skaičių pavidalo $m\mathbb{Z}$, t.y. skaičių, kurie dalinasi iš m, sudaro žiedo $(\mathbb{Z}, +, \cdot)$ požiedį. Tokiuose požiedžiuose, kai $m>1$, vienetų nėra. Žiedų su vienetais pavyzdžiai yra taip pat $\mathbb{Q}$ ir $\mathbb{R}$. Turime žiedo $\mathbb{R}$ požiedžių grandinėlę $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$

2 pvz. $n \times n$ matricų visų realiųjų skaičių žiedas $M_n(\mathbb{R})$. Šis žiedas nekomutatyvus, bet turi vienetą - vienetinę matricą E.

3 pvz. Funkcijų žiedas

Tegul X – bet kuri netuščia aibė, K – bet kuris žiedas. Tegul $K^X = \{X \to K\}$ – visų funkcijų (atvaizdavimų) $f: X \to K$ aibė. Apibrėšime joje dvi binariąsias operacijas $f+g$ ir fg tokiu būdu (pataškiui):

$$(f+g)(x) = f(x) \oplus g(x)$$

$$(fg)(x) = f(x) \odot g(x),$$

čia $\oplus$ ir $\odot$ – sudėtis ir daugyba žiede K.

Čia galima prisiminti pavyzdžių iš matematinės analizės, pvz. jei $X = \mathbb{R}$, $K = \mathbb{R}$ funkcijų tg ir sin sandauga

$$\mathrm{tg} \cdot \sin : x \to \mathrm{tg}\, x \cdot \sin x$$

Galima įsitikinti, kad K^X tenkina visas žiedo aksiomas.

Jo požiedžiai $\mathbb{R}^{[0,1]}$, $\mathbb{R}^{[0,1]}_{bounded}$, $\mathbb{R}^{[0,1]}_c$ – tolydžių f-jų, $\mathbb{R}^{[0,1]}_d$ – visų tolydžiai diferencijuojamų f-jų požiedis.

Daugelis žiedų savybių išplaukia iš atitinkamų jo adicinių grupių ir multiplikacinių pusgrupių savybių. Kitos savybės panašios į sveikųjų skaičių savybes. Paminėsime kai kurias

1) $a\cdot 0 = 0\cdot a = 0 \quad \forall\, a\in K$

Įrodymas:

$$a+0=a \Rightarrow a(a+0)=a\cdot a \Rightarrow a^2+a\cdot 0=a^2 \Rightarrow$$

$$a^2+a\cdot 0 = a^2+0 \Rightarrow a\cdot 0=0$$

Analogiškai $0\cdot a=0$

2) $0\neq 1$

Įrodymas. Jei yra priešingai, t.y., jei $0=1$, tai $a=a\cdot 1=a\cdot 0=0$, t.y. visi $a\in K$ lygūs 0, t.y. K susideda iš vienintelio elemento 0.

3) $(-a)\cdot b = a(-b) = -ab$

Įrodymas.

$$0=a\cdot 0=a(b-b)=ab+a(-b)\Rightarrow a(-b)=-(ab)$$

4) Kadangi $-(-a)=a$, tai $(-a)(-b)=ab$, taip pat $(-1)(-1)=1$, $-a=(-1)a$

5) Bendrasis distributyvumo dėsnis

$$(a_1+a_2+\dots+a_n)(b_1+b_2+\dots+b_m)=\sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$$

6) jei $n\in\mathbb{Z}$, $a,b\in K$, tai

$$n(ab)=(na)b=a(nb)$$

7) Niutono binomas žiede. Bet kuriems $a, b \in K$, K - komutatyvusis žiedas, turime
$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} \quad \left(\text{arba } \sum_{i=0}^{n} C_n^i a^i b^{n-i}\right)$$