Paskaitų ciklas apie kūnus
Turinys

Literatūra.

1. K.Bulota, P. Survila. Algebra ir skaičių teorija.
2. B.L.Van Der Waerden. Algebra.
3. R.Grigutis. Baigtinės algebrinės struktūros.

Išankstinės žinios.

Tai algebros paskaitų kursas skirtas MIF informatikos specialybės magistrams. Šiose paskaitose dėstomi kūnų plėtinių teorijos klausimai, išsprendžiantys algebrinių lygčių išsprendžiamumo radikalais klausimą, taip pat nemažai klasikinių brėžimo tik skriestuvu ir liniuote uždavinių. Nors paskaitose stengtasi pateikti visus reikalingus apibrėžimus ir naudojamų teiginių formuluotes, reiktų, kad klausytojas būtų susipažinęs su bendruoju algebros kursu, skaitomu MIF informatikams pirmąjame ir antrąjame semestruose, o taip pat diskretinės matematikos(antrasis kurso pavadinimas: diskretinės algebrinės struktūros) kursu, skaitomu MIF informatikams trečiąjame semestre. Dabar norėtųsi priminti tas savokas ir teiginius iš minėtų kursų, kuriais dažniausiai remsimės savo tolesniuose samprotavimuose.

$\odot$ *GRUPĖS*

•Grupės apibrėžimas ir pavyzdžiai.

Liekanų klasių adicinė grupė Z_n,primityviųjų klasių multiplikacinė grupė U_m, $|U_m| = \varphi(m)$.

Vieneto šaknų multiplikacinė grupė $U(n)$.

• Homomorfizmas ir izomorfizmas.

• Normalusis pogrupis

Apibrėžimas. Grupės A pogrupis vadinamas normaliuoju, jeigu visiems $a \in A$

$$a \cdot B = B \cdot a$$

Normaliojo pogrupio požymis: $a \cdot B \cdot a^{-1} \subseteq B$.

Svarbiausia normaliųjų pogrupių savybė yra ta, kad grupės A sluoksnių normaliojo pogrupio B atžvilgiu aibėje (žymuo A/B) galima apibrėžti grupės struktūrą.

Beto, bet kurio grupių homomorfizmo branduolys yra normalusis pogrupis ir bet kuris normalusis pogrupis yra homomorfizmo branduolys:

Teorema(homomorfizmų teorema grupėms). Tegu $f : A \to B$ yra grupių homomorfizmas. Tada egzistuoja vienintėlis homomorfizmas $\bar{f} : A/\ker f \to B$, kurio dėka diagrama

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \searrow_{p} & & \nearrow_{\bar{f}} \\ & A/\ker f & \end{array}$$

yra komutatyvi, t.y. $f = \bar{f} \cdot p$, $\bar{f}$ yra grupių $A/\ker f$ ir $f(A)$ izomorfizmas, o $p \Leftrightarrow$ siurjektyvusis homomorfizmas.

• Izomorfizmas $U(n) \approx Z_n$, $\alpha\left(\varepsilon^k\right) = k \,(\mathrm{mod}\, n)$

• Ciklinės grupės (begalinės c.g. izomorfiškos Z, baigtinės - Z_n):

Funkcijos $\varphi_n : Z_n \to \langle a \rangle_n, \varphi_n\left(\bar{k}\right) = a^k$ ir $\varphi_0 : Z \to \langle a \rangle, \varphi_0(k) = a^k$ yra izomorfizmai.

• simetrinė grupė S_n; alternuojanti grupė A_n;
Dar vienas izomorfizmas $S_n/A_n \approx C_2$.

• A.Cayley teorema apie tai, kad kiekviena baigtinė grupė yra izomorfiška simetrinės grupės pogrupiui.

Apibrėžimas. *Tegu* π *,* ρ *- keitiniai aibėje* V*. Keitinių sandauga* $\sigma = \pi \circ \rho$ *vadinsime keitinį, apibrėžtą lygybe*

$$\sigma(v_i) = \rho(\pi(v_i)), \ \forall v_i \in V.$$

Pastebėsime, kad taip apibrėžta sandauga yra funkcijų kompozicija. Ji nėra komutatyvi.

Pavyzdys. Kai $\pi = \begin{pmatrix} v_1 & v_2 & v_3 \\ v_3 & v_2 & v_1 \end{pmatrix}$, o $\rho = \begin{pmatrix} v_1 & v_2 & v_3 \\ v_3 & v_1 & v_2 \end{pmatrix}$, tai $\pi \circ \rho = \begin{pmatrix} v_1 & v_2 & v_3 \\ v_2 & v_1 & v_3 \end{pmatrix} \neq \begin{pmatrix} v_1 & v_2 & v_3 \\ v_1 & v_3 & v_2 \end{pmatrix} = \rho \circ \pi$.

Tačiau, keitinio π kanoniniame skaidinyje esantys nepriklausomi ciklai komutuoja poromis.

Teiginys. *Tegu S(V) - visų keitinių aibė aibėje* V*. Tada* $(S(V), \circ)$ *- grupė.*

Teorema(A.Cayley). *Tegu* $(G, \cdot)$ *yra baigtinė grupė, turinti* n *elementų. Tada egzistuoja funkcija*

$$f : G \to S(G) = S_n,$$

tenkinanti savybes

$$\begin{gathered} f(g_1) = f(g_2) \Longleftrightarrow g_1 = g_2, \text{ (injektyvumas)} \\ f(g \cdot h) = f(g) \circ f(h). \text{ (homomorfizmas)} \end{gathered}$$

Įrodymas.$\forall a \in G$ konstruojame keitinį $L_a : G \to G$, $L_a(g) = g \cdot a$. Taigi $L_a \in S_n$.

Turime aibių lygybę

$$\{g_1, g_2, ..., g_n\} = \{g_1 \cdot a, g_2 \cdot a, ..., g_n \cdot a\} = G.$$

Turime

1) $L_a \in S_n$,

2) $L_a^{-1} = L_{a^{-1}}$,

3) $L_{a\cdot b}(g) = g\cdot(a\cdot b) = (g\cdot a)\cdot b = L_b(L_a(g)) = (L_a \circ L_b)(g)$, taigi, $L_{a\cdot b} = L_a \circ L_b$.

Gavome, kad keitiniai $L_{g_1}, L_{g_2}, ..., L_{g_n}$ sudaro grupę $H \subset S(G) = S_n$.

Funkcija $f : G \to H \subset S_n$ apibrėžta formule $f(g) = L_g$.

Įrodyta.

Pavyzdys1. Rombo simetrijų grupės įdėjimas į simetrinę grupę.

Tegu $G = \{e, a, b, c\}$ - rombo simetrijų grupė. Čia e ir a posūkiai atitinkamai $0°$ ir $180°$ kampu, o b ir c simetrijos įstrižainių atžvilgiu. Tada veiksmų lentelė šioje grupėje

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

ir $L_e = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix} = id$, $L_a = \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix} = (ea)(bc)$, $L_b = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix} = (eb)(ac)$, $L_c = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix} = (ec)(ab)$.

Pavyzdys2. Ciklinės grupės (pvz. n-ojo laipsnio šaknų iš 1 multiplikacinės grupės) įdėjimas į simetrinę grupę.

Tegu ε - primityvioji n-ojo laipsnio šaknis iš vieneto. Tada visos n-ojo laipsnio šaknis iš vieneto yra primityviosios šaknies ε laipsniai : $\varepsilon, \varepsilon^2, ..., \varepsilon^{n-1}, \varepsilon^n = 1$ ir

$$L_\varepsilon = \begin{pmatrix} \varepsilon & \varepsilon^2 & \varepsilon^3 & \cdots & \varepsilon^{n-1} & \varepsilon^n \\ \varepsilon^2 & \varepsilon^3 & \varepsilon^4 & \cdots & \varepsilon^n & \varepsilon \end{pmatrix}$$
$$L_{\varepsilon^2} = \begin{pmatrix} \varepsilon & \varepsilon^2 & \varepsilon^3 & \cdots & \varepsilon^{n-1} & \varepsilon^n \\ \varepsilon^3 & \varepsilon^4 & \varepsilon^5 & \cdots & \varepsilon^{n+1} & \varepsilon^{n+2} \end{pmatrix}$$

ir t.t. Pavyzdžiui, kai $n = 6$ turime reiškimą keitiniais:

$$L_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} = (123456)$$

$$L_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} = (135)(246)$$
$$L_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} = (14)(25)(36)$$
$$L_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix} = (153)(264)$$
$$L_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (165432)$$
$$L_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = id.$$

$\odot$ *ŽIEDAI.*

- Žiedo apibrėžimas ir pavyzdžiai :
- polinomų žiedas ;
- Idealas, $K[x]$ - pagrindinių idealų sritis,
- Faktoržiedis ir homomorfizmų teorema žiedams.

Teorema (homomorfizmų teorema žiedams).
Jeigu $\varphi : R \to S$ yra žiedo R homomorfizmas **ant** žiedo S, tai $Ker\ \varphi$ - idealas ir $S \approx R/_{Ker\,\varphi}$.

Jeigu $J \subset R$ yra idealas, tai $\phi : R \to R/_J$, $\phi(a) = a + J$ yra žiedų homomorfizmas, kurio branduolys $Ker\ \phi = J$.

Teorema. Tegu $f(x) \in K[x]$. Faktoržiedis $K[x]/(f)$ yra kūnas tada ir tik tada, kai $f \Leftrightarrow$neredukuojamas virš kūno K polinomas.

$\odot$ *KŪNAI*

- Kūno apibrėžimas ir pavyzdžiai:
- kūno charakteristika ir pirminai kūnai.
- Baigtiniai kūnai.
- Racionaliųjų funkcijų kūnas $K(x)$.

Apibrėžimas.Tegu $K \Leftrightarrow$kūnas. Trupmenų aibėje $\left\{ \dfrac{f(x)}{g(x)} | f(x), g(x) \in K[x], g(x) \not\equiv 0 \right\}$, kurioje $\dfrac{f_1}{g_1} = \dfrac{f_2}{g_2} \Longleftrightarrow f_1 g_2 = f_2 g_1$ (tai ekvivalentumo sąryšis, įrodyti!), apibrėžus dvi operacijas: $\dfrac{f_1}{g_1} + \dfrac{f_2}{g_2} = \dfrac{f_1 g_2 + f_2 g_1}{g_1 g_2}$

ir $\dfrac{f_1}{g_1} \cdot \dfrac{f_2}{g_2} = \dfrac{f_1 \cdot f_2}{g_1 \cdot g_2}$ gauname racionaliųjų funkcujų kūną $K\left(x\right)$

$\odot$ *VEKTORINĖS ERDVĖS.*

•Vektorinė erdvė: apibrėžimas, tiesiška vektorių priklausomybė, tiesinis apvalkalas, bazė.

• Faktorerdvė

• Tiesinis atvaizdis, jo Im ir Ker .

• Baigtinio matavimo vektorinių erdvių izomorfizmas aritmetiniai erdvei.

• Izomorfizmo teorema vektorinėms erdvėms.

Teorema apie izomorfizmą. *Tegu* $\mathcal{A} : U \to V \Leftrightarrow$ *tiesinis atvaizdis. Poerdvis* $im\mathcal{A}$ *izomorfinis faktorerdvei* $U/\ker\mathcal{A}$.

Įrodymas. Apibrėžkime funkciją $i : U/\ker\mathcal{A} \to im\mathcal{A}$ formule $i\left(\bar{u}\right) = \mathcal{A}\left(u\right)$. Parodysime, kad tai ir yra ieškomas izomorfizmas.

Funkcija i yra tiesinis atvaizdis:

$i\left(a_1\bar{u}_1 + a_2\bar{u}_2\right) = i\left(\overline{a_1u_1 + a_2u_2}\right) = \mathcal{A}\left(a_1u_1 + a_2u_2\right) = a_1\mathcal{A}\left(u_1\right) + a_2\mathcal{A}\left(u_2\right) = a_1 i\left(\bar{u}_1\right) + a_2 i\left(\bar{u}_2\right)$.

Tiesinis atvaizdis i yra monomorfizmas:

$i\left(\bar{u}\right) = 0 \Leftrightarrow \mathcal{A}\left(u\right) = 0 \Leftrightarrow u \in \ker\mathcal{A} \Leftrightarrow \bar{u} = \bar{0}$.

Tiesinis atvaizdis i yra epimorfizmas:

su kiekvienu $v \in im\mathcal{A}$ egzistuoja $u \in U$, kad $\mathcal{A}\left(u\right) = v$, t.y. $i\left(\bar{u}\right) = \mathcal{A}\left(u\right) = v$.

Įrodyta.

Teorema apie izomorfizmą dažnai reiškiama tokia komutatyvia diagrama:

$$\begin{array}{ccc} U & \overset{\mathcal{A}}{\Leftrightarrow} & V \\ \searrow^{p} & & {}^{i}\nearrow \\ & U/\ker\mathcal{A} & \end{array},$$

čia $p\left(u\right) = \bar{u}$, $i\left(\bar{u}\right) = \mathcal{A}\left(u\right)$, taigi, $\mathcal{A}\left(u\right) = i\left(p\left(u\right)\right)$.

Pastaba. Paskutiniųjų teoremų dėka matome, kaip galėtume mąstyti faktorerdvę. Kiekvienam vektorinės erdvės poerdviui galime apibrėžti tiesinį atvaizdį, kurio vaizdas yra šis poerdvis, o branduolys - poerdvio tiesioginys papildinys. Pagal teoremą apie izomorfizmą faktorerdvę galime mąstyti kaip poerdvio tiesioginį papildinį.

Teorema. *Vektorinė erdvė* U, k ,$\dim U = n$, *yra izomorfinė aritmetinei erdvei* k_n .

Įrodymas. Tegu vektorių sistema $v_1, ..., v_n \Leftrightarrow$ vektorinės erdvės U bazė.

Apibrėžkime tiesinį atvaizdį $\mathcal{A} : k_n \to U$ formule

$$\mathcal{A}\begin{pmatrix} a_1 \\ \cdots \\ a_n \end{pmatrix} = (v_1, ..., v_n)\begin{pmatrix} a_1 \\ \cdots \\ a_n \end{pmatrix}.$$

$im\mathcal{A} = U$, nes sistema $v_1, ..., v_n \Leftrightarrow$ generuojanti erdvę U sistema.

$\ker \mathcal{A} = 0$, nes sistema $v_1, ..., v_n \Leftrightarrow$ tiesiškai nepriklausoma sistema.

Gavome, kad U yra izomorfinė aritmetinei erdvei k_n.

Įrodyta.

Pastaba. $U \approx k_n$, bet šis izomorfizmas nėra kanoninis,- jis priklauso nuo bazių.

Paskutinioji teorema rodo, kad baigtinės dimensijos vektorinę erdvę galima reikšti aritmetinės erdvės elementais, t.y. stulpeliais: $\alpha_1 u_1 + \cdots + \alpha_n u_n \to \begin{pmatrix} \alpha_1 \\ \cdots \\ \alpha_n \end{pmatrix}$.

.